ISO/IEC 42001監査への準備

― AIマネジメントシステムのベストプラクティス ―



PECB REGIONAL WEBINARS

講師紹介

中 村　玲 子（ナカムラ レイコ）
ドイツ品質システム認証株式会社（DQS Japan Inc.）
営業部　セールス・マネージャー

■ **プロフィール**
- アメリカ西海岸の大学 建築学部卒業
- 衆議院議員 秘書を経て、外資系認証機関にてキャリアを構築
- 米系認証機関5年、欧州系認証機関17年勤務。22年以上にわたり認証ビジネスに従事

■ **実績**
- 750社以上の認証営業・統括を担当
- 組織再編（統合・合併・拡大・縮小）に伴う認証支援、研修カスタマイズ提案、プレスリリース発信
- 新規規格の市場導入・立ち上げを主導

■**主な立ち上げ・推進規格**
TISAX（自動車情報セキュリティ）,VCS（車両サイバーセキュリティ）
ISO 42001（AIマネジメントシステム）,ISO 20121（国際イベント規格）,IRIS（鉄道産業規格）

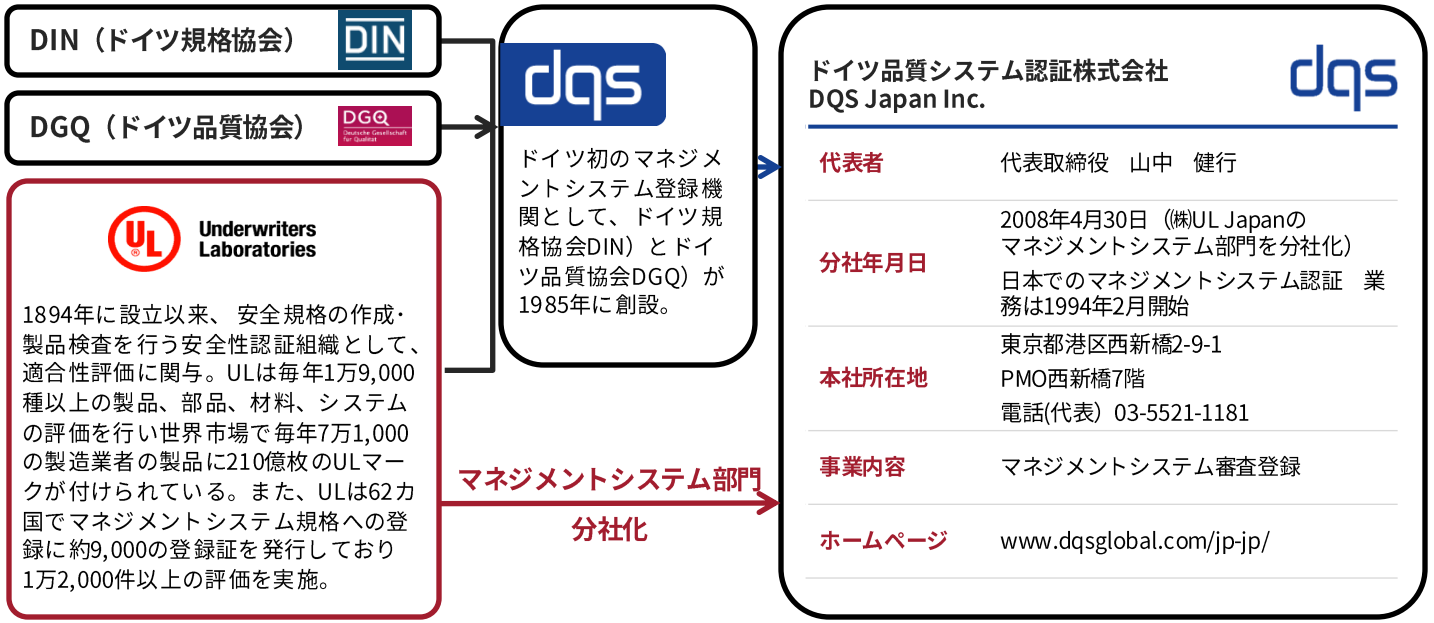
DQSグループのご紹介



- 1985年にドイツで最初のマネジメントシステム認証機関として設立
- グループで2,500人の審査員
- 世界60ヶ国に80事務所/支店
- 100ヶ国以上において63,000の登録証を発行
- 世界各国トップクラスの認証機関が加盟するネットワーク及び１か国で１組織しか認められていない「IQNet」の正会員
- 発行認証数30万件以上、世界シェア　20%



DQS Japan 会社概要



DQS Japan ビジネス

受審企業様のシステム改善と発展をサポートするマネジメントシステム規格の認証機関

DQS Japan の具体的な認証サービス

- **AIマネージメントシステム（ISO42001）**
- 車載情報セキュリティ(TISAX)
- 情報セキュリティマネジメントシステム（ISO27001)
- 自動車産業品質マネジメントシステム（IATF16949）
- 品質マネジメントシステム（ISO 9001）
- 環境マネジメントシステム（ISO 14001）
- 労働安全衛生マネジメントシステム（ISO 45001）
- 車載サイバーセキュリティー（ISO21434／VCS）
- 医療機器ー品質マネジメントシステム（ISO13485)

当社の主要な認定機関

ENX
ANAB
VDA QMC Qualitäts Management Center im Verband der Automobilindustrie
JAB
DAkkS
isms-AC

Agenda

1. 本日の目的
2. なぜ今ISO/IEC 42001なのか
3. ISO/IEC 42001
4. 他規格との親和性
5. ISO/IEC 42001認証プロセス
6. 審査の現場で見られる課題
7. 認証取得までの一般的ステップ ～ベストプラクティス～
8. まとめ

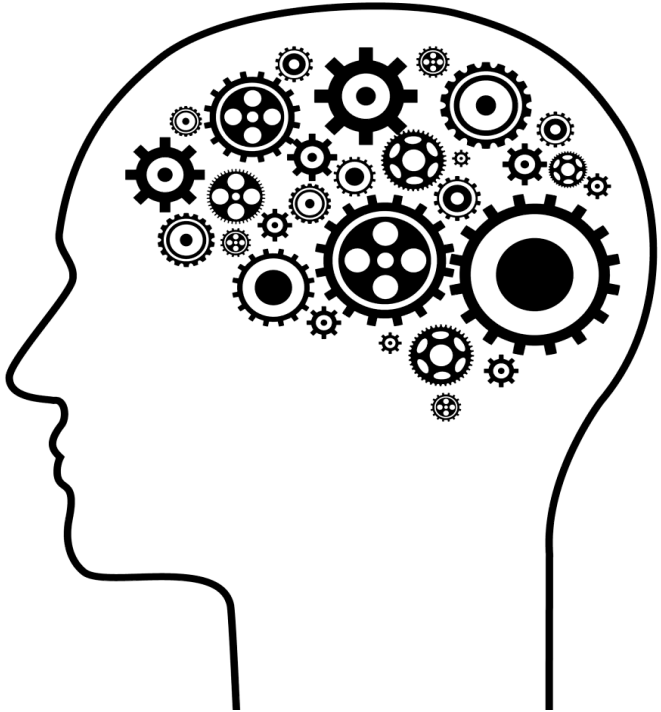
1.本日の目的

1. ISO/IEC 42001の本質を理解する

2. ISO/IEC 42001の認証プロセス

3. 実践的な準備方法を学ぶ

2.なぜ今、ISO/IEC 42001なのか



AIとは

- AIはArtificial Intelligence(人工知能）を意味し、1956年にダートマス会議で初めて使用されました。
- 未だ確立された定義は存在しませんが、「人工」「知能」とあるように、人間の思考プロセスと同じような形で動作するコンピュータープログラム、コンピュータ上で知的判断を下せるシステム等を指します。



AIとは

- **AIシステム**

・人間が定義した所与の目標の集合に対して、コンテンツ、予測、推奨、意思決定等の出力を生成する工学的システム（ISO/IEC 22989:2022）

- **AI 開発者（AI Developer）**

・AI システムを開発する事業者(AIを研究開発する事業者を含む）。

- **AI 提供者（AI Provider）**

・AI システムをアプリや製品、既存システムや業務プロセスに組み込み、AI利用者や場合によっては一般利用者へ提供する事業者。

- **AI 利用者（AI Business User）**

・事業活動において、AIシステム又はAIサービスを利用する事業者

AIの「管理」が経営課題になる

■AIは「試す」段階から「事業に組み込む」段階へ

●現状：
各部門で生成AI等のツール導入が進み、業務効率は向上しています。一方、その利用は個々の従業員のスキルやリテラシーに依存しており、全社的な統制がとれていない「シャドーAI」状態
⇒統制できない

●顕在化するリスク：
・情報漏洩・セキュリティリスク：機密情報や顧客情報をセキュリティが担保されていないAIサービスに誤って入力してしまうインシデント発生
・コンプライアンス・倫理リスク：学習データの管理が甘く、AIの生成物に著作権侵害や差別的な表現、不正確な情報が含まれる可能性
・業務品質のばらつき：AIの出力結果を鵜呑みにすることで、業務品質が低下、不安定化。
・システム性能や公平性に対するバイアス：ユースケースに適した性能や公平性の確保不足。

●結論：
AIの利便性を享受し続けるためには、もはや「自由な活用」だけでは不十分。
「攻め（活用推進）」と「守り（リスク管理）」を両立させる
体系的なマネジメントシステムの構築が不可欠な経営課題となっている。

情報セキュリティ10大脅威　2026

IPA 独立行政法人 情報処理推進機構

IPAについて

情報セキュ

情報セキュリティ10大脅威 2026

公開日：2026年1月29日
最終更新日：2026年3月12日

「情報セキュリティ10大脅威 2026」は、2025年に発生した社会的に影響が大きかった情報セキュリティの事故や攻撃の状況などから、IPAが脅威候補を選定し、情報セキュリティ分野の研究者、企業の実務担当者など約250名のメンバーからなる「10大脅威選考会」が審議・投票を経て決定したものです。
「組織」向け脅威については順位を併記し、「個人」向けでは脅威名のみを五十音順で記載しています。複数の脅威にまたがる事案もあるため、各自の環境に照らし選出された脅威については、極力もれなく対策を行うことが求められます。

情報セキュリティ10大脅威 2026 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

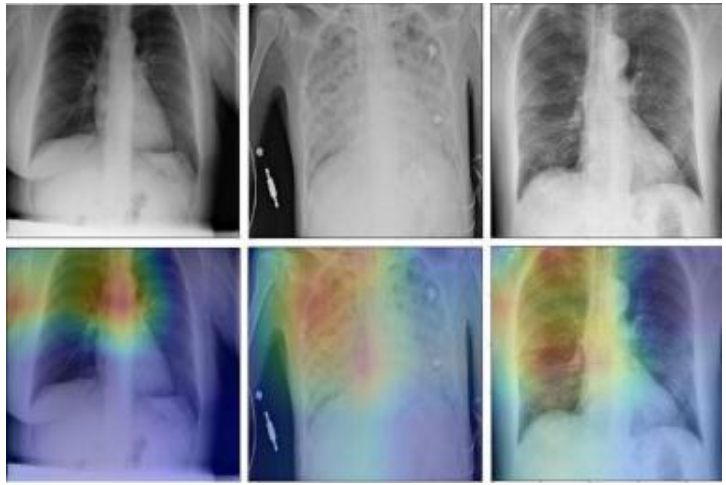
医療分野におけるAIの影響力

インゼル病院およびベルン大学の研究成果
胸部X線画像のAI解析手法を開発

主な結果（全症例対象）
- **AI**の正確性：**94%**
- 放射線技師の正確性：**61%**

COVID-19の検出精度
- **AI**：**97%**
- 放射線技師：**53%**

ISO/IEC 42001などの標準は、医療のような重要な分野で**信頼性が高く、透明性があり**、安定したAIシステムを保証するのに役立ちます。





刑事司法制度におけるアルゴリズムによる意思決定



– **アメリカの裁判所におけるAI活用**

・被告人の再犯リスクをAIで評価

・過去の犯罪データを基に分析

⚠過去の偏見を引き継ぐ可能性

– **法執行機関でのAI活用が拡大**

・**予測的パトロール：**
⇒ アルゴリズムを通じて警察官の重点巡回地域を決定

・**顔認識：**
⇒ 容疑者をリアルタイムで特定

・**リスク評価ツール**
⇒ 個人情報から再犯スコアを計算

日本におけるAIガバナンスの規制アプローチ

人間中心、アジャイル的アプローチ

・AI推進法（AI基本法）が2025年に成立
  -イノベーションを創出するための法律であり、AIのリスクに対しての規制ではない
・法規制ではなく、**ガイドラインベース**の対応が主流
・AI事業者ガイドライン（第2.0版）による官民共通の指針（2026年改訂）
・AI戦略会議による機動的な方針決定（アジャイル・ガバナンス）
・**既存法律によるAI問題への対処**
  -AIの利用そのものを直接規制する罰則法はない。

監査・評価の動向：

・事業者の自主点検（セルフチェック）とディスクロージャーを推奨
・AIセーフティ・インスティテュート（AISI）による安全性評価や、“レッドチーミング”の標準化が進行中（特に国産LLMや高度AIモデル）
・「AIガバナンス・コード」の導入検討
・「遵守するか説明するか（コンプライ・オア・エクスプレイン）」方式を採用し、社会的な信頼性を確保



政策の基本方針：「人間中心のAI社会」を掲げ、アジャイル（機動的）なガバナンスを通じて、安全性とイノベーションの最適バランスを追求する。

米国におけるAIガバナンスの規制アプローチ

イノベーション志向かつ断片的なアプローチ

- AIに関する包括的な連邦法は未整備（2025年現在）
- 法規制ではなく、**ガイドラインベースの対応**が中心
  - **NISTによるAIリスクマネジメントフレームワーク（任意適用）**
  - **大統領令による行政的指示**
    例：2023年 バイデン政権による「安全かつ信頼できるAI」に関する大統領令
  - **業界別の規制（例：医療、金融など）**

監査・評価の動向：

- **セルフチェックや内部リスク評価**による自己規制が主流
- AIモデルに対する初期的な評価手法や“レッドチーミング”の導入が進行中（特に最先端モデル）
- **採用・融資などにおけるアルゴリズム監査の圧力が高まる傾向**
  例：ニューヨーク市のAEDT法（自動化雇用意思決定ツール規制）など、**地方レベルの規制**が先行



政策の基本方針：「企業の自主的責任あるAI運用」を促進しつつ、最小限の連邦規制でイノベーションと競争力を守る。

中国におけるAIガバナンスの規制アプローチ

国家主導・政治目標に強く連動した集中管理

- 国家による高度な中央集権的管理・社会的安定や共産党の統制といった政治目標の実現に向けた積極的な規制運用
- 主要な規制ルール：
  - 生成系AI規制（2023年）
    セキュリティ審査、コンテンツフィルタリング、ユーザーの実名確認を義務付け
  - アルゴリズム規制（2022年）誘導的・操作的なアルゴリズムの制限
    「正のエネルギー（ポジティブな価値観）」の推進を強制
    すべての主要アルゴリズムは政府への登録・審査対象

監査・評価体制：

- **コンテンツ管理、セキュリティチェック、価値観との整合性**に重点
- 政府による**直接的な検査**と、企業内部による**自己管理体制の整備**を要求
- 違反時には**罰金、機能制限、最悪の場合はサービス禁止**の可能性もあり



政策の基本方針：経済成長にAIを活用する一方で、強力なイデオロギー的・社会的統制を維持すること。

EUにおけるAIガバナンスの規制アプローチ

規制主導型アプローチ

- 中核となる枠組み：EU AI法（2024年に採択）EUのアプローチは予防原則と基本的人権の尊重に基づいており、リスク管理、透明性、人による監督に重点を置いている。

- **主要な要素：**
  - **リスク分類**（許容不可、高リスク、限定リスク、最小リスク）
  - **高リスクシステムに対する適合性評価と独立監査の義務**
  - **生成AIに対する厳格な透明性要件**（例：AI生成コンテンツの明示）
  - **データ品質および非差別性に関する高度な要件**

監査:
- **独立機関による定期的な監査**
- **文書化・トレーサビリティ・責任の明確化**に対する検証義務



政策の基本方針：基本的人権の保護、リスク回避、信頼できるAIの育成。
—— たとえ**イノベーションのスピードを犠牲にしても**、これらを優先する。

欧州連合（EU）の人工知能法（AI法）第71条 罰則

- AIシステムが、第5条および第10条に規定されているもの以外の、本規則に基づく要件または義務を遵守しない場合、最大2,000万ユーロの行政罰金、または違反者が企業の場合は、前会計年度の全世界年間売上高の4%のいずれか高い方の金額が科せられる。

– 誤った情報、不完全な情報、または誤解を招く情報を、通知機関や各国の主管当局からの要請に対して提供した場合、行政罰の対象となります。
– その罰金は最大1,000万ユーロ、または企業の場合は前年度の全世界年間売上高の最大2%のいずれか高い方が適用されます。

€20,000,000

法令違反に対する罰金

比較のまとめ

特徴	日本	EU（欧州連合）	US（アメリカ）	中国
アプローチ	人間中心、アジャイル型	リスクベース、権利主導型	イノベーション主導、ライトタッチ（緩やかな規制）	国家管理、安全保障主導型
主な焦点	イノベーションとリスク対応の両立	信頼、安全性、基本的人権	イノベーション、競争	統制、安全保障、政治的安定
監査	事業者による自主点検、ガイドライン準拠	外部監査、高リスクAIには義務付け	自発的、セクター別、内部監査	国家監査、検閲メカニズム
透明性	努力義務、ガイドラインでの明示推奨	多くのシステムで義務化	推奨されるが、強制力はない	限定的、国家による指示
執行（罰則）	非拘束的（現時点では罰則より指導重視）	独立機関による監視、罰金	断片的（省庁や法律に依存）	中央集権的な執行、多額の罰金

最終評価（Final Assessment）

日本：柔軟なガイドラインと法整備を組み合わせた「アジャイル・ガバナンス」を推進
→「世界で最もAIを使いやすい国」を目指し、社会実装を加速。欧米の規制格差を埋める国際的な橋渡し役を担う。

EU：規制の詳細性と監査可能性において主導的立場
→ グローバルスタンダードを形成する一方で、導入スピードの低下の可能性あり

米国：規制面では遅れがあるものの、イノベーションを最優先
→ 柔軟性は高いが、説明責任は相対的に弱い

中国：AI規制を国家統制の手段として活用
→ 権利保護や企業の透明性よりも、安全保障と政治的統一性を重視

AIがISO 42001によって規制されるべき理由

- 信頼の構築
  標準規格は透明性とトレーサビリティを実現します ユーザーと顧客は、検証済みの標準規格に従って運用されるAIシステムに対して信頼感を抱きます

・リスク
ISO 42001は、組織が差別、誤情報、システム障害などのリスクを体系的に特定し、管理するのに役立ちます

・法的側面
明確な規制により、企業は既存および今後施行される法律（例：EU AI法）への準拠が容易になります 文書化されたプロセスと責任範囲によって、法的責任の問題がより明確になります

・相互運用性と国際競争力
国際標準規格は国境を越えた協力を促進します ISO 42001の認証を取得した企業は、グローバル市場でより容易に事業を展開できます

・倫理原則の推進
この規格は、公平性、データ保護、セキュリティ、人間中心主義などの倫理原則を支持します

AIが規制されなかった場合、何が起こるのか？

● 信頼の喪失
適切なルールがなければ、欠陥・偏り・操作の可能性を持つAIシステムが広まり、社会からの信頼を失う恐れがあります。

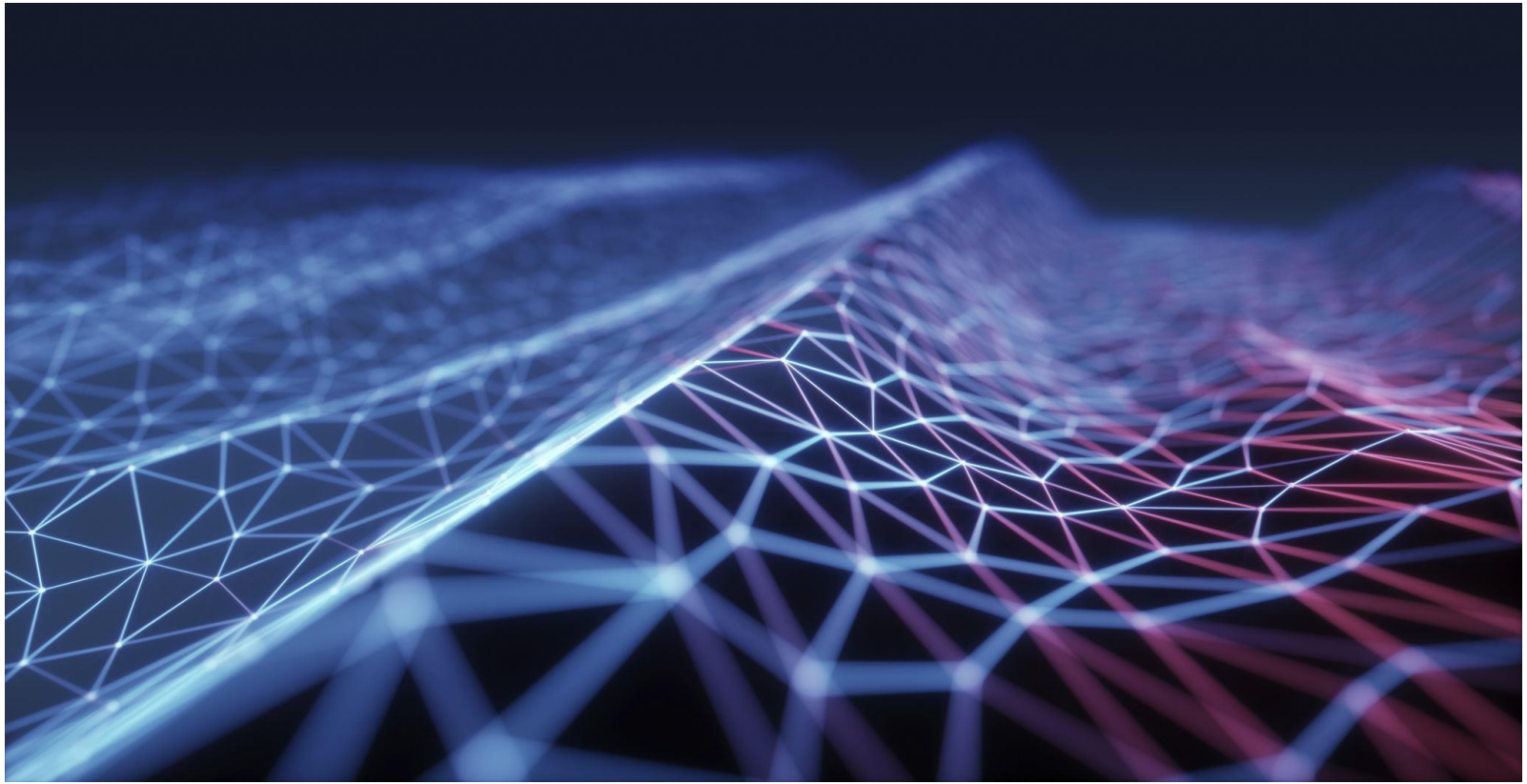
● 被害や差別の拡大
倫理的な管理がないAIは、差別を助長したり、危険な判断を下す可能性があります。
（例：医療、司法、金融など）

● 制御されない発展と透明性の欠如
共通の基準がなければ、企業は仕組みが不透明な「ブラックボックス型」のAIを開発し、追跡や検証が困難になります。

● 不公平な市場環境
倫理やセキュリティに配慮する企業が、最低基準がない市場では競争上不利になる可能性があります。

● 地政学的リスクの拡大
国際的なルールがなければ、AIは一部の国家や巨大企業による権力の手段となり、民主主義や国際秩序に大きな影響を及ぼす可能性があります。

3.ISO/IEC 42001





ISO 42001について

PECB REGIONAL WEBINARS

ISO/IEC 42001(AI マネジメントシステム/AIMS）とは①

【名称】

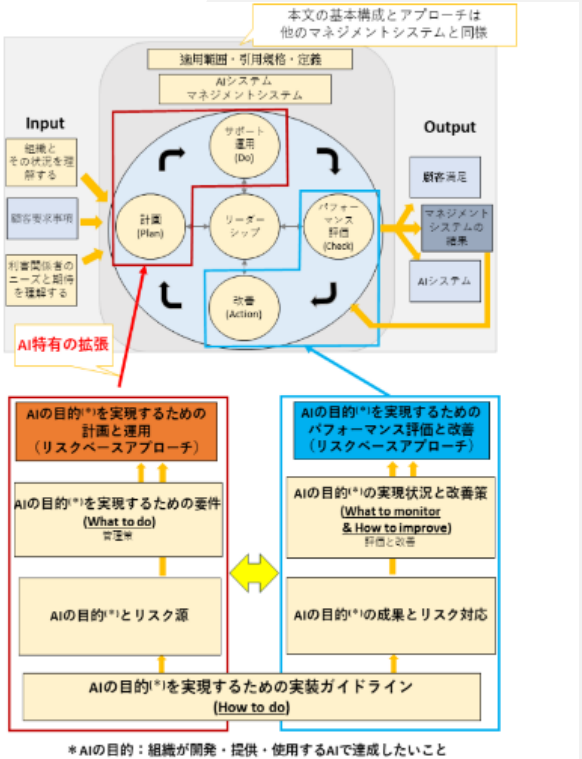
「ISO/IEC 42001:2023 Information technology-
Artificial intelligence-Management system」

「情報技術－人工知能－マネジメントシステム」

発行日：2023年12月18日

【発行背景】

AIシステム自体の機能評価基準というよりも、企業、公的機関等といった組織のなかで、**誰がAIシステムについて責任を持つべきなのか、また、どのようにAIマネジメントシステムの体制を確立すべきなのか、そのポイントとあるべき姿は何なのか、という面からガイダンスを示すものです。**



＊AIの目的：組織が開発・提供・使用するAIで達成したいこと

図：AIマネジメントシステムの構成

ISO/IEC 42001(AI マネジメントシステム/AIMS）とは②

【定義】

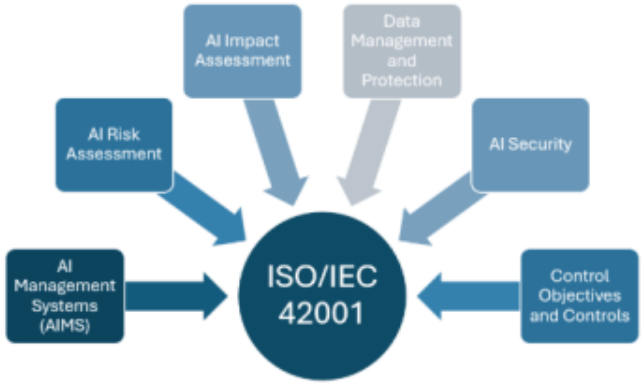
ISO/IEC 42001は、AIマネジメントシステム（AIMS)の構築、実施、維持、継続的改善に関する要件を規定した国際規格です。

【なぜ重要？】

AIの偏り・説明責任・倫理課題への対策が必要不可欠なため

【誰が対象？】

AIを開発・利用・提供する全ての組織（企業、政府、教育機関等）



人工知能マネジメントシステム（AIMS）

目的：
ISO/IEC 42001は、人工知能（AI）に特化して策定された、
世界初の国際的なマネジメントシステム規格です。

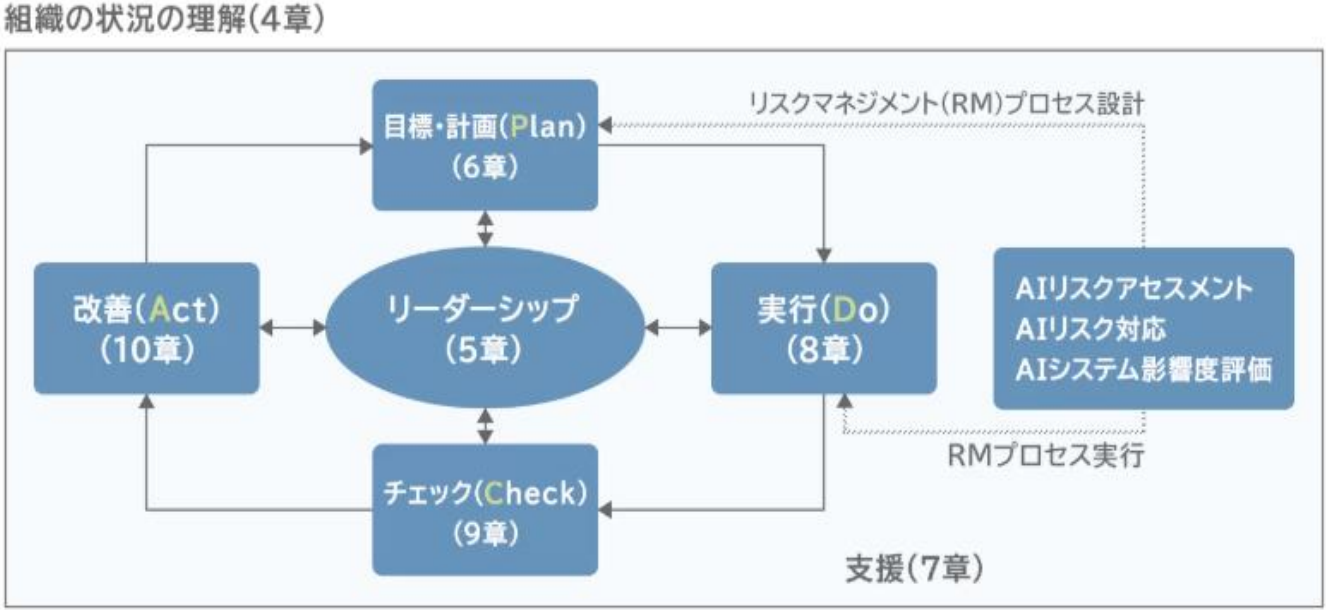
ゴール：
組織が以下を満たすための**体系的・監査可能・認証可能な枠組み**を提供
・信頼性（公平・安全・透明性・説明責任）
・法令順守（EU AI Actなど）
・有効性と継続的改善
ISO 27001が情報セキュリティを運用可能にしたように、ISO 42001はAIに関する倫理的・技術的・規制要求を**実務的なガバナンスに落とし込む**。

中核コンセプト：
- リスクベースアプローチ
- ガバナンスと説明責任
- データとモデル管理
- 透明性と説明可能性（Explainability）
- 人による監督（Human Oversight）
- 市場投入後のモニタリング（Post-Market Monitoring）



ISO/IEC 42001 フレームワーク

本認証のフレームワーク（Framework）は、組織の状況を理解し、経営陣の支援（リーダーシップ）の下で、計画（P）→支援および運用（D）→成果評価（C）→改善（A）のサイクルを実施することにより、意図した結果を達成できるように設計されています。



【図3. ISO/IEC42001（AIマネジメントシステム規格）の章構成】

ISO/IEC 42001要求事項

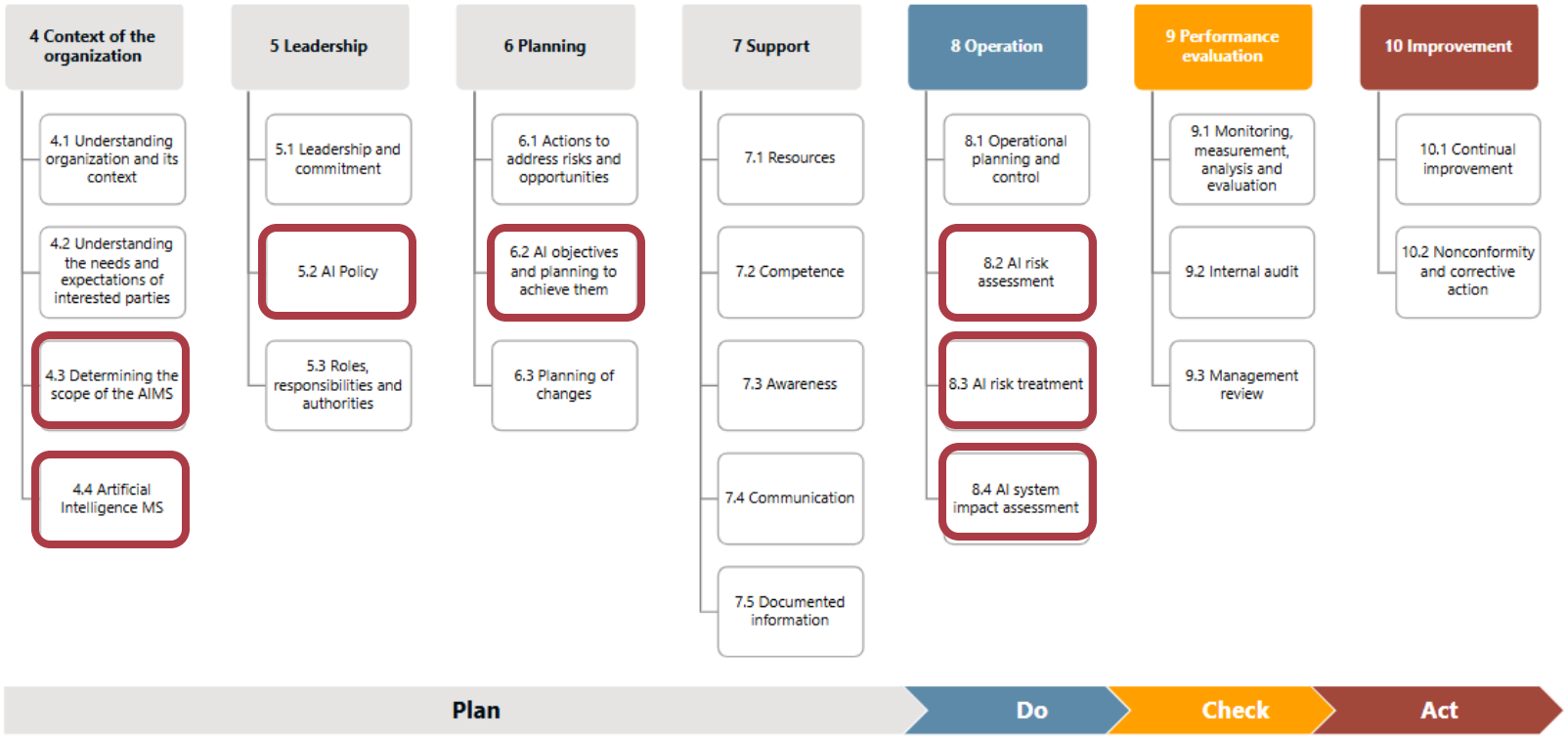
- 4.組織の状況（Context of the organization）
- 5.リーダーシップ（Leadership）
- 6.計画策定（Planning）
- 7.支援（Support）
- 8.運用（Operation）
- 9.パフォーマンス評価（Performance Evaluation）
- 10. 改善（Improvement）

ISO/IEC 420001付属書

- 附属書A(規定）参考となる管理目標及び管理策
- 附属書B(規定）AI管理策実施の手引き
- 附属書C(規範）AI関連の潜在的な組織の目的及びリスク源
- 附属書D(規範）複数の領域又は分野にわたるAIマネジメントシステムの利用
- **＜付属書A＞**

A.2 AIに関する方針
A.3 組織体制（Internal Organization）
A.3 AIシステムのためのリソース
A.4 AI影響評価
A.5 AIシステムのライフサイクル
A.6 AIシステム開発ライフサイクル
A.7 AIシステムのためのデータ
A.8 AIシステムに関する利害関係者への情報提供
A.9 AIシステムの利用
A.10 第三者関係

ISO/IEC 42001 フレームワーク



出典：産業通商資源部

ISO 42001で要求される文書化された情報

- AI管理システムマニュアル
- AIポリシーと倫理ガイドライン
- 役割と責任に関する文書
- リスク管理文書
- AIライフサイクルのプロセス文書
- データ管理およびデータ保護文書
- 利害関係者分析とコミュニケーション計画
- 監査報告書および管理レビュー
- トレーニング証明書および能力証明
- 第三者との契約書および合意書
- インシデントおよびログの文書化

ISO 42001の文書化

別紙A

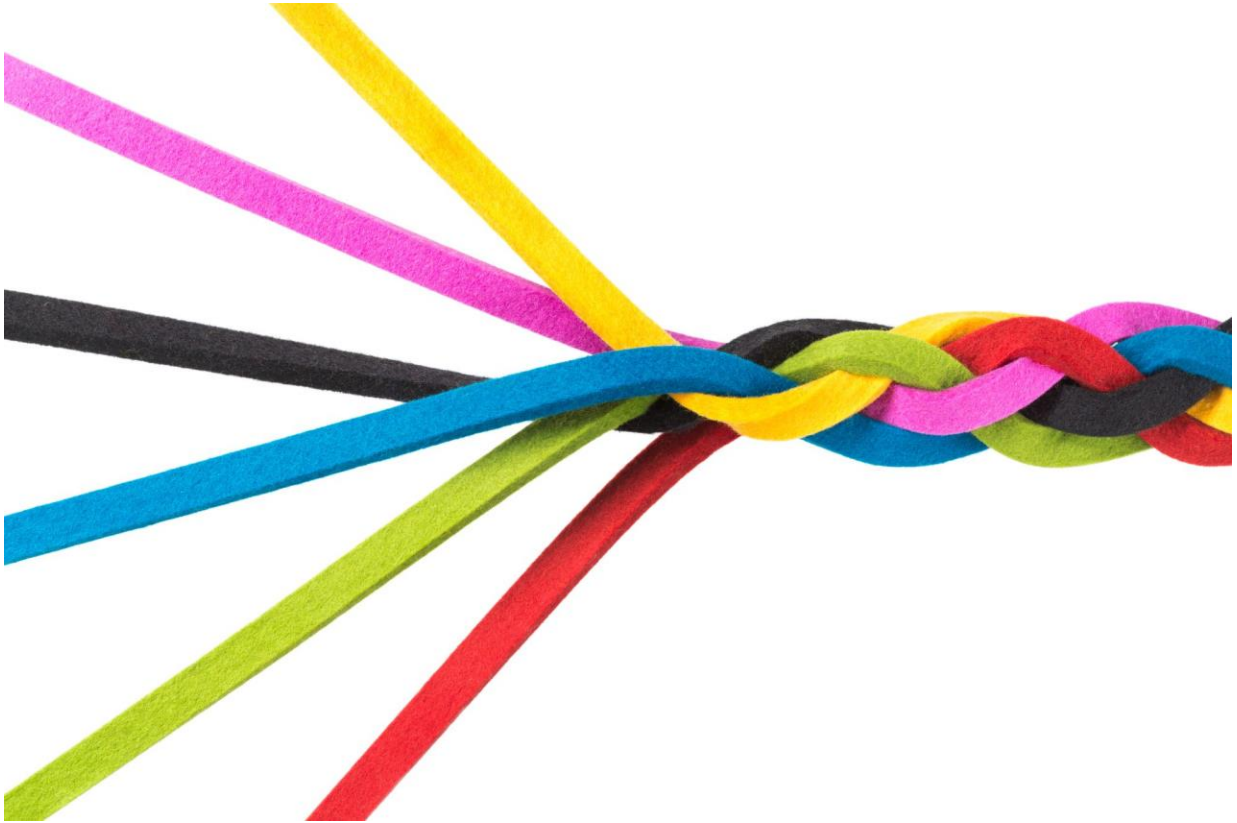
対象領域（附属書A）	必要な文書
A.2 AIに関連するガイドライン	AIに関するガイドラインと倫理原則
A.3 内部組織	組織構造、役割、責任
A.4 AIシステムのためのリソース	AIコンポーネント、データ、ツール、インフラストラクチャ、人材
A.5 影響の評価	リスクと影響の評価
A.6 AIシステムのライフサイクル	要件、開発および展開計画
A.7 AIシステムのためのデータ	データ管理、品質、データ保護
A.8 関係者のための情報	コミュニケーションと透明性
A.9 AIシステムの利用	利用ガイドラインと制御
A.10 第三者および顧客との関係	外部パートナーの契約と遵守

ISO/IEC 42001 附属書A - 参照制御目的と制御

Annex A（規範的）は、人工知能経営システム（AIMS）の構築のために、9つの制御目的（control objectives）と38の制御項目（controls）を提示しています。

NO	制御目的	制御項目の主な内容	NO	制御目的	制御項目の主な内容
A.2	AI関連ポリシー (AIに関するポリシー)	- AIシステムの開発および運用に関する組織のポリシー 策定 - AI倫理原則および責任に関する方針の策定	A.7	AIシステムのためのデータ (Data for AI Systems)	- データ収集、保存、処理、削除に関するポリシーの策定 - データ品質、セキュリティ、プライバシー保護措置の整備
A.3	内部組織 (Internal Organization)	- AI経営システムの役割と責任の定義 - AIガバナンス構造および意思決定体系の確立	A.8	利害関係者向けの情報 (Information for Interested Parties)	- AIシステムの目的、機能、限界などに関する 透明な情報提供 - 関係者と効果的なコミュニケーション体系の構築
A.4	AIシステムのためのリソース (Resources for AI Systems)	- AIシステムの開発および運用に必要なリソースの特定 および管理 - データ、ツール、人材などのリソースの文書化および維持	A.9	AIシステムの利用 (AIシステムの利用)	- AIシステムの使用範囲および条件の定義 - 使用中に発生する可能性のあるリスクに対する 対応策の策定
A.5	AIシステムの影響評価 (AIシステムの影響評価)	- AIシステムが組織および利害関係者に与える影響分析 - 社会的、倫理的、法的影響の考慮	A.10	第三者および顧客関係 (Third-Party & Customer Relationships)	- 外部のサプライヤーおよびパートナーとの契約および協力時のAIに関する要件を明示 - 顧客データの保護およびAIシステムの責任性 確保
	AIシステムライフサイクル	-	**[Annex A 活用時の注意事項]** 1. 選択的適用：Annex Aの制御項目は、組織のAIリスク評価結果および組織の特性と必要に応じて適切な制御を選択		

4.他規格との親和性



附属書SL / High Level Structure(HLS)

【箇条構成】

1 適用範囲

2 引用規格

3 用語及び定義

4 組織の状況

5 リーダーシップ

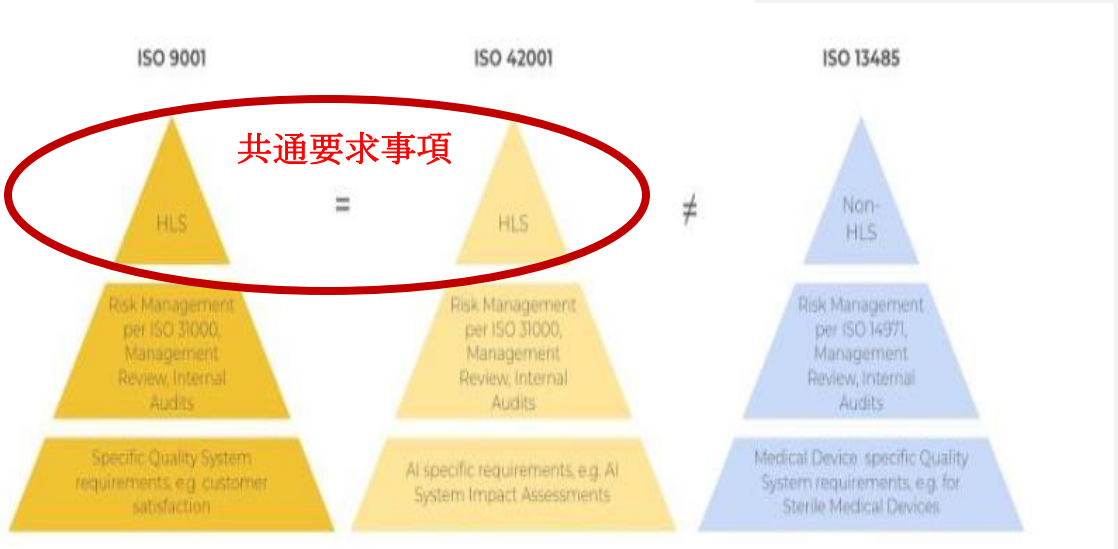
6 計画

7 支援

8 運用

9 パフォーマンス評価

10 改善



マネジメントシステムの共通要求事項

Structure of ISO management system standards

Requirements	ISO 9001:2015	ISO 14001:2015	ISO/IEC 27001:2022	ISO 22301:2019	ISO/IEC 42001:2023
Leadership and commitment	5.1	5.1	5.1	5.1	5.1
Policy	5.2	5.2	5.2	5.2	5.2
Objectives	6.2	6.2	6.2	6.2	6.2
Documented information	7.5	7.5	7.5	7.5	7.5
Internal audit	9.2	9.2	9.2	9.2	9.2
Management review	9.3	9.3	9.3	9.3	9.3
Continual improvement	10.3	10.3	10.1	10.2	10.1

ISO/IEC 42001 の他の規格への統合

- ISO 42001 附属書D

(複数の領域又は分野にわたるAIマネジメントシステムの使用)

では、以下の規格との統合可能性が強調されています：

- ISO 9001
- ISO 27001



ISO27001 VS ISO42001

ISO27001	ISO42001
情報セキュリティシステム	AIマネジメントシステム
CIA（機密性・可用性・完全性）を重視	バイアス・説明性・倫理性を重視
ISMSを構築	AIMSを構築
管理策のポイント	
・アクセス制御 ・暗号化 ・物理的セキュリティ ・インシデント対応	・データ品質 ・透明性 ・倫理的保護 ・AIシステムの検証
共通点	
・PDCAサイクル ・リスクベース思考 ・政策・役割・監視・改善を含む	
統合の利点	
ISO27001とISO42001を統合することで、**安全かつ責任あるデジタル変革の基盤が構築されます**	



5. ISO42001 認証プロセス



ISO/IEC 42001 認証プロセス

認証プロセス（DQSの場合）：

1. **予備調査（任意）**＜現状把握と改善点の抽出＞
2. **第1段階審査**　＜文書と体制の確認＞
3. **第2段階審査**　＜実運用の確認＞

継続審査＆再認証審査＜認証後も3年ごとに継続的な評価＞

ISO/IEC 42001:2023 審査の実施

	第一段階審査	第二段階審査
審査のねらい	AIマネジメントシステム（AIMS)の**構築状態**を確認する審査	AIマネジメントシステム（AIMS)の**実施状況**を確認する審査
審査の対象	**・AIMSの適用範囲** **・AI方針** **・AIMS文書** ・重要なマネジメントシステムのフレームワークに関する記録 （AIリスクアセスメントの結果、教育訓練、内部監査、マネジメントレビューの結果）	**・AIMSの運用状況** （インタビューや観察、手順書・記録によって確認）
受審対象者	AIMS管理責任者、AIMSの推進事務局メンバー、（AIMS内部監査チーム及びトップマネジメント）	AIMS管理責任者、AIMS推進事務局メンバー、AIMS内部監査チーム及びトップマネジメントに加え各部門の責任者だけでなく、手順や管理策を実行している各スタッフ
審査報告書の内容	発見された不適合や観察事項、及び第**二段階審査の実施可否**	発見された不適合や観察事項、及び認証の推薦の可否

ISO42001審査工数の事例　～ ISO/IEC 42006（第1版　2025/7）より～

認証範囲 対象人員：１～10名

AI開発者	AI提供者	AI利用者
5.0人日	3.5人日	3.5人日

認証範囲 対象人員：86～125名

AI開発者	AI提供者	AI利用者
12.0人日	8.0人日	8.0人日

認証範囲 対象人員：626～875名

AI開発者	AI提供者	AI利用者
17.5人日	11.5人日	11.5人日

6. 審査の現場で見られる課題



審査員からの声：

- ISMSとの親和性が高い点は、意図的なので全体像は把握しやすく良いのですが、リスクアセスメントを行っても情報セキュリティに偏りがちだと、AIMSの価値を見出せないと思います。

- AIシステムのライフサイクル(開発、提供、利用)を意識していただければと存じます。



審査員からの声：これだけは絶対準備して欲しい

AIMSに限った話ではないですが、第二段階審査**前**までには一通りの運用を完了していただかないと審査できないため、**少なくとも第一段階審査までに運用の準備はしていただきたいです。**

第二段階審査で一発勝負になると審査の進行も結果も厳しいものになる可能性があります。

また、AIシステム影響分析**(箇条6.1.4, 8.4)はAIMSのみの要求事項**ですなので、ご注意ください。



これから取得されるお客様へアドバイス



AIシステムであってもOUTPUTに対する説明責任を求められています。

どのようなシステムでもPDCAを回すことで改善が必要ということだと思います。

マネジメントシステムの運用はこのサイクルが継続することに価値があると思います。

7.認証取得までの一般的ステップ ～ベストプラクティス～



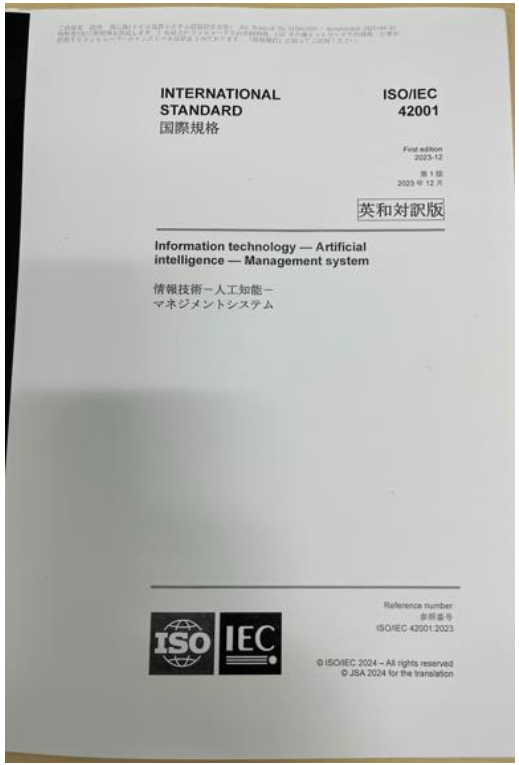
認証取得までの一般的ステップ

- ISO/IEC 42001規格文書を入手

1.　AIMSの体制の確立
⇒管理責任者の任命やチーム設置

2.　AIMSの適用範囲の定義
⇒適用範囲の決定

3．AI方針の確立
⇒基本方針の策定



認証取得までの一般的ステップ

4.　AIシステム影響評価（AIシステムインパクトアセスメント）の実施
⇒AIシステムの潜在的な影響を評価

5.　AIリスクアセスメント及びAIリスク対応の実施
⇒AIリスクの分析・評価、管理策の選択、適用宣言書の作成

6.　AIMS文書の作成

7.　AIMSの導入教育

認証取得までの一般的ステップ

8.　付属書Aに基づく管理策の整備

⇒AIガバナンスに関する役割と責任の明確化

⇒関係者への教育訓練

9.　内部監査・マネジメントレビューと是正処置

⇒内部監査の実施

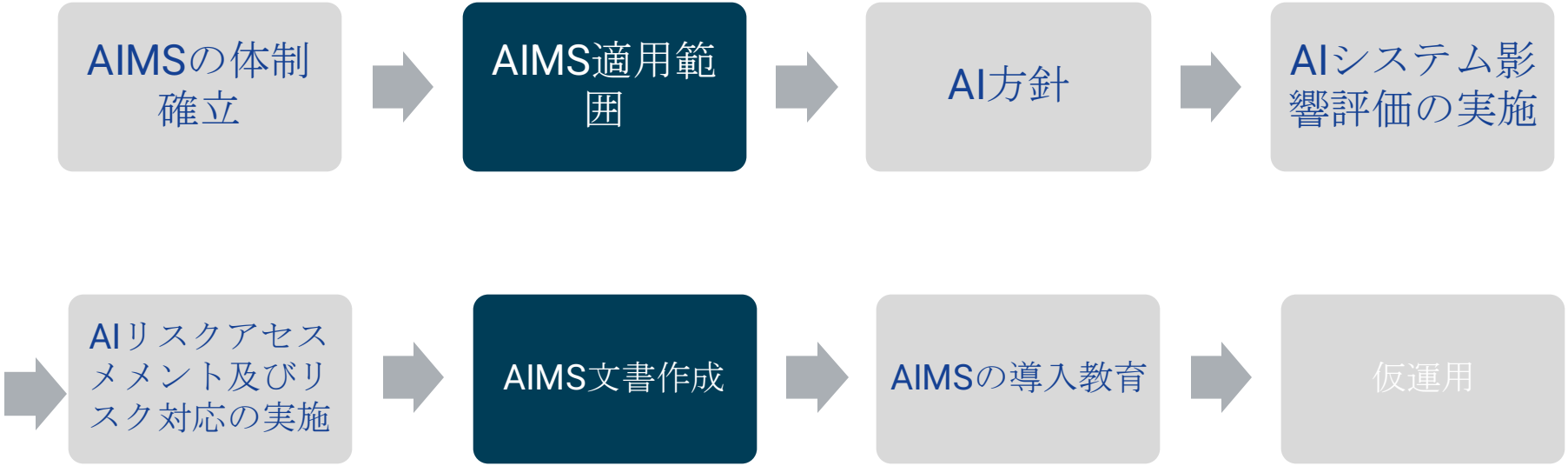
⇒マネジメントレビューの実施

⇒不適合に対しての是正処置

↓

準備完了！AIMSの認証審査　受審へ

AIMSの構築・導入のステップ



AIMSの構築・導入のステップ



ISO/IEC 42001審査の事例紹介

Ｒ社様　（東京都千代田区/DQS既存顧客様　ISO9001,14001,27001認証企業）

事業内容：プロジェクト(SI)サービス事業、ソリューションサービス事業、基盤(プロフェッショナル)サービス事業、Webコンテンツ・教育サービス事業

認証背景：社長より＞AIを取り巻く環境の変化は非常に激しいです。ここで立ち止まって考えるより、世の中の変化に合わせて「歩きながら考える」というスピード感を重視しました。また、当社の主要顧客である金融機関に対して、AI活用の「安全・安心」を客観的にアピールするためにも、早期取得は不可欠なエポックメイキング（画期的な出来事）になると確信していました。

認証範囲：AIユーザー

準備期間：2025.9～11

審査時期：2025.11 第一段階審査　1.0人日

2025.12 第二段階審査　1.5人日

■構築にあたって、印象に残っていることや苦労された点

既存の知見を活かした構築プロセス

先行事例が少ないため、具体的な表現方法などは手探りでした。一方で、ISMSとの親和性が非常に高かったのは助かりました。社内に蓄積されたISMSをベースにしつつ、差分を読み解くことで対応できました。また、今回はAI開発に携わる比較的小規模な部隊にフォーカスしたため、内部監査も含めてスムーズにスタートすることができました。

ISO/IEC 42001審査の事例紹介（続き）

■ISOは「足かせ」ではなく「確実性へのツール」

DQS： 認証取得後の、ビジネスにおける期待やビジョンを教えてください。

社長：一般的にISOは「管理」や「足かせ」と捉えられがちですが、我々は非常にポジティブに捉えています。リスクとは「不確実性」のことです。この規格をツールとして使い、不確実なものを「確実」へとシフトさせていく。そうしたポジティブなモチベーションを生む仕組みとして運用していきたいですね。

DQS： 素晴らしい視点ですね。社外へのアピールという点ではいかがでしょうか。

社長：顧客のデータを大切に守りながら、ビジネスの成長に貢献するAIソリューションを提供していくための「信頼の証」になります。中長期的には、個別のお客様だけでなく、社会全体にサービスを提供できるプラットフォームビジネスやサブスクリプションモデルの柱として、このガバナンスを機能させていきたいと考えています。

8.まとめ



結論：解決策としてのISO/IEC 42001認証「AIMS」とは

AIマネジメントシステム（AIMS）とは

ISO/42001(AIMS)はAIを組織として管理する「仕組み」の国際標準です。

●QMS, ISMSなどと同様の馴染みやすいフレームワーク：

•品質管理における**ISO 9001**、情報セキュリティにおける**ISO 27001**と同様に、AIを組織として適切に管理するための「マネジメントシステム」の規格です。

•多くの管理職が精通しているPDCAサイクル（Plan-Do-Check-Act）を用いて、AIガバナンスを継続的に改善していくことができます。

● AIMSが定めること：

•AI方針の策定：会社としてAIをどう扱うか、トップの方針を明確にします。

•リスク評価：AI利用に伴うリスク（バイアス、公平性、プライバシー等）を体系的に特定評価・対処するプロセスを構築し、AIシステム影響評価を実施します。

•ライフサイクル管理：AIツールの選定・導入から運用、廃棄までを一貫して管理します。

•役割と責任の明確化：誰がAI活用の責任を負うのか、組織体制を整備します。

•継続的な監視、測定、分析、評価：AIリスクの継続的な監視と対応を行い、リスク軽減を行います。

●ポイント：

• 特定のAIツールを縛る規則ではなく、どんなAI技術が登場しても対応できる、持続可能な管理を社内に導入するものです。

結論： ISO/IEC 42001 は、AIリスクを「見える化」し、継続的に管理するための枠組みを提供します。

- **リスクの体系的な特定と評価**
  バイアス、データセキュリティ、誤判断など、AI特有のリスクを網羅的に洗い出し、優先順位付けを実施
- **実効性のある管理策の導入**
  特定したリスクに対し、組織として統制・低減措置の実装を要求
- 継続的モニタリングによるリスク抑制
  AIの挙動を常時監視し、異常検知・性能劣化・環境変化に対応
- AIインパクトアセスメントの実施
  個人・社会への影響を評価し、倫理的・法的リスクへの配慮を強化
- ガバナンスとリスク管理の統合
  AI活用を「管理された状態」に置くことで、
  ▶ 被害の最小化
  ▶ システムの信頼性向上
  ▶ 意思決定の説明責任（アカウンタビリティ）強化
- 国際的なリスクマネジメント整合性
  ISO/IEC 23894:2023 に基づく実践と整合

結論：ISO/IEC 42001認証のメリット

- 内部管理機能の強化
- 顧客へわかりやすい形で「安心」の提供
- ビジネスパートナーシップや投資を呼び込む



さらに、認証は組織がAIリスク管理プロセスを効率化し、長期的な持続可能性を確保する上で役立ちます。

AIは、単なる技術アップグレードではありません。

ガバナンス、倫理的な先見性、そして積極的なコンプライアンスを求める
戦略的変革だと、我々は考えています。

ご清聴ありがとうございました



Q&A Session



Contact

- www.dqsglobal.com/jp-jp/
- Phone: 090-4715-5048
- Email: **reiko.Nakamura@dqs.de**

For any questions or comments you can contact us below:

- support@pecb.com

補足資料：ISO42001 審査員要件

	審査員/技術レビューアー	ISO/IEC DIS 42006に準拠	DQS要件
a	学歴	大学教育と同等レベルの専門教育または訓練	情報技術の理学士・BS（Bachelor of Science ）または同等の学位
b	経験	情報技術またはデータ保護の分野で4年間のフルタイムの実務経験があり、そのうち少なくとも2年間はAIシステムに関連した経験があること	情報技術分野で4年の経験。AI関連システム（エキスパートシステム、プロセス制御、ソフトウェアなど）分野で2年の経験。
c	教育訓練	AIMS審査と審査管理を含む少なくとも3日間のトレーニングを完了していること	研修機関によるAIMS主任審査員認定コースを受講し、合格すること
d	審査経験	過去5年間に少なくとも3回の審査（初回審査1回、継続監査1回）で合計30日間の審査（ISO9001 or ISO27001)	ISO27001, ISO27701, ISO20000-1,TISAXなどの他の技術・マネジメントシステムで30日間の審査を実施すること
a	主任審査員	3 回のISO/IEC42001審査	
b	リーダーシップスキル		
c	コミュニケーションスキル		
Note :	これは全く新しい規格であるため、DQSの経営陣は、基準a、b、c、dを満たしていれば最初の新審査員として資格認定することを決定しました。ISO27001などの他の技術管理システム監査のいずれかで審査員として資格認定されている場合は、監督監査は必要ありません。		

中国の学校におけるAI活用
教室のデジタル革命か、それとも全監視社会か？

30秒ごとに顔をスキャン

・知能型カメラが30秒ごとに生徒の顔をスキャンし、感情と行動を分析。
・システムは6種類の行動タイプと7種類の気分状態を区別。



運用方法

・収集データはリアルタイムで教師へ送信
・クラス全体の集中度や感情傾向を可視化
・集中していない生徒の名前は自動で強調表示

組織はどのようにしてISO/IEC 42001を導入できるのか？

- 組織は、まずギャップ分析を実施して、現在のAIガバナンスの実践状況を規格の要件と照らし合わせることで、ISO/IEC 42001を導入できます。
- 次のステップは、AIの目標を定義し、経営陣のコミットメントを確立し、AIリスク管理をビジネスプロセスに統合することです。
- 組織は、AIポリシーを文書化し、影響評価を実施し、モニタリングメカニズムを導入する必要があります。
- 定期的な監査とパフォーマンス評価は、コンプライアンスの確保と継続的な改善に役立ちます。
- 従業員へのAIガバナンスに関するトレーニングと、AI戦略を規制要件に整合させることも重要です。
- 外部認証を取得することで、コンプライアンスをさらに検証し、AIを活用したサービスへの信頼を高めることができます。





サマリー：適用範囲の概要

ISO/IEC 42001導入の戦略的メリット

- **積極的なコンプライアンス対応**
  施行期限前に**EU AI法への適合を第三者認証で証明可能な体制**を構築
- **統合的なガバナンス**
  ISO 27001（情報セキュリティ）やISO 9001（品質）との整合性を確保し、マネジメントの複雑さを軽減
- **信頼と市場アクセスの確保**
  認証取得により**規制当局・ビジネスパートナー・顧客への信頼性を可視化**
  特に**高リスクAI分野における競争優位性の獲得**につながる
- **スケーラビリティ**
  組織が複数のAIアプリケーションを地域や事業部門を横断して一貫して管理することを可能にする。

EU AI法が「何をすべきか」を定めるのに対し、ISO/IEC 42001は「どう実行するか」を示します。

ISO 42001を導入することで、**EU AI法の法的・倫理的原則を、継続的改善の枠組みの中で実務に落とし込む**ことができます。
これにより、AIシステムは**そのライフサイクル全体において、安全性・適合性・信頼性**を維持し続けることが可能になります。

ISO/IEC 42001:2023

ISO/IEC 42001:2023は、企業および社会がAIの利用から最大の価値を安全かつ効率的に得られるよう支援することを目的としている。

この規格により、以下が可能となる。

- AIアプリケーションの品質・セキュリティ・トレーサビリティ・透明性・信頼性の向上
- AI導入時の課題の解決
- AIシステムへの信頼性向上
- AI開発コストの削減
- 規制遵守の維持
- AIの倫理的かつ責任ある利用に関する顧客・従業員・ステークホルダーの期待への対応
- 業務効率およびリスクマネジメントの改善

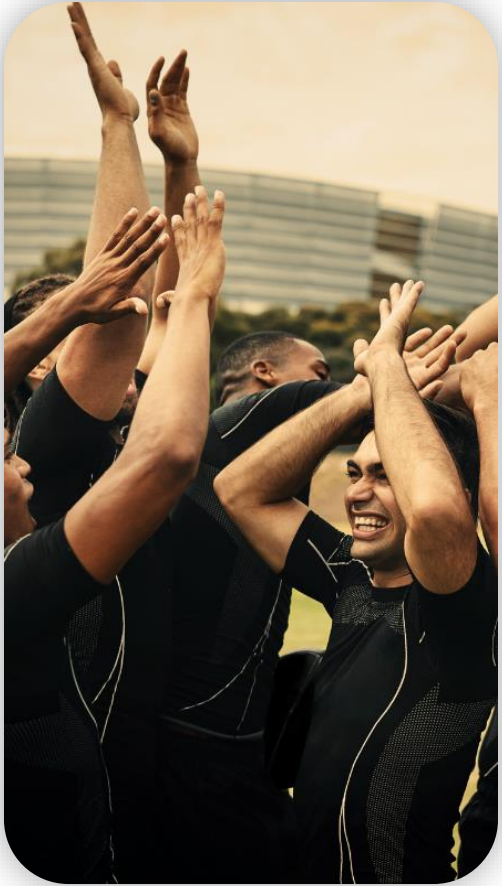
Different approaches by two U.S. Presidents

Category	Donald Trump's EO	Joe Biden's EO
Title	*Maintaining American Leadership in Artificial Intelligence*	*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*
Primary Focus	Promote AI **innovation and global leadership**	Ensure **safety, security, and ethical use** of AI
Regulatory Approach	**Light-touch**, pro-innovation	**Regulation-focused**, with safety and oversight requirements
Research & Development	Prioritized **federal R&D funding** for AI	Continued support for R&D but with emphasis on **safety testing**
AI Safety & Risk Assessment	Minimal regulatory direction	Mandatory **safety testing and red-teaming** for powerful AI models
Civil Rights & Consumer Protection	Not explicitly addressed	Strong emphasis on **bias, discrimination, and consumer harms**
International Collaboration	Encouraged, with focus on keeping U.S. competitive	Supported, but with stronger attention to **national security risks**
Transparency & Standards	Promoted **open data and models**, voluntary standards	Directed agencies to create **mandatory standards** for transparency
Workforce Impacts	Encouraged workforce development via STEM education	Called for studies on **AI's impact on jobs** and protection of workers
Overall Tone	**Pro-growth, innovation-oriented**	**Precautionary, rights- and security-oriented**

日本におけるAIガバナンスの規制アプローチ

人間中心、アジャイル的アプローチ

- • AIのガバナンスを考えるうえで、「日本国内」のAI規制動向を整理してみます。
- ■ **AI推進法の施行**
- ・2025年9月にAI推進法（人口知能関連技術の研究開発及び活用推進に関する法律）が施行されました。
- ・イノベーションを創出するための法律であり、AIのリスクに対しての規制ではありません。
- ■ 既存法律による**AI問題への対処**
- ・AIの利用そのものを直接規制する罰則法はありませんが、既存の法律でAI悪用事例に対応しています。
- （個人情報保護法、不正競争防止法、著作権法、刑法、特許法、独占禁止法等）
- ■ **AI事業者ガイドライン（1.1版2025年3月28日総務省・経済産業省）**
- ・AIシステムの開発・提供・利用に当たって、人間中心に照らし、法の支配、人権、民主主義、多様性
- 及び公正公平な社会の尊重といった倫理的な指針遵守の重要性が示されています。



なぜAIを戦略的に考慮すべきか

人工知能（AI）は、競争力、イノベーション、レジリエンスの鍵を握る技術として、あらゆる業界で決定的な役割を果たすようになっています。予測分析や自律型システム、業務変革をもたらす生成AIまで――AIはもはや「未来の技術」ではなく、グローバル市場でのリーダーシップを左右する中核的な能力となっています。

ガバナンスと規制適合の必要性

世界中の規制当局は、AIの革新的かつ潜在的に破壊的な側面を認識しています。

- **欧州連合のAI法（EU AI Act）**は、AIシステムを健康・安全・基本的人権への影響度に応じて分類するリスクベースの枠組みを導入し、特に高リスク用途に対して明確な義務を課しています。
- ISO/IEC 42001（AIマネジメントシステム）のような**補完的な国際規格**は、透明性、説明可能性、継続的なリスク管理を実現するための体系的なアプローチを提供します。
- 米国、中国、日本を含む他の地域でも独自の規制枠組みの整備が進められており、組織はこうしたグローバルな規制動向を能動的に監視し、整合性を保つことが不可欠です。

基準による規制に反対する議論

- イノベーションの障壁

厳格な規制は、スタートアップ企業や中小企業の参入を阻害する可能性がある 官僚的な手続きは、イノベーションサイクルを遅らせる可能性がある

・コストとリソース

認証されたマネジメントシステムの導入には時間とコストがかかる 小規模組織は、専門知識や予算が不足していることが多い

・均一性 vs. 柔軟性

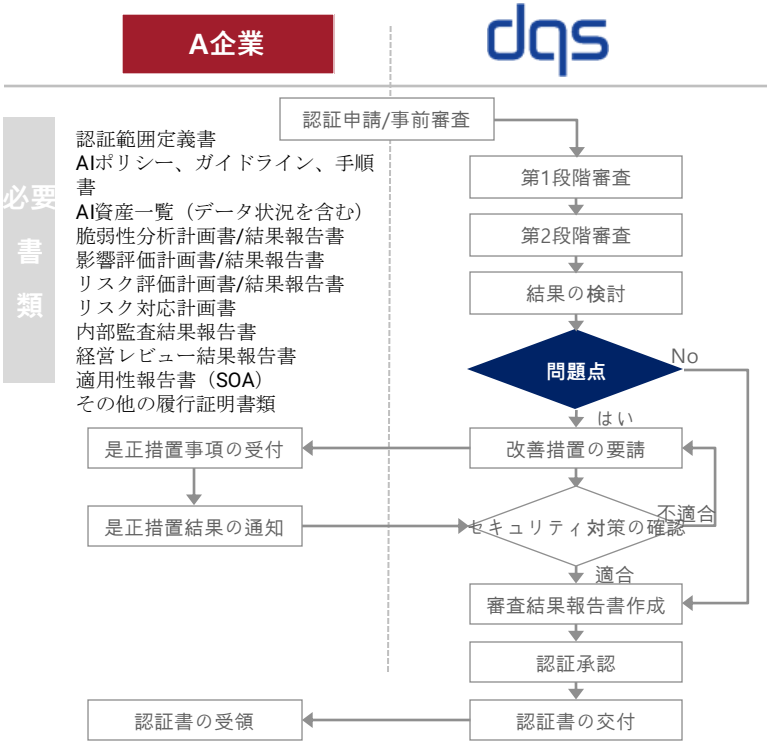
標準化は、すべてのAIアプリケーションに適合しない「万能型」ソリューションにつながる可能性がある AIのような高度にダイナミックな技術分野には、機敏で柔軟な規制形態が必要である

・規制は技術の進歩に遅れている

規格や法律は、しばしば時間差を伴って策定される その頃には、問題のある技術が既に定着している可能性がある

"AIのような急速に進化する技術には、柔軟で機動的な規制が必要"

ISO/IEC 42001 認証審査手順



ISO/IEC 42001:2023 認証審査要求事項

- **認証申請**
  - 認証審査申請書、認証範囲定義書の提出
- **第1段階審査**
  - AIMS関連文書（ポリシー/ガイドライン、手順書など内部規程）、実施証拠資料の審査
  - 保護対策の適用状況の確認など、管理的な要素の審査
- **2段階審査**
  - 文書に明記された管理措置の実施状況の確認
  - 1段階審査時に発見された問題点の原因と、各管理項目に対する保護対策の実施状況の確認
  - 実施に伴う証拠書類または電子的記録の点検
- **是正措置の要請**
  - AIMS不具合報告に基づく是正措置の実施を要請

ISO/IEC 42001は誰が導入すべきか？

- ISO/IEC 42001は、AIシステムを開発、提供、または利用するあらゆる組織に適用可能です。
- これには、AIテクノロジー企業、金融機関、医療機関、政府機関、教育機関などが含まれます。
- 意思決定、自動化、分析にAIを活用する組織は、倫理的および法的要件への準拠を確保するために、この規格を導入することでメリットを得られます。
- また、AI関連リスクの軽減、AIガバナンスの改善、公共の信頼の向上を目指す組織にも適しています。ISO 42001は、組織の規模、業界、特定のAIユースケースに合わせてカスタマイズ可能なフレームワークを提供するため、幅広い適用が可能です。