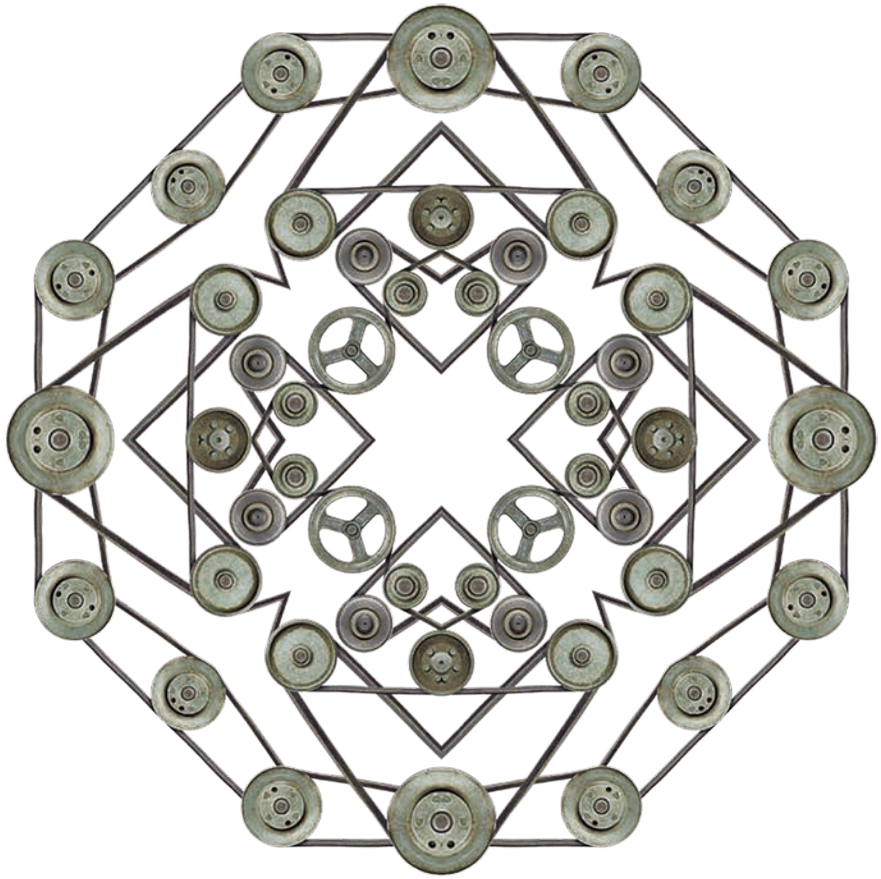
Deloitte.
デロイト トーマツ



All together now

サードパーティーのガバナンスとリスクマネジメント

EERMグローバル調査2019

目次

序文

今年度の拡大企業リスクマネジメント（EERM：Extended Enterprise Risk Management）グローバル調査をご覧いただき、ありがとうございます。私たちがこの調査を4年前に開始した目的は、EERMの成熟を目指す各企業の道のりにおける経験、機会および課題の共有にありました。EERMが成熟すると、サードパーティーリスクマネジメントへのアプローチは、組織全体にわたって統合され、一貫性を持った、トップ先導型となります[1]。

Kristian Park
EMEA Leader, Extended Enterprise Risk Management
Global Leader, Third-party Risk Management
Global Risk Advisory

今年の調査には、1,055人[2]、世界19カ国[3]という、これまでで最多の人数の回答者の方々にご協力いただいたことを私は誇らしく思っています。これには、サードパーティーリスクマネジメントへの関心とリーダーシップによる注目が高まりつつあることが反映されています。

この調査は、2018年11月から2019年1月にかけて実施され、この期間の景況感が結果に影響しています。グローバルな経済成長の鈍化の兆しが明らかになり始め、組織の不確実性の高まりを伴っています。本調査では、各企業が効率化を進めており、いかにこの変化を認識しているかが明らかになっています。

今年の主な所見は、以下のとおりです。

- EERMの成熟への投資のドライバーは、コスト削減への意欲が最大であり、サードパーティー関連のインシデントの削減、規制、社内の精査が続きます。

- 慢性的な投資不足によって、企業が目指すEERM成熟度の達成が困難となっています。さらに根本的に、基本となるコアタスクの適切な実行が阻害されている企業が多く見られます。「基本ができていないこと」が原因で、最先端のイニシアティブとソリューションによる恩恵を最大限に得ることが不可能な状態になっています。

- 効率性の追求のため、企業は数多くのソリューションの導入を求められています。この潮流には以下を含みます。中央の経営幹部、組織ユニットおよびカントリーチームが責任を共有する「フェデレーテッド構造」、「エマージングテクノロジー」、「シェアードアセスメントおよびユーティリティ」、「マネージドサービスデリバリーモデル」です。また、各企業は、イネーブリングテクノロジーの標準化および簡素化に取り組んでいます。

- 取締役会および経営幹部は引き続き、サードパーティーリスクマネジメントに深い関心を寄せ、より調整され実態を踏まえたインプットを求めています。これは、実行可能なインテリジェンスへの投資に反映されており、また、あらゆるリスクについて、組織全体にわたって情報を集約し、分析することを目指すものです。

- 新たなインサイトとして、企業がEERMの向上を目指そうとすると、EERMの経験が豊富で、EERMを主導できる人材を採用するために、十分な資金を費やす必要があることが徐々に認識されています。

本レポートの豊かな情報が、EERMの取り組みを進める企業の皆様にとって、EERMにおける主な動向と展開についての理解を深める一助となれば幸いです。

堅牢なEERMガバナンスが企業の成功に不可欠

企業は、人材、最先端テクノロジー、さらには堅牢なオペレーティングモデルへの投資によって、サードパーティーリスクの管理の改善を図ろうとしています。この市場における劇的な市場の変化と効率性の追求は、EERMへの注目が高まり続ける一因となっています。

過去3年間にサードパーティー関連のインシデントを経験した企業は、83%という驚くべき割合に上る一方、すべての重要なEERM問題への取り組みが「最適化」されている、と自社をとらえている企業は、わずか1%に過ぎず、EERM領域への投資不足が顕著に映し出されています。

20%の回答者は、大半のEERM要素に対応していると述べている一方で、50%は「管理化」というカテゴリーに位置付けていますが、デロイトの所見によると、これらは戦略的な長期ソリューションというよりは、ターゲットを絞った戦術的な改善を重視した、断片的な投資であることが示されています。

今回の調査では、取締役会がEERMに対するインサイドアウトアプローチを支持していることが明らかになっており、これには、より優れた関与、協調、データのよりスマートな使用が含まれます。さらにリーダーは、イノベーションの推進を目指しています。今年の所見によると、サードパーティーリスクに関する役員向け報告を目的とし、オンラインで生成され、簡潔でリアルタイムに実行可能なインテリジェンスが出現しています。

サードパーティーリスクマネジメントについては、より持続可能なオペレーティングモデルが受け入れられつつあります。このモデルの特徴としては、センターオブエクセレンスとシェアードサービスセンターによって支えられるフェデレーテッド構造、エマージングテクノロジー、シェアードアセスメントとマネージドサービスモデル、さらには予算の共同オーナーシップへの動きが挙げられます。

EERMに対するテクノロジー投資の標準化を目指す段階的手法の成長について、デロイトの予測が現実になっています。企業は、多様な業務部門にわたるサードパーティーリスクマネジメントテクノロジーの合理化および簡素化を志向しています。

サードパーティーによるネガティブな行為から生じる、企業のレピュテーション、業績、株主価値に対する影響の重大性が高まり続け、この背景から、企業が自社のEERMプロセスおよびフレームワークの改善への投資を促がされるだろうとデロイトは考えています。

EERMガバナンスの明確な指揮系統は、企業の総合的な成功に不可欠です。サードパーティーリスクを軽減し、コンプライアンスを改善し、さらに風評被害と規制上の過失を回避する目的で、説明責任を負う能力のあるEERM組織を構築する際、経営幹部は重要な役割を果たすことができます。

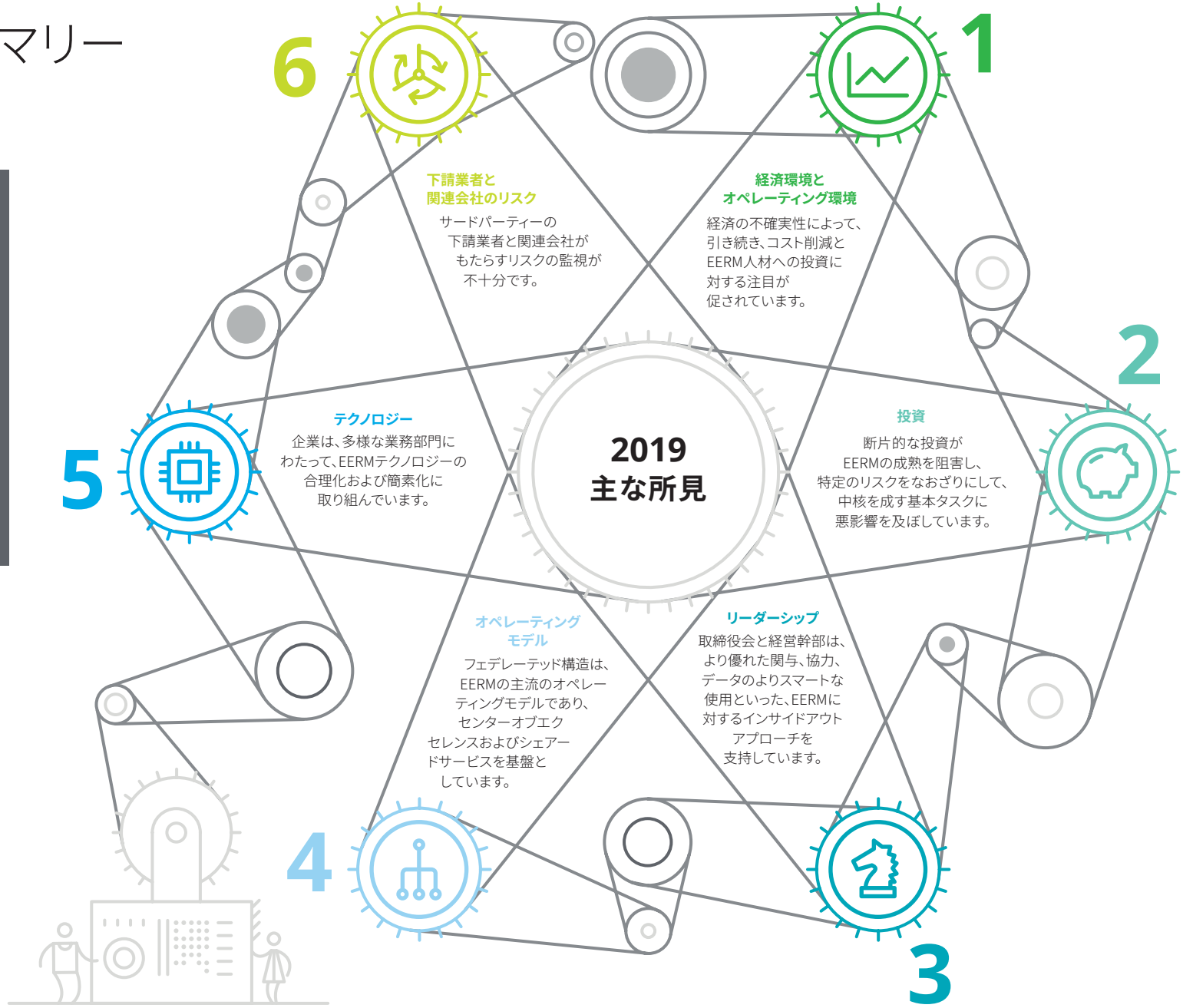
世界中のデロイトのリスクアドバイザリーのプロフェッショナルは、本調査の詳細と、サーベイでの発見事項が貴社の機会にどう関係するかについての理解を深めるお手伝いをさせていただきます。

詳しくは、www.deloitte.com/jp/risk-advisory をご覧ください。

Donna Glass
Managing Partner, Deloitte Advisory US
Business Leader, Deloitte Global Risk Advisory

エグゼクティブサマリー

多くの企業において、EERM実行の成熟化に向けた活動が改めて注目されています。これは、EERMへの投資が不足しているという認識と、経済環境の不確実性が広がるのではないかという不安が相まって、促されているようです。



1 エグゼクティブサマリー

経済環境とオペレーティング環境

調査が行われた2018年11月から2019年1月は、経済状況が不確実な時期であったことが、各企業の見通しに影響を及ぼしています。

経済とビジネスの不確実な見通しが企業に以下を強いることによって、EERMに影響を及ぼしています。

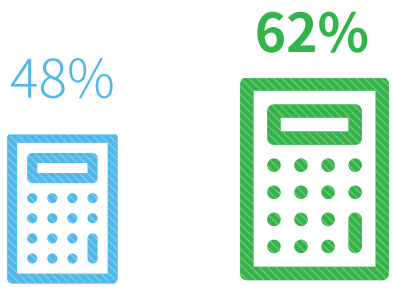
- EERMの予算と 投資に対する疑問の呈示
- コスト削減を目指して、オペレーションの効率性を改善
- サードパーティーに委託する内容に関する戦略の見直し

さらに、以下の2つの方向からの監視の強化が挙げられます。

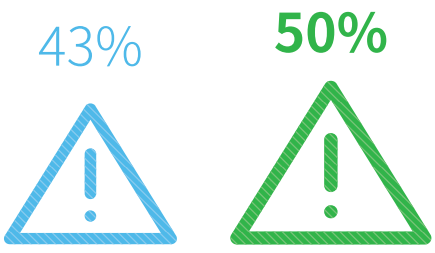
- **社外的:** 世界的に見て規制当局は、サードパーティーリスクマネジメントのフレームワークを企業が構築し、推進することを求めている。
- **社内的:** より先進的な企業においては、規制当局が適用する監視を忠実に反映させた社内コンプライアンス機構を設置している。

企業は、EERMへの投資に対する明確な動機を有する

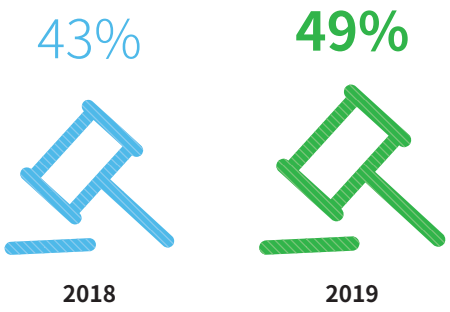
トップは昨年に引き続き、コスト削減であると**62%**の回答者が挙げており、昨年の48%から増加しました。



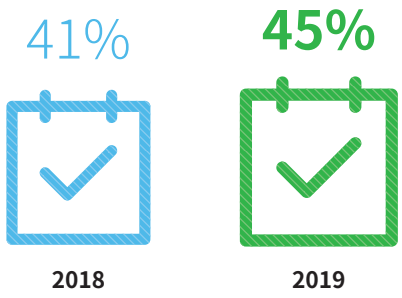
2位には、価値の保全が続きました。「サードパーティー関連のインシデント数の減少」を**50%**の回答者が選択しており、昨年の43%から増加しました。



規制当局による監視を懸念する企業が昨年より増加していると**49%**が挙げており、昨年の43%から増加しています。

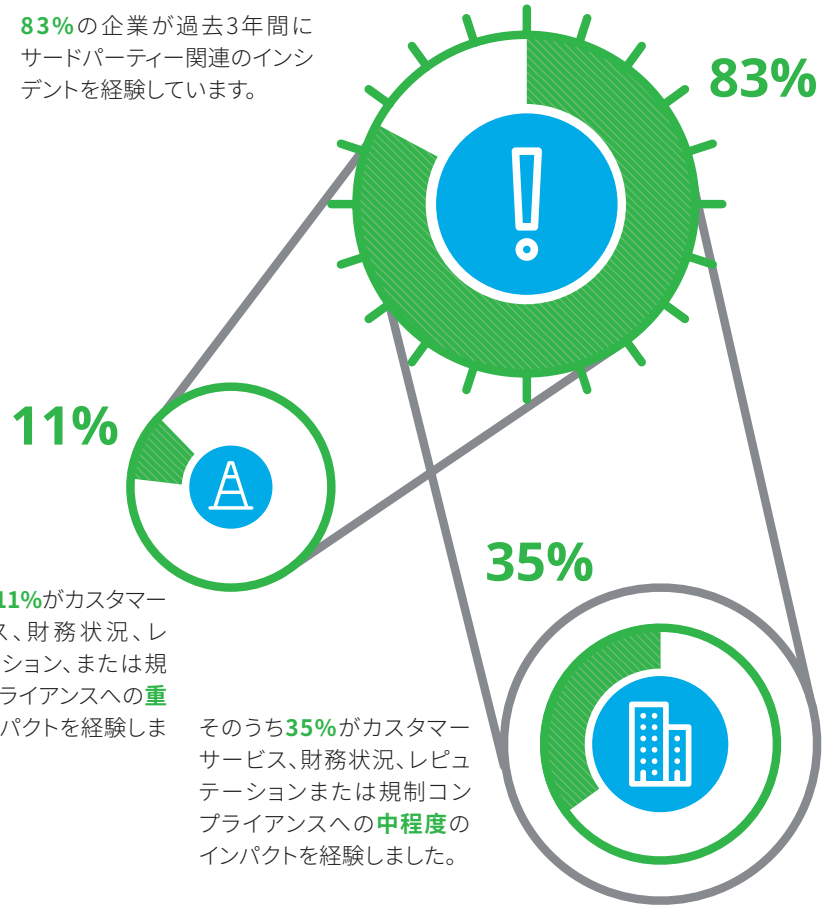


企業は、社内コンプライアンスの要求事項に従来よりも動機付けられています。この項目を理由として挙げた企業は**45%**で、昨年の41%から増加しています。



サードパーティー関連のインシデントは、引き続き、様々なインパクトを伴う混乱の原因となっています

83%の企業が過去3年間にサードパーティー関連のインシデントを経験しています。



そのうち**11%**がカスタマーサービス、財務状況、レピュテーション、または規制コンプライアンスへの**重大な**インパクトを経験しました。

そのうち**35%**がカスタマーサービス、財務状況、レピュテーションまたは規制コンプライアンスへの**中程度**のインパクトを経験しました。

企業のEERMへの信頼を損なう要素とは？

協調的で全社的に一貫したEERMへのアプローチの欠如を挙げたのは、**53%**の企業でした。

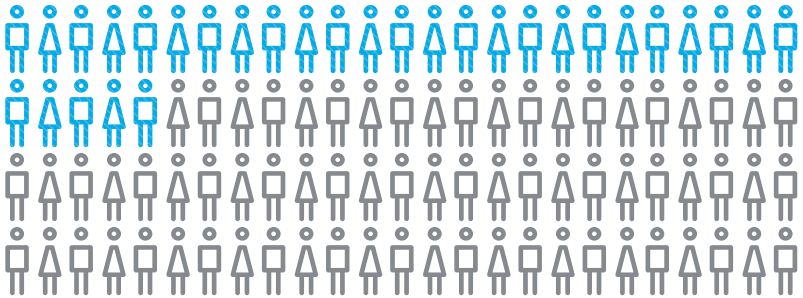
続いて、EERMに関するプロセス、テクノロジー およびリアルタイムのマネジメント情報についての懸念を挙げた企業が**49%**に上りました。

回答者は、EERMに全社的に協調し、一貫して取り組み、すべての重大リスクにおけるプロセス、テクノロジーおよびリアルタイムのマネジメント情報を改善する、という喫緊のニーズを感じています。

興味深い新しいインサイトとして、予算のプレッシャーにもかかわらず、EERMを実現するには人材投資を必要としており、現時点での投資が将来の支出を抑制するということについて、経営陣が認識している点が挙げられます。これは主に、専門家の採用を指します。また、本調査では、優先順位の変化が明らかにされています。

- 人件費は高いが、経験がありEERM活動を主導できるEERMリーダの採用が増加。
- 若手のEERMスキルを持つ人材の採用が低下：これは、サードパーティーサービスとユーティリティモデルの増加および可用性によると思われます。今年、この項目を優先項目に挙げた回答者はわずか30%でした。

30%



2 エグゼクティブサマリー

投資

企業の多くは、EERMへの投資不足を確信：

EERMへの設備投資額が理想的な金額以上であると考える企業は、10社中**3社**未満です。

EERMスタッフやその他の運営費（OPEX）に対して、理想的な金額以上を支出していると考える企業は、10社中**3社**未満です。

EERMの年間運営費（OPEX）は、企業間で顕著な差異が見られる：

EERM活動の年間運営費（OPEX）は、業種、マネジメント、EERMデリバリーモデルなどによって、顕著な差異がありました。

50%の企業の支出は、100万米ドル[5]を超えています。

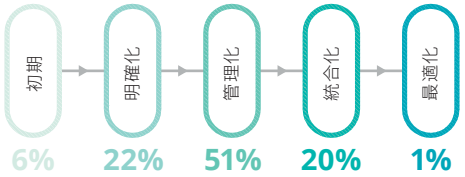
50%

11%

トップの**11%**は、それぞれ1,000万米ドルを費やし、100FTE（常勤換算で100人）以上のスタッフを雇用しています。

断片的な投資によって、EERMの成熟が損なわれる：

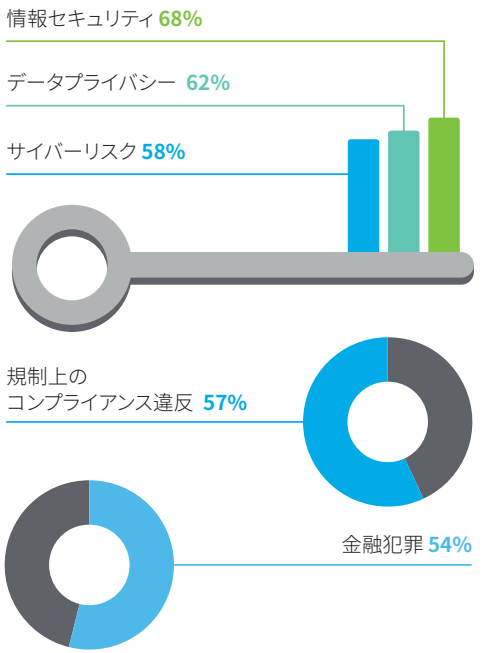
私たちは、この4年間のEERMの成熟への企業投資を追跡しました。
この長期スパンの調査によると、多くの企業が戦略的な長期ソリューションというよりは、ターゲットを絞った戦術的な改善を重視した、限定的で断片的な投資を行っています。
自社が「最適化」されており、すべてのEERM問題に対応していると考えている企業は、わずか**1%**でした。
次の**20%**は、自社が「統合化」されていると答えています。このカテゴリーは、最高レベルではないものの、大半のEERM項目に対応しています。
51%は、自社を「管理化」というカテゴリーに位置付けています。つまり、重要な要素をすべて検討していますが、改善の余地を把握しています。
22%は、自社を「明確化」の段階ととらえています。対応している要素はありますが、取り組みが限定されています。
6%は、自社が「初期」の段階にあると述べています。取り組んでいる要素は、皆無か、ごくわずかです。



デロイトEERM成熟モデルに関しては、図 2.5を参照。

投資が特定のリスクドメインに偏る：

年間の投資はその年の規制上の課題のうち最大のものに重点が置かれることが典型的です。例えば、2018年と2019年の重点項目は、情報セキュリティ、データプライバシー、サイバーリスクおよび金融犯罪でした。最も多くの企業がEERM予算を割り当てた項目は、以下のとおりです。



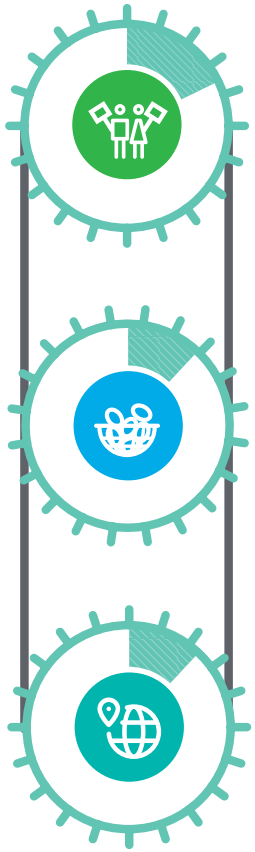
断片的なアプローチにより、特定のリスクドメインがなおざりに：

企業が年次の検証を行っていない重要な領域は、以下のとおりです。

半数近くの企業は、集中リスクを毎年検証していません。これは、EERMプロセスの一環としての能動的な対応ではなく、レポーティングを介した受け身の検証となっている傾向があります。

60%以上の企業が 重要なサードパーティーに関する出口戦略を毎年検証していません。

企業では、特定の領域に対する投資が不足しています。



わずか

18%のみが労働に関する権利に投資

12%のみが集中リスクに投資

12%のみが地政学リスクに投資

EERMへの投資不足は、「基本ができていないこと」につながる：

50%

50%の企業が個別のサードパーティーとの関係の内容を把握していません。

43%

43%が契約条件に関する知識が不十分です。

41%

41%がリスクプロファイルに基づきサードパーティーの監視を行っていません。

このため、より最先端のソリューションによる恩恵が限定され、リスクに比例して行うべきリスクマネジメントの取り組みが妨げられています。

3 エグゼクティブサマリー

リーダーシップ

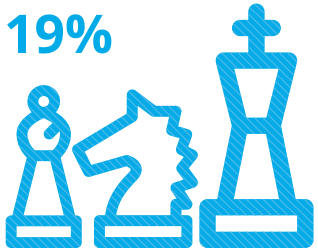
企業は引き続き、サードパーティーリスクマネジメントを戦略設定に不可欠な要素として認識しているため、EERMに関する最終的な説明責任を担うのは、ほとんどの場合、取締役会と経営幹部です。

CRO（最高リスク管理責任者）が責任を担うのが最も一般的事例の**24%**

24%

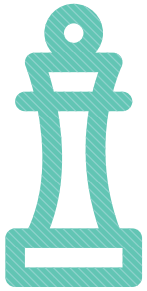
取締役会メンバーが責任を担う企業が**19%**

19%



CEO（最高経営責任者）が責任を担う企業が**17%**

17%



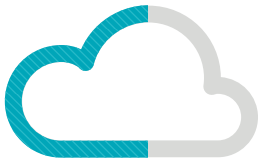
リーダーは、エマージングテクノロジーで水準を引き上げる

2018年の調査から、経営陣が取締役会およびエグゼクティブコミッティーのミーティングへの情報提供では、赤色・黄色・緑色（RAG）のダッシュボードを好んでいることが判明しました。この時点では、多くの企業は静的なRAGレポートを用いて、関連するサードパーティーのデータを定期的に分析していました。

しかし、最新調査によると、経営陣は、定期的に生成されるデータの使用から、オンラインで生成される、より簡潔かつリアルタイムで実行可能なインテリジェンスに移行しています。

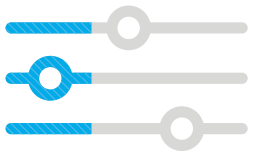
新しいリスクインテリジェンスツールは、全社的なあらゆるリスクに関する、リアルタイムの自動化情報を取り入れ、集約し、検証しています。これらのツールは、アラート、トレンド分析を提供し、シナリオ分析を可能にすると共に、クラウド、ロボティック・プロセス・オートメーションおよび人工知能を始めとするエマージングテクノロジーを用いています。

この潮流は、規制当局がリスクマネジメントと監督におけるイノベーションの推奨を開始した時期に発生しています。



56%の企業は、EERM用にクラウドベースのプラットフォームを使用中、または使用を予定しています。

56%



45%は、ロボティック・プロセス・オートメーションを使用中、または使用を予定しています。

45%

36%は、実行可能なインテリジェンスを創造するために、ビジュアリゼーション技術を使用中、または使用を予定しています。

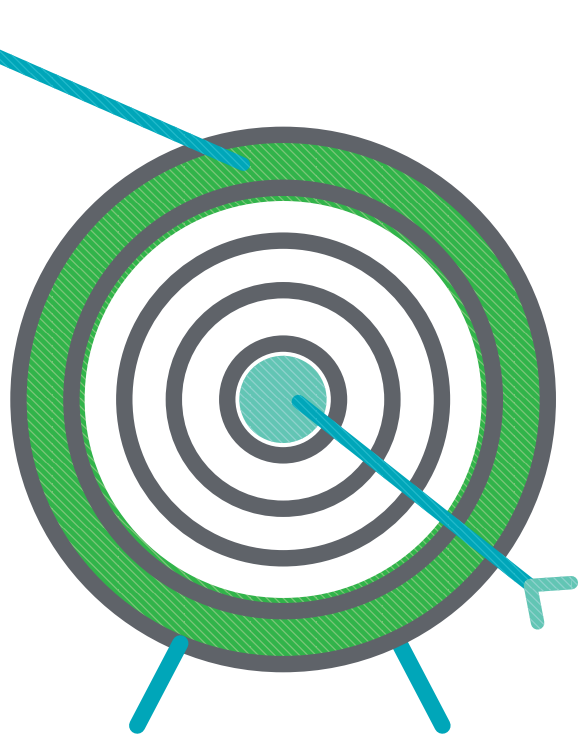
36%

取締役会が現在支持しているのは、EERMに対するこれまでのアウトサイドインのアプローチに加えて、インサイドアウトのアプローチです。このアプローチは、企業内のより優れた関与と協力によって開始され、組織ユニット、地域、リスクドメインおよび当該領域の専門家を含みます。

多くの企業が社内のEERMステークホルダーの関与と協力が不十分であることを認めている…

35%

35%は、関与と協力のレベルが低い、ほとんどない、またはわからないと答えています。



16%

わずか**16%**の企業だけが高いと確信しています。

… 一方で、改善を望んでいる：

3社に2社
は、EERMの優先実施項目として、社内の関与と協力の向上を挙げています。

37%

37%は最優先事項に掲げています。

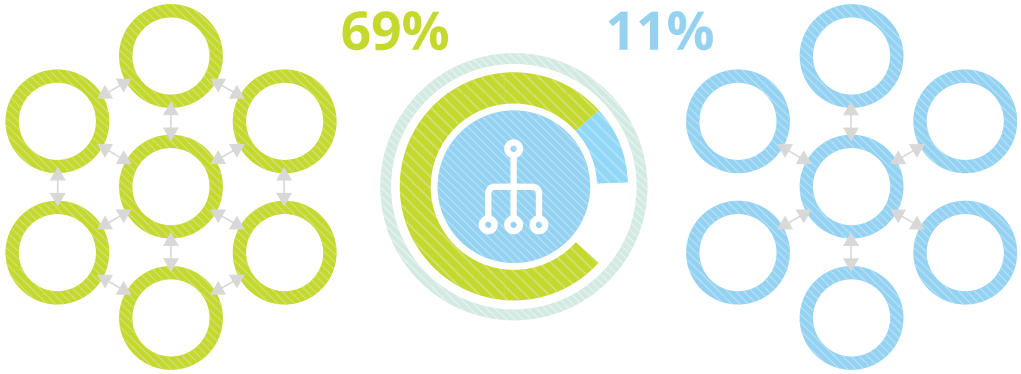
4 エグゼクティブサマリー

オペレーティングモデル

フェデレーテッド構造は、EERMのオペレーティングモデルとして主流となりつつあります。大多数の回答者が現在、このモデルを採用していると答えています。このモデルでは、様々な国の組織ユニットやリーダーが担うアカウンタビリティを中央集権的に監督し、主要ポリシー、規格、サービス、テクノロジーを組み合わせることで強化します。

69%がフェデレーテッドモデルを採用していると答えています。

わずか**11%**の企業しか、高度な一元管理を実行しておらず、昨年の17%から減少しています。



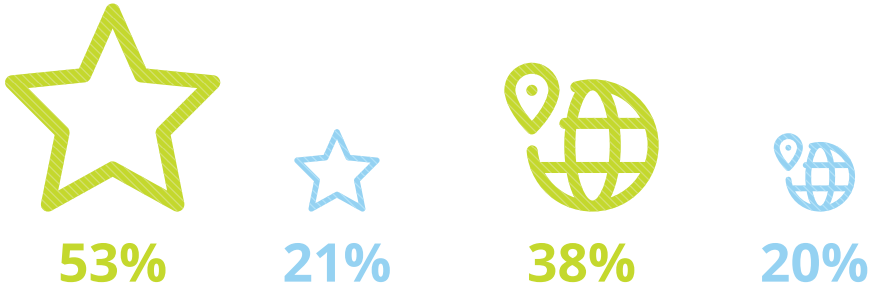
フェデレーテッド構造は通常：

- センターオブエクセレンスまたはシェアードサービス機能を基盤とする
- マネージドサービス（これにより人員および設備投資が削減される）、エマージングテクノロジーやシェアードアセスメントおよびユーティリティによるサポートが増加

企業によるセンターオブエクセレンスとシェアードサービスセンターの使用が増加：

53%の企業がセンターオブエクセレンスを使用し、さらに**21%**が設立を予定しています。

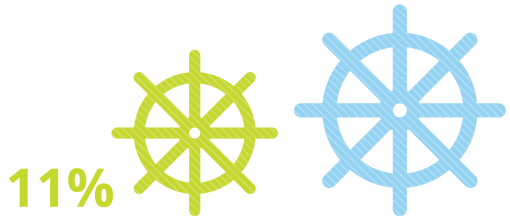
38%がシェアードサービスセンターを有し、さらに**20%**が構築を目指しています。



最新トレンドは、マネージドサービス：

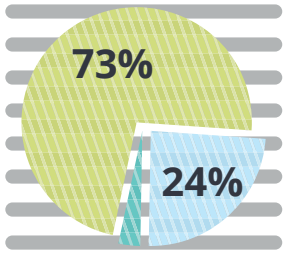
18%の企業が社内スタッフによる社外マネージドサービスプロバイダーを使用し、さらに**13%**が使用する意向です。

18%の回答者が、リスクインテリジェンスを取得するためのマネージドサービスを使用しており、さらに**21%**が使用を計画しています。



11%がサービスとしてのEERMを展開するマネージドサービスソリューションを使用し、さらに**14%**が使用を計画しています。

テクノロジー、マネージドサービスおよびユーティリティモデルの使用増加によって、資本的支出（CAPEX）を大幅に削減：



73%の企業は、次世代ソリューションの導入後、累積資本的支出（CAPEX）が年間運営費（OPEX）を上回るべきでない、と考えています。

次の**24%**は、年間運営費（OPEX）の2～3倍に下げるべき、ととらえています。

これは、昨年の回答者による、EERMの累積CAPEXが通常、年間運営費（OPEX）の3～5倍になるという見積もりから劇的に減少しています。

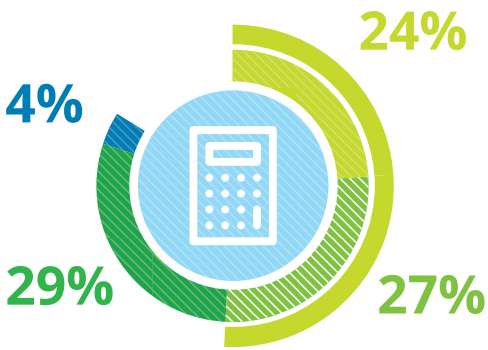
残りの**3%**は、このコストが引き続き、年間運営費（OPEX）の3倍を超えると考えています。

もう一つの新しいトレンド、予算の共同オーナーシップ：

最終的な予算管理は、組織のリーダーと調達部門などのその他の第一線の中央機能が担っています。半数以上（**51%**）の企業は、CEO／経営陣／取締役会（**24 %**）または調達（**27%**）が担っている、と述べています。

その一方で増えているのは、ビジネスユニット（**29%**）または各地域の責任者（**4%**）による共同担当です。これらの領域は、担当分野のEERM予算について発言権を持ちます。

このアプローチは、企業がアジャイルで一貫性を持つことを可能にします。

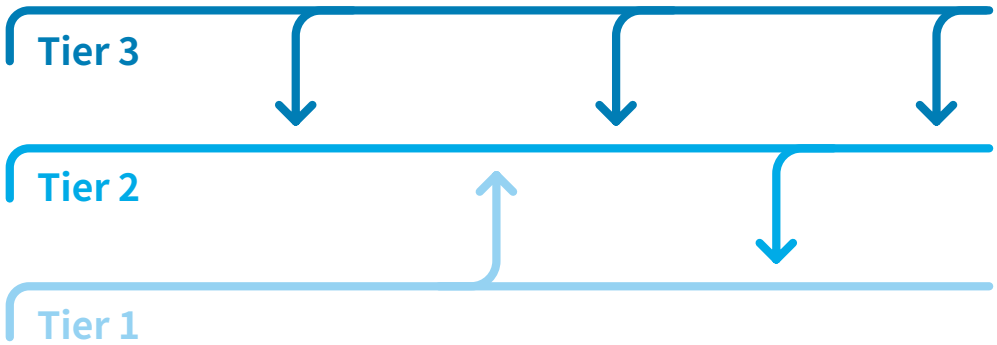


5 エグゼクティブサマリー

テクノロジー

昨年、企業がEERMテクノロジーに関する決定を一元的に下すようになることをデロイトは予測し、標準三層技術アーキテクチャの出現を強調しました。今年の調査によると、この二つは現実のものとなり、三層技術アーキテクチャにおいて、企業がEERMに関する特定のテクノロジーソリューションの合理化および簡素化を進めていることが明らかになっています。

EERMツールとテクノロジーに関する多層アーキテクチャの進化



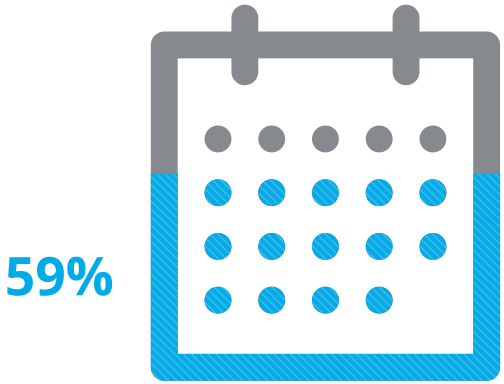
3層テクノロジーアーキテクチャの構成：
Tier 1： EERMに関する共通の基盤と運用上の規律を構築するエンタープライズリソースプランニング（ERP）または購買プラットフォーム。

Tier 1は以下によりサポートされる：
Tier 2： 企業のサードパーティーマネジメント要件に合わせた、EERM特化型リスクマネジメント・パッケージ、またはEERM機能を含む市販のガバナンス・リスク・コンプライアンス（GRC）や統制マネジメントプラットフォーム。

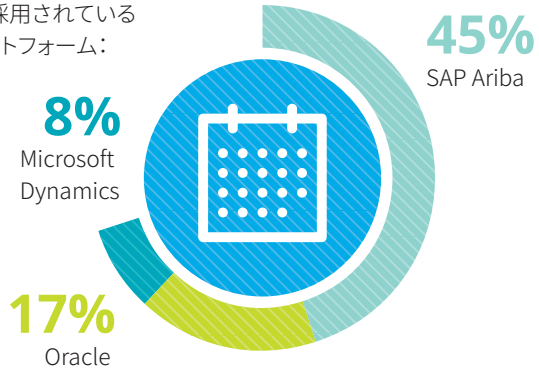
Tier 3： 財務的実行可能性、金融犯罪、契約管理およびサイバー脅威などの専用のリスクドメインからのフィードを提供する、特定のEERMプロセスまたはリスクのためのニッチパッケージ。

Tier 1

回答者の過半数（**59%**）は、EERMの基幹システムとして、ERPまたはプロキュアメントプラットフォームを採用しています。

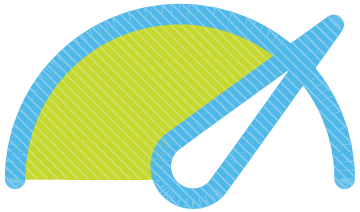


最も採用されているプラットフォーム：



Tier 2

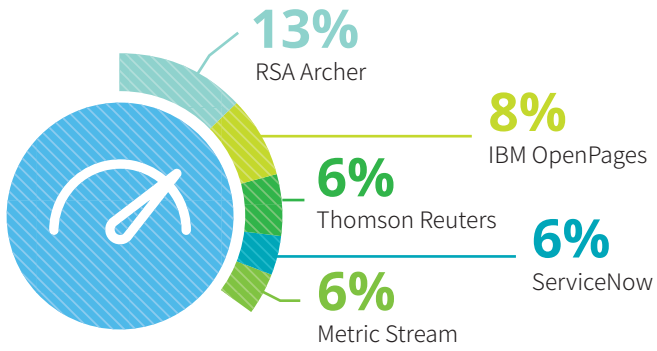
さらに多くの企業（**75%**）がEERMに関するリスクマネジメントソリューションを採用しています。



以下の二つのうちどちらを選択するかについては、意見が分かれています。

- EERM専用パッケージ：現在、**18%**の企業が使用しています。
- EERM用に合わせた市販の統合型リスクマネジメント・ソリューション：現在、**57%**の企業が使用しています。

回答者の企業においては、統合型リスクマネジメントソリューションの方が普及していますが、これは必ずしも好ましいソリューションであるという意味ではありません。回答者からのコメントによると、一部の企業は、これらの市販のリスクマネジメントプラットフォームの使用を選択した理由として、自社にすでに存在していたため、EERMアクティビティのサポートに活用する上で、最も容易で費用対効果が高いことを挙げています。最も一般的なソリューション：

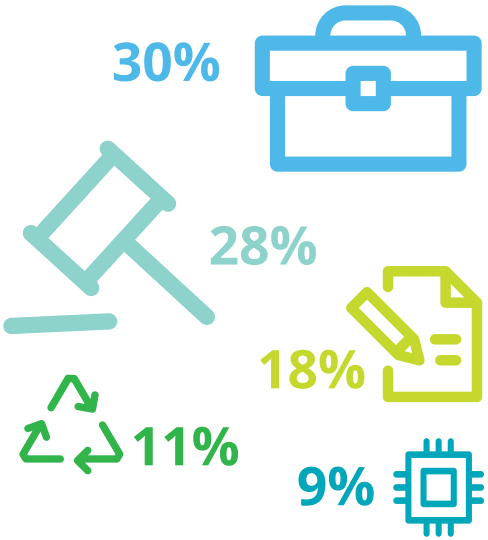


Tier 3

企業は、特定のEERMプロセスまたはリスクに関して、専用のリスクドメインからのフィードを用いたニッチ領域向けパッケージの使用を増加させています。

これには、以下が含まれます。

- 財務の健全性（**30%**）
- 金融犯罪（28%）
- 契約管理（**18%**）
- 持続可能性（**11%**）
- サイバー脅威（**9%**）



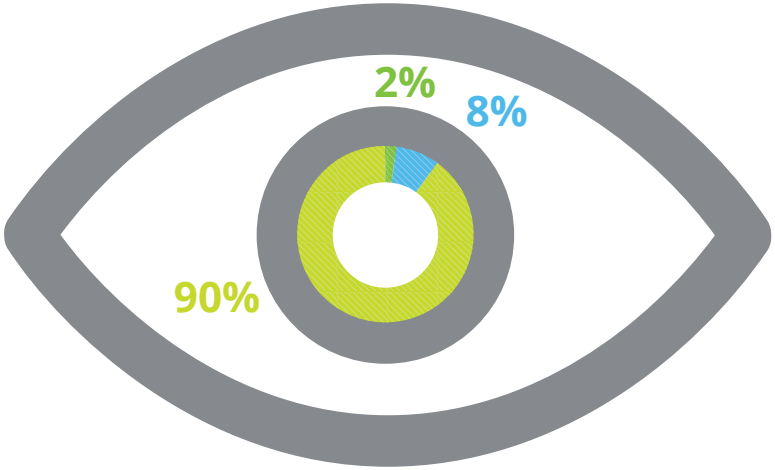
6 エグゼクティブサマリー

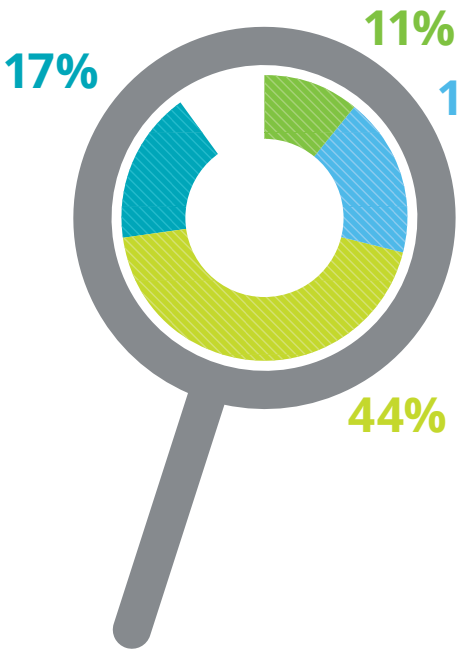
下請業者と関連会社のリスク

i) 下請業者および ii) 関連会社という、サードパーティーリスクマネジメントの2つの重要な要素に対しては、適切な対応がなされていません。

下請業者（2次／3次請け、またはフォース／フィフスパーティー）リスク：

企業は、自社のサードパーティーが委託する下請業者について、十分に把握していません。これは、企業が下請業者リスクを管理し、規律と厳格さをもってこの戦略を適用する方法を決定することを困難にしています。
自社のサードパーティーが委託するすべての下請業者を特定・監視している企業は、わずか**2%**であり、自社の最も重要な関係に関して、この特定・監視を行っている企業も、**8%**（昨年の10%から減少）に過ぎません。
残る**90%**は、下請業者を監視するニーズを認識していないか、監視するための適切な知識、可視性またはリソースを有していません。





11%は、新規のサードパーティーを受け入れる際にのみ、下請業者を審査しています（昨年の8%から増加）。

18%は、下請業者の把握・審査を不定期に行っています。

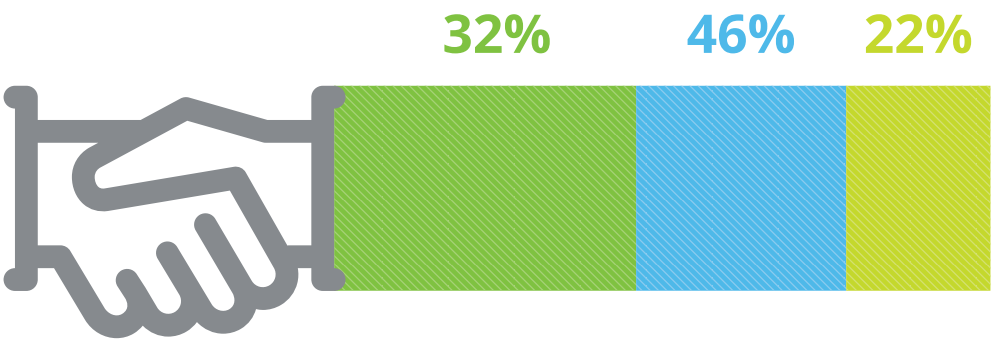
44%は、下請業者のチェックをサードパーティーに委ねていますが、その実行方法を監視しています。

17%は、下請業者の把握、審査または監視を一切行っていません。

この課題は特定の規制産業でよく当てはまります。例えば、金融業界では、システミックリスク、集中リスクが規制当局の懸念事項です。とはいえ、この課題は、英国現代奴隷法およびEUのGDPR（一般データ保護規則）などの幅広い法令や規制を考慮すると、規制産業だけの問題ではありません。

関連会社リスク

関連会社[6]リスクについて、ほかのサードパーティーと同一の厳格さをもって、評価と監視を行っている企業は、3分の1未満です（**32%**）。一方で、これより高い割合の企業（**46%**）においては、関連会社リスクマネジメントに対して、一般的により簡素なアプローチを採用しています。残りの**22%**は、関連会社を有していないと述べています。



関連会社に関する事前スクリーニング、デューディリジェンス、モニタリングは、ほかのサードパーティーに比べると、あまり厳格ではない様子が見受けられます。これは、関与するリスクに相応である場合は妥当と言えますが、このアプローチは明確に定義され、一貫性を保つことが求められます。

もう一つの展開として、グローバルビジネスサービス（GBS）構造の出現が挙げられます。このサービスの目的は、すべてのサードパーティーと、社内のシェアードサービスのデリバリーチーム全体における、ガバナンスの機構とグッドプラクティスの統合にあります。ただし、この構造のスコープや、その構造に所属する組織体は、企業によって異なります。このため、サードパーティーリスクマネジメントに複層的な課題をもたらしています。

エグゼクティブサマリー

今後の予測

ビジネスケースのドライバー

EERMへの投資要因としてのコスト削減は短期的なものとなる傾向があります。より中長期的には売上・利益の成長につながる投資要因が顕著になると期待されます。これには、以下の要素に取り組むために、サードパーティーのスキルと機能の使用を可能とするEERM投資が含まれます。

- 新規市場への参入
- 新規の収益源の創出
- 競争優位性の確立

規制当局

企業がサードパーティーリスクを管理する方法について、すでに規制当局は多大な期待を寄せています。デロイトの予測では、現代奴隷法およびGDPRを始めとする、最近の法令や規制に見られるように、規制が強化され、エマージングリスクに対処するための当局の権限がより幅広いものになる見込みです。

さらに、規制当局によって、リスクマネジメントおよびコンプライアンスにおけるイノベーションが推奨されることが予測されます。例えば、2018年12月に、米国の金融サービスを規制する機関の一つである連邦準備制度理事会によって、高度な金融インテリジェンスユニットの構築から、取引監視のための人工知能の採用まで、多岐にわたる革新的なアプローチが示されています。今後、欧州銀行監督機構および英国金融行為規制機構が同様のスタンスを取り入れることが予想されます。

オペレーティングモデル

関与するリスクに比例して、企業は様々なリスクドメインにわたる効率性とより一貫したアプローチの獲得を目指して、EERMオペレーティングモデルの変更に投資しています。デロイトの予測では、これは、2020年末または2021年には投資に対する効果を生み出し始めます。これは投資の効果の具現化に2〜3年を要するという、回答者による現実的な判断に沿ったものです。

さらにデロイトの予測では、EERMデリバリーの望ましいモデルは、テクノロジーソリューションの機能性が発展し、市場ユーティリティおよびマネージドデリバリーソリューションへの信頼と理解が深まるにつれて、引き続き変化していきます。

テクノロジー

テクノロジーの合理化という要望が継続していきます。

これに対応するために、

- 主要ERPベンダーは、各社のツールの機能の向上に取り組む
- サードパーティーリスクマネジメントツールは、より範囲の広いサードパーティーマネジメントツールに進化を遂げ、パフォーマンス、契約および取引の内容は、リスクと連動して管理されるようになる

さらに、デロイトの予測では、テクノロジーソリューションに関する評価基準は、「より安く、より早く、より良く」を超えて進化を遂げ、以下を含むようになります。

- 新興市場におけるサポート
- ロボティクスおよびコグニティブオートメーション
- 将来のシェアードユーティリティおよびマネージドサービスプラットフォームが提供できる内容についての検討

支出

デロイトの予測では、2019年から2020年にかけて、EERMの資本的支出（CAPEX）は、長期的なEERMの成熟を向上させるためのプラットフォームの転換に向けたイニシアティブ、および関連する設計および導入活動に対して増加していきます。

必要とされる先行投資が一段落すると、この活動を順調に実施した企業は、最大でEERMの年間運営費（OPEX）と同一レベルまで継続的な資本的支出（CAPEX）を抑え込む、という目標を達成できるでしょう。

その一方で、より小規模で俊敏な企業においては、シェアードユーティリティモデルに移行して、エマージングテクノロジーを導入する能力と意欲が高まっていく可能性があります。これを受けて、運営費（OPEX）のレベルが高まり、資本的支出（CAPEX）額は増分のみにとどまるという反対の動向が現れることになるかもしれません。

下請業者リスク

2次請け、3次請けに関するリスクマネジメントは、その固有リスクに加えて、レピュテーションリスクの潜在的な源としての重大性について、企業が理解を深めるにつれて、注目が集まり、投資が増えていくでしょう。

01

経済環境と
オペレーティング環境

経済の不確実性によって、引き続き、
コスト削減とEERM人材への投資が促されています。

これまでの経緯

過去4年間のEERM調査は、サードパーティーへの委託とサードパーティーリスクマネジメントへの投資に関する主要なドライバーを追跡してきました。この調査で繰り返し明らかになっているのは、企業のサードパーティーの使用が増えているのは、単なるコスト削減ではなく、より広い戦略的な目標を達成するためである、という点です。これには、以下が含まれます。

- 組織的なアジリティ（フレキシビリティおよびスケーラビリティなど）。
- 製品やサービスのイノベーション。サードパーティーの専門的な知識やスキルが用いられることが多い。

2015年には、EERMへの投資は、規制エクスポージャーやサードパーティー関連のインシデントを始めとする、ダウンサイドリスクの管理にほぼ集中していました。以下のイニシアティブのような組織的なパフォーマンスを向上させるアップサイドリスクの活用については、ほとんど注目されていませんでした。

- サードパーティーマネジメントの効率性によるコスト削減。
- サードパーティーのモニタリング向上による新しい収益源の発見。

2018年までに、取締役会メンバーおよび経営陣を含む調査回答者は、サードパーティーリスクマネジメントがもたらすリスクと機会への理解をはるかに深めてきました。このことは、EERMへの投資が目に見える成果につながるという自信を深めてきたことを意味しています。

その一方で、直近のグローバル経済の不確実性により、サードパーティーリスクマネジメントの包括的で統合型なアプローチ実現を目指した変革イニシアティブに対する多額の設備投資がより難しくなっています。

経済の不確実性によって、引き続き、コスト削減とEERM人材への投資が促されています。

2019年所見

企業は、規制の強化や市場の破壊的な転換を伴う、ますます複雑で困難な経済環境と事業環境で活動しています。

さらに、グローバルビジネスに悪影響を与えかねない、閉鎖的で非協力的な行動を、複数の国の政府が推奨しているという懸念を多くの回答者が抱いていることが特定されました。

直近の調査で明らかになったのは、この複雑で困難な経済環境がEERMへの投資に重大な影響を及ぼしているという点です。企業は、効率性を追求し、コストを削減するために、それぞれのオペレーティングモデルの見直しに取り組んでいます。

投資ドライバー

今年、EERMへの投資に関して最も多く挙げられたドライバーは、以下のとおりです。

- **コスト削減**
  （62%の回答者、昨年の48%から増加）
- **サードパーティー関連のインシデントの削減**
  （50 %の回答者、昨年の34%から増加）
- **規制当局による監視**
  （49 %の回答者、昨年の43%から増加）
- **社内コンプライアンス要件**
  （45 %の回答者、昨年の41%から増加）

サードパーティー関連のインシデント

サードパーティー関連のインシデントは、引き続き、様々なインパクトを伴う混乱を引き起こしています。大半（83%）の企業は、過去3年間に、サードパーティー関連のインシデントを経験しています。このうち、カスタマーサービス、財務状況、レピュテーションまたは規制コンプライアンスに深刻なインパクトを経験したのは11%に過ぎませんが、3分の1以上（35%）が中程度の組織的なインパクトを経験しています。

EERM改善のための領域

コスト削減が注目される一方で、組織の各機能にわたる、EERMへのより協調的で一貫したアプローチを求める回答者は、半数強（53%）に上っており、アクションを求める最優先領域となっています。

2番目は、EERMに関するプロセス、テクノロジーおよびリアルタイムのマネジメント情報を改善するニーズとなりました（49%）。

マネージドサービスおよびユーティリティモデルが利用可能なことにより、さらに基本的なEERMスキルの獲得や、EERM遂行のための総合的な能力に関する懸念は減少しています。むしろ、企業が求めるのは、イニシアティブのコーディネートとリーダーシップを担う、EERM を主導できる人材への投資となっています。

図 1.1 EERMに関する投資ドライバー

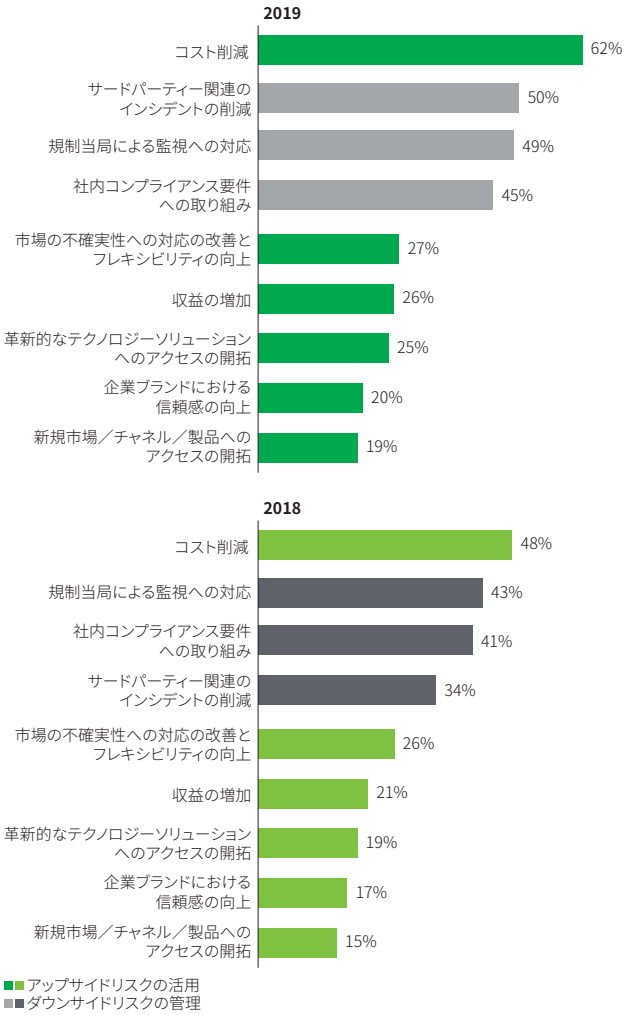


図 1.2 過去3年間に経験したサードパーティー関連のインシデントのインパクト

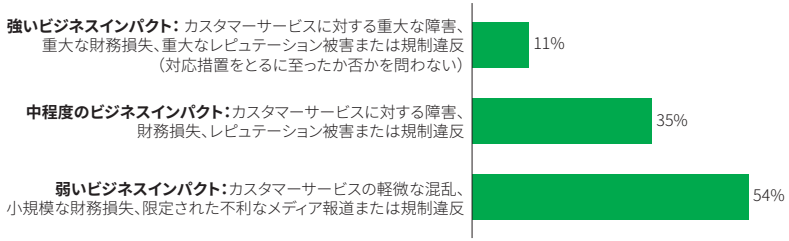
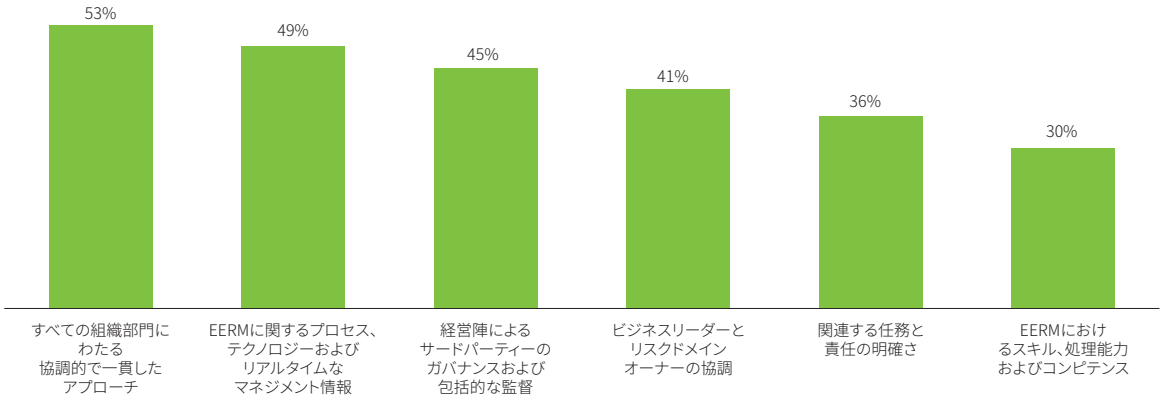


図 1.3 EERMに対する組織の自信を高めるために改善が必要な領域



デロイトの視点

企業は、数年間にわたって、サードパーティーマネジメントの改善によるコスト削減に注力しています。この点について、以下の両面からのアプローチを取る企業が増えていることが顕著になってきています。

・過払いまたは収益の漏れを回収するためのプログラムの確立
・戦略的なEERMソリューションへの投資とシェアードサービスなどの仕組みによる効率性の達成

EERMを主導できる人材の不足は、長年の問題でもあります。しかし、効率化を進め、社内の協調を向上させるためのイニシアティブは、リーダーシップスキルとEERMの専門知識を持った人が統率する場合にしか成功が望めない、と認識されており、この問題はますます注目されています。デロイトが確信しているのは、企業のレピュテーション、業績、株主価値への損害など、サードパーティーによってもたらされる不利益が、ますます深刻になっていくことです。これは、サードパーティーリスクマネジメントのプロセスとフレームワークの改善に企業が投資する、有力なドライバーであり続けるでしょう。

同時に、規制を適用することによって、社内における監視要件やコンプライアンス要件に反映され、より能動的で継続的なプロセスになっていくでしょう。

サードパーティーマネジメントは、金融サービス、ライフサイエンスおよびヘルスケア、化学品、食品およびリテールといった幅広い業界の規制当局の厳格な行動に加えて、米国の連邦海外腐敗行為防止法などのグローバルな影響力を持つ法規制など、極めて厳格さを増した措置によって推進されていきます。

業種別ハイライト

コスト削減、サードパーティー関連のインシデントの削減、さらに規制当局による監視および社内コンプライアンス要件は、多くの業種において、EERMへの投資を促す最も強力な動機となっています。その一方で例外もあり、個別の優先項目は、セクターによって異なります。

・消費財・産業機械セクターにおける懸念は、社内コンプライアンス要件への対応（47%）が、規制当局による監視（44%）より高くなっています。

・エネルギー・資源セクターのEERMへの投資のドライバーとして最も多く挙げられたのは、サードパーティー関連のインシデント数の削減（74%）です。これは、次に高い割合で回答した業種、金融サービスの55%を大きく上回りました。

・政府・公共サービスセクターの3分の1（33%）の組織は、革新的なテクノロジーソリューションへのアクセスをEERMへの投資に求めています。同セクターでこの項目を挙げた組織の多くが高等教育機関であるため、おそらく、遠距離学習などのイニシアティブを可能にするためのテクノロジーのイノベーションを求めているものと思われます。他にテクノロジーソリューションを求める回答者が多かったのは、金融サービス（27%）とテクノロジー・メディア・通信（26%）でした。

・政府・公共サービスセクターは、組織全体にわたるアプローチの協調と一貫性を高めることの必要性を、90%と、他のセクターに比べて極めて高く認識していました。

ライフサイエンス・ヘルスケアセクターでは、サードパーティー関連のインシデントによって強い（19%）もしくは中程度（46%）のビジネスインパクトを受けた企業がほかの業種より多く見られ、次いで、消費財・産業機械セクターとなりました。17%が強いビジネスインパクトを伴うサードパーティー関連のインシデントに遭遇し、31%が中程度のインパクトを経験しています。さらに、金融サービスセクターが続き、強いインパクトが10%、中程度が36%となっています。

すべてのセクターにおいて、多数の企業がEERMに関するプロセス、テクノロジーおよびリアルタイムなマネジメント情報の改善のニーズを認識しています。

また、ビジネスユニットリーダーとリスクドメインオーナーのより良い関係の向上を特に考えているセクターは、ライフサイエンス・ヘルスケア（60%）と政府・公共サービス（50%）となっています。

図 1.4 EERMに関する投資ドライバー（業種別）

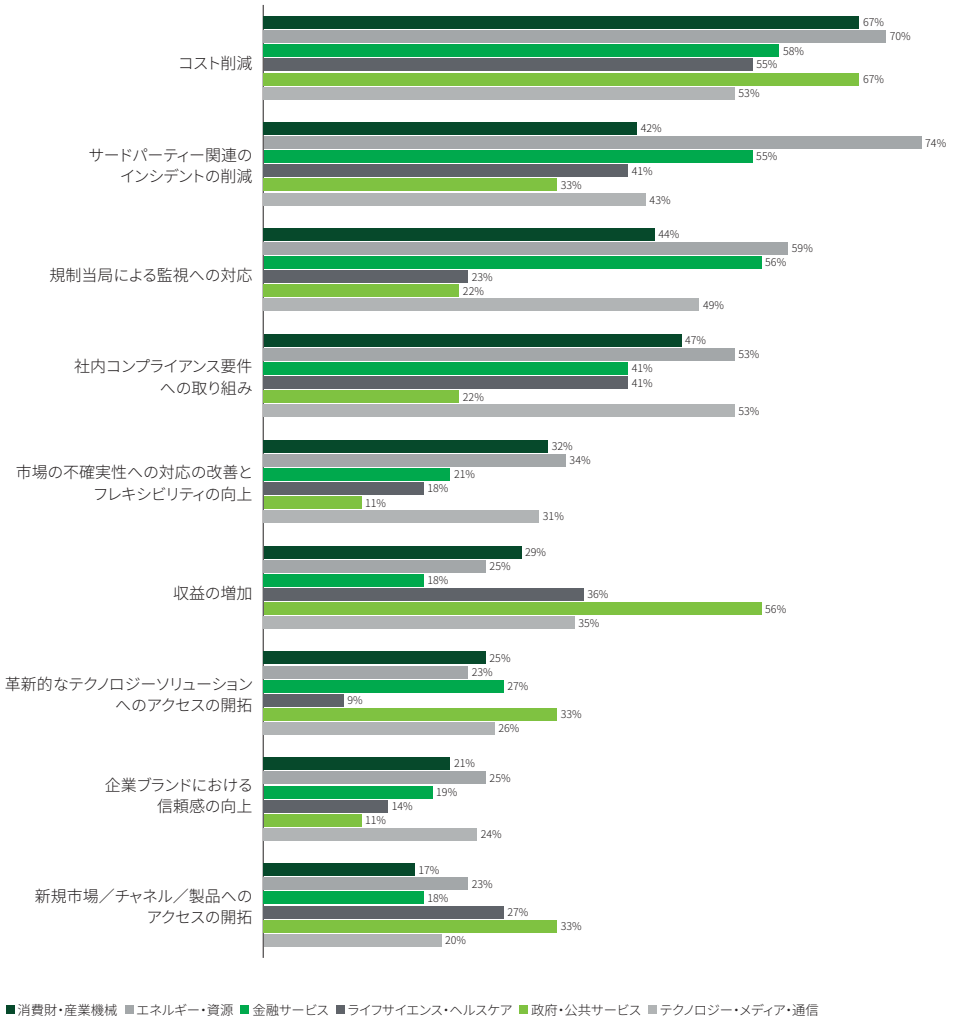
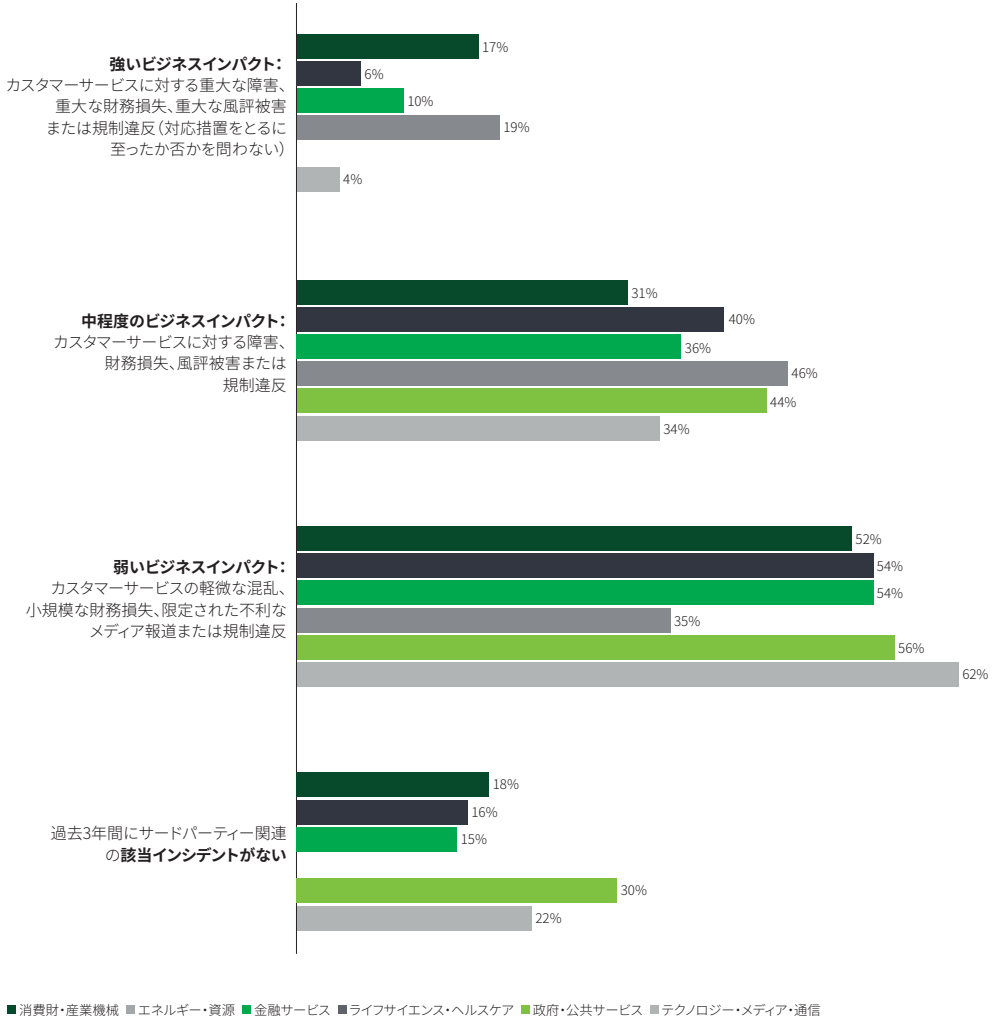


図 1.5 過去3年間に経験したサードパーティー関連のインシデントのインパクト（業種別）



地域別ハイライト

EERMへの投資がコスト削減と価値保全戦略によって促されるとした比率が最も高かったのは、EMEA（欧州・中東・アフリカ）地域で、米州地域、アジア太平洋地域が続きました。

- **コスト削減：**EMEA地域が63%、米州地域が60%、アジア太平洋地域が57%
- **サードパーティー関連のインシデントの削減：**EMEA地域が54%、米州地域が46%、アジア太平洋地域が40%
- **規制当局による監視への対応：**EMEA地域が52%、米州地域が50%、アジア太平洋地域が38%
- **社内コンプライアンス要件への取り組み：**EMEA地域が47%、米州地域が46%、アジア太平洋地域が38%

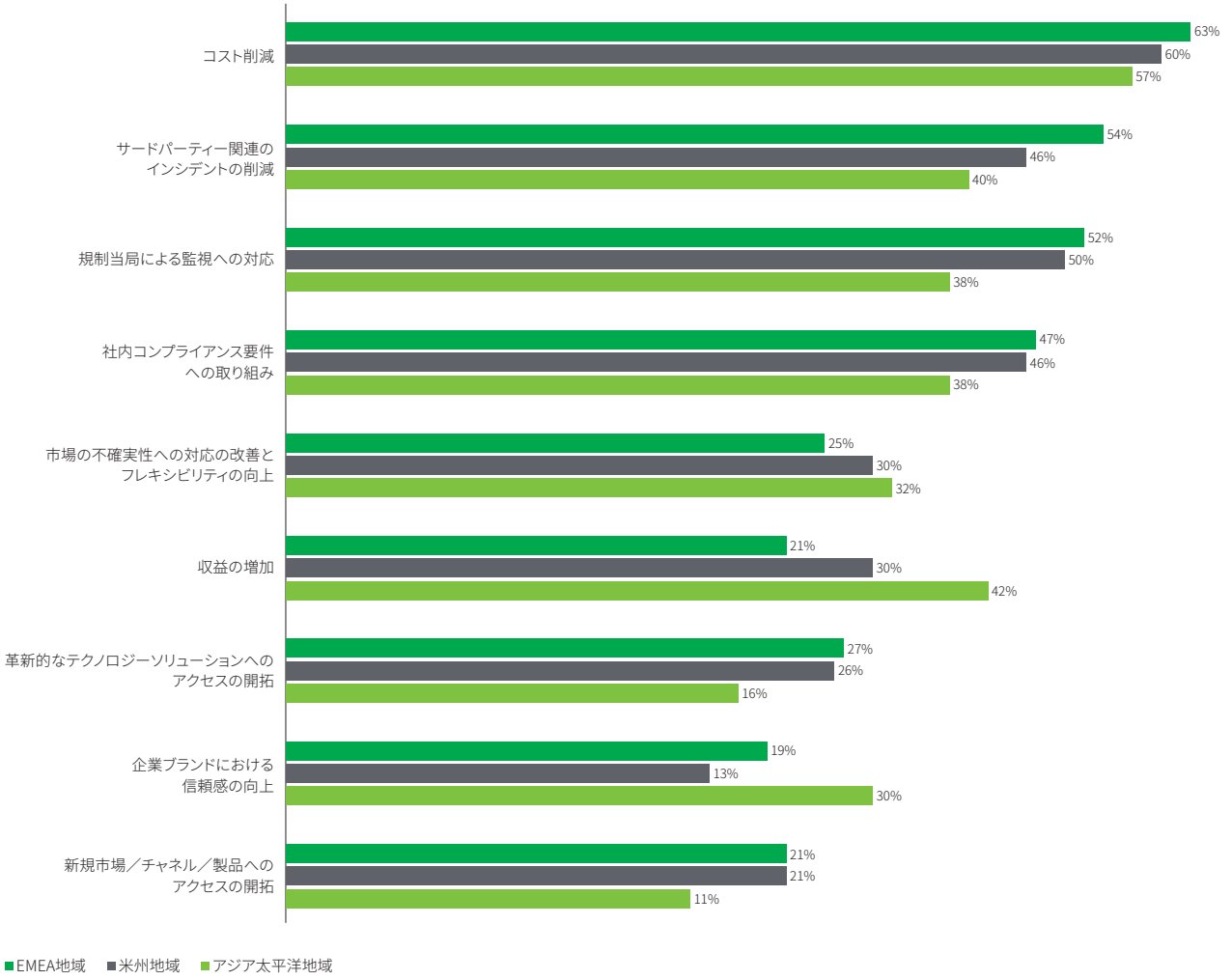
これらの統計値は、おそらく、上記地域の事業環境の相対的な不確実性のレベルを反映しています。また、上位のドライバーは、アジア太平洋地域の国々と比較して強いと考えられる、EMEA地域と米州地域における規制の適用の歴史を反映したものと考えられます。

コスト削減以外の価値創造型ドライバーは、アジア太平洋地域でやや高くなっています。例えば、

- 収益の増加（例：過少報告されている収益源の特定による）：アジア太平洋地域の42%に対して、米州地域は30%、EMEA地域は21%のみ
- 市場の不確実性への対応の改善とフレキシビリティの向上：アジア太平洋地域の32%の回答者に対して、米州地域は30%、EMEA地域は25%

すべての地域で、サードパーティー関連のインシデントは同様の発生状況でしたが、アジア太平洋地域では、強いビジネスインパクトを伴うインシデントの比率が14%となり、EMEA地域の11%、米州地域の9%に比べてやや高くなっています。

図 1.6 投資ドライバー（地域別）



02

投資

断片的な投資がEERMの成熟を阻害し、
特定のリスクをなおざりにして、
中核を成す基本タスクに悪影響を及ぼしています。

これまでの経緯

2015年の最初の調査から、サードパーティーへの依存の度合いがますます重要なものになっていく潮流にもかかわらず、EERMの成熟は追い付いていません。2015年から2018年にかけて、アプローチの統合と最適化を行ったのは、5社中1社の割合に過ぎません。

企業は、理想的な状態への到達を目指して、関連するリスクマネジメントの機構を統合および最適化するための現実的な期間を再設定しました。以前考えられていたような6カ月から1年のプロジェクトではなく、少なくとも2、3年を要する道のりになると徐々に認識されています。

現実には、最適なEERMとして目指されるあり方は時間と共に変わりつつあります。いまだに多くの企業は、サードパーティーと関連サービスのイノベーションの可能性への高まる期待に追い付こうと奮闘しています。グッドプラクティス、テクノロジーソリューション、ユーティリティおよびマネージドサービスのコンセプトが、より高度になりつつあります。このため、回答者は、以前の成熟度の自己評価を見直しています。

数年にわたって、一部の回答者は、その年の最大の規制面での課題を中心に年間の投資を集中させるという、自社のEERMへの、いくぶん散発的なアプローチを報告しています。例えば、2018年には、データプライバシーがこれに該当しました。企業は、より幅広いリスクをなおざりにせずに、機能の進化に追い付くよう心掛ける必要があります。

断片的な投資がEERMの成熟を阻害し、特定のリスクをなおざりにして、コアな基本タスクに悪影響を及ぼしています。

2019年所見

この数年間にわたって、EERM投資への断片的なアプローチによって組織が成熟できる速度が損なわれてきた、という強力な証拠が存在しています。最新の調査において、自社を「統合化」または「最適化」の段階にあると考えている回答者は、わずか21%です（昨年の20%から微増）。ほぼ半数（51%、昨年の50%から微増）は、自社を「管理化」カテゴリーにあると考えています。

今年、EERMへの投資について、回答者に質問したところ、70%以上は、理想的な金額より支出が少ないと思う、または、理想的な金額を支出しているかどうか分からない、としています。さらに、10人中7人は、EERMの必要人員よりも実際の人員が少ないと思う、または、分からない、としています。

多くの企業で投資不足が共通の認識であるとはいえ、EERMの年間運営費（OPEX）には大きな開きがあります。半数（50%）は、EERMの年間運営費（OPEX）に100万米ドル以上を費やしています。トップの11%は、それぞれ1,000万米ドル以上を費やし、100人以上のFTE（常勤換算）スタッフを雇用しています。

さらに2019年は、個別のリスクドメインへの投資の詳細についても調査しています。

投資は、情報セキュリティ（68%の回答者）、データプライバシー（62%）、サイバーリスク（58%）に偏っています。

その一方で、多くの企業において投資不足となっているその他の領域として、労働に関する権利（18%）、地政学リスク（12%）、集中リスク（12%）が挙げられます。

多くの企業において、以下の2つの領域の投資に対して十分に関心が寄せられていません。

- **重要なサードパーティーに関する出口計画および契約終了業務：**重要なサードパーティーに関する出口計画について、60%以上の回答者が毎年検証をしていません。

- **集中リスクの管理：**半数近くの回答者は、集中リスクを毎年検証していません。集中リスクをEERMプロセスの一環として積極的に検証するのではなく、レポーティングを通じて、事後的な検証がなされている傾向があります。

このような断片的なアプローチによって、基本的なコアタスクを適切に実行する組織能力が弱められていると、回答者が認識している点は新しいインサイトです。関与するリスクのレベルに対するモニタリング活動の調整を困難にしている最も一般的な要因は、サードパーティー関係の内容の把握（50%）および関連する契約条件の把握（43%）でした。

図 2.1 EERM成熟度の変化（2016年～2019年）

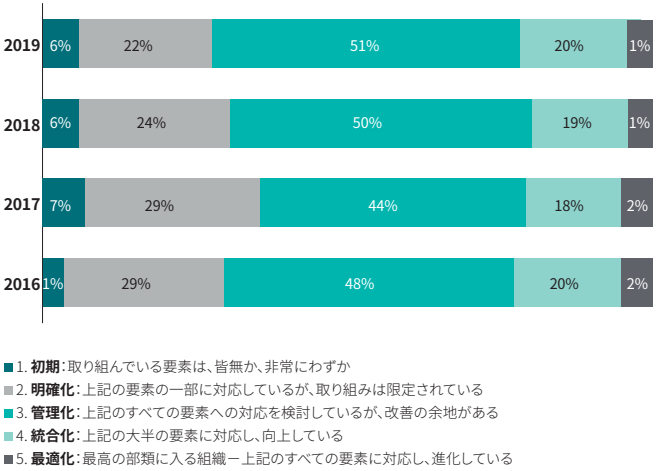


図 2.2 多くの企業がEERMへの投資不足を確信

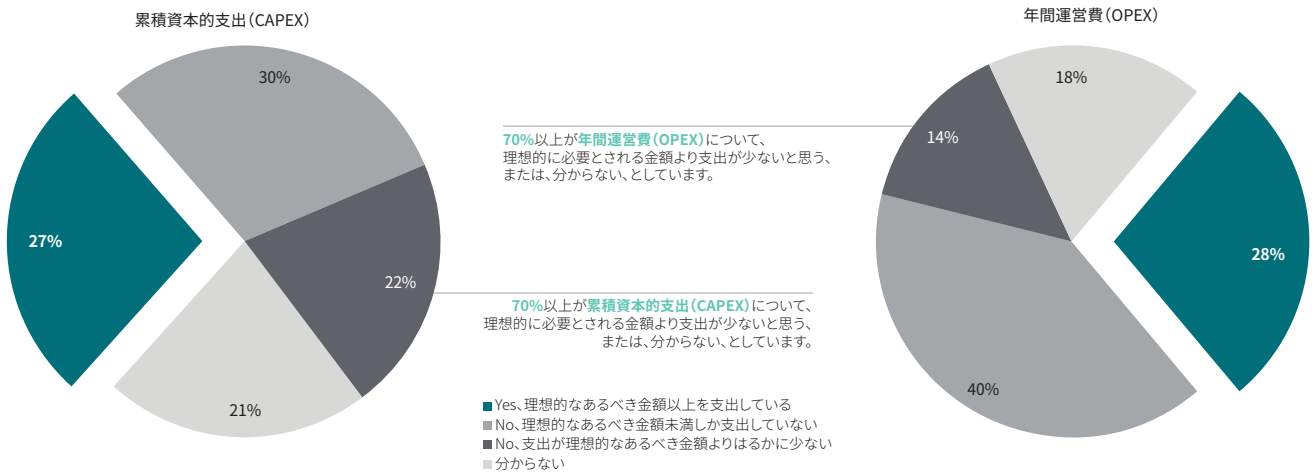
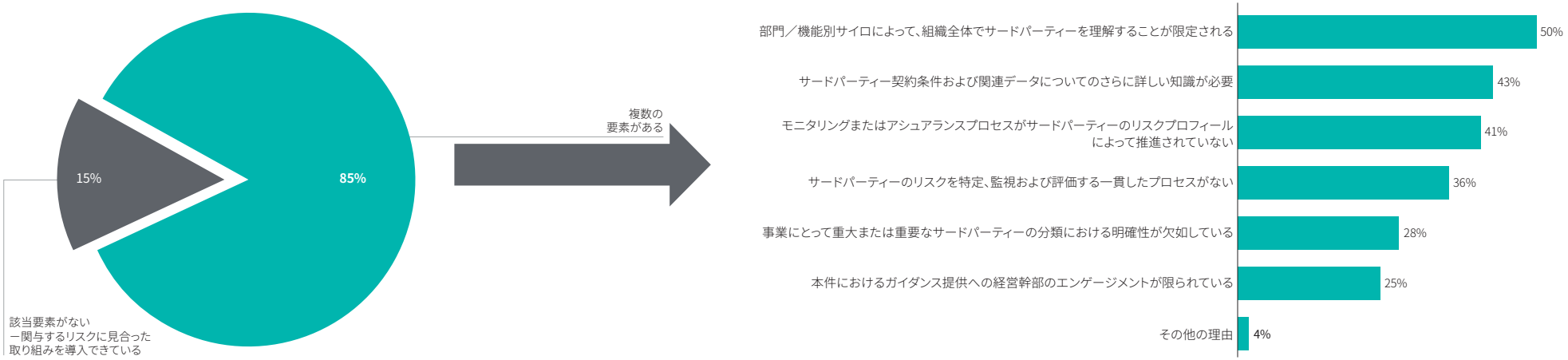


図 2.3 サードパーティーリスクに見合った取り組みへの対応を阻害するトップ要素



デロイトの視点

以前のEERM調査で浮き彫りになった点として、サードパーティーリスクは従来、リスクドメインごとにサイロ化され、個別のアクティビティを行う複数の関係者によって推進されていました。例として、サプライチェーンが断絶する途絶リスク、サードパーティーが提供するITサービスに関連する情報セキュリティリスクなどが挙げられます。

2016年には、先進的企業は、すべてのタイプのサードパーティーとすべてのリスク領域を対象とする、包括的なアプローチの導入を開始していました。一連のリスクドメインにおける幅広いサードパーティーの網羅という点で、これらの企業は順調な進捗を遂げている一方で、予算が十分でない場合は、法的な課題となっている特定のリスクドメインへの大幅な投資に重点を絞っています。2018年の事例として、以下が挙げられます。

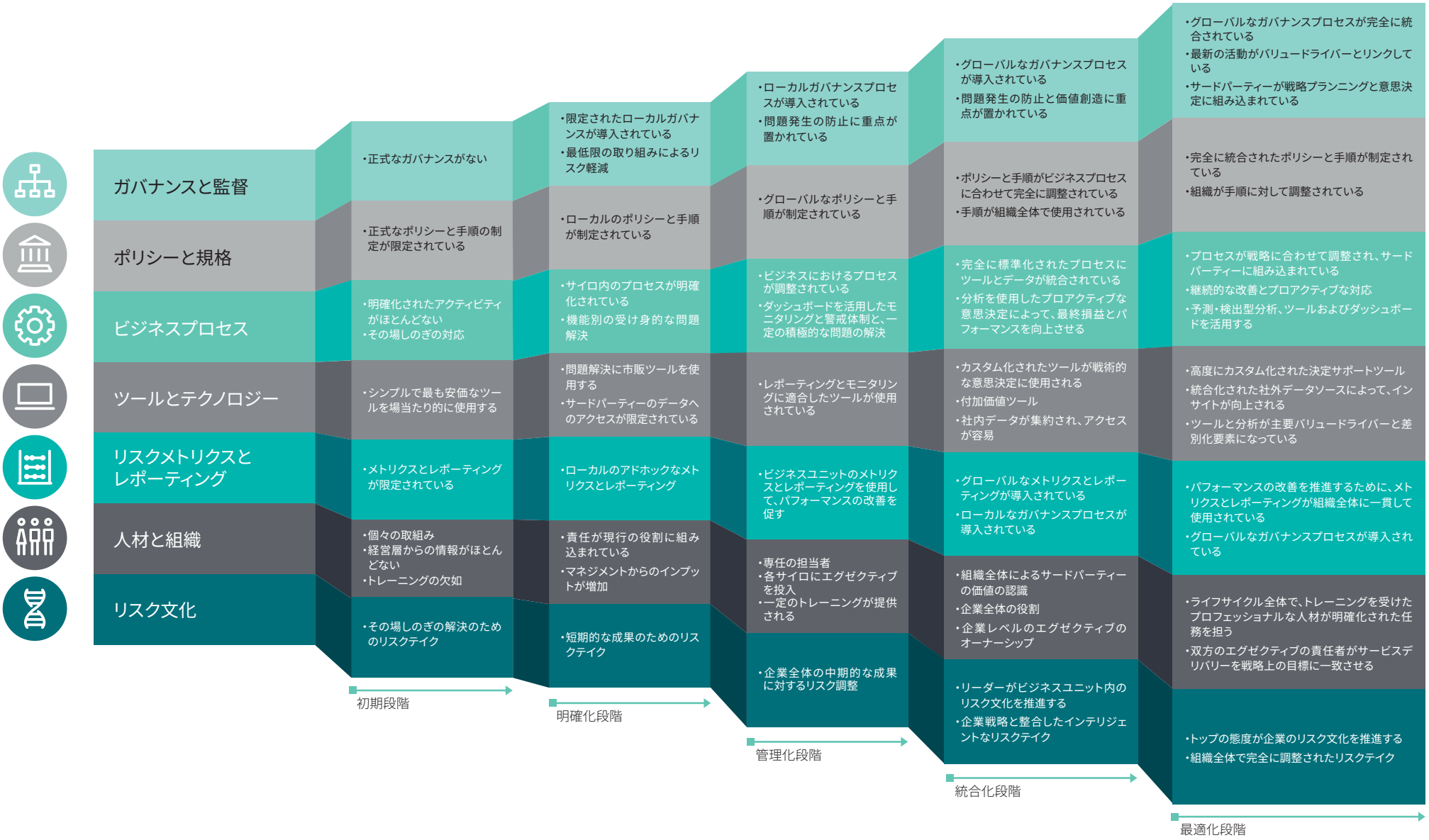
- 欧州の一般データ保護規則（GDPR）およびほかの地域の同様の法律によって促される、プライバシーに関する懸念
- 世界で発生している破壊的サイバー攻撃の後のサイバーセキュリティに関する不安

この限定的で断片的なEERMへの投資は、組織としての成熟における成長を損ない、戦略的な投資アプローチを困難にしています。重大な点として、基本的な能力の不足によって、最先端のイニシアティブによるベネフィットを実現するための企業の努力が損なわれる恐れがあります。その結果、実現されるベネフィットは、潜在的に期待できるベネフィットのごく一部でしかありません。

企業は、プロセスとフレームワークを合理化すると同時に、それらを統合して、効率と効果を高める機会を定期的に活用することで、サードパーティーリスクマネジメントを統合することに再度注力すべきです。

また、企業は、EERMの年間運営費（OPEX）に関して、事前審査と出口計画および契約終了業務への配分の増加（それぞれ約10%程度）を検討する必要があります。これにより、選定への視点を補うことになります（デューデリジェンスおよび契約業務に予算の20～30%、継続的モニタリングに50%強程度）。このような支出構成をとることで、企業にとって「発見型」アプローチから「予防型」アプローチへの進化につながります。

デロイトのEERM成熟モデル



業種別ハイライト

本調査で明らかになった点として、ライフサイエンス・ヘルスケアセクターと政府・公共サービスセクターを除き、各業種でEERM成熟度が似通っていることが挙げられます。ライフサイエンス・ヘルスケア企業は、ほかのセクターと比べて、自社の成熟について楽観的にとらえており、28%が自社のEERMを「統合化」または「最適化」の段階にあるとしています。一方の政府・公共サービスセクターは、ほかのセクターに比べて楽観度が低く、自組織が「統合化」または「最適化」の段階にあるとする回答者は、わずか10%でした。

EERMの資本的支出（CAPEX）と運営費（OPEX）がどちらも投資不足という認識は、各セクター共通となっています。しかし、金融サービスセクターにおいては、組織の投資が十分であると見なす回答者の比率が、CAPEXでは31%、OPEXでは34%と最大でした。その対極が政府・公共サービスセクターで、EERMの投資が十分と見なす回答者は、CAPEXとOPEXともにわずか11%でした。

特定のリスクドメイン（情報セキュリティ、データプライバシー、サイバーリスクおよび規制のコンプライアンス違反）は、すべてのセクターにおいて、ほかの領域より投資優先度が高くなっています。ただし、業種によっては、ほかのリスクドメインをなおざりにして、特定のリスクドメインに重点を置く傾向があります。

例として、以下が挙げられます。

- マネーロンダリング、収賄および制裁措置などの金融犯罪への対策に特に重点を置いているのは、政府・公共サービスセクター（78%の回答者）、エネルギー・資源セクター（68%）、および金融サービスセクター（58%）でした。
- 政府・公共サービスセクターは、レピュテーションリスク（56%）および物理的セキュリティ（67%）の管理への継続的な取り組みにおいて、ほかのセクターを上回っています。
- 金融サービスおよびエネルギー・資源セクターは、レジリエンシーおよび事業継続性の管理を特に重視しています（両セクターとも46%）。
- エネルギー・資源セクターにおいて優先度が高いのは、契約リスク（59%の回答者）、安全衛生リスク（66%）および下請業者リスク（55%）への対応となっています。
- 金融サービスセクターは、規制当局による懸念の高まりに対応しており、23%が集中リスクを重視しています。
- テクノロジー・メディア・通信セクターが最大の関心を寄せているのは、知的財産リスク（36%）で、ほかのセクターと比べ、極めて比率が高くなっています。

図 2.4 EERM成熟の企業自己評価（業種別）

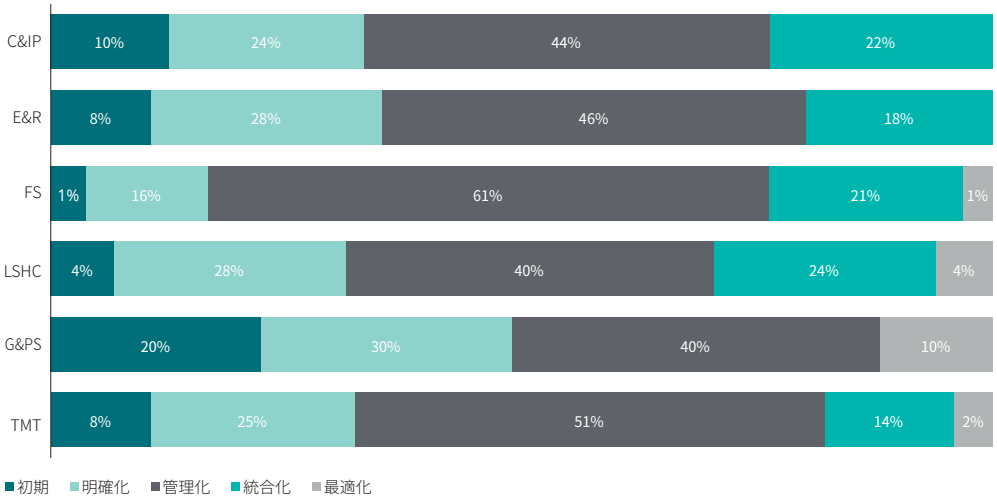
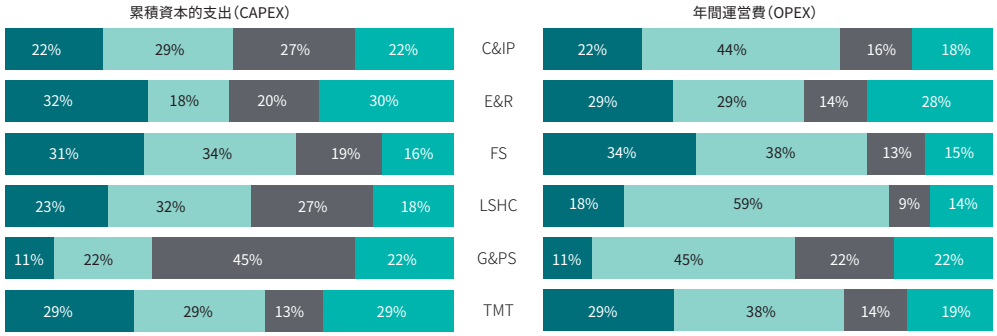
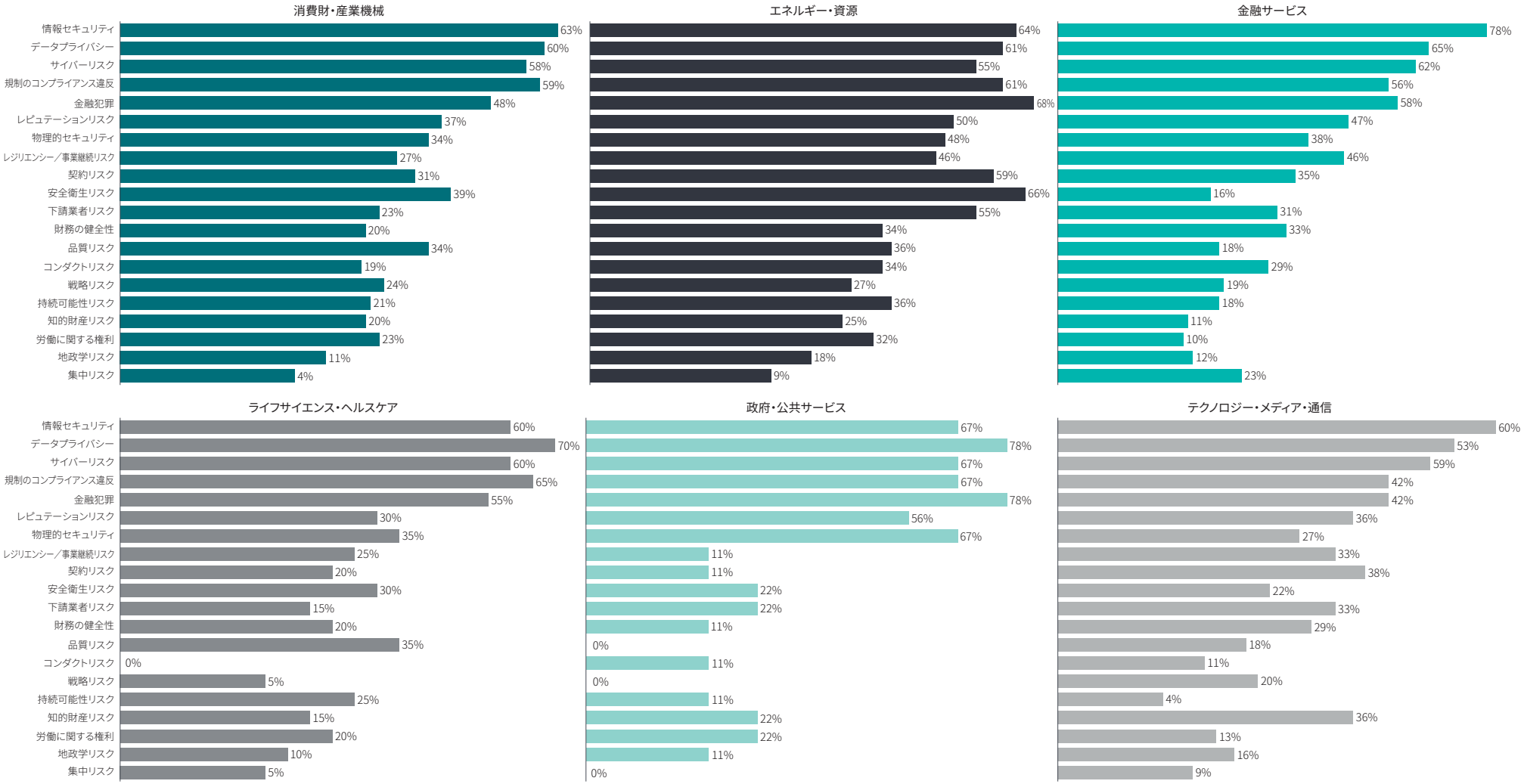


図 2.5 企業がEERMに対してあるべき金額を支出しているかについての考え（業種別）



*業種カテゴリーの正式名称については、巻末注 4参照

図 2.6 EERMの特定リスクドメインへの投資（業種別）



地域別ハイライト

企業が委託するサードパーティーの数に、極端な地域差はありません。

FTE数は、すべての地域で年間投資レベルにおおむね合致しています。ただし、マネージドサービスの導入が拡大すると、変わる場合があります。

EERM関連アクティビティに100万米ドルを上回る支出をする比率が最も高いのは米州地域で、EMEA地域、アジア太平洋地域と続きます。

- 米州地域の65%の回答者が100万米ドルを上回る支出をしており、25%はOPEXに年間500万米ドルを上回る金額を費やしています。
- EMEA地域の48%の回答者は、100万米ドルを上回る支出をしており、17%は500万米ドルを上回る金額を費やしています。
- アジア太平洋地域では、100万米ドルを上回る支出をしたのは38%のみで、500万米ドルを上回るのはわずか10%となっています。

アジア太平洋地域の回答者は、EERMへの支出額が理想以上であると考える比率が最も低く、CAPEXでは19%、OPEXでは23%でした。大多数の回答者は、自社を投資不足ととらえています。上記の比率は、米州地域（CAPEXが21%、OPEXが23%）およびEMEA地域（CAPEXおよびOPEXとも30%）では、やや多くなっています。

世界的に、優先度が高いリスクドメインはおおむね共通しており、データプライバシー、情報セキュリティおよびサイバーセキュリティとなっています。

一方で、興味深い相違点として、サードパーティー関係におけるライフサイクルの各ステージで使われるEERM予算の比率が挙げられます。通常、このライフサイクルで最も長いフェーズは継続的モニタリングで、支出の中でも最も高い比率を占めるのが一般的です。

アジア太平洋地域の回答者は、事前スクリーニング、デューデリジェンスおよび契約終了に費やす予算の比率が最も低くなりました。具体的には、アジア太平洋地域の60%にも上る回答者は、事前スクリーニング業務に年間予算の5%未満しか支出しておらず、米州地域の41%、EMEA地域の37%と対照的です。EERMの成熟が進んだ組織は通常、約10%を費やします。

この現象は、契約終了業務および出口計画に関しても同様ですが、この領域の投資不足については、各地域がさらに似通っています。アジア太平洋地域の3分の2近く（64%）の回答者は、この項目に年間運用予算の5%未満しか支出しておらず、米州地域では59%、EMEA地域では55%と、やや少ない比率になっています。

一方、成熟カーブの上方に位置する企業は、契約終了および出口計画に予算の少なくとも10%を費やします。回答者は、契約終了または撤退に多大な労力を要する重要なサードパーティー契約に関して、特にこの項目の支出が高いことを示唆しています。

図 2.7 EERMへの財務および人材投資（地域別）

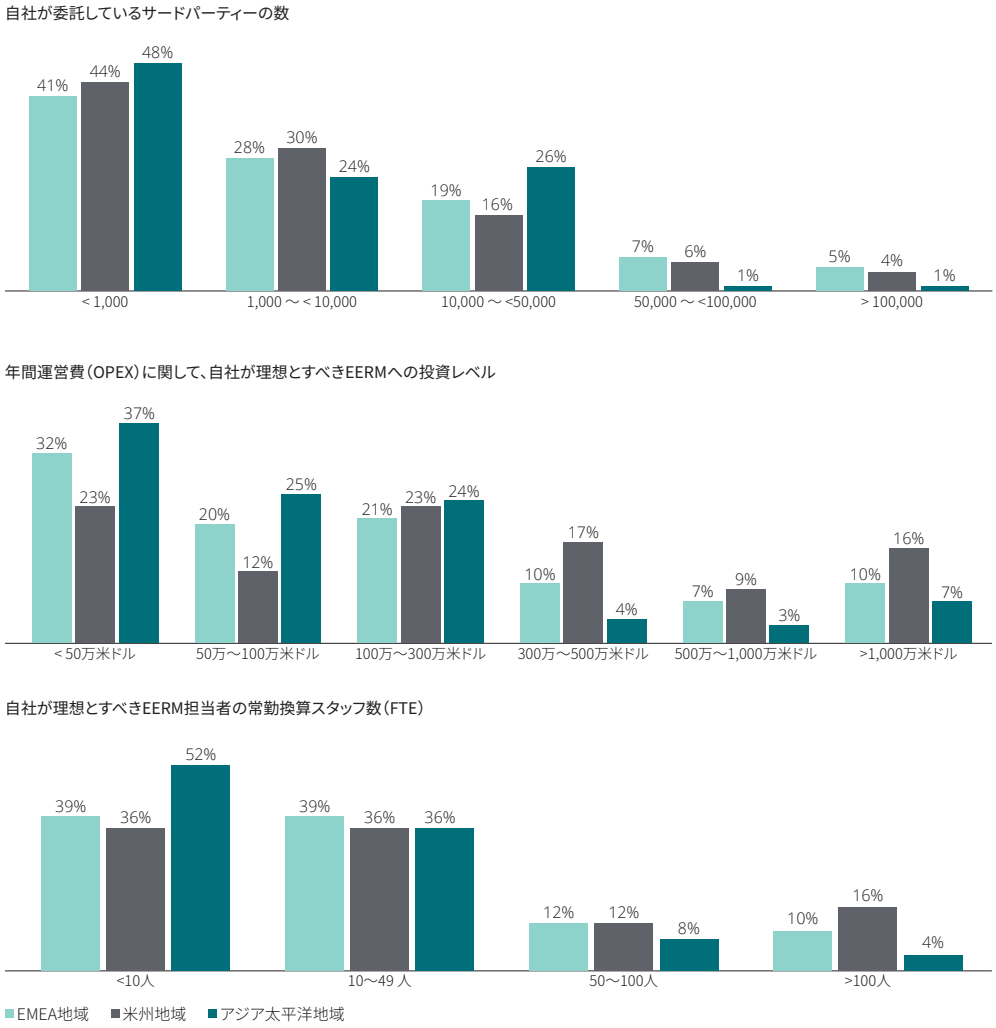


図 2.8 EERMにあるべき金額を支出しているかについての回答企業の考え（地域別）

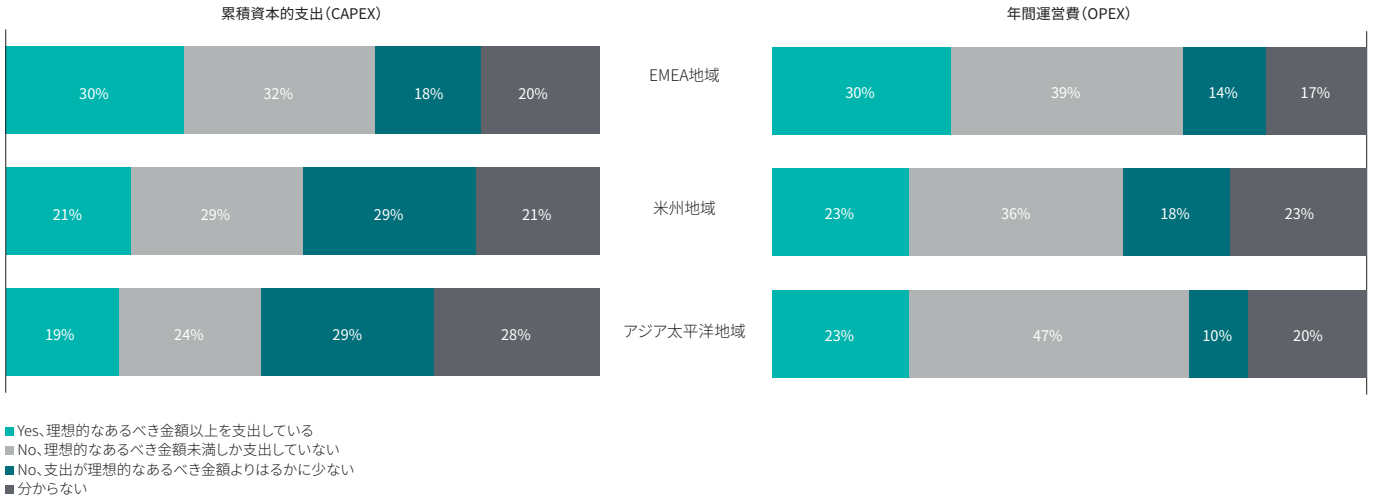
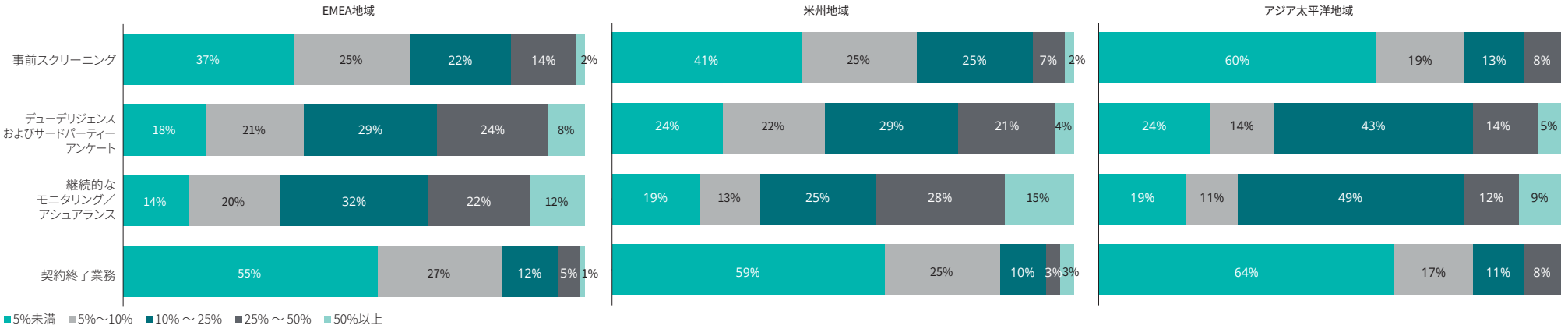


図 2.9 サードパーティーライフサイクルの各ステージにおけるEERMの年間運営費（OPEX）の内訳（地域別）



03

リーダーシップ

リーダーは、より優れた関与、
より良い協力およびデータの
よりスマートな使用を求めています。

これまでの経緯

2016年から、私たちの年次EERM調査は、取締役会と経営陣（最高経営幹部）がサードパーティーリスクの理解を深めることで、リスク監視、成長、パフォーマンスおよび戦略に関する責任のバランスをより適切に取ることができるようになっている様子をとらえています。

これは、重要な変化です。サードパーティーリスクマネジメントは、数十年にわたって、取締役会や企業のトップの問題ではなく、オペレーション上の問題と見なされていました。ようやく数年前に、EERMの位置付けに関するこの考え方が生まれ、先進的な組織にとって変革する機会となり始めました。

2016年から2018年に、EERMに関する最終的なアカウンタビリティを取締役会および最高経営幹部に移す組織の数が飛躍的に増加しました。現在、サードパーティーリスクは、緊急度に様々な違いはあるものの、先進的な企業と規制が厳しいセクターの企業において、取締役会の議題に常に取り上げられています。

とはいえ、2018年調査では、取締役会メンバーとリスクドメインオーナー間で、EERMに関する関与レベルに改善の余地があることが明らかになっています。調査回答者は、リスクドメインオーナーによる関与と理解の低さによって、協調が損なわれていると考えています。リーダーとリスクドメイン担当チーム、ビジネスユニットおよび調達、法務および内部監査などの部門における協調の向上は、組織におけるEERMの最優先事項となっています。

リーダーは、より優れた関与、より良い協力およびデータのよりスマートな使用を求めています。

2019年所見

今年の調査によると、取締役会と経営幹部がEERMに関する最終的な責任を引き続き担っていると回答した組織は、4分の3を超えています。責任の内訳は次のとおりです。

- **リスク責任者**が24%
- **CEO**が17%
- **取締役会**が19%
- **CPO**が10%
- **CFO**が8%

取締役会と経営幹部は、自身の役割をより責任をもって達成し、特定のリスクドメイン固有の問題やそれらを扱う社内スペシャリストとより密に関与したいと考えています。このような「インサイドアウト」のアプローチは、これまでの「アウトサイドイン」の観点を補うものです。3分の1以上（37%）の回答者は、組織におけるEERMの最優先事項は、リーダーとリスクドメインのチーム、ビジネスユニットに加えて、調達、法務および内部監査などの部門との間の社内的な協調の向上であると考えています。

その一方で、自社内の協調が組織内で強固であると考える回答者はわずか16%で、49%は社内協調が中程度である、としています。残りの35%は、低い、ほとんどない、または分からない、としています。

また、このインサイドアウトの思考は、サードパーティーのデータをよりスマートに活用するための組織的なイニシアティブに反映されています。取締役会とシニアリーダーは、定期的なカラーコード型（赤・黄・緑）ダッシュボードから、アラートとトレンド分析を備えた、簡潔かつリアルタイムに実行可能なインテリジェンスへの移行を求めています。

- 56%の回答者は、EERM用に**クラウドベースのプラットフォーム**を使用中または使用を予定しています。
- 45%は、**ロボティック・プロセス・オートメーション（RPA）**に着目しています。
- 36%は、このインテリジェンスをより実行可能にするために、**ビジュアリゼーション技術**を使用中または使用を予定しています。

図3.1 取締役会と経営陣が引き続き、EERMの最終的な責任を保持している

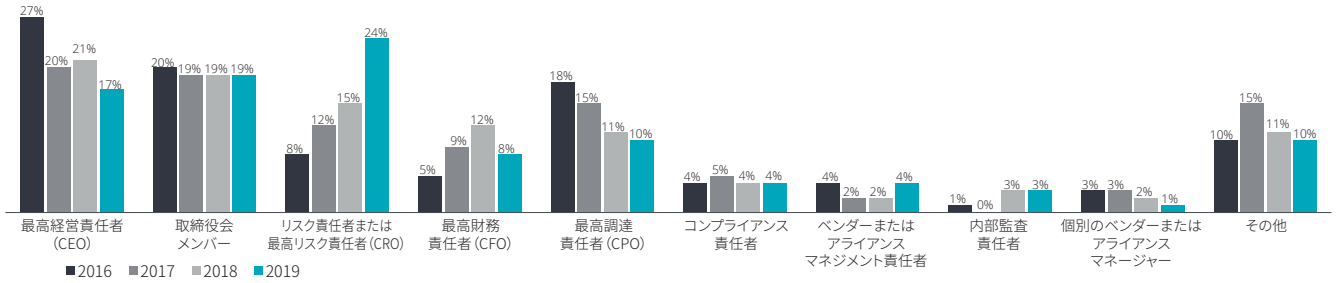


図 3.2 リスクドメインオーナー、調達、法務およびビジネスリーダーなどの主要EERMステークホルダー間の関与と協力のレベル

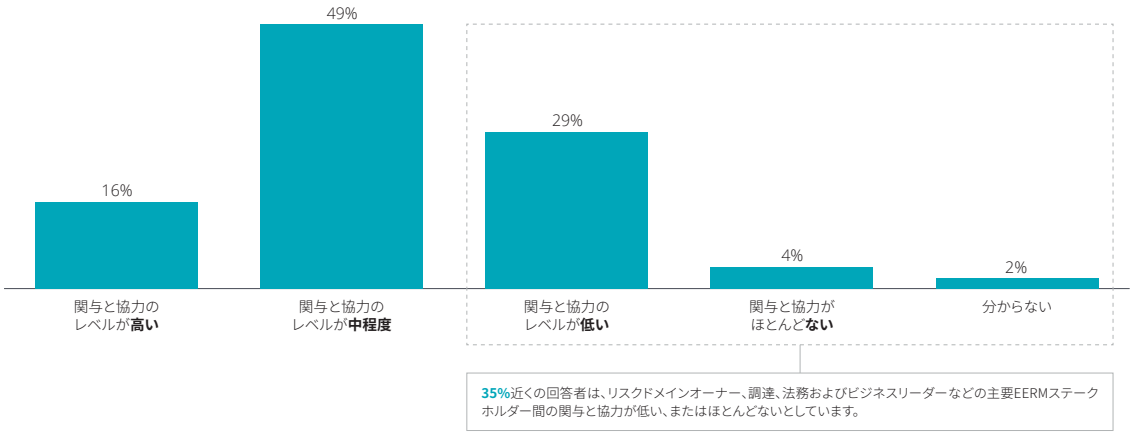
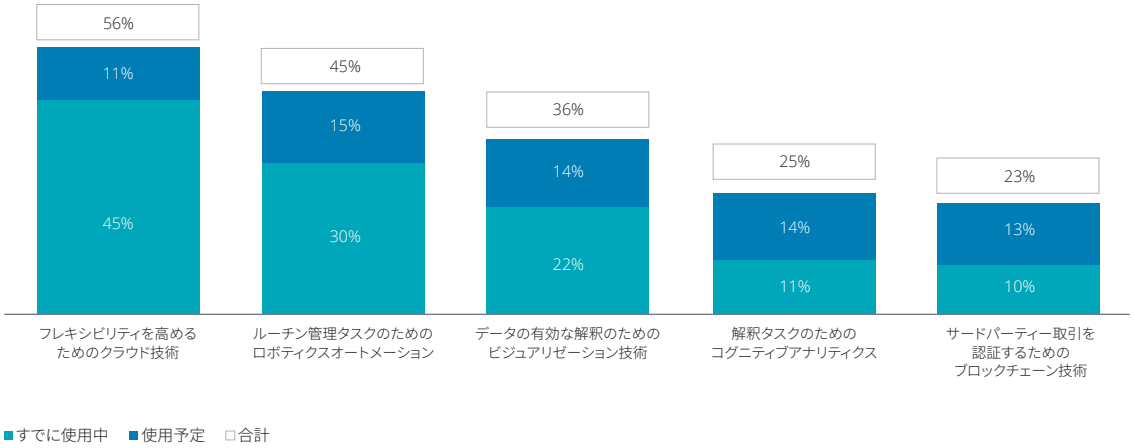


図 3.3 EERMに使用されているエマージングテクノロジー



デロイトの視点

企業が効率的かつ効果的に、サードパーティーがもたらす機会の実現とリスク管理とを開始できるようにする上では、取締役会および最高経営幹部によるEERMのオーナーシップと監督が不可欠です。

サードパーティーリスクマネジメントの責任を負うチームは、このシニアレベルの関心を利用し、予算の制約に対して問題提起し、課題を解決するための投資を要求すべきです。

また、シニアレベルのオーナーシップは、協調的な戦略投資を推進するために、組織全体の協調を促進し、相反する優先項目を解決することもできます。これによって、セクション2で検討した断片的な投資へのアプローチからの切り替えが促されるでしょう。

2018年には、EERMにおけるイノベーションの拡大を取締役会が要望していることがわかりました。サードパーティーに関する情報を 理解しやすく、意義あるものにすることを目指した、取締役会向けレポーティングおよびダッシュボードの出現が挙げられます。サードパーティーに関する自警の仕組みのタイムリーな導入とシームレスな統合によって、各チームが差し迫ったリスクや業績面での課題をより効率的に特定できるようになります。これは、脅威が現実となるのを防ぐことになります。

組織内の協調的なアプローチにより、EERMに関与する人々が事業にもたらす様々な観点とスキルセットが結び付けられます。これによって、懸念と機会が生じる最も重要な領域に対して、リスクマネジメントのリソースを効果的に配置することができます。

業種別ハイライト

各業種において、EERMの最終的な責任は、取締役会と最高経営幹部が担う傾向にあります。その一方で、興味深い差異がいくつかあります。CROが最終責任を有する割合が最も多い業種（消費財・産業機械、金融サービス、ライフサイエンス・ヘルスケア）では、EERMの成熟度が最も高くなっています。

エネルギー・資源セクターとテクノロジー・メディア・通信セクターでは、取締役会の比率が最も高く、政府・公共サービスセクターでは、CEOまたはCFOとなっています。サードパーティーがサプライチェーンと関連する企業においては、最高調達責任者（CPO）が責任を負う傾向が強くなります。

エネルギー・資源セクターは、自組織が十分な関与と協力を有している、と考える企業が最も多くなっています。これに、金融サービスセクターとテクノロジー・メディア・通信セクターが続きます（各セクターの16%）。反対に、政府・公共サービスで同じ考えの回答者はいませんでした。

多くのセクターにおいて、最も利用されているエマージングテクノロジーは、クラウド技術で、RPAが続きます。さらに興味深い所見を以下に挙げます。

- **クラウド技術**の導入率が最も高いのは、消費財・産業機械セクターです。3分の2近く（65%）がこのテクノロジーを使用中、または使用を計画中で、ライフサイエンス・ヘルスケア（55%）、エネルギー・資源（53%）、金融サービス（52%）、テクノロジー・メディア・通信（49%）、政府・公共サービス（44%）の各セクターが続きます。
- 消費財・産業機械セクターは、**RPA**についても導入率が最大です。過半数（52%）がこのテクノロジーを使用中、または使用を計画中で、ライフサイエンス・ヘルスケア（50%）、テクノロジー・メディア・通信、政府・公共サービス（それぞれ44%）、金融サービス（41%）、エネルギー・資源（40%）の各セクターが続きます。
- **ビジュアリゼーション技術**が最も浸透しているのは、ライフサイエンス・ヘルスケアセクター（55%）で、消費財・産業機械（39%）、テクノロジー・メディア・通信（37%）、エネルギー・資源（33%）、金融サービス（32%）、政府・公共サービス（22%）の各セクターが続きます。

図 3.4 主要EERMステークホルダーとビジネスリーダー間の関与と協力のレベル（業種別）

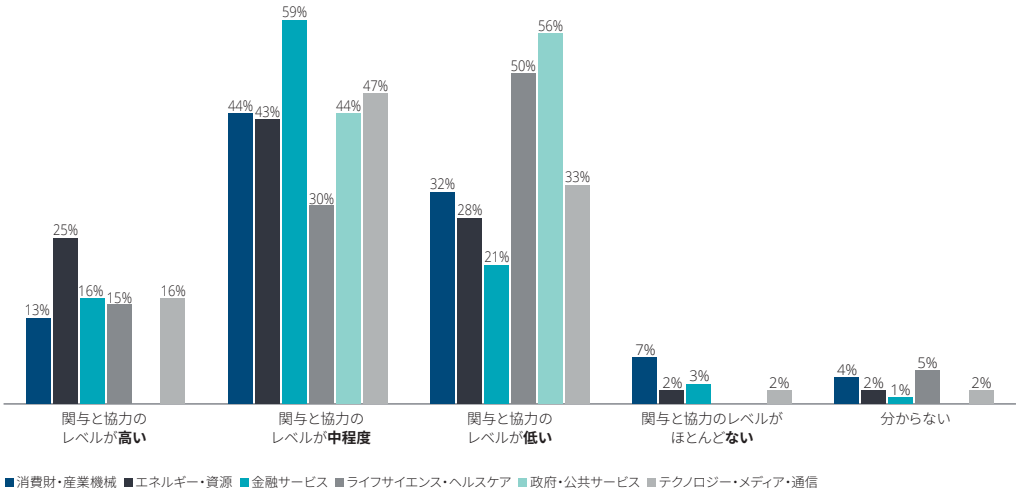


図 3.5 EERMに関する最終的な責任（業種別）

	消費財・産業機械	エネルギー・資源	金融サービス	ライフサイエンス・ヘルスケア	政府・公共サービス	テクノロジー・メディア・通信
最も比率が高い	CEO	取締役会	CRO	CRO／取締役会	CEO／CFO	取締役会
2番目に比率が高い	CEO	CPO	取締役会	CEO	取締役会／CRO	CEO
3番目に比率が高い	取締役会	CEO	CEO	CPO	コンプライアンス	CRO

図 3.6 使用中のエマージングテクノロジー（業種別）

地域別ハイライト

取締役会と経営陣による、リスクドメインオーナー、調達および法務チームとの関与と協力を改善するニーズが最も高いのは米州地域で、現在の関与レベルが高いとした回答者は、わずか11%でした。この数値は、アジア太平洋地域（16%）、EMEA地域（17%）では、わずかに米州地域を上回っています。

アジア太平洋地域が傑出しているのは、EERMのためのテクノロジーの利用または利用の計画で、クラウド（65%）およびRPA（58%）となっています。

これはおそらく、同地域のEERMへの設備投資がかなり遅い時期に始まったため、その時点で、新しいテクノロジーがかなり進んだ導入段階になっていたことに原因があります。

その一方で、米州地域とEMEA地域の企業は現在、クラウドへの移行やRPAの導入を可能とする追加機能を活用するために、EERMへの初期投資のアップグレードに取り組んでいます。

クラウドまたはRPA技術の導入についての比率は、EMEA地域ではそれぞれ56%と43%となっており、米州地域では43 %と42%になっています。

同様の傾向は、エマージングテクノロジーのすべての形態で見られますが、例外として、コグニティブアナリティクスの導入については、米州地域が僅差でトップとなり（27%の回答者）、続いてEMEA地域（26%）、アジア太平洋地域（23%）となっています。

図 3.7 主要EERMステークホルダーとビジネスリーダー間の関与と協力のレベル（地域別）

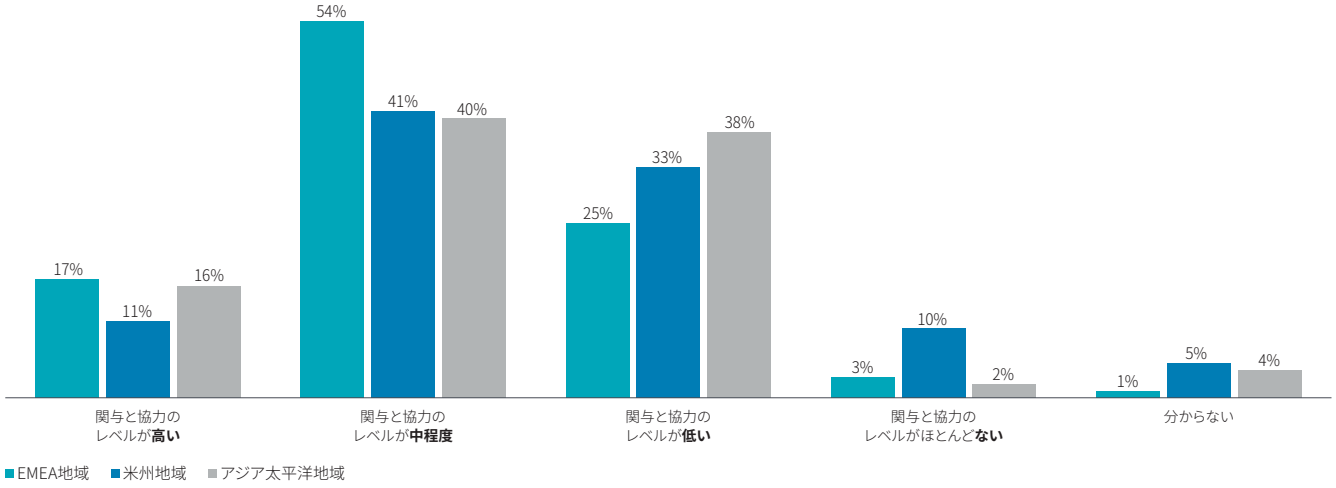
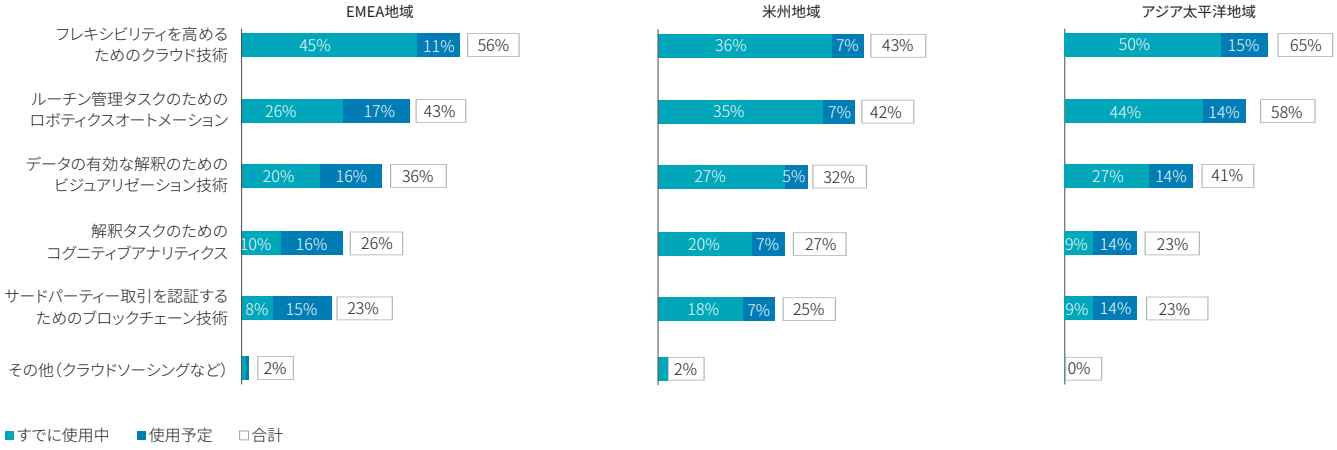
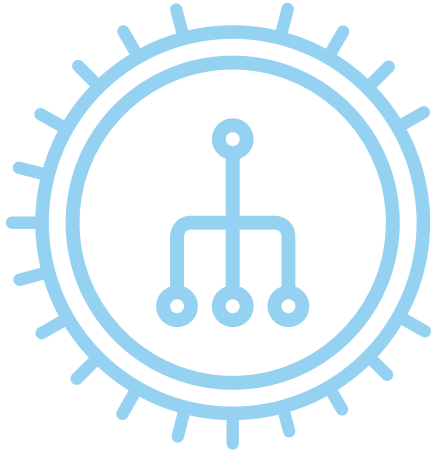


図 3.8 EERMに使用されているエマージングテクノロジー（地域別）



04



オペレーティングモデル

フェデレーテッド構造は、
EERMの主流のオペレーティングモデルであり、
シェアードサービスとセンターオブエクセレンスを
基盤としています。

これまでの経緯

2015年から2018年の私たちの調査によって、サードパーティーリスクマネジメントのオペレーティングモデルにおける、様々な変化が明らかにされています。

2016年には、企業は、集権型の社内モデルと社外サービスプロバイダーをベースとするモデルのどちらを選択するかを決定するプロセスの過程にありましたが、これはサードパーティーのモニタリングのみに関するものでした。

2016年半ばにこの問題は、ガバナンスとリスクマネジメントの主要要素において分散型と集権型のどちらを選択するかという、より幅広い議論となりました。市場と顧客の要求の変化に対して、業務部門が俊敏に対応するには、ある程度の分散化が必要でしたが、EERM機能自体は、一貫性を実現するために、より集権的であることが求められました。

2017年と2018年には、役割、テクノロジーおよびプロセスにおける要素の集権化がさらに一般的になりましたが、それは分散型構造に組み込まれていました。その結果、最も一般的なオペレーティングユーティリティモデルとして登場し始めたのが、センターオブエクセレンス（CoE）とシェアードサービスセンター（SSC）です。これは、サードパーティーベンダーによって提供される、市場ユーティリティモデルとマネージドサービスモデルの活用への要望の高まりを伴っています。

フェデレーテッド構造は、EERMの主流のオペレーティングモデルであり、シェアードサービスとセンターオブエクセレンスを基盤としています。

2019年所見

今回の調査によると、CoEまたはSSCによって支えられる、EERMのフェデレーテッド構造は、現在、3分の2（69%）の企業に存在しています。この構造は、EERMのための持続可能なオペレーティングモデルへの転換を加速しています。高度な集権型を維持している企業は、わずか11%に過ぎません（昨年の17%から減少）。高度な集権型ではない、残りの89%の多くは、EERMのフェデレーテッド構造を導入しています（69%）。

EERMの新しいフェデレーテッド構造は、以下によって支えられることが多くなっています。

- **CoE：53%**の組織がすでに有しており、さらに21%が構築を予定しています。
- **SSC：38%**の組織が使用しており、さらに20%が構築を目指しています。

今回の2019年調査では、マネージドサービスとシェアードアセスメントおよびユーティリティについて、様々な業務部門にまたがる共通の機能として浸透が進んでいる点が再確認されました（従来は業務部門は個々で自律的に活動していました）。このような業務部門には、事業または地域、コーポレート機能領域が該当します。

今回の2019年調査で初めて捉えた現象として、3種類のマネージドサービスモデルがあります。

1. **リスクインテリジェンスを取得するためのマネージドサービス**には、該当データの共有交換を推進するユーティリティモデルが挙げられます。18%の企業がこのモデルを使用し、さらに21%が計画しています。これは、最も浸透しているマネージドサービスソリューションです。
2. **社内スタッフを配置するマネージドサービス：**18%の企業がこのサービスを使用し、さらに13%が計画しています。
3. **EERMテクノロジーを用いたマネージドサービスソリューション：**11%がこのサービスを使用し、さらに14%が計画しています。

マネージドサービスとシェアードアセスメントおよびユーティリティへの投資は、人員増のニーズを削減し、設備投資を大幅に削減することによって、効率性を向上させます。

4分の3近く（73%）の回答者は、これらの持続可能なソリューションを導入後は、累積資本的支出（CAPEX）がEERMの年間運営費（OPEX）を上回るべきでない、と考えています。さらに14%は、そこまでは行かないまでも、CAPEXがOPEXのおよそ2倍に下がるべきだと考えており、10%はその比率を3倍としています。これは、昨年の回答者による、EERMの累積CAPEXが通常、OPEXの3〜5倍になる、という見積もりから大幅に減少しています。

今回の調査で、新たな協調的トレンドとして、予算の共同オーナーシップが挙げられます。これを支えているのは、根本的に強力な集権型管理です。EERMの予算管理を担うのは、コアビジネスのリーダーと調達部門が増えています。

- **CEO／取締役会／経営陣：24%**
- **調達：27%**
- **ビジネスユニット：28%**
- **各地域のリーダー：4%**

図 4.1 EERMのフェデレーテッド構造が標準となる

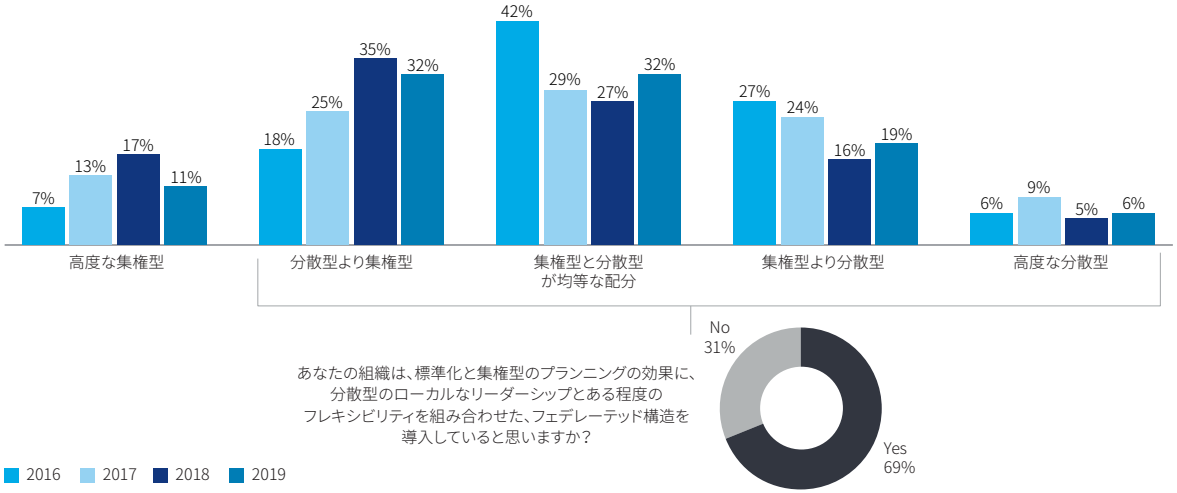


図 4.2 CoE、SSC、マネージドサービスおよびユーティリティの使用

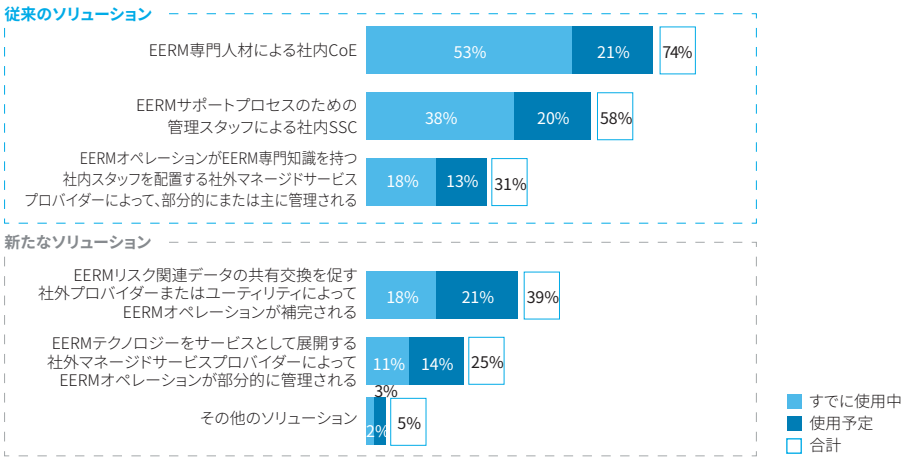
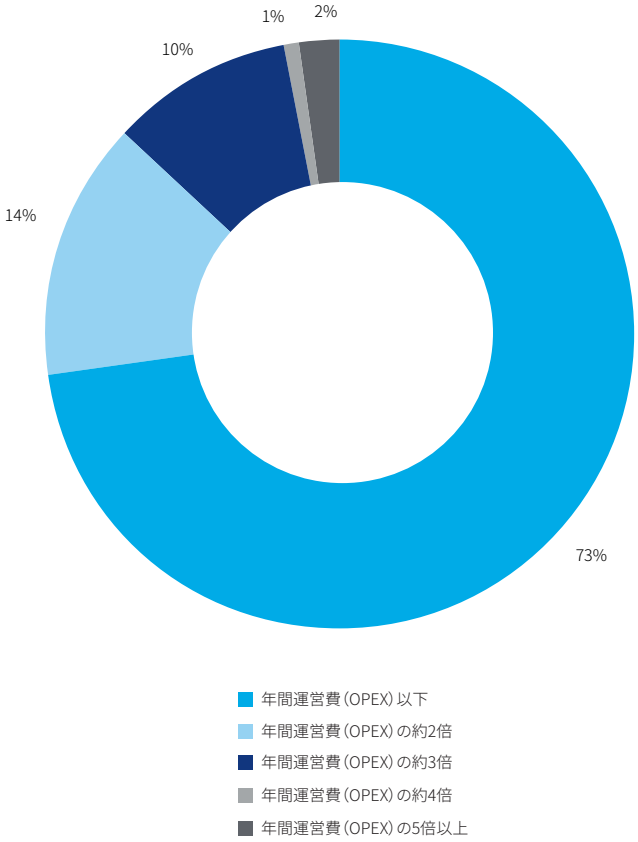


図 4.3 EERMのCAPEXへの投資レベル



デロイトの視点

集権型でありながら協調的なEERMへのアプローチを目指すトレンドは、現実的な進め方です。このアプローチにより、以下をはじめとする重要な価値が創出されます。

- 財務上の利益
- 効率性の向上
- 品質の改善
- 統制されたアジリティを通じた厳格な一貫性

CoEとSSCは、組織内で自律的に活動する業務部門間を連携させるアプローチをとることで、上述のような価値を引き出すことができます。

EERM予算の共同オーナーシップという新しいトレンドは、業務部門環境の多様性と各拠点のステークホルダーのニーズを考慮したものです。企業は、EERM予算を引き続き中央で管理する一方で、事業や業務部門のリーダーによる関与をさらに強化します。例えば、業務部門のリーダーは、自身の部門固有のEERM活動に参加を求められることがありますが、これにより、一貫性と柔軟性のバランスがよくなります。

取締役会と経営陣は、オンラインでリアルタイムなEERMに関するインサイトを提供する新たなテクノロジーへの投資を始めています。これらテクノロジーは、取締役会とエグゼクティブがサードパーティーに関する問題についての意思決定を支援すると共に、継続可能なオペレーティングモデルの中枢を担います。中央管理しつつ協調するアプローチを採ることで、EERMの包括的なイニシアティブの導入が容易になります。

共通のEERMの確立にあたって、マネージドサービスソリューションの検討は論理的に考えて次の段階といえます。

自律的に活動している事業部門が、自部門のサードパーティーリスクを管理するために自部門にとって最も重要で関連性があると思われる個別のマネージドサービスソリューションを選定・構築したいという考えは抑制すべきです。もし、このような独自の動きが行われれば、組織全体のEERMに非効率性と非一貫性がもたらされるでしょう。

企業によっては、特定の業務部門や、タイムゾーン別の要望に応えるための中継機能を設置することが適切な場合もあるかもしれません。ただし、このような中継機能の設置には、方法論と品質の一貫性を保つために必要なスキルを備えたスタッフを適切に配置することが求められ、すべての組織に適している訳ではありません。

業種別ハイライト

すべての業種において、EERM予算における集権的な統制と、協調と共同オーナーシップを向上させようという意図とのバランスが見られます。

自らを高度な集権型と見なす企業が最も少なかったのは、テクノロジー・メディア・通信セクター（9%）で、金融サービス（10%）と政府・公共サービス（11%）が続きました。自社を高度な集権型と見なす企業が最も多かったのは、ライフサイエンス・ヘルスケア（15%）で、僅差でエネルギー・資源（14%）が続きました。

政府・公共サービスセクターは、フェデレーテッド構造を導入していると考える組織が最も多くなりました（88%）。続いて、消費財・産業機械（72%）、ライフサイエンス・ヘルスケア（71%）となっています。

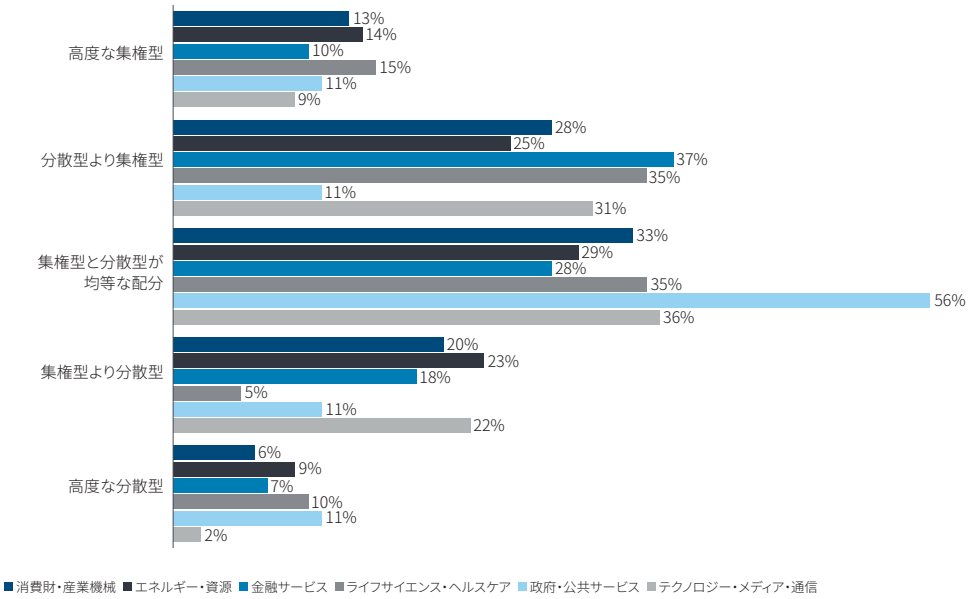
CoEの導入率が最も高かったのはライフサイエンス・ヘルスケアセクターで、設立済みまたは予定している企業が95%に上っています。続いて、政府・公共サービス（78%）、金融サービスおよび消費財・産業機械（共に73%）となっています。

社内シェアードサービスセンターの導入についても、最も比率が高かったのはライフサイエンス・ヘルスケアセクターで、導入済みまたは予定している企業が70%に上りました。続いて、消費財・産業機械（62%）、政府・公共サービス（56%）、エネルギー・資源（55%）となっています。

マネージドサービスソリューションの検討は、すべてのセクターで増加しています。社内スタッフを配置する、従来型のマネージドサービスソリューションが最も多かったのは、ライフサイエンス・ヘルスケアセクターで、50%がすでに導入しているか、このソリューションの導入を予定しています。政府・公共サービスセクターが44%、消費財・産業機械セクターが35%でした。

ライフサイエンス・ヘルスケアセクターは、データの共有交換を促進するユーティリティモデルを始めとする、リスクインテリジェンスを取得するためのマネージドサービスソリューションについても、導入の比率が最も高く（55%）なっています。他に導入率が高いセクターは、テクノロジー・メディア・通信（51%）、消費財・産業機械およびエネルギー・資源（それぞれ41%）でした。

図 4.4 導入されているEERM構造（業種別）



あなたの組織は、標準化と集権型のプランニングの効果に、分散型のローカルなリーダーシップとある程度のフレキシビリティを組み合わせた、フェデレーテッド構造を導入していると思いますか？

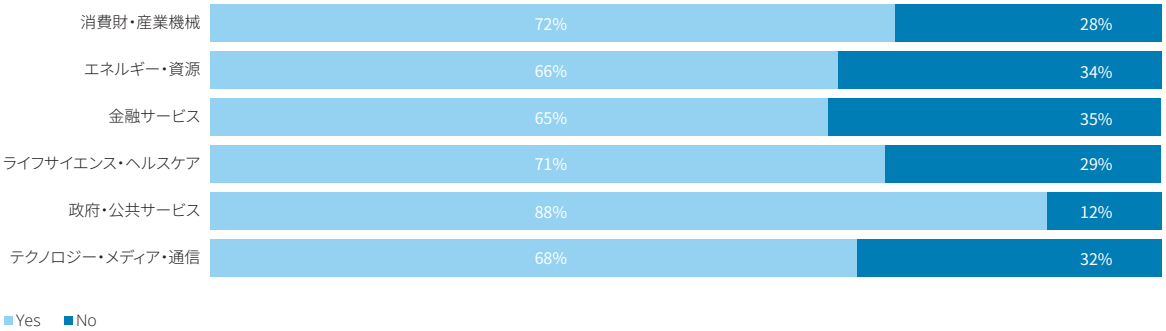
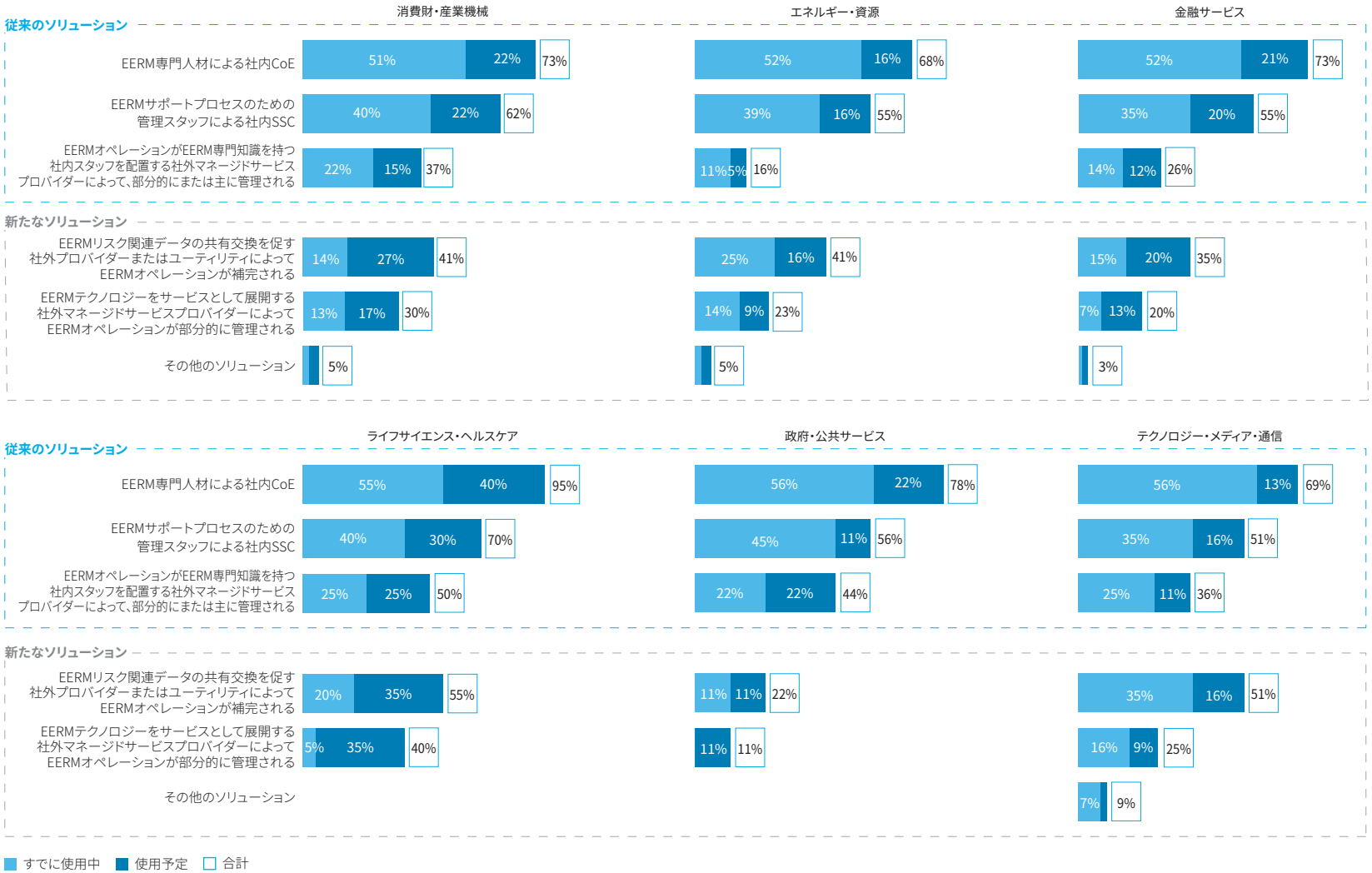


図 4.5 フェデレーテッド構造をサポートするために使用している、または使用する意図があるモデル（業種別）



地域別ハイライト

3つの地域すべての圧倒的多数の企業が何かしら分散型の要素を取り入れ、高度な集権型の企業はごく少数になっています。高度な集権型の企業の比率は、EMEA地域でわずか12%となり、米州地域で10%、アジア太平洋で9%となっています。

アジア太平洋地域の4分の3以上（76%）の企業は、EERMに集権型統制の効果をもたらすために、フェデレーテッド構造を導入しています。この比率は、EMEA地域（69%）と米州地域（60%）ではアジア太平洋地域に比べてやや低くなっています。

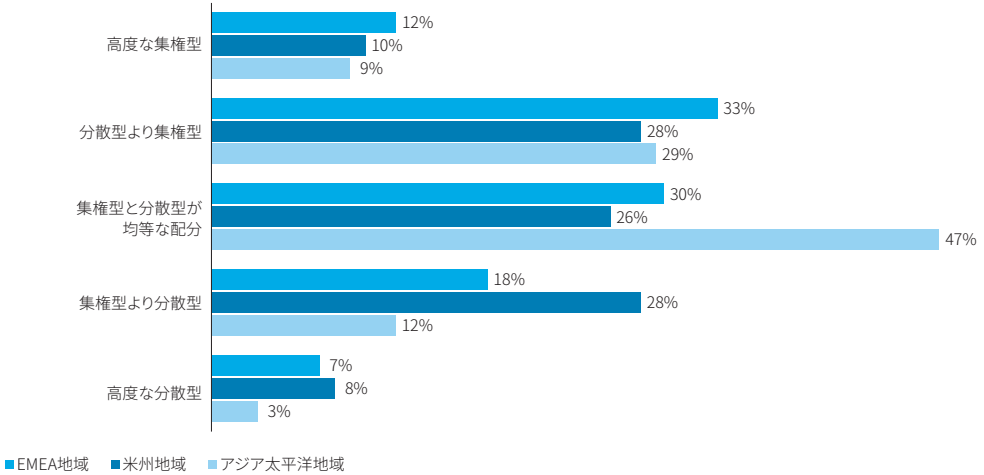
また、アジア太平洋地域はCoEおよびSSCの導入予定でもトップでしたが、実際の導入率は世界で同様の傾向となっています。これは、EMEA地域と米州地域に比べて、同地域でのSSCへのアクセスの優位性や容易さによるものと思われます。

おそらく同一の理由で、社内スタッフの配置を特徴とするマネージドサービスモデルについても、アジア太平洋地域の導入率が高くなっています。半数近く（46%）の回答者がこのモデルを導入しており、さらに22%が導入を予定しています。ここでも、米州地域とEMEA地域にとっての潜在的な機会が示されました。

アジア太平洋地域は、サードパーティーリスクデータの共有交換、またはサービスとしてのテクノロジーの展開を含むマネージドサービスについても、トップとなっています。

米州地域では、EERM予算の統制権を与えられることが最も多いのは、組織／ビジネスユニットのリーダー（60%）と購買チーム（30%）でした。これは、EMEA地域にも該当します（組織／ビジネスユニットのリーダーが58%、購買チームが30%）。一方、アジア太平洋地域では、組織／ビジネスユニットのリーダーがEERM予算を統制する事例は43%しかなく、購買チームは15%となっています。同地域では、リスクマネジメント部門が予算を統制する比率が最も高くなりました。

図 4.6 導入されているEERM構造（地域別）



あなたの組織は、標準化と集権型のプランニングの効果に、分散型のローカルなリーダーシップとある程度のフレキシビリティを組み合わせた、フェデレーテッド構造を導入していると思いますか？

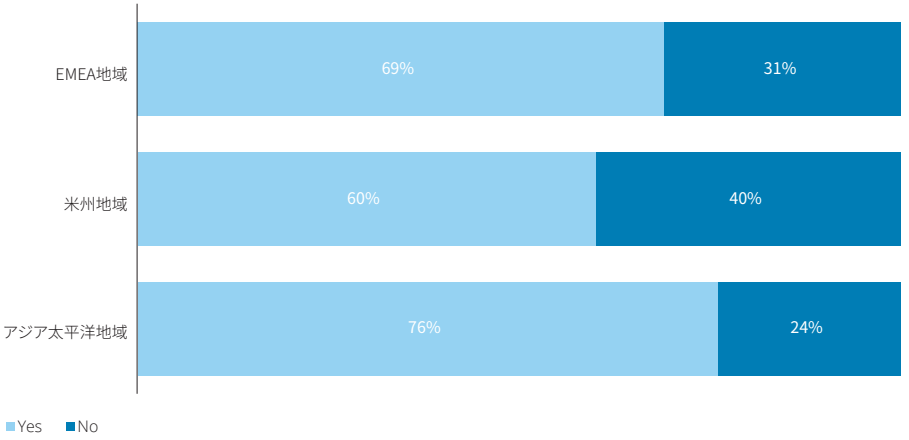


図 4.7 フェデレーテッド構造をサポートするモデル(地域別)

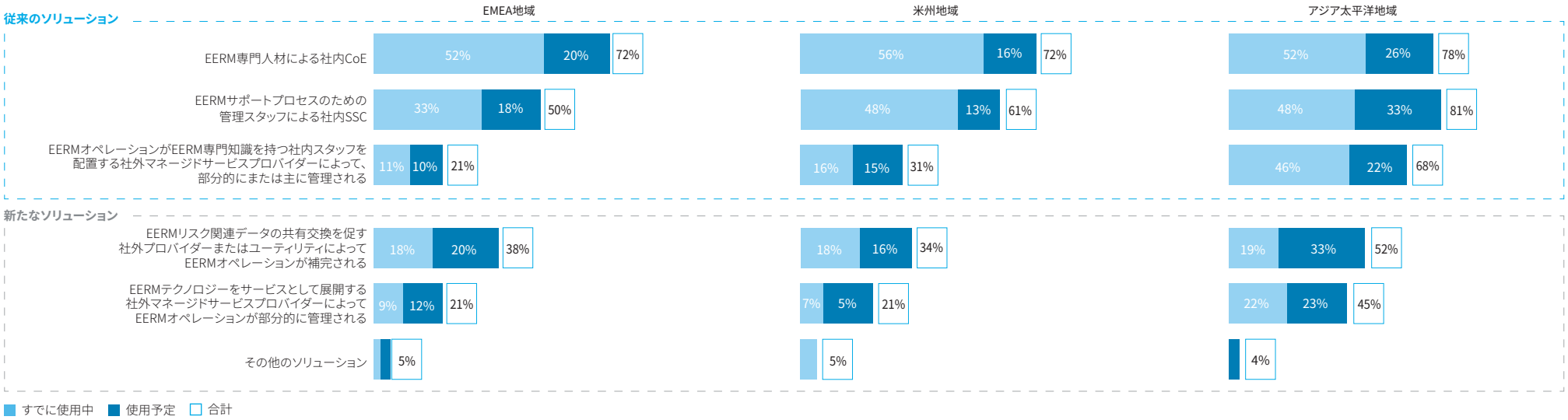
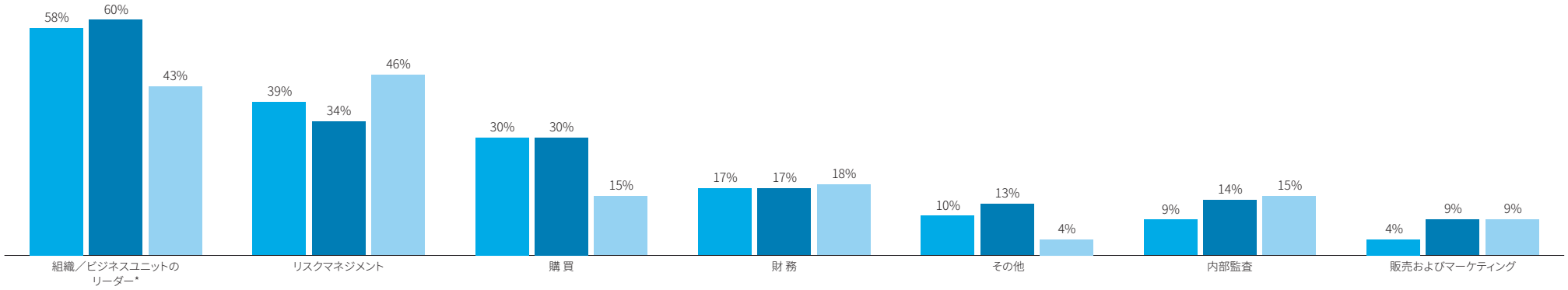
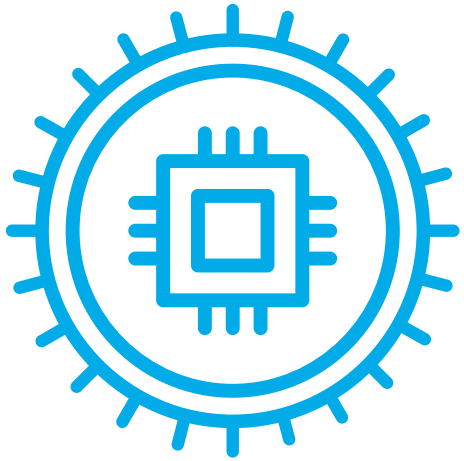


図 4.8 EERM予算のオーナーシップ(地域別)



*注:
組織/ビジネスユニットのリーダーは、CEO/経営陣/取締役会、ビジネスユニットおよび各地域のリーダーによって構成されます。
本チャートで合計が100%を超える場合、EERM予算に複数のオーナーシップ(通常はリーダーとほかの機能)が存在することを示しており、フェデレーテッド構造の意図が反映されています。

05



テクノロジー

企業は、多様な業務部門にわたる
EERMテクノロジーの合理化および
簡素化に取り組んでいます。

これまでの経緯

デロイトのEERM調査により、2016年時点では、エンドツーエンドのEERMプロセスに対してのテクノロジー活用アプローチが秩序立っていなかったことが明らかになりました。

その翌年までには、圧倒的多数（90%）の回答者がEERMに使用するツールとテクノロジーに関する課題を表明していました。懸念として挙がっていた点は、サードパーティーリスクを包括的に管理するための一元的なテクノロジーの欠如、および組織内で用いられるサードパーティーマネジメントプロセスの不協和が挙げられました。EERMを統合し、最適化することが困難になっていた原因はこの点にありました。

その一方で、2018年には、2つの新たなトレンドがこの懸念を軽減し始めています。

1つは、本レポートで前述したように、テクノロジーへの投資に対する、より協調的なアプローチの段階に入ったことが挙げられます。これは、以下の2点によるものです。

- 集権的なオーナーシップとマネジメントの導入
- CoEおよびSSCの浸透

もう1つは、3層テクノロジーアーキテクチャ（次ページの図を参照）が登場したことです。EERMのための単一のテクノロジーソリューションは、まだ出現しつつある段階でした。

企業は、多様な業務部門にわたるEERMテクノロジーの合理化および簡素化に取り組んでいます。

2019年所見

今回の調査は、EERMにおける合理化および標準化テクノロジーへの投資のための階層（Tier）アプローチが継続するという、デロイトの予測を裏付けるものになりました。自社独自の複雑なカスタムメイドのソリューションの開発を求める企業はごくわずかです。これは、本レポートのこれまでのセクションですでに述べたように、持続可能なオペレーティングモデルの導入を裏付けています。

Tier 1

今回の調査で判明したのは、Tier1内で、主要なERPおよび購買プラットフォームの位置付けがさらに強固なものになったことです。これらのプラットフォームは、新しいフェデレーテッド構造をサポートするための共通の基盤と運用上の規律の構築に役立っていると回答者は述べています。半数以上（59%）の企業は、EERMの中核を成す基幹コンポーネントとして、ERPまたは購買プラットフォームを活用しています。主なソリューションには、以下が挙げられます。

- SAP（30%の回答者）
- Oracle（17%）
- SAP Ariba（15%）
- Microsoft Dynamics（8%）

Tier 2

4分の3（75%）の回答者は、EERMのためのリスクマネジメントソリューションを導入しています。回答者の間で、以下の2つの意見に分かれています。

- **EERM特化型リスクマネジメントパッケージ**：10社中2社近く（18%）の企業は、EERM特化型リスクマネジメントパッケージを使用しています。このパッケージは、「ベストオブニーズ」ソリューションと称される場合があります。
- **市販の統合型リスクマネジメントソリューション**：サードパーティーマネジメントのために使用されます。半数以上（57%）の企業は、EERM用に市販の統合型リスクマネジメントソリューションを使用しています。これは、組織における全社的なテクノロジーアーキテクチャを合理化するもので、「ベストオブブリード」ソリューションと称される場合があります。このソリューションには、RSA Archer（13%の回答者）、IBM OpenPages（8%）、Thomson Reuters（6%）、ServiceNowおよびMetricStream（それぞれ4%の回答者）が挙げられます。

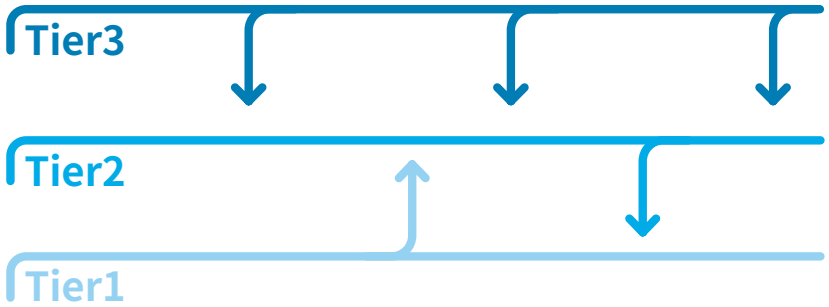
Tier 3

現在、Tier3として一般的なのは、ドメイン固有のリスクインテリジェンスソリューションです。このソリューションが増加している特定リスクドメインには、以下が挙げられます。

- 財務的実行可能性：30%
- 金融犯罪：28%
- 契約管理：18%
- 持続可能性：11%
- サイバー脅威：9％

企業が求めているのは、社内のリソースや人員に投資することなく、マネージドサービスまたはユーティリティなどを使用して、ほかのリスクドメインにおけるリスクインテリジェンスを得ることです。

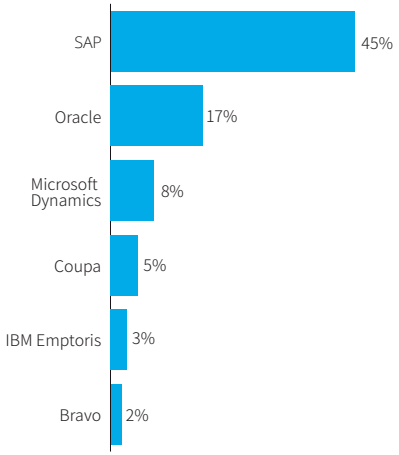
EERMツールとテクノロジーに関する階層アーキテクチャの進化



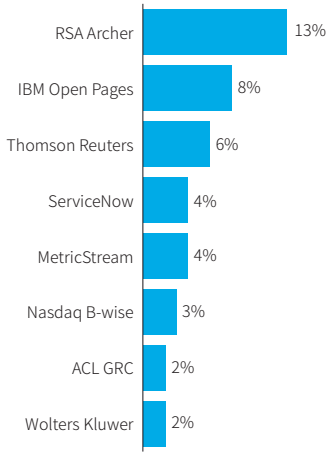
- **Tier1**：EERMに関する共通の基盤と運用上の規律を構築するエンタープライズリソースプランニング（ERP）または購買プラットフォーム。
- **Tier2**：企業のサードパーティーマネジメント要件に合わせた、EERM特化型リスクマネジメントパッケージ、またはEERM機能を含む市販のガバナンス・リスク・コンプライアンス（GRC）や統制マネジメントプラットフォーム。
- **Tier3**：財務的実行可能性、金融犯罪、契約管理およびサイバー脅威などの専用のリスクドメインからのフィードを提供する、特定のEERMプロセスまたはリスクのためのニッチパッケージ。

図 5.1 EERM テクノロジーソリューションの使用

(a) ERPおよびP2Pシステムまたは
その他のバックボーンインフラストラクチャ：**59%**



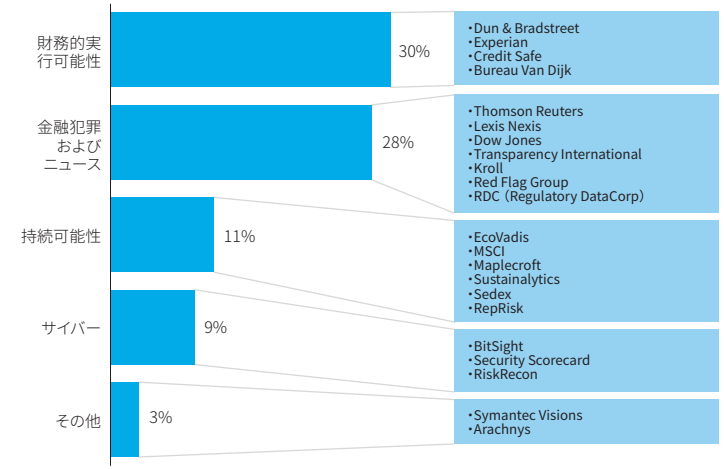
(b) GRCおよび統制
マネジメントソリューション：**57%**



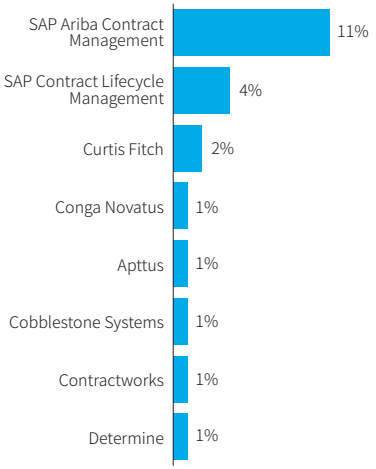
(c) EERM特化型リスクマネジメントプラットフォーム
またはユーティリティ：**18%**

本調査で特筆すべきプラットフォームは
明らかになりませんでした。

(d) EERMに関するリスクインテリジェンスを提供する
ドメイン特化型フィーダーシステム：



(e) 契約管理および分析：**18%**



デロイトの視点

多岐にわたるビジネスユニットと業務部門において、EERMテクノロジーの標準化と合理化への強い要望があります。3層にわたるEERMテクノロジーへの投資を最適化することにより、効率性の推進、コストの削減、サービスレベルの改善、株主資本利益率の向上、さらには持続可能なオペレーティングモデルへの移行が可能になります。

2019年と2020年は、変革イニシアティブ、および関連する設計と導入に対して、EERMのCAPEXの投資が増加していくことが予測されます。多くの企業は、これらのイニシアティブが順調に導入された時点で、継続的なCAPEXをEERMの年間OPEXと同一レベルまで抑え込むという目標を達成していくでしょう。

また、サードパーティーリスクマネジメントツールは、パフォーマンス、契約、商業上のイシュー、これらの問題によって生み出されるリスクと連動した、より包括的で統合された管理が可能にする広義のサードパーティーマネジメントツールに集束されるでしょう。

標準化されたガバナンス・リスク・コンプライアンス（GRC）ソリューションとEERM専用ソリューションのどちらを選ぶかについての議論は続くことが予想されます。組織内での統合推進を容易にするとはいえ、GRCソリューションが提供する標準化された機能の目的への適合度合いに対する不満は高まっていくでしょう。

今回の調査結果によると、現在のトレンドとして、主にサードパーティーマネジメントに関連する機能性に対応するために、「ベストオブニーズ」のシステムを導入する企業の増加が示唆されています。このシステムは、場合によっては、現行のGRCソリューションを補っていくでしょう。

この考察は、シンクタンクのOpen Compliance and Ethics Group（OCEG）による、GRC技術に関する2019年調査による裏付けがあります。この調査によると、標準化されたGRC技術アーキテクチャは、多目的のユーザーニーズを効果的にサポートすることができなくなっています。このようなニーズには、サードパーティーリスクマネジメントやドメイン固有のコンプライアンス要件が含まれており、例としてユースケースアプローチによるサイバーリスクマネジメントが挙げられます。このため、GRC技術アーキテクチャに対する満足度が下がっています。2018年に、単一のGRCソリューションに基づく、複数のユースケースとの組織の調整が十分である、または優れていると主張するユーザーはわずか21%で、2016年の28%から減少しています。

さらに、EERMテクノロジーソリューションに対する評価基準は、「より安く、より早く、より良く」を超えて進化し、以下を含むようになることをデロイトは予測しています。

- 新興市場におけるサポート
- ロボティクスおよびコグニティブオートメーションを利用する機能
- 将来のシェアードユーティリティおよびマネージドサービスプラットフォームとのシームレスな統合

06

下請業者と関連会社のリスク

サードパーティーの下請業者と関連会社がもたらすリスクへの監視が不十分です。

これまでの経緯

2018年EERM調査では、アウトソーシングに関連する重大なリスクが認識されました。多くの事例において、サードパーティーが受注した下請契約のプロセスの一部を外注することによって、下請業者である2次請け、3次請けを作り出し、さらに4次請け、5次請け、その先へと続いていく可能性があります。

この下請の連鎖の拡張は、元請け企業と連鎖の反対側に位置するため一見するとほとんど関係がないと思われる企業によって引き起こされる破壊的なインシデントの増加をもたらしています。例えば、6次請けが2次請け、3次請け、4次請け、そして5次請けによって構成される輪でつながり、発注元企業のオペレーションを害することもありえます。このため、様々な規制当局の注目を集めており、自社のサプライチェーン関係の監視の欠如に対して、企業に説明責任を課すようになっています。

何年もの間、企業は関連会社との関係を管理する方法について、十分な対策を講じることができていません。

2018年には、企業の多くが、ITおよびビジネスサービスデリバリーユニットに関する監視構造の構築に取り組み始めました。これらは、社内、アウトソース、関連会社（あるいはその組み合わせ）により提供されます。一般的にこの構造は、グローバルビジネスサービス（GBS）と呼ばれ、サードパーティー、社内（シェアードサービス）および関連会社チームの複雑な組み合わせを管理するために、別法人として設置される場合もあります。このようなGBSユニットは、EERMに複層的課題を生み出し、下請業者のリスクと類似したリスクや未知のリスクが伴います。

サードパーティーの下請業者と関連会社がもたらすリスクへの監視が不十分です。

2019年所見

今回の調査によると、持続可能なオペレーティングモデルとそれを実現するテクノロジーの活用に対するコミットメントにもかかわらず、企業による下請企業と関連会社のリスクへの対応は不十分です。

下請業者リスク

下請業者リスクは、2次請け／3次請けリスクとも称され、依然としてEERM を主導するリーダーから適切なレベルの注意を引いていません。

自社のサードパーティーが委託しているすべての下請業者を特定・監視している回答者は、わずか2%（昨年と同率）です。自社にとって最も重要な関係に関しては特定・監視を行っている回答者は、8%（昨年の10%から減少）です。残る90%は、継続的に求められる注意が欠如しています。

- 11% は、新規のサードパーティーを受け入れる際にのみ、2次請け、3次請け等の審査をしています（昨年の8 %から増加）。
- 44%は、2次請け、3次請け等の審査をサードパーティーに依存しています（昨年と同率）。
- 18%は、2次請け、3次請け等の審査を不定期に行っています（昨年と同率）。
- 17 %は、サードパーティーの特定、審査または監視をまったく行っていません（昨年と同率）。

関連会社リスク

企業は、関連会社に関するリスクの監視と管理へのアプローチについても、依然として、明確性に欠けています。3分の1近く（32%）の企業は、サードパーティーと同一の厳格さで、リスクの評価と監視を行っています。しかし、半数近く（46%）は、ある程度のあいまいさやその場しのぎのアプローチといった、異なる基準を挙げています。全体として、関連会社に関する当初のデューデリジェンスプロセスと継続的なモニタリングは、ほかのサードパーティーに比べて、あまり厳格ではない様子が見受けられます。
残りの22%の企業は、関連会社との関係を有していませんでした。

図 6.1 サードパーティーが委託する下請業者 - 2次請け／3次請け-のモニタリング

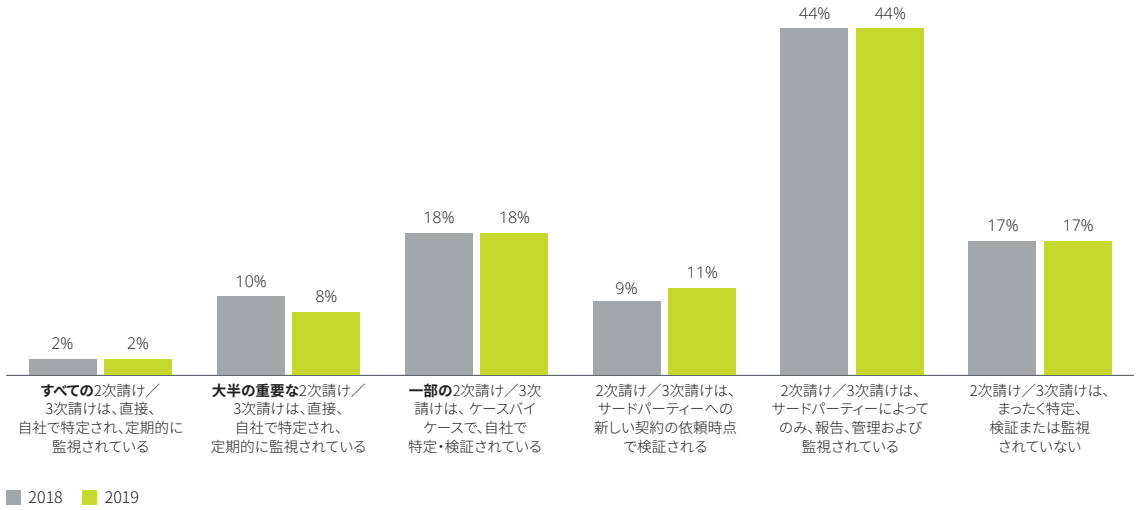
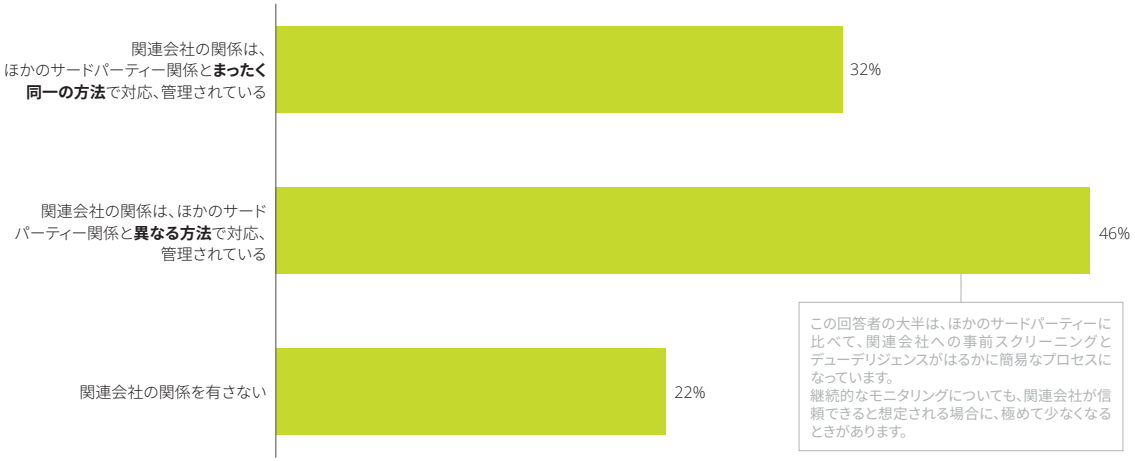


図 6.2 関連会社の管理へのアプローチ



デロイトの視点－下請業者リスク

下請業者に対する適切な監視の不足によって、下請業者リスクマネジメントに対する戦略とアプローチの決定が困難になります。通常、このリスクはサードパーティーのエコシステムの奥深くに存在しているため、監視の不足は、規律と厳格性をリスクマネジメントに適用する能力を損ないます。

この課題は、金融サービスをはじめ、システム全体の集中リスクが重大な懸念事項となっている、規制型産業に特に関連があります。とはいえ、直近の法律と規制は、2次請け／3次請けとの関係を管理する要件を含めているため、この懸念はほかの産業にも拡大しています。ここには、英国の現代奴隷法およびEUのGDPRが含まれます。集中リスクは、継続的なアセスメントを必要とする、拡張エンタープライズ(Extended enterprise)の複数の層に内在している場合もあります。

これらの「ネットワークの中のネットワーク」を発見し理解するため、先進企業は「イルミネーション」イニシアチブを通して、このような盲点への取り組みを開始しています。重要な下請企業を把握したら、次のステップは、これらの2次請けについて、サードパーティーが取得しているアシュアランスの内容を理解することです。このアシュアランスには、エビデンスによる裏付けが必須です。
企業によってはさらに先に進み、2次請けのアシュアランス業務を行うために、サードパーティーとの合同で検査のためのチームを形成している場合があります。また、ある企業は、追加のアシュアランス業務を自社で完了するという選択を依頼しています。これは通常、サードパーティーが下請業者との契約を締結する必要があります。

さらに一般的に、トップ企業は、支払い能力を始めとする、重要な下請け業者の統制環境を理解するためにリスクインテリジェンスツールを使用して、相手への負担が少ないアプローチを取り入れています。場合によっては、企業があまりにもリスクが高いと考える場合に、サードパーティーに対して下請業者を拒否する権限を要求することがあります。

デロイトの視点－関連会社リスク

関連会社は通常、同一グループに含まれるため、企業が有するリスクインテリジェンスのレベルは高くなる傾向があり、その例として、共通（グループ全体）のリスクポリシーの存在、あるいはグループ内部監査チームが履行する検証が挙げられます。さらに、グループ全体にインパクトを及ぼす財務的実行可能性などの特定リスクについて、別途、審査する必要がありません。

このため、関連会社の管理を社外プロバイダーほど厳格に行わないことは、関与するリスクに相応である場合は妥当と言えます。ただし、このスタンスは、適合性とコンプライアンスに関して、適切かつ継続的なアセスメントを基本としていなければなりません。このアセスメントを実施するアプローチには、統一性がなく場当たり的なものではなく、明確な定義化と一貫性が求められます。

同時に、GBS構造が（子会社または関連会社の関係の新しいバリエーションとして）組織に浸透し始めています。GBS構造は、すべてのサードパーティーに加え、社内シェアードサービスのデリバリーチームを含め、ガバナンス機構とグッドプラクティスの統合を目指すものです。これらの構造の範囲や属する法人は、企業によって異なります。そのため、サードパーティーリスクマネジメントが一層複雑になり、複層的な課題がもたらされています。

規制は通常、法人ごとに管理されているため、多くの場合、これらGBS組織は、関連する業界規制の直接の対象にはなりません。このため、リスクが実害として発生する場合、これらの組織を使用する発注側企業の全社的なレピュテーションが損なわれ、事業継続性が害されると共に、サービスを提供する子会社または関連会社によって、組織が重大な処罰や規制上の執行措置を招くことになります。

業種別ハイライト

政府・公共サービスセクターでは、下請業者によるリスクの特定、審査または監視が不十分である比率が最も多く、回答者の44%となりました。さらに44%は、この取組みをサードパーティーに委ねることを選択しています。

下請業者によるリスクの特定、審査または監視が不十分である比率が次に多かったセクターは、ライフサイエンス・ヘルスケアで、30%となりました。50%は、この取組みをサードパーティーに委ねています。

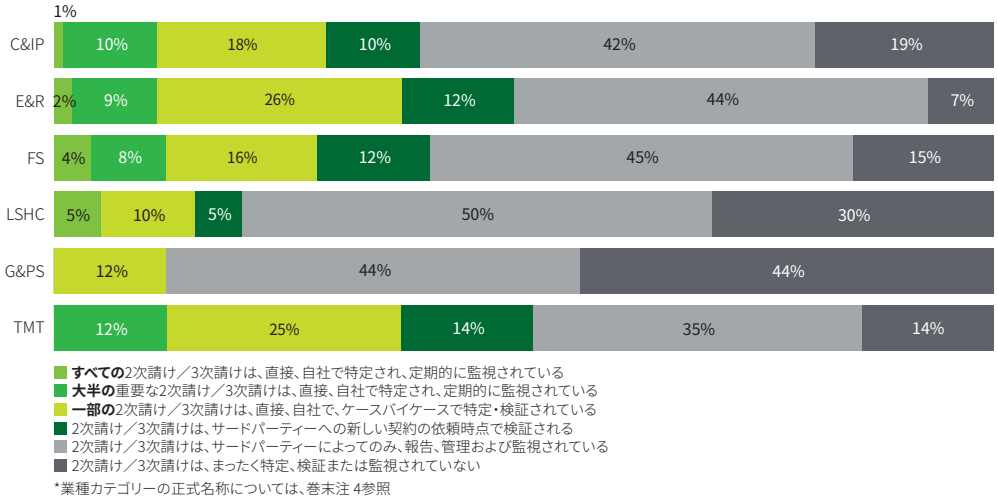
下請業者のリスク特定、審査または監視をしていない回答者は、エネルギー・資源セクターでは7%、金融サービスセクターでは15%のみとなっています。ただし、下請業者のリスク特定、審査・監視をサードパーティーのEERM手続きに依存している回答者の比率は、政府・公共サービスの比率と同様、または非常に似通っています（エネルギー・資源が44%、金融サービスが45%）。

ライフサイエンス・ヘルスケアセクターと政府・公共サービスセクターは、下請業者によるリスクと同等に、関連会社によってもたらされるリスクに対して真剣に取り組んでいるという割合が最も低くなっています。

政府・公共サービスセクターの70%、さらに、ライフサイエンス・ヘルスケアセクターの67%の回答者は、厳格さを減じたアプローチを適用しています。このアプローチは、正式なアセスメントに基づき確認された事実に基づくというよりは、関連会社であれば社外の同業者より信頼できるはずという考えに基づいています。つまり、企業は、自社の関連会社にはレベルを下げたデューデリジェンス、事前スクリーニングおよびモニタリングしか必要ではない、と考えていることになります。

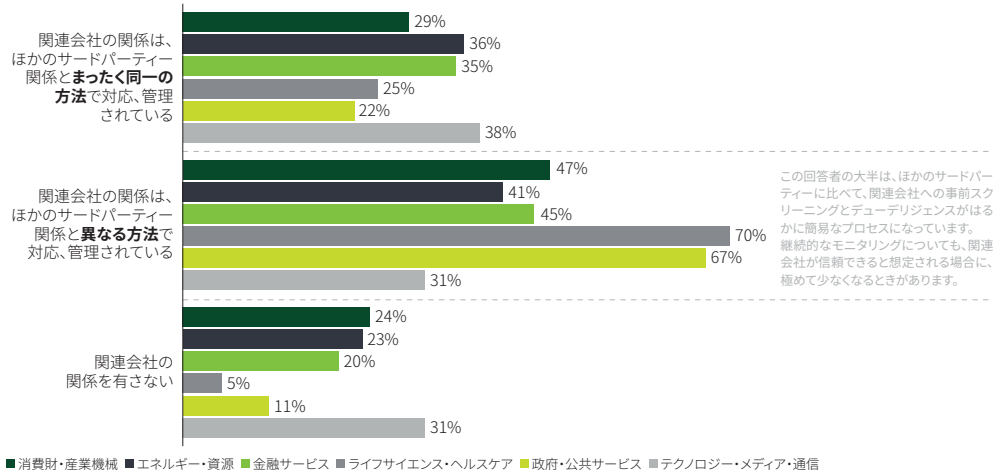
テクノロジー・メディア・通信セクターは、関連会社をほかのサードパーティーと同様に一貫して管理する比率が最も高くなりました。38%がこのアプローチに準拠していると答えています。31%は、重大な関連会社の関係を有さないと述べており、残りの31%の回答者は、簡易なアプローチを選択しています。

図 6.3 サードパーティーの下請業者のモニタリング（業種別）



*業種カテゴリーの正式名称については、巻末注 4参照

図 6.4 関連会社の管理へのアプローチ（業種別）



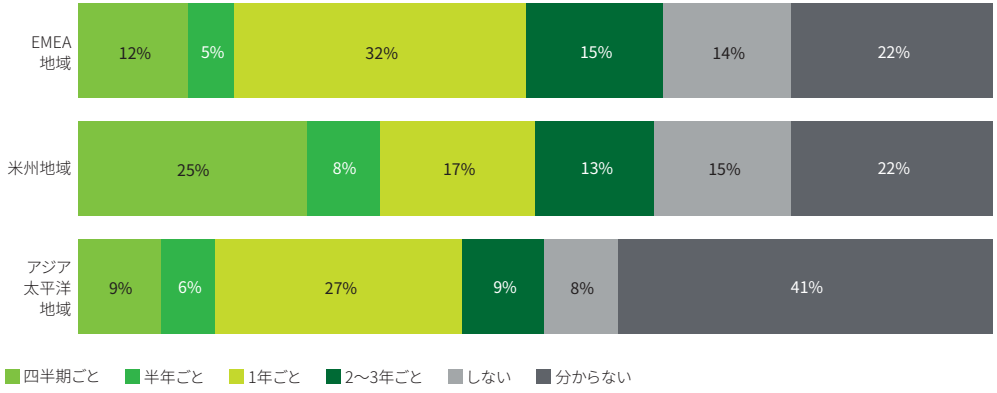
地域別ハイライト

下請業者と関連会社の管理において、世界で大きな差異はありませんでした。ただし、全体として、関連会社の関係を有する米州地域の回答者は、EMEA地域とアジア太平洋地域の80%と比較すると、少なく（67%）なっています。

その一方で、関連会社とその他のサードパーティー関係の複数の層に内在する、集中リスク（単一障害点／単一の地理的地域）のアセスメントについては相違が見られました。

- アジア太平洋地域の41%の企業は、集中リスクの審査方法を把握しておらず、8%は集中リスクをまったく審査していませんでした。
- 米州地域の22%の企業は、集中リスクの審査方法を把握しておらず、15%は集中リスクをまったく審査していませんでした。
- EMEA地域の22%の企業は、集中リスクの審査方法を把握しておらず、14%は集中リスクをまったく審査していませんでした。

図 6.5 拡張エンタープライズの複数層にわたる集中リスクの検証（地域別）



著者紹介

Kristian Park
EMEA Leader, Extended Enterprise Risk Management
Global Leader, Third-party Risk Management
Global Risk Advisory
Deloitte LLP

Kristian ParkはEMEA地域のEERMチームのリーダーであるほか、デロイト グローバルのサードパーティーリスクマネジメント（TPRM）グループのリーダーも務めています。デロイトUKのパートナーとして、クライアントと協力し、プロセスと技術的ソリューションの両面に配慮しながらあらゆる種類のサードパーティーリスクを特定・管理するためのガバナンスのフレームワークを開発し、クライアントに代わってビジネスパートナーであるサードパーティーの検査を行い、サードパーティーが契約条件を順守しているかどうかを評価しています。

また、デロイトUKのソフトウェア資産管理チームおよびソフトウェアライセンシングチームの責任者を務め、クライアントによるソフトウェアライセンス義務の管理を支援し、効率性の改善と経費削減に貢献しています。ライフサイエンス、金融サービス、エネルギーおよび資源、スポーツ、テクノロジー、メディア、消費財および工業製品など、幅広い産業セクターで経験を積んでいます。

Danny Griffiths
Director, Extended Enterprise Risk Management
Deloitte LLP

Danny Griffithsはロンドンを拠点とするEERMチームのディレクターを務めています。クライアントに対し、12年にわたりサードパーティーリスク分野のアシュアランスおよびアドバイザリーサービスを提供してきました。英国EERMチームではサードパーティーアドバイザリー業務のリーダーを務めており、サードパーティーに関するガバナンスおよびリスクマネジメントのフレームワーク開発におけるクライアント支援を専門としています。

また、大規模な国内組織や多国籍組織のコンプライアンスプログラムをリードし、サードパーティーが契約上の義務を順守しているかを評価した豊富な経験を持っています。これまでにサプライヤー、アウトソーサー、マーケティングエージェント、流通業者、再販業者、ライセンシーなど、幅広いサードパーティーに対する検査を指揮してきました。

金融サービス、テクノロジーおよびメディア、コンシューマービジネス、スポーツビジネス、エネルギーおよび公益事業、不動産、公共部門といった幅広い業種での実務経験を有しています。また、EMEA地域、米州およびアジアの複数の地域でプロジェクトを率い、定期的にサードパーティーリスクに関するラウンドテーブルを主催し、フォーラムに出席しています。

Mark Bethell
Partner, Extended Enterprise Risk Management
Deloitte LLP

Mark Bethellは英国EERM部門のパートナーを務めています。FTSEトップ 5 のグローバル企業に4年間勤務した後、2015年にデロイトに復帰。前職では世界的なリスクマネジメントフレームワークの設計と実施を指揮したほか、内部監査リーダーシップチームの一員として、拡大企業（受託業者、サプライヤーおよび非合弁事業）に関するすべての内部監査業務に対する責任を負っていました。

デロイト復帰後は、拡大企業に関連した多くのリスクマネジメントプロジェクトを指揮し、複数の業種のクライアントを支援してきました。サードパーティーリスクマネジメントのフレームワークを設計、構築および実施し、様々な種類のリスクをカバーする大規模な世界的サードパーティー監査プログラムを設計・運営することで、クライアントを支援しています。特にクライアントのためのEERMマネージドサービスや、リスクの自動スクリーニングおよびモニタリングを支援するテクノロジーの継続的な開発を専門としています。

Dr Sanjoy Sen
Head of Research and Eminence
Extended Enterprise Risk Management
Deloitte LLP

Sanjoy Senはデロイトでサードパーティーリスクマネジメントのリサーチアンドエミネンスの責任者を務めています。

英国のアストン大学で、サードパーティーエコシステムに関するグローバルリサーチに基づき、ビジネスアドミニストレーションの博士号を取得しています。また、英国のラフバラー大学のスクール・オブ・ビジネス・アンド・エコノミクスで、戦略およびガバナンスの客員シニアフェローの名誉称号を有しています。2014年以降、世界の様々な学術誌や専門誌、新聞および会議論文で研究が引用されてきました。

取締役会、上層部、リスクマネジメント部門や内部監査部門の責任者に対して、拡大企業、アウトソーシングおよびシェアードサービスに関する戦略的ガバナンスとリスクマネジメントについてのアドバイス提供し続け、幅広い経験を積んできました。英国、ジブラルタル、インドおよび中東の数カ国での勤務経験があります。

公認会計士（FCA）、原価・管理会計士および公認情報システム監査人（CISA）資格の保有者であり、デロイトやほかのビッグ4ファームで17年にわたりパートナーの役職を務めたことを含め、30年以上ものキャリアを有しています。

問い合わせ先

仁木　一彦
有限責任監査法人トーマツ
リスクアドバイザリー事業本部
パートナー
kazuhiko.niki@tohmatsu.co.jp

菊永　ブルース
有限責任監査法人トーマツ
リスクアドバイザリー事業本部
パートナー
bruce.kikunaga@tohmatsu.co.jp

近藤　宏治
有限責任監査法人トーマツ
リスクアドバイザリー事業本部
シニアマネジャー
koji.kondo@tohmatsu.co.jp

中山　崇
有限責任監査法人トーマツ
リスクアドバイザリー事業本部
シニアマネジャー
takashi.nakayama@tohmatsu.co.jp

巻末注

1. 「拡張エンタープライズリスクマネジメント(Extended Enterprise Risk Management)」の語句は、本レポートにおいて、「サードパーティーリスクマネジメント」と同義で使用しています。これは、組織が使用するサードパーティーのエコシステムを表現するために、「拡張エンタープライズ」の用語の使用が増加していることを考慮したものです。

2. データ分析およびレポート作成において、調査票への回答が全回答か一部かを考慮して（これらの回答者によって回答された範囲内で）、考察しています。

3. 場合によっては、2019年の結果をこれまでの年度の調査と比較することが難しくなっています。これは、サードパーティーリスクの理解・成熟レベルが比較的進んでいない地域からの回答者が増加したためです 。

4. 本調査で対象とした業種は、消費財・産業機械（C&IP）、エネルギー・資源（E&R）、金融サービス（FS）、政府・公共サービス（G&PS）、ライフサイエンス・ヘルスケア（LSHC）ならびにテクノロジー・メディア・通信（TMT）です。

5. 投資に関するセクション2に表示されている数値は、回答者によるEERM支出の見積りを集約したものです。一部の回答者は、支出や活動が分権化されているため、組織全体のEERMへの支出金額が大幅に高い可能性があると述べています。

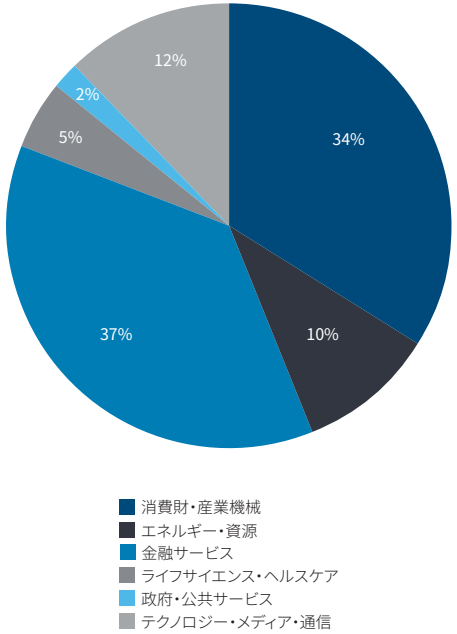
6. 関連会社は、子会社と異なり、中核組織が過半数の持ち分を有していません。統制は、共通の親会社などの間接的手段によって実行されます。調査の対象となった国によっては、「affiliate（関連会社）」という用語が幅広い意味を有する場合があります。これには、例えば、マーケティング契約（例：オンラインリテール販売）によって対象となるサードパーティー、特定の独立請負業者などが含まれる場合があります。

巻末注

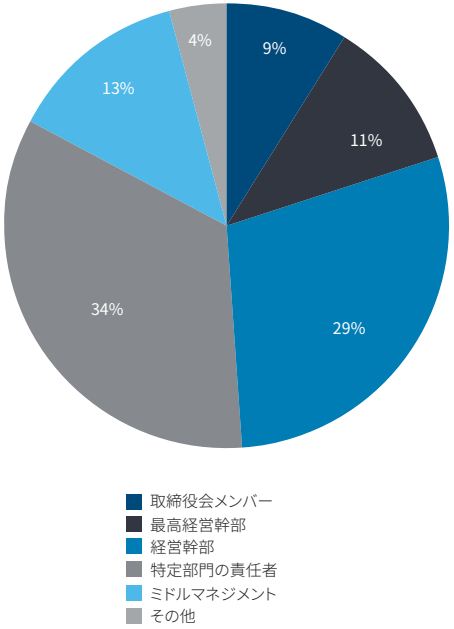
調査回答者プロフィール

今年は、すべての主要業種を網羅する、世界19カ国の参加企業から1,055件の回答を頂きました。回答者は、通常、各組織における拡張エンタープライズのガバナンスおよびリスクマネジメントの責任を負っています。

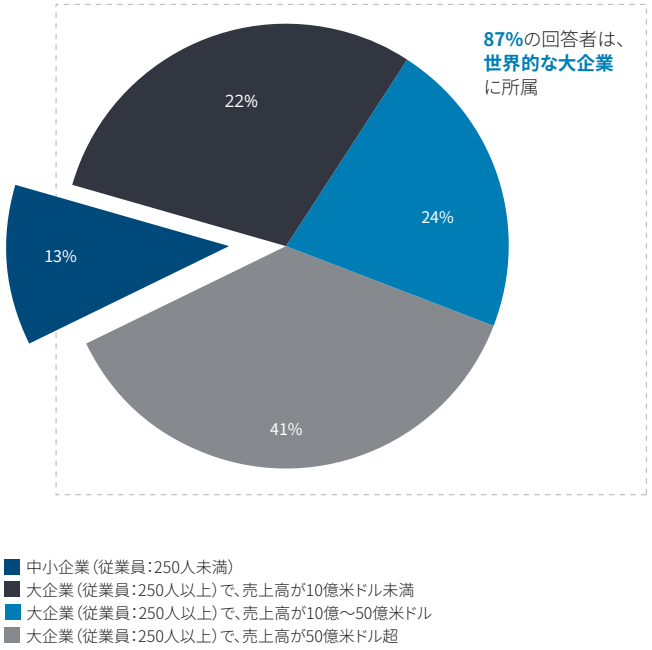
回答者の主要業種



回答者の役職（または最も近い相当する役職）



回答者の規模および売上高



Deloitte.

デロイト トーマツ

bsi. ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

IS 669126 / ISO 27001