KPMG



サイバーセキュリティ 主要課題 2026

変化の激しい世界における
信頼の構築とイノベーションの実現

目次

はじめに 03

2026年における8つの重要なサイバーセキュリティ主要課題 05

セクター別のインサイト：新たに浮上するサイバーセキュリティの優先事項 06

2026年におけるサイバーセキュリティ戦略 40

KPMGによる支援 41

執筆者 42

謝辞 43



© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

はじめに

組織が成長に向けて変革を進めるなかで、テクノロジーが変化するスピードと激しさは機会とリスクの両方をもたらします。CISO（最高情報セキュリティ責任者）、そしてビジネスの俊敏性とサイバーリスクのバランスを取ることに責任を負う人々は、サイバーセキュリティに直接影響するテクノロジーの進展、地政学的状況、そして進化するコンプライアンス要件に対応しなければなりません。サイバー攻撃対象領域（アタックサーフェス）の拡大に直面しながらも、信頼できるオペレーションとイノベーションを支える必要があります。テクノロジーの遍在化により、CISOの役割はあらゆる業務機能にわたって拡大し続けており、CISOには複数のステークホルダーと協働し、サイバーセキュリティ投資の強い根拠を示すことが求められています。こうした要請は、CISOと企業のリーダー双方にとって、現在のサイバーセキュリティの世界を形作る複数の重要な要因に基づいています。

AIがもたらす機会と脅威

AIは今日の破壊的変化の中心にあり、サイバーセキュリティの専門家にとって諸刃の剣であることが明らかになっています。一方では、防御・保護・対応を担う人々がAIを活用することで、人間だけの場合よりも迅速かつ効率的に脅威を検知し対処できます。他方で、脅威アクターはAIにより強化されることで攻撃を自動化・拡大させるだけでなく、より高度な手法やツールを用いてサイバー防御を突破します。エージェントAIとデジタルエージェントの増殖は、CISOが多数のNHI（非人間アイデンティティ：Non-Human Identity）を保護し、その活動を制御下に置こうとするなかで、デジタルID管理に対する監視をさらに強めています。

規制と主権による複雑性の増大

世界の規制環境がより細分化されるにつれ、CISOとCRO（最高リスク責任者）は、デジタルの安全、主権、レジリエンスに関する要件への準拠に向けた取組みに対する関与を深めています。これらの義務の範囲と複雑性が、データの安全性とプライバシーを守ろうとするサイバーセキュリティチームのリソースと能力に負荷をかけています。

地政学的状況によるサイバーリスクの増大

地政学はサイバーに関する議論において一般的な論点となっており、緊張の高まりにより従来の貿易相手国間の（場合によっては急速な）分断が生じています。組織が事業を行う場所や調達先を見直すなかで、これらの意思決定は国家主体からの脅威を管理し、新たなサプライチェーンへの安全な移行を支えるCISOに連鎖的な影響を及ぼします。

高まり続けるCISOの存在価値と責任

サイバーセキュリティは今や誰もが責任を負うものであり、CISOは継続してリスク認識を高め、責任あるデジタル行動を浸透させ、リーダー、従業員、サプライヤー、パートナーに対して事業影響の観点からサイバーリスクを伝えるべきです。CISOは「徹底した透明性」の原則を採用することで、組織とそのパートナーエコシステムがサイバーセキュリティの重要性を理解し、シグナル（兆候）、リスク、インテリジェンスに基づいた意思決定を支援できます。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

中期的に現実の脅威となる量子

耐量子暗号（PQC）への移行は、非常に重要な変革要件であり、金融や防衛などのセクターにとっては存続にかかわるものです。量子関連のサイバーリスクに今から先手を打って備えることは、レジリエンスを高め、事業継続を支え、規制変更を管理して、組織の将来を守るのに役立ちます。

IT/OTのハイパーコネクティビティへの対応強化

デジタルシステムとフィジカル（物理）システムが融合するにつれ、ハイパーコネクティビティは公益事業、石油・ガス、天然資源、製造、通信などのセクターにおける運用技術（OT）環境を、膨大なIoTデバイスを介した侵害に対してより脆弱にします。データセンターは今や重要インフラとみなされており、膨大な電力需要に対応して発電・公益設備を保護するよう求められています。発電所が新設され、古い設備も再稼働されており、それに伴ってOTセキュリティリスク（特に陳腐化したレガシーテクノロジーに起因するリスク）が増大しています。

差別化要因および事業資産としてのサイバーセキュリティと信頼

テクノロジーは自らのペースで発展し続け、組織はある意味で「飛びながら飛行機を作っている」状態にあります。AIを安全に運用する責任が非常に大きい一方で、AIを最大の強みとして活用し、サイバー防御と生産性を高める大きな機会が生まれています。組織はテクノロジーの採用方法を完全にはコントロールできないかもしれませんが、サイバー機能の支援を得ることで責任ある、かつ信頼性の高い形で採用することが可能です。

サイバーセキュリティは組織全体の優先事項となっており、完全に組み込まれるべきです。特に「KPMGグローバルCEO調査2025」は、サイバーセキュリティとデジタルリスクのレジリエンスを、投資判断に影響する主要なプレッシャーの1つとして挙げています。より安全でレジリエントなオペレーションを構築することで、CISOは継続してステークホルダーの信頼を築き、資本コストを低減させ、新製品開発を可能にし、事業の競争力を維持できます。

本レポートについて

「サイバーセキュリティ主要課題2026」は、20名を超える世界各国のKPMGのサイバーリーダーの知見に加え、Google、Microsoft、Palo Alto Networks、ServiceNowを含むサイバーセキュリティアライアンスパートナーのシニアエグゼクティブの視点を提示します。さらに、KPMGのグローバルおよび地域別調査の結果からもインサイトを得ています。

本レポートは、複数のセクターにまたがる組織において、CISOをはじめとする経営層が取り組むべきテーマとして掲げている重要な8つの主要課題を考察しています。サイバーに関する課題が深刻化するなか、本レポートはサイバーセキュリティの将来の方向性に貢献することを目指し、レジリエンスの強化、組織パフォーマンスの改善、そしてAIの安全かつ効果的な導入の機会を明らかにします。



Laurent Gobbi
Global Cybersecurity and
Tech Risk Centre of Excellence Leader
KPMGインターナショナル
E: lgobbi@kpmg.fr



Jim Wilhelm
Global Cybersecurity Investment Leader
KPMGインターナショナル
E: jameswilhelm@kpmg.com

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2026年における8つの重要なサイバーセキュリティ主要課題

それぞれの主要課題をクリックし、詳細をご覧ください。

01 自律型セキュリティに向けたサイバー人材の準備

セキュリティが自動化されるにつれ、エージェントはセキュリティオペレーションセンター（SOC）における業務に加え、コンプライアンス、リスク管理、アイデンティティ管理においても、より多くのタスクを担うようになっています。自律型セキュリティは、NHIの活動を特定・監視するうえで、重要な役割を果たすと見込まれています。

02 地政学リスクへの対応、レジリエンスとコンプライアンスの構築

デジタル防御とフィジカル資産の双方が、敵対的な国家からの潜在的な攻撃によって脅かされています。組織は潜在的なリスクを評価するとともに、AI、自動化、アナリティクスを活用して統制を効率化し、証跡収集を迅速化し、規制遵守を強化すべきです。

03 AIシステムの保護

AIが組織の業務運営に深く組み込まれるにつれ、そのセキュリティは重要な優先事項として浮上しています。AIの保護はもはや技術的な課題にとどまらず、コンプライアンス、信頼、オペレーショナルレジリエンスと交差する戦略的必須事項となっています。

04 AI時代における非人間アイデンティティ（NHI）の管理

デジタル化と自動化が進む環境では、エージェントAI、サービスアカウント、マシン認証情報といったNHIは、すでに人間のユーザーの数を上回っています。組織は、AIが自ら生み出した複雑性の管理を含め、人間とマシンの双方の主体について、そのライフサイクル全体を含めたアイデンティティガバナンスを再考する必要があります。

05 信頼できるIT/OTハイパーコネクティビティの実現

組込みセンサー、IoTデバイス、完全に接続された環境は、特にインフラ集約型およびサービス主導型のセクターで一般的なものとなっています。ハイパーコネクテッドなシステムを保護するには、動的なメッシュアーキテクチャ、責任所在の明確化、そしてサイバーとフィジカルの境界を越えて監視・対応できる能力が求められます。

06 耐量子暗号への移行

耐量子暗号（PQC）への移行は世界的にますます想定されるようになっており、回避することは難しいと考えられています。世界各国で量子サイバーリスクを管理するため、暗号技術の移行に関する指針や規制が導入されています。これは大きな課題となり、金融や防衛のような分野にとっては存続にかかわる問題となります。

07 検知と対応によるサプライチェーンの保護

今日の複雑なサプライチェーンは、AIや無数のIoTデバイスを含む広大なデジタル攻撃対象領域を生み出しています。組織は継続的な監視と監督を通じてサードパーティリスク管理の範囲を拡張し、オペレーショナルレジリエンスを維持すべきです。

08 CISOの役割と影響力の拡大

セキュリティがビジネスおよびオペレーションにより深く統合され、サイバーとフィジカルの2つの領域が融合するなかで、CISOの職務範囲と責任は引き続き拡大しています。同時に、CISOはAIの大規模導入に伴う機会と脅威を管理しなければなりません。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

セクター別のインサイト：新たに浮上するサイバーセキュリティの優先事項

業界横断で行ったサイバーセキュリティリーダーとの対話から、**サプライチェーンリスク、地政学、NHI管理**が、8つのサイバーセキュリティ主要課題のなかでも最重要テーマとして浮上していることが明らかになりました。
以下の図は、これらの優先事項がセクターごとにどのように現れているか、また経営層がどこに注力しているかを示しています。

ガバメント・パブリックセクター	金融サービス	防衛	エネルギー・天然資源・化学	テクノロジー・メディア・通信	ヘルスケア
• 地政学	• 地政学	• 地政学	• 地政学	• 自律型セキュリティ	• IT/OTハイパーコネクティビティ
• AIシステムの保護	• 自律型セキュリティ	• NHIの管理	• NHIの管理	• NHIの管理	• NHIの管理
• 量子	• サプライチェーンの検知と対応	• サプライチェーンの検知と対応	• サプライチェーンの検知と対応	• サプライチェーンの検知と対応	• サプライチェーンの検知と対応

セクター別の視点と示唆

ガバメント・パブリックセクター：

- PQCへの移行に失敗すると、政府と市民の機微データがリスクにさらされ、デジタル公共サービスへの信頼が損なわれます。ガバメント・パブリックセクターは、レジリエンスと公共の信頼を維持するため、PQC対応アーキテクチャを優先的に整備することが求められます。

金融サービス：

- AI主導による高精度な不正検知を実現する一方、透明性の欠如、データプライバシーリスクの増大、結果の偏りといった課題を抱える可能性があります。組織はセキュリティ・バイ・デザインを組み込み、AIシステムの継続的モニタリングを含むガバナンスと人による監督を強化すべきです。

防衛：

- 政治的分断と継続的なグレーゾーンのサイバー活動により、防衛のサプライチェーンは特にソフトウェア、OT、重要インフラにおいて恒常的な侵害リスクにさらされています。継続的なサプライチェーンの検知と対応は、厳しい状況下でシステムが機能する際のオペレーショナルレジリエンス、即応性、任務の確実性を守るのに役立ちます。

エネルギー・天然資源・化学：

- グローバルに構成要素を含む複雑なサプライチェーンは、特にIT/OTの接点で完全な可視性を妨げる可能性があります。真にレジリエントなエコシステムを構築するため、組織は必要に応じてマネージドサービスを活用し、強固な可視性、標準化フレームワーク、継続的モニタリングを実装すべきです。
- 高度なID中心のセキュリティは、AI主導の運用や相互接続されたOT環境におけるサイバーセキュリティを改善しますが、レガシーシステムや分断された責任体制が実装の障害となる場合があります。

テクノロジー・メディア・通信：

- 通信事業者は、NHIを検証し、機械間音声トラフィックを保護することで、国際的な収益不正を検知するシステムを展開しています。

ヘルスケア：

- AIによる複雑な臨床ワークフローの最適化には、透明性が高く、倫理的かつ安全なエージェントAI開発が必要です。オスロ大学病院におけるAIスケジューリングソリューションが手術の生産性を向上させた事例が示すように、組織はこのような特徴を備えたAIを積極的に導入し、成果の整合性を確保して信頼を構築するべきです。
- 相互接続された医療機器や臨床システムは、攻撃者のラテラルムーブメントの機会を生み、インシデント対応を複雑化させ、停止した場合は患者のケアに影響を与えます。組織は、IT/OTセキュリティを事業目標に整合させ、レジリエンスとクロスドメインのインテリジェンスに注力すべきです。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題1

自律型セキュリティに向けたサイバー人材の準備



> サイバーセキュリティは幾度もの進化を経てきましたが、AI時代の到来により、新たな課題や制約に対処するための機会が無限に広がるもう1つの転換点を迎えています。AIの世界でこの機会を最大化できるサイバー人材を備えることは、決定的な分岐点となります。

Atul Gupta
Global Cyber Technology, Media, and Telecommunications Leader
KPMGインド

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題1

セキュリティが自動化されるにつれ、エージェントは特にセキュリティオペレーションセンター（SOC）において、またコンプライアンス、リスク管理、アイデンティティ管理を含むサイバー領域のほかの分野においても、よりインテリジェンス主導の業務を担うようになっています。こうした状況下でのセキュリティ専門家の役割とは何でしょうか。また、サイバーセキュリティ人材に求められる将来のスキルとは何でしょうか。まずは、エージェントと自動化がサイバー機能をどのように変革しているのかを見ていきます。

エージェントの台頭

エージェントは、SOCアナリストには追いつけない速度でインシデントデスクに届く膨大なアラートをスキャンし、意思決定を行っています。マシン資格情報、サービスアカウント、他のエージェントを作成・削除できるデジタルエージェントなどといったNHIが増大するなかで、自律型セキュリティはそれらの活動を特定し監視するうえで重要な役割を果たすことになります。AIと自動化は、現在主にクラウドで行われているオンボーディングプロセスを加速できます。従来のオンプレミス型データセンターでは、これほど大量のデータ処理は困難です。

自動化は、ワークフローの自動化、リアルタイムサポート、アプリケーションのオンボーディング、パフォーマンス管理といった、他の重要な業務プロセスも支えています。サイバー攻撃者は脆弱性を突くためにハイパースケーラーやSaaSプロバイダーなどのサードパーティを経由して、NHIを通じたマシン認証情報を狙い、悪用するようになっています。これにより、サイバーセキュリティチームには急増するエージェントを特定してアクセス権限を監視し、インベントリに記録するという大きなプレッシャーがかかっています。

データを安全に保存・管理し、AIシステムを規制要件に確実に準拠させるには、AIシステムの実装、さらにはエージェントによる他のエージェントの展開の際に、強固なクラウドおよびデータガバナンスが不可欠です。しかし、多くの組織は単一のハイパースケーラーに依存しているため、サービス停止が発生した場合に脆弱な状態に置かれます。銀行、小売業、通信ネットワーク、政府機関などは、クラウドプロバイダーの一時的な停止によりサービスアカウントID（SAI）がサービスにアクセスできなくなる被害を受けてきました。

テクノロジーによるレジリエンスの構築

CISOは、自律型AIに対してゼロトラストの原則、明確なポリシー、アクセス制御を用いた、動的なリスク管理アプローチを採用しています。セキュリティチームはAIの専門家やデータサイエンスチームと連携し、内部監査や外部規制当局に対してレジリエンスを示すためのセーフガードを構築しています。重要なのはAI技術の利用をリスク限度や管理基準に沿って進めることです。この点についてCISOは、従来の境界防御型セキュリティからゼロトラストセキュリティへの移行過程で培われた知見や対応アプローチを活用することができます。エージェントの台頭によって、3つすべての防衛線において十分なスキルが確保されているか疑問が生じています。従来は内部監査が担ってきた第3の防衛線も、急速なテクノロジー変化に対応するために高度なスキルを必要としています。

> “これは航空機のオートパイロットに例えられます。人間のパイロットに取って代わるものではなく、仕事をより効果的かつ安全にするものです。人間の作業を中心に、多数の自動化ワークフロー、セーフガード、その他の複雑なシステムを組み合わせることで、人間だけでは到達し得ないほど高い有効性を実現できます。”

Chris Corde氏
Head of Product, Security Operations
Google

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題1

新たなエージェントが次々に登場するなかで、CISOはそれらを特定・把握できないことや、どこに脆弱性があるかを判断できないことを懸念しています。

「シャドーエージェント」（自律型または半自律型のエージェントAI）は、SaaSプロバイダーから、さらに自らエージェントを生成する既存エージェントに至るまで、あらゆる場所で出現しています。NHIの管理には、中央集約型のIDストアとポリシーベースのアクセス制御が必要です。CISOはまた、AI主導の新しい世界で生成される膨大なイベント量や強化された脅威アクターの能力に対処するため、SOCに自律型セキュリティアーキテクチャを導入する必要があります。この大きな変革には、AIモデル、データ、インフラの継続的なモニタリングと改善に支えられた、AIセキュリティポスチャ管理（AI SPM）を確立する強固なセーフガードとポリシーが求められます。まだ初期段階ではあるものの、AI SPMはAIセキュリティポリシーに沿って脆弱性や不正アクセスを特定することに焦点を当てています。AIソリューションが普及するにつれ、CISOはAIセキュリティを組み込むため、これらのソリューションに対するレッドチーミングを確立する必要があります。

人間の新たな役割

エージェントがますます自律化するにつれ、組織およびセキュリティ機能は高度な脅威分析、戦略的なサイバー意思決定、AI統合といったより付加価値の高い業務を担えるよう、人材の再教育と再配置を行う必要があります。新たな役割としては、エージェントの活動を監督するエージェントAIマネジャーや、データガバナンスの専門家などが考えられます。これはもはやニッチなテクノロジー課題ではありません。「KPMGグローバルテクノロジーレポート2026」では、テクノロジー分野の上級管理職の92%が、エージェントAIの管理が今後5年間で重要なスキルになると回答しており、自律システムにおける人間の監督、ガバナンス、介入へのより広範なシフトを示しています。Google社のHead of Product, Security OperationsであるChris Corde氏は「エージェント型アプローチがあらゆるワークフローに組み込まれるにつれ、サイバーセキュリティの専門家はエージェント機能を構築し、有効性をテスト・検証し、モデルの追加学習を行う必要があります。これは高度に専門化されたAI主導の専門性であり、ほとんどのセキュリティエンジニアにとってまったく新しい分野でしょう」と述べています。CISOはまた、AIの機能に対する需要を満たすため、内部監査部門で働くエンジニアを惹きつける方法を見つける必要もあるでしょう。

エージェント主導のサイバーセキュリティは、組織のデジタル資産に対する可視性と統制を高める大きな機会をもたらします。強力なセキュリティデータレイクに支えられたこのアプローチは、サイバーセキュリティを手作業から自動化へと移行させ、CISOとそのチームに主導権を取り戻させます。

92%

のテクノロジー分野の上級管理職が、エージェントAIの管理が今後5年間で重要なスキルになると回答

出典：KPMGグローバルテクノロジーレポート2026

> 攻撃対象領域がより多くのエンドポイントに拡大し、保護すべきデータ量が大幅に増加するなかで、AIや自動化を活用して膨大な情報から重要なシグナルを抽出し、対応が必要なセキュリティイベントを優先的にエスカレーションすることが、組織内のすべての部門にとって不可欠になります。

Charlie Jacco
Global Cyber Managed Services Leader
KPMGインターナショナル

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題1

推奨アクション

AIの専門家やデータサイエンスチームと連携し、セーフガードを共同設計するとともに定義済みのリスク限度・管理基準にAIの利用を整合させ、外部規制当局に対してレジリエンスを示します。

AI／エージェントのレッドチーム機能を設置し、AIソリューションとエージェントの挙動を定期的にテストして、その知見を統制改善や保証活動に反映させます。

AIと自動化をSOCにとどめず、オペレーション、第3の防衛線、その他のサイバー領域に拡張し、脅威の監視と対応を強化します。

NHIの課題に先手を打ち、組織全体のIDガバナンスに組み込みます。

より付加価値が高く戦略的な業務に向けて従業員を再教育し、AIに特化した新たな役割を設け、「ヒューマンインザループ（人間による監督・介在）」を強化してAI活動に対する統制を維持します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題2

地政学リスクへの対応、レジリエンスとコンプライアンスの構築



> 地政学的緊張とレジリエンス上の課題を背景に、テクノロジーの観点では標準化と国際協調の10年を終え分散化と主権の新たな時代に入っており、CISOにとっての複雑性は増大しています。

Dani Michaux
Cyber Security Leader, EMA region
KPMGアイルランド

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題2

地政学はサイバーセキュリティに深刻な影響を及ぼしており、デジタル防御と宇宙衛星や海底ケーブルといったフィジカル資産の両方が、敵対的な国家からの潜在的な攻撃にさらされています。国家間の緊張が高まるなか、CISOにはサービスやテクノロジー基盤の強靭性を確保するとともに、そのレジリエンスの不足が企業の競争力にどのような悪影響をもたらす可能性があるのかを評価することが求められています。脅威としては、スパイ活動、知的財産の窃取、バックドア侵入によるシステム停止などが挙げられます。国家と企業の境界が曖昧になるなかで、ハイブリッド型のサイバー攻撃が進化しています。

一部の国では政府が「非友好的」とみなされる国家からの分断を進め、テクノロジーを購入できる国家、またはできない国家を組織に義務付けています。関税はさらなる複雑性をもたらし、特定地域からの輸入価格を押し上げています。グローバル化が後退するなか、企業のリーダーはサプライチェーンのローカライズを進め、新たなパートナーシップやアライアンスを模索しています。

通信、テクノロジー、防衛などの重要インフラ分野の企業は、特に厳格な調達制限の対象となる可能性があります。規制は地域・国ごとに異なり、AIの利用やデータ主権などに関する報告要件の違いがコンプライアンス負担を増大させています。

グローバルからローカルへの転換は、統合・集中化されたシステムを構築してきた多国籍組織に一定の分散化を迫り、コストと複雑性を増大させています。たとえば、単一のグローバル倉庫システム、グローバルなIT／セキュリティサービス、あるいはID管理システムを維持できなくなる可能性があります。CISOはセキュリティサービスおよびツールのアーキテクチャのレジリエンスを高めつつ、グローバルなテクノロジースタック全体の可視性を確保する必要があります。これは、攻撃からの防御、混乱の最小化、そして規制・政府要請への対応に不可欠です。テクノロジーの複雑化、サードパーティエコシステムの拡大、エージェントAIによるNHIの導入により、完全な透明性の確保が大きな課題となっています。

一部の規制はサイバーセキュリティのガバナンスと統制について経営層の責任をより重くし、実質的なリスクを生むとともにレジリエンスを示すことに対するプレッシャーを一層高めています。

新たに浮上するサイバーセキュリティ規制：

- EU NIS2（ネットワークおよび情報セキュリティ指令2）は、重要インフラおよび重要サービスのサイバーレジリエンス向上を目的とし、リスク管理の強化やインシデント報告の迅速化を求めています。
- EU CER（重要エンティティレジリエンス）は、組織に国家戦略、リスク評価、予防および対応を求め、重要インフラのレジリエンス強化を要求します。
- 米国の大統領政策指令21（PPD-21）／ NSM-22（2024年）
- 英国のサイバーセキュリティおよびレジリエンス（ネットワークおよび情報システム）法案
- カナダの重要サイバーシステム保護法（CCSPA）— 法案C-8
- オーストラリアの重要インフラ安全保障法（SOCI法）
- 中国のサイバーセキュリティ法（CSL）およびレジリエンスを重視した2025年改正（2026年1月施行）

重大なデータ侵害や大規模なインシデントが発生、あるいはその疑いが生じた際には、組織のサイバーセキュリティ対策はただちに規制当局の厳しい監督下に置かれます。こうした状況を背景に、AIを活用した継続的な統制の有効性検証や、自動化された報告体制の重要性がますます高まっています。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題2

戦略的必須事項としてのサイバーセキュリティ

地政学とコンプライアンスが、組織にとって主要なリスクになっています。フロントオフィスからバックオフィスに至るまでの製品、サービス、オペレーションの接続が進むなか、組織にはCISOのみが提供できる包括的な監督体制が必要です。サイバーの専門家は、製品チームやテクノロジーの調達・実装に関与し、スピードとイノベーションをセキュリティ、レジリエンス、コンプライアンスと両立させながら、サイバーセキュリティを初期段階から組み込むべきです。規制遵守はCISOにリスク状況の理解と強固なガバナンスの実践を促し、事業継続を支える前向きな力になり得ます。

多くの企業は単一のテクノロジーベンダーに依存しており、そのベンダーが特定の国で制限されると問題が生じます。テクノロジーサプライチェーンには複数の小規模ベンダーが含まれることが多いため、サードパーティリスク管理（TPRM）の複雑性が増し、レジリエンスやコンプライアンスの対象が第4、第5、さらには第6の事業者にまで拡張されます。これらのいずれかでセキュリティ侵害が1件でも発生すると、業務停止や規制上の罰則、評判の毀損につながる、より大規模で体系的な障害につながる可能性があります。

これほど広範な資産（パブリック／プライベートクラウドにまたがるハードウェア、ソフトウェア、データ）に可視性を確保し弱点を見つけ出すことは、非常に大きな課題です。こうしたなか、規制によってデジタルレジリエンスが促進されています。EUのDORA（デジタルオペレーショナルレジリエンス法）は、金融機関に対し、インシデントの管理・報告、レジリエンステストの実施、サードパーティリスクの管理を求めています。また金融サービス分野では、オペレーショナルレジリエンスが重要／中核的な業務サービス（VBS/CBS）と混乱に対する影響許容度の設定に焦点を当てています。CISOの役割は、サプライチェーンリスクの透明性を高め、組織のリスク許容度に基づく意思決定を可能にすることです。CISOは、シナリオ思考によりサイバー脅威下でも経営層が事業を維持し、顧客への影響を最小化できるよう支援できます。

ServiceNow社のChief Information Security OfficerであるBen de Bont氏は次のように述べています。「脅威インテリジェンス、ベンダー管理、サプライチェーン管理、サードパーティからフィフスパーティーに至るリスク管理はサイロ化してはなりません。リアルタイムの脅威情報をベンダー管理プロセスに統合することで継続的なリスクの相関分析が可能となり、外部環境で発生している脅威と組織が依存している取引先との関係を結び付けて把握できるようになります」

> “サプライチェーンは今や攻撃チェーンです。分断が進み、国別に特化しています。その分断はクラウドの相互依存性やAIモデルの調達と相まって、サプライチェーンリスクを地政学的な問題に大きく変えており、それが実際にコードの一行一行を地政学的なものにしていると思われます。”
>
> **Ben de Bont氏**
> Chief Information Security Officer
> ServiceNow

コンプライアンスからレジリエンスへ

サイバーセキュリティおよびレジリエンスの推進者として、CISOはサイバーセキュリティを組織のより広範な目標に統合し、コンプライアンス対応を戦略的なリスク低減と整合させるべきです。そのためには、クラウドベンダー契約、AI導入、新製品開発などの重要なテクノロジーの判断にCISOが関与する必要があります。また、CISOは事業部門およびITのリーダーシップと緊密に連携し、協働的な文化を醸成する必要があります。CISOは、技術的選択肢を測定可能で重要性の高い事業インパクトの観点で捉えることを支援し、リーダーが許容可能なリスク管理基準の範囲に収まる製品・サービス・インフラに投資できるようにします。この複雑性を効率的に管理するため、CISOは関連施策のリスクと影響を定量化すべきです。KPMGの主要なサイバーリスク定量化プラットフォームであるCyber Risk Insights（CRI）は、シナリオを用いてサイバー攻撃の発生可能性と影響を評価します。AI、自動化、アナリティクスは、統制の合理化、証跡収集の迅速化、リスク分析と規制遵守の強化に向けて、負荷の大きい業務の一部を担うことができます。

CISOとそのチームは、組織の継続的なリスクセンサーとして機能し、リーダーが変化を評価し、新たな脅威を理解し、レジリエンスを維持できるよう支援することが重要です。

> “CISOは、テクノロジーのリスクを事業への重要性の高いインパクトとして説明し、サイバーセキュリティとレジリエンスを統合する、信頼されるビジネスアドバイザーになる必要があります。”
>
> **Marko Vogel**
> Head of Cyber Security and Resilience
> KPMGドイツ

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題2

推奨アクション

- 地政学リスクや新たな規制基準をCISOのプログラムに統合し、先見性とレジリエンスを強化します。
- サイバーリスクおよびセキュリティ施策が事業に与える影響を、取締役会および経営層に伝えます。
- 取締役会、IT部門、調達部門、リスク管理部門と連携し、協働的かつ包括的なリスク文化を醸成します。
- データ、サービス、テクノロジーアーキテクチャを能動的に定義・実装し、変化する状況に適応します。
- 組織内部およびサプライチェーン全体のテクノロジー資産に対する可視性を確保し、既存または潜在的な脆弱性を検知・緩和します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題3

AIシステムの保護



“AIはイノベーションを推進する強力な原動力であり、CISOはAI導入を阻止するのではなく、安全に活用できるよう導くべきです。強固なAIガバナンスと先回りしたセキュリティは信頼性と責任あるAI利用の基盤となり、インテリジェンスシステムを脅威に強い安全なビジネス加速装置に変革します。”

Javier Garcia
Global AI Security Leader
KPMGスペイン

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題3

組織は、AI、そしてますます多くのエージェントAIを導入するにあたって、AIシステムに入力されるデータだけでなくエージェントAIそのものの挙動も保護しなければなりません。これは、AIモデルが公平かつ倫理的であることを担保するだけでなく、攻撃力を上げるために革新的なAI活用型の自動化を取り入れる脅威アクターに対しても、十分な堅牢性とレジリエンスを備えることを意味します。AIの利用に関する規制はセクターや地域をまたいで進化しており、CISOはシステムの完全性と信頼性に対する適切なガバナンスを示すよう迫られています。しかしAIシステムは、現在のセキュリティ実務では対応が難しい規模とスピードで動作します。これには、独立して動作する数百あるいは数千のエージェントが統率して実行する自動化サイバー攻撃も含まれます。攻撃者が自動化、AI、エージェントAIで手法を高度化するなか、組織には監視と統制のための新たなアプローチが必要です。

AIの管理

エージェントAIはより大きな権限を得て膨大なデータにアクセスし、協働し、コーディングして、前例のないペースで自律的に行動するようになっています。しかし、エージェントAIはブラックボックスのように振る舞うこともあり、組織は「見えないもの」を信頼しづらくなります。エージェントAIの活動に対する確信を高めるために、CISOは情報源の信頼性、エージェントの権限境界の明確化、データの適切な利用を確保しなければなりません。これは、エージェントが「悪意ある者」に操作または破損されていないことを検証し、過去の意思決定が人間によるものかエージェントAIによるものかを区別することを意味します。

エージェントAIのチェックリスト

- エージェントはどこで稼働しているか
- エージェントのIDは何か
- エージェントは何にアクセスできるか
- エージェントの権限は何か
- エージェントの権限は承認されたユースケースに整合しているか
- 承認されたユースケースの範囲外のアクションを、どのように停止するか

Microsoft社のChief Security AdvisorであるSaira Mohammed氏は次のように述べています。「責任あるエージェントの作成と導入には、明確なポリシーと定義された説明責任が不可欠です。効果的なエージェントAIガバナンスには、正確なスコープ、強固なガードレール、そしてエージェントができること・できないこと、また意図した目的から逸脱した時の対応方法について、責任の所在を明確にすることが重要です。エージェントの乱立と誤用が増えると、セキュリティ運用チームは逸脱が起きた時に適切な措置を判断するため、事業部門と緊密に連携しなければなりません。明確な説明責任がなければ継続的なモニタリング、検知、対応は機能しなくなり、セキュリティチームは十分な情報に基づく意思決定や効果的なリスク低減ができなくなります。これは製造現場において、機械が正常に稼働しなくなった場合に直ちに停止措置を講じるのと同じ考え方です」

一部のエージェントAIはサードパーティのサプライヤーから直接調達されるか、エンタープライズリソースプランニング（ERP）ソフトウェアを含む製品に組み込まれています。これは利用しやすさを高める一方で、新たなリスクももたらします。バイアスやセキュリティ侵害のリスクを低減するため、組織は継続的なレッドチーミングと是正の演習を実施する必要があります。AIが組み込まれた製品は、展開前に安全に設定し、テストする必要があります。AIシステムへの信頼を醸成するため、CISOはサードパーティのAIを把握し、セキュリティ条項および侵害時の説明責任を含む、AI利用に関する正式なサードパーティ契約などを通じてAIガバナンスを適用する必要があります。

> 「AIセキュリティには、非常に大きなリスクと影響が伴います。セキュリティを一から作り直す必要はありませんが、AIがもたらす前例のない規模とスピードに対する新しいアプローチが求められます。それはすなわち、セキュリティ・バイ・デザインを組み込み、プロセス全体で自動化されたAIを活用することです。」
>
> **Kristy Hornland**
> Director, Cyber Threat Management
> KPMG米国

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題3

Microsoft社のSaira Mohammed氏は、「開発者は、AIソリューションが本番環境に到達するはるか前の段階から、セキュリティを組み込まなければなりません」と述べています。「デジタル資産全体で真の可視性を実現するには、セキュリティ・バイ・デザインとセキュアデフォルトに根差した、プラットフォーム中心のモデルが必要です。またこれは、サードパーティのAPI（アプリケーションプログラミングインターフェース）とシームレスに接続でき、組込みのセキュリティを備えた、オープンで統合されたプラットフォームスタックを採用することで、セキュリティチームが運用アプローチを近代化する機会でもあります」

組織が数百、さらには数千のエージェントを利用する場合、それらの行動の検知・観測やアクセス権の確認を、手作業のプロセスに完全に依存することはできません。AIは、セキュリティ運用の自動化、膨大なデータとテレメトリの処理、パターンや異常の分析を支援することで、「予測的シールド」の一形態として攻撃を予測し、未然に防ぐことに役立ちます。

The Open Web Application Security Project（OWASP）のAgent Observability Standard（AOS）[1]は、エージェントAIの透明性を高めることを目的としています。これはエージェントが「計測・制御可能、追跡可能、検査可能」であることを求め、実行できることとできないことに対する強固な統制、あらゆる行動をその背後にある推論と起点となったタスクにまで遡って追跡できる能力、そして利用しているツール、モデル、機能を明示できることを要件としています。このアプローチの一部には、データがAIモデルに入力・処理される前にデータをフィルタリングする一種の「ファイアウォール」を設け、セキュリティ・バイ・デザインをプロセスに組み込んだAIシステムを開発することが含まれます。エージェントAIセキュリティの次の段階は、Gartner社が「guardian agents[2]」と呼ぶ、エージェントを継続的にモニタリングして不審な挙動を検知し、インシデントを報告する仕組みです。

責任あるガバナンスによるAIへの信頼構築

AIへの多大な投資を踏まえると、組織が従業員に対してこのテクノロジーを安全かつ日常的に活用することを求めるのは当然です。それを可能とするには、モデルが信頼できるデータで学習されていることへの確信とともに、学習プロセスとデータが可視化されていることが不可欠です。KPMGとUniversity of Melbourneが実施した、47ヵ国の約5万人を対象とする最新のグローバル調査では、半数超の54%がAIの信頼性に懐疑的だと回答しています。

CISOの重要な役割の1つはAIの価値提案を伝えることですが、同時に規制上の罰則リスクについても周知する必要があります。エージェントのプロセス、あるいはAIシステム全体が信頼に欠ける、あるいは規制要件を満たさないと判断された場合には、組織はそれらを停止せざるを得ない可能性があります。事業継続および災害復旧計画に責任を持つ立場であるCISOは、業務中断を回避し、システムへの信頼を維持するうえできわめて重要な役割を担っています。AIセキュリティの重要性を取締役会に伝えるには、CISOは侵害やモデルのバイアスが事業に及ぼし得る影響を示し、セキュリティを運用継続性とレジリエンスを支える重要な要素として位置付けることで、リスクの観点から説明する必要があります。

> “AIは、データを分析し、見落とし得る攻撃を検知し、SOCチームを24時間体制で支援することで、セキュリティ運用を効率化します。AIはデータに基づいて推論し分解して再構成することで、見逃していた攻撃などの事象を含め、全体像を把握できます。つまり、SOCに24時間365日（多くの場合は自律的に）稼働する信頼できる助手がいることで、人間のオペレーターは徹底した調査と緩和策の実施に集中できます。”
>
> **Saira Mohammed氏**
> Chief Security Advisor
> Microsoft

1 The Open Web Application Security Project (OWASP)、OWASP Agent Observability Standard、2025年

2 Gartner、「CIOs, Leverage Guardian Agents for Trustworthy and Secure AI」、webinar、2025年5月19日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題3

CISOが主導し、データセキュリティ、テクノロジー、リスク、法務、プライバシーの各分野の幹部で構成されるAIガバナンス委員会は、AI導入のためのフレームワークと原則を確立できます。「KPMG Trusted AI」フレームワークは、AI技術の責任ある倫理的な設計、開発、調達、利用に向けた統合的アプローチを提供します。優先事項はデータおよびAIのアーキテクチャとインフラの保護であり、反復的かつ自動化されたテスト、特にレッドチーミングを重視します。これらの取組みは、セキュリティ運用（SecOps）と併せてセキュリティチームとIT運用チームの統合を促し、協働の促進、脅威検知、対応の迅速化に寄与します。人による監督は安全なAI利用の中核であり、モデルの出力結果や推奨事項を検証し、データ精度を高めて介入を可能にします。

AIガバナンスに向けた必須ステップ

- エージェントの初期導入段階からセキュリティ人材を関与させ、業務プロセスへの理解を深める。
- エージェントを検知・把握するツールにより、インベントリ管理を実施する（APIファーストの機能を活用）。
- 実行時の可観測性を確保する：操作制御（動作を制御するため）、追跡（活動履歴を記録するため）、検査（使用ツール／モデルを特定するため）。

テクノロジーと人の融合

テクノロジー業界全体で、レッドチーミングの自動化や機微情報のマスキングによりAIシステムを保護するガードレールに特化したスタートアップが台頭しています。主要なセキュリティベンダーがこれらのスタートアップを買収することで、CISOには既存のテクノロジースタックに高度なAIセキュリティを統合する機会が生まれています。

AIセキュリティを管理する人材の確保は、非常に大きな課題です。データサイエンスのバックグラウンドを持ち、AIシステムやエージェント型ワークフローの脅威モデリングに精通した高度な専門知識を持つセキュリティエンジニアは、きわめて稀です。

採用に加え、一部の組織は大学と連携し、既存社員に対してサイバー分野向けの特定のAI技術のトレーニングを実施しています。脅威モデリングやセキュリティ・バイ・デザインの経験を持つ社員は、スキル向上の有力な対象です。AI保護を担う専任の役割を設ける組織もあれば、セキュリティチームにOWASPや情報共有ネットワークと連携して新たなリスクを理解する役割を担わせる組織もあります。また、AIセキュリティをマネージドサービスとしてサードパーティに委託する選択肢もあります。

採用、トレーニング、戦略的パートナーシップは出発点にすぎません。真の競争優位性は、イノベーションのスピードに合わせてAIを安全に運用できるよう従業員を支援することから生まれます。

テクノロジーの進化自体は目新しいものではありませんが、変化のスピードこそがこの局面を特異なものにしており、組織には迅速なAI導入以外の選択肢がほとんどありません。脅威アクターがAIによって強化されるなか、セキュリティチームはAIを用いた早期検知、権限・アクセス管理、エージェントAI利用に対する厳格なガバナンスを行うよう、革新を迫られています。AIと協働するためのスキルと知識を従業員に提供することで、CISOはAIとデータへの信頼を強化できます。

> “もし私がセキュリティエンジニアであれば、組織内のツール上に構築するあらゆるワークフローにエージェント型アプローチをどのように組み込むかを真剣に考える必要があります。さらに、エージェント機能をどう構築するかだけでなく、有効性をどのようにテスト・検証し、モデルの追加学習を行って機能させるかも考えなければなりません。”
>
> **Chris Corde氏**
> Head of Product, Security Operations
> Google

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題3

推奨アクション

AI導入を監督し、ポリシーと統制を定める部門横断のガバナンス委員会を設置します。

人を置き換えるのではなく補完する形でAIを活用し、特に高リスクまたは重要領域で、モデルと結果に対する強力な監督のもとにヒューマンインザループを維持します。

AIシステム開発全体にセキュリティ・バイ・デザインを組み込み、エージェント展開やワークフロー設計の初期段階からセキュリティを統合します。

レッドチーミング演習を含め、AIシステムを継続的に監視します。

高リスクかつ成熟度の低いサプライヤーを優先対象として、サードパーティリスク管理を強化します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題4

AI時代における非人間アイデンティティティ（NHI）の管理



> 将来のIDおよびアクセス管理（IAM）は、静的な統制を超え、リアルタイムの意思決定と自動化されたポリシーオーケストレーションによって、人間IDとNHI双方の拡大する規模を適切に統治・管理する、知的で適応性に優れたエコシステムに進化しなければなりません。

Juan Manuel Zarzuelo Diaz
Global Digital Identity Leader
KPMGスペイン

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題4

サービスアカウント、ワークロード、エージェントAIなどのNHIが急増し、すでに人間ユーザーの数を上回っています[3]。これらのIDは、OT、オンプレミス、クラウド、ハイブリッド環境、さらにはシャドーAI領域に分散して存在し、過剰な権限を持つことも多いため、把握がますます困難になっています。なかには他のNHIによって生成されたものもあります。従来型の「静的」なIDおよびアクセス管理（IAM）だけではセキュリティを確保できず、組織には一時的・動的・自律的なシステムに適応できるAI主導のガバナンスと統制が必要です。

59%

の企業が、過去12ヵ月間にサードパーティ起因のデータ侵害を経験している

出典：Reducing Non-Employee Access Risks for Franchisors with SailPoint NERM

見えないところで何が起きているのか？

CISOにとって、ID管理の対象はもはや人間だけではなくなっています。従来のマシンIDとは異なり、エージェントAIは広範かつ変化する権限を持ち、文脈やプロンプトに基づいて複雑なタスクを実行し、意思決定を行います。スクリプトやロボティックプロセスオートメーション（RPA）とは異なり、エージェントAIは予測可能なパターンでは動作せず、人間のようにアクセスを開始してコードを作成・使用し、新たな仮想テクノロジーインフラを構築します。そして、24時間365日稼働し続けるのです。特定のタスクのために他のエージェントを生成し、すぐに削除するものもあり、その痕跡がほとんど、あるいはまったく残らない場合もあります。

このように一過性かつ自律的な性質を持つIDについて、CISOはどのように追跡して挙動を監査し、それらの利用に対する確信を高め、組織、従業員、顧客、その他ステークホルダーの最善の利益に沿ってそれらが機能していることを確認できるのでしょうか。従来のIAM統制は、検証されたIDに基づく認可と、潜在的な違反を検知するための定期的な追跡によって、「適切な人が、適切な時に、適切なリソースへ、適切なレベルでアクセスする」ことを確保するポリシーの確立を目的としています。しかし多くの場合、組織は非人間エージェントの明確なインベントリを持っておらず、人間ID、マシンID、エージェントAIを容易に区別できていません。人間は、NHIが生成され、動作し、消去されるスピードについていくことができません。NHIはそれぞれ固有のIDを持ち、それぞれ重要な役割を担っています。

KPMGのインサイト「見えないアクセス、見えるリスク」では、NHIの侵害がすでに重大なセキュリティ侵害事案で顕著に見られること、さらに自立的に高速で動作するエージェントAIが人手を介さずに資格情報を作成・変更・使用することで、問題が増幅されていることが指摘されています。

61%

の米国企業は、自律型エージェントにまだ不安を感じており、ヒューマンインザループによる監督を必要としている

出典：KPMG AI Quarterly Pulse Survey: Q3 2025

NHIを把握・管理する

IDは、SaaS、インフラ、プラットフォームアズアサービス（PaaS）全体に共通するセキュリティの基盤となっています。統制を取り戻すための第一歩は、エージェントがどこに存在し、何をしているのかを把握することです。中央集約型のIDストアを確立することで、CISOとそのチームはエージェントAIをタグ付けして追跡し、IDプロバイダー内で認識・管理し、継続的に更新されるインベントリに記録することができます。自動化されたAIの規模を考えると、従来の手作業による承認プロセスでは対応できません。特にエージェントは非決定的で、同じ作業を異なる方法と実行内容で完了することがあり、そのたびに異なる権限が必要になるためです。組織はポリシーベースのアクセス制御を実装することでリアルタイム監視が可能となり、エージェントの権限の制限や停止により不適切または不正確なデータ利用などの不正行為を防止できます。統制は脅威検知を迅速化し、不審な挙動を検知した場合にはIDを即座に停止できるものであるべきです。「キルスイッチ」を押すということは、エージェント全体ではなく、個々のエージェントを停止することを意味します。

統制は、ID、ネットワーク、デバイスの各レイヤーにわたり、「人間であれ非人間であれ、いかなるIDも信頼しない」というゼロトラストの原則に基づくべきです。その他の統制機能には、適応型アクセス、ジャストインタイム権限、最小権限アクセス、そして不正なソースコードアップロードを検知するためのデータフローの継続的モニタリングが含まれます。ハイパースケーラーはゼロトラスト機能に投資し、顧客がプラットフォームをどのように利用し、どの程度の頻度で権限を要求しているかに関する情報を収集しています。こうした支援により、CISOはポリシーを適切に施行するための貴重なインサイトを得ることができます。

エージェントはクラウド上のAPIやトークンで構成されるワークロードのように動作するため、ホワイトリスト化、フィルタリング、ポリシー施行といった既存のクラウドネイティブ機構の活用が必要になります。CISOは、AIの利点を享受しながら組織の安全を維持するという難しい問題に直面しています。SPIFFE、SPIRE、権限委任のためのOAuthなどのオープンソースのフレームワークや標準技術は、安全なエージェント運用を実現するうえで重要な役割を果たすことが見込まれています。

3 CyberArk、「Machine Identities Outnumber Humans by More Than 80 to 1」、press release、2025年4月23日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題4

> 将来のIAMは、実行時の強制、動的なポリシーオーケストレーション、そして複数プラットフォームにまたがるデータを集約するIDファブリックを統合する可能性が高いでしょう。

Hemal Shah
Principal, Advisory, Cyber Security Services
KPMG米国

NHIの効果的な管理は、X.509であれJWTであれ、デジタル証明書の安全な発行、ローテーション、失効にますます依存するようになっています。これらの資格情報は、一時的なワークロード、API、マシン間相互作用の認証および信頼モデルを支えています。組織がマイクロサービス、サーバーレス、コンテナオーケストレーションプラットフォームなどの高度に動的なアーキテクチャを採用するにつれ、短命なIDの量と生成速度は劇的に増加します。この変化により、強固な証明書ライフサイクル管理（CLM）は、セキュリティ上の必須事項であるだけでなく、運用上の必要事項にもなります。CLMは、侵害された、または期限切れの資格情報に起因するリスクを最小化しつつ、自動化システムが継続的な信頼を維持できるようにします。

IDガバナンスの強化

監査人からの情報要求に応えるため、IDガバナンスにはプロセスを加速する自動応答機能を含めるべきです。こうした機能はリアルタイムログ、SIM（加入者識別モジュール）／SOAR（セキュリティのオーケストレーションと自動化によるレスポンス）データ、および行動分析を用い、管理者がNHIについて十分な情報に基づくアクセス判断を行えるようにします。AIは、アプリケーションのオンボーディング、権限のレビュー、認証取得といった労働集約的プロセスの自動化を加速できます。認証取得は、誰が何にアクセスできるかを確認するため、あらゆる監査の重要な要素です。

自動化の重要性にもかかわらず、人による監督はポリシーの定義、リスクの優先順位付け、ガバナンスフレームワークにおいて引き続き不可欠です。AIは戦略的な意思決定に取って代わるのではなく、それを補完すべきです。IDセキュリティプラットフォームは、ハイブリッドおよびマルチクラウド環境にまたがって、人間IDとマシンIDを保護するためにAIを採用しています。それらは、監査とセキュリティの両面から組織全体のどこにリスクがあるかを示す中央集約型ダッシュボードに、ID分析を投入できます。

これらの機能に加え、組織は現在、ID脅威の検知と対応（ITDR）を採用し、異常な挙動を能動的に特定してID中心の攻撃が深刻化する前に封じ込めています。ITDRを補完するIDセキュリティポスチャ管理（ISPM）は、IDシステム全体にわたって構成ドリフト、統制のギャップ、ポリシーの不整合を継続的に評価し、セキュリティチームが一貫したコンプライアンス基準（ベースライン）を維持できるよう支援します。さらに戦略的なレベルでは、ID可視化およびインテリジェンスプラットフォーム（IVIP）を組み込んだプラットフォームが、IDガバナンス自動化（IGA）、アクセス管理（AM）、特権アクセス管理（PAM）、およびクラウドIDインフラからのテレメトリを統合し、中央集約されたAI主導のインサイトを生成します。

セキュリティ文化の中心にあるのは人

より広範なセキュリティ文化を醸成する際には、組織が人間IDをどのように保護しているかを示すことが重要です。そうすることで、人々は不正アクセスやなりすましのリスクと強固な統制の重要性を理解でき、そこからマシンIDやエージェントの挙動を評価することに進むのは自然な流れといえます。AI導入パターンについてトップダウンのモデルを策定することで、CISOは権限と影響に基づいてIDリスクの優先順位を付けられます。最大の懸念事項は、広範な権限を持つ高リスクのエージェントAIと、重要インフラに紐づくマシンIDです。

セキュリティはサイロ化した形で取り組むべきではなく、CISOは包括的なIDガバナンスを統合する、より広範で信頼できるAI機能フレームワークを推進する必要があります。そのためには、CROや最高データ責任者（CDO）、データプライバシー責任者（DPO）、ならびに法務を含む組織内の各部門を巻き込む必要があります。CISOはまた、潜在的リスクと便益を定量化することでAIセキュリティ投資の必要性を正当化し、取締役会および経営層からの資金と支援を確保できます。規模の拡大によって管理不能になる前に、AI／エージェントAIにセキュリティ・バイ・デザインを組み込める期間はわずかです。すべてをセキュリティの観点から設計することで、組織はリスクを管理しながらAIの便益を享受できます。

> ワークロード、デバイス、エージェントAIをはじめとしたNHIは急速に増加しています。私たちは、人間に対して用いるのと同じ規律と原則をそれらに適用しなければなりません。すなわち、強固な認証、明確な認可、そして責任の所在の明確化です。エージェントを単に停止するだけでは説明責任を果たしたことになりません。人が責任を持たないマシンIDは、管理不能なリスクとなります。

Sitaram Iyer氏
Area VP Emerging Technologies
Palo Alto Networks

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題4

推奨アクション

中央集約型のIDストアを確立するとともにエージェントAIをタグ付けして追跡し、可視性と統制を維持します。

ポリシーベースのアクセス制御、分散型ID管理、継続的モニタリングを用いて、ゼロトラストの原則を適用します。

セキュリティ施策を事業目標に整合させることで、セキュリティと事業ニーズのバランスを取ります。

AIがIDガバナンスを主導するようになっている一方で、戦略的な統制を維持するため、人による監督を引き続き優先事項とします。

セキュリティ、リスク、プライバシー、法務、事業部門の各チーム間の連携を強化し、IDをより広範で信頼できるAIフレームワークの一部として位置付けます。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題5

信頼できるIT/OTハイパーコネクティビティの実現

“ITとOTの融合は、もはやそれだけにとどまりません。新たな柱としてのAIが加わり、適切に管理された運用能力のもとでの導入が求められています。すなわち、AIリスクの深い理解、慎重な評価、そして安全性と監督機能を組み込んだ動的なメッシュアーキテクチャの設計が必要です。そうして初めて、AIは可用性、安全性、継続性を損なうことなく運用の信頼性を高めることができます。常に念頭に置くべきは、OTのゼロトラスト、データ主権、ローカライゼーション、そして文化です。”

Hossain Alshedoki
Global Internet of Things and Operational Technology Security Lead
KPMGサウジアラビア



© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題5

IT、OT、スマート接続システム、サプライヤー、顧客の融合は、サイバーリスクの状況を再形成します。デジタルツイン、ロボティクスを含む組込み型のIoTセンサー、AI主導の環境は、特にエネルギーや製造といったインフラ集約型セクターで一般化しつつあります。この相互接続性は新たな脆弱性を生み、フィジカル領域とデジタル領域にまたがる潜在的な攻撃対象領域を拡大します。たとえばIoTの増加は、悪意ある者にデータ窃取、ITシステム侵害、デバイスへのランサムウェア感染、分散型サービス拒否（DDoS）攻撃の機会を与えます。

産業および重要インフラを含む統合IT/OT環境で事業を行う組織は、プロセスの合理化やITセキュリティの機能をOT環境へ（またはその逆へ）拡張することで、セキュリティの有効性と効率性を高めようとしています。こうした組織は、AIをはじめとする先進テクノロジーをOT領域に導入することに強い関心を示しているものの、多くのアーキテクチャは硬直的な設計原則に依存しているため、CISO／CTO（最高技術責任者）／COO（最高執行責任者）により制限されています。

ITとOTを分離する従来のPurdueモデル[4]（他の静的モデルを含む）は、多くの業界フレームワークに適用されてきました。しかし、柔軟性、リアルタイムのデータ分析、ゼロトラストの原則や相互運用性への対応を欠くため、現代の産業ネットワークには適さなくなりつつあります。これは、サイバー攻撃者に悪用され得る死角を生みます。

重要インフラに対するサイバー攻撃の影響は、組織、従業員、さらには社会全体にとって壊滅的になり得ます。リスクには、身体的被害、環境破壊、サプライチェーンや重要サービスの重大な混乱が含まれます。

規制当局はこれらのリスクに強い懸念を抱き、組織のレジリエンスに一層の注意を払っており、その結果コンプライアンス負担は増大しています。KPMGのインサイト「Critical Entities Resili-ence (CER) Directive」では、エネルギー、輸送、医療、銀行など11の主要セクターにわたり、重要サービスのフィジカルセキュリティとオペレーショナルレジリエンスを強化することを目的としたEUの新規制について論じています。デジタル資産に焦点を当てるEU NIS2（ネットワーク情報およびセキュリティ指令2）を基盤に、CER指令は自然災害、テロ、サボタージュ、内部脅威などのリスクも対象としています。組織は、ITとOTの双方を含むテクノロジースタック全体で強固なサイバー統制を示す必要があります。

> “もはや境界は存在しません。セキュリティは、データ、ID、意図とともに移動する必要があります。デジタルシステムとフィジカルシステムが融合するにつれ、責任の所在が曖昧になり、ガバナンスの逸脱が生じます。問題はハイパーコネクティビティそのものではなく、融合が管理されていないことです。”
>
> **Ben de Bont氏**
> Chief Information Security Officer
> ServiceNow

動的セキュリティアーキテクチャへの移行

この領域で事業を行う組織は、ITとOTを別個に扱うのではなく、ITとOTにまたがる動的なメッシュ型へと、静的なセキュリティアーキテクチャを再編する必要があります。このアーキテクチャでは、最小権限アクセスや多要素認証を含むゼロトラストの原則がIT層とOT層に分散され、変化する脅威インテリジェンスに継続的に適応できます。これらのネットワークにより、デバイスはポイント間の信頼できる通信を通じて自立的な防御が可能となります。また、資産インベントリと組み合わせることでOT環境内のすべての資産に対する可視性が向上しますが、これは特に複数拠点・地域にレガシーテクノロジーが分散するセクターで重要です。継続的な検出とモニタリングにより、防御レベルを高め、潜在的な脆弱性をリアルタイムで特定・緩和できます。さらにこれらのアーキテクチャは、新技術を既存システムに統合することにも寄与します。

新旧システムの統合を含む大規模なシステム変更は、サイバー攻撃に対する脆弱性を高め、重大なインシデントにつながる可能性があります。そのため、メッシュ型アーキテクチャへの移行は、ネットワークの流れを妨げることなく、セキュリティ統制の強化と規制遵守を実現することを目指す必要があります。セグメンテーションや監視といった適応的統制を含む、安全な変更管理が不可欠です。

IT/OTチームを統合SOCに融合することで、両環境の監視を改善できます。これはセキュリティ上の懸念に対処するためにITとOTのさらなる融合を求める米国のCybersecurity and Infra-structure Security Agency（CISA）による論文[5]と一致しています。一方で、その論文ではOT固有のポリシーや手順の重要性も強調されています。

4 The Purdue Model provides a common language and structure for integrating business and manufacturing systems by organizing systems into different levels with clear boundaries, responsibilities and interfaces.、Claroty, ICS Security、The Purdue Model、2023年3月2日

5 Cybersecurity and Infrastructure Security Agency、Cross-Sector Cybersecurity Performance Goals Version 2.0、U.S. Cybersecurity and Infrastructure Security Agency、2025年12月

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題5

AI時代におけるセキュリティへの信頼の獲得

資産集約型の組織では、自律ロボティクスを用いた機械学習が脅威検知の高度化に活用され始めています。しかしAIの活用はまだ初期段階で主に予知保全に用いられており、異常検知、負荷分散、品質管理での利用が拡大しています。

それでもAIは、24時間365日の稼働、定型作業の自動化、迅速な学習、トレンドの特定、さらにはエージェントAIによる自律的な意思決定と脅威対応といった大きな可能性を持っています。製造業がAI導入の先頭を走る一方、高リスク環境にある業界のリーダーは、特に自律型AIの導入に対して慎重な姿勢を維持しています。

各国のサイバーセキュリティ機関による最近のガイダンス[6]では、AIをOT環境に統合することにより、OTプロセスモデルの時間経過による逸脱、安全プロセスの回避、新たな攻撃対象領域の創出といった重大なリスクが生じると警告しています。そのため、信頼性への懸念や、もっともらしいが誤った応答の可能性があることを踏まえると、AIは「OT環境における安全判断に用いるべきではない」としています。

AIリスクを低減するため、CISOはAIモデルの学習に用いられるOTデータを特定し、OTベンダーが強固なデータ利用ポリシーを適用してAIとデータを安全に使用していることを確認する必要があります。

> “ゼロトラストアーキテクチャと完全な資産可視化に向けたIT/OTハイパーコネクティビティは実現可能ですが、経営層の賛同とステークホルダーへの利点についての明確な伝達が必要です。OTエンジニアは、自律型AIが仕事を奪うどころか、効率を高め先駆的な文化を生み出すことに気付くでしょう。”

Ronald Heil
Global Cyber Security Leader for Energy and Natural Resources
KPMGオランダ

サイバーセキュリティ加速のための協働

デジタル化、AIイノベーション、地政学的プレッシャーにより、CISO、CTO/COO、事業部門、エンジニアリングチーム、さらにはOEM（製造元）、政府、規制当局といった幅広いステークホルダーを巻き込む、より協働的なセキュリティアプローチが求められています。OEMは、設計段階から展開、運用に至るまでのライフサイクル全体でセキュリティを優先しつつ、新技術を統合するための有益なインサイトと革新的な手法を提供できます。サードパーティによるサイバーセキュリティ統制の検証は監視とテストの価値を強調し、さらなる保証をもたらします。

AIやロボティクスへの信頼に基づき、サイバー脅威を検知するプロセスと規制を共に構築できます。責任はCISOのみが負うべきものではなく、変革を成功させるにはCEO（最高経営責任者）やCOOなどのトップダウンの後ろ盾が不可欠です。CISOは、工場やプラントなど資産ネットワーク全体の変革にサイバーセキュリティを組み込むため、意思決定の場に席を得る必要があります。ある大手企業のIT/OT変革プログラムでは、CISOが諮問委員会の一員として参画することで影響力を高めました。この諮問委員会には、CISO、エンジニアリング部門の責任者、工場長、そして400人のステークホルダーが参加していました。最終的に、あらゆる大規模な変革プログラムと同様、安定した委員会の体制と長期的なビジョンが成功の可能性を高めるといえます。

> “あらゆるセンサー、ビル制御、物流プラットフォームが、共有クラウドやAIシステムにデータを送信しています。次の飛躍は孤立したテレメトリから相関インテリジェンスへの移行であり、AIを用いて人間には捉えきれないITとOTにまたがるわずかな兆候を結び付けることです。”

Ben de Bont氏
Chief Information Security Officer
ServiceNow

6 Cybersecurity and Infrastructure Security Agency、Principles for the Secure Integration of Artificial Intelligence in Operational Technology、2025年12月3日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題5

推奨アクション

OEMと協働し、進捗を阻害しないよう性能を管理しつつ、規制動向を把握しながらアーキテクチャを再設計しセキュリティを統合します。

規制上の期待事項を満たし、組織と社会全体を守るためサイバーおよびオペレーショナルレジリエンスに注力します。

トップダウンの後ろ盾を得て早期に経営層を巻き込み、CISOを支えるための全社的な支援体制と投資を確保します。

ITとOTのテレメトリを相関させ、予測的防御と運用上のインサイトを実現するクロスドメインインテリジェンスを推進します。

IT/OTセキュリティ施策を事業目標に整合させ、組織の目的を妨げるのではなく支援するものとします。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題6

耐量子暗号への移行



> 暗号方式の変更は、突然新しい言語を話し始めるようなものです。取引先も同時に暗号方式を変えなければ通信は止まります。安全な通信はビジネスに不可欠であり、この移行はきわめて重要です。時間はありますが、無駄にする余裕はありません。

Michael Egan
Director, Quantum Technologies
KPMGオーストラリア

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題6

量子コンピューティングは今まさに産業を変革するところであり、従来型コンピューターよりも指数関数的に速く複雑な問題を解けるようになる可能性があります。しかし、この革命は前例のないサイバーセキュリティリスクももたらします。量子コンピューターが十分に成熟すれば、現在の暗号アルゴリズム[7]は陳腐化し、ビジネス、金融、医療、国家安全保障にかかわる機微データが危殆化します。

公開鍵暗号は現代のサイバーセキュリティの基盤であり、データの機密性、完全性、真正性を確保します。これがなければ、重要なオペレーションは停止します。また、組織は「Harvest Now, Decrypt Later（HNDL）」攻撃の脅威にも直面しています。これは、脅威アクターが将来的に量子コンピューティング能力が成熟した時点で復号する意図を持って、現時点で暗号化データを収集するというものです。

CIO（最高情報責任者）、CISO、CRO、CEO、そして取締役会メンバーにとって、耐量子暗号（PQC）への備えは免れることのできない責務です。サイバーセキュリティにとどまらず、移行の遅れがもたらすリスクには事業の混乱、金銭的損失、規制上の罰則、評判の毀損が含まれます。それにもかかわらず多くの組織はすでに出遅れていることを認識しており、「認識」と「準備」のギャップはPQCが「将来の検討事項」から「能動的な変革プログラム」に移行しなければならない理由を浮き彫りにしています。このきわめて重要な移行の舵取りをするため、組織は移行における責任者を明確に任命し、CIOとCISOが先手を打ってリスクを評価して移行戦略を策定し、量子レジリエンスに向けた世界的な競争に参加できるようにする必要があります。

41%

の組織が、量子コンピューティングがもたらす脅威への準備とPQCの導入において、後れを取っていることを懸念していると回答

出典：KPMGグローバルテクノロジーレポート2026

規制環境 — PQC適応を後押しする推進力

既存および今後の規制がPQC移行を推進しています。米国の「量子コンピューティングサイバーセキュリティ準備法」は、政府機関に迫り来る量子の脅威への対策を義務付ける枠組みです。米国行政管理予算局（OMB）の2025年の報告によれば、2025年から2035年にかけての連邦政府のPQC移行に要する推計コストは71億米ドル[8]と見込まれています。しかもこれは優先システムに限定した試算であり、ほぼすべての組織にとって大きなコスト負担となり得ます。

国際的には、G7サイバー・エキスパート・グループが金融機関にPQCの採用を促し、量子脆弱性にさらされる越境金融取引の重大リスクを強調しています。同グループは世界の金融フレームワークに対する重大な影響に対処するため、国境を越えた調和的な採用を提案し、移行ロードマップを示しています。

欧州では、欧州委員会（EC）が2025年6月にPQC移行ロードマップを公表しました。主な関連法令として、EUサイバーレジリエンス法、ネットワークおよび情報セキュリティ指令2（EU NIS2）、デジタルオペレーショナルレジリエンス法（DORA）、一般データ保護規則（GDPR）のコンプライアンス枠組みが挙げられます。

これらの取組みはすでに最新テクノロジー水準、実装コスト、対象データの機微性を考慮し、リスク水準に見合ったセキュリティ対策の実装を組織に求めています。FIPS（連邦情報処理標準）203、204、205の公表により、「最新テクノロジー水準」の定義が変化し、量子安全への備えに対する期待が高まっています。一部の組織は暗号部品表に関するPCI DSS（Payment Card Industry Data Security Standard：ペイメントカード業界データセキュリティ基準）V4要件への対応がすでに求められており、暗号システムのインベントリ化と管理体制整備の必要性が高まっています。オーストラリア通信電子局（ASD）は、米国国立標準技術研究所（NIST）の最新PQC標準を反映するため、新たに承認された暗号アルゴリズム[9]を含むガイドラインを改訂し、この移行の目標時期を2030年としています。

これらの動向は、政府と組織が今後10年、さらにその先に向けてデータを保護しようとするなかで、PQC移行の必要性に関する国際的合意が拡大していることを示しています。

PQC移行のタイミング

PQCの実装は複数年におよび、戦略的な計画と業界横断の継続的な協働を要します。NISTのPQC標準化プロジェクト[10]で示されているとおり、標準化アルゴリズムを展開するためのマイルストーンは今後10年にわたって続きます。

7 現在の暗号アルゴリズムの例として、RSA（Rivest–Shamir–Adleman）およびECC（Elliptic-Curve Cryptography）が挙げられます。
8 Executive Office of the President of the United States、Report on post-quantum cryptography、2024年7月
9 ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) (FIPS 203)、ML-DSA Module-Lattice-Based Digital Signature Algorithm (FIPS 204)
10 National Institute of Standards and Technology、「What is Post-Quantum Cryptography?」、2026年2月27日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題6

金融機関向けのFS-ISAC（Financial Services Information Sharing and Analysis Center）ガイダンスも、越境金融システムを保護しようとする業界の取組みのなかで、PQC統合のタイトなタイムラインを反映しています。同様に、金融セクター向けのG7ロードマップは協調的な移行に対するプレッシャーを高めています。

組織のIT資産全体でPQCに移行することは複数年にわたる取組みであり、特にPQCの長い鍵長に対応できない旧式ハードウェアを管理するには、多くのステークホルダーの賛同が必要です。移行の遅延は、コンプライアンス違反のリスクだけでなく、重要システムが新たに求められる暗号要件に対応できない場合、運用上の陳腐化のリスクも招きます。

主要マイルストーンを達成できない場合、組織は多くの脆弱性にさらされ、顧客取引から通信、国家安全保障、重要インフラに至るまで、あらゆる領域に支障が出る可能性があります。

サードパーティおよび調達上の課題

PQCに移行するには、PQCへの対応ができないシステムやハードウェアを導入しないよう、調達慣行を抜本的に見直す必要があります。これには、サードパーティベンダーに厳格な量子安全標準の採用を求めることも含まれます。

TNO[11]のPQC移行ハンドブックは、組織が直面する複数の課題を明らかにしています。

- サードパーティの脆弱性：多くのベンダーがPQC採用で遅れており、特にレガシーシステムに保存された暗号化データの管理で遅れが目立ちます。
- 調達計画：量子安全標準に準拠し、準備不足のベンダーに起因するリスクを低減させるには、調達のセキュリティ要件を迅速に調整することが不可欠です。

組織は、サプライヤーの暗号能力を特定・評価するための包括的な計画を早急に策定する必要があります。ベンダーとの迅速な連携と一貫したコミュニケーションは、混乱の軽減につながります。特にサプライチェーンがタイムリーな暗号化データ交換に依存している場合には、その重要性が高まります。

金融セクターへの示唆

金融セクターは、安全な取引、顧客データ保護、越境金融の安定性確保に対する暗号技術への依存度が高いことから量子脆弱性の影響を最も受けやすい領域の1つです[12]。PQC採用の遅れは顧客の信頼を損ない、受託者責任に抵触し、世界的な金融ネットワークを混乱させる可能性があります。

Australian Financial Review（AFR）の記事[13]で、オーストラリア準備銀行（RBA）総裁のMichel Bullock氏は、金融セクター全体での能動的な協働を呼び掛けています。先進企業はリスク低減のため量子安全プロジェクトを実行に移し、他社がテクノロジーロードマップに能動的に取り組むための模範を示しています。

防衛セクターの主要課題：リスクにさらされる国家安全保障

PQC移行は、防衛産業にとって存続にかかわるリスクです。準備不足は機密通信、指揮統制システム、新たな防衛テクノロジーを脅かし、国家および世界の防衛エコシステムを脆弱にします。注目度の高いサイバー攻撃は、デジタルシステムがオフラインになることで事業運営が麻痺し得ることを示しています。

将来を守るための時間は限られている

PQCへの移行は、きわめて重大なサイバーセキュリティ課題の1つであり、規制当局と業界リーダーが主導する能動的かつ世界的な足並みの揃った対応を必要とします。これは技術的な課題にとどまらず、早期の着手と継続的なリーダーの関与が求められる、根本的な事業上の優先事項です。

CIO、CISO、そして取締役会は、量子リスクへの対応に今すぐ着手し、運用上の脆弱性や長期的な金銭的損失から組織を守る必要があります。英国国家サイバーセキュリティセンター（NCSC）は次のように述べています。「PQC移行は世界的に起こるため、対応を避けることはできません。したがって、今準備し計画することで安全で秩序立った移行ができます[14]」

重要なのは今日から行動を開始することです。リスクを評価し、教育に取り組み、量子安全な将来に向けたパートナーシップを築くことです。

> 予算とリソースを確保し、ロードマップ推進の勢いを作るため、CISOはリスク、規制、内部監査部門のリーダーのなかに協力者を見つける必要があります。これにより、PQCをITやデータの問題から戦略的に重要な能力へと捉え直すことができます。

Alexander Rau
Partner, Cybersecurity
KPMGカナダ

11 TNOは、応用科学研究に注力するオランダの組織です。
12 US Government, Department of War、「Preparing for Migration to Post Quantum Cryptography」、2025年11月20日
13 Eyers, James、「Bullock warns banks of 'scary' quantum computing security threat」Australian Financial Review、2025年10月24日
14 Timelines for migration to post-quantum cryptography、UK National Cyber Security Centre、2025年3月20日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題6

推奨アクション

量子リスク評価を実施し、影響の大きさを明らかにするとともに移行に向けた明確なビジネスケースを構築します。

重要な依存関係を可視化し理解するために暗号インベントリを構築し、移行期間を通じて暗号アジリティと継続的モニタリングを重視します。

調達標準を見直し、早期連携をすることでベンダーのコンプライアンス対応を支援します。複数年に及ぶ移行期間中のサードパーティのセキュリティリスクを管理するため、調達ルールを整備します。

組織全体で必要なスキルを備えられるようチームのスキルを向上させ、ステークホルダー全体に向けた教育プログラムを実施して、課題と影響に関する共通理解を形成します。

専門家と協働し、体系的なリスク評価と詳細な計画策定のためのフレームワークを活用します。運用上の実装リスクと予算を管理するうえでは、計画が鍵となります。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題7

検知と対応によるサプライチェーンの保護



> サプライチェーンにおける検知と対応は、サプライヤーとファーストパーティとのコミュニケーションと信頼を向上させ、データ共有を可能にします。前向きなアクションを促進することで、サイバーセキュリティ上の問題を「特定するだけ」と「実際に解決すること」の間にあるギャップを埋めることができます。

Raj Ahuja
Managing Director, Cyber Managed Services
KPMG米国

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題7

今日のサプライチェーンはクラウドプラットフォーム、SaaSプロバイダー、そしてディストリビューター、ビジネスパートナー、小売業者を含む、数百から数千に及ぶサードパーティ、フォースパーティ、フィフスパーティに依存しています。これまで膨大なIoTデバイスにまたがっていた攻撃対象領域は、今やAIを含むまでに拡大しています。組織は、知的財産を盗み、オペレーションを妨害しようとする犯罪者、悪意あるハッカー、国家レベルの脅威アクターからの攻撃にさらされています。「KPMGグローバルテクノロジーレポート2026」によれば、セキュリティ上の懸念、知的財産およびデータ保護に関する懸念が、組織間のより広範な協力を妨げる上位5つの障壁のなかに挙げられています。

サプライチェーンレジリエンスは、企業の短期的な意思決定を左右する最大の要因です。

出典：KPMGグローバルCEO調査2025

従来型で手作業に依存することの多いサードパーティリスク管理（TPRM）は、AIボットやディープフェイクによって増幅されるサイバー脅威の頻度と深刻度に、もはや追いつけません。主な焦点は、組織に直接サービスを提供するサードパーティベンダーに置かれがちで、時点ベースで評価が行われるという特徴があります。その結果死角が生まれ、従来型の紙ベースのレビューに重点が置かれることになります。このようなアプローチでは、完全でリアルタイムなサプライチェーンの可視性を確保できず、不審な活動を見逃してしまいます。

セキュリティ専門家は、AIシステムやアプリケーションを含むことが増えているサプライヤーのテクノロジースタックを把握できない場合があり、攻撃機会が増大しています。その結果、組織のセキュリティが低下する可能性があるため、TPRMを自組織の脅威監視ワークフローに統合する方向へ転換することが必要になります。TPRMのコンプライアンス対応は負担が重く、評価疲れを招き、サプライヤーが実質的なリスクの対処ではなく形式的なチェック対応に終始する要因ともなり、悪意ある者に悪用される隙を生みます。さらに、実際のインシデント発生時であっても、静的な質問票では実行可能なインテリジェンスをほとんど提供できません。

複雑化が進む規制対応

サプライチェーンとTPRMに関する脅威は世界的に規制圧力を高めており、各種法制は組織のレジリエンスと重要インフラの保護を重視しています。例として、SOCI（重要インフラ安全保障法）、EU NIS2（ネットワークおよび情報セキュリティ指令2）、DORA（デジタルオペレーショナルレジリエンス法）があります[15]。これは、OTのデジタル化を踏まえると、製造業のサプライチェーンにとって特に重要です。また、医療のように大量の個人情報を扱う業界では、データ保護もさらなる懸念事項です。さらに、サプライチェーン全体においてデータ主権規制も満たさなければならず、特定のデータを国境内に保存することが求められます。「2026 KPMGグローバルサードパーティリスクマネジメント（TPRM）に関するサーベイ」では、45%の組織でTPRMにおいて規制およびコンプライアンスリスクの重要性が高まっていることを示しており、サプライチェーンのサイバーセキュリティに対する規制当局の監視が強まっていることを浮き彫りにしています。

関税、紛争、地政学的連携の再編に直面するなかで、組織はサプライチェーンを精査し、制裁対象または「非友好的」とみなされる地域の組織との関係を避ける必要があります。また、地政学的緊張が高まるにつれ、一部の組織はサプライチェーンを短縮して拠点の国内回帰を進めており、その結果、デューデリジェンスを要する新たな事業者が増加しています。これらの要因はすべて、コンプライアンス負担を押し上げます。こうした変化を反映し、「KPMGグローバルテクノロジーレポート2026」によれば、36%の組織がパートナーシップエコシステム全体でデータ主権監査の強化を計画していると回答しています。詳しくは、本レポートの主要課題2「地政学リスクを読み解き、レジリエンスとコンプライアンスを構築」で、この点について論じています。

45%

の組織が、規制およびコンプライアンスリスクの重要性が高まったと回答

出典：2026 KPMGグローバルサードパーティリスクマネジメント（TPRM）に関するサーベイ

15 Critical Infrastructure Security Centre、Security of Critical Infrastructure Act 2018（SOCI）、2024年8月27日 | European Commission、NIS2 Directive: securing network and information systems、2026年1月20日 | European Insurance and Occupational Pensions Authority、Digital Operational Resilience Act (DORA)、2025年12月15日

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題7

サードパーティエコシステム全体でのリスク統合

対照的に、サプライチェーンにおける検知と対応（SCDR）は、焦点をベンダーのコンプライアンスからレジリエンスへと移します。SCDRは、サプライチェーンのサイバー攻撃を防ぎ、重要プロバイダーに停止やセキュリティ障害が生じた場合の集中リスクを低減するために、サプライヤーエコシステム全体の脆弱性を特定し、優先順位を付けて対処します。これはサプライチェーン内のすべての関係者を対象としており、AIと自動化により、データ主導の継続的モニタリングを行います。

ゼロトラストの原則は、とりわけOT環境において不正アクセスのリスク低減に役立ちます。ゼロトラストの原則に基づいてシステムを設計することは、サードパーティリスクの対象領域を縮小し、効果的なTPRMの基盤となります。

最終的にSCDRは、サイバー攻撃が起きる前に脆弱性に起因するリスクを特定し、緩和するための能動的な取組みとなります。

サイバー脅威インテリジェンスは、継続的モニタリングを含む、より広範なTPRMプログラムに統合されるべきです。これにより組織は、サードパーティエコシステムに起因するリスクをより的確に理解できるようになります。AIレイヤーを追加することで、CISOは人間では対応しきれない複数のサードパーティ関係を対象に活動規模を拡大することができます。すでに、エージェントAIがサードパーティのリスクプロファイルの決定、サードパーティ情報の統合、潜在的脅威のトリアージを支援し、追加の対応が必要な領域を可視化する動きが見られています。今後については、KPMGの調査で回答した組織の約4〜5割は、今後3年間でTPRMの中核業務においてAIを中程度に活用する見込みであり、脅威インテリジェンス強化のためにAIを活用する方向への明確な移行を示しています。

SCDRに対してリスクベースのアプローチを取ることで、組織は高リスクのパートナー（特にサイバー成熟度の低いパートナー）に対してより厳格で自動化された継続的モニタリングを適用でき、可視性を高められます。

これには、ダークウェブ上の流出資格情報の監視に加え、信頼しているベンダーが侵害された可能性を示す他の指標の監視も含まれます。

サードパーティとの協働によるレジリエンス強化

組織は、サプライヤーとより緊密に協働して防御を強化し、サイバーセキュリティに対する相互の責任を強化することができます。あるいは、「コンプライアンスだけではセキュリティにならない」という考え方を採用し、リスクベースのアプローチを取ることもできます。ServiceNow社のBen de Bont氏は次のように述べています。「それは、形式的な認識の確認だけでなく、運用上のアクションを促すことができます」

契約書には、期待されるサイバーセキュリティ水準（量子暗号への対策を含む）を明記し、侵害の通知義務、ならびにセキュリティインシデント発生時に侵害された資産やシステムを停止するための対応計画を盛り込む必要があります。従来のTPRMでは評価項目が広範にわたり、対応に時間を要する場合があります。一方でSCDRは、サプライヤーネットワークにおけるリスクの高い領域に絞って監視し、AIと自動化によりプロセスを高速化し、エラーを減らします。

脆弱性が特定された場合、組織はサードパーティが脅威を無力化できるよう支援できます。社内では、TPRMチームは24時間365日の監視を担うマネージド検知・対応（MDR）チームとの連携を強化し、より強固でリスク認識の高い文化を醸成すべきです。侵害は組織全体に影響を与えますが、責任を共有することで脅威が低減し、評判が維持され、規制要件が遵守されます。

> “クラウドベースのAIが台頭するなかで、組織はAIがどこでどのように使われているのかを把握しづらくなる場合があります。可視性を高めるため、組織はサプライチェーン全体にわたる包括的なAI構成要素一覧の作成を検討すべきです。”

Srijit Menon
National Head for TPRM in India
KPMGインド

> “最大の死角は「時間」であり、多くの組織はいまだに年次監査や定型化された質問票に依存していて、それらは完了する前にすでに最新情報を反映していない場合があります。継続的モニタリングは、リアルタイムのベンダーテレメトリと自動スコアリングを統合し、年1回の認証ではなくリアルタイムの情報に基づく評価へと転換すべきです。セキュリティは継続的で、自動化されていて、測定可能でなければなりません。そして、その実現にAIは大きく貢献できるでしょう。”

Ben de Bont氏
Chief Information Security Officer
ServiceNow

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題7

推奨アクション

サードパーティリスク管理を従来のベンダーにとどめず、ディストリビューター、パートナー、小売業者まで拡張し、オペレーショナルレジリエンスに焦点を当てます。

リスクプロファイルに基づいてリソースを配分し、強固なサイバーセキュリティ統制を欠く高リスクかつ成熟度の低いサードパーティを優先します。

事業影響分析および最新の継続計画を通じて、資産管理のレジリエンス（特にOT）を強化します。

最もリスクが高いベンダー（社内アクセス権限を持つヘルプデスク提供者など）を特定して、監視を強化し継続的にモニタリングします。

サプライヤーとの契約で、リスクベースのコンプライアンス要件、明確なインシデント対応計画、アクセス管理・監視・特権アクセスに関する統制を定義します。

インシデント対応、事業継続、机上演習などのレジリエンス活動にサプライヤーを関与させることで、サプライヤーとの共同責任の文化を醸成します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題8

CISOの役割と影響力の拡大



> 先見性のあるCISOは、責任範囲をサイバーから事業全体に広げ始めています。彼らは、コンプライアンスをただ振りかざすのではなく、取締役会に対してサイバーに関する問題をビジネスの観点で説明し、財務面・評判面・運用面の影響を理解できるよう支援しています。

Anna Poole
Cyber Security, Energy, Mining & Property Sector Lead
KPMGオーストラリア

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題8

セキュリティが事業やオペレーションにより深く統合され、サイバー領域とフィジカル領域が融合するにつれ、CISOの職責と責任範囲は拡大し続けています。同時に、CISOはAIの大規模導入に伴う機会と脅威の双方を管理しなければなりません。しかし、こうした変化はCIOやCTO、ひいては取締役会レベルでの意思決定における影響力の向上につながっているのでしょうか。また、これらの変化はサイバー機能の在り方にどのような影響を与えるのでしょうか。

CISOは大きく2つのタイプに分けられます。1つは、レジリエンス、統制の有効性、測定可能なサイバーリスク低減を重視する、従来型のオペレーションおよびテクノロジー志向のCISOです。この役割は不可欠であり、厳格な指標、エンジニアリングの規律、一貫した実行を通じて、セキュリティの基盤を構築・維持します。このアプローチでは取締役会を含む事業全体への日常的な関与は相対的に少ないかもしれませんが、組織の基本的な防御力とコンプライアンスを堅牢かつ信頼性の高いものにします。

一方で近年は、事業戦略に沿ってサイバーセキュリティを組織全体に組み込もうとする、先進的なCISOも台頭しています。このようなCISOは、サイバー脅威に起因する財務面・評判面・運用面のリスクに対する経営幹部の認識を高めています。そして、サイバーセキュリティを単にコンプライアンスという位置付けではなく、デジタルトランスフォーメーション（DX）、クラウドやAIの導入、新規事業を支える戦略的な推進要素として捉え直しています。

KPMGのGlobal Chief Information Security OfficerであるJohn Israelは次のように述べています。「CISOの役割は、本質的に『セキュリティ変革推進リーダー』へと進化しています。私たちはもはや事業を守るだけでなく、推進する存在です。私たちの主な目標は、業務プロセスからテクノロジー導入に至るまで、組織のあらゆる部分にセキュリティをシームレスに組み込み、イノベーションやスピードを阻害するのではなく、むしろ加速させることです。そのためには、純粋に技術的、あるいはリスク助言的な役割を超え、取締役会、CIO、CTOと真の戦略的パートナーとなり、主要な事業目標を達成するための安全な変革を推進する必要があります」

リスクと規制のバランス

データプライバシーやセキュリティに関する規制は、組織のあらゆる領域に影響を及ぼします。インシデント報告を含め規制を遵守しなかった場合、罰金や評判の毀損につながりかねません。規制当局の焦点は、機密性や完全性だけでなくレジリエンスや可用性へと移行しており、組織にはサイバー攻撃を防止し耐え抜く能力を備えるとともに、サプライチェーンや業務に対する影響の最小化が求められています。CISOは、規制要件を満たしながらも、新製品・新サービスの提供スピードを落とさないよう、コンプライアンスとイノベーションのバランスを取る必要があります。コンプライアンスは達成すべき上限ではなく、あくまで最低限の基準と捉えるべきです。

> “CISOにより大きな影響力を与えることは、セキュリティを重視している姿勢を示すものであり、企業リスクを包括的に捉える視点を確立します。そして、サイバーリスクを後付けとするのではなく、戦略の中核に据える議論を促します。”

Del Heppenstall
UK Cyber Lead
KPMG英国

組織はまた、業界や地域ごとに規制体制がますます乖離する状況に直面しています。規制要件は欧州と米国では異なり、さらに州や地域単位でも異なる場合があります。コンプライアンスコストが上昇するなかで、CISOは各地域の規制義務と、コスト効率が高くグローバルに整合したコンプライアンスモデルの必要性とのバランスを取らなければなりません。特にデータプライバシー分野において法務責任者との関係を強化することで、CISOは規制動向を把握し、ブランド価値の保護・向上、高額な制裁の回避、そして何よりもレジリエンスの維持に貢献できます。

統合されたサイバーリスクリーダーシップモデルへ

デジタルとフィジカルの世界が交錯するなかで、CISOの役割は、IT、OT、組織全体、さらにはサードパーティにまで広がり、組織のセキュリティの方向性を形作るものになっています。CISOはまた、特に非構造化データ管理を含め、データセキュリティ施策と連動したデータ管理を主導する役割も担いつつあります。これは、通常はCIOやCDOの配下で機能する領域を束ね、より広範なリスクを管理することを意味します。一部の業界では、CISOが最高セキュリティ責任者に任命されるケースも見られます。

一部のCISOやそのチームは、フィジカルセキュリティやOT環境、さらにはAIや新たなコンプライアンス要件の複雑さに十分対応できる体制や権限を持っていない場合があるため、大幅なスキル向上や組織構造の見直しが求められます。セキュリティ部門に限らず、組織全体に向けた継続的な教育・意識向上プログラムは、従業員がセキュリティ課題に対応する力を高めるのに役立ちます。加えて、ITチームとOTチームがサイロ化して領域横断的なセキュリティ連携を阻害していることも多いため、CISOは部門間の信頼ギャップを埋める役割を果たすべきです。

IT/OTが融合した環境で成功するためには、CISOは取締役会と緊密に連携し、セキュリティ目標と事業目標を整合させるとともに、オペレーション、営業・マーケティング、調達、人事といった部門間の関係構築を担うことが求められます。また、脅威の状況を把握し、それをビジネスの観点で説明することで、意思決定の質を高めていく必要があります。

CEOおよび取締役会は、サイバーセキュリティは全員の責任であることを強く打ち出し、取締役会レベルおよび組織全体での説明責任を高めることで、支援を示す必要があります。セキュリティが民主化されたこの新たな文化のもとでは、従業員が報復を恐れることなく懸念やインシデントを報告できることが重要であり、これは早期検知と迅速な対応に不可欠です。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題8

AIの運用段階への移行

生成AI、そして現在のエージェントAIは、インターネットの登場に匹敵するほどの巨大な技術的転換点を示しています。AI開発のスピードは戦略計画の期間を4〜5年から最短18ヵ月にまで短縮しており、CISOはAIシステムのセキュリティを「対象として」「活用しながら」「起点として」定義するために、より早期かつ能動的な関与が求められています。組織がコンプライアンス重視から安全なAI導入へと舵を切るなかで、CISOとそのチームは、CIO/CTO主導の大規模AIプログラムの初期段階にセキュリティを組み込むようになっています。CISOが早い段階から議論に加わり、プログラムや製品におけるセキュリティの重要性を明確にし、データを保護することでパフォーマンス向上につなげることが、付加価値の核心です。

> AI時代において、データは持続的な競争優位性を生み出すための価値の源泉です。データは企業内で最も変化の速いリスクの1つである一方、新たな収益源や競争優位性を生み出す鍵でもあります。CISOとして私たちは、危険性だけでなく機会の視点からデータに関する議論を主導しなければなりません。私たちの役割は、組織がデータの力を最大限に引き出せるような安全な枠組みを構築し、潜在的な負債を最大の資産へと転換することです。

John Israel
Global Chief Information Security Officer
KPMGインターナショナル

> CIOやCTOに対して影響力を得るためのコツは、必ずしも取り締まる側になることではありません。セキュリティを通じて、スピード、効率性、創造性を支援することです。

Gary Berletti
Deputy Global Chief Information Security Officer
KPMGインターナショナル

AIはまた、バイアス回避やデータセキュリティプライバシー要件への準拠といった、倫理上・規制上の懸念も引き起こします。CISOは、イノベーションの阻害者とみなされることなく無制限・無秩序なAI利用を抑制するという、倫理的な綱渡りを強いられています。フレームワークの整備、継続的かつ自動化されたテスト、AIレッドチーミングを確立することで、CISOはAIを信頼して活用するためのガードレールを提供し、事業を前進させることができます。

AIは課題であると同時に、CISOにとっては大きな学習機会でもあり、加速するイノベーションのスピードに対応し続けるとともに、戦略・市場・オペレーションの各レベルでAIをどのように活用できるかを理解することが可能になります。サイバー領域を超えて、戦略やオペレーションにおけるAIを主導することで、CISOは役割と影響力を拡大しています。セキュリティ変革推進リーダーとして活動するCISOは、プライベートエクイティ投資家のように思考し、非効率なレガシーテクノロジーを大胆に切り離し、大きな改善と実質的な効率化をもたらす能力を追求する必要があります。

AI主導のサイバーセキュリティ

サイバーチーム内では、AIが時間と労力を大幅に削減して生産性を高めます。AIによる自動化は、継続的モニタリングやインシデント対応を飛躍的に高速化し、セキュリティチームは脅威を検知してデータを集約し、対象を優先付けすることができるようになります。主要課題4で述べたとおり、エージェントAIはエージェントの特定、アクセス権の確認、行動追跡といった点で新たな課題を生んでおり、これらが合意された範囲内で運用されていることを担保する必要があります。さらに、従業員が組織の統制外で機密データにアクセス可能な独自エージェントを利用しようとすることによる内部リスクも存在します。

> AIは新たな機会を生み出しただけでなく、サイバー機能そのものを格上げしました。攻撃対象領域が拡大するなかで、セキュリティは事業上の必須要件となっています。また、AIはデータによって駆動されるため、データセキュリティとガバナンス、特にID・アクセス管理の重要性が一段と高まり、信頼の中核を成しています。

Saira Mohammed氏
Chief Security Advisor
Microsoft

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主要課題8

推奨アクション

AIファーストの姿勢をとり、継続的モニタリング、ID・アクセス管理、生産性向上を通じて、脅威アクターに先行します。

セキュリティテレメトリの活用によりサプライチェーン全体のサイバーレジリエンスを強化して、サードパーティリスクを評価し、混乱から迅速に回復できるようにします。

データ、クラウド、IDセキュリティ全体にわたる強固なポスチャ管理により、混乱を最小化し、攻撃を未然に防ぎます。

イノベーションのスピードを維持するため、不確実性を受け入れ、8割程度の確信が得られた段階で意思決定を行います。

事業部門の声に耳を傾け、進捗を妨げるのではなく促進するような、適切なサイバー統制を適用します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2026年におけるサイバーセキュリティ戦略

組織がAIの価値を引き出し、信頼を維持するなかで、サイバーセキュリティを組織目標の真の戦略的な推進要素とするために、CISOや事業部門のリーダーは今後1年でどのような行動を取るべきでしょうか。
以下の提言は、ますます複雑化する環境において、CISOが事業を守ると同時に事業を推進するための指針を示しています。

人材

- 取締役会、IT部門、リスク管理部門と連携し、協働的かつ包括的なリスク文化を醸成します。
- 「KPMG Trusted AI」やKPMGの「Quantum Care フレームワーク」などを活用し、専門家と協働して体系的なリスク評価と詳細な計画の策定を行います。
- 人を置き換えるのではなく補完する形でAIを活用し、モデルや結果に対する強力な監督のもと、ヒューマンインザループを維持します。
- IDをより広範で信頼できるAIフレームワークの一部として位置付け、セキュリティ、リスク、プライバシー、法務、事業部門の各チーム間の連携を強化します。
- コンプライアンスのみに依存するのではなく、サイバーセキュリティに対する共同責任に基づくサプライヤー文化の醸成を促進し、すべての事業者に価値を創出します。

プロセス

- ポリシーベースのアクセス制御、分散型ID管理、継続的モニタリングを用いてゼロトラストの原則を適用します。
- 継続的モニタリングおよびレッドチーミング演習に支えられた形で、AIシステム開発全体にセキュリティ・バイ・デザインを組み込みます。
- 量子リスク評価を実施して影響の大きさを明らかにするとともに、移行に向けたビジネスケースを構築します。
- サードパーティリスク管理を従来のベンダーにとどめず、ディストリビューター、パートナー、小売業者まで拡張し、オペレーショナルレジリエンスに焦点を当てます。
- 事業影響分析および最新の継続計画を通じて、資産管理のレジリエンス（特にOT）に注力します。

テクノロジー

- 変化する状況に適応するため、データ、サービス、テクノロジーアーキテクチャの定義と実装を支援します。
- 分類、タグ付け、ラベリングをデータセキュリティの基盤と位置付け、データを生存のための仕組みとして扱います。
- 中央集約型のIDストアを確立し、エージェントAIをタグ付けおよび追跡して、それらが認証されていることと、許可された範囲内で動作することを保証します。
- 自律型セキュリティアーキテクチャをSOCに導入し、継続的モニタリングによってセキュリティアラートのトリアージ、脆弱性の特定、AI主導の脅威管理を行います。
- 暗号インベントリの構築により重要な依存関係を可視化して理解し、移行期間を通じて暗号アジリティと継続的モニタリングを重視します。

規制

- 規制要件を満たし、組織と社会を守るため、サイバーおよびオペレーショナルレジリエンスに注力します。
- 地政学リスクや新たな規制基準をCISOのプログラムに統合し、先見性と意思決定の質を高めます。
- サプライヤーとの契約で、リスクベースのコンプライアンス要件と明確なインシデント対応義務を定義します。
- OEMと協働し、性能を管理し規制動向を把握しながらアーキテクチャを再設計し、セキュリティを統合します。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMGによる支援

KPMGの各ファームは、取締役会からデータセンターに至るまで幅広い領域にわたる経験を有しています。組織のサイバーセキュリティを評価し、事業上の優先事項に整合させることに加え、KPMGのプロフェッショナルは高度なデジタルソリューションの開発・導入、継続的なリスクのモニタリング、そしてサイバーインシデントへの効果的な対応の支援を提供することが可能です。サイバーセキュリティの取組みがどの段階にあっても、KPMGの各ファームは目標を達成するために支援します。

この支援は、サブスクリプション型の成果志向のモデルで知識集約型の業務プロセスを運用するKPMG Cyber Managed Servicesを通じて、継続的なオペレーションにも及びます。先進テクノロジーと機能・プロセス・セクターに関する深い知見を組み合わせることで、本アプローチは、業務機能の継続的な進化、サイバーおよびオペレーション能力の強化、コスト削減、そして混乱とリスクの抑制を支援します。

サイバーセキュリティの主要な提供者であり導入者でもあるKPMGのプロフェッショナルは、最先端のセキュリティ手法を適用し、目的に適合した新たな手法を構築する方法を熟知しています。KPMGの先進的なサイバーセキュリティへのアプローチはサービス提供の方法にも反映されており、KPMGがどのような形で関与する場合でも、ビジネスとテクノロジーに精通したプロフェッショナルと協働することができます。

KPMG Velocityによるビジネストランスフォーメーションを通じて、AI対応の製品・サービスを一元的に提供し、企業全体でスピード、セキュリティ、価値のバランスを取りながら、より賢く変革し、より速く前進できるよう支援します。新市場への参入、製品・サービスの立ち上げ、顧客との新しいかかわり方のいずれであっても、KPMGのプロフェッショナルは将来を見据え、安全で信頼できるテクノロジーによって優位性を得るための取組みを支援します。



© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

執筆者



Laurent Gobbi
Global Cybersecurity and
Tech Risk Centre of Excellence Leader
KPMGインターナショナル
lgobbi@kpmg.fr

アドバイザリーサービスで30年以上の経験を有するGlobal CybersecurityおよびTech RiskのLeaderです。フランスにおけるテクノロジー分野の体制構築に重要な役割を果たし、20名のチームから600名超のプロフェッショナルへの成長を統括してきました。また、フランスのリスクコンサルティングおよびマネジメントコンサルティング部門でリーダーを務め、EMEAのTech Risk Leaderでもあり、2023年にはGlobal Trusted AI initiativeを立ち上げました。テクノロジー分野におけるM&A、IT戦略、CIOアドバイザリー、テクノロジーリスク（サイバーおよびプライバシーを含む）、内部監査、リスク、ガバナンスなど、さまざまな領域でKPMGのクライアントに助言しています。



Jim Wilhelm
Global Cybersecurity
Investment Leader
KPMGインターナショナル
jameswilhelm@kpmg.com

KPMGのGlobal Cybersecurity Investment Leaderで、フィラデルフィアのオフィスに所属しています。幅広い業界のクライアントに対し、情報セキュリティおよびID・アクセス管理の支援を提供してきた20年以上の経験があります。KPMGでは米国のサイバーおよびTech Riskのリーダーシップチームの一員として、金融サービスおよびヘルスケア分野のクライアントとともに変革的なサイバーセキュリティソリューションを推進してきました。



Dani Michaux
Cybersecurity Leader, EMA
Partner, KPMGアイルランド
dani.michaux@kpmg.ie

サイバーセキュリティ分野で22年以上の経験を持ち、政府機関と国家サイバーセキュリティ戦略に取り組み、国際的な規制機関とサイバーリスクに取り組んできました。取締役会レベルでのサイバーセキュリティ理解を高めるためにクライアントと協働してきた豊富な経験があります。さらに、アジアの通信会社や電力会社でCISOとしてサイバーセキュリティチームを構築し、運営を担ってきました。また、インクルージョン＆ダイバーシティ、ならびにコンピューターサイエンスとサイバーセキュリティにおける女性の参画を提唱しています。以前はKPMGマレーシアおよびASPACにおけるサイバーセキュリティおよびEmerging Technology Riskの部門を率い、KPMGのglobal IoTワーキンググループも主導しました。



澤田 智輝
Cybersecurity Leader, ASPAC
Partner, KPMGジャパン
motoki.sawada@jp.kpmg.com

サイバーセキュリティおよびIT分野で25年以上の経験を有するASPAC Cyber Leaderです。日本において、ID管理、セキュリティ運用、脆弱性管理、Microsoftセキュリティ、OTセキュリティを含むサイバーセキュリティ変革の取組みを主導してきました。サイバーセキュリティとリスクコンサルティングの双方に強いバックグラウンドを持ち、さまざまな業界の多数のクライアントに対して、サイバーセキュリティ戦略・ロードマップの策定、サイバーセキュリティソリューションのグローバル導入、サイバーインシデントからの復旧支援を行ってきた豊富な経験があります。



Prasanna Govindankutty
Cybersecurity Leader, Americas
Partner, KPMG米国
pkgovindankutty@kpmg.com

米国を拠点とするKPMGのCybersecurity ServicesのPrincipalです。サイバーセキュリティとテクノロジーリスク変革に関する20年の専門経験を持つ、米州地域のCyber Leaderです。以前は、KPMGのGlobalおよびUS Powered Cyberソリューションを主導しました。サイバー分野およびガバナンスリスクコンプライアンス（GRC）機能向けの市場をリードするテクノロジーソリューションを深く理解し、クライアントの統合的な変革を支援しています。また、テクノロジー主導の変革に関する豊富な経験を生かし、エネルギー、メディア、通信セクターのクライアントを支援しています。

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

謝辞

本レポートは、世界各地のプロフェッショナルによる貴重な計画、分析、執筆、制作への貢献なしには実現しませんでした。

グローバルサイバーセキュリティ主要課題チーム：

John Hodson
Billy Lawrence
Leonidas Lykos
Aman Manhas
Danielle Moriana
Peter Valentin

KPMGの協力者：

Raj Ahuja
KPMG米国
rajeshahuja@kpmg.com

Hossain Alshedoki
KPMGサウジアラビア
halshedoki@kpmg.com

Gary J Berletti
KPMGインターナショナル
gberletti@kpmg.com

Chris Crevits
KPMG米国
ccrevits@kpmg.com

Juan Manuel Zarzuelo Diaz
KPMGスペイン
jzarzuelo@kpmg.es

Michael Egan
KPMGオーストラリア
megan5@kpmg.com.au

Javier Aznar Garcia
KPMGスペイン
jaznar@kpmg.es

Atul Gupta
KPMGインド
atulgupta@kpmg.com

Ronald Heil
KPMGオランダ
heil.ronald@kpmg.nl

Del Heppenstall
KPMG英国
del.heppenstall@kpmg.co.uk

Kristy Hornland
KPMG米国
khornland@kpmg.com

John W Israel
KPMGインターナショナル
johnisrael@kpmg.com

Charlie Jacco
KPMGインターナショナル
cjacco@kpmg.com

Srijit Menon
KPMGインド
srijitmenon@kpmg.com

Anna Poole
KPMGオーストラリア
annapoole@kpmg.com.au

Alexander Rau
KPMGカナダ
alexanderrau@kpmg.ca

Hemal P Shah
KPMG米国
hpshah@kpmg.com

Marko Vogel
KPMGドイツ
mvogel@kpmg.com

アライアンス協力者：

Ben de Bont
CISO
ServiceNow

Chris Corde
Senior Director
Google Cloud Security Products
Google

Sitaram Iyer
Area VP
Emerging Technologies
Palo Alto Networks

Saira Mohammed
Chief Security Advisor
Microsoft

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

お問合せ先

KPMGコンサルティング株式会社

T : 03-3548-5111

E : kc@jp.kpmg.com

kpmg.com/jp/kc

本レポートで紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。

本レポートの一部の画像は、人工知能技術を使用して作成されています。

本レポートは、KPMGインターナショナルが2026年3月に発行した「Cybersecurity Considerations 2026 : Building trust and enabling innovation in a dynamic world」を、KPMGインターナショナルの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査したうえで提案する適切なアドバイスをもとにご判断ください。

KPMGは、グローバル組織、またはKPMG International Limited（「KPMGインターナショナル」）の1つ以上のメンバーファームを指し、それぞれが別個の法人です。 KPMG International Limitedは英国の保証有限責任会社（private English company limited by guarantee）です。KPMG International Limitedおよびその関連事業体は、クライアントに対していかなるサービスも提供していません。KPMGの組織体制の詳細については、kpmg.com/governanceをご覧ください。

本レポートにおいて、「私たち」および「KPMG」はグローバル組織またはKPMG International Limited（「KPMGインターナショナル」）の1つ以上のメンバーファームを指し、それぞれが独立した法人です。

文中の社名は各社の商標または登録商標である場合があります。本文中では、Copyright、TM、Rマーク等は省略しています。

© 2026 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

© 2026 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. C26-1019

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Designed by Evalueserve.

Designed by Evalueserve. Publication name: Cybersecurity considerations 2026 | Publication number: 140420-G | Publication date: March 2026