Gartner

2026 年の戦略的テクノロジ・トレンドのトップ 10

AI を原動力とするハイパーコネクテッド型の世界で舵を取る

2026 年、テクノロジ・リーダーは、ディスラプション (破壊)、イノベーション (革新)、リスクがかつてないスピードで加速する転換点の年を迎えます。Gartner の 2026 年の戦略的テクノロジ・トレンドのトップ 10 は、単なるテクノロジのトレンドではなく、ビジネス変革を促すきっかけとなり、C レベル幹部による対応を求めるものです。

2026 年のトレンドは、単一の能力では対応しきれない、AI が前提となるハイパーコネクテッド型な世界の現実を映し出しています。これらのトレンドは、先進的な企業や組織がどのように革新を起こし、競争し、価値を守るかを示す 3 つのテーマに整理できます。

アーキテクト

AI ネイティブ開発プラットフォーム、AI スーパーコンピューティング、コンフィデンシャル・コンピューティングにより、セキュアでスケーラブルかつ適応性の高いデジタル基盤を構築する。

シンセシスト

マルチエージェント・システム、ドメイン特化言語モデル、フィジカル AI に至るまで、多様なテクノロジをオーケストレーションし、新たな価値の源泉を切り拓く。

ヴァンガード

先制的サイバーセキュリティ、デジタル属性、AI セキュリティ・プラットフォーム、ジオパトリエーションを通じて、信頼を高め、ガバナンスとセキュリティを強化する。

本 eBook を読み進める中で、これらのトレンドが自社の戦略的目標にどのように整合し、持続可能な成長と競争優位性を生み出すための計画にどのように組み込むことができるかをご検討ください。

Gene Alvarez
Distinguished Vice President,
Business and Technology Insights, Gartner

2026 年の戦略的テクノロジのトップ・トレンド

Gartner は、AI を原動力とするハイパーコネクテッド型の世界において、イノベーションを促進し、レジリエンスを強化し、信頼を高める潜在力を基準に、これらの 10 のトレンドを選定しました。

これらは戦略上の緊急課題であり、テクノロジ・リーダーの熟考と断固たる意思決定／アクションを必要とします。

● **現在**
(1～3年未満)

○ **近未来**
(3～5年未満)

アーキテクト

1. AI ネイティブ開発プラットフォーム
2. AI スーパーコンピューティング・プラットフォーム
3. コンフィデンシャル・コンピューティング

シンセシスト

4. マルチエージェント・システム
5. ドメイン特化言語モデル
6. フィジカル AI

ヴァンガード

7. 先制的サイバーセキュリティ
8. デジタル属性
9. AI セキュリティ・プラットフォーム
10. ジオパトリエーション

アーキテクト

セキュアでスケーラブルかつ適応性の高いデジタル基盤を構築する

テクノロジ・リーダーは、イノベーションとレジリエンスを加速させるために、プラットフォームとインフラストラクチャの近代化に取り組む必要があります。「アーキテクト」に分類されるトレンドは、AI を原動力とするハイパーコネクテッド型の世界で成功するために不可欠な、スピード／セキュリティ／スケーラビリティを実現する AI-Ready なデジタル基盤の構築に重点を置きます。

1 AI ネイティブ開発プラットフォーム

どのようなものか

生成 AI を活用して、これまでになく簡単かつ高速にソフトウェアを開発できるプラットフォームです。単一のプロンプトからコードを生成する「単発」型のツールから、深い技術知識がなくても開発を可能にする「バイブ・コーディング」型のツール、さらに複数の AI エージェントを連携させてソフトウェアを作り上げる仕組みまで、幅広い形態が含まれます。

注目されている理由

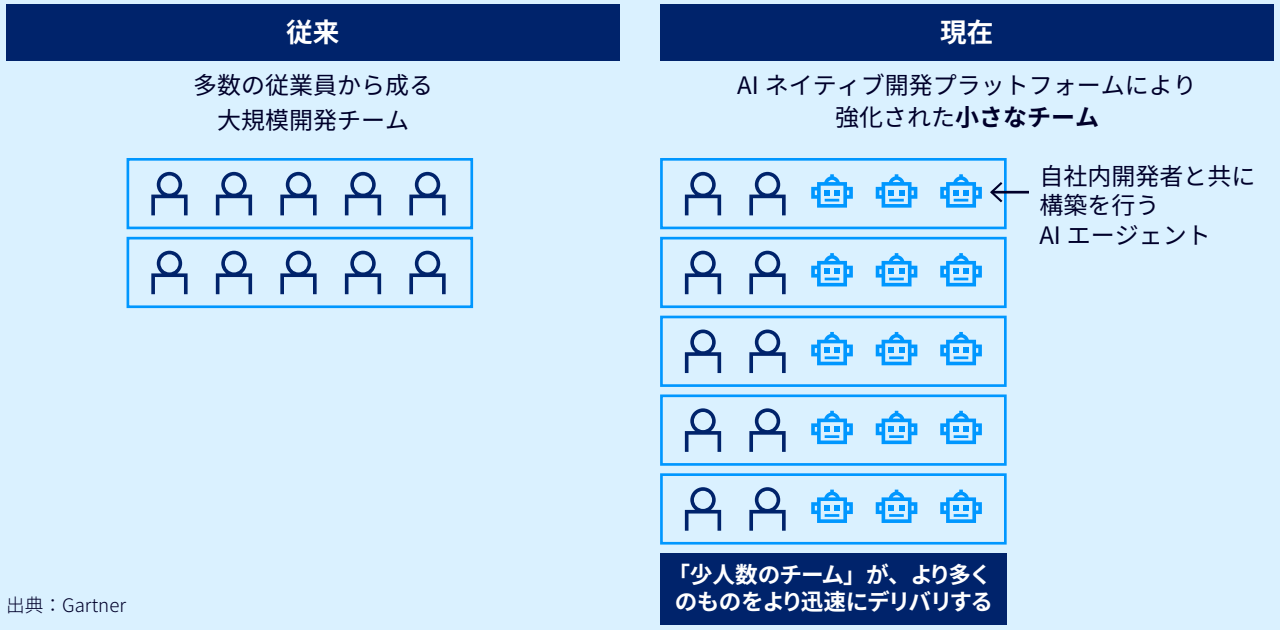
CIO (最高情報責任者) はソフトウェアの迅速なデリバリと生産性の向上を期待しており、また CEO (最高経営責任者) や CFO (最高財務責任者) もコスト削減効果に注目しています。AI ネイティブ開発プラットフォームは、「少人数のチーム」が同じリソースでより多くのアプリケーションを構築できるようにします。例えば、2 人ずつの 5 チームで、同時に 5 つのアプリケーションを構築できるイメージです。このトレンドによって、CIO が開発バックログの解消を進めるようになり、「自社開発か購入か」のバランスを、自社開発側にシフトさせることができます。

今後の動向

80% の組織が、2030 年までに、大規模なソフトウェア・エンジニアリング・チームを、AI によって増強されたより小規模なチームへ移行させるようになる。

40% のエンタプライズ・アプリケーション・ポートフォリオが、2030 年までに、AI ネイティブ・プラットフォームを使って構築されたカスタム・アプリケーションを含むようになる (2025 年時点の 2%から増加)。

小さなチーム



出典：Gartner

1

AI ネイティブ開発プラットフォームで成果を出す

スピードを向上し、コストを削減し、イノベーションを促進するためのアクション・プラン

ステップ	1 プラットフォーム・チームを設置する	2 セキュリティ・ガードレールを導入する	3 AI ネイティブ開発を試験運用する	4 AI ファーストのマインドセットを根付かせる	5 組織のスキルを高め、チームを強化する
期待される成果	中央集約された管理により、一貫した基準とガバナンスを確保できる。	セキュアでないコードやコンプライアンスに反するコードのリスクを低減できる。	短期的な成果による価値を示し、信頼を高める。	デリバリを加速し、イノベーション能力を向上させる。	全社的な浸透を進め、関係者と円滑に連携できる。
アクション	AI ネイティブ・プラットフォームを管理し、AI モデルを選定する専任チームを編成する。	コード・レビューとコンプライアンス・チェックのために AI ガバナンス・プラットフォームを統合する。	低リスクのプロジェクトから開始し、生産性の向上を検証する。	新たな開発案件では、AI ネイティブ・ツールを優先させる。	プロンプト・エンジニアリングとガバナンスについて、開発者とビジネス・パートナーをトレーニングする。

導入の成功を支える主要プレーヤー

CIO

連携：AI ファーストな戦略とガバナンスの枠組みを定義する。

協力：プラットフォームの能力をビジネス優先課題に整合させる。

ガバナンス：AI ネイティブ開発のためのコンプライアンスとセキュリティ・ガードレールを確保する。

IT パートナー

プラットフォーム・エンジニアリング：AI ネイティブ・ツール、統合、パフォーマンスを管理する。

セキュリティ：コード・レビューとリスク・マネジメントのために AI ガバナンスを導入する。

調達：AI ネイティブ・プラットフォームのベンダーとサービスを評価し、選定する。

ビジネス・パートナー

プロダクト・オーナー：領域の専門知識を提供し、AI 主導のソリューションを検証する。

財務：AI ネイティブ開発の取り組みを支援するために、資金提供モデルを調整する。

2

AI スーパーコンピューティング・プラットフォーム

どのようなものか

高度な AI モデルのトレーニングと実行に必要とされる大規模な処理能力を提供するプラットフォームです。高性能コンピューティング (HPC)、特殊プロセッサ、スケーラブルなアーキテクチャを組み合わせて、データ集約的なワークロードを処理します。

注目されている理由

従来のインフラストラクチャの限界を超える、より大規模で複雑な AI モデルが開発されるようになり、AI スーパーコンピューティングの需要が急増しています。

今後の動向

40% の企業が、2028 年までに、ハイブリッド型コンピューティングのアーキテクチャを採用するようになる (8% から増加)。

20 以上 を超えるベンダーが、2028 年までに、スーパーコンピューティング環境を活用する統一された開発者プラットフォームを提供するようになる。

AI スーパーコンピューティング・プラットフォーム

出典：Gartner

2

AI スーパーコンピューティング・プラットフォームで成果を出す

膨大な処理能力を引き出すためのアクション・プラン

ステップ	1 重要度の高いワークロードを特定する	2 統一されたソフトウェア・スタックに投資する	3 段階的な統合戦略を策定する	4 環境にわたって開発を効率化する	5 ガバナンスとコンプライアンスの計画を策定する
期待される成果	価値を実証し、自社内の知見とスキルを蓄積できる。	連携が簡素化され、柔軟なワークロード配置が可能になる。	将来に備えたインフラと人材体制を整備できる。	デリバリを加速し、摩擦や無駄を低減できる。	リスクを軽減し、管理／監督の質を向上させる。
アクション	ハイブリッド・オーケストレーションを使って、試験運用プロジェクトを実施する。	既存システムと先進システムの両方で、オープン・スタンダードを採用する。	新しいコンピューティング・パラダイムを徐々に導入し、IT スタッフを育成する。	ハイブリッド・プラットフォームとコンポーザブル・アーキテクチャの採用をチームに促す。	システム・レベルでセキュリティ／コンプライアンス戦略を策定する。

導入の成功を支える主要プレーヤー

CIO

定義：ビジネス優先課題に沿ったハイブリッド・オーケストレーション戦略を定義する。

確保：ワークロードの配置、セキュリティ、コンプライアンスのガバナンスを確保する。

協力：ビジネス・リーダーと協力し、重要度の高いワークロードを優先させる。

IT パートナー

インフラストラクチャ／オペレーション：先進のアクセラレータをレガシー・システムと統合する。

セキュリティ：マルチアーキテクチャ環境のガバナンスを導入する。

DevOps：統一されたソフトウェア・スタックとオーケストレーション・ツールを採用する。

ビジネス・パートナー

プロダクト：ハイブリッド・コンピューティングのユースケースを特定する (シミュレーション、AI 対応アプリなど)。

財務：段階的な統合と持続可能性の目標のために資金提供を調整する。

オペレーション：重要な業務プロセスにおける AI 主導のワークフローに向けて準備する。

3

コンフィデンシャル・コンピューティング

どのようなものか

ハードウェア・ベースの信頼できる実行環境 (TEE) を使用して、処理中のデータを保護し、クラウド・プロバイダーも含めて不正アクセスを防止します。

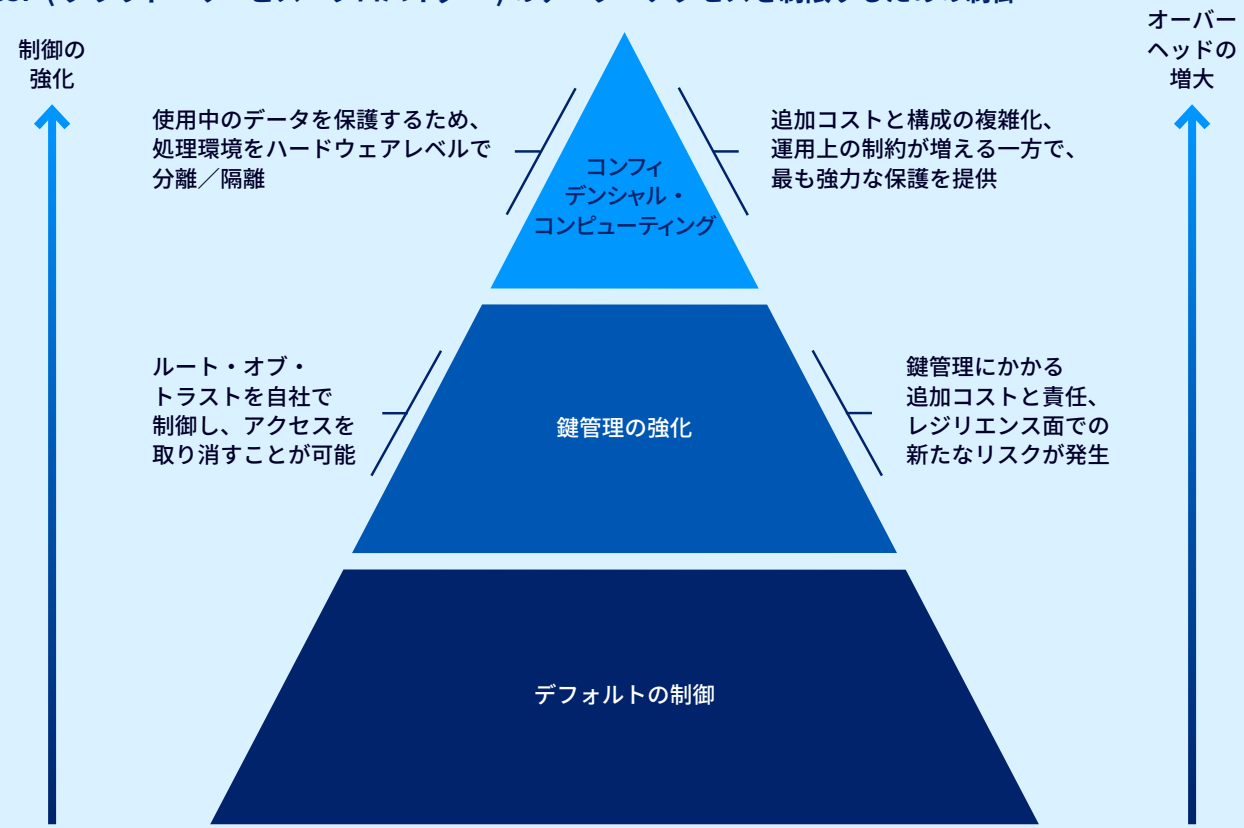
注目されている理由

個人情報保護法の厳格化、データのローカル化ルール、AI の採用により、使用中データの保護がこれまで以上に重要になっています。コンフィデンシャル・コンピューティングは、機密性の高いワークロードに対して、セキュアなクラウド戦略とコンプライアンスを両立させる手段となります。

今後の動向

75% の信頼されていないインフラストラクチャでの処理が、2029 年までに、コンフィデンシャル・コンピューティングによって保護されるようになる。

CSP (クラウド・サービス・プロバイダー) のデータ・アクセスを制限するための制御



出典：Gartner

3

コンフィデンシャル・コンピューティングで成果を出す

あらゆる環境でセキュアかつコンプライアンスに準拠したデータ処理を実現するアクション・プラン

ステップ	1 機密性の高いワークロードを監査する	2 AI モデル向けに TEE を試験運用する	3 セキュアなコラボレーションを実現する	4 独立した鍵管理を確立する	5 統合の課題に備える
期待される成果	使用中データの保護が必要な領域を特定できる。	機密保持と知的財産保護を強化できる。	未加工データを公開することなく、インサイトのみを共有できる。	データ・アクセスを自社で完全に制御できる。	異なる環境間でも円滑に展開できる。
アクション	プライバシー法／データの現地化ルールの対象となるワークロードを洗い出す。	自社独自モデルとオープンソース AI モデルの双方で、TEE をテストする。	アナリティクス／ BI プロジェクトにコンフィデンシャル・コンピューティングを適用する。	自社が所有／管理する暗号鍵システムを導入する。	複数のチップセット／クラウド・プロバイダーにまたがるオーケストレーションを計画する。

導入の成功を支える主要プレーヤー

CIO

定義：プライバシー、コンプライアンス、クラウドの目標に沿ったコンフィデンシャル・コンピューティング戦略を定義する。

協力：法務／コンプライアンス・チームと連携し、データの現地化や主権の要件への対応を進める。

監督：TEE のガバナンスを統括し、既存のセキュリティ・フレームワークとの統合を確実にする。

IT パートナー

インフラストラクチャ／オペレーション：ハイブリッド環境やマルチクラウド環境にわたって TEE を展開する。

セキュリティ：認証プロセスと暗号鍵管理のガバナンスを導入する。

DevOps とプラットフォーム：コンフィデンシャル・コンピューティングにワークロードを適応させ、パフォーマンスを継続的にモニタリングする。

ビジネス・パートナー

コンプライアンス：規制上の義務の遵守と監査準備状況を検証する。

財務：コンフィデンシャル・コンピューティングの導入とリスク軽減のために資金提供を調整する。

データ・オーナー：使用中のデータ保護のために機密性の高いワークロードを特定し、優先度の高いプロジェクトを選定する。

シンセシスト

新たな価値創出に向けて多様なテクノロジをオーケストレーションする

新たな差別化の源泉を切り拓くために、テクノロジ・リーダーは専門モデル、マルチエージェント・システム、フィジカル AI を統合して、ドメインに特化したソリューションを提供する必要があります。「シンセシスト」に分類されるトレンドは、ワークフロー、プロダクト、エクスペリエンスにわたってイノベーションを推進する、適応力のあるインテリジェントなエコシステムを構築するために、多様なテクノロジをオーケストレーションすることに重点を置きます。

4

マルチエージェント・システム (MAS)

どのようなものか

複数の専門特化した AI エージェントが役割分担し、互いの結果を受け渡しながら、一連の業務プロセスを完了させる仕組みです。それぞれのエージェントが特定のタスクを担当することで、モノリシックな AI ソリューションに比べて効率性と拡張性を大きく高めることができます。

注目されている理由

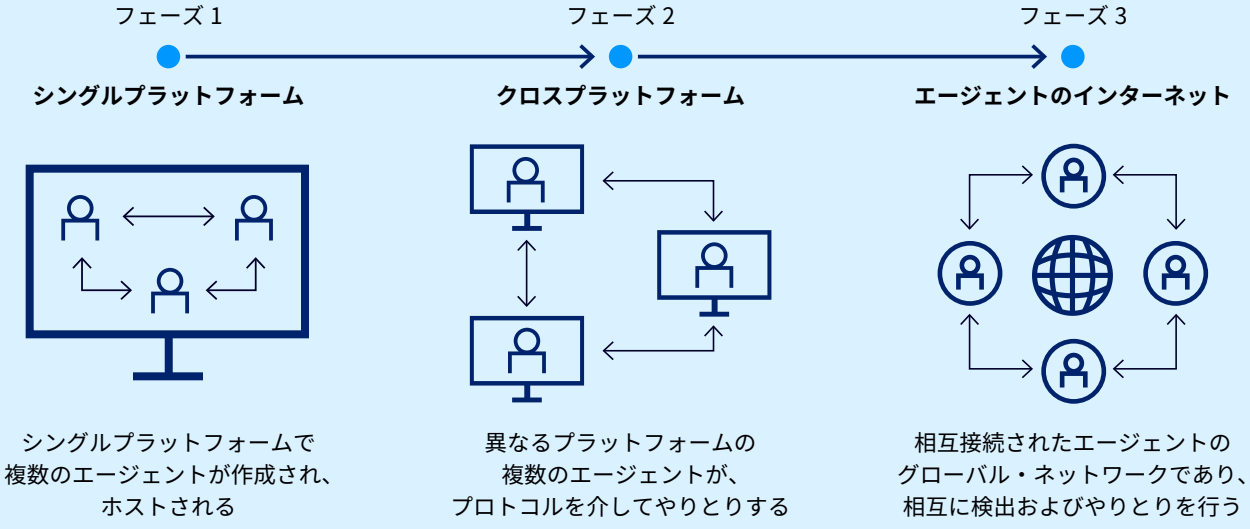
単一エージェント型の AI では、複数の工程にわたる処理が困難な一方で、MAS はモジュール型の自動化とクロスプラットフォームの統合を可能にします。 2024 年第 1 四半期から 2025 年第 2 四半期にかけて、MAS に関する問い合わせが 1,445% 急増し、企業の関心が急速に高まっていることがうかがえます。

今後の動向

70% の MAS が、2027 年までに、特定領域に特化したエージェントを使用するようになり、精度が向上する一方で、調整や連携の複雑さは増していく。

60% の MAS が、2028 年までに、マルチベンダー環境での相互運用性をサポートし、イノベーションと柔軟性を促進するようになる。

マルチエージェント・システムの進化



出典：Gartner

4

マルチエージェント・システム (MAS) で成果を出す

モジュール型の自動化とシームレスな統合を推進するためのアクション・プラン

ステップ	1 高付加価値のユースケースを特定する	2 モジュール型のエージェントを設計する	3 ガバナンスと可観測性を導入する	4 相互運用性の標準を採用する	5 チームのスキルを向上させる
期待される成果	影響を定量化し、導入スピードが速まる。	信頼性と拡張性が向上する。	リスクを軽減し、制御を向上させる。	将来を見据えた MAS 投資を実現できる。	効果的な導入を実現し、リスクを軽減できる。
アクション	MAS の試験運用のワークフローを明確にすることから開始する。	モノリシックなソリューションではなく、役割特化型のエージェント群として設計する。	強力な API ガバナンスとモニタリング・ツールを適用する。	マルチベンダー環境での、エージェント・コラボレーションを可能にする新しいプロトコルを使用する。	MAS のフレームワークとチェンジ・マネジメントについて、スタッフをトレーニングする。

導入の成功を支える主要プレーヤー

CIO

定義：高付加価値なワークフローを対象に MAS 戦略を定義し、ビジネス優先課題に整合させる。

確立：エージェントの相互運用性、セキュリティ、コンプライアンスのガバナンスを確立する。

伝達：従業員の懸念に対処するためのチェンジ・マネジメント計画を伝達する。

IT パートナー

プラットフォームと DevOps：モジュール型のエージェントを設計し、オーケストレーション・ツールを管理する。

セキュリティ：API のガバナンスを導入し、エージェント間のやり取りをモニタリングする。

統合チーム：相互運用性と可観測性を確保するための標準を採用する。

ビジネス・パートナー

プロセス・オーナー：MAS の試験運用のワークフローを特定し、結果を検証する。

財務：予測不可能なコストを管理し、可観測性ツールに資金を供給する。

オペレーション：人間とエージェントのコラボレーションとトレーニング施策のイニシアティブを支援する。

5 ドメイン特化言語モデル (DSLM)

どのようなものか
特定の業界や業務領域に特化したデータセットを使用してトレーニングした AI モデルであり、一般的な大規模言語モデル (LLM) よりも高い精度とコンプライアンスを実現します。

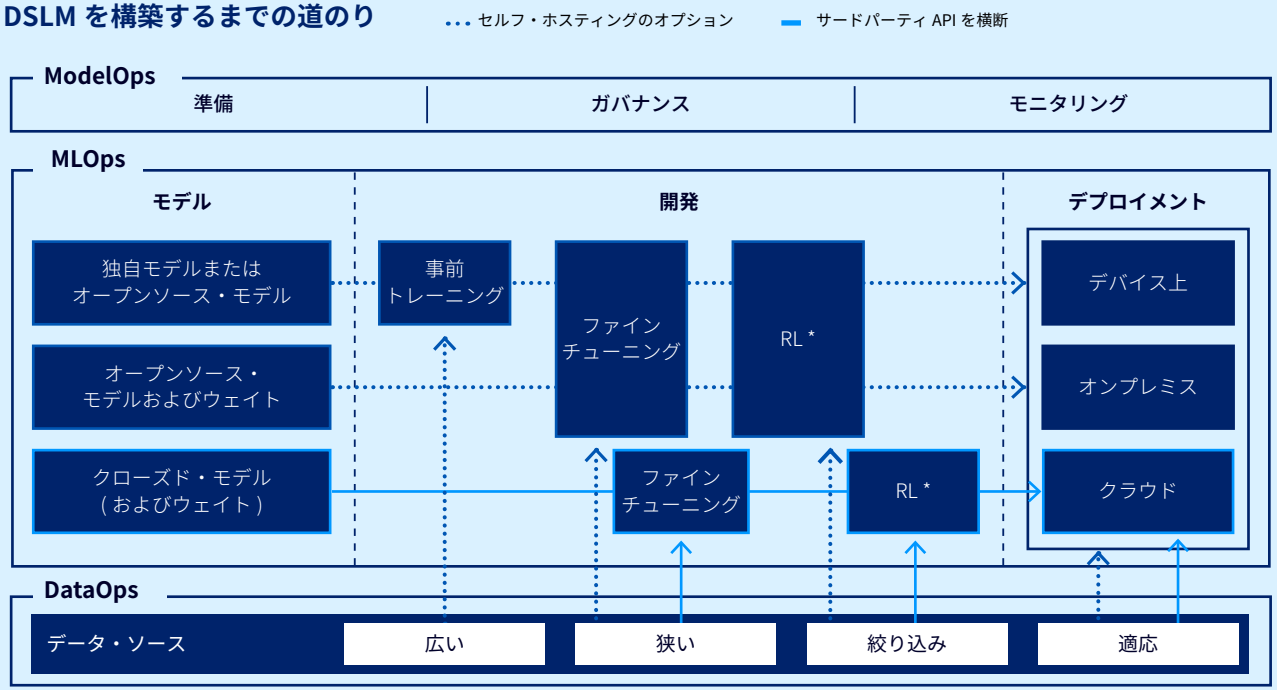
注目されている理由
CIO は、AI から得られるビジネス価値を定量的に証明できることを求められています。DSLM によって、金融、医療・ヘルスケア、人事などの重要なワークフローにおいて、エラーを減らし、導入を加速し、コストを削減できます。

今後の動向

50%以上 の生成 AI モデルが、2028 年までに、企業が使用するモデルの中でドメイン特化型になる。

30% の生成 AI ワークロードが、2028 年までに、オンプレミスまたはデバイス上で動作する DSLM で実行されるようになる。

DSLM を構築するまでの道のり



出典：Gartner

* 強化学習 (RL: Reinforcement Learning)

5

ドメイン特化言語モデル (DSLM) で成果を出す

業界に特化したコンプライアンスを的確に実現するためのアクション・プラン

ステップ	1 高い効果の得られるユースケースを特定する	2 データ・ガバナンスを強化する	3 重要なドメインでDSLM を試験運用する	4 部門横断型のチームを結成する	5 モニタリングし、最適化する
期待される成果	ROI を加速し、正確性を高める。	信頼性が高く、準拠したDSLM の出力を得る。	定量化可能なビジネス価値を実証できる。	スムーズな統合と導入を実現できる。	持続可能なパフォーマンスとコスト管理を実現できる。
アクション	一般的な LLM のパフォーマンスが低いワークフローを対象とする。	堅牢なプライバシー／品質管理を実施する。	財務、ヘルスケア、人事プロセスから開始する。	IT、領域専門家、コンプライアンスを DSLM プロジェクトに巻き込む。	説明可能性とコンプライアンスのフレームワークを適用する。

導入の成功を支える主要プレーヤー

CIO

定義：規制対象ドメインや高付加価値ドメインに対する DSLM 戦略を定義する。

確保：精度、コンプライアンス、説明可能性のガバナンスを確保する。

整合：DSLM の導入を ROI とリスク・マネジメントの目標に整合させる。

IT パートナー

データ／アナリティクス：ドメインに特化したデータセットを準備し、品質を維持する。

ModelOps：ファインチューニング、モニタリング、ライフサイクル全体のガバナンスを管理する。

セキュリティ：DSLM 本番環境におけるプライバシーとコンプライアンスを徹底させる。

ビジネス・パートナー

領域専門家：DSLM 出力の精度と業務への関連性を検証する。

財務：DSLM 導入とコスト最適化のための予算を確保する。

コンプライアンス：規制基準への遵守を徹底する。

6 フィジカル AI

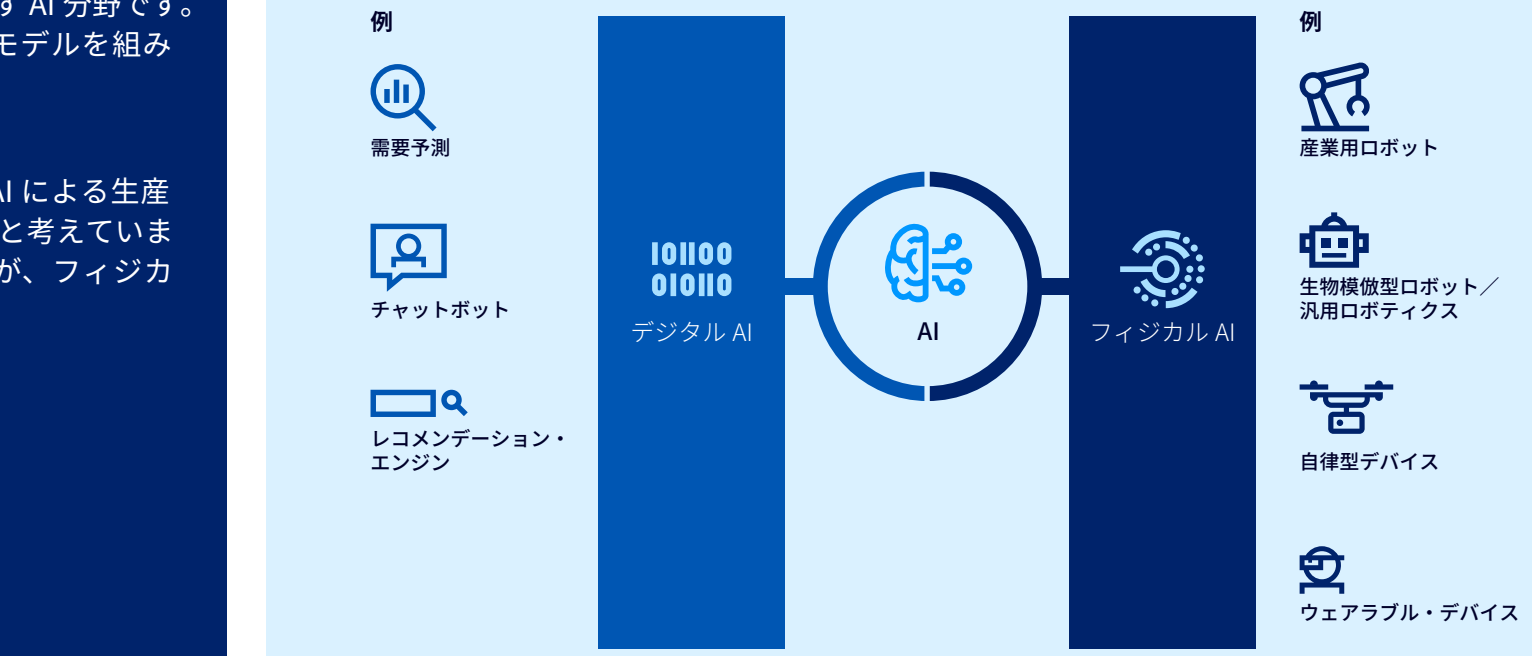
どのようなものか
検知・判断・行動するロボット／ドローン／車両／スマート・デバイスを通じて、現実世界にインテリジェンスをもたらす AI 分野です。これらのシステムは、センサ、アクチュエータ、AI モデルを組み合わせて、物理的なタスクを自動化します。

注目されている理由
多くの企業や組織が、デジタル領域で実現してきた AI による生産性向上を、工場や倉庫などの物理環境にも適用したいと考えています。2028 年までに、上位の AI ベンダー 10 社中 5 社が、フィジカル AI プロダクトを提供するようになります。

今後の動向

80% の倉庫で、2028 年までに、ロボティクスや自動化が使用されるようになる。

AI の分類



出典：Gartner

6

フィジカル AI で成果を出す

現場業務を自動化し、あらゆる場所で生産性を高めるためのアクション・プラン

ステップ	1 業務ドメインを棚卸し診断する	2 フィジカル AI システムを試験運用する	3 部門横断型のチームを結成する	4 ステークホルダーを教育する	5 マルチエージェントの連携を見据えた計画を立てる
期待される成果	自動化とコスト削減の対象となる領域を特定できる。	パフォーマンスと ROI を検証できる。	効果的なガバナンスと統合を実現できる。	混乱や投資の不整合を回避できる。	将来を見据えた拡張可能な展開が可能になる。
アクション	物流、保守、安全のワークフローを重点対象として洗い出す。	本番導入前に、シミュレーションやデジタル・ツインで検証を行う。	企画段階から IT、オペレーション、エンジニアリング部門を巻き込む。	フィジカル AI、組み込み型 AI、エッジ AI の区別を明確に説明する。	多数のデバイス群を管理するためのオーケストレーション・プラットフォームを検討する。

導入の成功を支える主要プレーヤー

CIO

定義：オペレーションの目標に沿ったフィジカル AI 戦略を定義する。

確保：安全性、信頼性、説明可能性のガバナンスを確保する。

協力：オペレーションやエンジニアリングと協力して、統合とリスク・マネジメントに取り組む。

IT パートナー

インフラストラクチャ／オペレーション：フィジカル AI を IoT やレガシー・システムと統合する。

セキュリティ：自律型システムの保護策を導入する。

データ／アナリティクス：シミュレーションとデジタル・ツインを利用したテストを支援する。

ビジネス・パートナー

オペレーション：価値の高いユースケースを特定し、パフォーマンスを検証する。

財務：ロボティクスと自動化への投資のために予算を確保する。

コンプライアンス：安全や規制基準への遵守を徹底する。

ヴァンガード

信頼、ガバナンス、セキュリティを向上させる

リスクが高まり、規制当局の監視が強まっている中、「信頼」はもはや交渉の余地のない前提条件です。「ヴァンガード」に分類されるトレンドは、プロアクティブなセキュリティ、透明性の高いガバナンス、デジタルの完全性を重視し、これにより、企業や組織が AI とデジタル・トランスフォーメーションを拡張させながら、評判を守り、コンプライアンスを確保しつつ、ステークホルダーの信頼を維持することができます。

7

先制的サイバーセキュリティ

どのようなものか

AI を活用した高度な手法を用いてサイバー攻撃を事前に予測して妨害し、無力化します。従来の「検知してから対応する」セキュリティを超え、予測／先制防御を重視する点が特徴です。

注目されている理由

ネットワーク、アプリケーション、IoT システムを標的として、AI を活用した脅威が急増しています。2029 年までに、プロアクティブな防御があらゆるプロダクトに不可欠な要件となり、先制的サイバーセキュリティを備えていないテクノロジ・プロダクトは市場での存在意義を失います。

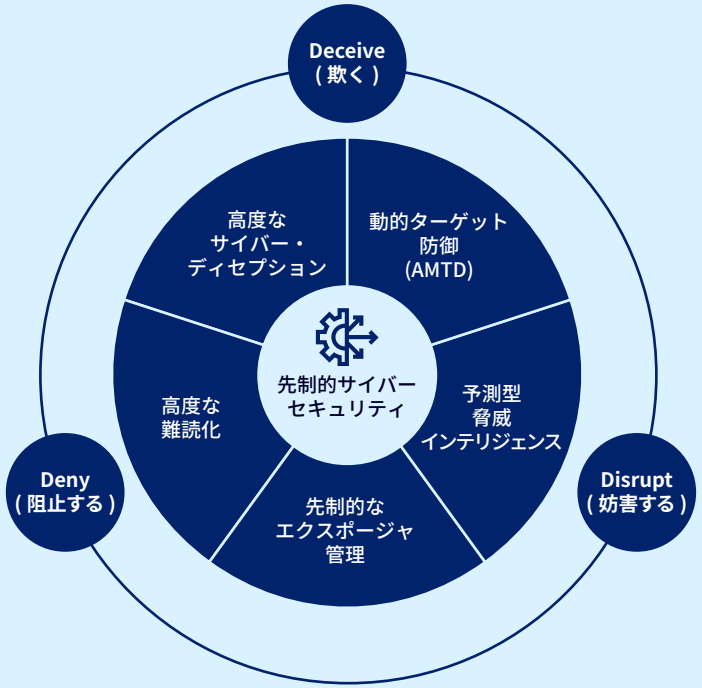
Gartner では、テクノロジ・プロバイダーやサービス・プロバイダーに特化したインサイトを提供しています。ベンダー向けの先制的サイバーセキュリティについては、**Don’t Delay in Building Preemptive Cybersecurity Solutions** をご覧ください。

今後の動向

50% のセキュリティ・ソフトウェア支出を、2030 年までに、先制的ソリューションが占めるようになる。

100 万 件を超える文書化された脆弱性が、2030 年までに年間で発見される。

先制的サイバーセキュリティにおける「3 つの D」



出典：Gartner

7

先制的サイバーセキュリティで成果を出す

脅威が発生する前に資産を防御するためのアクション・プラン

ステップ	1 現在のセキュリティ・アーキテクチャを評価する	2 リスクの高い領域で PCS を試験運用する	3 ベンダー選定基準を定義する	4 先制的サイバーセキュリティ (PCS*) 戦略を周知させる	5 PCS を既存のツールと統合する
期待される成果	ギャップを特定し、PCS 投資の優先順位を明確にできる。	リスク軽減の実効性を実証できる。	将来を見据えた PCS の導入を確保できる。	経営層および取締役会レベルで支援を獲得できる。	ROI を最大化し、導入スピードを早める。
アクション	リスクを分析し、準備状況を確認する。	予測的な脅威防御とサイバー・ディセプションを実装する。	先制的な能力に関する詳細なロードマップをベンダーに求める。	PCS がビジネスに与える影響と ROI を明確に伝える。	PCS を既存のセキュリティ／コンプライアンス・プロセスと組み合わせる。

導入の成功を支える主要プレーヤー

CIO

推進：受動的なセキュリティ戦略から先制的なセキュリティ戦略への転換を主導する。

定義：PCS 能力の購入基準を定義し、他の経営幹部を教育する。

監督：積極的な防御策とコンプライアンスのガバナンスを監督する。

IT パートナー

セキュリティ：予測的な脅威防御とサイバー・ディセプションのテクノロジを導入する。

インフラストラクチャ／オペレーション：PCS をクラウド、OT (オペレーショナル・テクノロジ)、サイバー・フィジカル・システムと統合する。

リスク／コンプライアンス：プライバシーや規制基準への遵守を徹底する。

ビジネス・パートナー

財務：PCS の試験運用と長期的な導入に向けて予算を割り当てる。

オペレーション：セキュアなデジタル・トランスフォーメーション施策をサポートする。

プロダクト：市場差別化のために、先制的セキュリティをプロダクト・サービスに組み込む。

* 先制的サイバーセキュリティ (PCS: Preemptive Cybersecurity)

8

デジタル属性

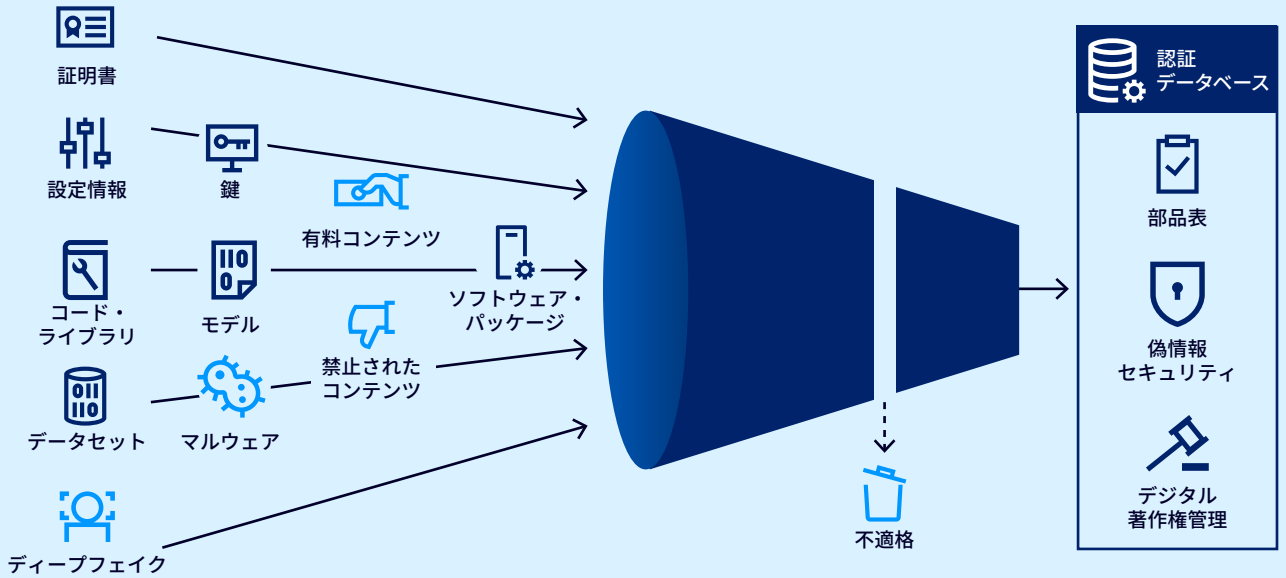
どのようなものか
部品表 (BOM)、認証データベース、ウォーターマークのようなツールを使用して、ソフトウェア、データ、メディアの出所と完全性を検証します。サードパーティのコンポーネントや AI 生成コンテンツで構築されたシステムの透明性と信頼性を確保します。

注目されている理由
多くの企業や組織が、コードの改ざん、放棄されたオープンソースのプロジェクト、ディープフェイクを使用した偽情報によるリスクの高まりに直面しています。

今後の動向

規制義務 (EU の AI 法など) が強化され、
AI 生成コンテンツに対してウォーターマークの追加と
属性の追跡が要求されるようになる。

デジタル属性を使用したフィルタリング



出典：Gartner

8

デジタル属性で成果を出す

データとコンテンツの真正性を検証し、信頼を築くためのアクション・プラン

ステップ	1 部品表 (BOM) を展開する	2 認証データベースを実装する	3 偽情報セキュリティ・ツールを導入する	4 デジタル・ウォーターマークを適用する	5 ガバナンスを強化する
期待される成果	ソフトウェア属性、透明性、安全性を確保できる。	一元化された信頼できる属性の記録を実現できる。	なりすましや詐欺からの保護を強化できる。	AI コンテンツ規制に準拠できる。	法的リスクやレピュテーション (評判) リスクを軽減できる。
アクション	ソフトウェア部品表 (SBOM) と AI モデルの機械学習部品表 (MLBOM) を導入する。	暗号署名された出所証明を保管する。	合成アイデンティティの検知をアイデンティティ脅威検知／対応計画に組み込む。	AI が作成したメディアを機械で読み取り可能な形式でマーク付けする。	IT、コンプライアンス、マーケティング・チームが連携して協力する。

導入の成功を支える主要プレーヤー

CIO

定義：コンプライアンスとリスク・マネジメントに沿ったデジタル属性戦略を定義する。

監督：BOM と認証データベースの実装を統括する。

協力:CISO や CMO と連携し、偽情報への対応とレピュテーションの保護をリードする。

IT パートナー

DevOps：SBOM と MLBOM をデリバリのパイプラインに組み込む。

セキュリティ：偽情報セキュリティ・ツールやデジタル著作権管理 (DRM) を展開する。

データ：AI モデル用トレーニング・データの来歴を文書化する。

ビジネス・パートナー

コンプライアンス：新たな規制への遵守を徹底する。

法務：著作権やライセンスのコンプライアンスを検証する。

マーケティング：ディープフェイクや合成コンテンツに関連するレピュテーション・リスクを管理する。

9

AI セキュリティ・プラットフォーム

どのようなものか

サードパーティの AI サービスと自社開発の AI アプリケーションの両方を保護するための統合的な制御を提供するプラットフォームです。プロンプト・インジェクション、不正なエージェント・アクション、データ漏洩といった AI 特有のリスクに対処します。

注目されている理由

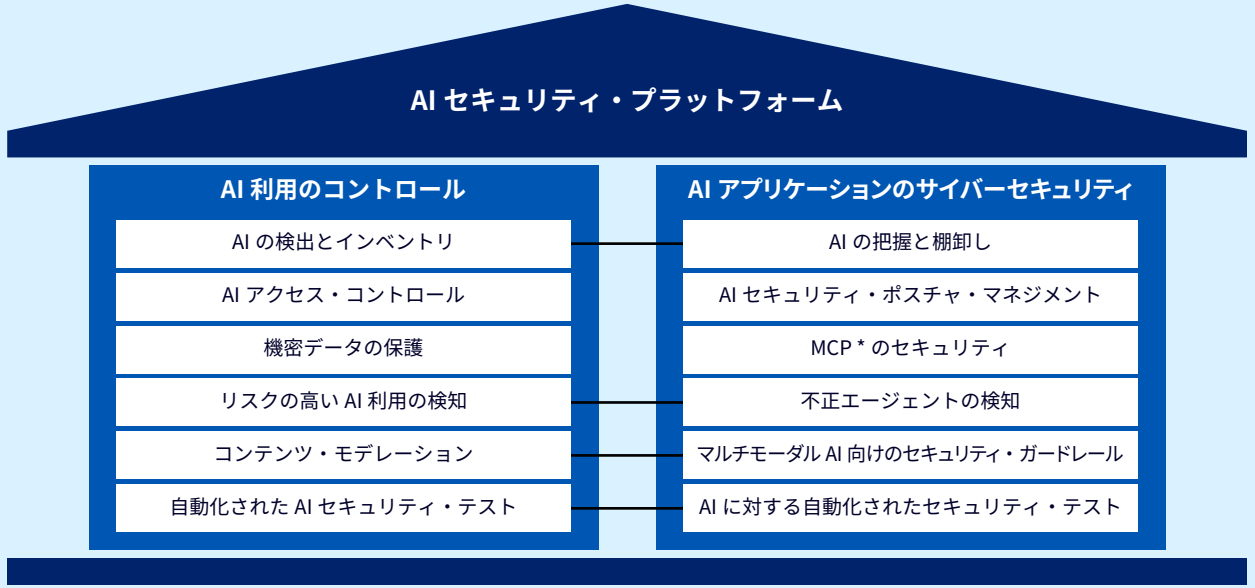
AI 活用が急速に広がる中、従来のセキュリティ・ツールだけでは AI のワークフローを十分に保護できなくなっています。

今後の動向

50%以上 の企業が、2028 年までに、AI セキュリティ・プラットフォーム (AISP*) を採用するようになる。

80% の不正 AI トランザクションが、外部からの攻撃ではなく、内部のポリシー違反によって発生するようになる。

AI セキュリティ・プラットフォームのケイパビリティ・マッピング



出典：Gartner

* AI セキュリティ・プラットフォーム (AISP: AI Security Platforms)
* モデル・コンテキスト・プロトコル (MCP: Model Context Protocol)

9

AI セキュリティ・プラットフォームで成果を出す

高度化する AI 主導のビジネス・オペレーションを保護するためのアクション・プラン

ステップ	1 AI リスク環境を評価する	2 AISP* ソリューションを試験運用する	3 統一されたプラットフォームを優先させる	4 セキュリティ・テストを統合する	5 ベンダーのイノベーションをモニタリングする
期待される成果	現在のセキュリティ・スタックのギャップを特定できる。	効果と ROI を検証できる。	管理を簡素化し、複雑さを軽減できる。	プロンプト・インジェクションに対するレジリエンスを高められる。	新たな脅威に先手を打って対応できる。
アクション	ワークフロー全体で AI 特有のリスクを棚卸してマッピングする。	リスクの高い AI サービスやカスタム AI アプリから開始する。	AI 利用のコントロールとアプリ・セキュリティを包括的にカバーする AISP を選択する。	自動化された AI セキュリティ・テストをパイプラインに追加する。	先進機能を持つスタートアップおよび既存大手ベンダーの動向を継続的に注視する。

導入の成功を支える主要プレーヤー

CIO

定義：サードパーティの AI アプリとカスタム AI アプリにわたって AI セキュリティ戦略を定義する。

選択：統一された AI 利用のコントロールとアプリケーション・セキュリティを提供するベンダーを選択する。

伝達：AI リスク・ポスチャとコンプライアンス要件を取締役会に伝達する。

IT パートナー

セキュリティ：プロンプト・インジェクションと不正エージェント検知のためのガードレールを導入する。

DevOps：AI セキュリティ・テストを開発パイプラインに組み込む。

インフラストラクチャ／オペレーション：クラウド環境とオンプレミス環境の互換性を確保する。

ビジネス・パートナー

コンプライアンス：AISP を規制の枠組み (EU の AI 法など) に整合させる。

財務：プラットフォーム導入とリスク軽減のために必要な予算を確保する。

プロダクト：AI 対応サービスにセキュリティ機能を組み込む。

* AI セキュリティ・プラットフォーム (AISP: AI Security Platforms)

10 ジオパトリエーション

どのようなものか
グローバルなハイパースケール・クラウド上で動いているワークロードを、ソブリン・クラウドやローカル環境へ移すことで、地政学リスクを軽減する取り組みです。これには、ソブリン・クラウド・リージョンへの再配置や、オンプレミス環境への回帰といった戦略も含まれます。

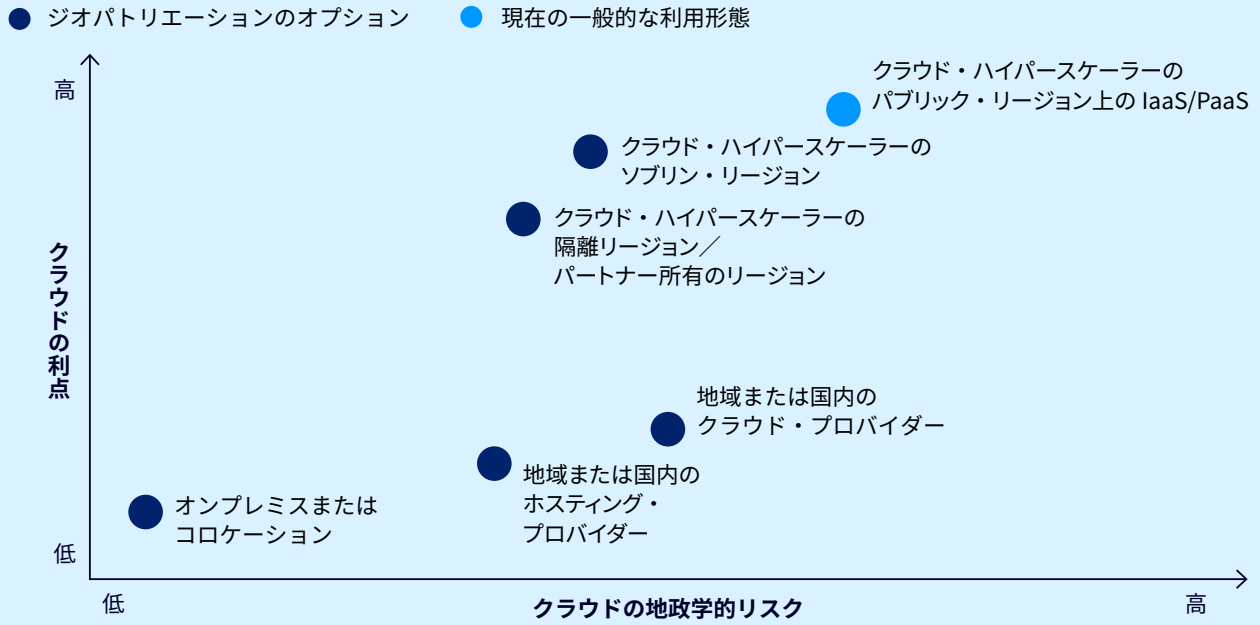
注目されている理由
地政学的な緊張の高まりと、各国／地域の規制要件の強化により、多くの企業や組織がクラウドへの依存のあり方を見直さざるを得なくなっています。

今後の動向

75% の企業が、2030 年までに、ワークロードのジオパトリエーションを採用するようになる。

ハイパースケーラーやローカル・プロバイダーが提供するソブリン・クラウドが急速に拡大していく。

クラウドの利点と地政学的リスク



出典：Gartner

10

ジオパトリエーションで成果を出す

重要なデジタル・ワークロードを現地に配置してリスクを軽減するためのアクション・プラン

ステップ	1 ワークロードの重要度を評価する	2 ソブリン・クラウドのオプションを評価する	3 ハイブリッド戦略を計画する	4 ガバナンス管理を実装する	5 地政学的な動向をモニタリングする
期待される成果	高リスク資産のジオパトリエーションの優先度を明確にできる。	俊敏性と主権要件のバランスがとれる。	レジリエンスとパフォーマンスを維持できる。	コンプライアンスとセキュリティ・リスクを軽減できる。	戦略を積極的に適応できる。
アクション	機密性と地政学的なリスクに基づいてワークロードを評価する。	ハイパースケーラーのソブリン・クラウドとローカル・プロバイダーのサービスを比較する。	ソブリン・クラウドをオンプレミスまたはコロケーションと組み合わせる。	認証と主権ガバナンスのフレームワークを導入する。	リスクの変化に応じてワークロードの配置を更新する。

導入の成功を支える主要プレーヤー

CIO

定義：主権、俊敏性、レジリエンスのバランスを取って、ジオパトリエーション戦略を定義する。

評価：ローカル・プロバイダーとグローバル・ハイパースケーラーのソブリン・クラウド・オプションを比較し、利点とリスクを評価する。

監督：重要なワークロードのリスク評価とコンプライアンスとの整合を監督する。

IT パートナー

インフラストラクチャ／オペレーション：移行経路とレガシー・システムとの統合を計画する。

セキュリティ：主権管理を検証し、コンプライアンスを確保する。

クラウド・アーキテクト：ワークロードの配置を最適化して、パフォーマンスとレジリエンスを維持する。

ビジネス・パートナー

コンプライアンス：規制の動向や主権に関する要件の変化をモニタリングする。

財務：移行コストとリスク軽減のための予算を確保する。

オペレーション：ワークロードの移行中の事業継続性を確保する。

実用的で客観的なインサイト

ビジネス・リーダーと IT リーダーのためのリソース／ツールを無償でご利用いただけます。

Template

IT 戦略プランニングのための ガイドブック

効果的な IT 戦略計画に役立つ 5 つのベスト・プラクティスを理解し、1 ページでまとめる IT 戦略計画テンプレートを利用できます。

テンプレートを利用する

Tool

Gartner Benchmarking and Diagnostics

よりスマートな IT 意思決定に役立つベンチマーキングをご紹介します。

詳細を見る (英語)

Insights

2025 Gartner Hype Cycle ™

2025 年の人工知能のハイプ・サイクルは、生成 AI にとどまりません。

今すぐ読む (英語)

Insights

Trending Questions on AI and Emerging Technologies

Gartner のエキスパートが、先進テクノロジに関して最近寄せられた顧客企業からの質問に対するクイック・アンサーを共有します。

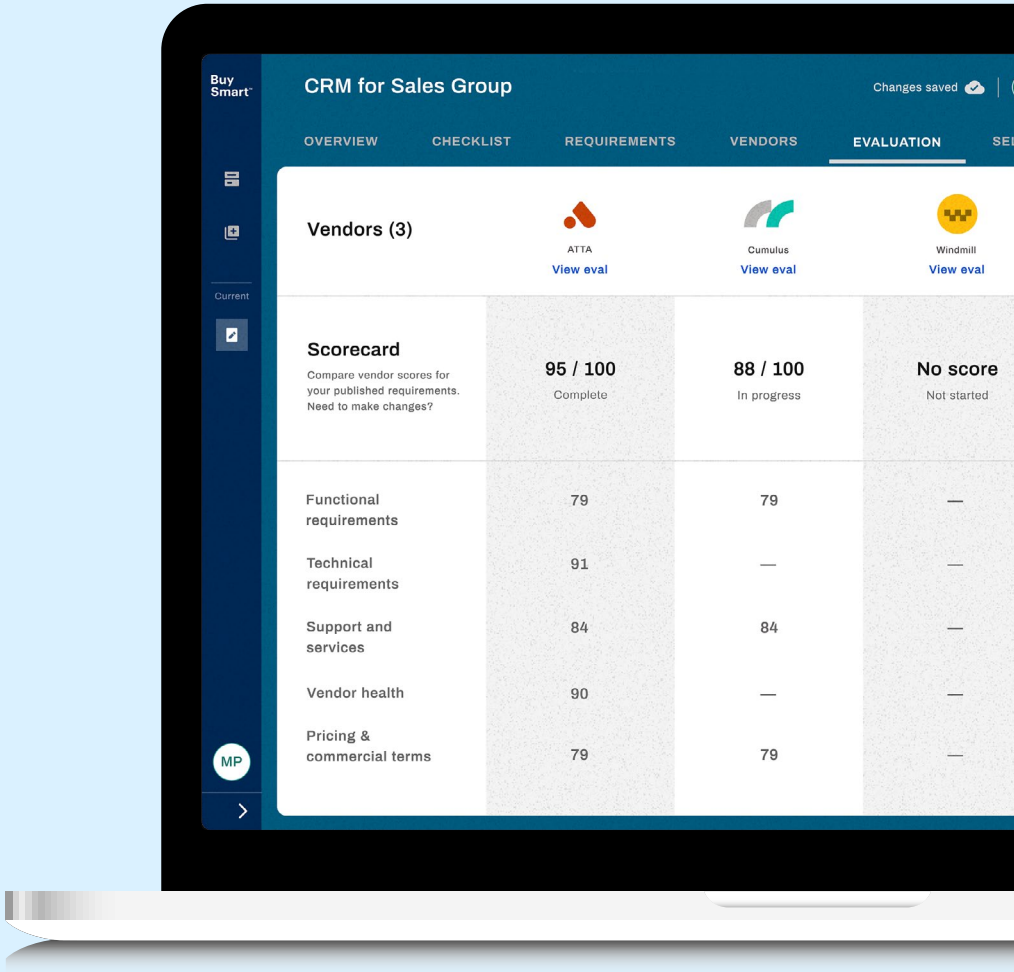
回答を確認する (英語)

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 BuySmart ™

より適切なテクノロジ選定へと、チームを効率的に導きます。



ご提供の内容：

- 主要テクノロジ市場をカバーする 100 以上のテンプレートへのアクセス
- 事前定義済みで全面的にカスタマイズ可能なチェックリスト／要件
- お客様のチームのワークフローを一元的にサポートするコラボレーション機能
- ベンダー選定における自信を高めるための標準化されたスコアリング

詳細を見る ↗

リサーチ　最終候補リスト　評価　交渉

Connect With Us

Gartner は、経営幹部およびそのチームに対し、実行可能かつ客観的なビジネスおよびテクノロジのインサイトを提供します。Gartner のエキスパートによるガイダンスやツールは、組織の重要な課題について、迅速で優れた意思決定と大きな成果の創出を可能にします。

Gartner のサービスに関するお問い合わせ

CIO ／ IT エグゼクティブを成功に導く Gartner のサービス
gartner.co.jp/ja/chief-information-officer

最新のインサイトをご確認ください

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®