Gartner

AI 時代のサイバーセキュリティ戦略：将来に向けた展望と実践ガイド

混乱を最小限に抑え、リスク・マネジメントを行いながら、AI の価値を活用する

ハイプ（過熱状態）から脱却し、サイバーセキュリティにおける AI の価値を最大化する

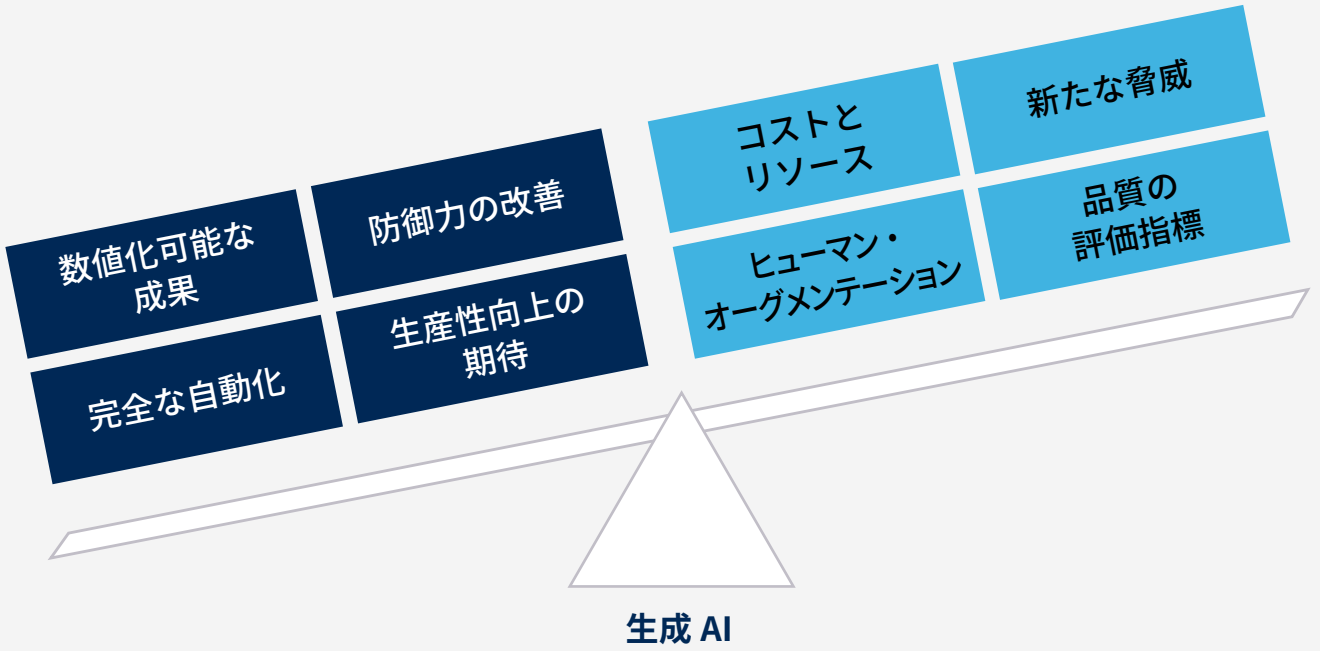
現在、AI や生成 AI を取り巻くビジネスは依然として過熱しており、多くの企業がその導入や活用を模索しています。一方で、サイバーセキュリティの観点から見ると、新たなリスクや課題が浮かび上がっています。さらに現時点で、AI は当初期待された成果を十分に発揮できていない状況です。

しかし、これを単なる混乱と捉えるのではなく、適切な戦略を講じることで、AI がもたらす可能性を最大限に引き出し、「昨日の混乱は明日の機会」となり得ます。ハイプを超えた先には、AI の価値を活用するための確かな可能性が秘められています。

AI には、セキュリティを含む組織のオペレーション方法を変革する力があり、将来的にはそれを実現していくでしょう。このような状況下で、AI の課題がより明確になり、その応用が徐々に成熟していく中、サイバーセキュリティ・リーダーとして、以下のような注力すべき重要な 4 つの方向性が見えています。

- AI の影響が及ぶ範囲を最適化する
- 主要なリスク領域に優先順位を付ける
- AI の価値を最大限に高める
- 将来の変化に備える

「サイバーセキュリティの現実」と「生成 AI への期待」のバランスを取る



出典：Gartner

AI の影響が及ぶ範囲を最適化する

Gartner の分析によると、**企業の 90% 近くが**依然として生成 AI を調査中または試験導入中であり、そのほとんどが AI TRiSM (トラスト／リスク／セキュリティ・マネジメント) のテクニカル・コントロールやポリシーを整備できていない状況にあります。そのため、セキュリティ対策の見直しが求められています。企業や組織が直面するリスクは右のように分類できます。

直接的かつ緊急性が高い

- 即座の対応を必要とする現実の問題で、具体的には、サードパーティのアプリケーションにおける機密データの管理・制御が不十分な状況
- 著作権侵害と、それに伴うブランドへの損害

直接的で、緊急性が高いと過度に騒がれる

- 生成 AI への関心を喚起するために過度に強調された初期の発表

間接的だが、不安を喚起する

- プライバシー・リスクや攻撃者に対する懸念
- ビジネス・プラクティスの混乱から生じる新たなアタック・サーフェス (攻撃対象範囲)

間接的で、潜在的

- セキュリティの適応を絶えず必要とする継続的な生成 AI の採用
- セキュリティ・チームの備えを必要とする今後の規制要件やコンプライアンス要件
- 将来的なスキル・ギャップと人材確保の課題に関する不確実性

AI 戦略に必要なガバナンスとリスク管理の方向性を定める

生成 AI へと舵を切るにあたっては、新しいガバナンス原則の策定、もしくは既存原則の修正が必要となります。同時に、AI に焦点を当てた、明確なサイバーセキュリティのロードマップを構築することも不可欠です。

AI ガバナンスの対象範囲は組織の AI 成熟度によって異なりますが、どの組織でも、以下の 3 つのロードマップに同時進行で注力する必要があります。

1. **AI に対応したアプリケーション・セキュリティ戦略にする**
   従来型の安全な開発プラクティスを継続的に実施すると同時に、開発サイクル全体にわたって実行時における新たなアタック・サーフェスを保護する。プライバシーを強化するテクノロジを実装し、アプリケーション・セキュリティにおける新たな生成 AI 手法を評価する
2. **新しい AI テクノロジをサイバーセキュリティに統合する**
   3 年間のロードマップを策定する際には、現在の AI テクノロジの影響だけでなく、将来的な AI テクノロジの発展による影響も考慮に入れる
3. **AI に関する検討事項をリスク・マネジメント・プログラムに組み込む**
   スキル要件と同様に、評価指標、リスク・レジスタ、脅威にさらされるリスクも進化することを把握する

サイバーセキュリティ・リーダーが生成 AI の活用に対して抱いているリスク関連の懸念事項トップ 3：

- 機密データへのサードパーティによるアクセス
- 生成 AI アプリケーション／データへの侵害
- 誤った意思決定

出典：Gartner

AI のトラスト／リスク／セキュリティ・マネジメント (AI TRiSM) ソリューションを実装する

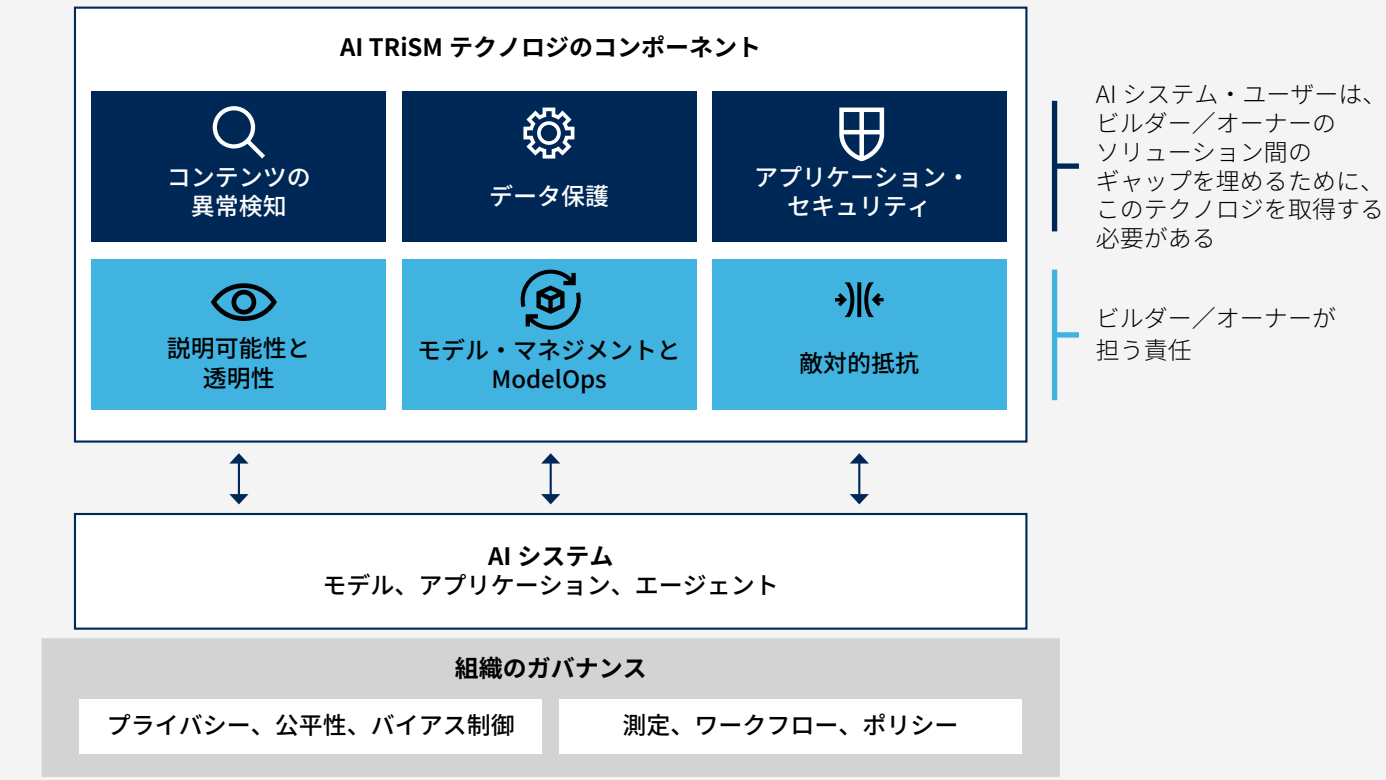
現在、多くの組織が外部でホストされる大規模言語モデル (LLM) や他の生成 AI モデルを活用しようとしています。しかし、これらの外部 AI モデルを利用する場合、組織はアプリケーション・プロセス、データ処理、およびストレージを直接制御することができないため、さまざまなリスクが増大することになります。

これらのリスクが外部の AI モデルに限らず、組織が自社内でホストし管理するオンプレミスのモデルにも存在するため、適切なセキュリティ管理やリスク管理が行われていない場合、そのリスクは顕著となります。

AI TRiSM (AI のトラスト／リスク／セキュリティ・マネジメント) を用いてリスク・マネジメントを行う必要があります。AI TRiSM は継続的な管理と信頼性確保のための制御機能を提供するフレームワークであり、主に以下の重要な領域をカバーしています。

1. コンテンツの異常検知
2. データのガバナンスと保護
3. アプリケーションのセキュリティ・リスクの低減

AI TRiSM (AI のトラスト／リスク／セキュリティ・マネジメント) テクノロジ



出典：Gartner

生成 AI アプリケーションの保護を優先する

まず、生成 AI アプリケーションのセキュリティを確保する前に、基盤となるインフラストラクチャのセキュリティを確実にする必要があります。これには、Web、SaaS (サービスとしてのソフトウェア)、クラウド IaaS (サービスとしてのクラウド・インフラストラクチャ)、PaaS (サービスとしてのプラットフォーム) といった基本的なプラットフォームに対するセキュリティ管理の確立が含まれます。この基盤が整った上で、生成 AI アプリケーションのセキュリティ確保に向けた具体的な対策を実施していきます。

Web ／ SaaS アプリケーションの利用

- ☐ 生成 AI の許容可能な使用方法に関するポリシー (AUP)
- ☐ SaaS アプリケーションの検証／承認／オンボーディングに必要なセキュリティ要件のチェックリスト
- ☐ パブリック・クラウドで機密データを保護する方法に関するデータ・セキュリティ基準
- ☐ Web や SaaS の利用を保護するセキュリティ・サービス・エッジ (SSE) プロダクト

クラウド・ホスト型エンタプライズ・アプリケーション

- ☐ パブリック・クラウドの利用を保護する方法に関するセキュリティ基準
- ☐ クラウド／ Web アプリケーションのセキュリティ・テクノロジ
- ☐ カスタム構築アプリケーションの保護機能
- ☐ 人間だけが生成 AI アプリケーションを利用できるようにするボット検知機能
- ☐ 内／外向けの API エンドポイントを保護する機能

3 つの重要なリスク領域に焦点を絞る

生成 AI は、効率性や生産性の向上をはじめ、さまざまなメリットをもたらすと期待されています。一方で、生成 AI の普及に伴い、新たなセキュリティリスクが発生しています。特に、右の 3 つの領域においてリスク管理が求められます。

コンテンツの異常検知

- 不適切または悪意のある使用
- ハルシネーション (虚偽の出力)
- 不正確性、違法性、著作権侵害など損害を与える出力

データの保護

- データ漏洩
- コンテンツやユーザー・データの侵害
- プライバシー／データ保護に関するポリシーのガバナンス
- プライバシー・インパクト・アセスメント
- 地域ごとの規制コンプライアンス

アプリケーション・セキュリティ

- 敵対的なプロンプト攻撃
- ベクトル・データベース攻撃
- ハッカーによる不正アクセス

AI TRiSM の取り組みについて方向性を定める

AI TRiSM は組織全体での協調的な取り組みとして捉える必要があります。AI、セキュリティ、コンプライアンス、オペレーションの担当者が連携して新たな AI TRiSM 対策を実装すべきです。具体的な取り組みを開始するにあたっては、いくつかの重要なアクションを起こすことから始めます。

- [ ] AI TRiSM の取り組みを管理する組織的なタスクフォースまたは専任チームを設置する
- [ ] 組織全体で協力して、包括的な AI TRiSM プログラムの一環として、最適なツールセットの管理を行う
- [ ] 許容可能な使用方法に関するポリシー (AUP: Acceptable Use Policies) を策定する。ユーザーの申請／文書利用を体系的に記録および承認するシステムを確立する
- [ ] 設定した目標に照らして継続的に利用状況を監視し、継続的に利用パラメータを調整する

2026 年までに、AI アプリケーションに TRiSM コントロールを適用する企業は、誤った意思決定につながる不正確あるいは不正な情報の利用を、少なくとも **50% 排除**できるようになる

出典：Gartner

CIO が生成 AI の可能性を最大限に引き出すには

生成 AI は、セキュリティやビジネス・プロセス全般に変革をもたらすと期待されています。しかし、その可能性を最大限に活用するためには、CIO として以下のような戦略的なアプローチが必要となります。

- ☐ サードパーティの生成 AI アプリケーション／機能の**利用状況を把握し、監視／管理を行う**
- ☐ プライバシー、著作権、トレーサビリティ (追跡可能性)、説明可能性に関する課題に対処するために、**テクノロジ・プロバイダーの選定要件を更新する**
- ☐ 新たなアタック・サーフェスを保護対象として組み込むために、**AI のアプリケーション／データに関するセキュリティ・プラクティスを更新する**
- ☐ **生成 AI をサイバーセキュリティ・プログラムに組み込む前に概念実証 (PoC) を実行し、**人間の作業を完全に置き換えるのではなく、補完／強化することを目指す
- ☐ 既存のセキュリティ・コントロールの検知精度やパフォーマンスの低下など、**脅威環境の変化を監視する。**変化する脅威環境について適切な情報にアクセスできるようにする。将来の生成 AI 攻撃に対するシナリオ・プランニングは、必ずしもリソースの最適な活用方法とは限らないため、慎重に検討する

2025 年末までに、生成 AI の安全性を確保するために必要とされるサイバーセキュリティのリソースが急増し、**アプリケーションおよびデータのセキュリティへの支出が 15% 以上増加する**

出典：Gartner

CISO が生成 AI の可能性を最大限に引き出すには

CISO は、生成 AI の価値を最大限に高めるために、以下を優先すべきです。

- 機密データに新たなリスクが生じるかどうかを評価するために、**生成 AI テクノロジを他のツールと同様に評価する**
- **「良い状態」とは何かを明確に定義し、**既存のセキュリティ評価指標を AI によってどのように改善できるかを見極める。この際、新しい評価指標を追加することは避け、既存の指標の改善に焦点を当てることで、評価の複雑化を防ぐ
- **既存のセキュリティ・プロバイダーが提供する新機能で実験を行う。**まずは、セキュリティ・オペレーションとアプリケーション・セキュリティの領域で、限定的かつ具体的なユースケースから着手する
- 大規模言語モデル (LLM) と生成 AI を活用する新しいファーストパーティ／サードパーティ・アプリケーションを開発／利用する場合には、**AI TRiSM フレームワークを適用する**
- 組織全体の生成 AI 利用から生じる直接的な影響 (プライバシー、IP、AI アプリケーションのセキュリティに対する影響) と、間接的な影響 (人事／財務／調達など生成 AI を利用する他のチームへの影響) に対処できるように、**チームの態勢を整え、トレーニングを実施する**

2028 年までに、生成オーグメントを採用することでスキルのギャップが解消され、**エントリ・レベルのサイバーセキュリティ職の 50% は専門教育を受ける必要性がなくなる**

出典：Gartner

AI の価値を最大限に活用するために サイバーセキュリティ戦略の方向性を定める

次に取るべきステップは以下のとおりです。

- ☐ AI テクノロジの評価と組織にとっての「理想的な状態」の定義を**明確にする**
- ☐ 不確実で曖昧な脅威に対する優れた検知／対応能力を**維持し、改良する**
- ☐ 最も関連性の高い脅威を特定するためにエクスポージャ管理と脅威インテリジェンスに**投資する**

組織の **3 分の 1 (34%)** は、
1 年以内に生成 AI を導入する
計画を立てている

出典：Gartner

AI 戦略／実装計画の策定を成功させるために重要なリーダーシップの役割

CIO ／テクノロジ責任者

CIO は、CEO ／同僚／取締役会から、正式な AI 戦略の策定や AI リーダーの指名のほか、具体的には以下を成功させることを期待されています。

- AI に関する全社レベルの目標を設定し、ユースケースを特定し、メリットとリスクを数値化する
- ビジネス・チームとテクノロジ・チームの連携を図り、AI をサポートするための組織の能力を変革する
- アイデアを取りまとめ、イノベーションの促進を担う AI リーダーを指名する

CISO (最高情報セキュリティ責任者) またはセキュリティのリーダー + チーム

サイバーセキュリティとデータ・プライバシーが AI 戦略の不可欠な要素として組み込まれるようにし、以下のような役割を期待されています。

- セキュリティとリスクに関するプログラム全体を監督する
- データ漏洩や著作権侵害などの不測の事態を予測し、対策を講じる
- 新たな脅威に対抗するためのスキルと準備態勢を継続的に更新する

CDAO (最高データ分析責任者) またはデータ／アナリティクス (D&A) のリーダー + チーム

AI 戦略のためのデータ整備において組織を主導すること、そして以下のような役割を期待されています。

- 拡張アナリティクスとデータ管理に関する AI ユースケースを特定する
- 既存の D&A プラクティスを活用し、AI に関する D&A ガバナンス・ポリシーを策定する
- AI を活用して新しいデータの価値を開発し、組織が AI データを効果的に活用できる準備を整える
- AI-Ready のデータに対応できるようになる

エンタプライズ・アーキテクチャ (EA) のリーダー + チーム

AI から具体的なビジネス価値を引き出すこと、そして以下のような役割を期待されています。

- AI インフラストラクチャのロードマップ全体のオーナーシップを持つ
- AI テクノロジ・アーキテクチャの投資判断についてのカバナンスを担う
- ビジネス成果を推進するための AI ソリューションの採用に関する意思決定を主導する

ソフトウェア・エンジニアリングのリーダー + チーム

AI テクノロジの影響を深く理解し、以下のような役割を期待されています。

- AI 統合に関する望ましいビジネス成果を明確にする
- 組織全体で AI エンジニアリングのベスト・プラクティスを確立する
- プロダクト／サービス／ユーザー体験を変革し、AI ファーストのアプローチをロードマップに組み込む

Gartner の調査結果から、**AI の価値ある成果に向けて、組織のリーダーの各役割が効果的に行動を起こせるようになるための知見**

	1 ビジネス目標と整合する AI 目標を確立する	2 ユースケースを選定し、テストを展開する	3 テクノロジやビジネス・オペレーションに AI を組み込む
CIO ／テクノロジ責任者	Gartner のベスト・プラクティスに従って、最も大きな影響をもたらすビジネス指標を選定し、**AI の取り組みの焦点を慎重に定める**	潜在的なビジネス価値と実現可能性に基づいて**パイロット・プロジェクトを整理し、**戦略的目標を実現しながら破壊的イノベーションの可能性を追求する	専任のリーダーシップ、適切に割り当てられたリソースと資金、ガードレール、ガバナンスを伴うイノベーション・プラクティスを確立することで、**企業全体の AI 採用を主導する**
CISO またはセキュリティのリーダー＋チーム	AI 行動モデルを用いて脅威検知能力を改善させ、**高度な攻撃者に対して先手を打ち続ける**	Gartner の「サイバーセキュリティのための AI プリズム」を活用し、実現可能性とリスク軽減に基づいて **AI の最適なユースケースを特定する**	AI 開発の各段階でサイバーセキュリティの考慮事項を評価するチームと協力することで、**AI リスクをより効果的に管理する**
CDAO またはデータ／アナリティクス (D&A) のリーダー＋チーム	特定の KPI に対する AI の期待値を定量化し、監視のための先行指標と遅行指標を確立することで、**方向性の一致を推進する**	ビジネス価値のどの側面に注力するかを選定し、ユースケースを改良し、エンゲージメントと意思決定を促進することで、**より効果的にユースケースの優先順位付けを行う**	部門横断的なチームをデータ専門家で補強し、最適な手法を利用し、技術的負債を抑制することで、**AI のデリバリを効率的に推進する**
エンタプライズ・アーキテクチャ (EA) のリーダー＋チーム	より深く調査すべき領域を特定し、AI 活用の計画と戦略を策定することで、**効果的な AI エコシステムを構築する**	Gartner が提唱する最適な AI インフラストラクチャのための 4 ステップのケイパビリティ・モデリング・アプローチを活用して、**AI イニシアティブを戦略的に計画する**	Gartner が提唱する AI 実行に対する 5 段階のアプローチに従うことで、**目標のビジネス成果を実現し、失敗を回避する**
ソフトウェア・エンジニアリングのリーダー＋チーム	AI 拡張型ソフトウェア・エンジニアリングのプラクティスを採用することで、**ワールドクラスのアプリケーション開発オペレーションを実現する**	AI の適用可能性と適用効果が最も高いソフトウェア・テスト領域 (視覚テストなど) を特定することで、**AI の価値を最大限に高める**	人間の専門家と生成 AI を組み合わせてソリューション領域の調査と理解を改善することで、**画期的なアイデアを生み出す**

実用的で客観的な知見

各種のリソース／ツールを無償でご利用いただけます。

Insights

セキュリティ・ガバナンス (集約と分散) の進め方

セキュリティ侵害のインシデントはいつ発生してもおかしくない状況であり、企業はインシデントに備えた取り組みを今すぐに開始する必要があります。

Tool

Gartner Cybersecurity Business Value Benchmark (英語)

同業他社との比較、リスクの軽減、ビジネス目標の達成に役立つ、新しく標準化された測定基準を確認することができます。

Insights

ランサムウェア対策は事前の準備が 9 割：正しい準備とは

感染した後に「やっておけばよかった」と後悔する抜けや漏れに気付き、ランサムウェア対策の改善を図る方法について解説します。

Webinar

情報漏えい対策の最新トレンド：AI 時代に向けて押さえるべき 3 つのポイント

企業がデータ保護やアクセス管理について知っておくべきセキュリティの基本や、最新のトレンドを、推奨事項と共に解説します。

Gartner が提供するその他の AI 関連の知見：

生成 AI 導入プラン策定のためのワークブック

AI の活用機会を理解する - 成功に向けて IT チームの準備を整える

生成 AI とは？

AI TRiSM (AI のトラスト／リスク／セキュリティ・マネジメント) とは？

Gartner のお客様は、クライアント・ポータルでさらに多くのリソースをご利用いただけます。ログイン

Gartner

Gartner のコンファレンスに参加して、AI 戦略を前進させましょう

AI の機会やリスクの伝達／戦略策定／試験運用／規模拡大を行う方法や、企業のソフトウェア／人材／スキル／リスク／信頼／ガバナンスに及ぼす AI の影響を管理する方法について、参加者同士で貴重な知見を共有できます。

ぜひご参加ください

今すぐコンファレンス・カレンダーで、
ご自身に最適なコンファレンスをご確認ください。

→ **セキュリティ＆リスク関連のコンファレンスを確認する**

→ **CIO ＆ IT エグゼクティブ関連のコンファレンスを確認する**







Connect With Us

Gartner は、お客様のミッション・クリティカルな課題について、
より優れた意思決定と大きな成果へと導く実行可能かつ客観的な
知見を提供します。

リサーチ・サービスに関するお問い合わせ

サイバーセキュリティ・リーダーを成功に導く Gartner のサービス
gartner.co.jp/ja/cybersecurity

最新の知見をご確認ください

Gartner のコンファレンスにご参加ください
コンファレンスの最新情報を見る

Gartner®