EXECUTIVE BRIEFING & STRATEGIC PLAYBOOK

生成AIの「単なる利用者」が終わる日

AI事業者ガイドライン改訂（第1.2版）が迫る実務上のパラダイムシフトと、
企業が取るべきガバナンス構築の全ロードマップ

BASED ON THE UPCOMING METI/MIC AI GUIDELINES V1.2 (SCHEDULED MARCH 2026)

旧来の前提：単なるツール導入

AIツールを購入するだけ。
リスク管理はAIベンダー（提供者）の責任

- ◆ 入力: 従業員が自由にプロンプトを入力。
- ◆ 出力: 生成された結果をそのまま業務や意思決定に利用。
- ◆ 責任: 外部からの問い合わせには「AIの仕様」と回答。

v1.2の現実：統合されたガバナンス

利用企業（AI利用者）自身が、
入力・処理・出力・説明の全フェーズで責任を負う

- ◆ 入力: 個人情報・機密情報の入力制限とDLPによる技術的ガード（U-4, U-5）。
- ◆ 出力: 人間の判断（HITL）を介在させ、精度とリスクを検証（U-2）。
- ◆ 責任: ステークホルダーへの通知、問い合わせ窓口の設置、ベンダー規約の遵守と文書管理（U-6, U-7）。

第1.2版は「AI利用者」に対する実務上の期待水準 (“やるべきこと”の標準) を劇的に引き上げます。

監査・取引先からの統制要請

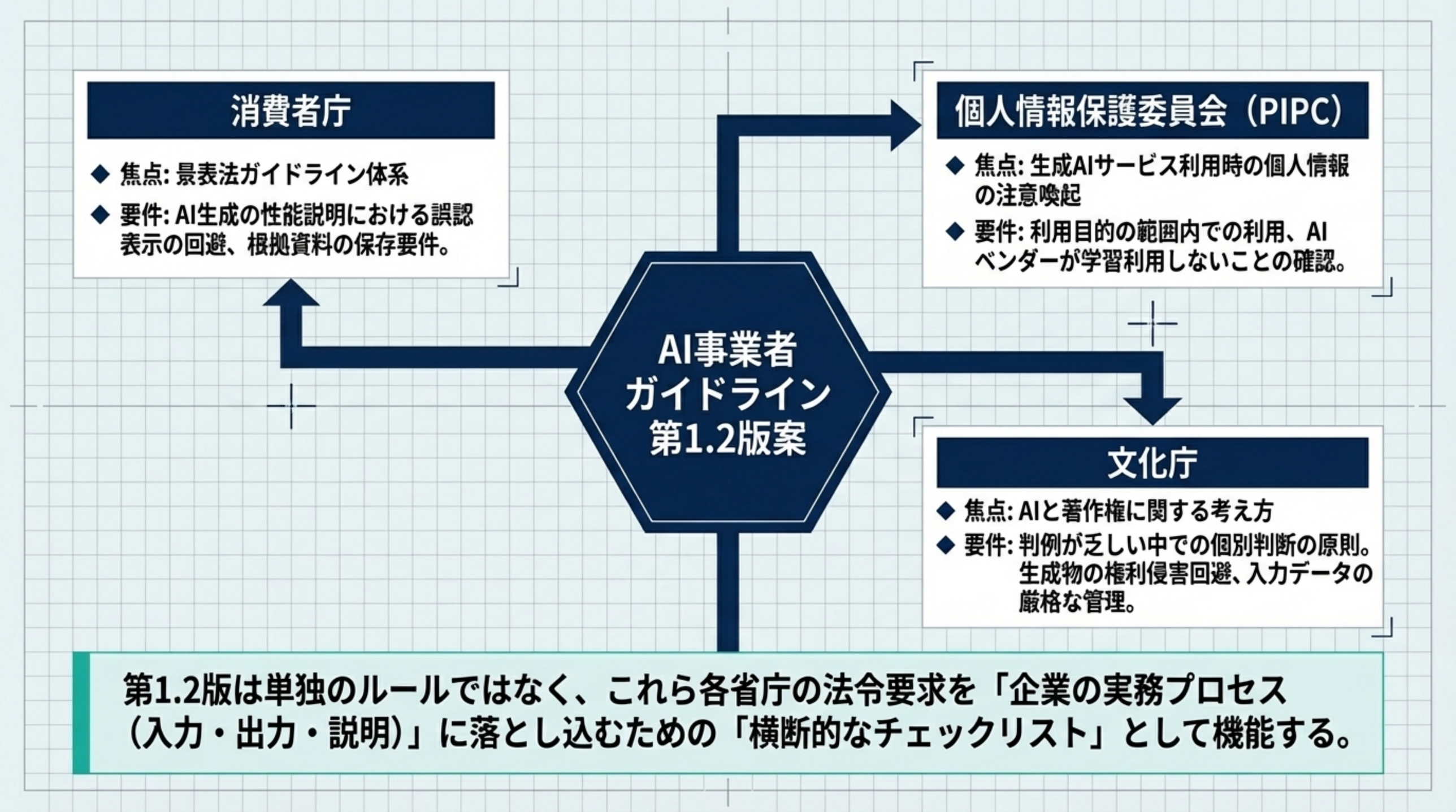
著作権・プライバシー侵害の訴訟

事故時のレピュテーション低下

ソフトロー（合理的な注意の証明）

ガイドライン自体に直接の強制力はない。しかし、遵守していることが企業としての「善管注意義務」を果たした強力な証拠となる。

未対応のリスク: ガイドラインを無視した状態で事故が起きれば、「国が示す標準的な対策すら怠っていた」として、過失責任や経営責任が厳しく問われる。


消費者庁
◆ 焦点: 景表法ガイドライン体系
◆ 要件: AI生成の性能説明における誤認表示の回避、根拠資料の保存要件。
個人情報保護委員会（PIPC）
◆ 焦点: 生成AIサービス利用時の個人情報の注意喚起
◆ 要件: 利用目的の範囲内での利用、AIベンダーが学習利用しないことの確認。
AI事業者ガイドライン第1.2版案
文化庁
◆ 焦点: AIと著作権に関する考え方
◆ 要件: 判例が乏しい中での個別判断の原則。生成物の権利侵害回避、入力データの厳格な管理。
第1.2版は単独のルールではなく、これら各省庁の法令要求を「企業の実務プロセス（入力・出力・説明）」に落とし込むための「横断的なチェックリスト」として機能する。

Stage 1: 入力 (Input) - The Filter Gate

条項: U-4 & U-5

「個人情報/機微情報は原則入力禁止」の設定。
DLP・プロンプト監査。
RAG用社内DBの最小権限化。
ベンダーの学習利用OFF設定。

Stage 2: 処理 - The Black Box Management

条項: U-2

ベンダー規約の遵守。
出力の精度とハルシネーションリスクの理解。
禁止用途（バイアスを含む）の策定。

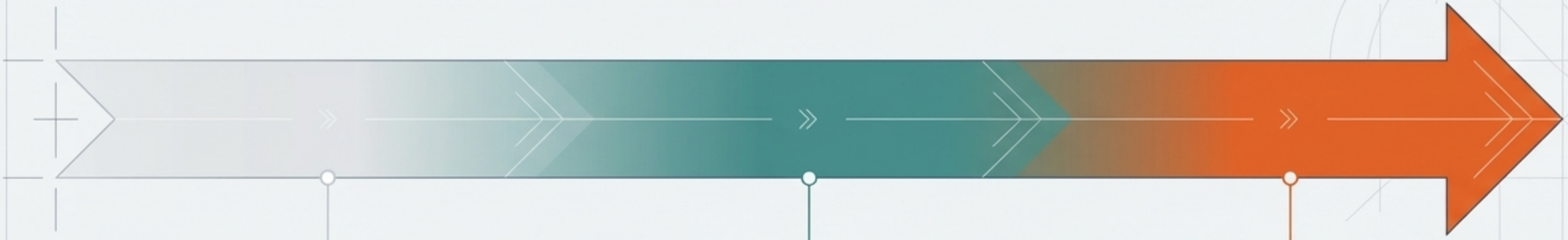
Stage 3: 出力と説明 (Output & Transparency)

条項: U-3, U-6, U-7

外部向け成果物の人間レビュー（HITL）。
ステークホルダーへの「AI利用の通知」と問い合わせ窓口の設置。
ベンダー評価シートを通じた文書管理。

「利用者側の運用」が重くなる：ログ・権限・運用監査まで含めた“継続運用設計”が第1.2版の主戦場。

人間の介在（HITL）要求水準のスペクトラム



内部業務の効率化
低リスク / 低い人間介入

社内メールの起草、議事録の要約、ブレインストーミング。

Governance
従業員のリテラシー教育に依存。標準的な注意書き（「AI出力＝確定情報ではない」）の表示で対応可能。

対外コンテンツの生成
中リスク / レビュー必須

顧客向け提案書の作成、広告コピーの生成、コード生成。

Governance
出力に基づく事業利用判断の前に、人間による内容確認・誤情報のスクリーニング・権利侵害チェックを義務付け。

個人・集団への重大な影響
高リスク / 人間の承認必須と文書化

採用評価、与信審査、人事評価、自律型AIエージェントによる自動発注。

Governance
人間の承認（HITL）を必須化。AI利用の事前通知、異議申立て導線の整備、人間による再審査プロセス、操作履歴の定期監査。

通常の生成AI利用

Profile:
汎用的なChatGPTやCopilotの業務利用。

Focus:
U-2〜U-7の基本遵守。データ漏洩防止、社内ルール整備、基本的な教育。

Burden:
現場の運用ルールとSaaS設定（学習OFF等）で多くをカバー可能。

高度なAIシステム

Profile:
広島AIプロセス準拠が強く効く、上乗せ統制が推奨される領域。

Trigger Scenarios

1. 決済・顧客対応を自律的に実行する「AIエージェント / フィジカルAI」
2. 個人の権利に重大な影響を及ぼす用途（採用、与信、監視）
3. 大規模な対外コンテンツ発信（IR、報道対応）

Additional Mandates:
導入前のリスク特定・評価・軽減。導入後のインシデント緩和。AIの能力限界の公表による透明性確保。

自社のAI利用ケース棚卸し（台帳管理）において、右側の「高度なAIシステム」に該当するユースケースが存在するかを至急特定せよ。

リスクと法的根拠のマッピング・マトリクス

リスク種別	影響と関連根拠	v1.2該当条項	緩和策・実務対応
Privacy/法的	個人情報保護委員会。プロンプトへの個人情報入力・目的外利用。	U-4 （不適切入力対策）	入力禁止＋例外承認フロー、学習OFF契約/設定、ログ最小化。
Copyright/法的	文化庁。生成物の既存著作物への類似、著作物を含む入力。	広島指針XI（知財保護）	対外利用前のレビュー必須化、類似性・検索スクリーニング。
Security/運用	機密情報漏えい、プロンプトインジェクション、RAG経由の情報漏洩。	U-5 （セキュリティ対策）	DLP導入、RAGデータ分離・最小小権限化、ベンダー要求。
Reputation/運用	消費者庁。ハルシネーションによる誤判断、AIへの丸投げ。	U-2, U-6, U-7 （適正利用・情報提供・説明）	広告審査フローでのAI明示、問い合わせ窓口設置、重要判断のHITL。

短期 (～4 Weeks): 事故が起きる入口を塞ぐ

防御 (Defense) | 推定工数: 10～30人日

入力禁止ルールの徹底と技術的ガード（DLP）、ベンダー規約の初期点検、AI台帳による利用ケースの棚卸し開始。

中期 (1～3 Months): ガバナンスを回し始める

統制 (Control) | 推定工数: 20～80人日

リスク分類に基づく承認ゲートの設置、購買プロセスへのベンダー審査の組込み、必要最小限のログ・監査設計。

長期 (3～12 Months): 説明可能な状態を標準化

透明性 (Transparency) | 推定工数: 80～200人日

マネジメントシステム化（ISO/IEC 42001等に準拠したPDCA）、重要用途の第三者評価、対外的なAI利用表示の整備。

※確定版の公開日・最終差分は未指定のため、ドラフト（第1.2版案）の方向性で前倒し実装し、確定版で微調整するアプローチを推奨。

導入前・運用中の緊急アクションと体制整備（RACI）

導入前・運用中の緊急アクション

- 個人情報・機密・営業秘密の入力防止と例外承認フローの構築。
- 契約・規約における入力データの利用範囲、保持、再利用条件の点検。
- 事故対応用の「社内問い合わせ窓口」の設置とベンダー連携SLAの確認。

タスク	経営層	CAIO/統括	法務/コンプラ	情シス/セキュリティ	事業部門
利用ポリシー制定	A	R	C	-	-
契約・規約レビュー	-	-	R	C	-
入力データ統制	-	-	-	R	R
重要用途のHITL設計	-	R	C	-	R
事故対応・窓口	-	R	-	R	R

（A=Accountable 最終責任, R=Responsible 実行責任, C=Consulted 協議, I=Informed 情報共有）

フェーズ3：グローバル標準への拡張とシステム化

先行企業の対応事例（ピア・プレッシャー）

NEC

AI・生体認証等の人権リスクを特定。規程・ガイドライン・チェックシートを整備し、部門間連携でリスク軽減プロセスを回す体制を開示。

富士通 & ソソフトバンク

富士通：AI倫理ガバナンス（コミットメント、外部委員会等）の体系化。

ソフトバンク：社外有識者が参画する「AI倫理委員会」の設立を公表。

NTTデータ

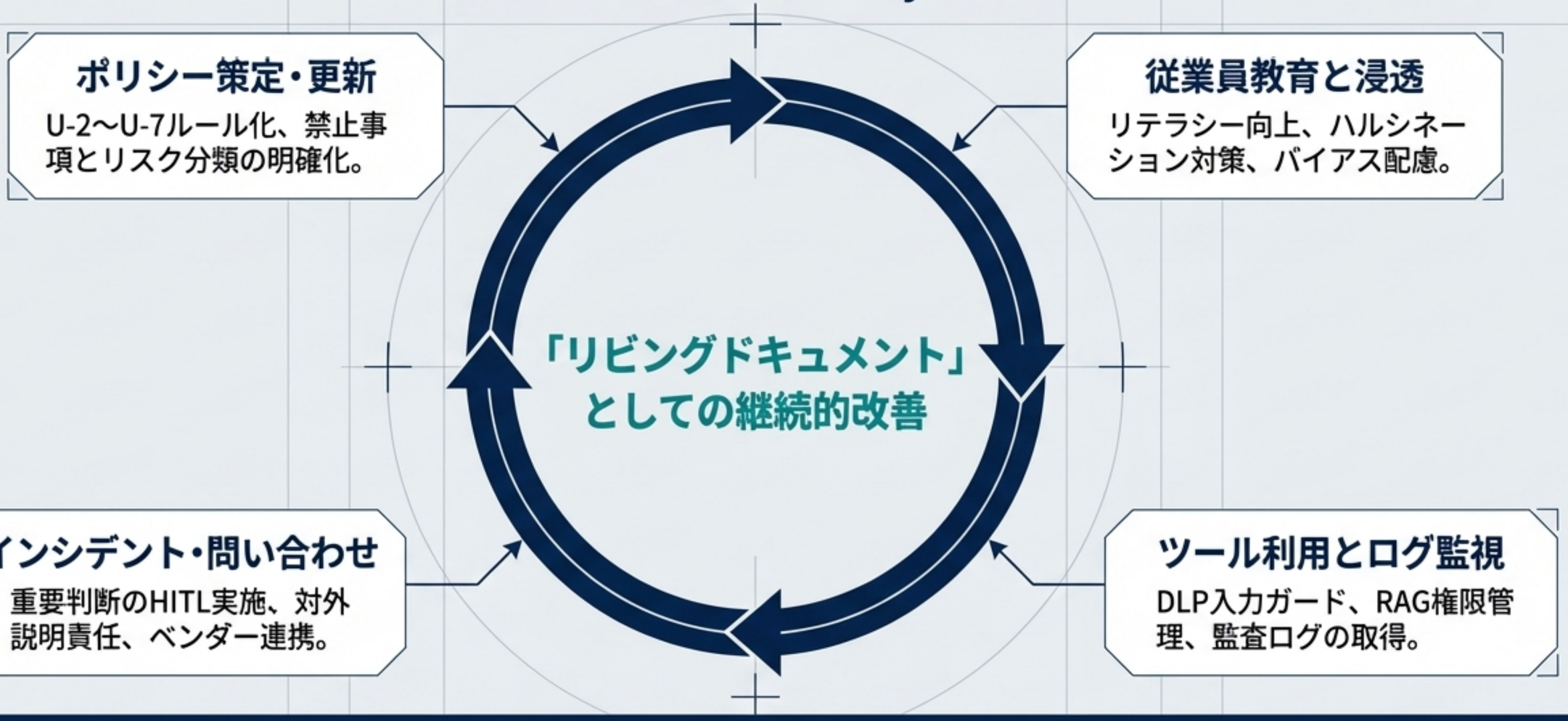
AI憲章、AIリスクマネジメントポリシー、生成AIを含む社内ガイドラインを整備。グローバル展開を前提とした統制フレームワークを確立。

AWS & Global Standards

AWS：ISO/IEC 42001（AIMS）認証取得を公表し、対象サービスを列挙。

インサイト：グローバル企業ほど、第1.2版案が採る方向性をNISTやISO等の国際規格と接続し、先行して「仕組み化」している。

The AI Governance Flywheel



AI事業者ガイドライン第1.2版への対応とは、単なる「ルールの策定」ではありません。それは企業がAIを安全に操るための「連続的な管理システム」を設計し、回し続けることに他なりません。機は熟しました。今すぐフェーズ1の実行へ移行してください。