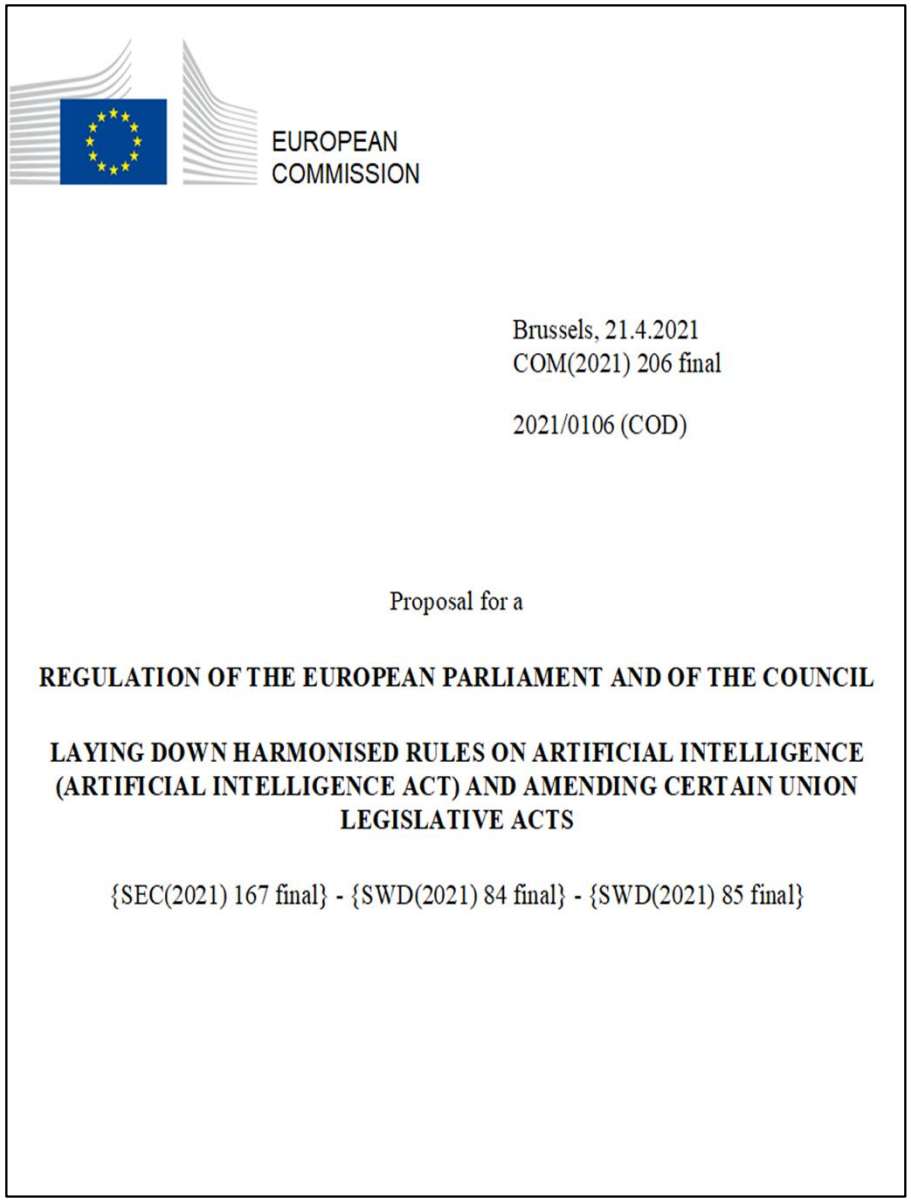
EU AI規則案の最新動向

2023年9月

欧州連合日本政府代表部

※原文が英語の内容の日本語訳は仮訳です。
※AI規則案及びその修正案の内容は網羅的なものではありません。
※条番号は別途明示しない限り欧州委員会提案のものです。

EU AI規則案（AI Act）とは



EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

○ 欧州委員会は、**2021年4月21日、AI規則案を公表**。その目的として、利用者の信頼を増すことで、EUにおけるAIの活用・イノベーションやAIへの投資を強化するとともに、人々と企業の安全と基本的権利を保護するとしている。

○ **リスクベースアプローチを採用**し、4つのリスクレベルを設け、各々のリスクに応じた要件・規制を設定。

○ EU域内にAIシステムを提供する**域外企業も適用対象**。

○ **違反の場合、最大で3,000万ユーロ又は年間世界売上高の6%の罰金**。

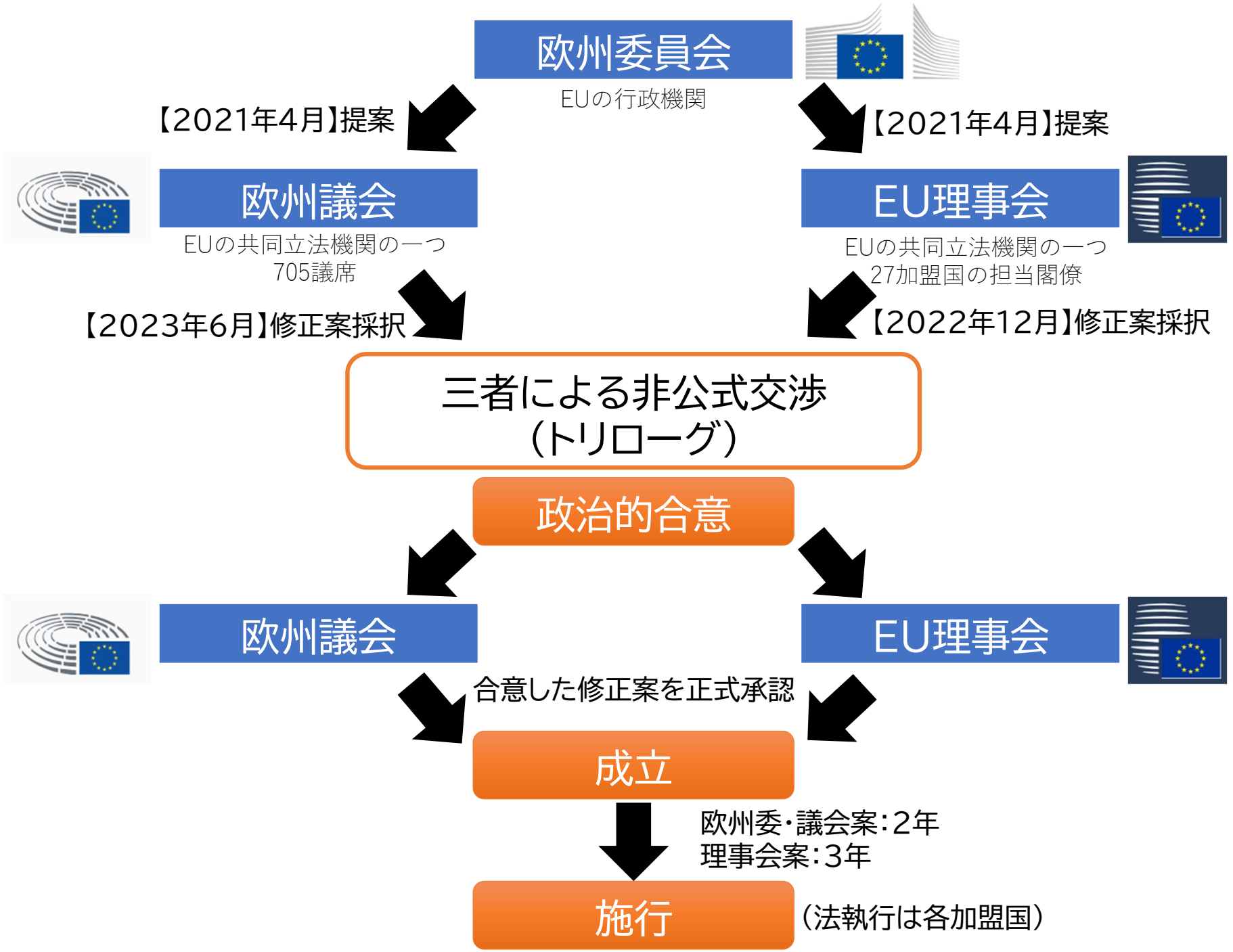
議会修正案

■ **最大で4000万ユーロ又は7%。**

○ AIシステムの市場投入前に、革新的なAIシステムの**開発、試験、検証を実施できる環境として「AI規制サンドボックス」を提供する**。

○ 2022年12月にEU理事会が、2023年6月に欧州議会が、それぞれ修正案を採択。**現在、両立法機関による交渉中。**

審議経過と今後のスケジュール



適用対象範囲（第2条）

対象事業者

1. AIシステムをEU域内で市場に投入する又はサービス提供するプロバイダー（provider）。**設立場所がEU域内か第三国かは問わない**。
2. EU域内に所在するAIシステムの利用者（user）。
3. **アウトプットがEU域内で利用される**場合、**第三国に所在するAIシステムのプロバイダー及び利用者。**

適用除外

1. **下記個別法の適用対象は、第84条（見直し規定）のみ適用**。
   a. 民間航空の安全性に関する規則（Regulation (EC) 300/2008）
   b. 農林業用車両に関する規則（Regulation (EU) No 167/2013）
   c. 二輪、三輪及び四輪車両に関する規則（Regulation (EU) No 168/2013）
   d. 船舶用機器に関する指令（Directive 2014/90/EU）
   e. 鉄道網の相互運用性に関する指令（Directive (EU) 2016/797）
   f. 自動車及びその部品に関する規則（Regulation (EU) 2018/858）
   g. 民間航空分野の共通ルールに関する規則（Regulation (EU) 2018/1139）
   h. 自動車の型式承認に関する規則（Regulation (EU) 2019/2144）
2. **軍事目的のみ**のために開発又は利用されるAIシステム

理事会修正案

- **研究開発活動**は適用除外。
- **科学的研究目的のみのために開発・市場投入されたAIシステムとそのアウトプット**は適用除外。
- **個人的な非職業的活動の過程でAIシステムを使用する自然人**は適用除外。

議会修正案

- **市場投入前又はサービス開始前の研究、試験及び開発活動**は適用除外。ただし、現実世界の環境でのテストは対象外。詳細は欧州委員会が委任法令を作成。
- **無料かつオープンソースライセンスの下で提供されるAIコンポーネント**については、ハイリスクAIシステムの一部とならない限り、適用除外。**ただし、基盤モデルは対象外**。

定義①（第3条）

AIシステム（AI system）

欧州委提案	理事会案	議会案	（参考）OECDの定義
Annex Ⅰに記載された技術及びアプローチの1つ以上を用いて開発され、人間が定義した所定の目的のために、相互作用する環境に影響を与えるコンテンツ、予測、推奨又は決定などのアウトプットを生成できるソフトウェア。 <Annex Ⅰ> (a) 機械学習アプローチ：教師あり学習、教師なし学習、強化学習など、深層学習を含む多様な手法を用いるもの。 (b) 論理及び知識ベースアプローチ：知識表現、帰納的（論理）プログラミング、知識ベース、推論・演繹エンジン、（記号）推論、エキスパートシステムなど。 (c) 統計的アプローチ、ベイズ推定、探索・最適化手法。 ※Annex Ⅰを欧州委が委任法令で改正可能。	自律性の要素をもって動作するように設計され、機械又は人間が提供したデータ及びインプットに基づいて、機械学習又は論理及び知識ベースアプローチを用いて所定の一連の目的を達成する方法を推論し、コンテンツ（生成AIシステム）、予測、推奨又は決定などのシステムにより生成されるアウトプットを生み出し、相互作用する環境に影響を及ぼすシステム。 ※「機械学習又は論理及び知識ベースアプローチ」の技術的詳細を欧州委が実施法令で規定可能。	様々なレベルの自律性で動作するように設計され、明示的又は暗黙的な目的のために、物理的又は仮想的な環境に影響を与える予測、推奨又は決定などのアウトプットを生成できる機械ベースのシステム。	人間が定義した目的に対して、現実又は仮想的な環境に影響を与える予測、推奨又は決定を行うことができる機械ベースのシステムであって、様々なレベルの自律性を持って動作するように設計されているもの。

定義②（第3条）

プロバイダー（provider）

「プロバイダー」とは、**有償・無償を問わず**、**AIシステムを開発し**、又は**自己の名称若しくは商標の下に市場に投入若しくはサービス提供することを目的として開発されたAIシステムを有する**自然人若しくは法人、公官庁、機関又はその他の団体をいうものとする。

利用者（user）

「利用者」とは、**自らの権限の下でAIシステムを使用する**自然人又は法人、公的機関、代理店又はその他の機関をいう。ただし、AIシステムが**個人的な非職業的活動の過程で使用される場合を除く**。

理事会修正案

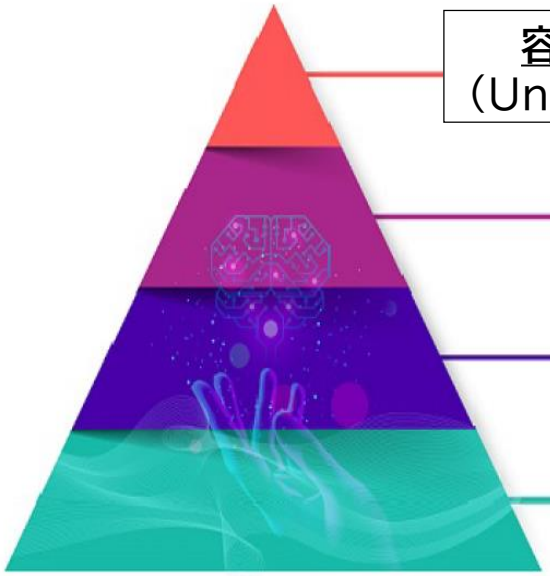
- 「利用者」の但し書きを適用除外規定に移動。

議会修正案

- 「user」を「delpoyer」（導入者）に修正（定義はそのまま）。

リスクベースアプローチ

○ AI規則案では、**リスクベースアプローチを採用**し、4つのリスクレベルを設け、各々のリスクに応じた要件・規制を設定。



（欧州委員会HP等の資料から一部加工）

容認できないリスク（Unacceptable Risk）	➢ サブリミナル技術、ソーシャルスコアリング、公共空間における法執行目的でのリアルタイム遠隔生体認証システム　等 ➢ **原則禁止**
ハイリスク（High Risk）	➢ 機械、医療機器、重要インフラ、教育、雇用、法執行　等 ➢ **プロバイダー、輸入者、販売業者、利用者それぞれに対して、リスク管理、データガバナンス、技術文書の作成、人的監視措置、適合性評価手続、ログ保存など厳格な規制**
限定的なリスク（Limited Risk）	➢ 自然人とやり取りするAI、感情認識システム　等 ➢ **AI使用の告知など限定的な義務**
最小限のリスク（Minimal Risk）	➢ 上記以外 ➢ **自由に利用可能** **（自主的な行動規範の推奨あり）**

理事会修正案

■ **汎用AI（general purpose AI）というカテゴリー及び対応する義務を追加。**
- ➢ **画像・音声認識、音声・映像生成、パターン検出、質問応答、翻訳などの一般的に適用可能な機能**を実行することをプロバイダーが意図したAIシステム。
- ➢ プロバイダーが使用説明書等において、全てのハイリスク用途を明確に排除している場合、各種要件・義務は不適用。
- ➢ それ以外の場合、一部の要件・義務が適用。

議会修正案

■ **基盤モデル（foundation model）、生成AI（generative AI）というカテゴリー及び対応する義務を追加。**
- ➢ 生成AI：**複雑なテキスト、画像、音声、動画などのコンテンツを、様々なレベルの自律性をもって生成することを特に意図したAIシステムに使われる基盤モデル。**
- ➢ 透明性確保、違法コンテンツの生成を防ぐセーフガードの確保、学習に使用した著作物に関する十分に詳細な概要の作成・公表を義務づけ。

全てのAIシステムに適用される一般原則

議会修正案（第4条a）

本規則の適用を受ける**全ての事業者は**、倫理的で信頼できるAIに対する首尾一貫した人間中心の欧州のアプローチを促進するハイレベルの枠組みを確立する**以下の一般原則に従って、AIシステムまたは基盤モデルを開発し、使用するよう最善の努力を払わなければならない**。

人的監視	AIシステムが、人間に奉仕し、人間の尊厳と個人の自律性を尊重し、人間が適切に管理・監督できる形で機能するツールとして開発・使用されること。
技術的な堅牢性と安全性	AIシステムが、意図しない予期せぬ危害を最小化するように開発され、利用されること、また、意図しない問題が発生した場合に堅牢であること、悪意のある第三者によるAIシステムの用途や性能を改変しようとする試みに対して強靭であること。
プライバシーとデータガバナンス	AIシステムが、品質と完全性の面で高い基準を満たすデータを処理しながら、既存のプライバシーとデータ保護規則を遵守した上で開発・使用されること。
透明性	AIシステムが、適切なトレーサビリティと説明可能性を可能にする方法で開発され、使用されること。同時に、人間がAIシステムとやり取りすることを認識させ、また、AIシステムの能力と限界について利用者に、また、影響を受ける人々にその権利について適切に通知すること。
多様性、非差別、公平性	AIシステムが、多様な主体を含み、平等なアクセス、男女平等、文化的多様性を促進する方法で開発・使用されるとともに、法令で禁止されている差別的影響や不当なバイアスを回避すること。
社会的・環境的福祉	AIシステムが、個人、社会、民主主義への長期的な影響を監視・評価しながら、持続可能で環境に優しい方法で、また全ての人間に利益をもたらす方法で開発・使用されること。

※具体的には本規則の各義務規定や欧州標準の採用等を通じて達成されるため、新たな義務を創設するものではない、と規定されている。

AIリテラシー

議会修正案（第4条b）

- EU及び加盟国は、AIシステムの民主的な管理を可能にする観点から、教育訓練、スキリング及びリスキリングプログラムを通じて、十分なレベルのAIリテラシーの発展のための措置を促進するものとする。
- **AIシステムの提供者及び導入者は、職員の十分なレベルのAIリテラシーを確保するための措置を講じなければならない**。
- このようなリテラシー対策は、特に、**様々な種類の製品及び用途、そのリスク及び便益を含む、AIシステム及びその機能に関する基本的な概念及びスキルの教育**から構成されるものとする。
- 「十分なレベルのAIリテラシー」とは、プロバイダー及び導入者が本規則の遵守及び実施を確保する能力に資するものである。

禁止されるAIシステム（第5条）

1. サブリミナル技術を使用するAIシステム

人に身体的又は心理的な損害を与える又は与え得る方法で人の行動を実質的に歪めるために人の意識を超えたサブリミナル技術を導入するAIシステムの上市、サービス展開、使用。

2. 子供や障害者等を搾取するAIシステム

人に身体的又は心理的な損害を与える又は与え得る方法で人の行動を実質的に歪めるために年齢、身体的又は精神的障害に起因する特定の集団の脆弱性を利用するAIシステムの上市、サービス展開、使用。

理事会修正案　議会修正案　「公的機関による」を削除。

3. ソーシャルスコアリング（公的機関による）

公的機関又はその代理人による、社会的行動又は既知若しくは予測される個人的若しくは人格的特徴に基づいて一定期間にわたって自然人の信頼性を評価又は分類するためのAIシステムの上市、サービス展開、使用であって、ソーシャルスコアが以下のいずれか又は両方をもたらすもの。

（1）データが元々生成又は収集された文脈とは無関係な社会的文脈において、特定の自然人又はその集団全体を不利に扱うこと。

（2）特定の自然人又はその集団全体に対して、その社会的行動又はその重大性に照らして不当又は不相当な不利な扱いをすること。

4. 公衆がアクセス可能な空間における法執行目的でのリアルタイム遠隔生体認証システムの利用。ただし、以下の目的のために厳密に必要な場合は除く。

（1）行方不明の子供を含む、特定の潜在的な犯罪被害者の的を絞った捜索

（2）自然人の生命又は身体の安全に対する特定の、重大かつ差し迫った脅威、又はテロ攻撃を防止すること

（3）少なくとも3年の最長期間の拘留刑又は拘留命令により罰せられる犯罪の実行者又は容疑者の発見、位置特定、特定又は起訴

議会修正案

- **リアルタイム遠隔生体認証システムの利用禁止について、「法執行目的」及び例外規定を削除（＝全面禁止）。**
- **以下を追加。**
  - **「事後」遠隔生体認証システム。**司法承認後、重大な犯罪の起訴のための法執行目的は例外。
  - **機微な特徴（例：性別、人種、民族、市民権、宗教、政治的指向）を利用した生体分類システム。**
  - **予測的取締りシステム**（プロファイリング、位置情報、過去の犯罪行動に基づく）。
  - **法執行、国境管理、職場、教育機関における感情認識システム。**
  - 顔認識データベース作成のためのインターネットや監視カメラ映像からの**生体データの無差別収集**

ハイリスクAI①（第6条、AnnexII及びIII）

1. 以下の条件の**両方を満たす**AIシステム。
（1）AIシステムが、**Annex IIに記載されている法令の対象となっている製品の安全部品**として使用されることを意図しているか、またはそれ自体が製品であること。
（2）AIシステムを安全部品とする製品又は製品としてのAIシステム自体が、**Annex IIに掲げる法令に基づく第三者による適合性評価義務の対象**であること。

2. **Annex III**に記載されているAIシステム。

理事会修正案

- Annex IIIに記載されているAIシステムは、**システムのアウトプットが、関連する行動又は決定に関して純粋に付随的なものであり、したがって、健康、安全又は基本的権利に対する重大なリスクにつながる可能性がない場合を除き**、ハイリスクとみなされる。
- 欧州委員会は、どのような状況が「付随的」かを規定する実施法令を採択する

議会修正案

- Annex IIIで言及されているユースケースに該当するAIシステムは、**自然人の健康、安全又は基本的権利に重大な危害を及ぼすリスクがある場合、ハイリスクとみなされる**。
- Annex IIIの「重要インフラ」に該当する場合、**環境に重大な危害を及ぼすリスクがあるときは、ハイリスクとみなされる**。
- 欧州委員会は、どのような状況が「重大な危害を及ぼすリスクがある場合」かを規定するガイドラインを提供する。
- Annex IIIで言及されているユースケースに該当する**プロバイダーは、AIシステムが上記の重大なリスクをもたらすものではないと考える場合**、本規則が定める要件の対象とならない旨の**理由付き通知を監督当局に提出**しなければならない。
- 監督当局は、通知をレビューし、AIシステムが誤って分類されていると判断した場合、3ヶ月以内に回答しなければならない。

ハイリスクAI② （第6条、AnnexII及びIII）

Annex IIA

1. 機械指令（Directive 2006/42/EC）
2. 玩具の安全性指令（Directive 2009/48/EC）
3. レジャー用・個人用船舶指令（Directive 2013/53/EU）
4. エレベーター及びその部品に関する指令（Directive 2014/33/EU）
5. 爆発性環境下での保護システムに関する指令（Directive 2014/34/EU）
6. 無線機器指令（Directive 2014/53/EU）
7. 圧力機器指令（Directive 2014/68/EU）
8. ロープウェイ設備規則（Regulation （EU） 2016/424）
9. 個人用保護器具規則（Regulation （EU） 2016/425）
10. ガス燃料機器規則（Regulation （EU） 2016/426）
11. 医療機器規則（Regulation （EU） 2017/745）
12. 体外診断用医療機器規則（Regulation （EU） 2017/746）

※Annex IIBは、第84条（見直し規定）のみが適用される製品に関する法令を列挙（P3参照）。

ハイリスクAI③（第6条、AnnexII及びIII）

Annex III

1. 生体認証・分類

リアルタイム及び事後の遠隔生体認証用AIシステム

2. 重要インフラの管理・運営

道路交通の管理・運営及び水・ガス・暖房・電気の供給における安全部品用AIシステム

理事会修正案 ■ 「重要デジタルインフラ」を追加。

3. 教育・職業訓練

（1）教育機関及び職業訓練機関へのアクセス又は割当て決定、（2）学生の評価・入試評価

4. 雇用、労働者管理及び自営業へのアクセス

（1）採用・選考、（2）昇進、雇用関係の終了、タスク割り当て、パフォーマンス評価

5. 必須の民間・公共サービスへのアクセス

（1）公的支援給付及びサービスの適格性の評価、付与、減額、取消し又は再請求、（2）クレジットスコア、（3）緊急時初動対応サービスの派遣（消防士、医療等）

理事会修正案 ■ （4）「生命保険・健康保険における評価・価格決定」を追加。

6. 法執行（全て主体は法執行機関）

（1）個人の犯罪・再犯リスク評価、犯罪の潜在的被害者のリスク評価、（2）ポリグラフ、感情検出、（3）ディープフェイク検知、（4）証拠の信頼性評価、（5）プロファイリングや性格特性又は過去の犯罪行動の評価に基づく犯罪発生の予測、（6）犯罪捜査・訴追過程でのプロファイリング、（7）異なるデータソース又はデータフォーマットで入手できる複雑な大規模データセットを検索し、データ中の未知のパターンや隠れた関係性を発見することを可能にする犯罪分析用AIシステム。

理事会修正案 ■ （3）（7）を削除。

※欧州委員会が委任法令で**追加**可能。

理事会修正案
- 欧州委員会に委任法令で**削除**する権限を付与。

議会修正案
- 欧州委員会に委任法令で**修正・削除**する権限を付与。

ハイリスクAI④（第6条、AnnexII及びIII）

Annex III(続)

7. 移民、亡命、国境管理（全て主体は所管の公的機関）

（1）ポリグラフ、感情検出、（2）入国者の安全保障上のリスク、不正移民のリスク又は健康上のリスクなどの評価、（3）旅行書類及び補助書類の真正性の検証、（4）亡命、査証及び滞在許可申請の審査

理事会修正案 ■ （3）を削除。

8. 司法及び民主的プロセスの運営

司法当局による事実と法律の調査・解釈及び法律の適用の支援

ハイリスクAIシステムが満たすべき要件①（第8条～第15条）

要件	内容
リスク管理システム	■ **リスク管理システムの確立・実施・文書化・維持**。 ■ 以下のプロセス： ➢ **既知のリスク及び予見可能なリスクの特定及び分析** ➢ 本来の用途に従って使用され又は**合理的に予見可能な誤用が行われた際に出現し得るリスクの推定及び評価** ➢ 市販後モニタリングに基づくリスク評価 ➢ **適切なリスク管理措置の採用** ■ **リスク管理措置**：残留リスクは、本来の用途に従って又は合理的に予見可能な誤用の状況下で使用されることを条件に、許容可能と判断されるものでなければならない。以下を確保。**残留リスクは、利用者に要伝達**。 ➢ 適切な設計及び開発により、可能な限りリスクを排除又は低減 ➢ 排除できないリスクに関して、適切な緩和及び管理手段を実施 ➢ 適切な情報提供 ■ **テスト**：適切なリスク管理措置を特定するため、**開発中、遅くとも上市前にテストを実施。**
データガバナンス	**以下の品質基準を満たす**学習・検証・テスト用**データセットに基づいて開発**する。 ➢ 適切なデータガバナンス・管理プラクティスに服する。 ➢ **関連性があり、代表的で、誤りがなく、完全なもの**。 理事会修正案：**「可能な限り」**を追加。 議会修正案：「関連性があり、**十分に**代表的で、誤りがないか**適切に検証**され、本来の用途に照らして**可能な限り**完全なもの」。 ➢ ハイリスクAIシステムの使用が意図されている地理的、行動的、機能的設定に特有の特性又は要素を考慮する。

ハイリスクAIシステムが満たすべき要件② (第8条～第15条)

要件	内容
技術文書	Annex IV記載の要素を含む**技術文書を上市前に作成し、最新に維持**する。
記録保存	システム動作中の**自動ログ記録機能**を備える。
人的監視措置	■ **適切な人間・機械間インターフェース**を含め、AIシステムが使用されている期間中、人間が効果的に監督できるような方法で設計・開発。 ■ 人間による監視は、プロバイダーが特定した上で、自らAIシステムに組み込むか、利用者による実施に適した措置を通じて確保する。 ■ 人間による監視措置は、**監視業務要員が以下を行うことを可能にする**ものとする。 ➢ AIシステムの能力及び限界を十分に理解し、その動作を適切に監視し、**異常、機能不全及び予想外の性能の兆候をできるだけ早く検知して対処する** ➢ AIシステムによって生成されるアウトプットに自動的に依存し又は過度に依存する傾向(**「自動化バイアス」)の可能性について認識する** ➢ AIシステムの**アウトプットを正しく解釈する** ➢ 特定の状況において、**AIシステムを使用しないこと、又はAIシステムの出力を無視、上書き若しくは反転させる**ことを決定する ➢ AIシステムの動作に介入し、**「停止」ボタン**または同様の手順でシステムを中断する 議会修正案 ■ 監視業務要員は、**十分なレベルのAIリテラシー**と、AIシステムの使用中及び事故後の徹底的な調査を可能にするために**必要な支援及び権限**を有していなければならない。

ハイリスクAIシステムが満たすべき要件③（第8条～第15条）

要件	内容
透明性及び利用者への情報提供	■ 利用者がAIシステムの**アウトプットを解釈して適切に利用できるよう、透明性を確保**。 ■ 利用者に関連し、アクセス可能で理解可能な、**簡潔、完全、正確かつ明確な情報が含まれる使用説明書を添付**。具体的には以下の情報を含める。 ➢ **プロバイダーの身元及び連絡先** ➢ **AIシステムの特徴、能力及び性能の限界** ・本来の用途 ・正確性、堅牢性及びサイバーセキュリティのレベル ・健康及び安全又は基本的権利に対するリスクにつながる可能性がある状況 ・データセットに関する情報など ➢ 適合性評価時点からの性能の変更点 ➢ **人的監視措置** ➢ **想定寿命**及び適切な機能を確保するために必要な**保守・ケア措置**

ハイリスクAIシステムが満たすべき要件④（第8条～第15条）

要件	内容
正確性、堅牢性、サイバーセキュリティー	■ **適切なレベルの正確性、堅牢性、サイバーセキュリティを達成し、ライフサイクルを通じて一貫した性能を発揮する**ように設計・開発。 ■ AIシステムの**正確性レベル及び関連する指標は、添付の使用説明書に明記。** ■ 発生する可能性のあるエラー、障害又は不整合に関して強靭でなければならない。 ■ 堅牢性は、**バックアップ又はフェイルセーフプランを含む技術的な冗長性ソリューション**によって達成することができる。 ■ 上市後又はサービス提供開始後も学習を続けるAIシステムは、将来の運用のためのインプットとして使用されるアウトプットに起因する偏ったアウトプットの可能性（「**フィードバックループ**」）が、適切な緩和手段によって適切に対処されなければならない。 ■ システムの脆弱性を悪用してその使用や性能を変更しようとする第三者による試みに対して強靭でなければならない。 ■ AI特有の脆弱性に対処するための技術的解決策には、適切な場合、学習データセットを操作しようとする攻撃（「**データポイズニング**」）、モデルに誤りを犯させるように設計された入力（「**敵対的事例**」）、または**モデルの欠陥**を**防止し、制御するための対策を含まなければならない。** 議会修正案 ■ 「学習で使用される事前学習済みコンポーネントを操作しようとする攻撃（モデルポイズニング）」、「機密性攻撃」を追加。

ハイリスクAIシステムプロバイダーの義務（第16条～第25条、第48条～第51条、第62条）

1. ハイリスクAIシステムが**本法の要件（前ページまで参照）に準拠していることを確保**すること。
2. **品質管理システム**を策定・文書化すること。以下の内容を含める。
   - ・設計、設計管理、設計検証、開発、品質管理、品質保証に使用される技術、手順及び体系的措置
   - ・開発前、開発中、開発後に実施すべき審査、試験、検証手順、それらの実施頻度
   - ・適用される規格を含む技術仕様
   - ・データ管理のためのシステム及び手順
   - ・リスク管理システム
   - ・市販後モニタリングシステムの設定、実施及び維持
   - ・重大インシデント及び故障の報告に関する手順
   - ・当局、顧客その他の利害関係者とのコミュニケーションの取扱い
   - ・関連文書及び情報の記録保持のためのシステム及び手順
   - ・供給確保に関する措置を含む資源管理
   - ・各項目の管理者その他の職員の責任を定めた説明責任の枠組み

理事会修正案
- ■ 中小企業は適用除外。

議会修正案
- ■ 「インプットデータの仕様又はデータセットに関する関連情報を提供すること」を追加。

3. **技術文書を作成**すること。
4. 自己の管理下にある場合、自動的に生成する**ログを保管**すること。
   - ・保存期間は本来の用途と適用される法的義務に照らして適切な期間。
5. 上市前に関連する**適合性評価手続を受ける**こと。
6. **市販後モニタリングシステム**の確立・文書化。
7. **EUデータベースへの登録**。
8. ハイリスクAIシステムが本法の要件に適合していない場合、**必要な是正措置（リコール含む）を講じる**こと。
9. **法令違反となるインシデント、要件の不適合及び講じた是正措置について当局に通知する**こと。
10. **EU適合性宣言の作成**及び**CEマークの貼付**。
11. **当局への協力：**要請があった場合、**ログへのアクセス提供、本法の要件遵守の証明等**。
12. EU域外プロバイダー：**EU域内代理人を設置**すること。

ハイリスクAIシステムの適合性評価手続（第40条～第44条）

【前提】
- 本法が定める要件をカバーする**欧州標準に適合しているハイリスクAIシステムは、本法が定める要件に適合していると推定**される。
- 欧州標準の不存在等の場合、欧州委員会は共通仕様を策定可能。本法が定める要件をカバーする**共通仕様に適合しているハイリスクAIシステムは、本法が定める要件に適合していると推定**される。

対象AIシステム	適合性評価手続
リアルタイム及び事後の遠隔生体認証用AIシステム	■ 欧州標準又は共通仕様を**適用している**場合　→　以下の**いずれか**。 ・Annex VIに基づく**自己評価**：品質管理システム、技術文書、設計開発プロセスや市販後モニタリングの検証 ・Annex VIIに基づく**第三者認証**：品質管理システム、技術文書、認証団体による監視 ■ 欧州標準も共通仕様も**適用していない**場合　→　Annex VIIに基づく**第三者認証**。
Annex IIA（他の法令の対象）	■ **当該他の法令の規定に従って実施**
その他	■ Annex VIに基づく**自己評価**　理事会修正案　■ 汎用AIシステム含む。 **※欧州委員会が委任法令で第三者認証必須に変更することが可能。**

※ハイリスクAIシステムが**大幅に変更された場合は、新たな適合性評価手続の実施**が必要。
※上市後も学習を続けるハイリスクAIシステムについて、最初の適合性評価の時点でプロバイダーが事前に決定していた変更で、技術文書に含まれるものは、「大幅な変更」とはならない。（＝**これ以外の場合は、学習の結果大幅な変更があった場合も、新たな適合性評価手続の実施が必要**。）
※適合証明書の**有効期間は最長5年**。更新には適合性評価手続と同様の再査定が必要。

市販後モニタリングシステム（第61条）

- ハイリスクAIシステムの性能について、その耐用期間を通じて、**利用者から提供された又は他の情報源を通じて収集された関連データを積極的かつ体系的に収集、文書化、分析**する。
- プロバイダーが、**AIシステムが本法の定める要件に継続的に適合していることを評価**するためのもの。

＜関連規定＞

- 市販後モニタリングシステムは、**市販後モニタリング計画**に基づいて実施。市販後モニタリング計画は、**技術文書の一部**を構成。
- **欧州委員会は、市販後モニタリング計画のテンプレート及び盛り込まれるべき要素を定める実施法令を策定**。
- Annex IIAのハイリスクAIシステム（他の法令の対象）で、当該他の法令に基づき既に市販後モニタリングシステム・市販後モニタリング計画が策定済みのものについては、当該システム・計画に統合する。

ハイリスクAIシステム輸入者及び販売業者の義務(第26条～第28条)

輸入者の義務

1. ハイリスクAIシステムを市場に投入する前に、**以下を確認しなければならない**。
   ・プロバイダーが適切な**適合性評価手続**を実施していること。
   ・プロバイダーが**技術文書**を作成していること。
   ・**適合性表示**が付され、**必要文書及び使用説明書**が添付されていること。
2. ハイリスクAIシステムが**本規則に適合していないと考える場合、当該システムを市場に出してはならない**。
3. **輸入者の名称、登録商号又は登録商標及び連絡可能な住所**を表示しなければならない。

理事会修正案

■ 適合証明書、使用説明書及びEU適合性宣言の**コピーの上市後10年間保存義務**を追加。

販売業者の義務

1. ハイリスクAIシステムを市販する前に、**以下を確認しなければならない**。
   ・**CEマーク**が付されていること。
   ・**必要文書及び使用説明書**が添付されていること。
   ・**プロバイダー及び輸入者が本法に定める義務を遵守している**こと。
2. ハイリスクAIシステムが**本法が定める要件を満たしていないと考える場合、当該システムを市販してはならない**。
3. 市販したハイリスクAI システムが本法が定める要件を満たしていないと考える販売業者は、**必要な是正措置を講じ、撤回し、若しくはリコールし、又は、プロバイダー、輸入者若しくは関係事業者が当該是正措置を講じることを確保しなければならない。**

※輸入者、販売業者、利用者、その他関係者であっても、①ハイリスクAIシステムを**自己の名称又は商標で市場に投入する場合**、②ハイリスクAIシステムの**本来の使用目的を変更する場合**、③ハイリスクAIシステムに**大幅な変更を加える場合**、**「プロバイダー」とみなされる**。

ハイリスクAIシステム利用者の義務(第29条)

1. 使用説明書に従って使用すること。
2. インプットデータとハイリスクAIシステムの本来の用途との関連性を確保すること。
3. ハイリスクAIシステムの動作を監視すること。

理事会修正案
議会修正案

■ 必要な能力、訓練及び権限を有する者にアサインして人的監視を行う義務を追加。

4. AIシステムが健康、安全又は基本的人権に関するリスクをもたらす可能性があると考える理由がある場合、プロバイダー又は販売業者に通知し、システムの使用を停止すること。
5. 重大な事故又は故障を発見した場合には、その旨をプロバイダー又は販売業者に通知し、AIシステムの使用を中断すること。
6. 自動的に生成するログを保管すること。
   ・保存期間は意図されている使用目的と適用される法的義務に照らして適切な期間。

理事会修正案
議会修正案

■ 保存期間は少なくとも6ヶ月間とする規定を追加。

議会修正案

■ 職場でハイリスクAIシステムを使用する前に、利用者は、合意に達することを目的として労働者代表と協議するとともに、影響を受ける従業員にハイリスクAIシステムの対象となることを通知しなければならない。

基本的権利影響評価

議会修正案(第29条a)

- **AnnexIIIのハイリスクAIシステム(重要インフラ分野を除く)の利用者**は、利用開始前に、特定の使用状況における当該システムの**影響を評価しなければならない。この評価には、最低限、以下の要素を含める。**
  a. AIシステムの本来の用途の明確な概要
  b. AIシステムの利用が意図される地理的及び時間的範囲の明確な概要
  c. AIシステムの利用によって**影響を受ける可能性のある自然人及び集団のカテゴリー**
  d. AIシステムの利用が**基本的権利に関する関連するEU法・加盟国法に準拠していることの検証**
  e. AIシステムの利用による、**基本的権利に対する合理的に予見可能な影響**
  f. **社会から疎外された人々又は脆弱な集団**に影響を及ぼす可能性のある具体的な危害のリスク
  g. AIシステムの利用が**環境に及ぼす合理的に予見可能な悪影響**
  h. 特定された基本的権利に対する**危害と悪影響を軽減する方法についての詳細な計画**
  i. 利用者が導入する**ガバナンスシステム**(人的監視、苦情処理、救済措置を含む)
- 影響評価の過程で概説された**リスクを軽減するための詳細な計画が特定できない場合、**利用者は、ハイリスクAIシステムの**使用を差し控え、プロバイダー及び当局に遅滞なく通知**しなければならない。
- 影響評価は、ハイリスクAIシステムの最初の使用に適用される。使用中に上記基準を満たさなくなったと考える場合、利用者は新たな基本的権利影響評価を実施しなければならない。
- 影響評価の過程において、利用者(中小企業を除く)は、可能な限り、平等団体、消費者保護機関、社会的パートナー及びデータ保護機関を含む、ハイリスクAIシステムによって**影響を受ける可能性のある者又はそのグループの代表者を関与させなければならない。**各機関が回答するために**6週間の期間**を与えなければならない。

透明性義務 （限定的なリスク）（第52条）

1. **自然人とやり取りするAIシステム**
   → プロバイダーは、**自然人がAIシステムとやり取りしていることを認識できるように設計・開発する**こと。状況や使用の文脈から明らかな場合を除く。

議会修正案

■ 提供される情報には、どの機能がAIで実現されているか、人的監視があるか、意思決定プロセスの責任者は誰か、また、自然人が当該AIシステムの適用に反対し、AIシステムによって下された決定又はAIシステムによって引き起こされた損害に対して司法的救済を求めることができる既存の権利およびプロセスも含むものとする。

2. **感情認識システム・生体分類システム**
   → **利用者**は、**対象者にそのシステムの運用について通知する**こと。

3. **ディープフェイク生成AIシステム**
   →**利用者**は、**コンテンツが人為的に生成又は操作されたものであることを開示する**こと。ただし、表現の自由及び芸術・科学の自由の権利の行使のために必要であり、かつ第三者の権利と自由のための適切な保護措置が講じられている場合を除く。

※ディープフェイクの定義：既存の人物、物体、場所、その他の実体または事象に著しく類似し、真正または真実であるかのように人に見せかける画像、音声または映像コンテンツ

議会修正案

■ 可能な場合、当該**コンテンツを生成又は操作した個人・法人の名称**を開示する。

理事会修正案　議会修正案

■ 情報提供は、**遅くとも最初のやり取り又は接触の時点で**、明確かつ識別可能な方法で行われなければならない。

汎用AIシステム

理事会修正案(第4条a～c)

汎用AIシステム(general purpose AI system)とは

- **画像・音声認識、音声・映像生成、パターン検出、質問応答、翻訳などの一般的に適用可能な機能**を実行することをプロバイダーが意図したAIシステム。
- **オープンソースソフトウェアを含め**、どのような形で市場に投入され、あるいはサービスに供されるかを問わない。複数の文脈で使用され、複数の**他のAIシステムに統合される**ことがある。

分類	要件・義務　※中小企業は適用除外。
プロバイダーが使用説明書又は付随情報において、全てのハイリスク用途を明確に排除している場合	■ **下記要件・義務は適用されない。** ■ ただし、この「排除」は、**プロバイダーがシステムが悪用する可能性があると考える十分な理由がある場合には、正当化されない。** ■ プロバイダーは、**不正使用を発見した場合又は不正使用について通報を受けた場合、更なる不正使用を防止するために必要かつ適切なあらゆる措置を講じなければならない。**
汎用AIシステム	■ プロバイダーは、そのシステムをハイリスクAIシステム又はそのコンポーネントとしてEU市場に投入しようとする**他のプロバイダーが本法に基づく義務を遵守できるよう、当該プロバイダーと協力し、必要な情報を提供しなければならない。**共有すべき情報に関して、欧州委員会は、実施法令を採択できる。
ハイリスクAIシステム又はそのコンポーネントとして使用される可能性のある汎用AIシステム	■ 本規則の発効後18ヶ月以内に、欧州委員会は、**本法が定めるハイリスクAIシステムが満たすべき要件を汎用AIシステムへ適応させるための実施法令を採択**する。汎用AIシステムは、**この実施法の適用日から、本法が定めるハイリスクAIシステムが満たすべき要件に適合**しなければならない。 ■ **プロバイダーの義務**:①名称・住所等のAIシステム又は添付文書への記載、②技術文書の作成・保管、③適合性評価(自主点検)、④登録義務、⑤不適合時の是正措置、⑥CEマーク貼付、⑦当局の要請に応じて要件適合の証明、⑧EU域内代理人の設置、⑨EU適合性宣言、⑩市販後モニタリング ■ 各条文中「本来の用途」(intended purpose)については、汎用AIシステムに対しては「潜在的用途」(possible use)と読み替える。

基盤モデル

議会修正案(第28条b)

基盤モデル(foundation model)とは

- **大規模なデータで訓練され、アウトプットの汎用性を考慮して設計され、幅広い異なるタスクに適応可能なAIシステムモデル**。
- スタンドアロンモデルとして提供されるか、AIシステムに組み込まれるか、無料のオープンソースライセンスの下で提供されるか、その他の流通経路で提供されるかを問わない。

＜基盤モデルプロバイダーの義務＞

- 適切な設計、試験、分析を通じて、健康、安全、基本的権利、環境、民主主義、法の支配に対する**合理的に予見可能なリスクを、開発前及び開発期間中に特定し、軽減すること**。また、**開発後に残る軽減不可能なリスクを文書化すること**。
- **適切なデータガバナンス措置**、特にデータソースの適切性、起こりえるバイアス、適切な軽減策を検討する措置**の対象となるデータセットのみを処理し、組み込む**こと。
- **性能、予測可能性、解釈可能性、適格性、安全性及びサイバーセキュリティの適切なレベル**を、そのライフサイクル全体を通じて達成するよう、基盤モデルを設計・開発すること。
- **エネルギー使用、資源使用及び廃棄物を削減し、エネルギー効率及びシステム全体の効率を向上させる**よう、基盤モデルを設計及び開発すること。
- 基盤モデルは、エネルギー及び資源の消費の測定及び記録、その他の環境への影響の測定を可能にする機能をもって設計されなければならない。
- **川下のプロバイダーが義務を遵守できるよう、詳細な技術文書及びわかりやすい使用説明書を作成すること**。
- **品質管理システム**を確立すること。
- **EUデータベースに基盤モデルを登録する**こと。

生成AI

議会修正案(第28条b)

生成AI(generative AI)とは

■ **複雑なテキスト、画像、音声、動画などのコンテンツを、様々なレベルの自律性をもって生成することを特に意図したAIシステムに使われる基盤モデル。**

＜生成AIプロバイダーの追加義務＞

- 「限定的なリスク」向けの**透明性義務を遵守すること**と(＝自然人がAIシステムとやり取りしていることを認識できるように設計・開発すること)。
- 表現の自由を含む基本的権利を損なうことなく、**EU法に違反するコンテンツの生成に対する適切なセーフガードを確保するような方法で、基礎モデルを学習させ、設計し、開発する**こと。
- **著作権法に基づいて保護される学習データの使用に関する十分に詳細な概要を文書化し、一般に公開する**こと。

AI規制サンドボックス（第53条～第55条）

AI規制サンドボックスとは

- AIシステムの市場投入・サービス提供開始前の限られた期間、革新的なAIシステムの**開発、試験、検証を手助けする管理された環境を提供する**もの。
- EU加盟国の当局又は欧州データ保護監督機関（EDPS）により設置。
- サンドボックス内では、法定の条件を満たせば、**他の利用目的のために収集した個人データを、革新的なAIシステム開発・試験目的に利用可能**。

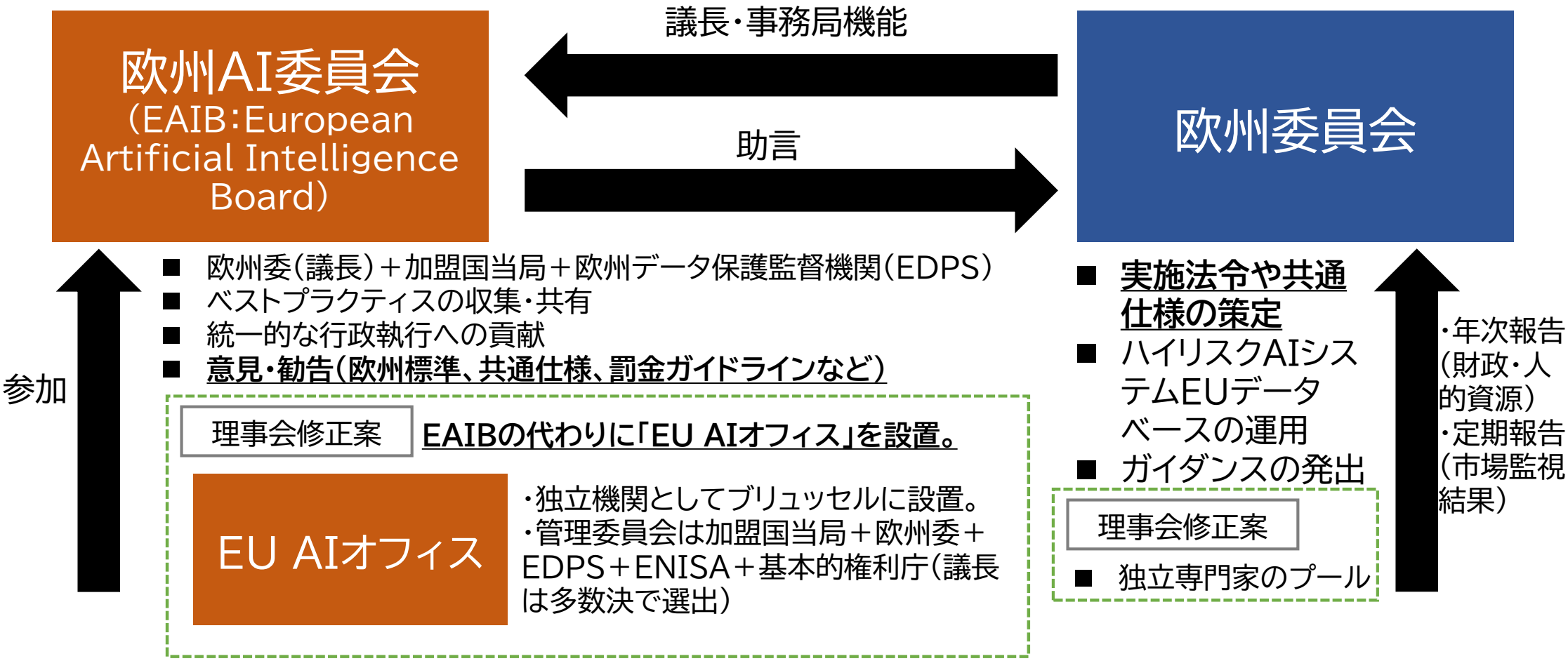
＜関連規定＞

- 当局による直接的な監督および指導の下で実施。AIシステムが他の当局の監督権限に関わる場合、当該**他の当局（例：データ保護機関）の関与を確保**する。
- システムの開発及び試験中に特定された、健康、安全、基本的権利に対する重大なリスクは、直ちに緩和策を講じる。できない場合は、緩和策が講じられるまで開発及び試験プロセスを一時停止する。
- 参加者は、サンドボックス内で行われた実験の結果、**第三者に与えた損害について責任を負う**。
- **申請・選考・参加・脱退の資格基準及び手続**を含むAI規制サンドボックスの運営方法・条件、参加者の権利・義務は、**実施法令で定める**。
- **中小企業に**AI規制サンドボックスへの**優先アクセス**を与える。

理事会修正案

- 参加者が、サンドボックス計画及び参加条件を尊重し、かつ、当局の指導に誠実に従うことを条件として，本規則を含むEU又は加盟国の**法令に違反した場合でも、当局は制裁金を課さない**ものとする。
- 当局は、サンドボックス内で成功裏に実施された**活動の書面による証明**と、サンドボックスで実施された活動、結果及び学習成果を詳述した**終了報告書**を提供しなければならない。これらは、適合性評価手続又は市場活動の中で考慮されることがある。
- **AI規制サンドボックス「以外」での現実環境での試験**に関する規定を追加。

ガバナンス（第56条～第59条）



EU加盟国当局
（対EU機関の当局はEDPS）

- **本法の適用・執行**
- 適合性証明機関の指定
- 市場監視当局としての機能
- ガイダンスの発出

執行（第63条及び第64条）

市場監視

- 市場監視規則（Regulation（EU）2019/1020）をAIシステムにも適用。
  ・EU域内代理人の設置義務、市場監視当局への協力義務等。
  ・市場監視当局へ資料・情報提出命令、立入検査、是正措置命令（リコール含む）等の権限を付与。

当局によるアクセス

- 市場監視当局は、API等を通じて、プロバイダーが使用する学習、検証及び試験の**データセットへの完全なアクセス**を認められる。
- ハイリスクAIシステムの本法が定める要件への適合性を評価するために必要であり、合理的な要請があれば、市場監視当局は、当該システムの**ソースコードへのアクセス**を認められる。

罰則(第71条)

- **利用禁止AI**又は**データガバナンス**規定への違反:**3000万ユーロ又は全世界年間売上高の6%のいずれか高い方が上限。**

  理事会修正案 ■ **中小企業の場合は3%が上限。**

- **その他の**規定への違反:**2000万ユーロ又は全世界年間売上高の4%のいずれか高い方が上限。**

  理事会修正案 ■ **汎用AIシステム含む。** ■ **中小企業の場合は2%が上限。**

- 当局又は適合性認証機関への**不正確、不完全又はミスリーディングな情報の提供**:**1000万ユーロ又は全世界年間売上高の2%のいずれか高い方が上限。**

  理事会修正案 ■ **中小企業の場合は1%が上限。**

議会修正案

- **利用禁止AI**規定への違反:**4000万ユーロ又は7%が上限。**
- **データガバナンス規定**又は**利用者への情報提供義務**への違反:**2000万ユーロ又は全世界年間売上高の4%のいずれか高い方が上限。**
- **その他**の規定への違反(**基盤モデル含む**):**1000万ユーロ又は全世界年間売上高の2%のいずれか高い方が上限。**
- 当局又は適合性認証機関への**不正確、不完全又はミスリーディングな情報の提供**:**500万ユーロ又は全世界年間売上高の1%のいずれか高い方が上限。**

行動規範（第69条）

行動規範（Code of Conduct）

- 欧州委員会及び加盟国は、システムの本来の用途に照らして、本法が定める**ハイリスクAIシステムの要件のそれ以外のAIシステムへの自発的な適用を促進することを目的とした行動規範の作成**を奨励し、促進する。
- 欧州委員会及びEAIBは、例えば、**環境の持続可能性**、**障害者のためのアクセシビリティ**、AIシステムの設計及び開発への利害関係者の参加、**開発チームの多様性**に関連する要求事項のAIシステムへの自発的な適用を促進することを意図した行動規範の作成を奨励し、促進する。
- AIシステムの個々のプロバイダー又はそれらを代表する組織によって作成される。行動規範は、関連するシステムの本来の用途の類似性を考慮して、1つ又は複数のAIシステムを対象とすることができる。