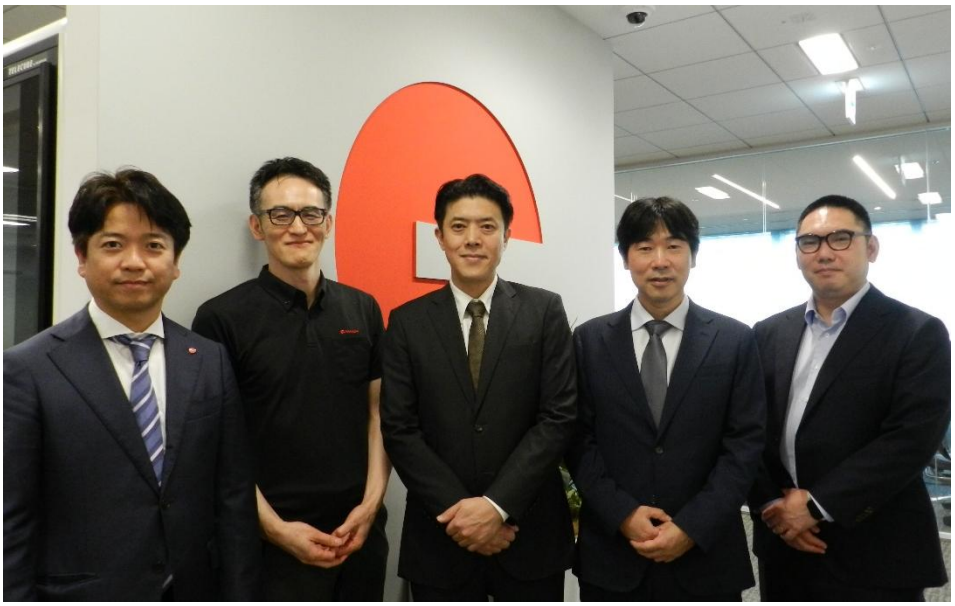
2026 年 11 月 9 日
タニウム合同会社

タニウム、パートナー企業・アイソプラの操作ログ収集機能「iScope」提供開始に伴う記者説明会を開催

～Tanium Autonomous IT Platform で取得・分析できるデータを拡張し、外部・内部双方のセキュリティリスクに対応～

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、販売パートナー企業である株式会社アイソプラ（東京都千代田区、代表取締役：寺村 淳士、以下アイソプラ）が開発した、Tanium Autonomous IT プラットフォーム（以下、Tanium）向け操作ログ収集機能「iScope」の提供開始に伴い、記者説明会を 10 月 21 日（水）に開催しました。



近年、不正アクセスに伴う情報漏えいや、退職者による情報の持ち出しといった内部不正など、企業を取り巻く外部・内部のセキュリティ脅威が深刻化しています。これらの脅威への対策には、端末の状況把握に加え、「人の操作」を把握することも重要となっています。今回アイソプラが開発した「iScope」は、Tanium の標準機能だけでは取得が難しい PC 操作ログを収集する機能です。Tanium の標準センサーで取得する端末情報と組み合わせることで、「誰が、いつ、どの端末で、何をしたのか」の把握を支援し、外部・内部双方のセキュリティリスクへの対応を支援します。

当日は、タニウム合同会社からマーケティング本部 ディレクターの村井新太郎、セキュリティーソリューションズプリンシパルストラテジストの楢原盛史、執行役員 ソリューションエンジニアリング統括本部 統括本部長の阿部俊、株式会社アイソプラから代表取締役の寺村淳士氏、テクニカルサービス本部取締役の下田泰輝氏が参加しました。説明会では、現状の課題や「iScope」の開発経緯と機能、「Tanium Atlas」と組み合わせた具体的な活用シーンなどを紹介しました。

■タニウムの会社概要や特徴を説明



村井は、タニウムの会社概要とプラットフォームの特長を紹介しました。タニウムは、大規模な環境で端末情報をリアルタイムかつ網羅的に収集できることを強みとしています。まず、「一つのプラットフォームで、エンドポイント管理、エクスポージャー管理、セキュリティ運用の 3 つのユースケースを提供しています」と説明しました。

また、ServiceNow などとの連携や、EDR 製品との共存についても紹介しました。導入当初は EDR 製品と競合するものと見られることもありましたが、現在はすみ分けが進み、共存モデルが主流になっていると話しました。

さらに、AI を活用した「リアルタイムインテリジェンス」の考え方に言及し、「人と AI が正確に判断し、即時に実行できるように、端末の『今』の状態を取得し、業界標準の情報と照らし合わせていく」と述べました。さらに、グローバルで 3,600 万台超の端末を管理している規模を生かし、端末のメタ情報を活用して、今取るべき対応を示していくと説明しました。

■AI 時代に高まる内部不正リスクと対策を解説



楢原は、組織シニシズムが高まるとモチベーションが低下し、組織への恨みが内部犯行につながるおそれがあると説明しました。フロンティア AI の登場など、AI の活用によって企業の IT インフラが大きく変化するなか、現在の不正アクセスに続き、来年以降は内部犯行がクローズアップされるとの見方を示しました。

従来の内部不正では、従業員や委託先による USB メモリーや資料、メールを通じた情報の持ち出しが想定されていました。一方、生成 AI の利用が広がると、機密情報が未承認の AI に入力されるなど、本人に持ち出す意図があるかどうかにかかわらず、情報が外部に渡った経路を把握しにくくなると指摘しました。そのうえで、日本の組織では「内部犯行への認識が弱い」と述べ、不正競争防止法や個人情報保護法、不正アクセス禁止法、刑法、経済安全保障に関する制度、特定秘密保護法など、関連する法律や罰則が定められていることにも触れました。

対策としては、人と AI、ヒューマン ID とノンヒューマン ID のアクセス制御や、攻撃経路（アタックパス）の把握が必要だと説明しました。また、「定期監査のような静的な監査では、これからは追いつきません。テクノロジーによって実態を正確に把握していくことが必要です」と述べました。

続いて、iScope は操作ログから行動の軌跡を可視化し、内部犯行につながる行動の意図も推定できると紹介しました。Tanium Atlas の AI と iScope が取得するデータを組み合わせ、Atlas への質問に応じて iScope のクエリやアプリケーションを連動させることで、変化する手口に対応した分析へ発展していくと説明しました。

■AI 時代の IT 業務実態と Tanium Atlas を解説



続いて阿部が、AI 時代の IT 業務と「Tanium Atlas」について解説しました。Confluent の調査*では、グローバルの IT リーダーの 72%がリアルタイムデータ基盤の不足を AI 活用の課題に挙げています。阿部は「AI が何を考えられるかと同じくらい、AI に何を見せられるかも重要」と指摘しました。

Tanium は、端末からリアルタイムに情報を取得し、不足があればその時点で追加できます。阿部は、このデータ取得方式が AI の回答の信頼性を支えると説明。端末データや各種インテリジェンスなどを活用する「Tanium Atlas」では、日本語で質問し、端末の可視化・分析から是正までを支援し API を通じた各種コントロールにも対応すると解説しました。

デモでは、脆弱性情報から該当端末を特定し、「修正版の展開計画を進めたい」と続けて質問する流れを紹介しました。また、環境全体の対策状況を確認し、「次に取り組むべきことを効果が高い順に 5 つ提案して」と尋ねると、端末の情報に基づく改善案が示されます。阿部は、提案を人が判断し、自社環境に合わせて対話しながら対応を進めると説明し、「Tanium Atlas によって自社環境に基づく調査が容易になり、活用するデータが広がることで、これまで見えなかった状況も把握できる」と述べました。

*出典: Confluent 社 Data Streaming Report 2026
https://www.confluent.io/ja-jp/press-release/2026-data-streaming-report/

■アイソプラの強みとタニウムとの連携について紹介



アイソプラ代表取締役の寺村様は、同社の事業とタニウムとの連携について説明しました。アイソプラは DX 開発を主力事業として設立し、現在はサイバーセキュリティ製品の開発や導入支援を主力としています。従業員は 71 名（2026 年 4 月 1 日時点）で、サイバーセキュリティ事業に注力し、タニウム製品への理解や導入実績を積み重ねてきました。

寺村様は、パートナーとなった経緯について、「2021 年にタニウムの技術について詳しく知り、今後多くの企業で必要になると考えた」と紹介しました。また、アイソプラには国内パートナーの中で最も多くのタニウム技術者が在籍し、製品への深い理解や導入実績、少数精鋭のエンジニアによる技術力、DX 開発で培ったソリューション開発力を同社の強みとして挙げました。「これらの強みとタニウムの技術を組み合わせ、これまでにない次世代型のサイバーセキュリティ・インテリジェンスを提供できると考えている」と語りました。

■iScope と Tanium Atlas を組み合わせた活用を紹介



続いて、アイソプラ取締役の下田様は、タニウムの導入・運用支援を通じて、顧客満足度の高さを実感する一方、標準機能に加えて日本企業のガバナンス上のニーズに対応する機会も得てきたと説明しました。その知見を生かして開発した iScope は、アイソプラが提供する Tanium Platform 向けの連携製品です。

iScope は新たなログ収集専用サーバーを設けず、タニウム標準の画面や操作感で利用できます。操作ログと Tanium Atlas を組み合わせ、点として記録さ

れた操作を行動の軌跡として分析することで、「専門知識がなくても、操作履歴の収集から行動分析、意図推定まで行える」と紹介しました。従来は専門家が担っていたユーザー行動分析（UBA）を社内で実現し、「サイバーセキュリティ・インテリジェンスの民主化」につなげると説明しました。

デモでは、「機密ファイルの流出が疑われる端末と経路を調査して」と日本語で指示し、Tanium Atlas が複数のログを横断して調査結果をまとめる様子を紹介しました。情報解析結果は全 8 章で構成され、第 1 章では流出が起きた端末と経路の概要、第 2 章では使用したデータや調査手法、第 3 章では検出したユーザー操作とその評価を示します。第 4 章では確認した事象を時系列で整理し、第 5 章で外部流出経路を評価、第 6 章で調査した操作を MITRE ATT&CK にマッピング、第 7 章で今後の対応の優先順位を示し、第 8 章では調査上の制約や留意事項を補足します。第 2 章では、印刷ログやブラウザーの URL、ファイル操作ログなど、iScope で収集した情報も調査に活用されていました。下田様は、専門家が数時間から数日かけていたログ解析や報告書作成にかかる時間を大幅に短縮できると説明しました。また、今後も国内のビジネスや企業ニーズに合わせて、iScope の機能を拡張していく方針を明かしました。

■アイソプラについて

会社名 ：株式会社アイソプラ
代表取締役：寺村 淳士
本社所在地：〒101-0054　東京都千代田区神田錦町三丁目 19 番地　廣瀬第 2 ビル 4 階
事業内容：サイバーセキュリティ製品開発及び導入支援、デジタルトランスフォーメーション開発
URL：https://isopra.co.jp/

■タニウムについて

タニウムは、自律型 IT «Autonomous IT» カンパニーです。AI がイノベーションとリスクの双方を加速させる中、タニウムの自律型運用システムである Tanium Atlas は、人間か AI エージェントかを問わず、すべての IT およびセキュリティの担当者を、Tanium Autonomous IT Platform の総力で支えます。タニウムは、担当者がエンドポイント環境全体にわたってマシンスピードで検知・判断・修復を行うために必要な、リアルタイムのインテリジェンス、エージェント型の意思決定、そして自律的な実行力を提供します。

タニウムは、2026 年に初めて発表された Gartner® Magic Quadrant™（エンドポイント管理ツール部門）においてリーダーとして評価されたほか、IDC MarketScape：Worldwide Client Endpoint Management Software for Windows Device Management 2025–2026 Vendor Assessment、および The Forrester Wave™：Endpoint Management Platforms, Q2 2026 においてもリーダーと位置付けられています。

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、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：オリオン・ヒンダウィ
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。

©2026 Tanium Inc. All rights reserved. Tanium は Tanium Inc. の登録商標です。その他の社名、製品名、サービス名は各社の商標または登録商標です。