News Release

報道関係各位

2026 年 3 月 19 日
トビラシステムズ株式会社

会社員の 4 人に 1 人が「ニセ社長詐欺」のメールを受信
急増するビジネスメール詐欺の手口＆アンケート調査レポートを公開

特殊詐欺やフィッシング詐欺の対策サービスを提供するトビラシステムズ株式会社（本社：愛知県名古屋市、代表取締役社長：明田 篤、証券コード：4441、以下「トビラシステムズ」）は、法人の経営者等になりすまして偽のメールやメッセージを送り、業務を装って指定した口座に送金させ、金銭をだまし取る「ニセ社長詐欺」（いわゆるビジネスメール詐欺）について、実際の手口を調査しました。また、全国の会社員を対象に、昨今増加する「ニセ社長詐欺」に関するアンケート調査を行いました。

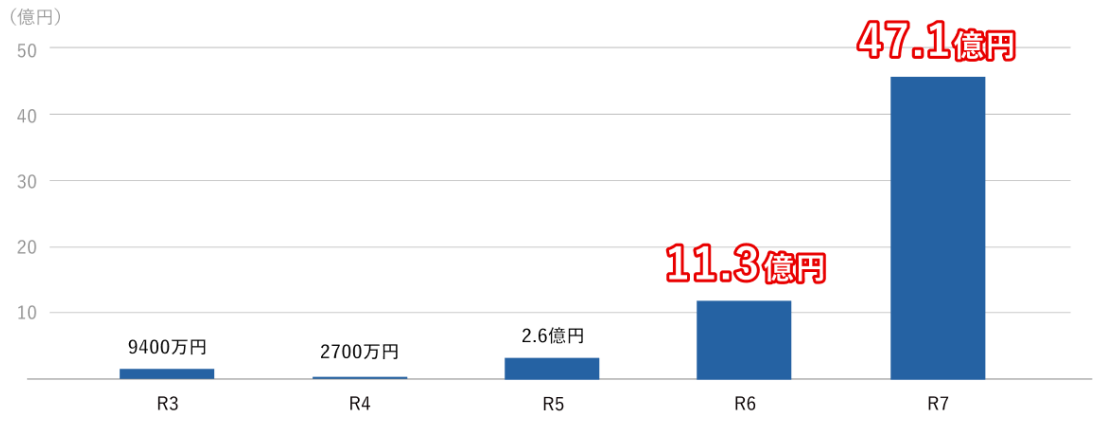
新年度は、新入社員の入社や人事異動などにより、社内体制が変化しやすい時期です。本レポートを、法人における詐欺被害防止にお役立てください。

＜調査サマリー＞

- ◉ 詐欺の標的が“個人”から“法人”へ、インターネットバンキング不正送金被害 47 億円
- ◉ 社長をかたり「今すぐ送金」LINE で指示、ニセ社長詐欺の実際の手口を公開
- ◉ ニセ社長詐欺の認知度は約 50%、知ったきっかけは「テレビ」や「社内の注意喚起」
- ◉ 会社員の 4 人に 1 人が社内でニセ社長詐欺のメールを受信した経験あり
- ◉ 対策は「注意喚起」が中心、セキュリティ教育・訓練など実践的対策は約 3 割ほど

■概況：拡大するビジネスメール詐欺の脅威

インターネットバンキングに係る不正送金の発生金額推移（法人の抜粋）



警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」をもとに当社作成

警察庁サイバー警察局の発表によると、令和 7 年の法人におけるインターネットバンキングの不正送金被害額は 47 億円で、前年の約 4 倍に増加しています。

近年、企業を標的としたサイバー犯罪として「ビジネスメール詐欺」の被害が深刻化しています。特に、社長や役員を装ったメールを送り、業務を装ってメッセージアプリに誘導し、指定の口座に送金を指示することで企業から金銭をだまし取る「ニセ社長詐欺」が増加し、一件で数億円規模の被害も発生しています。

これまで詐欺の主な標的は個人でしたが、現在は法人を狙うケースが増加しています。特に中小企業では、大企業と比べてセキュリティ対策のリソースが限られていたり、承認フローが十分に整備されていなかったりする場合があり、標的となりやすい状況が指摘されています。

また、新年度は人事異動や新入社員の入社で組織内のコミュニケーションが変化しやすく、こうした隙を突いた攻撃に備え、社内でのセキュリティ教育や意識向上が求められます。

＜参考資料＞

令和 7 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁サイバー警察局）

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

■ニセ社長詐欺の実態調査

トビラシステムズでは、「ニセ社長詐欺」の手口について、実際の手口をもとに調査を行いました。

【手口の流れ】

1．実在する企業の社長になりすました人物から、公開されている企業のメールアドレスや従業員のメールアドレス宛にメールが届く。メールの中で「業務に必要なため、LINE グループを作成し、招待用のコードを送付するように」などと指示される。

2. メールの指示に従うと、従業員が作成した LINE グループに、社長になりすました人物が参加する。グループに経理担当者を追加するように指示されたり、法人の口座情報や口座残高を教えるよう指示されたりする場合がある。

3. 「今すぐ取引先に送金が必要」などの理由で、指定の口座に金銭を振り込むよう命じられる。振り込むと、詐欺グループに金銭が渡る。

社長を装う「ビジネスメール詐欺」の手口 （トビラシステムズ調べ）

詐欺メールの例

メールを受け取った後
今後の業務プロジェクトに対応するため、新しいLINEのワークグループの作成をお願いいたします。
グループへの他のメンバーの追加は、私が参加した後に行います。
グループ作成が完了しましたら、そのグループのQRコードを生成し、このメールにご返信ください
<[redacted]@outlook.jp>。
私がQRコードからグループに参加し、その後の業務調整を進めさせていただきます。
お手数をおかけしますが、よろしくお願いいたします。

トビラシステムズ株式会社
代表取締役
明田 篤

（当社に届いた実際のなりすましメール）

LINE グループを作成

（実際のLINEのやり取り）

【被害にあわないための対策】

・差出人のメールアドレスを確認

なりすましメールには、フリーメールのアドレスが使用される場合が多数確認されています。
届いたメールの送信元のアドレスが正しいものかよく確認してください。
送信元のメールアドレスが会社公式のドメインでなく、フリーメールの場合は注意してください。

・LINE でお金の話は詐欺を疑う

LINE などのメッセージアプリに移動し、銀行口座の情報や残高を教えるよう求められたり、送金を指示されたりした場合は、詐欺を疑ってください。

・一人で判断せず周りに相談

不審なメールやメッセージが届いた場合は、一人で判断せず、周りの人に相談してください。
社内での注意喚起や相談フローの確認などを行い、連携を強化してください。

実際の手口をもとに解説した動画を、当社 YouTube で公開しています。
（動画 URL）https://youtube.com/shorts/aYHpwbAEVw4

■「ニセ社長詐欺」に関するアンケート調査

トビラシステムズは、全国の会社員を対象に、「ニセ社長詐欺」に関するアンケート調査を行いました。

【調査概要】

調査実施会社：トビラシステムズ株式会社

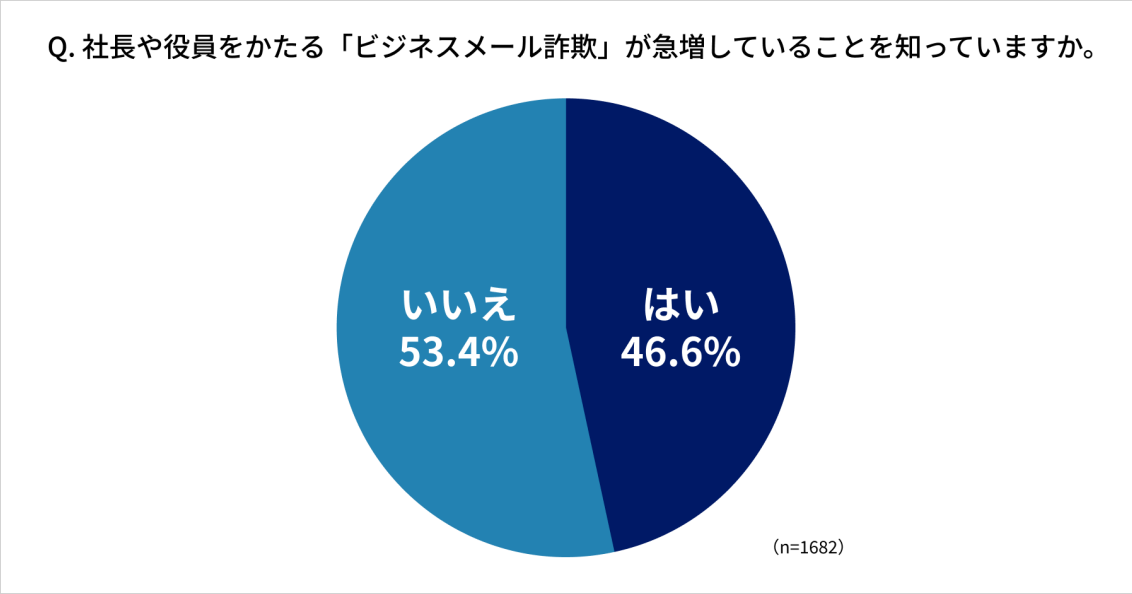
実施期間：2026 年 2 月 9 日～2 月 10 日

対象：全国の 25～60 歳の会社員の男女

有効回答数：1,682

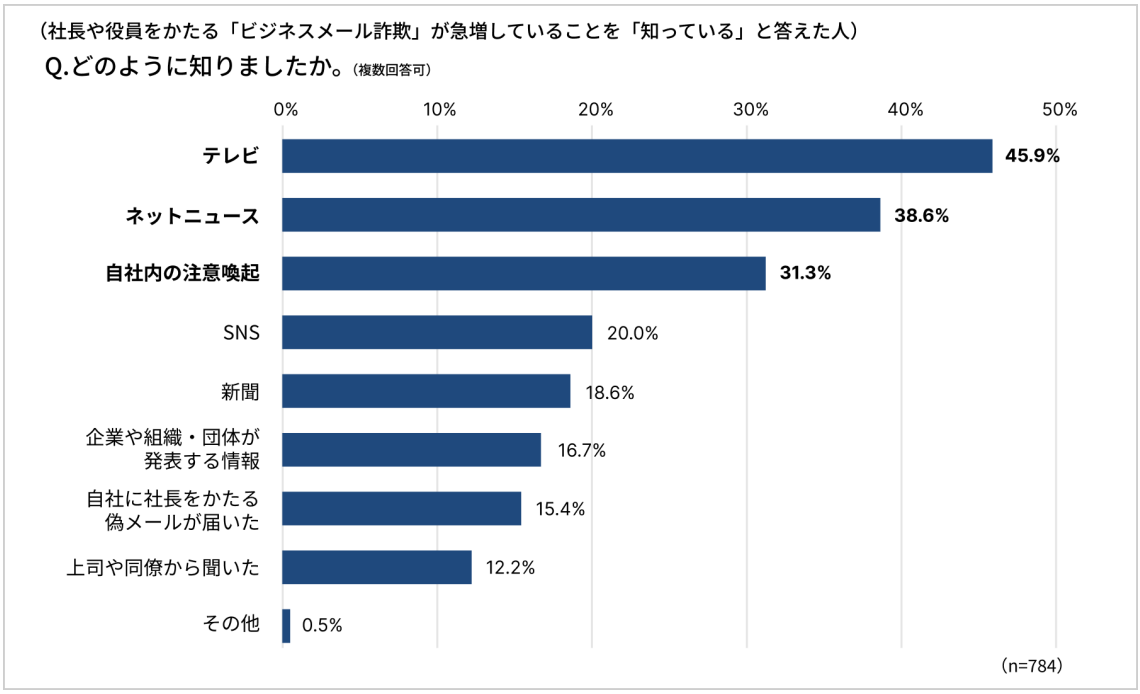
調査方法：インターネット調査（Surveroid を利用）https://surveroid.jp/

◯ニセ社長詐欺の認知は約半数にとどまる



社長や役員をかたるビジネスメール詐欺（ニセ社長詐欺）が急増していることを知っているかという質問で、「はい」と答えた人は 46.6%で、会社員のおよそ半数が手口について認識していることがわかりました。一方で、53.4%の人は手口について知らない可能性があります。

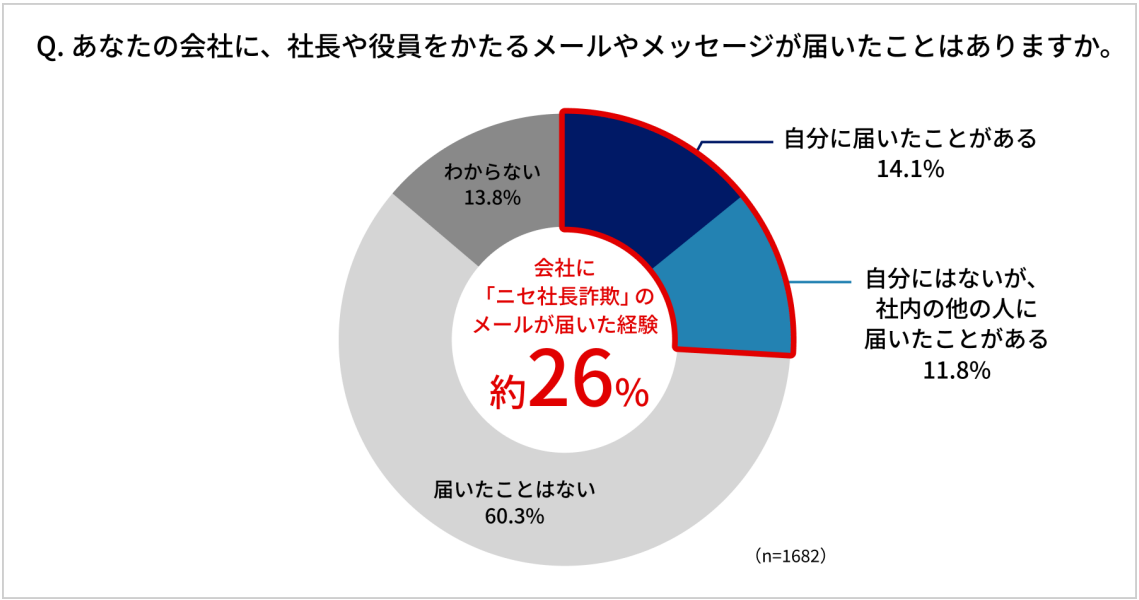
◯認知のきっかけはテレビ・ネットニュースなどの報道が中心



前述の質問で、ニセ社長詐欺が急増していることについて知っていると答えた人に対し、どのように知ったかを聞いたところ、最も多かったのは「テレビ」が 45.9%、次いで「ネットニュース」が 38.6%、「自社内の注意喚起」が 31.3%でした。

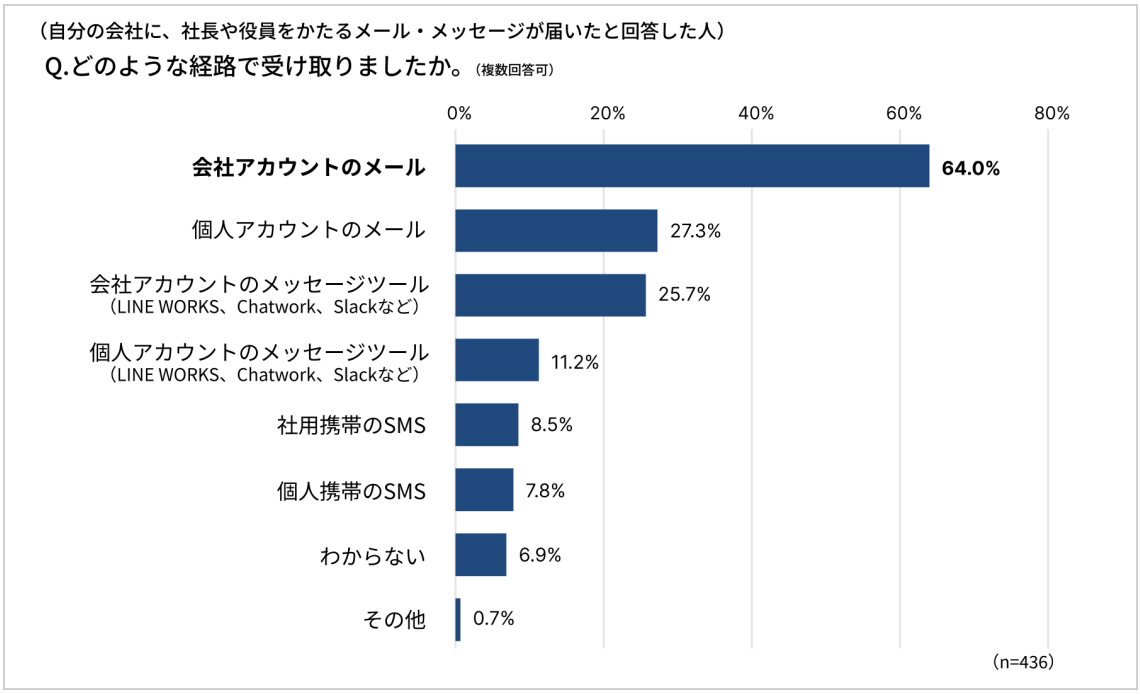
「自社に社長をかたる偽メールが届いた」ことで知ったと回答した人も 15.4%おり、一定数の会社員に同手口のメールが届いていることがわかりました。

◯4 人に 1 人が社内でニセ社長詐欺のメールを受信した経験



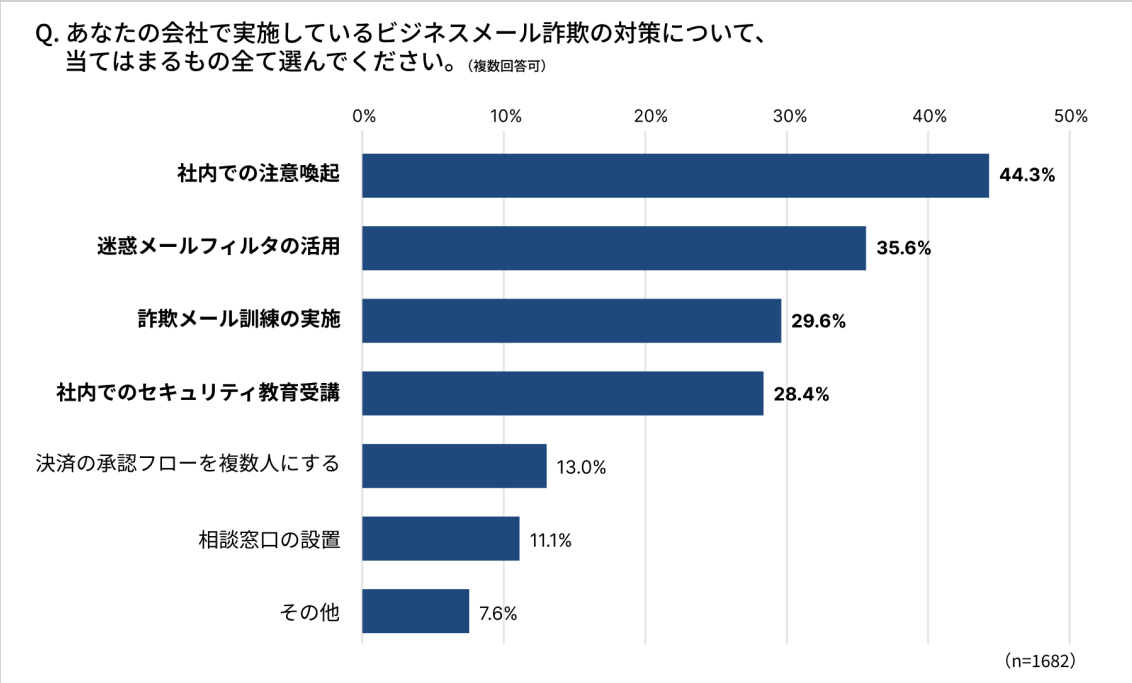
「あなたの会社に、社長や役員をかたるメールやメッセージが届いたことがあるか」と質問したところ、「自分に届いたことがある」は 14.1%、「自分にはないが、社内の他の人に届いたことがある」が 11.8%で、４人に１人（合計 25.9%）の会社員が、自身や周囲で「ニセ社長詐欺」のメールが届いた経験があることがわかりました。

◯ニセ社長詐欺の主な受信経路は「会社アカウントのメール」



自分の会社に、ニセ社長詐欺のメールやメッセージが届いたことがあると答えた人に対し、どのような経路で受け取ったかを聞いたところ、「会社アカウントのメール」が 64.0%で最も多い結果となりました。次いで、「個人アカウントのメール」が 27.3%となりました。会社アカウントの様々なメッセージツールにおいても、偽のメッセージを受けとっている人が 25.7%いることがわかりました。

◯企業の対策は注意喚起が中心、実践的対策は約 3 割にとどまる



会社で実施しているビジネスメール詐欺の対策について、最も多かったのは「社内での注意喚起」が 44.3%でした。また、「迷惑メールフィルタの活用」も 35.6%となりました。「詐欺メール訓練の実施」は 29.6%、「社内でのセキュリティ教育受講」が 28.4%で、日頃から詐欺やサイバー犯罪に対して備えている会社も一定数あることがわかりますが、その数は 3 割程度にとどまりました。

■調査結果のまとめ

◯ニセ社長詐欺の認知は半数程度にとどまる

社長や役員をかたるビジネスメール詐欺（ニセ社長詐欺）が急増していることを「知っている」と回答した人は 46.6%で、会社員の認知は約半数程度でした。主な情報源は「テレビ」や「ネットニュース」である一方で、「社内の注意喚起」も一定の役割を果たしていると考えられます。

◯4 人に 1 人が自分または社内でニセ社長詐欺のメールを受信

社長や役員をかたるメールやメッセージが「自分に届いたことがある」は 14.1%、「自分にはないが社内の他の人に届いたことがある」は 11.8%で、合計 25.9%（約 4 人に 1 人）が、自分または周囲でビジネスメール詐欺を受信した経験があることがわかりました。受信経路は「会社アカウントのメール」が最も多く、業務用のメールアドレスが主なターゲットとされていることがわかります。

◯企業の対策は進みつつあるが、十分とは言えない状況

企業の対策としては「社内での注意喚起」や「迷惑メールフィルタの活用」が多く挙げられました。一方で、「詐欺メール訓練」や「セキュリティ教育」など、実践的な対策を実施している企業は約 3 割にとどまり、組織的な対策強化の余地があることがうかがえます。

■法人向け詐欺メール・SMS 訓練サービス「サギトレ」

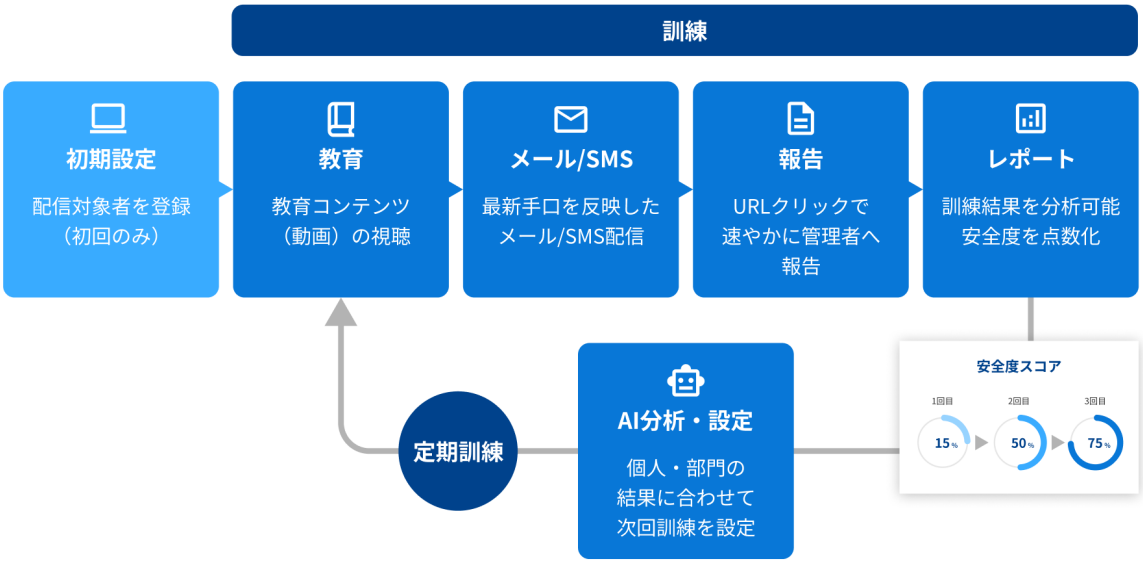
「サギトレ」は、法人におけるセキュリティ教育やリスクへの対応力向上を目指した、詐欺メール・SMS 訓練サービスです。

ユーザー企業の従業員は、「サギトレ」のシステム上で詐欺の手口や注意すべきポイントを学ぶ教育コンテンツを視聴し、その後、実際の業務環境の中で疑似的な詐欺メール・SMS を受信します。AI がその対応結果を分析し、個人や部門ごとのリスク傾向を可視化。分析結果に基づき、最適な訓練内容や配信スケジュールを自動で設定します。

これにより、運用担当者の負担を抑えながら継続的に訓練を実施することができます。さらに、訓練の積み重ねを通じて、従業員のセキュリティ意識と組織全体のセキュリティレベルを向上させます。

「サギトレ」サービスサイト：https://sagitore.com

「サギトレ」AI自動訓練イメージ



■トビラシステムズについて

テクノロジーで社会課題の解決を目指し、特殊詐欺やフィッシング詐欺、グレーゾーン犯罪撲滅のためのサービスを提供しています。詐欺電話・詐欺 SMS 等の情報を収集・調査してデータベースを構築し、自動でフィルタリングする「迷惑情報フィルタサービス」は、固定電話、モバイル、ビジネス向けに展開し月間約 1,500 万人にご利用いただいています。

＜会社概要＞

会社名　　：トビラシステムズ株式会社
代表者　　：代表取締役社長　明田 篤
証券コード：4441（東証スタンダード市場）
設立　　：2006 年 12 月 1 日
所在地　　：愛知県名古屋市中区錦 2-5-12 パシフィックスクエア名古屋錦 7F
公式サイト：https://tobila.com/

＜本件に関する報道関係のお問い合わせ先＞

トビラシステムズ株式会社　広報担当
電話番号：050-3646-6670（直通）
お問い合わせフォーム：https://tobila.com/contact/