



 CROWDSTRIKE

COMPLETEの  
全体像を把握：新  
しい調査により完  
全マネージド型検  
知・対応サービスに  
の利点が明らかに



「多数のサービスを見てきましたが、中でも、Falcon Completeは最も包括的なセキュリティモデルです。」 – CISO, Building Products, Inc.

サイバーセキュリティへの投資からこういった利点が得られていますか？ その内容は対価に見合っていますか？

答えに窮する質問です。セキュリティが目に見えて収益を上げるということは滅多にありません。むしろ、その価値は発生しなかったセキュリティ侵害、被害がなかったことで免れた出費、組織が負担しなかった機会費用等の観点から考えなければなりません。

これに対し、サイバーセキュリティのコストはすべて極めて現実的です。技術ライセンスなどの明確な出費だけでなく、技術の保守や運用に要する人員、隠れて実行される攻撃を特定する脅威ハンター、監視と対応を担うアナリストなどの隠れたコストも含まれます。他にも、エンドユーザーに発生するダウンタイムのコスト、重大な侵害インシデントへの対応にかかる数百万ドルにもものぼる可能性のある出費もあります。

CrowdStrikeの委託を受け、Forrester Consultingは、こうした問題を調査しました。「**The Total Economic Impact™ of CrowdStrike Falcon Complete** (CrowdStrike Falcon Completeに関するTotal Economic Impact™)」と題するこの包括的な調査では、Forresterが、市場を定義するCrowdStrikeの**マネージド型検知・対応(MDR)**アプローチについて、そのコストと利点のすべてを初めて明らかにしています。

このForresterの調査により、CrowdStrikeのMDRソリューションである**Falcon Complete™**が、侵害を阻止し、隠れたコストなくして400%を越える投資収益率(ROI)を実現したことが示されました。では、ForresterのTotal Economic Impact (TEI) メソドロジーを確認して、この結果についてひもといてみましょう。



**CROWDSTRIKE**

**FORRESTERの  
調査により確認された  
FALCON COMPLETE  
が提供するもの：  
403%の投資収益率  
100%の自信**

「Falcon Completeは私が見た中では間違いなく最高の製品です。絶対の自信があります。」 – Senior Director for Security Operations, Pharmaceuticals

## FORRESTER TEIメソドロジー

この調査において、ForresterはFalcon Complete製品を利用するさまざまな企業のセキュリティリーダーに聞き取り調査を行いました。対象となった組織は、さまざまな規模（ユーザー規模700人から22,500人）、そして世界の地域（北米からヨーロッパ、オーストラリアまで）を代表する組織が選ばれました。いずれも聞き取り調査の時点でFalcon Completeを1年以上使用しているお客様です。

これらの組織が共通して報告したのは、「セキュリティチームには膨大な量の仕事があるものの、それを処理する人手は不足している」というものでした。回答したリーダーらは、常にフルスピードで走ることを余儀なくされていることから、次の侵害を阻止するのに十分な対策ができていないのではないかと常に危惧しており、こうした状況について非常にリスクが高いと認識していました。またアラートを処理するという喫緊の使命にすべての労働力を集中させているため、組織は行き詰まりを感じており、戦略的イニシアチブと改善に集中することができていませんでした。

Forresterは、聞き取り調査中に収集したデータに基づいて、「典型的な」モデル組織を構築し、聞き取り調査の実際のデータを使用して財務モデルを構築し、Falcon Completeのコスト、利点、ROIを定量化しています。

## FORRESTERが定量化したFALCON COMPLETEの利点

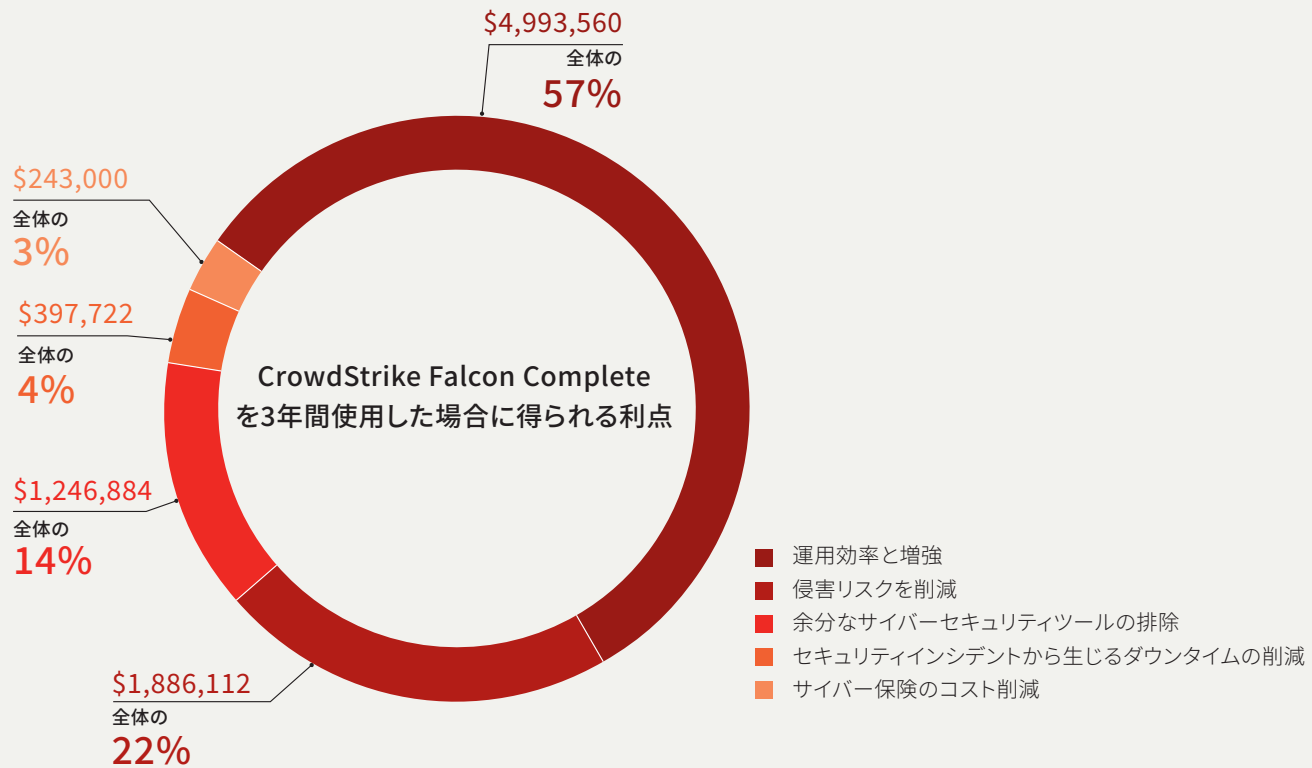


図1.CrowdStrike Falcon Completeを3年間使用した場合に得られる利点

Falcon Completeを使用する多様なお客様の聞き取り調査をとおして、ForresterはFalcon Completeの使用により組織にもたらされる5つの異なる利点を測定しました：

- 運用効率と増強。Forresterは、Falcon CompleteがFTEベースで11人の経験豊富なチームと同等のカバレッジを提供し、24時間体制の監視、対応、脅威ハンティングを提供したと評価しました。これは、組織にとって変化の契機となりました – アラート疲れをなくし、セキュリティチームの人手不足のプレッシャーを大幅に緩和しました。
- 侵害リスクを大幅に削減。Forresterの分析では、Falcon Completeチームによるプロアクティブな管理、チューニング、そしてCrowdStrikeの侵害防御保証の組み合わせにより、ほぼ完全に侵害リスクがなくなったことが示されました。
- 余分なサイバーセキュリティツールの排除。CrowdStrikeは、保護とパフォーマンスを強化し、他の複数の冗長セキュリティツール（およびそれらを管理する負担）に代わることで、コストを削減しました。

- セキュリティインシデントから生じるダウンタイムの削減。セキュリティインシデントへの対応は、すでに多忙なITスタッフに負担をかけるだけでなく、エンドユーザーにも影響を及ぼしていました。Forresterの調査により、Falcon Completeの実装後、組織に発生するセキュリティインシデント件数が減り、IT部門やユーザーが脅威に対処する時間が大幅に削減されたことが示されました。さらに、セキュリティインシデントの影響は、手間のかかる再イメージングや侵害されたエンドポイントの交換に頼るのではなく、数分で完全な修復を実行するFalcon Completeの機能によって大幅に削減されました。
- サイバー保険のコスト削減。最後に、複数の回答者から報告されたとおり、Falcon Completeチーム独自の専門知識およびCrowdStrikeの侵害防止保証に裏打ちされたCrowdStrike Falcon®プラットフォームの効果は他に類を見ず、サイバー保険業者からより好ましい条件を獲得してコスト削減につながる可能性があります。

## しかし、それだけではありません...

Forresterは、定量化された利点に加えて、調査に参加したセキュリティリーダーより説明のあった、定量化されないさまざまなメリットも挙げました。

「Falcon Complete製品、そして製品が提供する快適さとセキュリティにより、チームは他の大規模プロジェクトに集中できるようになります。」

「...他のことにフォーカスできます... (Falcon Completeが) 支えてくれますから。」

Falcon Completeにより、組織は、サイバーセキュリティチームの重要なリソースを確保して、エンドポイント保護の管理とセキュリティアラートへの対応というリソースを大量に消費する事後対応的な作業ではなく、戦略的な優先事項に集中できるようになります。

「Falconの修復能力と対応能力に完璧な自信を持っています。」

「...夜だいたい良く眠れるようになります...」

調査を受けた組織は、防御について不安を感じ、十分な保護対策ができていないか常に疑問に思っていたと語っていますが、Forresterは、Falcon Completeがこの不確実性を解消し、組織が防御に対する自信と信頼を獲得できるようになったと報告しています。

「実際のオンボーディングは驚くほど簡単で、対応してくれたチームは非常に付き合いやすい人たちでした。」

その上、導入に時間はかかりませんでした。聞き取り調査を受けた組織は、Falcon Completeにサインアップしてから、Falconプラットフォームが展開され、ベストプラクティスに従って構成され、Falcon Completeチームの監視下で完全に稼動するまでにかかった時間は平均して2週間であったと報告しています。

# 侵害ゼロ、隠れたコストゼロ

「Falcon Completeの欠点を探そうとしているんですが、印象が変わるようなことを挙げるのは、難しいですね。」

当然、無料のものはないため、どのソリューションにもコストが伴います。本調査を通じて、Forresterはエンドポイント保護のライフサイクル全体にわたってセキュリティチームが負担したコストを細かく追跡しました。これには、以下に関連するコストが含まれます：

- 必要なエンドポイント保護技術の調達と実装
- 24時間365日体制のグローバル監視と管理
- 24時間365日体制のプロアクティブ脅威ハンティング
- セキュリティアラートの監視と対応
- インシデントに巻き込まれたシステムの完全な修復と復旧
- 継続的なプラットフォームの管理、保守、チューニング

Forresterは、これらの包括的なコストを組織が実現した実際の利点と比較して、Falcon Completeが驚異的な403%のROIを実現すると算出しました。

さらに重要なのは、聞き取り調査に参加した組織のいずれもCrowdStrike Falcon Completeを導入してから、大きな影響を伴う侵害を報告していないという点です。Falcon Completeは社内でも機能を構築するよりもはるかに低コストで、予測可能なセキュリティ結果を実現しました。

## サプライズはなし

Forresterの調査は、当社のFalcon Completeチームが長年主張してきたことを検証するものであると考えます。「エンドポイント保護」とは実現困難なものではなく、合理的で予測可能なコストで実現できるものです。注意、集中、そしてきめ細かく調整されたプロセスが必要です。品質の高いMDRサービスなら、すぐにこれらを手にすることができます - そしてビジネスに重要なものにフォーカスを合わせることが可能になります。

追加のリソース

- Forresterの調査「[The Total Economic Impact™ of CrowdStrike Falcon Complete \(CrowdStrike Falcon Completeに関するTotal Economic Impact™\)](#)」を読む
- Falcon Completeの動作をデモで確認
- 詳細情報：[Falcon Complete white paper \(Falcon Completeのホワイトペーパー\)](#)を読む。