

株式会社サテライトオフィス

---

---

# 標的型攻撃メール対策訓練機能 for MudFix

---

---



全社員の方向けに、標的型攻撃メール対策のトレーニング

## サテライトオフィス・ 標的型攻撃メール対策訓練機能 for Mudfix

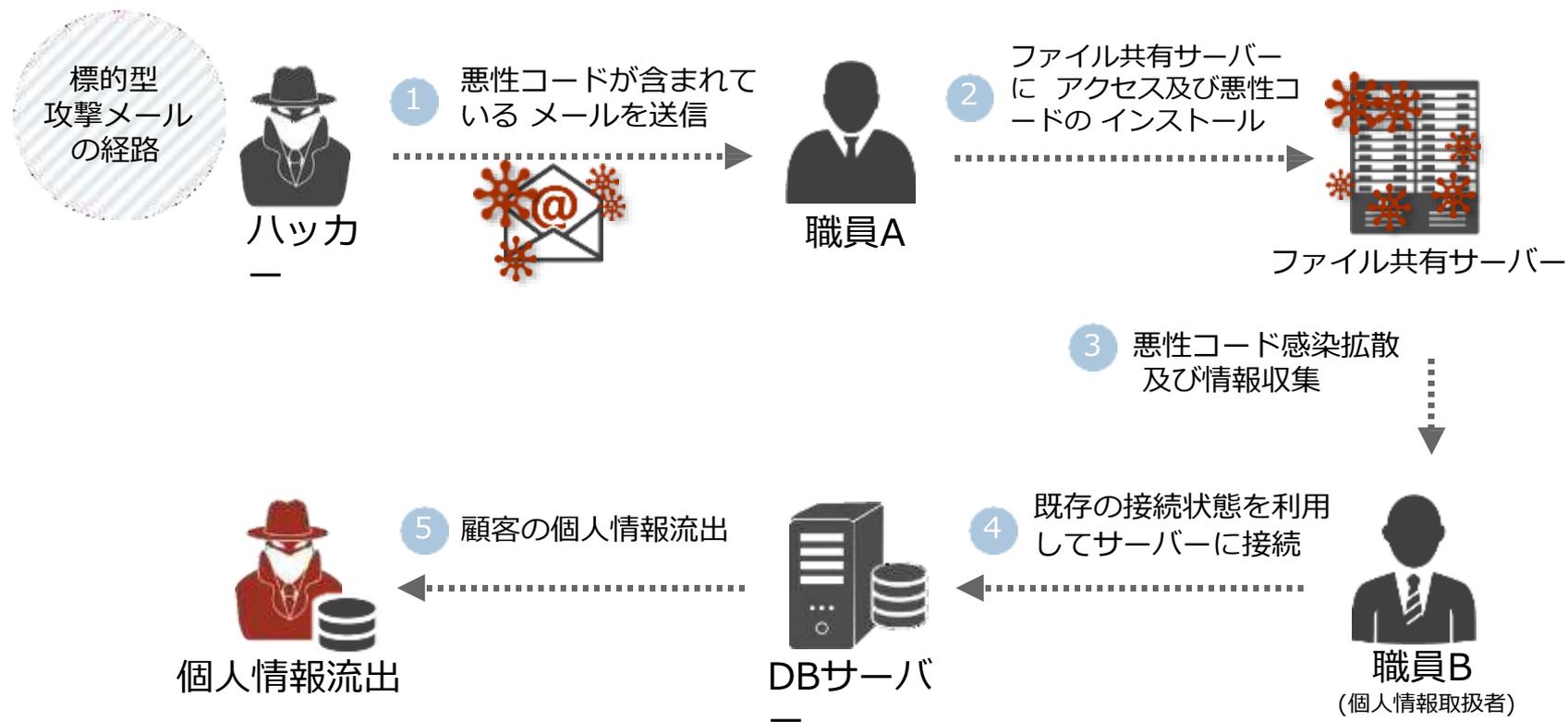


### 標的型攻撃メール対策訓練機能 for Mudfix とは？

全社員の方向けに、標的型攻撃メール対策のトレーニングをする事が可能です！  
疑似メールを送り、見たか？/クリックしたか？/ダウンロードしたか？を確認できます。  
トレーニング回数無制限 / 非常に安価です！

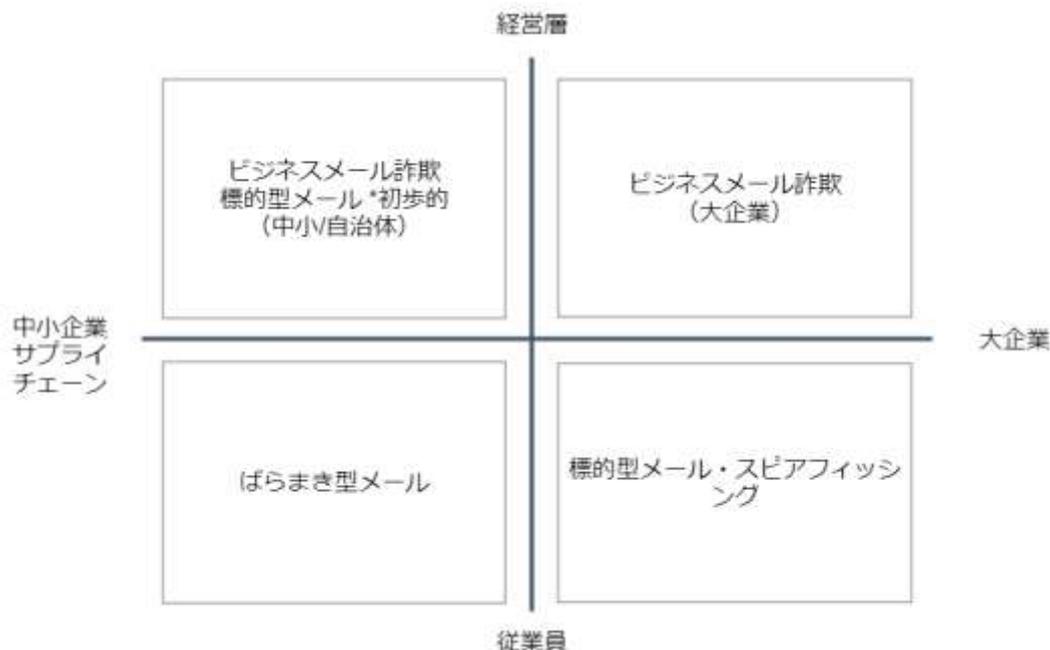
# 標的型攻撃メールとは

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です。



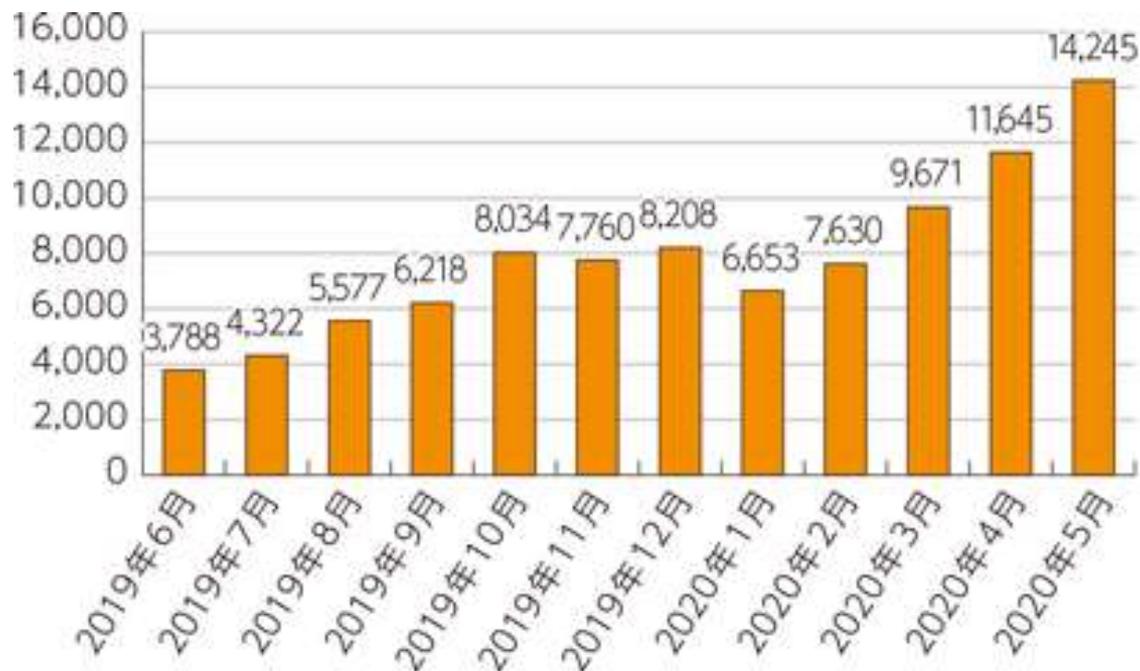
# メールの種類

- **ビジネスメール詐欺**：海外の取引先や自社の経営者層等になりすまして、偽の電子メールを送って入金を促す詐欺
- **ばらまき型メール**：機関・企業の機密情報や個人情報を盗み出すことを目的とし、ウイルスメールを不特定多数の標的に対して送信する攻撃
- **スパイフィッシング**：特定のターゲットをピンポイントで攻撃



# ばらまき型メール件数/フィッシングメール件数の実態

フィッシングの報告件数は2020年1月から5月までにかけて急増しており、2020年5月には14,245件に達しています。また、警察庁によれば、2019年9月からインターネットバンキングに係る不正送金事犯による被害が急増しているとのことであり、被害の多くは、SMS（ショートメッセージサービス）や電子メールを用いて、金融機関を装ったフィッシングサイトへ誘導する手口によるものと考えられるとしています。



(出典) フィッシング対策協議会 (2020) 「2020/05 フィッシング報告状況」を基に作成

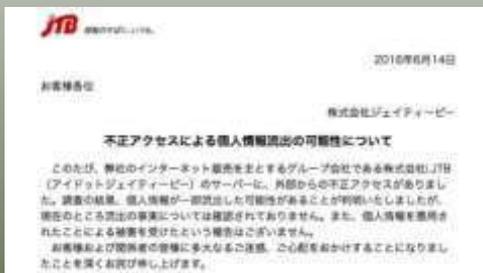
# 標的型攻撃メールの傾向と被害事例

IPAによると、標的型攻撃メールの傾向は、①メール本文のURLや添付ファイルに開かざるを得ない内容 ②これまでに届いたことがない公的機関からのお知らせ ③組織全体への案内 ④心当たりのない決済の配送通知 ⑤IDやパスワードの入力を要求する内容で、ユーザーのウイルス感染を誘導します。

## [事例 1]

### J社 “APT攻撃” 被害

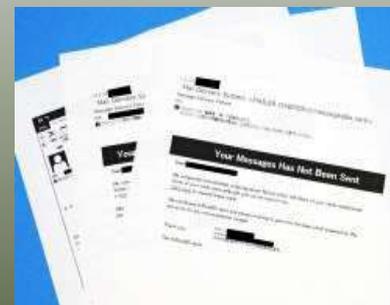
取引先になりすましたEチケット添付メールでマルウェア感染させ793万人分の個人情報流出



## [事例 2]

6大学 “フィッシングメール” 被害  
 1.2万件の個人情報流出

メール本文の偽サイトにクリックするよう誘導し、パスワードの入力を求められる。誤って入力すると犯人に情報が渡る。



(出典) IPA

# 標的型メール攻撃事例：スパイフィッシング

米パイプライン最大手の企業でサイバー攻撃を受けシステムが停止しました。身代金に応じ、4.8億円を支払ったことがわかりました。

パイプライン稼働停止 ダークサイドのサイバー攻撃は日本企業にも

6/5(土) 0:00 配信 5

**Forbes** JAPAN



コロニアル・パイプラインへのサイバー攻撃は市民生活にも影響を及ぼした  
 (ノースカロライナ州フェイエットビル・5月12日) (Photo by Sean Rayford/Getty Images)

米パイプライン最大手のコロニアル・パイプラインが5月7日、サイバー攻撃を受けて稼働停止に追い込まれた。同社は米東海岸の燃料供給の約5割を占める。同社は12日前後から操業を再開したが、稼働停止を受けてガソリン価格が高騰するなど、社会が混乱した。

米紙ウォール・ストリート・ジャーナルによれば、同社のプラント最高経営責任者（CEO）は、ハッカー集団からの身代金要求に応じ440万ドル（約4億8千万円）を支払ったことを認めた。米連邦捜査局（FBI）は、今回の事件はハッカー集団「ダークサイド」による犯行だと断定している。

今回の事件から、日本を含む企業社会が学ばなければいけない教訓とは何なのか。

専門家の間でも、今回の事件に驚きの声が上がった。情報セキュリティ大手トレンドマイクロのセキュリティエバンジェリスト石原龍平氏は「かなり時間を要する攻撃。数日や数週間ですでできる仕事ではない。パイプラインを止めざるを得なくなるほどの被害を与えることは難しい。被害を受けるデータが重要であるほど、警戒も厳しくなる」と指摘する。

トレンドマイクロによれば、ダークサイドはまず、標的とした企業のシステムの弱い場所や、関係者へのフィッシングメールなどを使って侵入する。

サイバー攻撃で、ドイツの製鋼所が甚大な被害を被っていた

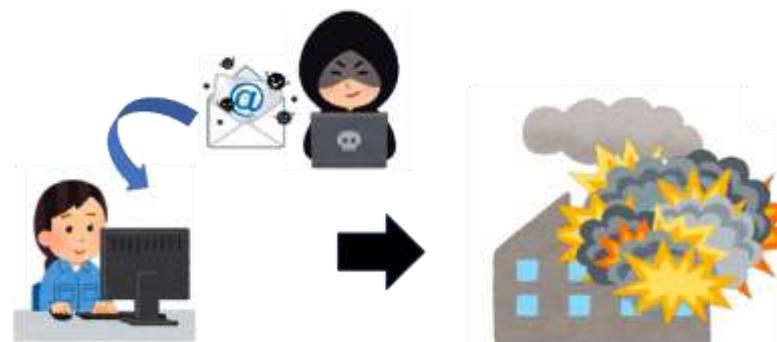
2015年09月01日 (火) 17時30分

いいね! 1 コメント 0 ツイート 0 共有 0



政府機関が認めた製鋼システムへのサイバー攻撃として2週目に Ina Fassbender-REUTERS

2014年12月末、ドイツ政府の情報セキュリティ庁（BSI）からサイバーセキュリティに関する報告書が公表された。BSIは、もともとドイツ政府の主要インテリジェンス機関（諜報機関）である連邦情報局（BND）の番号部だったが、2011年に切り離されて独立の機関になっている。その報告



# 標的型メール攻撃事例：ビジネスメール詐欺

日本国内でも大企業がビジネスメール詐欺の被害に遭っています。  
偽の請求メールにだまされ、3.8億円の被害に遭ったと発表されました。

## JAL 3.8億円詐欺被害 ビジネスメールに割り込み偽請求【サイバー護身術】

2018/10/12 10:20 [サイバー護身術](#)

日本航空（JAL）がビジネスメール詐欺に遭い、約3億8000万円をだまし取られた。警視庁が詐欺容疑で捜査しているという。JALが取引先のパソコンをウイルス感染させてメールを送り見たり、メールアカウントを乗っ取ったりする手口が使われた可能性があると、専門家は指摘している。（ITジャーナリスト・三上洋）



図1 日本航空が被害に遭った原因のサイバー攻撃手口

通称はBEC スカイマークでは未遂

JALは昨年12月20日、偽の請求書メールにだまされて約3億8000万円の被害に遭ったと発表した。

ビジネスメール詐欺（BEC=Business E-mail Compromise）と呼ばれる事件だ。犯人は、JALと取引先のメールのやり取りに割り込み、取引先になりすまして、口座に金を振り込ませ

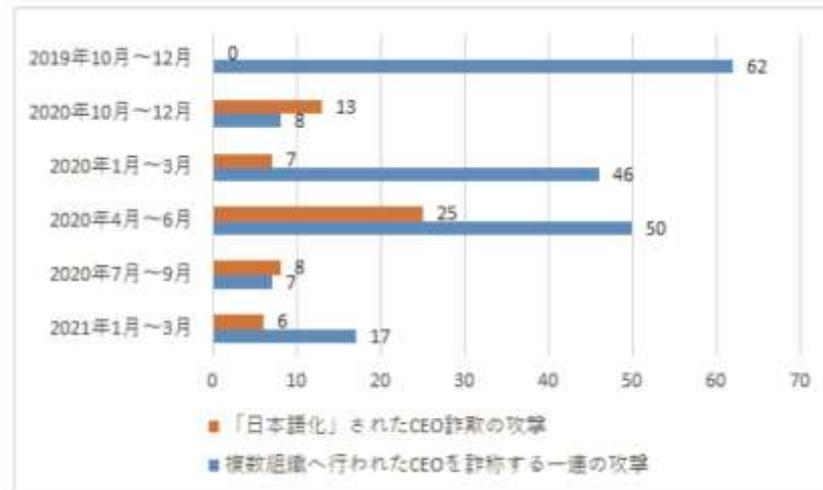


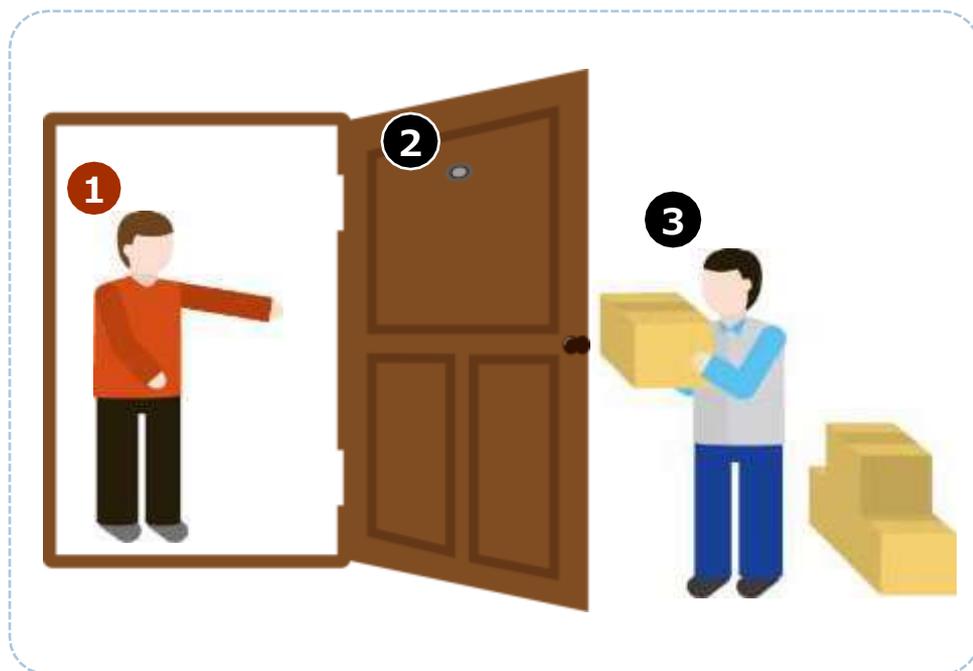
図5 これまで入手したメール件数の推移

[<https://www.yomiuri.co.jp/fukayomi/20180109-OYT8T50178/>]

[<https://www.ipa.go.jp/files/000090633.pdf>]

# 発生原因 — セキュリティ意識の不足

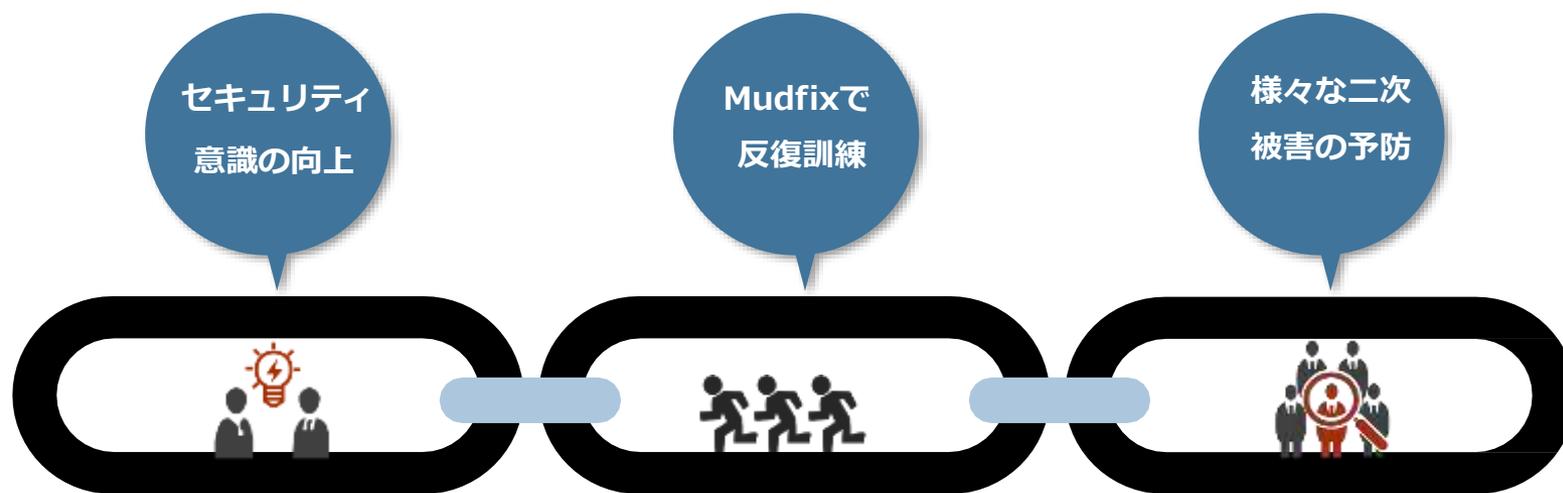
被害の原因は、不十分なセキュリティ意識と知識不足です。  
メールを受信した際に、いつもの違いに気づき、慌てずに上司やセキュリティ担当者に相談  
するなど適切な対応を取ることが大切です。



- **1** 家主(被害者)  
何も疑わずにメールの添付ファイルを実行するのはNG
- **2** 玄関ドアの防犯レンズ  
添付ファイルを開く、実行する前に不審な点を見つけましょう！反復的な訓練で見分け方を身につける。
- **3** 配達員(攻撃者)  
無条件的な信頼は禁物！  
あなたも標的型攻撃メールのターゲットになる可能性があります。

# 反復訓練こそ、全てのセキュリティ事故を予防する鍵

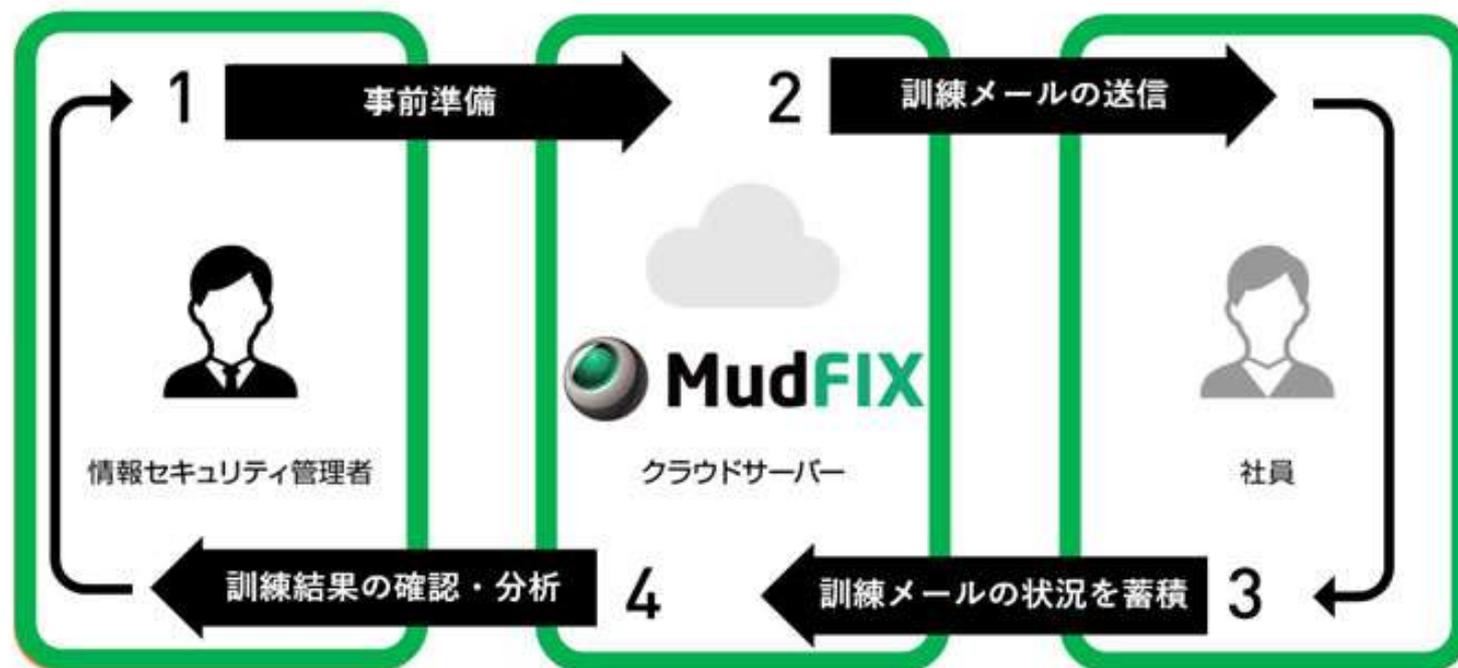
標的型攻撃メールへの対応力を身に付けて頂くためには、普段から定期的に訓練を行う必要があります。反復訓練を行うことで、対応力の定着度は大幅にUPします。



**標的型攻撃メールは、Mudfixで解決しましょう！**

# 標的型攻撃メールの被害予防に最適化したソリューション

MudFixは、標的型攻撃を模した訓練メールを従業員・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付けて頂くための要望訓練サービスです。



# MudFinの主な機能

MudFixは、対象管理、メール送信、結果確認の3つの機能に分かれます。



# 主な機能 — 訓練対象の管理

対象管理タブで、対象者登録、対象者の情報確認、タグ設定が可能です。

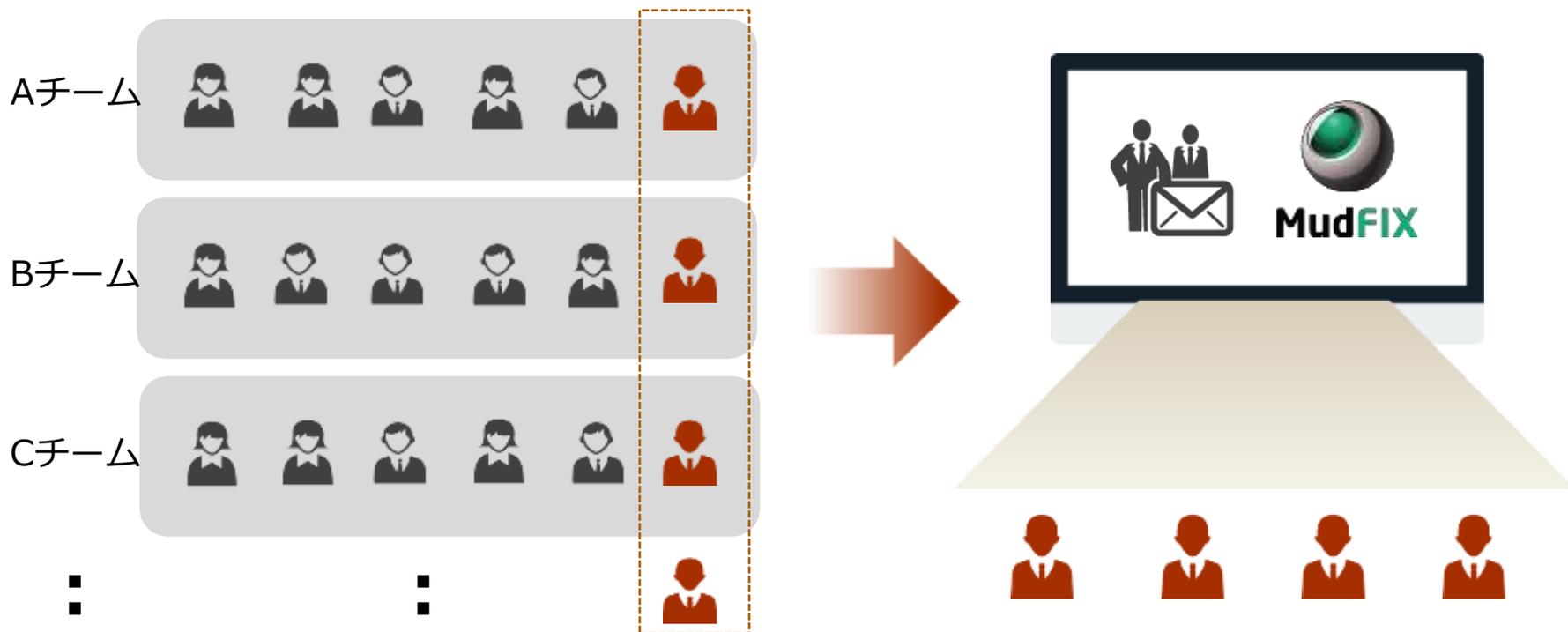
**タグ一覧・検索・フィルタ**  
 -タグ別管理機能

**タグ設定**  
 -対象者にタグ追加  
 -対象者のタグ修正及び削除

**対象者登録フィールド**  
 -個別または一括登録可能

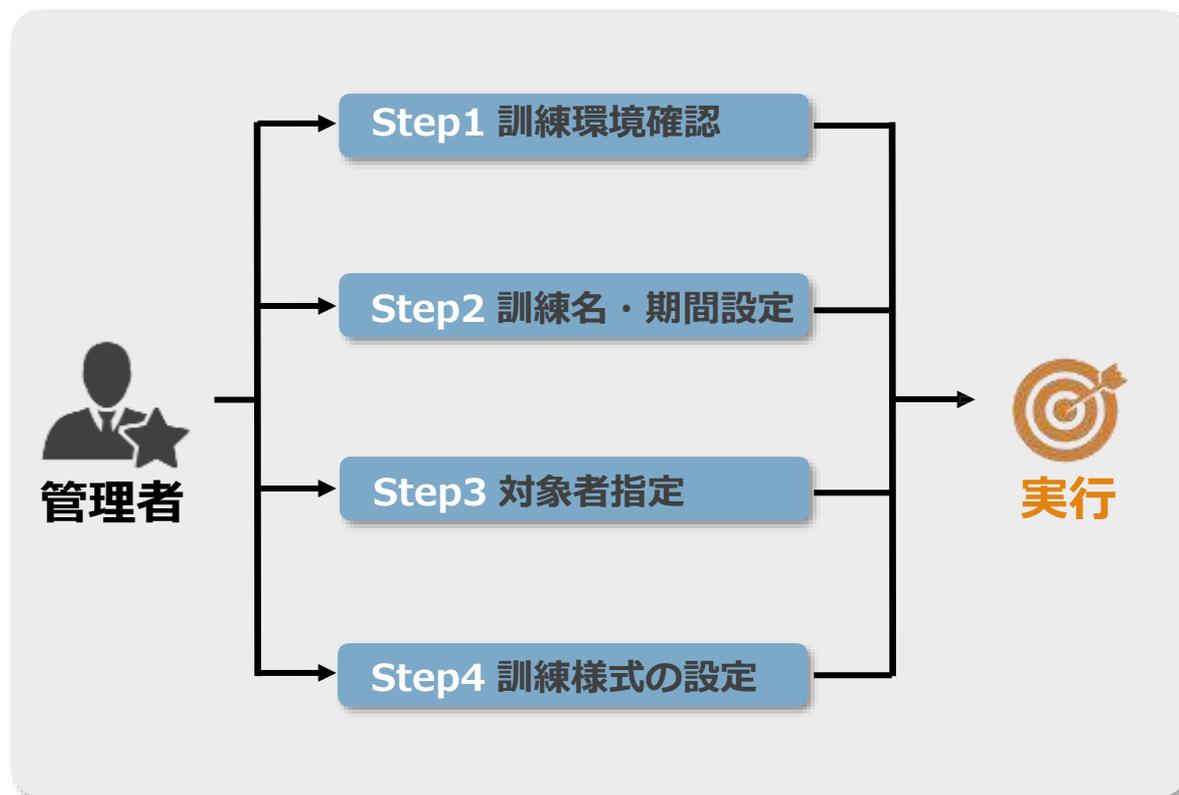
# 主な機能 — 感染対象のみグループピングして再訓練を実施

感染対象を別々のタグで管理することができ、かんたんに感染者のみ再訓練を実施できます。



# 主な機能 — 訓練メール送信

訓練実施の流れを4段階に分けて、各段階で必要な項目をすぐに把握して設定することができます。



# 主な機能 — 結果の確認

個別及び全体訓練の進捗状況、訓練情報及び結果がひと目で把握できるように構成



Ex.)5名のPCのうち**1台感染**を確認可能！  
(流出される恐れがあるファイルの個数と  
サイズを抽出して警戒心を持たせる)

訓練結果を統計グラフで簡単に確認！



# MudFixの特長

MudFixは下記の通り5つの特長を持っています。



1

感染対象のデータを抽出

2

訓練テンプレートを細かくカスタマイズ

3

回数無制限ならでの反復訓練で早期に  
セキュリティレベルアップ

4

リーズナブルな価格

5

個々の顧客に対応したサービス

# 特長 — 流出や感染の恐れのあるデータリストを作成

単純なメール閲覧の可否だけではなく、感染PC及び流出の恐れのあるファイルのリストを作成し、訓練対象者のセキュリティに対する危機意識を高めます。

The screenshot displays a web application interface with a table of infected PCs and a detailed view of files. The top table lists PCs with columns for PC name, IP, contact, counterparty, training ID, training name, total number of infections, total size of infected files, and number of files. The bottom table shows a list of files with columns for file name, size, contact, PC, training name, and infection date.

PC	IP	対象者	対—	訓練番号	訓練名	感染個数の合計	感染ファイルの合計サイズ	ファイル個数
DESKT—	192.168.5—	安藤義志	mas—	457	1	3	8.3 MB	3
DESKT—	192.168.5—	安藤義志	mas—	444	2018年_1月—	3	8.3 MB	3
DESKT—	192.168.5—	加藤秀俊	boy—	443	2018年_10—	3	8.3 MB	3
DESKT—	192.168.5—	石飛真彦	boy—	443	2018年_10—	3	8.3 MB	3
DESKT—	192.168.5—	安藤義志	mas—	442	2018年_7月—	3	8.3 MB	3

名前	対—	PC	訓練名	感染日時
2.txt	安藤義志 mas—	DESKT—	1	2018-11-21 18:03:46
MudFix HP原稿	安藤義志 mas—	DESKT—	1	2018-11-21 18:03:46
9509 - MudFix HP原稿	安藤義志 mas—	DESKT—	1	2018-11-21 18:03:46
9541 - 2.txt	安藤義志 mas—	DESKT—	2018年_1月_定期—	2018-11-16 12:32:32
9540 - MudFix HP原稿	安藤義志 mas—	DESKT—	2018年_1月_定期—	2018-11-16 12:32:32
9539 - MudFix HP原稿	安藤義志 mas—	DESKT—	2018年_1月_定期—	2018-11-16 12:32:32

# 特長 — ユーザーの好みに合わせて細かくカスタマイズできる

充実した基本テンプレートを提供しておりますので、お客様が別途テンプレートを作成する手間が省けます。また、お好みに合わせて本文内容から訓練の種類・添付ファイルのタイプまで細かくカスタマイズできます。

**!!Alert 情報が流出しました!!**  
 これは標的型攻撃メールの訓練です。

1. 不審なメールのURLリンクや添付ファイルはクリックせず、該当メールを破壊するようにしましょう。
2. 万が一クリックした場合は、セキュリティ部門もしくはシステム部門の担当者にすぐに報告してください。
3. クリックしたために放置してしまうと、機密情報や個人情報が盗み取られ、重大な事故に発展することになります。

訓練目的に合わせて、テンプレーを選択可能

パスワード付き圧縮ファイルなど多様な添付ファイルタイプ

拡張子の有効性検証による精度向上

**訓練テンプレート(テンプレート)修正**  
 ユーザーテンプレート (No. 2322 / サービスNo. 291)

---

**添付ファイル情報**

添付ファイルのインポート

14               HTMLメール

ダウンロードタイプ

リンク参照(メール本文にダウンロードボタン)

添付タイプ

圧縮ファイル名(メールに添付された圧縮ファイルのファイル名を指定できます)  圧縮パスワード  圧縮ファイル種類

原本ファイル名(メールに添付された圧縮ファイルのファイル名を指定できます)

**送信情報**

送信者  送信元メールアドレス  エンベロープ送信元メールアドレス

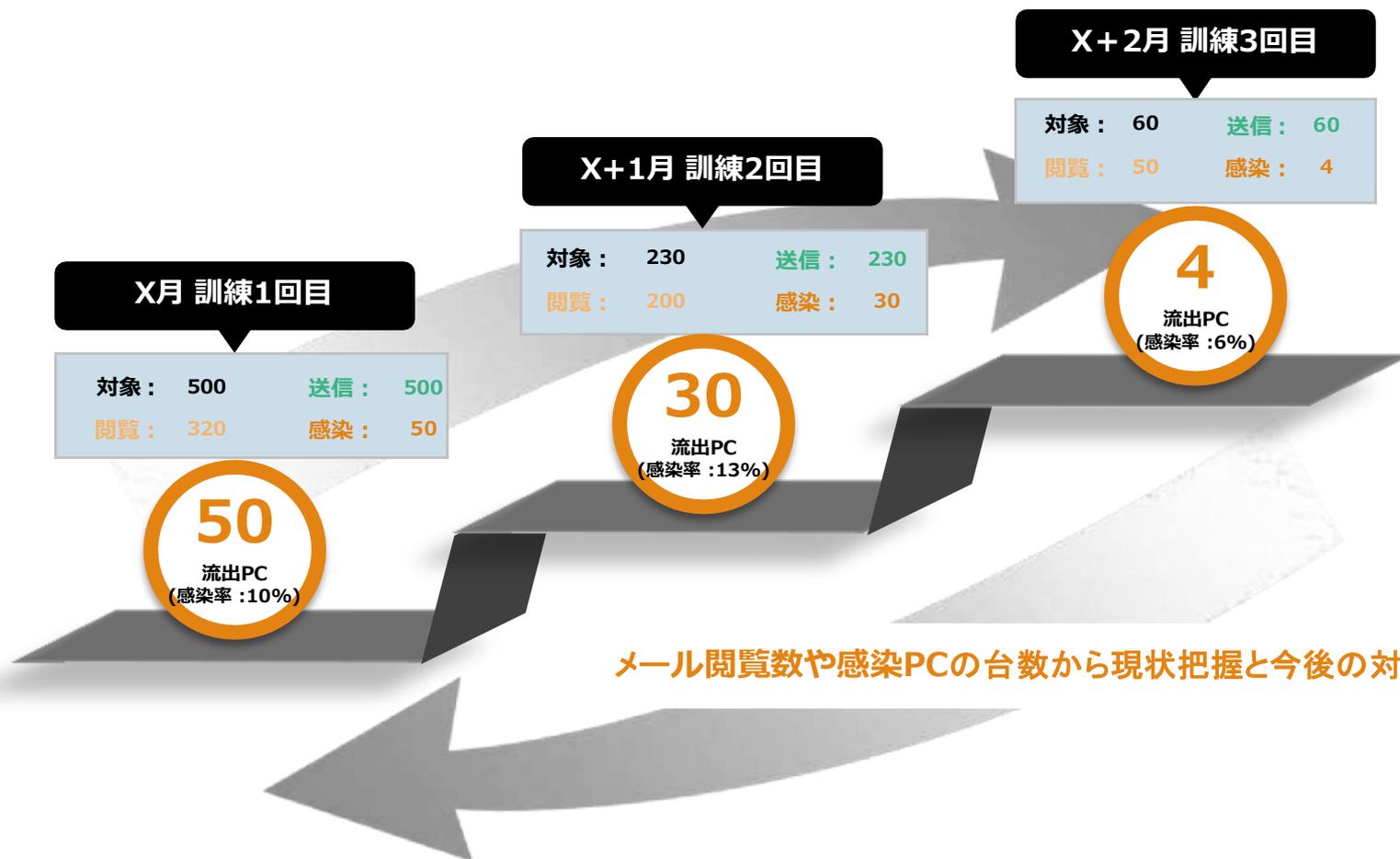
メール内容

# 特長 — 充実したテンプレートで多様な訓練を実施

訓練タイプ	メール部分			画面部分
	方法	ファイル種別	補足	
<b>① 模擬悪性ファイル</b> (PCのファイルサーチまで可能、 但しexeの時にのみ)	<b>ファイル添付</b> ・ 原本 ・ zip ・ PW付zip  <b>URLリンク</b> (クリックするとファイルをダウンロード。以降はファイル添付と同じ動き)	<b>原本ファイル</b> ・ *.exeファイル → Word、Excel、PowerPoint、Jpeg、PDF、HTMLアイコンから選択 ・ *.pdfファイル → PDFアイコン ・ *.htmlファイル → HTMLアイコン  <b>zipファイル</b> Pw付zipファイル → 原本ファイル圧縮	簡易エディタで編集可能	簡易エディタで編集可能
<b>② 警告案内</b> (クリックでPCに画面表示)				
<b>③ 実態調査</b> (クリックしてもPC動きなし)				
<b>④ フィッシング誘導</b>	<b>URLリンク</b>	添付ファイルなし	HTMLエディタでフル編集可能	HTMLエディタでフル編集可能

# 特長 一反復訓練により早期にセキュリティレベルアップ

訓練は、一度行っただけでは高い効果は期待できません。  
 継続して定期的に何度も繰り返すことで、いざという時の対応力を養うことができます。



# 訓練メール例①

事例にありましたスパフィッシングへの対応も可能です。  
実際に行われる会議の詳細を調べ、会議の日程に合わせて送信した事例もあるそうです。

**送信情報**

送信者  送信元メールアドレス  エンベロープ送信元メールアドレス

\*存在しないドメインを使うとメールの送信が失敗することがあります。

**送信者情報・件名編集可能**

**メール内容**

メール件名

メール本文

あなたを予約されたZoomミーティングに招待しています。

トピック: 緊急会議  
時間: 2021年7月2日 06:00 PM 大阪、札幌、東京

Zoomミーティングに参加する  
<https://zoom.us/j/56754323972?pwd=QUUvT0JUNHIzand0U1RyNkIyKzA0QT09>

ミーティングID: 567 5432 3972  
パスコード: 039043

**メール本文編集可能  
HTMLエディタでカスタマイズ**

## 訓練メール例②

取引先を装った詐欺メールの訓練も可能です。  
緊急の内容だとしても、お金が絡む場合は「確認する」ことが大事であることを訓練を通して身につけることができます。

### ～実際の訓練メール例～

差出人: [JSONIC](#)

送信日時: 2021年8月17日 18:02

宛先: [shin](#)

件名: 緊急のお願い

株式会社JSONIC 高森 様

いつもお世話になっております。J.S Holdingsの坂本です。

以前から計画していたB社の買収の件ですが、緊急かつ秘密で進めることになりました。  
至急、先方が指定する海外の口座に送金する必要があるため、ご対応お願いできますと幸いです。  
詳細情報は後ほど送らせていただきます。

何卒よろしくお願い申し上げます。

-----  
株式会社J.S Holdings

坂本 あゆみ

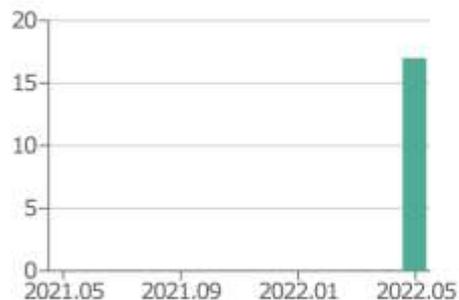
〒195-0029

東京都港区東新橋9-19-2 JSビル3F

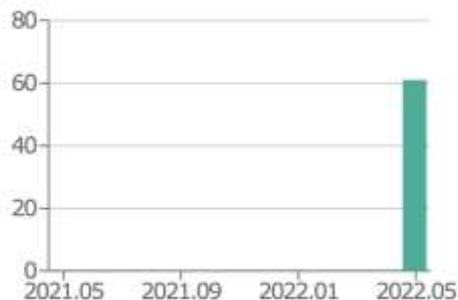
TEL:03-6915-2016 / FAX:03-9391-2016  
-----

# ダッシュボード機能

月別訓練数



月別訓練対象数



全ての訓練

17 個

予約訓練

0 個

進行中の訓練

7 個

終了した訓練

10 個

訓練結果



メール送信率

100 %



メール閲覧率

89 %



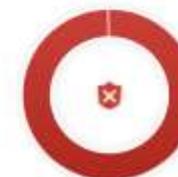
ダウン接続率

31 %



感染/流出率

21 %



# 訓練結果の一覧表示

The screenshot displays the 'MudFIX v1.0' interface with the '訓練結果' (Training Results) tab selected. The main area shows a list of training sessions under the heading '全ての訓練 合計 17回 訓練'. The table includes columns for training ID, dates, and various status indicators. A sidebar on the left provides filters for training status, and a detailed view on the right shows specific data for a selected session, such as '訓練番号: 7968' and '進行率: 100.0%'. A blue banner at the bottom contains the text: '訓練結果を一覧表示。訓練毎にソートすることも可能です。'

# ユーザー管理（タグ管理）

The screenshot displays the 'MudFIX v1.0' user management interface. The main area shows a list of users under the heading '全ての対象者' (All Targets), with 58 targets and 7 tags. A modal window titled 'タグを作る' (Create Tag) is open, allowing users to create new tags with a name field and a color selection grid. The interface includes a sidebar with navigation options like '全ての対象者', 'OSチーム', and '人'. A top navigation bar contains '対象者登録', '対象者削除', '対象者一括登録', and '対象者エクスポート'. A right sidebar shows a 'タグ' section with 'OSチーム' and 'OSサポート' tags, and a '統計概要' (Summary) section with a chart showing '全体の件数' (Total Cases) and '稼働/廃出率' (Operational/Disposal Rate) at 35%.

複数のタグでユーザーの属性管理が可能です。ユーザーの一括登録も可能。

# テンプレート管理

MudFIX v1.0

最新メール 送信記録 対象管理 テンプレート管理

最新テンプレートの管理

フィッシング情報検索

全体

1:17/25 17

No.	区分	送信タイプ	送信ファイル情報	フィッシング情報設定	テンプレート名	メールの件名	送信結果	発送者名	送信者の電
4700	ユーザー	フィッシングメール		(基本)新型コロナワクチン接種予約受付メー	(基本)新型コロナワクチン接種予約受付の...	接種券からのお知らせ   新型コロナワク...	-	総務部	admin@sateraito.jp
4701	ユーザー	フィッシングメール		個人情報フィッシングふるさと納税 (1)	個人情報フィッシングふるさと納税	ふるさと納税 年々高額になり続け	-	総務部	admin@sateraito.jp
4702	ユーザー	署名内	HTML	(基本)みずほ銀行からの進捗のお知らせ	(基本)みずほ銀行からの進捗のお知らせ	メンテナンスの予定	流出率: 13% (44名)		admin@sateraito.jp
4703	基本	フィッシングメール		(基本)みずほ銀行からの進捗のお知らせ	(基本)みずほ銀行からの進捗のお知らせ	みずほ銀行からの進捗にお	流出率: 13% (4403名)		miho@direct@ms...
4704	基本	フィッシングメール		(基本)個人番号カード申請情報開示のしよ	(基本)個人番号カード申請情報開示のしよ	個人番号カード申請情報開			Nikkyu@msbcard@...
4705	基本	フィッシングメール		(基本)新型コロナワクチン接種予約受付のメ	(基本)新型コロナワクチン接種予約受付のメ	新型コロナワクチン接種			tsuchi@novokel...
4706	基本	フィッシングメール		(基本)メルマガ詐欺_クリック型詐欺テニス	(基本)メルマガ詐欺_クリック型詐欺テニス	PCデバイスの購入、変更	流出率: 10% (614名)	総務	campaign@drinke...
4707	基本	フィッシングメール		(基本)Web会議系_クリック型詐欺テニス	(基本) Web会議系_クリック型詐欺テニス	会議室予約メール	流出率: 5% (741名)		souru_dept@se...
4708	基本	フィッシングメール		(基本)メルマガ詐欺	(基本)メルマガフィッシング	PCデバイスの購入、変更に関するお問い合わせ	流出率: 4% (80名)	Nike@P	campaign@drinke...
4709	基本	フィッシングメール		(基本)Web会議系	(基本) Web会議系フィッシング	会議室予約メール	流出率: 7% (523名)	総務部	souru_dept@se...
4710	基本	フィッシングメール		(基本)インフルエンザ予防接種の会社様へ	フィッシングインフルエンザ予防接種の	インフルエンザ予防接種の会社様へについて	流出率: 1% (360名)	人事部	hrng_dept@siggr...
4711	基本	フィッシングメール		(基本)請求書送ります。	フィッシング請求書を送ります	請求書を送ります。	流出率: 13% (400名)	経理部	kenr_dept@living...
4712	基本	フィッシングメール		個人情報フィッシングふるさと納税	個人情報フィッシングふるさと納税	ふるさと納税ポータルサイト「ふるさとリ...	流出率: 7% (300名)	ふるさとリンク	maki@system@mu...

テンプレート毎の流出率（感染率）を表示

複数のテンプレートを提供。オリジナルテンプレートの作成も可能です。

## オリジナルテンプレートの作成

The screenshot shows the MudFIX v1.0 email editor. On the left, there's a sidebar with options like 'フィッシングタイトル' (Phishing Title), 'フィッシングステップ' (Phishing Step), and 'ファイルのアップロード' (File Upload). The main area is split into 'HTML' code on the left and a 'プレビュー表示' (Preview) on the right. The HTML code includes placeholders for stage finish and recipient information. The preview shows a phishing email titled '総務部からのお知らせ【コロナワクチン接種予約】' (Notice from the General Affairs Department [COVID-19 Vaccine Vaccination Appointment]). The email body contains a warning about a vaccination appointment, a link to '予約内容照会' (Check Appointment Details), and a link to '接種券番号確認' (Check Vaccination Certificate Number). The footer includes a warning about a security alert and a disclaimer from Sateraito Office.

**メール本文/警告文のカスタマイズ**

**プレビュー表示**

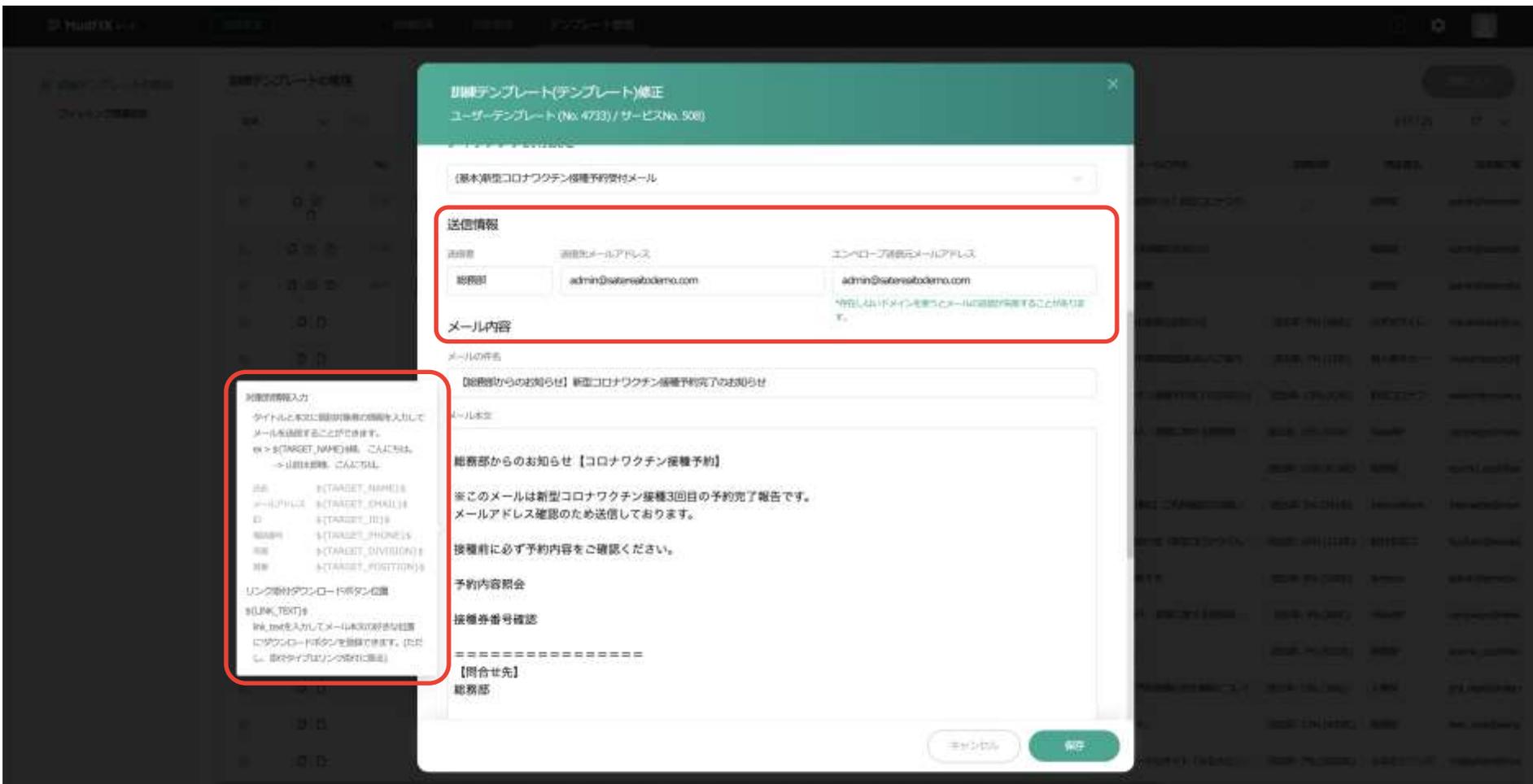
**!!Alert 情報が流出しました!!**  
これは標的型攻撃メールの訓練です。

1. 不審なメールのURLリンクや添付ファイルはクリックせず、該当メールを破棄するようにしましょう。
2. 万が一クリックした場合は、セキュリティ部門もしくはシステム部門の担当者すぐに報告してください。
3. クリックしたのに放置してしまうと、機密情報や個人情報が盗み取られ、重大な事故に発展することになります。

【サテライトオフィス・総務部より】  
訓練メールになりますので実部には感傷してませんのでご安心ください。  
本訓練に関するお問い合わせはこちらまで→総務部: [omnu@sateraitodemo.com](mailto:omnu@sateraitodemo.com)  
攻撃型メールをクリックしてしまうと会社に多大な被害を与えますことになります!

オリジナルテンプレート作成機能。プレビューで確認しながら作成が可能。

# テンプレートのカスタマイズ機能



メール件名や送信先/エンベロープ送信元のメールアドレスも変更可能。

# 簡単に訓練を実施



**送信期間や時間帯  
などの設定が可能**

**送信者タグは複数  
設定が可能**

**複数のテンプレート  
を設定が可能**

**訓練メールの送信も簡単。画面に従ってすすめるだけで送信可能です。**

# インパクトのある警告画面で訓練の効果を上げる

The image shows a Gmail interface on the left and a browser window on the right. The Gmail interface displays an email from '総務部 <admin@sateraitodemo.com>' with the subject '【総務部からのお知らせ】新型コロナワクチン接種予約完了のお知らせ'. The email body contains a warning about a phishing attempt and a link to '予約内容照会'. A red box highlights this link, and a black arrow points to it. The browser window shows a warning page with the text '!!Alert 情報が流出しました!!' and 'これは標的型攻撃メールの訓練です。' followed by a list of instructions: 1. Do not click on suspicious URLs or attachments. 2. Report to security or IT if clicked. 3. Do not click on links in the email. The page also includes contact information for Sateraito Office and a disclaimer about the training email.

インパクトのある警告画面で訓練の効果を上げることが可能です。

# 訓練結果の報告書作成機能

The screenshot displays the MudFIX v1.0 web application interface. The main content area shows a list of training sessions under the heading "全ての訓練" (All Trainings), with a sub-heading "合計 20回 訓練" (Total 20 trainings). A red box highlights the "報告書" (Report) button in the top navigation bar. A modal dialog titled "レポートのダウンロード" (Report Download) is open, showing options for report types: "個別報告書" (Individual Report), "統合報告書" (Consolidated Report), and "統合報告書ベータ" (Consolidated Report Beta). Below these options, there are toggle switches for "マスキング使用" (Masking Use) for "氏名" (Name), "メールアドレス" (Email Address), and "電話番号" (Phone Number). A red box highlights the "ダウンロード" (Download) button at the bottom of the modal.

訓練ID	期間	人数	感染PC	感染ファイル	報告書
訓練	2022-05-21 ~ 2022-05-22	5	5	5	1
訓練0521-10	2022-05-21 ~ 2022-05-27	5	1	1	0
訓練0521-9	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-8	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-7	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-5	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-4	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-3	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521-2	2022-05-21 ~ 2022-05-22	1	1	1	1
訓練0521	2022-05-21 ~ 2022-05-22	5	5	5	1
訓練0517-2	2022-05-17 ~ 2022-05-18	5	5	5	1
訓練0517	2022-05-17 ~ 2022-05-18	5	5	5	1
訓練0513	2022-05-13 ~ 2022-05-14	5	5	5	1
訓練0512-4	2022-05-12 ~ 2022-05-13	5	5	5	1

訓練結果の報告書を作成・ダウンロードが可能です。

## 最後に

本章は、その他の説明をします。

# サテライトオフィスの強みについて

サテライトオフィスが提供するソリューションのメリットは何か説明させていただきます。

## 50000社以上の導入実績によるノウハウ提供

50000社（中小規模～大規模）以上の導入支援によるGoogle Workspaceの情報が豊富です。新しい機能や新しい技術に関しても、導入済みのお客様とのコミュニケーションによりいち早く解決して行きます。また、50000社様の要望の多いものから拡張アプリケーションとしてリリースして行きます。

## Google Workspace ビジネステンプレート+アドオンアプリケーションの提供

多くのビジネステンプレートをご用意しております。今までのグループウェアの様な、テンプレートも用意しております。また、Google Workspace内では実現できない部分は、拡張アプリケーションとして、API + Google App Engine などを利用する事で、今後も実現して行きます。是非、ご要望をください！

## Google App Engine や APIによる開発（カスタマイズ）ソリューション

弊社Google App Engineフレームワークによるシステム開発が可能です。またAPIを利用した社内システムとの連携ソリューションも有効的です！今後もGoogle App EngineやAPI技術は、早い速度で拡張して行きます。サテライトオフィスでは、いち早く技術を習得し、ソリューションとして、提供して行きます。

## 弊社スペシャリストとのテレビ会議&オンサイトによるスピーディーなサポート体制

サテライトオフィスの**一番の強みはサポート**です。電話やテレビ会議や画面共有ソフトを利用し、とにかくスピーディーに解決して行きます。満足度高いサポートを提供して行きますので、よろしくお願いたします。

*Sateraito ~ for your best solution*



BayTech Systems,  
The Finest Solution  
Company



サテライト オフィス  
**Sateraito Office**



Google for Education  
Partner



Google Cloud  
Partner

認定ソリューション開発パートナー

株式会社サテライトオフィス  
〒135-0016  
東京都江東区東陽4-3-1

東陽町信栄ビル4F

TEL : 050-5835-0396 (代表)

FAX : 050-6861-2893

E-Mail : contact-info@sateraito.co.jp