



第7回人工知能戦略専門調査会

参考資料

2026年10月26日

株式会社ABEJA

— ミッションクリティカル業務で AIを安全に活用するための要件

● AIを安心・安全に使うための7本柱

- ✓ AI単体では安全性を担保できない為、多角的な仕組みが不可欠
- ✓ 7本柱を継続的に適用してはじめて、安心・安全なAI運用が実現



ABEJA
PLATFORM

AIを安心・安全に
使うための

7 本柱

01

セキュリティ

守り続ける



ミッションクリティカル基準

障害や攻撃が起きても、重要な機能やデータを守ることができる

02

ガードレール

防ぎ続ける



ミッションクリティカル基準

AIが誤っても、重大な事故に繋がらない

03

ガバナンス

統制し続ける



ミッションクリティカル基準

人が必要な時に介入・停止でき、経緯を追跡できる

04

冗長化・障害対応

動かし続ける



ミッションクリティカル基準

一部が止まっても、重要な業務を継続できる

05

復旧・再発防止

戻れるようにする



ミッションクリティカル基準

異常が起きても、安全な状態に戻して再開できる

06

評価・監視

測り続ける



ミッションクリティカル基準

通常時だけでなく、例外も含めて安全性を評価できる

07

学習・改善

高め続ける



ミッションクリティカル基準

安全性を確認しながら、継続的に改善できる

共通AI基盤がもたらす付加価値

個別最適の限界

- ✓ 機能ごとに最適なサービスを選ぶと、データが複数のサービス境界をまたいで流れ、経路が複雑化
- ✓ 外部サービス内部の処理は、利用企業側から把握・検証できない

共通AI基盤による一元管理

- ✓ 顧客環境の内側で完結し、データの保管・アクセス・利用を一貫して統制するため、ガバナンスが行き届いたセキュアな環境で運用可能



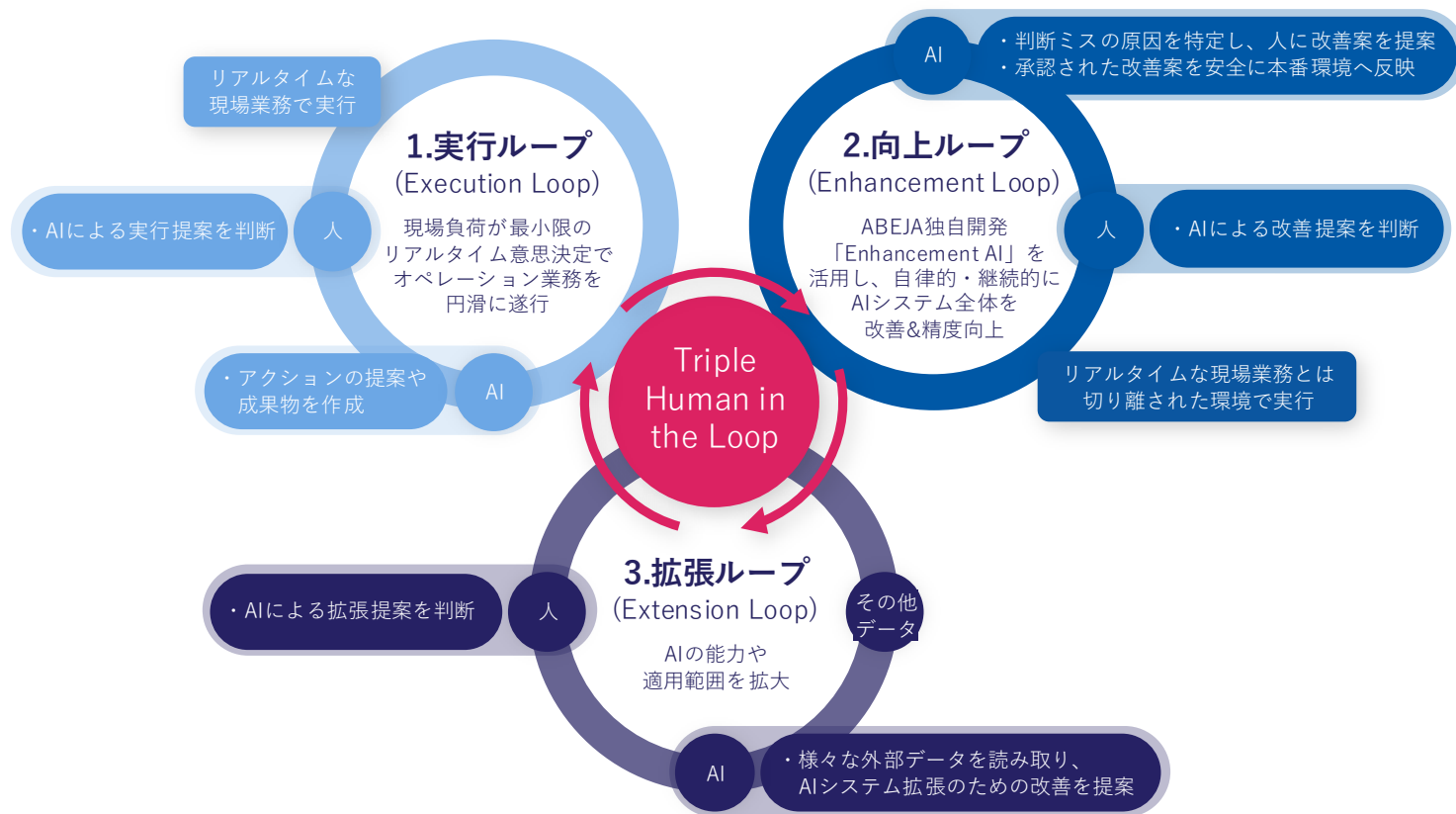
外部サービスの内側はブラックボックス 送信後のデータの保持・非学習を自社側から証明できない	処理の 透明性	処理が基盤の内側で可視化 入力から出力までの実行履歴を一貫して保持
複数の境界をまたいで複雑化 複数のサービスをまたぐ為、データの追跡が困難	データの 流通経路	一つの基盤内で完結 保管・アクセス・利用を一貫して管理できる
サービスごとに管理が分散 それぞれのサービスを個別に監査・統制する必要がある	管理・統制	AIシステム全体を一元管理 権限・設定・ログをまとめて統制・監査

「Human in the Loop」の進化版 「Triple Human in the Loop」の特許出願

● 「安全性」と「AIシステム全体の自律的な改善」の両立で、ミッションクリティカル業務のAI実装を推進

- ✓ 実行・向上・拡張の3つのループそれぞれに、人とAIのフィードバックプロセスを組み込み
- ✓ 現場の業務負荷を最小限に抑えながら、高品質な再学習データを自動で抽出・蓄積
- ✓ ABEJA Platformに搭載済みの「ガードレール機能」と組み合わせることで、安全性・堅牢性をさらに強化

「Triple Human in the Loop」によって実現可能になるAI利活用



日常の現場業務負荷を最小限に抑えながら、
「安全性」と「AIシステム全体の自律的な改善」を両立し、
ミッションクリティカル業務のAI実装をより強固に推進することが可能