Press Release

2025 年 4 月 22 日
フューチャー株式会社
(東証プライム:証券コード 4722)

脆弱性対応の実施状況、41.2%が「多くは手動で対応」
5 割以上の企業で「専門知識を持つ人材の不足」が課題
大企業の情報システム・セキュリティ対策担当者に聞いた「セキュリティ対策実態調査」

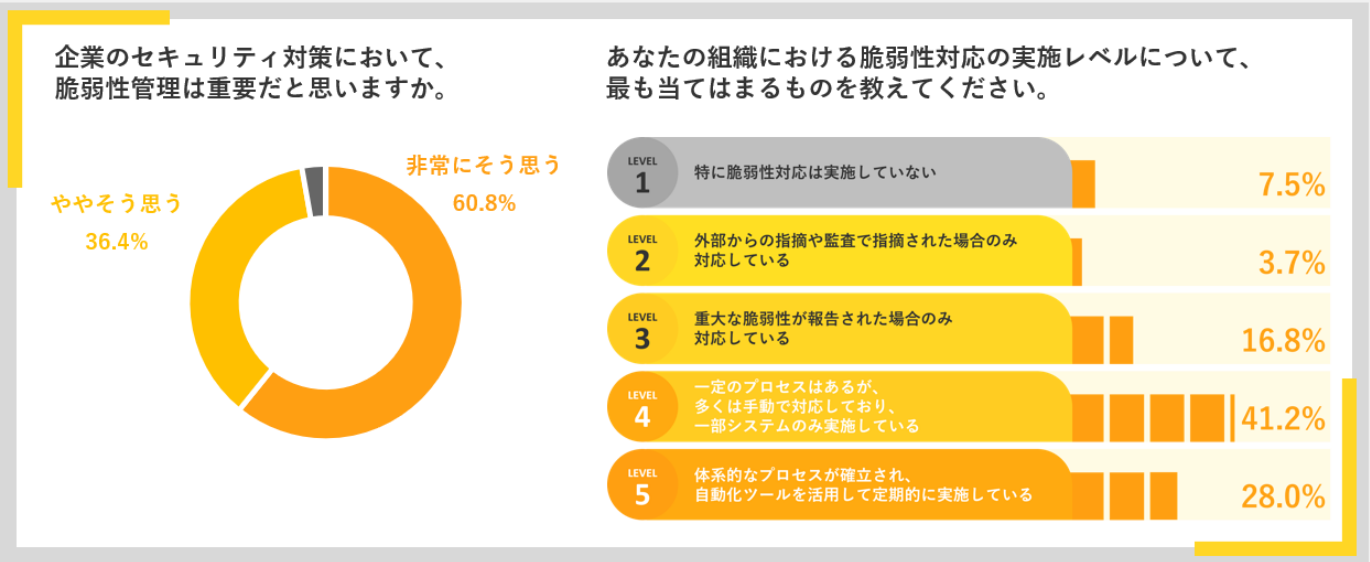
フューチャー株式会社(本社:東京都品川区、代表取締役会長兼社長 グループ CEO 金丸恭文、以下フューチャー)は、従業員数 1,000 名以上の大企業の情報システム担当者またはセキュリティ対策担当者 107 名を対象に、サイバー攻撃による侵入を防ぐための初期対応である「脆弱性管理」に関するセキュリティ対策実態調査を実施し、2025 年 4 月 21 日に結果を公表しました。

※調査結果の詳細はホワイトペーパーとしてダウンロードいただけます(https://vuls.biz/resource/)。

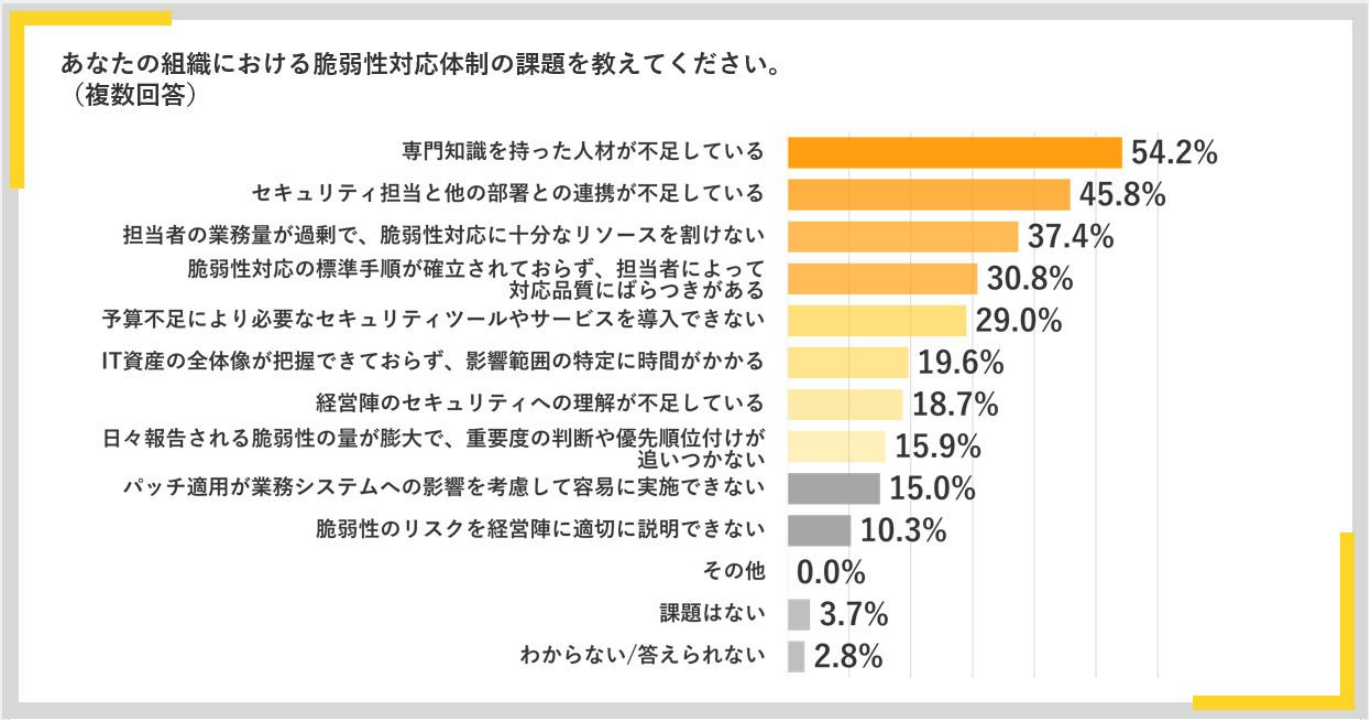
■ **サマリー**

- **97.2%が脆弱性管理は重要**と回答。
- 脆弱性対応体制の課題として、**「専門知識を持った人材の不足」が 54.2%**で最多。
- 組織における脆弱性対応の実施レベルでは**「一定のプロセスはあるが、多くは手動で対応しており、一部システムのみ実施している」が 41.2%**と最多。
- 脆弱性対応の課題では**「パッチ適用作業の長期化」**や**「アプリケーションの動作不良が生じること」がそれぞれ約 4 割**。
- 脆弱性管理の効率化・高度化に向けた今後の取り組みとして、**「脆弱性対応プロセスの標準化」**と**「専門人材の育成・確保」**を挙げる回答が最多。

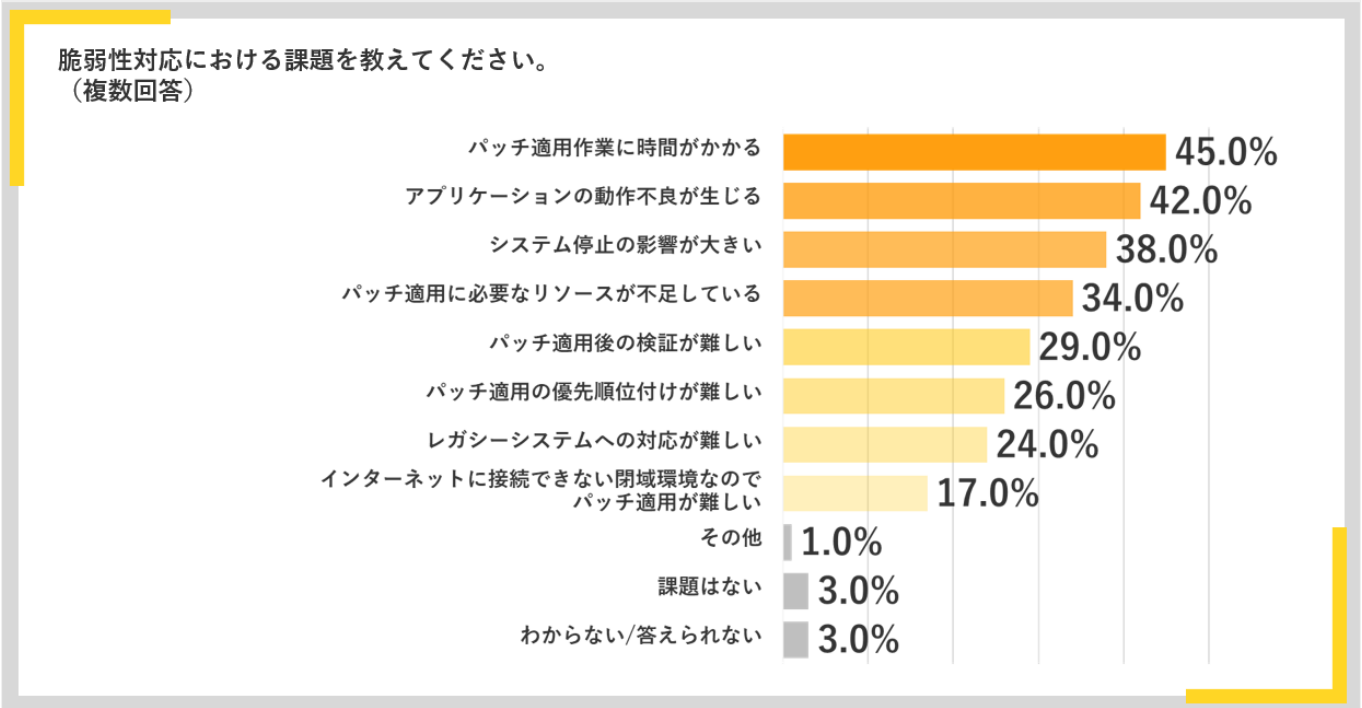
今回の調査では、回答者の 97.2%が企業のセキュリティ対策において、「脆弱性管理が重要」と回答しました。一方で、組織における脆弱性対応の実施レベルについて、「実施していない(レベル 1)」から「重大な脆弱性が報告された場合のみ対応(レベル 3)」が 28.0%、「一定のプロセスはあるが、多くは手動で対応しており、一部システムのみ実施(レベル 4)」が 41.2%という結果でした。サイバー攻撃が増加傾向にあり、企業のセキュリティが重要性を増すなか、脆弱性対応の自動化・効率化・標準化が遅れ、セキュリティ担当者には負担が大きい状況と考えられます。



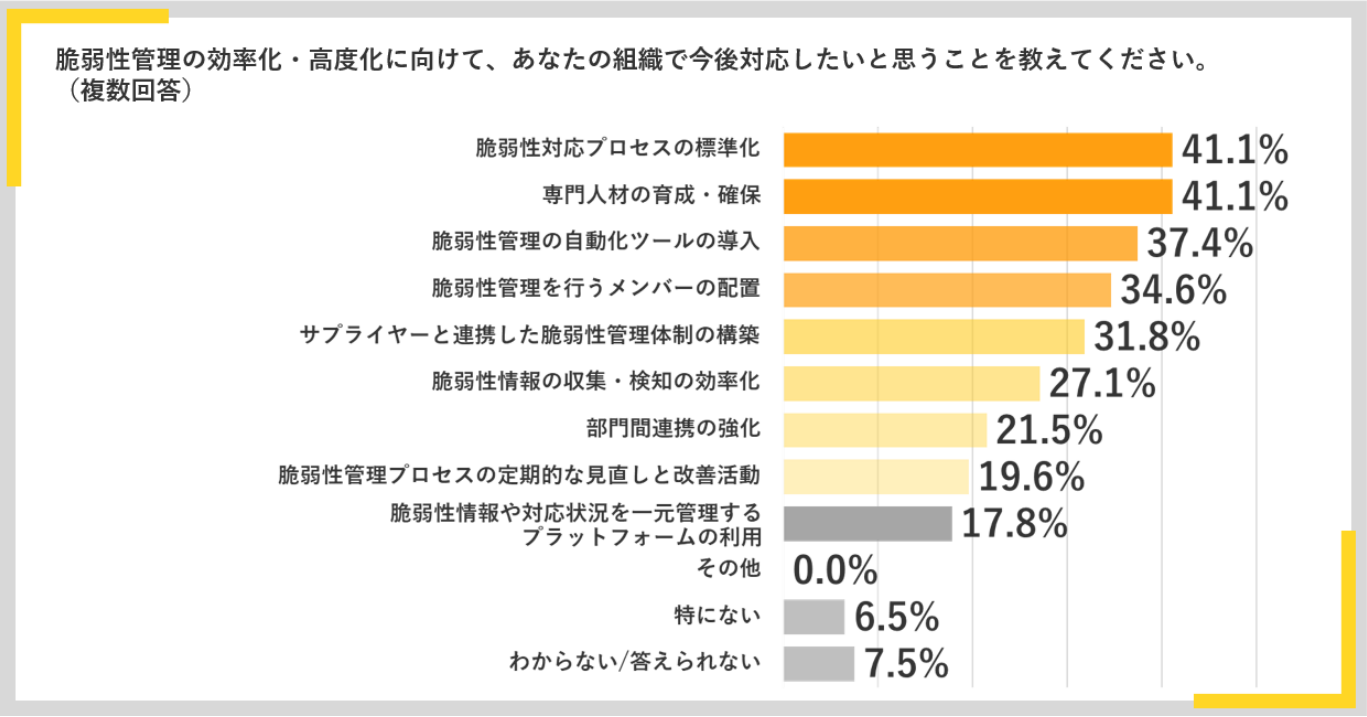
組織における脆弱性対応体制の課題としては、「専門知識を持った人材の不足」が 54.2%と最も多く、「セキュリティ担当と他の部署との連携不足」が 45.8%、「担当者の業務量が過剰で、脆弱性対応に十分なリソースを割けない」が 37.4%と続き、人材不足により業務がひっ迫している状況がうかがえます。



また、脆弱性対応における課題として、「パッチ適用作業に時間がかかる」が 45.0%、「アプリケーションの動作不良が生じる」が 42.0%となりました。サイバー攻撃のリスク増大や、攻撃による業務停止といった重大な事態につながるだけでなく、顧客にも影響を及ぼし得る課題が顕在化しています。



脆弱性管理の効率化・高度化に向けて今後対応したいことでは「脆弱性対応プロセスの標準化」と「専門人材の育成・確保」が 41.1%と同率で最多となりました。いずれも多くを手動での作業に依存した脆弱性対応のありかたや、専門知識を持つ人材の不足といった課題を解決するために、非常に重要な取組みです。対応プロセスを標準化することで、自動化ツールの導入も容易になり、担当者の経験やスキルにかかわらず誰でも一定の品質で対応できるようになります。



■ 調査レポート総括

今回の調査結果から、脆弱性管理の重要性や、自社組織において脆弱性情報の収集・検知に課題があることが担当者レベルでは強く認識されていることがわかりました。一方で、多くの企業で課題を解決するために必要なセキュリティの専門人材や、ツール導入のための予算が不足するなど、セキュリティ投資が十分でない現状が明らかになりました。

しかし、毎年公開される脆弱性情報は数万件※といわれており、限られた人員が手動で対応できる件数ではありません。脆弱性管理ツールの導入により、対応を自動化することで、注力すべき業務が絞り込まれ、専門人材がいなくても優先度をつけた適切な脆弱性管理が可能になります。

DX が経営の中核となるいま、脆弱性管理をはじめとしたセキュリティ対策は、将来的な損失を回避し、企業活動を継続的に守るうえで欠かせません。経営層がセキュリティへの投資をコストではなく「企業価値を守り・高めるための投資」と位置づけ、責任をもって取り組むことが重要です。

フューチャーでは、脆弱性管理ソリューション「FutureVuls」の提供をはじめ、あらゆる業種・業界のお客様を対象に、企業における組織、業務、ICT システムに関わるセキュリティリスクを整理し、現状の可視化および最適化を実現する総合的なセキュリティコンサルティングサービスを提供しています。今後も企業のセキュリティ対策の高度化をつうじて、お客様の未来価値最大化に貢献してまいります。

※ 共通脆弱性識別子「CVE」（Common Vulnerabilities and Exposures）を特定、管理する Web サイト「cve.mitre.org」に公開される脆弱性情報の件数。

■調査概要

・調査名称：大企業のセキュリティ対策実態調査
・調査方法：インターネット調査
・調査時期：2025 年 3 月 26 日、27 日
・調査対象：従業員数 1,000 名以上の企業に勤める情報システム部門担当者またはセキュリティ対策を担当する方 107 名（調査は IDEATECH に委託）

※端数の処理を行っているため、合計が 100%にならない場合があります。
※本調査を引用される際には、「フューチャー株式会社 CSIG 調べ」とご記載ください。

■FutureVuls とは

脆弱性管理ソリューション「FutureVuls」は、システムの脆弱性検知から情報収集、対応判断、タスク管理、パッチ適用といった脆弱性管理の自動化を可能にしたソリューションです。SSVC（Stakeholder-Specific Vulnerability Categorization）による自動トリアージ機能を搭載することで、リスクベースでの対応優先度の判断から緊急度に合わせた対応指示までを全自動化し、大規模な組織での運用においてもスピーディーで安定した脆弱性管理を実現しています。製造業の SBOM 管理効率化、脆弱性管理の一元化により PSIRT 業務を支援することに特化した PSIRT プランも展開しています。

FutureVuls 製品サイト：https://vuls.biz/

FutureVuls PSIRT 製品サイト：https://vuls.biz/psirt-lp/

■FutureVuls に関するお問い合わせ先

https://vuls.biz/contact/

■本件に関する報道機関からのお問合せ先

フューチャー株式会社　広報担当：松本、石井　　TEL：03-5740-5721

お問い合わせフォーム：https://www.future.co.jp/apps/contact/corp/press_interview_entry.php