ISO/IEC42001 人工知能マネジメントシステム
(AI Management System, AIMS)における AI 活用の標準化とリスク管理

発表主旨

2025 年現在、人工知能(以下、AI)は業務効率化や人手不足の解消、データ分析による意思決定支援などを目的に、幅広い産業の分野で急速に活用が進んでいる。また、生成 AI の急速な普及により、文書、画像、音声、映像等の生成にて社会的影響が拡大している。

企業活動においては、クラウド型の AI に組織の機密情報を学習させ回答を得る活用方法が増えている。しかし、多くの組織で AI 活用に関する明確なルールや標準が整備されておらず、AI が十分な管理や制約なく利用されている実態がある。このため、AI 活用には組織の機密情報漏えいや精査されていない AI 生成データの好ましくない使用等の多様なリスクが内在していると言える。これらの課題に対処するため、組織全体での AI 活用の統制強化と標準化が不可欠であり、適切なリスク管理体制の構築と運用が求められている。

ISO/IEC42001 は、AI の開発および運用に関わる組織が、その利用に伴うリスクを適切に管理し、倫理性・透明性・信頼性を確保するために策定された AI マネジメントシステムに関する国際規格である。本規格は、従来の情報セキュリティ(ISO/IEC 27001)や品質(ISO 9001)といったマネジメントシステム規格との整合性を保ちつつ、AI 特有の課題への対応を目的としている。ISO/IEC42001 の要求事項を整理した上で、AI 活用における統制強化と標準化、リスクアセスメントや継続的改善の必要性を考察する。

発表者紹介

氏　名	青山　誠　　主任コンサルタント コンサルティング統括事業部　生産・業務改革コンサルティング部
専 門 分 野	IT 戦略立案 各種 IT システムの要件定義・導入・運用による業務改善 情報セキュリティ管理体制の構築・運用
コンサルティング歴	IT システム化計画作成支援 IT システム導入計画における RFP(提案依頼書)作成、導入評価支援 情報セキュリティリスクアセスメント及びリスク対策構築実行支援 各種 ISO マネジメントシステム認証取得支援

ISO/IEC42001
人工知能マネジメントシステム
(AI Management System, AIMS)における
AI活用の標準化とリスク管理

主任コンサルタント　青山　誠

一般社団法人　中部産業連盟

目次

1.現代のIT社会情勢と企業におけるAI活用の意識

・IT社会はクラウド、IoT、ビッグデータの進化で急速に発展
・5Gの普及など、リアルタイム共有や膨大なデータ処理が可能
・AIは効率化の枠を超え、社会や産業の競争力に直結する戦略的要素
・自然言語処理・画像認識・予測分析など、多様な分野でAI活用が拡大中
・企業では需要予測・在庫管理・製造自動化等様々な分野で活用拡大中
・生成AIはコンテンツ制作を加速させる一方、誤情報や著作権問題あり
・AI活用は二極化しており、積極導入派と慎重派が存在

1.現代のIT社会情勢と企業におけるAI活用の意識

・透明性確保や制度整備の不足が、社会的課題
・国際的にはISO/IEC 42001など、信頼性確保のルール作りが進行
・メリットとリスクを総合的に評価し、説明可能で持続的なAI活用が必要
・AI活用には、透明性・公平性・安全性を担保する文化が不可欠

2.企業においてAIを活用するリスク

（1）経営視点でAI活用の統制不能

リスク内容：

AIの活用が組織全体に広がると、業務担当者や部門ごとに異なるツールやモデルを独自に導入するケースが増える。組織全体で統制が取れなくなると、意思決定の一貫性が失われるほか、法規制や社内ルールの遵守が困難になる。

影響例：

部門ごとに異なるAIを利用し、機密情報や不適切なデータが共有される。

意思決定の透明性が欠如し、経営層が正確な状況把握を行えなくなる。

2.企業においてAIを活用するリスク

（2）機密情報漏洩リスク

リスク内容：

社内の機密情報（顧客データ、技術情報、戦略情報など）をAIに学習させることで、情報が意図せず外部に流出する可能性がある。

影響例：

機密情報が他社のAIモデルに利用される。

契約違反や訴訟リスクが発生する。

2.企業においてAIを活用するリスク

（3）著作権等の侵害

リスク内容：

AIの出力結果や学習データが第三者の著作権や特許権を侵害する。逆に、自企業の知的財産権が不正利用される。

影響例：

法的責任が発生する。

企業ブランドや市場競争力への悪影響が出る。

2.企業においてAIを活用するリスク

（4）誤情報・ハルシネーションリスク

リスク内容：

AIはハルシネーション(事実と異なる情報の生成)や誤情報を出力することがある。これを業務判断や意思決定に使用すると誤った判断につながる。

影響例：

誤った投資判断や製品・サービス設計の意思決定をしてしまう。

顧客対応でのミスやクレームが増加する。

2.企業においてAIを活用するリスク

(5)　その他リスク

その他のリスク内容としては、AI利用の倫理的問題、
経営戦略との不整合、組織文化との摩擦なども想定される。

AIを活用する際、前述のような多面的なリスクに対応しておく必要がある。
そのため、標準化された管理体制の下、ISO/IEC 42001規格要求に対応したAIMS（人工知能マネジメントシステム）を構築し運用する。
これにより、企業は、AI活用を戦略的かつ安全に進めることが可能となり、競争優位性の維持とリスク最小化を両立できる。

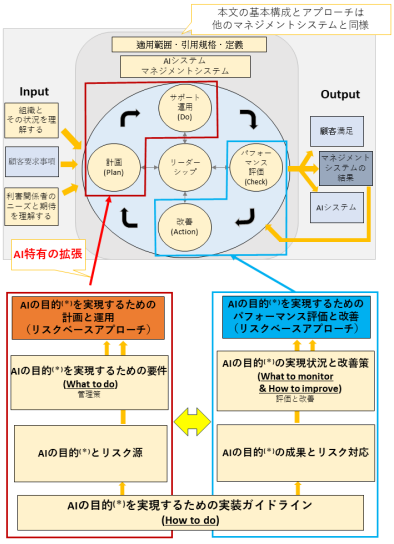
3.　ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

本規格は、AIシステムを開発、提供または使用する組織を対象とし、組織がAIシステムを適切に利活用（開発・提供・使用）するために必要なマネジメントシステムを構築する際に遵守すべき要求事項について、リスクベースアプローチによって規定したものである。

信頼性や透明性、説明責任を備えたAIシステムの利活用ができるよう、そのリスクを特定し、軽減すると共に、AIの公平性や個人のプライバシーなどへの配慮についても要求している。

ISO/IEC 42001:2023は、他のマネジメントシステム規格との関係性を整理しており、既存の規格と統合可能である。既存のマネジメントシステム規格と同様のアプローチを採用し、同じ構成で要求事項を規定している。

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは



【AIMSのPDCAの概略図】

本文の基本構成とアプローチは、
他のマネジメントシステムと同様

出典：
経済産業省記事：「AIマネジメントシステムの国際規格が発行されました
URL:
https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

他のマネジメントシステムとの関係

①ISO/IEC27001情報セキュリティマネジメントシステム（ISMS）

ISMSでは、情報の機密性・完全性・可用性の確保、個人情報を含む機密情報の適切な管理、リスクアセスメントが求められている。AIMSの運用により、ISMSの情報管理の枠組みの中で、 AIモデルや学習データに発生するリスクへの対策が可能となる。

②ISO9001品質マネジメントシステム（QMS）

QMSでは、顧客要求に基づく製品サービスの品質保証が求められている。AIMSの運用により、AIシステムの精度維持や顧客要求適合性の確保、AIシステムの品質確保が可能となる。

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

ISO/IEC 42001:2023 本編

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.改善である。特に、6.計画の「6.1 リスク及び機会への取組」を紹介する。

箇条番号	項目名称	要求事項
6.1.1	一般	AIリスクと機会を洗い出して、それに対処する計画を立てる
6.1.2	AIリスクアセスメント	AIシステムに関連するリスクを特定し、発生可能性、影響度を考慮しリスクを評価する
6.1.3	AIリスク対応	6.1.2で洗い出したリスクに対しての対策内容を定める
6.1.4	AIシステムの影響評価	AIシステムが社会・組織・人等に与える潜在的な影響を体系的に評価し、倫理・法令・社会的側面を含めて検討し、リスク管理に反映させる

参考： (一財)日本規格協会 ISO/IEC 42001:2023 人工知能マネジメントシステム要求事項 英和対訳版

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

附属書A「制御目的及び管理策の参考」、附属書B「AI管理策の実装ガイダンス」

附属書A「制御目的及び管理策の参考」は、AIリスクに対しての対策項目の参考管理策である。前述の「6.1リスク及び機会への取組」で洗い出したリスクと決定した管理策と比較して、必要な管理策が省略されていないことを確認する。

附属書B「AI管理策の実装ガイダンス」は、附属書Aに示された参考管理策の実装ガイダンスである。

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

附属書A	附属書B	項目名	管理目的
A.2	B.2	AIに関する方針	事業に対して、AIシステムの管理の方向性を定める
A.3	B.3	内部組織	AI管理のための責任・権限・役割を明確する
A.4	B.4	AIシステムの資源	利用データやAIツール等、資源を明確にする
A.5	B.5	AIシステムの影響の評価	AIシステムに影響を受ける、人、社会に対して影響度を評価する
A.6	B.6	AIシステムのライフサイクル	AIの設計から廃止までの全ライフサイクルを管理する
A.7	B.7	AIシステムのデータ	データの品質・正確性・信頼性を確保する
A.8	B.8	AIシステムの利害関係者のための情報	AIの利用目的や特性を利害関係者に適切に伝え、透明性を確保する
A.9	B.9	AIシステムの使用	AIシステムの運用を適切に管理し、誤用や不適切利用を防止する
A.10	B.10	第三者と顧客との関係	外部供給者や顧客との契約等通じて責任あるAI利用を確保する

参考： (一財)日本規格協会 ISO/IEC 42001:2023 人工知能マネジメントシステム要求事項 英和対訳版

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

6.1.4 AIシステムの影響評価

ISO/IEC 42001:2023 「6.1.4 AIシステムの影響評価」は、ISO/IEC 27001（情報セキュリティマネジメントシステム：ISMS）では要求事項とされておらず、ISO/IEC 42001:2023（人工知能マネジメントシステム：AIMS）において特徴的な要求事項である。その要求事項の意味を解説する。

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

6.1.4　AIシステムの影響評価

位置づけとねらい：

組織がAIシステムの開発・提供・使用に伴い、個人・集団・社会に及ぼす潜在的影響を体系的に評価することを要求するものである。

目的：

AIシステムが社会や人に与える影響をライフサイクル全体にわたって把握し、適切に管理することにある。

※附属書A5/B5では、影響評価プロセスの具体的な管理策や文書化手順が示されており、組織は評価方法と結果の記録を整備する必要がある。

3. ISO/IEC42001人工知能マネジメントシステム(AIMS)とは

6.1.4　AIシステムの影響評価

具合的な要求事項

プロセス定義：影響評価の方法、担当者、評価頻度の明確化
影響の決定　：AI導入やその用途、誤用から生じる社会への結果を特定
状況考慮　　：技術的・社会的状況、地域規制や文化の違いを反映する
文書化　　：評価結果を記録し、利害関係者が利用可能にする
リスクアセスメントとの統合：6.1.2のリスク評価結果に反映する

附属書A/Bでは、ライフサイクル全体にわたる個人・集団・社会への影響の評価や文書化の管理策が示されている。

4. AIシステムの影響評価事例

評価項目	評価結果
AIシステムの名称・バージョン	顔画像認識AI v2.2
評価実施日	2025/9/10
評価責任者	情報セキュリティ部門責任者
対象範囲（開発/提供/利用）	利用（公共空間での監視）
意図する用途	不審者検知
予見可能な誤用	誤検知による一般市民の不利益
技術的状況の考慮点	画像認識精度が限定的
社会的状況の考慮点	社会的偏見の増幅リスク
適用される法規制・管轄区域	個人情報保護法、GDPR
影響を受ける主体（個人/集団/社会）	市民、特定集団、社会全体
潜在的な影響（安全性,プライバシー,差別など）	誤認識による差別、プライバシー侵害
影響の重大性（低・中・高）	高
影響の発生可能性（低・中・高）	中
リスクレベル（重大性×可能性）	高
利害関係者への情報共有の有無	必要有
6.1.2リスクアセスメントへの反映状況	AIリスク番号　XXXXXとYYYYに考慮済み

5. まとめ

1. AIMSを導入し、AI活用の統制を標準化
   方針・責任・規程を明文化し、全社統制を継続的に強化する

2. リスクアセスメントを仕組み化
   AIの内外のリスクを継続的に可視化し、対策を実施する

3. 継続的改善と人材育成の実施
   教育、状況監視・監査を繰り返し、組織成熟度を引き上げ続ける