Press Release
2026 年 9 月 18 日（金）
ウォッチガード・テクノロジー・ジャパン株式会社

ウォッチガードのグローバル調査で、シャドーAI や安全性に欠ける業務習慣の急増に伴い、従業員がサイバーセキュリティリスクの高まりを招いていることが判明

従業員の行動と組織のセキュリティ対策との間にギャップが拡大

2026 年 9 月 18 日（金）- 企業向け統合型サイバーセキュリティソリューション（ネットワークセキュリティ／アイデンティティセキュリティ／エンドポイントセキュリティ）のグローバルリーダーである WatchGuard（R）Technologies の日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、以下ウォッチガード）は、従業員の行動が、中堅／中小企業（SMB）にとって見過ごされがちな、サイバーセキュリティ上の重大リスクを生み出していることを明らかにしました。

「2026 Cybersecurity Hygiene Report」によると、従業員の 64%が業務で許可されていない AI ツールを使用していることを認めており、急速に拡大しているシャドーAI 問題の一因となっていますが、ほとんどの組織が管理できていないのが現状です。

一方で、職場で一般的な習慣がリスクをさらに高めています。従業員の 76%がパスワードを再利用し、70%が業務で公衆 Wi-Fi を利用し、50%が VPN による保護なしに社内リソースにアクセスしており、これにより組織は認証情報の盗難、データの傍受、不正アクセスといったリスクに晒されています。

ウォッチガードのセキュリティオペレーション担当ディレクタ、マーク・ラリベルテ（Marc Laliberte）は次のようにコメントしています。「企業はセキュリティツールに投資していますが、多くの企業では依然として、従業員が実際にどのように業務を行っているかについて、十分に可視化できていません。AI の利用からパスワードの管理方法に至るまで、日常的な行動が、従来の対策では対処できないリスクを生み出しています。」

AI の導入が加速するにつれ、管理が困難に

一般消費者向けの AI ツールの登場により、新たなセキュリティリスクの分野が急速に拡大していますが、ほとんどの組織では、これに対して未だに正式なガバナンス体制を整備できていません。本レポートで概説されているように、回答者の 30%未満しか、自社が使用中のソフトウェアの正確なインベントリを管理していると認識しておらず、40%近くが、従業員が使用するアプリケーションを完全に把握できていないまま業務が遂行されていると回答しました。

ツールの利用承認に対する指針や、外部へ漏れる可能性のある情報についてのガバナンスの欠如は、IT およびサイバーセキュリティチームにとって危険な死角を生み出しています。

広範囲におよぶ安全ではない作業習慣が、依然として横行

シャドーAI 以外にも、従業員の広範な行動が組織のセキュリティ基準を損ない続けており、ハッカーに攻撃の機会を与え続けています。その例としては、次のようなものがあります：

- 従業員の 76%が、複数のアカウントで同じパスワードを再利用していることを認めており、これは、たった 1 つの認証情報が漏洩しただけで、アカウントの乗っ取り、水平移動、および複数のシステム、プラットフォーム、アプリケーションにわたる大規模なデータ流出のリスクに組織が晒されることを意味します。さらに、回答者の 30%が、他人とパスワードを共有していると回答しました。
- 70%の人が業務で公衆 Wi-Fi を利用しており、50%の人は VPN による保護なしに企業のリソースにアクセスしています。これにより、組織の攻撃対象領域が大幅に拡大し、セキュリティ対策が施されていない接続を標的とした、中間者攻撃やその他の脅威を通じて、データの傍受、認証情報の盗難、および不正なネットワークアクセスに晒されるリスクが高まります。
- 55%の人が業務用端末を私的な用途に使用しており、これにより、マルウェア感染やフィッシング攻撃のリスクが高まるほか、組織のセキュリティ制御を迂回する可能性のあるアプリケーションや Web サイトに晒されるリスクも生じています。ハイブリッドワークやリモートワークの普及により、私生活と仕事の境界線が曖昧になり、攻撃者が企業データを侵害する新たな機会が生まれているため、セキュリティチームがリスクを効果的に軽減することがより困難になっています。

MSP が増大する従業員のリスクに対処できる体制を整備

生産性向上への圧力の高まり、労働環境の変化、そして技術の急速な導入が、従業員全体にリスクを伴う行動を引き起こしています。

これにより、マネージドサービスプロバイダー（MSP）にとっては、中小企業が深刻なインシデントにつながる前に、サイバーセキュリティの基礎的な対策における不備を解消できるように支援する明確なチャンスが生まれます。

ラリベルテはさらに続けます。「これらの調査結果は、サイバーセキュリティリスクにおけるより広範な変化を浮き彫りにしています。組織が新しいテクノロジーを導入し、分散型の勤務を支援するにつれ、人間の行動を管理することが重大な要件となりつつあります。MSP にとって、これはテクノロジーの枠を超えて、ユーザーのリスクの可視化、ポリシーガバナンス、そして継続的なセキュリティ意識向上へと事業を拡大する好機となります。」

リスクを軽減するため、ウォッチガードは、SMB（中堅／中小企業）および MSP パートナーに対し、パスワードマネージャーや多要素認証（MFA）の導入、不正なシャドーテクノロジーの使用の特定、AI の利用に関する明確な利用規定の策定、VPN やゼロトラストアプローチによるオフィス外への保護範囲の拡大、そして技術的指標と併せて人的リスクの指標を追跡しながら継続的なセキュリティ研修を実施することなど、6 つの実践的な対策に注力することを推奨しています。

調査結果の全文「2026 Cybersecurity Hygiene Report」は以下よりダウンロードしてください。
https://www.watchguard.com/wgrd-resource-center/2026-cyber-hygiene-report

調査方法

本調査結果は、米国、英国、ドイツ、フランス、スペイン、オーストラリア、メキシコ、ブラジルにおける中堅／中小企業および中堅企業（従業員数 50～500 名）に勤務する従業員 684 名を対象とした、独立したオンライン調査に基づいています。 本調査は 2026 年 4 月に実施されました。すべてのパーセンテージは、従業員の自己申告に基づいています。

*本資料は、本社が発表したプレスリリースの翻訳版です。

【WatchGuard Technologies について】

ウォッチガードは、マネージドサービスプロバイダー（MSP）向けに設計された統合型サイバーセキュリティ分野におけるグローバルリーダーです。30 年以上にわたり、MSP が大規模なセキュリティ対策を提供する方法を確立し、脅威情勢のあらゆる大きな変化に先んじるべく、絶えず革新を続けてきました。AI を活用した「Unified Security Platform（R）」により、ゼロトラストに対応したネットワーク、エンドポイント、アイデンティティ保護機能を単一の統合プラットフォームで提供

し、複雑な運用の軽減、対策成果の向上、ビジネスの効率的な成長を可能にします。世界中で 150 万社以上の顧客を保護する 25,000 社以上の MSP に利用されており、パートナーが世界中の顧客に対して、強力かつ測定可能なセキュリティの成果を提供できるよう支援しています。

さらなる詳細情報、プロモーション活動、最新動向は X（@WatchGuardJapan）、Facebook（@WatchGuard.jp）、をフォローして下さい。
X： https://twitter.com/WatchGuardJapan
Facebook： https://www.facebook.com/watchguard.jp

また、最新の脅威に関するリアルタイム情報やその対策法は SecplicityJP までアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041 東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
マーケティング担当
Tel： 03-5797-7205 Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL：https:/www.watchguard.co.jp