

標的型攻撃メール訓練・教育サービス

2026年版・お役立ち資料

導入から運用定着までの ステップガイド

セキュリティ意識も定着させる
実践的メール訓練の教科書



本資料の目的・留意事項

Purpose and Notes

メール訓練を「一度きりの施策」ではなく、
組織に定着するセキュリティ文化へと
進化させるための実践ガイドです。



本資料の目的は、メール訓練を単なる注意喚起や形式的な取り組みで終わらせず、社員・職員の方々一人ひとりが無意識のうちに正しい判断・行動を取れる状態をつくることにあります。

そのために、「なぜ従来の訓練は形骸化しやすいのか」という課題を整理したうえで、アクモスが提供する訓練サービスを活用しながら、導入・運用・改善を継続するための考え方と具体策を解説しています。

本資料は、情報システム部門や総務部門など、訓練の企画・運用を担う方が、自社の状況に合わせて施策を検討・説明・実行できることを意図して構成されています。

本資料でお伝えするポイント

- ✓ メール訓練が「やったつもり」で終わってしまう構造的な原因
- ✓ セキュリティ意識を“習慣”として定着させるための考え方と設計要素
- ✓ 実運用を見据えた、無理なく続けるための具体的ステップと工夫

※本資料は、一部生成AIを使用した画像が含まれています。

※組織内部での参考資料としてご活用ください。第三者への無断配布やネット上での再配布などは禁止しています。

※本資料の内容は、当社が提供する「標的型攻撃メール訓練・教育サービス」の機能をベースに、これまでの運用実績から得られた知見をもとにまとめたものです。機能の適用範囲について、記載されている施策や運用例の一部は、お客様のご契約プランや導入環境の差異により、標準機能として提供できない場合があります。また、内容の解釈について、本資料は一般的な運用ガイドとしての提示を目的としており、すべての組織において同一の効果を保証するものではありません。

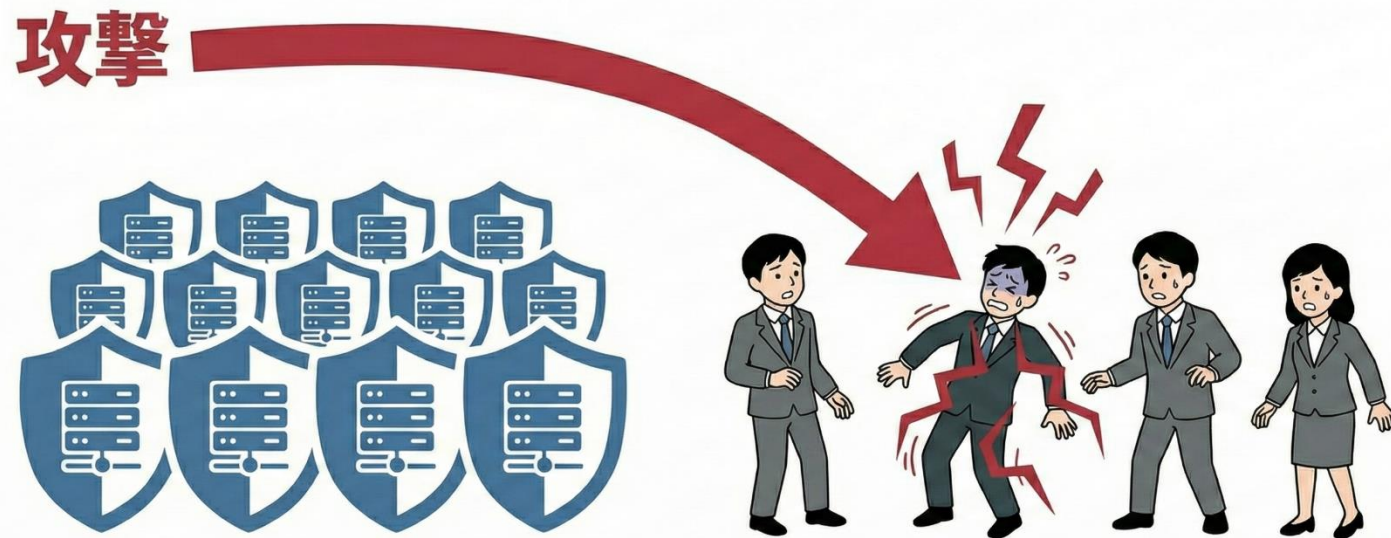
※運用方法は一例であり、実際の導入にあたっては各社の環境・規程・リスクレベルに応じた検討が必要です。

システムだけでは守れない時代

セキュリティ投資をしても、最後の1クリックを防ぐのは「人」の意識です。

ゼロトラストや境界防御が進化する一方、攻撃者はシステム内部の「人の判断」を狙っています。

実効性あるセキュリティには、システム防御に加え、最後の砦となる“人の判断・行動”の強化が不可欠です。



ソーシャルエンジニアリングによる被害



データ侵害の約7割は「人のミス」

フィッシングへの反応や設定ミスなど、技術対策をすり抜けた人的要因が主要な侵入経路となっている。



攻撃の入口は「社内の人」

侵害の93%は外部攻撃者によるもの。しかし実態は、人をだまして内部者の権限を奪う手口が中心。



攻撃の目的はほぼ「金」

サイバー攻撃の97%は金銭目的。攻撃は偶発ではなく、利益を狙ったビジネスとして行われている。

出典元：Verizon社『2024 Data Breach Investigations Report (DBIR)』より

なぜ、思ったようにメール訓練は効果が出ない？

実際の攻撃を防ぐ力へと変えるためには、「体験」と「継続・習慣」が大切です

よくある課題

多くの企業でメール訓練の導入・検討が進む一方、実際にはリスクを見過ごした“形骸化した訓練”も少なくありません。

不審点に気づく成功体験と成長機会の不足

- ✓ まずは典型的な不審点に気づく成功体験を積み重ねることが、教育効果向上につながる
- ✓ 基本的な防御行動を定着させるため、初期段階では分かりやすい訓練設計が重要



一過性の訓練と継続視点の不足

- ✓ 年1回でも継続的な訓練実施が、セキュリティ意識維持には重要
- ✓ 単発施策で終わらせず、難易度や頻度を見直しながらか継続運用することが必要



目指すのは習慣化

攻撃メールは「急ぎ」「重要」といった感情に訴え、無意識の反射行動を狙うため、正しい対処習慣の定着が重要です。

「理解している」から「実践できる」への定着

- ✓ 分かりやすい訓練による「気づけた」成功体験が、教育効果を高める
- ✓ 「見破る・破棄・報告」を繰り返し経験することで、自然な防御行動が定着する



「防御行動」の習慣化と継続運用

- ✓ 継続的な訓練により、不審メールを瞬時に見抜く判断力を定着
- ✓ 難易度や頻度を定期的に見直し、中長期的に組織の防御力を強化



運用ロードマップ

担当者が押さえるべき、メール訓練の全体像と実施フローです。

計画・準備フロー

実施・教育フロー

STEP 01



計画

目的・目標設定や
プラン設定

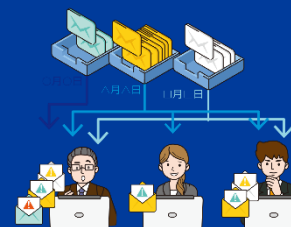
STEP 02



準備

訓練対象者・グループや
訓練内容(タスク)を作成

STEP 03



実施

訓練メールの送信
種明かし

STEP 04



分析・教育

レポートでの結果確認や
教育コンテンツの展開

STEP 01 計画（自社の成熟度に合わせて目標設定）

① 自社のIT教育のフェーズや訓練経験の有無によって目的や目標、配信対象などプランを設定します。

項目	プランA・初訓練の場合(例)	プランB・継続訓練の場合(例)
目的例	攻撃メールに対するITリテラシーの現状把握 ベースラインを測定したい	攻撃に対する行動を変えたい セキュリティ文化を醸成したい
科学的な視点	組織の「能力」の現状値を測定する	忘却の壁を越え、継続的なきっかけによって記憶 と行動として定着させる
目標・ 効果測定指標	①リンククリック率	①リンククリック率 ②添付ファイル実行率 ③報告数など（システムでの計測は不可・手動計測）
配信方式	一斉配信（全社または部署単位）	ランダム・分散配信
対象設定	全社員を対象に送信	前回クリック率の高かった部署や、重要部署にむ けて送信
その他	・まずはスポットで効果測定をしたい ・初めての訓練のため社員の反応を知りたい	・継続的な訓練で、人の防御を文化にする ・正しく報告、対応する行動を定着させる

POINT！



ポジティブな動機付けを

自社の実態を正確に把握するには、**抜き打ちの訓練も有効**です。
ただし実施前に、「セキュリティ向上を目的とした訓練を行う」と**周知しておくことを推奨**します。
万が一、メールを開封した社員がいても、処罰ではなく学習の機会とするという方針を共有することで、**安心して参加できる訓練**になります。

STEP 01 計画（自社の成熟度に合わせて目標設定）

②スケジュールやプランに直結するため、目標設定が最も重要となります。

目標は最初から高く設定するのではなく、**段階的にテーマを持ちながら訓練を実施することが効果的**です。

【段階別目標例】



STEP 02 準備（ターゲットとシナリオの最適化）

効率化



訓練の成否は、
適切な**対象設定**と
運用の効率性に左右されます

- CSVによる一括登録で、大規模組織でも迅速に登録・管理できる
- 部署・役職・拠点など**グループ化**して、特性に合わせた柔軟な訓練設計が可能

シナリオ案



URL型

まずは**不審なURL**をクリック
しないという、セキュリティの
基本動作を徹底させる



添付ファイル・標的型

訓練に慣れてきた段階で、
実務を装った「業務連絡風」や
「添付ファイル型」へ移行



品質保持



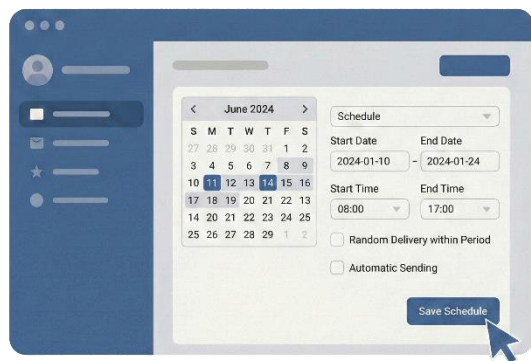
事前周知や**種明かしのタイミング**、
内容を適切に設定することで、
訓練の公平性と教育効果を担保

- 訓練があることを**事前に社内周知**して混乱を防ぐ
- 訓練メールの**種明かしタイミング**によって、訓練の効果が異なる
 - 即時：危機感を即座に醸成できる
 - 時間を置く：訓練メールのURLをクリックするなどの報告・対応行動の有無を確認できる

STEP 03 実施（運用工数を最小化する自動化と品質向上）

スケジュール設定

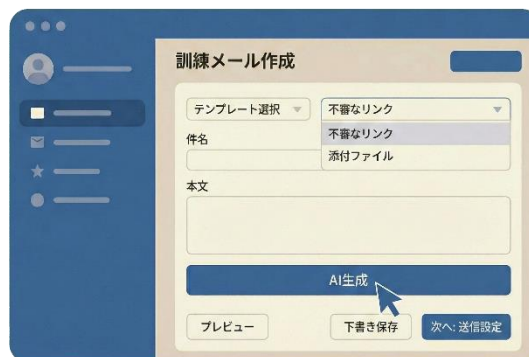
管理者の手間を減らすスケジュール運用



配信期間を設定するだけで自動配信が行われ、送信操作なしに日常業務を止めず訓練を継続でき、さらにランダム配信により受講者にとって予測不能な実戦に近い環境を構築できます。

訓練メールの作成

最新かつ現実的なメール作成・編集



最新の攻撃トレンドを反映したテンプレートを基に、目的に合わせて編集でき、AI機能により手間をかけず実践的な訓練メールを作成できます。

※AI機能はCoTraプランのみの提供です

種明かし

学びを最大化する種明かしの工夫



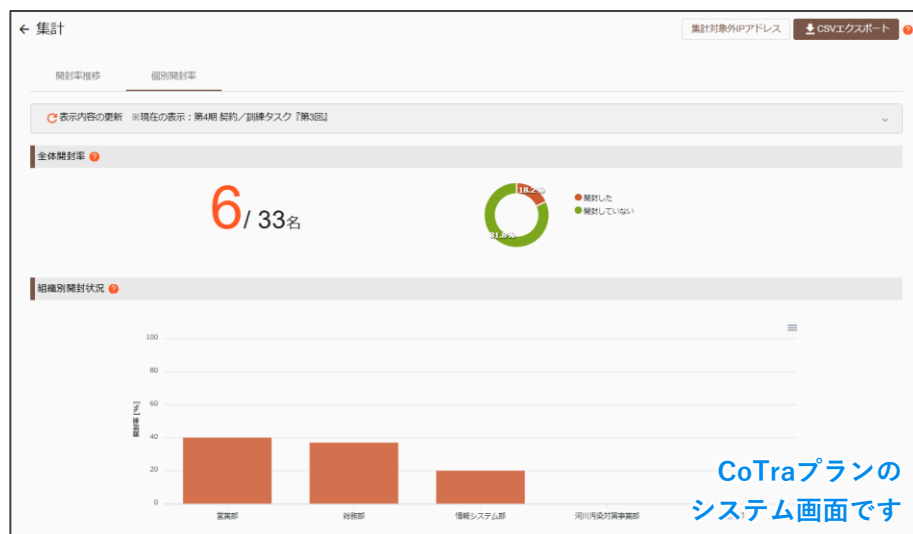
記憶が最も鮮明なタイミングで種明かしを行い、教育コンテンツへの誘導や次の行動（報告など）を促す工夫により、訓練効果を高めます。

準備と実施の負担を最小化することで、
年1回の行事ではなく日常的なセキュリティチェックとして定着させ、訓練効果を高めます。

STEP 04 分析・教育（改善に向けた分析と気づきを促すフォローアップ）

クリック率に加え多角的な分析でリスクを可視化し、的確な教育につなげます。

集計結果で分析



システムで計測できるリンククリック率や添付ファイル実行率などを把握することで、組織の真のITリテラシーを測定でき、より良い改善につながります。

eラーニングや教育用コンテンツ



訓練対象者には可能な限りその場で教育コンテンツを提供し、訓練時に限らず多様かつ最新の内容で定期的に教育を行うことが、組織全体のセキュリティ力向上を支えます。

①リアリティを持たせる

課題

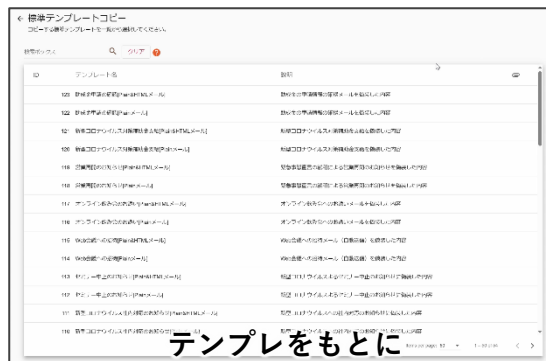
01

訓練だとすぐに見破られてしまわないようにする

解決策

攻撃メールを完全再現する「最新テンプレート」活用

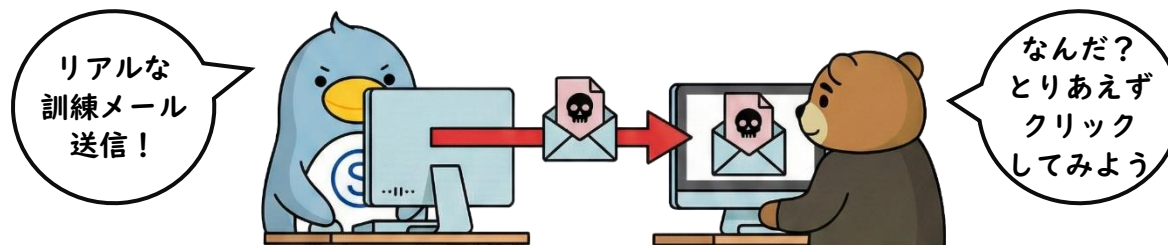
最新事例を基にした攻撃・詐欺メールのテンプレートや自作機能、生成AI機能を活用。巧妙化する攻撃手法の「今」を捉えた、リアルな訓練環境を整えることが重要です。



テンプレをもとに
精巧な訓練メールを作成



生成AIによる
攻撃メール作成
※AI機能はCoTraプランのみの提供です



効果

危機感が「自分事化」を加速させる



本物と見紛う体験により、「自分も騙されるかもしれない」という気づき生まれる



本番と同じ緊張感を体験することで、セキュリティを他人事ではなく、自分に関わるリスクとして認識する



この健全な危機感が、日常業務における反射的な防御行動の土台となる

②いつ来るかわからない緊張感を

課題

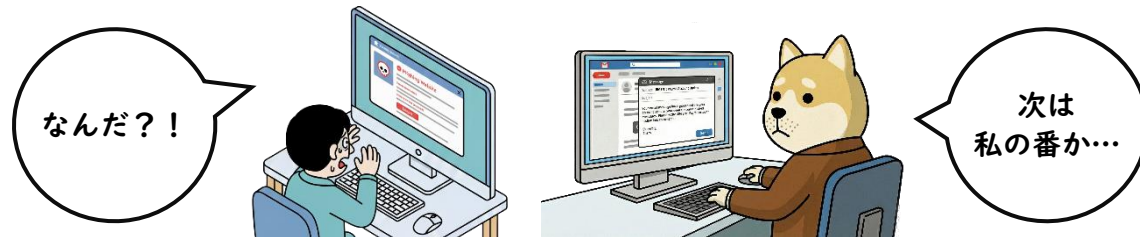
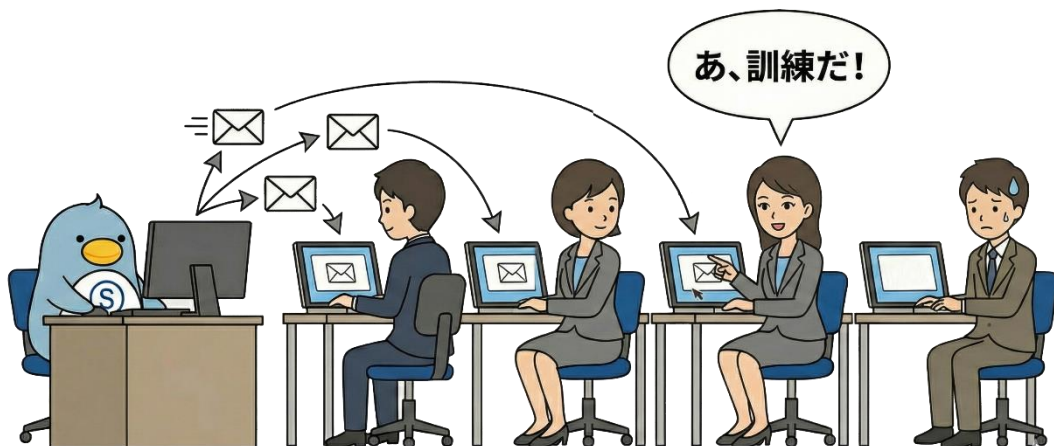
02

他社員に届いたから自分も訓練がある、という情報回覧を防ぐ

課題

「答え合わせ」が訓練の効果を半減させる

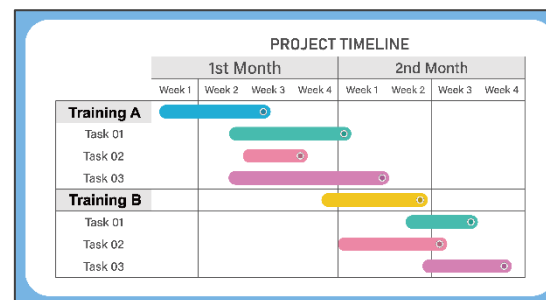
従来のメール訓練の大きな課題は、周囲の受信状況からすぐに訓練だと気づいてしまい、本番を想定した状態で受信できない点にあります。



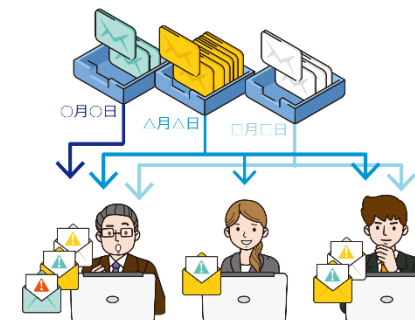
解決策

配信スケジュールを工夫して実戦に近い環境状況に

本質的な防御力を養うため、「いつ来るかわからない」という実戦に近い環境を意図的に作り出し、予測不能な配信にして社員の意識を実戦モードにします。



1年に全社1回だけではなく、複数回に分けてメール配信する



同一組織内であっても、一人ひとり異なるタイミングでメールを配信

アクモスメール訓練「CoTraプラン」で実現可能

③鉄は熱いうちに打つ

課題

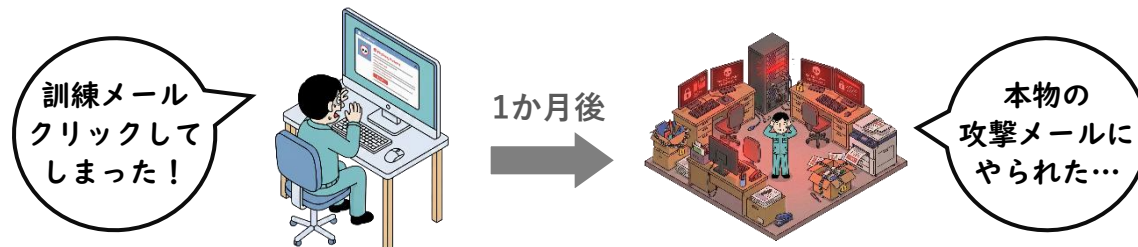
03

クリックした瞬間の感覚を 忘れられないようにする

課題

時間の経過とともに風化する「失敗の記憶」

従来の訓練で最も大きな損失は、「教育までのタイムラグ」による機会損失です。訓練実施から1ヶ月後にレポートでフィードバックを受けても、社員はクリックした瞬間の状況や心理状態を既に忘れていきます。



解決策

感情が動いた瞬間に届ける「即時種明かし画面」

クリックという「ミス」を最大の学習機会に変えるため、訓練メールの即時種明かしなどにより、気づきが最も高まるタイミングで学習を行う計画にします。



訓練メールの計画時に
即時種明かしを選ぶ



訓練直後に教育コンテンツへ誘導し
関心が高いタイミングで学習させよう

形骸化させないための「運営術」

01 経営層を巻き込む



社長自らが「私も訓練対象だ」と宣言してもらうインパクト

メール訓練が現場任せになると、「やらされ施策」と受け取られやすくなります。経営層が自ら訓練対象になる姿勢を示すことで、セキュリティは全社で取り組む経営課題であることが明確になります。

02 サンクス文化の醸成



怪しいメールを報告した社員を褒める仕組みづくり

引っかけたこと以上に、気づいて報告した行動に着目して評価することが重要です。感謝のメッセージなど小さなフィードバックを重ねることで、報告しやすい雰囲気が生まれ、被害の未然防止につながります。

03 結果のオープン化



ゲーム性を少し持たせることで参加意識を高める

部署別などで結果を可視化することで、訓練は他人事から自分事へと変わります。軽いランキングや共有により、責めるのではなく、前向きな改善意識と継続参加を促します。

組織のセキュリティ意識が劇的に変わった2つのケース

一過性のイベントから脱却し、継続的な文化として定着したことでセキュリティ力が向上。

事例 1 製造業・社員2,000名



課題

年1回の訓練がマンネリ化する中、相次ぐランサムウェア被害に強い懸念を抱いていた。



施策

個別・ランダム配信が可能なプランを導入し、月1回、テンプレートを活用した訓練を実施。クリックさせない行動を身につける教育に注力した。



成果

初回開封・クリック率から、1年後には4分の1以下に改善。実際に届いた不審メールに対する報告文化が作られた。

事例 2 IT・社員300名



課題

リモートや出張先でのPC利用が多く、端末ごとの認証情報漏えいリスクや、セキュリティ意識の属人化が課題となっていた。



施策

まず一斉配信でセキュリティレベルのベースラインを測定後、部署別の継続訓練を開始。



成果

例えば経理部では請求書を装った詐欺メールを開封しやすいなど、部署ごとの弱点が可視化され、結果として組織全体のレベルを平準化できた。

運用担当者の不安を解消するQ&A

Q 全社員に一斉送信すると、業務が混乱したり、すぐに話題になって訓練が形骸化しませんか？

A 事前に詳細を伝えずとも「セキュリティ訓練」と告知しておけば混乱は起きにくく、さらにアクモスサービスの場合、ランダム配信プランを活用すれば、業務への影響を抑えながら情報共有による形骸化を防ぎ、より実践的な訓練が実施できます。

Q 効果的な訓練メールの文面を考えるのが難しそうで、準備に時間がかかりそうです。

A 一から文面を考える必要はありません。例えば「業務連絡（添付あり）」のような、実際の攻撃でよく使われる手口を模したテンプレートやAI生成機能を活用できます。自社の状況に合わせて少し修正するだけで、リアルな訓練メールを簡単に作成可能です。

Q 間違って開封してしまった社員がショックを受けたり、過度に萎縮してしまわないか心配です。

A 訓練の目的は叱責ではなく教育です。リンクをクリックしてしまった社員には、その場で「これは訓練メールです」と大きく明示し、まずは安心させます。その上で、なぜ見抜けなかったのかのポイントを解説する教育コンテンツを表示し、前向きな学習の機会とします。

Q 訓練をやっても、具体的な行動改善につながるのでしょうか？単なる周知で終わらないか不安です。

A 訓練では「不審なメールを開封しない・添付ファイルを開かない」といった具体的なアクションがとれたかどうかを測定します。その結果に基づき、できていなかった社員に対して具体的な指導を行うことで、精神論ではない実践的な対応力を養うことができます。

訓練を成功させる運用の極意とは

人の脆弱性を克服するために、科学的なアプローチで「最強の訓練」へ進化。

従来の訓練（精神論寄り）



問題の捉え方：不注意・意識の低さ



対策：ルール、罰則、年次研修



ゴール：クリック率や添付ファイル実行率の低下



結果：形骸化、訓練対象者の疲弊



これからの訓練（行動科学を重視）



脳の仕組みの「速い思考」で処理させず、「遅い思考」を起動させ不審メールを暴かせる



適切なステップで実施することで、セキュリティ行動を定着させる



文化の醸成、トラブルに強い組織づくり



自律的な検知・報告

アクモスの会社概要



私たちは輝くICTサービスで
社会の向上に貢献します

確かな開発基盤・技術力

企業の業務システム、自治体のITソリューション、宇宙関連システムなど、重要な社会・情報インフラを支えるシステムを手掛けています。

安心できる開発・サービス提供環境

情報セキュリティマネジメントの国際規格「JISQ27001:2014」やプライバシーマークなど取得済みです。

信頼性と透明性が高い企業運営

東証スタンダード市場に上場。IR情報の公開やコーポレートガバナンスの整備により、信頼性抜群の企業運営に努めています。

商号	アクモス株式会社 東証スタンダード市場（証券コード：6888）
設立	1991年8月23日
資本金	6億9,325万円
代表	代表取締役社長 兼 COO 清川 明宏
社員数	308名(単体) / 490名(連結) 2025年6月現在
事業内容	ITソリューションサービス（IT基盤・構築・SI・運用・保守） グループ事業マネジメント
本社(本店) 所在地	東京都港区虎ノ門1-21-19 東急虎ノ門ビル8F
その他事業所	茨城本部・茨城開発センター・つくばオフィス
取得認証	QMS（JIS Q9001:2015） プライバシーマーク（JIS Q15001:2023） ISMS（JIS Q27001:2023）
加盟団体	サイバーセキュリティ協議会 / 一般社団法人 高度ITアーキテクト育成協議会 一般社団法人 日本情報システム・ユーザー協会 一般社団法人 茨城県情報サービス産業協会 / 茨城県高度情報化推進協議会 茨城県情報通信ネットワークセキュリティ協議会
ホームページ	https://www.acmos.co.jp

詳細はお気軽にお問い合わせください。
無料体験プランもお申し込み受付中です！

お問い合わせ先

アクモス株式会社 営業本部 首都圏営業部

東京都港区虎ノ門1-21-19 東急虎ノ門ビル8F

TEL : 03-5539-6480

E-Mail : acmos-sales-support@acmos.jp

<https://cloud-srv.acmos.co.jp/>



サービスサイトはこちら