基礎研レポート

EU の AI 規則(2/4)

―高リスク AI システム

保険研究部 専務取締役 研究理事　松澤　登
(03)3512-1866　matuzawa@nli-research.co.jp

1――はじめに

前回(1 回目)のレポートで述べた通り、EU の AI 規則（以下、本規則）は、2024 年 6 月 13 日に EU ジャーナル（日本の官報に相当）に掲載され、同年 8 月 1 日に発効した。本シリーズでは本規則の内容を解説することを目的とする。4 回中、2 回目の本稿では高リスク AI システムについて解説を行う。全体の中の位置づけとしては下記図表 1 の色付き部分である。

【図表 1】本稿で取り扱う部分(色付き部分)

総論・定義	適用範囲や定義
禁止されるAIの行為	許容できないリスクをもつAI
高リスクAIシステム	許容される高リスクAIシステムの果たすべき要件
適合性審査	EUの基準に合致しているか審査
透明義務・汎用AIモデル	汎用AIモデルのシステミック・リスクの防止
イノベーション支援	AIの革新を推進
EU及び域内国のガバナンス	AIシステムに係るEUレベルのガバナンス
市販後モニタリング	市場投入後の監視・是正
法律の執行・罰則	行動規範の作成・違反行為に対する罰則

2――前回レポートの振り返り

ここでは本稿から読まれる方のために、簡単に前回レポートの振り返りを行っておきたい。内容を単純化してお示しするので、正確には前回レポートを参照願いたい。

前回レポートでは各種定義、適用範囲、禁止される AI の行為等を解説した。

まず定義としては、AI システムは入力から推論して出力を行う機械のシステムとされていた。適用対象になるのは、主には AI システムを EU 域内に市場投入するか又は稼働させる提供者と、EU 域内で

事業上AIシステムを利用する配備者である。

前回レポートの重点は禁止されるAIの行為であった。これには、人の意識や感情に干渉するシステム（サブリミナル技術を使用するシステムなど）や、人を監視し、分類するシステム（生体データを無差別収集するシステムなど）があった。これらはAIシステムの及ぼす悪影響のリスクが高すぎると判断され、EU域内での使用が禁止されている。また、禁止違反には罰金が科される。

3――高リスクAIシステムとは

1｜高リスクAIシステムとは（その1）

AIシステムが以下の(a)と（b）のいずれも満たすときに、そのAIシステムは高リスクとみなされる（6条1項。図表2）。

【図表2】高リスクとみなされる要件

(a)AIシステムが製品の安全のための部品として使用されることを意図している場合、またはAIシステム自体が製品であり、付属書Ⅰに記載されているEU調和法[1]の適用を受ける場合、かつ、
(b)(a)に従った安全のための部品がAIシステムである製品、又は製品としてのAIシステム自体が、付属書Ⅰに列挙されたEU調和法に従って、その製品の市場投入又は使用開始を目的とした第三者適合性評価を受ける必要がある場合。

ここで触れられている付属書Ⅰには機械に関する欧州指令（Directive）、玩具の安全性に関する欧州指令などが列挙されている（図表3、図表4）。

【図表3】付属書Ⅰのセクション A

機械に関する指令
玩具の安全性に関する指令
レクリエーション・個人向け船舶に関する指令
リフト及びリフト用安全部品に関する指令
潜在的に爆発力のある気体向けの用具及び防御システムに関する指令
無線機器の市販に関する指令
圧力機器の市販に関する指令
策動設備に関する規則および指令（指令は廃止予定）
個人用保護具に関する規則および指令（指令は廃止予定）
ガス燃料を燃焼する機器に関する規則および指令（指令は廃止予定）
医療機器に関する規則および指令（指令は廃止予定）
体外診断用医療機器における規則および指令（指令は廃止予定）

[1] EUで製品を流通させるにあたり、特定分野の製品が満たすべき要件を調和（ハーモナイゼーション）させることとしているEU指令や規則（Union harmonization legislation）のことを指す（EU整合化法令と訳されることもある）。

【図表 4】付属書Ⅰのセクション B

民間航空安全分野における規則
二輪車、三輪車、四輪車の認可と市場監視に関する規則
農業・林業用車両の承認と市場監視に関する規則
船舶機器に関する指令
鉄道システムの相互運用性に関する指令
自動車及びトレーラー、自動車を対象とするシステム、部品及び個別技術ユニットの承認及び市場監視に関する規則
自動車及びトレーラー、自動車を対象とするシステム、部品及び個別技術ユニットの安全性および車両乗員・交通弱者の保護に関する型式承認要件に関する規則
民間航空分野における共通規則および欧州連合航空安全機関の設立に関する規則

（注記）本条文は EU 調和法（図表 3、4 に掲げるものに限る）の適用を受ける製品またはその安全装置であって、かつ適合性評価を受ける必要のある製品等を高リスク AI システムと分類することを定めた条文である。前文では「高リスク AI システムは、一定の必須要件に適合する場合にのみ、域内市場に投入され、使用されるべきである。これらの要件は、域内で利用可能な、あるいは域内で利用される高リスクの AI システムが、域内法で認識され保護されている域内の重要な公共の利益に対して許容できないリスクをもたらさないことを保証するものでなければならない」（前文 46）とする。

ここで、高リスクかどうかは「憲章が保護する基本的権利に AI システムが与える悪影響の程度が特に重要となる。これらの権利には、人間の尊厳、私生活と家族生活の尊重、個人情報の保護、表現と情報の自由、集会と結社の自由、差別のない権利、教育を受ける権利、消費者保護、労働者の権利、障害者の権利、男女平等、知的財産権、効果的な救済と公正な裁判を受ける権利、防御と無罪推定の権利、善良な管理者の権利などが含まれる」（前文 48）を考慮するものとする。

前回レポートで述べた通り、AI システムのうち禁止されるものがある。他方、高リスク AI システムとは、リスクはありながらも、何らかの措置を加えることなどにより、リスクの発生を十分に抑制するか、リスクが発生しても社会的に許容できるリスクにとどめることができるものが該当すると位置づけられる。

2｜高リスク AI システムとは（その 2）

付属書Ⅲ（図表 5）に記載されている AI システムは高リスクとみなされる（6 条 2 項）。ここで付属書Ⅲには自然人の健康、安全または基本的権利に重大な危害を及ぼすリスクがある AI システム（＝これには生体識別や教育、職業訓練、雇用、必須の民間・公共サービスへのアクセス、法執行、移民・亡命・国境管理、私法及び民間プロセスの運営などが含まれる）および重要インフラに該当する場合や環境に重大な危害を及ぼす AI システムが記載されている。

ただし、付属書Ⅲに言及される AI システムであっても、意思決定の結果に重大な影響を与えないことを含め、自然人の健康、安全又は基本的権利に危害を及ぼす重大なリスクをもたらさない場合には、高リスクとはみなされないものとする（同条 3 項）。なお、AI システムが自然人のプロファイリング

を行う場合には、常に高リスクであるとみなされる（同条3項但書）。

そして、付属書Ⅲで言及されるAIシステムが高リスクではないと考える提供者は、当該システムが市場投入され、又は使用開始される前に、その評価を文書化しなければならない。このような提供者は、49条2項(3回目のレポートで解説予定)に定める登録義務の対象となる。欧州委員会は付属書Ⅲの修正権限を有する(7条)。

（注記）前文では「本規則であらかじめ規定された領域で言及されているAIシステムが、意思決定に重大な影響を与えないか、またはそれらの利益を実質的に害しないため、それらの領域で保護される法益を害する重大なリスクにつながらない特定の場合があり得ることを明確にすることも重要である。本規則において、意思決定の結果に実質的な影響を与えないAIシステムとは、人為的か自動的かを問わず、意思決定の実質、ひいては結果に影響を与えないAIシステムと理解すべきである」（前文53）とある。すなわち、付属書Ⅲに記載されているAIシステムは、人の意思決定やその結果に重大な影響を及ぼす可能性があるものとの認識のもとで、高リスクであるとみなされる。したがって意思決定やその結果に重大な影響をもたらさないものと提供者が判断しうるものであれば、登録を条件として高リスクAIシステムから除外されているものと考えられる。

【図表5】付属書Ⅲ（高リスクAIシステム）

1.生体に関するもの。
- a)遠隔生体識別システム（本人確認のためのものを含まない）
- b)生体のカテゴライズのために用いられるAIシステム
- c)感情認識を目的としたAIシステム

2.重要なインフラにかかわるAIシステム。重要なデジタルインフラ、道路交通、水道、ガス、暖房、電気の供給の管理運営にかかわる安全部品としてのAIシステム

3.教育と職業訓練にかかわるもの。
- a)教育と職業訓練施設のどこに入学させ、割り当てるかを決めるAIシステム
- b)学習結果を表化するためのAIシステム
- c)個人の適切な学習レベルを評価するためのAIシステム
- d)生徒の行動を監視し、禁止行為を検知するためのAIシステム

4.雇用、労働者管理及び自営業の自己評価にかかわるもの。
- a)採用や自然人の選考のためのAIシステム
- b)仕事に関連する条件、昇進や解雇に影響を与えるAIシステム

5.必須な民間サービスおよび公的サービスや給付を受けるためのアクセスにかかわるもの。
- a)公的機関が、または公的機関のために必須の公的支援給付のために自然人の適格性を評価するためのAIシステム
- b)自然人の信用度や信用スコアを評価するためのAIシステム
- c)生命保険・医療保険において自然人の健康評価と保険料決定のためのAIシステム
- d)自然人からの緊急要請に対して警察・消防者・救急車の派遣の優先順位を評価し順位付けするAIシステム

6.法の執行にかかわるもの
a)法執行機関が、または法執行機関のために、自然人が犯罪被害者になるリスクを評価するAIシステム
b)法執行機関が、または法執行機関のためにうそ発見器として利用されるAIシステム
c)法執行機関が、または法執行機関のために犯罪捜査または提訴のために証拠の確からしさを評価するためのAIシステム
d)法執行機関が、または法執行機関のために自然人のリスクをプロファイリングだけでなく評価すること、または個人的特徴、性格、過去の犯罪行為によって個人または集団を評価するAIシステム
e)法執行機関が、または法執行機関のために犯罪検知、捜査、訴訟のために自然人をプロファイリングするAIシステム
7.移民、難民保護および国境管理に関するもの
a)主管官庁が、または主管官庁のためにうそ発見器として使われるAIシステム
b)主管官庁が、または主管官庁のために使われる、域内国に入国した自然人の安全リスク、不正規移民、健康リスクといったリスクを評価するAIシステム
c)主管官庁が、または主管官庁のために難民申請、ビザ、居住許可を検査することを助けるため、あるいは居住資格にかかわる苦情処理を支援するためのAIシステム
d)主管官庁が、または主管官庁のために移民、難民保護又は国境管理を目的として自然人を検知し、認識し、特定するためのAIシステム
8.司法行政と民主的プロセスに関するもの
a)司法当局あるいは仲裁機関が事実及び法律の調査や解釈、事実の法律への適用において司法当局等を支援するためのAIシステム
b)選挙や国民投票の結果、または選挙や国民投票における自然人の投票行動に影響を与えるためのAIシステム

4――高リスクAIシステムが満たすべき要件

1｜高リスクAIシステムが満たすべき要件(総論)

高リスクAIシステムは、その意図される目的、及びAI及びAI関連技術に関する一般的に認知された技術状況を考慮し、Ⅲ章2節(8条～15条)に定める要件に準拠しなければならない(8条1項。図表6)。

【図表6】高リスクAIシステムが満たすべき要件

リスク管理システム及びリスク管理措置―8条、9条
データガバナンス―10条
技術文書および記録保存－11条、12条
使用説明書－13条

人的監視措置－14 条
正確性および堅牢性など―15 条

（注記）前文には「市場に投入され、または運用が開始された高リスクの AI システムから生じるリスクを軽減し、高水準の信頼性を確保するために、AI システムの意図された目的および使用状況を考慮し、かつ提供者が確立するリスク管理システムに従って、高リスクの AI システムに一定の義務的要件が適用されるべきである」（前文 64）とある。ここで課される義務としては図表 6 の通りである。

2｜高リスク AI システムが満たすべき要件（その 1:リスク管理システム）

(1) リスク管理システム：高リスクの AI システムに関しては、リスク管理システムを確立し、実施し、文書化し、維持しなければならない（9 条 1 項）。
（注記）次項の注記を参照。

(2) リスク管理システムとして、具体的には、以下（図表 7）を行わなければならない（同条 2 項）。

【図表 7】リスク管理システム

(a) 高リスク AI システムが健康、安全又は基本的権利にもたらす可能性のある既知のリスク及び合理的に予見可能なリスクを特定し、分析すること
(b) 高リスク AI システムがその意図された目的に沿って使用され、合理的に予見可能な誤用が行われる状況下で使用された場合に出現する可能性のあるリスクの見積もりと評価をすること
(c) 市販後モニタリングシステム（72 条。次々回レポートで解説）から収集されたデータの分析に基づき、発生する可能性のあるその他のリスクを評価すること、および、
(d) リスクに対処するために設計された、適切かつ的を絞ったリスク管理措置を採用すること

（注記）前文では「リスク管理システムは、高リスク AI システムのライフサイクル全体を通じて計画・実行される、継続的かつ反復的なプロセスで構成されるべきである」とし、さらに「このプロセスは、提供者がリスク又は悪影響を特定し、健康、安全及び基本的権利に対する AI システムの既知のリスク及び合理的に予見可能なリスクについて、その意図された目的及び合理的に予見可能な誤用に照らして、AI システムとそれが運用される環境との相互作用から生じる可能性のあるリスクを含め、緩和措置を実施することを確保するものでなければならない」（前文 65）とする。

AI システムから排除しきれないリスクが存在する以上、このリスクの発生の頻度を最小限に抑え、かつ万一発生した場合にそれを直ちに特定し、そして悪影響を最小化する必要がある。この条文が規定するのは AI システムを社会に実装する以上、避けられない問題に対処するものである。

(3) リスク管理措置の要求事項：上記 9 条 2 項(d) に言及するリスク管理措置は、各ハザードに関連する残余リスク、及び高リスク AI システムの全体的な残余リスクが許容可能であると判断されるものでなければならない。そして、最も適切なリスク管理策を特定するにあたっては、以下（図表 8）を確

保しなければならない（同条 5 項）。

【図表 8】リスク管理措置の要求事項

(a)高リスク AI システムの適切な設計および開発を通じて、技術的に可能な限り、2 項に従って特定および評価されたリスクを排除または低減すること
(b)適切な場合、排除できないリスクに対処する適切な緩和策と管理策の実施、および
(c)必要とされる情報の提供、および適切な場合には、配備者に対する訓練

（注記）本条は、リスク発生時においてもリスク管理措置によって抑止されないリスクが許容範囲内にとどまるようなリスク管理措置を設けるべきことを定める。また、配備者に対する訓練について、前文では「予見可能な誤用に対処するために、提供者が高リスク AI システムに対して特別な追加訓練を行うことを必要とすべきではない。しかし、提供者は、必要かつ適切な場合には、合理的な予見可能な誤用を軽減するための追加的な訓練措置を検討することが奨励される」（前文 65）とする。

(4) 高リスク AI システムにつき、最も適切で的を絞ったリスク管理措置の作動を確認する目的でテストを実施するものとする。テストは、高リスク AI システムが、その意図された目的に対して一貫して機能し、かつ、本項に定める要件に準拠していることを確認するもの（同条 6 項）である。
（注記）リスク管理措置が実際のリスク発生時に実効的に稼働するかどうかテストすることを求める項目である。テストについては次項参照。

3｜高リスク AI システムが満たすべき要件(その 2:データガバナンス)

データによる AI モデルの学習を行う高リスク AI システムは、学習用のデータセット[2]を使用する場合は、常に以下（図表 9）で言及される品質基準を満たす学習、検証、テストのデータセットに基づいて開発されなければならない(10 条 1 項)。

【図表 9】要求されるデータセット

(1)学習用、検証用及びテスト用のデータセットは、高リスク AI システムの意図された目的のために、適合するデータガバナンス及び管理実務に従うものとする（同条 2 項)。
(2)学習用、検証用及び試験用のデータセットは、意図された目的に照らして、関連性があり、十分に代表的であり、可能な限り誤りがなく、完全なものでなければならない(同条 3 項)。
(3)データセットは、意図された目的によって必要とされる範囲において、高リスク AI システムが使用されることが意図されている特定の地理的、文脈的、行動的又は機能的設定に特有の特性又は要素を考慮しなければならない(同条 4 項)。

（注記）前文では「学習、検証、テストのための高品質なデータセットには、適切なデータガバナン

[2] データセットとは、機械学習をするコンピュータによる自動処理を行うために用意された大量の標本データのことを指す。

スと管理の実践が必要である。学習、検証、テストのためのデータセットは、関連性があり、十分に代表的で、可能な限り誤りがなく、システムの意図された目的に照らして完全なものでなければならない」（前文 67）とある。前文で指摘する点は重要である。たとえば、従業員採用に関して過去のデータセットを読み取らせたところ、過去には男性しか採用していなかったため、女性というだけで採用対象外判定となったという事例がある[3]。客観的に公平なデータセットと考えていても、実はそうでない場合がある。このような場合に備えて開発過程では慎重な取り扱いが重要となる。

4｜高リスク AI システムが満たすべき要件（その 3：技術文書・記録保存）

（1）高リスク AI システムの技術文書は、そのシステムが市場に出回る前、あるいは使用開始される前に作成され、常に最新の状態に保たれなければならない。技術文書は、高リスク AI システムが本項に規定する要件に適合していることを実証し、AI システムがこれらの要件に適合していることを評価するために必要な情報を明確かつ包括的な形で国家所轄官庁及び被通知団体（適合性評価機関のこと。次回レポートで解説予定）に提供するような方法で作成しなければならない。AI システムの技術文書には、最低限、付属書Ⅳ（図表 10）に定める要素を含まなければならない（11 条）。

【図表 10】付属書Ⅳ（技術文書）

1.AIシステムについての一般的な説明
2.AIシステムの要素とその開発プロセスについての詳細な説明
3.AIシステムの監視、機能及び制御に関する詳細情報
4.特定のAIシステムに対するパフォーマンスメトリクスの適切性の説明
5.リスク管理システム(9条)の詳細
6.システムのライフサイクルを通じて提供者が行った関連する変更の説明
7.3章2節に規定された要件を満たすために採用された解決策の詳細な説明
8.EU適合宣言書の写し
9.市販後の性能評価のために設けられているシステムの詳細な説明

（注記）前文では「高リスクの AI システムがどのように開発され、その耐用期間を通じてどのように機能するかについて、理解しやすい情報を持つことは、システムのトレーサビリティ（追跡可能性）を可能にし、本規則の要求事項への適合性を検証し、運用のモニタリングや市場投入後のモニタリングを行うために不可欠である。そのためには、AI システムの関連要求事項への適合性を評価し、市場投入後のモニタリングを容易にするために必要な情報を含む、記録と技術文書の保管が必要である」（前文 71）とする。AI システムもシステムそのもののバグがありうることや学習データの偏向による誤った出力をすることがあり、この場合、PDCA を回して改善をする必要がある。その基本となるのが、当該 AI システムに関する技術文書である。この技術文書をスタートとしてどこに問題が発生し、問題が想定されていた場合に、想定通りに収束したか、収束しない場合に何が問題になるのかということ等を考えていくことになる。

[3] AI 事業者ガイドライン別添 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_3.pdf p 14 参照。

(2) 高リスク AI システムは、システムの耐用年数にわたって、イベントの自動記録（ログ）を技術的に可能になるようにしなければならない(12 条 1 項)。

（注記）前文では「技術文書は、AI システムのライフタイムを通じて、適切に最新の状態に維持されるべきである。さらに、高リスクの AI システムは、技術的に、システムの有効期間中、ログによるイベントの自動記録を可能にすべきである」（前文 71）とする。上記(1)で技術文書を踏まえて運用したにもかかわらず不適切な結果が発生した場合に、どこがどうおかしかったのかを判断するためには出力記録であるログの記録が必要となる。このように技術文書とログを照らし合わせて問題を発見することが想定されている。

5｜高リスク AI システムが満たすべき要件(その 4:使用説明書)

(1) 高リスク AI システムは、その運用が、配備者がシステムの出力を解釈し、適切に利用することができるよう、十分な透明性を確保するような方法で設計・開発されなければならない(13 条 1 項)。

（注記）前文では「特定の AI システムの不透明性や複雑性に関連する懸念に対処し、配備者が本規則に基づく義務を果たすのを支援するため、リスクの高い AI システムについては、市場に投入される前や運用が開始される前に透明性を確保することが求められるべきである。リスクの高い AI システムは、配備者が AI システムの仕組みを理解し、その機能を評価し、その長所と限界を理解できるように設計されるべきである」（前文 72）とする。高リスク AI システムの運営が適切になされるためには、実際に利用する配備者にとって透明性が担保されるように AI システムの構築がなされる必要がある。設計・構築時における透明性の確保に加え、配備者に対する透明性を保証するのが次項で規定されている使用説明書である。

(2)高リスクの AI システムには、適切なデジタル形式またはその他の方法で、配備者に関連し、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を含む使用説明書（図表 11）を添付しなければならない（同条 2 項)。

【図表 11】使用説明書の内容

・提供者の身元と連絡先、および該当する場合はその正式な代理人の連絡先
・高リスク AI システムの特徴、能力、性能の限界
・初回適合性評価の時点で提供者が事前に決定していた高リスク AI システムおよびその性能に対する変更
・配備者による高リスク AI システムの出力の解釈を容易にするために導入された技術的措置を含む人的監視措置(14 条に後述)
・必要とされるコンピュータ資源、高リスク AI システムの予想耐用年数、AI システムの適切な機能を確保するために必要なメンテナンスとケアの手段
・関連する場合、配備者が第 12 条に従ってログを適切に収集、保管、解釈できるよう、高リスク AI システムに含まれる仕組みの説明

（注記）前文では「特定の AI システムの不透明性と複雑性に関連する懸念に対処し、配備者が本規則に基づく義務を果たすのを支援するため、高リスク AI システムについては、市場に投入される前、または運用が開始される前に透明性を確保することが求められるべきである。高リスク AI システムは、配備者が AI システムの仕組みを理解し、その機能を評価し、その長所と限界を理解できるように設計されるべきである」とされ、したがって「リスクの高い AI システムには、使用説明書の形で適切な情報を添付すべきである」（前文 72）とする。高リスク AI システムの運営にあたっては、リスク発生抑止のため配備者が AI システム構築にあたって予定されていた適正運用を行うことが特に大事であり、これを実効化するために提供者から配備者に提供される使用説明書が必要となる。

6｜高リスク AI システムが満たすべき要件（その 5：人的監視措置）

(1)高リスク AI システムは、適切なヒューマン・マシン・インターフェース・ツールを含め、使用期間中、自然人が効果的に監視できるような方法で設計・開発されなければならない（14 条 1 項）。
(2)監視措置は、高リスク AI システムのリスク、自律性のレベル、使用状況に見合ったものでなければならず、以下（図表 12）のいずれかのタイプの方策またはその両方を通じて確保されなければならない（同条 3 項）。

【図表 12】監視措置

(a)技術的に可能であれば、市場に投入する前に、あるいは運用を開始する前に、提供者が高リスク AI システムに監視ツールを導入、及び/あるいは
(b)高リスク AI システムを市場に投入する前、あるいは運用を開始する前に、提供者が特定したうえで配備者が実施する監視ツールの組み込み。

(3)高リスク AI システムは、適切かつ比例的に、人間による監視を行う自然人が以下のこと（図表 13）が可能となるような方法で、配備者に提供されなければならない（同条 4 項）。

【図表 13】14 条 4 項の掲げる項目

・高リスク AI システムの関連する能力と限界を適切に理解し、異常、機能不全、予期せぬパフォーマンスの検出と対処の観点も含め、その運用を正当に監視できること
・特に、自然人による意思決定のための情報や勧告を提供するために使用される高リスク AI システムについては、リスクの高い AI システムによって生成された出力に自動的に依存したり、過度に依存したりする傾向（自動化バイアス）がある可能性に留意すること
・高リスク AI システムの出力を正しく解釈するために、例えば利用可能な解釈ツールや方法を考慮すること
・特定の状況において、高リスク AI システムを使用しないこと、または高リスク AI システムの出力を無視、上書き、もしくは逆に判断することを決定すること
・高リスク AI システムの操作に介入するか、「停止」ボタンまたは同様の手順でシステムを中断し、安全な状態でシステムを停止させること

（注記）前文では「適切な人間による監視手段を、システムの提供者が、そのシステムの市場投入またはサービス開始前に特定すべきである。そのような措置は、システムが、システム自身によって上書きされることのない、内蔵された運用上の制約を受け、人間の操作者に反応することを保証する必要がある。また、監視の役割を割り当てられた自然人が、その役割を遂行するために必要な能力、訓練、権限を有していることを確保すべきである。また、高リスク AI システムには、適切な場合、監視を割り当てられた自然人が、悪影響やリスクを回避するために、いつ、どのように介入するか、あるいはシステムが意図したとおりに機能しない場合に停止するかどうかについて、十分な情報を得た上で判断できるよう誘導し、通知する仕組みが含まれていることが不可欠である」（前文 73）とする。

ここで言われていることは、人の生命・身体・財産をはじめとする権利についての判断について、AI システムが人間の関与の余地なく最終的な結論を出すことは避けなければならず、そのために適切な人による監視措置が行わなければならないということである。

7｜高リスク AI システムが満たすべき要件（その 6：正確性・堅牢性など）

(1) 高リスク AI システムは、適切なレベルの精度、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・開発されなければならない（15 条 1 項）。

(2) 高リスク AI システムの精度レベルおよび関連する精度指標は、添付の使用説明書で宣言されなければならない（同条 3 項）。

(3) 高リスク AI システムは、発生する可能性のあるエラー、不具合または不整合について、可能な限り強靭でなければならない。この点に関して、技術的および組織的な対策を講じなければならない（同条 4 項）。

(4) 高リスク AI システムの堅牢性は、バックアップやフェイルセーフ計画（＝障害発生時に安全となる方向に作動する計画）を含む技術的な冗長性ソリューションによって達成される（同項）。

(5) 市場投入、あるいは運用が開始された後も学習を続ける高リスク AI システムは、偏った出力が将来の運用のための入力に影響を及ぼす可能性（フィードバック・ループ）のリスクを排除、または可能な限り低減するような方法で開発されなければならない。また、そのようなフィードバック・ループは適切なリスク緩和措置によって適切に対処されるようにしなければならない（同項）。

(6) 高リスク AI システムは、システムの脆弱性を悪用することによって、その使用、出力、性能を変更しようとする無権限の第三者による試みに対して強靭でなければならない（同条 5 項）。

(7) AI 固有の脆弱性に対処するための技術的解決策には、必要に応じて、学習データセット（データポイズニング）、または訓練に使用される事前訓練済みコンポーネント（モデルポイズニング）、AI モデルに誤りを犯させるように設計された入力（敵対的な事例またはモデル回避）、機密性攻撃、またはモデルの欠陥を操作しようとする攻撃を防止、検出、対応、解決、および制御するための対策を含まなければならない（同項）。

（注記）前文では「高リスクの AI システムは、そのライフサイクルを通じて一貫した性能を発揮し、その意図された目的に照らして、また一般的に認められている技術水準に従って、適切なレベルの精度、堅牢性、サイバーセキュリティを満たすべきである」（前文 74）とする。また「有害又はその他の望ましくない挙動を防止又は最小化するための適切な技術的解決策を設計及び開発することによって、

技術的及び組織的措置を講じるべきである。このような技術的解決策には、例えば、特定の異常が発生した場合、またはシステム外部の要因で誤動作が行われた場合に、システムの動作を安全に中断することを可能にするメカニズム（フェイルセーフ計画）などが含まれる」（前文 75）としている。さらに「サイバーセキュリティは、システムの脆弱性を悪意のある第三者が悪用することで、AI システムの使用、挙動、性能を変更したり、セキュリティ特性を侵害しようとしたりする試みに対して、AI システムが回復力を持つことを保証する上で重要な役割を果たす」とし、したがって、「リスクに見合ったレベルのサイバーセキュリティを確保するために、高リスク AI システムの提供者は、基盤となる ICT インフラも適宜考慮しながら、セキュリティ管理などの適切な対策を講じる必要がある」（前文 76）とする。

本条では、AI システムそのもの、AI システムの運用に生ずる事態、外部からの攻撃などによる AI システムの堅牢性、強靭性の確保が求められることを述べている。本条は高リスク AI システムにおいて、技術的に、社会あるいは個人への悪影響の発生の抑止、被害の最小化を求める条文である。

5――高リスク AI システム提供者の義務

1｜高リスク AI システム提供者の義務（総論）

高リスク AI システム提供者の義務は図表 14 の通りである（16 条）。高リスク AI システムの開発・提供にあたって課せられる義務が列挙されている。

【図表 14】高リスク AI システム提供者の義務

(1) 高リスク AI システムが上記 4（8 条～15 条）記載の要件に準拠していることを確保すること
(2) 高リスク AI システムに氏名、登録商号（商標）、連絡可能な住所を明記すること
(3) 品質管理システム（17 条、後述）を策定・文書化すること
(4) 技術文書等（18 条）を作成すること
(5) 自己の管理下にある場合、自動的に生成するログを保管（19 条、後述）すること
(6) 新規投入前に適合性評価手続き（43 条、次回レポート）を受けること
(7) EU 適合宣言書（47 条、次回レポート）を作成すること
(8) 本規則への適合を示す CE マーキング（48 条、次回レポート）を添付すること
(9) EU データベースへ登録（49 条、次回レポート）すること
(10) 本規則に不適合の場合、必要な是正措置を講じ、情報を提供（20 条、後述）すること
(11) 所轄官庁の合理的な要請があれば、高リスク AI システムが上記 4（8 条～15 条）に定める要件に適合していることを証明（21 条、後述）すること
(12) EU 指令（アクセシビリティ指令）に従って障がい者等の利用を容易にすること

（注記）本条は本規則の各所で規定されている提供者の義務をまとめて記載したものである。

2｜高リスク AI システム提供者の義務（各論）

(1)品質管理システム：高リスク AI システムの提供者は、本規則の遵守を確実にする品質管理システムを導入しなければならない。当該システムは、体系的かつ整然とした方法であって、方針、手順書及び指示書の形で文書化されるものとする(17 条 1 項)。

（注記）品質管理システムに含まれる項目は、規制遵守のための戦略などをはじめとする 13 項目が挙げられているが、ここでは省略する。

前文では「提供者は、健全な品質管理システムを確立し、要求される適合性評価手順の達成を確保し、関連文書を作成し、強固な市販後モニタリングシステムを確立しなければならない」（前文 81）とする。キーワードは EU の定めた AI ルールである①適合性評価 （43 条、次回レポートで解説予定）の手順を遵守するものであることと、②必要な情報の文書化(11 条、18 条)、③市販後モニタリングシステム(72 条、次々回のレポートで解説予定)を確立するものである。

(2)提供者は、高リスクの AI システムが市場投入または使用開始されてから 10 年を経過するまでの期間、各国所轄当局の裁量のもと、以下（図表 15）を保管しなければならない(18 条 1 項)。

【図表 15】提供者の保管すべき文書

(a)第 11 条で言及されている技術文書
(b)第 17 条の品質マネジメントシステムに関する文書
(c)該当する場合、通知機関が承認した変更に関する文書
(d)該当する場合、通知機関が発行した決定書及びその他の文書
(e)第 47 条で言及されている EU 適合宣言

（注記）前文では「高リスクの AI システムがどのように開発され、その耐用期間を通じてどのように機能するかについて、理解しやすい情報を持つことは、システムのトレーサビリティ（追跡可能性）を可能にし、本規則の要求事項への適合を検証し、運用のモニタリングと市場後のモニタリングを行うために不可欠である。そのためには、AI システムの関連要求事項への適合性を評価し、市場投入後のモニタリングを容易にするために必要な情報を含む、ログと技術文書の保管が必要である」（前文 71）とする。本条では保管すべき文書類について規定している。これら文書は AI システムの稼働状況や重大インシデント発生時の発生原因調査や改善措置対応などに用いられる。

(3)ログの保管：高リスク AI システムの提供者は、その高リスク AI システムによって自動的に生成される第 12 条(1)に言及するログを、当該ログが自己の管理下にある限りにおいて保管しなければならない。ログは、適用される EU 法又は国内法、特に個人情報の保護に関する EU 法に別段の定めがない限り、高リスク AI システムの意図された目的に応じた適切な期間、少なくとも 6 ヶ月間保管されなければならない(19 条 1 項)。

（注記）ログを取得・保管する理由は、前条の注記と同様である（前文 71）。

(4) 是正措置：高リスク AI システムの提供者は、その提供者が新規投入又は運用を開始した高リスク AI システムが本規則に適合していないと考え、又はそう考える理由がある場合には、直ちに、当該システムを適合させるために必要な是正措置を講じ、適宜、撤回し、使用不能にし、又は回収しなければならない。また、当該高リスク AI システムの販売業者、配備者、認定代理店及び輸入業者にその旨を通知しなければならない(20 条 1 項)。

（注記）前文において是正措置とは「システミック・リスクの可能性がある汎用 AI モデルに関連するリスクを特定し、防止するための努力にもかかわらず、当該モデルの開発または使用により重大なインシデントが発生した場合、汎用 AI モデルの提供者は、過度の遅滞なくインシデントを追跡し、関連する情報および可能な是正措置を欧州委員会および各国の所轄当局に報告すべきである。」(前文 115)とする。この前文は次回レポートで述べるシステミック・リスクを有する汎用 AI モデルについての記述であるが、重大インシデントが発生した場合には是正措置および報告を行うことが高リスク AI システムの提供者にも求められている。

(5)当局との協力：高リスク AI システムの提供者は、所管当局からの合理的な要請があった場合、当該当局に対し、高リスク AI システムが上記 4(8 条～15 条)に定める要件に適合していることを証明するために必要なすべての情報及び文書を、当該当局が容易に理解できる言語であって、当該加盟国が指示する EU の公用語の一つで提供しなければならない(21 条 1 項)。

（注記）当局への報告について前文では「本規則の施行を可能にし、事業者に公平な競争条件を設けるため、また、デジタル製品のさまざまな利用可能化形態を考慮すると、いかなる状況においても、域内に設立された者が、AI システムのコンプライアンスに関するすべての必要な情報を当局に提供できるようにすることが重要である」(前文 82) とされる。本条は高リスク AI システム提供者に本規則遵守状況を所管当局に報告させるための規定である。

(6)第三国に設立された提供者は、その高リスク AI システムを域内市場で販売する前に、書面による委任状により、域内に設立された認定代理人(authorized representative)を任命しなければならない(22 条 1 項)。

（注記）前文によると認定代理人は「域内に設立された者が、AI システムのコンプライアンスに関するすべての必要な情報を当局に提供できるようにすることが重要である。したがって、AI システムを域内で利用可能にする前に、第三国に設立された提供者は、書面による委任により、域内に設立された認定代理人を任命しなければならない」(前文 82) こととされている。また、情報の当局への提供のほか「認定代理人は、域内に設立されていない提供者が域内で市場投入または使用する高リスク AI システムのコンプライアンスを確保する上で、また域内に設立された提供者の連絡窓口として、極めて重要な役割を果たす」(同前文) とする。

6――高リスク AI システム輸入業者・販売者・配備者の義務

1｜高リスク AI システム輸入業者の義務

輸入業者（importers）は、高リスク AI システムを市場に出す前に、以下（図表 16）を確認することにより、当該システムが本規則に適合していることを保証しなければならない(23 条 1 項)。

【図表 16】輸入業者の確認事項

(a)適合性評価手続(43 条、次回レポート)が、高リスク AI システムの提供者によって実施されていること
(b)提供者が技術文書(11 条)を作成していること
(c)システムに必要な CE マーキング(48 条、次回レポート)が付され、EU 適合宣言書(47 条、次回レポート)および使用説明書(13 条)が添付されていること
(d)提供者が認定代理人を任命（22 条）していること

(注記)ここで輸入業者とは第三国に設立された自然人または法人の名称または商標が付された AI システムを市場に流通させる、域内に所在または設立された自然人または法人をいう(3 条(6))。この認定代理人は、前文では「AI システムのバリューチェーンの性質と複雑性に鑑み、また、新たな法的枠組みに沿い、法的確実性を確保し、本規則の遵守を促進することが不可欠である。したがって、AI システムの開発に貢献する可能性のある輸入業者や販売業者など、バリューチェーンに沿った関連事業者の役割と具体的な義務を明確にする必要がある」（前文 83）こととされている。23 条はこの観点から輸入業者が果たすべき義務を列挙している。

2｜高リスク AI システム販売業者の義務

販売業者(distributors)は、高リスク AI システムを市販する前に、そのシステムに必要な CE マーキング（48 条、次回レポートで解説予定）が付されていること、EU 適合宣言書（47 条、次回レポートで解説予定）の写し及び使用説明書（13 条）が添付されていること、並びに、該当する場合、そのシステムの提供者及び輸入者が、提供者の商標・住所を表示すること(16 条(b))、 品質マネジメントシステムを有すること(16 条(c))、 輸入業者の商標・住所を表示すること(23 条(3))を確認しなければならない(24 条 1 項)。

（注記）ここで販売業者とは提供者または輸入業者以外のサプライチェーンにおける自然人または法人で、AI システムを域内市場で入手できるようにする者をいう(3 条(7))。販売業者に関して前文では「AI システムのバリューチェーンの性質と複雑性に鑑み、また、新たな法的枠組みに沿い、法的確実性を確保し、本規則の遵守を促進することが不可欠である。したがって、AI システムの開発に貢献する可能性のある輸入業者や販売業者など、バリューチェーンに沿った関連事業者の役割と具体的な義務を明確にする必要がある」（前文 83）とある。開発を行わず、単に AI システムの販売を行う者の義務を列挙した条文である。

3｜高リスク AI システムのバリューチェーンにおける責任

販売業者、輸入業者、配備者又はその他の第三者は、以下の図表 17 のいずれかに該当する場合、本規則上、高リスク AI システムの提供者とみなされ、16 条に基づく提供者の義務を負うものとする(25

条1項)。

【図表17】提供者としての義務を負う者（販売業者、輸入業者、配備者等）

(a)既に市場投入され又はサービスを開始した高リスクAIシステムに自らの名称又は商標を付した者
(b)その者が既に市場投入された、または既にサービスを開始したAIシステムに、6条に基づき高リスクAIシステムであり続けるような大幅な変更を加える者
(c)その者が高リスクと分類されていない汎用AIシステムを含むAIシステムを6条にいう高リスクAIシステムとなるように目的を変更した場合

（注記）前文では「法的確実性を確保するため、特定の条件下では、販売業者、輸入業者、配備業者、その他の第三者は、高リスクAIシステムの提供者とみなされ、したがって関連するすべての義務を負うことを明確にする必要がある。これは、当該第三者が、既に市場に投入されている、またはサービスが開始されている高リスクAIシステムにその名前または商標を付した場合であり、義務を別の方法で割り当てることを定めた契約上の取り決めを損なうものではない」（前文84）とする。これは販売業者等がAIシステムを変更した場合において責任者を明確にし、かつ被害や弊害が発生した場合に、責任がどこに存するかを定めるための規定である。

4｜高リスクAIシステムの配備者の義務

高リスクAIシステムの配備者の義務は以下の図表18の通りである(26条)。

【図表18】高リスクAIシステム配備者の義務

1. 使用説明書(13条)に従うための技術的・組織的措置を講ずること
2. 能力があり、訓練を受け、権限を有する者による人的監視措置(14条)を講ずること
3. 適切で十分に代表的であるデータを入力することについての管理を行うこと
4. 使用説明書に基づき監視し、重大インシデント発生時には提供者および市場監督当局に報告するとともに使用を中止すること
5. 高リスクAIシステムによって自動生成されたログを、システムの意図された目的に照らして、少なくとも6か月は保管するものとすること
6. 職場で高リスクAIシステムを使用する場合は、事前に労働者に対して、使用の対象となることと、およびその影響を通知しなければならないこと
7. 公的機関、またはEUの機関、団体、事務所もしくは機関である高リスクAIシステムの配備者は、登録義務（49条、次回レポート）を遵守しなければならないこと
8. 犯罪者捜査のために事後遠隔生体識別のために高リスクAIシステムを使用する者は遅くとも48時間前までに司法当局の使用の認可を要請すること

（注記）本条は配備者の義務をまとめて規定したものである。前文では、「AIシステムの性質と、その使用に関連する可能性のある安全や基本的権利に対するリスク（現実の環境におけるAIシステム

の性能の適切な監視を確保する必要性を含む）を考慮すると、配備者の具体的な責任を定めることが適切である。配備者は特に、リスクの高いAIシステムを使用説明書に従って使用することを確保するために、適切な技術的・組織的措置を講じるべきであ」る（前文91）とする。すなわち、AIシステムを実際に利用するのは配備者であり、そのため配備者の利用如何により人権などに悪影響を及ぼす可能性があることから、モニタリングや、ログの記録、司法当局への使用認可申請（8. 事後遠隔生体識別AIについて）などの義務を果たさなければならないというものである。

5｜高リスクAIシステムの基本的権利影響評価

6条2項にいう高リスクAIシステム[4]の配備に先立ち、公法に準拠する機関である配備者、又は公共サービスを提供する民間団体である配備者、並びに付属書Ⅲの5項（b）（＝自然人の信用度評価・スコアを算出するためのAIシステム）及び5項（c）（＝生命保険や医療保険において、自然人に関するリスク評価やプライシングに使用されることを意図したAIシステム）にいう高リスクAIシステムの配備者は、当該システムの使用が基本的権利に及ぼす影響の評価を実施しなければならない（27条1項）。

（注記）前文では「基本的権利の保護を効率的に確保するため、公法に準拠する機関である高リスクAIシステムの配備者、または公共サービスを提供する民間団体、および銀行や保険団体など本規則の付属書に記載された特定の高リスクAIシステムの配備者は、使用開始前に基本的権利影響評価を実施する必要がある」とし、「基本的権利影響評価の目的は、影響を受ける可能性のある個人または集団の権利に対する具体的なリスクを特定し、それらのリスクが現実化した場合に取るべき措置を特定することである」（前文96）とする。公的な配備者およびそれに準ずる者は住民や契約者の基本的権利にかかわる業務を行うため、これら住民等に与えうる影響の事前評価が求められる。

7――小括

本稿で取り扱ったのは、AI規則のうち、高リスクAIシステムの定義と満たすべき要件、および高リスクAIシステムの提供者等の義務である。

高リスクAIシステムとは人間の権利と安全にリスクを生じさせかねないAIシステムのことを言うのは本文の通りである。対象となるAIシステムは網羅的に定義されているが、提供者が高リスクではないと判断した場合に登録義務はあるものの、規制を受けない方法も規定されている。

高リスクAIシステムの場合、要件として、①リスク管理システムの確立・文書化、②適切な学習用データの利用（データガバナンス）、③技術文書の作成・ログ保存、④配備者に対する使用説明書の作成、⑤人的監視措置の組み込み、⑥正確性・堅牢性の確保が求められる（8条～15条）。

システムの設計時の文書作成、運営時のログ保存、運営監視などAIシステムが適切に運用するにあたっての必要な措置は一通りそろっていると考えられる。

そして、これらのリスク管理を行っていたにもかかわらず、万一、重大事故（重大インシデント）

[4] 付属書IIIの2項に掲げる分野における使用を意図する高リスクのAIシステムを除く。

が発生した場合についての規律については 71 条(次々回レポート参照)が存在する。71 条は重大インシデントを把握した提供者が市場管理当局へ報告することが定められている。

さらに、この様な重大インシデントを引き起こすような AI システムが引き続き提供され、「リスクをもたらす」と市場監視当局が判断した場合には提供者に対して是正措置を求めることができ、是正措置を取らない場合には AI システムの撤去・回収を命ずることができる(79 条、次々回レポート参照)とされている。

次回レポートでは「適合性審査」と「汎用 AI モデル」を解説する。

