

不審メールの報告件数が 約5〜6倍に。

AI分析で負担を軽減し、
訓練・教育を日常の行動につなげる



お話を伺った方

静岡銀行 リスク統括部

オペレーショナルリスクグループ

ITセキュリティ統括室長 木村 和紀 様

訓練から教育、日々の報告まで。 継続して学ぶ仕組みをつくる。

導入目的

- ・ 全役職員が繰り返し学び、不審メールへの判断力・行動力を高める
- ・ 訓練の結果を教育につなげ、日常の報告・対応まで一体で運用する

導入前の課題

- ・ 訓練の企画・実施・集計・教育に2〜3か月を要し、対象や頻度にも制約があった
- ・ 受信後の行動を十分に把握できず、不審メールの分析にも人手がかかっていた

導入効果

- ・ 全役職員への通年訓練と、結果に応じた教育を実施
- ・ 不審メールの報告件数が約5〜6倍に増加
- ・ AI分析で担当者の負担が大幅に減り、重要なメールの確認・対応に集中

※報告件数・業務負担の変化は、取材時点のお客様の申告に基づきます。

01 / INTERVIEW

システムの防御と人の行動を両輪に、役職員の対応力を継続的に高めていく

木村様：私たちITセキュリティ統括室は、静岡銀行のサイバーセキュリティを横断的に管理しています。サイバー脅威や脆弱性への対応、インシデント発生時の初動対応、そして役職員への教育が、主な役割です。

サイバー攻撃は、システムだけで防げるものではありません。特にフィッシングメールは、受信した一人ひとりが不審な点に気づき、迷ったら報告するという行動が重要です。技術的な対策と、役職員の判断力・行動力を高める取り組みを両輪で進めています。

2025年にスタートしたサイバーセキュリティの中期計画でも、役職員への教育研修を重点目標に据えました。訓練を一度実施して終わりにするのではなく、継続して学び、実際の対応力を高めていく。そのための仕組みが必要だと考えていました。

企画から教育まで2〜3か月。訓練をしても、実際の対応力を把握しきれなかった

木村様：導入前に最も困っていたのは、不審メール訓練にかかる実施コストの高さと、実効性の低さでした。従来の仕組みでは対象者が限られ、添付ファイルを開いたのか、URLをクリックしたのか、その後にどのような行動を取ったのかを、システム上で十分に把握できなかったのです。

過去には約200人に個別アンケートを行い、結果を手作業で集計したこともあります。配信にも時間がかかり、企画・実施・集計・教育という一連のサイクルに2〜3か月を要していました。

さらに、メールの文面や添付ファイルにも制約があり、最新の攻撃手口を柔軟に反映しにくい状況でした。すぐに訓練だと分かるメールでは、本番の攻撃への対応力を測りにくくなります。対象を広げること、リアリティを高めること、行動を正確に把握すること、結果を教育につなげること。この4つが課題でした。

最も危機感があつたのは、役職員の実際の対応力が分からないまま、攻撃手口が進化してしまうことです。生成AIの普及もあり、業務連絡やクラウドサービスの通知に似せた自然なメールが増えていると感じています。限られた対象者に同じような訓練を行うだけでは、組織全体の弱点を把握し、改善するには十分ではありませんでした。



インタビューの様子

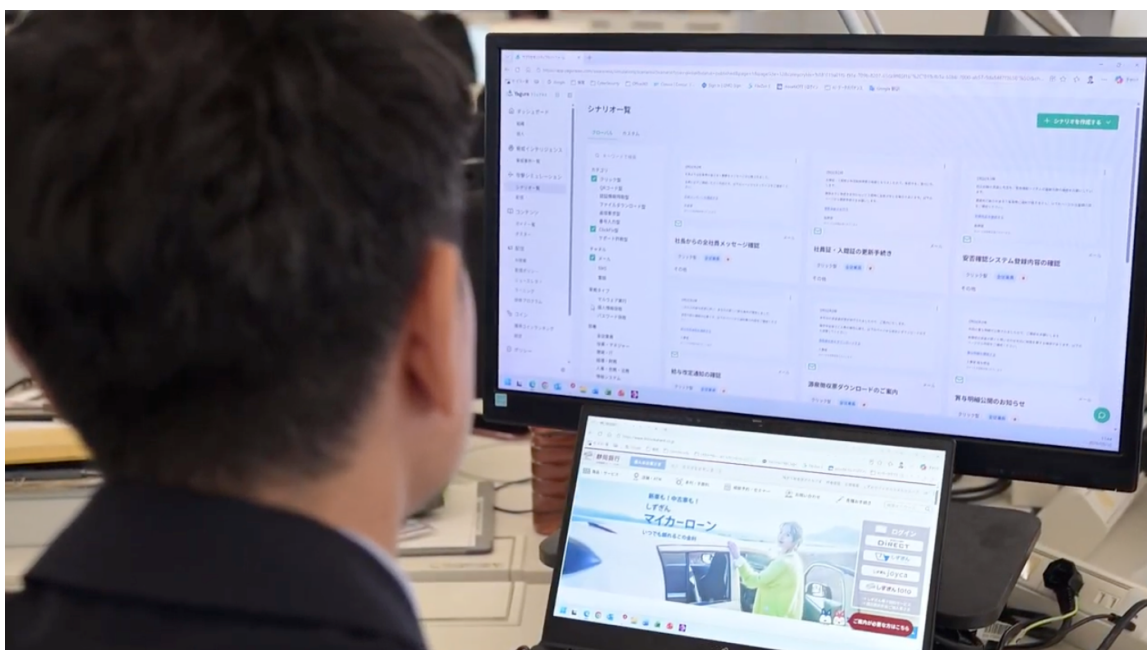
年1〜2回の「イベント」から、全役職員が繰り返し学ぶ訓練へ

木村様：従来の訓練結果から、役職員のリテラシー向上を急ぐ必要があると感じました。当時は限られた職員に年1〜2回の訓練を行うのみで、開封率も高い状態でした。より実効性の高い訓練を、全役職員に繰り返し実施したいと考えたことが、ヤグラを検討するきっかけです。

年に1回だけでは、訓練がイベント化し、「1回実施すればよい」と、実施そのものが目的になりかねません。誤った操作をしてしまった方に改善を促し、その後の変化を確認するためにも、継続して訓練と教育を行うことが重要です。

また、役職や業務によって普段受け取るメールは異なります。例えば、役員にはビジネスメール詐欺、システム部門にはクラウドサービスの通知、一般の役職員には認証情報を求めるメールといった形です。対象者に合わせて内容を変えることで、よりリアリティのある訓練にできると考えています。

現在はヤグラを通年のメール訓練に活用し、望ましくない対応をした役職員には教育コンテンツを提供しています。訓練の結果を、その後の学びにつなげる運用を進めています。



ヤグラの訓練シナリオを確認する様子

決め手は、訓練から教育までの一体化と、運用を一緒につくる支援の姿勢

木村様：ヤグラを選んだ決め手は、私たちの課題を、訓練の企画から教育まで一つの流れで解決できる点でした。全役職員への配信、行動の把握、結果の可視化、誤った操作をした人への教育コンテンツの提供まで、同じサービスで実施できます。最新の攻撃を反映したシナリオで、訓練だと見抜かれにくいメールを作成できる点も評価しました。

もう一つ大きかったのが、導入時の支援です。ヤグラの皆さんには、私たちと一緒に課題を一つずつ解決し、要望した配信期間や報告機能にも対応いただきました。機能だけでなく、導入後の運用を一緒につくっていただける姿勢と、レスポンスの速さが決め手になりました。

導入前には、当行のセキュリティ環境で訓練メールが正しく届き、必要な情報を取得できるのかという不安もありました。その点もサポートを受けながら課題を一つずつクリアでき、大きな不安を感じることなく導入できたのは、非常に助かりました。

報告件数は約5〜6倍に。判断に迷うメールも報告されるようになった

木村様：ヤグラは訓練だけでなく、役職員が日々受信する不審メールの報告にも使っています。Outlookのアドインを導入したことで、ボタンから簡単に報告できるようになりました。

これまでは多い日でも1日に数件程度でしたが、導入後は1日に10件以上、以前の5〜6倍程度の報告が実際に来ています。報告しやすくなれば、その分、確認するメールは増えます。そこでAI分析を活用することで、すべてを手で分析する業務の増大を避けられました。

報告されるメールの内容にも変化があります。以前は、個人のアカウントを狙ったフィッシングメールなど、明らかに怪しいと分かるものが多い印象でした。今は、Teamsで役職員から届く通知に見せかけたメールなど、本物かどうか判断しづらいものも報告されるようになっています。実際に引っかけやすい脅威に気づけるようになったことは、大きな変化です。

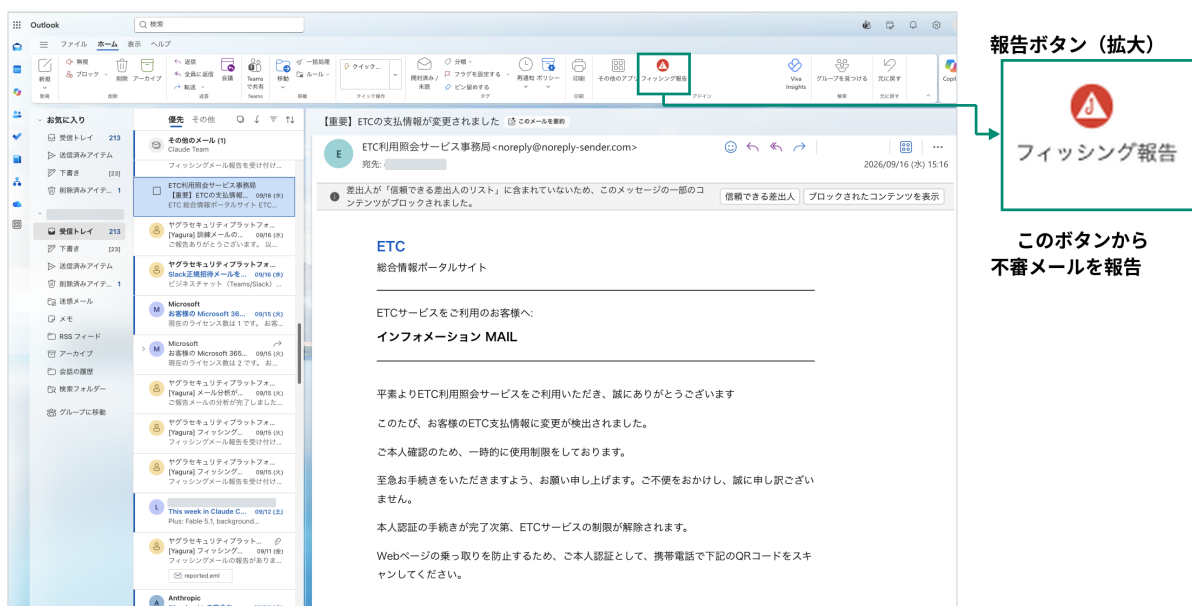
報告した役職員が、AIによる分析結果を数分で受け取れる点も重要です。不審かどうか分からないまま待つ不安が減り、より報告しやすくなるという効果も実感しています。「迷ったら報告する」という行動を、日常の中で取りやすくなりました。

現場から最も多かったのは、「不審メールを報告しやすくなった」という声

木村様：役職員から最も多かったのは、「不審メールを報告しやすくなった」という声です。とにかくボタンを押せば報告できます。以前は、転送によってヘッダー情報が壊れてしまうことがあり、スクリーンショットを撮って送るといった手順が必要でした。その手間が減ったことが喜ばれています。

全役職員に頻繁に訓練を行うようになった当初は、「このメールは訓練なのか」「不審だと思ったら報告ボタンを押せばよいのか」といった問い合わせもありました。これは、繰り返し訓練を行う中で解消していくものだと考えています。

訓練は、どうしても普段の業務の邪魔になるのではないかという懸念があります。簡単に報告できることで役職員の負担感が大幅に減り、訓練も行いやすくなったことは、うれしい点でした。



※ヤグラのデモ環境の画面です。静岡銀行様の環境・データではありません。
個人情報・重複する報告ボタンのみ非表示にしています。

大半のメールはAIが判定。人は、本当に注意すべきメールの分析に集中する

木村様：分析の負担は、かなり減ったと実感しています。以前は報告を受けると、自分でメールのヘッダー情報を確認していましたが、それでも「不明」となることが多く、悪性か良性かを判断しづらい部分がありました。今はAIが判定してくれるため、私たちが分析する作業が大幅に減りました。

AIの判定は基本的に信頼しています。個人のアカウントを狙うようなフィッシングメールはAIに任せる一方、役職員をかたる成りすましメールなどは、判定結果を確認したうえで、私たち自身でも内容を把握し、分析しています。

初期には曖昧な判定もありましたが、随時チューニングしていただき、最近はそうしたケースもなくなってきたと感じています。大半のメールをAIが判定してくれるため、本当に重要なメールに分析対象を絞れることに、最も効果を感じています。

The screenshot displays the AI SOC interface. On the left is a sidebar with navigation options: ダッシュボード, アラート, メモリ, SIEM, ログ検索, データソース, 収集サーバー, 使用量, 検知ルール, 参照リスト, 連携, 設定, Microsoft 報告連携, 通知設定, AI プロバイダ. The main area shows an alert titled '外部の gmail.com アドレスから Google フォームへ誘導する、株式会社ヤグラを名乗ったフィッシングメール'. It includes a summary section 'アラート要約' with details about the email's origin and content, a '元のメール' section showing the email header and body, and a '結論' section stating the email is a malicious phishing attempt. The interface also features filters for '対応状況' (未着手, 要対応, 悪意あり), '判定' (判定), and '担当者' (担当者を選択), along with buttons for '再調査', 'AIに質問', and 'コピー'.

ヤグラの自社環境でのサンプル画面

※静岡銀行様の環境・データではありません。フィッシングメール本文のURLは黒塗りしています。

AIによる不審メールの分析結果

※掲載画面はデモ環境のものです。静岡銀行様の環境・データではありません。

訓練・教育と日常の対応をさらに一体化。教育コンテンツを集約し、海外拠点にも学びを広げたい

木村様：今後は、訓練・教育と日常の不審メール対応をさらに一体化し、実効性を高めたいと考えています。最新の攻撃を反映した訓練や、要望に沿った教育コンテンツの充実には、引き続き期待しています。

現在は、訓練で望ましくない対応をした役職員への教育に使っていますが、今後はコンテンツをヤグラに一元化し、教育のハブとして活用していきたいですね。

教材作成の負担軽減にも期待しています。階層別の講習では、自分たちで話して動画を収録しているため、アバターなどを活用できれば助かります。海外拠点の教育も今後の課題です。多言語でのコンテンツ提供についても、ぜひ支援いただきたいと考えています。



業務中の様子

目的は、訓練を実施することではなく、組織全体のセキュリティレベルを上げること

木村様：不審メール訓練は、メールを送ってクリック率を測るだけでは、十分な効果につながりにくいと考えています。重要なのは、実際の攻撃に近い形で訓練を行い、利用者の行動を把握し、誤った操作をした人に教育を行って、それを日常の行動につなげることです。

不審メール訓練は、実施すること自体が目的ではありません。組織全体のセキュリティレベルを上げることが目的であり、メール訓練はその手段です。

同じような課題を持つ金融機関の皆さまにも、目的を達成するために何が必要かという視点で、サービスを比較していただきたいと思います。そうすると、訓練と教育を繰り返すことの重要性が見えてくるはずです。ぜひ、継続的な教育を重視して取り組んでいただければと思います。