2025年日本のヒューマンリスクの現状

AI時代における「人」を守る新しいパラダイム

進化するワークフォースには、進化するセキュリティが必要

ワークフォースは、前例のないスピードと規模で進化しています。近い将来、それは人とAIエージェントが協調して働き、その両方の行動リスクをプロアクティブに管理するセキュリティプログラムが支えることになるでしょう。

今日の現実として、サイバーセキュリティリーダーは複数の戦線でセキュリティ課題と戦っています。人は、今も、サイバー犯罪者の標的となり、ミスを犯し、意図的にデータを持ち出しています。そこに加えて、AIが、さらなるリスクを生じさせつつあります。

本レポートは、日本のサイバーセキュリティリーダーが人とAIのリスクをどのようにマネージしているか、そして従業員が自組織のセキュリティプログラムについて実際にどのように考えているかを調査したものです。

日本の調査結果の主なポイント

- サイバーセキュリティリーダーの96%が、人的セキュリティ強化を困難だと感じています。
- 94%の回答者が、過去12ヶ月間に人が原因であるセキュリティインシデントが増加したと回答しています。
- Eメール関連のインシデントが最も増加しており、72%。
- 次にAIアプリケーション関連が44%。
- ディープフェイクに関連するインシデントは24%増加。
- サイバーセキュリティリーダーの98%が、AIによるサイバーセキュリティリスクに対処するための措置を講じています。
- 従業員のうち、必要なAIツールを直ぐに利用できていると考えているのはわずか15%です。
- ヒューマンリスクマネージメント（HRM）プログラムが確立されている組織はわずか8%であり、ヒューマンリスクを有効に可視化できている組織は29%にすぎません。
- 従業員のうち、自社のサイバーセキュリティプログラムを変更する必要がないと考えているのはわずか6%です。
- サイバーセキュリティリーダーの98%が、人的セキュリティ確保のためにより多くの予算を求めています。

組織は、この「人」とエージェントというパラダイムの変化に、迅速に対応する必要があります。少なくともセキュリティのために、ヒューマンリスクマネジメント（HRM）を導入し、そのマネジメントの考え方を新たな労働力とも言えるAIエージェントにまで拡張することで、それをワークフォーストラストマネジメントまで発展させる必要があります。

ヒューマンリスクの現状

外部攻撃と自身のミス、両方から「人」を守ることは、組織にとって引き続き重大な課題です。実際、人的要素によるリスクは増加しており、サイバーセキュリティリーダーの94%が昨年インシデントが増加したと回答しています。

調査対象となったサイバーセキュリティリーダー全員が、過去12ヶ月間に従業員という人が関わるセキュリティインシデントを経験していました。

主な原因は以下のとおりです。

- 94%がサイバー犯罪者によって従業員が騙されてしまったことが原因であると回答しました。
- 90%が人のミスが原因でインシデントが発生したと回答しました。
- 40%が悪意のある内部関係者によるインシデントがあったと回答しました。

日本の従業員250名を調査したところ、以下の結果が得られました。

- 自社のデータの保護について全従業員がそれぞれが責任を負っていると回答した人は、わずか21%です。
- それ以外はデータの保護は、ITおよびセキュリティチーム（49%）、上級管理職（15%）、または直属の上司（14%）の責任であると考えています。

人々の意思決定行動に影響する当事者意識を含む多様な要因について日本の250名の従業員を対象に調査を実施しました。会社のデータに対する責任について以下のことが明らかになりました。

- 会社がデータに対する責任を負っている。と答えたのは36%
- 責任の所在は不明確、と答えたのは26%
- 残る35%は、会社が持つデータに対する責任はそこで働く全員、またはそれを作成・使用するチームや個人が負っていると回答。

当事者意識は注意と責任感を促す一方で、従業員がデータの使用・保管・共有方法について独自のルールを作り始めた場合、リスクをもたらす可能性もあります。

さらに懸念されるのは、会社が保有するデータの保護は当事者全員が責任を負うべきだと考えている従業員がわずか21%しかいない点です。残りの従業員は、主にIT・セキュリティチーム（49%）、上級管理職（15%）、直属の上司（14%）の責任だと認識しています。

この認識のギャップが組織を危険に晒しています。従業員は日々機密情報を扱っているにもかかわらず、その責任の重大さを十分に自覚していないケースは非常に多く見られます。

最もリスクの高い従業員は誰か?

日本のサイバーセキュリティリーダーの100%が、セキュリティ確保を困難だと感じているグループが組織内に少なくとも1つ以上あると回答しています。

最もセキュリティ確保が困難な従業員グループのトップ3は以下の通り。

- IT部門以外の一般従業員（30%）
- 中間管理職（16%）
- 上級役員およびシニアリーダーシップ（16%）

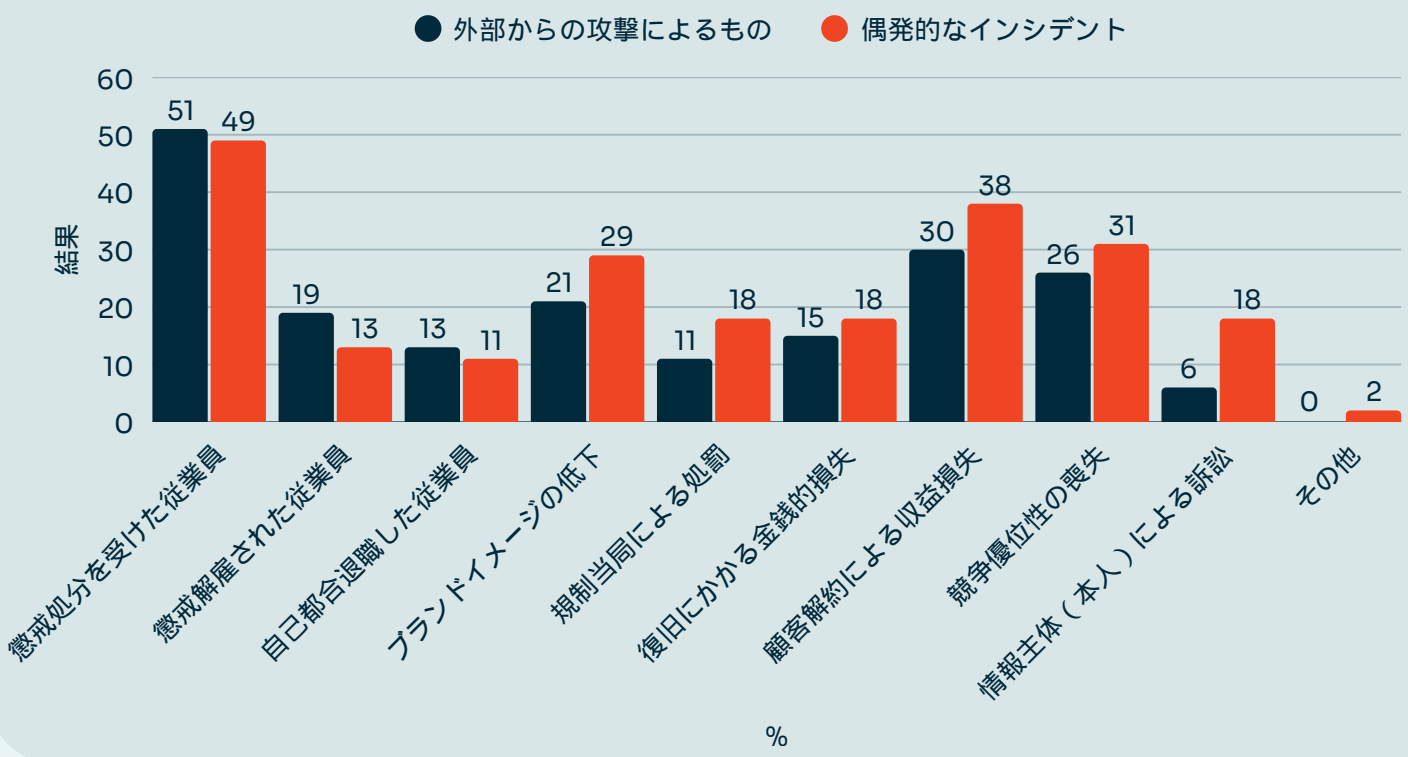
日本で最もセキュリティ対策が難しい部門を尋ねたところ、サイバーセキュリティの責任者は営業・マーケティング部門を挙げました。これらの部門は通常、メールやTeams、Slack、ソーシャルメディアを通じて多様な外部関係者とのやり取りを行うため、フィッシング被害に遭ったり、誤ってデータを漏洩したりするリスクが他の部門と比べて高くなります。

インシデントの代償を払うのは誰か?

サイバー犯罪者に騙されることもミスを犯すことも、どちらも意図しない行動です。しかしどちらの場合も、他のいかなる結果よりも懲戒処分を受ける可能性は高くなっています。

実際、どちらのタイプのインシデントもそれが招く結果は驚くほど類似しており、上位3つの影響は次の通りである：従業員の懲戒処分、企業のブランドイメージの低下、規制当局による処罰。

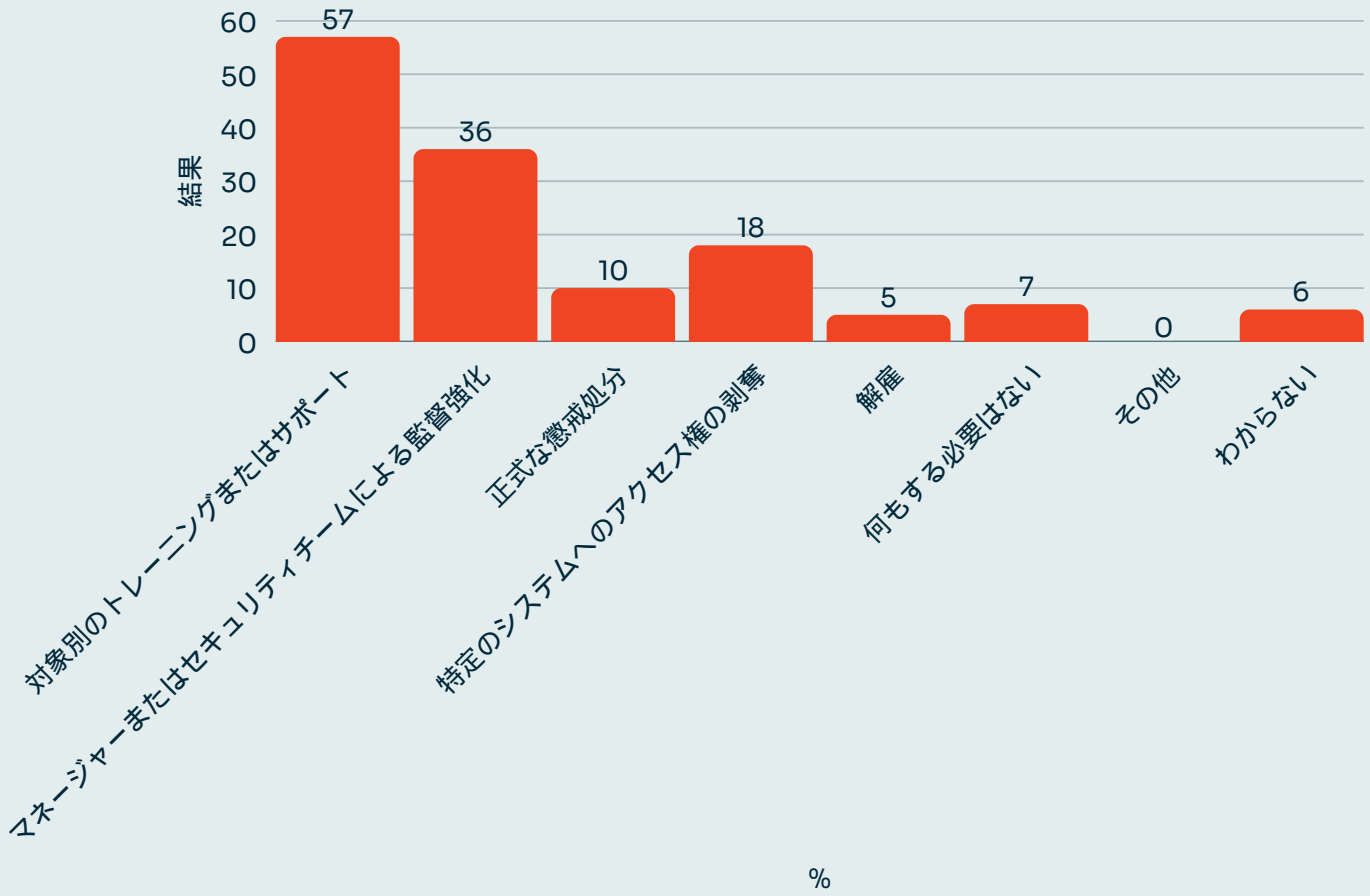
日本のサイバーセキュリティリーダーが外部攻撃と偶発的インシデントの結果を共有



厳罰との認識のズレ：従業員が望むのはより柔軟な対応

このような現実にもかかわらず、日本の従業員は、偶発的にインシデントを引き起こした人々（フィッシングリンクをクリックした場合を含む）に対して、より寛容なアプローチを取っています。正式な懲戒処分を受けるべきだと考えているのはわずか10%に過ぎず、解雇されるべきだと考えているのはわずか5%です。

日本の従業員が偶発的なセキュリティインシデント後に取るべき対応について考えていること



○ィッシング（フィッシング、ヴィッシング等）リスク

サイバー犯罪者が従業員を標的にする手段は数多くあり、サイバーセキュリティのリーダーたちはそれを痛感しています。94%が、過去12か月間に自身の組織が外部攻撃に起因するインシデントに見舞われたと回答しています。

電子メールは最もリスクの高い経路であり、サイバーセキュリティリーダーの 58% がこの方法で発生したインシデントを報告しています。さらに、72% が過去12か月間で（メール経由のインシデントが）増加したと述べています。

それに次いでインシデントの原因として多いのが、社用デバイスを介したソーシャルメディアプラットフォーム上でのメッセージングで 42% です。TeamsやSlackなどのメッセージングアプリケーションも同様のリスクをもたらしており、38% となっています。スミッシング（SMSフィッシング）はそれをわずかに下回る 32% です。

これは、境界のない（ネットワーク境界を超えた）フィッシングへの移行を示唆しています。ネットワーク上の場所を問わず従業員に脅威は到達し、増大しており、ネットワーク境界ベースの防御策は時代遅れになりつつあります。

日本の組織の78%がアカウント乗っ取り攻撃を経験しており、その認証情報は以下の経路で漏洩しています。

- Eメール: 54%
- 脆弱なパスワード: 26%
- メッセージングアプリ (Teams、Slackなど): 36%
- オンラインに流出したパスワード: 20%

攻撃手法の戦略的シフト

電子メールは今後数年間、最もリスクの高いチャネルであり続けると予測しています。しかしながら、マルチチャネル攻撃の台頭と、サイバー犯罪者によるAIツールの悪用が高まる中、組織がこれに対して適切な備えをしなければ、無防備な攻撃対象領域を晒してしまうことになります。

効果的なヒューマンリスクマネジメント（HRM）プログラムは、単に攻撃をブロックするだけでなく、高度な行動科学と脅威インテリジェンスを活用してリスク指標（IoR: Indicators of Risk）を高めることができます。HRMにより警告シグナルを提供し、セキュリティを、先を見越した（プロアクティブな）姿勢へと転換させます。これにより従業員が攻撃者に騙されて操られないように前もって備えることができるようになります。

AI：制御不能な脅威ベクトル

AIはワークフォースを変革（新しい労働力となってきている）しており、急速に重要な脅威ベクトル（脅威の経路）となっています。

自律型AIプラットフォームやAIエージェントの台頭は、サイバー犯罪者がAIエージェントを標的として行う未検知の操作、従業員による機密データの不用意な共有、そしてアプリケーション自体による「ハルシネーション」といった、新たなリスクをもたらします。さらに、サイバー犯罪者も独自のAIツール群を活用し、より巧妙な攻撃を大規模に展開しています。

サイバーセキュリティのリーダーたちが痛感している問題は以下の通りです:

- 44% が、過去12か月間にAIアプリケーションに関連したセキュリティインシデントが増加したと回答しています。これは（増加率において）メールに次いで2番目に大きな増加です。
- 24% が、ディープフェイクに関連するインシデントが増加したと回答しています
- AIを活用した脅威は、行動リスクに対処する上での2番目に大きな課題として位置づけられています。

これは、サイバーセキュリティリーダーの98%がAI関連のサイバーセキュリティの懸念に対処するための対策を講じているにもかかわらず、AIに関わるインシデントが発生していることを示しています。

AIによる脅威の巧妙化は、セキュリティ担当以外の従業員にとっても関心事になっています。91%の従業員が、サイバー犯罪者がディープフェイクを利用して、自社のデータやシステムへアクセスを可能にするように従業員を騙すことについて、懸念していると回答しています。

しかしながら、AIへの従業員のアクセスを維持しつつ、AIを活用した脅威から人々を保護するための対策は、従業員から評価されていないようです。必要な時にAIツールに直ぐにアクセスできる、と回答した従業員はわずか15%に留まりました（これはグローバル平均の26%を下回っています）。一方で、7%は、自分のアクセスを制限するものが何もないことに懸念を示しています。約3分の2（62%）の従業員は、必要な時に必要なAIツールへ直ぐにアクセスできない、または、まったくアクセスできないと回答しています。

「恐怖の文化」はまだ残っているのか

組織の文化はHRMの中核となる要素です。HRMは、一人ひとりのリスクプロフィールを深く理解し、インシデントが起こる前に、適切なタイミングで介入と、きめ細かくパーソナライズされたコーチングを提供することに重点を置いています。そうすることで、従業員は単に企業ポリシーに受け身で従うだけの存在ではなく、組織のセキュリティに主体的に関わる存在になります。

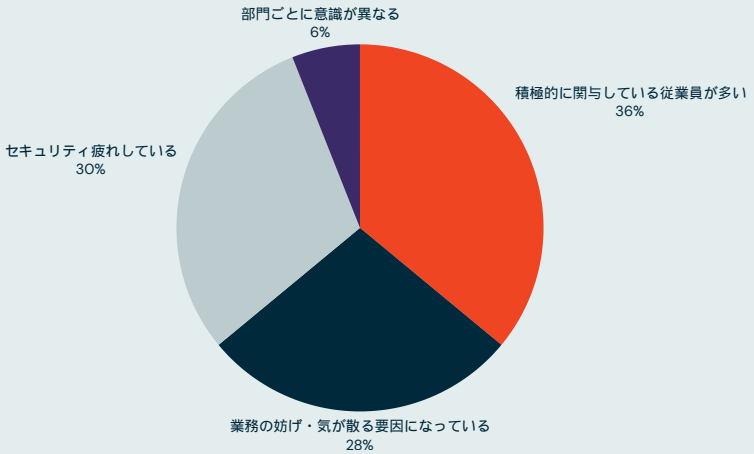
しかし、調査に答えていただいたサイバーセキュリティリーダーのうち、「従業員の大半がセキュリティに積極的に関与している」と見ているのは3分の1（36%）にとどまります。残る64%は、セキュリティによって業務が遅くなったり気が散らされたりしている、セキュリティ疲れの問題を抱えている、部門ごとに関与度がばらついている、と感じています。ここでHRMプラットフォームは、こうした従業員を主体的な参加者へと変えていく「テクノロジーの架け橋」として機能します。

従業員が求めるプロアクティブなセキュリティ

従業員の94%は、自社のサイバーセキュリティプログラムに何らかの変更を加えたいと考えています。上位3つの要望は次のとおりです。

- ミスが起こる前に止めるプロアクティブなセキュリティツール (40%)
- 失敗を責める文化から、ミスから学ぶ文化への転換 (34%)
- 一人ひとりの業務内容と関連性の高いトレーニング (30%)

サイバーセキュリティリーダーが見る、従業員のサイバーセキュリティ意識



これらの結果は、従業員は適切なHRMプログラムを求めていることを示しています。適切なHRMプログラムとは、テクノロジーを使ってリスクが顕在化するポイントで介入し、パーソナライズされたコーチングによって気づきを高め、ミスを正していく取り組みです。

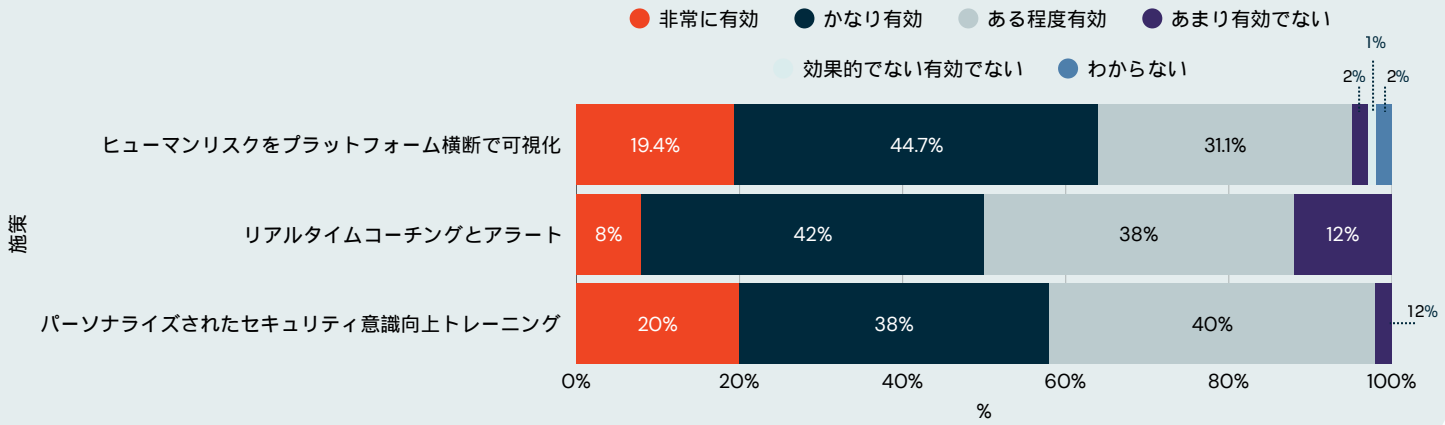
「HRM実行」のギャップを埋める

日本は、アルゼンチンや英国・アイルランドと並んで、HRMの導入率が最も低い地域です。HRMについて「十分に確立されたプログラムがある」と答えたのは8%で、グローバル平均16%の半分にとどまっています。言い換えると92%が遅れを取っている状況ですが、そのうち40%は導入に向けて取り組んでいます。

ただ、「人」に関わるセキュリティインシデントを防ぐうえで、HRMの考え方が有効であるという点については、サイバーセキュリティリーダーの間で共通の認識があります。

- 98%が、プラットフォーム横断的なヒューマンリスクの可視化がHRMを改善すると考えており、そのうち66%は極めて効果的、または非常に効果的だと回答と答えています
- 98%が、パーソナライズされたトレーニングは有効だと認めています
- 88%が、リアルタイムのコーチングも有効だと答えています

サイバーセキュリティリーダーによるHRMの有効性評価



サイバーセキュリティリーダーの96%が、「人」を要因とするインシデントで課題を抱えていると認めています。そのうち3分の1（36%）は、リスクへの対応が主にインシデント発生後になってしまう「事後対応型」のアプローチを問題視しています。

リスクを測定し、インシデントを検知する

HRMの改善にクロスプラットフォームでの可視化が有効だと考えるサイバーセキュリティリーダーは93%にのぼる一方で、実際に「従業員ごとのリスクスコアまで把握できる、非常に高いレベルの可視性がある」と答えたのは5分の1（20%）にすぎません。

残る76%は、自社の中で一人ひとりがどのようにリスクに関与しているのかを把握し、その違いに合わせてアプローチを調整することに苦労しています。内訳は次のとおりです。

- 「可視化はできているが、システム毎に断片的に分かれている」：30%
- 「ある程度可視化はできている」：42%
- 「可視はあまりできていない」：6%

予算をめぐる攻防

従業員リスクを十分に低減するためには、より多くの予算が必要だと答えたサイバーセキュリティリーダーは98%にのぼります。上位3つの要望は次のとおりです。

- リスクの高い行動に対するリアルタイムのアラートとコーチングを行う監視ツール(24%)
- メールセキュリティ (24%)
- AIアプリケーションのセキュリティ強化 (18%)

こうした監視強化への要望は、リスクを顕在化させその時点で介入するHRMの実現に向けて、戦略的な投資が必要だという認識を反映しています。その後の課題は、過去12か月でインシデントを調べ、増加が大きい2つのチャネルをどのように保護するかです。

現在と未来のワークフォースを守るには

ワークフォースを守ることは、ますます難しくなっています。

「人」によるインシデントは増加しており、アタックサーフェス(攻撃対象領域)は広がり続けています。セキュリティチームは、従来からあるシステムの脆弱性を保護するだけでなく、あらゆるコミュニケーションプラットフォームで高まるリスクにも対応しなければなりません。

同時に、AIによってワークフォースの姿も「人だけの組織」から「人とエージェントの組み合わせ」へと急速に変わりつつあります。その結果、AIはリスクの議題において一気に優先度を上げ、インシデントの増加幅という点では、よく知られた脅威ベクトルであるメールに次いで2番目に大きくなっています。

組織は、速やかに進化しなければ、致命的に時代に取り残されてしまうリスクがあります。
この問題を解決するためのパズルには2つのピースがあります。1つ目は、HRMへの移行です。必要なタイミングで、一人ひとりに合わせたセキュリティコントロールとガイダンスを提供し、人に関するリスクを管理することで、従業員を組織のセキュリティを支える主体的な担い手へと変えていきます。

2つ目は、AIエージェントを、実際にワークフォースの一員としてトレーニングしていくことです。

このアプローチを「取るかどうか」ではなく、「いつ取るか」が問われています。早期に取り組む組織は、対応が遅れた組織よりも優位な立場を築くことができるでしょう。

About KnowBe4

KnowBe4 empowers workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk.

KnowBe4 offers a comprehensive AI-driven “best-of-suite” platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats.

The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization’s biggest asset.

For more information, please visit www.KnowBe4.com.

調査方法

KnowBe4はArlington Researchに委託し、サイバーセキュリティの責任を持つグローバルなリーダー700名と、サイバーセキュリティの責任を持たないグローバルな従業員3,500名を対象に調査を実施しました。本レポートで引用しているデータは、日本で勤務するサイバーセキュリティリーダー50名と従業員250名の回答を集計したものです。

KnowBe4, Inc. | Midtown Tower 18F, 9-7-1 Akasaka, Minato-ku, Tokyo, Japan | www.KnowBe4.com | Sales@KnowBe4.com