knowbe4

リアルタイムコーチング

「セキュリティ意識」を「安全な行動」へとつなげる

ユーザーを狙ったソーシャルエンジニアリング攻撃は、技術的なセキュリティがどんなに強固であってもその防御策を簡単にすり抜けるため、最も多く発生する脅威の一つとなっています。Verizonの2026年度データ漏洩/侵害調査報告書（DBIR）によると、データ漏洩の62%は人的要因によるものであり、AIを活用したフィッシング、ビッシング、ディープフェイクの登場により、これらの攻撃を見抜くことはますます困難になっています。

トレーニングを実施することには一定の効果はありますが、学んだ内容が定着しなければすぐに忘れられてしまいます。ユーザーの間違った行動がアラートとして検知された時点では、適切な対処のタイミングとしては遅すぎます。よって、SOCチームは繰り返し発生する同じような検知の精査に時間を取られることになるでしょう。

リアルタイムコーチングは、その問題を解消するためのソリューションです。リスクのある行動が生じたその瞬間を学びの機会に変え、ユーザーが最も必要とするタイミングでコーチングを実施。これにより、安全な行動の定着を促すと同時に、SOCチームのアラート対応の負担を大幅に削減します。

リアルタイムコーチングとは？

リアルタイムコーチングは、KnowBe4が提供する「AIネイティブのセキュリティ意識向上トレーニング（SAT）」の中核機能であり、ユーザーが学んだ知識を定着させ、組織全体における行動変容を大規模に推進することを目的として設計されています。従業員が怪しいリンクをクリックした場合や、ブロックされたサイトへのアクセスを試みた場合、あるいはフィッシングテスト実施時にレッドフラッグを見落とした場合、リアルタイムコーチングがその状況に応じたSecurityTipをメールや各種コミュニケーションツールへ直接送信します。そして何が発生したのか、なぜそれが重要なのかを分かりやすく解説します。これにより、知識の定着率が向上し、同様のリスクの再発を防止できるほか、ユーザーは自分の行動がもたらす影響を理解することができるようになります。

リアルタイムコーチングは、トレーニング、模擬フィッシング、そして実際に改善を目指す従業員の行動を相互に連携し、単発のトレーニングで終わらせるのではなく、一つひとつの状況を継続的なフィードバックループへと変えていきます。

主なメリット

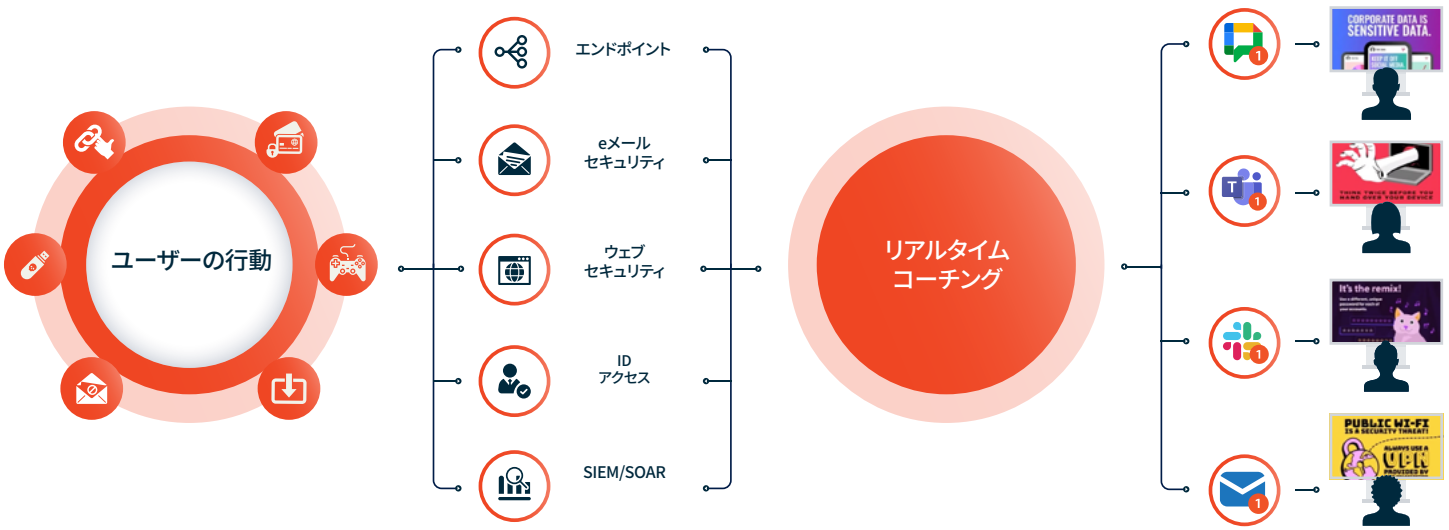
- トレーニングを行動につなげる：
  4人中およそ3人のユーザーが、リアルタイムのコーチングメッセージを1度受け取るだけで、リスクのある行動を繰り返しません。
- ユーザーが普段使うツールでアプローチ：
  メールではなく、Slack、Microsoft Teams、Google Chatといった使い慣れたツールを通じてその場ですぐにSecurityTipsを届けることで、より高いレスポンスを得られます。
- 継続的な学習サイクルを構築：
  トレーニング、模擬フィッシング、コーチングを組み合わせ、リスクを継続的に減らしていくための戦略を確立します。
- SOCの負担を軽減：
  インシデントの再発とアラートを減らし、アナリストにかかる大きな負担を解消。SOCが優先度の高い脅威に集中的に対処できるようにします。
- 導入しているセキュリティツールを有効活用：
  使用しているツールからのアラートをコーチングの機会へと変換します。
- 効果を実証：
  リアルタイムコーチングはリスクスコアに直接反映されるため、行動の具体的な変化やリスク低減の効果を数値として明確に示すことができます。

リアルタイムコーチングの仕組み

リアルタイムコーチングは、セキュリティ意識向上トレーニング（SAT）プログラムや模擬フィッシングに加え、Microsoft、CrowdStrike、Ciscoといったベンダーの連携サードパーティ製セキュリティ製品からの警告を活用します。これにより、リスクの全体像をより詳細かつ正確に把握することが可能となります。

また、一連の行動を常に把握して必要なその瞬間に的確なフィードバックを提供することで、これまで実施されたトレーニングの成果をより一層確実なものにします。これにより、SOCチームに新たな業務負担をかけることなく、よりスマートなセキュリティ判断、類似インシデントの再発防止、リスクの低減、そしてセキュリティカルチャーの醸成を実現します。

リアルタイムコーチングのワークフロー



1 検知

セキュリティ意識向上トレーニングやフィッシングシミュレーション、連携されたサードパーティ製セキュリティツールから警告を読み取ります。

2 分析

警告データを分析し、ユーザーへの指導やトレーニングの定着に最適な機会を判断します。

3 指導

Google Chat、Microsoft Teams、Slack、またはメールを通じて警告の内容に合ったSecurityTipを配信します。

4 改善

適切な行動が定着することでリスクスコアが更新され、同様のインシデントの再発やSOCが対応するアラート件数の削減につながります。

リアルタイムコーチングの機能

その場でのリアルタイムコーチングとSecurityTips

リスクのある行動が検知されたその瞬間にリアルタイムでコーチングを行い、Microsoft Teams、Slack、Google Chat、またはメールを通じて、状況に応じたSecurityTipsやアドバイスを送信します。これにより、行われた操作の詳細と、今後はどのように回避すべきかを分かりやすく伝えます。従業員が危険な行動を起こしたその瞬間にセキュリティ意識を高めることは、組織のセキュリティカルチャーを強化する上で非常に効果的です。

リアルタイムでのメッセージ送信

トレーニング通知、個別のアドバイス、さらに「セキュリティの実践ヒント」や「今週の詐欺」といったユーザー向けメッセージが、Slack、Microsoft Teams、またはGoogle Chatを通じて送信されます。リアルタイムで情報を送信することで、ユーザーを飽きさせることなく、安全な行動習慣を定着させ、学習を日常業務の一部にすることができます。

リスクスコアとリスクの可視性

リアルタイムコーチングはリスクスコアの算出に反映されるため、社内環境で実際に起きている事象に基づいて、ユーザーに起因するリスクを定量化するのに役立ちます。これにより、リスクの全体像が明確になり、それを軽減するための道筋が見えてきます。

規定のコーチングカテゴリー

KnowBe4には、フィッシング、データ漏洩、リスクの高いオンライン行動など、20種類以上のコーチングカテゴリーがあらかじめ用意されています。手動でルールを記述したり検知ロジックを設定したりする必要はありません。起動するだけで、すぐにコーチングをスタートすることができます。

サードパーティ製品の警告を活用したコーチング

リアルタイムコーチングは、CrowdStrike、Microsoft、Ciscoなど、セキュリティスタック内にある既存のメール、ID、ウェブサイト、エンドポイントのベンダー製品と連携。お客様の環境で発生した実際のアラートを活用して、適切な指導を行います。これにより、組織全体で何が起きているのかをより網羅的に把握できるようになります。

ソーシャル エンジニアリングの兆候

模擬フィッシングトレーニング中に見落とされた具体的なソーシャルエンジニアリングの兆候やレッドフラッグについて、従業員が普段使っているツール上で即座にフィードバックを提供します。

AIDAオーケストレーションによるリアルタイムコーチング対応

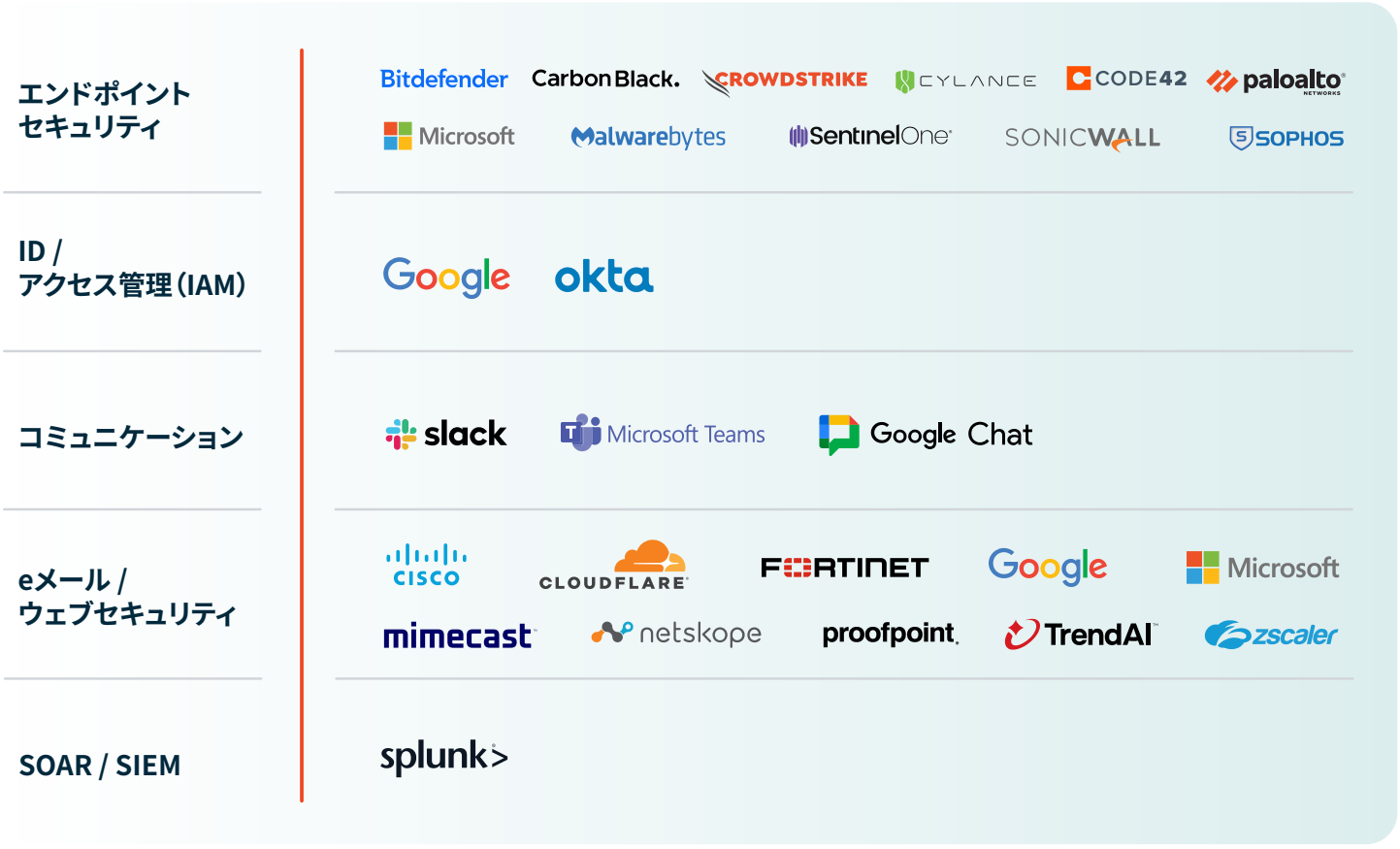
ユーザーが模擬フィッシングで不合格となった場合、そのリスクの程度に応じて、AIDA（AI Defense Agents）オーケストレーションが簡単なSecurityTipを送るか、またはトレーニング課題を課すかを自動で判断します。これにより管理者の手間が省けるだけでなく、AIDAオーケストレーションが状況に応じた適切な対応を即座に提供することで、より効果的な行動変容を促します。

ダッシュボードとレポート

あらかじめ設定されているダッシュボードで、コーチングの内容や検知されたセキュリティイベントの全体的な概要を確認できます。詳細レポートは、組織のセキュリティリスクに対する考察を提供し、ユーザーの危険な行動の傾向を時系列で追跡するのに役立ちます。

強力なセキュリティインテグレーション

リアルタイムコーチングは標準APIを介して、CrowdStrike、Microsoft、Cisco、Netskope、Zscalerなどのベンダーによる既存のセキュリティ製品と迅速かつ容易に統合することができます。当社の技術パートナーシップのエコシステムは、お客様をサポートし、お客様のセキュリティカルチャーを強化するために、急速に拡大しています。



トレーニングを行動の変容につなげましょう。

さらに詳しく →

knowbe4

KnowBe4 Japan合同会社 | 〒107-0052 東京都港区赤坂 9−7−1 ミッドタウン・タワー 18F | 03-4586-4540
www.knowbe4.com/ja | info@KnowBe4.jp

本書に記載されている他社の製品および会社名は、各社の商標または登録商標です。

Copyright © 2026 KnowBe4 All Rights Reserved.