守りと攻めを兼ね備えたITインフラ戦略
－セキュリティとAIを支える基盤設計の指針－

2026年6月23日

取締役 / プリンシパル・アナリスト
入谷 光浩
株式会社アイ・ティ・アール

入谷 光浩
Mitsuhiro Iriya

プリンシパル・アナリスト
ITR

【 業務内容 】

- 市場・技術動向に関する調査とレポート執筆
- ユーザー企業のDX・IT戦略コンサルティング
- ベンダーのビジネス・製品戦略支援コンサルティング
- 外部セミナーや社内研修での講演

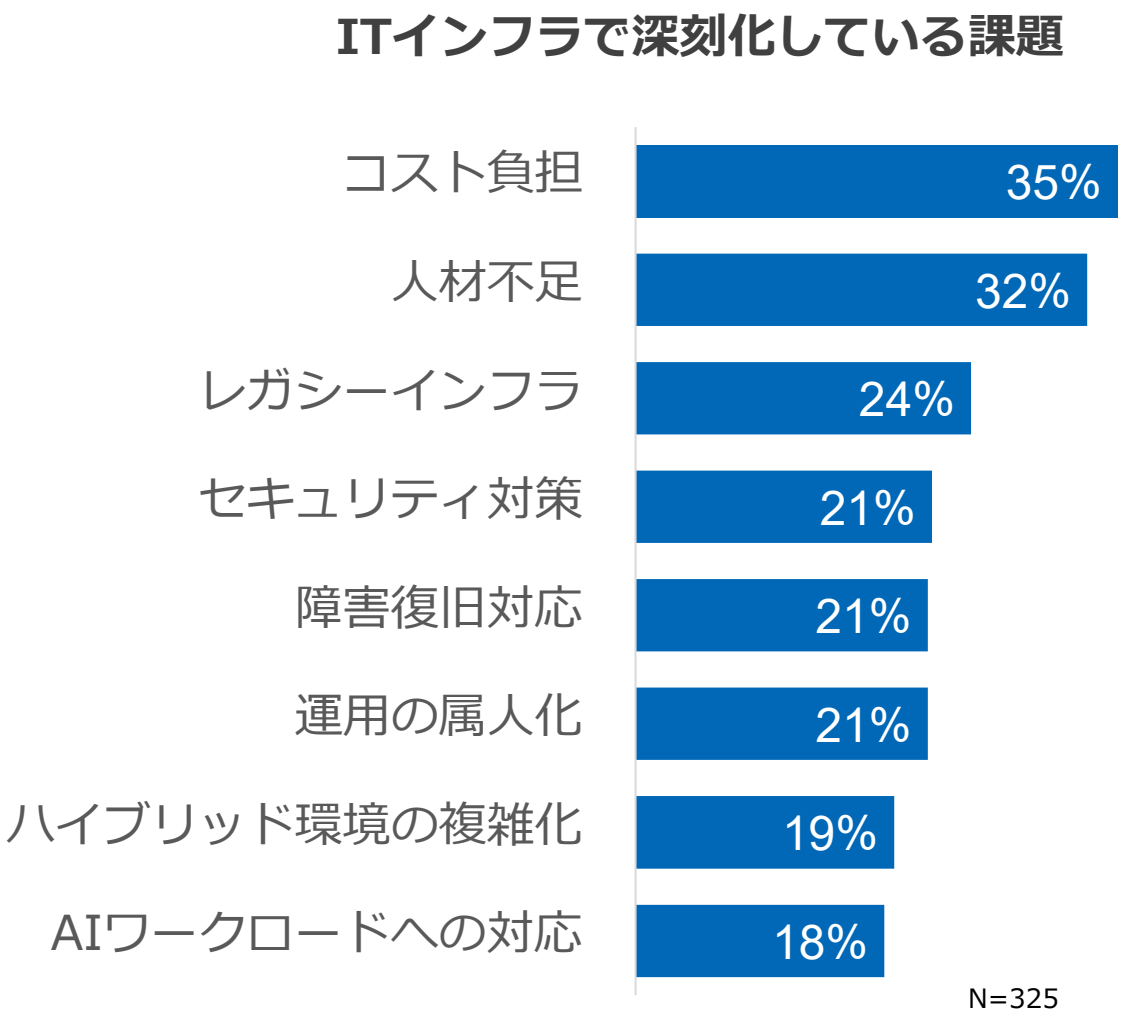
【 専門分野 】

- クラウドサービス（IaaS、PaaS）
- インフラストラクチャ
- IT運用／サービスマネジメント
- レジリエンス戦略

【 経歴 】

- ITアナリスト歴20年以上
- 外資系リサーチファームで15年間アナリストとして従事し
  クラウド・ソフトウェア・セキュリティの日本市場調査責任者
- 複数の外資系ITベンダーにて事業戦略・新規事業開発を担当
- セミナーでの講演実績多数
- ITmedia エンタープライズで連載中
  「新しい乱世」を生き抜くためのIT羅針盤

ITインフラで深刻化する課題



出典：ITR『ITインフラ実態調査2025』

本日の論点

戦略 ➡ 仮想化基盤の再定義

守り ➡ セキュリティ前提の設計

攻め ➡ AIインフラへの拡張

本日の論点

戦略 ➡ 仮想化基盤の再定義

守り ➡ セキュリティ前提の設計

攻め ➡ AIインフラへの拡張

VMware製品体系の変更に対しユーザーはどのような対応をとるべきか

項目	VMware仮想基盤製品の主な変更点
ライセンス	永久ライセンスの販売が終了しサブスクリプション契約に一本化
保守	永久ライセンス向け有償保守サービスが終了し、保守はサブスクリプション契約内に含まれる
課金単位	CPUソケット単位からCPUコア単位に変更（1CPUあたり最小16コアから購入可能）
パッケージ	SKU単位ではなくバンドルされた4つのエディションから購入（最上位はVCF※）

※VMware Cloud Foundation（VCF）

VMware問題で「継続か？」「移行か？」だけに捉われるのではなく
不確実な将来を見据えてITインフラの構造を戦略的に再定義する機会とする

「VMwareの次」の選択肢

	VMware仮想基盤	非VMware仮想基盤
オンプレミス	**移行せずにVMware仮想基盤をそのまま継続** • サブスクリプション契約への変更が必要 • 購入できるパッケージが限定される	**異なる仮想基盤への移行** • Hyper-V、Nutanix、KVM OpenShift、Proxmoxなど • 仮想マシン移行 • HCIでの導入が主流
クラウドサービス	**VMware仮想基盤のクラウドサービスへの移行** • ホステッド型vSphere基盤で構成されたIaaSを利用 • マネージド型VMware環境のサービスを利用	**IaaS（非VMware基盤）への移行** • IaaSの標準仮想マシンインスタンスを利用 • Azure、AWS、Googleなど • リフト＆シフトによる段階的な移行が可能

仮想化基盤を6つの観点から再定義する

技術

- ☑ 仮想基盤＝VMwareという前提からの脱却
- ☑ 特定製品の固有機能を前提としない設計
- ☑ ワークロードに最適な基盤を柔軟に選択可能

配置

- ☑ オンプレミスとクラウドの使い分け
- ☑ 基盤横断でのワークロード可搬性の確保
- ☑ ハイブリッド環境を見据えた設計

コスト構造

- ☑ ライセンス条件の変更に左右されない構造
- ☑ 利用量に応じたコスト管理ができる設計
- ☑ 中長期で見通しの立つコストモデルを重視

スキル・運用

- ☑ VMwareスキルに依存した運用からの脱却
- ☑ クラウドと共通化できる汎用スキルの獲得
- ☑ 自動化された運用モデルの実現

セキュリティ・ガバナンス

- ☑ セキュリティを前提とした基盤設計
- ☑ ランサムウェア耐性を備えた復旧能力の確保
- ☑ データ・AI主権の確保に必要な統制

将来性

- ☑ 既存基盤を前提とした二者択一からの脱却
- ☑ AI前提時代に向けたAIインフラへの拡張
- ☑ 不確実性や次の変化に対応できる余地を残す

ハイブリッドがITインフラの主流

**中長期のITインフラ戦略において
ハイブリッドインフラ方針を
採用している企業**

52%

クラウドサービスのみ	28%
オンプレミスのみ	15%
方針なし	5%

N=325

出典：ITR『ITインフラ実態調査2025』

- システム要件の多様化
- 環境変化への迅速な対応
- コスト最適化
- セキュリティ強化・データ主権
- AI・データ活用の拡大／高度化

セキュリティ前提の設計

ハイブリッド環境におけるセキュリティとITインフラの考え方

ハイブリッド環境では、セキュリティは個別対策ではなく
ITインフラ設計・運用の前提条件となる

ハイブリッドでの課題

- 管理対象がオンプレミスとクラウドへ分散
- ID・権限管理が複雑化
- データの所在や移動経路が見えにくくなる
- 設定ミスや運用のばらつきが増える
- 監視・検知・対応がサイロ化しやすい

セキュリティの考え方

- IDを起点にした一貫したアクセス統制
- データの機密性・重要度に基づく分類・配置・保護
- ポリシーの共通化と継続的な準拠の確認
- 監視・検知・対応の統合
- ランサムウェア耐性のあるバックアップ

ITインフラの考え方

- セキュリティ要件を前提としたクラウドとオンプレミスの役割分担
- ハイブリッド環境全体を一貫して統制できる構造
- データ主権や規制対応、事業継続性を踏まえた基盤配置
- 迅速なリスク対応を可能にする復旧しやすい設計

ゼロトラストへの転換でインフラ担当者が押さえておくべき設計領域

仮想基盤のハイブリッド化により境界防御の前提が崩れ、ゼロトラストへの転換が迫られている

セキュリティ設計の考え方の変化

従来：境界防御モデル

守るべき資産は境界の内部にある

- FWやIDS/IPSで「境界」を防御する
- 内側は信頼できる　外側は信頼できない

これから：ゼロトラスト

守るべき資産は境界の内外にある

- 「何も信頼せず、常に検証する」を原則とする
- 境界ではなく、個々のリソースを守る
- ID・デバイス・コンテキストで信頼を判断
- 必要最小限の権限を、必要なときだけ付与

ゼロトラストに必要なセキュリティ設計領域

ID：
オンプレミス／クラウドのID・認証基盤の統合
IDaaS、特権アクセス管理、ID統制、多要素認証、パスワードレス認証

サーバ・ワークロード
サーバ・デバイスの監視・検知・対応、クラウド上のVM・コンテナの保護
EDR、XDR、CWPP

ネットワーク
ネットワーク一元管理、仮想環境間のアクセス制御、IDベースのアクセス
SD-WAN、マイクロセグメンテーション、ZTNA

データ
データの漏洩防止、機密度に応じたデータの分類・配置、暗号化・鍵管理
DLP、DSPM、KMS

可視化・統制
ハイブリッド環境横断のログ監視・検知、クラウド設定の一元管理・監視
SIEM、XDR、CSPM、CNAPP

EDR：Endpoint Detection and Response
XDR：Extended Detection and Response
CWPP：Cloud Workload Protection Platform
SD-WAN：Software-Defined Wide Area Network
ZTNA：Zero Trust Network Access）

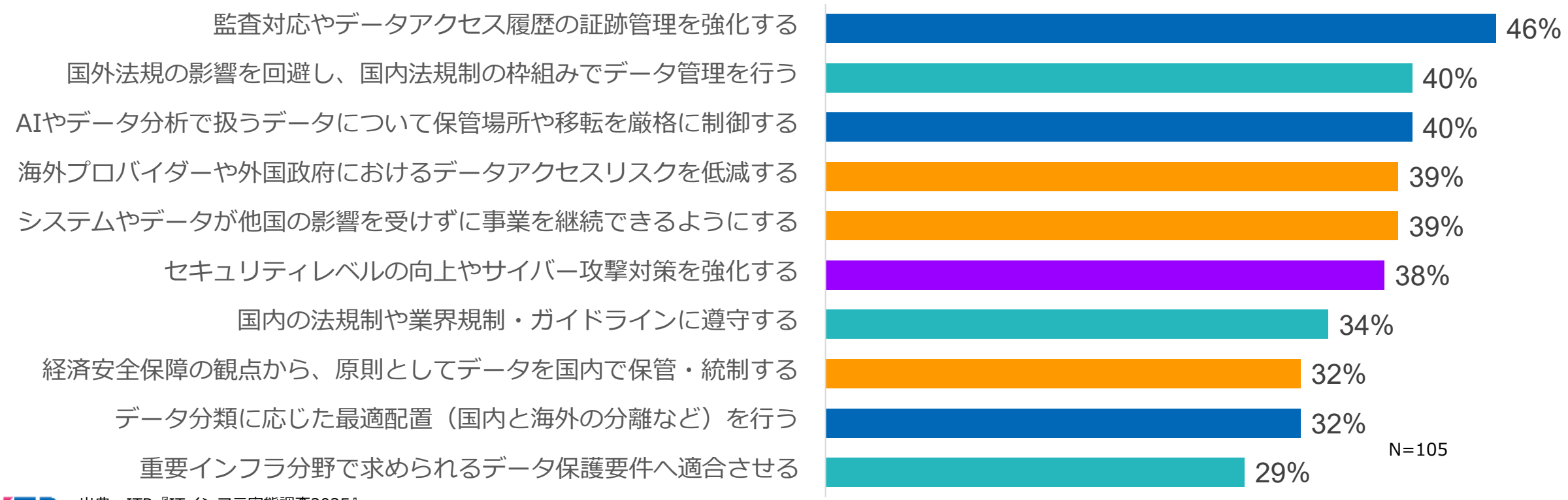
DLP：Data Loss Prevention
DSPM：Data Security Posture Managemen
KMS：Key Management System
SIEM：Security Information and Event Management
CSPM：Cloud Security Posture Management
CNAPP：Cloud Native Application Protection Platform

データ主権への対応が必要とされている背景・目的

データ主権とは

- データを生成・保存される国・地域の法規制にしたがって管理する考え方
- 自社データの所在・アクセス・利用・統制について、自社で主体的に管理できる状態にしておく必要がある

データ統制・配置　規制・法的対応　地政学リスク　セキュリティ強化



出典：ITR『ITインフラ実態調査2025』

データ主権を踏まえた配置設計 ― 3つの選択肢と判断軸

データ配置は3つの選択肢を機密度・規制・性能・連携の観点で判断

パブリッククラウド
事業者ポリシーに従った運用

特徴
- 海外事業者が運用、データは海外DC含む
- 域外法（CLOUD Act等）の適用可能性
- 事業者の運用ポリシー・SLAに準拠

適用領域の例
- 非機密データ、機密データ
- 汎用ワークロード、開発・検証環境

ソブリンクラウド
事業者が国内法規制に準拠して運用

特徴
- 事業者が運用、データは国内DCに限定
- 域外法の適用を排除、国内法規制に準拠
- 監査・証跡・アクセス制御機能を提供

適用領域の例
- 高機密データ
- 個人情報、業界規制対応、重要インフラ

オンプレミス
自社ポリシーによる統制・運用

特徴
- 自社運用、データは自社DCに格納
- 自社ポリシーでデータを制御・管理
- 監査・証跡・アクセス制御を自社で設計

適用領域の例
- 最高機密データ
- 未公開の経営情報、知的財産、独自技術

配置設計における判断軸

機密度・重要度
高機密ほど統制可能な環境へ

規制要件
データ越境・所在制限への対応

性能要件
レイテンシ・処理性能の要求

連携要件
AI・他システムとの連携可能性

ランサムウェアの脅威がすべての企業に迫っている

ランサムウェア感染経験割合

46%

業種、企業規模に関係なく狙われる

N=1107

被害後のデータ復旧失敗割合

46%

バックアップデータの暗号化・破壊

N=507

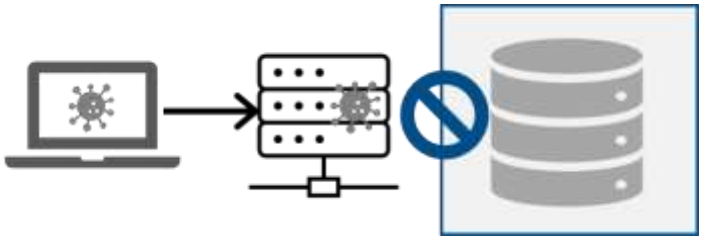
出典：JIPDEC『企業IT利活用動向調査2026』

ランサムウェア耐性を備えたバックアップによって復旧能力を確保する

イミュータブルバックアップ

- 保存したデータの変更を不可能にし、改ざん、暗号化、削除を阻止してバックアップデータを保護する
- サイバー攻撃や内部不正からバックアップ環境を防御する
- データ可視化やリストア機能により迅速な復旧ができる
- 運用性が高く日常のバックアップ管理に適している

エアギャップバックアップ



- ネットワークから物理的または論理的に切り離された環境にバックアップデータを保管することで、不正なアクセスを遮断する
- システム全体が侵害されても、バックアップは独立した環境で生き残る
- 災害対策や監査・法規制に対する長期保管に対応できる
- 運用性は低いため非常時のためのバックアップが目的となる

ニューオンプレミスの特徴と戦略的価値

クラウドの拡張性・俊敏性とオンプレミスのコントロール性を融合したハイブリッドITインフラ

クラウドの運用モデル

- 従量課金・オンデマンド拡張などクラウドベースの利用形態
- IT基盤を所有ではなくサービスとして利用できる
- キャパシティ計画を前倒しせず需要に応じて調整できる

標準化・自動化を前提

- コンテナ/k8sやHCI構成によりアプリケーション基盤を標準化
- リソース管理や構成管理を自動化しプロビジョニングを迅速化
- クラウドとの環境差異を小さくし両環境間の可搬性を高められる

オンプレの強みを維持

- 構成やチューニングで低レイテンシ・高パフォーマンスを確保
- データ主権や規制対応、BCP要件に合わせた設計ができる
- 自社ポリシーに基づいて運用・セキュリティを制御できる

基幹系・ミッションクリティカルシステム

厳しい規制対応が必要なデータ基盤

クラウドと高頻度で連携が必要なシステム

利用量が安定した定常ワークロード

高速処理を必要とするデータ分析・AI基盤

- ■ データ主権の確保 – 自社完全統制によるガバナンスの最終的な拠り所
- ■ セキュリティの自社設計 –ゼロトラストとランサムウェア耐性を統合的に実装できる統制基盤
- ■ AIインフラへの拡張性 – 高いパフォーマンスとAI主権を確保した競争力のあるAI基盤の構築

AIインフラへの拡張

生成AIの利用形態と効果

Use（利用）
- 生成AI機能が組み込まれた市販サービスを利用
- 多くの従業員が共通して行う汎用的なタスクに適用
- 情報収集、調査、文書・資料作成、汎用コンテンツ作成など

Build（構築）
- APIなどにより生成AI機能を組み込んだアプリケーションを作成して利用
- 特定の業務ワークフローに関わるタスクに適用
- 汎用チャットボット、ナレッジ検索、コード生成など

Custom（特製）
- 用途向けにLLMをカスタマイズしてアプリケーションに実装して利用
- RAG環境の構築や専門タスク向けAIエージェントの開発
- 専門性が高く複雑な問題解決が求められるタスクに適用
- 専門チャットボット、高度な情報分析、専門分野のレポート作成など

Develop（開発）
- LLMを独自開発しアプリケーションに実装して利用
- 既存LLMが未学習の特殊用途や将来の革新につながるタスクに適用
- 新製品・サービス開発、研究開発、高度な意思決定など

自動化、差別化、価値創出を図るためにはLLMを迅速にデプロイ／カスタマイズ／独自開発が可能なAIインフラが必要となる

AIインフラを構築する理由 ― 戦略的な競争力の源泉とする

1	2	3
37%	34%	32%
AIのモデルや構成を自社要件に合わせてカスタマイズできる	AI基盤を自社のコアコンピタンスとして保持したい	データ主権に基づき自社基盤でデータの学習・推論が必要

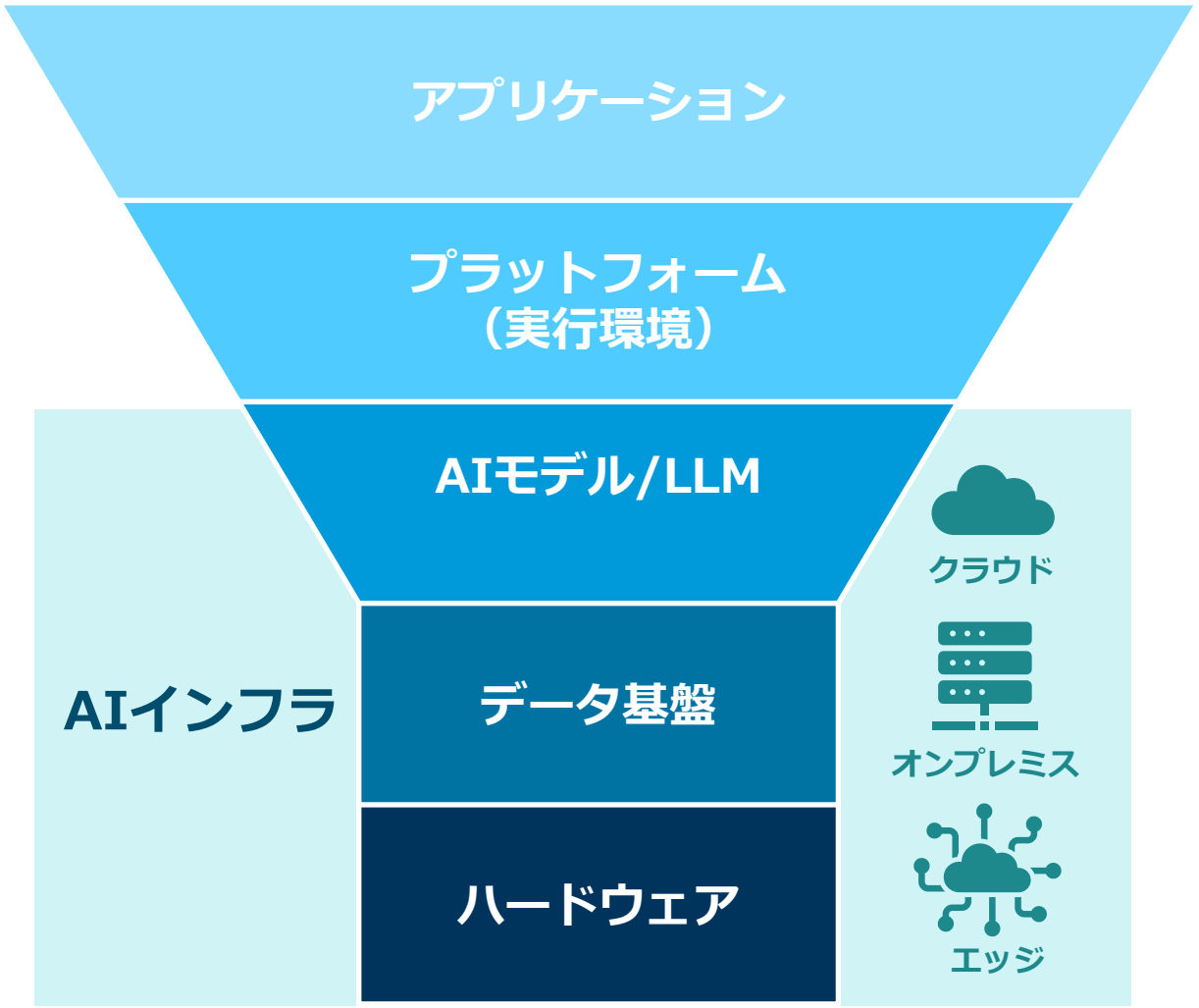
その他の理由

（N=148）

- AIに必要なデータが既に自社データ基盤に大量にある (30%)
- AI基盤に関するノウハウやナレッジを蓄積できる (30%)
- 自社のポリシーに合わせてセキュリティ対策ができる (30%)
- 学習・推論処理の性能を高くできる (29%)
- レイテンシ要件(リアルタイム処理など)に対応できる (28%)
- 自社構築の方がコストを最適化できると試算した (26%)
- 他のシステムと連携しやすい (25%)

出典:ITR「ITインフラ動向調査2025」

AIのパフォーマンスと俊敏性を高めるAIインフラの構築を見据える



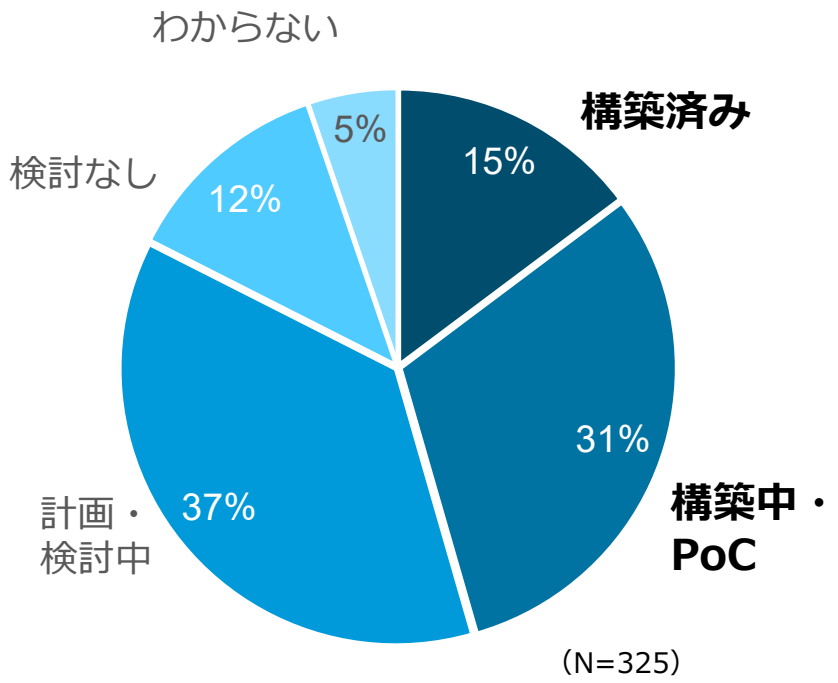
AIインフラに求められる要件

- AIモデルの学習・推論を高速かつ大量に処理できる高性能リソース（GPU、大容量メモリ、フラッシュストレージなど）
- AI利用の需要変動に応じて柔軟にスケールアウト・インできる拡張性
- データの生成から収集・抽出・加工に至るデータパイプラインの迅速な構築
- Kubernetes／コンテナによるAIモデルやAIアプリケーションの迅速なデプロイ
- AIモデルとデータ向けのプライバシー保護とセキュリティ

AIインフラの構築状況

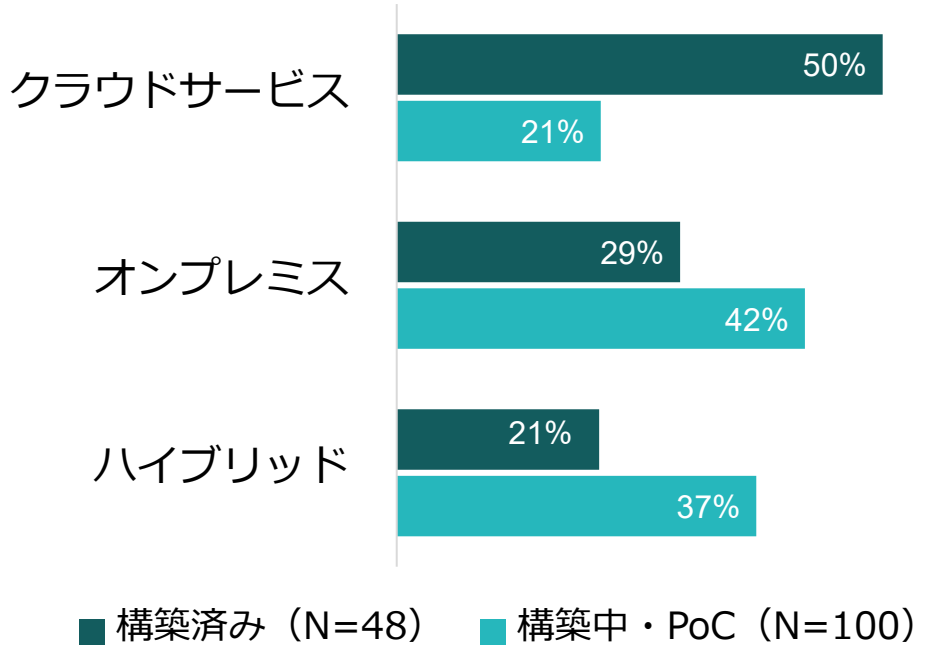
- AIインフラは一部の先進企業が先行しているが、多くの企業はこれから本格構築の段階
- 現時点では、GPUをすぐに導入・活用しやすいクラウドサービスが主流
- 今後はオンプレミスもしくはハイブリッドによるAIインフラ構築が増加するとみられる

AIインフラの構築状況



(N=325)

AIインフラの構築環境



出典：ITR『ITインフラ実態調査2025』

AIインフラの設計はハイブリッド型が最適解

クラウドサービス

- 柔軟なスケーラビリティ
- 初期コストの抑制
- 多種多様なAIサービス
- 迅速なAI環境の構築

・変動性の高い推論処理
・試行錯誤しながらの学習

オンプレミス

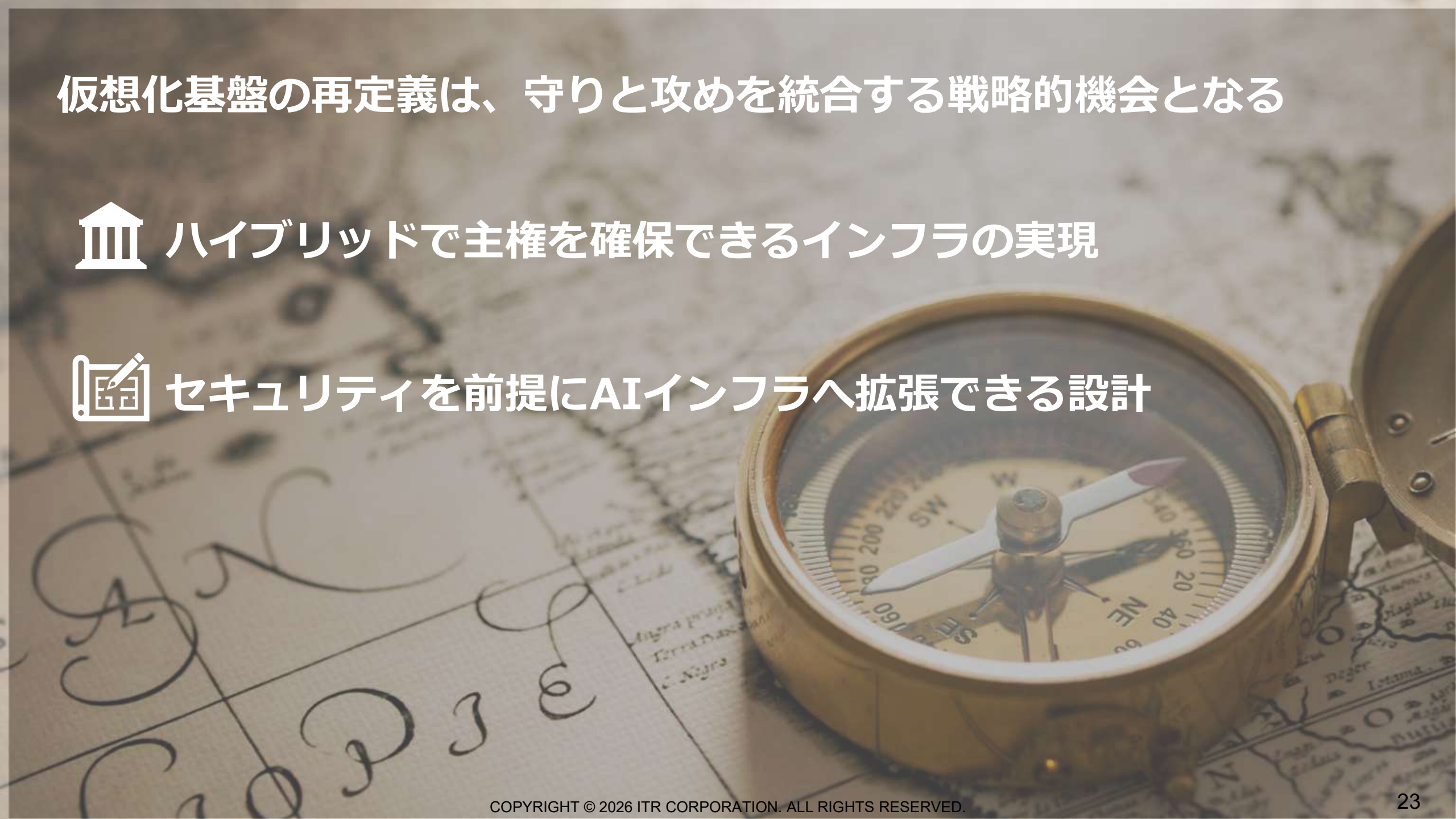
- レイテンシの低い高性能環境
- 長期間でのコスト効率性
- カスタマイズ性と安定性
- データ主権と機密性

・低レイテンシな推論処理
・機密性の高い学習・推論

クラウドとオンプレミスの特性や強みを踏まえたハイブリッド構成が主流になっていく

仮想化基盤の再定義は、守りと攻めを統合する戦略的機会となる

- ハイブリッドで主権を確保できるインフラの実現
- セキュリティを前提にAIインフラへ拡張できる設計



問いを、答えに。