NEWS RELEASE

2026 年 4 月 28 日
タニウム合同会社

タニウム、国内企業 675 社を対象に実施した「サイバーインシデントと事業継続性の実態調査レポート」を発表

AI を活用した自律型 IT «Autonomous IT» のリーダーであるタニウム合同会社（日本法人本社：東京都千代田区、代表執行役社長：原田英典、以下タニウム）は、国内企業 675 社を対象に実施した「国内におけるサイバーインシデントと事業継続性の実態調査レポート」を発表しました。

「国内におけるサイバーインシデントと事業継続性の実態調査レポート」の全文はこちら：
https://explore.tanium.com/archive-japan-resource-center/col/2867cf5b-67e2-4d31-92ab-5096d09190cc/AR-State-of-Cyber-Incidents-and-Business-Continuity-Japan

現代のデジタル経済下において、サイバー空間を取り巻く安全保障環境は、かつてないほど地政学的緊張と技術進化が交錯する局面を迎えています。警察庁が公表した「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について（※）」によれば、サイバー攻撃は匿名性の高さから攻撃者側が優位に立ちやすい非対称的な構造にあり、国家を背景とした攻撃、生成 AI を悪用したランサムウェア、匿名・流動型犯罪グループによる金融犯罪など、サイバー脅威は多様化・深刻化しています。（※）：https://www.npa.go.jp/bureau/cyber/pdf/R07_cyber_jousei.pdf

歴史的に、多くの企業は自然災害やパンデミックを前提に BCP（事業継続計画）を整備してきました。しかし、サイバー脅威が多様化・深刻化する中、分秒単位で状況が変化するサイバーインシデントに対して、従来型 BCP が十分な実効性を持ち得るのか、いま改めて問われています。

本調査は、この課題意識のもと、国内企業が現時点でどの程度サイバーインシデントに対応し得る事業継続体制を整備しているのかを定量的に把握するとともに、製造、金融、流通・小売・商社、公務員・公共サービス、建設など業種を横断して共通する構造課題と、各業界特有のリスク・対応状況を明らかにすることを目的に実施しました。

■ 調査結果サマリー

- **経営と現場で復旧目標を合意できている企業は 2 割**
  サイバーインシデント発生時における復旧目標時間（RTO）について、経営が許容できるビジネスの限界停止時間と「協議して合致させている」と回答した企業は 20.4% に留まりました。

- **IT 資産を 100%把握・リアルタイム監視できている企業は 19.1%、シャドーIT への懸念は 72.3%**
  ネットワーク接続デバイスを 100%把握し、その脆弱性までリアルタイムに監視できている企業は 19.1% に留まり、約 8 割の企業が「見えない資産」や「監視の空白時間」を抱えている結果となりました。
  また、企業が把握しきれていない管理外資産（シャドーIT）に何らかの懸念を持つと回答した企業は 72.3% にのぼりました。

- **セキュリティ運用を一元管理できている企業は 27.3%**
  複数のセキュリティ機能を統合管理し、一元的な状況把握ができている企業は 27.3% に留まり、ツールの分散・サイロ化が依然として課題であることが分かりました。インシデント対応を全面的に自動化している企業は 19.7%に留まりました。

- **セキュリティ投資を“経営投資”と捉える企業は 4 割未満**
  セキュリティ投資を「KPI 化された投資」として捉えている企業は 36.9% にとどまり、44.7% の企業が「コスト」として認識していることが分かりました。依然として、サイバー対策が事業継続や競争力強化に向けた経営投資として位置づけられていない実態が浮き彫りとなりました。

- **製造業は IT 資産可視化・投資意識で先行、金融業は訓練・初動対応で高水準、流通業は対策格差が顕著**
  業種別に見ると、製造業は IT 資産可視化や投資意識で先行する一方、OT 環境やサプライチェーン由来のシャドーIT への懸念が高い結果となりました。金融業は訓練実施率や初動フロー整備率など実行面で高水準を示し、規制対応を背景とした成熟度がうかがえます。
  一方、流通・小売・商社では、セキュリティを投資として捉える企業とコストとして捉える企業の差が大きく、対策レベルの“二極化”が顕著となりました。公務・公共分野では、意思決定や経営報告体制の整備余地が浮き彫りとなっています。

■総論

本調査により、多くの企業で従来型 BCP と現代のサイバーリスクとの間にギャップがある実態が明らかになりました。経営層が関与した復旧目標（RTO）の設定や迅速な意思決定体制、初動訓練まで整備できている企業は限定的です。また、IT 資産の可視化やシャドーIT の統制も十分とは言えず、「見えない資産」が侵入口や復旧遅延の要因となる可能性があります。

今後は、分散した運用を統合するプラットフォーム整備と、自動化による迅速な対応体制の構築が不可欠です。したがって、サイバーレジリエンス強化は、IT 部門だけでなく経営課題として取り組むことが必要です。

■調査概要

調査名：国内におけるサイバーインシデントと事業継続性の実態調査

調査主体：タニウム合同会社

調査実施期間：2026 年 1 月 19 日～31 日

調査方法：オンライン

有効回答数：675 社

主要業種構成：製造業 218 社（32.3%）、サービス 140 社（20.7%）、流通・小売・商社 79 社（11.7%）、公務員・公共サービス 69 社（10.2%）、金融業 61 社（9.0%）、建設業 41 社（6.1%）、その他 67 社（9.9%）

設問数：全 32 問（うち、本レポートの 3 つのテーマに直接関連する設問を選択的に抜粋して分析）

■タニウムについて

タニウムは自律型 IT «Autonomous IT» 企業です。Tanium Autonomous IT は 、AI とリアルタイムのエンドポイントインテリジェンスを駆使し、IT およびセキュリティチームに、組織を「アンストッパブル」な存在にする力を与えます。

世界の主要企業の多くが、エンドポイント管理とセキュリティを統合したタニウムの単一プラットフォームを信頼し、より迅速なイノベーション、強靭性の維持、そしてビジネスを自信を持って前進させています。
タニウムがどのように自律型 IT «Autonomous IT» でアンストッパブルなビジネスを実現しているかについては、**https://www.tanium.jp/**と **LinkedIn** をご確認ください。

日本法人名：タニウム合同会社
グローバル代表 CEO：ダン・ストリートマン
日本代表執行役社長：原田英典
設立年：2007 年
設立年（日本）：2015 年
所在地（日本オフィス）：〒100-0004 東京都千代田区大手町 2 丁目 6-4 常盤橋タワー25F

事業内容：自律型エンドポイント管理のプラットフォーム提供
URL：https://www.tanium.jp/

■免責事項

ここに記載されている情報は一般的な情報提供のみを目的としています。本情報は、当社が将来の製品、特徴、または機能を提供することについて確約、保証、申し出、および約束を行うものでも、法的義務を負うものでもありません。また、いかなる契約にも組み込まれることを意図しておらず、そのように見なされるものでもありません。最終的に提供される製品、特徴、または機能の実際の時期は記載されているものと異なる可能性があります。