システム監査学会2022年度　第36回研究大会

「AIとシステム監査」研究プロジェクト報告

「システム管理基準に取り込んだAIガバナンスとAIマネジメント」

2022年6月10日

報告者　朝倉 俊道 CISA

目次

1．経緯

国内外の企業でAIシステムの利活用が浸透してきていますが、新しい形態のシステムであるため、システムの企画、開発、保守、運用のプロセスが確立されているとは言えず、従来のシステム開発・導入アプローチでは対応しきれていないと感じます。システム構築のガイドラインと言えるステム管理規準にAIシステムの特性を取り込むことで、AIシステムの企画、開発、保守、運用に関わるITマネジメントとそのプロセスに対して、経営陣が評価し、指示し、モニタできるようになることを目指したいと思っています。

2. 活動メンバー　研究プロジェクトメンバー　5名

氏名	所属		研P
朝倉　俊道	CISA		●
稲垣　隆一	稲垣隆一 法律事務所	主査	●
黒澤　兵夫	TAKE国際技術士研究所	副主査	●
牧野　博文	株式会社 東芝		●
芳仲　宏	「法とシステム監査研究」プロジェクト		●

3. 活動状況

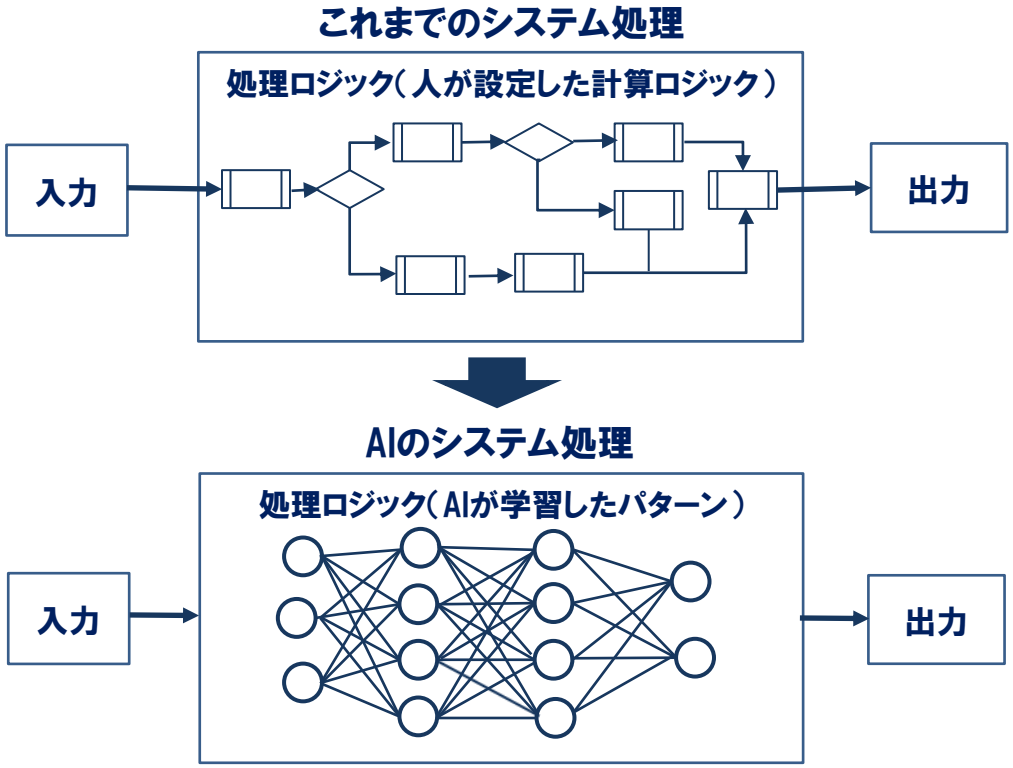
- 月に一回ペース　平日　18:30 or 19:00開始　約1時間30分

回数	開催日	場所	内容
第１回	11月30日	オンライン会議	「AI要件とシステム監査」「AIと個人情報保護～クラウドと契約～」の今後の進め方等
第2回	1月12日	オンライン会議	「AI要件とシステム監査」の今後の進め方等
第3回	2月24日	オンライン会議	「AI要件とシステム監査」の今後の進め方等
第4回	4月5日	オンライン会議	研究大会発表内容について（ディスカッション）
第5回	5月10日	オンライン会議	研究大会発表内容について（ディスカッション）

4. 参考文献

No	書名・資料名	著者	発行年月日	出版社	参照名
1	システム管理規準	経済産業省	2018年4月20日		経産省①
2	AI・データの利用に関する契約ガイドライン －AI編－	経済産業省	2018年6月		経産省②
3	GOVERNANCE INNOVATION Ver.2 アジャイル・ガバナンスのデザインと実装に向けて	経済産業省	2021年7月		経産省③
4	我が国のAIガバナンスの在り方 Ver. 1.1	経済産業省	2021年7月9日		経産省④
5	AI原則実践のための ガバナンス・ガイドライン Ver. 1.1	経済産業省	2022年1月28日		経産省⑤
6	AI時代における監査の取り組みとポイント	ISACA東京支部　稲垣 敦夫	2019年10月8日		ISACA⑥
7	AIシステムの監査　～監査実施モデル　ポイント・プロセス～	ISACA東京支部　阿古島 隆	2020年7月3日		ISACA⑦
8	「AIを監査する･･･」 ～ビジネスにAIを活用するITCへの提言～	企業内ITC・ITガバナンス研究会（久住 昭之/坂本 徳明/瀬戸 昭彦/滝沢 康/千枝 和行/古川 正紀/牧田 一雄/山崎 直和）	2020年3月31日		ITC⑧
9	持続可能な開発のためのITとAIのガバナンスと評価	第3回SWIM研究会　小倉 博行（日本大学）／原田 要之助（情報セキュリティ大学院大学）／馬奈木 俊介（九州大学）	2020年11月28日		SWIM⑨
10	企業ITに人工知能を生かす AIシステム構築実践ノウハウ	アビームコンサルティング P&T Digital ビジネスユニット Advanced Intelligenceセクター	2019年6月24日	日経BP	ｱﾋﾞｰﾑ⑩

5. 対象とするAIシステムのイメージ（1）



○業務を行う中で、これまで人が設定していた「予測・判断」の役割を、AIが代替または支援するシステムをAIシステムとする。
○「予測・判断」以外の入力、出力に関わる仕組みの開発は、これまでのシステム開発と大きく変わらない。
○AIシステムは、学習データをアルゴリズムへ投入することで、アルゴリズムがデータのパターンを自動で学習し、予測・判断を行うモデルを生成する。

AIシステムの例

入力	処理ロジック	出力
画像	画像認識	画像内容（文字データ）
	顔認識	顔判別
音声	音声認識	文字起こしデータ
	感情分析	感情状態
POSデータ	売上予測	予想売上金額

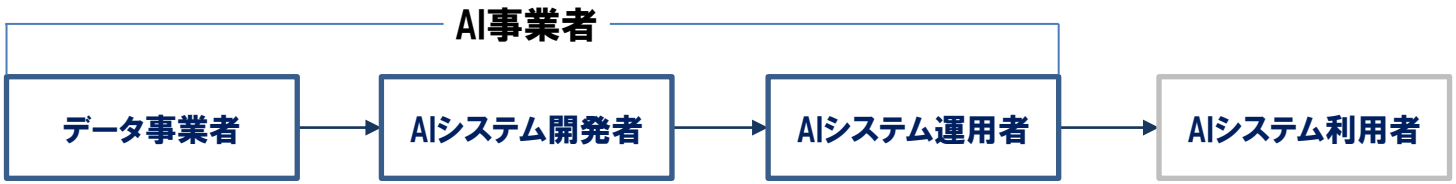
（アビーム⑩p.65一部変更、AIｼｽﾃﾑの例を追加）

5. 対象とするAIシステムのイメージ（2）

AIシステムの対象範囲

AIシステム：深層学習を含む様々な方法からなる、教師あり、教師なし、強化学習を含む**機械学習アプローチを用いたシステム**であって、人間が定義した特定の目的のために、現実又は仮想環境に影響を与えるような**予測、助言、決定を行う性能を有するシステム**。このAIシステムには、ソフトウェアだけではなく、ソフトウェアを要素として含む機械も含まれる。
（OECDのAIシステムの定義参考）

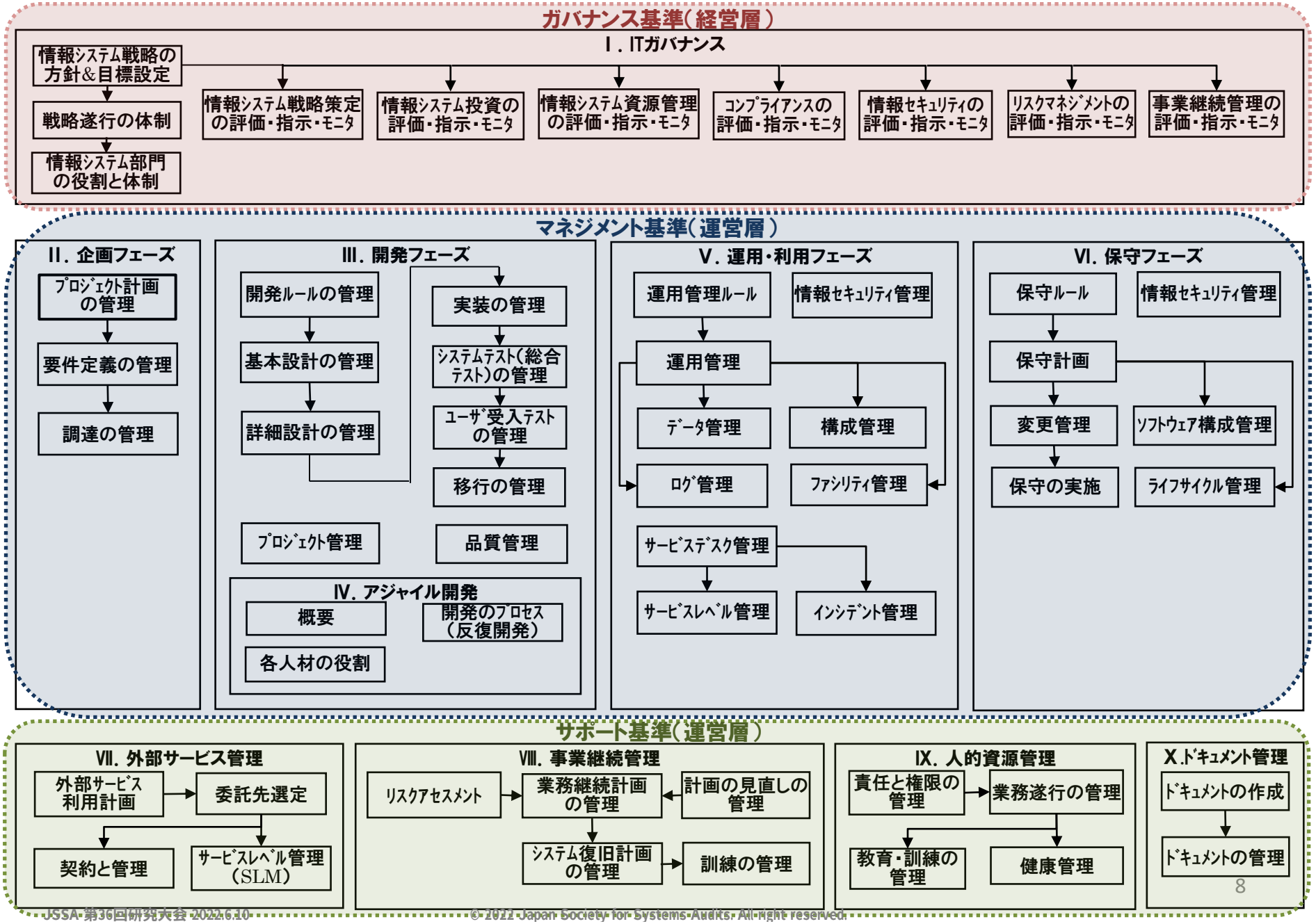
広義のAI：人間の判断を代替しうるものであって、利用者から判断過程が見えにくいソフトウェア等については、機械学習アプローチを用いていない場合であっても対象となりうる。



（経産省⑤p.5-6一部変更）

6. システム管理基準-全体図

（経産省①2018年4月を基に作成）



6．システム管理基準-AI対応追記（1）

No.	システム管理基準		AIのポイント	影響度	出所
	システム管理基準	着眼点			
	Ⅲ.企画フェーズ				
	1．プロジェクト計画の管理				
	(1) 経営陣は、プロジェクト運営委員会を設置すること。	① プロジェクト運営委員は、プロジェクトに利害関係を有していること。			
		② プロジェクト運営委員は、IT 投資に対する責任を有していること。			
			③ AIシステムを導入する場合、AIシステムに関する知見があるメンバーを加えたプロジェクト運営委員会を設置していること。	○	ISACA⑥
	(2) プロジェクト運営委員会は、プロジェクトマネージャ(PM)を任命すること。	① PM は、プロジェクトの対象となる業務に関する知見を有していること。			
		② PM は、プロジェクト管理に関する体系的な知識・経験を有していること。			
		③ PM は、プロジェクト管理に関する資格を取得する等、継続的なスキル向上に取り組んでいること。			
			④ AIシステムを導入する場合、PMは、ビジネスとアナリティクス（データを処理して操作し、データから知見を抽出し、その情報を利用してビジネスパフォーマンスを向上）をつなげるために、双方向の視点を持って意思決定を行うこと。	◎	アビーム⑩
	(3) PMは、プロジェクト計画を策定し、プロジェクト運営委員会の承認を得ること。	① プロジェクトの目的が情報システム戦略と整合していること。			
		② 対象業務が明確に定義されていること。			
		③ プロジェクト体制において、利用部門及び情報システム部門の役割が明確になっていること。			
		④ システムリリースの時期が適切に設定されていること。			
		⑤ スケジュールに利用部門への教育及び情報システム部門への訓練が含まれていること。			
		⑥ 既存システムを更改する場合は、既存システムの評価を行うこと。			
			⑦ AIシステムを導入する場合、AIシステムが自社の経営に役立つものなのかについて検討していること。	◎	ISACA⑥
			⑧ AIシステムを導入する場合、PoCを行い学習データとアルゴリズムの検証を行うスケジュールになっていること。	○	ISACA⑥
	(4) PMは、要件定義に必要な体制を確保すること。	① 実務に精通している利用部門の担当者が参画すること。			
		② 開発、運用及び保守の担当者が参画すること。			
	2．要件定義の管理				

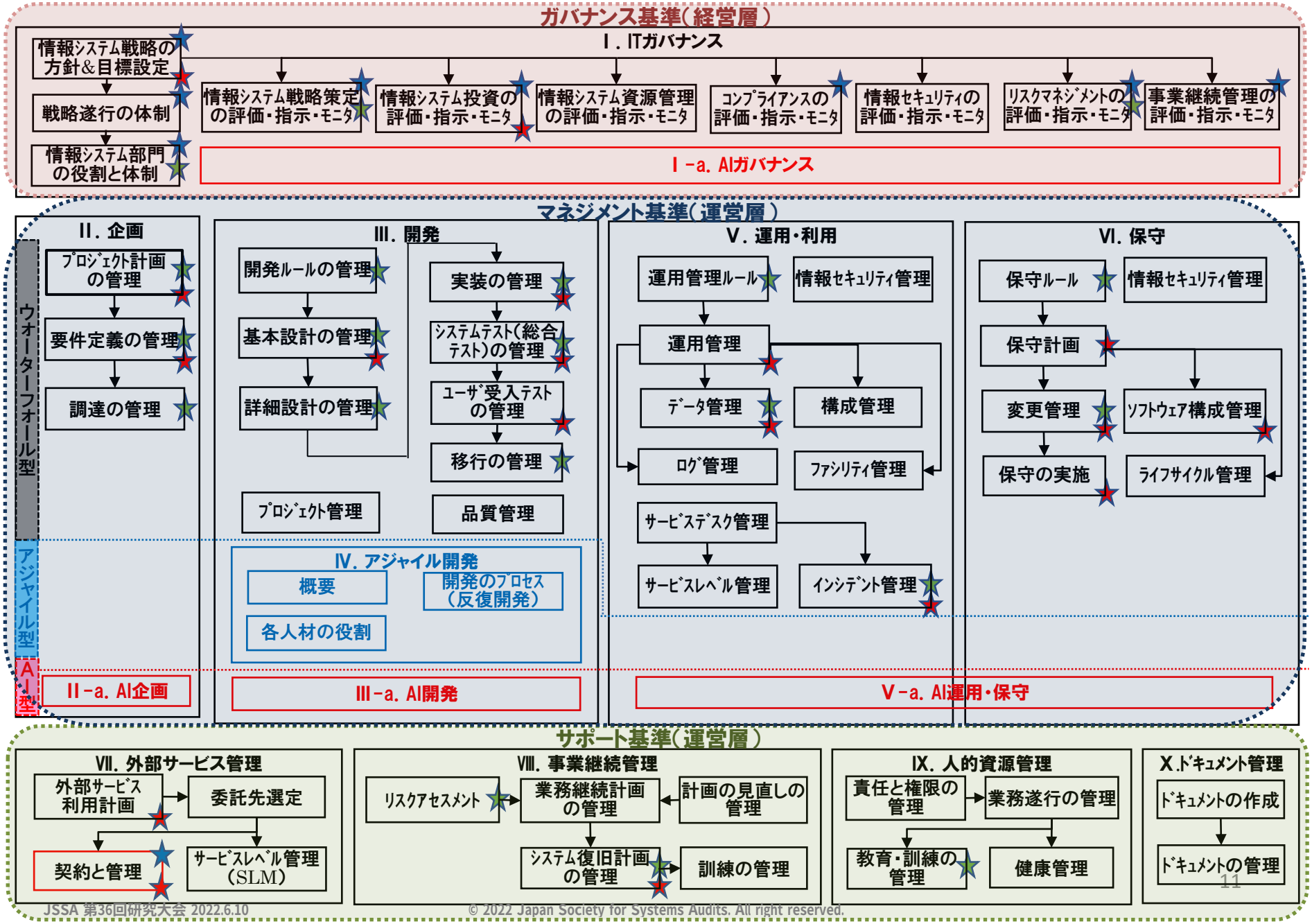
6. システム管理基準-AI対応追記（2）

No.	システム管理基準		AIのポイント	影響度	出所
	システム管理基準	着眼点			
			Ⅶ. AI開発		
			3．プログラム設計		
			3.1 設計全般		
			(1) AI システム開発者は、潜在的な利用者のリテラシーや経験不足の課題に対処していること。	○	経済産業省⑤
			(2) AI システム開発者は、予見可能な悪用に関する課題に対処していること。	○	経済産業省⑤
			(3) AI システム開発者は、AI システム運用者のリテラシーや経験不足の課題に対処していること。	○	経済産業省⑤
			(4) AI システム開発者は、AI システムの身体、精神、財産等への悪影響に関する課題に対処していること。	○	経済産業省⑤
			(5) AI システム開発者は、AI システムの公平性に関する課題に対処していること。	○	経済産業省⑤
			(6) AI システム開発者は、AI システムに対して期待されている個人への配慮事項に対処していること。	◎	経済産業省⑤
			(7) AI システム開発者は、AI システムのサイバーセキュリティに関する課題に対処していること。	◎	経済産業省⑤
			(8) . AI システム開発者は、必要な場合に、システムの設計上、人間の主体的な関与の機会を確保していること。	○	経済産業省⑤
			(9) AI システム開発者は、AI システムの機能、効果について、AI 以外のシステムと比較しながら、AI システム運用者とすりあわせをしていること。	○	経済産業省⑤
			(10) AI システム開発者は、AI システム運用時のモニタリングを容易にする設計をしていること。	○	経済産業省⑤
			3.2 AIアプリケーション設計・AI基盤設計		
			(1) PoCの結果をベースに、機械学習モデルと業務オペレーションの整合をとりながら設計すること。	◎	アビーム⑩
			(2) モデル周辺に付随するシステムも含めた全体構成を検討すること。	○	アビーム⑩
			(3)学習フェーズと推論フェーズ、２つの基盤を検討すること。	○	アビーム⑩
			(4) モデルが処理できないケースを想定し、その場合のフローを用意すること。	◎	アビーム⑩
			4．AIモデル実装		
			4.1 モデル・システム		
			(1) AI システム開発者は、開発しようとしているAIシステムに求められる十分な精度を確保していること。	◎	経済産業省⑤
			(2) AI システム開発者は、開発しようとしているAIシステムに求められる十分な堅牢性を確保していること。	○	経済産業省⑤
			(3) AI システム開発者は、開発しようとしているAIシステムの公平性を確保していること。	○	経済産業省⑤
			(4) AI システム開発者は、開発しようとしているAIシステムの妥当性を確保していること。	○	経済産業省⑤
			(5) AI システム開発者は、開発しようとしているAIシステムの説明可能性に配慮していること。	◎	経済産業省⑤
			(6) AI システム開発者は、AI モデルおよび AI システムの管理方法を定めていること。	◎	経済産業省⑤
			4.2 AI学習基盤構築		
			(1) モデルが要件通りに実装できていることを検証するため、モデルの予測精度のチェックを行い、予測精度のチェック結果によっては、要件定義で定めた業務内容を部分的に見直すこと。	◎	アビーム⑩

6. システム管理基準-AI対応図

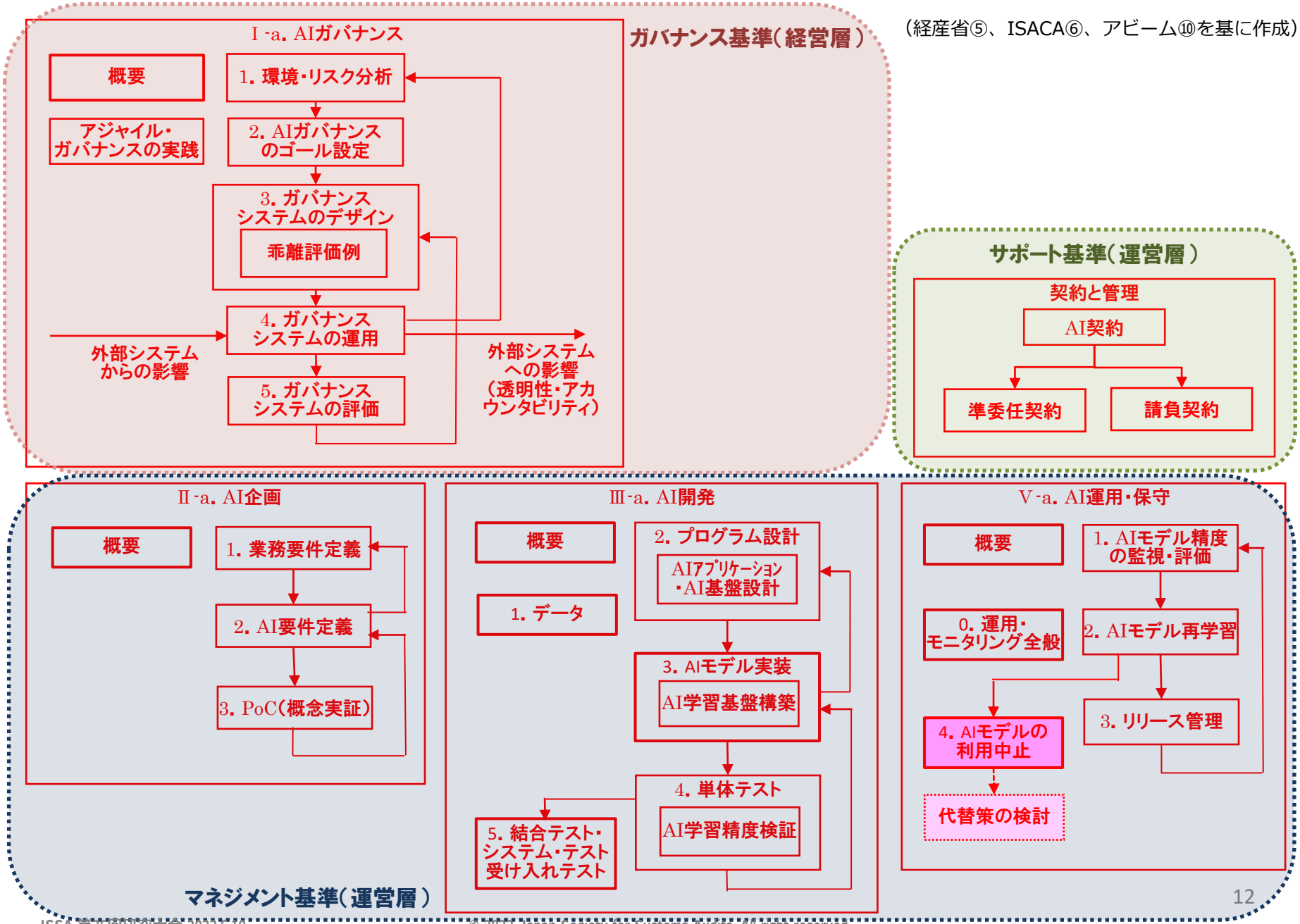
★経産省⑤ ★ISACA⑥ ★アビーム⑩

（経産省①⑤、ISACA⑥、アビーム⑩を基に作成）

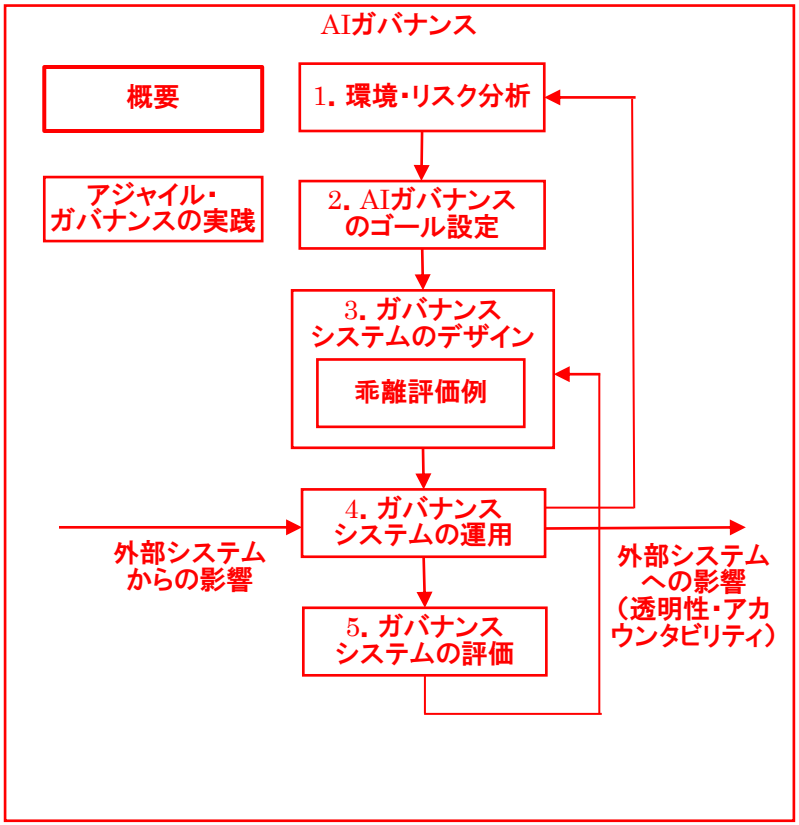


6．システム管理基準－AI追加部分

（経産省⑤、ISACA⑥、アビーム⑩を基に作成）



7．AIガバナンス（1）



（経産省③、⑤を基に作成）

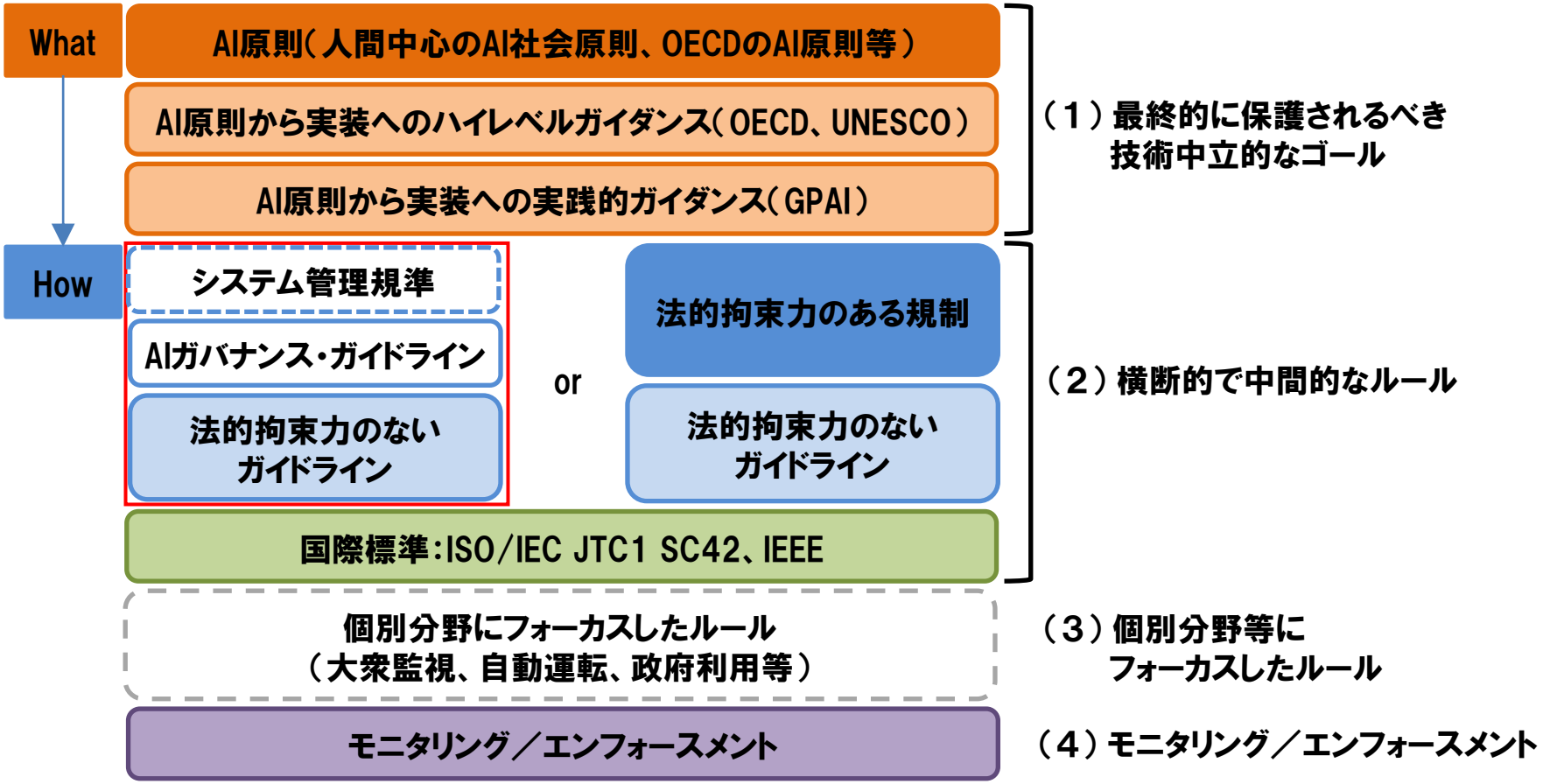
概要

○AIシステムに代表されるCPS（サイバー・フィジカルシステム）を基盤とする社会のガバナンスモデルは、常に変化する環境とゴールを踏まえ、最適な解決策を見直し続けるものである必要がある。そのために、最適な解決策を見直し続けるガバナンスのモデルとして、経済産業省で推進している「アジャイル・ガバナンス」の枠組みを活用している。

○AIガバナンスは二重ループから成る。環境・リスク分析では、AIシステムがもたらしうる正負のインパクト、社会の受け止め方、AI習熟度を理解する。この分析を踏まえて、AIガバナンスのゴールを設定し、それぞれの企業が大切にしていく価値を特定していく。その後、ゴールを達成するためにAIマネジメントシステムを構築するが、設定したゴールを達成するための、ゴールからの乖離の評価と乖離への対応、リテラシーの向上や事業者間連携に取り組む。運用では、AIマネジメントシステムや個々のAIシステムの状況をモニタリングするが、必要に応じて、外部に開示していく。評価では、AIマネジメントシステムが適切に機能しているか、機能していないとすればどのように改善すべきかを検討する。事業環境が大きく変化する場合には、環境・リスク分析を再度行い、ゴール設定から見直す。

7．AIガバナンス（2）

7-1 AIガバナンスの全体像

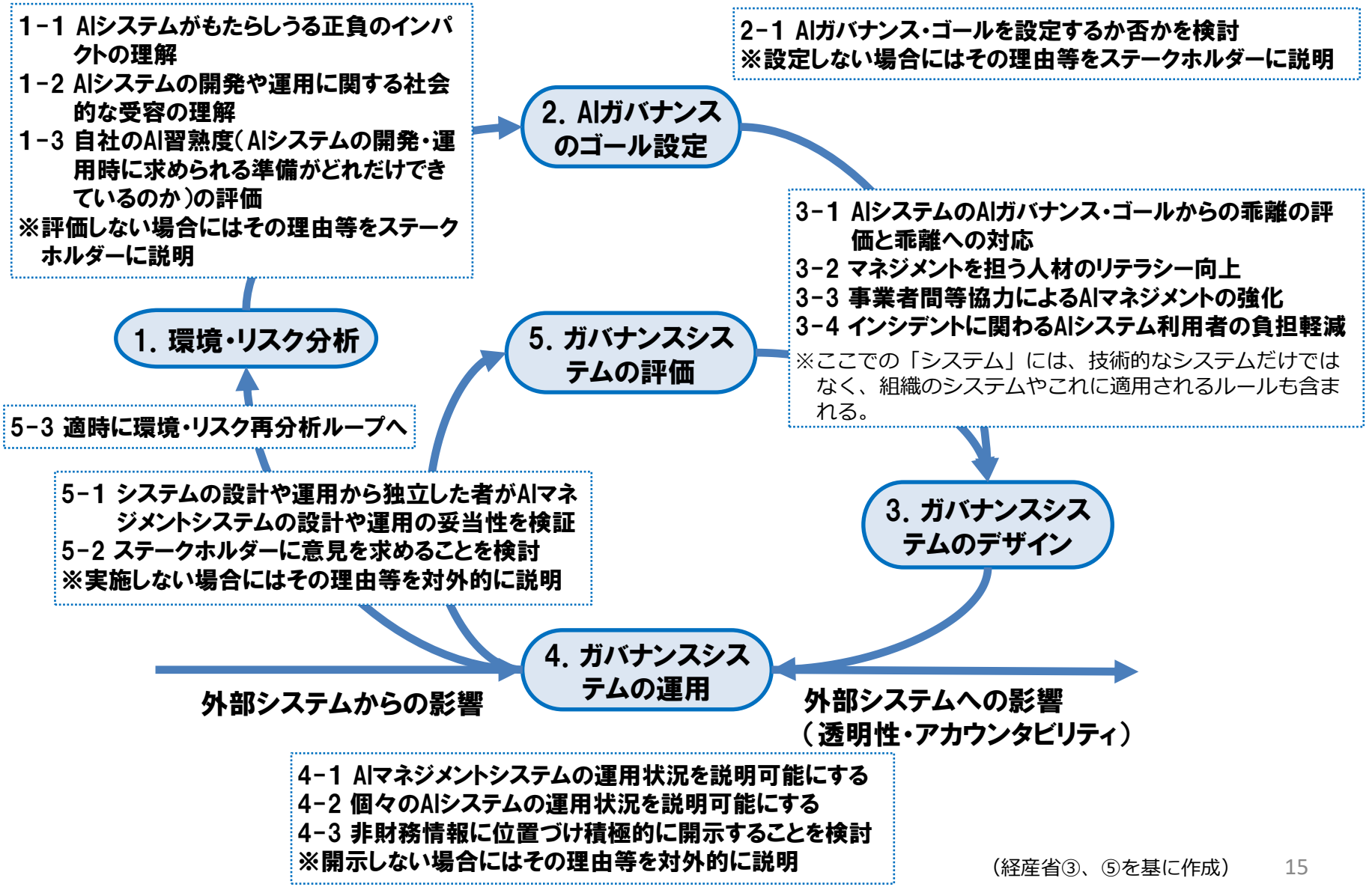


○AI原則で示される社会のめざすべき価値は図の「What」に位置づけられる。現在の課題は「How」の部分になる。 AI原則を実現する方法はたくさんあるが、経済産業省では、横断的なルールについて検討し、法的拘束力のないガイドラインを提供すべきということで策定されたのが、「AIガバナンス・ガイドライン」である。

（経産省④p.9-19一部変更）

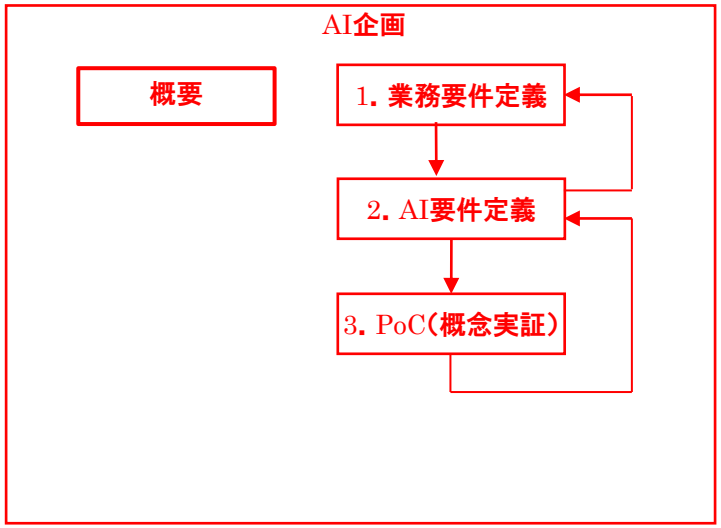
7．AIガバナンス（3）

7-2 アジャイル・ガバナンスの採用



（経産省③、⑤を基に作成）

8. AI企画（1）



概要

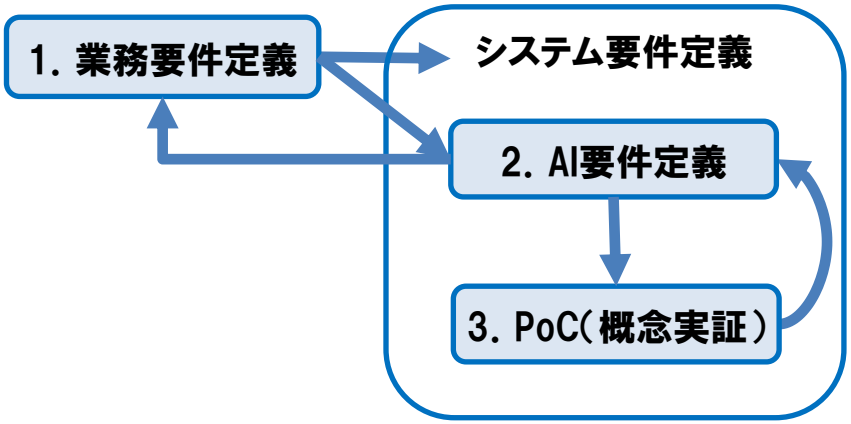
〇業務要件を定め、システム要件の定義を行うとともにAI要件定義を行う。AI要件定義では、システムを構成するAIの機能や非機能要件を定め、AI要件の実現可能性を実データを用いてPoC（Proof of Concept）で検証し、その結果を基にAI要件の見直しや詳細化を行う。

〇業務要件定義からAI要件定義、AI要件定義からPoC、PoCからAI要件定義の見直し、AI要件定義から業務要件定義の見直しと、試行錯誤を繰り返す。

（アビーム⑩p.76-97一部変更）

8. AI企画（2）

◆業務要件を定め、システム要件の定義を行うとともにAI要件定義を行う。AI要件定義に基づく学習データとアルゴリズムで実際にモデルを生成し、要件通りの機能・非機能が実現可能かどうかPoC（概念実証）により検証し、要件を満たせない部分がある場合は、業務要件定義・AI要件定義へフィードバックして、業務フローの変更や、AIの学習データ・アルゴリズムを見なおすなど、要件を調整する。



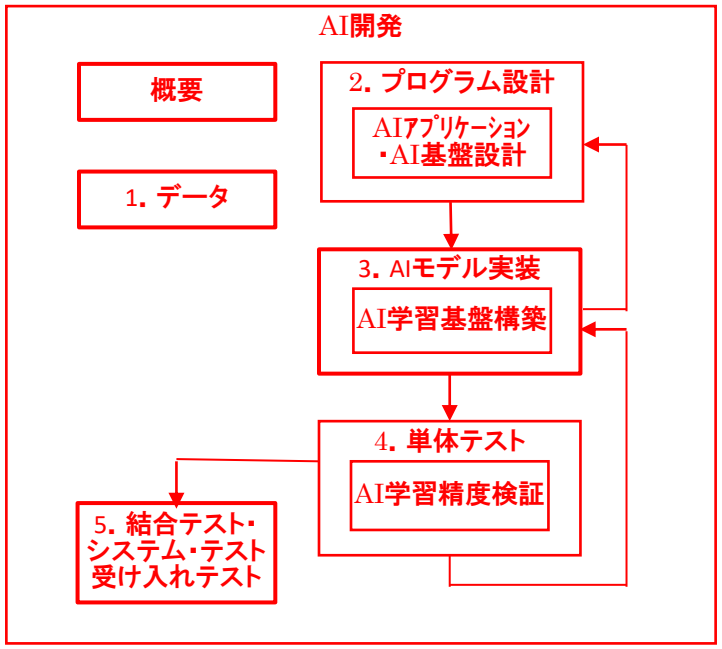
2-1：知覚機能の要件定義では、データの網羅性、粒度を確認すること。
2-2：予測・判断機能の要件定義では、データの種類、アルゴリズムの性質、例外の検討をすること。
2-3：実行機能の要件定義では、業務目的を考慮して決定すること。
2-4：AI基盤の検討とシステム稼働後の運用設計を検討すること。
2-5：PoC要件の検証論点を検討すること。

1-1：業務課題を整理し、システムの導入範囲を明確にすること。
1-2：AI導入の目的を明確にして、プロジェクト全体の期間や予算を検討すること。
1-3：AIによる判断の公平性、説明責任および透明性の確保に努めること。
1-4：AIシステム構築の目的や効果を定量化・具体化し、プロジェクトスコープを明確にすること。
1-5：業務要件整理により、AIの予測結果を採用しないケースを検討すること。

3-1：PoCは、業務課題に対応できる範囲でスモールスタートで実施し、段階的に高度化していくこと。
3-2：アプローチの絞り込みや完了基準となる目標精度を鑑みて、無理のないスケジュールを設定すること。
3-3：要件の実現可能性を見極めること。
3-4：計画・準備は、分析要件の整理、データ準備、モデル構築方針の検討、PoC環境の構築のステップで行うこと。
3-5：分析は、データアセスメント、データ加工、モデル構築のステップで行うこと。
3-6：構築したモデルを、統計的な観点、業務オペレーションの観点、ビジネス上の効果の観点から評価すること。

（アビーム⑩p.76-97一部変更）

9. AI開発（1）



概要

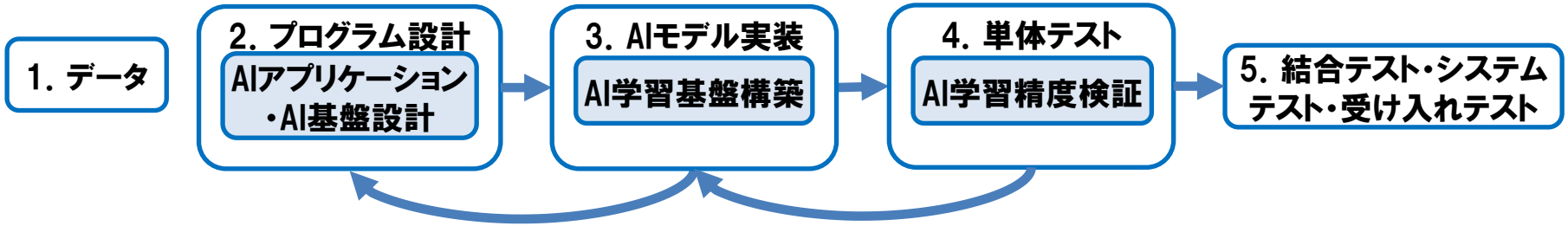
〇業務要件に合ったプログラム設計（AIアプリケーションとAI基盤の設計）を行い、AIモデルの実装を行う。AIモデル実装では、AI学習基盤を構築し、単体テストでAI学習精度を検証し、その結果を基にAIモデルの修正を行う。

〇プログラム設計からAIモデル実装、AIモデル実装から単体テストと、設計での不確実性を取り除くため反復的に進める。

（経産省⑤p.67-73一部変更、アビーム⑩p.98-120一部変更）

9. AI開発（2）

◆機械学習モデルの不確実性を排除するため、プログラム設計からAIモデル実装、AIモデル実装から単体テストと、反復的にすすめる。



1-1：データ事業者及びAIシステム開発者は、適法、公正、一般的に妥当な方法でデータを取得・収集していること。
1-2：データ事業者及びAIシステム開発者は、適法、公正、一般的に妥当な方法でデータを管理・利用していること。
1-3：AIシステム開発者は、データセットの設計にあたり、特定の社会属性に基づく不当な差別を維持・助長しないよう配慮していること。

2-1：PoCの結果をベースに、機械学習モデルと業務オペレーションの整合をとりながら設計すること。
2-2：モデル周辺に付随するシステムも含めた全体構成を検討すること。
2-3：学習フェーズと推論フェーズ、2つの基盤を検討すること。
2-4：モデルが処理できないケースを想定し、その場合のフローを用意すること。

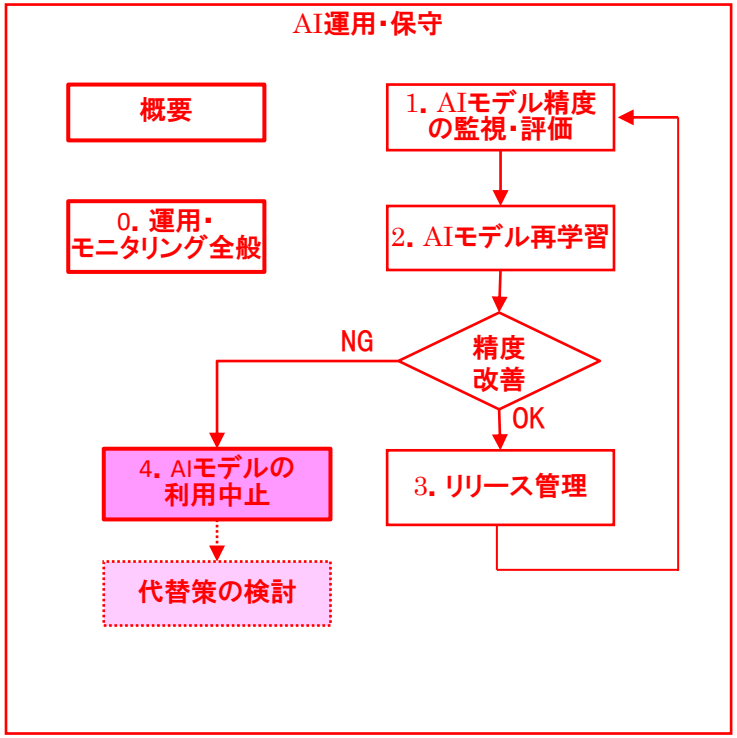
3-1：モデルが要件通りに実装できていることを検証するため、モデルの予測精度のチェックを行い、予測精度のチェック結果によっては、要件定義で定めた業務内容を部分的に見直すこと。
3-2：AI システム開発者は、開発しようとしているAIシステムに求められる十分な精度を確保していること。
3-3：AI システム開発者は、開発しようとしているAIシステムの説明可能性に配慮していること。

4-1：機械学習モデルの単体テストは、入力と出力の関係性を検証すること。

5-1：結合テストでは、従来のアプリケーション機能とモデルをつなげ、仕様通りに動作することを検証すること。
5-2：システムテストでは、要件定義で決定した業務フローに沿った業務シナリオテストを行い、実運用に耐えられるかどうか検証すること。
5-3：障害回復テストでは、バックアップデータを復元できること、および復元後に業務シナリオを問題なく実施できるかどうか検証すること。
5-4：受け入れテストでは、ユーザー部門が主体となって最終業務確認を行うこと。

（経産省⑤p.67-73一部変更、アビーム⑩p.98-120一部変更）

10. AI運用・保守（1）



概要

〇AIシステムの運用は、通常の業務システムの運用と違い、システム化の対象となるAIモデルが変化し続けるので、AIモデルの性能、機能を維持するための保守が必要になる。

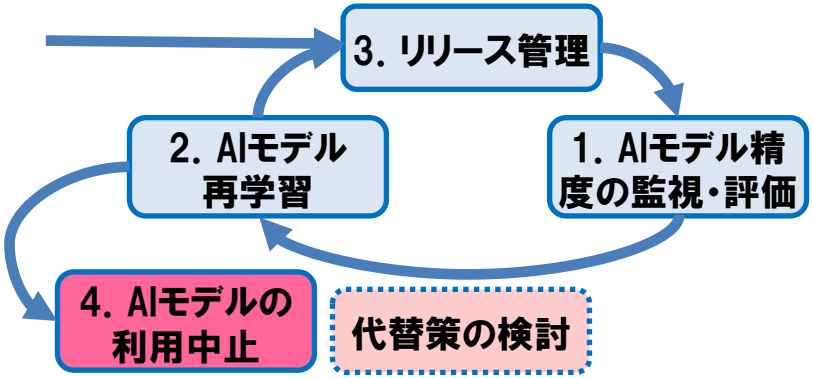
〇AIシステムの運用では、AIモデルの精度の監視・評価を行い、AIモデルの精度が低下した際は、モデルの再学習（原因となるデータの傾向変化に、AIモデルを対応させる）を行い、一定の条件を満たすことで本番環境にリリースする、サイクル運用を行う。

〇アルゴリズムやインプットデータを変更しても精度の改善が見込めない場合や、精度向上に対して投資が見合わない場合、また特異な結果、契約外の結果が出てきた場合は、AIモデル利用の中止を決断して、必要な代替策を検討する。

（経産省⑤p.73-78一部変更、アビーム⑩p.121-132一部変更、4.AIモデルの利用中止を追加）

10. AI運用・保守（2）

◆AIシステムの運用では、AIモデルの精度の監視・評価を行い、AIモデルの精度が低下した際は、モデルの再学習（原因となるデータの傾向変化に、AIモデルを対応させる）を行い、一定の条件を満たすことで本番環境にリリースする、反復的な保守プロセスをとる。



1-1：モデルの精度（KPI、KGI上の目標水準）が維持できているかどうか定期的にモニタリングし、評価すること。
1-2：AIの行った判断の内容を説明可能にしておくため、モデルの再現が可能な情報（学習データ、データ定義、アルゴリズム、ハイパーパラメーター、モデル精度を確認した結果）を保管・記録しておくこと。

2-1：モデルの精度が悪化したモデルに対して、精度を維持するための対応を実施すること。

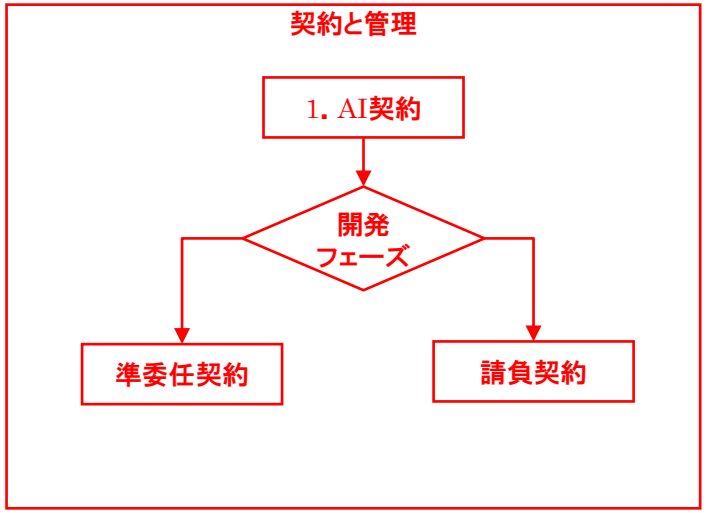
3-1：モデルのリリース管理とバージョン管理を行うこと。

4-1：精度の改善が見込めない場合や精度向上に対して投資が見合わない場合、特異な結果、契約外の結果が出てきた場合は、AIモデル利用の中止を決断すること。

0. 運用・モニタリング全般
0-1： AI システム運用者は、予見可能な悪用に関する課題に対処していること。
0-2：AI システム運用者は、自らのリテラシーや経験不足の課題に対処していること。
0-3：AI システム運用者は、AI システム開発者による個人への配慮事項への対処の内容を理解していること。
0-4： AI システム運用者は、AI システム開発者によるAIシステムのサイバーセキュリティに関する課題への対処の内容を理解していること。
0-5：AI システム運用者は、AI システムの機能、効果について理解していること。
0-6： AI システム運用者は、AI システム運用時のモニタリング支援機能やAIモデルや AI システムの管理方法を理解して、適切に運用していること。
0-7： AI システム運用者は、適法、公正、一般的に妥当な方法でデータを取得・管理していること。
0-8：AI システム運用者は、AI システム利用者に対する説明責任を果たしていること。
0-9：AI システム運用者は、人的資源や運用体制を含め、AI システムの運用方法を明確に定めていること。

（経産省⑤p.73-78一部変更、アビーム⑩p.121-132一部変更、4.AIモデルの利用中止を追加）

11. AI契約（1）



概要

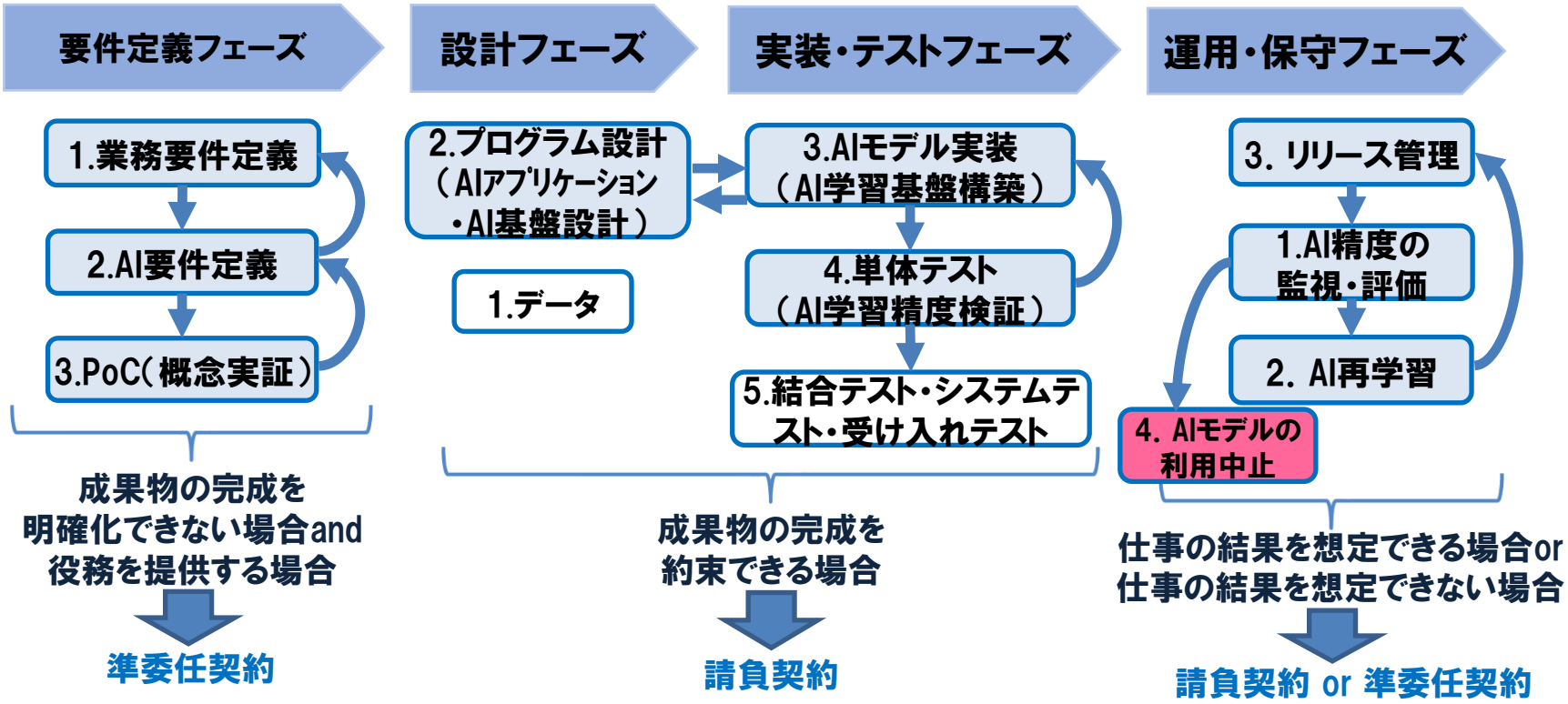
〇AIシステムの開発では、要件定義やPoCフェーズまでは、成果物の要件をあまり明確化できないため、準委任契約で行い、設計フェーズ、実装・テスフェーズは請負契約とするなど、開発フェーズごとに契約形態を適切に設定する。

〇AIシステムの開発では、成果物について契約時に合意しておく。準委任契約の場合、成果物の要件を特定できないが、作成すべき成果物の種類を事前に決めておく。

（経産省②p.38-55、アビーム⑩p.141-145を一部変更）

11. AI契約（2）

◆AIシステムは、契約時に先を見通すことが困難であるため、「探索的段階型（アセスメント段階、PoC段階、開発段階、追加学習段階）」の開発方式を想定する。またAIシステムでは、成果物について契約時に合意しておき、構築したモデルに関しての権利関係も事前に合意しておく。



1-1：フェーズに応じて適切な契約を締結すること。
1-2：各フェーズで想定される成果物について事前合意すること。準委任契約の場合、成果物の完成を明確化できないが、作成すべき成果物の種類は事前に決めておくこと。
1-3：著作権や特許権などに関して事前合意すること。

（経産省②p.38-55、アビーム⑩p.141-145を一部変更）

12. 今後の展開

・これまでに分かったことは、
「AIガバナンスにしても、AI企画・開発にしても、AI運用・保守にしても、AIシステムの開発では、AIの技術特性を理解し、注意点を考慮した上で、業務課題の解決に向けて、試行錯誤を繰り返し、反復的に進めていく、アジャイルな取り組みが有効である。」ということです。
・今後は、AIシステムにも対応したシステム管理規準の項目の見直しに、今回取り上げた経済産業省、ISACA、アビームの知見以外も利用して、AIシステムを取り込んだ新システム管理基準暫定案を作成できないかと思っています。
・新型コロナの影響もあり、今後の活動でカバーできればと考えています。

ご清聴、ありがとうございました。