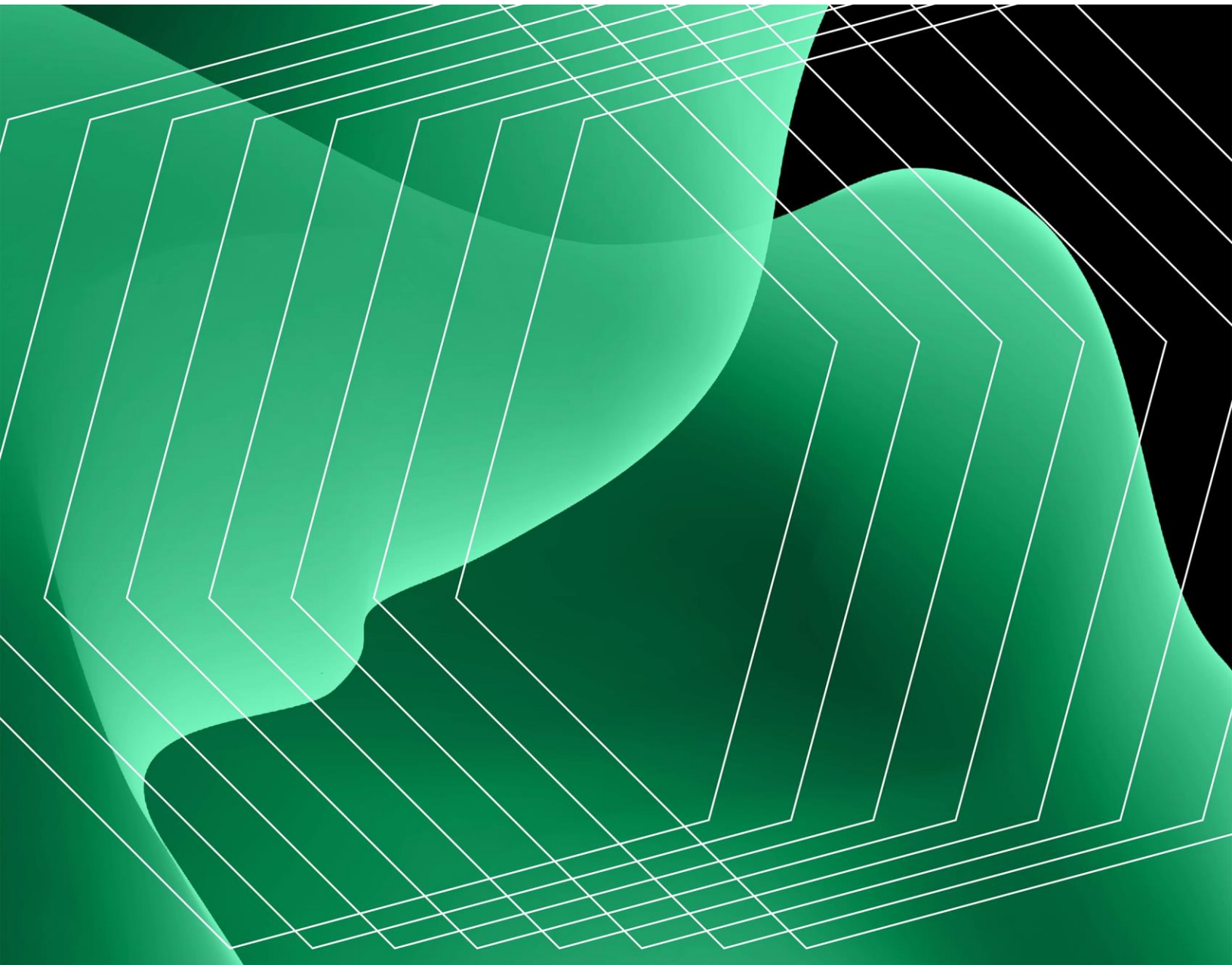
FORRESTER®

Tanium コンバージド・エンドポイント管理 (XEM) の Total Economic Impact™（TEI、総経済効果）

Tanium XEM が可能にするコスト削減とビジネス上の利益

TANIUM 委託による FORRESTER の
TOTAL ECONOMIC IMPACT 調査（2024 年 1 月）



目次

コンサルティングチーム：

Nikoletta Stergiou

Adam Birnberg

Forrester Consulting について

Forrester は、組織のリーダーが主要な成果を実現できるよう、独自の客観的調査に基づくコンサルティングを提供しています。Forrester の経験豊富なコンサルタントは、顧客志向の調査に基づいて、持続的な効果をもたらす独自のエンゲージメントモデルを駆使しながら、リーダーの優先課題に取り組みます。詳細については、forrester.com/consulting をご覧ください。

エグゼクティブサマリー

セキュリティと IT の専門家は、世界に広がる攻撃対象領域への対応に苦戦しています。ハイブリッドワーク、BYOD（個人所有デバイスの業務利用）の増加、クラウドの普及、IoT への継続的な関心により、脆弱性とパッチの管理はかつてないほど難しくなっています。[1] Tanium は、セキュリティのコントロールとパフォーマンスを維持しつつ、エンドポイント環境をリアルタイムに可視化し、コントロールを可能にする XEM プラットフォームのアプローチを通じて、組織がこの課題を克服できるよう支援することを目指しています。

Tanium XEM プラットフォームを使えば、単一のコンソールから IT とセキュリティの問題をリアルタイムに特定し、優先順位をつけて修正できます。IT チームおよびセキュリティチームは、スムーズなワークフローを通じて、環境内のすべてのエンドポイントをコントロールできるようになり、複数のポイントソリューションを排除することによって、効率を向上し、複雑さを軽減できます。さらに、組織はエンドポイントのリスクを長期的に追跡して低減し、未使用のソフトウェア資産を再利用して、違反や罰金の可能性を減らすことができます。

Forrester Consulting は、Tanium の委託により Total Economic Impact™（TEI：総経済効果）調査を実施し、Tanium XEM プラットホームを導入することで企業が実現し得る投資対効果 (ROI) を検証しました。本調査の目的は、Tanium XEM が企業にもたらす可能性のある経済的影響を評価するためのフレームワークを読者に提供することです。[2]

この投資に関連する利益、コスト、リスクをよりよく理解するために、Forrester は Tanium XEM を使用した経験を持つ 5 人の顧客にインタビューしました。この調査では、Forrester はインタビュー参加者の経験を集計し、2,200 から 140,000 のエンドポイントを持つさまざまな組織の結果を組み合わせて、1 つのモデル組織にまとめました。このモデル組織には 40,000 人の従業員と 48,000 のエンドポイントがあるものとします。

主な統計データ

投資対効果 (ROI)
228%

正味現在価値
1,257 万ドル

回収期間
6 か月未満

利益の現在価値 (PV)
1,807 万ドル

インタビュー参加者によると、Tanium XEM を導入する前には、組織ではエンドポイント管理のワークフロー全体にわたり、複数の複雑で分散したソリューションや手作業のプロセスがありましたが、エンドポイント環境を管理するためのこれまでの試みでは、エンドポイント環境やセキュリティの脆弱性に対する可視性が制限されていたため、その成果は限定的でした。こういった制限により、ソフトウェアライセンスやツールに多大なコストがかかり、社員が働き過ぎとなるほか、セキュリティインシデントや侵害の発生、エージェントの肥大化によるデバイスのパフォーマンス低下、統一性のないツール間の時間のかかるデータ照合といった問題につながっていました。

Tanium XEM を導入した後、インタビュー参加者はエンドポイント管理プロセスを自動化し、一元化することができました。この投資の主な結果には、ソフトウェアの再利用によるコスト削減、エンドポイント管理の効率化によるコスト削減、リスクの緩和によるコスト回避、ツールの統合によるコスト削減が含まれます。

主な調査結果

定量化された利益。モデル組織のリスク調整後の 3 年間の現在価値 (PV) で示す定量化された利益には、以下が含まれます。

- **90%のエンドポイントで、未使用、過少使用、または許可されていないソフトウェアの再利用に成功。**モデル組織の 48,000 のエンドポイントでは、20%が再利用可能なソフトウェアを使用しています。Tanium XEM

が、エンドポイントに包括的な可視性と制御を提供することで、これらのライセンスを再利用することができます。Tanium XEM による再利用に起因する 3 年間の削減額は 480 万ドルを超えます。

- **エンドポイント管理の効率が 60%向上。**Tanium XEM によって実現された効率化により、モデル組織はエンドポイント管理チームの効率を向上し、ソフトウェアの導入、パッチ適用、セキュリティ評価などの作業を自動化しています。ユーザーによる Tanium XEM の活用が増えるにつれて使用効率も上がります。結果として、3 年目の終わりまでには 60%の効率化が達成されると推定されます。3 年間のエンドポイント管理の効率化によるコスト削減額は 100 万ドルを超えます。
- **パッチ適用の改善により、ソフトウェアの脆弱性を 97%削減。**モデル組織は Tanium XEM を使用してパッチの適用を自動化し、脆弱性を評価して、リアルタイムのデータを活用することで、セキュリティポスチャーを向上できます。Tanium で OS やサードパーティー製ソフトウェアのパッチ適用を改善することで、ソフトウェアの脆弱性が 97%減少します。3 年間で、リスク軽減に伴うコスト回避額は 790 万ドルを超えます。
- **エンドポイント管理とセキュリティツールの統合を 70%改善。**Tanium XEM のプラットフォームアプローチと包括的なカバレッジにより、資産管理、コンプライアンス管理、インシデント対応、パッチ管理、脅威からの保護、データ検出など、さまざまなユースケースにわたって、エンドポイント管理およびセキュリティツールが統合できます。3 年間で、ツール統合によるコスト削減額は 410 万ドルを超えます。

Taniumのパッチ適用によるソフトウェアの脆弱性の削減

97%

定量化されなかった利益。本調査では定量化は行われなかったものの、モデル組織に価値をもたらすその他の利益は以下のとおりです。

- **M&A の効率化とコスト削減。**Tanium XEM の機能により、組織は買収後のエンドポイント環境を完全に把握し、統合することができます。Tanium XEM は、M&A の IT 統合作業の効率を 70%向上し、不必要なソリューションを特定することで技術的負債を回避します。
- **独自のテクニカルアカウントマネージャー (TAM)。**ソフトウェアの価格に含まれる Tanium 独自のサポートモデルにより、組織はプラットフォームを最適化し、その機能を最大限に活用できます。Tanium の TAM は、組織とベンダーとの懸け橋となり、プラットフォームを成功に導きます。

コスト。リスク調整後の 3 年間の PV コストには、以下が含まれます。

- **ライセンス。**ライセンスは主要モジュールに基づいており、資産管理、コンプライアンス管理、インシデント対応、パッチ管理、脅威からの保護、データ検出などの領域をカバーする追加のソリューションが含まれています。価格はエンドポイント数に基づいています。
- **社内導入とトレーニング。**社内導入のコストとトレーニングコストには、エンドポイント管理チームの 2 人の社員がソリューションを完全に導入するために数か月費やす時間が含まれます。30 人のユーザーがそれぞれトレーニングに 8 時間ずつ使います。クラウド版を導入する組織では、インストール時間が大幅に短縮される可能性があります。
- **社内の継続的管理。**モデル組織では、2 人の社員が Tanium XEM のオンプレミスソリューションの継続的管理に 50%の時間を費やします。一部の組織は Tanium XEM をオンプレミスで導入しましたが、組織によってはクラウド版のソリューションとして導入することもあり得ます。この場合、全体的な継続サポートコストが削減されます。

代表者のインタビューと財務分析の結果、モデル組織は 3 年間で 1,807 万ドルの利益と 550 万ドルのコストを計上し、正味現在価値 (NPV) は 1,257 万ドルで、投資対効果 (ROI) は 228%となります。

投資対効果 (ROI)

228%

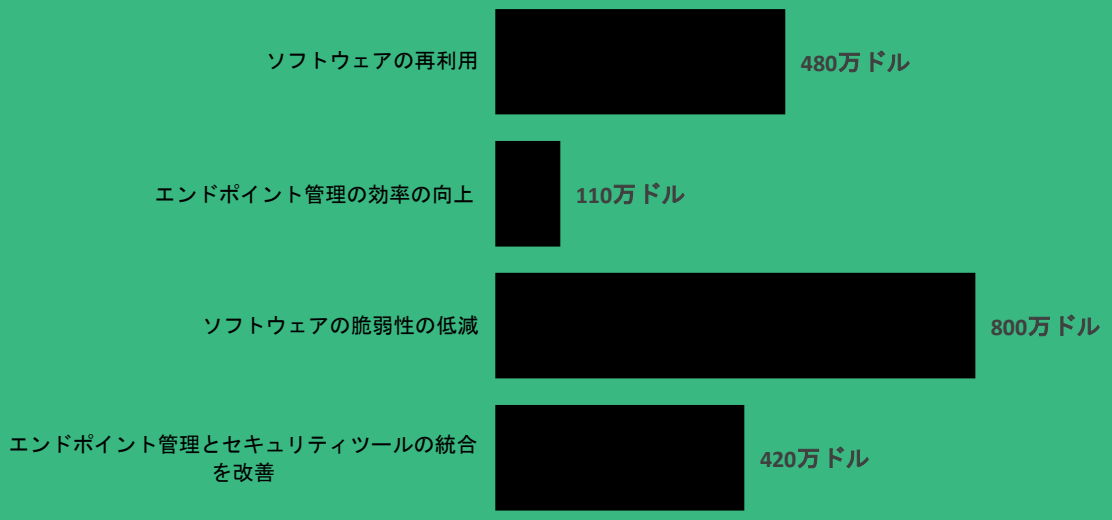
利益の現在価値 (PV)

1,807 万ドル

回収期間

6 か月未満

利益（3年間）



「Tanium XEM は、組織全体を積極的に統制します。さまざまな種類の OS、環境、地域的な要素、政治的な問題が存在するため、組織全体を完全に指揮統制するのは困難です。Tanium XEM は、他のベンダーとは異なる方法で、その問題を解決します」

保険会社のサイバーセキュリティ責任者

TEI のフレームワークと調査手法

インタビューで提供された情報を基に、Forrester は Tanium XEM への投資を検討している組織向けに、Total Economic Impact™（TEI、総経済効果）の枠組みを構築しました。

このフレームワークは、投資決定に影響を及ぼすコスト、利益、柔軟性、リスク要因を特定することを目的としています。Forrester は、Tanium XEM が組織に与える影響を評価するために、多段階のアプローチを取りました。

開示事項

以下の点にご注意ください。

本調査は、Tanium の委託を受け、Forrester Consulting が実施したものです。競合分析として使用されることを意図したものではありません。

Forrester は、他の組織が得る潜在的 ROI に関して、いかなる仮定もしていません。Forrester は、Tanium XEM への投資の妥当性を判断する際には、本調査で提供されているフレームワークおよび Tanium を通じて利用可能な Forrester の計算ツールに読者自身の予測を適用することを強く推奨します。

Tanium は本調査の報告内容を確認した後、Forrester にフィードバックを提供しました。ただし、本調査の内容と結果については Forrester が編集する権限を有し、Forrester の見解と矛盾する変更や調査の意味を曖昧にする変更は承認しません。

Tanium はインタビューを行う顧客名を提供しましたが、インタビューには参加していません。

1. **デューデリジェンス**
   Tanium の利害関係者および Forrester のアナリストにインタビューし、XEM に関連するデータを収集しました。
2. **インタビュー**
   XEM を利用している組織の代表者 5 人にインタビューし、コスト、利益、リスクに関するデータを取得しました。
3. **モデル組織**
   インタビューした組織の特性に基づき、モデル組織を作成しました。
4. **財務モデルのフレームワーク**
   TEI 手法を使用してインタビュー結果を表す財務モデルを構築し、インタビューした組織の課題と懸念に基づいて財務モデルをリスク調整しました。
5. **ケーススタディ**
   TEI の 4 つの基本要素である利益・コスト・柔軟性・リスクに基づいて投資がもたらす影響をモデル化しました。IT 投資に関連する ROI 分析が高度化するなか、Forrester の TEI 手法は購入判断に役立つ総経済効果の全体像を提供します。TEI 手法の詳細については付録 A をご参照ください。

Tanium XEM のカスタマージャーニー

XEM への投資に至った要因

インタビュー				
役職	**業種**	**地域**	**平均年間収益（米ドル）と従業員数**	**エンドポイント数**
企業 IT および情報技術部門責任者	小売	英国に本社を置き、グローバルに事業を展開	68 億ドル 従業員数 45,000 人	17,000
バイスプレジデント	銀行	米国に本社を置き、グローバルに事業を展開	349 億ドル 従業員数 77,000 人	140,000
サイバーセキュリティ責任者	保険	カナダに本社を置き、グローバルに事業を展開	124 億ドル 従業員数 40,000 人	75,000 ～80,000
主任サイバーセキュリティエンジニア	保険	本社米国	350 億ドル 従業員 26,700 人	40,000
情報技術担当バイスプレジデント兼 CISO	ヘルスケア	本社米国	4 億ドル 従業員 5,000 人	2,200

主な課題

インタビュー参加者は、可視性の制限、手作業によるプロセス、セキュリティとコンプライアンスの脆弱性、技術的負債など、Tanium 導入前の環境におけるいくつかの課題を強調しています。複雑で分散しているレガシーソリューションではエンドポイントの可視性が制限されるため、組織はネットワーク全体で一貫したセキュリティ対策を実施し、エンドポイントを効果的に管理することに課題を抱えていました。これにより、脆弱性とセキュリティ侵害の可能性が生じ、トラブル対応が困難になります。インタビュー参加者は、非効率的なレガシーソリューションやプロセスの結果、サイバーハイジーンが悪化し、組織は潜在的なセキュリティインシデントや侵害にさらされていたと述べ、効果的なエンドポイント管理の重要性を強調しました。

またインタビュー参加者は、非効率なレガシーソリューションやプロセスの結果、サイバーハイジーンが悪化し、組織は潜在的なセキュリティインシデントや侵害にさらされていたと述べ、効果的なエンドポイント管理の重要性を強調しま

した。M&A を行う組織では、技術的負債が適応性と保守性を阻害し、統合のコスト増や潜在的な脆弱性につながっていました。

インタビュー参加者の組織に共通して見られた課題には、次のようなものがありました。

- **エンドポイントの可視性の制限。**インタビュー参加者は、複数のソリューションがあるにもかかわらず、エンドポイントの可視性が限られていた点を指摘しました。これは、一貫したセキュリティ対策を行い、組織のネットワーク全体でエンドポイントを効果的に管理するのが難しい状況を招きました。そのため、組織は脆弱性にさらされ、潜在的なセキュリティ侵害に直面し、トラブル対応や問題の解決に苦労していました。ある保険会社の主任サイバーセキュリティエンジニアは、次のように述べています。「以前の環境では、すべてのエンドポイントにおいて EDR (Endpoint Detection and Response) の可視性が不足していました。ほとんどのサーバー担当者は、Tanium XEM が本質的に何をしているのかを理解していませんでしたが、エンドポイントからデータを収集していたため、可視性を向上したことで、セキュリティチームはその情報を利用することができました」
- さらに、ある保険会社のサイバーセキュリティ責任者は、分散したソリューションが大組織に与える影響について次のように説明しました。「多くのグローバル企業がそうであるように、当社も特に大量の流通や、国や地域によって異なる IT のあり方に関する問題に悩まされています」
- **非効率な手作業。**一部のインタビュー参加者は、組織のエンドポイント管理における手作業のプロセスが、エンドポイント管理チームにとって時間のかかるものであったと述べています。自動化された手法がない場合、インタビュー参加者は異なるデバイス間でソフトウェアを確認する継続的な努力が必要となる点を説明しました。あるヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、「エンドポイント管理に、計り知れないほどの時間を費やしてました。10 人のチームが現場で機器をアップデートしても必要なソフトウェアのチェックが徹底できていないので、堂々巡りの作業を延々と行うことになっていました」と述べています。
- **セキュリティとコンプライアンスの脆弱性。**インタビュー参加者は、レガシーソリューションとプロセスにパッチを適用している不適切なサイバーハイジーンについて言及しており、多様な潜在的セキュリティインシデン

トにさらされていることが浮き彫りになりました。エンドポイント管理とリスク削減に関連するため、侵害の回避が最優先事項だと強調しています。セキュリティインシデントや侵害による影響と評判への損害は計り知れないからです。あるヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、「会社がセキュリティ侵害に見舞われましたことが一因となり、採用されました。再発しないように最善を尽くし、会社のセキュリティの現状を確認するためです」と述べています。

- **M&A の技術的負債。**インタビュー参加者は、組織の適応能力、拡張能力、環境の効果的な維持を妨げる原因となっているとして、組織の M&A による技術的負債の影響について話しました。このため、統合にコストがかかり、システムのダウンタイムによって脆弱性が生じる可能性がありました。ある小売企業の IT および情報セキュリティ責任者は、次のように述べています。「Tanium XEM は、技術的負債の継承を回避するのに役立ちました。最近買収した企業では、買収前に導入していたテクノロジーの方が優れていたため、いくつかのテクノロジーは導入する必要がありませんでした」

投資の目標

インタビュー参加者の組織は、次のようなソリューションを必要としていました。

- 組織のセキュリティポスチャーを改善する。
- エンドポイントの可視性を改善する。
- 自動化されたプロセスにより効率性を改善する。
- ソリューションを一元化および統合する。

> 「Taniumの迅速かつ効率的な運用により、セキュリティチーム、エンドポイント管理チーム、ITチーム全体が、これまで使用していたどのソリューションよりも素早く情報を収集し、可視化できるようになりました。これは全体的な効率化にもつながります」
>
> 保険会社の主任サイバーセキュリティエンジニア

モデル組織

Forrester は、インタビューに基づき、TEI フレームワーク、モデル組織、ROI 分析を構築し、財政的に影響する領域を具体的に示しました。モデル組織は、インタビュー参加者が所属する 5 社をモデルとして便宜上 1 つの組織としてまとめたものです。次のセクションでは財務分析の総合結果を表すためにこのモデル組織を使用しています。組織によっては、Tanium XEM をクラウド版のソリューションとして導入したり、メリットやコストに影響を与える可能性のある他の特徴を持つソリューションと一緒に導入する場合があります。このモデル組織には以下の特徴があります。

モデル組織の概要。モデル組織は、米国に本社があり世界的に事業を展開しています。40,000 人の従業員と 48,000 のエンドポイントがあります。平均して、モデル組織は年に 1 回企業買収を実施します。

導入の特徴。モデル組織は、エンドポイント管理とセキュリティのためのソリューションを求めており、エンドポイントに対する可視性、制御、保護を確保したいと考えています。モデル組織は、Tanium XEM をオンプレミスのソリューションとして導入します。この組織は、Tanium Core と Asset、Discover、Benchmark モジュールを含む Core X1 Tier に投資しています。さらに、エンドポイント管理（Provision、Patch、Deploy モジュール）、リスク＆コンプライアンス（Comply、Integrity Monitor、Reveal モジュール）、インシデント対応

（Threat Response および Impact モジュール）を含むソリューションを追加することを選択しています。

主な想定

従業員数40,000人

48,000のエンドポイント

年に1回の企業買収

利益分析

モデル組織に適用する定量化された利益データ

総利益						
参照コード	**利益**	**1 年目**	**2 年目**	**3 年目**	**合計**	**現在価値**
Atr	ソフトウェアの再利用の成功	$1,944,000	$1,944,000	$1,944,000	$5,832,000	$4,834,440
Btr	エンドポイント管理の効率の向上	$224,640	$449,280	$673,920	$1,347,840	$1,081,850
Ctr	ソフトウェアの脆弱性の低減	$3,216,638	$3,216,638	$3,216,638	$9,649,915	$7,999,303
Dtr	エンドポイント管理とセキュリティツールの統合を改善	$1,406,250	$1,687,500	$1,968,750	$5,062,500	$4,152,188
	総利益（リスク調整後）	$6,791,528	$7,297,418	$7,803,308	$21,892,255	$18,067,781

ソフトウェアの再利用の成功

エビデンスとデータ。インタビュー参加者は、Tanium XEM がエンドポイントに対する包括的な可視性と制御が、ソフトウェアの再利用に与えた影響について説明しました。Tanium XEM を使用することで、インタビュー参加者はエンドポイント上の未使用、過少使用、許可されていないソフトウェアを特定および評価し、効果的に再利用することができました。Tanium XEM のエンドポイント管理機能により、チームがリモートでソフトウェアをアンインストールできるようになり、ライセンスを効率的に再利用して、ソフトウェアのコストを削減できるようになったと付け加えています。

- ある保険会社のサイバーセキュリティ責任者は、Tanium XEM の検出機能が他のソリューションよりも詳細な情報を提供する能力について、「当社が Tanium Discover を使用しているのは、他の多くのツールよりも検出する能力がはるかに高いからです。エージェントからの N-map スキャンを利用しており、効率的です。実際に侵害が検出されても、ネットワークに大きな混乱は生じません」と述べています。

- ある小売企業の IT および情報セキュリティ責任者は、監査の準備のためにソフトウェアを削除するユースケースの例を共有しました。「Tanium の Asset モジュールを使用して、環境全体で（ソフトウェアが）インストールされ課金されている端末を把握することができます。Tanium XEM を使用して、そのような端末を検出し、該当するソフトウェアを削除し、そのソフトウェアが環境にはもはや存在しないことを、監査人に証拠として示すことができました」
- ある保険会社の主任サイバーセキュリティエンジニアは、Tanium XEM がハードウェアの再利用に活用される場合もある点を強調しました。「当社では、CMDB [構成管理データベース] でシステムが廃止するように設定されているインスタンスを見つけ、Tanium XEM を使用して、実際には廃止されていないか、誤って廃止されておらず、まだアクティブであることを確認しました」

モデリングと想定。顧客のインタビュー調査をもとに、Forrester はモデル企業に対して以下を想定しました。

- 48,000 のエンドポイント。
- これらのエンドポイントの 20%には、再利用可能なソフトウェアが存在します。
- Tanium XEM を使用すると、再利用可能なソフトウェアがあるエンドポイント上のソフトウェアの 90%が正常に再利用されます。
- 各エンドポイント上のソフトウェア再利用による平均価値は 250 ドルです。

リスク。Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

- エンドポイント数。
- 再利用可能なソフトウェアがあるエンドポイントの割合。
- エンドポイントごとの再利用の価値。

結果。これらのリスクを考慮するため、Forrester はこの利益を 10%下方修正し、3 年間のリスク調整後の正味現在価値（10%の割引を適用）を 483 万ドルとしました。

Tanium XEMで再利用されたエンドポイント

90%

「以前に別の企業でTanium XEMを導入した際、4,000のエンドポイントがありました。3分でCTOにエンドポイントの侵害がいくつあるかを伝え、その後2分で対処できました」

ヘルスケア企業の情報技術担当バイスプレジデント兼CISO

ソフトウェアの再利用の成功					
参照コード	**指標**	**ソース**	**1 年目**	**2 年目**	**3 年目**
A1	エンドポイントデバイス数	モデル組織	48,000	48,000	48,000
A2	再利用可能なソフトウェアがあるエンドポイントの割合	モデル組織	20%	20%	20%
A3	Tanium で再利用に成功したエンドポイントの割合	インタビュー	90%	90%	90%
A4	エンドポイントごとの再利用の平均価値	モデル組織	$250	$250	$250
At	ソフトウェアの再利用の成功	A1*A2*A3*A4	$2,160,000	$2,160,000	$2,160,000
	リスク調整	↓10%			
Atr	ソフトウェアの再利用の成功（リスク調整後）		$1,944,000	$1,944,000	$1,944,000
	3 年間の合計： $5,832,000			**3 年間の現在価値： $4,834,440**	

エンドポイント管理の効率の向上

エビデンスとデータ。インタビュー参加者は、Tanium XEM による自動化とリアルタイムデータの活用により、エンドポイント管理全体の効率が向上したと話しました。Tanium XEM を使用することで、ソフトウェアの導入、パッチ適用、セキュリティアセスメントなどのエンドポイント管理業務に従事する複数の社員の雇用コストを削減できました。

- ある保険会社の主任サイバーセキュリティエンジニアは、Tanium XEM のリアルタイムデータの効率性についてこう述べています。の社員の雇用コストを削減できました。「Tanium は他のソリューションを寄せ付けません。他のポイントソリューションでは、サーバーに”全エンドポイントからこの情報を取得せよ”と指示し、エンドポイントがその情報を収集して、サーバーに送信した後、情報が返ってくるまでに 1〜2 日待たねばならない可能性があります。Tanium を使えば 10 秒で取得できます」
- ヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、Tanium XEM の迅速なパッチ適用機能がエンドポイント管理に必要な労力に影響を与えたとコメントしています。「Tanium があれば、担当者を 10 人採用しなくとも、エンドポイントを管理できます。環境内の状況を把握できるように設定し、適切なバージョンへのアップグレードや、迅速なパッチ適用などができるほか、使ったことがない人にトレーニングを受けてもらい、コードの展開とクリーンアップのエキスパートになってもらうこともできます」
- 保険会社の主任サイバーセキュリティエンジニアは、Tanium が組織のさまざまな部門に与えた影響を共有しました。「サーバーチームやワークステーションチームだけでなく、セキュリティチームや DevOps チームなど複数の部門でスタッフを削減できました。プラットフォーム全体で 20%から 30%の削減です」

モデリングと想定。顧客のインタビュー調査を基に、Forrester はモデル企業に対して以下を想定しました。

- エンドポイント管理担当の社員は 10 人。
- Tanium XEM により、1 年目に 20%、2 年目に 40%、3 年目に 60%の効率が改善されます。

- エンドポイント管理担当の社員の全経費込み平均年間給与は 156,000 ドル。
- Forrester は、ワークライフバランスの改善を考慮して、80%の生産性回復を想定しています。

リスク。Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

- エンドポイント管理担当の社員の人数。
- エンドポイント管理担当の社員の全経費込みの平均年間給与。
- 生産性の回復。

結果。これらのリスクを考慮するため、Forrester はこの利益を 10%下方修正し、3 年間のリスク調整後の正味現在価値（10%の割引を適用）を 108 万ドルとしました。

Taniumによる効率改善（3年目まで）

60%

「比較対象になるのは、おそらく弊社の2倍の規模の組織です。本当に無駄のない強力なチームを維持できています。Taniumのおかげで5人の社員を削減できたと思います」

小売企業の企業ITおよび情報セキュリティ部門責任者

エンドポイント管理の効率の向上					
参照コード	**指標**	**ソース**	**1 年目**	**2 年目**	**3 年目**
B1	エンドポイント管理担当の社員の人数	モデル組織	10	10	10
B2	Tanium による効率改善率	インタビュー	20%	40%	60%
B3	エンドポイント管理担当の社員の全経費込みの平均年間給与。	モデル組織	$156,000	$156,000	$156,000
B4	生産性の回復	モデル組織	80%	80%	80%
Bt	エンドポイント管理の効率の向上	B1*B2*B3*B4	$249,600	$499,200	$748,800
	リスク調整	↓10%			
Btr	エンドポイント管理の効率の向上（リスク調整後）		$224,640	$449,280	$673,920
	3 年間の合計： $1,347,840		**3 年間の現在価値： $1,081,850**		

ソフトウェアの脆弱性の低減

エビデンスとデータ。インタビュー参加者は、Tanium XEM のパッチ管理とソフトウェア展開機能が、パッチ展開の自動化、脆弱性の評価、リアルタイムのデータの提供により、どのようにリスクを軽減し、組織全体のセキュリティポスチャーを向上させたかを力説しました。パッチ管理には、基盤となる OS の脆弱性を修正する作業が含まれます。一方、ソフトウェア展開機能では、サードパーティ製ソフトウェアの修正、インストール、削除を実行します。インタビュー参加者は、Tanium XEM を使用したパッチ適用の効果について説明し、エンドポイントが最新のパッチで保護されていることを確認しました。最終的に、OS およびサードパーティ製ソフトウェアの改善により、潜在的なセキュリティインシデントと侵害のリスクが低減しました。

- 保険会社のサイバーセキュリティ責任者は、Tanium XEM の可視化と迅速な対応がゼロデイの脆弱性の解決に与えた影響について次のように述べています。「ポイントは可視化と対応能力、そのための効率性の向上です。Tanium の原則は”どんな疑問にも、すぐに回答が返って来る。そして回答するだけでなく、どんな問題でも解決する機会を提供する”というものです。それはパッチの適用やゼロデイの脆弱性、セキュリティの実施やコンプライアンスの仕組みなどです」
- ある銀行のバイスプレジデントは、Tanium XEM が数千台のサーバーで不正なソフトウェアアップデートを阻止した事例を紹介しました。「当社

は、あるサービスを 2 万台のサーバーで停止する必要がありました。Tanium XEM のようなツールを使わずに、2 万台のサーバーでサービスを停止するにはどうすれば良いのでしょうか？別のポイントソリューションでも可能ですが、スクリプトを書いて全コンピュータ名を特定する必要があり、しかもその名称は保持できません。しかし、20 分以内にインフラ全体で任意のサービスを停止するというなら、Tanium XEM 以外のツールは見当たりません」

- ヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、Tanium がリスク軽減管理において、どのように重要な役割を果たしたかについて言及しました。「Tanium が当社の機器が不十分であることを特定し、現在アップグレードしています。その作業にはある程度時間がかかります。しかし、ビジネスのリスクを特定することで、アップタイムとダウンタイムをより的確に数量化できるようになり、ネットワークや Wi-Fi などのダウンタイムの原因となるものに、エネルギーとリソースを集中できます。Tanium XEM は、ビジネスのアップタイムと継続性を最大化すべく、エネルギーを正しい場所に集中させる上で有用なツールです」

モデリングと想定。顧客のインタビュー調査を基に、Forrester はモデル企業に対して以下を想定しました。

- 40,000 人の従業員を擁する組織でのセキュリティ侵害の平均コストは、1 回のセキュリティ侵害あたり$2,167,400 であり、年間平均で 3 回のセキュリティ侵害が発生します。[3]
- Tanium XEM の OS およびサードパーティ製ソフトウェアに対するパッチ適用により、ソフトウェアの脆弱性が 97%削減されます。[4]

リスク。Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

- セキュリティ侵害の平均コスト。
- セキュリティ侵害の頻度。
- ソフトウェアの脆弱性、脆弱な認証情報または盗まれた認証情報、および紛失/盗難された資産の悪用によるセキュリティ侵害の割合。

結果。これらのリスクを考慮するため、Forrester はこの利益を 15%下方修正し、3 年間のリスク調整済み総現在価値（10%の割引を適用）を 800 万ドルとしました。

ソフトウェアの脆弱性、脆弱な認証情報または盗まれた認証情報の使用、および紛失/盗難された資産の悪用によるセキュリティ侵害

60%

「リスク軽減に関して言えば、Taniumは環境内に修復が必要なエンドポイントがあるかどうかを特定するのに役立っています」

銀行のバイスプレジデント

ソフトウェアの脆弱性の低減					
参照コード	**指標**	**ソース**	**1 年目**	**2 年目**	**3 年目**
C1	セキュリティ侵害のコスト	Forrester	$2,167,400	$2,167,400	$2,167,400
C2	セキュリティ侵害の頻度（年間）	Forrester	3	3	3
C3	ソフトウェアの脆弱性、脆弱な認証情報または盗まれた認証情報の使用、および紛失/盗難された資産の悪用によるセキュリティ侵害の割合	Forrester	60%	60%	60%
C4	Tanium のパッチ適用によるソフトウェアの脆弱性の削減	インタビュー	97%	97%	97%
Ct	ソフトウェアの脆弱性の低減	C1*C2*C3*C4	$3,784,280	$3,784,280	$3,784,280
	リスク調整	↓15%			
Ctr	ソフトウェアの脆弱性の低減（リスク調整後）		$3,216,638	$3,216,638	$3,216,638
	3 年間の合計：$9,649,915			**3 年間の現在価値：$7,999,303**	

エンドポイント管理とセキュリティツールの統合を改善

エビデンスとデータ。インタビュー参加者は、以前の環境におけるさまざまなセキュリティおよびエンドポイント管理ツールの統合に関連する組織のコスト削減について説明しています。Tanium XEM で、資産管理、コンプライアンス管理、インシデント対応、パッチ管理、脅威からの保護、データ検出を包括的にカバーできるので、一部のツールを完全に排除できました。

- ある銀行のバイスプレジデントは、Tanium XEM で数個のセキュリティツールを置き換えたことを説明しています。「1 対 1 の交換でした。Integrity Monitor については、以前は特定の部分にのみ別のポイントソリューションを使用していましたが、Tanium XEM を使えば全体をカバーできます。脅威対応には別のポイントソリューションを使っていましたが、その機能は Tanium XEM に置き換えられました」
- ヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、エンドポイント管理のポイントソリューションの廃止について力説しています。「アンチウイルス製品はすべて廃止しました。監視中にあるレガシーソリューションが侵害されましたが、幸いにも Tanium XEM を導入していました。そのおかげで、Tanium チームと協力してそのソリューションをすぐに環境から削除するパッケージを作成することができました。しかも 2 日以内にできました」
- ある小売企業の IT および情報セキュリティ責任者は、いくつかのレガシーソリューションの置き換えについて次のように言及しています。「当社では、リモートデスクトップ、パッチ管理、脆弱性の管理に関連するレガシーソリューションを廃止しました」

モデリングと想定。顧客のインタビュー調査を基に、Forrester はモデル企業に対して以下を想定しました。

- Tanium 導入前の環境には 5 つのレガシーソリューションがありました。
- 各レガシーソリューションの平均ライセンス料は、サポートインフラとソリューションのサポートに必要な社員の人件費を含めて 625,000 ドルです。
- Tanium XEM を使用することで、レガシーソリューションの 50%が 1 年目に、60%が 2 年目に、70%が 3 年目に廃止されます。

リスク。Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

- レガシーソリューションの数。
- レガシーソリューションの平均コスト。

結果。これらのリスクを考慮するため、Forrester はこの利益を 10%下方修正し、3 年間のリスク調整済み総現在価値（10%の割引を適用）を 415 万ドルとしました。

Taniumにより3年目までに廃止されるレガシーソリューション

70%

「Taniumの単一エージェントアーキテクチャにより、リソースの利用が軽減されます。特定のタスクに使用するエージェントが減少することで、エンドポイントのリソースのオーバーヘッドが低下します。単一エージェントなので、複数のエージェントが壊れて社内チームが修正する際の複雑さと労力が軽減されます」

銀行のバイスプレジデント

エンドポイント管理とセキュリティツールの統合を改善					
参照コード	**指標**	**ソース**	**1 年目**	**2 年目**	**3 年目**
D1	レガシーソリューションの数	モデル組織	5	5	5
D2	レガシーソリューションあたりの平均ライセンスコスト	モデル組織	$625,000	$625,000	$625,000
D3	レガシーソリューションのうち、Tanium の使用により廃止されたソリューションの割合	インタビュー	50%	60%	70%
Dt	エンドポイント管理とセキュリティツールの統合を改善	D1*D2*D3	$1,562,500	$1,875,000	$2,187,500
	リスク調整	↓10%			
Dtr	エンドポイント管理とセキュリティツールの統合を改善（リスク調整後）		$1,406,250	$1,687,500	$1,968,750
	3 年間の合計：$5,062,500			**3 年間の現在価値：$4,152,188**	

定量化されなかった利益

インタビュー参加者が言及したものの、定量化が不可能であったその他の利益は次のとおりです。

- **M&A の効率化とコスト削減。**インタビュー参加者は、Tanium XEM がどのように M&A の効率化（例 統合）を推進し、技術的負債の管理/削減に役立ったかを説明し、結果的に買収に伴う時間の節約と技術的負債の排除によるコスト削減ができたと述べています。ある小売企業の IT および情報セキュリティ責任者は、「Tanium の導入により、環境を詳細にマッピングし、買収の一環として購入したものを正確に把握できるようになりました。その後、環境を別会社化して、データを移動するか、もし環境に不要な部分があることが判明した場合には、完全に切り離すことができます」とコメントしています。
- **独自のテクニカルアカウントマネージャ (TAM) モデル。**インタビュー参加者は、他のソリューションと比較して Tanium が提供する独自のサポートが、投資からの価値を加速させるのに役立つと述べています。ある保険会社のサイバーセキュリティ責任者は、「当社が実施を試みているすべてについて、Tanium の技術アカウントチームから多くのサポートを受けています。彼らは自社の製品や、いかに顧客を支援できるかについて、非常に熱意を持っています」と述べています。

M&A効率の改善

70%

「当社は使用するサードパーティの数を大幅に減らすことができました。[以前は] 外部委託が多い環境でしたが、Tanium XEMのようなツールのおかげで、特定の脆弱性を監視・検出するために、外部委託しているサードパーティが不要になりました」

小売企業の企業ITおよび情報セキュリティ部門責任者

> 「Tanium XEMのサポート体制は非常に優れています。サポート担当者は、製品を活用して組織の目標を達成したり、カスタム製品の開発を行うための支援をしてくれます。これらは業務の一環として行われ、追加料金を支払う必要はありません。Taniumのツールを使って、当社が可能な限り成功をおさめることを望んでくれています」
>
> 保険会社の主任サイバーセキュリティエンジニア

柔軟性

柔軟性の価値は、顧客によって異なります。顧客が Tanium XEM の追加ユースケースを活用し、ビジネス価値の向上を実現できるシナリオは以下のように複数存在しています。

- **サイバー保険料の減額。**インタビュー参加者は、Tanium XEM が組織全体のサイバーハイジーンにどう影響し、最終的にサイバー保険料に影響を与えたかを指摘しています。あるヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、サイバー保険料の削減の要因の半分ほどは Tanium XEM によるものだと考えています。「当社のサイバー保険料は、様々な要因が重なり、今年度は例外なく 10%減少しました。その根本的な要因は Tanium XEM です。リスクプラットフォーム全体に加えて、ハイジーン、対処方法、迅速な修復の方法のおかげです」
- **シャドーIT の削減。**Forrester Research では、組織内の事業部門チームが認可されていないまたは非管理の IT デバイス、システム、アプリケーション、またはサービスを導入、使用することをシャドーIT と定義していま

す。インタビュー参加者は、デバイス上のソフトウェアを制限するルールを設定できる Tanium XEM の機能により、シャドーIT を削減または排除できると述べています。ヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は次のようにコメントしています。「弊社のシャドーIT はソフトウェアの購入の上に成り立っています。Tanium XEM の導入に伴い、デバイスで使用できるソフトウェアを整理する際にいくつかのルールを設定しました。Tanium XEM は、[潜在的なシャドーIT が生じることを] シャットアウトします」

柔軟性は、特定のプロジェクトの一部として評価される場合にも数値化することができます（詳細は添付資料 A に記載）。

> 「サイバー保険料削減の10%のうち、準備において主要な役割を担っていたTanium XEMの貢献が4%から6%を占めていると思います」
>
> ヘルスケア企業の情報技術担当バイスプレジデント兼CISO

コストの分析

モデル組織に適用される定量的コストデータ

総コスト							
参照コード	**コスト**	**初期**	**1 年目**	**2 年目**	**3 年目**	**合計**	**現在価値**
Etr	ライセンス	$0	$2,016,000	$2,016,000	$2,016,000	$6,048,000	$5,013,494
Ftr	社内導入とトレーニング	$61,050	$0	$0	$0	$61,050	$61,050
Gtr	社内の継続的管理	$0	$171,600	$171,600	$171,600	$514,800	$426,744
	総コスト（リスク調整後）	$61,050	$2,187,600	$2,187,600	$2,187,600	$6,623,850	$5,501,288

ライセンス

エビデンスとデータ。Tanium は、主要モジュールと、機能や性能を追加できるソリューションを含む、幅広いパッケージを提供しています。これらのパッケージは、資産管理、コンプライアンス管理、インシデント対応、パッチ管理、脅威からの保護、データ検出などの領域をカバーしています。各パッケージは、特定の IT やセキュリティの課題に対処し、組織が全体的なサイバーセキュリティおよびエンドポイント管理の能力を向上するよう設計されています。

モデリングと想定。顧客のインタビュー調査をもとに、Forrester はモデル組織に対して以下を想定しました。

- 各エンドポイントのライセンス料は 40 ドル。
- **リスク。**Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。
- エンドポイント数。
- 価格。詳細については Tanium にお問い合わせください。

結果。これらのリスクを考慮するため、Forrester はこのコストを 5%上方修正し、3 年間のリスク調整済み総現在価値（10%の割引を適用）を 501 万ドルとしました。

ライセンス						
参照コード	**指標**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
E1	エンドポイント数	モデル組織		48,000	48,000	48,000
E2	エンドポイントあたりのコスト	モデル組織		$40	$40	$40
Et	ライセンス	E1*E2		$1,920,000	$1,920,000	$1,920,000
	リスク調整	↑5%				
Etr	ライセンス（リスク調整済み）		$0	$2,016,000	$2,016,000	$2,016,000
	3 年間の合計：$6,048,000			**3 年間の現在価値：$5,013,494**		

社内導入とトレーニング。

エビデンスとデータ。インタビュー参加者は、Tanium XEM に関連する社内での導入とトレーニングコストについて話しました。組織の規模によって異なりますが、 インタビュー参加者は、オンプレミスソリューションとして実装されたため、導入に 1 か月から数か月かかり、複数の社員が導入に専念する必要があると推定しています。また、トレーニングは主観的なものであり、Tanium XEM プラットフォームの習得に時間を割くかどうかは、ユーザー次第であると強調しました。

一部の組織は Tanium XEM をオンプレミスで導入しましたが、組織によってはクラウド版のソリューションとして導入する場合もあります。クラウドの場合は、全体的な社内導入、トレーニング、継続的なサポートコストが削減されます。

- 小売企業の IT および情報技術担当の責任者は、初回の導入について、「Tanium XEM の完全な導入には数か月かかりましたが、その一部は新しいツールであればどこでも発生する、ツールに対する信頼感によるものでした」とコメントしています。
- ヘルスケア企業の情報技術担当バイスプレジデント兼 CISO は、Tanium のユーザートレーニングについて次のように語っています。「Tanium のユーザートレーニングのセッションを 3 回ほど実施しました。各セッションは 1 時間から 2 時間程度でした」

モデリングと想定。顧客のインタビュー調査を基に、Forrester はモデル企業に対して以下を想定しました。

- Tanium を導入するエンドポイント管理担当の社員は 2 人。
- 各社員は社内導入に 250 時間を費やす。
- Tanium XEM のユーザーは 30 人。
- 各 Tanium XEM ユーザーには、8 時間の社内トレーニングが必要。
- 1 ユーザーあたりの全経費込みの平均時給は 75 ドル。

リスク。Forrester は、これらの結果がすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

- Tanium をオンプレミスで導入するか、クラウド版のソリューションとして導入するか。クラウド版の方が導入期間が短くなるため、コストを大幅に削減可能。
- Tanium XEM を導入するエンドポイント管理社員の人数。
- Tanium XEM の導入に費やした時間。
- Tanium XEM のユーザー数。
- エンドポイント管理担当の社員の全経費込みの平均時給。

結果。これらのリスクを考慮するため、Forrester はこのコストを 10%上方修正し、リスク調整後の 3 年間の現在価値 (PV) 総額（10%の割引を適用）を 61,000 ドルとしました。

> 「3人ほどで十分なのが、Tanium XEMの素晴らしい点です。Taniumのエンジニア1人、社内のエンジニア1人、さらに障害を解消するリーダーの約3人で導入できます」
>
> ヘルスケア企業の情報技術担当バイスプレジデント兼CISO

社内導入とトレーニング						
参照コード	**指標**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
F1	Tanium を導入するエンドポイント管理社員の人数	モデル組織	2			
F2	導入に費やした時間数	モデル組織	250			
F3	社員あたりの全経費込み平均時給	モデル組織	$75			
F4	小計：社内導入	F1*F2*F3	$37,500			
F5	Tanium XEM のユーザー数	モデル組織	30			
F6	トレーニング時間数	モデル組織	8			
F7	小計：社内トレーニング	F3*F5*F6	$18,000			
Ft	社内導入とトレーニング	F4+F7	$55,500	$0	$0	$0
	リスク調整	↑10%				
Ftr	社内導入およびトレーニング（リスク調整後）		$61,050	$0	$0	$0
	3 年間の合計：$61,050			**3 年間の現在価値：$61,050**		

社内の継続的管理

エビデンスとデータ。インタビュー参加者は、Tanium プラットフォームの継続的管理について、組織内で数人の社員が必要と推定しています。いくつかのケースでは、社員は継続的管理に業務時間の一部を割り当てていますが、より大規模な組織ではより多くの時間を割り当てています。ある情報技術担当バイスプレジデント兼 CISO は、継続的管理の労力が最小限で済むと述べています。「Tanium XEM の素晴らしい点は、管理が必要なソリューションではないということです。管理が必要なソリューションはペットのように育てて養う必要があります。一方で、Tanium XEM は言わば自律的に狩りをする鳥なので、獲物を指定しておけば戻ってきて報告します」

モデリングと想定。顧客のインタビュー調査を基に、Forrester はモデル企業に対して以下を想定しました。

- 2 人のエンドポイント管理担当の社員が、Tanium XEM の運用管理にそれぞれ 50%の時間を費やします。このコストは、Tanium Cloud を使用する組織では低くなります。

- エンドポイント管理担当の社員の全経費込み平均年間給与は 156,000 ドル。

リスク。Forrester は、これらの結果が必ずしもすべての経験を代表するものではなく、次の要因によって結果が異なることを認識しています。

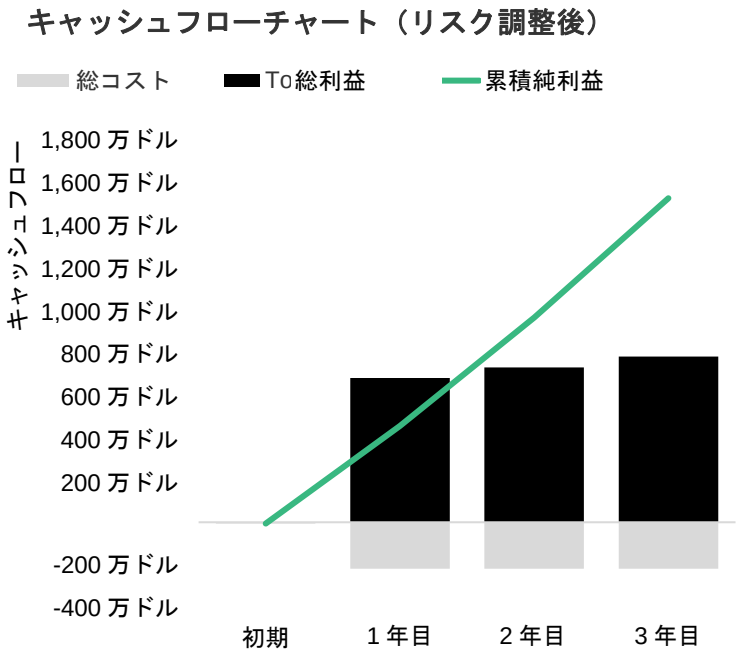
- 継続的管理に費やされた社員の人数。
- エンドポイント管理担当の社員の全経費込み平均年間給与。

結果。これらのリスクを考慮するため、Forrester はこのコストを 10%上方修正し、3 年間のリスク調整済み総現在価値（10%の割引適用）を 427,000 ドルとしました。

社内の継続的管理						
参照コード	**指標**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
G1	社員の人数	モデル組織		2	2	2
G2	Tanium の継続的管理に費やされる時間の割合	モデル組織		50%	50%	50%
G3	社員の全経費込み平均給与（年間）	モデル組織		$156,000	$156,000	$156,000
Gt	社内の継続的管理	G1*G2*G3		$156,000	$156,000	$156,000
	リスク調整	↑10%				
Gtr	社内の継続管理（リスク調整後）		$0	$171,600	$171,600	$171,600
	3 年間の合計：$514,800		**3 年間の現在価値：$426,744**			

財務サマリー

3 年間のリスク調整後の連結指標



利益とコストのセクションで算出される財務上の結果を使用して、複合型組織の投資の ROI、NPV、回収期間を決定することができます。Forrester は、この分析において年 10%の割引率を想定しています。

リスク調整後のこれらの ROI、NPV、回収期間の値は、「利益」と「コスト」の各セクションの未調整結果にリスク調整因子を適用することで決定されます。

キャッシュフロー分析（リスク調整後推定値）

	初期	1 年目	2 年目	3 年目	合計	現在価値
総コスト	($61,050)	($2,187,600)	($2,187,600)	($2,187,600)	($6,623,850)	($5,501,288)
総利益	$0	$6,791,528	$7,297,418	$7,803,308	$21,892,255	$18,067,781
純利益	($61,050)	$4,603,928	$5,109,818	$5,615,708	$15,268,405	$12,566,493
投資対効果 (ROI)						228%
回収期間（月単位）						6 か月未満

付録 A Total Economic Impact

Total Economic Impact（TEI）は Forrester Research が開発した手法で、企業のテクノロジーに関する意思決定プロセスを改善させるとともに、ベンダーが自社の製品やサービスの価値提案を顧客に伝えることを支援するものです。この TEI 手法は、企業が IT の取り組みの有形価値を、その経営陣と他の主要ビジネス利害関係者の両方に対して実証、正当化、実現するのに役立ちます。

Total Economic Impact アプローチ

利益は、この製品によって企業にもたらされた値を表します。TEI 手法では、利益の測定とコストの測定に同じ重みを与えることで、企業全体に与える技術の恩恵を徹底的に評価することが可能になります。

コストは、提案された製品の価値、または利益を実現するために必要なすべての経費を表します。TEI のコスト区分では、ソリューションに関連した運用コストとして、既存環境から追加コストが発生する場合は、そのコストも含みます。

柔軟性は、すでに行った初期投資に加え、将来の追加投資から得られる戦略的な価値を表します。この利益を獲得できるということは、推定可能な PV があることになります。

リスクは、1) 概算が当初の予想に合う可能性、2) 概算が経時的に追跡される可能性に基づいて、利益とコストの概算の不確実性を測定します。TEI ではリスクファクターは「三角分布」に基づいています。

現在価値 (PV)

特定の利率（割引率）を使用した（割引後の）コストと利益の推定値の現在価値。コストと利益の PV は、キャッシュフローの総 NPV に組み入れられます。

正味現在価値 (NPV)

特定の利率（割引率）を使用した（割引後の）将来の正味キャッシュフローの現在価値。プロジェクトの正味現在価値 (NPV) の値が正であれば、その他のプロジェクトの NPV がこれを上回っていない限り、通常は投資すべきであると考えられます。

投資対効果 (ROI)
パーセンテージで表したプロジェクトの期待利益。ROI は、純利益（粗利益からコストを引いた値）をコストで割ることによって求められます。

割引率
金銭の時間価値を考慮するうえで、キャッシュフロー分析において使用される利率。通常、組織は 8%～16% の割引率を使用します。

投資回収期間
投資の損益分岐点。純利益（利益からコストを引いた値）が初期投資額またはコストと等しくなる時点を指します。

初期投資の欄には、「時間 0」、すなわち 1 年目の始まりに発生するコストが記載されます。その他すべてのキャッシュフローは、年末時点の割引率を使用して割引されます。現在価値 (PV) は、それぞれの総コストと利益評価に対して計算されます。サマリー表の NPV の数値は、初期投資と各年の割引されたキャッシュフローの合計です。総利益、総コスト、キャッシュフローの表の合計および現在価値の数値は、四捨五入されている場合があるため、合計と正確に一致しない場合があります。

付録 B 脚注

[1] 出典： “Assess Your Vulnerability Risk Response And Patch Management Maturity,” Forrester Research, Inc.、2023 年 7 月 10 日。

[2] Total Economic Impact は Forrester Research が開発した手法であり、テクノロジーに関する企業の意思決定プロセスを強化し、ベンダーが製品やサービスの価値提案をクライアントに提示するうえで有用となります。この TEI 手法は、企業が IT の取り組みの有形価値を、その経営陣と他の主要ビジネス利害関係者の両方に対して実証、正当化、実現するのに役立ちます。

[3] このコストには、問題解決や報告に関する労働の平均コスト、対応と通知の平均コスト、罰金、損害、コンプライアンスに関するコスト、顧客への補償、営業収益の平均損失、顧客獲得の追加コスト、組織全体でのセキュリティ侵害に関連するエンドユーザーのダウンタイムが含まれます。出典：Forrester Consulting セキュリティ侵害のコスト調査、2020 年第 4 四半期。

[4] 出典：Forrester のセキュリティ調査、2022 年。

FORRESTER®