TANIUM

HITACHI

エンドポイント管理の課題	Taniumによる改善
セキュリティリスクの増大 リアルタイムで棚卸や設定確認ができず、脆弱な端末が放置される恐れがある	資産を常時可視化し、**設定違反や脆弱な端末**を即座に発見・対応
情報収集の困難 正確な資産データが得られず、投資判断やリスク報告が遅れる	正確な資産情報を即時取得し、**迅速な意思決定と報告**を実現
管理負荷の増加 分散した端末の情報を手作業で集約するため、工数とミスが増加する	端末の連携により情報を統合し、**手作業の負荷とエラー**を最小限に抑制

日立ソリューションズがTaniumの導入から運用までをトータルに支援

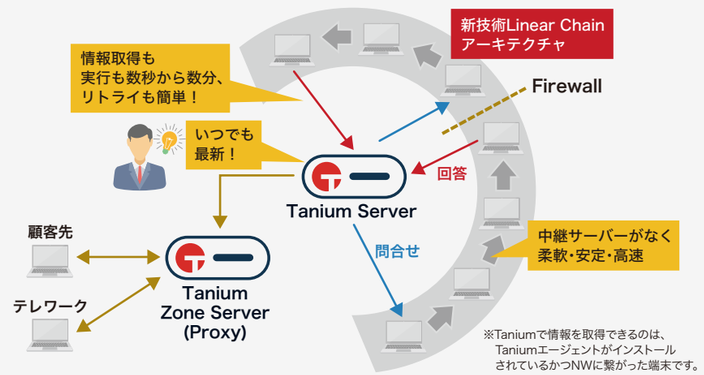
株式会社 日立ソリューションズ

リアルタイム性、スケーラビリティ、自動化、多機能性
Taniumは、脅威が激化する時代に即応する、統合エンドポイント管理サービスです

リアルタイム

リアルタイムで端末の状態を把握し、その場で対処

独自の通信方式により、常に最新の情報が自動で更新され、検索エンジンのような直感的な操作が可能です。従来の「情報取得に時間がかかる」「データが古く信頼性が低い」といった課題を解消します。



スケーラブル

大規模環境への対応も1つの管理コンソールで可能

Taniumはクラウドもオンプレミスも対応。大規模環境を前提として設計されているため、何万台ものエンドポイントに対しても、ネットワークやクライアントに負荷をかけることなく、リアルタイムで情報取得や操作が可能です。

情報収集

数万台規模のマシンから、OSの詳細情報などを柔軟に収集でき、転送量も少なく数秒から数分で完了。

コマンド実行

作成したスクリプトを数万台のマシンに一斉送信し、都度状態を確認しながら数秒から数分でコマンドを実行。

ファイル配信

多様な機能でネットワーク負荷を抑えつつ、各マシンの状態を確認しながら確実にファイルを配信。

自動化・自立型

継続的な運用改善を支える自動化と自立型運用

ポリシー設定など、エンドポイントへの変更が及ぼす影響をリアルタイムかつ正確に測定・分析。その結果をもとに自動化を実行することで、生産性の向上とセキュリティリスクの低減に貢献します。

AEM 機能例

- トレーニングやダッシュボードカスタマイズ、スクリプト作成などを支援。
- パッチ適用、コンプライアンス対策、脆弱性対策など複雑なタスクを自動化。
- AIを活用した自然言語インターフェイスで、Taniumへの問い合わせが可能に。

他製品連携

TANIUM + Microsoft

リアルタイムのエンドポイント情報をCopilotに統合し、迅速な脅威検出・対応とリスク評価を実現。

TANIUM + ServiceNow

リアルタイム分析と各種IT・セキュリティワークフローを統合し、変更管理および承認プロセスを効率化。

機能の豊富さ

エンドポイント管理からインシデント対応まで、運用負荷を軽減しながらセキュリティを強化
NIST CSF 2.0フレームワーク※に基づき多彩な機能を提供します

一つのプラットフォームで、資産管理、パッチ適用、設定変更、脆弱性管理、脅威検知など、事故発生前のサイバー・ハイジーンと、事故発生後のサイバー・レジリエンスに必要な機能を統合。部門間の連携が円滑になり、組織全体の運用効率が向上します。

※米国国立標準技術研究所(NIST)が策定した「サイバーセキュリティを改善するためのフレームワーク

統治 → 特定 → 防御 → 検知 → 対応 → 復旧

サイバー・ハイジーン 事故が発生する“前”の施策：原因特定、感染予防

サイバー・レジリエンス 事故が発生した“後”の施策：早期発見、波及防止

Taniumがエンドポイント管理の課題解決を全方位から支援

Asset（アセット） オフライン端末を含め、エンドポイント情報を管理するモジュール	**Benchmark（ベンチマーク）** エンドポイントのサイバーリスクを可視化・制御するモジュール
Comply（コンプライ） セキュリティ監査と脆弱性診断を実行するモジュール	**Reveal（リビール）** センシティブデータの存在を特定するモジュール
Deploy（デプロイ） ソフトウェアのインストール、更新、削除を行うモジュール	**Provision（プロビジョン）** ベアメタルプロビジョニングを行うDeployのAdd-on機能
Discover（ディスカバー） 非管理のIPデバイスを検出・特定するモジュール	**Performance（パフォーマンス）** エンドポイントの状態やリソース利用状況を可視化するモジュール
Enforce（エンフォース） エンドポイントのポリシー、防御機能を管理するモジュール	**Integrity Monitor（インテグリティモニタ）** ファイル・フォルダ・レジストリの変更を監視・検知するモジュール
Patch（パッチ） Microsoft/Linux/macOSのパッチをスキャン・配信するモジュール	**Impact（インパクト）** ADユーザーやコンピュータのつながりを可視化するモジュール
Threat Response（スレットレスポンス） リアルタイムの検知、過去情報の探索、対応までを行うEDRモジュール	**Engage（エンゲージ）** 通知やアンケート調査・問題の自己解決等、DEX推進モジュール
SBOM（エスボム） ソフトウェアパッケージの可視化を行うAsset/ComplyのAdd-on機能	**Certificate Manager（サーティフィケートマネージャ）** サービスが使用しているTLS詳細、証明書の可視化Add-on機能
Investigate（インベスティゲート） エンドポイントのトラブル調査を行うモジュール	**Automate（オートメイト）** IT管理やセキュリティ対応自動化のための拡張機能
Connect（コネクト） 取得した情報を外部に出力・連携するための標準モジュール	**Trends（トレンズ）** 取得した情報や推移をグラフで表示する標準モジュール
Interact（インタラクト） リアルタイム情報収集・対応を行う標準モジュール	**Tanium Core（タニウムコア）** リアルタイムの可視化と制御、管理機能を提供する基盤

パッケージ販売となります

日立ソリューションズの強み

❶ 大規模導入にも対応できる確かな実績　ー 数万台規模のTanium展開を含む実績を保有 ー

長年にわたりエンドポイントセキュリティ、IT資産管理などのソリューションを提供してきた実績があり、Tanium導入においても業種・業態に応じた適切な構成提案と展開が可能です。特に多拠点・大規模環境での導入における統合支援のノウハウが豊富です。

❷ 上流から運用まで、一貫したトータル支援を提供

ー セキュリティの視点を取り入れた上流設計により、「導入して終わり」にしない確実な定着を実現 ー

Taniumは強力な製品ですが、現場で“使える状態”にするには、明確な運用設計と課題整理が不可欠です。
日立ソリューションズは、「セキュリティコンサルティングによる上流支援」「IT資産管理の専門人材によるコンサルティング」などの支援をします。

❸ Microsoft・ServiceNow とも連携可能

Taniumは単独でも強力ですが、Microsoft や ServiceNow との連携によりIT運用を一気通貫で最適化できます。日立ソリューションズは Tanium 社および Microsoft 社、ServiceNow 社の公式パートナーとして、製品仕様の裏側まで踏まえた実践的・適切な設計提案を提供可能です。

導入にとどまらず、“運用できる”Tanium活用を実現。日立ソリューションズが、業務運用の視点から継続的に支援します。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/tanium/

S25K-09-00 | 2025.09