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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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

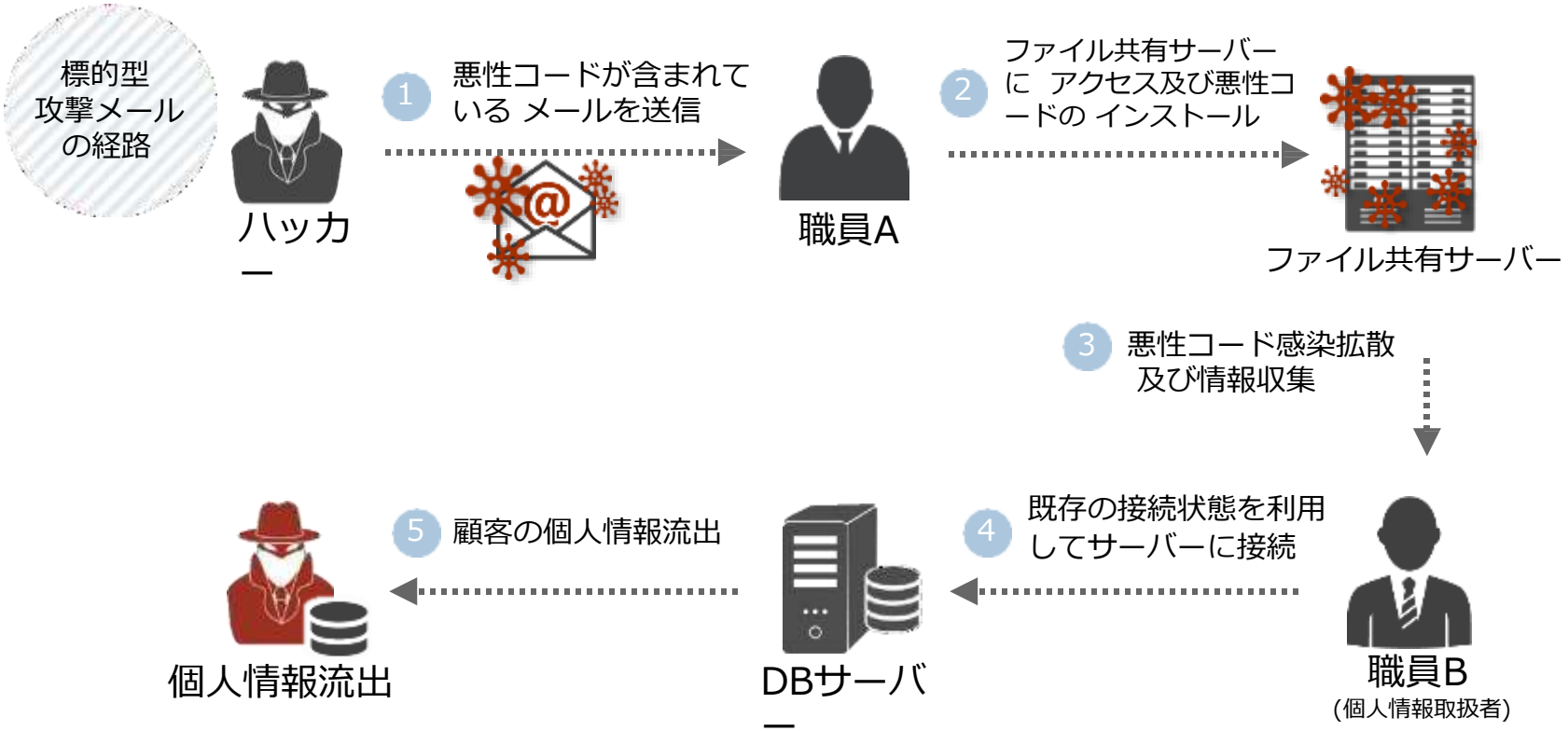
標的型攻撃メール対策訓練機能 for Mudfix とは？

**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！**

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。



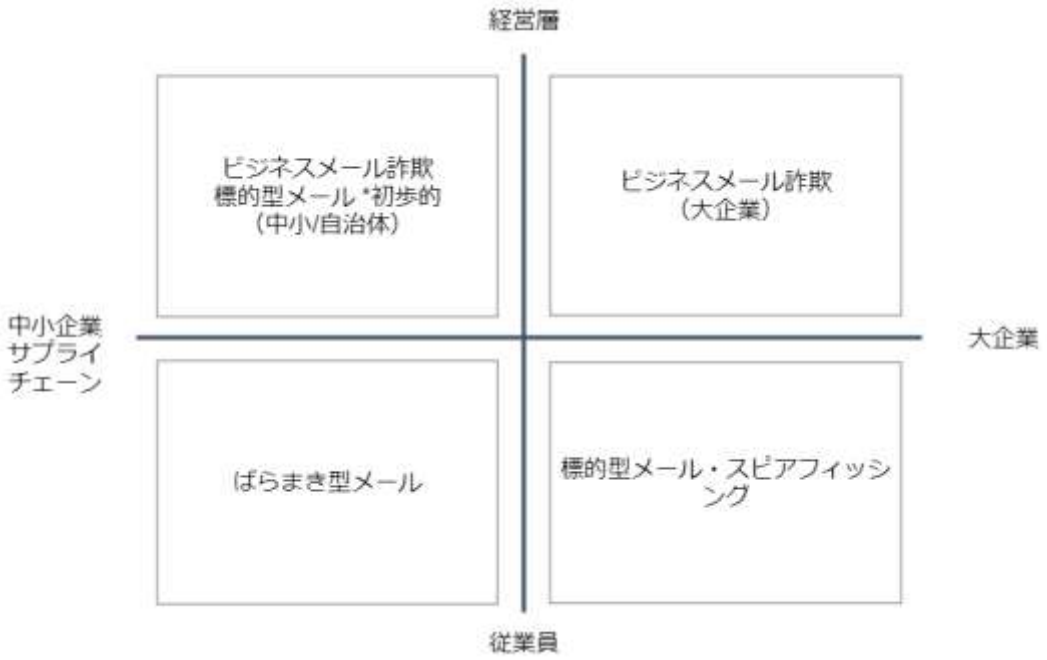
Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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

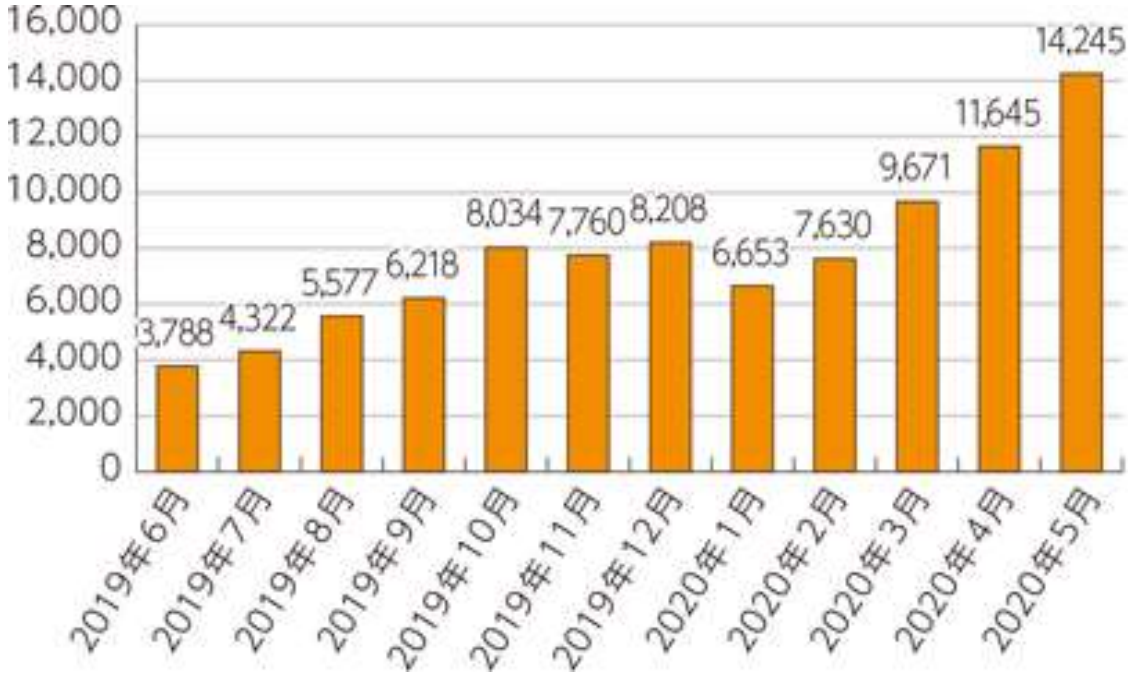
●**スピアフィッシング**：特定のターゲットをピンポイントで攻撃



Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

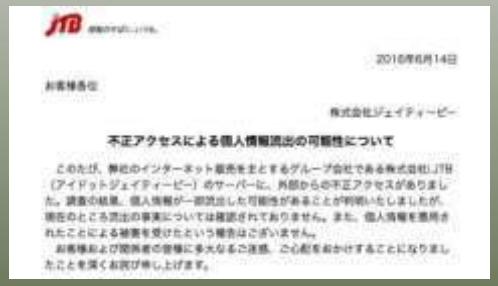
標的型攻撃メールの傾向と被害事例

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が流出



2015年6月14日

お客様各位

株式会社ジェイティービー

不正アクセスによる個人情報流出の可能性について

このたび、弊社のインターネット販売を主とするグループ会社である株式会社JTB（アイドットジェイティービー）のサーバーに、外部からの不正アクセスがありました。調査の結果、個人情報が一部流出した可能性があることが判明いたしましたが、現在のところ流出の事実については確認されておりません。また、個人情報を悪用されたことによる被害を受けたという報告はございません。

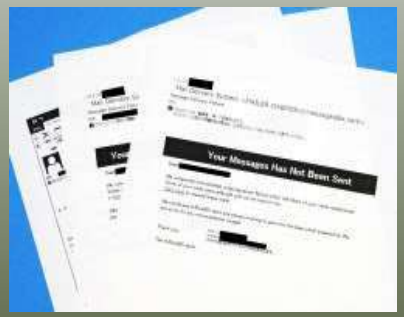
お客様および関係者の皆様に多大なるご迷惑、ご心配をおかけすることになりましたことを深くお詫び申し上げます。

NEWS

[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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

標的型メール攻撃事例：スピアフィッシング

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

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。情報セキュリティー大手トレンドマイクロのセキュリティーエバンジェリスト石原雄平氏は「かなり時間を要する攻撃。数日や数週間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

政府機関が認めた初のシステムへのサイバー攻撃として２例目に　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、もともとは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）の暗号部だったが、2011年に切り離されて独立の機関になっている。その報告

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

ＪＡＬ３．８億円詐欺被害　ビジネスメールに割り込み偽請求【サイバー護身術】

2018/01/12 10:30 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か取引先のパソコンをウイルス感染させてメールを盗み見たり、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）

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３億８０００億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

[https://www.yomiuri.co[.]jp/fukayomi/20180109-OYT8T50178/](https://www.yomiuri.co[.]jp/fukayomi/20180109-OYT8T50178/)

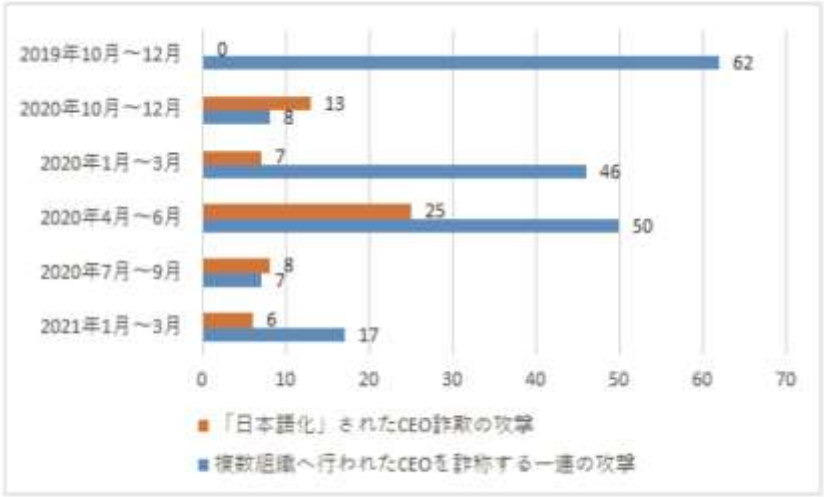


図 5 これまで入手したメール件数の推移

[https://www.ipa.go[.]jp/files/000090633.pdf](https://www.ipa.go[.]jp/files/000090633.pdf)

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

発生原因 ー 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。

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。

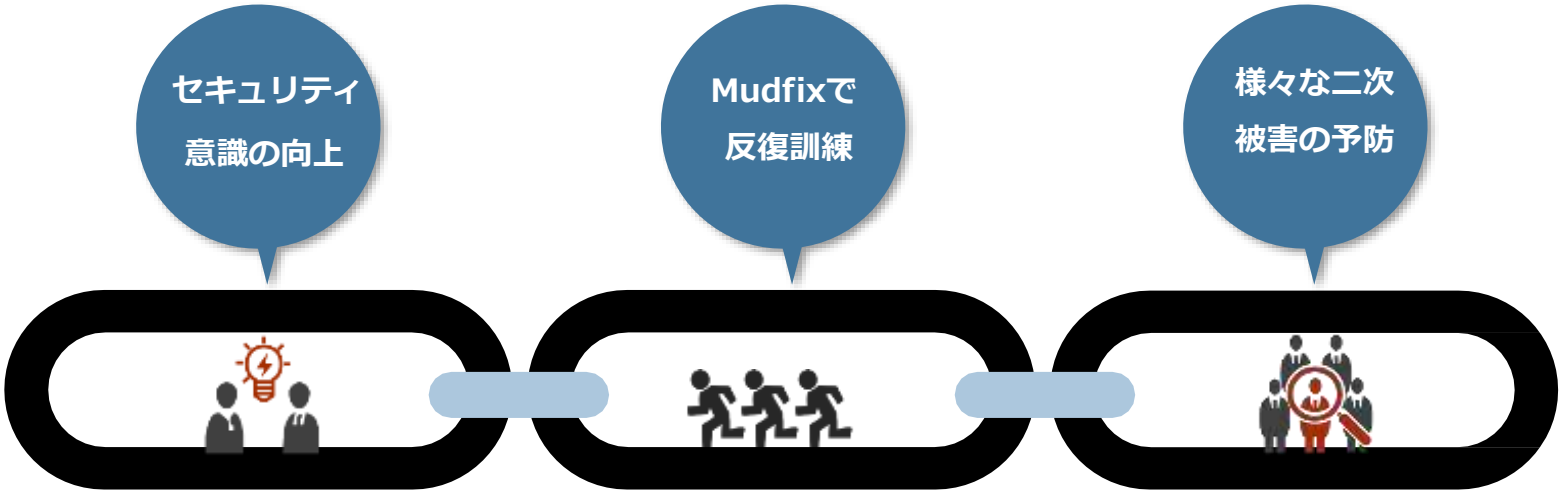
3 配達員(攻撃者)

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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着けて頂くためには、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！

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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着けて頂くための要望訓練サービスです。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

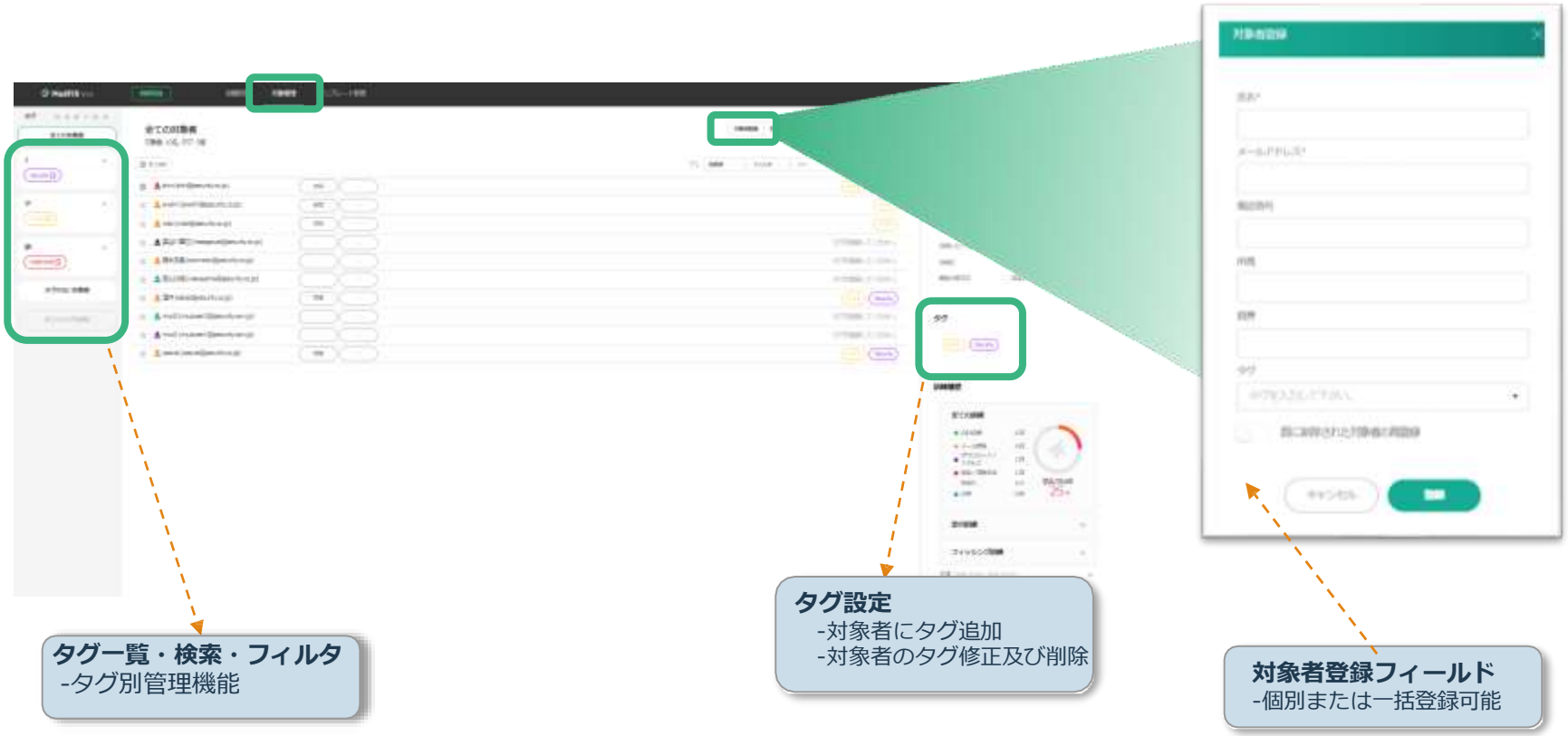
MudFinの主な機能

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

主な機能 ― 訓練対象の管理

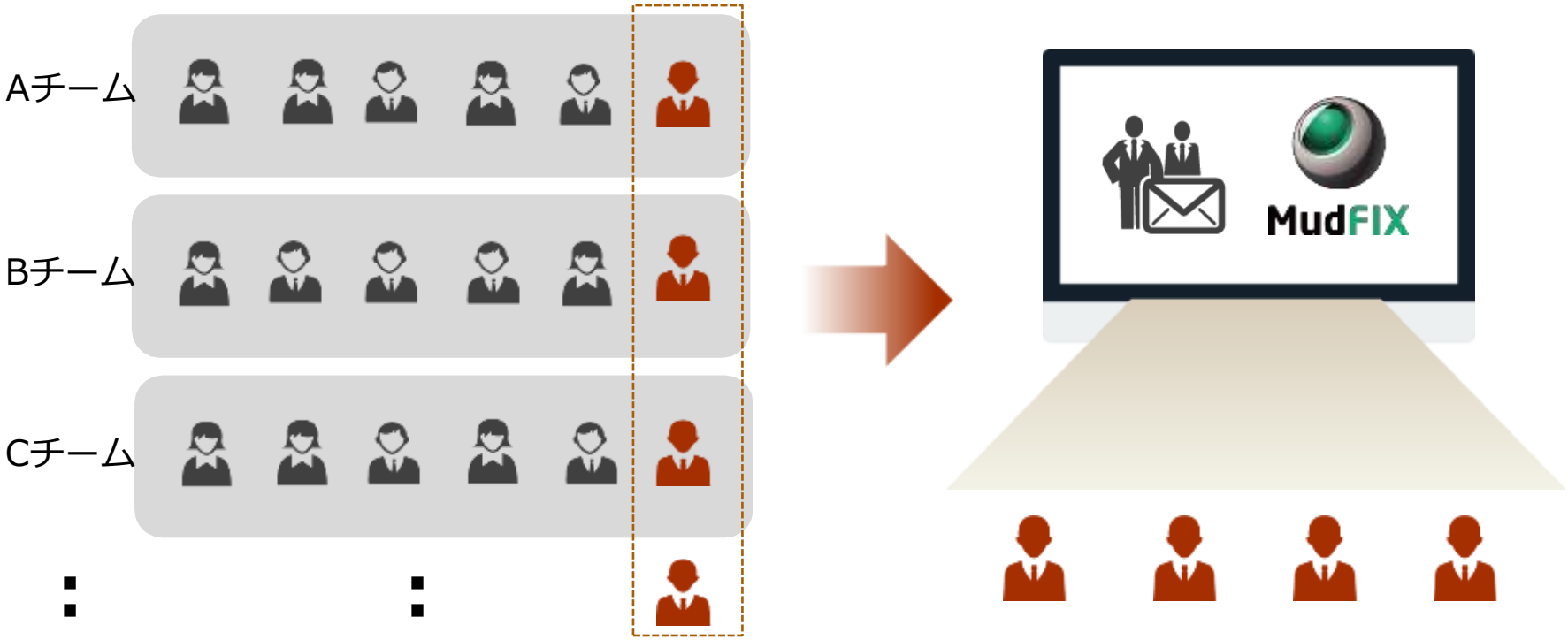
対象管理タブで、対象者登録、対象者の情報確認、タグ設定が可能です。



Copyright(c)2022 Sateraito Office, Inc. All rights reserved

主な機能 ― 感染対象のみグルー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。



Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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！

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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. 回数無制限ならではの反復訓練 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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

特長 ー 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。

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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

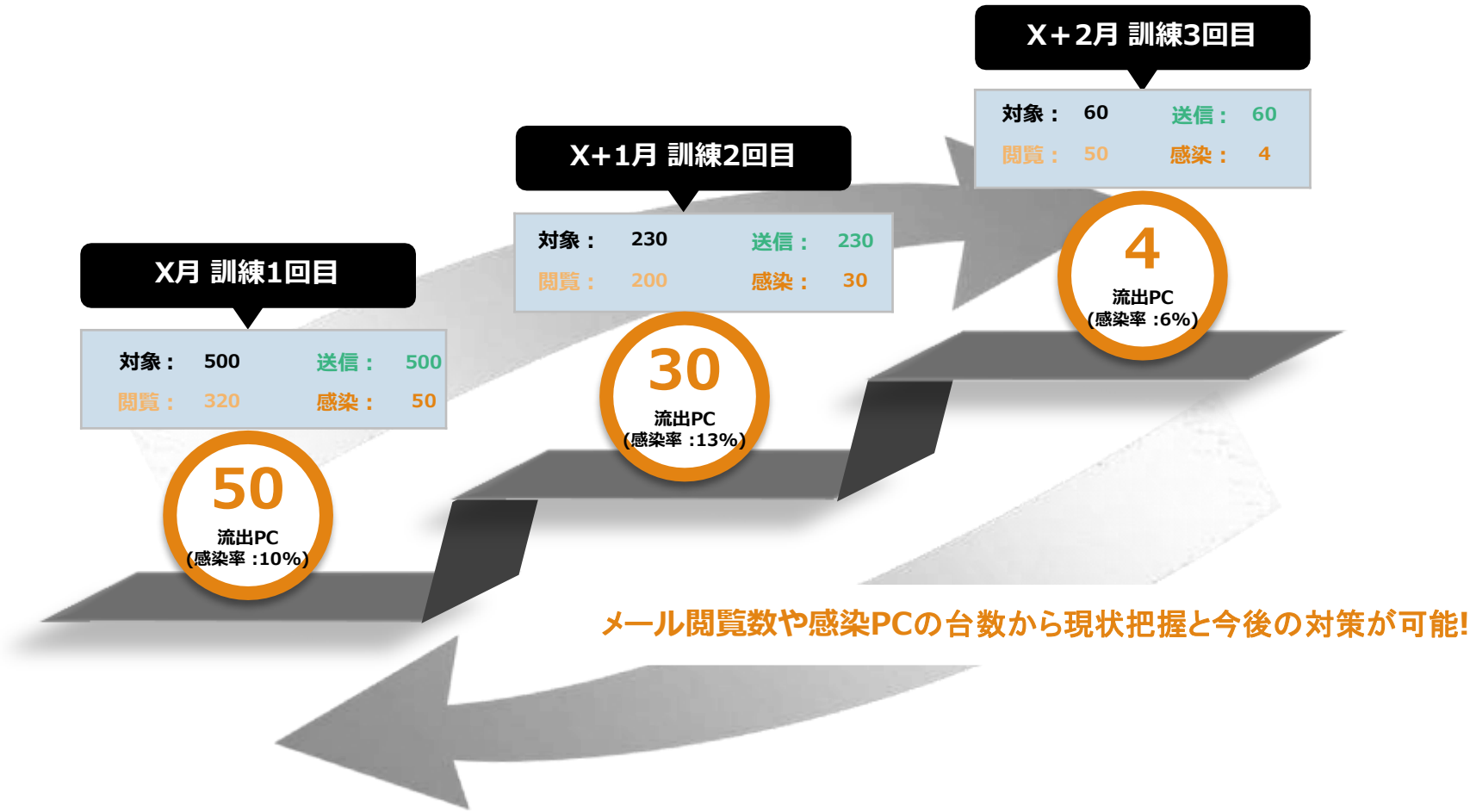
特長 ー 充実したテンプレートで多様な訓練を実施

訓練タイプ	メール部分			画面部分
	方法	ファイル種別	補足	
①模擬悪性ファイル (PCのファイルサーチまで可能、但しexeの時にのみ)	**ファイル添付** ・原本 ・zip ・PW付zip **URLリンク** (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)	**原本ファイル** ・*.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 **zipファイル** 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
②警告案内 (クリックでPCに画面表示)				
③実態調査 (クリックしてもPC動きなし)				
④フィッシング誘導	**URLリンク**	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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

特長 ー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。



Copyright(c)2022 Sateraito Office, Inc. All rights reserved

訓練メール例①

事例にありましたスピア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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

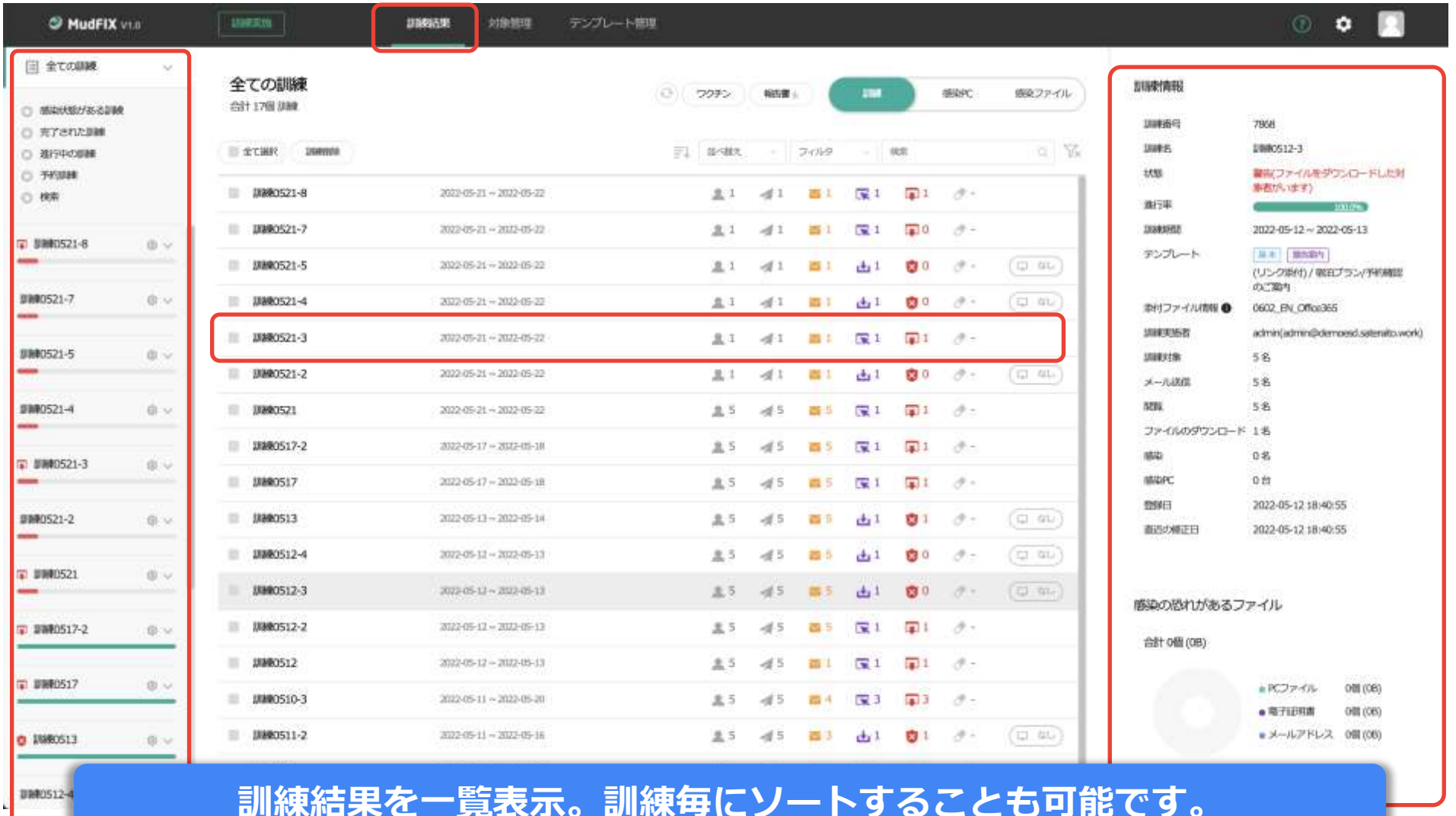
株式会社J.S Holdings
坂本 あゆみ
〒195-0029
東京都港区東新橋9-19-2 JSビール3F
TEL:03-6915-2016 / FAX:03-9391-2016

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

ダッシュボード機能

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

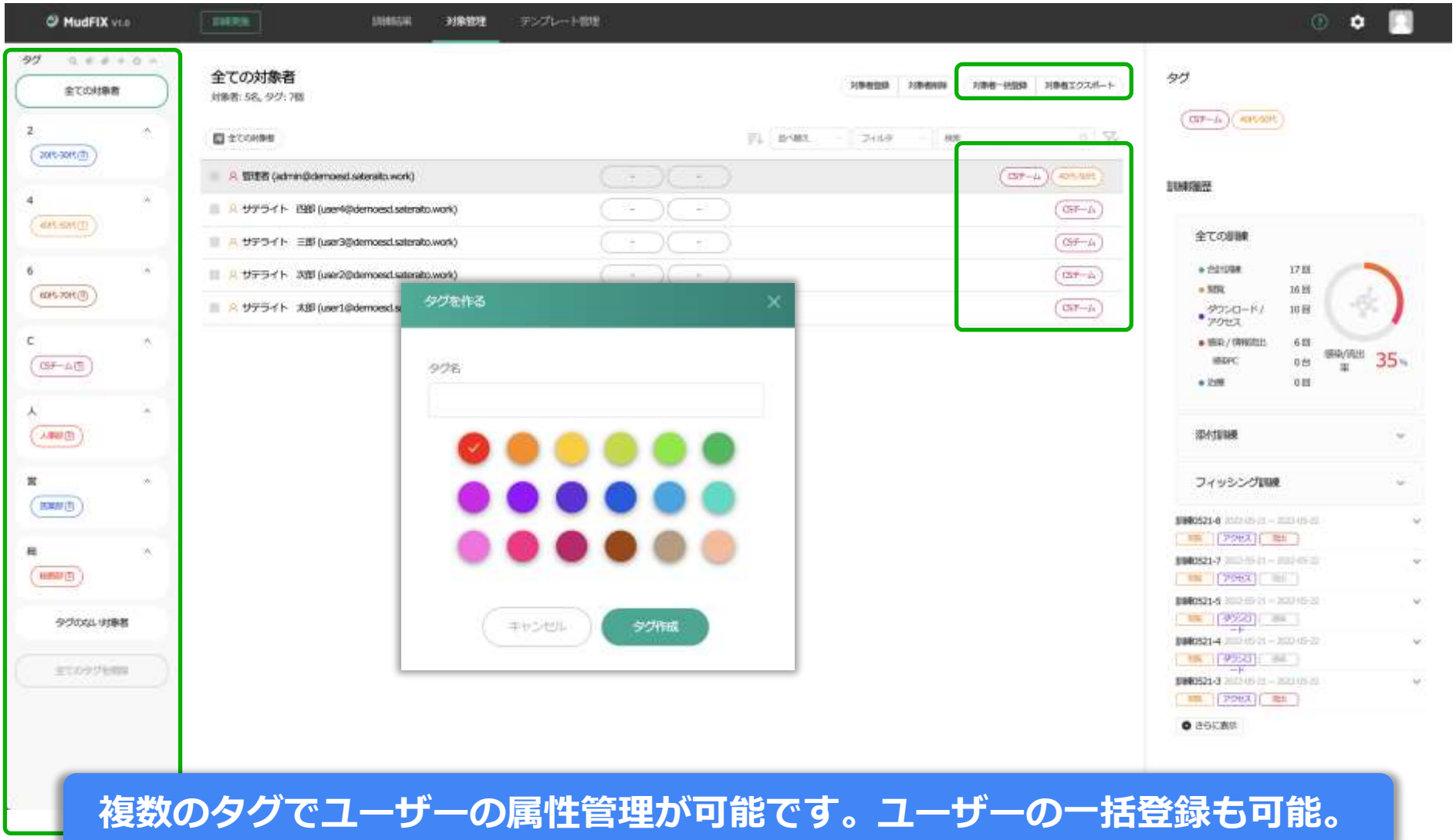
訓練結果の一覧表示



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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

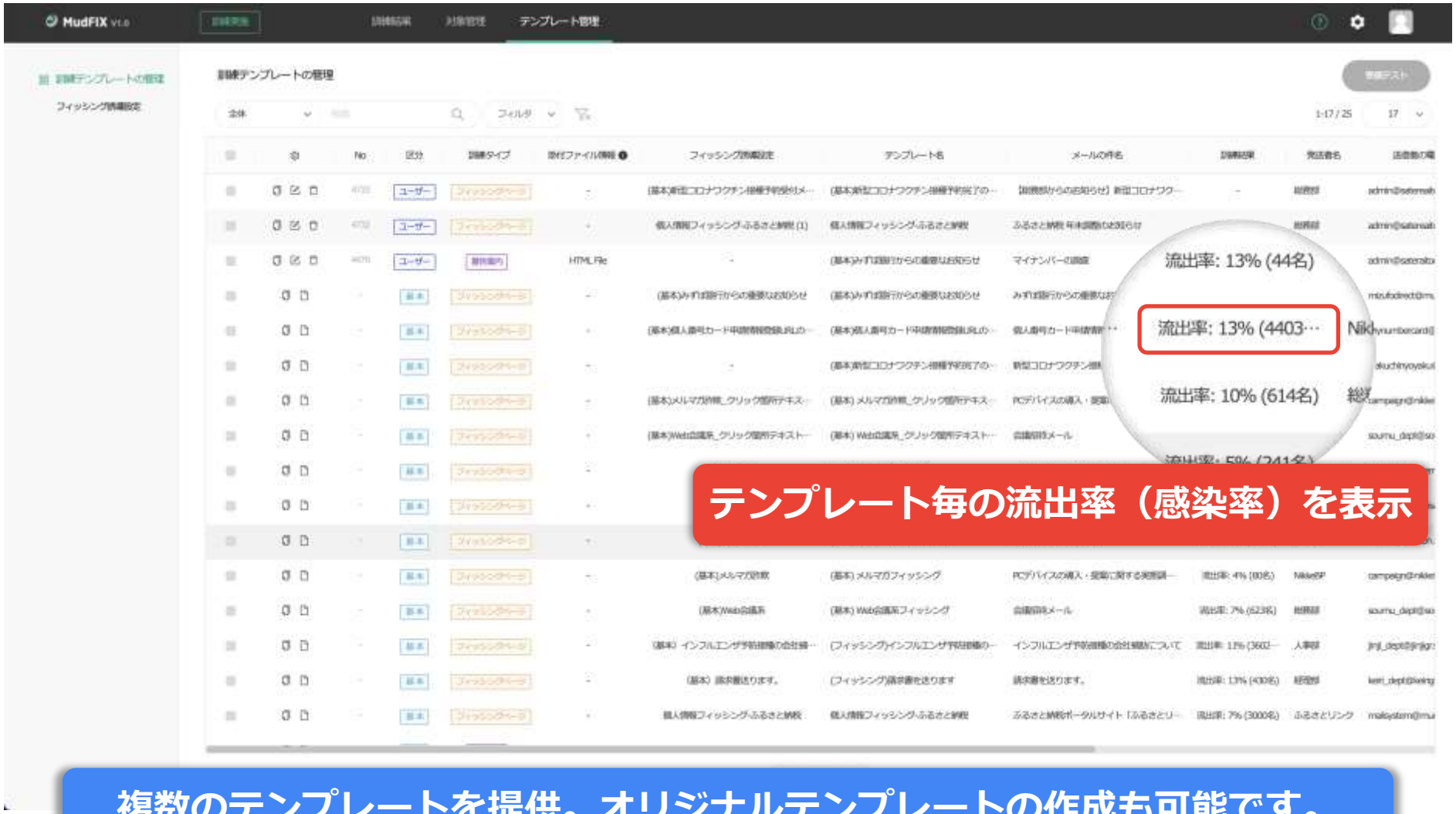
ユーザー管理（タグ管理）



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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

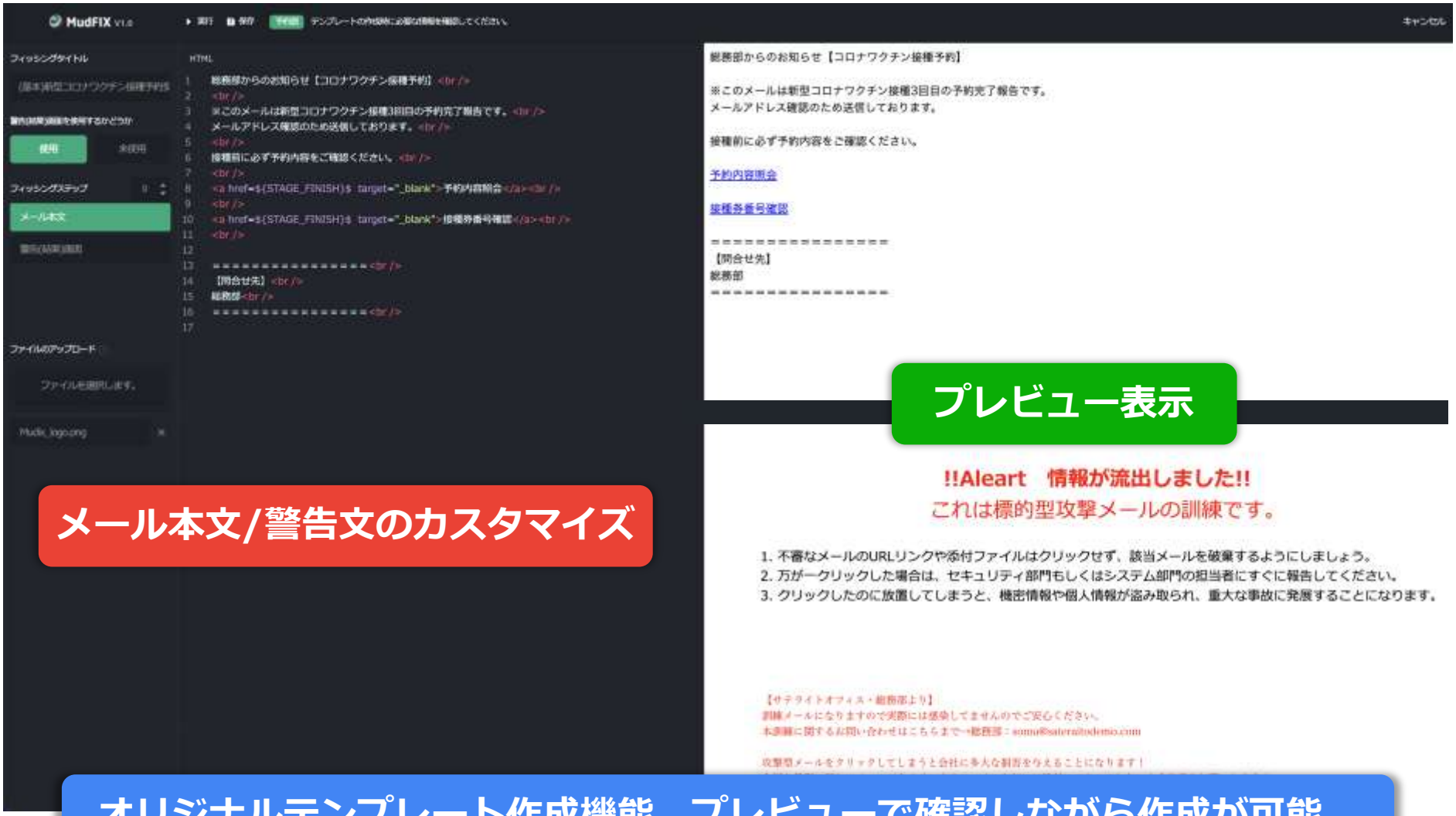
テンプレート管理



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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

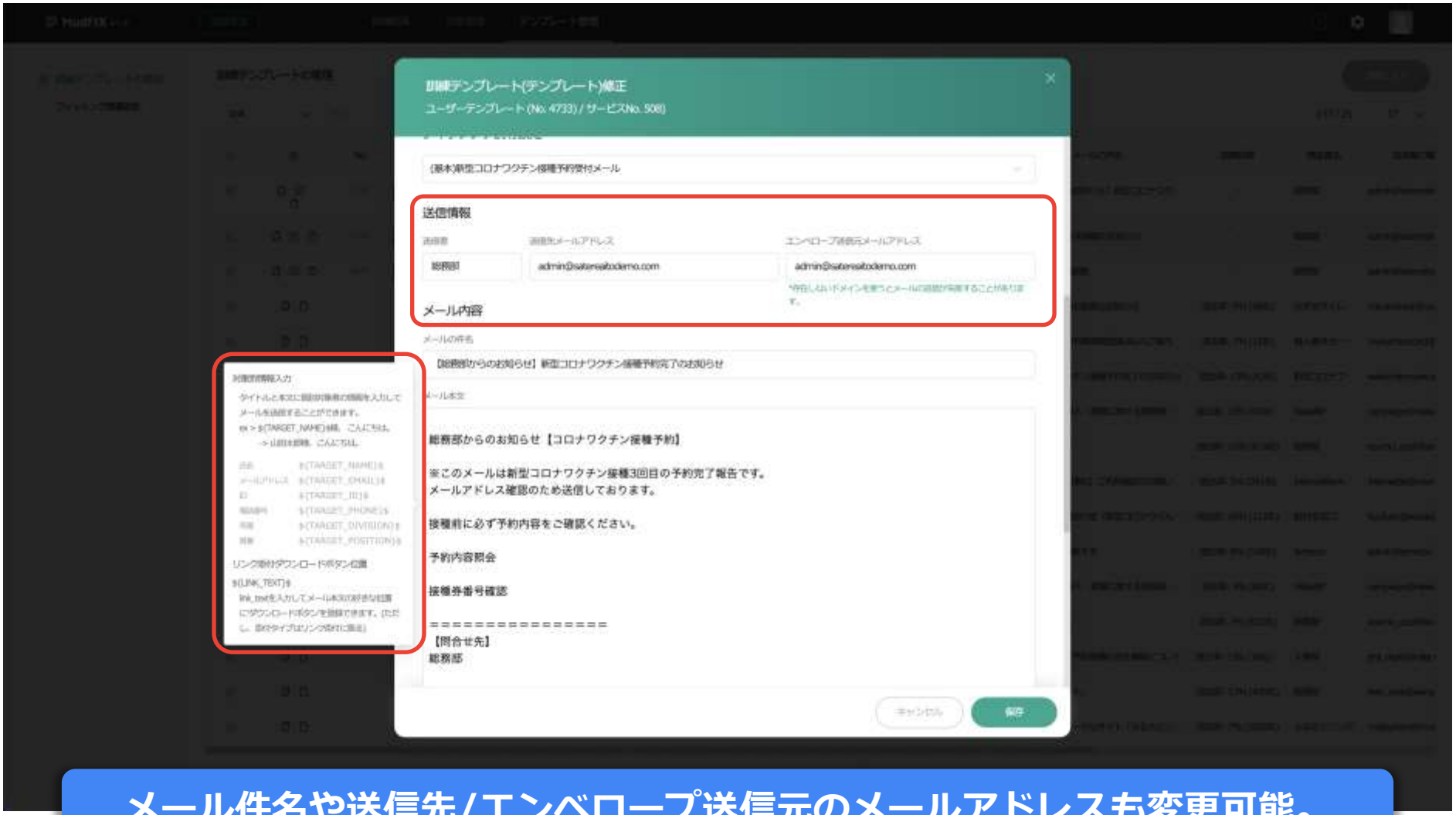
オリジナルテンプレートの作成



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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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。

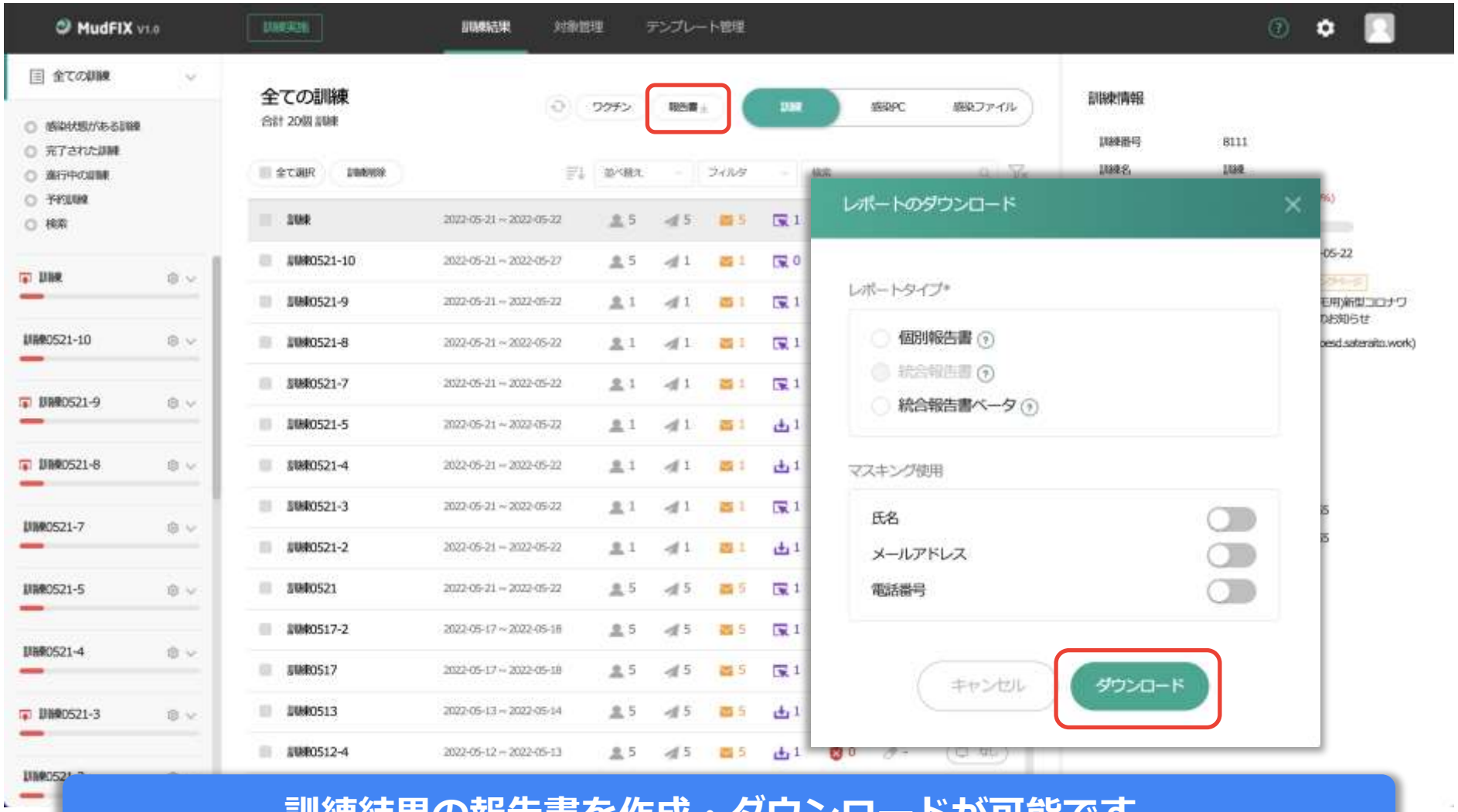
Copyright(c)2022 Sateraito Office, Inc. All rights reserved

インパクトのある警告画面で訓練の効果を上げる

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。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

訓練結果の報告書作成機能



訓練結果の報告書を作成・ダウンロードが可能です。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

最後に

本章は、その他の説明をします。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

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頂きます。

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ーの様な、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いきます。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いきます。満足度高いサポートを提供していきますので、よろしくお願いいたします。

Copyright(c)2022 Sateraito Office, Inc. All rights reserved

Sateraito ~ for your best solution

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

Copyright(c)2022 Sateraito Office, Inc. All rights reserved