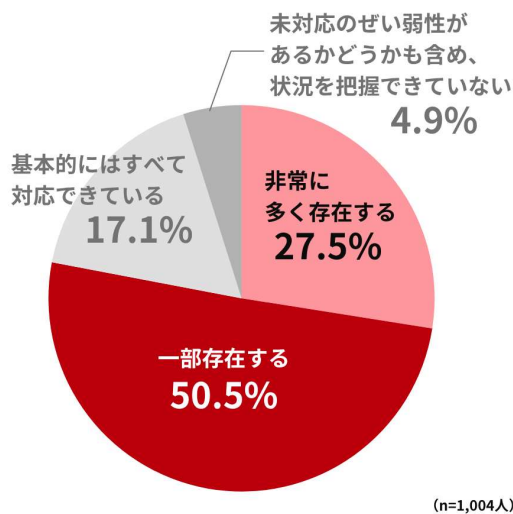


2026 年 9 月 29 日  
株式会社日立システムズ

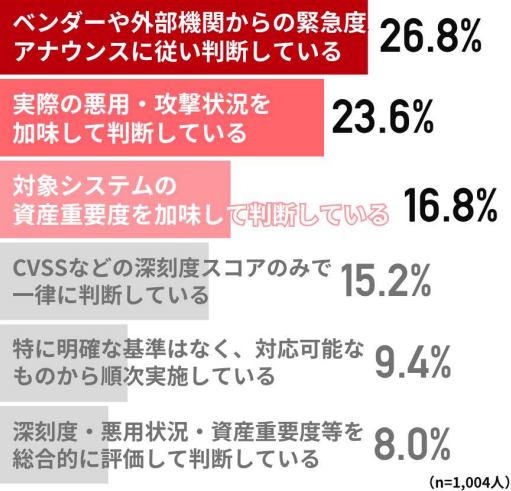
## フロンティア AI 時代のサイバーレジリエンス（パッチ適用の壁と復旧体制）の調査結果について

「経営課題化の遅れ」とパッチ適用を阻む現場の壁

ぜい弱性のアラートに対し、実務上の対応が追いつかず実質的に未対応のまま放置されているぜい弱性がありますか？



発見されたぜい弱性の対応優先度（どれから先にパッチを当てるか）は、主にどのような基準で決定していますか？  
※全7項目中上位6項目を抜粋



《調査概要：「フロンティアAI時代のサイバーレジリエンス（パッチ適用の壁と復旧体制）」に関する調査》  
 ・調査期間：2026年9月1日（火）～2026年9月4日（金） ・調査方法：インターネット調査 ・調査元：株式会社日立システムズ  
 ・調査対象：調査回答時に①企業（金融業・保険業を除く）の情報システム部門・セキュリティ部門の責任者・担当者／②地方金融機関（地方銀行・第二地方銀行・信用金庫・信用組合）の情報システム部門・セキュリティ部門の責任者・担当者と回答したモニター  
 ・モニター提供元：PRIZMAリサーチ ・調査人数：1,004人（①791人／②213人）

株式会社日立システムズ(以下、日立システムズ)は、セキュリティ対策の重要性を啓発することを目的に、企業の情報システム部門・セキュリティ部門の責任者や担当者約 1,000 名を対象に、「フロンティア AI 時代のサイバーレジリエンス（パッチ適用の壁と復旧体制）」に関する調査を行いました。

近年、生成 AI をはじめとするフロンティア AI の急速な進展に伴い、AI を悪用してシステムのぜい弱性を自動かつ超高速で探索・攻撃する高度なサイバー脅威が現実化しています。これを受け、金融庁が金融機関に向けて「フロンティア AI」を悪用したサイバー攻撃への対応要請を出すなど、超高速の脅威が現実となる中、その危険性は全業界に及んでいます。前回の調査「[フロンティア AI の脅威に対する認知・対策実態とセキュリティ運用課題](#)」（※）では約 9 割の企業が未知の脅威に危機感を抱く一方、パッチ適用の遅れなど現場の深刻な「運用の壁」が浮き彫りになりました。

そこで今回、技術負債の実態から復旧訓練の実効性まで、サイバーレジリエンス強化を阻む課題に関する実態調査を実施しました。本調査からは、フロンティア AI 時代における高度なサイバー脅威に対し、企業のセキュリティ運用が抱える構造的な限界と「実効性」の欠如が浮き彫りになりました。

サイバー攻撃の予兆や検知があった際、被害拡大を防ぐためシステムを能動的に緊急停止する明確な判断基準（経営層への即時報告・決裁フロー含む）は整備されていますか？

明確に整備されており、  
速やかに実行可能な体制がある

33.0%

整備されているが、有事を想定した  
訓練・演習は実施していない

47.6%

基準やルールはあるが、業務への影響を  
恐れ現実的に実行ハードルが高い

13.5%

判断基準や決裁フロー自体が  
整備されていない

5.9%

(n=1,004人)

《調査概要：「フロンティアAI時代のサイバーレジリエンス（パッチ適用の壁と復旧体制）」に関する調査》  
・調査期間：2026年9月1日（火）～2026年9月4日（金） ・調査方法：インターネット調査 ・調査元：株式会社日立システムズ  
・調査対象：調査回答時に①企業（金融業・保険業を除く）の情報システム部門・セキュリティ部門の責任者・担当者／②地方金融機関（地方銀行・第二地方銀行・信用金庫・信用組合）の情報システム部門・セキュリティ部門の責任者・担当者と回答したモニター  
・モニター提供元：PRIZMAリサーチ ・調査人数：1,004人（①791人／②213人）

金融庁が求める対応要請において、多くの企業が「優先システムの特定」や「経営課題化」といった戦略段階でつまずいています。守るべき自社資産の優先順位が明確でないため、外部のアラートに振り回される一面的な評価に依存し、結果として約 8 割の企業で未対応のぜい弱性が放置されるという深刻なキャパシティ不足を引き起こしているのが実状です。さらに、7 割以上の企業に残存する「レガシーシステム」などの技術負債や、不具合検証・他部署調整といった日々の実務負荷が、迅速なパッチ適用を物理的に阻む大きな壁となっています。

また、侵入を前提とした事後対応の要である「復旧体制」においても、ぜい弱な実態が明らかになりました。半数以上の企業が同時暗号化リスクを防ぐ強固なバックアップ保護を実施できておらず、定期的な復旧テストを行えている企業は約 3 割にとどまります。復元時の世代選定基準の欠如や、システムの緊急停止訓練の未実施など、ルールやマニュアルは存在しても有事に即座に機能する「実効性」が伴っていない現状が推測されます。

巧妙化・高速化するサイバー攻撃に対し、もはや自社の人材とリソースだけで完璧な防御と復旧体制を維持することは極めて困難です。企業は自社の限界を正確に把握したうえで、専門的な知見や BPO サービスを効果的に活用し、経営層を含めた全社横断的なサイバーレジリエンスの強化に取り組むことが求められています。

日立システムズは、急速進化するセキュリティ脅威へのタイムリーな対応や、限られたリソースの中での運用体制構築に苦勞している企業をサポートするべく、日立グループで取り組んでいるフロンティア AI 対策を通じて得た知見や自社のセキュリティサービスを活用してまいります。

フロンティア AI 時代のサイバーレジリエンス（パッチ適用の壁と復旧体制）の調査結果の詳細について

[https://www.hitachi-systems.com/-/media/secure/info/report\\_20260929\\_frontierai2.pdf](https://www.hitachi-systems.com/-/media/secure/info/report_20260929_frontierai2.pdf)

日立システムズのセキュリティソリューションの Web サイト

<https://www.hitachi-systems.com/secure/index.html>