Forrester Total Economic Impact™ 調査
委託元：IBM

プロジェクト責任者：
Adrienne Capaldo
2015 年 9 月

IBM Security Guardium に関する Total Economic Impact™

データのセキュリティは、組織にとって複雑な課題になります。データのセキュリティについては、組織が関心を寄せるだけでなく、顧客もより意識するようになっています。顧客データの価値は、時間の経過と共に飛躍的に増加していますが、同時に、法的責任や漏えいの恐れも高まっています。このような状況に、組織環境内のデータの急増、業界全体での規制やコンプライアンスの複雑さ、組織内外からの攻撃の脅威といった要因が組み合わさり、セキュリティとコンプライアンスについての企業戦略を成功に導く重要性が注目されています。また、企業はユーザー アクセス特権を積極的に監視および制御する方法の把握に取り組んでいます。しかし、多くの場合、どのデータが危険にさらされているかの視認性が不足しており、このことはセキュリティの壊滅的な脅威につながる可能性があります。

Forrester Consulting は IBM の委託を受け、全データのセキュリティとコンプライアンスの企業戦略の一環として IBM Security Guardium を導入することにより企業にもたらされる投資対効果 (投資利益率、ROI) に関する調査 Total Economic Impact™ (TEI) を実施しました。本調査の目的は、Guardium の導入によって組織にもたらされる経済効果を評価するための枠組みを提示することです。

Guardium の導入による便益、費用、およびリスクについて十分に把握するため、Forrester は既に Guardium を導入し、数年にわたって利用しているユーザー企業数社に対して面接調査を実施しました。IBM Security Guardium は、データ セキュリティとコンプライアンスのライフ サイクル全体を管理するための統合モジュールのファミリーを提供します。Guardium は、1 つの統一インフラストラクチャと統一ユーザー インターフェイスを土台に構築されています。Guardium は、データベース、データ ウェアハウス、ファイル システム、クラウドベースのシステム、仮想システム、ビッグ データに基づくシステムなど、広範なデータ環境をサポートし、そのセキュリティを確保するよう設計されています。

面接調査とその後の財務分析の結果、モデル組織では以下に示すような ROI、便益および費用 (いずれもリスク調整後) が発生することがわかりました。

主な調査結果：IBM SECURITY GUARDIUM は機微な企業データのセキュリティを効果的に確保し、リスクを軽減する

ROI：218%	NPV (正味現在価値)：1800 万ドル	回収期間：7.4 ヶ月

手法

Forrester Consulting は IBM の委託を受け、全データのセキュリティとコンプライアンス戦略の一環として Guardium を導入することにより企業にもたらされる投資対効果 (投資利益率、ROI) に関する調査 Total Economic Impact™ (TEI) を実施しました。この調査目標を実現するため、Forrester は IBM Guardium を使用している大手企業 3 社にアンケート調査を実施しました。

次に、この 3 社の特性に基づいてモデル組織を作成しました。このモデル組織の財務モデルは TEI 法を用いて構築しました。

最後に、アンケート調査を実施した企業が指摘した問題点や懸念事項に基づいて、財務モデルのリスク調整を行いました。調査対象の企業には費用や便益の見積もりを依頼しましたが、項目によっては回答にばらつきがあり、結果に影響する外的要因も多いため、費用と便益の総額についてリスク調整を行っています。リスク調整の詳細については各項で説明しています。

Guardium の論拠

Forrester は調査を実施した企業に対し、データ セキュリティに関して直面しているビジネス上の課題について尋ねました。この面接調査によって、企業データのセキュリティに投資しなければならない理由について、以下のような共通要因があることが明らかになりました。

- 規制やコンプライアンスの要件を満たす必要があるため
- Hadoop、NoSQL、インメモリなど、ビッグ データ プロジェクトに関連して、データ セキュリティとコンプライアンスの強化が必要になるため
- セキュリティ、コンプライアンス、データ プライバシー戦略に対する注目度が上がり、組織内での重要性が増しているため
- データ セキュリティとコンプライアンス戦略に対して、受動的ではなく、より積極的になることが求められているため
- 事前監査を実施できないことから、将来起こるリスクを最小限に抑える必要があるため

Guardium に投資する前、アンケート調査を実施した組織では、さまざまなツール、社内開発したソリューション、手動のプロセスなど、寄せ集めのアプローチを使用してデータ セキュリティとコンプライアンスを管理していました。こうした寄せ集めのアプローチは、セキュリティとコンプライアンスに対する最近のニーズでは、不十分かつ不適切と見なされています。調査を実施した各企業は、競合製品の中から Guardium を選択していますが、面接調査から以下のような選択理由が明らかになりました。

- **コンプライアンスのレポートと監査の要件を満たすことができる。**調査企業は、Guardium によって特権を有するユーザーの監視や、未承認アクセスのブロックにも効果があると回答しています。Guardium は、データ プラットフォーム、データベース、データ ウェアハウス、Hadoop、ビッグ データ、リポジトリ、ファイルとアプリケーション、プロトコルなどが異なる多種多様な環境をすべて対象にします。
- **以前の環境を所持していなくても、機微なデータへの視認性が向上する。**調査企業は、Guardium が機微なデータへの視認性を向上し、そうしたデータを発見、理解、および分類するのに役立つと回答しています。時折機微なデータを見落とすことがあっても、Guardium は問題が起こりそうな原因を明らかにするのに役立つことがわかりました。企業がビッグ データ プロジェクトを数多く手掛けるようになると、データ セキュリティの危険性が増加するため、機微なデータが存在する場所を適切に把握しておくことがますます重要になります。さらに、Guardium は自社のデータに対する新たな洞察を見出し、企業データに関する決定を以前よりも賢明かつ適切に行えるようにします。
- **環境全体に散在する機微なデータのセキュリティの確保と保護に役立つ。**組織の機微なデータへの視認性を向上できるだけでなく、Guardium は組織の機微なデータをリアルタイムに保護し、セキュリティを確保するのに役立っています。Guardium は、環境全体へのアクセスを絶えず監視、制御し、データベース、データ ウェアハウス、Hadoop、NoSQL、インメモリ システム、ファイル共有などのデータ リポジトリのセキュリティを確保します。
- **IBM がデータのセキュリティとコンプライアンスの分野での信頼のおける業界リーダーであるため。**調査企業は、当該分野に信頼できる環境を生み出した強力なパートナーと連携していると感じていました。また、スケーラブルなソリューションは、Guardium がさまざまな規模の環境をサポートできることを意味します。そして、その非侵襲設計により、Guardium は組織のデータベースやデータ ウェアハウスのパフォーマンスに悪影響を与えません。つまり、Guardium に投資することによって、運用を単純化しながら、データ セキュリティの企業戦略の品質を向上できます。

分析結果

面接調査の結果に基づいて TEI の枠組みとモデル組織を作成した後、費用便益分析/ROI 分析を行いました。これにより、経済的に影響を受ける分野が明らかになりました。このような結果に基づいて構築したモデル組織は、以下の特性を備えています。

- モデル組織は、20,000 人の従業員を擁し、年間売上高 10 億ドルを超える、米国の金融サービス企業です。
- モデル組織は、Sarbanes-Oxley、PCI DSS、およびデータ プライバシーによって課せられる監査要件に効率的かつ効果的に準拠するように、自社のデータベースに対してセキュリティと監査の機能を必要としています。財務データに試みられたアクセスをすべてログに記録する必要があります。疑わしいアクセス要求は分析し、定義済みのポリシーに従っていることを確認する必要があります。ネットワークとローカルのトラフィックはすべて Guardium システムによって監視されています。
- モデル組織は、大規模異種データベース環境を所持しています。現状では、多くのエンタープライズ アプリケーションから約 8,000 件のデータベース アクセスが行われています。データベースのサイズは、格納されるデータの種類と毎年のデータ量の増加に応じて、100GB ～ 1TB になります。サーバーは、複数のマルチコア IBM System x86 サーバーで構成されています。
- モデル組織は、SOX、PCI DSS、およびデータ プライバシーに関連する機微なデータベース サーバーに関与するすべてのアクセスと変更を監視するために Guardium ソリューションを購入しました。Guardium は多種多様なデータベースやアプリケーションを幅広くサポート対象にするため、モデル組織は企業全体に 1 つのソリューションを導入するだけです。

便益

Guardium に投資した結果としてモデル組織にもたらされる便益は以下のとおりです (定量的に評価した便益のみ)。

- セキュリティとコンプライアンスの要件を満たす際の処理効率の向上
- データ侵害からの回復費用の削減
- 規制による罰金の恐れの減少
- 監視や監査の機能の社内開発作業費用の回避
- 監査や監視の機能の運用中の社内サポート作業費用の回避

セキュリティとコンプライアンスの要件を満たす際の処理効率の向上

本調査で明らかになった最初の便益は、セキュリティとコンプライアンスの要件を満たす際の処理効率の向上です。Guardium を導入することにより、モデル組織では、データベースのセキュリティ、監査プロトコル、およびレポート機能を改善、自動化することができ、スタッフはセキュリティ要件を迅速に処理できるようになりました。制御が自動化され集中管理されるようになったことと、監査のレビュー処理が単純になったことで処理効率が上がり、コンプライアンスに関する時間と費用が削減されます。Guardium によって、データベース管理者、データ プライバシーの専門家、監査担当者など、個々のスタッフの処理効率が向上し、モデル組織の費用が削減されます。

セキュリティとコンプライアンスの要件を満たす際に向上した処理効率を計算するため、モデル組織ではセキュリティとコンプライアンスの要件を満たすのに、45 人の DBA とそれ以外に前述の役割を担う 5 人の担当者が関与していると推定します。各 DBA はセキュリティとコンプライアンスの問題に自身の時間の平均 40% を費やしており、他の担当者も規制とセキュリティの要件を満たす処理に自身の時間の平均 20% を費やしていると仮定します。Guardium を導入することにより、モデル組織では 1 年目にこうした要件に費やす時間を 10% 削減できたと見ています。時間が経つにつれ、チームのメンバーが Guardium の使い方に徐々に慣れていくため、3 年目には、セキュリティの要件に費やす時間を 20% 削減できます。Forrester では、こうして削減される時間の 50% しか生産的な仕事に使われていないと想定しています。表 1 にこの便益の計算方法を示します。

チームがセキュリティの要件に費やす時間を削減できる要因はたくさんあります。このような変動要因を考慮して、本調査ではこの便益についてリスク調整率 10% で下方修正しています。この結果、リスク調整後の総便益は、3 年間で合計 390,242 ドルになります。

本調査では、ビッグ データ プロジェクトのセキュリティとコンプライアンスの確保については直接計算していませんが、そのような計算が必要になる場合は、この処理効率の向上の影響の大きさを考慮することをお勧めします。

表 1
セキュリティとコンプライアンスの要件を満たす際の処理効率の向上

参照番号	評価項目	計算式	1 年目	2 年目	3 年目
A1	DBA の人数		45 人	45 人	45 人
A2	セキュリティとコンプライアンスに関与する DBA 以外のスタッフの人数		5 人	5 人	5 人
A3	セキュリティとコンプライアンスの問題に DBA が費やす時間の割合		40%	40%	40%
A4	セキュリティとコンプライアンスの問題に DBA 以外のスタッフが費やす時間の割合		20%	20%	20%
A5	年間給与の平均		125,000 ドル	125,000 ドル	125,000 ドル
A6	IBM Guardium を使うことによってセキュリティとコンプライアンスの問題に費やす時間が削減される割合		10%	15%	20%
A7	捕捉率		50%	50%	50%
At	セキュリティとコンプライアンスの要件を満たす際の処理効率の向上	((A1*A3)+(A2*A4)) *A5*A6*A7	118,750 ドル	178,125 ドル	237,500 ドル
	リスク調整率	↓ 10%			
Atr	**セキュリティとコンプライアンスの要件を満たす際の処理効率の向上 (リスク調整後)**		**106,875 ドル**	**160,313 ドル**	**213,750 ドル**

資料：Forrester Research, Inc.

データ侵害からの回復費用の削減

Guardium を導入することにより、モデル組織では、コンプライアンスを強化するデータベースのセキュリティ、監査、レポートの各機能の効果と効率が大幅に向上しました。また、ユーザーの利用状況を監視して、潜在的な脅威をリアルタイムに検出し、対応できるようになりました。Guardium の監視と監査、脆弱性管理、データ変換、リアルタイム セキュリティ ポリシー、インテリジェント レポートを使用すれば、社内外の脅威を特定して保護できます。

こうした機能により、組織のレコードに対するデータ侵害が起こった場合に課せられる可能性がある多額の費用を回避することもできます。本調査では、データ侵害が起きる確率を年間 12% と推定しています。データ侵害によって被る実際の費用は天文学的数値に上る可能性がありますが、本調査では控えめに見積もり、データ侵害によってモデル組織が負担する可能性のある平均費用を年間約 300 万ドルと推定しています。この費用には、データ侵害の検出費用、法的費用、調査費用、管理経費、顧客のサポート費用、顧客離れによる収入減などを含みます。Guardium の特性や機能により、モデル組織ではデータ侵害の恐れを大幅に低下させることができるようになります。セキュリティ チームがデータの分析に徐々に慣れていくにつれ、データ侵害の恐れは毎年低下していきます。本調査では、3 年目には、データ侵害の恐れが 45% 削減されると見込んでいます。

データ侵害の費用やデータ侵害の確率低下に影響する外的要因は多数あります。この点を考慮して、本調査ではこの便益値を 10% 下方修正しています。この結果、リスク調整後の総便益は合計 276,897 ドルになります。表 2 にこの便益の計算方法を示します。

本調査では、この便益について控えめな計算を行っています。Guardium のリアルタイムのセキュリティと監視により、IBM は積極的なデータの保護とデータ侵害の除去を支援しています。独自の環境に Guardium を導入した場合の全体的な影響を評価するときは、この点を考慮に入れることをお勧めします。また、データ侵害がビッグ データ プロジェクトに与える影響の程度を検討しておくことが重要です。ビッグ データ プロジェクトには大量のデータが関係するため、データ侵害の危険性はますます大きくなり、組織が負担する費用も多額になります。

表 2
データ侵害からの回復費用の削減

参照番号	評価項目	計算式	1 年目	2 年目	3 年目
B1	データ侵害の平均費用		3,000,000 ドル	3,000,000 ドル	3,000,000 ドル
B2	データ侵害の確率		12%	12%	12%
B3	IBM Guardium によるデータ侵害の恐れの低減		25%	35%	45%
Bt	データ侵害からの回復費用の削減	B1*B2*B3	90,000 ドル	126,000 ドル	162,000 ドル
	リスク調整率	↓ 10%			
Btr	**データ侵害からの回復費用の削減 (リスク調整後)**		**81,000 ドル**	**113,400 ドル**	**145,800 ドル**

資料：Forrester Research, Inc.

規制による罰金の恐れの減少

データ侵害の費用の他にも、規制に準拠できなかった場合に法廷や規制団体から罰金が科せられるという大きなリスクがあります。Guardium を導入することにより、モデル組織では、コンプライアンス監査プロセス全体を自動化することで効果と効率が大幅に向上しました。

その結果、罰金を科せられる恐れを減少させることができます。このリスクを計算するため、本調査では罰金額を推定しています。実際の罰金額を予測することは困難ですが、本調査では控えめに見積もり、コンプライアンスを証明する適切な手段がないものとして、毎年 2500 万ドルの罰金が科せられると見込んでいます。Guardium を導入することにより、モデル組織はセキュリティの要件を満たす能力が向上し、罰金を科せられる確率が 2% に減少します。表 3 は、この便益の計算方法を示しています。本調査では、この計算に影響する可能性のある変動要素が多数あることを考慮しています。こうしたリスクを想定して、この便益を 15% 下方修正しています。その結果、リスク調整後の 3 年間総便益は合計 1,056,912 ドルになります。

ビッグ データに関連して法規制による罰金の可能性を考えると、罰金額や罰金の確率は増加すると見込まれます。本調査ではこの計算を直接行っていませんが、Gaurdium を使用することによってこのリスクは低減されます。

表 3
規制による罰金の恐れの減少

参照番号	評価項目	計算式	1 年目	2 年目	3 年目
C1	規制による平均罰金額		25,000,000 ドル	25,000,000 ドル	25,000,000 ドル
C2	罰金を科せられる確率		2%	2%	2%
Ct	規制による罰金の恐れの減少	C1*C2	500,000 ドル	500,000 ドル	500,000 ドル
	リスク調整率	↓ 15%			
Ctr	**規制による罰金の恐れの減少 (リスク調整後)**		**425,000 ドル**	**425,000 ドル**	**425,000 ドル**

資料：Forrester Research, Inc.

監視や監査の機能の社内開発作業費用の回避

モデル組織では、Guardium の導入により、代替ソリューションの開発費用を負担する必要がなくなりました。本調査で比較のために使用した「代替オプション」は、監査ログを取得、格納するためにデータベースプラットフォームがネイティブに提供するログ記録機能に基づいています。モデル組織では、この情報を解析して報告書を作成後、監査担当者や管理担当者にこの報告書を配布するために、新しいソフトウェアとスクリプトを社内で作成する必要があります。ただし、ログ記録ユーティリティはその性質上バッチ処理なので、社内開発するソリューションには Guardium 製品が提供するようなリアルタイムのセキュリティ制御は行われないことに注意してください。また、Guardium 製品と同レベルの自動機能や分析機能も提供できません。

データベースの監視と監査のための手動社内ソリューションなど、代替ソリューションを開発する場合、モデル組織は 3 人の開発者が 8 週間 (960 人/時) の工数をかけて、データベースの監査アクセス情報を安全にログ記録、保存、分析して、報告書にするのに必要な機能を開発、テスト、導入することになります。2 年後には、機能強化のために、初期開発の半分、つまり 480 人/時の作業も必要になると考えられます。表 4 にこの便益の計算方法を示します。

こうしたソリューションを開発するチームの能力に影響する要因はたくさんあります。このような変動要因を考慮して、本調査ではこの便益についてリスク調整率 10% で下方修正しています。この結果、リスク調整後の総費用削減は、3 年間で合計 73,261 ドルになります。

表 4
監視や監査の機能の社内開発作業費用の回避

参照番号	評価項目	計算式	導入時	1 年目	2 年目
D1	監視や監査の機能を社内開発するための作業工数 (人/時)	8 週間 * 3 人の開発者	960		480
D2	平均時給		60 ドル		60 ドル
Dt	監視や監査の機能の社内開発作業で回避される費用	D1*D2	57,600 ドル		28,800 ドル
	リスク調整率	↓ 10%			
Dtr	**監視や監査の機能の社内開発作業で回避される費用 (リスク調整後)**		**51,840 ドル**	**0 ドル**	**25,920 ドル**

資料：Forrester Research, Inc.

監査や監視の機能の運用中の社内サポート作業費用の回避

ソリューションの開発費用に加えて、モデル企業では、運用中のメンテナンスを担当するスタッフも 3 人必要になります。まず、専任の DBA が必要です。この DBA は、運用中のデータベース サポートを担当し、ログ データや監査データの保存と分析をサポートすると同時に、すべてのデータベース アクセスを報告する役割も担います。運用中のサポートを行う残りの 2 人のスタッフは、アプリケーション サポートのスペシャリストで、運用中の DBA 以外 (アプリケーションや DBA 以外のパワー ユーザー) からのデータベース アクセスの監査と報告を担当すると同時に、現在は Guardium システムによって可能になっている、データベースのエラー診断、トラブルシューティング、パフォーマンスの改善などのサポートも提供します。

この 3 人の担当者の平均年収を 125,000 ドルと推定します。表 5 にこの便益の計算方法を示します。この結果、リスク調整後の総費用削減は、3 年間で合計 839,313 ドルになります。

ここでもこの計算に影響する要因を考慮して、この便益のリスク調整として 10% 下方修正しています。

表 5
監査や監視の機能の運用中の社内サポート作業費用の回避

参照番号	評価項目	計算式	1 年目	2 年目	3 年目
E1	不要になる担当者数		3 人	3 人	3 人
E2	年間給与の平均		125,000 ドル	125,000 ドル	125,000 ドル
Et	監査や監視の機能の運用中の社内サポート作業で回避される費用	E1*E2	375,000 ドル	375,000 ドル	375,000 ドル
	リスク調整率	↓ 10%			
Etr	**監査や監視の機能の運用中の社内サポート作業で回避される費用 (リスク調整後)**		**337,500 ドル**	**337,500 ドル**	**337,500 ドル**

資料：Forrester Research, Inc.

総便益

以下の表に、上記で定量化した全便益の総額と、関連する現在価値 (割引率 10%) を示します。3 年間にモデル組織にもたらされる総便益のリスク調整後の現在価値は 260 万ドルになります。

表 6
総便益のキャッシュ フロー (リスク調整後見積値)

参照番号	便益項目	導入時	1 年目	2 年目	3 年目	合計	現在価値
Atr	セキュリティとコンプライアンスの要件を満たす際の処理効率の向上	0 ドル	106,875 ドル	160,313 ドル	213,750 ドル	480,938 ドル	390,242 ドル
Btr	データ侵害からの回復費用の削減	0 ドル	81,000 ドル	113,400 ドル	145,800 ドル	340,200 ドル	276,897 ドル
Ctr	規制による罰金の恐れの減少	0 ドル	425,000 ドル	425,000 ドル	425,000 ドル	1,275,000 ドル	1,056,912 ドル
Dtr	監視や監査の機能の社内開発作業で回避される費用	51,840 ドル	0 ドル	25,920 ドル	0 ドル	77,760 ドル	73,261 ドル
Etr	監査や監視の機能の運用中の社内サポート作業で回避される費用	0 ドル	337,500 ドル	337,500 ドル	337,500 ドル	1,012,500 ドル	839,313 ドル
	総便益 (リスク調整後)	**51,840 ドル**	**950,375 ドル**	**1,062,133 ドル**	**1,122,050 ドル**	**3,186,398 ドル**	**2,636,625 ドル**

資料：Forrester Research, Inc.

費用

モデル組織では IBM Guardium ソリューションの導入に伴い、以下のようなさまざまな費用が発生します。

› Guardium の導入費用と年間保守費用

› 計画、導入、およびプロフェッショナル サービスの費用

これらは、モデル組織において、本ソリューションに関する最初の計画策定、導入、および運用中の保守のために発生する内部費用と外部費用に相当します。

総費用

以下の表に、総費用と、関連する現在価値 (割引率 10%) を示します。3 年間にモデル企業が負担する総費用のリスク調整後の現在価値は 828,085 ドルになります。

表 7
総費用のキャッシュ フロー (リスク調整後見積値)

参照番号	費用項目	導入時	1 年目	2 年目	3 年目	合計	現在価値
Ftr	Guardium の導入費用と年間保守費用	555,500 ドル	99,990 ドル	99,990 ドル	99,990 ドル	855,470 ドル	804,160 ドル
Gtr	計画、導入、およびプロフェッショナル サービスの費用	23,925 ドル	0 ドル	0 ドル	0 ドル	23,925 ドル	23,925 ドル
	総費用 (リスク調整後)	**579,425 ドル**	**99,990 ドル**	**99,990 ドル**	**99,990 ドル**	**879,395 ドル**	**828,085 ドル**

資料：Forrester Research, Inc.

結果のまとめ

「便益」と「費用」の各項で計算した数値に基づき、モデル組織が IBM Security Guardium を導入した場合の ROI、NPV、および回収期間を算出しました。

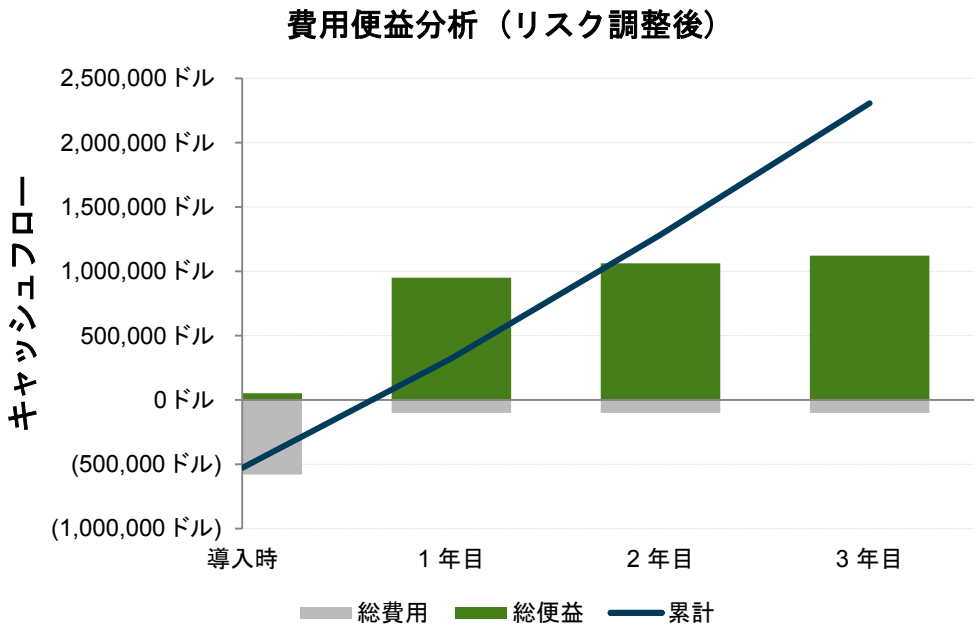
以下の表に、ROI、NPV、および回収期間のリスク調整後の値を示します。

キャッシュ フロー分析 (リスク調整後見積値)

項目	導入時	1 年目	2 年目	3 年目	合計	現在価値
総費用	(579,425 ドル)	(99,990 ドル)	(99,990 ドル)	(99,990 ドル)	(879,395 ドル)	(828,085 ドル)
総便益	51,840 ドル	950,375 ドル	1,062,133 ドル	1,122,050 ドル	3,186,398 ドル	2,636,625 ドル
合計	**(527,585 ドル)**	**850,385 ドル**	**962,143 ドル**	**1,022,060 ドル**	**2,307,003 ドル**	**1,808,540 ドル**
ROI (投資利益率)						**218%**
回収期間						**7.4 ヶ月**

資料：Forrester Research, Inc.

以下のグラフは、リスク調整後のキャッシュ フローを示しています。



資料：Forrester Research, Inc.

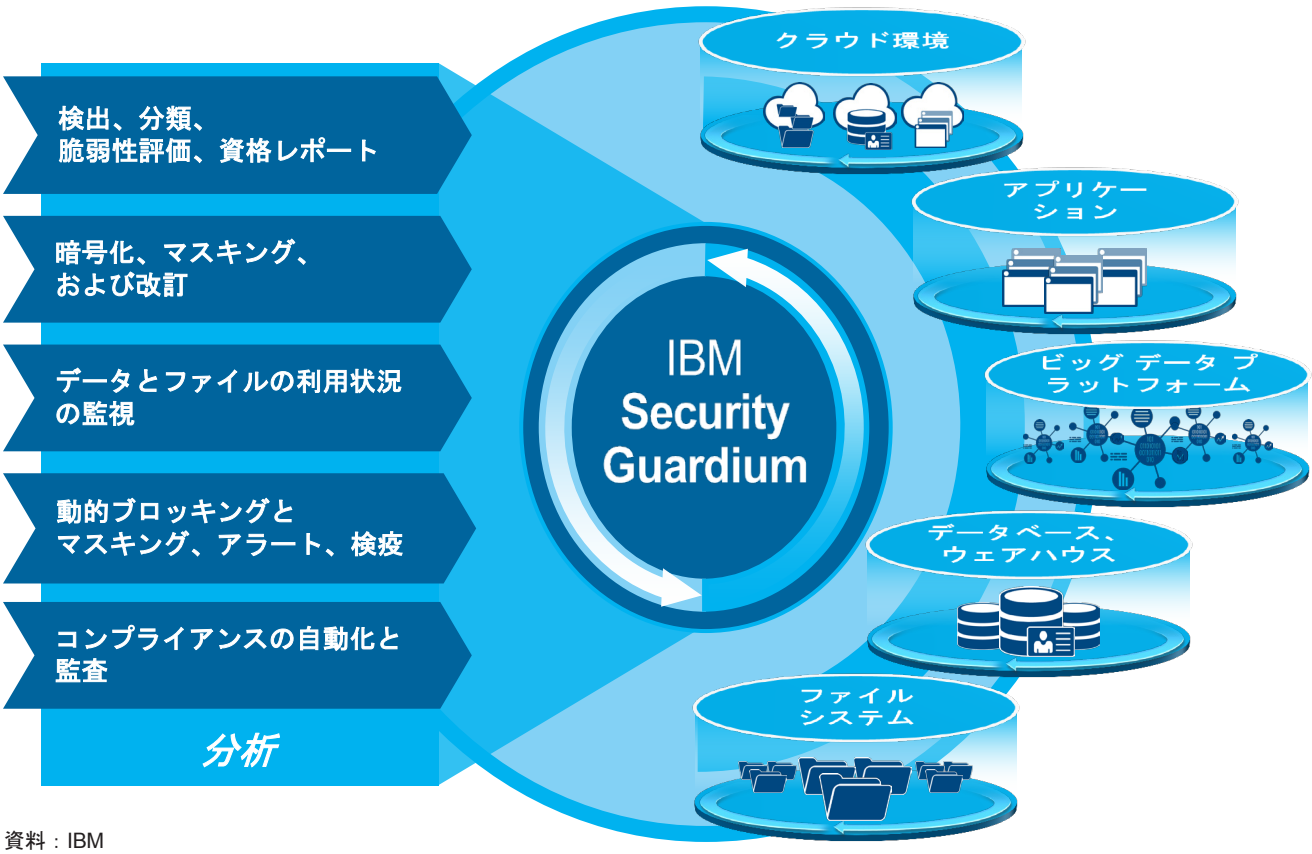
IBM Guardium について

以下の情報は IBM により提供されたものであり、Forrester はいかなる申し立ても一切受け付けず、また、IBM または同社の製品を推薦しているわけでもありません。

IBM Security Guardium (旧称、IBM InfoSphere Guardium) は、重要なデータを、そのデータが存在する場所を問わず、安全に保護するよう設計されています。この包括的なデータ保護プラットフォームにより、セキュリティ チームは、データ環境全体で何が起きているかを自動的に分析できるようになり、リスクを最小限に抑え、社内外の脅威から機微なデータを保護し、データ セキュリティに影響する変更をシームレスに適合させることができます。

Guardium は、大半の組織にとって中核をなすデータ、つまり、ビジネスを成功に導き、事業を存続させるために不可欠となる機微なデータを保護するための包括的なアプローチを提供します。Guardium のエンドツーエンドのグラフィカル インターフェイスを利用して、セキュリティ チームは、機微なデータが移動中か静止中かを問わず、データに対するリスクを特定し、修正できます。また、この統一アプローチは、データベース、データ ウェアハウス、Hadoop システム、NoSQL システム、インメモリ システム、ファイル システムなど、構造化されたデータのリポジトリにも構造化されていないデータのリポジトリにも広範囲に拡張されます。

実際には、Guardium は柔軟性のあるモジュール形式のアプローチを使用して、基本的なコンプライアンス、監視、暗号化から包括的なデータ保護に至るまで、データ セキュリティと保護の広範な要件を、費用対効果の高い、スケーラブルな方法で満たしています。また、ポイント ソリューションとは異なり、Guardium は業界最先端のセキュリティ ソリューション、脆弱性標準、アプリケーションなどとの異種統合をサポートします。Guardium は IBM Security ソリューションとのベストオブブリードの統合も提供します。IBM は戦略的パートナーとして、最も複雑な IT 環境全体でのセキュリティ脆弱性の削減とリスクの管理を組織が実行できるようにしています。



資料：IBM

情報開示

- 本調査は IBM からの委託により、Forrester Consulting が実施しました。本調査は比較分析を目的としたものではありません。
- Forrester は、他企業が得る潜在的な投資利益に関しては何の予測も行っておりません。各組織は、本報告書で提供される枠組みに基づいて独自に数値を予測し、IBM Security Guardium への投資の妥当性を判断してください。
- IBM は本報告書の内容を確認し、Forrester にフィードバックを提供しましたが、本調査および調査結果については Forrester がこれを編集・管理する権限を有し、調査結果と矛盾する変更や調査の趣旨が曖昧になるような変更は一切行っておりません。

用語解説

割引率：キャッシュフロー分析で、貨幣の時間的価値を考慮するために使用する利率。各企業は、通常、自社の事業環境や投資環境に基づいて独自の割引率を設定します。Forrester はこの分析において、年間割引率を 10% に設定しています。これを適用する場合は、各企業の経理部と相談の上、企業内で使用する適正な割引率を設定することをお勧めします。

正味現在価値 (NPV)：利率 (割引率) が設定されている場合の (割引後の) 将来の正味キャッシュフローの現時点での価値。あるプロジェクトの正味現在価値が正である場合、通常は、投資すべきであることを意味します。ただし、他のプロジェクトの正味現在価値の方が高い場合は別です。

現在価値 (PV)：利率 (割引率) が設定されている場合の (割引後の) 見積もり費用および便益の現時点での価値。費用および便益の現在価値からキャッシュフローの正味現在価値の合計を計算します。

回収期間：投資金額が回収され、損益分岐点に到達するまでの期間。正味利用価値 (利用価値からコストを引いた値) が初期投資に等しくなる時点。

投資利益率 (ROI)：プロジェクトに投資した金額に対する、期待される利益の割合。ROI は、正味利益 (便益から費用を引いた値) を費用で割ることによって求められます。

内部収益率 (IRR)：一連の正負のキャッシュフローの正味現在価値 (NPV) をゼロとする割引率。

FORRESTER CONSULTING について

Forrester Consulting は、企業からの委託により第三者機関として客観的な調査を行い、これに基づくコンサルティングを提供することで事業の成功を支援しています。短期の戦略セッションから個別のご要望に応じた長期のプロジェクトまで、専門知識と経験が豊富な Forrester Consulting のリサーチ アナリストが直接お客様に対応し、それぞれのビジネスに関する課題について専門的な知見を提供いたします。詳細につきましては、forrester.com/consulting をご覧ください。

TEI について

Total Economic Impact™ (TEI) は、Forrester Research によって開発された手法です。TEI は、テクノロジーに関する社内の意思決定プロセスの構築に役立ちます。また、ベンダーが自社の製品やサービスの価値提案を顧客に伝える際にも役立ちます。TEI 手法は、組織の経営幹部他の主要ビジネス利害関係者に向けて、IT イニシアチブの有形資産価値を実証、正当化および実現化する際に有益です。TEI 手法は、投資価値を評価するための 4 つの要素 (利用価値、コスト、リスク、柔軟性) で構成されています。

http://www.forrester.com/marketing/product/consulting/tei.html