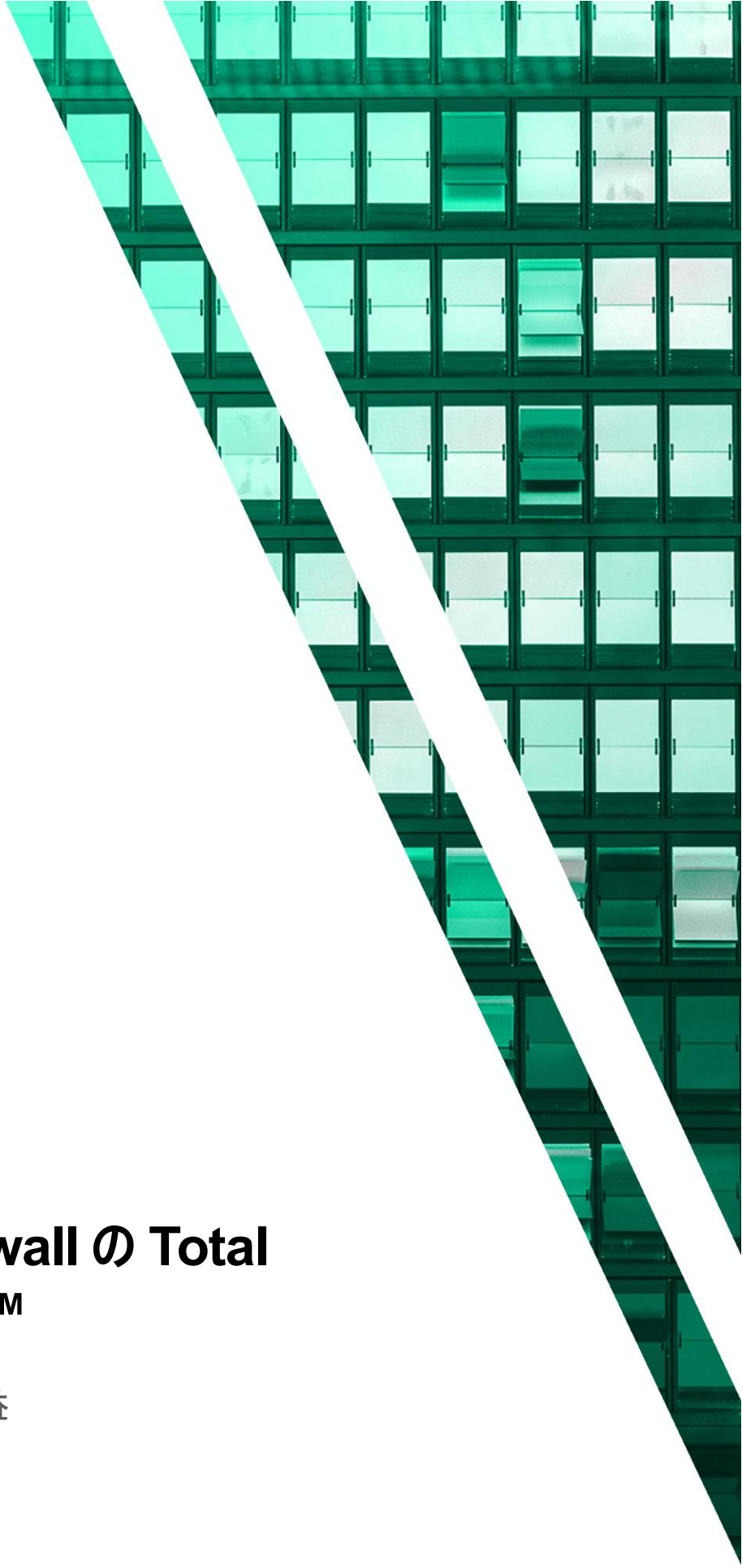
FORRESTER®



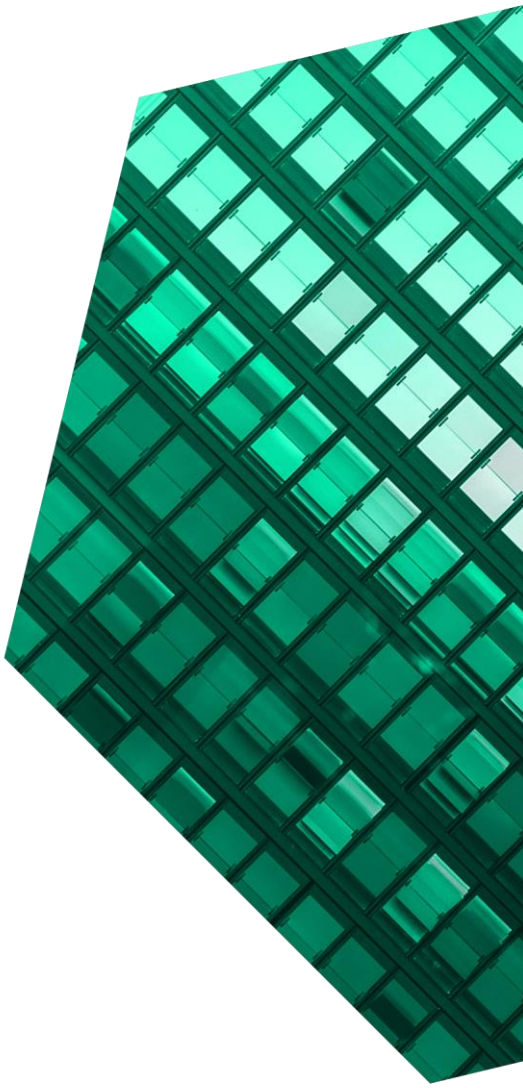
Cisco Secure Firewall の Total Economic Impact™

コスト削減およびビジネス上の利益
Secure Firewall で実現

2022 年 3 月

目次

コンサルティングチーム： *Henry Huang*
Nick Mayberry



FORRESTER CONSULTING について

Forrester Consulting は、独立した客観的なリサーチに基づき、リーダーが組織で成功するためのコンサルティングを提供しています。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

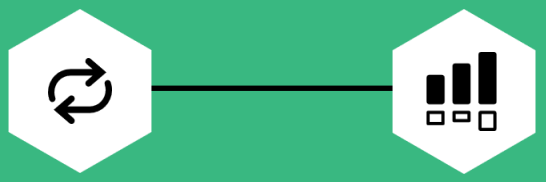
Cisco Secure Firewall と Firewall Management Center は、企業のネットワークセキュリティの可視性と制御を向上させます。インタビューした組織は、ファイアウォール関連のネットワーク専門家の仕事量を最大 95%、セキュリティ関連の専門家の仕事量を最大 83%削減しました。また、ネットワークや VPN の障害を最小限に抑えることで、エンドユーザーの生産性を向上させながら、重大なセキュリティ侵害のリスクを最大 80%削減しました。ファイアウォール展開数を 25%削減しながらも、セキュリティ態勢を改善することができました。

Cisco Secure Firewall は、第 7 層の次世代ネットワークセキュリティソリューションで、外部および内部の脅威から組織を保護するとともに、ファイアウォールと脅威管理の両方において、ネットワークおよびセキュリティチームの負担を軽減します。Cisco Secure Firewall は、ファイアウォール管理および脅威防御の一元化ハブである Firewall Management Center（FMC）により、ネットワークおよびセキュリティチームが、アプリケーション層や暗号化トラフィックで検出された脅威についても、より統合された全体像でネットワークアクティビティを可視化できるように管理することができます。さらに、Snort 3 侵入防御システム（IPS）による制御の強化、URL フィルタリングとマルウェア防御用のソフトウェアの強化が行われています。

Cisco Secure Firewall のライセンスには、Cisco Secure のポートフォリオとサードパーティ製のセキュリティツールから得られる脅威データを、迅速な調査と対応を促進するために設計された、コンテキストに富んだ単一のグローバルビューに統合することを可能にする Cisco の統合プラットフォーム、SecureX の使用も含まれています。

Cisco の委託で、Forrester Consulting は、Total Economic Impact™（TEI）調査を実施し、Secure Firewall を導入することで企業が実現しうる投資収益率（ROI）を検証しました。[1] 本調査の目的は、読者に Secure Firewall が組織に与える潜在的な財務的影響を評価するための枠組みを提供することです。

主な統計情報



投資利益率（ROI）
195%

正味現在価値（NPV）
1,229 万ドル

Forrester では、この投資に伴う利益、コスト、リスクをより深く理解するため、Secure Firewall の使用経験のある顧客 8 社の 10 人の意思決定者にインタビューを行いました。Forrester は、インタビューした顧客の体験を集計し、財務分析のベースラインとなる結果を、1 つのモデル組織としてまとめました。

これらのインタビュー回答者は、Secure Firewall を導入する前は、自社のネットワークを適切に管理し、効果的にセキュリティを確保するために必要な可視性と管理機能が欠けていたことを指摘しています。このような可視性と効率的なグラフィカルユーザーインターフェイス（GUI）のいずれも存在しなかった際には、ファイアウォールの導入、ポリシー作成、ファイアウォールのアップグレード、ポリシーの更新といったネットワークのワークストリームに多大な時間がかかっていたことも指摘しています。また、脅威の調査・対応やリモートアクセス管理などのセキュリティのワークストリームにも、更なる時間が費やされていました。さらに、需要が高い期間中のネットワークパフォーマンスの低下、複数のベンダーのソリューションを管理することによる複雑さについても指摘しています。

Secure Firewall への投資後、これらの組織は、上記のネットワークとセキュリティのワークストリームを形成するために必要な時間を短縮しただけでなく、組織全体のセキュリティを強化することにも成功しました。同時に、ポリシー更新の迅速化、ネットワークトラフィックの検査の強化、ネットワーク全体のパフォーマンスの向上により、従業員の生産性を向上させるとともに、レガシーソリューションを廃止し、関連する管理時間コストを大幅に削減できました。

利益総額

1,860 万ドル

主な調査結果

数字で見る利益。リスク調整後の現在価値（PV）の定量的利益には、以下のようなものがあります。

- **ネットワーク運用のワークストリームを最大 95%削減。** Cisco Secure Firewall の最新機能と Firewall Management Center による管理のしやすさのおかげで、インタビューした組織は、以下の時間短縮を実現できました。
  - ファイアウォール導入時間を 36%短縮。
  - ファイアウォール更新時間を 90%短縮。
  - 従来の Adaptive Security Appliance（ASA 5500-X）ファイアウォールと比較して、ファイアウォールポリシー更新時間を 95%削減。
  - Firewall Threat Defense（FTD）ベースのポリシーの初期バージョンと比較して、ファイアウォールポリシー更新時間を 80%短縮。
  - 仮想ファイアウォール更新時間を 80%短縮。
- **セキュリティ調査および対応ワークストリーム時間を最大 83%短縮。**また、Cisco Secure Firewall と Firewall Management Center を組み合わせることで、情報を消費・分析しやすくなり、セキュリティ専門家の仕事量が大幅に削減されたことも指摘しています。潜在的な脅威の調査時間が 49%、脅威への対応時間が 83%短縮されています。SecureX を Secure Firewall および FMC と併用することで、組織は調査や対応に費やされた残りの時間をさらに最大 77%短縮できました。

「当社はセキュリティ意識が非常に高く、会社を守るための製品を活用することを望んでいます。そのため、Cisco を選びました。セキュリティと共に発展してきた Cisco にとって、セキュリティは単なる付加価値ではありません。」
製造業者のシニアネットワークエンジニア

- **侵害リスクを最大 80%削減。** Cisco Secure Firewall と Firewall Management Center が提供する可視性と制御の組み合わせにより、インタビューした組織は、潜在的な重要侵害のリスクとそれに関連するコストを削減することができました。これらのソリューションは、従来の ASA 5500-X ファイアウォールと比較して 80%、早期の FTD ベースのファイアウォールと比較して 15%侵害リスクを低減しています。SecureX の導入により、インタビューした組織は、セキュリティ侵害のリスクとコストをさらに最大 23%削減することができました。

- **年間約 200 万ドルと評価されるエンドユーザーの生産性向上。** Cisco Secure Firewall と Firewall Management Center を導入することで，インタビューした組織の生産性は次の 2 点で向上しました。まず、ネットワーク専門家は、破壊的なポリシーの更新エラーを 80%短い時間で修正できるようになりました。次に、ネットワークパフォーマンスの低下レベルを軽減し、影響を受けたエンドユーザー1 人あたり年間約 9 時間の労働時間を取り戻しました。
- **レガシーツールの廃止によるコスト削減。** また、Cisco Secure Firewall の導入により、それまで使用していた高価なレガシーセキュリティソリューションを廃止することができました。インタビュー回答者は、スタンドアロンの IPS では年間数十万ドル、既存のセキュリティソリューションの買い替えコストでは数百万ドル、さらに Cisco Secure Firewall では少ないファイアウォールで同レベルの保護が可能なため、さらに 25%のコスト削減を実現できたと述べています。

非定量的利益。 本調査の非定量的な利益には、以下のようなものがあります。

- **VPN の生産性とセキュリティの強化。** Cisco Secure Firewall は、ロードバランシング、ローカル認証、マルチ証明書認証によって、リモートアクセス VPN の生産性とセキュリティの向上も実現しました。エンドユーザーは VPN を利用してより良い接続を確立し、組織はアクセスのコントロールを向上させることができました。
- **在宅勤務における操作性が向上。** また、在宅勤務への移行に伴い VPN が爆発的に普及した際にも、Cisco Secure Firewall の制御によりスムーズな運用が実現されました。ネットワークの専門家は、料金制限と冗長性の改善を活用することで、ピーク需要時でも従業員のエクスペリエンスと生産性を向上させることができます。
- **クラウドへの移行が容易。** 最後に、Cisco Secure Firewall は、サイト内、サイト間、および組織と複数のクラウド プラットフォーム間のトラフィックを保護する 1 つのプラットフォームを提供することで、クラウド構想の実現が容易になったと、インタビュー回答者は答えています。具体的には、Cisco が標準化したポリシーと、クラウドプラットフォームのマーケットプレイスを介してセキュアファイアウォールを展開するための有効な手段が提供されました。

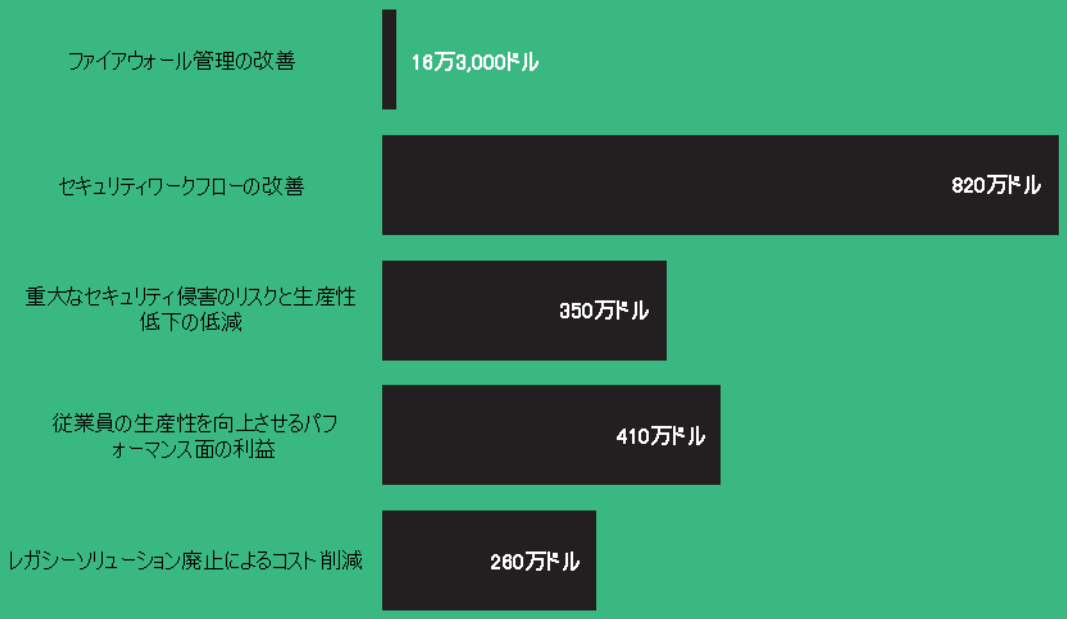
コスト。 リスク調整後の PV コストは次のようになります。

- **ライセンスコスト。** インタビューした組織が負担した最大のコストはライセンスコストでしたが、Cisco Enterprise Agreement を締結することで、これまで欠けていた機能やソリューションの追加に伴うコストを数十万ドルを節約し、組織のセキュリティ態勢をさらに強化することができました。SecureX のライセンス権利は、Secure Firewall に含まれています。
- **実装、ポリシー作成、トレーニングのコスト。** インタビュー回答者は、ファイアウォールの導入やポリシー作成に社内コストがかかることを指摘しました。ファイアウォールの導入には 1 サイトあたり 6 時間、ポリシーの作成には 30 時間かかると試算されています。SecureX の導入には 20 時間、継続的な管理には年間 100 時間の追加作業が必要です。また、Cisco Secure Firewall と Firewall Management Center を使用するために、ネットワークとセキュリティの専門家のトレーニングの必要性を指摘するインタビュー回答者もいました。トレーニングにかかる社内コストは、従業員 1 人あたり 2 時間で、インタビューでは、Cisco のセキュリティ専門家による一般公開のトレーニングビデオを活用したことが指摘されています。

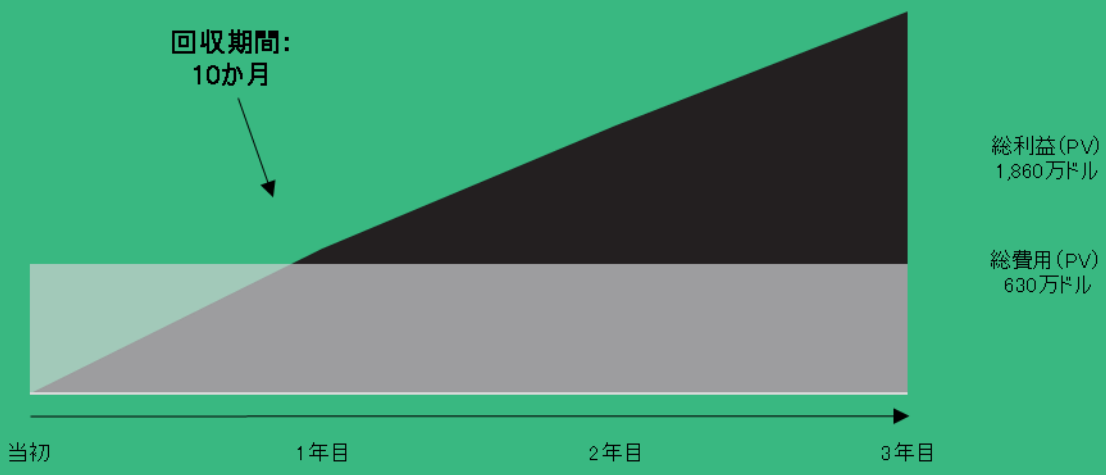
意思決定者へのインタビューと財務分析の結果、モデル組織の場合、3 年間で 630 万ドルのコストに対して 1859 万ドルの利益があり、正味現在価値（NPV）は 1229 万ドル、ROI は 195%であることが判明しました。

投資利益率（ROI）	利益の現在価値（PV）	正味現在価値（NPV）	回収期間
195%	**1,859 万ドル**	**1,229 万ドル**	**10 か月**

利益（3年間）



財務状況概要



TEI のフレームワークと調査手法

Forrester は、インタビューで得られた情報から、Cisco Secure Firewall への投資を検討している組織を対象とした Total Economic Impact™の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、柔軟性、およびリスク要因を特定することです。Forrester は、セキュアファイアウォール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。

デューデリジェンス（適正評価 ）
Cisco の関係者や Forrester のアナリストのインタビューを行い、Secure Firewall に関するデータを収集しました。

企業の意思決定者のインタビュー
Secure Firewall を導入している企業の意思決定者 10 人のインタビューを行い、コスト、利益、リスクに関するデータを取得しました。

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。

財務モデルのフレームワーク
TEI 手法を用いて、インタビュー回答者を表す財務モデルを構築し、意思決定者の課題や懸念に基づいて財務モデルのリスク調整を行いました。

事例紹介
TEI の 4 つの基本要素である利益、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。Forrester の TEI 手法は、ROI 分析が高度化していることを考慮して、購入判断の総合的な経済効果を完全に網羅しています。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

以下の点に注意してお読みください。

本調査は、Cisco の委託により、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、他の組織が受け取るであろう潜在的な ROI については、一切の想定をしていません。Forrester は、読者が Secure Firewall への投資の妥当性を判断するために、本調査で提供された枠組みの中で独自の推定を行うことを強く推奨します。

Cisco は、本調査のレポート内容を確認した後、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の編集は Forrester が権限を有しており、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されていません。

Cisco は、インタビューする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。

Cisco Secure Firewall のカスタマージャーニー

セキュアファイアウォールへの投資を推進した要因

企業意思決定者のインタビュー

インタビュー回答者	業種	地域	全従業員数
エンジニアリングサービスマネージャー	IT サービス	北米	750
リードインフラストラクチャエンジニア	金融サービス	北米	2,800
通信・テレフォニーサービス担当 アシスタントマネージャー	金融サービス	北米	2,800
プリンシパルサイバーセキュリティエンジニア	セキュリティサービス	北米	3,000
シニアネットワークエンジニア	製造	グローバル	5,500
ネットワークエンジニアリング担当 シニアマネジャー	テクノロジー	グローバル	40,000
シニアセキュリティエンジニア	テクノロジー	グローバル	40,000
セキュリティオペレーションチームリーダー	教育	北米	46,000
スタッフインフラストラクチャアーキテクト	産業用	グローバル	205,000
シニアネットワークエンジニア	テクノロジー	グローバル	275,000

主な課題

Cisco Secure Firewall と Firewall Management Center を導入する以前、インタビューした組織は、主に従来型の ASA 5500-X ベースのファイアウォールアプライアンスを利用して環境を保護していました。数年前に従来型の ASA ベースのファイアウォールから初期の FTD ベースのファイアウォールに切り替えたインタビュー回答者もいますが、Cisco Secure Firewall と Firewall Management Center で FTD の最新バージョンにアップグレードした後にさらなる利益を実感していると述べています。

インタビューした組織に共通して見られた課題には、以下のようなものがありました。

- **可視性が乏しい。** ASA 5500-X ベースのファイアウォールに依存していた環境では、セキュリティ全体に対する可視性が限られていたことが指摘されています。その原因の一つは、統合の欠如にありました。以前の環境では、さまざまなセキュリティソリューションを統合して統一的な管理と一貫したポリシーを確立し、同時に事実の単一バージョンを得ることは、インタビューした組織にとって困難なことでした。また、従来の環境では、ネットワークを見る中心的な視点がポート検査に依存していたことも、可視化が困難であった理由の一つです。そのため、アプリケーションの可視性が低く、履歴情報も限定的であるため、データを掘り下げて見ることができなかったとインタビュー回答者は答えています。

「以前は、最新のアプリケーションコントロールのような機能が不足していました。ユーザーがどのようにネットワークを利用しているかが見えず、その利用状況に十分対応できませんでした。」
教育機関のセキュリティオペレーションチームリーダー

- **ファイアウォールの導入・管理にかかる時間的コストが高い。**また、インタビュー回答者は、レガシーファイアウォールの導入と管理には多大な時間が必要だったことにも言及しました。その理由の多くは、複数のデバイスに一度にアップデートをプッシュする機能がないことでした。教育機関のセキュリティオペレーションチームリーダーは、以前は単純なファイアウォールルールの導入に 45 分から 1 時間程度かかっていたと推定しています。さらに、以前の環境では可視化されていなかったため、セキュリティ体制を確認するために異なるシステム間のデータの関連付けに膨大な時間を費やしていたとも言っています。

「管理・統合のしやすさは、Cisco の長所の一つでした。また、異なるシステム同士が容易に連携できるため、豊富なデータが得られるという利益もあります。また、特定の脅威に対しては、自律的な対応策を確立しています。以前はこれらは何一つできませんでした。」
セキュリティサービス業者のプリンシパルサイバーセキュリティエンジニア

- **業績が悪い。**また、インタビュー回答者は、以前のシステムパフォーマンスの低迷にも言及しました。例えば、教育機関のセキュリティオペレーションチームリーダーは、ネットワークとセキュリティインフラへの需要が急増したとき、以前のソリューションは「フォールオーバーし、再起動を繰り返して、パケットをドロップした」と話しています。その結果、「教授は授業中にネットワークを利用してビデオを再生したり、デモしたりできなかった」と、生産性にまで影響が及んでいることを指摘しています。
- **ベンダー管理。**最後に、お客様は、以前の環境では複数のベンダーを利用していたためベンダー管理に頭を悩ませていたことを指摘しました。金融サービス業者のリードインフラエンジニアは、「複数のベンダーが存在するため、同じ変更や更新を異種システム間で適用際、複数のコントロールプレーンにアクセスし、すべて何度も行う必要がありました」と指摘しています。

モデル組織

インタビューに基づき、Forrester は 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。モデル組織とは、Forrester が意思決定者に対するインタビュー調査を実施した 9 社を代表する組織であり、次のセクションで財務分析の総合結果を表すために使用されています。モデル組織の特性は以下の通りです。

モデル組織の説明。 モデル組織は、年間売上高 50 億ドル、従業員数 16,000 人の B2B テクノロジー企業です。全世界のクライアントにサービスを提供しています。この組織は、データセンターで保管されているデータへの顧客の一貫したアクセスを確保するために、データセンターの高い可用性を必要としています。また、これらのデータセンターでは、顧客の大切なデータを不正アクセスや攻撃から守るために、より高度なセキュリティが要求されます。データセンターに加え、この組織はマルチクラウドを活用した分散型アプローチに移行しています。さらに、エッジサイト/支社を保護するためにセキュアファイアウォールも使用しています。

導入の特徴。モデル組織では、すでに Cisco の次世代ファイアウォールに投資しています。ファイアウォールの在庫の 3 分の 2 は Cisco Firepower、3 分の 1 は ASA 5500-X です。現在、ホームオフィス、データセンター、本社の 102 拠点のファイアウォールをすべて最新版の Cisco Secure Firewall に移行し、68 の Firepower を更新、34 の ASA ベースの機器を切り替えています。インタビューした組織の中には、ハードウェアはそのままに、既存の従来型機器を FTD ソフトウェアにアップデートすることを選択した組織もありました。また、データセンターと支社間の East-West トラフィックや、データセンターと複数のパブリッククラウドプラットフォーム間のトラフィックを処理するために、データセンターに Cisco Secure Firewall 仮想ファイアウォールを導入しています。同社は、Secure Firewall のライセンスに SecureX が含まれることを利用して、セキュリティチームの脅威の調査・対応作業をさらに強化しています。

主な想定条件

- 収益 5 億ドル
- 従業員 16,000 人
- ASA ベースのファイアウォールを 34 個切り替え
- 68 の Firepower ファイアウォールを最新の Cisco Secure Firewall にアップデート

利益の分析

■ モデル組織に適用された定量化利益データ

総利益

基準	利益	1 年目	2 年目	3 年目	合計	現在価値
Atr	ファイアウォール管理の改善	134,951 ドル	25,556 ドル	25,556 ドル	186,064 ドル	163,005 ドル
Btr	セキュリティワークフローの改善	2,669,879 ドル	3,685,484 ドル	3,685,484 ドル	10,040,848 ドル	8,241,976 ドル
Ctr	重大なセキュリティ侵害や生産性低下のリスク低減	1,291,446 ドル	1,393,402 ドル	1,520,848 ドル	4,205,696 ドル	3,468,249 ドル
Dtr	従業員の生産性を向上させるパフォーマンス面の利益	1,656,403 ドル	1,656,403 ドル	1,656,403 ドル	4,969,210 ドル	4,119,230 ドル
Etr	レガシーソリューションの廃止によるコスト削減	1,985,115 ドル	503,513 ドル	503,513 ドル	2,992,142 ドル	2,599,074 ドル
	総利益（リスク調整済み）	7,737,795 ドル	7,264,360 ドル	7,391,805 ドル	22,393,959 ドル	18,591,534 ドル

ファイアウォール管理の改善

エビデンスとデータ。 インタビューした意思決定者は、レガシーファイアウォールからの切り替えや Firepower Threat Defense の初期バージョンからのアップデートにかかわらず、Cisco Secure Firewall 導入後はファイアウォールの管理に関わる時間とコストが削減されたと述べています。これらの改善の大部分は、ファイアウォール管理センターがファイアウォールを一元的に管理し、多くのデバイスに変更を加えることを可能にすることで、ネットワークの専門家を支援したことに起因しています。

「FMC のおかげで、以前のようにさまざまなファイアウォールを切り替えることなく、ファイアウォールの管理とアップグレードを一元的に行えるようになりました。」
IT サービス業者のエンジニアリングサービスマネージャー

インタビューした組織は、共通してファイアウォールの導入に関連する時間とコストを削減しています。従来の ASA ベースのファイアウォールでは、使用事例に応じたファイアウォールルールを作成し、それを多様なファイアウォールポリシーに手動で分散させる必要があり、ファイアウォールの導入に多大な時間がかかっていたとインタビュー回答者は述べています。

「Cisco Secure Firewall のおかげで、新しいファイアウォールを迅速に立ち上げ、導入することができました。ファイアウォールの増加に合わせて、従業員を増やす必要はありませんでした。」
ネットワークエンジニアリング、テクノロジー担当シニアマネジャー

Cisco Secure Firewall と Firewall Management Center に切り替えた後、ファイアウォールの導入にかかる時間を 30 ～ 40%削減できたとインタビュー回答者は答えています。この時間短縮は、Cisco Secure Firewall の導入を自動化でき

たことに起因しています。例えば、テクノロジー企業のネットワークエンジニアリング担当シニアマネージャーは次のように述べています。「Cisco Secure Firewall で導入を自動化しました。箱から出し、IP を設定し、シャーシをセットアップし、ポリシーを実施する工程が自動化できました。」

「自動化機能が搭載されているため、時間が大幅に節約できています。アップグレード周りでもそうです。もう、ASA の時のように、アップグレードプロセスの世話を焼く必要はありません。離席しても、Firepower が十分な時間内にオンラインに復帰しない時には知らせてくれます。」
ネットワークエンジニアリング、テクノロジー担当シニアマネジャー

自動化は、導入後の Cisco Secure Firewall の管理と保守に関してもインタビューした組織を支援しています。Cisco Secure Firewall には、自動アップグレード機能が搭載されています。ASA ベースのファイアウォールのアップグレードには、ファイアウォール間の移動、アップデートファイルのアップロード、システムのリブートなど、何時間もかかることがありましたが、Cisco Secure Firewall と Firewall Management Center を使用した場合、インターフェイスをクリックしてファイアウォールをアップグレードし、30 分後にアップグレードが成功したかどうかを確認するだけで良くなったと回答者は答えています。

「ASA から Cisco Secure Firewall に移行した後、ポリシー管理にかかる時間を 60%から 70%短縮することができました。」
IT サービス業者のエンジニアリングサービスマネージャー

Cisco Secure Firewall と Firewall Management Center では、オブジェクト指向のシステムにより、長いアクセス制御リスト（ACL）を必要とせずに、ポリシーをカテゴリやゾーンに整理することができるようになったとインタビュー回答者は述べています。また、従来はデバイスごとに手動で更新していたポリシーの展開や更新も、自動的に行えるようになりました。

「Cisco Secure Firewall は、ポリシーの 90%を自動展開してくれます。一回きりの設定に悩む時代ではなくなりました。」
ネットワークエンジニアリング業者のテクノロジー担当シニアマネジャー

Cisco Secure Firepower を使って早期の FTD から最新 FTD にアップグレードした後、さらに時間を節約できたとインタビュー回答者は述べています。例えば、金融機関のリードインフラストラクチャエンジニアは、初期の FTD ではポリシーの展開に 10～15 分かかっていたが、FTD のアップグレードにより展開時間が 3 分程度に短縮されたと述べています。

「Cisco Secure Firewall によるポリシー管理は、わかりやすく簡単です。Firewall Management Center の GUI は、軽量かつクリーンで、直感的に操作できます。」
ネットワークエンジニアリング業者のテクノロジー担当シニアマネジャー

あるインタビュー回答者は、Firewall Management Center ではなく、クラウド SaaS である Cisco Defense Orchestrator（CDO）管理を利用したと言っています。CDO について、産業部門のスタッフインフラストラクチャアーキテクトは、次のように話しています。「CDO を採用するのは簡単でした。当社のエンジニアはすでに「Cisco Security Manager（CSM）」を使いこなしていたので、コマンドラインインターフェイスの操作やマクロの構築はすでに可能でした。新しい上位層のコンセプトを学ばなければならない複雑さがある他のベンダーに乗り換えるよりも、はるかに簡単でした。」

モデリングと想定。 モデル組織については、Forrester のモデル。

- 従来の ASA 5500-X ファイアウォール 34 台を Cisco Secure Firewall に切り替え。
- このモデル組織では、従来のファイアウォールを交換するたびに、その導入とポリシー作成にかかる 55 時間の労働時間を回避することができます。
- このモデル組織は、従来は四半期ごとにファイアウォールを 1 つずつアップグレードしていた 30 分を 90%回避することができました。
- このモデル組織は、平均して 1 日に 1 回、ファイアウォールポリシーを更新しています。Cisco Secure Firewall に切り替えることで、これまで 1 回につき 1 時間かかっていたアップデート時間を 95%回避することができました。
- ネットワークセキュリティオペレーション（NetSecOps）専門家の全経費込みの平均時給は 65 ドルです。
- 68 台の FTD ファイアウォールが Cisco Secure Firewall の最新バージョンにアップグレードされました。毎日のポリシー更新のたびに、モデル組織は前世代の FTD ファイアウォールにかかる時間の 80%を節約しています。
- さらに、このモデル組織は、仮想ファイアウォールのポリシーの更新に要していた時間を 80%削減することができました。

リスク。 ファイアウォール管理の改善点は、以下と異なる場合があります。

- 既存のファイアウォールの種類と数。
- Cisco Secure Firewall に切り替えたファイアウォールの数およびその導入率。
- East-West トラフィックおよびパブリッククラウドのトラフィックを処理するために、データセンターに仮想ファイアウォールを導入することを決定。

結果。 これらのリスクを反映させるため、Forrester はこの利益を 10%下方調整し、リスク調整後の 3 年間の総額の PV（割引 10%）をおよそ 163,000 ドルとしました。

ファイアウォール管理の改善

基準	評価項目	ソース	1 年目	2 年目	3 年目
A1	レガシーファイヤーウォールを置き換える次世代ファイヤーウォールの台数	モデル組織、全 102 台の 1/3	34	0	0
A2	各ファイアウォールの導入時間を短縮	インタビュー	55.00	55.00	55.00
A3	各 ASA ファイアウォールのアップデート時間を短縮	90%*17 時間/四半期	61.2	61.2	61.2
A4	ASA ファイアウォールポリシーの手動更新時間を回避。	95%*1 時間、1 日 1 回 *33%環境	114	114	114
A5	NetSecOps 専門家の時間給	モデル組織	65 ドル	65 ドル	65 ドル
A6	小計：レガシーレイヤー4 ファイアウォールから次世代ファイアウォールへの置き換え/アップグレードにかかる時間を短縮	((A1*A2)+(A3+A4))*A5	132,938 ドル	11,388 ドル	11,388 ドル
A7	FTD ファイアウォールアップデート数	モデル組織、全 102 台の 1/3	68	68	68
A8	早期 FTD に対応したポリシー展開のための先行時間	インタビュー	0.25	0.25	0.25
A9	後期 FTD へのアップグレードによるポリシー展開時間の短縮	インタビュー、15 分～3 分	80%	80%	80%
A10	小計：旧レイヤー7 ファイアウォールから Firepower へのポリシー導入時間の短縮	365*A8*A9*A5*A7/102	3,163 ドル	3,163 ドル	3,163 ドル
A11	仮想ファイアウォールの総数	モデル組織	100	100	100
A12	仮想ファイアウォールポリシー更新のために無駄になった年間時間	年間 80%*266 時間	213	213	213
A13	小計：仮想ファイアウォール管理時間の短縮	A12*A5	13,845 ドル	13,845 ドル	13,845 ドル
At	ファイアウォール管理の改善	A6+A10+A13	149,946 ドル	28,396 ドル	28,396 ドル
	リスク調整	↓10%			
Atr	ファイアウォール管理の改善（リスク調整済み）		134,951 ドル	25,556 ドル	25,556 ドル
	3 年間の合計：186,064 ドル			**3 年後の現在価値：163,005 ドル**	

セキュリティワークフローの改善

エビデンスとデータ インタビュー回答者によると、Cisco Secure Firewall を導入し、FMC を利用することも、セキュリティワークフローの合理化に役立っているとのことです。この意思決定者は、ASA ベースのデバイスが、ファイアウォール全体のイベントを追跡し、ログを記録するために、複数の別々のツールを必要とすることを指摘しました。FMC により、Cisco Secure Firewall のデータは一箇所に集約され、侵害指標（IOC）やブロックされた侵入を追跡したり、セキュリティ情報およびイベント管理（SIEM）ソリューションに首尾よくレベルアップさせることができました。インタビュー回答者は、FMC の導入により、ネットワーク全体の接続、イベント、テレメトリをより相関的に確認することができるようになったと言っています。

「セキュリティ調査は、以前は 1 つのピースでパズルを作るようなものでした」。
教育機関のセキュリティオペレーションチームリーダー

インタビュー回答者は、Firewall Management Center の統合により、セキュリティ調査業務の時間的コストが削減できたと答えています。例えば、セキュリティサービス業者のリードサイバーセキュリティエンジニアは、Secure Firewall と Firewall Management Center の支援により、調査にかかる時間が数時間から 3〜5 分に短縮されたと述べています。以前、このインタビュー回答者は、SIEM や電子メールコンソールを含む複数のシステムを介してログインし、データを調整する必要があったと述べました。現在では、FMC にログインして、その環境にある特定の IOC を探し出すことができます。

「Firewall Management Center は、すべての Cisco Secure Firewalls を管理するための単一のコンソールとして機能します。管理が容易になり、イベントの調査や照合、悪意のある行為に関する判断にかかる時間が短縮されます」。
IT サービス、エンジニアリングサービスマネージャー

インタビュー回答者も、同様に応答時間が短縮されたことを指摘しています。例えば、教育機関のセキュリティオペレーションチームのリーダーは、Cisco Secure Firewall に投資する前は、クライアントサポートに週に何度もチケットを送信していたと述べています。サポートはユーザーを追跡し、マルウェアテストを実施しますが、そのスキャンには数時間かかることもありました。その後、チームはシステムをクリーンアップするか、システムのイメージを再作成していました。この作業には、丸 1 日かかることもありました。Cisco Secure Firewall では、同様のチケットを月に一度送ると、そのまま FMC に送信された、約 1 時間で問題が解決されます。

「レガシーファイヤーウォールでは、セキュリティインシデント対応を行うために多くのオーバーヘッドが必要で、多大な時間とコストがかかっていました。Firepower を使用することで、ブロックされる範囲が広がり、インシデント対応にかかる時間が大幅に短縮されました。」
教育機関のセキュリティオペレーションチームリーダー

FTD の初期バージョンから最新バージョンに移行したインタビュー回答者は、セキュリティ調査および対応ワークフローに関するメリットも経験しています。金融サービスセクターのリードインフラエンジニアの報告によると、FTD の以前のバージョンでも Firewall Management Center 経由でセキュリティ警告を集約して見ることができましたが、アップグレード後は定義とトリガー機能が改善されました。また、インタビュー回答者は、AMP や Umbrella などの Cisco 製品とのさらなる統合の更なる相関関係により、追加の利益が得られていると述べています。

「FMC は、私たちに大きな可能性を与えてくれます。現在、この可視化によって、問題がないことを視覚的に確認するためにより多くの時間を費やしています。しかし、インシデント対応に費やす時間は以前と比べて短くなっています。」
教育、セキュリティオペレーションチームリーダー

Secure Firewall のライセンスへの SecureX の組み込みを行った組織では、可視化とカスタマイズにより、セキュリティチームの業務効率がさらに向上しています。例えば、教育機関のセキュリティオペレーションチームリーダーは、SecureX ではダッシュボードをパーソナライズ、カスタマイズできるため、環境の可視性を高めるだけでなく、各ユーザーにその担当業務に最重要な情報を表示できると述べています。

モデリングと想定。 モデル組織については、Forrester のモデル。

- 年間総セキュリティ警告数 10 万件。
- このうち 26%はセキュリティアナリストの介入を必要としています。
- 介入を要するアラートの 7 割は、調査も必要です。
- Cisco Secure Firewall と Firewall Management Center は、アラートの調査に必要だった 2.8 時間を 49%短縮しました。
- 調査が必要なアラートのうち、対応が必要なものは 10%でした。
- Cisco Secure Firewall と Firewall Management Center は、対応に必要だった 6 時間を 83%短縮しました。
- SecureX により、調査・対応ワークフローの時間を 1 年目で 42%、2 年目、3 年目で 77%、さらに短縮することができました。

リスク セキュリティワークフローの改善は、以下の事項で変化する可能性があります。

- 年間警告数、注意を要する警告数、調査を要する警告数、および対応を要する警告数。
- NetSecOps の専門家の完全負担の時給です。

結果。 これらのリスクを反映させるため、Forrester はこの利益を 15%下方修正し、3 年間のリスク調整後の総 PV は 820 万ドル以上となりました。

セキュリティワークフローの改善					
基準	**評価項目**	**ソース**	**1 年目**	**2 年目**	**3 年目**
B1	年間総アラート数	モデル組織	100,000	100,000	100,000
B2	アナリストの注意を喚起するアラート	Forrester research、26%	26,000	26,000	26,000
B3	調査を必要とするアラートの割合	インタビュー	70%	70%	70%
B4	平均事前調査時間	インタビュー	2.8	2.8	2.8
B5	FMC による調査時間の短縮	インタビュー	49%	49%	49%
B6	対応を要するアラート	インタビュー	260	260	260
B7	対応までにかかる平均時間	インタビュー	6	6	6
B8	FMC による対応時間の短縮	インタビュー	83%	83%	83%
B9	SecureX による調査/対応時間のさらなる短縮	インタビュー	42%	77%	77%
B10	セキュリティ担当者の全経費込時給	A5	65 ドル	65 ドル	65 ドル
Bt	セキュリティワークフローの改善	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	3,141,034 ドル	4,335,864 ドル	4,335,864 ドル
	リスク調整	↓15%			
Btr	セキュリティワークフローの改善（リスク調整済み）		2,669,879 ドル	3,685,484 ドル	3,685,484 ドル
	3 年間の合計：10,040,848 ドル		**3 年後の現在価値：8,241,976 ドル**		

重大なセキュリティ侵害のリスクと生産性低下の低減

エビデンスとデータ。また、インタビュー回答者は、Cisco Secure Firewall の導入により、重大なセキュリティ侵害のリスクとそれに関連する生産性コストが削減され、経済的な利益を実感していると述べています。

Cisco Secure Firewall と Firewall Management Center が提供する可視性は、インタビューした組織のセキュリティ姿勢を向上させる一つの手段となりました。例えば、教育機関のセキュリティオペレーションチームリーダーは、次のように指摘しています。「従来の ASA と比較して、Cisco Secure Firewall はより優れた可視性を提供してくれます。特に、ユーザーがモバイル機器をネットワークに持ち込んで、ネットワーク経由での印刷などのサービスにアクセスするケースが増加し

「脅威」と「IOC」のブロック数が大幅に改善されました。桁違いの差です。以前の Secure Firewall を導入しない状態では、毎日ビジネスが危険にさらされていました。可視化されたことで、リスクは計り知れないほど軽減されました。今では安心できます。」

IT サービス、エンジニアリングサービスマネージャー

ているため、これは重要なことです。Firepower にアップグレードすることで、可視性が向上し、基幹トラフィックだけでなく、内部ネットワークのトラフィックをフィルタリングできるようになりました。」

また、自動ブロック機能の向上により、セキュリティ侵害があった場合の潜在的なリスクも低減することができました。テクノロジー分野のネットワークエンジニアリング担当シニアマネージャーは、次のように指摘しています。「Firepower は、[侵入防御システム(IPS)]の業界リーダーです。セキュリティ態勢を強化し、問題をすぐに修正することができました。潜在的なインシデントを早期に修正することで、コストを削減することができます。」この同じ顧客は、ASA ベースのシステムから Cisco Secure Firewall に移行したところ、ブロッキングが 80%改善されたと指摘しています。

「Secure Firewall のおかげで、人員を増やすことなく、すぐに 80%の脅威を排除することができました。」
ネットワークエンジニアリング業者のテクノロジー担当シニアマネジャー

重要なのは、インタビュー回答者は、FTD ファイアウォールを最新バージョンに更新することでブロッキングが改善されたと指摘したことです。テクノロジー企業のシニアネットワークエンジニアは、FTD の最新バージョンにアップグレードすることで、以前のバージョンよりも 10%から 15%多くの自動ブロッキングが可能になったと話しています。

また、自動ブロックがもたらす影響について、同じインタビュー回答者が、次のようなエピソードを話してくれました。「ソーシャルエンジニアリングによって、ハッカーが認証済みユーザーから 24 時間有効なアクセストークンを手に入れたことがあります。ハッカーが（トークンを）使おうとした時、Cisco Secure Firewall が私たちを救ってくれました。セキュリティ体制を確認し、攻撃者が会社のマシンを使っているかどうかを確認することができました。Secure Firewall は、ハッカーの VPN アクセスを自動的に拒否しました。これがなければ、ハッカーは私たちの企業ネットワークにアクセスできたはずで、それが当社にどれだけの被害を及ぼしていたか見当も付きません。」

「Cisco Secure Firewall ではあらゆる作業が完結します。他のツールとの連携機能をすべて備えており、セキュリティに役立つ関連データを提供します。さまざまな機能があり、異なるスループット要件に対応でき、垂直方向と水平方向の両方のスケーリングに対応しています。今日のセキュリティリスクに対応するために必要な機能をすべて備えており、しかも継続的に改善されています。」
インターネット事業者のシニアネットワークエンジニア

また、テクノロジー企業のシニアネットワークエンジニアは、Secure Firewall がアプリケーションレベルでアクセスを管理できるため、セキュリティ上の利点があると指摘しています。「ゲストネットワークで BitTorrent が大量に使用されていることが確認できました。FTD を活用して BitTorrent をブロックすることで、他のゲストへの潜在的な脅威を防ぐだけでなく、約 400Mbps 分、回線使用率を下げることができました。」とコメントしています。

アプリケーション層の検出とブロックに加え、Cisco Secure Firewall が Snort ベースの自動脅威フィードを使用することで、重大なセキュリティ侵害が発生するリスクを低減できるとの指摘もありました。。金融機関のリードインフラエンジニアは、「Cisco Secure Firewall を導入したのは、可視性の向上と Snort による自動応答、インターネットに公開されているパッチ

未適用のサーバーなどを探し、悪意のあるトラフィックを全体的にブロックするためです」と述べています。

SecureX が Secure Firewall のライセンスに含まれていることを利用した組織は、重大なセキュリティ侵害のリスクとコストをさらに削減することができました。例えば、金融機関のリードインフラエンジニアは、SecureX によって、セキュリティ問題の特定と潜在的な脅威の根本原因の特定をさらに可視化することができたと述べています。

「SecureX で当社のセキュリティ環境全体を一元的に把握できます。FMC では、すべてのファイアウォールを見ることができます。SecureX では、FMC だけでなく、Cisco のセキュリティソリューションのすべてを確認できます。」
教育機関のセキュリティオペレーションチームリーダー

モデリングと想定。 モデル組織について、Forrester は以下のモデルを設定:

- 年間の重大なセキュリティ侵害の回数が 3 回であったこと。
- 重大なセキュリティ侵害が発生した場合の内部および外部のコストを合わせた平均額は 968,480 ドル。
- 外部からの攻撃、内部からのインシデント、パートナーや第三者が関与する攻撃/インシデントの割合は 79%。
- Cisco Secure Firewall と Firewall Management Center は、従来型の ASA ファイアウォールによってカバーされていた侵害リスクの割合と比較して、侵害のリスクを 80%低減。
- Cisco Secure Firewall と Firewall Management Center は、これまで FTD ベースのファイアウォールでカバーされていた侵害リスクの割合と比較して、侵害のリスクを 15%低減。
- モデル組織の従業員の 66%は、各侵害によって影響を受け、Cisco Secure Firewall と Firewall Management Center による侵害リスクの低減によって、70%の生産性を回収。
- 一般従業員の全経費込み時間給は 40 ドルです。

リスク。 次の場合によって、重大なセキュリティ侵害のリスクの低減率が異なる場合があります。

- 現在経験している年間の重大なセキュリティ侵害の件数。
- 重大なセキュリティ侵害が発生した場合の、内部および外部のコストの合計。
- 外部からの攻撃、内部からのインシデント、およびパートナーや第三者が関与した攻撃/インシデントの割合。
- 既存のファイアウォールの種類と数。
- 重大なセキュリティ侵害によって影響を受ける従業員の数、全経費込み時間給、そしてこれらの重大なセキュリティ侵害が減少したときの生産性回復能力。

結果。 これらのリスクを反映させるため、Forrester はこの利益を 15%下方修正し、3 年間のリスク調整後の総 PV は約 350 万ドルとしました。

重大なセキュリティ侵害のリスクと生産性低下の低減					
基準	**評価項目**	**ソース**	**1 年目**	**2 年目**	**3 年目**
C1	重大なセキュリティ侵害の平均件数	Forester research	3	3	3
C2	重大なセキュリティ侵害 1 件あたりの平均コスト	Forrester Research	968,480 ドル	968,480 ドル	968,480 ドル
C3	外部からの攻撃、内部からのインシデント、およびパートナーや第三者が関与した攻撃/インシデントの割合。	インタビュー	79%	79%	79%
C4	ASA から Firepower に移行した組織の割合	モデル組織	33%	33%	33%
C5	Firepower によるリスク低減率	インタビュー	80%	80%	80%
C6	初期の Firepower からアップグレードした Firepower に移行した組織の割合	モデル組織	67%	67%	67%
C7	Firepower のアップグレードによるリスク低減率	インタビュー	15%	15%	15%
C8	SecureX によるさらなる削減率	インタビュー	14%	18%	23%
C9	小計：侵害リスクの低減	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	1,162,951 ドル	1,254,763 ドル	1,369,528 ドル
C10	各侵害の影響を受けたユーザー数	Forrester Research	10,600	10,600	10,600
C11	一般社員の全経費込の平均時給	モデル組織	40 ドル	40 ドル	40 ドル
C12	生産性向上率	モデル組織	70%	70%	70%
C13	小計：侵害リスク低減による生産性向上	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8	356,397 ドル	384,534 ドル	419,705 ドル
Ct	重大なセキュリティ侵害や生産性低下のリスク低減	C9+C13	1,519,348 ドル	1,639,297 ドル	1,789,232 ドル
	リスク調整	↓15%			
Ctr	重大なセキュリティ侵害のリスクと生産性損失の低減（リスク調整済み）		1,291,446 ドル	1,393,402 ドル	1,520,848 ドル
	3 年間合計：4,205,696 ドル		**3 年後の現在価値：3,468,249 ドル**		

従業員の生産性を向上させるパフォーマンス面の利益

エビデンスとデータ。 Cisco Secure Firewall は、1) アプリケーションレベルの可視化と制御によるネットワークパフォーマンスの向上、2) ポリシー更新によるダウンタイムの低減という 2 つの手段により、インタビューした組織の従業員の生産性を幅広く向上させることができました。

Cisco Secure Firewall は、アプリケーション層でネットワークアクセスを制御できるため、導入後にネットワークのパフォーマンスが低下することが少なくなったとインタビュー回答者は述べています。以前は、特定のアプリケーション、特にビデオメディアに関連するアプリケーションからの要求が高い場合、ネットワークが頻繁に遅くなり、従業員の生産性に影響を与えるほどパフォーマンスが低下することがあったとの指摘もありました。教育機関のセキュリティオペレーションチームリーダーは、次のように話しています。「ネットワークは毎日著しく速度が低下していましたが、数週間に一度は生産性に影響を与えるほどでした。これは、何千人ものユーザーがビデオを見るなど、アクティビティが急激に増加したときに起こることがほとんどでした。」

Cisco Secure Firewall は、アプリケーション層を含む複数のレイヤーでネットワークセキュリティのポリシーを設定できるため、インタビューした組織は、ネットワークの許可をより細かく制御することができました。その結果、これらの企業は、特定のアプリケーションがいつ、どのようにネットワークにアクセスするかをよりよく制御できるようになり、広帯域のアプリケーションによるネットワークの過負荷を防ぎ、ネットワークのパフォーマンスを向上させ、従業員の生産性を高めることができるようになりました。

「Cisco Secure Firewall のおかげで、ネットワークがどのように使用されているかが非常によく見えるようになり、この使用を制御することができるようになりました。現在、4,000 台の異なるシステムを監視しており、その気になれば、（動画ベースの人気ソーシャルアプリが）先週どれだけ使われたかを確認できます。必要であれば、この種のトラフィックを許可しないようなルールを設けることもできます。」と述べました。
教育機関のセキュリティオペレーションチームリーダー

他のインタビュー回答者は、自社がポリシー更新の人為的ミスによって生じることがある悪影響を制限することにより、従業員の生産性を向上させたと述べています。例えば、IT サービス企業のエンジニアリングサービスマネージャーは、Firewall Management Center ではポリシーの作成と更新が非常に速くなったため、更新がうまくいったかどうかのフィードバックも速くなったと述べています。

この会社が Secure Firewall を導入する前は、ポリシーの更新に 15 分、正しく設定されているか確認するのにさらに 15 分かかっていました。正しく設定されていない場合、2 回目のポリシー更新のために、さらに 15 分もかかってしまいます。特に生産現場では、誤ったポリシーの更新が、従業員の生産性に悪影響を及ぼすこともありました。

Cisco Secure Firewall を搭載した FTD の最新バージョンにアップグレードした後、エンジニアリング サービス マネージャーは、ポリシーの更新とフィードバックの時間を送信 3 分、受信 3 分に短縮したところ、更新、フィードバック、トラブルシューティングの合計時間が 60 分から 12 分に 80%短縮されたことを指摘しました。

モデリングと想定。 モデル組織について、Forrester は以下のモデルを設定：

- 誤って更新されたポリシーの修正に丸 1 時間かかっていた（誤更新の送信に 15 分、フィードバックを受けるのに 15 分、修正後の更新とフィードバックの受信に 30 分）。
- Cisco Secure Firewall と Firewall Management Center は、誤ったポリシーの修正にかかる時間を 80%削減。
- 誤ったポリシーの更新によって影響を受けるのは、平均で組織の 2%と想定。
- 以前は、2 週間に 1 回、20 分程度、従業員の生産性に影響を与える深刻なネットワーク障害が発生していた。
- 従来の ASA ファイアウォールがカバーしていた 33%の従業員が、ネットワーク劣化の影響を受けた。

リスク。 従業員の生産性に対するパフォーマンス面の利益は、以下により異なる場合がある：

- 誤ったポリシーの更新により影響を受けた従業員の割合。
- 従業員の生産性に影響を与えるネットワークの劣化の頻度と長さ。
- ネットワークの劣化により影響を受けた従業員の数。

結果。これらのリスクを加味したうえで、Forrester はこの便益を 10%下方調整し、リスク調整された 3 年間の総額 PV をおよそ 410 万ドルとしました。

従業員の生産性を向上させるパフォーマンス面の利益

基準	評価項目	ソース	1 年目	2 年目	3 年目
D1	早期 FTD に伴うポリシー調整に事前にかかる時間	インタビュー	1	1	1
D2	FTD の更新に伴い、ポリシーを調整するために新規にかかる時間	インタビュー	0.2	0.2	0.2
D3	影響を受けた平均従業員数	モデル組織	320	320	320
D4	一般社員の全経費込の平均時給	C10	40 ドル	40 ドル	40 ドル
D5	生産性の回収率	モデル組織	25%	25%	25%
D6	小計：ポリシーフィードバックによる生産性向上	365*(D1-D2)*D3*D4*D5	934,400 ドル	934,400 ドル	934,400 ドル
D7	ネットワーク不正利用による性能低下の頻度	インタビュー	26	26	26
D8	性能低下の平均時間（時間）	インタビュー	0.33	0.33	0.33
D9	影響を受ける従業員数（ASA 移行のみ）	モデル組織	5,280	5,280	5,280
D10	一般社員の全経費込の平均時給	C11	40 ドル	40 ドル	40 ドル
D11	生産性の回収率	モデル組織	50%	50%	50%
D12	小計：エンドユーザー従業員の生産性向上	D7*D8*D9*D10*D11	906,048 ドル	906,048 ドル	906,048 ドル
Dt	従業員の生産性を向上させるパフォーマンス面の利益	D6+D12	1,840,448 ドル	1,840,448 ドル	1,840,448 ドル
	リスク調整	↓10%			
Dtr	従業員の生産性を向上させるパフォーマンス面の利益（リスク調整済み）		1,656,403 ドル	1,656,403 ドル	1,656,403 ドル
	3 年間合計：4,969,210 ドル		**3 年後の現在価値：4,119,230 ドル**		

先行ソリューションの削減/回避コスト

エビデンスとデータ。Cisco Secure Firewall の最新バージョンにネットワークセキュリティインフラを移行することで、インタビューした組織は、レガシーネットワークインフラに関連するコストを削減・回避することができました。当然ながら、インタビュー回答者は、Cisco Secure Firewall がこれらに取って代わったため、従来の ASA ベースのファイアウォールと初期の FTD ベースのファイアウォールの再ライセンスにかかるコストを回避できました。

物理ファイアウォールや仮想ファイアウォールの切り替えに加え、ASA ベースの環境から切り替えた組織では、Cisco Secure Firewall に IPS が含まれているため、スタンドアロンの IPS ソリューションを廃止しています。

「従来型の ASA ファイアウォールでは、リンクとファイアウォールの間に設置する IPS ユニットへの投資も必要でした。Cisco Secure Firewall では、IPS が組み込まれています。2 つのエコシステムを持つ 2 つの異なるソリューションを管理する必要がなくなりましたし、IPS のエンジニアに頼ることもなくなりました。」
テクノロジー企業のネットワークエンジニアリング担当シニアマネジャー

重要なことに、インタビュー回答者は、組織のファイアウォールを初期の FTD から Cisco Secure Firewall にアップグレードすることでさらに節約できることに気付きました。これらの最新のファイアウォールは効率的であるため、同じ結果を得るために必要なファイアウォールは 20%から 25%少ないと述べています。

「Cisco Secure Firewall の初期の FTD から最新の FTD に移行したところ、処理効率が向上しました。Cisco Secure Firewall は、以前のバージョンと比べて 20%から 25%効率が向上しており、必要なファイアウォールの数が少なくて済むということです。」
インターネット事業者のシニアネットワークエンジニア

モデリングと想定。モデル組織について、Forrester は以下のモデルを設定:

- 従来の ASA ファイアウォールを Cisco Secure Firewall に切り替えることで、スタンドアロン IPS のライセンスコストが年間 171,600 ドル削減。
- 単体 IPS の保守コストをライセンス料の 20%相当分回避。
- IPS に関連する継続的な管理コストの 80%（2FTE、週 30 分）を削減。
- 1 年目に 130 万ドル以上の既存ファイアウォールを同タイプのものに交換するコストを回避。
- 年間 30 万ドルの仮想ファイアウォールの交換コストを回避。
- Cisco Secure Firewalls の効率性により、物理的なファイアウォールの追加コストを 25%回避。

「Cisco Secure Firewall の導入に伴い、コストが高く性能の低い IPS アプライアンスをようやく廃止させることができました。」
金融機関のリードインフラエンジニア

リスク 以下によって、レガシーソリューションのコスト削減が異なります。

- 既存のファイアウォールの数および種類。
- スタンドアロン IPS ソリューションの廃止が可能。

結果。これらのリスクを考慮したうえで、Forrester はこの利益を 10%下方調整し、調整された 3 年間の総額の PV をおよそ 260 万ドルとしました。

レガシーソリューションの廃止によるコスト削減

基準	評価項目	ソース	1 年目	2 年目	3 年目
E1	レガシーIPS のコスト削減	インタビュー	171,600 ドル	171,600 ドル	171,600 ドル
E2	保守のコスト削減	E1*20%	34,320 ドル	34,320 ドル	34,320 ドル
E3	レガシーIPS の継続的な管理コストを削減	インタビュー	53,539 ドル	53,539 ドル	53,539 ドル
E4	ファイアウォールの交換サイクルにかかるコストを削減	モデル組織	1,616,980 ドル	300,000 ドル	300,000 ドル
E5	ファイアウォールの効率化でコストを削減	モデル組織	329,245 ドル	0 ドル	0 ドル
Et	レガシーソリューションの廃止によるコスト削減	E1+E2+E3+E4+E5	2,205,684 ドル	559,459 ドル	559,459 ドル
	リスク調整	↓10%			
Etr	レガシーソリューションの廃止によるコスト削減（リスク調整済み）		1,985,115 ドル	503,513 ドル	503,513 ドル
	3 年間の合計：2,992,142 ドル		**3 年間の現在価値：2,599,074 ドル**		

非定量的利益

この他に、定量化されていないものの、顧客企業で認められたメリットは以下の通りです。

- **VPN の生産性とセキュリティの強化。**Cisco Secure Firewall によって、リモートアクセス VPN の生産性とセキュリティも向上したとインタビュー回答者は指摘しています。ロードバランシング機能により、グループ化されたデバイス間でセッションを分散し、パフォーマンス、回復力、エンドユーザーの生産性を提供します。同様に、Secure Firewall によるローカル認証では、リモートの AAA サーバーにアクセスできなくなった場合でも、ユーザーの生産性を維持することができました。セキュリティ面では、Cisco Secure Firewall はマルチ証明書認証が可能なため、企業はエンドユーザー自身の認証に加え、リモートデバイスが企業発行のものであることを確認することができます。
- **コンプライアンスの改善。**また、Cisco Secure Firewall と Firewall Management Center が、コンプライアンスワークフローに定量化できない利益をもたらしていることも、インタビュー回答者は指摘しています。金融機関のリードインフラエンジニアは、Secure Firewall と FMC を導入する前は、コンプライアンスに関するレポート作成が困難であったと話しています。以前のソリューションでは、簡単にレポート作成する機能がありませんでした。しかし、Secure Firewall と FMC を使うことで、より包括的なコンポーネントと、アクティビティやビューに関してより詳細なレポートを実行することが可能になりました。また、Cisco Secure Firewall が TLS 1.3 暗号化規格をサポートしていることについても、インタビュー回答者は指摘しています。例えば、インターネット事業者のシニアネットワークエンジニアは、管理負担が大きいため、現在そのようなフローの復号化は行っていないと述べています。Cisco Secure Firewall に投資してからは、TLS 1.3 の復号化が容易になり、効率的になりました。

「以前は、さまざまな構成要素を網羅するレポートがありませんでしたが、今ではより簡単に広範囲かつ詳細なレポートを得ることができます。例えば、過去 1 年間に行ったアクセスコントロールの全変更履歴レポートを手にしたばかりです。すべてのページビューの出力と、その変更点が表示されます。」
金融サービス企業のリードインフラストラクチャエンジニア

- 従業員**体験の向上。**インタビュー回答者は、自分たちの組織の従業員体験が改善されたことも指摘しています。例えば、インターネット会社のシニアネットワークエンジニアはこのように語っています。「ネットワーク上のアプリケーションへのアクセスをより適切に制御できるようになったことで、従業員の満足度が向上しました。以前は、現地の IT チームがユーザーを追跡して、特定のアプリの使用停止を求めたり、アクセスをブロックしたりするのに苦労していました。セキュアファイアウォールと FMC を使うことで、リモートでできるようになりました。」

柔軟性

柔軟性の価値は、お客様ごとに異なります。お客様が Secure Firewall を導入したシナリオは、次のように複数存在し、追加の使用やビジネスチャンスを後で実現する場合もあります。

- **Cisco Security の追加統合。** SecureX の利点に加えて、インタビュー回答者は、Cisco のセキュリティ製品のエコシステムが、組織のセキュリティ体制をさらに強化する柔軟性を提供していることを指摘しています。例えば、IT サービス企業のエンジニアリングサービスマネージャーは次のように話しています。「Cisco Security は、他のベンダーが苦手とする、統合セキュリティソリューションの深いスタックを備えています。Secure Firewall だけでなく、他のすべてのパーツがうまく統合され、より良い防御を構築することができます。」
- **在宅勤務の業務効率が向上。**また、在宅勤務への移行に伴い VPN が爆発的に普及した際にも、Cisco Secure Firewall の制御によりスムーズな運用が実現されました。インターネット企業のシニアネットワークエンジニアは、「パンデミック中、当社の VPN 同時接続数は、世界平均 10 万から 35 万近くまで増加しました。ネットワークの有効性を維持するために、Cisco Secure Firewall を使用して料金制限を設定し、運用をスムーズにしました」と述べています。
- **クラウドへの移行が容易。**最後に、インタビュー回答者は、Cisco Secure Firewall がクラウドイニシアチブの実現を容易にしたことを指摘しました。IT サービス業者のエンジニアリングサービスマネージャーは、次のように述べています。「オンサイト、リモートサイト、そしてクラウドにも対応できる単一のプラットフォームが必要でしたが、導入が簡単であることが条件でした。クラウドプラットフォームでは、FTD ボックスをドロップして、その場でインストールし、Firewall Management Center に接続するだけです。セットアップから導入まで、まったく時間がかかりませんでした。そして、そのまま標準的なポリシーをプッシュできます。」

柔軟性は特定プロジェクトの一環として評価すれば定量化できます（詳細は付録 A を参照）。

コスト分析

モデル組織に適用される定量的コストデータ

総コスト

基準	コスト	当初	1 年目	2 年目	3 年目	合計	現在価値
Ftr	ライセンスコスト	6,000,690 ドル	0 ドル	0 ドル	0 ドル	6,000,690 ドル	6,000,690 ドル
Gtr	実装、ポリシー作成、トレーニングのコスト。	278,220 ドル	7,924 ドル	7,924 ドル	7,924 ドル	301,990 ドル	297,924 ドル
	総コスト（リスク調整済み）	6,278,910 ドル	7,924 ドル	7,924 ドル	7,924 ドル	6,302,680 ドル	6,298,614 ドル

ライセンスコスト

エビデンスとデータ。 お客様は、Secure Firewall への投資に関連して、以下のような複数の異なるコストを負担していました。

- 物理的なファイアウォールのコスト。必要なスループットによって異なります。
- データセンターまたはデータセンターに配置され、East-West トラフィックを処理する仮想ファイアウォール。
- Threat Protection、Malware Defense、URL フィルタリングライセンスのコスト。
- Firewall Management Center のライセンス。

「Cisco Secure Firewall が持つアーキテクチャ、ツールセット、機能の深さを 1 つのボックスで実現できる選択肢を他に見つけるのは困難でした。しかし、それに加えて、価格対性能比も説得力がありました。」
金融サービス企業のリードインフラストラクチャエンジニア

Cisco SecureX は Secure Firewall のライセンスに含まれているため、追加コストなしで導入できたとの声をお客様からいただいています。

モデリングと想定。 100 のオフィスと冗長性を必要とする 4 つの物理データセンターを持つモデル組織の場合、Forrester のモデルは次のようになります。

- ライセンスはすべて定価で、有効期間は 3 年間です。
- 本社オフィス用ファイアウォールのコストは 328,443 ドルです。企業のオフィスでは、最大 75Gbps のスループットを持つ、エンタープライズクラスの大型ファイアウォールを必要としています。
- データセンター用ファイアウォールのコストは 978,067 ドルです。各データセンターで、コンポジットはデータセンターの境界クラスタリングまたは 2 つの物理ファイアウォールの高可用性バンドルを展開して、データセンターに出入りする基幹トラフィックを処理します。
- 仮想ファイアウォール 100 台のコストは 2,628,561 ドルです。これらの仮想ファイアウォールは、データセンター内の East-West トラフィックと、データセンターとパブリッククラウドプラットフォームの間のトラフィックを処理します。
- データセンターの物理ファイアウォールと仮想ファイアウォールには、すべて 3 年間のサブスクリプション料金で Threat Protection のライセンスが追加されています。これにより、

侵害の指標や悪意のあるトラフィックをより適切に検出/軽減する Snort 3 を含む、さらなるセキュリティが提供されます。

- 60 台の支店用ファイアウォールの総コストは 1,848,160 ドルです。60 か所のオフィスでは、最大 1.9Gbps のスループットを持つセキュアファイアウォールを必要としています。
- 39 台の小規模支店用ファイアウォールの総コストは 137,779 ドルです。残りの 39 か所のオフィスは、最大 650Mbps のスループットしか必要としませんでした。
- すべてのオフィス用ファイアウォールに、Threat Protection、Malware Defense、URL フィルタリングライセンスを 3 年間のサブスクリプション料金で追加することができます。
- Firewall Management Center も、これらすべてのファイアウォールを扱うのにふさわしいサイズでライセンスされています。Firewall Management Center の価格は、79,680 ドルです。

リスク Cisco Secure Firewall と Firewall Management Center のライセンスコストは、以下によって異なります。

- 希望する仮想ファイアウォール台数。
- エンタープライズグレードのファイアウォールの必要台数。
- データセンターの規模や数、高可用性の必要性。
- 支店の規模や数。

結果。Forrester はモデル組織の価格を Cisco と直接比較しているため、このコストをリスク調整せず、3 年間の総 PV（10%で割引）は 600 万ドルとしました。

「Cisco のエンタープライズセキュリティの契約により、個別で購入するよりもトータルコストが安くなりました。Firepower がそのコストの大部分を占めていますが、以前は持っていなかった製品で追加の保護を受けることで、何十万ドルも節約できています。」
教育機関のセキュリティオペレーションチームリーダー

ライセンスコスト

基準	評価項目	ソース	当初	1 年目	2 年目	3 年目
F1	仮想ファイアウォールのコスト	Cisco	2,628,561 ドル			
F2	企業内ファイアウォールのコスト	Cisco	328,443 ドル			
F3	データセンターの物理ファイアウォールのコスト	Cisco	978,067 ドル			
F4	小規模支社向けファイアウォールのコスト	Cisco	137,779 ドル			
F5	大規模な支店のファイアウォールのコスト	Cisco	1,848,160 ドル			
F6	ファイアウォール管理センターコスト	Cisco	79,680 ドル			
Ft	ライセンスコスト	F1+F2+F3+F4+F5+F6	6,000,690 ドル	0 ドル	0 ドル	0 ドル
	リスク調整	0%				
Ftr	ライセンスコスト (リスク調整済み)		6,000,690 ドル	0 ドル	0 ドル	0 ドル
	3 年間合計: 6,000,690 ドル			**3 年間の現在価値: 6,000,690 ドル**		

実施、ポリシー作成、トレーニングのコスト

エビデンスとデータ。 また、インタビュー回答者はデータセンターやオフィスへのファイアウォールの導入・実装に伴う社内の時間的・労力的コストが生じていると指摘しています。まず、物理的に各拠点にファイアウォールを配備するコストが発生しました。2 つ目は、ファイアウォールの実装で、それぞれのファイアウォールに適切なポリシーを作成し、展開することです。

「導入と展開が本当に早く、比較的簡単でした。実際の切り替えは、すでに設計が終わっていて、すべての電源を入れる方法がわかっていたため、3 週間で完了しました。」
教育機関のセキュリティオペレーションチームリーダー

最後に、意思決定者へのインタビューでは、トレーニングにかかる時間的なコストも指摘されました。Cisco Secure Firewall を導入・管理するためのトレーニングが必要な従業員は、2 時間程度で終了しました。また、一部のインタビュー回答者の中には、Cisco のセキュリティ専門家が出演する一般公開のトレーニングビデオを活用しているとの意見もありました。

モデリングと想定。 モデル組織について、Forrester は以下のモデルを設定:

- 2 つのデータセンターと 100 のオフィスそれぞれで平均 6 時間の導入時間が必要。
- ポリシー作成には、ファイアウォール 1 台あたり平均 30 時間かかる。
- SecureX の導入には先行投資として 20 時間、継続的な管理には年間 100 時間の作業が必要。
- 当初は 15 人の従業員がトレーニングを必要としており、従業員の入れ替わりにより毎年 3 人が追加でトレーニングを必要とする。

リスク。 以下の項目によって、導入や施策の作成にかかるコストは異なります。

- 配備する Cisco Secure Firewall の数。
- 最初にトレーニングが必要な従業員の数。
- 従業員の離職率。
- NetSecOps の専門家の完全負担の時給です。

結果。 これらのリスクを反映させるため、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 PV は 298,000 ドル以下となりました。

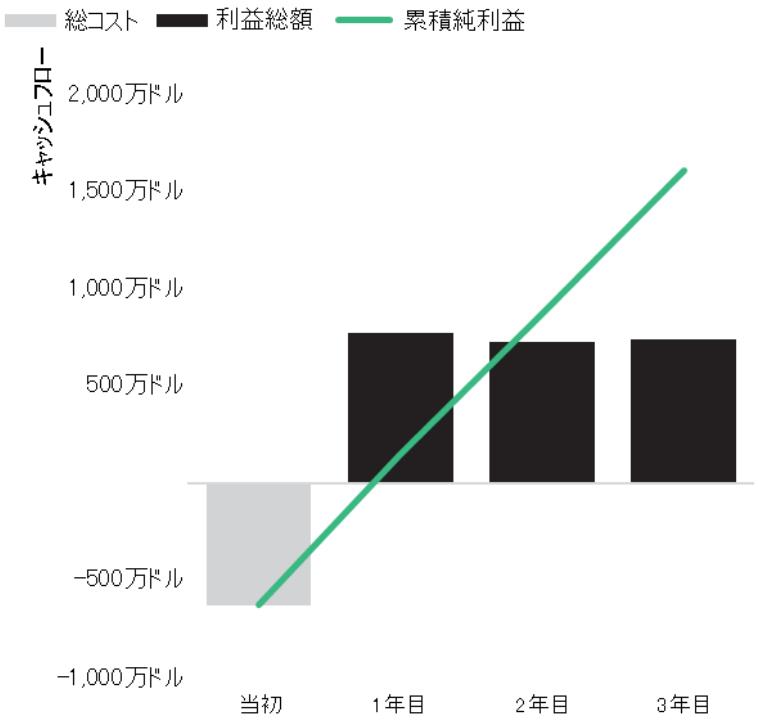
実施、ポリシー作成、トレーニングのコスト

基準	評価項目	ソース	当初	1 年目	2 年目	3 年目
G1	展開する拠点	モデル組織	102			
G2	各サイトの物理的な実装にかかる平均時間	モデル組織	6			
G3	ポリシー作成のための時間	インタビュー	30			
G4	SecureX の導入・運用にかかる時間	インタビュー	20	100	100	100
G5	トレーニングを必要とする従業員	インタビュー	15	3	3	3
G6	トレーニングに必要な時間	インタビュー	2	2	2	2
G7	NetSecOps 専門家の全経費込み平均時給	A5	65 ドル	65 ドル	65 ドル	65 ドル
Gt	実施、ポリシー作成、トレーニングのコスト	((G1*(G2+G3))+,G4+(G5*G6))*G7	241,930 ドル	6,890 ドル	6,890 ドル	6,890 ドル
	リスク調整	↑15%				
Gtr	実行、ポリシー作成、トレーニングのコスト（リスク調整済み）		278,220 ドル	7,924 ドル	7,924 ドル	7,924 ドル
3 年間の合計：301,990 ドル			**3 年後の現在価値：297,924 ドル**			

財務状況概要

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（リスク調整済み）



「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、このモデル企業の投資に対する ROI、NPV および回収期間を決定できます。Forrester は、この分析で年 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**、**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（リスク調整済み推定値）

	当初	1 年目	2 年目	3 年目	合計	現在価値
総コスト	（6,278,910 ドル）	（7,924 ドル）	（7,924 ドル）	（7,924 ドル）	（6,302,680 ドル）	（6,298,614 ドル）
利益総額	0 ドル	7,737,795 ドル	7,264,360 ドル	7,391,805 ドル	22,393,959 ドル	18,591,534 ドル
純利益	（6,278,910 ドル）	7,729,871 ドル	7,256,436 ドル	7,383,881 ドル	16,091,279 ドル	12,292,920 ドル
投資利益率（ROI）						195%
回収期間（月）						10

付録 A：Total Economic Impact（TEI、総経済効果）

Total Economic Impact は、Forrester Research が開発した手法であり、企業の技術関連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を顧客に提案するための支援を行います。TEI 手法を使用することで、企業は上級管理職やその他のビジネス上の主要な利害関係者に対して、IT イニシアチブの具体的な価値を説明し、根拠を示した上で実現に役立てることができます。

TOTAL ECONOMIC IMPACT の手法

利益とは、製品がビジネスにもたらす価値を意味します。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。

コストでは、製品の価値、つまり利益を提供するために必要なすべての経費が考慮されます。TEI のコスト区分は、ソリューションに関連する継続的なコストについて、既存環境からの増分コストを含んでいます。

柔軟性とは、すでに行われた当初投資の上に構築される、将来の追加投資で取得できる戦略的価値のことです。その利益を享受できる能力があるとは、見積もり可能な PV（現在価値）があることを意味します。

リスクとは、利益とコストの見積もりの不確かさを測定したもので、1) 見積もりが初期の予想に見合う可能性と、2) 時間の経過と共に見積もりが追跡される可能性が考慮されます。TEI ではリスク因子は「三角分布」に基づいています。

当初投資の欄には、「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。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には、年度末の割引率が適用されます。現在価値（PV）は、それぞれの総コストおよび利益の見積もりに対して計算されます。サマリーテーブルの正味現在価値（NPV）は、当初投資と各年の割り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の合計金額および現在価値については、四捨五入のため合計値が合わ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）コストおよび利益見積もりの現在価値。コストおよび利益の現在価値（PV）は、キャッシュフローの総正味現在価値（NPV）に適用されます。

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。プロジェクトの正味現在価値（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、通常は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

金銭の時間的価値を考慮するために、キャッシュフロー分析で使用される利率。通常、企業は 8%～16%の割引率を使用します。

回収期間

投資の損益分岐点です。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。

付録 B: 後注

[1] Total Economic Impact 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強化し、ベンダーが自社の製品やサービスの価値を顧客に伝えることを支援するものです。TEI 手法を使用することで、企業は上級管理職やその他のビジネス上の主要な利害関係者に対して、IT イニシアチブの具体的な価値を説明し、根拠を示した上で実現に役立てることができます。


FORRESTER®