# ヒューマンリスク管理

## パーソナルかつ適切な、適応性の高いソリューション

HRM+プラットフォームは、ヒューマンリスク管理に対するKnowBe4の革新的なアプローチです。AIを搭載した包括的なオールインワン型プラットフォームであり、最新のサイバーセキュリティ脅威に対するユーザーの行動を強化します。

HRM+はこの分野における唯一のグローバルセキュリティプラットフォームです。最大の攻撃領域である従業員を最大の資産へと変え、サイバーセキュリティの脅威から組織を積極的に守ります。

### HRM+プラットフォームに含まれる製品：

- **セキュリティ意識向上トレーニング**
  AIを活用したセキュリティ意識向上トレーニングと模擬フィッシングが、企業の意識を高め、ユーザーの行動に変化をもたらします。
- **クラウド電子メールセキュリティ**
  ヒューマンリスクを継続的に評価し、セキュリティ対策を動的に適合させる、唯一のメールセキュリティ基盤です。
- **フィッシング対策**
  セキュリティオーケストレーションとプロアクティブなフィッシング対策により、インシデント対応チームやセキュリティオーケストレーションチームは、ユーザーがメールを受信する前にフィッシングの脅威を特定し、阻止することができます。
- **リアルタイム コーチング**
  エンドユーザーの危険な行動を検知・対応し、即座にフィードバックを提供するリアルタイムセキュリティコーチング製品です。
- **コンプライアンス トレーニング**
  継続的に更新されるコンテンツを提供し、組織が包括的なアプローチでセキュリティ意識向上/コンプライアンストレーニングを実施できるようにする、コンプライアンストレーニングです。
- **AI Defense Agents**
  AIDAは、AIを活用した先進的なスイートであり、高度なヒューマンリスク管理戦略を提供します。

## 主なメリット

HRM+は、組織が以下のようなサイバーセキュリティにおける重要な課題を克服できるようサポートします。

ソーシャルエンジニアリングとフィッシング攻撃は、組織にとって最大のサイバーリスクであり、データ侵害やランサムウェアの主要な攻撃ベクトルである。

攻撃者はAIを利用して、フィッシングやソーシャルエンジニアリング攻撃を飛躍的に効果的かつ大規模に実行できるようにしている。

サイバーセキュリティへの取り組みの開示と報告に関する規制の強化が高まっている。

経営幹部は、セキュリティカルチャーの構築が最優先課題であることに同意しながらも、何を成功と定義するか、人的リスクをどのように測定し理解するかについて明確ではない。

ITチーム、情報セキュリティチームの人員不足やリソース不足、時代遅れのフィッシングメールの分析や対策のおかげで、フィッシングが組織にもたらすリスクは劇的に増大している。

年に一度のセキュリティ意識トレーニングではユーザーの関心を引くことができない。また、頻繁なフィッシングシミュレーションテストやリアルタイムのセキュリティ指導がなければ、ユーザーの行動を効果的に変えることはできない。

「サイバーセキュリティ分野でAIに関して最も懸念しているのは、エンドユーザーがフィッシング攻撃を識別するために役立つ多くの『ヒント』を削除することによって、サイバー犯罪者がより信憑性の高いフィッシング攻撃を作成できるという点です。」

– 情報セキュリティ責任者

## 製品の機能

### セキュリティ意識向上トレーニング

KnowBe4は、セキュリティ意識向上トレーニング、コンプライアンストレーニング、ソーシャルエンジニアリングシミュレーションにおいて、世界最大規模となる製品を提供しています。35以上の言語にローカライズされた魅力的なコンテンツ、AIを活用したユーザーに最適なフィッシングシミュレーションやトレーニング、エンタープライズグレードのレポート、堅牢なユーザーテストとアセスメントなど、業界で最も包括的なライブラリを組み合わせることで、意識向上と行動変容を促します。KnowBe4のセキュリティ意識向上トレーニング製品を利用することにより、平均12か月で組織のPPP（フィッシング詐欺ヒット率）は30%以上から5%未満にまで下がります。

さらに詳しく

### Compliance Plus

Compliance Plusは、700以上のモジュールで構成される包括的コンプライアンス研修ライブラリです。グローバルで継続的に更新されるほか、魅力的かつ的確で、無駄を削ぎ落とした教育を提供します。コンテンツはカスタマイズが可能なため、従業員の所属組織の規定に適切に準拠できるように学べる仕組みです。

Compliance PlusとKnowbe4のKSATトレーニングを確実に統合させることで、組織はセキュリティとコンプライアンスの両方のトレーニングに包括的なアプローチを取ることができます。罰金を命じられるリスク、風評被害リスク、顧客離れのリスクをはじめとしたコンプライアンス違反リスクの低減に寄与します。

さらに詳しく

### SecurityCoach

SecurityCoachは、ITチームやセキュリティオペレーションチームが、組織内で最大の攻撃対象である「従業員」を保護するために作られた初のリアルタイムセキュリティコーチング製品です。SecurityCoachは、ユーザーの危険なセキュリティ行動に対し、リアルタイムなコーチングを行うことでセキュリティカルチャーの強化をサポートします。

リスクのあるユーザーの振る舞いが検出されると、SecurityCoachはMicrosoft Teams、Slack、Google Chatまたはメールを通じてリアルタイムでそのユーザーにSecurityTipを直接送信します。すぐに通知が届くため、セキュリティ意識向上プログラムの内容をさらに習慣づけるという意味でも効果的です。

さらに詳しく

### PhishER

PhishERは、報告されたメールメッセージを自動的に分析し、優先順位をつけて、組織全体の悪意のあるメールを特定し隔離するフィッシング対策製品です。さらに、実際のフィッシングメールをトレーニングの機会に変換し、それらを模擬フィッシング訓練として活用できるようにします。

PhishER Plusは、AIによって検証されたクラウドソーシングのブロックリストとPhishRIP機能を搭載。ユーザーがフィッシング攻撃にさらされる前に、メールフィルターを回避した活発なフィッシング攻撃を積極的にブロック・削除します。SOCチームの処理数を削減し、予算と情報セキュリティにかかる時間を大幅に減らします。

機械学習とAIがメールの分析と優先順位付けを行い、報告された全メールの中から高リスクのフィッシング脅威の特定する際の憶測を排除。ユーザー報告メールの「残り90%」のセキュリティ確認を自動化します。これにより完全に統制された効率性の高いIRチームやSOCチームを社内に組織し、ソーシャルエンジニアリングの脅威をほぼリアルタイムで特定・軽減することが可能になります。

さらに詳しく

「ソーシャルエンジニアリングとフィッシング攻撃は、サイバーセキュリティの先陣を切る手口です。これらの脅威は、組織にとって最大のサイバーリスクであり、データ漏洩、ランサムウェア、マルウェアの主要な入り口となっています。」

– CISO

## 製品の機能（続き）

### Artificial Intelligence Defense Agents (AIDA)

AIDAは、ヒューマンリスク管理を自動化し、強化するために設計されたKnowBe4の革新的なAIネイティブのセキュリティエージェントです。脅威の状況に合わせて進化し、包括的で適応力のあるエクスペリエンスを提供します。複数のAI技術を活用することで、AIDAは人間と人工知能を融合させ、ヒューマンリスクを減らします。またAIDAには、役割別の高度なレポートやエグゼクティブレポートなどが含まれます。

さらに詳しく

### クラウド電子メールセキュリティ

KnowBe4クラウド電子メールセキュリティは、ヒューマンリスクを継続的に評価し、高度なフィッシング攻撃や外部へのデータ漏洩から防御するため、ポリシー制御を動的に適応させる、AI搭載型製品群です。文脈に即した機械学習とニューラルネットワークを活用し、クラウドネイティブなAPIアーキテクチャによるシームレスな統合を実現することで、電子メール保護の強化、ヒューマンリスクの詳細な可視化、そして価値実現までの時間の短縮を実現します。

さらに詳しく

「市場を評価するときは慎重に。多くのSATは、従業員の行動を変えるために必要な多様性、使いやすさ、幅広いコンテンツを提供できていません」

– IT 管理者

詳しくは以下をご覧ください：

KnowBe4.com/ja

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