講演録
Date: 2022.2.14
https://www.jilis.org/report/2022/jilisreport-vol4no4.pdf

EUのAI整合規則提案 ―新たなAI規制戦略の構造・意図とブリュッセル効果の威力

一般財団法人情報法制研究所　参与
慶應義塾大学　教授
新保 史生

EU の AI 規則提案 ―名称をどのように訳すか

慶應義塾大学の新保と申します。本日は、EUの新たなAI規則について、2021年6月21日に発行された「ビジネス法務2021年8月号」に掲載された拙稿「EU新AI整合規則提案にみるAI規制戦略の構造・意図とブリュッセル効果の威力」に基づきお話をしたいと思います。今回は、EUの新しい規則提案について、どのような目的・意図があって、今後どのような方向で、このAI規則というものが世界的にも影響を及ぼしていくのかということをお話しさせていただきたいと思います。

まず、今回の新たな規則提案の内容を確認する前の段階として、このタイトルの規則提案の名称をどのように訳すかが1つ目のポイントです。上

から、誰もが理解している用語から確認をすると、Europearn Commissionは欧州委員会、proposalとしてregulationであることから規則提案となります。問題は、Laying Down Harmonised Rules on Artificial Intelligenceについて、例えば総務省が2021年8月4日に公表したAIネットワーク社会推進会議「報告書2021」では、「人工知能に関する調和の取れたルールを定める規則の提案」と訳しています。調和法と訳しているものもあります。これまでも、Harmonised Rulesについては、国際調和といった観点からの法令については、Harmonised Rulesと訳すことが多かったと思います。今回、この規則提案の内容を確認するほど、今回の規則は製品安全規制と同様の義務を新たに高リスクAIにも課すことが主たる目的となっています。例えば、従来から欧州標準化委員会(CEN)で定めているHarmonised Standardsというものがありますが、これは製品安全規格としてHarmonised Standardsとして定め、用いられているものです。製品安全規格、整合規格として従来から適合性評価の対象となるものについてはHarmonised Standardsに基づいて取り組みが行われてきたわけです。今回のAI規則提案も、その内容は標準化とかなり近い内容になっています。したがって、私の訳としては、「人工知能に関する整合規則」として、人工知能法の制定としての今回の規則提案の内容を踏まえた訳にしています。

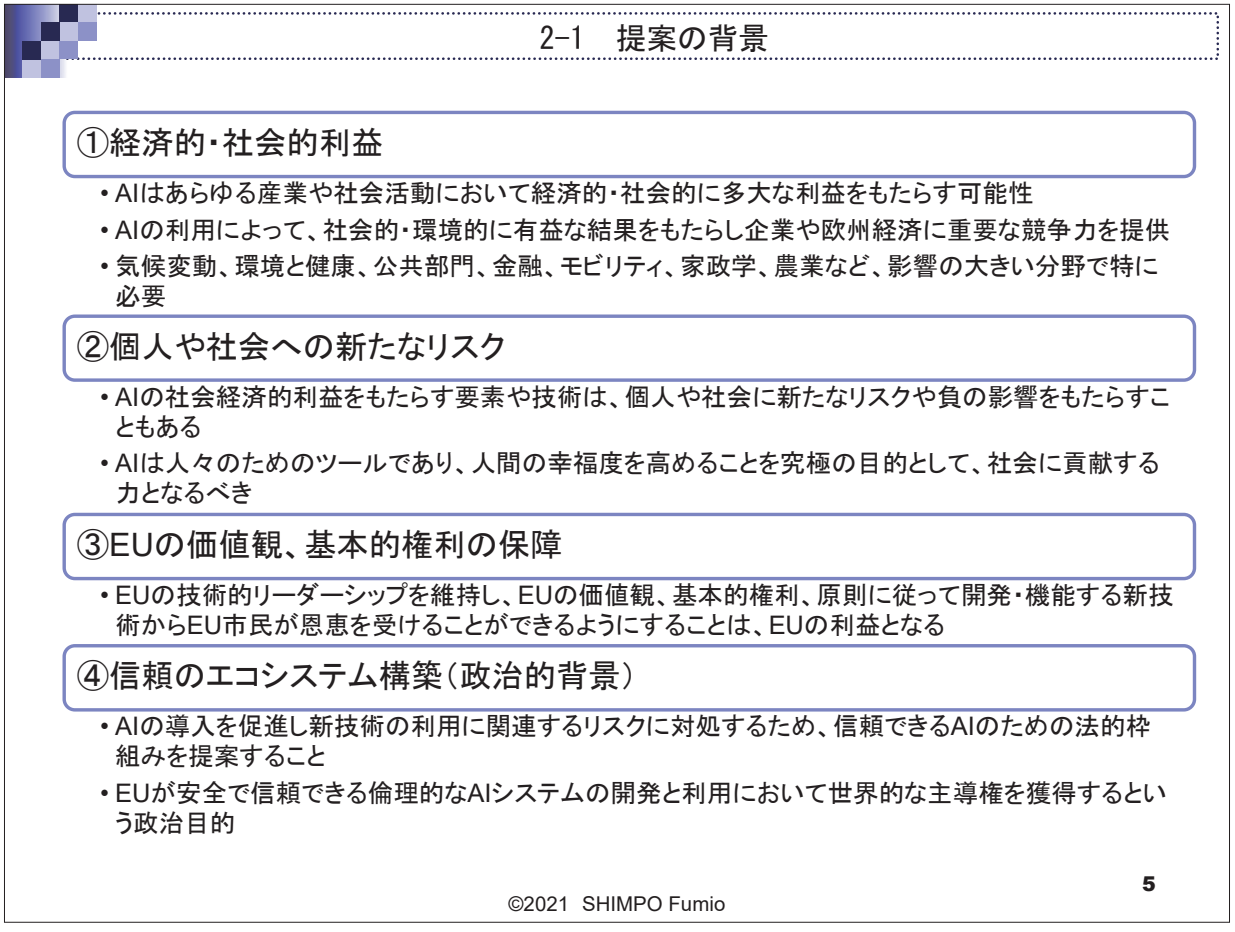
AI規則提案、3つのポイント

今回のEUの規則については、さまざまな観点から分析がなされているところではありますが、私の報告の内容は主に3点のポイントを主たる目的としています。この整合規則がAIシステムのリスクに応じた利用規制という方法での規制を目指していることが、まず1つ目の特徴です。

2つ目は、この整合規則の内容は、製品安全規制と同様の義務を課す内容といっても過言ではありません。したがって、高リスクに分類されるAIシステムをCEマーキングの対象にすることが今回の整合規則の主な柱となっているため、この点を把握・理解しておかないと、今回の整合規則の目的について十分に理解ができないといえます。

3つ目は、それを実現するための制度として適合性評価と第三者認証の構築が定められています。

提案の背景については、非常に多くの文書が公表されており詳細な記述がなされていますが、総務省



の情報通信政策研究所が発行している『情報通信政策研究』に原稿を掲載したときに、ＥＵの文書を一通り確認して、そのときの経緯も含めて、今回の提案の背景について整理をしてみました。これまでの経緯を踏まえて、４つに大きく集約されるであろうというのが私の分析結果です。

これまでＥＵが進めてきた取り組みについては、我が国においても、日本のほうが原則策定に向けた検討などは先に進めてきたといえます。AI原則を積極的に策定して、議論を進めることは日本が先行して行ってきたわけです。『情報通信政策研究』において、私は「AI原則は機能するか？」という内容の論文を公表させていただきました。この原稿を執筆している時点ではEUのAI白書なども公表されていませんでしたが、検討中の文書を事前に入手しEUの動きを事前に確認した上で、今後原則という形での取り組みを進めること、そしてこれを具体化するという方向になるということについてはかなり懐疑的な印象を持っていました。予想通り、EUの今回の規則提案は、原則については既に存在していることを前提とした内容になっています。今回の規則提案に基づいて今後さらに何らかの原則を策定し、例えば適合性評価といった仕組みに組み込むということは何も言及がないところは留意すべきです。

柱となる目的としては大きく分けて4つです。まずは経済的・社会的利益として、EUはこれまで特にこのルール作りを通じて主導権を握る規制を展開すること、これを、今回のタイトルにもしていますが、「ブリュッセル効果」と最近は呼んでいるものがあります。このブリュッセル効果が、特に独禁法、労働分野、環境分野、排出権取引といったものも含めて、世界的に大きな影響を及ぼしているのは周知の事実です。これは、AIについてもEUはネット企業にしてもAI関係にしても、アメリカ企業に比べると世界の覇権を握るような事業者がいないといえます。したがって、EUはそのような事業が十分に展開されていない反面、規制について細かく設定をすることについては、かなり批判的な意見が多いのは事実だと思います。ところが、そこがEUの戦略であり、ゲームはルールを作った者が有利になるということを一貫して進めてきているため、経済的・社会的利益ということについても、そのようなリーディングカンパニーがいるかどうかということに関係なく、非常に明確なメッセージを示していると考えられます。

一方で、AIの発展による新たなリスクについてどのように考えるべきかという点を、かなり細かくリスク認識をした上で今後の取り組みを検討するのが2つ目です。

3つ目は、GDPRに基づく現在の状況について確認することになります。欧州基本権条約では、基本的権利の保障を従来から非常に重視して、その観点に基づく取り組みを進めてきているわけです。今回注意しなければならないのは、AI整合規則は基本的権利の保護という観点から見てしまうと、その本来の趣旨を見誤るおそれがあります。つまり、GDPR同様の規則提案という趣旨で今回の整合規則を分析すると、ある意味で正しい分析はできないと考えています。

4つ目は、信頼のエコシステムとして、かなり政治的な背景に基づく法的枠組みを提案することによって世界的な主導権を獲得するということを明確にメッセージとして示していることです。

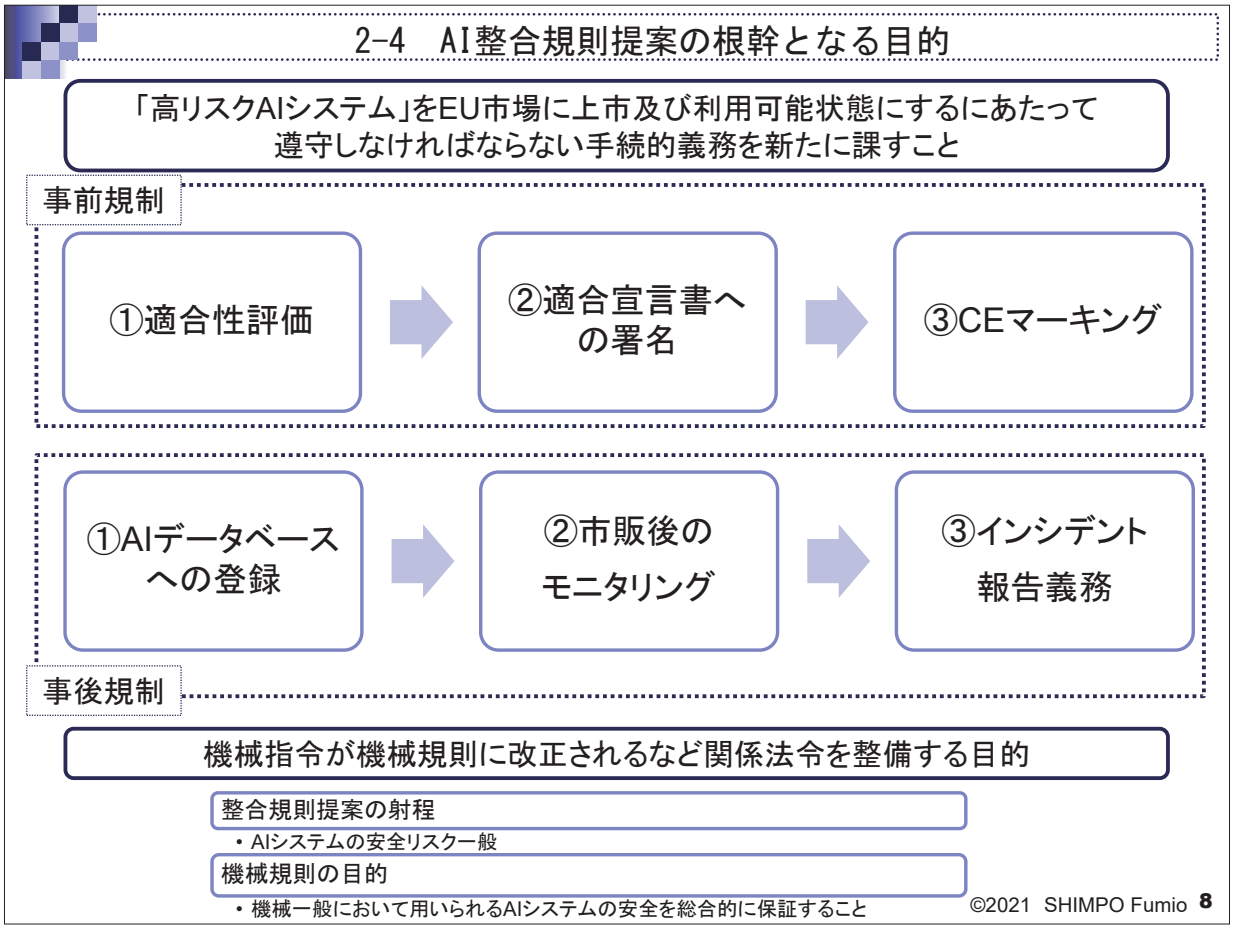
その意図については、欧州調整計画に基づく戦略の背景を分析し、さらに次の4つに集約されるのだろうと思います。EUの調整計画では従来から脈々とEUが目指すAI戦略を示してきたわけですが、その意図を踏まえて今回の調整計画に示されている内容を確認してみると、最初に示されているのは安全規制となっています。つまり、GDPRなどのように、実体的な権利を保護するという目的が主たる目的というわけではなく、あくまでEU市場に上市するAIシステムの安全規制をどのように行うのかを示すことが主たる目的となっています。それを踏まえて、AIへの投資とイノベーションを促進する。3つ目がガバナンスと効果的な法執行。そのための基本となるのが、やはり基本的権利の保障。ところが、ここで注意しなければならないのは、GDPRと違うところは、基本的権利の保障は当然のことであって、その前提を踏まえた上での安全性確保、つまり製品の安全確保のための規制同様の規制をAIシステムに適用することが目的となっています。よって、3つ目の部分は、基本的権利の保障と安全性確保という趣旨を適切に理解しないと、この整合規則の内容について、具体的にどのような意図があるのかがわからなくなってしまうおそれがあります。そしてＥＵ市場の断片化を防止するための取り組みを進めること。これらの取り組みを進めるために、今回新たに提案がなされているのが欧州人工知能委員会（EAIB）です。個人データ保護についても、European Data Protection Board (EDPB)を設置し、そのメンバーとしてEuropean Data Protection Supervisor(EDPS)を置くなど、様々な取り組みをしてきたわけですので、同様の取り組みを今回も進めるということが示されているといえます。

規制の根幹にある目的

今回の規則提案の整合規則としての内容は、まず

対象について確認していただきたいと思います。対象と目的について、AIシステムを上市する、またはサービスを開始・利用するための整合規則の制定が目的です。さらに、特定のAIを利用禁止すること。高リスクのAIについての要求事項と義務を定めること。自然人との対話を目的としたAIシステム、感情認識システム、生体情報分類システム等についてのルールの整合性を確保すること。その他モニタリングと監視が、今回の規制の目的・対象になっています。ここで、根幹となる目的は何かということですが、今回の整合規則についての解説を拝見していると、ほとんどの解説は、EUのプレスリリースに沿って、EUのAIシステムに対するリスク分析、AIについての利用禁止、高リスクのAIについての義務など、新たなリスク分析と分類を紹介しているものが多いように思います。確かにリスク分析については新たな視点からの取り組みであるとはいえ、そもそも整合規則の内容を理解する上で、根幹となる目的をきちんと把握しておかなければ、まったく異なる視点からの分析になってしまうおそれがあります。つまり分析に基づくメッセージとして最も適切ではないのがAIの包括規制という短絡的な分析を行うことです。さらに、AI規制については時期尚早であるといった、完全に的外れな指摘も見受けられます。このような意見を確認すると理解することができると思いますが、包括規制や時期尚早といった安易な反対論を展開したとしても、その考えに基づいてAI規則提案に定められているさまざまな手続きを検討し分析をしても意味がありません。今後、内容についてかなり修正がなされたとしても、根幹にある目的はおそらく変わらないと考えられます。高リスクのAIシステムをEU市場に上市、利用可能するにあたっての手続的義務を新たに課すことが目的でしかないわけです。ゆえに、今後この部分をきちんと把握していないと、規制が時期尚早であるとか、規制そのものへの反対意見のみを表明し、AIのリスク分析が適切ではないとか範囲が不明確といった点にこだわっているその裏では淡々と、あくまで適合性評価の手続きをどうするかという手順の具体化など、今後実施すべき手続を整備する検討が進み、気が付くと整合規則が完成した段階で適合性評価を受けなければならない状況が出現するという流れで制定に向けた取り組みが着々と進んでいくのだろうと思います。

事前規制としては、適合性評価を受け適合宣言書に署名するというCEマーキングの手順です。CEマーキングは、例えば、手元のリモコンの裏側を見てい

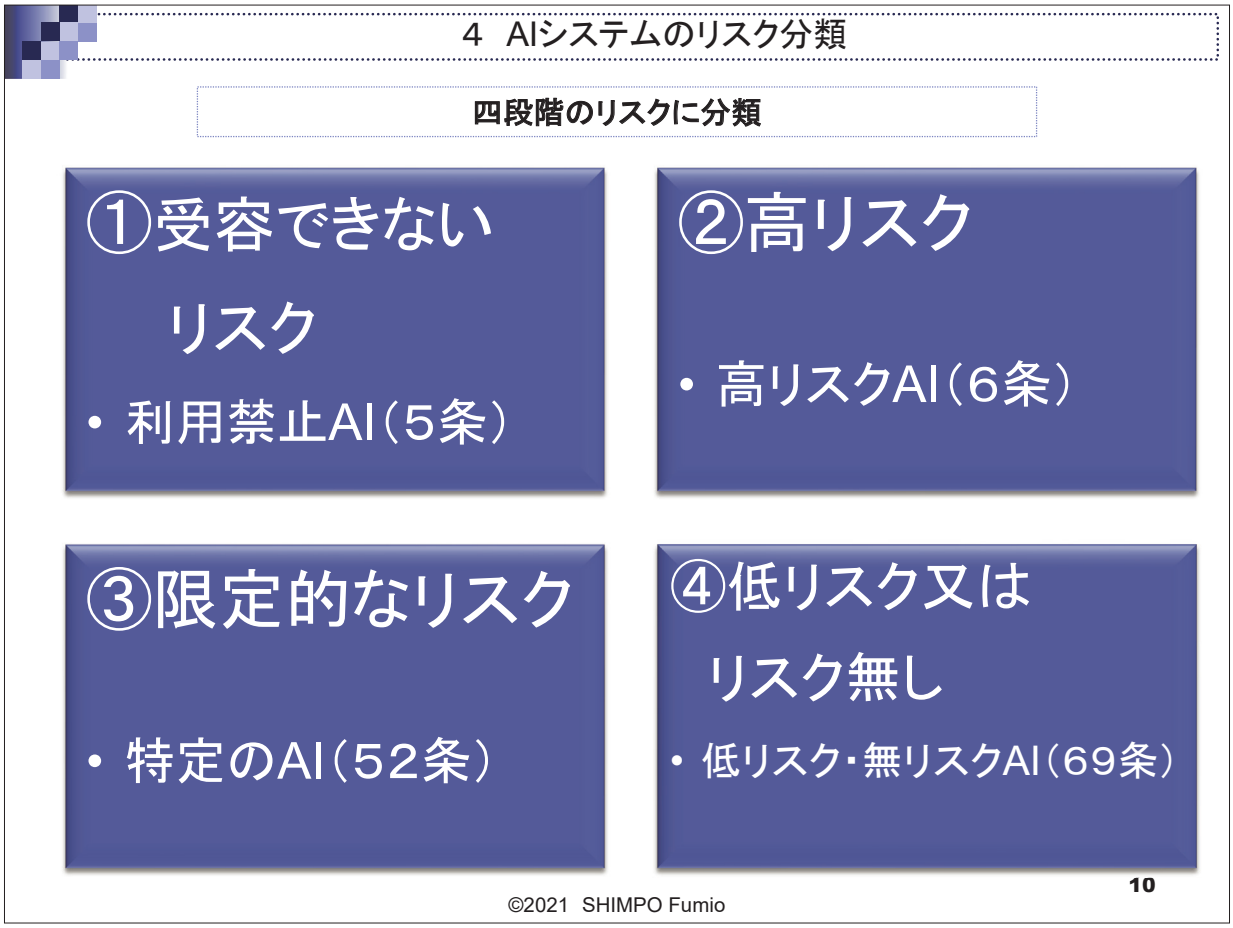


ただくと、CEと表示されています。製品安全規制としてEU市場に上市するために必要なのがCEマークです。ただ、CEと表記されるマークでChina Exportマークというものもあり、ほぼ同じようなロゴになっているので、CEマークとChina Exportマークの混同問題というものが別の問題としてありますが、本日は、China Exportマークのお話はしません。CEマークを付すことをCEマーキングというわけですけれども、事前規制をAIシステム、対象は高リスクのAIシステムに課すことが目的です。事後規制として、CEマーキングを課し、AIデータベースへ登録する義務を課して、市販後の製品安全規制同様のモニタリングを行い、インシデント報告をする仕組みになっています。

この図式を見ていただくと、ほとんど普通の製品安全規制を整合規則として課す内容です。その趣旨は、機械指令が機械規則として提案されていることからも明確に示されているわけです。よって、今回の本体の整合規則提案を見ただけでは、AIシステムの安全リスク一般についての記述がなされているので、あたかも、AIのリスク分析をしたうえでの安全性について考えるといったような趣旨が、本体の整合規則提案の趣旨であるかのように見受けられます。しかし、実際に関係法令、つまり今回の整合規則はあくまで関係法令も整備すると明記しているわけですので、関係法令を確認すると、AIシステムの安全性を総合的に保証することが、今回の目的であることがわかります。

4段階のリスク分類

規則提案の構造については、利用規制、高リスクAIに関する義務、適合性評価、透明性要件、ガバナンス、監督および法執行からなります。規則提案に関する解説の多くは、利用規制と高リスクAIに関する義務について解説をしているものが多いように思います。条文の内容の比率は、適合性評価以降のほうが、条文の数から見ても細かく規定されていることがわかります。高リスクAIに関する規定以降の部分は、適合性評価、透明性、ガバナンスと法執行の内容から占められているわけです。つまり、規制の主軸はもっぱら整合規格を求める整合規則としての内容になっています。もうひとつ別の側面として気になるのが、コンサルティングなどを実施されている事業者の方は気がついていると思いますが、第三者評価制度を組み込む仕組みになっていることから、GDPRに基づくSCC、標準契約条項やBCR認定と比較



しても、かなり大規模なコンサルティングが必要になると考えられます。とりわけ、今回の整合規則提案は、高リスクAIシステムをEU市場に上市するだけで、すべての事業者が関わってくる適合性評価の仕組みであるため、規則提案に定められているリスク・マネジメントシステムの構築や第三者評価制度への対応について、正確に理解しコンサルティングを行っている事業者の方に、適切にコンサルティングを行っていただく必要があります。EU市場に製品を輸出したりサービスを提供する事業者すべてに関わってくることになるためです。

リスク分類については、四段階のリスクに分類がなされ、受容できないリスク、高リスク、限定的なリスク、低リスクに分けられています。

今回の規則提案の評価として、この分類が適切か否かという議論がなされていますが、リスクが高い利用禁止対象のシステムは、サブリミナル、弱者の脆弱性につけ込むこと、公的機関による社会的スコアリング、法執行目的での公共の場におけるリアルタイム遠隔生体識別の4つが示されています。注意点は、民間企業による人事などの手続で利用するスコアリングは禁止していない点です。公的機関による社会的スコアリングのみが対象です。遠隔の生体識別についても、認証と訳している人もいますけれども認証までは求めていないので、あくまで生体識別をするだけのシステムであって、リアルタイムの遠隔生体識別システムを法執行目的で利用する場合に限られます。この意図、つまりEUの意図が何かということが禁止対象として定められているAIシステムの内容から、かなり透けて見えるわけです。サブリミナル、弱い者につけ込む、社会でのスコアリング、リアルタイム遠隔生体識別などを積極的に開発を進め利用しているのは、中国で進められているAIシステムの多くが、この4つにかなり該当するのではないかと思われます。そうすると、今後、EUとしては、EUにおける基本的権利を保障したうえでのAIシステムを、安全にEU市場に上市するための手続きを決めるにあたっては、そのような価値とは相容れないAIシステムについては利用禁止にすべきであるという趣旨が、この4つを見てみると、非常に明確であると思った次第です。

高リスクAIにかかる義務の中核

高リスクAIにかかる義務や利用禁止AIは、この分類や区分けが良いか悪いかという議論をしても、製品安全のための規制が決まってしまえば、日本としてはその善し悪しを議論しても意味がない。一方で、2番目以降のところについて、高リスクAIについては、日本の事業者が今後開発するものはこの分類に含まれるものが相当な比重を占めることになると考えられ、限定的なリスクと低リスクがそれに続くと考えられます。よって、整合規則の本体だけを読んで確認をしても、規制の全体像を十分に把握できないことから、附属書に示されている分類もすべて確認する必要があります。

附属書を見ていただくと、附属書Ⅱに記載されている製品安全規制の対象となるAIシステムが、高リスクAIにかかる義務の対象となっています。ここでは(a)と(b)両方を充たしている、「かつ」という条件なので、これらの要件を満たす場合に対象となるわけです。機械、玩具、海洋レクリエーションなどについては、高リスクAIに関する義務が適用されます。一方、民間航空、マイクロカー、農業・林業用トラクター、船舶、鉄道システム、自動車、無人航空機など、附属書ⅡのBについては、これは適用外となっています。この部分については、あたかもEUの今回の整合規則に穴があるとか、規制対象の分類が不十分であるとか、あたかもザル法であるかのように解説をしている論調の解説も見受けられますが、そのような解説は完全に誤りです。実に緻密に適用除外を定めていると言えます。つまり、単なる適用除外ではなく、新たな規則の適用について要検討・要配慮、裁量によって今後その検討の采配を検討する部分でしかないわけです。つまり、適用除外となっている部分は、84条の欧州委員会の評価・見直し条項が適用される仕組みになっています。飛行機や自動車、つまり自動運転、航空分野も無人航空機を含めて自律型のシステムが既に利用されており、船舶についても今後は大型の船舶などは自律航海が可能になる、鉄道も無人で運行されるわけで、これらの分野で用いられるAIシステムこそが、まさに今回の高リスクAIにかかる義務の中核部分です。この部分に今後どのように規制を適用するのかということについて、高リスクAIにかかる義務の適用の方法を検討することを、EUが実に見事に今後微妙に調整を行うのだろうと思われます。これは、整合規則の附属書ⅡのAとⅡのBに示されている内容を確認すると、EUがこの整合規則を定める意図するところは明確であると言えます。高リスクAIにかかる義務として、ⅡのAについては、整合規則がそのまま適用される一方で、見直し条項の適用については別途今後慎重に検討して決めることになるわけです。例えば、現時点ではあくまで無人航空機と記されていますが、無人の船舶、無人鉄道など、さまざまなものを無人による運行が想定されるものとして対象に含めているわけです。さらに、附属書Ⅲは、高リスクのAIについて見直し条項の対

6 高リスクAIに係る義務

高リスクAIの分類及び対象リスト（6条・7条）
高リスクAIの要件（8-15条）
プロバイダ等の義務（16-29条）

高リスクAI

「附属書 II」に記載されている製品安全規制の対象となるAIシステム

かつ

(a)安全構成要素において用いられるAIシステム

(b)安全構成要素として用いられるAIシステムを含む製品として第三者適合性評価を受ける義務があるもの

上記二つの要件を満たす場合

①機械、②玩具、③海洋レクリエーション船舶、④リフト、⑤爆発性雰囲気装置、⑥無線機器、⑦圧力機器、⑧索道設備、⑨個人用保護具、⑩ガス燃焼機器、⑪医療機器、⑫体外診断用医療機器：（6条1項）

2条2項により、以下は適用除外 → 84条の評価・見直し条項が適用される

①民間航空、②マイクロカー、③農業・林業用トラクター、④船舶用機器、⑤鉄道システム
⑥自動車及びトレーラー等、⑦無人航空機：附属書 IIのB

12

©2021 SHIMPO Fumio

6 高リスクAIに係る義務

6条1項の対象（附属書 IIのA）

- 1. 機械指令（2006/42/EC指令）
- 2. 玩具安全指令（2009/48/EC指令）
- 3. 海洋レクリエーション船舶指令（2013/53/EU指令）
- 4. リフト指令（2014/33/EU指令）
- 5. 爆発性雰囲気装置及び保護システム指令（2014/34/EU指令）
- 6. 無線機器指令（2014/53/EU指令）
- 7. 圧力機器指令（2014/68/EU指令）
- 8. 索道設備規則（(EU) 2016/424規則）
- 9. 個人用保護具規則（(EU) 2016/425規則）
- 10. ガス燃焼機器規則（(EU) 2016/426規則）
- 11. 医療機器規則（(EU) 2017/745規則）
- 12. 体外診断用医療機器規則（Regulation (EU) 2017/746規則）

13

©2021 SHIMPO Fumio

6 高リスクAIに係る義務

6条1項の対象の詳細（附属書 IIのB）（現時点では義務規定の適用なし）

2条2項により附属書 II B（航空機、車両、船舶等）は、現時点では適用外
84条の評価・見直し条項が適用される

- 1. 民間航空安全規則（ (EC) 300/2008規則）
- 2. 二輪・三輪及び四輪マイクロカー規則（(EU) No 168/2013規則）
- 3. 農業用及び林業用トラクター規則（ (EU) No 167/2013規則）
- 4. 船舶用機器指令（2014/90/EU指令）
- 5. 鉄道システム相互運用性指令（Directive (EU) 2016/797指令）
- 6-1. 自動車及びトレーラー等システム規則（(EU) 2018/858規則）
- 6-2. 自動車及びトレーラー等型式認証規則（(EU) 2019/2144規則）
- 7. 無人航空機規則（ (EU) 2018/1139規則）

14

©2021 SHIMPO Fumio

6 高リスクAIに係る義務

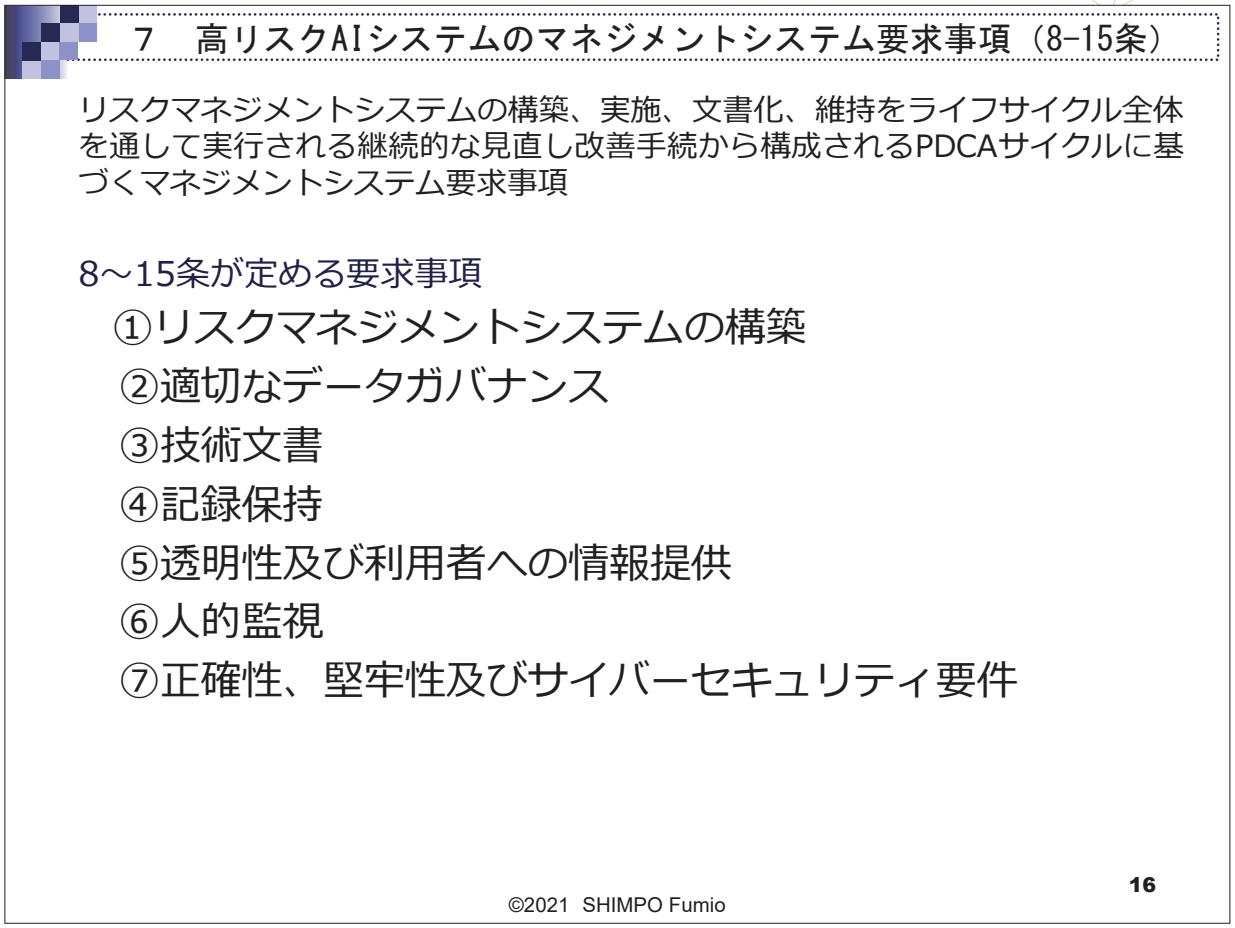
附属書IIIが規定する分野におけるAIシステムの利用も高リスクとしており、高リスクAIシステムがもたらす危害または悪影響のリスクに応じて欧州委員会が見直しを実施（７条）

6条2項（附属書Ⅲ）

- 1. 自然人の生体識別及び分類
- 2. 重要インフラの管理・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
- 使用することを目的としたAIシステム。
- 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

15

©2021 SHIMPO Fumio



象となるものを定めています。これらについては、いろいろな意見が出ている中で、この分類や規制の対象としての高リスクAIについての義務の内容についての議論を進める際に、その分類になっている趣旨をきっちりとまずは把握し、日本としても意見を表明していくことが必要です。つまり、AIのリスク分析が適切か否かとか、AIについての包括規制が時期尚早であるとか、そのような次元での意見表明ではまったく意味がない。詳細に定められている対象となる製品やサービス毎に、どのようなAIシステムに係る製品安全規制を適用するのかということが、今回の規制の中核にあるということを理解しなければなりません。

その点を明確に示しているのが、リスクマネジメント・システム、つまりPDCAサイクルに基づくマネジメントシステムの構築、実施、文書化、維持をライフサイクル全体を通して実行することが定められている点です。AI整合規則を理解する上で、AIのリスク評価やリスク分析については、マネジメントシステムを構築する際のリスク評価の観点からの検討は必要であると考えられますが、個人の権利・利益の保護基本的利益の保障の観点から、このリスク評価・リスク分類が適切ではないといった指摘は、まった く的が外れているということになると思います。

よって、AI整合規則に適切に対応するためには、マネジメントシステムの基本的知識がなければ対応できないということになります。したがって、我が国でも既にさまざまなマネジメントシステムが用いられているわけですが、そこに今回のAI整合規則に基づくマネジメントシステムの構築が新たに加わるということになります。

AI 整合規則におけるマネジメントシステムの仕組み

高リスクAIについては、プロバイダーの義務としてリスク・マネジメントシステムと品質マネジメントシステムの構築が必要となります。マネジメントシステムを構築するコンサル事業者向けにビジネス展開を推奨するような解説になってしまう点は少々不本意ではありますが、早目にマネジメントシステム構築の必要性に気がついていただいて、リスクマネジメントと品質マネジメントについてマネジメントシステムの構築義務がAI整合規則の主たる目的であるということを理解していただくことは重要です。なお、その詳細については時間の関係上解説はいたしませ

んが、資料を見ていただくと、マネジメントシステムを構築する際の要求事項が整合規則の本体に書かれているということがわかると思います。なお、整合規則に定められている要求事項の内容に私はかなり衝撃を受けています。例えば、JIS Q 15001についても、マネジメントシステムに関する要求事項を記載した本文と、管理策を記載した附属書Aである規定に分離した規格票の構成となっており、さらに、附属書Aの理解を助けるための参考情報を記載した附属書Bと附属書C、この規格と旧規格との対応を示した附属書Dから構成されています。つまり、本体にはあくまでマネジメントシステムに関する要求事項が書かれていて、具体的な管理策などの手続き部分については附属書に詳細が定められているのが一般的なマネジメントシステム規格の体系です。AI整合規則はマネジメントシステムだけでなく、附属書にあたる部分についてまで本体に書かれているということに驚きました。さらに、認証機関の設置についても定められています。Notified Body、つまり適合性評価を担う第三者認証機関の設置と、それに基づく認証の要件まで書かれています。ですから、このような一連の詳細な規定ゆえに、EUは製品安全規制を目的とする整合規則に基づくマネジメントシステムの構築義務を課すことを本当にやる気なのだろうと感じたわけです。高リスクAIシステムについての第三者認証制度の評価を行うための仕組みの整備がAI整合規則の目的であるということが、ここからも読み取れるわけです。

具体的な仕組みとしては、適合性については従来からの製品安全規制の整合規格との適合性要件がそのまま定められています。したがって、既存の安全規制の延長線上に高リスクAIの第三者認証を組み込むことになります。ゆえに、整合規格が存在する場合と存在しない場合に分けた上で、整合規格が存在しない場合であっても適合性を推定する規定が置かれているわけです。

一方で、高リスクAI以外の特定のAIシステムについては、行動規範を制定・策定して、透明性確保義務を課すことが定められています。つまりAIが使われているものの、リスクとしてはそれほど高くないものについては、それを本人に知らせる仕組みしか定められていないわけです。ただし、少々私が気になっているのが、この仕組みはcookie規制のようになるおそれがあると思っています。通知義務を今後課すことになると、「このシステムはAIを使っています」ということを毎回通知する。利用者側が通知されて「あ、これはAIが使われている」とわかるのは良いのですが、日常的に使われるシステムに今後全部AIが組み込まれてくるような状況になると、システムを立ち上げた時点で毎回cookie規制同様に、とにかくAIを使っていることを通知することになり、また無意味な表示が増えるのではないかという点が私の懸念事項です。

サンドボックスや中小規模であるSmall and Medium-sized enterprisesの支援。ガバナンスとしては、EAIBの設置という仕組みが用意されています。

法執行の仕組みは、データベースへの登録義務を課し、モニタリングを実施してインシデント報告義務を課しています。さすがにGDPRのように72時間という短い時間にはなっておらず、15日以内に報告する手続となっています。製品安全規制であるため、インシデント報告義務として重大なインシデントが発生した場合の報告義務を課す形態となっています。法執行についても、GDPRとAI整合規則の両方に違反した場合について考えてみると、GDPR違反事項についてはGDPRで確認をするとともに、サブリミナル、脆弱性、公的機関によるスコアリングや遠隔生体識別など利用規制に抵触する場合については、AI整合規則5条の利用規制違反となり、データガバナンス違反が問われる構造になっています。よって、今後AIシステムではAIを用いてデータを取り扱うと、その中にはGDPRの対象となる個人データの取り扱いに該当するものが含まれるとともに、学習データの取り扱いについてはデータガバナンス規定の対象となります。そうなると、データガバナンス要件の対象となる違反には、AI整合規則のほうがGDPRよりも一段階高くなっており、3,000万ユーロまたは全世界の年間総売上の6%が上限の制裁金になっているわけです。その他の違反についてはGDPRと同レベルです。

まとめ

最後に、今回の報告タイトルでは、「ブリュッセル効果」という用語をもちいました。Bradford先生が最近公刊した書籍のタイトル、The Brussels Effectです。Bradford先生がノースイースタン大学のNorthwestern University Law Reviewに公表した2012年の論文に端を発します。なお、ほぼ同じ時期に、遠藤乾先生と鈴木一人先生の『EUの規制力』が公刊されていますが、こちらの書籍におけるEUの規制の効果についての体系的な分析のほうが実質的には早かったと言えます。

最後に、EUのAI規制のこれまでの経緯は、総務省の情報通信政策研究所の『情報通信政策研究』に寄稿した拙稿「AI原則は機能するか？　-　非拘束的原則から普遍的原則への道筋　-」2020 年 3 巻 2 号をご参照ください。

EUのAI規制に向けた検討の系譜において、ターニングポイントとなったのは、2018年の「AI、ロボット、自律型システムに関するステートメント」であると考えられます。今後のAI規制の方向を決める上で重要な文書であったと位置づけられます。最終的には「AI白書」でかなり具体的な内容が示されていますが、ステートメントで示されたものがAI整合規則の策定につながっていることがわかります。ステートメントで最初に示されているのが、安全性、セキュリティ、危害の防止です。次に、人間の道徳的責任。さらに3つ目にガバナンス、テスト・認証に関する問題が示されています。この点からも、2018年の段階でEUが目指していたのはAIシステムの安全性を確保するための製品安全規制の整備であったことがうかがえます。そのためのガバナンス・法執行、そして第三者認証制度の構築という、実に見事な仕組みを考えたなと思います。

本日は、慶應義塾大学の新保から、EUのAI整合規則提案 -新たなAI規制戦略の構造・意図とブリュッセル効果の威力-についてお話をさせていただきました。

＝＝

本稿は2021年7月11日(日) 〜 22日(木)に開催された第5回情報法制シンポジウムでの講演を基に作成したものです。（本報告は、JSTムーンショット型研究開発事業(JPMJMS2011)の支援を受けたものである。）

情報法制研究所　参与
慶應義塾大学　教授

新保 史生（しんぽ　ふみお）

慶應義塾大学総合政策学部教授　博士（法学）。専門は、憲法、情報法、ロボット法。

専門は、憲法、情報法、ロボット法。個人情報保護委員会専門委員、情報法制学会代表、憲法学会常務理事、情報通信学会副会長、法とコンピュータ学会理事、情報ネットワーク法学会「ロボット法研究会」主査。総務省情報通信政策研究所特別研究員、経済協力開発機構（OECD）デジタル経済セキュリティ・プライバシー部会（SPDE）副議長(2009-2016)、Northeastern University School of Law(CLIC)訪問講師。