2026年3月25日
日機連Webセミナー

欧州機械規則の要点と対策

三菱電機　知的財産センター
神余浩夫

JMF 一般社団法人 日本機械工業連合会

©Japan Machinery Federation 禁無断転載

講演の狙い

● 狙い・目的

- 欧州は、デジタル製品に関するサイバーセキュリティやAI安全等の規制を世界に先駆けて打ち出した。これらの規制は輸出業者だけでなく、国内サプライチェーンへの影響を与えるため、欧州に直接関係ない業者も無視できない。
- 本講演は、欧州デジタル製品安全規制の概要（機械規則、サイバーレジリエンス法、ネットワーク情報セキュリティ指令、AI法等)と、その技術要件である標準化の状況について解説する。

● 到達目標

- 本セミナーにより、自社製品の対応方法について検討を始められるようにする。

● 対象者

- 欧州規制、規格の初心者＝設計、品証、営業、調達、規格等に関わる者

©Japan Machinery Federation 禁無断転載

講師略歴

●神余　浩夫（かなまる　ひろお）

1987 大阪大学大学院工学研究科原子力工学修士課程修了

1987 三菱電機中央研究所→産業システム研究所→先端技術総合研究所

- プラント制御システム、制御ネットワーク、安全システムなどの研究・開発に従事

2004 三菱電機名古屋製作所

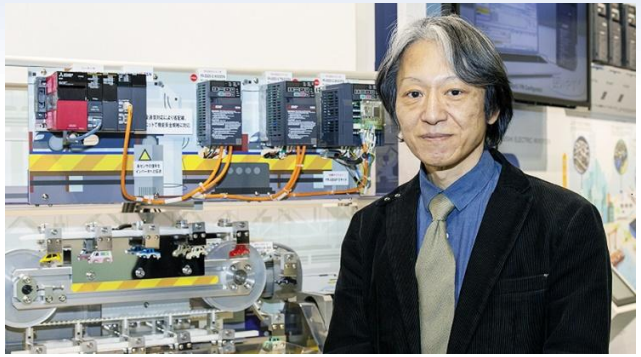
- 安全シーケンサMELSEC Safety, CC-Link Safetyの開発に従事

2011 三菱電機先端技術総合研究所

- 機能安全システム、OTセキュリティの研究・開発に従事

2023 知的財産センター

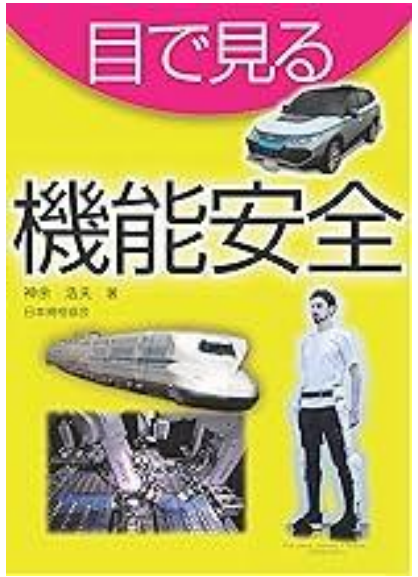
- 標準化・標準活用・普及に貢献



https://www.mitsubishielectric.co.jp/fa/the-art-of-manufacturing/column/the-inside-view04/index.html

●資格・委員

- TUV-Rheinland/SUD機能安全エキスパート(FSexp)
- 計測自動制御学会(SICE)国際標準化委員長、ISA日本支部長
- IEC 61508, IEC 62443, ISO/IEC TS 63069他の開発メンバ
- CENELEC/TC65X オブザーバ
- 著書：目で見る機能安全（日本規格協会、2017）



https://amzn.asia/d/0zxaF2z

©Japan Machinery Federation 禁無断転載

目次

©Japan Machinery Federation 禁無断転載

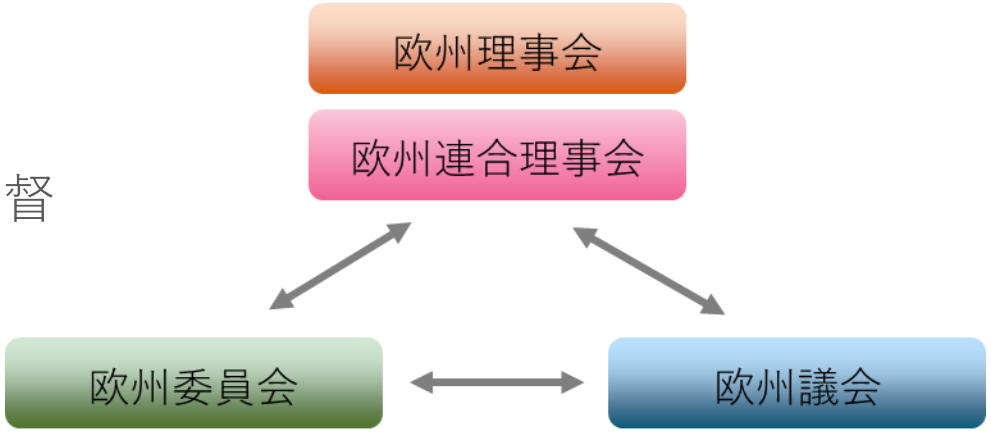
欧州法令の基礎知識

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

EUの主要機関

- 欧州理事会（European Council）
  - 加盟国の元首・首脳と欧州委員会委員長、欧州理事会議長で構成され、EU全体の政治指針を決定する
- 欧州連合理事会（Council of the European Union）
  - 欧州議会と立法機能/予算権限を共有し、安全保障政策と経済政策調整で中核的な役割を担う
- 欧州議会（European Parliament）
  - 欧州連合理事会と並ぶ、EUの主たる決定機関である。各委員会で討議された法案等についての報告書が審議されるほか、決議・勧告等が採択される。
- 欧州委員会（European Commission）
  - EUの執行・政策決定機関としての機能を担う。
    - EUの政策・法案の提案
    - EU法（条約、条約の規定に基づく決定等）の適用の監督
    - EUの行政・執行機関として機能
    - 競争法分野における立法



著者オリジナル

©Japan Machinery Federation 禁無断転載

EU法の種類

- 規則（Regulation/Act）
  - すべての加盟国を拘束し、直接適用性（採択されると加盟国内の批准手続を経ずに、そのまま国内法体系の一部となる）を有する。
- 指令（Directive）
  - 指令の中で命じられた結果についてのみ、加盟国を拘束し、それを達成するための手段と方法は加盟国に任される。
  - 指令の国内法制化は、既存の法律がない場合、新たに国内法を制定、追加、修正する。
  - 加盟国の法の範囲内で、指令内容を達成できる場合には、措置をとる必要はない。加盟国の既存の法体系に適合した法制定が可能になる半面、規則に比べて履行確保が複雑・困難になる。
- 決定（Decision）
  - 特定の加盟国、企業、個人に対象を限定し、限定された対象に対しては直接に効力を有する。
- 勧告・意見（Recommendation/Opinion）
  - 欧州連合理事会及び欧州議会が行う見解表明で、通常は欧州委員会が原案を提案するもので、規則/司令等とは異なり法的拘束力を持たない。

©Japan Machinery Federation 禁無断転載

関連組織

- CEN（European Committee for Standardization）
  - 欧州標準化委員会
    - 電気・通信を除く分野（機械、建設、消費財、食品など）を対象に、欧州規格（EN）を策定
- CENELEC（European Committee for Electrotechnical Standardization）
  - 欧州電気標準化委員会
    - 電気・電子技術分野に関する標準を担当し、電気安全・相互運用性を確保するENを策定
- ETSI（European Telecommunications Standards Institute）
  - 欧州電気通信標準化機構
    - 電気通信・ICT分野の標準化機関で、5G、IoT、サイバーセキュリティなどの技術標準を開発
- DG CONNECT（Directorate-General for Communications Networks, Content and Technology）
  - 欧州委員会 通信・ネットワーク・コンテンツ・技術総局
    - 欧州委員会の部局
    - デジタル政策・通信・ICT・AIを担当、デジタル単一市場、通信規制、サイバー政策の立案・執行
- ENISA（European Union Agency for Cybersecurity）
  - 欧州連合サイバーセキュリティ機関
    - EUのサイバーセキュリティ専門機関
    - リスク評価、インシデント対応支援、NIS指令やサイバーレジリエンス政策を技術面から支援

©Japan Machinery Federation 禁無断転載

CEマーキング

●CEマーキング制度

- 指定の製品がEUの基準（必須要求事項）に適合していることを表示するマーク。
- CEマーキングのある製品は、EU域内の自由な販売・流通が保証される。
  - 該当製品の製造業者（輸入者）または代理の第三者認証機関が所定の適合性評価を行い、製品、包装、添付文書に付与する。
- 必須要求事項：規則・指令によって規定。
  - 詳細な技術要件は、規則・指令ごとの整合規格(Harmonised standards)を参照
  - 指令：機械指令、低電圧指令、EMC指令、RoHS指令

●適合性評価・適合宣言

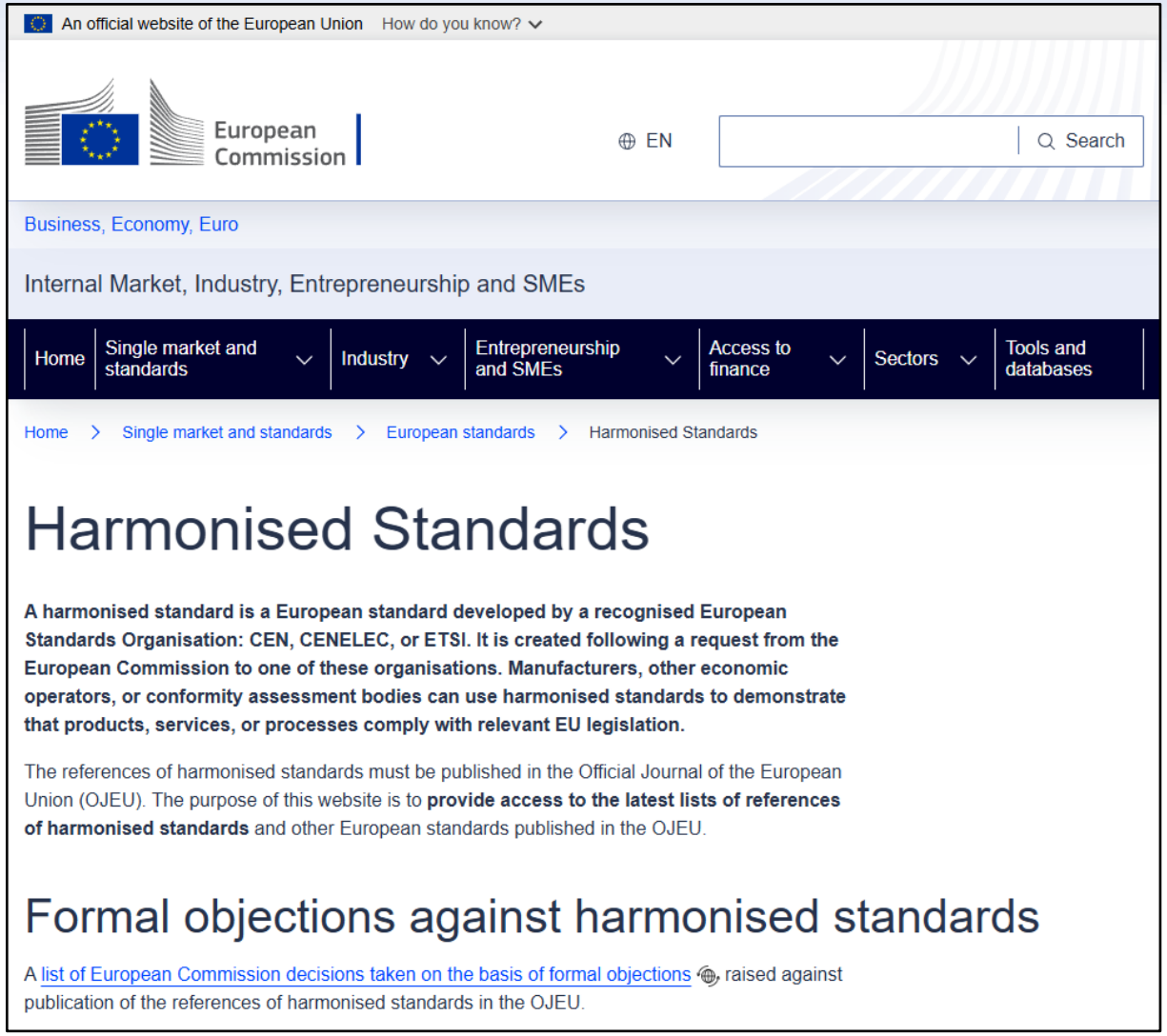
- 特定の製品については、認定を受けた第三者認証機関(Notified Body)の認証が必要
  - ほとんどの製品は、製造業者（輸入者）による自己宣言(Declaration)。
    輸入業者が代理人(Authorised Representative)になってもよい。
- 企業は自社製品が安全基準を満たしていることを証明する義務を負う。

CEマーキングの例

©Japan Machinery Federation 禁無断転載

整合規格(Harmonised Standards)

- 整合規格
  - 公認の欧州標準化機構 (CEN、CENELEC、または ETSI) によって開発された欧州規格
    - 欧州委員会からこれらの組織に要請された後に規格の作成が始まる。
  - 製造業者、その他の経済事業者、または適合性評価機関は、整合規格を使用して、製品等が関連する EU 法に準拠していることを証明できる。
    - 全ての技術要件を法令で規定していては、技術革新に追いつけない
  - 指令や規則は、参照する整合規格をEU官報(OJEU)に掲載する。
    - 指令や規則ごとに整理されている（右図）
    - 常に、最新動向を把握しておくこと



https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en

©Japan Machinery Federation 禁無断転載

Digital Europeと関連法令

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

Digital Europe プログラム

- Digital Europeプログラム
  - 企業、国民、行政機関にデジタル技術を導入することに重点をおいたEUの資金提供プログラム。
    - スーパーコンピューティング、人工知能、サイバーセキュリティ、高度なデジタルスキルといった主要な能力分野におけるプロジェクトを支援し、経済と社会全体におけるデジタル技術の幅広い活用の確保を目指す。
    - 総予算：81億€　→関連プログラム(Cybersecurity等)の報告書（右）
  - 重点課題
    - 人工知能 (AI) の推進
    - サイバーセキュリティとレジリエンスの強化
    - 欧州デジタルイノベーションハブ (EDIHs) の強化
    - 高度なデジタルスキルと教育
    - デジタルインフラの展開と活用
    - データ空間の構築
- 関連法令の整備
  - NIS2, GPDR, CRA, AIA, etc.

https://cybersecurity-centre.europa.eu/document/8af166e1-69c5-4ccd-b38f-5a3ffe43ad73_en

©Japan Machinery Federation 禁無断転載

サイバーセキュリティ政策-NIS/NIS2

- 目的
  - EU加盟国全体のサイバーセキュリティレベルの向上
  - 重要インフラのサイバー攻撃に対する防御力強化
  - EU域内におけるサイバーセキュリティ対策の調和
- Network and Information Security Directive: NIS指令 (2016/8月施行)
  - 加盟各国に、関連のリスクやインシデントに対応する機関の設立を義務付ける。
    - リスクとインシデントに関する情報共有及び協力を促進。
    - 基幹インフラ事業者（金融、運輸、電力、保険・衛生）、デジタル・サービス提供者（オンライン市場、クラウド・コンピューティング、検索エンジン）には、適切なセキュリティ対策を講じるとともに、重大インシデントに関する報告を義務付ける。
- NIS2指令（2022/2555）(2023/1/16施行)
  - 同指令の対象すべての分野におけるリスク管理対策及び報告要件の基準を設定。
  - NIS2は、指定された産業分野におけるすべての中規模及び大規模事業者と対象を大幅に拡大。
  - 対象事業者は、サイバーセキュリティ対策の見直しと強化が必須。
  - 罰則：主要事業体の場合、最高1,000万ユーロ、または全世界年間総売上高の2%。重要事業体の場合、最高700万ユーロ、または全世界年間総売上高の1.4%

©Japan Machinery Federation 禁無断転載

EU一般データ保護規則GDPR

- GDPR (General Data Protection Regulation)、(EU)2016/679、2018/5/25/施行
  - 目的
    - EU域内における個人データ保護に関する規則
    - 個人データの処理にかかる個人の権利と自由を保護すること、およびEU域内の規則を統合することによって、国際的なビジネスのための規制環境を簡潔にすること。
  - 内容
    - 適用範囲の拡大：EU域内に居住する個人の個人データを扱う全ての企業や組織（EU域内外）に適用。→EUに拠点のない日本企業も対象になりうる。
    - 個人の権利強化：個人が自身の個人データにアクセス、修正、削除、およびデータポータビリティを要求する権利の強化。
    - 企業の義務強化：企業は、個人データの取り扱いに関する透明性を確保し、データ保護責任者の設置やデータ保護影響評価を実施する。
  - 罰則：最大、全世界年間売上高4%、または2,000万ユーロ
  - 整合規格：未発表
    - ISO/IEC 27001等の情報セキュリティ規格が候補

©Japan Machinery Federation 禁無断転載

データガバナンス法DGA、データ法DA

- データガバナンス法 (Data Governance Act, (EU) 2022/868)、2023/9/24施行
  - EUにおけるデータ共有を促進し、データ経済の発展を目指すための法律
  - データ共有を促進するプロセスと構造を規制
- 目的
  - 公共部門が保有するデータの再利用を促進
  - データ仲介サービスを規制し、データ共有の透明性と公平性を確保
  - データ利他主義を促進し、社会的課題解決に貢献
- 内容
  - 公共部門が保有するデータの再利用、データ仲介サービス、データ利他主義をカバー
  - データ共有に関する共通のルールを定め、EU域内におけるデータの自由な流通を促進
  - データ共有における信頼性を確保するため、データ仲介サービスやデータ利他主義組織に対する規制

- Data Act (The Regulation on harmonised rules on fair access to and use of data、2022/868), 2024/1/11施行
  - データに活用ための包括的なイニシアチブであり、個人データの保護を確保しながら、公正なアクセスとユーザーの権利を確保
  - 誰がどんな条件でデータから価値を創造できるか
- 内容
  - IoT製品の利用者は、生成されたデータへのアクセス権を持ち、第三者とデータを共有する権利を持つ
  - 公的機関へのデータ提供の義務付け
  - IoT製品は、デフォルトでデータアクセスが可能な設計。製品データは、一般的に使用可能で機械読み取り可能なフォーマットで提供
  - クラウドサービスやエッジサービスの利用者は、サービスを他社に切り替える権利を持つ

2つの法律を組み合わせることで、データへの信頼性と安全性の高いアクセスが促進される

©Japan Machinery Federation 禁無断転載

機械規則
Machinery Regulation

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

機械指令(MD)から機械規則(MR)へ

- 機械指令(Machinery Directive, MD 2006/42/EC)、2012/12月施行
  - EU市場における機械類の安全性と自由流通を確保するために制定。
  - すべての機械は本法の要件を満たし、CEマーキングをつける（一部の機械は第三者認証）。
  - 新しい技術への対応が急務となってきた
    - AI、IoTやサイバーセキュリティへの対応
    - 協働ロボットや遠隔操作機械などハイリスク機械への対応
    - マニュアルや技術文書のデジタル化、ソフトウェアのアップデート等
  - EU市場における調和、他の法令との整合
- 機械規則(Machinery Regulation, MR (EU)2023/1230)
  - 上記の技術課題を考慮して2023年7月19日発効、2027年1月19日施行(MDを置換)
  - 目的
    - 健康、安全、環境の保護
    - 技術革新への対応、ハイリスク機械
    - 透明性と信頼性の向上、自由な流通

https://www.mitsubishielectric.co.jp/fa/products/rbt/assista/assets/img/assista_top.png

29.6.2023 EN Official Journal of the European Union L 165/1

REGULATION (EU) 2023/1230 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 June 2023

on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

https://eur-lex.europa.eu/eli/reg/2023/1230/oj/eng

©Japan Machinery Federation 禁無断転載

MRの構成

第1条 目的
第2条 範囲、部分機械にも適用
第3条 定義
第4条 市場行動の自由
第5条 加盟国による要件の追加
第6条 適合性評価の要求(付属書Ⅰ)
第7条 付属書Ⅱ安全コンポーネント
第8条 機械を市場投入できる条件
第9条 整合法令
第10条 製造業者の義務
第11条 部分機械に対する要求
第12条 権限ある代表者
第13条 輸入者の責務
第14条 機械部分の輸入者の責務
第15条 販売業者の注意点
第16条 機械部分の販売業者の注意点
第17条 輸入業者または販売業者の義務
第18条 機械の改造者の責務
第19条 経済事業者の情報提供
第20条 欧州委員会の職務
第21条 EU適合宣言書
第22条 EU組込宣言書
第23-24条　CEマーキング
第25条 適合性評価手順
第26-40条　認証機関、適合性評価機関
第41-42条　委員会
第43条1 市場監視当局の措置
第44条 加盟国の暫定措置が違法
第45条 経済事業者の是正措置の責務
第46条 経済事業者への不適合是正要求
第47条 委任法の権限
第48条 委員会の支援
第49条 守秘義務、情報の非開示
第50条 罰則事項
第51-54条　補則

付属書Ⅰ 高リスク機械製品のカテゴリ
付属書Ⅱ 部分的機械類の組込宣言
付属書Ⅲ 健康および安全に関する必須要求事項 (EHSR)
付属書Ⅳ 製造者が作成すべき技術文書
付属書Ⅴ EU適合宣言書
付属書Ⅵ 内部生産管理による適合性評価（Module A）
付属書Ⅶ EU型式試験（Module B）
付属書Ⅷ 型式への適合（Module C）
付属書Ⅸ 完全品質保証による適合（Module H）
付属書Ⅹ 適合性評価のユニット検証（Module G）
付属書Ⅺ 部分的機械類の技術文書
付属書Ⅻ 相関表（MD 2006/42/EC対応）

©Japan Machinery Federation 禁無断転載

対象となる機械（付属書Ⅰ）

付属書ⅠA=第25条(2)に従って適合性評価

1. ガードを含む取り外し可能な機械式伝達装置
2. 取り外し可能な機械式伝達装置用のガード
3. 車両整備用リフト
4. ポータブルカートリッジ操作の固定およびその他の衝撃機械
5. 機械学習アプローチを使用して完全または部分的に自己進化する動作を備えた安全コンポーネントにより、安全機能が保証される。
6. 機械学習アプローチを使用して完全または部分的に自己進化する動作を行う組み込みシステムを備えた機械は、それらのシステムのみに関して、市場に独立して配置されていない安全機能を確保する。

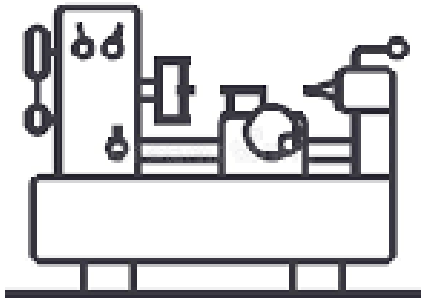
付属書ⅠB=第25条(3)に従って適合性評価

1. 丸鋸（単刃または多刃）
2. 木工用手送り式表面計画機
3. 機械送り装置を内蔵し、木工用に手動でロードおよび/またはアンロードできる片面ドレッシング用のシックナー
4. 手動ローディング機能付きバンドソーおよび/または以下の種類の木材および同様の物理的特性を持つ材料の作業のための荷降ろし:
5. 同様の物理的特性を持つ木材および材料を加工するための複合機械
6. 木工用のいくつかのツールホルダーを備えた手送りほぞ切り機械
7. 木材および同様の物理的特性を持つ材料を加工するための手送り垂直スピンドル成形機
8. 木工用ポータブルチェーンソー
9. 手動でロードおよび/またはアンロードする、金属の冷間加工用のプレスブレーキを含むプレス
10. 手動でロードまたはアンロードする射出または圧縮プラスチック成形機
11. 手動ロードまたはアンロードを備えた射出または圧縮ゴム成形機
12. 地下作業用機械
13. 圧縮機構を組み込んだ家庭ごみ収集用手動積載トラック
14. 垂直高さ3mを超える高さから落下する危険を伴う、人または人および物品を持ち上げるための装置
15. 人の存在を検出するように設計された保護装置
16. 機械の安全装置として使用するように設計された動力作動の連動可動ガード
17. 安全機能を確保するためのロジックユニット
18. 転倒防止構造（ROPS）
19. 落下物保護構造物（FOPS）

©Japan Machinery Federation 禁無断転載

製造業者の義務（第10条）

第10条1 全体：製品は付属書IIIの健康と安全要件を満たすこと
第10条2 出荷時の義務：付属書IV-Aの技術文書、EU適合宣言書とCEマーキング
第10条3 技術文書を10年間保管：ソースコードとプログラムロジックを含む
第10条4 手順の整備：規則に準拠する手順が整備されていることの確認
　　第20条（仕様変更）への適合。市場製品の試験、リコール対応、販売会社への通知
第10条5 名板表示：製品に名板が取り付けられない場合は、パッケージや文書にて提供
第10条6 機械に表示する情報：Webアドレス、デジタル連絡先を含む
第10条7 機械に、付属書IIIの情報が添付されていること。デジタルでも可
　　購入時に紙情報を1か月以内に入手できること。オンライン情報は10年間入手できること。非専門家には紙情報を提供。
第10条8 デジタルEU適合宣言：使用開始後10年間アクセス可能
第10条9 製造業者の是正措置：本規則に適合できない場合、適合性の撤回、リコール等
第10条10 情報提供：適合証明のすべての情報をデジタル形式で提供。当局への協力



©Japan Machinery Federation 禁無断転載

部分機械にも適用（第11条）

- 完成機械だけでなく部分機械も対象

  第1条 この規則は、人々の健康と安全を高レベルで保護しながら、機械、関連製品、および部分的に完成した機械の設計と製造に対する健康と安全の要件を定め、それらを市場で入手または使用できるようにする

  第2条 この規則は、部分的に完成した機械にも適用される

  第11条 部分機械に対する要求(付属書III参照)

  第11条1 付属書IV-Bの技術文書の作成、第11条の2 文書（ソースコード含む）の10年保管

  第11条5,6 部分機械の名板表示、記載内容（デジタル連絡先）

- EU組込宣言書(EU declaration of incorporation)

  第22条1 部分機械のEU組込宣言書の目的＝付属書IIIの要件を満足している

  第22条2 EU組込宣言書は付属書IV-Bに従う、市場で入手可能

  第22条3 関連法への適合について宣言、第22条4 製造者の責任

©Japan Machinery Federation 禁無断転載

デジタル情報

第10条5

- 製造事業者は、その上市又は使用開始する機械類又は関連製品に、少なくとも機械類又は関連製品の型式、シリー ズ又は型式、製造年、すなわち製造工程が完了した年、及びバッチ番号若しくはシリアル番号又はその識別を可能にするその他の要素が存在する場合、又は機械類又は関連製品の大きさ若しくは性質上それが不可能な場合、包装上又は機械類又は関連製品に添付する文書に必要な情報を記載することを確実なものとしなければならない。

第10条6

- 製造事業者は、その名称、登録商標又は登録商標、並びにその製造事業者に連絡可能な郵送先住所、 ウェブサイト、電子メールアドレス又はその他のデジタル連絡先を、機械若しくは関連製品に、又はそれが 不可能な場合は、その包装又は機械若しくは関連製品に添付する文書に表示しなければならない。

第10条7 使用説明書がデジタル形式で提供される場合、製造事業者は次のことを行う。

A) デジタル説明書へのアクセス方法を機械または関連製品にマークするか、それが不可能な場合はそのパッケージまたは付属文書にマークを付ける。

B) ユーザーがいつでも、特に機械の故障中にアクセスできるように、使用説明書を印刷およびダウンロードして電子機器に保存できる形式で提示すること。または関連製品。

C) 機械または関連製品の予想耐用年数中、および機械または関連製品の市場投入後少なくとも10年間は、オンラインでアクセスできるようにする。

©Japan Machinery Federation 禁無断転載

本質的安全衛生要求 (ESHR: Essential Safety and Health Requirements)

● 本質的安全衛生要求 ESHR

- 機械・関連製品・部分完成機械をEU市場に上市／使用開始するために必ず満たすべき最低限の安全・衛生要求
  - MR Annex III参照
- セキュリティ要件 (Annex III 1.1.9)
  - ソフトウェアの改ざん防止
  - 不正アクセスによる危険動作の防止
  - データの完全性・認証
  - アップデートの安全性確保
- AI・自律動作機械への要求追加 (Annex III 1.1.2他)
  - 自己学習による動作変化のリスク評価
  - 自律制御を含む制御システムの安全性
  - AIを含むソフトウェア更新の管理
- デジタルマニュアル (Annex III 1.7.4)
  - デジタル提供が可能．望めば紙も
- リスクアセスメントの範囲拡大 (Annex III 1.1.2)
  - サイバー攻撃リスク
  - AIによる動作変化リスク
  - ソフトウェア更新のライフサイクルリスク
- 技術文書(Technical File)の要求強化 (Annex III 1.7.4, Annex IV)
  - サイバーセキュリティ対策の記述
  - AIアルゴリズムの概要
  - ソフトウェア更新管理
  - デジタルマニュアル提供方法
- 高リスク機械の見直し (Annex I)
  - AI搭載協働ロボットなどが追加
  - 多くの機械が「Part B」に分類され、自己宣言が可能に

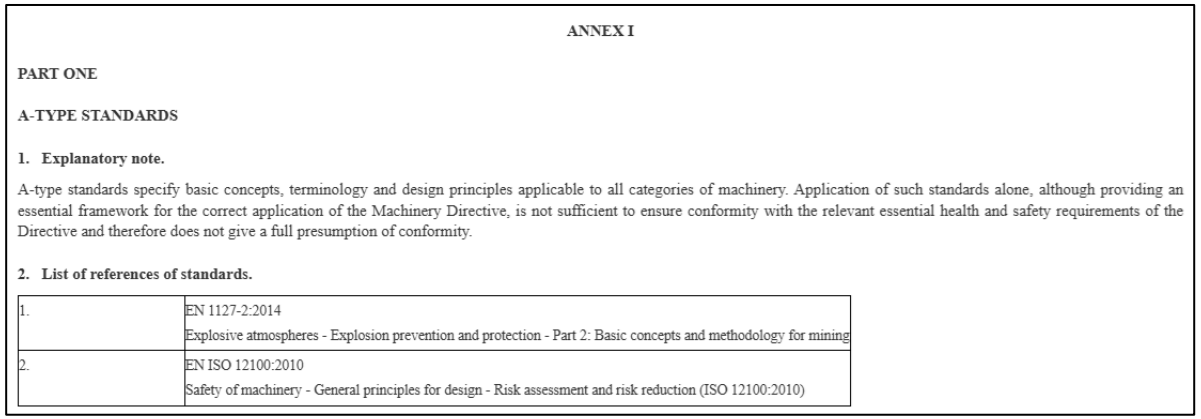
©Japan Machinery Federation 禁無断転載

MRの整合規格

- 未発表＝MDの整合規格を継承、追加（予想）
  - COMMISSION IMPLEMENTING DECISION (EU) 2023/1586 of 26 July 2023 on harmonised standards for machinery drafted in support of Directive 2006/42/EC of the European Parliament and of the Council

- Annex Ⅰ
  - A-Type（基本安全規格）：2本
    - EN 1127-2:2014爆発的な雰囲気　爆発防止と保護　マイニングの基本概念と方法論
    - EN ISO 12100:2010機械の安全性 -設計の一般原則 -リスク評価とリスク低減
  - B-Type(グループ安全規格)：105本
    - EN ISO 13849-1:2015 機械類の安全性 -制御システムの安全関連部 -第1部：設計のための一般原則
    - EN 61800-5-2:2007可変速駆動システム（PDS） － 第5-2部：安全要求事項 －機能
    - EN IEC 62061:2021 機械類の安全性-安全関連制御システムの機能安全

    など
  - C-Type（個別安全規格）：700本
    - 多種多様
- Annex Ⅱ,Ⅲ
  - 撤廃した指令の整合規格を継続



ANNEX I

PART ONE

A-TYPE STANDARDS

1. Explanatory note.

A-type standards specify basic concepts, terminology and design principles applicable to all categories of machinery. Application of such standards alone, although providing an essential framework for the correct application of the Machinery Directive, is not sufficient to ensure conformity with the relevant essential health and safety requirements of the Directive and therefore does not give a full presumption of conformity.

2. List of references of standards.

1.	EN 1127-2:2014 Explosive atmospheres - Explosion prevention and protection - Part 2: Basic concepts and methodology for mining
2.	EN ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010)

https://eur-lex.europa.eu/eli/dec_impl/2023/1586/oj

©Japan Machinery Federation 禁無断転載

整合規格-ISO 12100

- ISO/DIS 12100 改訂作業中
  - 1.Scopeの追加
    - この文書では、AI機械学習の実装における機械の安全性に関する主な影響と、安全性への影響に関するサイバーセキュリティ攻撃/不正行為に対する脆弱性について説明する。
  - 用語と定義: サイバーセキュリティを追加
  - 制御システムの要件を 6.3.5に移動　⇒
  - AIの学習行動への参照を 5.4、b) 2) に追加
  - ソフトウェア関連の章・節の全面見直し
  - 6.3.5.15サイバーセキュリティと不正防止の追加
- prEN 50742 Safety of machinery – Protection against corruption
  - 目的：機械がサイバー攻撃を受けた場合の影響を最小限に抑える
    - 改ざんに対する保護や制御システムの安全性に関する具体的要求

6.3.5 Design of control systems
6.3.5.1 General
6.3.5.2 Starting of an internal power source or switching on an external power supply
6.3.5.3 Starting or stopping of a mechanism
6.3.5.4 Restart after power interruption
6.3.5.5 Interruption of power supply
6.3.5.6 Failure of the power supply or communication network connection
6.3.5.7 Safety functions implemented by programmable electronic control systems
6.3.5.8 Minimizing probability of failure of safety functions
6.3.5.9 Selection of control and operating modes
6.3.5.10 Principles relating to manual control
6.3.5.11 Control mode for setting, teaching, process changeover, fault-finding, cleaning or maintenance
6.3.5.12 Applying measures to achieve electromagnetic compatibility (EMC) compatibility, see IEC 60204-1 and IEC 61000-6.
6.3.5.13 Use of automatic monitoring
6.3.5.14 Provision of diagnostic systems to aid fault-finding
6.3.5.15 Cybersecurity and protection against corruption

©Japan Machinery Federation 禁無断転載

サイバーレジリエンス法
Cyber Resilience Act

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

サイバーレジリエンス法CRA

● サイバーレジリエンス法CRA（Cyber Resilience Act, 2024/2847）

- コネクテッド製品（スマートフォン、コンピューター、IoTデバイス、産業用制御システムなどソフトウェアも含む）のサイバーセキュリティを強化するための規則。
- 2024/12/10発効、2026/9/11：インシデント報告義務化、2027/12/11：全面施行

• 目的

- EU市場製品のサイバーセキュリティレベルを向上させ、消費者や企業をサイバー脅威から保護

• 内容

- 製造業者の義務：
  - 製造業者は、製品の設計・開発段階からサイバーセキュリティを考慮し、既知の脆弱性がない状態で製品を市場に投入する。
  - 製品はCRAが定めた必須セキュリティ要件を満たす。
  - 製造業者は、製品の脆弱性を発見した場合、速やかにユーザーに通知し、適切な修正プログラムを提供する義務を負う。
  - 製造業者は、製品がCRA要件を満たしている適合宣言を行う。リスクの高い製品については、第三者認証機関による評価
- 罰則:最大で全世界年間売上高の5%、または500万ユーロ。

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

©Japan Machinery Federation 禁無断転載

サイバーレジリエンス法CRA

©Japan Machinery Federation 禁無断転載

付録III　デジタル要素を備えた重要な製品

■ Class I

1. 認証およびアクセス制御リーダーを含む、個人管理システムおよび特権アクセス管理SWとHW
2. スタンドアロンブラウザと組み込みブラウザ
3. パスワードマネージャー
4. 悪意のあるSWを検索、削除、または隔離するSW
5. 仮想プライベートネットワーク(VPN)機能を備えたデジタル要素を備えた製品
6. ネットワーク管理システム
7. セキュリティ情報およびイベント管理(SIEM)システム
8. ブートマネージャー
9. 公開鍵インフラストラクチャおよびデジタル証明書発行SW
10. 物理および仮想ネットワークインターフェース
11. オペレーティングシステム
12. インターネット接続用のルーター、モデム、スイッチ
13. セキュリティ関連機能を備えたマイクロプロセッサ
14. セキュリティ関連機能を備えたマイクロコントローラ
15. セキュリティ関連機能を備えた特定用途向けASICおよびFPGA
16. スマートホームの汎用仮想アシスタント
17. スマートドアロック、セキュリティカメラ、ベビーモニタリングシステム、警報システムなどのセキュリティ機能を備えたスマートホーム製品
18. 指令2009/48/ECの対象となるインターネット接続玩具で、社会的対話機能（例えば、会話や撮影）や位置追跡機能を備えているもの
19. 健康モニタリング（追跡など）の目的があり、規則(EU)2017/745または(EU)2017/746が適用されない、人体に着用または装着される個人用ウェアラブル製品、または子供が使用することを意図した個人用ウェアラブル製品

■ Class II

1. オペレーティングシステムや同様の環境の仮想実行をサポートするハイパーバイザーとコンテナランタイムシステム
2. ファイアウォール、侵入検知および防止システム
3. 改ざん防止マイクロプロセッサ
4. 改ざん防止マイクロコントローラ

■ 付属書IV　デジタル要素を備えた重要な製品

1. セキュリティボックス付きハードウェアデバイス
2. 指令(EU)2019/944 第2条に定義されるスマートメーターシステム内のスマートメーターゲートウェイ、及び安全な暗号処理を含む高度なセキュリティ目的のためのその他のデバイス
3. スマートカードまたは類似のデバイス（セキュアエレメントを含む）

©Japan Machinery Federation 禁無断転載

製造業者の義務（第10条）

① デジタル製品を市場に出す際、附属書Iの1「セキュリティ特性要件」を遵守して設計・開発・製造されていることを確認する。

② サイバーセキュリティ上のリスクアセスメントを実施し、その結果を設計・開発・製造・配送・メンテナンスの際の考慮に入れる。

③ デジタル製品を市場に出する際、上記のリスクアセスメントの結果を技術文書に含める。

④ 第三者から提供された部品を使用する際には、その部品により製品のセキュリティリスクを高めないことを保証する。

⑤ リスクに比例した方法でデジタル製品に関するサイバーセキュリティ側面を体系的に文書化する。

⑥ 上市後5年間または製品寿命のうち短い期間の間、脆弱性に効果的に対処する。製造業者は脆弱性開示ポリシー等、適切なポリシーや手続きを有する。

⑦ 上市前に製造業者は技術文書を作成する。対応する適合性評価手続きを行い、適合性が実証された場合はCEマーキングを貼付する。

⑧ 上市後10年間、技術文書と（該当する場合は）EU適合性証明書を市場監視当局が自由に使えるように保管する。

⑨ 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。

⑩ 附属書IIに規定される情報が製品に付属されていることを確認する。

⑪ EU適合性証明書を提供するか、その情報を記載したURLを提供する。

⑫ 上市後5年間または製品寿命のうち短い期間の間、附属書Iの1「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ、製品の撤回またはリコールを行う。

⑬ 市場監視当局からの要求に応じて製品の適合性を証明する情報・文書を提出する。

⑭ 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。

⑮ （欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。）

©Japan Machinery Federation 禁無断転載

整合規格と認証制度

- 整合規格の動向=開発中
  - CENELEC/JTC13 サイバーセキュリティとデータ保護
    - ISO/IEC JTC1/SC27 Securityとの連携（情報セキュリティ、プライバシー保護）
    - EN 40000sr – サイバーレジリエンスの基本規格
  - CENELEC/TC65X 産業オートメーション
    - OT(Operational Technology)セキュリティ＝IEC 62443シリーズのEN化
    - OTセキュリティの製品・分野規格の開発
  - CENELEC/TC47X 半導体と高信頼チップ
    - 組込システム向けの高信頼（セキュア）な半導体デバイス
- 認証制度
  - ENISA EUCC Certification Scheme
    - ICT製品のライフサイクルにおける認証方法に関するEU全体の規則と手続き
    - Common Criteriaベース
      - IEC 62443適合性評価（リスクベース）とのギャップ
  - IEC/CAB/IECEE/CMC/WG31 Cybersecurity
    - IEC 62443への適合性評価手順の開発→多くの審査機関が参加

https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en

©Japan Machinery Federation 禁無断転載

IEC 62443産業システムセキュリティ規格

- IEC 62443シリーズは，産業システムセキュリティの全レイヤ/プレイヤーをカバーした国際規格。IECと米国ISAの共同開発。
  - 汎用的な標準･基準として注目，一部事業者の調達要件にもなっている
  - いろいろな分野に適用できる水平規格の開発着手

Horizontal	OT Cybersecurity					
Part 1 General	62443-1-1 Ed1 Concepts & Models	62443-1-2 Terms & Abbs	62443-1-3 Conformance Metrics	TR62443-1-4 Security Lifecycle	TS62443-1-5 Security profiiles	PAS62443-1-6 Ed1 Industrial IoT
Part 2 Policies	62443-2-1 Ed2 Security Program	PAS62443-2-2 Security Protection	TR62443-2-3 Patch Management	62443-2-4 Ed3 Service Providers	Inccident Management?	
Part 3 System	TR62443-3-1 Security Technologies	62443-3-2 Security Risk Assessment	62443-3-3 Requuirements, Security Levels			
Part 4 Compo	62443-4-1 Ed2 Development Lifecycle	62443-4-2 Security Components		Security Lifecycle?		
Part 6 Conformity	62443-6-1 Service Providers (2-4)	TS62443-6-2 Components (4-2)				

太枠：作成中
白字：未審議

©Japan Machinery Federation 禁無断転載

無線機器指令
Radio Equipment Directive

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

無線機器指令RED

- RED(Radio Equipment Directive, 2014/53/EU)　2016/6/13施行
  - EU域内で販売される無線機器に関する安全、EMC（電磁両立性）、無線周波数の効率的な利用などを定める

- 目的
  - EU域内における無線機器の安全性の確保
  - 電磁両立性の確保
  - 無線スペクトルの効率的な利用の確保
  - 単一市場における無線機器の自由な流通の確保
- 無線指令委任法 RED-DA (Delegated Act)(EU) 2023/2444 (2025/8/1施行)
  - サイバーセキュリティに関する委任法がREDに追加され、インターネット接続された無線機器に対するサイバーセキュリティ要件が強化された。
  - 目的：無線機器を介したサイバー攻撃のリスク低減、IoT機器のセキュリティ強化、消費者の保護
- 整合規格
  - EN 18031-1～3:2024 Common security requirements for radio equipment
  - EN 303 645:2024 Cyber Security for Consumer Internet of Things: Baseline Requirements
    - IPAのセキュリティ要件適合評価及びラベリング制度（JC-STAR）でも採用

©Japan Machinery Federation 禁無断転載

セキュリティ要件適合評価及びラベリング制度（JC-STAR）

- セキュリティ要件適合評価及びラベリング制度（JC-STAR）
  - ETSI EN 303 645やNISTIR 8425等の国内外の規格とも調和しつつ、独自に定める適合基準（セキュリティ技術要件）に基づき、IoT製品に対する適合基準への適合性を確認・可視化する、我が国の制度。
  - 「IoT製品に対するセキュリティ適合性評価制度構築方針」(2024年、METI)に基づき構築された制度
  - インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価・可視化することを目的
  - 2025年3月より運用開始
  - 各国制度との相互承認

https://www.ipa.go.jp/security/jc-star/index.html

©Japan Machinery Federation 禁無断転載

人工知能(AI)法
AI Act

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

AI法 AI Act

- AI法 (AI Act, (EU) 2024/1689), 2024/8/1発効
  - AIに関する初の規制法：さまざまな用途で利用できるAIシステムを分析し、ユーザーにもたらすリスクに応じて分類。リスクレベルが異なると、多かれ少なかれ規制が必要になる。
  - 人工知能(AI)システムの開発、配置、使用に関する規則を定め、人間の安全と基本的権利を保護。
  - 段階的に施行。
    - 「許容できないリスク」の禁止：2025/2/2、「高リスク」AIシステムに関する規制：2026/8/2

- 目的
  - 人間の安全と基本的権利の保護
  - AI技術のイノベーション促進
  - EUの競争力強化、安心できるAI市場の創出

EU Artificial Intelligence Act

https://artificialintelligenceact.eu/

- 内容
  - AIシステムをリスクレベルに応じて分類し、規制→高リスクAIシステムに対する厳格な規制
  - 透明性、説明責任、データガバナンスに関する要件
  - 罰金：禁止されたAI利用の場合、最大全世界年間売上高の6%、または300万ユーロ
- 整合規格
  - CENELEC JTC21(AI)が開発中＝JTC1/SC42と連携

©Japan Machinery Federation 禁無断転載

AI法: リスクレベルごとに異なるルール

- 4段階リスクレベル
  - AI法は、AIによるリスクのレベルに応じて、プロバイダーとユーザーの義務を規定
  - 多くの AI システムは最小限のリスクをもたらすが、評価する必要がある

1	**許容不可リスク**	禁止	人々に対する脅威と見なされ、禁止されるシステム（EUの価値観と競合） • 人々または特定の弱い立場にあるグループの認知行動操作 • 社会的スコアリング: 行動、社会経済的地位、または個人的特徴に基づいて人々を分類 • 顔認識などのリアルタイムおよびリモート生体認証識別システム
2	**高リスク**	適合性評価	安全性や基本的権利に悪影響を与える AI システム • EU の製品安全法に該当する製品に使用されている AI システム（おもちゃ、航空、自動車、医療機器、エレベーター等） • EU データベースに登録する必要がある 8 つの特定領域に分類される AI システム
3	**限定リスク**	透明性確保	深刻なリスクはないが、透明性に関する要件を満たす • リスクが限定された AI システムは、ユーザーが情報に基づいた意思決定を行えるよう、最小限の透明性要件に準拠
4	**最小リスク**	無制限	リスクがごくわずか、またはリスクを伴わない

©Japan Machinery Federation 禁無断転載

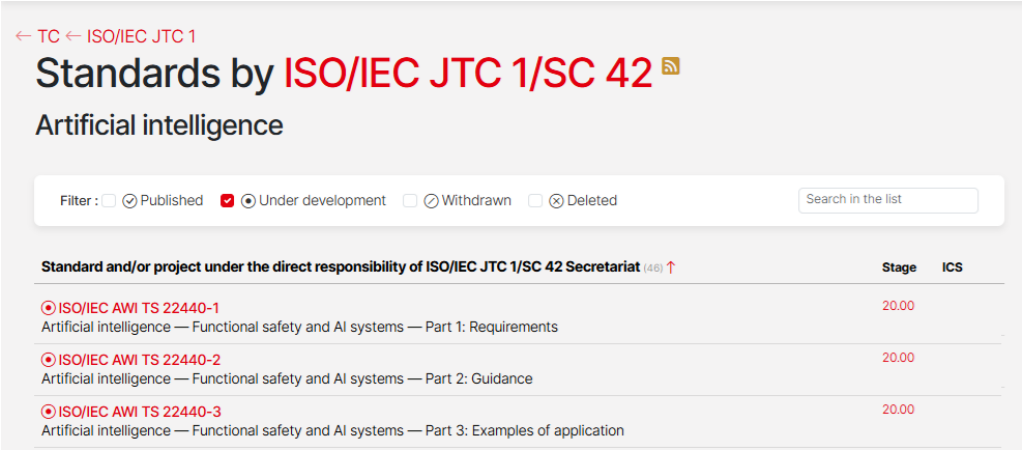
AI法：リスクレベルの要求事項

Risk	利用	要求事項	運用に関する要求事項
許容不可	禁止	－	
高リスク	適合性評価	• リスク管理プロセスを確立(第8条) • 高品質な学習、検証、テストデータの利用(第9条) • 文書化、ログ機能(第10条) • 適切な透明性確保、ユーザへの情報提供(第11,12条) • 人間による監視(第13条) • 堅牢性、正確性、サイバーセキュリティ(第14条) • 当規制の遵守義務(第15条)	[AI提供者の義務(第16条)] • 透明性・説明可能性に関連した義務 • 組織内に品質マネジメントシステムを確立 • 最新の技術文書を作成・更新 • AIの動作を監視するためのログ義務 • EUデータベースにAIシステムを登録 • システムの適合性評価と再評価の実施 • CEマーキングと適合宣言書 • 市場の製品のモニタリング • 市場監視当局と協力 • アクセシビリティ要件に準拠 [AI利用者の義務(第29条)] • 取扱説明書に従って操作 • 人間による監視 • 起こりうるリスクについて運用を監視 • 重大事故・誤動作について関係者に通知 • 既存の法的義務は継続適用(GDPR等)
限定リスク	透明性	• 人とAIシステムの相互作用の通知(第52条1) • 感情認識または生体認証システムの通知(第52条2) • ディープフェイクに対する警告ラベル付け(第52条3)	
最小リスク	無制限	• 必須義務はない。ハイリスクAIに対する要求を実施することを推奨(第69条)	

©Japan Machinery Federation 禁無断転載

整合規格と認証制度

- 標準化（整合規格：未発表）
  - ISO/IEC/JTC1/SC42 AI
    - TR 5469:2023 AIと機能安全 →TS 22440（開発中）
      - IEC61508機能安全のAI応用および、AI技術の安全適用のための条件＝AI技術を安全に使うための条件
      - Part1要求、Part2ガイド、Part3ユースケース→2027年発行予定
    - ISO/IEC 42001:2023 AI Management system
    - ISO/IEC 23894 AI - Guidance on risk management
      など
  - CEN-CENELEC JTC21 AI …EN規格の策定
- 認証制度
  - ETSIが開発中→AIセキュリティに注力したため停滞
  - IECEE/CMC/TF-AI&DTが開発検討開始
    - 状況を注視
  - 日本では、日本情報経済社会推進協会(JIPDEC)がAIMS認定（認証機関を認定）を開始



https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0

©Japan Machinery Federation 禁無断転載

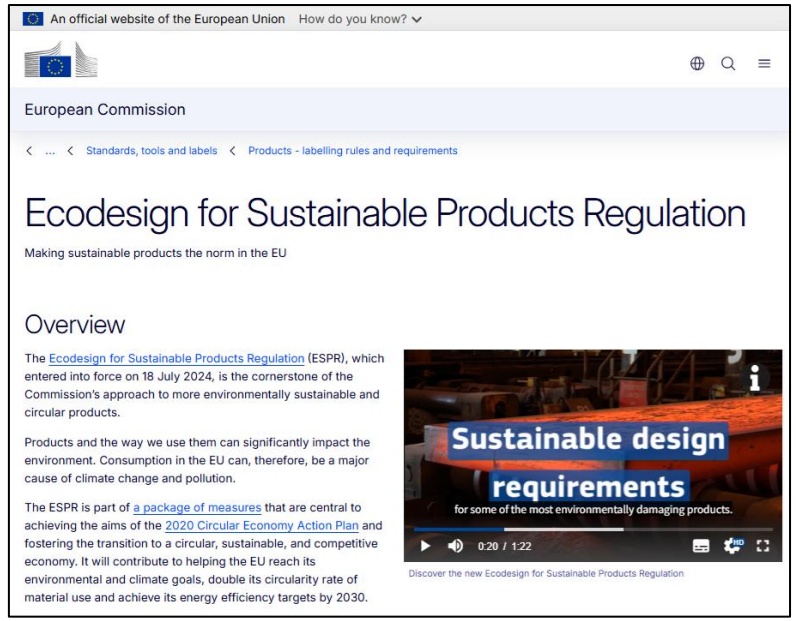
エコデザイン規則
ESPR

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

持続可能な製品のためのエコデザイン規則 ESPR

- エコデザイン規則(Ecodesign for Sustainable Products Regulation: ESPR, 2024/1781), 2024/7/18発効、2026/7/19DPP運用
  - エコデザイン指令をほぼすべての製品（食品、医薬品等を除く）を対象に、強化・拡大
- 目的
  - EU市場に流通する製品の持続可能性を大幅に向上させ、循環型経済への移行を加速する
  - 製品のライフサイクル全体にわたるカーボンフットプリントと環境フットプリントを削減し、持続可能な製品の域内での自由な移動を確保する
- 内容
  - 設定されるエコデザイン要件
    - 耐久性、修理可能性、リサイクル性、えネルギー資源効率、カーボンフットプリントおよび環境フットプリント
  - デジタル製品パスポート（DPP）の導入
  - 売れ残り製品の廃棄抑制（特に衣料品等）
  - グリーン公共調達（GPP）の促進
- 罰則：罰金および公共調達からの排除（第92条 各国規定）
- 整合規格：未定、DPPに関しては別紙



https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/ecodesign-sustainable-products-regulation_en

©Japan Machinery Federation 禁無断転載

デジタルプロダクトパスポートDPP

- DPP(Digital Product Passport)
  - 製品のライフサイクル全体に関する詳細な情報をデジタル形式で記録・管理し、関係者間で共有するための仕組み＝エコデザイン規則ESPRの主要な項目
- 目的
  - 製品ライフサイクル情報の透明化とアクセス性の向上
    - 製品の原材料の調達源、製造プロセス、使用される化学物質、エネルギー・水消費、耐久性、修理方法、リサイクル可能性、カーボンフットプリントなど、製品に関する広範な情報をデジタル形式で一元的に記録・管理し、関係者が必要な情報に容易にアクセスできる
  - 製品の「隠された」環境負荷を可視化し、サプライチェーン全体の透明性を高める
  - 循環型経済への移行の加速、修理と再利用の促進、効率的なリサイクルと資源回収
  - 情報に基づいた意思決定の促進（消費者、企業、規制当局）
- CENELEC/JTC24 – Digital Product Passport – Framework and System
  - WG1:Strategic Advisory Group
  - WG2:Unique identifiers and data carriers
  - WG3:Security
  - WG4:Interoperability framework

©Japan Machinery Federation 禁無断転載

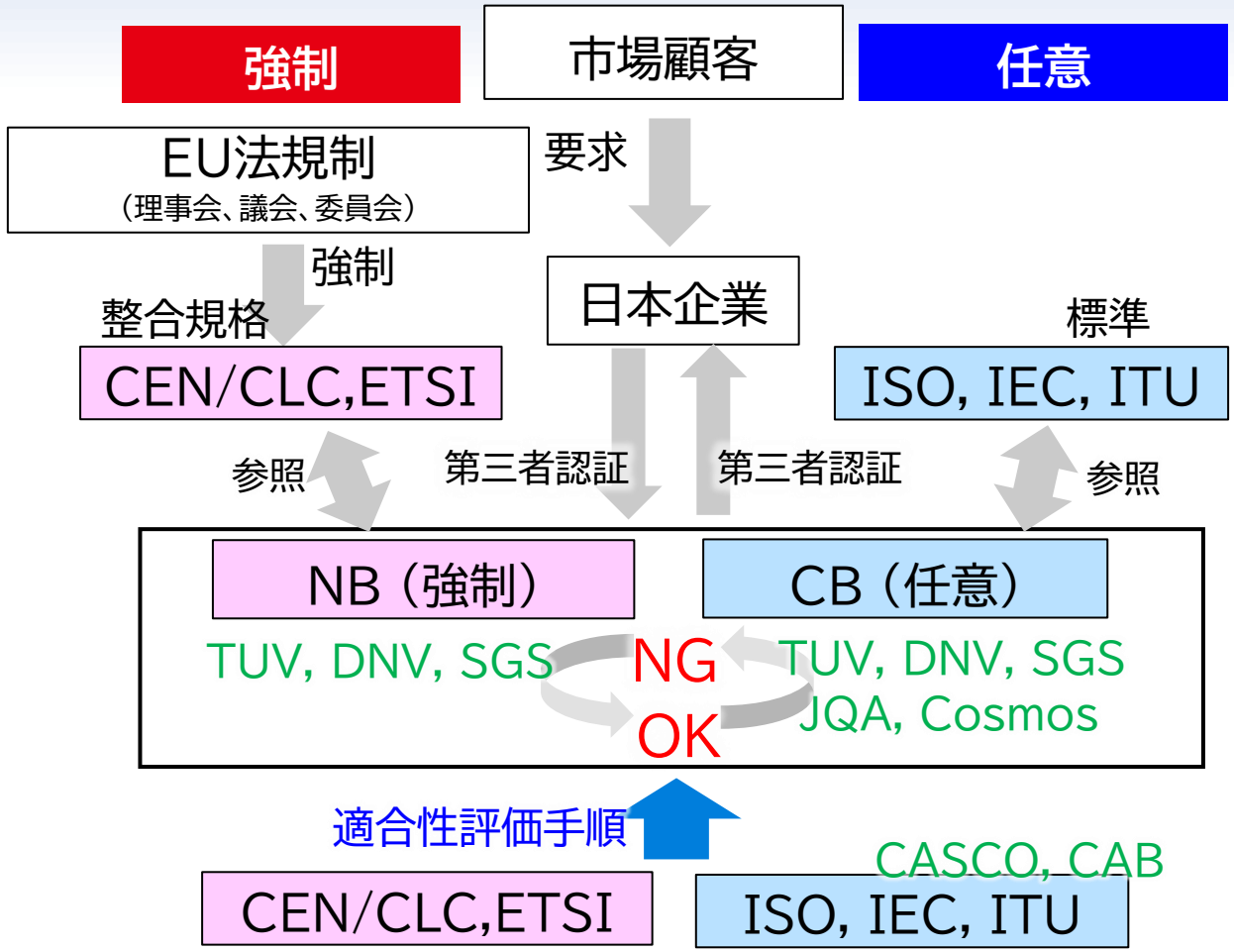
まとめ

欧州機械規則の要点と対策

©Japan Machinery Federation 禁無断転載

デジタルEU関連法制と標準化

- 法令による強制と任意
  - 法令による強制規格、強制認証
    - 指定機関（NB等）による認証手続き
  - 市場による任意の規格適合
    - 民間規格や認証制度も併用
  - 国や制度差が小さいことが望ましい
- 標準と制度の開発
  - デジタル法制は発効・施行済み
    - 2027年施行が多い
  - 整合規格は開発中
    - ETSI/CENELECに作成要請
    - ISO/IECを流用することも多い
  - 認証スキームも既存の手法を利用
    - AIやDXなどこれから



NB: Notified Body, Assesses product compliance with EU regulations
CB: Certification Body, Evaluate quality/environmental management systems based on international standards such as ISO 9001 and ISO 14001

©Japan Machinery Federation 禁無断転載
著者オリジナル

デジタルEU関連法制と標準化

法令	対象製品	整合規格	適合性評価
NIS2 2022/2555	デジタルサービス デジタル機器	未定	未定
DSA 2022/2065 DMA 2022/1925	一般的ITサービス	未定	未定
GPDR 2016/679	個人情報を扱う機器 サービス	なし 技術開発を阻害しないため	第40条：認証メカニズム 現時点で明確な認証スキームはない→既存スキームを利用
CRA 2024/2847	デジタル機器全般 (特に重要な機器)	未定 IEC 62443等(開発中)	第20条：適合性評価の手順 産業分野製品は対象外→NB認証スキームを流用
AIA 2024/1689	AIシステム (特にハイリスク用途)	未定 ISO/IEC 42001等(開発中)	第43条：適合性評価 認証スキームは不明→NB認証スキームを流用
RED 2014/53/EU	無線機器	(EN 303 645) EN 18031-1/-2/-3	ETSI/TS 103 701 Assessment Specification →各国でEN 303 645製品認証が進行している
機械規則(MR) 2023/1230	機械全般、機械部品	未定（MDを継承） ISO 12100他 EN 50742	付属書A記載の機械のみ →MDと同じく欧州NB認証スキーム

2026年3月10日、著者調べ

©Japan Machinery Federation 禁無断転載

Digital Omnibus Package

- デジタルオムニバスパッケージ （2025年11月19日発表）
  - 欧州委員会が推進している、複雑化したデジタル関連規制を整理・簡素化し、企業の負担を軽減するための法改正パッケージ
    - 規制緩和ではなく、ルール同士の矛盾を解消し、手続きをシンプルにする（最適化）ことを目指す
    - 企業のコンプライアンス（法令遵守）コストを少なくとも25%削減することを目指す
    - EU域内企業の競争力を高め、イノベーションを阻害しない環境を整える
  - パッケージの構成:
    - AIオムニバス: AI法の適用延期と運用の柔軟化
    - デジタル法制オムニバス: GDPR、データ法、サイバー規制等の横断的修正
    - データ・ユニオン戦略: AI開発のためのデータアクセス強化
    - ビジネス・ウォレット: 企業のデジタル身分証導入

https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

©Japan Machinery Federation 禁無断転載