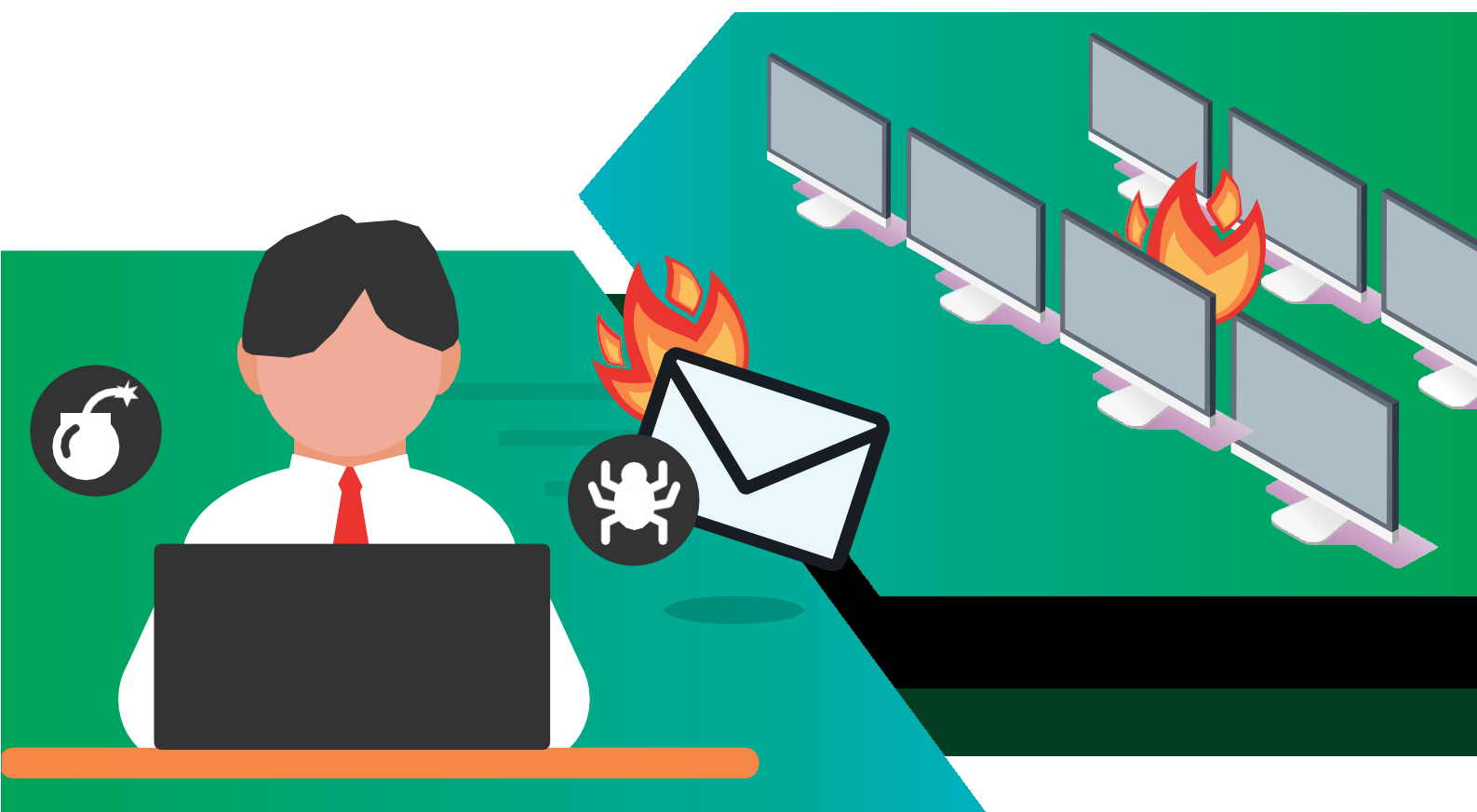


標的型攻撃メール訓練サービス



情報セキュリティ対策は、人で始まり人で終わる



■ 標的型攻撃メールとは

標的型攻撃メールとは、情報や金銭の窃取を目的として特定の組織に送られるウイルスメールのことです。テレワークが進むなか、標的型攻撃メールは増加の一途を辿り、その巧妙さも増えています。被害の主な原因は、不十分なセキュリティ意識と知識不足です。メールを受信した時に、いつもとの違いに気づき、慌てずに上司やセキュリティ担当者に相談するなど適切な対応を取ることが大切です。

大手企業でも中小企業でもメールサーバーからメールアドレスを含むメール情報を窃取され、従業員を装った第三者からの不審なメールの発信が確認されています。

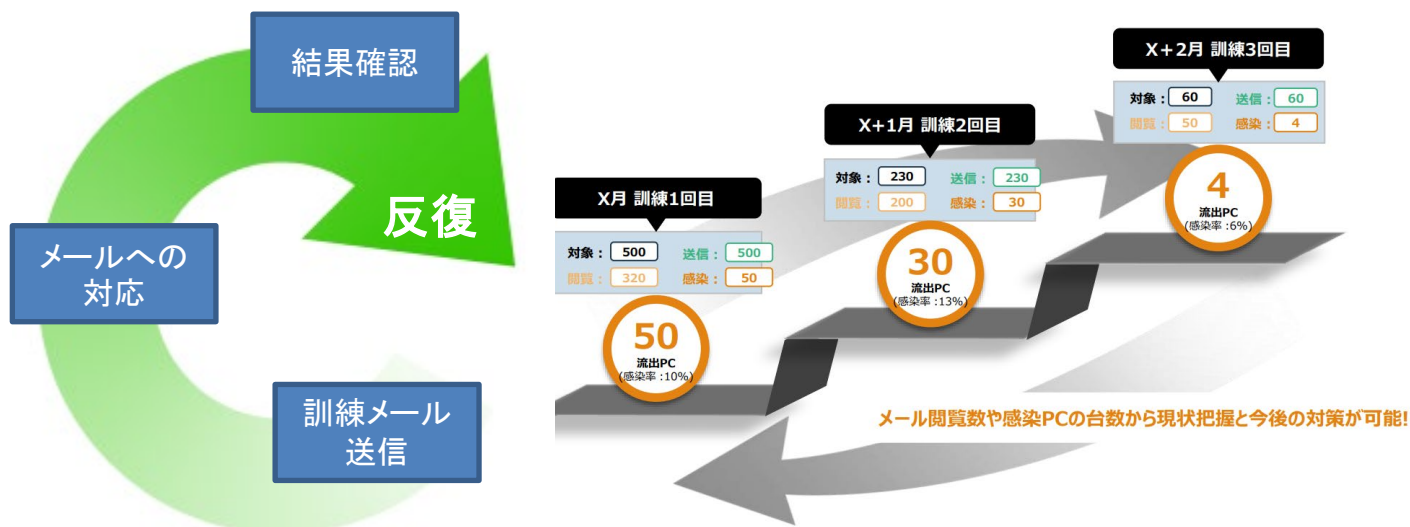
標的型攻撃メールへの対応力を身に付けて頂くためには、普段から定期的に訓練を行う必要があります。反復訓練を行うことで、対応力の定着度は大幅にUPします。



必要なのは
反復訓練！

■ 反復訓練の効果

訓練は、一度行っただけでは、高い効果を期待できません。継続して、定期的に、何度も繰り返すことが、大きな効果を生み出します。「添付ファイルタイプ」、「フィッシング誘導タイプ」など、さまざまな訓練を、MudFixの訓練無制限プランで、何度も繰り返し替えることにより、いざという時の対応力を養っていただきます。



■MudFixとは

MudFixとは必要な標的型攻撃を模した訓練メールに従業員・職員の方々に送信することで、標的型攻撃への対応力を身に着けて頂くための予防訓練サービスです。
MudFixでは、4ステップで訓練を実施します。

検証・準備

自社検証環境確認

- ・5ライセンス無料トライアル
- ・自社環境で課題洗出し
- ・有償申込でそのまま利用

メール環境設定

- ・受信サーバ、ポート
- ・プロトコル、タイムアウト

対象者、タグ管理

- ・個別やCSV一括登録
- ・タグ作成、変更
- ・対象者のタグ指定

テンプレート作成

テンプレートの種類

警告、模擬悪性、実態調査、フィッシング誘導
添付、リンク&DL、リンク

テンプレートの作成

件名、本文の変更
添付ファイル
警告画面設定

受信テスト

受信サーバでの確認
受信サーバの変更

訓練実施

訓練名と期間設定

訓練名
開始日、終了日
即時送信、期間設定

対象者指定

対象者のタグ指定
複数のタグ指定可能

訓練テンプレート選択

テンプレート選択
リンク先ドメイン種別選択
PCロック画面実行時間

結果確認

ダッシュボード

全体訓練
個別訓練
進行状態確認

感染状態

感染PC、感染ファイル
全体確認、対象者毎確認

報告書

ダウンロード
内容確認

■Point 1. 簡単な訓練設定

訓練設定の手順

簡単な設定ですぐ訓練が可能です。

1. 訓練環境の自動チェック



2. 訓練日程を設定



3. 訓練対象者選定



4. テンプレート選択



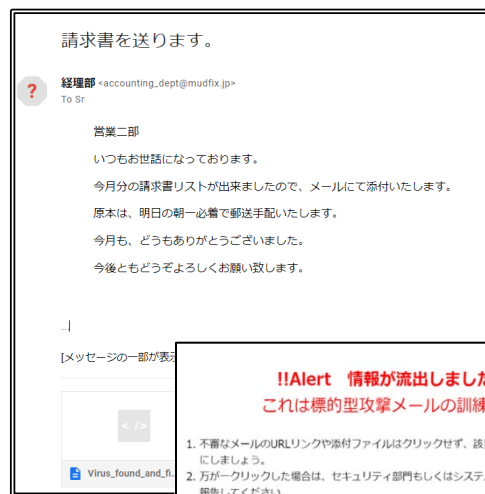
訓練実施



訓練者に届くメールの例

訓練効果を高めるリアルな模擬感染訓練ができます。

全ての訓練									
合計 66個 訓練									
<div>全て選択 訓練履歴</div>									
<div>並び替え フィルタ 検索</div>									
<input type="checkbox"/>	test05192010	2022-05-19 ~ 2022-05-20	1	1	0	0	0	0	-
<input type="checkbox"/>	test0519201923	2022-05-19 ~ 2022-05-20	1	1	0	0	0	0	-
<input type="checkbox"/>	test0519iPhone	2022-05-19 ~ 2022-05-19	2	2	2	2	2	2	-
<input type="checkbox"/>	test1323132	2022-05-19 ~ 2022-05-19	1	1	1	1	1	1	1台
<input type="checkbox"/>	test05190519	2022-05-19 ~ 2022-05-19	10	10	0	0	0	0	なし
<input type="checkbox"/>	test0519	2022-05-19 ~ 2022-05-19	10	1	0	0	0	0	-
<input type="checkbox"/>	test103231323	2022-05-18 ~ 2022-05-18	1	1	1	1	1	1	なし
<input type="checkbox"/>	test23232323	2022-05-18 ~ 2022-05-18	10	3	0	0	0	0	-
<input type="checkbox"/>	test4601	2022-05-18 ~ 2022-05-18	1	1	1	1	1	1	なし
<input type="checkbox"/>	test0516	2022-05-16 ~ 2022-05-18	10	5	0	0	0	0	-







訓練対象者に届く訓練メール

ステータスの反映

ユーザーごとに、「メール送信」「メール閲覧」「ファイルダウンロード」「感染」ステータスを確認できます。

■Point 2. 充実した訓練テンプレート

MudFixは、添付ファイルタイプ(「警告案内」「模擬悪性ファイル」「実態調査」タイプ)の3種類と、フィッシング誘導タイプの、4種類のテンプレートをご用意しております。内容は、エディタにより編集可能です。

	警告案内 最も基本的な訓練類型	<ul style="list-style-type: none">•PC(Windows)にロック画面を表示•訓練対象者は訓練であることを認識•画面を閉じるだけでロック解除
	模擬悪性ファイル 事後対応のための訓練類型	<ul style="list-style-type: none">•PCロック画面を非表示•訓練対象者は訓練であることを認識•別途提供するファイルを実行することでロック解除
	実態調査 実態把握のための訓練類型	<ul style="list-style-type: none">•PCロック画面を非表示•訓練対象者は訓練であることを認識できない•実態把握が目的
	フィッシング誘導 添付ファイル式訓練に慣れた時	<ul style="list-style-type: none">•フィッシングサイトのURLを挿入•個人情報入力ページ作成も可能•訓練対象者へ警告ページを表示

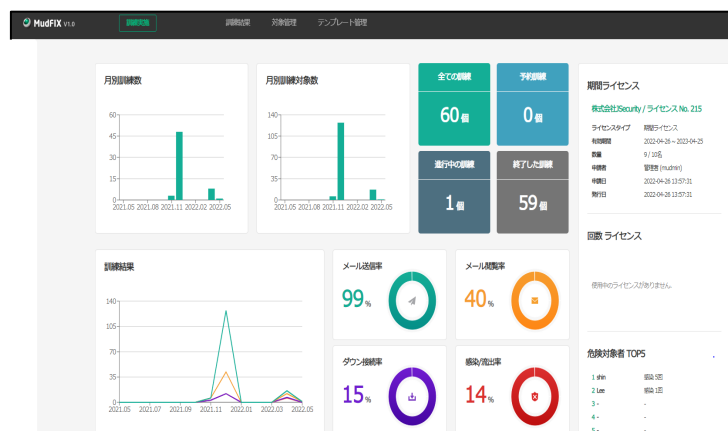
■Point 3. 一目で分かる状況確認

訓練状況は、リアルタイムに把握することが可能です。

ダッシュボードで確認できること

- 個別の詳細な訓練結果
- ご契約ライセンス情報
- 進行中の訓練
- 危険対象者 TOP5
- など

分かりやすいUIでまとめられています。



<Mudfixダッシュボード画面>

■Point 4. 報告書の簡単ダウンロード

訓練実施後に、Excelフォーマットでダウンロードすることが可能です。
全体結果や使用したテンプレート、訓練対象者別の訓練結果、タグ別の訓練結果など、
細かく訓練結果がまとめられているため、次の訓練に向けた計画に役立てることができます。

開発元



株式会社 JSecurity

東京都港区浜松町2-4-1 世界貿易センタービルディング 南館17階

TEL: 03-4567-2823 FAX:03-4567-2824

E-mail : sales - m@jsecurity.co.jp

URL : <https://www.jsecurity.co.jp>

お求めは信頼の