NEWS RELEASE

2025 年 10 月 9 日
タニウム合同会社

タニウム、新機能「Tanium Ask™」発表に伴う記者説明会を開催

～AI 時代に求められる「IT 資産管理 2.0」を提言～

AI を活用した自律型エンドポイント管理（AEM）プラットフォームで業界をリードするタニウム合同会社（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、2025 年 9 月 30 日（火）に AI 搭載の新検索機能「Tanium Ask™」の発表に伴う記者説明会を開催しました。

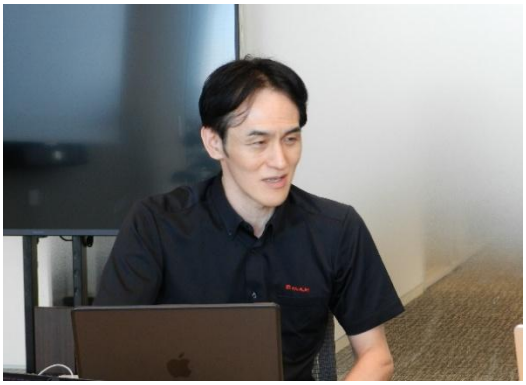
当日は、タニウム合同会社 チーフ IT アーキテクトの楢原 盛史（写真左上）、タニウム合同会社 執行役員 ソリューションアーキテクト本部 本部長の作野 竜（写真右上）、Tanium Inc. アジア太平洋日本地域 技術担当バイスプレジデント 兼 日本法人 最高技術責任者の小松 康二（写真左下）が出席しました。

説明会では、リアルタイムでのエンドポイント情報の可視化と動的管理を「IT 資産管理 2.0」と位置づけ、AI 時代に求められるセキュリティ戦略を提言しました。あわせて「セキュリティ投資×ガバナンス実態調査 2025」（※1）を発表するとともに、9 月から日本語での提供を開始した AI 検索新機能「Tanium Ask」（※2）を初披露しました。さらに、自然言語の入力による端末情報収集のデモンストレーション等により、操作性や実用性についても紹介しました。

※1 「セキュリティ投資×ガバナンス実態調査 2025」参考プレスリリース：https://www.tanium.jp/press-releases/security_investment_governance_survey2025/

※2 AI 検索新機能「Tanium Ask」参考プレスリリース：https://www.tanium.jp/press-releases/tanium_ask_2025/

■AI 時代に求められる「IT 資産管理 2.0」を提言



冒頭、楢原が登壇し、グローバルなセキュリティトレンドを概観しました。そのうえで、「DX が当たり前になった今、セキュリティが利便性を阻害してはいけない」と述べ、従来の統制一辺倒の考え方からの転換を呼びかけました。そして、自由度を認めつつ越えてはならない領域にガードレールを設け、本社が責任を持ってモニタリングするスタンスへと変化しつつあるトレンドを紹介しました。

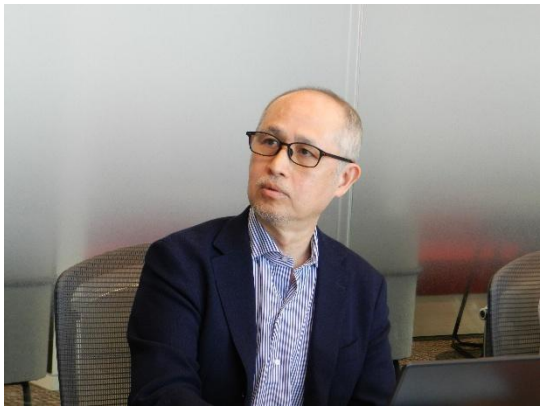
続いて、セキュリティと利便性のトレードオフからの脱却が各国で重要なテーマになっていることに触れ、「欧州の GDPR・NIS2・サイバーレジリエンス法・AI 規制法、米国の HIPAA 報告義務強化など制度変更が進む中、違反時には巨額のペナルティが科されるリスクがある」と指摘しました。さらに、「リモート／在宅／オフィスの多様な勤務環境をカバーするには、リアルタイムかつ高精度の可視化が不可欠だ」と強調しました。

また、楢原は、従来の IT 資産管理を「資産管理 1.0」と位置づけ、その役割は実態管理に留まっていると述べました。「クラウドやハイブリッド環境の拡大、サイバーリスクの高度化により、何がどこにどの状態で存在するかを正確に把握する必要性が増している」と言及し、従来型の IT 資産管理では限界があると指摘しました。

そのうえで、今後求められるものとして提言したのが、「データの活かす化」をテーマとした「IT 資産管理 2.0」です。「リアルタイムのデータ取得と正確性を前提とすることで、資産実態だけでなく利用状況も把握できるようになる。これにより、単なる把握から目的別の管理へと価値が進化していく。コスト・セキュリティ・コンプライアンスの観点から部門横断での最適化（統制管理）も可能となる」と説明しました。

主なツールはエンドポイントプラットフォームと台帳（CMDB）であり、さらに政府や金融庁のガイドラインでも最新状態の網羅的な把握が求められていることを背景に、「こうした公的方針が『IT 資産管理 2.0』への移行を後押ししている」とまとめました。

■「セキュリティ投資×ガバナンス実態調査 2025」から見えた課題とは



続いて、作野が「セキュリティ投資×ガバナンス実態調査 2025」の結果を解説しました。本調査は大企業を中心に 668 名の IT 管理者・担当者を対象に実施したもので、以下 3 つの視点から傾向が明らかになりました。

1. DX とセキュリティ予算: 多くの企業で DX の効果が現れており、合わせてセキュリティ投資も引き続き拡大傾向にある。昨年増額した企業は、現状維持」との回答も多く、DX 推進にはセキュリティが不可欠とする結果が示さ

れた。一方で、セキュリティ専門人材の不足や施策最適化による予算効率化が課題となっている。

2. セキュリティガバナンス：国内拠点では一定のガバナンスが確立されつつあるが、海外の子会社や拠点を含めた統制は依然として不十分。専門人材の不足やタイムリーな対応の難しさがボトルネックとなっている。

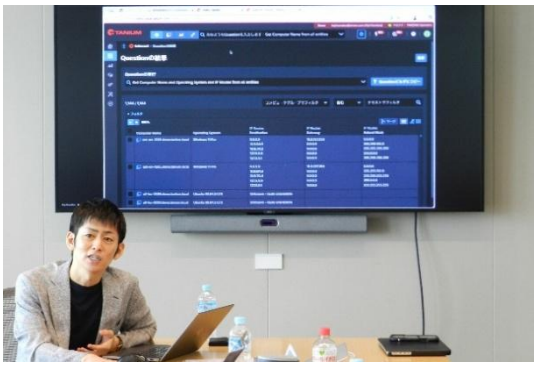
3. セキュリティ評価：約 7 割の企業が KPI を設定している一方、適切にかつ定期的に評価を実施しているのは 3 割未満にとどまる。網羅性・正確性・スピード・統一性が依然として課題。

作野は「投資の拡大に比べ、実効性ある評価体制が追いついていない」と述べ、セキュリティガバナンスの強化が喫緊の課題であるとしました。そのうえで、これを実現するにはテクノロジーの活用が不可欠であり、特に AI による専門人材の補完が重要だと訴えました。

■AI 搭載の自然言語で脆弱性を把握する新機能「Tanium Ask™」を紹介

最後に小松が登壇し、タニウムが提供する自律型エンドポイント管理（AEM）プラットフォームについて、「数十万台規模の端末をリアルタイムに可視化・管理し、資産管理から脆弱性対策、コンプライアンス対応までを統合的に担えるプラットフォームが自動化と AI で大幅に進化した」と特長を紹介し、そのうえで新機能「Tanium Ask™」を初披露しました。

「Tanium Ask」は、タニウムの管理コンソール上で利用できます。検索ボックスに日常的な表現で質問を入力するだけで、組織が管理する PC やサーバーなどのエンドポイントから、脆弱性のある端末の特定やパッチ適用状況の抽出などの様々な情報収集を行うことができます。小松は「特別な知識がなくても操作できるため、専門人材の不足を補い、迅速な対応を支援する」と強調しました。



会場ではデモンストレーションも行われ、自然言語による検索で「どのマシンに脆弱性があるのか、何のパッチがそれぞれのマシンにあたっているべきなのか」が瞬時に表示される様子などを実演しました。小松は「こうした可視化によって、これまで以上に迅速に脆弱性の状況を把握し対応できる」と述べ、AEM の進化を支える新機能の実用性を示しました。

■タニウムについて

Tanium Autonomous Endpoint Management (AEM) は、業種を問わずエンドポイントをインテリジェントに管理するための最も包括的なソリューションを提供し、IT 資産の発見とインベントリ、脆弱性管理、エンドポイント管理、インシデント対応、リスクとコンプライアンス、デジタル従業員体験の機能を提供します。タニウムのプラットフォームは、 Fortune 100 企業の 40%に導入され、世界中で 3,500 万のエンドポイント管理をサポートしています。より効率的な運用とより強化なセキュリティ体制を、規模に関わらず高い信頼性をもってリアルタイムで提供します。The Power of Certainty™の詳細については、**https://www.tanium.jp/**をご覧いただき、**Facebook**と**X** でフォローしてください。

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。