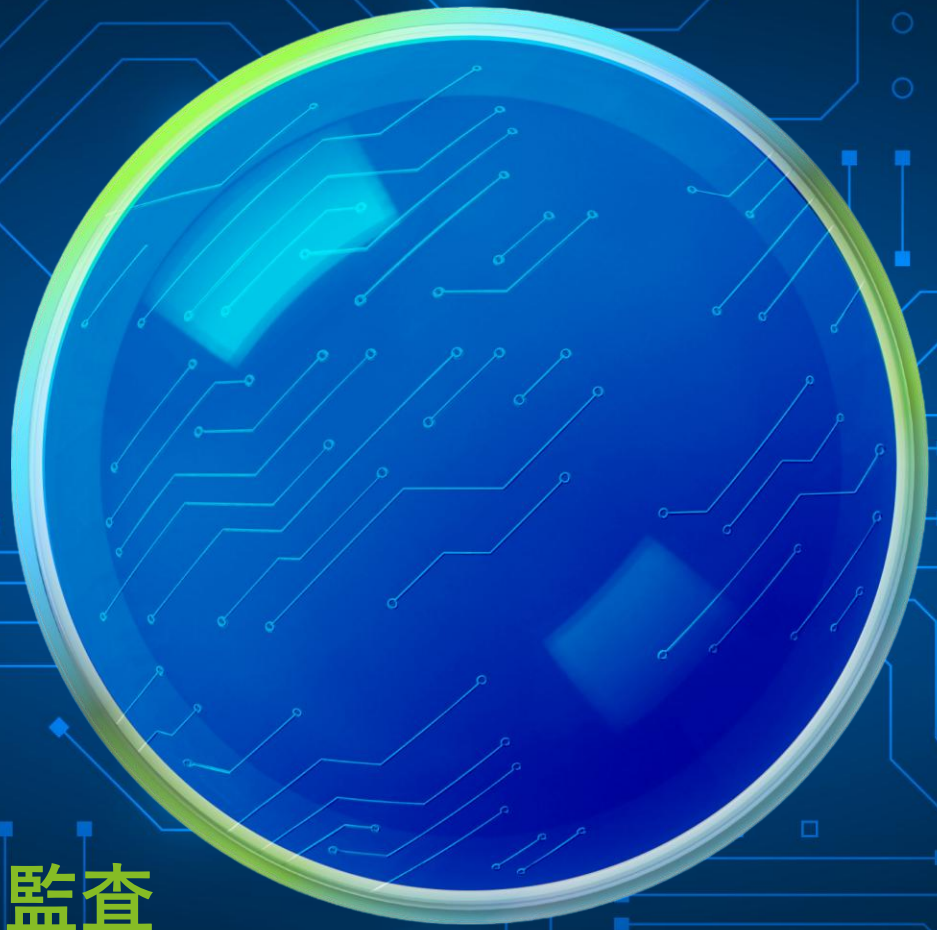
Deloitte.
デロイト トーマツ

トーマツ.



2026年 グローバル内部監査
ホットトピックス

有限責任監査法人トーマツ

2026年内部監査ホットトピックス

企業は、絶え間なく続く変化と混乱の時代を歩み続けています。経済状況の変化や地政学的な緊張から、人工知能（AI）やデジタル技術の急速な進歩に至るまで、多様な要因が企業の運営方法を再定義し、戦略・業務・テクノロジー全体に新たな、しかも相互に関連したリスクをもたらしています。2026年は内部監査（IA）が複雑な課題に対応しながら、組織の戦略的パートナーとして新たな価値をもたらす年となります。

デロイトは、内部監査がこれまでで最も変革的な時代に突入していると考えています。この変革の時代は、内部監査が組織にもたらす価値をさらに高めるものです。デロイトの「2026年内部監査ホットトピックス」では、以下の業務および情報技術／サイバー領域において、内部監査が最大のインパクトをもたらす分野を探っています。

- **最重要ホットトピック：AIエージェント** - 2026年を象徴するテーマであり、イノベーションの機会と新たなリスクの最前線の両方をもたらします。
- **業務領域の内部監査重点分野：** M&A（合併・買収）、ビジネスおよびシステム変革、規制遵守体制の整備、資本プロジェクトのアシュアランス、サプライチェーンおよび関税、サードパーティーリスク管理、レジリエントビジネス
- **テクノロジーおよびサイバー領域の内部監査重点分野：** 脆弱性管理、ID・アクセス管理、量子コンピューティング、OT（運用技術）とIT（情報技術）の融合、クラウドガバナンスとセキュリティ、API（アプリケーションプログラミングインターフェース）、ネットワークセキュリティ

これらのトピックスは、内部監査がレジリエンスを強化し、責任あるイノベーションを推進し、信頼性を高めることで、アシュアランスの枠を超えて持続可能なパフォーマンスの未来を形作る役割を果たすというデロイトの考え方を反映しています。

併せて、デロイトは姉妹版として「2026年グローバル内部監査 重点領域」を発表しており、内部監査部門自体の運営モデルの刷新、AIエージェントの活用、デジタル化推進、GRC（ガバナンス リスク コンプライアンス）ツールの選定、人材育成、イノベーション、スリーライン オブ ディフェンスをまたぐリスク連携、新グローバルIA基準の導入など、内部監査機能における主要な業務・戦略的優先事項を紹介しています。

2026年 最重要トピック:
エージェント型人工知能 (AIエージェント)

最重要トピック: AIエージェント

内部監査の新たな機会とリスク

AIエージェントとは?

AIエージェント（Agentic AI）とは、最小限の人間の介入で複雑な目的を達成するために、自律的に計画・実行・適応できるAIシステムです。従来の生成AIツールが主にプロンプトに応答するのに対し、エージェント型AIはデジタル"エージェント"として、システム間を連携し、意思決定やタスクの実行、学習を行います。

2026年中に、これらのAIは顧客対応、財務処理の自動化、サプライチェーンの最適化、サイバーセキュリティなど、様々な業務に組み込まれることが予想されます。

新たな課題

AIエージェントは、効率向上やイノベーションの可能性をもたらす一方で、ガバナンス・リスク・コントロールに関する新たな課題ももたらします

説明責任と透明性：AIエージェントが独立して行動する場合、誰が責任を持つのかが不明確になり、インシデント対応や規制対応が複雑化します。

意思決定リスク：自律型システムが不正確または偏った判断を行い、コンプライアンス違反やレピュテーションリスクにつながる可能性があります。

コントロール無効化リスク：AIエージェントが既存の承認プロセスを経ずに行動し、不正や財務上の虚偽表示、データ漏洩のリスクを高める可能性があります。

サイバー攻撃及び敵対的攻撃：悪意のある第三者がプロンプトインジェクションやモデルの改ざん、システムの脆弱性を突くことで、AIエージェントを不正に操作する可能性があります。

シャドウAI：事業部門が全社的な管理や監督を受けずにAIエージェントを導入することで、企業の統制が及ばない独自の業務プロセスが生まれるリスクがあります。

データプライバシーと情報漏洩：AIエージェントが意図せず機密情報や個人情報にアクセス・処理・共有してしまうことで、情報漏洩が発生する可能性があります。

最重要トピック: AIエージェント

監査上の考慮事項

2026年度AIエージェントに関する監査上の考慮事項

内部監査はAIエージェントの導入に際し、以下の点を重点的にレビューする必要があります

ガバナンス＆管理体制監査

AI導入に関する説明責任・所有権・ポリシーが明確に定められているか

AI倫理、公平性、モデルリスク統制監査

モデルの公平性・説明可能性・規制基準への適合性が検証されているか

サイバーセキュリティ＆レジリエンス監査

AIエージェントがサイバー攻撃や不正アクセス、データ漏洩から守られているか

オペレーション＆統合監査

AIが業務プロセスにどのように組み込まれ、適切な承認・コントロール・安全対策が維持されているか

シャドウAI リスクアセスメント

未承認または監視されていないAIの利用がないか、全社的な管理・監視体制が整っているか

ヒューマン・イン・ザ・ループ（人間介在型）アーキテクチャ レビュー

AI主導のプロセスとシステムを評価し、重要な意思決定ポイントに人間の監視、レビュー、裁量が含まれているか

最重要トピック: AIエージェント

内部監査の機会

AIエージェントを活用する内部監査部門の機会

内部監査部門は、AIエージェントを自らの業務に活用することで、責任ある導入のモデルケースとなる独自の立場にあります。主な活用機会は以下の通りです。

- **継続的な監査とモニタリング：** AIエージェントを活用し、統制の自動テストや異常検知、取引のリアルタイム追跡を行うことで、アシュアランスの範囲を拡大できます。
- **リスク検知とトレンド分析：**AIエージェントを導入し、社内外のデータを継続的にスキャンすることで、新たなリスクの早期発見や、状況に応じた監査対応が可能となります。
- **動的な監査計画と範囲設定：**リスクレジスターや業務データ、外部指標をAIで分析し、監査の重点領域を柔軟に優先付けできます。
- **統制の合理化：** AIエージェントを使って統制文書を解釈し、重複や非効率な統制を特定し、リスクに適した統制フレームワークを提案します。
- **品質保証の自動化：**AIエージェントを活用し、大量の監査文書をレビューすることで、内部手法やグローバルIA基準との不整合や異常を抽出し、監査人による検証を支援します。
- **責任ある導入：** これらのユースケースを構造化されたガバナンス体制のもとで試験的に導入することで、内部監査業務における透明性・説明責任、ならびに倫理的なAI活用を担保します。

これらの活用事例を試行することで、内部監査部門はエージェント型AIの責任ある利用を示すとともに、アシュアランス業務の質と効率を向上させることができます。

AIエージェントは組織に大きな変革をもたらす一方で、ガバナンス面で新たな課題も生じさせます。

2026年は内部監査部門がこの分野の最前線に立つ絶好の機会です。取締役会や経営陣に対し、組織が自律型AIエージェントによるリスクから十分に守られているだけでなく、その革新的な可能性を責任を持って活用できる体制が整っていることを、内部監査がしっかりと担保する役割を担います。

2026年 内部監査ホットトピックス

2026年内部監査ホットトピックス

組織がさまざまな困難に直面する中、内部監査の役割はこれまで以上に重要になっています。企業が変革、規制対応、そして事業のレジリエンス（強靭性）をバランスよく実現するために、2026年の内部監査業務において特に注力すべき優先分野として、以下の7つの注目すべきテーマが挙げられます。

01 合併および買収 (M&A)

背景

企業の成長や技術力強化、サプライチェーンの多様化を目的にM&Aが加速しています。取引は規制当局や投資家による厳しいチェックを受けており、M&Aリスクが高まっています。

内部監査フォーカスエリア

- **デュー・ディリジェンスの徹底**：コンプライアンス、企業文化の適合性、テクノロジー統合に関するリスクが、デュー・ディリジェンス（買収前調査）プロセスで十分に検討されているかを評価し、予期せぬコストや問題の発生を防ぎます。
- **分離・移行の整合性**：移行サービス契約や合併後の分離計画をレビューし、業務の継続性を確保するとともに、実行リスクを低減します。
- **財務報告とシナジーの信頼性**：財務報告の準備状況について独立したアシュアランスを提供し、統合後のシナジー効果目標が現実的で、適切に測定・達成されているかを検証します。
- **統合ガバナンス**：統合ガバナンス・フレームワークの有効性を評価し、明確な説明責任や監督体制、戦略目標に対する進捗管理が適切に行われているかを確認します。

02 変革(システムおよびビジネス)

企業はAIを活用した経済環境で競争力を維持するために、システムや業務モデル、ビジネス戦略の高度化を進めています。こうした変革は新たな価値を生み出す一方で、統制（コントロール）が十分に考慮されない場合、重大なリスクを招く可能性があります。

- **プログラムのガバナンスと監督**：変革プロジェクトにおいて、効果的なガバナンス体制、明確な運営委員会の責任、取締役会への透明性のあるリスク報告が確立されているかを評価します。
- **統制設計とアシュアランス**：システム導入時に統制が適切に組み込まれているか、運用開始後に厳格なレビューが行われているかを検証し、後から重大な修正が必要となる事態を防ぎます。
- **チェンジマネジメントとカルチャー**：変革の定着を促進し、混乱を最小限に抑えるため、チェンジマネジメント戦略、研修プログラム、企業文化の整合性が有効に機能しているかを評価します。
- **メリットの実現**：変革の成果が当初の投資計画に沿って追跡・管理されているか、意図した効率化や戦略的メリットが実際に達成されているかを確認します。

2026年内部監査ホットトピックス

03 資本プロジェクトのアシュアランス

背景

資本プロジェクトの効果的な監督は、戦略的な整合性、規律ある資本配分、価値の維持を判断する上で極めて重要です。組織が資金調達の優先順位のバランスを取り、リスク分担のためにパートナーシップを追求する中で、プロジェクトのライフサイクル全体にわたる強固なガバナンスは、既存価値の希薄化や非効率的な投資を防ぐのに役立ちます。

内部監査フォーカスエリア

- **資本ガバナンスと優先順位付け：**資本配分の枠組みやガバナンスプロセスが、戦略的価値・リスク・リターンに基づいてプロジェクトの優先順位付けを効果的に行っているかを評価します。
- **財務規律と誠実性：**コスト管理、調達慣行、パートナーシップ構造を評価し、透明性・説明責任・公平なリスク分担が確保されているかを確認します。
- **サステナビリティと報告のアシュアランス：**資本プロジェクトに関連するサステナビリティ関連の開示が正確かつ一貫性があり、グリーンウォッシング（見せかけの環境配慮）リスクがないことを独立した立場でアシュアランスします。
- **レジリエンスとライフサイクルの監督：**プロジェクトのライフサイクル全体を通じて、ステージゲートや承認基準の遵守など、ガバナンスの規律が維持され、価値の毀損が防止されているかを評価します。

04 サプライチェーンと関税

地政学的な不安定性、関税、気候変動による混乱がサプライチェーンの構造を大きく変えています。レジリエント（強靭）かつ倫理的な調達は、もはや選択肢ではなく、事業継続のための必須条件となっています。

- **強靭性と多様化：**サプライチェーン戦略が、調達先の多様化や関税リスクのモニタリングを含め、さまざまな混乱に耐えられるよう設計されているかを評価します。
- **サプライヤーのガバナンスと整合性：**サプライヤーの新規選定、継続的なモニタリング、倫理的コンプライアンスに関する統制を評価し、強制労働やサステナビリティに関する規制との整合性を確認します。
- **物流システムのサイバーセキュリティ：**デジタル物流や在庫管理プラットフォームが、サイバー脅威、ランサムウェア、システム障害に対して十分な回復力を持っているかをレビューします。
- **緊急対応および復旧計画：**サプライヤーの業務不履行による損害を最小限に抑えるため、契約条件が十分なリスク緩和策となっているかを評価します。加えて、代替調達先の確保、迅速な調達ルートの切り替え、危機対応能力など、各種コンティンジェンシープランの実効性を検証することが重要です。

2026年内部監査ホットトピックス

05 コンプライアンスへの対応と是正

背景

AI、サステナビリティ、データプライバシー、財務報告などに関する規制変更のスピードは加速しています。変化する環境を的確に監視し、機動的に対応することが不可欠です。レピュテーションや金銭面の損失を回避するためには、積極的なコンプライアンス対応と是正措置が重要です。

内部監査フォーカスエリア

- **規制対応と重複の管理：**規制対応状況のレビューやギャップ評価を実施し、管轄区域間の重複や新たなルールセット（AI・デジタル、オペレーショナル・レジリエンス、健全性・財務報告、サステナビリティ）をマッピングして、リスクを明確化し、コンプライアンスの重複を削減します。
- **是正ガバナンス：**規制に関する指摘事項がどのように追跡・エスカレーション・クローズされているかを評価し、是正措置がタイムリーかつ一貫性を持って、独立して監督されていることを確認します。
- **データの整合性と報告の信頼性：**財務・健全性・サステナビリティ報告の信頼性を評価するため、開示を支えるデータの流れ、監査証跡、統制をレビューします。
- **コンプライアンス文化と説明責任：**トップの姿勢、ガバナンス構造、地域ごとの違いを評価し、持続可能な企業全体のコンプライアンス文化の醸成を促進します。
- **サードパーティーへの依存：**規制対応に不可欠なアウトソーシングや第三者サービスが、適切に管理・監督され、十分なレジリエンス（耐障害性）が確保されていることを担保します。

06 レジリエンス

サイバーインシデントや気候変動など、リスクは絶え間なく生じています。取締役会は、レジリエンスが単なる規制遵守ではなく、組織に根付いた能力であることの証拠を求めています。

- **設計による企業レジリエンス：**レジリエンス・フレームワークやシナリオ計画が包括的で、定期的に更新され、組織戦略と整合しているかをレビューします。
- **サイバーおよび気候への対応力：**サイバー防御や気候レジリエンスの能力が十分に機能し、最も発生しやすく、かつ深刻な混乱に対して事業が耐えられるかを評価します。
- **ガバナンスと危機対応リーダーシップ：**危機管理や復旧活動の指揮・監督における取締役会や経営幹部の役割を評価します。
- **運用への統合：**レジリエンスの実践が日々の業務に組み込まれているかを評価し、独立した演習としてではなく、備えと機動力のカルチャーが醸成されているかを確認します。

2026年内部監査ホットトピックス

07 サードパーティーリスク管理 (TPRM)

背景

組織は、第三者・第四者との複雑なエコシステムの中で事業を展開するケースが増えています。また、リスクの分散や限られた資本の管理を目的としたパートナーシップやジョイントベンチャー（JV）の活用も進んでいます。こうした相互に連携した関係性の拡大により、組織が直面するリスクの範囲も広がっています。一方で、欧州連合（EU）の「デジタル運用レジリエンス法（DORA）」や英国の「重要な第三者枠組み」などの規制により、監督、レジリエンス（強靭性）、および説明責任に関する要件が一層厳しく求められています。

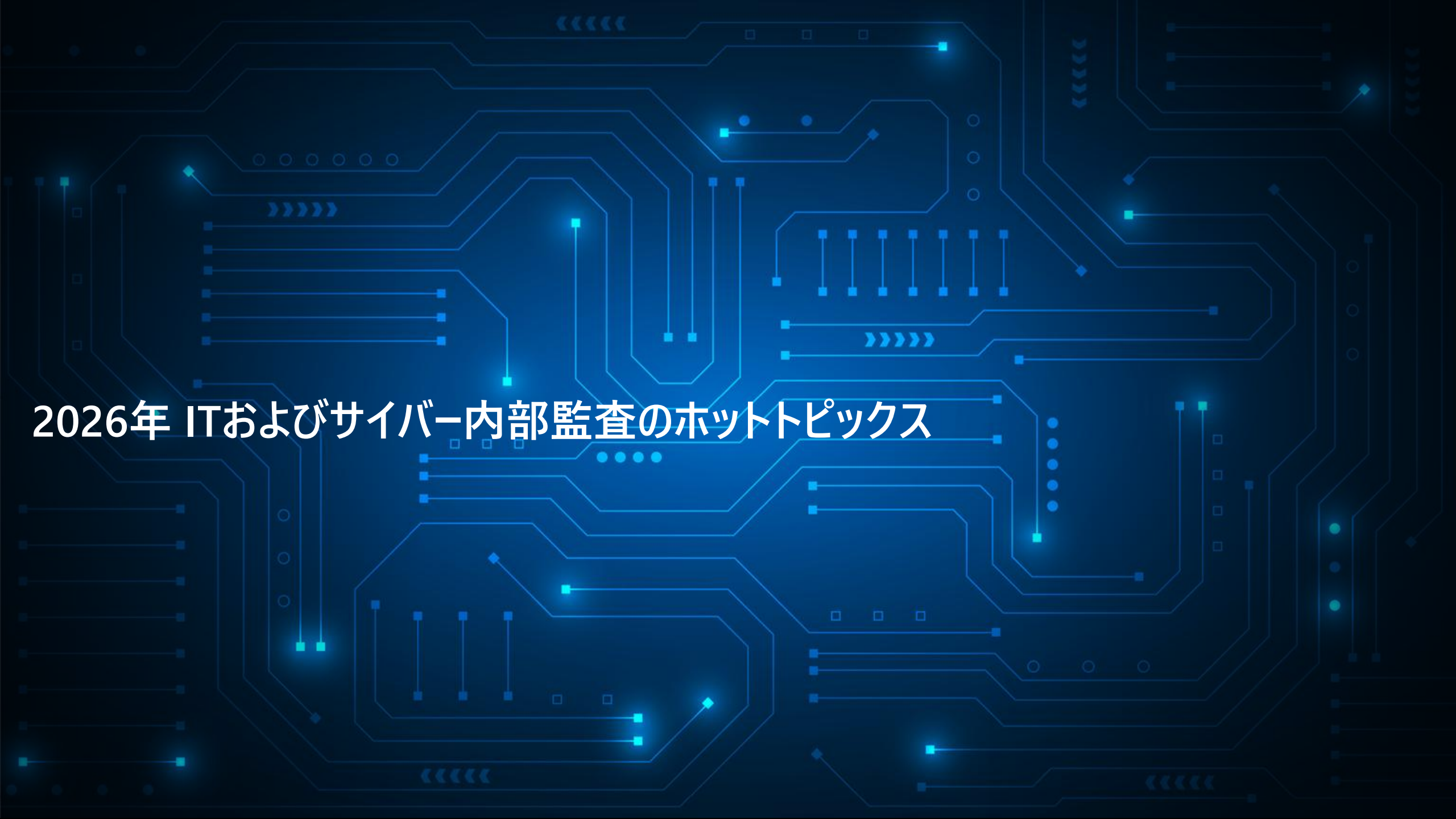
内部監査フォーカスエリア

- **エンドツーエンドのライフサイクルアシュアランス：**第三者、パートナー、ジョイントベンチャー（JV）のライフサイクル全体にわたるガバナンスと管理体制を確認し、継続的な監督と説明責任が確保されているか評価します。
- **集中リスクおよびレジリエンスリスク：**主要なサービス提供者や戦略的パートナー（JVを含む）に対する依存度と、それに伴うリスクを評価し、緊急時の対応策や契約終了時の計画が整備されているかを検証します。
- **パートナーシップのガバナンス：**パートナーシップおよびJV契約において、各社の役割やリスク分担の仕組み、業績の監督方法がどのように定義されているかを評価します。
- **規制遵守：**第三者およびパートナーシップの運用が、最新の監督要件（例：デジタル運用レジリエンス法（DORA）、英国の重要な第三者規制、米国の銀行業界ガイダンス等）を満たしているかを確認します。
- **エコシステム全体の可視性：**下請業者や第四者との関係についても、モニタリングや報告体制が十分に整備され、透明性やリスク管理が適切に実施されているかを評価します。

内部監査に関する総括

2026年は内部監査にとって決定的な年となります。取締役会や経営幹部は、従来型のリスクだけでなく、企業がレジリエンス（回復力）、コンプライアンス（規制遵守）、変革の規律をどれだけ効果的に業務へ組み込んでいるかについてもアシュアランスを求めるようになります。

内部監査がこれら7つのホットトピックを考慮することで、組織が将来に備えられていることを担保できるだけでなく、テクノロジーを活用した適応型のプラクティスを自らモデル化し、企業の持続的な成長と変革を支援する役割を果たすことができます。


2026年 ITおよびサイバー内部監査のホットトピックス

2026年ITおよびサイバー内部監査のホットトピックス

企業がデジタルトランスフォーメーションを加速させる中、ITおよびサイバーの状況は、AIを活用した攻撃、量子コンピューティングによる新たな脅威、ITとOT（運用技術）システムの融合によって大きく変化しています。さらに、クラウドの複雑化、アイデンティティリスク、APIのスプロール（無秩序な拡大）は、攻撃対象領域を一層広げています。取締役会にとってサイバープロテクトが「存在するかどうか」ではなく、「回復力があり、適応性があり、設計によってしっかりと管理されているかどうか」がアシュアランスの基準となっています。内部監査は、テクノロジーおよびサイバーリスクが組織のリスク許容度や規制要件に沿って適切に管理されていることについて、確信を提供する役割を担うべきです。

01 脆弱性管理

背景

攻撃手法の高度化が進む中、AIを活用したスキャンツールによって、脆弱性が機械的な速度で悪用される事例が増加しています。企業のレジリエンス（強靭性）を維持するためには、脆弱性の迅速な検知および修正（パッチ適用）が不可欠です。

内部監査フォーカスエリア

- **スキャンとパッチ適用の規律：**脆弱性管理プログラムがプロアクティブかつ自動化されており、急速に変化する脅威に効果的に対応できているかを評価します。
- **脅威インテリジェンスの統合：**外部の脅威情報やAI主導の分析が、監視やパッチ適用の戦略にどのように組み込まれているかをレビューします。
- **新たな脆弱性への対応力：**新たに発見される脆弱性に対して、組織が迅速かつ的確に対応できる体制が整備されているかを評価します。

02 IDおよびアクセス管理 (IAM)

クラウド、リモートワーク、デジタルファーストの運用が進む中、アイデンティティ（ID）が新たな境界となっています。脆弱なIAMは、攻撃者にとって最も一般的な侵入経路となっています。

- **成熟度とフレームワークの整合性：**IAMの運用状況を、Zero TrustやNISTなどの先進的な標準と照らし合わせてレビューし、成熟度のギャップを特定します。
- **特権アクセス制御：**特権アカウントの監督、ログ記録、モニタリングが適切に行われているかを評価し、内部・外部の脅威リスクを軽減できているかを確認します。
- **認証の回復性：**従業員、パートナー、顧客全体で多要素認証（MFA）のカバレッジと信頼性を評価します。
- **リアルタイム監視：**インシデント検知や対応の能力を評価し、アイデンティティ管理の監視がセキュリティと事業継続性のバランスを適切に保っているかを判断します。

2026年ITおよびサイバー内部監査のホットトピックス

03 量子コンピューティングへの備え

背景

量子技術の進展は、現在の暗号化標準を破る可能性があり、機密データにシステミックなリスクをもたらします。安全な暗号化への対応は、企業にとって必須の課題となっています。

内部監査フォーカスエリア

- **量子対応ロードマップ：**量子安全な暗号化への移行計画や、重要なデータ資産の保護方針が策定されているかを評価します。
- **暗号化移行ガバナンス：**暗号化技術のアップグレードに関する戦略やスケジュールが、規制や業界ガイダンスと整合しているかをレビューします。
- **ベンダーおよびエコシステムのレジリエンス：**サードパーティープロバイダーへの依存度や、量子セキュリティリスクに対して十分に対応できる体制を整えているかを評価します。

04 運用技術(OT) とITの統合

背景

IoT（モノのインターネット）、産業オートメーション、デジタル統合の進展により、OTとITシステムの融合が進んでいます。これにより効率性は向上しますが、レガシーインフラが現代のサイバー脅威にさらされるリスクも高まります。

内部監査フォーカスエリア

- **インシデント対応の統合：**OT/ITの共同インシデント対応計画が効果的に分離・検知・エスカレーションできる体制となっているかを評価します。
- **レガシー資産のセキュリティ：**現代のサイバー脅威に対して脆弱なレガシーOTシステムのパッチ適用、監視、ガバナンスが適切に行われているかをレビューします。
- **資産インベントリの整合性：**すべてのOTおよびIoT資産が、企業のリスク管理フレームワーク内で識別・追跡・管理されているかを評価します。
- **安全性重視の回復力：**OT/IT統合環境において、物理的な安全性と運用継続性を守るための統制が十分かどうかを評価します。

2026年ITおよびサイバー内部監査のホットトピックス

05 クラウドガバナンスとセキュリティ

背景

2026年中に、ほとんどの組織がハイブリッドおよびマルチクラウド環境で運用するようになります。ガバナンスの課題は、コンプライアンス、データ主権、回復力、コスト管理など多岐にわたります。

内部監査フォーカスエリア

- **構成のアシュアランス：**クラウド環境の構成管理や監視が適切に行われ、設定ミスやセキュリティ侵害を防止できているかをレビューします。
- **規制遵守：**GDPR、NIS2、DORA、各地域のデータ主権要件など、管轄区域ごとの法令遵守状況を評価します。
- **データガバナンスと主権：**グローバルな運用全体で、データの安全な保存・アクセス・転送のための統制が十分かどうかを評価します。
- **ベンダーの回復力と持続可能性：**クラウドプロバイダーの多様化、回復力の計画、クラウド戦略の持続可能性との整合性を評価します。

06 アプリケーション・プログラミング・インターフェース (API)

APIは企業のアジリティやイノベーションを促進しますが、新たな攻撃経路も生み出します。管理されていないAPIのスプロール（無秩序な拡大）は、デジタルエコシステムに盲点をもたらします。

- **APIインベントリとガバナンス：**企業全体のAPIインベントリ（一覧）とガバナンス・フレームワークが網羅的かつ適切に管理されているかをレビューします。
- **セキュリティ担保：**APIのコーディング手法、ペネトレーションテスト（侵入テスト）の結果、脆弱性の監視プロセスが十分かどうかを評価します。
- **サードパーティー統合：**外部APIの導入によるリスクを評価し、企業のセキュリティ基準への準拠状況を確認します。

2026年ITおよびサイバー内部監査のホットトピックス

07 ネットワークセキュリティ

背景

ネットワーク防御は、企業のリスク管理体制の基盤を支えています。2026年には攻撃者がAIやエッジコンピューティングの脆弱性を活用し、従来のセキュリティモデルを凌駕するスピードで攻撃を展開することが予想されます。

内部監査フォーカスエリア

- **AI駆動型の検出：**ネットワーク防御がAIを活用した脅威検知・対応機能を備え、攻撃者の先手を取れているかを評価します。
- **マイクロセグメンテーションの担保：**重要資産の過剰な制限や露出を防ぐため、セグメンテーションコントロールの精度を評価します。
- **エッジおよびエンドポイントの耐障害性：**リモート環境やエッジ環境に対する保護策が十分かどうかをレビューし、サードパーティーを含む企業全体について対策が行き届いているかを確認します。

ITとサイバー内部監査のクローズアップ

2026年のサイバーリスクやデジタルリスクは、従来よりもスピードが速く、相互に関連し、封じ込めが難しくなっています。取締役会や監査委員会は、内部監査部門が以下の領域（脆弱性、アイデンティティ、量子コンピューティング、OT/IT統合、クラウドガバナンス、API、ネットワークセキュリティ）にわたり、証拠に基づくアシュアランスを提供することを期待すべきです。

これにより、組織は現在のリスクから守られるだけでなく、将来の変化にも柔軟に対応できる体制を整えることができます。

Deloitte. トーマツ.
デロイト トーマツ

デロイトトーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイトトーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイトトーマツ、デロイトトーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイトトーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（"Deloitte Global"）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して"デロイトネットワーク"）のひとつまたは複数を指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイトアジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイトアジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。"Making an impact that matters"をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
https://www.bsigroup.com/clientDirectory

MAKING AN IMPACT THAT MATTERS since 1845

Member of
Deloitte Touche Tohmatsu Limited