FORRESTER®

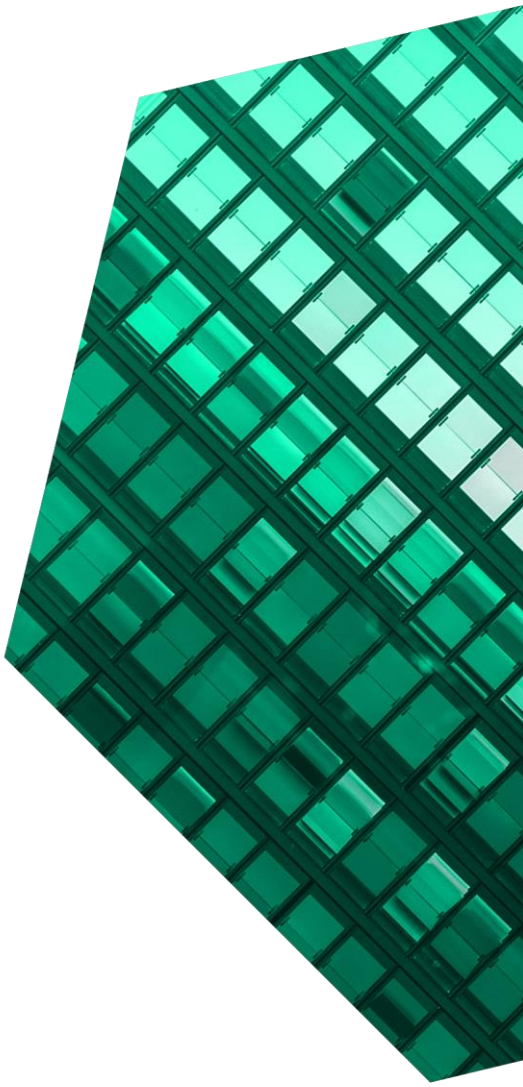
Juniper Connected Security の Total Economic Impact™ （TEI: 総経済効果）

Juniper Networks の Connected Security Strategy で実現するコスト削減と事業利益

2021 年 6 月

目次

コンサルティングチーム： *Casey Sirotnak*
Sanitra Desai



要旨

多くの企業がネットワーク戦略の目標として、ネットワークのコンセプト、製品またはテクノロジーを導入したいと考えていますが、その目標を正しく理解している企業はほとんどないと Forrester では認識しています。明確な戦略を持たない企業では、従業員に自由を与えすぎた結果、抜け道の多い、セキュリティが手薄なネットワークになる危険性があります。最悪の場合、ネットワークがデジタル化の妨げとなり、事業の競争力を低下させる恐れさえあります。[1]

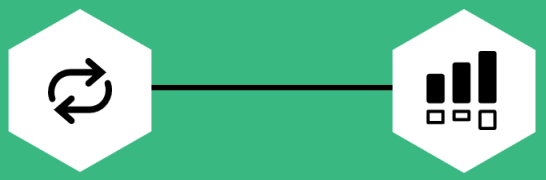
Juniper は、ネットワークの健全性とアクティビティに関する深い洞察を提供しながら、セキュリティの運用（SecOps）効率化を進めるダッシュボードとツールを提供する、フルスタック系セキュリティプロバイダーです。

Forrester Consulting はこの度、Juniper Networks の委託により Total Economic Impact™（TEI: 総経済効果）調査を実施し、Juniper Connected Security の導入で得られる企業の投資収益率 (ROI) を分析しました。本調査の目的は、Juniper Connected Security によって企業にもたらされる潜在的な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。

Forrester は、この投資に伴う利益、コストおよびリスクについて理解を深めるために、Juniper Connected Security の使用経験がある企業 1 社にインタビュー調査を実施しました。Forrester は各企業の使用経験を活用して、3 年間の財務分析を見積りました。

Juniper Connected Security を導入する前は、顧客企業がさまざまなベンダーの老朽化したセキュリティ機器を使用していました。そのため、従来のネットワークセキュリティハードウェアは、複数のベンダーと多種のコードにより管理が複雑だっただけでなく、安定した環境を確保するために必要な透明性にも欠けていました。このような制限により、管理間接費が膨大になり、従来のネットワークにおけるインシデントの危険性は高くなるばかりでした。

主な統計情報



投資利益率 (ROI)
283%

正味現在価値 (NPV)
65.77 万ドル

Juniper Connected Security を導入した後は、顧客企業は Juniper を唯一のベンダーとして利用し、ネットワーク機器のモダナイゼーションと効率化を実現しました。この投資による主な結果は、管理間接費の削減、より安定した信頼性の高いセキュリティ環境の実現です。これによりセキュリティ運用を担当する技術チームおよびエンドユーザー/従業員の信頼を得ることができました。

主な調査結果

定量的なメリット。リスク調整後の現在価値 (PV) の定量的なメリットは、以下のとおりです。

- **セキュリティ運用チームによる管理間接費の 60%を削減。**セキュリティ運用チームには、直感的なツール、ダッシュボード、レポート機能、オーケストレーションにより、ネットワークの診断と問題解決の取り組みの改善という利点がありました。さらに、ネットワークの透明性が高まることで、インシデントが減少して対応パスが明確になり、これまでより安定した環

従業員 1 人あたりのダウンタイム削減時間（年間）

20 時間

境が得られました。こうした効率化により、3 年間で合計 354,500 ドルの節約となりました。

- **システムの稼働率を 10%向上させ、従業員のダウンタイムを年間約 20 時間削減。**Juniper が構築するより安全で信頼性の高いネットワークは、システムのパフォーマンスを向上し、エンドユーザー/従業員のダウンタイムを削減します。従業員のダウンタイムが減ったことで、ビジネスの原動力となるコンテンツの制作と配信に注力でき、結果として 3 年間で合計 439,700 ドルのコスト削減を実現しました。
- **4.5 万ドルの初期費用と 3.5 万ドルの年間保守費用を回避。**老朽化したレガシー機器を廃棄することで、企業はその機器に関連した継続的な保守コストを毎年 3.5 万ドル削減できました。また、Juniper はフルスタックのプロバイダーであるため、ハードウェアの初期 CAPEX コストを統合することで、1 年目で 4.5 万ドルを節約し、3 年間で合計 121,600 ドルの節約を実現しました。

非定量的なメリット。顧客企業は、今回の調査では定量化できなかった利点として、ネットワークの信頼性向上を挙げています。Juniper は、より安定したセキュリティ環境を提供し、IT チームおよび従業員がクリエイティブ業務にもっと集中できるようにしました。その結果、IT チームの業務効率が大きく向上し、ビジネスの変革を支える、最新アーキテクチャの構築に業務時間を割けるようになりました。同様に、従業員もシステムのパフォーマンス低下に伴う技術的な障害に悩まされることがなくなり、さらに変革への取り組みを推進するクリエイティブなコンテンツの制作に専念できるようになりました。

コスト。リスク調整後の現在価値 (PV) には以下のものがあります。

- **ベンダー（Juniper を含む）に支払う初期費用と継続費用、およびトレーニングに費やされる社内リソースの時間的コスト。**Juniper の導入に関連する初期費用には、Juniper に支払われたハードウェア費用とサードパーティのベンダーに支払う導入サービスの費用が含まれます。さらに、Juniper のソリューションの継続的な保守・管理を担当する社内リソースは、ネットワークコンポーネントや利用可能なツールに慣れるまで、約 40 時間ほどを費やす必要がありました。継続的なトレーニングは必要最小限で済み、年間合計 10 時間でした。つまり、Juniper が提供する新機能と拡張機能を中心にしたトレーニングです。

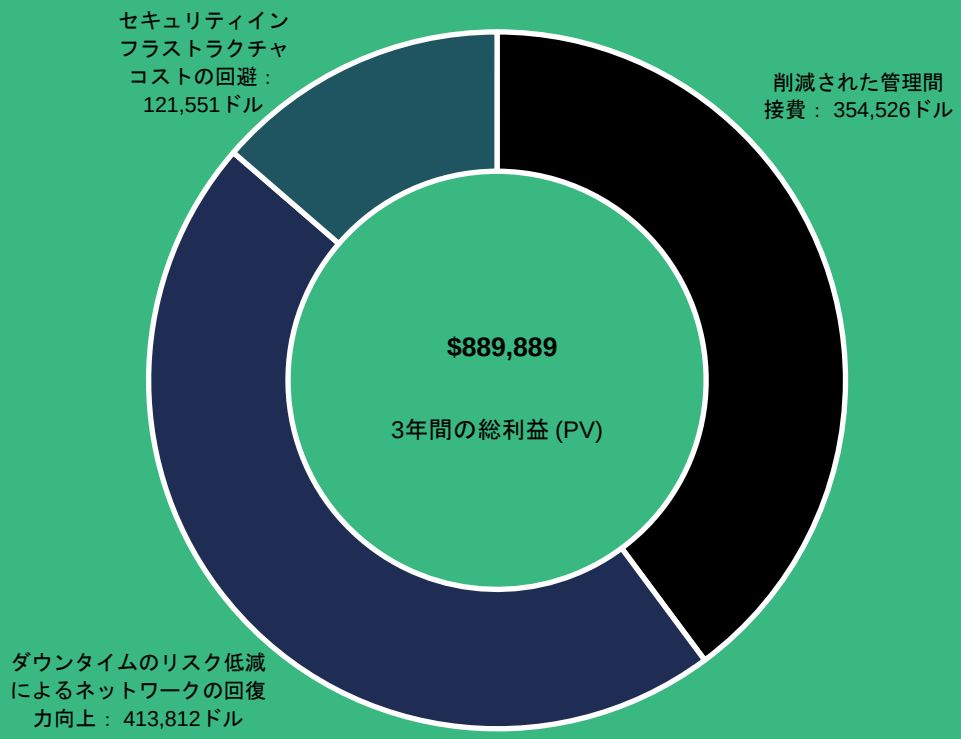
インタビュー調査と財務分析によると、この顧客企業は 3 年間で 232,200 ドルのコストに対して、889,900 ドルの利益を計上し、合計 657,700 ドルの正味現在価値 (NPV) と 283%の投資収益率 (ROI) を達成しました。

投資収益率 (ROI)
283%

利益PV
88.99 万ドル

正味現在価値 (NPV)
65.77 万ドル

利益（3年間）



TEI フレームワークと調査手法

インタビューで得られた情報を基に、Forrester は Juniper Connected Security の導入を検討中の企業のために、Total Economic Impact™ (TEI) フレームワークを構築しました。

このフレームワークの目的は、投資の意思決定に影響するコスト、利益や効果、柔軟性、およびリスク要因を特定することです。Forrester は Juniper Connected Security が組織にもたらす影響を、多段階アプローチを使用して評価しました。

デューデリジェンス（適正評価）
Juniper の利害関係者と Forrester のアナリストにインタビューを行い、Juniper Connected Security に関するデータを収集しました。

顧客企業への聞き取り調査
Juniper Connected Security を使用する企業の意思決定者にインタビューを行い、コスト、収益、リスクに関するデータを取得しました。

財務モデルのフレームワーク
TEI 手法とインタビュー調査対象企業の課題と懸念に基づきリスク調整した財務モデルを使用して、インタビュー調査結果から導かれる典型的な財務モデルを作成しました。

ケーススタディ
TEI の 4 つの基本要素である利益・効果、コスト、柔軟性、およびリスクを採用して投資の影響をモデル化しました。IT 投資に関する ROI 分析がますます高度化する中、Forrester の TEI 手法は、購入決定がもたらす経済的効果の全体像を提供するものです。TEI 手法の詳細については付録 A をご参照ください。

開示事項

読者は以下の点に注意してください。

本調査は Juniper の依頼により、Forrester Consulting が実施しました。本書は競合分析としての利用を意図するものではありません。

Forrester は、他の組織が得られる可能性のある ROI については、一切の予測を行っていません。Juniper Connected Security への投資の妥当性を判断するにあたり、本調査で提供されているフレームワークに読者自身の予測を適用することを強く推奨します。

Juniper はレビューを行った後、Forrester にフィードバックを提供しましたが、Forrester は、調査およびその結果に対する編集上のコントロールを維持し、Forrester の結果と矛盾する、または調査の意味を不明瞭にするような調査の変更は承認していません。

Juniper はインタビューの対象となる顧客の名称は提供しましたが、インタビューには参加していません。

Juniper Connected Security のカスタマージャーニー

Juniper Connected Security 導入を推進した要因

インタビューに応じた組織

Forrester がインタビュー調査を行った Juniper Connected Security の顧客企業は、次の特性を備えています。

- 100 万ドル規模のマルチメディア企業。
- 現在 2 名の FTE のチームが社内ネットワークの運用を担当。
- 技術的な障壁の排除と、コンテンツ制作を推進する 200 人の従業員にとってクリエイティブで協力的な環境の醸成に伴う、ビジネス上の利点がこの導入の推進要因。

「既存のツールがおかしく思えたのは、セキュリティ面で何も語られていない点でした。まさにブラックボックスと言えます。従来のツールでは社内ネットワークで何が起きているのか、何の情報も得られませんでした」
マルチメディア企業の IT 担当ディレクター

「当社では、社内のセキュリティネットワークに対してより最新のアプローチが必要だと考えていました。理想的にはフルスタックで、新規システムに関する学習が最小限に抑えられ、日常のネットワーク運用と変更の追加など、管理間接費を軽減できるアプローチです。古い機器は導入時期がバラバラであったため、機器ごとに異なるコードベースを実行していました」
マルチメディア企業の IT 担当ディレクター

主な課題

Juniper の導入前は、多様なベンダーの老朽化した機器で、セキュリティネットワークを構成していました。

その結果、企業は以下のような共通の課題に苦慮していました。

- **セキュリティ運用チームで管理間接費が増大する。**多様なプロバイダーが提供する老朽化した機器により、セキュリティ運用チームは、ネットワークの診断や問題解決を行うために、多種のコードで作業し、多くの関係者とのやり取りが必要でした。また、古い機器には、ネットワークの透明性を確保するために提供されるツール、ダッシュボード、レポート作成機能など、最新の機器に備わっている機能が欠けていました。その結果、企業ではセキュリティ管理に多くのリソースを割いていました。

- **人材確保のしやすさ、レベル、能力の面においてリソースに制約があった。**セキュリティ管理を担当するリソースは、ネットワーク管理を含む、広範囲にわたる責任を負うハイレベルなリソースでした。この企業は少数精鋭のチームで運営されており、意思決定者はそのような管理タスクに個別のリソースを追加またはリソースに時間を配分することができず、またその意欲もありませんでした。
- **従来のネットワークは不透明であるため、気付かないうちにセキュリティインシデントが発生するリスクが高まっていた。**古い機器では、ネットワークの健全性とアクティビティに対する視認性に制約がありました。このため、運用チームが任意の時点における潜在的なインシデントの脅威レベルと影響の範囲をほとんど把握できず、ネットワークのセキュリティを十分に信頼できない状態になりました。したがって、企業はインシデントへの対応が弱くなり、下流への影響が深刻になると対応しきれなくなっていました。

「何でも屋の器用貧乏な状態で、チームは最小限の編成になっています。従来の機器の老朽化が進み、有効な製品寿命が残っていませんでした。まもなく保守サービスが終了しますが、それよりも過ぎ去った時代のネットワーク機器であることが問題となっています。つまり、古い機器を使用すると、管理面で費用がかさみます。ネットワークに変更が必要なときは、いつも面倒で苦痛でした」
マルチメディア企業の IT 担当ディレクター

ソリューションの要件および投資目標

インタビューした企業はオフィスを移転していました。そのため、意思決定者は今後自社で使用するネットワークセキュリティプロバイダーを検討し、選択する機会がありました。

IT 担当のディレクターはこのように述べています。「オフィス移転を機に、旧オフィスのかなり古い機器をアップグレードし、当社コアネットワークの運用を変更しました。従来の機器の一部は、その時点で 7〜8 年が経過しており、中には 10 年前の機器もありました。変化のきっかけとなったのがオフィスの移転です。また、移転後の新しいオフィスでは、既存のオフィスから独立したネットワークを立ち上げられるようにする必要がありました」

したがって、意思決定者は社内にある従来の機器を廃棄し、以下を実現する新しいソリューションで再出発することにしました。

- フルスタックの機能を提供することで、ネットワークインフラのモダナイゼーションとプロバイダーの効率化を図る。
- 新しいオフィスにダウンタイムなく移転し、従業員への影響を最小限に抑える。
- 直感的なツールとオーケストレーションによる管理間接費の削減で、ネットワークに関するより深い洞察を得て全般的に安定した環境にする。

複数のベンダーを評価した結果、この企業は Juniper Connected Security の導入を決定し、開始しました。インタビュー回答者は次のように述べています。

- インタビューを受けた企業は、新しい移転先オフィスに、Juniper を使用したセキュリティネットワークをゼロから構築できました。
- Juniper はフルスタックのプロバイダーであるため、オフィス全体のネットワークを支えるスタックを一元化し、アクセスポイント数を大幅に削減できました。

- Juniper は、社屋とデータセンターにまたがるデュアルファイアウォール、デュアルファイバースイッチ、デュアルマネジメントを通じて、従来の環境になかったネットワーク全体の冗長性を確保しました。

Juniper を選んだのは、特に管理面と Junos オペレーティングシステムにより、すべてのデバイスで単一のオペレーティングシステムを利用できるという点で、実に説得力のある説明があったからです。その上、Junos の Web インターフェースでは、以前はなかったネットワークに対する視認性が向上し、習得にかかる時間を短縮することもできました。

— マルチメディア企業の IT 担当ディレクター

利益の分析

定量化利益データ

総利益						
参照コード	**メリット**	**1 年目**	**2 年目**	**3 年目**	**合計**	**現在価値 PV**
Atr	管理間接費の削減	$142,560	$142,560	$142,560	$427,680	$354,526
Btr	ダウンタイムのリスク低減によるネットワークの回復力向上	$166,400	$166,400	$166,400	$499,200	$413,812
Ctr	セキュリティインフラストラクチャコストの回避	$76,000	$33,250	$33,250	$142,500	$121,551
	総利益（リスク調整後）	$384,960	$342,210	$342,210	$1,069,380	$889,889

管理間接費の削減

エビデンスとデータ：インタビューに回答した企業では、少数精鋭のリソースで構成されたチームが、ネットワークの管理など、広範囲におよぶ業務を担当していました。従来の環境は、多様なベンダーの老朽化した機器で構成されていました。脆弱で透明性が低いだけでなく、必要に応じて変更や問題解決を行う際には多数のベンダーから難解なコーディングを取得しなければならないほか、ベンダー固有の知識が求められます。Juniper Security Director で管理する Juniper Connected Security は、ダッシュボードや直感的なツール、オーケストレーションを備えた最新のネットワークセキュリティのインフラストラクチャを提供し、管理の透明性と効率性を高めるとともに、より安定した環境を実現しました。その結果、ネットワークの管理間接費を大幅に削減できました。

- 同企業の IT 担当ディレクターは、Juniper がもたらす各種の効率化が、ネットワークの管理に費やす時間の短縮につながったことを次のように説明しています。「以前は、旧オフィスで 1 人の正規社員 (FTE) がネットワークの問題に 50%の時間を費やしていました。私もおそらく 10%～15%の時間を同様に費やしていたと思います。しかし、全体として、2 人のスキルの高い担当者でネットワークの対応をしていました。この 2 人の給与は低いものではありません。Juniper の導入により、ネットワークセキュリティの対応にかかる時間を 30%～35%削減でき、ネットワーク接続の問題を心配する必要がなくなりました」

  同企業はまた、ネットワークとセキュリティの管理を担当する個別のリソースを削減できました。インタビューの回答者はこう言っています。「管理者の間接費が以前より大幅に減りました。以前の環境で必要だった人員数と比較して担当者が 1 人減りましたが、運用がはるかにシンプルになったので、ネットワーク関連で管理が必要なことがすべて管理できています」

- 同社は、Juniper のネットワークで向上した効率性の多くが、直感的に操作できる Juniper Security Director の管理・運用ツールやビューに起因するとしています。インタビューの回答者とそのチームは、Junos ダッシュボードにより、その分野の専門家にならなくとも、無駄のない人員数で対応でき、ネットワークのセキュリティに信頼性がもたらされました。インタビューの回答者は次のように述べています。「以前の環境における管理者の間接費は、とにかく抑制しなければならないものでした。新しいネットワーク環境では『自分たちで探索』できることを望んでいたため、できるだけ早く、

ネットワークとその構成を把握する必要がありました。当初は Junos の Web インターフェースにかなり依存していました。言わば自転車の補助輪のようなものです。ネットワーク管理者を務めたことのない人員でも、Web ブラウザーにアクセスして CLI（コマンドラインインターフェース）以外で状態を確認して可視化できるのは、素晴らしいことです」

- Juniper の導入によりインタビューの回答企業では、統一性のなかった機器を統合できました。新しいエコシステムでは、Juniper のネットワークにより透明性が向上し、複数のコードやベンダーに対応する必要がなくなったことから、迅速な診断が可能になり、問題の解決が容易になりました。透明性の向上は、対策が必要なインシデントまたはアラームの種類が明確化することを意味します。インタビューの回答者は次のように述べています。「ネットワークの接続に問題があり、以前使用していたシステムの管理は多種のデバイスや複数世代のデバイスにまたがって断片化していたため、侵害の原因を発見するのは非常に困難でした。しかも、その時検出できたとしても、修正はその先です。今では Juniper Connected Security のおかげで、誤検出を見つけたり、必ずしも対応の必要のない不審な行動を特定したりすることが容易になりました」
- Juniper のネットワークと関連ツールにより、全体的に安定性が向上したセキュリティ環境が構築され、必要となる管理業務が減少しました。インタビューの回答者はこう述べています。「管理間接費が少ない理由のひとつは、社内のニーズが十分満たされる水準に達しているからです。社内のネットワークの状況で最適化できる部分は、既に最適化されています。VLAN（仮想ローカルエリアネットワーク）とサイト間の接続のデザインも見直しました。その後、ネットワークのセキュリティは盤石です」

モデリングと前提条件：管理に伴う間接費の削減額を算定するために、Forrester は以下を前提としました。

- 従来の環境では、取り組みの程度に差がある、3 人の FTE が管理に必要。Juniper 環境に移行した後は、1 人の FTE を配置換えし、残り 2 人の FTE が費やす時間を短縮できました。
- この企業は、SecOps FTE の業務の 60%効率化を 1 年目に達成。この効率性は、セキュリティネットワークの安定性により、導入後 3 年間は一貫的に維持されました。
- SecOps リソースの平均年収は 110,000 ドル。
- ツール、ネットワークの透明性、安定性の効率向上により得られた時間の 80%は、付加価値の高い業務に再配分されました。

リスク：管理間接費の削減は、以下の要因により変動する可能性があります。

- 従来のネットワーク環境の状態（使用年数、ベンダーなど）およびその管理を担当する SecOps リソースの人数。
- ネットワークの管理に従事するために必要なリソースの水準と、それに関連する年間給与。
- 地域により異なる給与。

「導入したソリューションの主な利点は、ツールと、それがネットワークにもたらす可視性です。これにより、管理者の立場から、ネットワーク上で誰が何をしているかを理解し、複数の環境にわたるポリシーを適用できるようになります」
マルチメディア企業の IT 担当ディレクター

- 回収できた SecOps チームの生産性のうち、より付加価値の高い業務に割り当てた割合（並行して実行されている技術的およびビジネスの取り組みに依存）。

これらのリスクを加味し、Forrester はこの利益を 10%下方調整し、リスク調整後の 3 年間の総現在価値 (PV) を 354,526 ドルとしました。

管理間接費の削減

参照コード	指標	ソース	1 年目	2 年目	3 年目
A1	Juniper Connected Security 導入前にネットワーク管理に従事していた SecOps FTE の人数	インタビュー	3	3	3
A2	Juniper Connected Security の導入で削減された管理間接費	インタビュー	60%	60%	60%
A3	SecOps FTE の平均年間給与	前提条件	$110,000	$110,000	$110,000
A4	生産性の回収率	前提条件	80%	80%	80%
At	削減された管理間接費	A1*A2*A3*A4	$158,400	$158,400	$158,400
	リスク調整	↓10%			
Atr	削減された管理間接費（リスク調整後）		$142,560	$142,560	$142,560
	3 年間の合計：427,680 ドル			**3 年間の現在価値：354,526 ドル**	

ダウンタイムのリスク低減によるネットワークの回復力向上

エビデンスとデータ：インタビューの回答企業では、以前インシデントや障害が発生すると従業員にダウンタイムという形で影響がありました。その影響の大きさは、従業員のネットワーク基盤に対する不信感を招き、本来行うべき共同のクリエイティブ作業の妨げとなっていました。Juniper の導入後、この企業では従業員のダウンタイムが大幅に減少し、技術的に中断することなく、お客様向けメディアコンテンツの配信に集中できるようになりました。

- ネットワークのセキュリティを支えていた従来の機器は「ブラックボックス」だったので、その操作と管理は困難でした。そのため、深刻な事態が発生するリスクが高まっていました。Juniper を導入してからは、透明性を高めてネットワークの安定性を向上させることで、致命的なイベントが発生する可能性を抑制できました。インタビューの回答者はこう言っています。「以前の機器でセキュリティイベントが発生したらどうなるか考えた場合、よほど壊滅的な影響が表れないと、発生時に気がつくことはなかったでしょう。つまり、ネットワークのダウンタイムを引き起こす、重大なセキュリティ侵害となったかも知れません。ですから、以前の環境では致命的なエラーが発生する可能性が非常に高かったのです。Juniper では主にシステムを可視化できるという理由から、こうしたセキュリティイベントを未然に防げるという安心感があります」
- 以前の環境における問題は主にダウンタイムで、従業員に影響を及ぼすネットワークの停止として現れ、環境が攻撃されやすい状態になっていました。インタビューの回答者はこう述べています。「以前の環境では、スイッチの接続に問題がありました。また、ポートインターフェースの問題や接続 VLAN の問題、更新、

アップグレード、それらに関連するダウンタイムも多くありました。最新バージョンをすべて管理できていなかったと思います。したがって、更新スケジュールはローリング方式でした。休日や業務時間外に更新を行うという最善の努力にもかかわらず、従業員のダウンタイムと環境へのリスクにつながる、ローリングによるネットワークの停止が発生する可能性がありました」

- Juniper では、ネットワークのパフォーマンスが大きく向上し、結果として従業員への影響が抑えられます。インタビューの回答者はこう言います。「Juniper の機器を使用すると、ネットワークの中断や侵害イベントが生じることはありません。実際のところ、過去 3 年間の達成率はこれまでで最高です。ネットワークを含む全担当業務で、99%近くを達成するのはかなりに容易になっています。以前は 80%強〜90%弱でした。約 10%向上しています」
- 従業員は、信頼度の向上という点で、ネットワークの回復力向上の恩恵を受けました。技術的な中断が生じないため、従業員は消費者向けコンテンツの配信に集中できます。インタビューの回答者はその影響について「背後に安定した堅牢な基盤があると感じられることから、混沌と中断が発生して苦情を招く環境とは大きな違いがある」と言っています。

モデリングと前提条件：ダウンタイムのリスク減少によるネットワークの回復力向上から数値を引き出すため、Forrester は以下を前提としました。

- この企業では、コンテンツ制作に携わる 200 人の従業員が、ダウンタイムの影響を受ける可能性がある。
- 従来の環境におけるシステムの可用性は 89%。つまり 11%の時間（年間 229 時間）は、従業員に影響を及ぼす致命的なダウンタイムイベントに弱いと言えます。
- Juniper の導入により、企業ではシステムのパフォーマンスが 10%向上し、1 年間の致命的なダウンタイムのリスクが減少する。
- すべてのダウンタイムイベントが従業員に影響を及ぼすわけではない。Forrester は、これらのイベントの 10%が、従業員のダウンタイムにつながる致命的なものと想定しています。
- ユーザー（従業員）1 人あたりのダウンタイムコストは 50 ドル。これは従業員の時給（システムのダウン時には従業員の業務遂行が制限されるため）と、ビジネスへの影響の両方を考慮に入れた金額です。システムのダウンタイムは従業員が消費者にコンテンツを配信する能力にも影響を与えるので、オポチュニティコストも減少します。

リスク。ダウンタイムのリスク低減によるネットワークの回復力向上は、以下の要因により変動する可能性があります。

- 従業員数に基づく企業の規模。
- 従来の環境で得られたシステムの可用性レベルと、Juniper による改善のレベル。
- 従業員に影響を及ぼす潜在的なダウンタイムイベントの割合。
- 従業員の平均時給（業種、地域、職種、職階により異なる）。また、従業員が従事する業務の性質が、ダウンタイム中に失われるオポチュニティコストに影響を与えます。顧客と多く接する業務であれば、オポチュニティコストへの影響も大きくなります。

これらのリスクを加味し、Forrester はこの利益を 20%下方調整し、リスク調整後の 3 年間の PV 総額を 413,812 ドルとしました。

ダウンタイムのリスク低減によるネットワークの回復力向上					
参照コード	**指標**	**ソース**	**1 年目**	**2 年目**	**3 年目**
B1	ユーザー/従業員数	インタビュー	200	200	200
B2	Juniper 導入前のネットワークインシデントに起因する年間ダウンタイム時間	前提条件	229	229	229
B3	Juniper 導入後のネットワークインシデントに起因する年間ダウンタイム時間	前提条件	21	21	21
B4	従業員に実際に影響があるネットワークインシデントの割合	前提条件	10%	10%	10%
B5	ユーザー1 人あたりのダウンタイムコスト	前提条件	$50	$50	$50
Bt	ダウンタイムのリスク低減によるネットワークの回復力向上	B1*((B2-B3)*B4)*B5	$208,000	$208,000	$208,000
	リスク調整	↓20%			
Btr	ダウンタイムのリスク低減によるネットワークの回復力向上（リスク調整後）		$166,400	$166,400	$166,400
3 年間の合計：499,200 ドル			**3 年間の現在価値：413,812 ドル**		

セキュリティインフラストラクチャコストの回避

エビデンスとデータ：インタビューに回答した企業では、意思決定者が従来の機器を廃棄し、セキュリティインフラストラクチャを新しい単一のベンダーに移行するという選択肢をとった後、コストを削減できました。従来の機器は老朽化していたので、毎年多額の保守費用が必要でした。セキュリティインフラストラクチャを Juniper へと移行したことで、このコストを回避できました。また、Juniper はフルスタックのプロバイダーであるため、ハードウェアの初期費用を抑制しやすく、最初の設備投資コストを抑えることができました。

- 同企業の IT 担当ディレクターは、コスト回避について、次のように詳述しています。「コスト削減をとってみると、これには購入コストだけでなく、サポート契約とその交渉による総所有コストの要因も含まれます。購入の観点では、ハードウェアと機器の設備投資の削減となります。フルスタックのプロバイダーである Juniper は、パッケージとして全部をまとめた最高のオファーを提示してくれました。価格面で大きな武器となりました」
- インタビューの回答者は、Juniper の設備購入および統合セットアップと設定にかかる初期費用の削減額を、4 万ドル～4.5 万ドルと見積もっています。また、インタビューを受けたある企業は、従来の機器に関連した保守コストを年間約 3.5 万ドル削減したと回答しています。

初期の設備投資コストの削減額

4.5 万ドル

継続的な保守コストの削減額

3.5 万ドル（年間）

モデリングと前提条件：セキュリティインフラストラクチャコストの回避額を計算するため、Forrester は以下を想定しました。

- Juniper の初期費用の設備投資コストは、代替ソリューションより 4.5 万ドル低くなっています。
- 以前のソリューションで必要だった年間 3.5 万ドルの保守コストは、Juniper ソリューションで削減されています。

リスク：セキュリティインフラストラクチャのコスト節約額は以下の要因で変動する可能性があります。

- 以前のソリューションの年間契約における保守要件。
- 検討代替ソリューション（設備投資の初期費用に影響するため）。

これらのリスクを加味し、Forrester はこの利益を 5%下方修正し、リスク調整後の 3 年間の現在価値 (PV) 総額を 121,600 ドルとしました。

セキュリティインフラストラクチャコストの回避

参照コード	指標	ソース	1 年目	2 年目	3 年目
C1	Juniper Connected Security により削減された CAPEX 設備投資コスト	インタビュー	$45,000	$0	$0
C2	回避できたレガシーソリューションの保守コスト	インタビュー	$35,000	$35,000	$35,000
Ct	セキュリティインフラストラクチャコストの回避	C1+C2	$80,000	$35,000	$35,000
	リスク調整	↓5%			
Ctr	セキュリティインフラストラクチャコストの回避（リスク調整後）		$76,000	$33,250	$33,250
	3 年間の合計：142,500 ドル			**3 年間の現在価値：121,551 ドル**	

非定量的メリット

定量化は不可能ながらもほかに顧客企業で認められた利益は以下のとおりです。

- **IT チームは、より複雑な最新アーキテクチャを試行できます。**Juniper Connected Security ソリューションは、ネットワークとセキュリティの管理に伴う間接費を大幅に削減するとともに、環境の安定性を向上させます。その結果、IT チームが革新的な取り組みに注力できる時間が増え、安心してハイブリッドクラウドのような複雑なアーキテクチャを環境に導入できます。
- **従業員はコンテンツ制作とコラボレーションに集中できます。**ネットワークの安定性が高まると、テクノロジーは日常的に従業員を阻害するものではなくなりました。そのため、ビジネスの成功に不可欠な、協力的でクリエイティブな制作環境の維持に注力できます。

「以前のセキュリティ環境では、多様なレベルの機器が微妙なバランスで配置されていました。Juniper には、セキュリティツールが組み込まれたシングルスタック構成の強力な基盤があります。Juniper のネットワーク設定により、セキュリティ機器やツールの各種機能をより深く理解できたことで、安心して新しい別の技術分野にも進出することができました」
マルチメディア企業の IT 担当ディレクター

「以前実行していたシステムに対して信頼を失っていたユーザーがいます。そのようなシステムを瀕死の状態から復活させるのは、技術的なタスクというより、ユーザーに対する純粋なマーケティング／PR の課題となります。信頼の要因であり、以前と現在の違いでもあります。ユニコーンゾーンと言うべき最善の結果です」
マルチメディア企業の IT 担当ディレクター

柔軟性

柔軟性の価値は顧客によってそれぞれ異なります。顧客企業が Juniper Connected Security ソリューションを導入するシナリオは複数存在し、追加の用途やビジネスチャンスが後から見つかる場合もあります。

そのような使用例では、より優れたビジネス変革の実現もあります。Juniper Connected Security の導入により、IT チームはハイブリッドクラウドなど、より複雑で柔軟な最新アーキテクチャを試行しますが、その際に従業員が技術的な問題による影響を受けることはありません。そのため、企業は Juniper が提供する技術的な基盤により、支障をきたすことなく、ビジネス変革の取り組みに注力できます。したがって、意思決定者は、新たに獲得した技術面での自由度と柔軟性を原動力に、さらなるイノベーションを期待しています。

柔軟性は、特定のプロジェクトの一環として評価することで定量化できます（付録 A に詳細を記載）。

コストの分析

定量化されたコストのデータ

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**
Dtr	初期費用とベンダーに支払った継続費用	$0	$218,500	$17,250	$17,250	$253,000	$225,853
Etr	オンボーディングとトレーニングに費やした社内リソースの時間	$0	$4,865	$1,216	$1,216	$7,298	$6,342
	総コスト（リスク調整後）	$0	$223,365	$18,466	$18,466	$260,298	$232,195

初期費用とベンダーに支払った継続費用

エビデンスとデータ：インタビューを受けた顧客企業は、導入に伴い、Juniper Connected Security のハードウェアとソフトウェアの初期費用を Juniper に支払っています。さらに、Juniper と継続的な保守とサポートに関する保守契約も結びました。

モデリングと前提条件：初期費用とベンダーに支払う継続費用を計算するため、Forrester は以下を想定しました。

- 初期費用には、Juniper に直接支払うハードウェアとソフトウェアの費用のほか、必要な統合などの導入サービスに対して、Juniper を通じてサードパーティのベンダーに支払われる導入費用が含まれます。企業には、1 年目にハードウェア、ソフトウェア、導入のコストが発生しました。
- 導入には 1 週の週末を費やし、費用は合計 17.5 万ドルです。
- 継続的なコストは、Juniper とインタビューを受けた顧客企業との間の、保守・サポート契約を示すものです。年間で合計 1.5 万ドルとなります。

リスク：初期費用とベンダーに支払う継続費用は、以下の要因により変動する可能性があります。

- 関連するセキュリティネットワークの運用に必要なハードウェアとソフトウェアに基づく Juniper 導入の規模と範囲。
- 導入スケジュールに関する期待。
- 初期費用でカバーされる年数と、カバーされない継続的な保守の金額に関して Juniper と顧客企業との間で結ばれた保守契約。

これらのリスクを加味し、Forrester はこのコストを 15%上方修正し、3 年間のリスク調整後の総現在価値を 225,853 ドルとしました。

初期費用とベンダーに支払った継続費用						
参照コード	**指標**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
D1	Juniper とサードパーティの導入パートナーに支払われるハードウェアとプロジェクトの初期費用	インタビュー	$0	$175,000	$0	$0
D2	Juniper に支払った継続費用	インタビュー	$0	$15,000	$15,000	$15,000
Dt	初期費用とベンダーに支払った継続費用	D1+D2	$0	$190,000	$15,000	$15,000
	リスク調整	↑15%				
Dtr	初期費用とベンダーに支払った継続費用（リスク調整後）		$0	$218,500	$17,250	$17,250
	3 年間の合計：253,000 ドル			**3 年間の現在価値：225,853 ドル**		

オンボーディングとトレーニングに費やした社内リソースの時間

エビデンスとデータ：インタビューを受けた顧客企業は、Juniper およびその他のベンダーに費用を支払うだけでなく、Juniper Connected Security ソリューションに関連するオンボーディングとトレーニングにもリソースの時間を割り当てています。

モデリングと前提条件：オンボーディングとトレーニングに費やされる社内リソースの時間を計算するため、Forrester は以下を前提としました。

- この企業では、2 人のセキュリティ運用担当 FTE が Juniper Connected Security ソリューションの継続的な保守・管理に専念する、少数精鋭チームを編成しています。
- SecOps FTE は、Juniper のシステムを完全に使いこなし、ツールの効果的な操作方法を習得するためのトレーニングに、まず 40 時間を費やしました。
- 翌年以降は、新たに追加された機能などを対象とした簡単なトレーニングが必要となり、年間で合計 10 時間を費やすことになります。

リスク：オンボーディングとトレーニングに費やした社内リソースの時間は、以下の要因で変動する可能性があります。

- SecOps FTE の人数と Juniper Connected Security ソリューションに費やす時間。
- セキュリティネットワークのハードウェアおよびソフトウェアの習熟度。
- Juniper 導入の規模と範囲。

これらのリスクを加味し、Forrester はこのコストを 15%上方修正し、3 年間のリスク調整後の総現在価値を 6,342 ドルとしました。

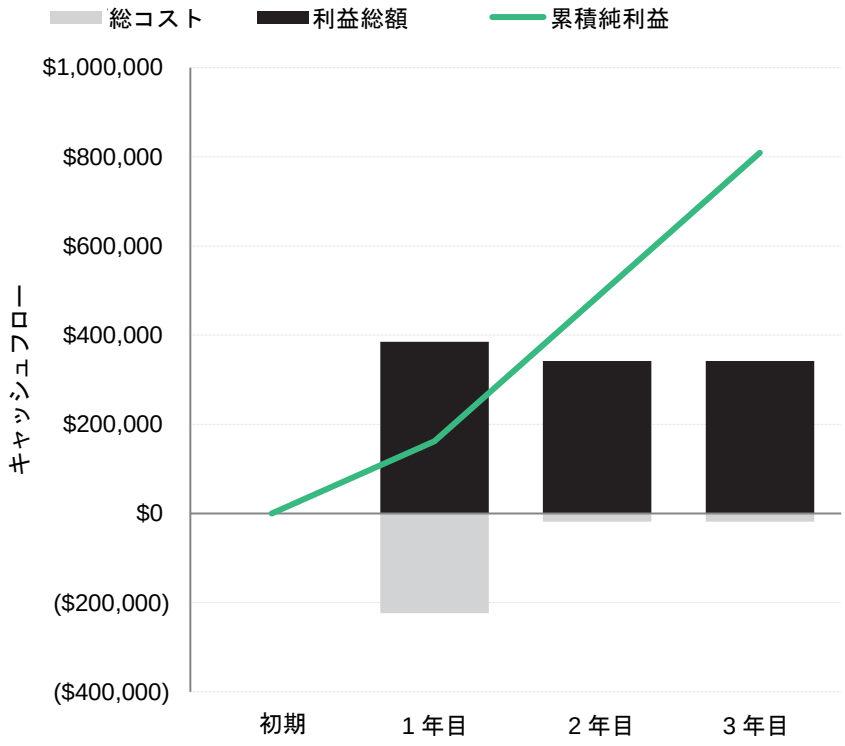
オンボーディングとトレーニングに費やした社内リソースの時間

参照コード	指標	ソース	初期	1 年目	2 年目	3 年目
E1	Juniper の継続的な保守と管理を担当する FTE の人数	インタビュー	0	2	2	2
E2	オンボーディングとトレーニングに必要な時間（単位：時間）	インタビュー	0	40	10	10
E3	SecOps FTE の平均時間単価	前提条件	$0	$53	$53	$53
Et	オンボーディングとトレーニングに費やした社内リソースの時間	E1*E2*E3	$0	$4,231	$1,058	$1,058
	リスク調整	↑15%				
Etr	オンボーディングとトレーニングに費やした社内リソースの時間（リスク調整後）		$0	$4,865	$1,216	$1,216
	3 年間の合計：7,298 ドル			**3 年間の現在価値：6,342 ドル**		

財務状況の概要

リスク調整後の 3 年連結評価

キャッシュフローチャート（リスク調整後）



「利益」と「コスト」のセクションで計算された経済的影響を使用して、このモデル組織の投資に対する ROI および NPV を決定できます。Forrester は、この分析に対し年 10%の割引率を想定しています。

これらのリスク調整後の **ROI** および **NPV** 値は、「利益」と「コスト」の各々の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（リスク調整後の推定値）

	初期	1 年目	2 年目	3 年目	合計	現在価値
総コスト	$0	($223,365)	($18,466)	($18,466)	($260,298)	($232,195)
利益総額	$0	$384,960	$342,210	$342,210	$1,069,380	$889,889
純利益	$0	$161,595	$323,744	$323,744	$809,082	$657,694
投資収益率 (ROI)						283%

付録 A: Total Economic Impact（TEI: 総経済効果）

Total Economic Impact（TEI：総経済効果）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伝えるのを支援します。TEI 手法を使用することで、企業は経営陣やその他の重要なビジネス関係者に対して、IT イニシアティブの具体的な価値を提示しながら妥当性を証明し、価値を実現させていけます。

TEI アプローチ

利益とは、製品がビジネスにもたらす価値のことです。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、テクノロジーが組織全体にもたらす効果を完全に検証することが可能です。

コストでは、提案されている製品の価値または利益をもたらすために必要なすべての支出が考慮されます。TEI でのコスト区分では、ソリューションに関連して継続的に発生するコストに対する既存環境上の増分コストを収集します。

柔軟性とは、既に行われた初期投資に加えて将来的に追加投資を行うことで得られる戦略的価値のことです。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。

リスクとは、利益とコストの見積りの不確実性を測定したもので、1) 見積りが初期の予測と一致する可能性と、2) 見積りが予測どおりに推移する可能性が考慮されています。TEI では、リスク因子は「三角分布」に基づいています。

初期投資の列には、「時間 0」、つまり 1 年目の開始時点で発生したコストが含まれます。これらのコストには割引率は適用されません。その他すべてのキャッシュフローは、年度末に割引率を使用して割引されます。PV は、総コストと総利益の各推定値に対して計算されます。概要の表の NPV の値は、初期投資と各年における割引後のキャッシュフローの合計になります。総利益、総コスト、キャッシュ フローの各表における合計と PV の値については、端数処理が行われている場合があるため、総和が正確に一致しないことがあります。

現在価値 (PV)

特定の利率（割引率）を使用した場合の（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）を使用した場合の（割引後の）将来の正味キャッシュフローの現在価値。通常、プロジェクトの NPV の値が正であれば、他のプロジェクトの NPV がそれより高くない限り、投資すべきであると考えられます。

投資利益率 (ROI)

パーセンテージで表したプロジェクトの予想利益。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

キャッシュフロー分析において現金の時間的価値を反映させるために適用する利率。通常、企業は 8% ～ 16% の割引率を適用します。

回収期間

投資金額が回収される損益分岐点。これは、純利益（粗利益からコストを引いたもの）が初期投資またはコストに見合うタイミングです。

付録 B: 注釈

[1] 出典：「Now Tech: Virtual Network Infrastructure Switching Fabric, Q2 2020」Forrester Research, Inc. 2020 年 4 月 22 日


FORRESTER®