

読者特典ハンドブック

AI ガバナンス実装ハンドブック

時制で動く、3 段階のロードマップ

本書「AI を使う会社、使われる会社」第 8 章の補完冊子

このハンドブックの使い方

本書（AI を使う会社、使われる会社）の第 8 章では、AI ガバナンスを取り巻く外部環境——国内のガイドライン、国際標準（ISO/IEC 42001）、グローバル規制（EU AI Act）——の全体像をお伝えしました。

このハンドブックは、「外部要請を理解した次のステップ」として、何を・いつ・どの順番で実装するかを時制ごとに整理した実践ガイドです。本書の第 1～9 章で学んだ内容を、実際の業務に落とし込む際のチェックシートとして活用してください。

本ハンドブックの 3 段階構成

Part 1（今すぐ～1 ヶ月）：国のガイドラインへの対応状況を確認する

Part 2（3～6 ヶ月）：ISO/IEC 42001 の最小実装を始める

Part 3（1～3 年先）：認証取得とグローバル規制への備えを計画する

【ご注意】 本ハンドブックおよび本書に記載の ISO/IEC 42001 の内容は意識しております。正確な内容は、ISO/IEC 42001 の正式な原文を参照ください。

時制	テーマ	主な内容
今すぐ～1 ヶ月	国のガイドライン対応確認	本書第 1～7 章の実践内容を AI 事業者ガイドラインに照合する
3～6 ヶ月	ISO/IEC 42001 の最小実装	要求事項の優先度に沿って Annex A 管理策・PDCA を整備する
1～3 年先	認証・グローバル規制への備え	認証取得ロードマップの確認・EU AI Act 対応タイムラインの把握

Part 1 今すぐ～1ヶ月

国のガイドラインへの対応状況を確認する

AI 事業者ガイドライン対応チェック

総務省・経済産業省が策定した「AI 事業者ガイドライン（第 1.1 版）」は、AI 利用者に対して 3 つの取り組みを求めています。本書で実践した内容が、すでにこれらに対応しているかを確認しましょう。

■ 取り組み① 利用方針の整備

社内での AI ツールを、どのような目的で使うかを明文化すること。

- ☐ AI 台帳を作成し、使用ツール・部門・目的を記録している（本書 第 8 章・第 9 章）
- ☐ AI 利用ガイドラインの初版を社内に配布している（本書 第 7 章）
- ☐ AI 方針文書（1 ページ）を経営者が承認・周知している（本書 第 6 章）

■ 取り組み② 適切な利用範囲の設定

どの業務に AI を使ってよく、どの業務には使うべきでないかを判断する基準を持つこと。

- ☐ 情報の 3 分類（公開情報・社内限定情報・機密情報）を定め、社内で共有している（本書 第 4 章）
- ☐ 入力判断フローチャートを社員が使える状態にしている（本書 第 4 章）
- ☐ 「AI を使わない領域」を経営者として明示的に決定している（本書 第 6 章）

■ 取り組み③ 利用者教育の実施

社員が判断に迷わないよう、必要な知識とルールを共有すること。

- ☐ 全社員に最小知識研修（30 分以上）を実施している（本書 第 7 章）
- ☐ 「困ったときの相談先」をガイドラインに明記し、周知している（本書 第 7 章）
- ☐ AI ガバナンス責任者を指名し、社内に告知している（本書 第 6 章）

対応状況の判断基準

9項目すべてにチェックが入った方：

ガイドラインへの基本対応は完了しています。Part 2 へ進んでください。

5～8項目チェックできた方：本書を再読しながら残りの項目を埋めてください。

4項目以下の方：まず本書の第2章・第4章・第6～7章から始めてください。

Part 2 3～6 ヶ月

ISO/IEC 42001 の最小実装を始める

※ ISO/IEC 42001 の記載内容は意識です。正確な内容は正式な原文を参照ください。

ISO/IEC 42001 とは（簡単なおさらい）

ISO/IEC 42001 は、AI のマネジメントシステムに関する国際規格（2023 年 12 月発行）です。

「完璧な AI システムを構築せよ」という要求ではなく、「AI を安全に使うための仕組みを持ち、継続的に改善せよ」という要求です。中小企業でも対応できる設計になっています。

2-1 要求事項の優先度

全 20 項目の要求事項のうち、AI 利用者として最低限押さえるべきものを優先度別に整理します。

【今すぐ対応する】（経営者として必須）

要求事項	対応内容と本書との対応
Req.1 組織の状況	四象限分析・自社の外部環境の整理（本書 第 1 章）
Req.3 スコープの定義	AI 台帳対象ツールの明文化（本書 第 8 章）
Req.4 リーダーシップ	経営者自身による AI 方針の承認と周知（本書 第 6 章）
Req.5 AI 方針	一ページの AI 方針文書の策定（本書 第 5～6 章）
Req.6 役割と責任	AI ガバナンス責任者の指名（本書 第 6 章）

【3 ヶ月以内に対応する】（ガバナンス基盤として推奨）

要求事項	対応内容
Req.7 リスクと機会	AI 台帳の各ツールへのリスクレベル付与
Req.8 リスクアセスメント	主要 AI ツールのリスク評価と記録
Req.13 認識・コミュニケーション	全員への最小知識共有（本書 第 7 章）
Req.15 運用管理	AI ツール変更時の手順書の作成

【半年以内に対応する】（成熟度向上として推奨）

要求事項	対応内容
Req.9 リスク対応と SoA	管理策の選定と適用宣言書（簡易版）の作成
Req.10 AI 影響評価	主要 AI ツールの「影響範囲チェックシート」記入
Req.14 文書管理	全 AI 関連文書への版数・承認者の記載
Req.16～19 監視・監査・ レビュー・改善	月次レポートと年次自己点検の開始

2-2 Annex A / Annex B 「何を」と「どのように」——整備すべき3管理策

ISO/IEC 42001 の Annex A は「何をするか」を定めた管理策、Annex B はその「どのように実装するか」を示す実装ガイダンスです。AI 利用者として特に押さえるべき3管理策を、「何を」——「どのように」のペアで整理します。

A.9.2 プロセス定義（AI の利用状況を業務プロセスと関連付ける）

求めていること：

新しいAI ツールを導入した場合、または利用範囲が変わった場合に、台帳を更新して再評価すること

対応する実践：

AI 台帳の「変更時の手順」として、新ツール導入時は1週間以内に台帳を更新するルールを設ける
(本書 第8章)

B.9.2 プロセス定義の実装ガイダンス——「どのように定義するか」

業務プロセスとAI 利用の対応関係を文書化する。

記述項目の例：

「提案書作成プロセス→ChatGPT を文章下書きに利用・担当：営業部」

- ✓ 「誰が・何のために・どのように」を業務手順書レベルで記述する。
- ✓ 初期は簡潔にし、ガバナンスの成熟度に応じて詳細化する。
- ✓ 見直しのトリガーを事前に定める。

例：新ツール導入・利用範囲の拡大・担当者変更・年次定期見直し

A.9.3 利用目的の特定（合理的な目的を明示する）

求めていること：AI を使う目的が明確で合理的であることを確認し、記録すること

対応する実践：

AI 台帳の「使用目的」欄に「なぜこのツールを使うか」を具体的に記載する
(「便利だから」ではなく「〇〇業務の△△のために使う」という形式)

B.9.3 利用目的の特定に関する実装ガイダンス——「目的のずれを検知する」

目的の記述は「なぜそのAIを使うか」だけでなく「何を達成したいか」まで含める。

例：「提案書作成の時間を半分にし、内容の一貫性を高める」

- ✓ 実際の利用状況と目的の一致を定期確認する。

方法の例：四半期ごとの部門ヒアリング、月次レポートの「利用目的」欄の突合

- ✓ 目的から逸脱した利用が発覚した場合の対処手順を事前に定める。
- ✓ AI ツールの機能アップデートにより目的自体が変わる可能性も考慮する。

A.9.4 利用実態の記録（AIの利用状況を追跡する）

求めていること：

AI がどのように使われているかを監視・記録すること

対応する実践：

月次のAI利用状況レポート（A4半ページ）の作成と保管。「今月の新規ツール」「インシデントの有無」「ガイドライン違反の有無」を確認する（次節のPDCA参照）

B.9.4 利用実態の記録に関する実装ガイダンス——「何を・どのように記録するか」

記録の最小セット：利用日時・利用者・ツール名・主な利用目的・入力情報の種別。

- ✓ 全利用ログを詳細に記録する必要はなく、台帳の月次更新と月次レポートの保管で対応できる形で運用する

保管期間の目安：内部監査サイクルに対応できる最低1年。

- ✓ インシデント調査に使用できる形式で保管し、「いつ・誰が・何を使ったか」を後から追跡できる状態を維持する
- ✓ 完全なログが取れない場合は、ツールの利用開始・変更・廃止の申告・承認フローを記録に代替することも許容される

2-3 PDCA サイクルの最小実装

ISO/IEC 42001 が求める PDCA サイクルを、中小企業が最小工数で回す方法を示します。

月次（毎月 15 分）：AI 利用状況レポートの確認

確認項目（A4 半ページのメモで十分）

- 今月、新しい AI ツールを使い始めた社員・部門はあるか
- AI に関するインシデント（情報漏えいの疑い・誤情報による問題等）は発生したか
- ガイドライン違反の報告はあるか
- AI 台帳の更新が必要な変化はあるか

年次（年に 1 日）：内部監査（自己点検）の実施

点検対象の 4 点セット

- AI 台帳：最新の状態に更新されているか
- AI 利用ガイドライン：現在の実態に合っているか、改訂が必要か
- 研修記録：全社員への研修が実施・記録されているか
- インシデント記録：発生したインシデントとその対応が記録されているか

年次（経営会議に 15 分追加）：マネジメントレビューの実施

年次の経営会議に「AI ガバナンスレビュー」の議題を追加します。以下の 3 点を経営者として確認・判断し、その記録を残します（ISO/IEC 42001 第 18 条「マネジメントレビュー」への対応）。

- ☐ 今年の AI 利用状況は適切だったか
- ☐ ガイドラインを更新する必要があるか
- ☐ 新たなリスクは発生しているか、来年度の対応方針は何か

Part 3 1～3 年先

認証取得とグローバル規制への備えを計画する

3-1 ISO/IEC 42001 認証取得のロードマップ

「ISO/IEC 42001 の認証を取りたい」という場合、どのような準備が必要かを整理します。認証取得は急ぐ必要はありません。本書で紹介した内容を一つずつ実装していくことが、最も着実な認証への道です。

認証取得の主なステップ（10 段階）

	内容
Step 1	AI マネジメントシステム導入への経営層コミットメント（AI 方針・目標の策定・承認）
Step 2	AI マネジメントシステムの文書化（方針・手順書・記録の整備）
Step 3	全社員への教育・啓発の実施と記録
Step 4	AI リスクアセスメントの実施と文書化
Step 5	プレアセスメント（事前評価・ギャップ分析）の実施
Step 6	内部監査の実施（定期的な自己評価）
Step 7	マネジメントレビューの実施と記録
Step 8	外部認証審査 ステージ 1（文書審査）の受審
Step 9	外部認証審査 ステージ 2（実地審査）の受審・合格
Step 10	認証維持のためのサーベイランス審査（3 年に 1 回）への継続対応

費用感の目安

企業規模・業種・審査機関によって異なりますが、中小企業では以下が目安です。

準備コスト（コンサルティング・社内工数・教育）：数十万円～

審査費用（認証機関への支払い）：数十万円～

合計目安：数十万円～数百万円（規模・範囲による）

審査前に一定の運用期間（通常 3 ヶ月～半年）が必要です。

「今すぐ取得できる」ものではありません。

認証を急ぐ必要はありません。「取得できる水準に向けて整備を始める」だけで、取引先や顧客への説明力という価値は生まれ始めます。

3-2 EU AI Act 対応タイムライン確認表

EU AI Act（人工知能法）は 2024 年 8 月に施行されました。日本の中小企業が直接の規制対象になるケースは限られますが、グローバルサプライチェーンを通じた間接的な影響を把握しておくことが重要です。

時期	内容	中小企業への影響
2024 年 8 月	EU AI Act 施行	日本企業への直接適用はなし。ただし EU 市場向けの AI サービスを提供する場合は注意
2025 年 2 月	禁止慣行・AI リテラシー義務の適用開始	EU 域内の組織は社員の AI リテラシー確保が義務化。日系企業の EU 拠点に影響
2025 年 8 月	GPAI（汎用目的 AI）モデルへの義務適用開始	ChatGPT 等の GPAI を使ったサービスを提供する企業に影響
2027 年 12 月	全面適用（予定）	サプライチェーン連鎖が本格化。大企業からの「AI ガバナンス方針の提出要求」が増加する可能性が高い

サプライチェーン連鎖への備え（今からできること）

取引先の大企業から「AI ガバナンス方針を提出してほしい」と求められる前に、以下を準備しておく

- ☐ AI 利用ガイドライン（社外提示版）の用意
- ☐ AI 台帳の概要を説明できる資料の準備
- ☐ 「どのような情報を AI に入力していないか」を説明できる体制の整備

経営者の自己点検シート

本書 第 8 章の「経営者として今日から持つべき 3 つの問い」を、週次・月次・年次で確認するシートです。

問い	確認タイミング	チェック項目
問い① 自社の AI 利用は問題ないか？	週次：AI 台帳と最新の利用申請を確認する	☐ 新しい AI 利用申請に未対応がない ☐ 直近 1 週間にインシデント報告がない
問い② ISO/IEC 42001 は中小企業に現実的か？	月次：自社のガバナンス成熟度を点検する	☐ 月次 AI 利用状況レポートが運用されている ☐ Annex A.9.2/9.3/9.4 の実装が進んでいる
問い③ EU AI Act は日本の中小企業に関係あるか？	年次：取引先からの要請への準備度を点検する	☐ AI 利用ガイドライン（社外提示版）の準備 ☐ 取引先からの AI 利用方針照会に答えられる

参考情報

本書との対応関係

ハンドブック	本書の参照箇所
Part 1（ガイドライン対応確認）	本書 第 1～7 章の実践内容と対応
Part 2（ISO/IEC 42001 最小実装）	本書 第 8 章 第 3 節・第 5 章を参照
Part 3（認証・グローバル規制）	本書 第 8 章 第 3 節・第 4 節を参照
自己点検シート	本書 第 8 章 第 6 節「経営者の 3 つの問い」を参照

参考資料

- 総務省・経済産業省「AI 事業者ガイドライン（第 1.1 版）」（2025 年 3 月）
- ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system
- 欧州連合「EU AI Act（Regulation 2024/1689）」（2024 年 8 月発効）
- 情報処理推進機構(IPA)「AI 利用時のセキュリティ脅威・リスク調査 調査報告」
(<https://www.ipa.go.jp/security/reports/technicalwatch/eid2eo00000022sn-att/report.pdf>)（2024 年）

【ご注意】 本ハンドブックおよび本書に記載の ISO/IEC 42001 の内容は意訳しております。正確な内容は、ISO/IEC 42001 の正式な原文を参照ください。

本ハンドブックは「AI を使う会社、使われる会社」の読者特典です。転載・複製はご遠慮ください。

■ 本テンプレートの利用条件

本資料は、書籍『AIを使う会社、使われる会社』
(中小企業経営者のためのAI安全活用戦略)の読者特典です。

【できること】

- ・ご自身が経営・所属する組織の業務のために、複製・編集・社内配布して利用すること

【できないこと(禁止事項)】

- ・第三者への再配布・転売・貸与(社外への共有を含みます)
- ・有償の研修・セミナー・コンサルティング等の教材・成果物としての利用
- ・自社の製品・サービスとしての再パッケージ・再頒布
- ・インターネット上へのアップロード(公開の有無を問いません)

【著作権・免責】

- ・本資料の著作権は著者に帰属します。
- ・本資料は情報提供を目的としており、法的助言ではありません。実際の経営判断・法的判断は弁護士等の専門家にご相談ください。本資料の利用により生じた損害について、著者は責任を負いません。

【正規入手先】

- ・本資料の正規配布元: grclab.jp(ハイフンなし)
- ・上記以外の場所で本資料を入手された場合は、正規配布元から最新版をご入手ください。

© 新田晃啓 All Rights Reserved.