

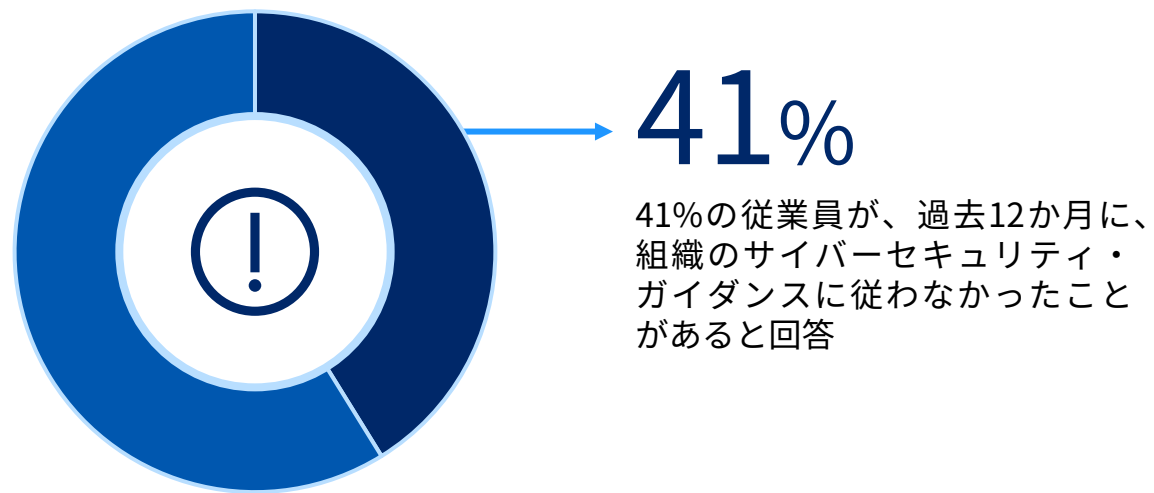


従業員に働きかけ、 セキュアな行動を促す 4つの施策

Christine Lee、Prashast Gupta、Richard Addiscott、
Alex Michaels、Phillip Shattan

はじめに

従業員が誤情報に惑わされたり、リスクの高い行動を取りやすいことは、従来のテクノロジーの脆弱性と同じくらい大きな脅威です。従業員の41%が、過去12か月に、組織のサイバーセキュリティ・ガイダンスに従わなかったことがあると認めています。なかには、機密データを不適切に扱ったり、未承認のアプリケーションを使用したりする例もあります。



インサイトの要点

より高度なアプローチが必要です。サイバーセキュリティ・リーダーは、一律の意識向上研修に頼らず、従業員の心理を理解したうえで、セキュアな働き方を広げていかなければなりません。



- 実際に従業員がどのようなリスク行動をとっているのかを測定し、対策を絞る。従業員の行動をベンチマーキングすることで、リスク行動がフィッシングだけにとどまらないことが分かります。



- さまざまな実際のシナリオを使い、研修を一人ひとりに合わせる。従業員は、研修の量を増やすだけでなく、質も高めることを望んでいます。具体的には、短時間で要点が絞られ、実際のシナリオに沿った内容です。



- 関係部門と連携し、サイバーセキュリティ対策による業務上の負担や障壁を減らす。ガイダンスに違反した従業員のうち、60%近くが「サイバーセキュリティ・リスクより、業務上のニーズを優先した」と答えています。



- 罰則ではなく称賛で、セキュアな行動を後押しする。大半の従業員は、違反の罰則ではなく、望ましい行動への称賛に反応します。



生成AIの登場で、未承認のアプリケーションを使うこと
のリスクは、これまで以上に高まっています。Gartner
のベンチマーキングでは、生成AIを不適切に利用してい
る従業員が、大きな割合に上がることがわかっています。

AIで成果を出すように求められる以上、シャドーAIは今
後さらに増加すると考えられます。実用的な代替手段を
提供せずに生成AIアプリケーションの利用を制限すると、
従業員は個人の生成AIアカウントを業務に利用するよう
になります。

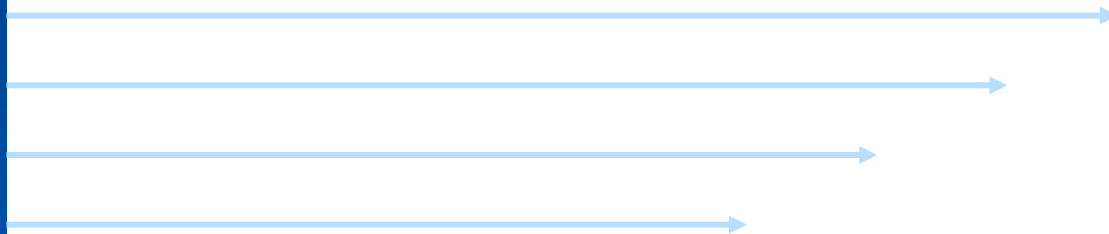


図1：生成AIを不適切に使う従業員

57% の従業員が、業務に個人の生成AIアカウントを使用	
48% の従業員が、生成AIの出力を、正確性を確認せずに使用	
38% の従業員が、コード生成に、一般公開されている生成AIや未承認の生成AIを使用	
37% の従業員が、IT部門やサイバーセキュリティ部門の承認を得ずに、業務用デバイスで生成AIのアプリケーションや機能をダウンロードまたは使用	
33% の従業員が、リスク評価やIT部門・サイバーセキュリティ部門の承認も経ずに、AIを使った独自の自動化の仕組み(例：Agentforce)を構築	

n = 145人 (従業員)
設問：過去12か月の職場での行動を振り返って、一般公開されている生成AIやエージェント型AIのアプリケーション (例：ChatGPT、Quillbot、Perplexity) を、次の各行為についてどのくらいの頻度で使用しましたか。
出典：2025 Gartner Secure Behavior: Employee Perspective Survey

図2：従業員が、よりセキュアに行動する動機になると答えたこと

サイバーセキュリティ・チームが主体的に連携し、摩擦を減らし、ユーザー体験を改善するとともに、業務フローに合わせて統制を最適化してくれる

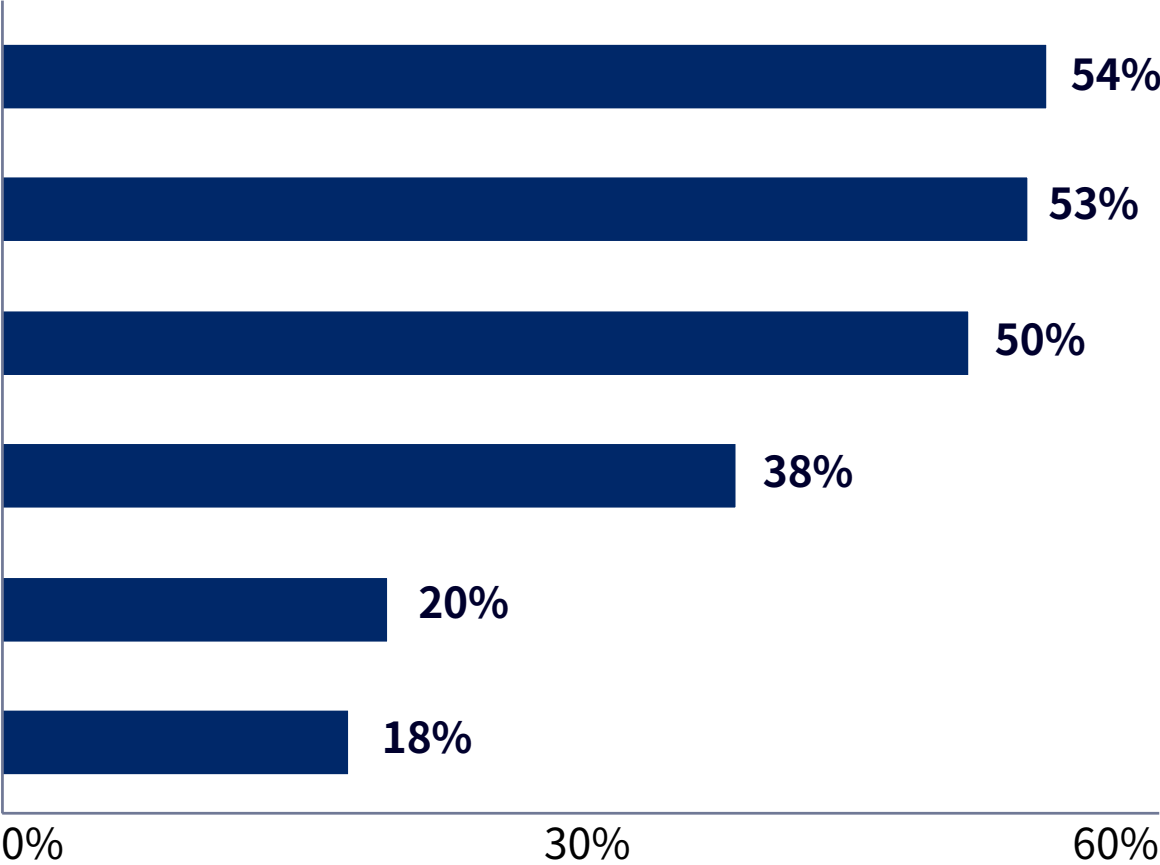
研修の改善 (個人に合わせた内容、ゲーミフィケーション、短時間化)

称賛 (全社集会での紹介、ささやかな賞品やギフトカードなど)

具体的な報酬 (ボーナスの支給、年次の人事評価への実質的な反映など)

重い罰則 (解雇、報酬の減額など)

軽微な罰則 (権限の剥奪、再研修など)



n = 145人 (従業員)
設問：次のうち、あなたがよりセキュアに行動する(組織のサイバーセキュリティ・ガイダンスに常に従う)動機になるものはどれですか。最大3つまで選択してください。
出典：2025 Gartner Secure Behavior: Employee Perspective Survey

実用的で客観的なインサイト

成功に向けて、組織の態勢を整えましょう。ITリーダーおよびそのチーム向けの無料リソースとツールも、ぜひご活用ください。



コンファレンス

ガートナー サイバーセキュリティ & リスク・マネジメントサミット

複雑化し、変化し続けるサイバー脅威に対して、組織を守るためのインサイトを入手できます。

詳細を見る



Gartnerによるご支援

Gartner for CISOs: 最高情報セキュリティ責任者 (CISO) 向けサービス

AI搭載ツール、オンデマンドのインサイト、インタラクティブな体験で、成果の創出を加速します。

詳細を見る



Webinar

ランサムウェア対策：事業停止リスクに備えるバックアップの再定義と復旧戦略

ランサムウェア被害時に重要なのは、バックアップの有無ではなく迅速な復旧能力です。事業再開を阻まれたケースから学び、事業停止期間を短縮するための復旧戦略を解説します。

今すぐ視聴



Webinar

AI時代のセキュリティ運用に求められる新しいアプローチ方法

AIを活用して自社のセキュリティをどのように強化すべきか、そしてその取り組みをどのように推進するのかについて、「AIセキュリティ戦略」の観点から解説します。

今すぐ視聴

Gartner のお客様は、クライアント・ポータルでさらに多くのリソースをご利用いただけます。 [ログイン](#)

Connect with us

Gartner は、経営幹部およびそのチームに対し、実行可能かつ客観的なビジネスおよびテクノロジーのインサイトを提供します。Gartner のエキスパートによるガイダンスやツールは、組織の重要な課題について、迅速で優れた意思決定と大きな成果の創出を可能にします。

Gartnerのサービスに関するお問い合わせ

サイバーセキュリティ・リーダーを成功に導く
gartner.co.jp/ja/cybersecurity

最新のインサイトをご確認ください



Gartner のコンファレンスにご参加ください
[コンファレンスの最新情報を見る](#)