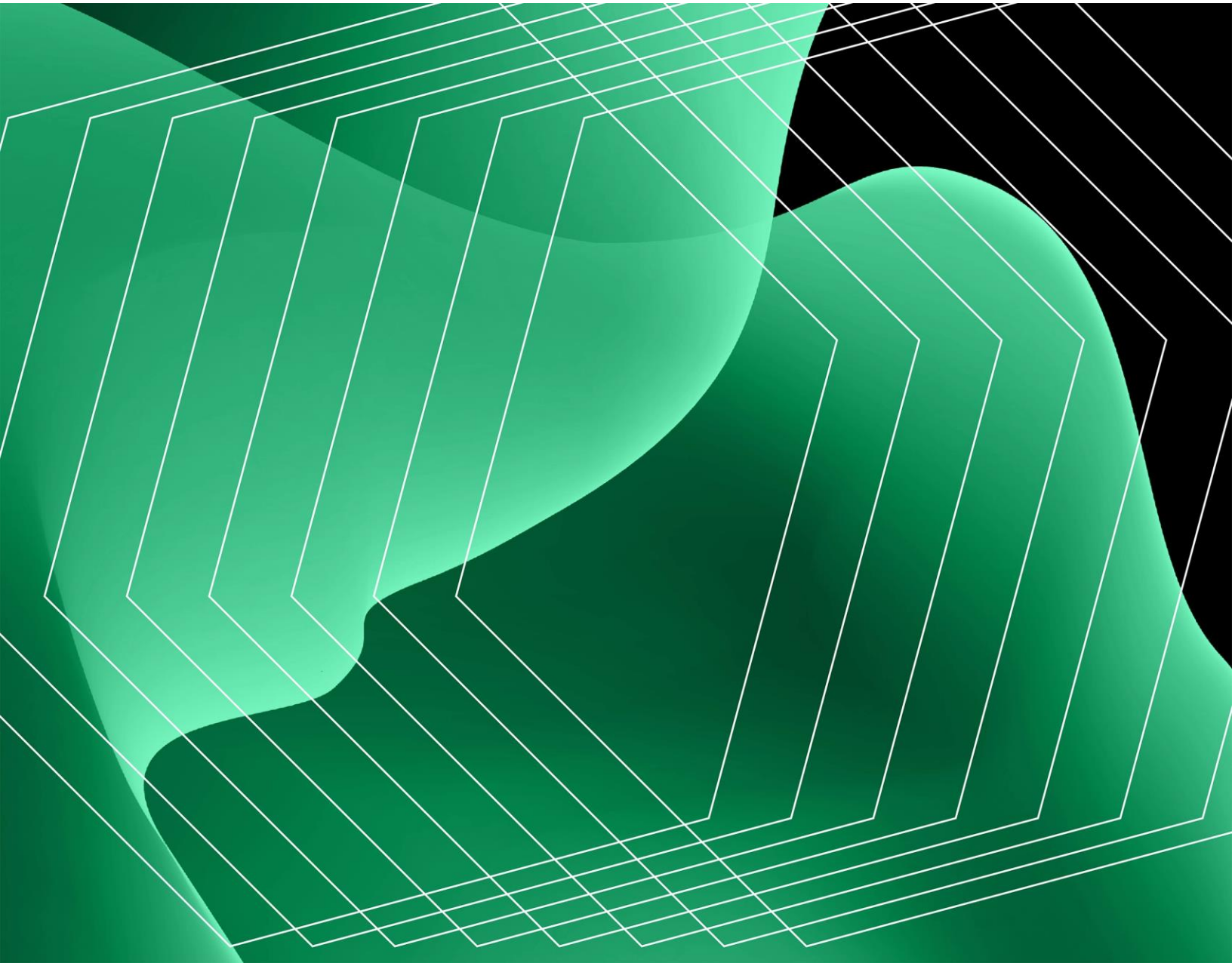
FORRESTER®

Okta Identity Governance の Total Economic Impact™

Identity Governance が可能にするコスト削減とビジネス上の利点

FORRESTER TOTAL ECONOMIC IMPACT™調査（OKTA 委託）2025 年 6 月



目次

コンサルティングチーム:

Kris Peterson

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

あらゆる規模の組織には、アクセスと権限を効果的に管理する積極的なポリシー主導のアプローチが必要です。そうすることで、セキュリティ脅威の増大や SOX や PCI-DSS などの規制の圧力に対応するため、統制、監視、コンプライアンスと、俊敏性とスケーラビリティのバランスを取ることができます。分散したシステムや手作業のプロセスには盲点が生じることが多く、アクセスの付与を遅らせ、過剰に権限を有するユーザーや過剰な報告作業の原因となります。アイデンティティ環境の規模が拡大して複雑化が進むに伴って、組織は、コアとなるアイデンティティインフラストラクチャと統合し、運用効率とリスク軽減を共に支援するガバナンスソリューションを必要としています。

Okta Identity Governance（OIG）は、クラウドベースのアイデンティティガバナンスおよび管理（IGA）ソリューションです。アイデンティティインフラストラクチャと直接統合して、アクセス要求、認証、権限レビュー、ポリシーの実施、レポート作成を一元化および自動化します。手作業によるワークフローをイベント駆動型の自動化と動的なアクセスロジックに置き換えることで、OIG は、組織が最小特権アクセスの強制、プロビジョニングとデプロビジョニングの迅速化、大規模なコンプライアンスの維持を実現しながら、管理労力とアクセスリスクを最小限に抑えるのを支援します。

Forrester Consulting はこの度、Okta の委託により Total Economic Impact™（TEI）調査を実施し、Okta Identity Governance の導入で得られる企業の投資利益率（ROI）を分析しました。[1] 本調査の目的は、Okta Identity Governance によって企業にもたらされる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。

投資利益率（ROI）
211%

正味現在価値
180 万ドル

OIG への投資で得られる利益、発生するコスト、想定されるリスクについての理解を深めるため、Forrester は OIG の使用経験を持つ意思決定者 8 名にインタビュー調査を実施しました。本調査のため、Forrester はインタビュー参加者の経験を集約し、結果を単一のモデル企業（年間収益 15 億ドルのグローバル企業、5,000 のアイデンティティ、100 のアプリケーション、そしてアイデンティティおよびアクセス管理（IAM）、監査サポート、コンプライアンスの担当者 12 人）としてまとめました。

OIG の導入前には、手作業、断片化されたツール、一貫性のないアクセスポリシーに大きく依存していたため、非効率性、人為的ミス、セキュリティの脆弱性が生じていたとインタビュー参加者は述べています。これまでもアイデンティティガバナンスの制度化を試みたものの、その多くは不完全または持続不可能であり、プロビジョニングの遅延、権限の過剰付与、監査の摩擦、リスクの増大につながっていました。

OIG の導入後では、受動的な監視から、ポリシー駆動型のプロアクティブなガバナンスに移行したとインタビュー参加者は報告しています。IAM チームは、一元化された可視性、主要なワークフローの自動化、アクセス制御の一貫した適用を実現し、サービス提供の迅速化、監査の簡素化、およびセキュリティ態勢の強化が可能になりました。

主な調査結果

定量的利益： モデル企業の 3 年間のリスク調整後の現在価値（PV）で示される定量的利益は、以下のとおりです。

- **アイデンティティガバナンスの効率向上（110 万ドル相当の PV）。**アクセス要求、認証レビュー、権限の管理を自動化することで、モデル企業の IAM チームおよび IT サポートチームでは必要な作業が最大 60%削減されます。この削減は、アクセスレビュー、権限の適切な管理、および一時的なアクセス要求に関連する手作業が不要になったこと、およびアクセスレビューと承認のサイクルでマネージャーが節約できた時間を反映しています。
- **監査準備およびコンプライアンス報告の作業負担を削減（合計で 23.2 万ドルに相当）。**アクセスの可視性の向上とレビューの自動化により、エビデンスの収集が簡素化され、SOX、PCI-DSS、その他の規制フレームワークに関連する内部監査と外部監査の要求への対応時間がモデル企業で短縮されます。また、認証およびアクセス制御のワークフローの一貫性が向上することで、監査結果の指摘を回避し、全体的なガバナンス体制を強化することができます。
- **プラットフォームの効率性強化とソフトウェアの合理化（56.7 万ドル相当の効率向上）。**レガシーツールや費用がかかるコネクタを、すぐに使える統合機能に置き換え、権限の可視性を高めることで、モデル企業はライセンスおよびコンサルティングのコストを削減し、オンボーディング、オフボーディング、アクセス権限の変更に伴う管理作業を軽減しました。ガバナンスワークフローにより、入社、異動、退職に関する重要なプロセスが自動化され、管理担当者を増員することなく、ポリシーに基づく実施が可能になります。
- **アクセスガバナンスの強化による生産性の向上（49.7 万ドル相当の PV）。**モデル企業のエンドユーザー、マネージャー、アプリケーション所有者は、手作業の承認チェーンやアクセス問題の解決に費やす時間を減らし、他の付加価値の高い業務により多くの時間を割くことができるようになります。ユーザー 1 人あたりの削減される時間はわずかでも、大規模なユーザーベースでは大きな効果が得られます。

また、効率化したユーザーエクスペリエンスと、監査しやすい一貫性のあるワークフローにより、遅延が減少し、ビジネスの俊敏性が向上します。

- **セキュリティ侵害リスクの軽減（23.1 万ドル相当の PV）。**モデル企業は、ガバナンス体制を強化し、過剰なアクセスまたは期限切れアクセスを排除することで、測定可能なセキュリティ侵害リスクを軽減しています。さらに、ガバナンスの自動化とプロアクティブな権限の見直しにより、特権の不正使用や内部脅威のリスクを制限すると同時に、複数のシステム間で一貫性に優れたアクセスポリシーのフットプリントを実現します。

非定量的利益。 本調査では定量化は行われなかったものの、モデル企業に価値をもたらすその他の利益は以下の通りです。

- **価値創出までの時間の短縮。**Okta Identity Governance は、従来の IGA ソリューションと比べて迅速に導入できます。モデル企業は、自動化のメリットを即座に実感できるほか、ユーザーとアプリケーションのオンボーディングが迅速化されて導入期間を大幅に短縮できるため、定量化可能な利点を数週間から数か月で実感できます。
- **IAM チームの士気が向上。**モデル企業のチームは、手作業で繰り返しの多いアイデンティティガバナンスのタスクではなく、ポリシーの設計、例外処理、ロードマップの策定など、より価値の高い戦略的な業務に専念できるようになります。
- **従業員体験とエンドユーザーエクスペリエンスの向上。**エンドユーザーではアクセス遅延や中断が少なくなり、管理者ではアクセス認証やリクエストのレビューや承認に費やす時間が短縮されます。セルフサービスアクセスと承認の効率化により、モデル企業は摩擦を軽減し、業務に欠かせないシステムへのアクセスを改善します。

コスト。モデル企業のリスク調整後の 3 年間における PV（現在価値）ベースで算出したコストは、以下のとおりです。

- **OIG のライセンス料金 82.1 万ドル。**これは、アイデンティティ 5,000 のユーザーベースにおける OIG 機能と標準サポートのライセンス費用の合計を反映したものです。
- **合計 2.8 万ドルの実装および導入費用。**これには 1 回限りのセットアップ、社内のプロジェクト管理、設定作業、およびガバナンスワークフローとポリシーの維持に必要となる軽微な継続的作業が含まれます。

インタビュー調査の財務分析の結果、モデル企業は 3 年間で 84.9 万ドルのコストに対して 260 万ドルの利益を計上し、合計 180 万ドルの正味現在価値（NPV）と 211%の投資利益率（ROI）を達成すると算出されます。

アイデンティティガバナンス、監査、コンプライアンスの取り組みおよびアクセスガバナンスの強化による労力削減と効率向上の合計価値

180万ドル

「導入初日から（OIGは）本来の目的以上のことを実行します。
コンプライアンスに必要な機能が手に入ったほか、ユーザーも満足します。
この事実がすべてを物語っています」

シニアディレクター、グローバルIAM責任者（プロフェッショナルサービス）

「サービスデスク、セキュリティ、監査、アプリケーション所有者、アクセス要求のレビューと承認を担当するビジネスマネージャーなど、全ユーザーの労力削減に目を向ければ、その全体的コストは正当化されます。さらに、組織のリスク低減と全体的なセキュリティ体制の向上も大きな利点です」

CIO（金融サービス）

投資利益率（ROI）

211%

利益の現在価値（PV）

260 万ドル

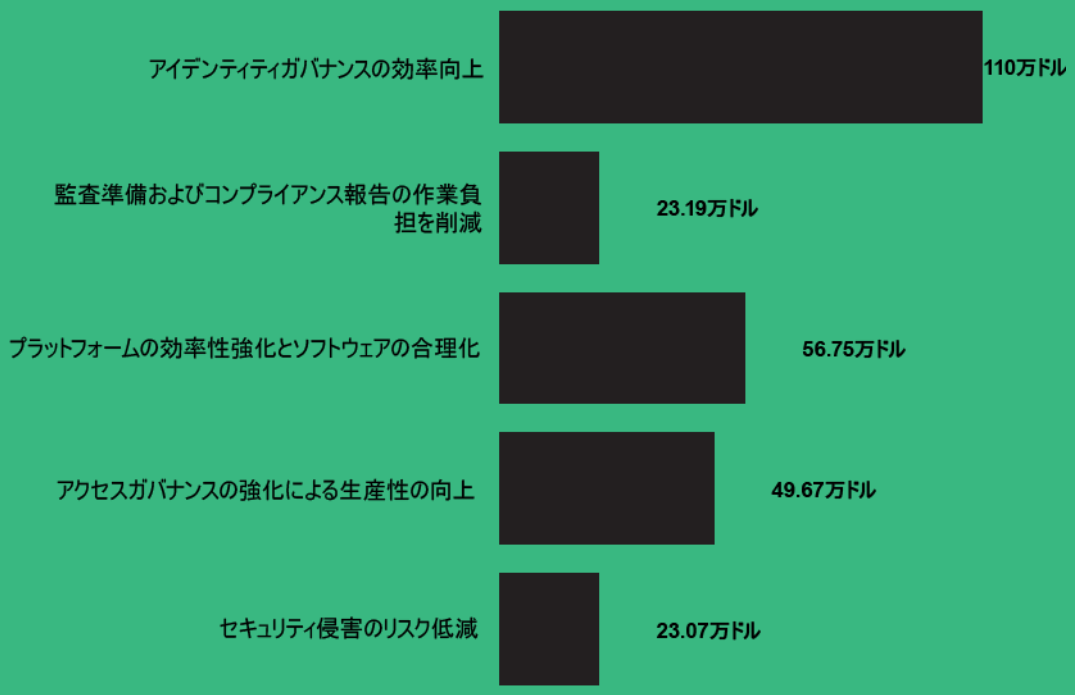
正味現在価値（NPV）

180 万ドル

回収期間

6 か月未満

利益（3年間）



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を基に Identity Governance の導入を検討中の組織のために 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・柔軟性・リスクの要因を明らかにすることです。Forrester は、Identity Governance が組織にもたらし得る影響を、多段階アプローチを使用して評価しました。

開示事項

以下の点に留意してお読みください。

本調査は Okta の依頼により、Forrester Consulting が実施しました。本調査は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、他の組織が得られる可能性のある ROI について一切仮定していません。Identity Governance 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に読者自身の予測を適用することを強く推奨します。

Identity Governance は本調査の内容を確認後、Forrester にフィードバックを提供しましたが、調査の内容および結果については Forrester が編集権を有し、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。

Okta 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。

1. **デューデリジェンス**
   Identity Governance に関連するデータを収集するために、Okta の利害関係者および Forrester のアナリストに面接調査を行いました。
2. **インタビュー調査**
   Identity Governance を利用している組織の代表者 8 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. **モデル企業**
   インタビュー調査に参加した組織の特性を基に、モデル企業を設計しました。
4. **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結果を反映した財務モデルを構築し、インタビュー対象組織の課題や懸念に基づき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、費用、柔軟性、リスクを用いて、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 分析が高度化する中、Forrester の TEI 手法は、購入判断における総経済効果の全体像を明確に示します。TEI 手法の詳細については、付録 A をご参照ください。

Okta Identity Governance のカスタマージャーニー

Identity Governance への投資を推進した要因

インタビュー調査			
役職	**業界**	**地域**	**アイデンティティ数/管理対象アプリ数**
ディレクター、IAM	IT サービス	グローバル、北米に拠点	104,000/200
セキュリティアーキテクチャ担当ディレクター	IT コンサルティング	グローバル、北米に拠点	100,000/1,500
マネージングディレクター	金融サービス	グローバル、北米に拠点	70,000/90
シニアディレクター、グローバル IAM 責任者	プロフェッショナルサービス	グローバル、北米に拠点	8,000/400
CIO	金融サービス	グローバル、EMEA に拠点	8,000/100
情報セキュリティディレクター	ヘルスケア	北米	7,200/370
IT ソリューション アーキテクト	ソフトウェア	グローバル、北米に拠点	3,000/70
CISO (情報セキュリティ最高責任者)	IT サービス	欧州／中東／アフリカ	2,200/200

主な課題

インタビュー参加者は、レガシーIGA プラットフォーム、自社開発ツール、手作業のプロセスが混在する、Okta Identity Governance 導入前の断片化したアイデンティティ環境について説明しています。この環境は、IT チームには運用効率の低下を、セキュリティチームにはコンプライアンスとアクセス制御のギャップを生じさせていました。アクセス要求の主流はチケットベースであり、認証はスプレッドシートに依存し、権限管理は標準化されていませんでした。これらの制限は、一貫性のないユーザーエクスペリエンスとコンプライアンスリスクの拡大を引き起こし、IT とセキュリティ担当者に過度の負担を強いていたと言います。

インタビュー参加者が指摘した共通の問題点は以下のとおりです。

- **生産性を低下させ、リスクを生み出す手作業のプロビジョニングとアクセス変更。** 多くのインタビュー参加者は、アクセス権が SLA 目標 5 日間以上のヘルプデスクチケットを通じて付与または取り消されていたと述べています。また、役職の変更や退職の後も、ユーザーが不必要なアクセス権を長期間保持

し、特権の拡大や内部漏洩リスクの可能性が高まっているとの意見も寄せられています。ソフトウェア企業の IT ソリューションアーキテクトは、大量のアクセス要求にチームが圧迫され、他チームから動員する必要があったと説明しました。「約 30 人が関わっていました。3 人の IAM チームではすべてのアクセス要求に対応できないため、30 人全員に均等に分散させるという共同作業でした」

- **時間と手間がかかり、エラーが発生しやすかったアクセス認証。** 企業は、監査およびコンプライアンス要件を満たすため、スプレッドシートと手作業による確認に大きく依存していました。認証には IAM 担当者が数週間の準備を要し、マネージャーや事業責任者が数時間を費やしてビューすることが多かったと複数のインタビュー参加者が報告しています。医療分野の情報セキュリティ責任者は、「悲惨な体験」だったと表現し、次のように述べています。「実は認証を完了したことがありません。リーダーたちの抵抗が激しく、取り組みの途中で失敗に終わっていました。認証が拒否され、ポリシーを遵守していると断言できる段階に到達していませんでした」
- **可視性と標準化のない権限管理。** 一元化されたガバナンスがないため、役割ベースのアクセスが統一的に適用されておらず、ユーザーは過剰な権限または期限切れの権限を蓄積していることが多くなっています。プロフェッショナルサービス企業の IAM グローバル責任者であるシニアディレクターは、「人々はアクセス権を蓄え込む傾向がある」と説明し、同社のチームでは手作業で過剰に付与されたアカウントを識別して解決する必要があったと言います。
- **監査準備に多大な時間と調整が必要。** インタビュー参加者は、OIG 導入前の監査が業務に大きな支障をきたし、アクセスログの収集、レビュー完了の追跡、監査結果への対応に数週間の準備期間と複数の人員を要したと述べています。

> 「OIG導入前は、私たちが来るのを誰もが恐れていましたが、今ではビジネス支援部門として評価されています。非常に大きな変化です」
>
> ITソリューションアーキテクト（ソフトウェア）

> 「OIGの導入により、エラーが発生しやすい手作業の多くを排除し、アプリケーション、ユーザー、顧客などの（OIGによる）アカウント管理とプロビジョニングの精度が高まりました」
>
> CIO（金融サービス）

モデル企業

Forrester はインタビュー調査をもとに、TEI フレームワーク・モデル企業・ROI 分析を作成し、財務面で影響を受ける業務領域を具体的に示しました。モデル企業とは、インタビュー参加者が所属するそれぞれの組織をモデルとして便宜的に 1 つの組織としてまとめたものです。次のセクションで財務分析の総合結果を表すためにこのモデル企業を使用しています。モデル企業には以下の特徴があります。

モデル企業の概要。このグローバル企業の年間収益は 15 億ドルで、5,000 のアイデンティティと 100 のアプリケーションを保有しています。IAM チームには、アイデンティティエンジニアリング、ガバナンス運用、ポリシーの実施、認証キャンペーンを担当する 10 人の FTE と、監査およびコンプライアンスサポートを担当する 2 人の FTE が所属しています。OIG の導入前にモデル企業は、コアのアイデンティティサービスに Okta を使用し、アクセスガバナンスには別のレガシーソリューションと手作業のプロセスを使用していました。

導入の特徴。 モデル企業は、1 年目の開始時に 8 週間の実装期間を経て、アクセスの認証と要求、権限管理、監査とコンプライアンス報告、および Okta Workflows による自動化のために OIG コンポーネントを展開しています。

主な前提条件

収益15億ドル

5,000のアイデンティティ

10人のFTEで構成されるIAMチームがアイデンティティガバナンスを管理し、2人のFTEが監査およびコンプライアンスサポートを提供

利益の分析

モデル企業に適用される定量的利益データ

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	アイデンティティガバナンスの効率向上	$323,366	$475,538	$570,645	$1,369,548	$1,115,709
Btr	監査準備およびコンプライアンス報告の作業負担を削減	$69,401	$99,144	$115,668	$284,213	$231,932
Ctr	プラットフォームの効率性強化とソフトウェアの合理化	$225,900	$229,500	$229,500	$684,900	$567,460
Dtr	アクセスガバナンスの強化による生産性の向上	$199,750	$199,750	$199,750	$599,250	$496,749
Etr	セキュリティ侵害のリスク低減	$92,757	$92,757	$92,757	$278,270	$230,672
	総利益（リスク調整後）	$911,173	$1,096,688	$1,208,320	$3,216,181	$2,642,522

アイデンティティガバナンスの効率向上

エビデンスとデータ。 インタビュー参加者は、Okta Identity Governance 導入前のアクセス認証、権限管理、アドホックなアクセス要求の処理に関する広範な手作業のプロセスについて説明しました。

- ある IT サービス企業の IAM ディレクターは、チームが自動化とセルフサービス機能に重点を置いていることについて次のように説明しています。「現在、OIG により 5 人で対応している IAM 業務に、以前は 36 人以上の専任スタッフが従事していました。Workflows を使用した自動化と各種の機能により、この業務向けの基盤の開発や構築を実施する必要がなくなっています。ローコード/ノーコードの Workflows を活用して自動化を実行し、すっかり Okta プラットフォームに頼っています」

- IAM 担当ディレクターは、自社で 20,000 から 80,000 のアイテムをカバーするキャンペーンを毎月 80 件から 90 件実施していますが、IAM チームの作業時間は 1 件あたり 1 時間未満だと付け加えました。
- ある医療機関の情報セキュリティ責任者は、「情報セキュリティの面で、以前は 1 人のエンジニアと 1 人のアナリストがキャンペーンの準備に約 4 週間を費やしていました。さらに、キャンペーンを監視してマネージャー（時には数百人）を指導しなければなりませんでした。2 人のリソースが、1 年の 4 分の 1 をアクセスレビューのみに費やしていました。現在では、キャンペーンの設定が 30 分未満で完了します」と述べています。
- 金融サービス企業の CIO は、「自動化率が（OIG の導入により）50%から 90%に上昇し、人件費が 50%削減されました」と述べています。
- あるプロフェッショナルサービス企業のグローバル IAM 責任者であるシニアディレクターは、9 人の IAM チームで現在 14～15 人の分の業務をこなしていると推定しています。
- IT サービス企業の CISO は、OIG の提供する自動化を最大のメリットとして挙げ、会社が「基本的にすべてを Workflows と自動化プロセス上に構築し、手作業を排除している」と説明しました。
- あるソフトウェア企業の IT ソリューションアーキテクトは、Okta Workflows の影響について次のように述べています。「自動化は導入していましたが、PowerShell スクリプト、Python スクリプト、AWS Lambda 関数など、あらゆるものがごちゃ混ぜの状態でした。すべてを Okta Workflow スタックに移行し、組み込みのフックを当社のさまざまなアイデンティティ関連オペレーションに活用したのですが、複雑さが劇的に解消され、多様なプラットフォームの維持管理に必要な時間も大幅に短縮されました」

モデル化と前提条件：インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- 10 人の IAM 担当 FTE が、アクセス要求やレビュー、権限管理などのアイデンティティガバナンスのコアタスクに割り当てられている。
- IAM 担当 FTE の全経費込の平均年間給与は 140,900 ドル。
- 8 週間の導入期間終了後、チームは残りの 44 週間でアイデンティティガバナンス業務に費やす時間を 40%削減し、1 年目の正味削減率は 34%になった。
- OIG が管理するアプリケーションが増加し、自動化がさらに統合されるのに伴い、節約時間は 2 年目で 50%、3 年目で 60%まで増加し、以前の手作業の業務がさらに削減される。

- このように節約された時間は、75%の割合で他の価値創造活動に再配分される。

リスク。現実的かつ妥当な見積もりを支えるため、Forrester は、インタビューのエビデンスの一貫性と報告された結果のばらつきの程度に基づいて、リスク調整を適用しています。TEI 調査手法のこの要素は、実装環境の違いを考慮する上で有用です。この利益の程度は、以下の相違点により顧客組織によって異なります。

- 自動化のレベルと時間短縮の割合。レガシーシステムの複雑さやコンプライアンス要件によって異なる場合があります。
- 手作業での監視の必要性。規制や業界固有の制約がある組織ではより高くなる可能性があります。
- 利益の規模。ユーザー数、キャンペーンの頻度、管理対象のアプリケーションの数と複雑さに依存します。
- IAM 担当 FTE の全経費込み年間給与。

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%下方修正し、リスク調整後の 3 年間の現在価値（PV）総額（10%割引）を 110 万ドルとしました。

アイデンティティガバナンス関連タスクの所要時間短縮の割合（3年目まで）
60%

「従来のソリューションを使用していた頃に比べ、10倍近くか、それ以上の作業量を簡単にこなせるようになりました」

情報セキュリティディレクター（ヘルスケア）

> 「Workflowsで多数のFTEを削減できました。当社のアプリケーション数では、Workflowsなしでの管理はほぼ不可能だったでしょう」
>
> セキュリティアーキテクチャ担当ディレクター（ITコンサルティング）

アイデンティティガバナンスの効率向上					
参照コード	**評価基準**	**ソース**	**1 年目**	**2 年目**	**3 年目**
A1	アクセス要求およびレビュー、権限管理、その他のアイデンティティガバナンス関連タスクに割り当てられた IAM 担当 FTE	モデル企業	10	10	10
A2	アイデンティティガバナンス業務を行う IAM 担当 FTE の全経費込み年間給与	モデル企業	$140,900	$140,900	$140,900
A3	OIG をアイデンティティガバナンス関連業務に導入して節約できた正味時間の割合	インタビュー調査	34%	50%	60%
A4	生産性の回収	TEI 調査手法	75%	75%	75%
At	アイデンティティガバナンスの効率向上	A1*A2*A3*A4	$359,295.0	$528,375.0	$634,050.0
	リスク調整	↓10%			
Atr	アイデンティティガバナンスの効率向上（リスク調整後）		$323,365.50	$475,537.50	$570,645.00
	3 年間の合計: $1,369,548		**3 年間の現在価値: $1,115,709**		

監査準備およびコンプライアンス報告の作業負担を削減

エビデンスとデータ。 OIG は、反復的に行われる監査、アクセスレビュー、コンプライアンス報告に関連する膨大な手作業を効率化または回避するのに役立っているとインタビュー参加者は述べました。アクセス制御の検証、エビデンスや報告書の作成を担当していたチームは、大幅な時間の短縮と監査関連作業の削減を報告しています。削減または回避された作業の具体的な分野は以下の通りです。

- インタビュー参加者は、OIG 導入前には監査準備作業に数週間を要したと説明しています。これには、認証データの手作業による収集、アクセス承認のスクリーンショットの取得、システムを横断したアクセス制御ログの検証などの作業が含まれていました。

- 自動化された認証ワークフローにより、レビュープロセスの完全性と一貫性が向上し、調査につながる可能性のある記録の欠落や誤った記録のリスクが軽減された点が、複数のインタビュー参加者により指摘されています。また、OIG で一元化されたポリシー、ワークフロー、監査ログは、監査人に対するガバナンスプロセスの説明や例外の文書化に必要な労力を削減する要因であるとも指摘しました。
- インタビュー参加者は、OIG のダッシュボードを使用してアクセスレビュー、ユーザーの役割、権限に関するアドホックレポートを生成することで、時間の短縮と複雑さの軽減を実現したと説明しています。これらの機能は、チームが内部監査や外部規制当局の問い合わせに迅速に対応するのに役立ちました。
- プロフェッショナルサービス部門のグローバル IAM 責任者であるシニアディレクターは、OIG の自動化がなければ「エビデンス収集の一貫性の管理に 3〜5 人のチームが必要だった」と説明しています。
- 同じシニアディレクターはさらに次のように述べました。「監査人に 30 分のセッション 1 回で説明し、それで完了します。フォローアップは一切不要でした。（監査人は、自社の）セキュリティエンジニアに（当社に）連絡して（OIG を）導入するよう依頼してきました。その依頼は 2 回ありました。最大の賛辞だと言えるでしょう」

モデル化と前提条件：インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- 監査およびコンプライアンス業務は 2 人の FTE に割り当てられる。
- 監査およびコンプライアンス担当 FTE の全経費込み平均年間給与は 122,400 ドル。
- 8 週間の導入期間終了後、チームは残りの 44 週間で監査準備およびコンプライアンス報告業務に費やす時間を 50%削減し、1 年目の正味削減率は 42%になった。
- IAM チームの効率向上と OIG ガバナンスの拡張に伴い、時間の節約は 2 年目に 60%、3 年目には 70%に増加する。
- このように節約された時間は、75%の割合で他の価値創造活動に再配分される。

リスク。 この利益の程度は、以下の相違点により顧客組織によって異なります。

- 業界および地域で必要な監査の数および複雑さ。
- OIG を採用する前の既存のプロセスおよびツールの成熟度。
- IAM およびコンプライアンスチームの規模と構成。

- 監査関連タスクの自動化または他のガバナンスシステムへの統合の程度。
- 監査およびコンプライアンス担当 FTE の全経費込み平均年間給与。

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%下方修正し、3 年間のリスク調整後の PV 総額（10%割引）を 23.2 万ドルとしました。

監査およびコンプライアンス業務で節約できる時間（3年目まで）
70%

監査準備およびコンプライアンス報告の作業負担を削減

参照コード	評価基準	ソース	1 年目	2 年目	3 年目
B1	監査およびコンプライアンス業務を行う IAM 担当 FTE の人数	モデル企業	2	2	2
B2	監査およびコンプライアンス業務を行う IAM 担当 FTE の全経費込み年間給与	モデル企業	$122,400	$122,400	$122,400
B3	OIG により監査およびコンプライアンス業務で節約できた正味時間の割合	インタビュー調査	42%	60%	70%
B4	生産性の回収	TEI 調査手法	75%	75%	75%
Bt	監査準備およびコンプライアンス報告の作業負担を削減	B1*B2*B3*B4	$77,112.00	$110,160.00	$128,520.00
	リスク調整	↓10%			
Btr	監査準備およびコンプライアンス報告の作業負担を削減（リスク調整後）		$69,400.80	$99,144.00	$115,668.00
	3 年間の合計: $284,213		**3 年間の現在価値: $231,932**		

プラットフォームの効率性強化とソフトウェアの合理化

エビデンスとデータ。 Okta Identity Governance により、高価な外部コンサルタントへの依存度を低減し、カスタムコネクタを排除し、ローコード/ノーコードのツールで社内チームに権限を付与することで、プラットフォームの効率が向上したとインタビュー参加者は伝えています。同時に、組織で権限の可視性と使用状況の洞察を

向上させ、ソフトウェア支出を合理化し、未使用のライセンスを削除することもできたと言います。こういった変更により、運用効率が向上してガバナンスの範囲が強化されました。

プラットフォームの効率性：

- 医療分野の情報セキュリティ担当ディレクターによると、OIG の導入前はレガシーソリューションでの取り組みを進めるために、年間 15 万ドルから 20 万ドルをコンサルタントに費やしていたと言います。OIG を導入することで、直ちに使えるコネクタ、ローコード/ノーコードの自動化、より最新のツールで強化された社内リソースにより、その追加コストは不要になりました。
- 金融サービス企業の CIO は次のように加えます。「OIG には事前構築済みの統合機能が数多く備わっているため、現在の環境への接続が容易になりました。（OIG はまた、）未使用アカウントを削減することで、ライセンスとリソース管理面で利点の実現に役立っています」
- プロフェッショナルサービス企業のグローバル IAM 責任者であるシニアディレクターは、自社におけるアプリケーション接続に 1.5 万ドルから 2.5 万ドルを支払っていましたが、その結果は「API 経由で接続されていないため、ガバナンス目的で接続すべきシステムを一部接続しておらず、ギャップが生じるリスクがありました。（OIG の採用により）SSO がアイデンティティプロバイダーに接続しているものは、ガバナンスに自動追加されます。これが本来あるべき姿です」

ソフトウェアの合理化：

- インタビュー参加者は、OIG による権限の可視化で、未使用または重複しているライセンスを特定して削除できたと言います。IT ソリューションアーキテクトが所属するソフトウェア会社では、アプリケーションを実際に使用しているユーザーに関するリアルタイムの情報を得るために、一時的な認証キャンペーンを実施しており「実施するたびに多大な利点がある」そうです。一例では、550 人のユーザーが利用するアプリケーションのライセンスを約 200 件削減し、ユーザー1 人あたり月額 5 ドルから 10 ドルのコスト削減を実現していました。
- プラットフォームの効率化とソフトウェアの合理化に関連するコスト削減について尋ねると、ある金融サービス企業の CIO は、年間 20 万ドル超のコスト削減を実現していると見積もりました。

モデル化と前提条件：インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- モデル企業は、従来のソリューションでは有料コネクタが必要だった 10 の増分アプリケーションを OIG を使用して接続する。
- コネクタの利用料はアプリケーションあたり 2 万ドル。

- OIG の導入で 10 のアプリケーションのライセンスを整理できるようになり、平均で 50 の未使用または重複するライセンスが削除され、1 ライセンスあたり月額 5 ドルのコスト削減になる。
- 8 週間の導入期間後、モデル企業は 1 年目に 2.1 万ドルのコンサルティングまたはサードパーティのサポート費用を回避し、2 年目と 3 年目にはそれぞれ 2.5 万ドルを回避する。

リスク。この利益の程度は、以下の相違点により顧客組織によって異なります。

- レガシーIGA ソリューション用の事前構築済みコネクタのコストと可用性。
- OIG 経由で追加または管理されるアプリケーションの数と種類。
- エンタープライズソフトウェア環境におけるライセンス構成と過剰なプロビジョニングのパターン。
- IAM 機能における外部コンサルタントまたはマネージドサービスプロバイダーへの依存度。

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%下方修正し、3 年間のリスク調整後の PV 総額（10%で割引）を 56.8 万ドルとしました。

プラットフォームの効率性強化とソフトウェアの合理化					
参照コード	**評価基準**	**ソース**	**1 年目**	**2 年目**	**3 年目**
C1	レガシーソリューションのコネクタ料金（アプリケーションあたり）	インタビュー調査	$20,000	$20,000	$20,000
C2	OIG により可能になったアプリケーション接続の増加	モデル企業	10	10	10
C3	**小計：OIG の導入で回避されたコネクタ料金**	**C1*C2**	**$200,000**	**$200,000**	**$200,000**
C4	OIG によるライセンス整理が有効なアプリケーション	モデル企業	10	10	10
C5	削除された不必要なライセンス数（アプリケーションあたり）	インタビュー調査	50	50	50
C6	ユーザー1 人あたりの平均ライセンス月額	インタビュー調査	$5	$5	$5
C7	**小計：OIG の導入で回避されたライセンス料金**	**C4*C5*C6*12**	**$30,000**	**$30,000**	**$30,000**
C8	回避された IAM に関するコンサルティング/サードパーティのサポートコスト	インタビュー調査	$21,000	$25,000	$25,000
Ct	プラットフォームの効率性強化とソフトウェアの合理化	C3+C7+C8	$251,000.00	$255,000.00	$255,000.00
	リスク調整	↓10%			
Ctr	プラットフォームの効率性強化とソフトウェアの合理化（リスク調整後）		$225,900	$229,500	$229,500
	3 年間の合計: $684,900		**3 年間の現在価値: $567,460**		

アクセスガバナンスの強化による生産性の向上

トレーニング、実装、最適化。 インタビュー参加者は、OIG がエンドユーザー、マネージャー、アプリケーション所有者のアクセス関連ワークフローをどのように合理化したかを説明しています。OIG 導入前は、エンドユーザーが過剰な要求を行うことが多く、その結果、遅延や追加のフォローアップが発生していました。OIG 導入後は、要求が効率的なルーティングを通じて解決されるため、要請者および承認者の負担が軽減されました。アクセス要求、認証、権限レビューの自動化と簡素化により、古くなったインターフェースの操作、手作業による承認の待ち時間、一貫性のないガバナンスプロセスへの対応に費やす時間が削減されました。

- ソフトウェア企業の IT ソリューションアーキテクトは次のように述べています。「（OIG 導入前は、）承認を得るまでに 45 分から 2 時間、アクセス権限の付与までに最大 24 時間かかっていました。現在では要求の完了までを 30 分に短縮できました」
- 金融サービス企業のマネージングディレクターは、アクセス要求や変更について「以前は SLA の 5 営業日以上かかっていましたが、現在は自動化により 30 分以内に完了します」と言っています。

モデル化と前提条件：インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- 5,000 人のエンドユーザーは、アクセスの問題の減少、アクセス承認およびプロビジョニングの改善により、OIG で年間平均 2 時間の時間を節約する。
- エンドユーザー1 人あたりの全経費込みの平均時給は 47 ドル。

リスク。 この利益の程度は、以下の相違点により顧客組織によって異なります。

- ビジネスユーザーに割り当てられるアクセス関連タスクの種類と量。
- OIG 導入前のガバナンスワークフローの成熟度と一貫性。
- 展開時に導入された自動化とカスタマイズのレベル。
- 組織全体での要求と認証ワークフローの採用範囲。
- エンドユーザー1 人あたりの全経費込みの平均時給。

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 PV 総額（10%割引）を 49.7 万ドルとしました。

アクセスガバナンスの強化によりエンドユーザーが節約できる時間の価値
$497,000

「（OIGにより）ユーザーエクスペリエンスが大幅に改善されました。ユーザーは必要な作業を短時間で迅速に完了し、ほかの仕事や重要な業務に移ることができます。以前は、そのような作業に多くの生産性を奪われていました」

マネージングディレクター（金融サービス）

アクセスガバナンスの強化による生産性の向上

参照コード	評価基準	ソース	1 年目	2 年目	3 年目
D1	エンドユーザー総数	モデル企業	5,000	5,000	5,000
D2	OIG の導入によるアクセス承認とプロビジョニングの改善、アクセスの問題の減少により、エンドユーザー1 人あたり節約できた時間	インタビュー調査	2	2	2
D3	エンドユーザー1 人あたりの全経費込みの時給	モデル企業	$47	$47	$47
D4	生産性の回収	TEI 調査手法	50%	50%	50%
Dt	アクセスガバナンスの強化による生産性の向上	D1*D2*D3*D4	$235,000	$235,000	$235,000
	リスク調整	↓15%			
Dtr	アクセスガバナンスの強化による生産性の向上（リスク調整後）		$199,750	$199,750	$199,750
	3 年間の合計: $599,250		**3 年間の現在価値: $496,749**		

セキュリティ侵害のリスク低減

エビデンスとデータ。 Okta Identity Governance では最小権限アクセスを強制、不要な権限を削除、レビューと削除を自動化することで、セキュリティ侵害のリスクが軽減したとインタビュー参加者は認めています。複数の参加者は、OIG がアクセス権の拡大を抑制し、レガシーアクセスを整理する役割を強調しており、これがゼロトラストアーキテクチャへの移行で基盤となる機能だと指摘しました。

- あるプロフェッショナルサービス企業のグローバル IAM 責任者であるシニアディレクターは、OIG が過剰なアクセス権限を削除して人的ミスを最小限に抑えることで、会社が不要なリスクにさらされるのを防いだと言っています。「ユーザーは、職務と有害な特権の分離を好みます。（OIG による）自動化は、既存の役割と衝突する可能性のある役割を迅速に検出し、問題が発生する前に是正します。極めて大きな利点です」
- 医療分野の情報セキュリティ担当者は、保護対象保険情報（PHI）に関連するリスクへの暴露が、OIG により大幅に減ったと説明しています。OIG は、PHI へのアクセスについてガバナンスの強化を支援し、必要なユーザーのみに機密データへのアクセス権を付与しました。不必要なアクセスに的を絞って削減することで、コンプライアンスおよびセキュリティ上の潜在的なリスクを軽減することができます。
- 金融サービス企業の CIO は、次のように述べます。「職務の分離とポリシーの実施機能により、利益相反を防ぎ、潜在的な不正行為を減らすことができます。アクセスレビューと認証の可視性が大幅に向上した結果、特に請負業者やサードパーティのパートナーに関する内部脅威が減少しました。さらに、アクセス権の自動削除により、退職した従業員や請負業者、ベンダーにアクセス権が残ることを防ぎ、リスクを軽減しています」

モデル化と前提条件：インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- モデル企業は、年間 302.7 万ドル相当の侵害リスクにさらされている。[2] 1 件以上の侵害が発生する可能性は 63%。[3]
- これらの侵害のうち、76%は外部からの攻撃や内部インシデントに起因するか、外部エコシステムに関連している。[4]

- これらのインシデントの 80%は、OIG が提供するより強力なアイデンティティガバナンスおよびアクセス制御によって対処可能。
- モデル企業は、インタビュー参加者が報告したアクセスの健全度およびレビューの有効性の改善に基づき、OIG の導入を通じてリスクへの暴露を 10%削減している。

リスク。この利益の程度は、以下の相違点により顧客組織によって異なります。

- 組織規模、業界、および内在するセキュリティリスクプロファイル。
- 既存のアイデンティティガバナンスの成熟度とツール。
- OIG の展開範囲とアクセスポリシーの適用状況。
- IAM、セキュリティ、コンプライアンスチーム間の内部連携。

結果。これらのリスクを反映させるため、Forrester はこの利益を 20%下方修正し、リスク調整後の 3 年間の PV 総額（10%割引）を 23.1 万ドルとしました。

> 「セキュリティ体制が大幅に強化され、CISO、コンプライアンス、リスクの各チーム、顧客、株主の皆が満足しています。（OIGは）セキュリティ面で数多くの利点があります」
>
> CIO（金融サービス）

セキュリティ侵害のリスク低減

参照コード	評価基準	ソース	1 年目	2 年目	3 年目
E1	モデル企業の侵害の累積コスト	Forrester 調査	$3,027,000	$3,027,000	$3,027,000
E2	モデル企業で 1 件以上の侵害が発生する可能性	Forrester 調査	63%	63%	63%
E3	組織を標的とした外部の攻撃、内部インシデント、または外部エコシステムに関連するセキュリティ侵害の割合	Forrester 調査	76%	76%	76%
E4	OIG で対応可能な攻撃の割合	Forrester 調査	80%	80%	80%

E5	**小計：OIG で対応可能な年間侵害リスク**	**E1*E2*E3*E4**	**$1,159,462.0**	**$1,159,462.0**	**$1,159,462.0**
E6	OIG で対応可能な攻撃によるデータ侵害コストに対する露出リスクの低減	インタビュー調査	10%	10%	10%
Et	セキュリティ侵害のリスク低減	E5*E6	$115,946	$115,946	$115,946
	リスク調整	↓20%			
Etr	セキュリティ侵害のリスク低減（リスク調整後）		$92,757	$92,757	$92,757
	3 年間の合計: $278,270		**3 年間の現在価値: $230,672**		

非定量的利益

インタビュー調査参加者からは、以下のように、恩恵が認められたものの定量化できなかった利益についてのコメントもありました。

- **迅速な価値創出。**数か月にわたるプランニング、カスタマイズ、統合作業が必要な従来の IGA プラットフォームと比較した、OIG の導入から価値実現までのスピードについて、インタビュー参加者は一様に高く評価しました。OIG により、チームは、アクセス要求や認証ワークフローなどのコア機能を、最小限のリソースと設定作業で稼働させることが可能です。この迅速な立ち上げにより、組織は、ほぼ即座に有意義なガバナンスの改善を実現することができました。しかも完全な最適化や広範な展開より早くです。

  金融サービス企業の CIO は、OIG が組織の既存の Okta インフラストラクチャ（シングルサインオン、多要素認証、API アクセス管理など）と高度に統合されているため、価値創出までの時間が短縮されたと指摘しています。OIG ではこういったコアサービスが既に導入されているため、競合ソリューションに比べてより迅速な展開も、統合の障害が少ないことも当然でした。

  医療分野の情報セキュリティディレクターは次のように述べています。「実装は瞬時に完了しました。すべきことも特にありませんでした。その点も（Okta）プラットフォームの特性です。2 週間で本番環境に移行できましたが、まさに大成功でした」

  あるプロフェッショナルサービス企業のグローバル IAM 責任者であるシニアディレクターは、展開プロセスについて次のように話しています。「当時、私とエンジニア 2 名で、木曜日と金曜日に電話で打ち合わせをしただけでした。気が付くとすべて完了していました。アクセス要求も、ガバナンスと認証も機能して

いて、本番環境に移行するだけでした。自分たちの能力にもっと自信があったなら、初日に完了できたかもしれません」

- **IT チームとセキュリティチームの士気向上。**OIG を導入して反復的な手作業を排除し、アクセス要求や認証の管理に伴う負担を軽減したことで、インタビュー参加者のチームではより戦略的で価値の高い業務に専念できるようになったといいます。また、IT、IAM、セキュリティチームの生産性と文化面での向上と表現しています。IT コンサルティング企業のセキュリティアーキテクチャ担当ディレクターは「現在では手作業のプロセス管理が減少したため、より戦略的な目標に集中できる」と述べました。プロフェッショナルサービス企業のグローバル IAM 責任者であるシニアディレクターは、次のようにまとめています。「チームメンバーは、以前は希望していたが経験不足で無理だった他の役割に、事実上ステップアップしています。（OIG では）異なる仕事を優先するのをリーダーが許可できます。その仕事をアナリストとして片付けたいと思うだけでなく、その仕事を本当にやりたいと願っているからです。主体的にやらせてくださいと願い出るやりがいのある仕事です」

> 「（Oktaが提供する）専門知識が高く評価できるだけでなく、Oktaとの仕事は本当に実りあるものです。Customer Successとサポートのスタッフはその分野に精通しています」
>
> マネージングディレクター（金融サービス）

柔軟性

柔軟性の価値は、顧客によって異なります。顧客が Identity Governance を導入するシナリオは、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。

- **将来への対応力と俊敏性の向上。**OIG の柔軟性は、短期的な成果と長期的な戦略的成長を実現する重要な要因の一つだとインタビュー参加者は指摘しています。複数の企業では、アクセス要求やオンボーディングなど狭い範囲から始めて、その後、時間をかけて追加のアプリケーション、事業部門、またはコンプライアンスのフレームワーク全体へと適用範囲を拡大しました。インタビュー参加者は、内部の準備状況と変化する規制上の優先事項にガバナンスの範囲を合わせるためには、この段階的なアプローチが不可欠だと説明しています。OIG が Okta のアイデンティティプラットフォームとネイティブに統合されているため、会社は、管理の負担を追加したり既存のワークフローを中断したりすることなく規模を拡大できました。また、制御は多様な地域や基準（例：SOX、HIPAA、ISO）に対応するよう設

定可能でした。医療分野の情報セキュリティ責任者は「（OIG があれば）自社の運命を自らの手でコントロールできる」と簡潔にまとめています。

柔軟性も、特定のプロジェクトの一環として評価する場合には数値化されます（詳細は TEI アプローチを参照）。

> 「ツール、サポート、そしてツールをサポートするために導入されたメカニズムには、非常に柔軟性があります」
>
> シニアディレクター、グローバルIAM責任者

コストの分析

モデル企業に適用される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	OIG 使用料	$0	$330,000	$330,000	$330,000	$990,000	$820,661
Etr	トレーニング、実装、最適化	$27,878	$0	$0	$0	$27,878	$27,878
	総コスト（リスク調整後）	$27,878	$330,000	$330,000	$330,000	$1,017,878	$848,539

OIG 使用料

エビデンスとデータ。 インタビュー参加者はコストの詳細を提供しましたが、これは Okta による確認がとれています。モデル企業の場合、ユーザー1 人あたり月額 5 ドルのコスト見積もりは、そのモデル企業に関連する具体的な実装およびシナリオに基づいています。実際の現在価値コストは、Okta および OIG が特定の顧客に提供するサービスの種類によって異なります。詳細については Okta にお問い合わせください。

モデル化と前提条件： インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- OIG は 5,000 の管理対象アイデンティティに展開されている。
- 料金は 1 アイデンティティあたり月額 5 ドル。

リスク。 この費用は、交渉による価格設定やライセンス体系の違いにより、顧客ごとに異なる場合があります。

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 10%上方修正し、3 年間のリスク調整後の PV 総額（10%割引）を 82.1 万ドルとしました。

OIG 使用料						
参照コード	**評価基準**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
F1	OIG 管理対象のアイデンティティ	モデル企業		5,000	5,000	5,000
F2	アイデンティティごとの OIG 月額使用料	インタビュー調査		$5	$5	$5
Ft	OIG 使用料	F1*F2*12	$0	$300,000	$300,000	$300,000
	リスク調整	↑10%				
Ftr	OIG 使用料（リスク調整後）		$0	$330,000	$330,000	$330,000
	3 年間の合計: $990,000			**3 年間の現在価値: $820,661**		

トレーニング、実装、最適化

エビデンスとデータ。 インタビュー参加者は、OIG の設定、人員のトレーニング、アクセスワークフローの微調整を行うために、ある程度のトレーニング、実装、最適化が必要だったと述べています。こういった活動の期間は、数週間から数か月までさまざまでした。

モデル化と前提条件: インタビュー調査をもとに、Forrester は以下をモデル企業の前提条件としました。

- IAM チームと専任の監査およびコンプライアンスサポートスタッフは、OIG の実装に 8 週間を費やし、そのうちの平均 10%を OIG 関連タスクに割り当てる。
- IAM および監査・コンプライアンス担当 FTE の全経費込み平均年間給与は 66 ドル。

リスク。 このコストの程度は、以下の相違点により顧客組織によって異なります。

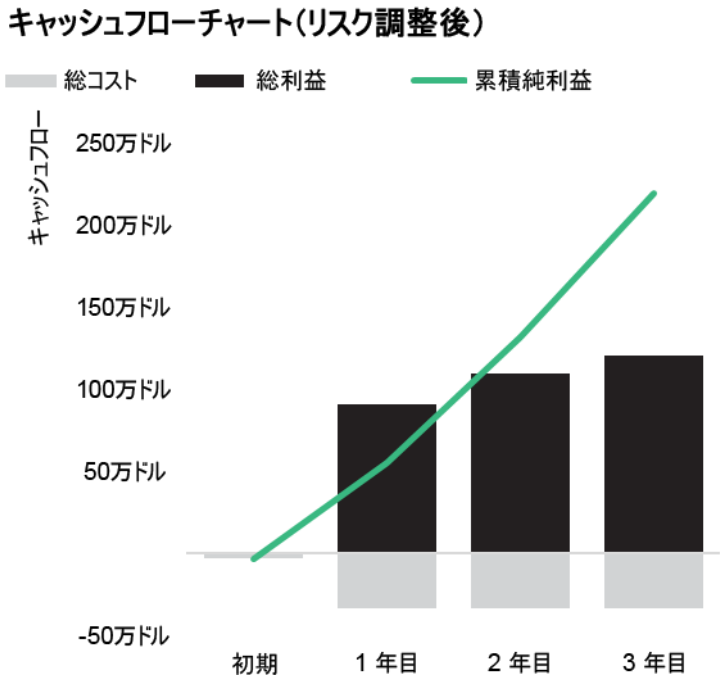
- 内部 IAM チームの規模と経験レベル。
- 既存のシステムと統合の複雑さ。
- IAM および監査・コンプライアンス担当 FTE の全経費込み平均年間給与。

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 10%上方修正し、3 年間のリスク調整後の PV 総額（10%割引）を 2.8 万ドルとしました。

トレーニング、実装、最適化						
参照コード	**評価基準**	**ソース**	**初期**	**1 年目**	**2 年目**	**3 年目**
G1	IAM 担当 FTE および専任の監査/コンプライアンス担当 FTE	モデル企業	12			
G2	統合期間（週）	インタビュー調査	8			
G3	OIG のトレーニング、実装および/または最適化に割り当てられた時間（平均）	インタビュー調査	10%			
G4	**小計：OIG の統合に費やされた時間**	**G1*G2*40*G3**	**384**			
G5	IAM および専任の監査/コンプライアンス担当 FTE の全経費込み年間給与。	モデル企業	$66			
Gt	トレーニング、実装、最適化	G4*G5	$25,344	$0	$0	$0
	リスク調整	↑10%				
Gtr	トレーニング、実装、最適化（リスク調整後）		$27,878	$0	$0	$0
	3 年間の合計: $27,878			**3 年間の現在価値: $27,878**		

財務概要

リスク調整後の 3 年連結評価



「利益」と「コスト」のセクションで計算された財務的結果を使用して、このモデル企業の投資に対する ROI、NPV および投資回収期間を決定できます。Forrester は、この分析において年 10 % の割引を想定しています。

リスク調整後のこれらの ROI、NPV、投資回収期間の値は、「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)

	初期	1 年目	2 年目	3 年目	合計	現在価値
総コスト	($27,878)	($330,000)	($330,000)	($330,000)	($1,017,878)	($848,539)
総利益	$0	$911,173	$1,096,688	$1,208,320	$3,216,181	$2,642,522
純利益	($27,878)	$581,173	$766,688	$878,320	$2,198,303	$1,793,983
投資利益率(ROI)						211%
投資回収期間						6 か月未満

付録 A : TOTAL ECONOMIC IMPACT

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提示する際に有用となります。TEI 手法を使用することで、企業は経営陣や他のビジネス上の主要な利害関係者に対して、IT の取り組みの具体的な価値を示し、根拠を挙げ、証明することができます。

TEI アプローチ

利益は、製品がビジネスにもたらす価値を表します。TEI 手法では、利益の算定と費用の算定に均等の重みを置き、テクノロジーが組織全体に与える影響を細部にわたって検証することを可能にします。

コストでは、提案されている製品の価値または製品の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 内のコストカテゴリでは、そのソリューションに関連した継続的な費用について、既存環境での増分費用を把握します。

柔軟性とは、既存の初期投資を基盤として、将来的な追加投資によって得られる戦略的な価値を指します。その利益を把握できる場合、PV を推定できます。

リスクとは、利益とコストの見積りの不確実性を想定したもので、1）見積りが初期の予測と一致する可能性と、2）見積りが時間を経て予測どおりに推移する可能性が考慮されています。TEI のリスク要因は、「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 NPV がプラスの場合、通常、他のプロジェクトの NPV が高い場合を除き、投資を行うべきであることを示します。

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。

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費用が記載されます。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、それぞれの総費用と利益の見積りに対して計算されます。概要表にある NPV の算出値は、初期投資と各年の割引率適用後のキャッシュフローの合計になります。総利益、総費用、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。

付録 B：注釈

[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、ソリューションプロバイダーがクライアントに自社の価値提案を伝える際に役立ちます。TEI 手法を使用することで、企業は上級管理職やビジネスの他の主要利害関係者に対して、ビジネスとテクノロジーのイニシアティブの具体的な価値を実証し、正当化し、実現することができます。

[2] 過去 12 か月間にセキュリティ意思決定者の組織が経験した、報告済みの侵害すべての累積総コストの回帰分析。回帰式への入力としてモデル企業の売上高を使用。出典：Forrester のセキュリティ調査、2024 年。「過去 12 か月間に貴社で発生したすべての侵害の累積総コストはどれくらいでしたか？ 最善の推定値をご提示ください」調査対象：過去 12 か月間に侵害を経験した 1,660 人のグローバルセキュリティ意思決定者。

[3] セキュリティ意思決定者が報告した過去 12 か月間の侵害発生頻度を基に、1 件以上の侵害を経験する可能性の回帰分析。回帰式への入力としてモデル企業の売上高を使用。出典：Forrester のセキュリティ調査、2024 年。「過去 12 か月間に、貴社の機密データが侵害または漏洩した可能性のある回数は、およそ何回ですか？」調査対象：2,769 人のグローバルセキュリティ意思決定者。

[4] 過去 12 か月間に少なくとも 1 回の侵害を経験した企業のセキュリティ意思決定者が報告した、侵害の主な攻撃ベクトル別の侵害の割合。出典：Forrester のセキュリティ調査、2024 年。「過去 12 か月間に、貴社の機密データが侵害または漏洩した可能性のある回数のうち、以下の各カテゴリーに該当する回数を示してください」調査対象：過去 12 か月間に侵害を経験した 1,542 人のグローバルセキュリティ意思決定者。

FORRESTER®