KnowBe4
Human error. Conquered.

# セキュリティ意識向上トレーニング／フィッシングシミュレーション・分析プラットフォーム

継続的に脅威となる**ソーシャルエンジニアリング**への対策を実現可能にするベストプラクティス

## KnowBe4 のセキュリティ意識向上トレーニングとは？

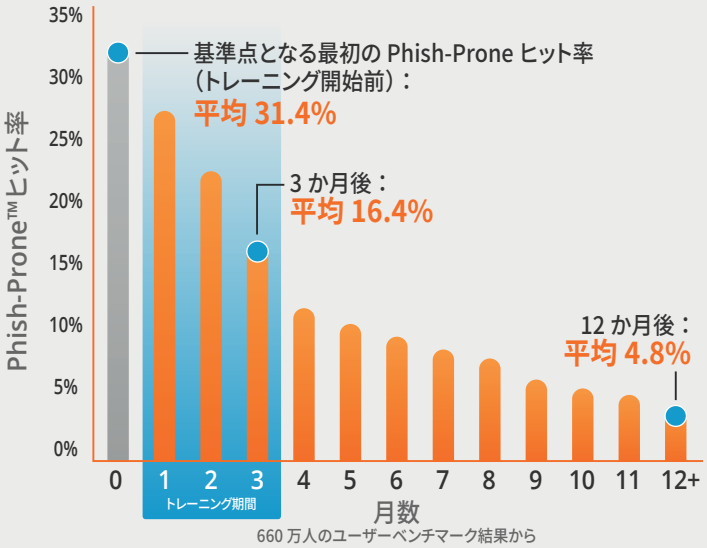
これまでの古いスタイルのセキュリティ教育（KnowBe4 では“Old School”と呼んでいます）ではもはや限界がきています。今、あらゆる従業員は、日々進化するフィッシング攻撃やランサムウェア攻撃に頻繁にさらされているのです。

**ベースラインテスティング**
無償の模擬フィッシング攻撃を通して社員一人ひとりがどれくらい攻撃被害を受けやすいかを PPP (Phish-Prone ™ Percentage: フィッシング詐偽ヒット率 ) としてアセスメントし、トレーニング前の現状を把握。

**ユーザーのトレーニング**
インタラクティブな教材モジュール、ビデオ、ゲーム、ポスター、ニュースレターなどを含む世界最大のセキュリティ意識向上トレーニングコンテンツライブラリー。スケジュールされたリマインダーメールの送信。自動化されたトレーニングキャンペーンの実施。

**ユーザーへのフィッシング**
完全に自動化されたクラス最高の模擬フィッシング攻撃、無制限に利用できる数千ものテンプレート、各種のコミュニティフィッシングテンプレート。

**結果を見る**
エンタープライズクラスの最強のレポーティング。トレーニング状況とフィッシングテスト結果をともに表示する統計とグラフ分析。セキュリティ管理者に最適。同時に、ROI も可視化。


## 驚きの効果を実証

KnowBe4 の膨大なユーザーデータベースを使って、12 ヶ月間以上にわたり 660 万人のトレーニング受講者を対象に分析を行いました。2021 年度の調査結果によると、警鐘を鳴らすレベルが続いています。全業種でのトレーニング開始前の PPP ( フィッシング詐偽ヒット率 ) は 2020 年と比べて若干低下しましたが、未だに 31.4%というリスクの高さが結果として報告されています。

このデータによると、“New School” ( セキュリティ意識向上トレーニングと疑似フィッシング訓練の組み合わせ ) を導入後 90 日で、31.4% から 16.4%へほぼ半減しました。さらに、1 年後の結果では、これらのベストプラクティスに従うことで、平均で 4.8%へ大幅に削減することが可能です。

自社の PPP を他社と比較してください。サブスクリプション契約には、**業界ベンチマーキング機能**が含まれています。

出典：2021 年の KnowBe4 業界別フィッシングベンチマーキングレポート
*注：フィッシング詐欺ヒット率の初期値は、評価対象の全ユーザーに基づいて算出されています。これらのユーザーは、評価前に KnowBe4 コンソールを使ったトレーニングをいっさい受けていません。その後の各期間の数値は、全ユーザーのうち KnowBe4 コンソールを使ったトレーニングを受けたユーザーのフィッシング詐欺ヒット率を反映しています。*

# KnowBe4 のセキュリティ意識向上トレーニングが いかに**効果的**かを確認してください

KnowBe4 はセキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。防御の最終ラインとして「人」による防御壁を構築している多くのお客様の一人としてご協力ください。

## KnowBe4 のセキュリティ意識向上トレーニングにはどんな機能が含まれるか？

**無制限の利用**
サブスクリプションレベルに基づいて 1,000 項目を超えるコンテンツライブラリーへのアクセスを許可する 3 つのトレーニングアクセスレベルを提供。柔軟なライセンシングによって、すべてのフィッシング機能への無制限のアクセスが可能になります。さらに、KnowBe4 では新機能を定期的に追加しています。

**インターネットを通しての学習意欲を高めるインタラクティブなトレーニング**
インタラクティブなトレーニングは、全く新しい学習体験を提供し、学習する喜びと意欲を向上させます。トレーニング全体のユーザーインターフェイスには、お好きな言語を自由に選択いただけます。これによって、没入感の高いトレーニング体験を生み出すことができます。

**自社ロゴ使用可能コンテンツ**
このセルフサービス機能により、対象の KnowBe4 トレーニングモジュールの最初と最後にカスタマイズコンテンツを追加できます。お客様にお届けしたいメッセージに合わせて、自社ロゴやカスタムグラフィックス、コーポレートカラーなど企業ブランドを構築する要素を追加できます。

**各自コンテンツのアップロード**
KnowBe4 セキュリティ意識向上トレーニングプラットフォーム上に自社独自の教育プログラムや他社の教育プログラムを追加したいというニーズはございませんか？このような場合、KnowBe4 の堅固な LMS ( 学習管理システム：Learning Management System) を使用すると、独自の SCORM 準拠の教育コンテンツや動画コンテンツをアップロードして、すべての KnowBe4 ModStore トレーニングコンテンツとともに一箇所で管理することが可能です。しかも、追加料金は一切かかりません。

**アセスメント**
従業員各自がどれほどのセキュリティ知識を持っているか、またセキュリティカルチャーをどれだけ理解しているかを評価し、ベースラインセキュリティの評価指標の確立に役立てます。スキルをベースにしたアセスメントとセキュリティカルチャー調査を使って、時間の経過とともに変わる従業員のセキュリティ知識とセキュリティを意識した文化に対する感情を測定・監視します。

**独自のフィッシングテンプレートとランディングページ**
KnowBe4 が用意した数千もの使い勝手のよい既存テンプレートに加えて、受講者独自の情報をベースにフィッシング攻撃シナリオをカスタマイズして、本番さながらの偽装添付ファイルを作成して、自社独自の標的型スピアフィッシングキャンペーンを展開できます。それぞれのフィッシングメールテンプレートには、それぞれのカスタムランディングページを設定させることができ、インシデント発生時点の教育を可能にします。

**Phish Alert ボタン**
KnowBe4 では、アドイン機能として Phish Alert ボタンを用意しています。このボタンによって、不審メールを安全に分析のためにセキュリティ担当者へ転送できます。Phish Alert ボタンによって報告後は、受信ボックスから疑わしいメールを削除して今後の脅威の拡散を防止できます。すべてが、Phish Alert ボタンをワンクリックするだけで完了します。

**ソーシャルエンジニアリングインディケーター**
特許取得済みのテクノロジーによって、それぞれの模擬フィッシングメール体験を「セキュリティ教育のプラットフォーム」に変えます。模擬演習メール内で見逃した点については、暗黙のうちにレッドフラグが評価指標として立てられ、個人のスコアとして数値化されます。

**AI を活用した模擬フィッシングとセキュリティ教育を推奨**
各受講者に現在の知識レベルに合わせたよりパーソナルな体験を提供するのに、AI は絶大な威力を発揮します。AI を活用した模擬フィッシングによって、各受講者のセキュリティ教育とフィッシング履歴に応じて、最適な模擬フィッシングテンプレートを自動的に選択します。AI を活用した教育を推奨することで、KnowBe4 ModStore は組織全体の PPP ( フィッシング詐偽ヒット率 ) に合わせた教育コンテンツを作成します。

**ユーザー管理**
KnowBe4 の Active Directory インテグレーションによって、容易に受講者データをアップロードすることが可能になり、手動による変更管理を不要とし、大幅な時間短縮を実現します。さらに、Smart Group ( スマートグループ ) 機能を活用して、自社のフィッシングキャンペーン、学習課題、各受講者の振る舞いや受講者属性に基づいた是正学習などを自動化することが可能になります。

**アドバンスドレポーティング機能**
60 種を超えるビルトインレポートが提供されており、全体を俯瞰する包括的なビューに加えて、時系列に主要なトレーニング評価指標を追跡する詳細レポーティングをサポートしています。各種のレポーティング API を通して、各自の KnowBe4 コンソールからデータを抽出できます。

**Virtual Risk Officer ™（VRO）**
革新的な Virtual Risk Officer（VRO）機能は、機械学習を通して受講者毎、部署毎、企業レベル毎のセキュリティリスクを予測･特定します。この継続的な学習モデルによって、自社のセキュリティ意識向上プログラムにおいてデータドリブンな意志決定を下すことが可能になります。

**PhishER ™**
受講者によって報告される大量の不審メールを管理するためのオプショナルなアドオン PhishER です。PhishER を実装することで、メール脅威を迅速に特定して、対応することが可能になります。PhishER は、KnowBe4 の教育プログラムと組み合わせることで、危険なフィッシング攻撃メールを、実際に発生しているフィッシング脅威に即時に対応するメール演習へ置き換えます。

**情報漏えいの 88%は、「人」を標的とした攻撃よって引き起こされていることをご存じですか？**
無償のフィッシングテストを試してみてください。自社の従業員がフィッシングに対してどれだけ脆弱であるかをご確認ください。
www.KnowBe4.com/PST

KnowBe4 Japan 合同会社 | 〒 100-0004 東京都千代田区大手町 1-9-2 大手町フィナンシャルシティグランキューブ 3 階 Global Business Hub Tokyo | 01DSSB35R01
電話：03-4588-6733 | www.KnowBe4.jp | Email:Info@knowbe4.jp