\Orchestrating a brighter world NEC

電子情報通信学会 バイオメトリクス研究会

安全安心な人工知能システムへ向けて
－EU人工知能法とバイオメトリック識別システムを例に－

ISO/IEC JTC 1/SC 37委員長・同WG 4主査
ISO/IEC JTC 1/SC 42/WG5主査
日本電気株式会社 パブリックビジネスユニット
　BU CIPO・副CTO
主席サイエンティスト（DID／AI） 坂本 静生

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

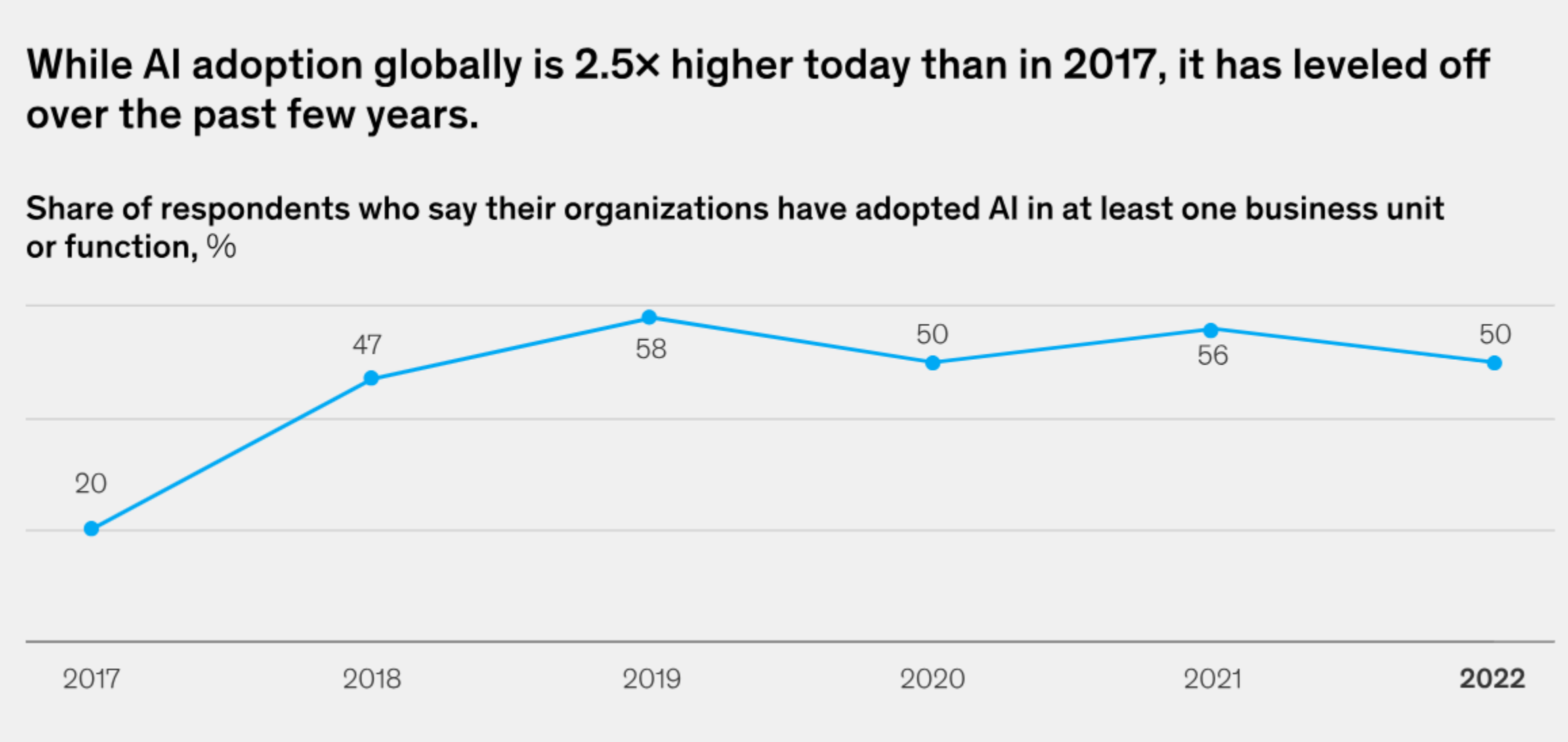
安全安心な人工知能システムへ向けて
－EU人工知能法とバイオメトリック識別システムを例に－

1. 安全安心なAIシステムとは
2. AIに対する世界的な規制の動き
3. 欧州AI法とその整合規格
4. バイオメトリクスと、想定される適合性評価
5. わたしたちにとって安全安心なAIシステムとは

※個社としての実際の対応とは異なる場合があります。

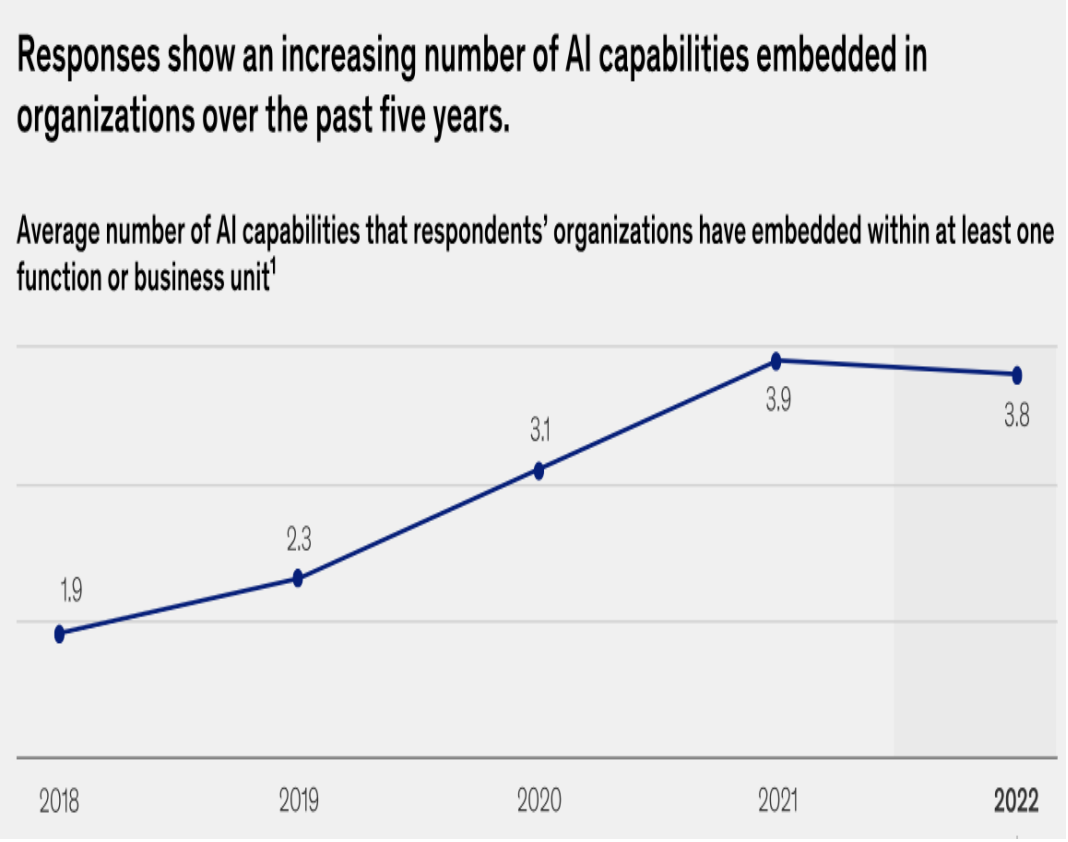
１．安全安心なAIシステムとは

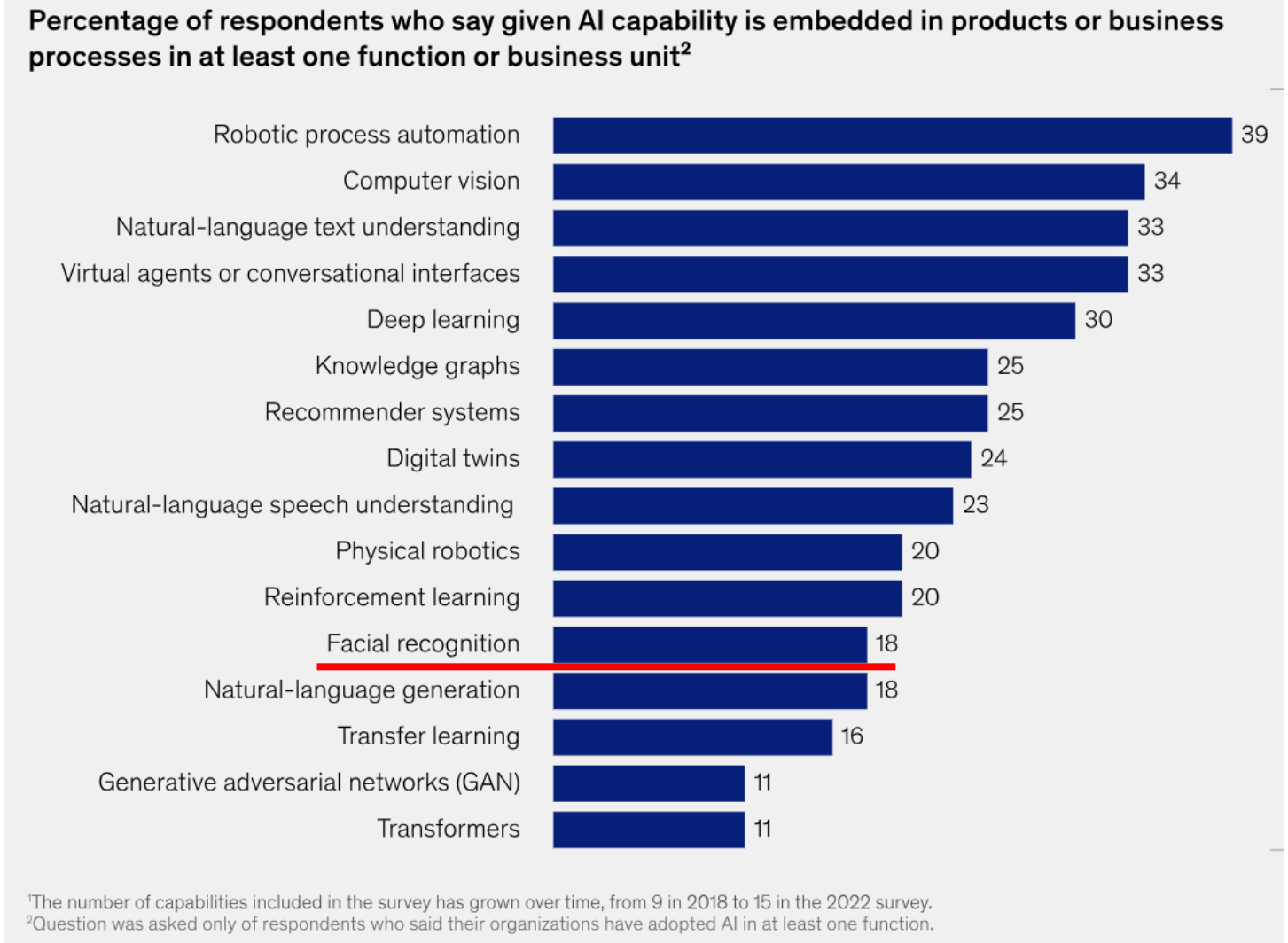
AIシステムの急速な伸張 その1



https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review

AIシステムの急速な伸張 その2





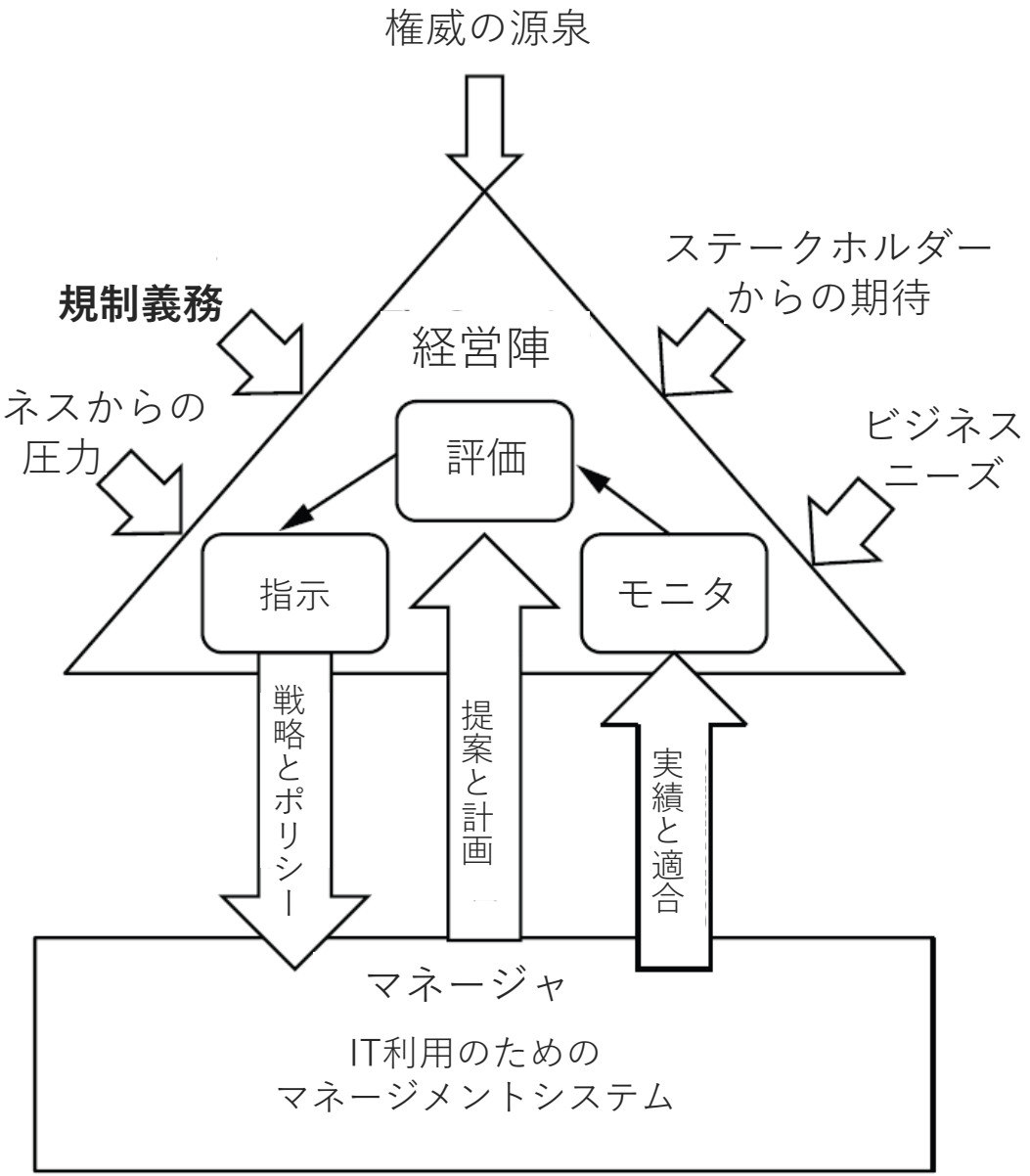
AIシステムの急速な伸張 その3

企業におけるITシステムの活用

- マネージャ
  - ITシステムを、PDCAを回しながら開発・管理
  - → マネージャ（人）に対する資格：PMBOK他
  - → 組織（プロセス）に対する認証：ISO 9001・14001他
  - → 個々の製品等に対する認証：ISO/IEC 15408、**CEマーク**他
  - →（組織に対する参考情報：ISO 31000）
  - AI技術を取り入れたITシステムの開発・管理は、以前と同様なマネージメントで十分か？
- 経営陣
  - 企業パフォーマンスが＋となるようガバナンス
  - → 善管注意義務（**善**良な**管**理者）

民法644条「受任者は、委任の本旨に従い、善良な管理者の注意をもって、委任事務を処理する義務を負う」
会社法330条「株式会社と役員及び会計監査人との関係は、委任に関する規定に従う」
経営判断の原則「経営上の専門的判断について、決定の過程及び内容に著しく不合理な点がなければ、善管注意義務にあたらない」

  - AIシステム開発・管理にあたって、以前と同様なガバナンスで十分か？



ITガバナンスのためのモデル

ISO/IEC 38500:2015より発表者が和訳引用

２．AIに対する世界的な規制の動き

米ホワイトハウスOSTP（科学技術政策局）：AI権利章典の青写真

- 米権利章典：1791に米合衆国憲法の修正として追加された人権条項
  → バイデン政権は、AIに関わる権利章典の検討を開始、2022年10月青写真公表

安全で効果的なシステム

アルゴリズムによる差別の保護

データプライバシ

通知と説明

人間の代替案、配慮と縮退運転

- ５原則を提示
- 適用対象は（AIそのものではなく）、
  1. 自動化されたシステム
  2. 米国民の権利、機会、重要な資源やサービスへのアクセスに重大な影響を与える可能性
- 米連邦政府各機関で、本青写真の推進と米国民を保護し支援する取り組みを推進

米ホワイトハウスOSTP（科学技術政策局）：AI権利章典の青写真

- **市民権、市民的自由、またはプライバシー：**
  - 自動コンテンツ調整ツールなどの言論関連システム；リスク評価、予測取締、自動ナンバープレート読取、**リアルタイム顔認識システム（特に公共の場や平和的抗議活動のような保護活動中に使用）**、SNS監視、足首監視装置などの監視及び刑事司法システム・アルゴリズム；署名照合ツールなどの投票関連システム；
  - スマートホームシステム及び関連データ、健康関連データの使用／収集システム、教育関連データの使用／収集システム、刑事司法システムデータ、広告標的システム、個人に関するプロファイルの構築／個人情報推論のためのビッグデータ分析システムなど、プライバシーに影響を与える可能性のあるシステム；
  - アルゴリズムによる差別につながる可能性のあるシステム。
- 機会均等：
  - 学生の不正行為／剽窃検出するアルゴリズム、入試アルゴリズム、オンラインまたはVRによる学生監視システム、学生の進度／成果予測、資源やプログラムへのアクセスの決定アルゴリズム、授業監視など、教育関連のシステム；
  - 入居審査アルゴリズム、住宅ローン引受／住宅保険用の住宅価値自動評価システム、オンラインアグリゲーターWebサイトからの自動評価などの住宅関連システム；
  - 給与／昇進／雇用や解雇のアルゴリズム、VR／ARの職場訓練プログラム、電子的な職場監視・管理システムなど、雇用条件のあらゆる側面に情報を提供する職場アルゴリズムなどの雇用関連システム。
- **重要な資源やサービスへのアクセス：**
  - 医療AIシステム及び機器、AI支援診断ツール、臨床的意思決定の支援用アルゴリズムまたは予測モデル、医療または保険健康リスク評価、薬物中毒リスク評価及び関連アクセスアルゴリズム、ウェアラブル技術、ウェルネスアプリ、保険ケア配分アルゴリズム、健康保険コスト及び引受アルゴリズムなどの健康及び健康保険技術；
  - ローン配分アルゴリズム、金融システムアクセス決定アルゴリズム、クレジットスコアリングシステム、リスク評価を含む保険アルゴリズム、自動金利決定、罰則を適用する金融アルゴリズム（例えば、給与差押や確定申告の源泉徴収が可能なもの）などの金融システムアルゴリズム；
  - 自動交通制御システム、電力網制御、スマートシティ技術、産業排出物及び環境影響制御アルゴリズムなど、地域社会の安全に影響を与えるシステム。情報の照合や分析、記録の照合など、給付の裁定を行う意思決定者の支援システム、同様に行政罰や刑事罰裁定の支援システム、不正検知アルゴリズム、サービスや給付へのアクセス制御アルゴリズム、**アクセス制御用の生体認証システム**、完全または部分的かつ自律的に給付やサービスに関する決定を行うシステム（給付を取り消す決定など）など、給付やサービスへのアクセス、または罰則の付与に関連するシステム。

英DSIT（科学・イノベーション・技術省）：AI規則へのイノベーション促進アプローチ

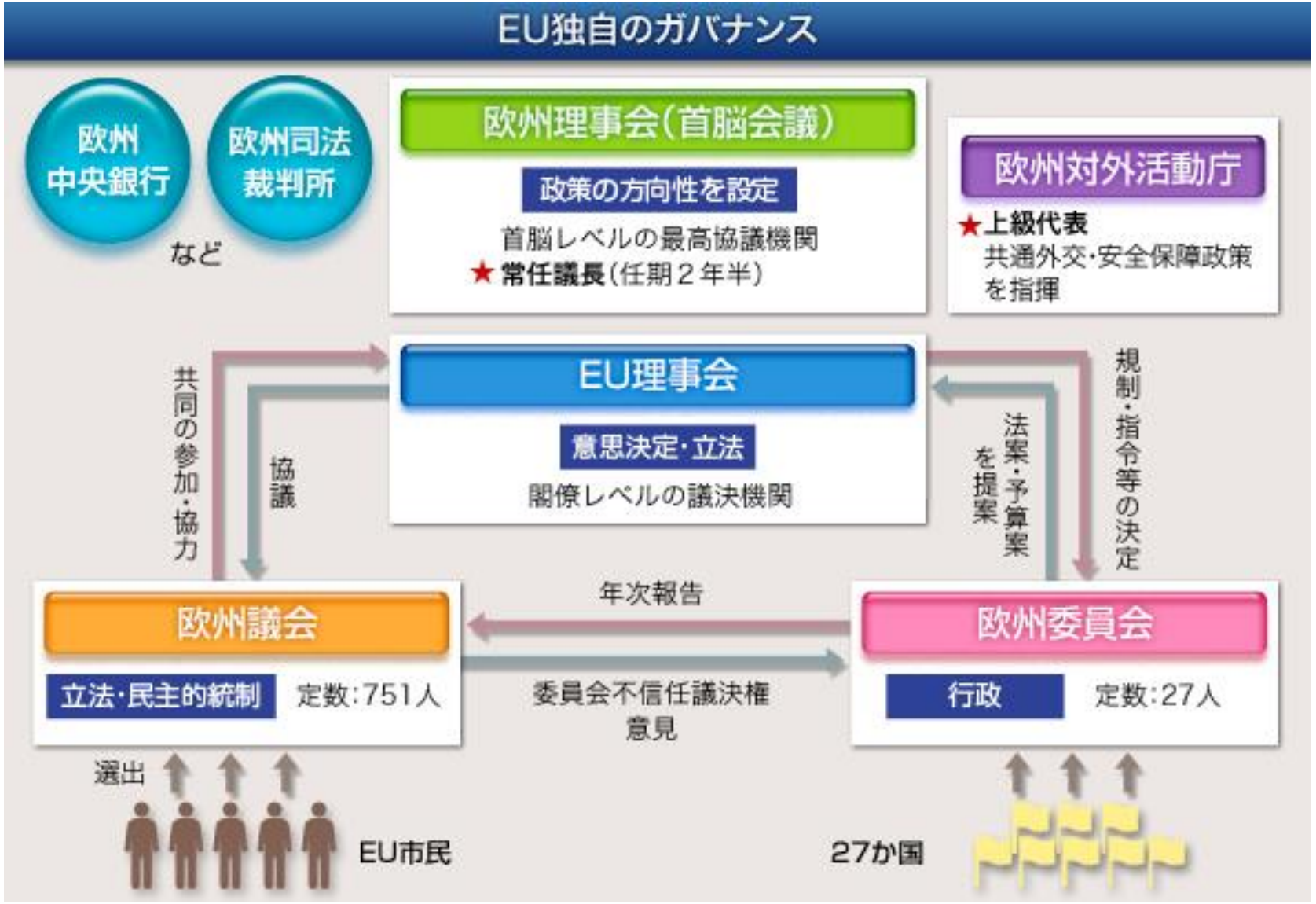
- 2023年2月にDSITを新設、英国がイノベーションのトップランナーとなることを目指す。
- AIに対する五原則：
  - 安全性、セキュリティ、堅牢性
  - 適切な透明性と説明可能性
  - 公平性
  - 説明責任とガバナンス
  - 競合性と救済
- 法制化は目指さない方針（イノベーションを抑制しない、規制当局が分野固有の専門知識を活用して対応）
- 初期期間で、原則の適切な適用を妨げる障壁を特定。必要に応じ規制当局に対して、本原則を十分に考慮することを義務付ける法的義務を導入検討する予定。

G7：広島AIプロセス閣僚級会合

- 令和5年9月7日（木）「広島AIプロセス閣僚級会合」開催
  - 参加国：カナダ、フランス、ドイツ、イタリア、日本（議長国）、イギリス、アメリカ、EU
  - 招待国際機関：OECD、GPAI
- 「G7広島AIプロセス G7デジタル・技術閣僚声明」採択
  1. OECDレポートに基づく優先的なリスク、課題、機会の理解
     - G7共通の優先的な課題・リスク及び機会を特定。
  2. 高度なAIシステム（基盤モデルや生成AIを含む。以下同じ。）に関する国際的な指針（guiding principles）及び行動規範（code of conduct）の策定
     - AI開発者を対象とする国際的な行動規範の策定が国際社会の喫緊の課題の1つであるという共通認識の下、行動規範策定の基礎として、AI開発者を対象とする指針の骨子を策定。
     - 年内に、開発を含む全てのAI関係者向けの国際的な指針を策定。
  3. 偽情報対策に資する研究の促進等のプロジェクトベースの協力
     - 国際機関と協力し、AIによって生成された偽情報を識別するための最先端の技術的能力に関する研究の促進等、プロジェクトベースの取組を推進することを計画。

３．欧州AI法とその整合規格

EU独自のガバナンス



https://www.mofa.go.jp/mofaj/press/pr/wakaru/topics/vol53/index.htmlより引用

欧州AI白書におけるハイリスクアプリケーション（1）

- 2020年2月、AI白書「卓越性と信頼性を追求する欧州の取り組み（A European approach to excellence and trust）」を発表。
  https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf
- 「C. 将来の欧州規則枠組の範囲」の中で、次の記載：
  - In light of its significance for individuals and of the EU acquis addressing employment equality, the use of AI applications for recruitment processes as well as in situations impacting workers' rights would always be considered "high-risk" and therefore the below requirements would at all times apply. Further specific applications affecting consumer rights could be considered.
    個人にとっての重要性と、雇用の平等に対処するEU協定を考慮すると、採用プロセスや労働者の権利に影響を与える状況でのAIアプリケーションの使用は、常に「ハイリスク」と見なされるため、次の要求事項が常に適用される。消費者の権利に影響を与える特定のアプリケーションも検討される可能性がある。

欧州AI白書におけるハイリスクアプリケーション（２終）

- the use of AI applications for the purposes of *remote biometric identification* and other intrusive surveillance technologies, would always be considered “high-risk” and therefore the below requirements would at all times apply.
  離れた距離からの生体識別や、その他の侵害的な監視技術のためのAIアプリケーションの使用は、常に「ハイリスク」と見なされるため、次の要件が常に適用される。

◆「D. 要求事項のタイプ」

- training data; 訓練データ
- data and record-keeping; データ及び記録保持
- information to be provided; 提供される情報
- robustness and accuracy; 頑健性と精度
- human oversight; 人による監査
- specific requirements for certain particular AI applications, such as those used for purposes of *remote biometric identification*
  離れた距離からの生体認証の目的で使用されるような、特定のAIアプリケーションに対する特有の要件

→ そもそも何を守らないといけないのか、守らないといけない程度とはどのようなものか

（参）日本国憲法において保証される人権カタログ

包括的基本権	13条（幸福追求権）	
法の下の平等	14条	
自由権	精神的自由権	19条（思想・良心の自由） 20条（信教の自由） 21条（集会・結社の自由、表現の自由） 23条（学問の自由）
	経済的自由権	22条（職業選択の自由、居住・移転の自由、外国渡航の自由、国籍離脱の自由） 29条（財産権の保障）
	人身の自由	18条（奴隷的拘束からの自由） 31条（法的手続きの保障） 33条～39条（被疑者・被告人の権利）
国務請求権	16条（請願権） 17条（国家賠償請求権） 32条（裁判を受ける権利） 40条（刑事補償請求権）	
参政権	15条（選挙権）	
社会権	25条（生存権） 26条（教育を受ける権利） 27条・28条（労働基本権）	

永井・森：法学入門（中央経済社）より引用

欧州委員会による「AIにおける卓越性と信頼性のための新しい規範と行動」の提案

- M. Vestager上級副委員長（デジタル時代の欧州戦略担当）
  - On Artificial Intelligence, trust is a must, not a nice to have. With these landmark rules, the EU is spearheading the development of new global norms to make sure AI can be trusted. By setting the standards, we can pave the way to ethical technology worldwide and ensure that the EU remains competitive along the way. Future-proof and innovation-friendly, our rules will intervene where strictly needed: when the safety and fundamental rights of EU citizens are at stake.
    AIにおいては信頼は必須であり、あればいいというものではない。この画期的な規範により、EUはAIが信頼できることを確認するための新しいグローバル規範開発の先頭に立つことになる。基準を設定することで、われわれは世界中で倫理的な技術への道を開き、その過程でEUが競争力を維持できるのである。未来志向でイノベーションに優しいわれわれの規範は、EU市民の安全と基本的権利が危機に瀕している場合など、厳密に必要なところに介入するものである。

→ 2021年4月21日　欧州AI規則（案）の公開

人工知能に関する整合規則（人工知能法）の制定及び、関連するEU法令改正のための提案（Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts））

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206

AI法成立へ向けて

REUTERS　マーケット　外為　株式市場　ニュース　ビデオ　More

テクノロジー　2023年5月11日 / 8:25 午後 / UPDATED 20日前

世界初のＡＩ包括的規制案、欧州議会委が承認　来月本会議採決へ

By Reuters Staff　1 MIN READ

AI法と整合する国際標準の審議が既に始まっている

いった生成人工知能（ＡＩ）の規制案が欧州連合（ＥＵ）欧州議会の二つの委員会で
た。（２０２３年　ロイター/Florence Lo/Illustration/File Photo）

ブリュッセル　１１日　ロイター］ - チャットＧＰＴといった生成人工知能（ＡＩ）規制案が欧州連合（ＥＵ）欧州議会の二つの委員会で１１日に承認された。来月、本議で採決が実施される見通しとなった。

制案は２年前に策定され、協議が続いていた。承認された規制案は顔認識や生体認証視、その他ＡＩアプリケーションの使用に関する規則を盛り込み、ＡＩ技術を管理す世界初の包括的規制となる。

制案では、ＡＩツールは、リスクの程度に応じて、低いものから許容できないものに類される。ツールを使用する政府や企業は、リスクのレベルに応じて異なる義務を負う。

公共の場での顔認識や予測的取り締まりツールの使用を禁止し、オープンＡＩのチャットＧＰＴのような生成ＡＩアプリケーションに新たな透明性措置を課す。

今後、欧州議会、欧州評議会、欧州委員会の各代表による協議で内容をさらに詰め、６月に欧州議会の本会議で採決する。可決成立した場合、順守のため２年程度の経過措置を設定する見通し。

AI法の現状

- 2021年4月：欧州委員会はAI法案（EU規則）を公表
- 2022年12月：EU理事会はAI法修正案を採択
- 2023年6月：欧州議会はAI法修正案を採択（EU理事会の修正案とは異なる）
- 2023年7月：欧州委員会、EU理事会、欧州議会の三社協議（トリオローグ開始）

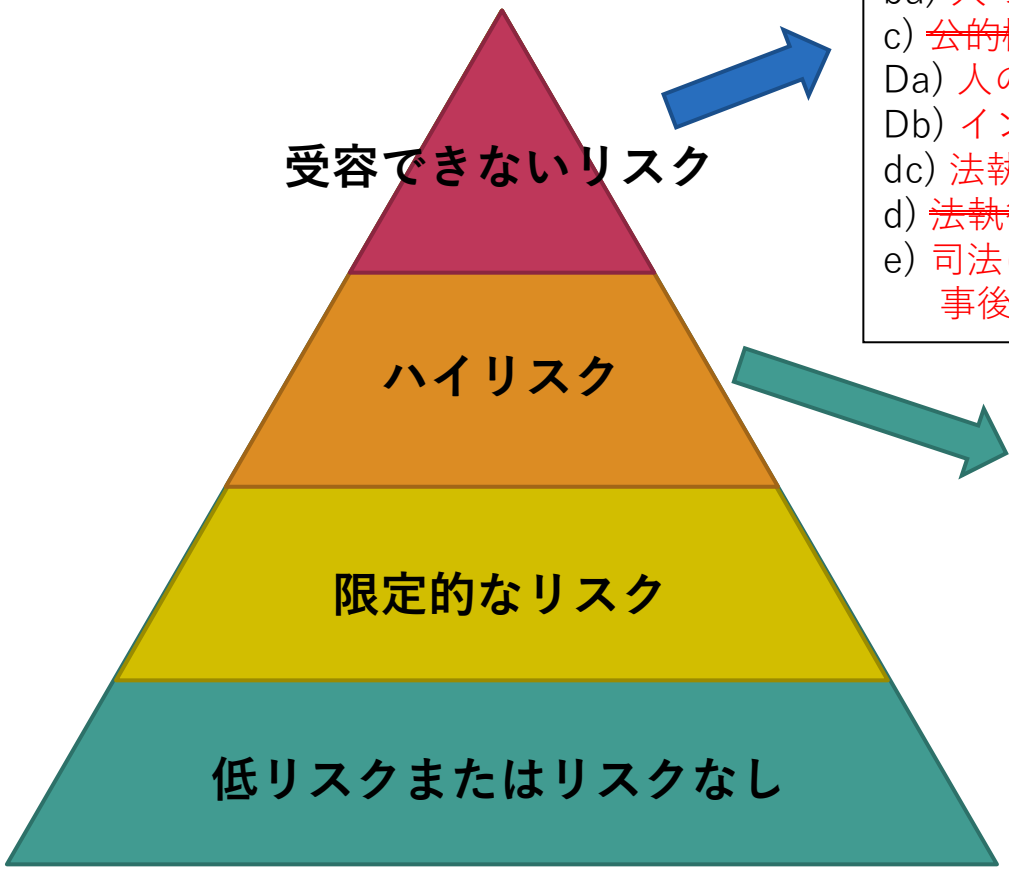
　欧州委員会のAI法案（原案）、EU理事会のAI法修正案、欧州議会のAI法修正案は、骨子は同じものの、相違点が存在（後で紹介）

→ 今のところ、年内をめどに合意に至る見込み、2026年をめどとして施行されると思われる

欧州AI法におけるAIシステムのリスク分類

◆ AI技術そのものではなく使い方によってリスクが生じる

■ リスクベースアプローチ＋比例原則に基づく規則　※原案・欧州議会AI修正案に基づく



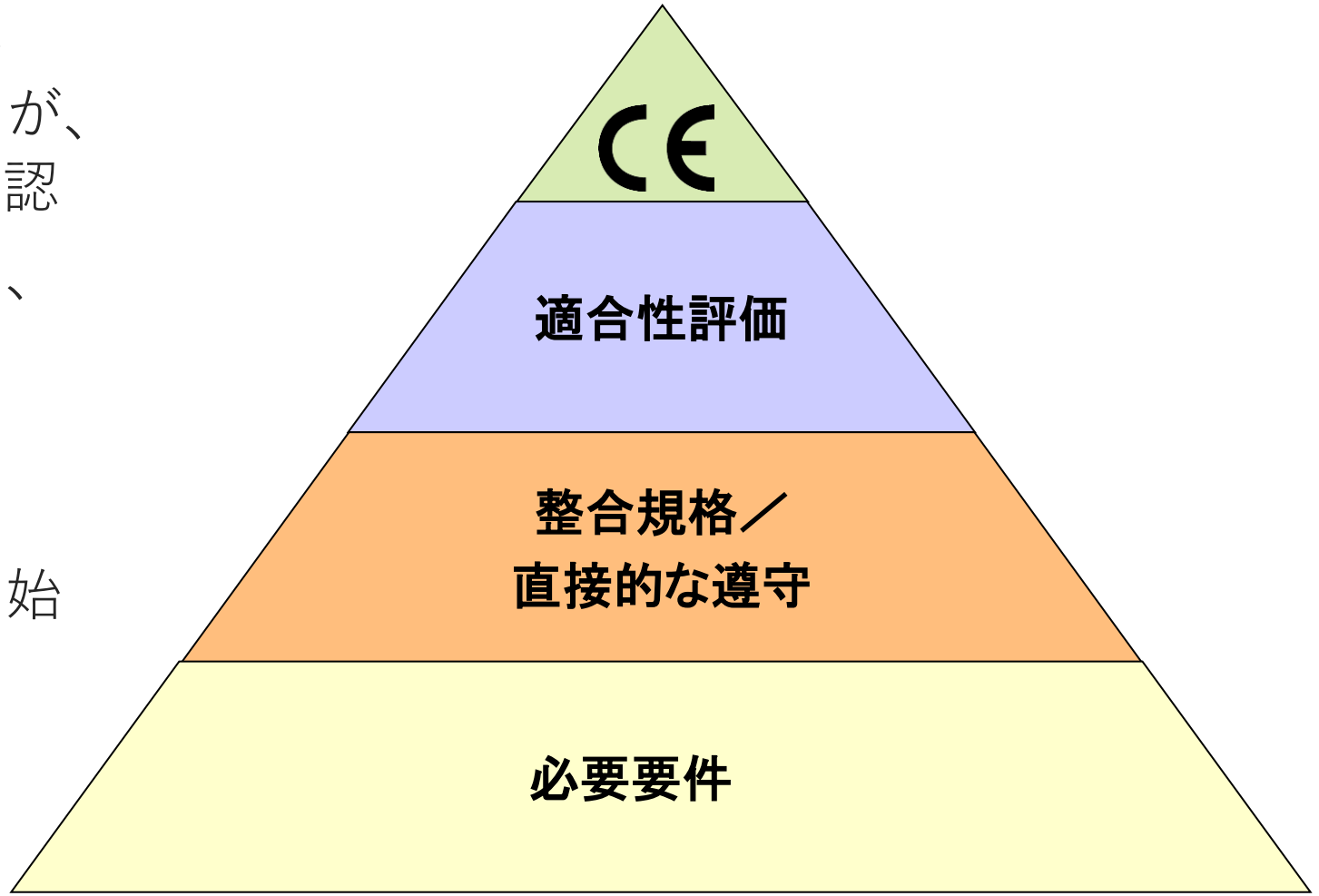
5条1項
a) サブリミナル技術あるいは意図的な操作的・欺瞞的技術で人の行動を歪曲
b) 弱い立場にある者の脆弱性につけこむ利用
ba) 人の機微な属性や属性からの推論に基づき分類する生体情報からの分類
c) ~~公的機関による~~社会的スコアリング
Da) 人のプロファイリング等による犯罪や再犯発生や再発生予測
Db) インタネットや防犯カメラから画像収集しDB作成・拡大
dc) 法執行機関、国境管理、職場及び教育機関での人の感情推測
d) ~~法執行機関による~~リアルタイムでの公共スペースでの遠隔生体識別システム
e) 司法による認証がありかつ特定の重大犯罪に対するものを除く、公共スペースでの事後遠隔バイオメトリクス識別システム

6条1項 → 附属書II記載の、NLFに基づく、あるいはそうでない整合法に基づく
6条2項 → 附属書III記載のAIシステム
1. バイオメトリクス、バイオメトリクスベースのシステム
   a) 自然人のバイオメトリクス識別システム
   aa) バイオメトリクス、バイオメトリクスベースの人の特徴推定システム
2. 極めて重要なインフラの管理・運用
3. 教育及び職業訓練
4. 雇用、労働者管理、自営業へのアクセス
5. 必要不可欠な民間サービスや公共サービス
6. 法執行
7. 移民、亡命、国境管理
8. 司法行政及び民主主義プロセス

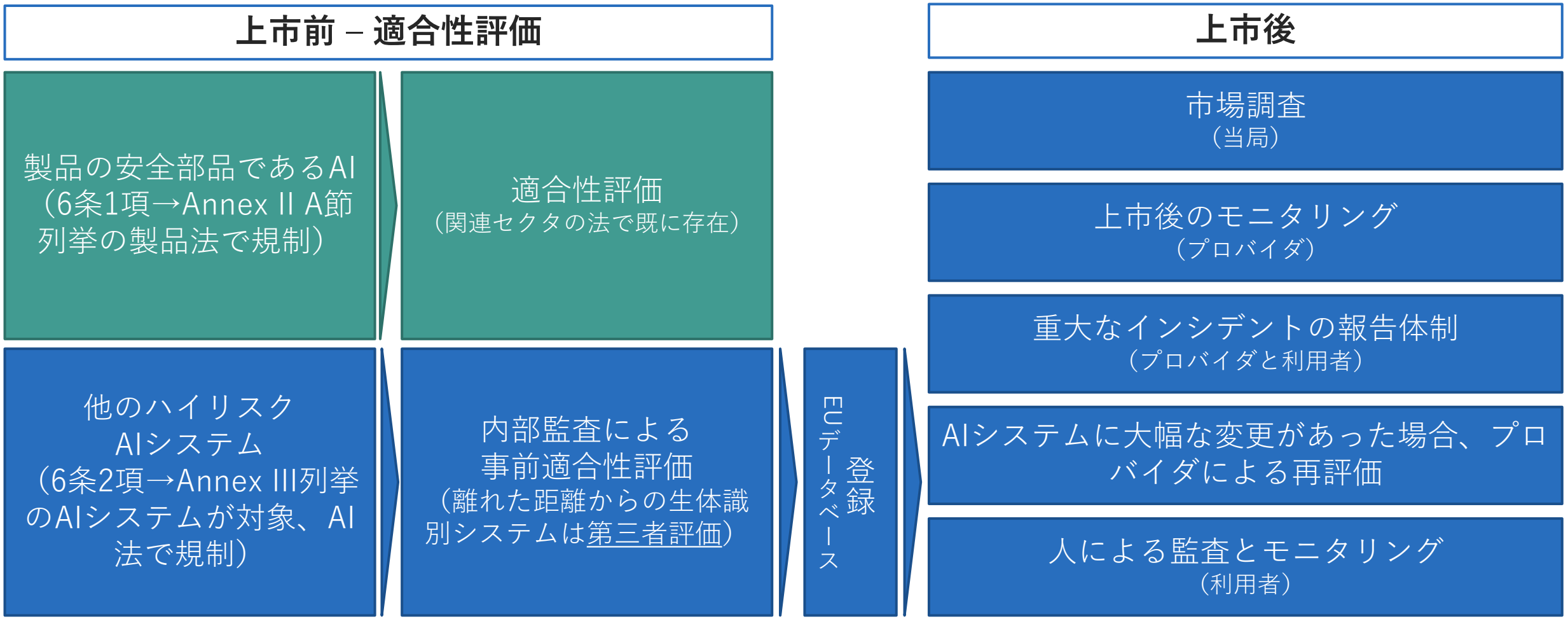
これらについても（案）に比較し詳細な記述に修正されている

ハイリスクAIシステムのEU市場上市までの手続き

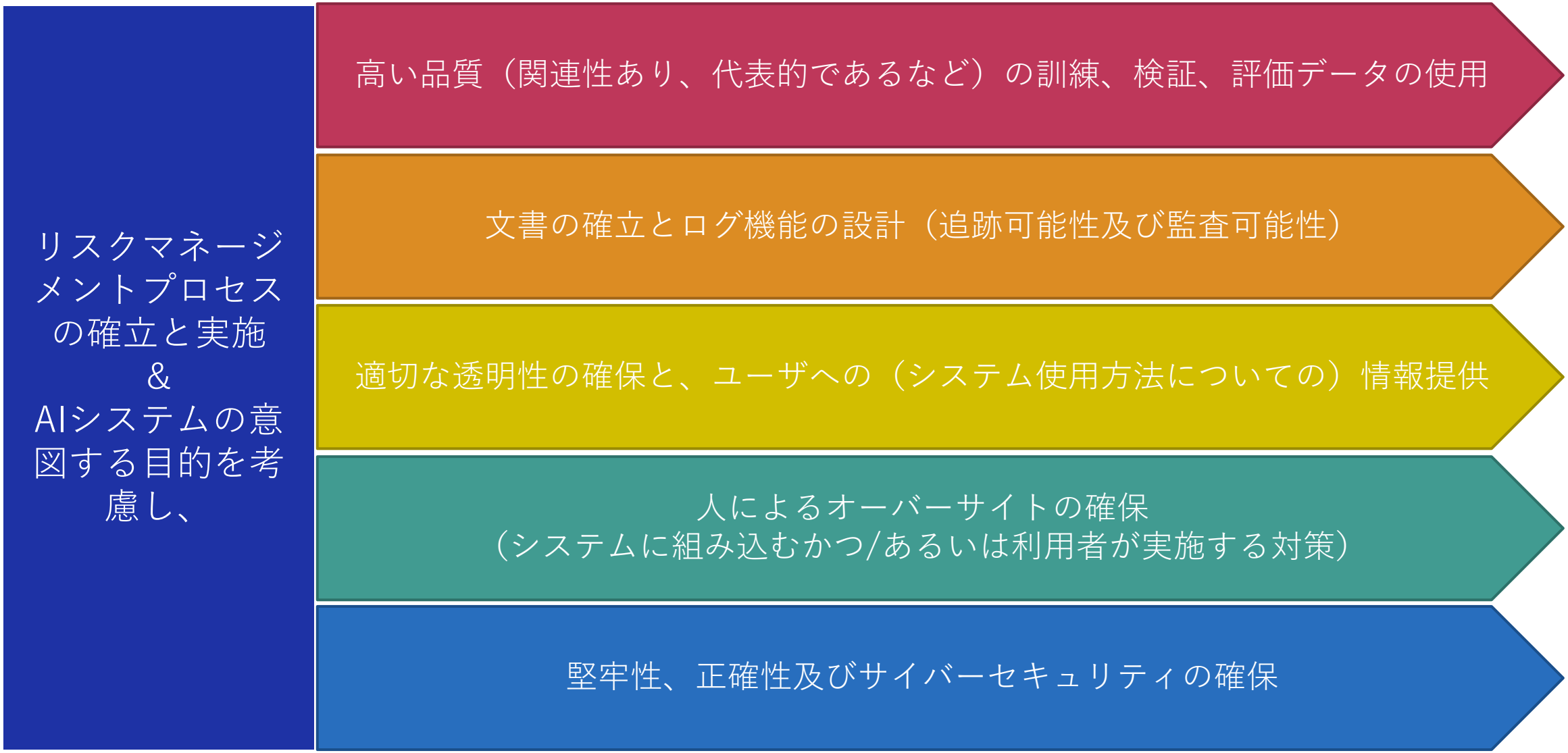
1. AIシステムが新しいAI規則の下で
   ハイリスクに分類されるか決定
2. 設計・開発および品質管理体制が、
   AI規則に適合していることを確認
3. 適合性を評価し証明するために、
   適合性評価手続きを受ける
4. CEマークをシステムに貼付し、
   適合宣言書に署名
5. 市場に出すまたはサービスを開始



適合性評価と執行



ハイリスクAIに対する要件の概要



AI法原案とふたつの修正案の差異 その1

	欧州委員会原案	欧州議会	EU 理事会
AI Act の適用対象	• 研究開発のみを目的とした AI 開発が含まれる	• 研究開発のみを目的とした AI 開発を除外	
AI の定義	• 独自の定義を提案	• OECD の定義*を基に修正	• 原案と OECD の定義を折衷
禁止 AI のスコープ	• サブリミナル利用 • 社会的弱者の脆弱性を利用 • 公的機関による信用スコアリング • 法執行目的の遠隔生体識別(テロ等、安全への脅威の予防は例外)	• 犯罪プロファイリング、法執行目的の感情推定や顔認証データベースの生成などを追加 • 遠隔生体識別の例外規定を削除	• 重要インフラへのテロ予防などを目的とした遠隔生体識別を例外範囲に追加
ハイリスク AI のスコープ	• 既存の EU 製品安全規制がある分野: 機械、玩具、リフト、無線機器および通信端末機器、圧力機器、旅客用ロープウェイ設備、ガス燃焼機器、医療機器、体外診断用医療機器等 • スタンドアロン AI: 遠隔生体認証、ライフラインインフラ、教育・職業訓練、採用・勤務評価、民間等	• 法執行目的以外の感情推定などを追加	-
		• 保険料の算定分野を追加 • 生体認証(authentication)と生体識別(identification)を区別	

https://www.eu-japan.eu/sites/default/files/publications/docs/EU-Digital-Policy8.pdf

AI法原案とふたつの修正案の差異 その2

	欧州委員会原案	欧州議会	EU 理事会
ハイリスク AI の法定要件	• リスクマネジメント • データとガバナンス • 文書化と記録保持 • 透明性と情報提供 • 人間の監視 • 堅牢性・正確性・安全性	• 欧州委員会などに同要件の詳細に係るガイドラインの発行を義務付け • ハイリスク AI のサプライチェーン間の責任移転に係る考え方を提示 • データガバナンス要件につき、生体データを取り扱う場合の要件を具体化(匿名化、仮名化及び組織的・技術的なデータ管理の運用など) • 訓練データセットの品質要件を一定度緩和 • 人の監視要件を一定度緩和	
生成 AI	(規定なし)	• 法定義務を新たに提示(後述)	-
執行体制	• 欧州委員会の諮問機関として EU 統一運用を担う EAIB(European Artificial Intelligence Board)を設立	• EU 統一運用を担う組織の位置づけを欧州委の諮問機関から独立組織 AI Office に変更	-
適合性評価	• 第三者認証に係る規定が不明確	• 既存の製品安全規格に準拠する場合(AnnexII SectionA)は、追加での適合性評価を原則不要と明記 • 欧州標準に準拠するスタンドアロン AI は、自社検査に基づく書類審査か第三者認証のいずれかを選択可能と明記	
事故対応	• 罰金は最大世界売上の 6%	• 罰金の上限を 7%に引上げ • 不利益を被った際、当局に申し出る権利を消費者に付与 • 重大事故発生時の当局への報告期限を 15 日から 72 時間に短縮	-
適用開始時期	• 施行 2 年後	• (変更なし)	• 施行 3 年後に延伸

（参）基盤モデル及び生成AIに係る規定

◆ 欧州議会AI法修正案が、上記規定を策定（禁止／ハイリスクAIとは独立）

■ 基盤モデル、生成AIのスコープを定義

- 基盤モデル：「基盤モデルとは、大規模なデータで訓練され、出力の汎用性を考慮して設計され、幅広い特徴的なタスクに適応できるAIシステムのモデルを指す」
- 生成AI：「複雑なテキスト、画像、音声、映像などのコンテンツを、様々な自律性のレベルで生成することを特に意図したAIシステム（「生成的AI」）で使用される基盤モデルのプロバイダー、および、基盤モデルを生成的AIシステムに特化させたプロバイダーは、さらに、次をを行わなければならない」

■ 基盤モデル提供者に対し、データガバナンス確立や、独立した専門家によるモデル評価、EUデータベースへの登録などを義務付け

■ 生成AI提供者にはさらに、透明性の確保、十分な安全措置、学習に利用した著作物やデータに係るサマリ情報の開示を義務付け

欧州AI法（案）の影響調査の結果（コスト）

- 欧州AI法（案）発表前に公開されたAI白書の分類に基づき、ハイリスクAIシステムの開発と運用に追加的に必要となるコスト等、影響調査を実施。
- 社内に品質マネジメントシステムを構築するには、193,000～330,000ユーロ（2億7,000万～4億6,000万円）、QMSの第三者認証に毎年71,400ユーロ（1,000万円）必要
  ＃なお金額は前提条件他により揺らぎ得る

AI白書：https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

平均的なハイリスクAIシステム
（開発コスト：170,000ユーロ（2,380万円）に
必要な追加コスト推計結果

AI白書に基づく項目	追加コスト推計結果
訓練データ	2,763ユーロ（約40万円）
文書化及び記録管理	4,390ユーロ（約60万円）
情報提供	3,627ユーロ（約50万円）
人による監査（／年）	7,764ユーロ（約110万円／年）
頑健性及び精度	10,733ユーロ（約150万円）

※140円/ユーロで算出

https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulationより引用

４．バイオメトリクスと、想定される適合性評価

ISO/IEC JTC 1/SC 37配下のWG構成と主要なプロジェクト

WG1：調和された生体認証用語
- ISO/IEC 2382-37:2022（定期的に更新）

WG6：生体認証の管理管轄及び社会に跨る側面
- ISO/IEC DIS 24714:2022（一般的なガイダンス）
- ISO/IEC 24779シリーズ（ピクトグラム）
- ISO/IEC TR 29194:2015（アクセシビリティ）
- ISO/IEC TR 30110:2015（生体認証と子供）

WG4：生体認証システムの技術実装
- ISO/IEC TR 24741:2018（概要とアプリケーション）
- ISO/IEC PWI 24358（顔検出画像撮影システム）

WG2：生体認証の技術インタフェース
- ISO/IEC 19784シリーズ（BioAPI / C言語用）
- ISO/IEC 30106シリーズ（BioAPI / Java, C#, C++）
- ISO/IEC 19785シリーズ（CBEFF）

WG3：生体認証データ交換形式
- ISO/IEC 19794シリーズ（G1 / G2）
- ISO/IEC 39794シリーズ（G3）
- ISO/IEC 29794シリーズ（データ品質）

WG5：生体認証の試験及び報告
- ISO/IEC 19795シリーズ（認証精度）
- ISO/IEC 30107シリーズ（偽造弁別）
- ISO/IEC CD 5152（日本提案精度推定）

整合規格として期待されるSC37プロジェクト

ISO/IEC 9868

- タイトルは、Remote biometric identification systems – Design, development, and audit（遠隔からのバイオメトリクス識別システム – 設計、開発と監査）
- ISO/IEC JTC1に対し欧州委員会がNPを出し承認され、同SC37が担当し開発中
- CD2へ進めることで合意したところ
- 欧州委員会がリエゾンとして参加、コメントも寄せており審議にも参加
- 新たにCEN-CENELEC JTC21ともリエゾン関係を締結、審議への参加を期待しているところ

ISO/IEC 19795-10

- タイトルは、Biometric performance testing and reporting – Part 10: Quantifying biometric system performance variation across demographic groups（バイオメトリクス性能試験と報告 – 第10部：人口統計グループ間でのバイオメトリクス性能変動の定量化）
- ISO/IEC JTC1/SC37に対し米国がNPを出し承認されて開発中
- DISへ進めることで合意したところ

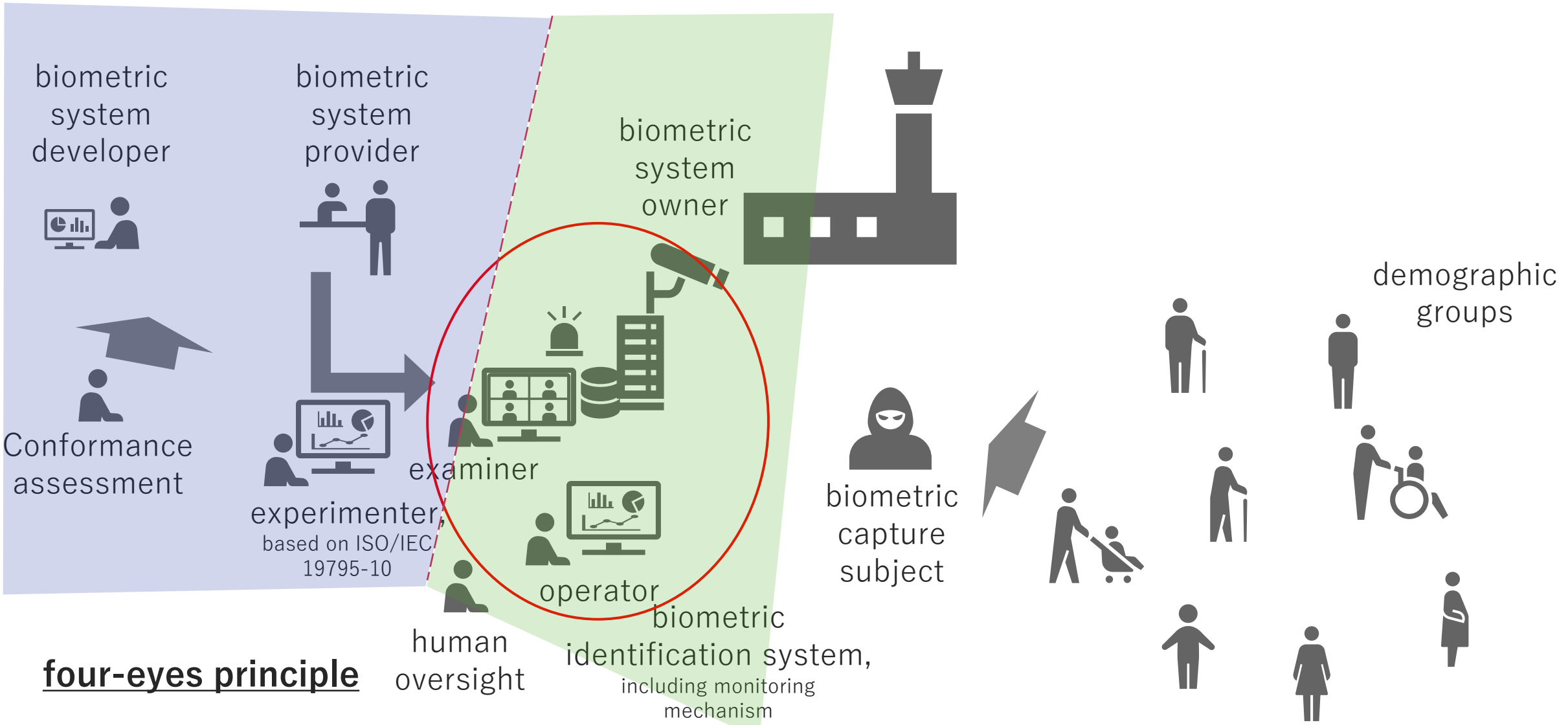
AIシステム ライフサイクル関連の義務概要

- 要件に応じた設計
  - AIシステムが所定の目的で一貫して機能し、AI法が規定する要求事項を遵守することを確認
- 適合性評価
  - 事前実施（遠隔からのバイオメトリクス識別システムは第三者評価）
- EU市場上市後のモニタリング
  - プロバイダは、AIシステムの信頼性、性能及び安全性に関する関連データを、AIシステムの存続期間を通じて積極的かつ体系的に収集、文書化、分析し、AIシステムが規制に対して継続的に準拠しているかどうかを評価
- インシデント報告システム
  - 重大なインシデントや、基本的人権に違反する機能不全（管轄権者による調査の根拠となる）の報告
- 新しい適合性評価
  - プロバイダや第三者による重要な変更（目的変更や規則に適合するAIシステムへと影響を及ぼす変更）がある場合の新しい適合性評価（プロバイダが示す「事前定義した範囲」外の変更を含む、継続的に学習するAIシステムも含む）

オペレータの義務概要

プロバイダの義務	➢組織内における品質マネジメントシステム確立と実施 ➢技術文書の作成と、最新状態への保持 ➢ハイリスクAIシステム運用監視のための、ログ記録 ➢事前適合性評価と、重要変更時の再評価 ➢AIシステムのEUデータベース登録 ➢CEマーク付与と適合性宣言への署名 ➢上市後の監視の実施 ➢上市後の監視当局との連携
ユーザの義務	➢使用説明書に従いAIシステムを運用 ➢AIシステム使用時に、人によるoversightの確保 ➢潜在的なリスクに対する運用モニタリング ➢重大なインシデントや機能不全についてプロバイダやディストリビュータに通知 ➢既存の法的義務について引き続いての適用（例：GDPRに基づく義務）

ISO/IEC CD 9868より（審議中のため今後変更の可能性あり）



※ISO/IEC 9868もAI法も「顔」に限定しない

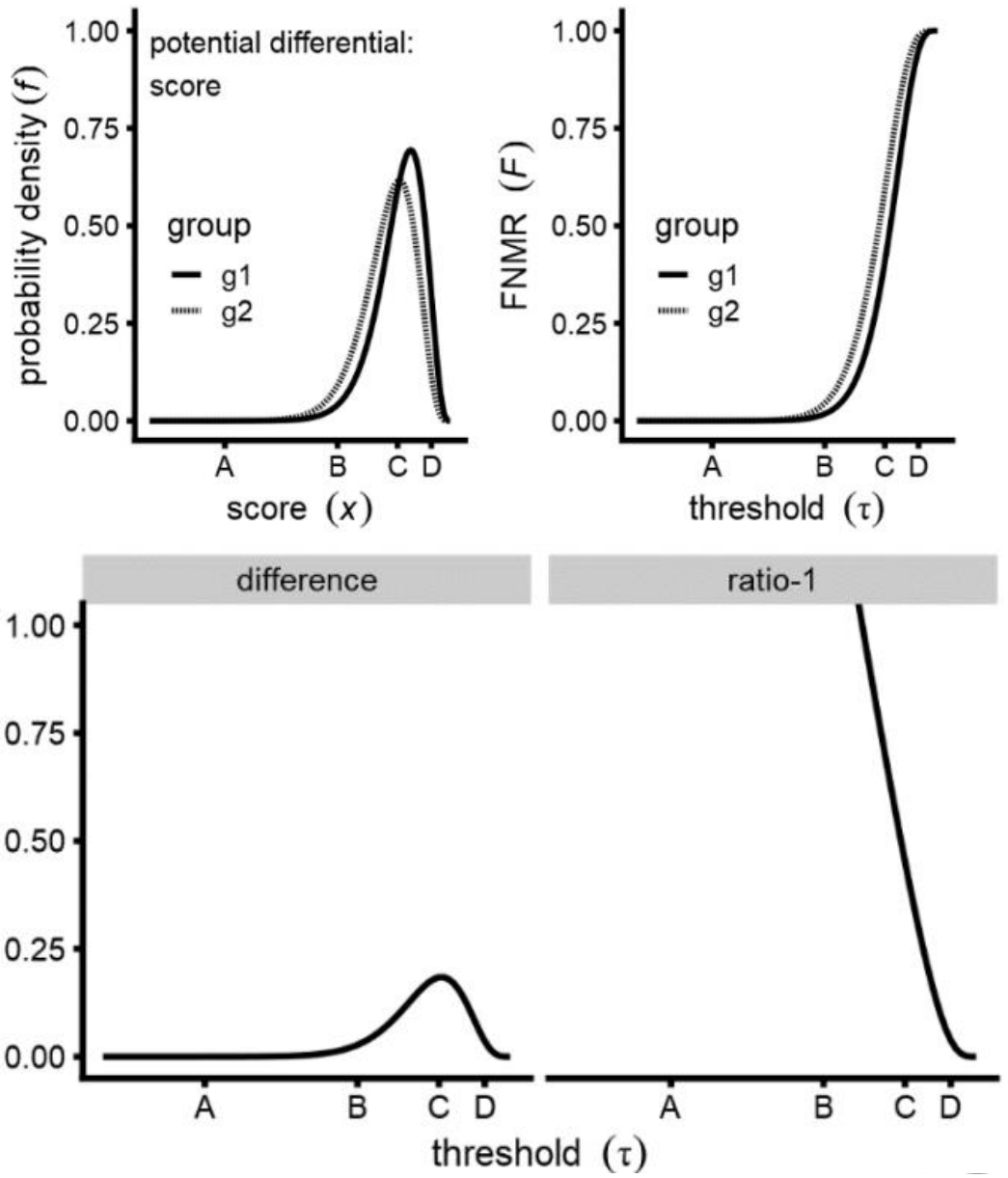
ISO/IEC CD 9868より（審議中のため今後変更の可能性あり）

主題		役割	責任（高レベル）	関連する詳細要件記載の条番号（ISO/IEC 9868）
リスク評価		Biometric system provider	予見されるシステムの使用方法に対する評価	7条
		Biometric system owner	特定の意図するユースケースに対する評価	
設計及び開発		Biometric system provider	システムの適切な開発、全ての必要な技術的機能の検証	8条及び9条
運用	能力	Biometric system provider	文書及び訓練の提供	10.1条
		Biometric system owner	能力の妥当性検証	
	運用上のセキュリティ	Biometric system owner	システムプロバイダ提供のセキュリティ機構利用	10.2条
	プライバシ対策	Biometric system owner	適切な対策を実施	10.3条
	社会的認知	Biometric system owner	情報公開	10.4条
	運用監視	Biometric system provider	モニタリングの仕組みと支援の提供	10.5条
		Biometric system owner	システムのモニタリング	
	改善	Biometric system provider	改善のための支援を提供	10.6条
		Biometric system owner	プロバイダ支援の下で改善の検証	

※Biometric system developerはbiometric system providerが責任を果たすための実装・支援を実施

ISO/IEC 19795-10より（審議中のため今後変更の可能性あり）

- 考慮すべき人口統計グループ
  - 分類上の人口統計グループ：Sex（生物学的な性）、Gender（社会的な性）、Ethnicity（民族性）、Birthplace（出生地）、Place of residence（居住地）
  - 連続する人口統計グループ：Age（年齢）、Weight（体重）、Height（身長）、Skin lightness（肌の明るさ）
  - その他（上記だけとは限定していない）
- 問題点
  - 差がどの程度であれば許容されるのか
  - 複数の人口統計グループの関係が十分考慮されていない（グループ分割数を多くすると必要なサンプル数が爆発し実施不可能となり得る）
  - オペレーションデータには正確なラベル付けが困難なことがある



（参）2005年10月27日開催 PRMU研究会 特別講演

お知らせ 2023年度・2024年度 学生員 会費割引キャンペーン実施中です
お知らせ 技術研究報告と和文論文誌Cの同時投稿施策(掲載料1割引き)について
お知らせ 電子情報通信学会における研究会開催について

電子情報通信学会 研究会発表申込システム
研究会 開催プログラム

技報閲
[ログイ
技報ア

トップ　戻る　前のPRMU研究会 / 次のPRMU研究会　[HTML] / [HTML(simple)] / [TEXT]　[Japanese

パターン認識・メディア理解研究会（PRMU）　[schedu

専門委員長　村瀬 洋
副委員長　中村 裕一，佐藤 真一
幹事　佐藤 洋一，目加田 慶人
幹事補佐　黄瀬 浩一

日時	2005年10月27日(木) 10:30 – 17:00 2005年10月28日(金) 09:30 – 17:15
議題	顔・ジェスチャーの認識・理解
会場名	東北大学工学部 電子情報システム・応物系1号館 4階 453号室
住所	〒980-8579 仙台市青葉区荒巻字青葉6-6-05
	市バス：仙台駅前西口バスプール9番乗り場から「工学部経由動物公園循環」「宮教

10月27日(木) 午後　テーマセッション(1)
13:45 – 15:45

(5)	13:45–14:15	ユビキタス環境における対話型ロボットのための顔識別システム	○坂上文彦・右田剛史・尺長　健(岡山大)・佐竹純二・近間正樹・上田博唯(NICT)
(6)	14:15–14:45	物体表面の見え属性分類に基づくSelf Quotient Image を用いた顔認識	○西山正志・山口　修(東芝)
(7)	14:45–15:15	隣接画素差分量子化による顔認識	○李　菲菲・小谷光司・陳　キュウ・大見忠弘(東北大)
(8)	15:15–15:45	ガウシアンフィルタによる画像分解を用いた照明変動にロバストな顔画像認識	○坂上文彦・尺長　健(岡山大)
	15:45–16:00	休憩　（ 15分 ）	

10月27日(木) 午後　特別講演
16:00 – 17:00

(9)	16:00–17:00	[特別講演]IC旅券と，顔認証技術導入へ向けての評価	○榊　純一(松下電器)・坂本静生(NEC)・矢野博司(オムロン)・神田　宰(松下電器)・塩原守人(富士通研)・助川　寛(東芝)・磯部義明(日立)・春山　智(NTTデータ)・村田伸一(OKI)・吉澤正浩(NTT)・平野誠治(凸版印刷)・室田秀樹(大日本印刷)・瀬戸哲司(富士フイルム)・松中耕二(コニカミノルタフォトイメージング)・山越　学(国立印刷局)

10月28日(金) 午前　テーマセッション(2)
09:30 – 11:30

(10)	09:30–10:00	クラスタ化された特徴セットにより学習された複数識別器を用いた性別認識	○桑原隆比古・池田　仁・加藤典司・鹿志村洋次(富士ゼロックス)
(11)	10:00–10:30	対話調整的役割を果たす顔表情の	○中島　慶・藤江真也・松坂要佐・小林哲則(早大)

電子情報通信学会誌 2006年1月号にも
ほぼ同内容の解説あり、参照願いたい。

残された課題

◆ プロセスや評価方法の整備は進むが、適合性判定をどう行うべきか明確でない

→ 欧州議会修正案には6条に次のパラグラフが追加される：

「この規則発効の6ヶ月前に、AIオフィス及び関連する利害関係者への協議の後、欧州委員会は、Annex III記載のAIシステム出力が、自然人の健康、安全、または基本的人権に重大な損害を生じさせる事例やそうでない場合において、明確に状況を指定するガイドラインを提供することとする。」

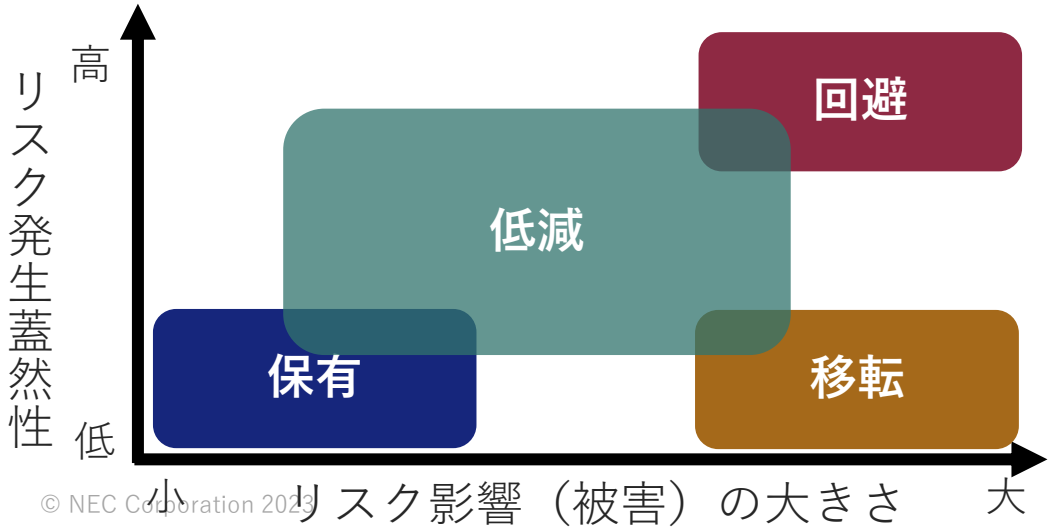
◆ 国際規格の開発と並行して、欧州委員会へ向けガイドラインの内容に対する調整を継続する必要がある

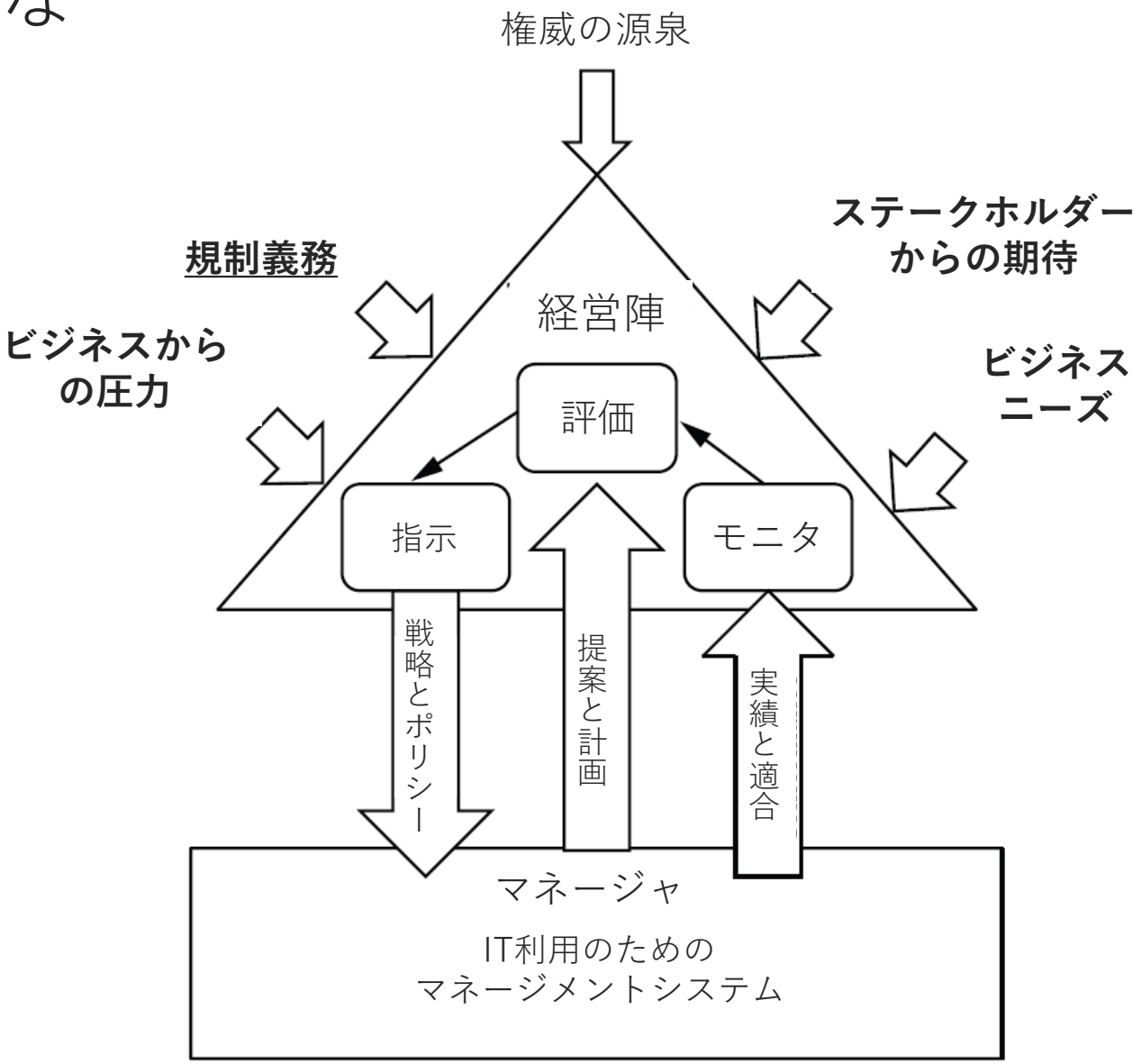
◆ 上記とは別に、AI MSS（マネージメントシステム標準、ISO/IEC 42001）準拠も求められる。

5．わたしたちにとって安全安心なAIシステムとは

わたしたちにとっての安全安心なAIシステムとは

- AIリスクの程度**にも**見合う、信頼性確保努力
  コスト：ベンダーとユーザの相互理解へ
- ガバナンス：経営判断の原則を踏まえ、経営が過度に委縮することのないように
- マネージメント：想定されるリスクを管理し、影響を最小限に
  → マネージャ（人）に対する資格
  → 組織に対する認証
  → 個々の製品・サービス等に対する認証





ITガバナンスのためのモデル

ISO/IEC 38500:2015より発表者が和訳引用


Orchestrating a brighter world
NEC