ISSN 2432-6089

法と情報雑誌

The Law and Information Magazine

第 10 巻第 2 号（通巻第 63 号・2025 年 2 月）

法と情報研究会　編

本 号 目 次

規則(EU) 2024/2847（サイバー回復力法）
[参考訳]

2025 年 2 月 23 日
明治大学法学部教授
夏 井 高 人

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)（OJ L, 2024/2847, 20.11.2024, p. 1–81）のテキスト（英語版）に基づき，その和訳を試みた。

原文のテキストを入手できるサイトの URL は，下記のとおりである。

https://eur-lex.europa.eu/eli/reg/2024/2847/oj
[2024 年 12 月 20 日確認]

この規則(EU) 2024/2847 の参考訳は，あくまでも原文を読む際の参考として提供しているものであり，個人的な見解としての法解釈の結果を「日本語以外の言語で書かれた文書の日本語による翻訳文」というスタイルを用いて表現した文書の一種である。

規則(EU) 2024/2847（サイバー回復力法）の表題は，Corrigendum（OJ L, 2024/90780, 5.12.2024）によって一部訂正されている。ただし，同じ誤記が含まれている第 66 条及び第 67 条は，この Corrigendum によっては訂正されていないので，明白かつ大きな悪影響をもつ誤記が残存したままである。

http://data.europa.eu/eli/reg/2024/2847/corrigendum/2024-12-05/oj
[2025 年 2 月 9 日確認]

この規則(EU) 2024/2847（サイバー回復力法）の参考訳は，同規則の提案書（2022/0272(COD)）に含まれていた原案の 2023 年 12 月から作業を開始し，その後の修正を踏まえて 2024 年 3 月の時点で暫定的な参考訳を作成し，法と情報研究会の会員限定で配布した後，2024 年 10 月 23 日に採択された正文（Corrigendum による一部訂正後の正文）と比較対照して検討・考察した結果に基づいて作成した。

ちなみに，Eur-lex 上で提供されている規則(EU) 2024/2847（サイバー回復力法）の正文の末尾には「A statement has been made with regard to this act and can be found in...」との文言に続けて ELI の表示がある。しかし，この部分は，規則(EU) 2024/2847 の採択過程において発された声明文（statement）が存在することを示す EU 官報上の記載の一部ではあるが，規則(EU) 2024/2847（サイバー回復力法）の正文の一部を組成する文ではない。この部分は，正文の一部として扱われる限り誤記の一種となるので，無視することにし，訳出しなかった。

―解 説―

1. 規則(EU) 2024/2847（サイバー回復力法）について

1.1 概要

規則(EU) 2024/2847（サイバー回復力法）は，欧州連合における IT 製品及び IT サービスのセキュリティに関し，特にサプライチェーンの防護と回復力の確保を重視した EU の現行法令である。

デジタルの要素をもつ製品は，ハードウェアとソフトウェアの両方を含む概念である。規則(EU) 2024/2847（サイバー回復力法）の適用対象となるソフトウェアまたはコンポーネントは，それが無料でオープンソースのソフトウェア（free and open-source software）に該当する場合を含む。

デジタルの要素をもつ製品は，デジタルの要素をもつ重要な製品（important products with digital elements）とデジタルの要素をもつ不可欠の製品（critical products with digital elements）とに区分され，異なる厳しさの要件がそれぞれ適用される（第 7 条及び第 8 条参照）。

デジタルの要素をもつ製品（products with digital elements）及びそのコンポーネントの情報セキュリティ上の安全性と回復力を確保するため，規則(EU) 2024/2847（サイバー回復力法）は，そのような製品の製造者，流通業者及び輸入業者の義務を定めている。

製造者は，設計や製造などの段階において，脆弱性のない製品を製造すべき義務，規則(EU) 2024/2847（サイバー回復力法）及び関連法令の中で定められた必須のサイバーセキュリティ要件（essential cybersecurity requirements）を遵守することを確保し，そのような要件を遵守していることを示すための適合性評価を受ける義務または適合性評価と均等な安全性の保証をすべき義務などを負う。

流通業者及び輸入業者との関係においては，デジタルの要素をもつ製品（products with digital elements）及びそのコンポーネントは，必須のサイバーセキュリティ要件を遵守している場合に限り，欧州連合の市場内において流通させることができる。流通業者の義務の中には，当該製品に適正に CE マークが付されていることの確認義務なども含まれる。

デジタルの要素をもつ製品が遵守すべき必須のサイバーセキュリティ要件は，規則(EU) 2024/2847（サイバー回復力法）の別紙 I（Annex I）の中で定められている。

1.2 適用

規則(EU) 2024/2847（サイバー回復力法）は，2027 年 12 月 11 日から適用される（第 71 条第 2 項）。

規則(EU) 2024/2847（サイバー回復力法）は，2027 年 12 月 11 日よりも前に市場に置かれたデジタルの要素をもつ製品に対しては遡及適用されることがないのが原則であるが（第 69 条第 2 項），例外とし

て，同規則の第 14 条は，2027 年 12 月 11 日よりも前に市場に置かれたデジタルの要素をもつ製品に対しても適用される（第 69 条第 3 項）。

なお，EU 法の体系においては，日本国の法制におけるのと同一の意味での「施行」という法概念が存在しないので，EU 法の翻訳文において「施行」という訳語を使用するのは妥当ではない。

2 法適用において問題となり得る他の関連法令

機械装置である場合とソフトウェアである場合の両方を含め，デジタルの要素をもつ製品の安全性を確保するための EU の法令が多数存在する。

それらの法令の中には，直接的には情報セキュリティとは関係のない製品に適用される法令もあるが，機械装置やソフトウェアとしてのモジュールが他の製品の中に組込まれる場合には，規則(EU) 2024/2847（サイバー回復力法）を含め複数の法令の関連条項が競合的に適用されるのか，または，規則(EU) 2024/2847（サイバー回復力法）の条項が適用されるのかが判断されなければならなくなる。また，デジタルの要素をもつ製品に対して適用される法令であるか否かを問わず，サイバーセキュリティ及びサイバー回復力を確保することを目的とする EU の法令が多数存在する。

そのため，規則(EU) 2024/2847（サイバー回復力法）の適用範囲を理解するためには，それらの関連法令の全体像を把握することが重要である。

同様に，規則(EU) 2024/2847（サイバー回復力法）と競合して適用される他の法令中の関連条項と規則(EU) 2024/2847（サイバー回復力法）の中で定められている条項の適用上の優先劣後の法解釈が必要となる場面が多々存在する。

規則(EU) 2024/2847（サイバー回復力法）の中にはこの点に関する法解釈上の判断基準となる条項も含まれてはいるが，具体的な事案において疑義が生ずることは避けられない。

今後，調整のためのベストプラクティスが集積され，法解釈上の疑義を解消するための判例が蓄積されることになると予想されるので，関連分野の法学研究者としては，そのような意味でのベストプラクティスと判例の動向を注視し，それらを丁寧に分析・考察することにより，問題となった事案を基礎とする帰納法的な手法による法解釈論の形成のための努力を尽くすべきである。

2．1 機械指令 2006/42/EC 及び機械規則(EU) 2023/1230

規則(EU) 2024/2847（サイバー回復力法）は，デジタルの要素をもつ製品のサイバーセキュリティ上の安全確保のための EU の基本的な法令である。

規則(EU) 2024/2847（サイバー回復力法）は，デジタルの要素をもたない機械装置に対しては適用さ

れない。

一般に，デジタルの要素をもたない機械装置に関しては，機械指令 2006/42/EC（OJ L 157, 9.6.2006, p. 24–86）が適用される。

機械指令 2006/42/EC は，機械規則(EU) 2023/1230（OJ L 165, 29.6.2023, p. 1–102）の第 51 条により，2027 年 1 月 13 日の経過をもって廃止される。
2027 年 1 月 14 日以降，機械装置に関しては，規則(EU) 2024/2847 が優先して適用される事項を除き，機械規則(EU) 2023/1230 が適用されることになる。

あくまでも形式論としては，規則(EU) 2024/2847（サイバー回復力法）は，サイバーセキュリティ上の安全確保と全く無関係の事項に関しては適用されないと解し得る。

しかし，一般論としては，デジタルの要素をもつ機械装置がサイバーセキュリティ上のリスクまたは脅威と全く無関係な状態を維持可能であるとは考えられないので，結局，デジタルの要素をもつ機械装置に対しては，原則として，規則(EU) 2024/2847（サイバー回復力法）のみが適用されることになると解される。

機械規則(EU) 2023/1230 と規則(EU) 2024/2847 との間の法適用上の相互関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(53)の中で述べられている。

2．2 医療機器規則(EU) 2017/745 及び体外診断用医療機器規則(EU) 2017/746

デジタルの要素をもつ製品の中でも医療機器の範疇に含まれる製品との関係においては，医療用の機械装置及びソフトウェアのサイバーセキュリティ要件を定める EU の法令として，医療機器規則(EU) 2017/745（OJ L 117, 5.5.2017, p. 1–175）及び体外診断用医療機器規則(EU) 2017/746（OJ L 117, 5.5.2017, p. 176–332）が採択されている。

医療機器規則(EU) 2017/745 及び規則(EU) 2017/746 の中には規則(EU) 2024/2847 に定めるサイバーセキュリティ要件と競合するサイバーセキュリティ要件も定められている。

同一のデジタルの要素をもつ製品に関し，規則(EU) 2017/745 または規則(EU) 2017/746 の中に競合する要件を定める規定が存在する場合，これらの規則に定めるサイバーセキュリティ要件に関する規定が優先的に適用され，規則(EU) 2024/2847（サイバー回復力法）に定めるサイバーセキュリティ要件は適用されない（第 2 条第 2 項(a)及び(b)参照）。

医療機器規則(EU) 2017/745 及び規則(EU) 2017/746 と規則(EU) 2024/2847（サイバー回復力法）との相互の適用関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(25)の中で述べられている。

2．3 型式承認に関する規則(EU) 2019/2144 及び規則(EU) 2018/1139

自動車の型式承認と関連する情報セキュリティ要件に関しては，規則(EU) 2019/2144 (OJ L 325, 16.12.2019, p. 1)が採択されている。
航空機及びその部品等の情報セキュリティに関しては，規則(EU) 2018/1139 (OJ L 212, 22.8.2018, p. 1)が採択されている。

規則(EU) 2019/2144 が優先的に適用される。また，航空機及びその部品等の情報セキュリティに関しては，規則(EU) 2018/1139 が優先的に適用される。
そのため，規則(EU) 2019/2144 または規則(EU) 2018/1139 が適用される製品に関しては，規則(EU) 2024/2847（サイバー回復力法）のサイバーセキュリティ要件が適用されない（第 2 条第 2 項(c)及び同条第 3 項参照）。
規則(EU) 2019/2144 及び規則(EU) 2018/1139 と規則(EU) 2024/2847（サイバー回復力法）との間の法適用上の相互関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(27)の中で述べられている。

なお，規則(EU) 2024/2847（サイバー回復力法）の第 32 条及び別紙 VIII は，EU 型式審査証明書を基礎とする型式の適合性を定めている。

3 製造物責任との関係

欠陥のある製品の製造物責任に関する EU の現行の基本法令は，理事会指令 85/374/EEC (OJ L 210, 7.8.1985, p. 29)である。

理事会指令 85/374/EEC は，2024 年 10 月 23 日に採択された欠陥製品の法的責任に関する欧州議会及び理事会の指令(EU) 2024/2853（OJ L, 2024/2853, 18.11.2024）の第 21 条により，2026 年 12 月 9 日に廃止されるが，同日よりも前に市場において利用できるようにされた製品またはサービスに供された製品に対しては，理事会指令 85/374/EEC が有効な法令として適用され続ける。

指令(EU) 2024/2853 の第 2 条第 1 項により，2026 年 12 月 9 日以後に市場において利用できるようにされた製品またはサービスに供された製品に関しては，指令(EU) 2024/2853 が適用される。

3．1 指令(EU) 2024/2853

規則(EU) 2024/2847（サイバー回復力法）の条項と指令(EU) 2024/2853 と条項との相互の適用関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(31)の中で述べられている。

製品の中に含まれているセキュリティアップデートが適正ではない場合，指令(EU) 2024/2853 が定めている製品の欠陥として法的に評価され得る。規則(EU) 2024/2847（サイバー回復力法）は，製品の中

に含まれているセキュリティアップデートが適正であるようにすべき製造者の義務を定めている（第 6 条，別紙 I 及び別紙 II 参照）。

3．2 一般製品安全性規則(EU) 2023/988

一般製品安全性規則(EU) 2023/988（OJ L 135, 23.5.2023, p. 1）は，製品の安全性に関して定める EU の基本法令である。

一般製品安全性規則(EU) 2023/988 と規則(EU) 2024/2847（サイバー回復力法）との関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(50)の中で述べられている。また，第 11 条は，デジタルの要素をもつ製品に対して一般製品安全性規則(EU) 2023/988 が適用される場合の条件を定めている。

4 情報セキュリティ関連法令との関係

他方，個々の IT 製品や IT サービスではなく，必須インフラ及び重要インフラにおいて使用されるネットワーク及び情報システムの防護と回復力の確保を目的とする EU の法令としては，NIS2 指令(EU) 2022/2555（OJ L 333, 27.12.2022, p. 80–152）がある。
これらの法令以外にも部分的に規則(EU) 2024/2847（サイバー回復力法）と競合して適用される可能性のある法令が複数存在する。

4．1 NIS2 指令(EU) 2022/2555

規則(EU) 2024/2847（サイバー回復力法）は，NIS2 指令(EU) 2022/2555 と相補的な関係にある。そのため，情報システム及びネットワークとそれを組成する製品及びサービス全体のセキュリティという観点から EU の法令を考察しようとするときは，両者の法令を一体のものとして理解する必要性がある。

規則(EU) 2024/2847（サイバー回復力法）は，個々のデジタルの要素をもつ製品の情報セキュリティという側面における安全性を確保することを重視している法令である。
これに対し，NIS2 指令(EU) 2022/2555 は，データが伝達され及び処理される情報システム及び情報ネットワークの情報セキュリティという側面における安全性を確保することを重視している法令である。
この点において，相互に観点を異にする法令であると言える。

そのような観点の相違を明確に認識しながら考察すると，例えば，規則(EU) 2024/2847（サイバー回復力法）の第 14 条第 2 項に定める脆弱性の通知手続と指令(EU) 2022/2555 の第 12 条第 1 項に示す調整された脆弱性開示手続との優先劣後関係を検討しなければならないことがあるということに気づくことができる。

規則(EU) 2024/2847（サイバー回復力法）の条項と NIS2 指令(EU) 2022/2555 の条項相互の適用関係

に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(23)及び前文(24)の中で述べられている。

4．2 規則(EU) 2019/881（サイバーセキュリティ法）

規則(EU) 2019/881（サイバーセキュリティ法）（OJ L 151, 7.6.2019, p. 15）は，欧州連合における統治組織の一部である情報セキュリティに特化した部局（Agency）である ENISA（the European Union Agency for Cybersecurity）の法的根拠，権限及び職務を定める法令である。
情報セキュリティと関連するインシデント情報は，ENISA によって専門的に吟味され，欧州連合としてのインシデント対応が提案・実施されることになる。また，そのために，関連情報が ENISA に集められる。

ただし，ENISA は，情報セキュリティを統括する組織なのであって，欧州連合の法執行機関及び捜査機関ではない。欧州連合におけるサイバー犯罪としてのインシデント対応や犯罪捜査は，Europol の欧州サイバー犯罪センター（European Cybercrime Centre (EC3)）によって統括されている。

4．3 インシデント情報及び脆弱性情報等のエスカレーション

規則(EU) 2024/2847（サイバー回復力法）の第 17 条は，インシデント報告の内容及び手続等に関して定めている。

ENISA 及び調整者として指定された CSIRT と関連に関して，特に，製造者からの脆弱性悪用情報の提供・他の CSIRT に対する迅速な情報伝達と（例外的な措置としての）その情報伝達の制限・抑制に関しては，規則(EU) 2024/2847（サイバー回復力法）の前文(65)～前文(76)の中で述べられている。

ENISA 及び CSIRT に対する脆弱性情報の伝達のために使用される単一報告プラットフォーム（single reporting platform）に関しては，規則(EU) 2024/2847（サイバー回復力法）の第 16 条で定められている。

デジタルの要素をもつ製品の製造者のインシデント報告義務は，第 14 条によって定められている。

リスク要素も報告義務の対象の中に含まれ得るが，その中には非技術的なリスク要素も含まれる。非技術的なリスク要素とは，例えば，「供給者に対する第三国からの不適正な影響」などを指す（規則(EU) 2024/2847（サイバー回復力法）の前文(52)参照）。
規則(EU) 2024/2847（サイバー回復力法）の第 54 条第 2 項は，報告されたリスク要素に対する各構成国の国内レベルの対応に関して定めており，第 56 条第 2 項は，欧州連合レベルの対応に関して定めている。

5 規則(EU) 2024/1689（人工知能法）との関係

規則(EU) 2024/1689（人工知能法）との関係に関しては，規則(EU) 2024/2847（サイバー回復力法）の前

文(51)の中で述べられている。

規則(EU) 2024/2847（サイバー回復力法）の第 12 条は，特に高リスク AI システムの回復力との関係において，調整規定を設けている。

規則(EU) 2024/2847（サイバー回復力法）の第 12 条第 1 項は，所定の要件を充足すれば，規則(EU) 2024/2847（サイバー回復力法）に定める適合性評価を受けることによって規則(EU) 2024/1689（人工知能法）の第 15 条に定める必須のサイバーセキュリティ要件も充足しているとみなされる旨を定め，二重の手間がかかることを防止している。

規則(EU) 2024/2847（サイバー回復力法）の第 12 条第 2 項は，同条第 1 項を実際に機能させるために，一定の条件の下において，規則(EU) 2024/2847（サイバー回復力法）の下にある適合性評価組織が規則(EU) 2024/1689（人工知能法）の下にある適合性評価組織としての職務権限ももち得ることを定めている。
この点に関し，規則(EU) 2024/1689（人工知能法）の下にある適合性評価組織の権限が原則として規則(EU) 2024/2847（サイバー回復力法）の下にある適合性評価組織よりも優先すると解すべきかどうかについては，見解が分かれ得る。

他方，規則(EU) 2024/2847（サイバー回復力法）の第 52 条第 14 項は，高リスク AI システムとして分類されるデジタルの要素をもつ製品を所管する市場監視当局等の監督機関が複数存在する場合に関し，それらの機関相互の連絡と調整に関して定めている。

これらの関連規定の定め方には国際政治学上の要素と関連する本質的問題が伏在しており，純粋に法解釈論上の理由によるというよりは国際情勢の変化によって影響を受ける可能性が高い。
そのことから，今後，この点に関す法適用上及び法解釈上の紛議が発生する可能性を含め，EU の動向に十分に留意すべきである。

もっとも，各構成国において，現実には同一の組織が則(EU) 2024/1689（人工知能法）の下にある適合性評価組織と規則(EU) 2024/2847（サイバー回復力法）の下にある適合性評価組織とを兼ねることが多いだろうと予測され，現実にそうである場合には，解釈論上の問題は生じない。そのような場合においては，規則(EU) 2024/2847（サイバー回復力法）の第 12 条第 2 項は，当然のことを明確にしているだけということになる。

6 適合性評価制度及び CE マーク

規則(EU) 2024/2847（サイバー回復力法）の第 29 条及び第 30 条は，デジタルの要素をもつ製品に適用される必須のサイバーセキュリティ要件を遵守している製品であることを示すための適合性評価手続と CE マークについて定めている。更に，規則(EU) 2024/2847（サイバー回復力法）の別紙 VIII は，適合性評価手続の詳細について定めている。

他方，規則(EU) 2019/ 881（サイバーセキュリティ法）は，欧州サイバーセキュリティ認証制度（European cybersecurity certification scheme）を定めている。

規則(EU) 2024/2847（サイバー回復力法）は，事柄の性質に応じて，欧州サイバーセキュリティ認証制度を基礎とするセキュリティ認証と CE マークの利用を認めている。

欧州サイバーセキュリティ認証制度に関しては，その実装法令として，委員会実装規則(EU) 2024/482（OJ L, 2024/ 482, 7.2.2024）が定められている。このような実装法令を含め，規則(EU) 2024/2847（サイバー回復力法）の条項と規則(EU) 2019/ 881（サイバーセキュリティ法）の条項との相互の適用関係が判断されなければならない。

7 関連する制度や情報システム等の情報提供のある Web サイトなど

EU における CE マークに関する公式の Web サイトは，下記のところにある。

CE marking
https://single-market-economy.ec.europa.eu/single-market/ce-marking_en
[2025 年 2 月 10 日確認]

NANDO 情報システム（NANDO Information System）と略称される新アプローチの被通知団体及び被指定団体情報システム（New Approach Notified and Designated Organisations Information System）に関する公式の Web サイトは，下記のところにある。

NANDO (New Approach Notified and Designated Organisations) Information System
https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies
[2025 年 2 月 10 日確認]

EU の製品規定の実装に関するブルーガイド（The ‘Blue Guide’ on the implementation of EU product rules 2022）（2022/C 247/01）（OJ C 247, 29.6.2022, p. 1–152）が委員会告示（Commission Note）として公示されている。
このブルーガイドの中には，規則(EU) 2024/2847（サイバー回復力法）の条項を解釈する上で有用な情報が含まれている。

The ‘Blue Guide’ on the implementation of EU product rules 2022（2022/C 247/01）
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2022.247.01.0001.01.ENG
[2025 年 2 月 23 日確認]

2. 参考訳作成における基本方針

この参考訳においては，Corrigendum（OJ L, 2024/90780, 5.12.2024）による一部訂正後の規則(EU) 2024/2847（サイバー回復力法）の前文（recital），条文（articles）及び別紙（Annex）の全文を訳出した。

この参考訳においては対訳方式を採用することにした。ただし，原文を表示することが無意味な部分（特に脚注内）に関しては，原文または訳文の表示を省略した。

この参考訳は，あくまでも規則(EU) 2024/2847（サイバー回復力法）の私的な和訳である。公式訳でも確定訳でもない。

この参考訳は，現時点における研究成果を反映するものである。将来，更に研究を深めた結果として修正すべき部分を発見したときは，その時点において，改訂版等を作成すべきかどうかを検討する。

この参考訳の訳出に際しては原則として直訳とすることとしたが，直訳のままでは日本語になりにくい箇所に関しては，やむを得ず意訳とした。

原文中にある誤記と疑われる箇所に関しては，赤色字で示すことにした。この原文中の誤記と疑われる箇所は，形式的なミスという意味で誤記であるものと意味的な誤りを含むことになるために誤記であるものの両者を含む。
ただし，原文中に存在する誤記と疑われる箇所の全てが赤色字で表示されているという趣旨ではない。判断を保留した箇所が存在する。
なお，規則(EU) 2024/2847 の脚注内で示されている引用法令の出典を示す箇所の表記において「ELI:」が付されているものがある。しかし，その場合の「ELI:」の表記はそれが存在しなくても典拠である EU 官報の該当号の特定性に欠けることが全くないので，法情報学及び立法学の観点からすると，それらの「ELI:」の表記は，余事記載という意味で誤記の一種であると解し，そのような意味で，赤色字で表示することにした。
原文中に誤りがあると判断した場合，原則として，そのまま直訳とした。しかし，そのまま直訳にしたのでは正しく法解釈された法規範を適正に示したことにならない場合，合理的に法解釈した結果を反映した訳文とすることにし，その箇所を灰色字で示すことにした。

この参考訳に訳注はない。参考訳中にある脚注は，全て原注である。

読みやすさを重視し，条文中の号(point)の表記を一部省略した。例えば，「point(a)」は「第(a)号」であるが，「第」と「号」を省略し，「(a)」と表記することにした。

この参考訳は，Eur-lex のデータ二次利用条件を遵守して作成した。

3. 参考訳作成において留意した事項

Economic operators

「economic operators」とは，私経済取引において取引の当事者となり得る法主体（自然人または法人）のことを意味する（指令(EU)2024/2853 の第 4 条第 15 号参照）。

「economic operators」は，様々な訳が考えられ，この参考訳において「経済運営者」という訳を使用することも検討した。
しかし，国レベルにおける「経済運営者」は，国家の経済政策を決定・執行する（当該国の）政府である。そして，この場合の「経済運営者」は，「私経済取引における取引の当事者」を意味していない。そのため，「経済運営者」という訳語では混同・混乱が生ずる危険性があると判断し，「経済運営者」との訳語を用いないことにした。
加えて，規則(EU)2022/2065（デジタルサービス法）の参考訳（法と情報雑誌 8 巻 2 号 1～299 頁）における訳語と揃えることが望ましいと判断し，「economic operators」を「経済取引主体」と訳すことにした。

Qualifying as free and open-source software

「qualifying as free and open-source software」は，「無料でオープンソースのソフトウェア」の範疇に含まれると判断されるための規則(EU) 2024/2847（サイバー回復力法）及び関連法令の中で定められている要件（requirements）または条件（conditions）を満たしていると判断されているということを意味する形容詞句である。
この形容詞句がかかる対象となる名詞は「products with digital elements」なので，「products with digital elements qualifying as free and open-source software」を分解しないで一個の熟語として理解すべきである。

このようなまわりくどい表現が用いられているのは，規則(EU) 2024/2847 の中で定められているセキュリティ上の要件の適用を回避するため，「無料でオープンソースのソフトウェア」の各人各様の定義が恣意的に用いられることを防止するためである。
特に，規則(EU) 2024/2847 は，IT 製品または ICT 製品のサプライチェーンのセキュリティを確保することを狙いとしていることから，同一の製品やサービスのサプライチェーンに関与する複数の関係者における定義の解釈・運用が区々になっていると，同規則が目指すレベルのセキュリティを確保できなくなってしまう可能性がある。

それゆえ，関係者が各自の判断基準を基礎として「無料でオープンソースのソフトウェア」であるかどうかを判断するのではなく，統一的な判断基準に従って検証可能なかたちで客観的にそのことが判定されているということを確保することが重要である。

以上のことを踏まえた上で，この参考訳においては，「qualifying as free and open-source software」は，「無料でオープンソースのソフトウェアとして適格な」と訳すことにした。

Software bill of materials

「SBOMs」または「SBOM」と略称される「software bill of materials」は，一般に，「ソフトウェア部品表」と訳されている。これは，ソフトウェアが存在せず，機械装置だけで構成されていた工業生産の時代における「bill of materials」の概念とその訳語である「部品表」という語を無思慮に継承しただけの結果として生じた誤訳の一種であるので，その使用を禁止されるべきである。
一般に，デジタル時代には，デジタル時代に即した造語が求められる。技術の急激な変化に対応できるだけの十分な言語能力を養い，可能な限り潤沢な語彙を脳内に蓄蔵することが望ましい。

この参考訳においては，提案的な試みの一種として，デジタルの要素をもつソフトウェア製品に関しては，「bill of materials」を「素材表」と訳すべきであるとの理解を前提にした上で，「software bill of materials」を「ソフトウェア素材表」と訳すことにした。

なお，現代の機械装置は，古典的なタイプのものだけではなく，電子チップやファームウェアを組み込んだハイブリッドのタイプのものが普通になっている。

それゆえに，そのようなデジタルの要素をもつ製品のサイバーセキュリティを確保する必要性を重視して規則(EU) 2024/2847（サイバー回復力法）が採択されたという経緯に鑑み，今後は，非デジタルの機械装置を含め，全ての種類の製品（products）との関係において，「bill of materials」の訳語として「部品表」を因習的に使用するのではなく，この参考訳において提案している「素材表」との訳語またはこの訳語よりも優れた別の訳語を使用すべきである。

Critical infrastructures

「critical infrastructures」は，一般に，「重要インフラ」と訳されている。私もこれまではそのように訳してきた。しかし，EU の法制全体を見渡した場合，「critical infrastructures」と「important infrastructures」とを分けて理解する必要性が高い。

そこで，この点に関する考え方を改め，「critical infrastructures」を「不可欠なインフラ」または「不可欠インフラ」と訳し，「important infrastructures」を「重要なインフラ」または「重要インフラ」と訳すことにした。

なお，日本国の関連法制における「重要インフラ」との概念は，基本的には，EU の関連法制における「critical infrastructures」の概念に対応するものなので，日本国法の語彙と EU 法の語彙とは一致していない。

Refurbishing

「refurbishing」の名詞形である「refurbishment」の語義に関し，規則(EU) 2024/2847 の前文(42)で参照されているエコデザイン規則(EU) 2024/1781（OJ L, 2024/1781, 28.6.2024）の第 2 条第 18 号は，次のように定義している。

> ‘refurbishment’ means actions carried out to prepare, clean, test, service and, where necessary, repair a product or a discarded product in order to restore its performance or functionality within the intended use and range of performance originally conceived at the design stage at the time of the placing of the product on the market;

この定義条項を踏まえた上で，「refurbishing」を「改修」と訳すことも検討したが，使用をやめた廃棄物である製品の修理によってその機能を再生して実行される再利用を含む概念なので，「再生」のほうがより適切なニュアンスを示す訳語であると判断した。
その結果として，この参考訳においては，このとりあえず，「refurbishing」を「再生利用」と訳すことにした。

Assurance level

「assurance level」は、「保証レベル」と訳すことにした。

この保証レベルは、サイバーセキュリティ認証における信頼性の程度を示す尺度（指標）であり，一般的には，「低（low）」，「十分（substantial）」及び「高（high）」に区分される。「lower」または「higher」または「highest」は，「substantial」を基準として評価される。

EUCC と略称される欧州共通基準ベースのサイバーセキュリティ認証制度（the European common criteria-based cybersecurity certification scheme）に対して規則(EU) 2019/881 を適用するための 2024 年 1 月 31 日の委員会実装規則(EU) 2024/482（OJ L, 2024/482, 7.2.2024）の第 4 条第 1 項は，「十分（substantial）」及び「高（high）」と評価できた場合には認証機関が EUCC 証明書を発行するものと定めている。
また，同規則の第 4 条第 2 項は，保証レベルの「十分（substantial）」が「AVA_VAN level 1 or 2」に相当することを定め，同条第 3 項は，保証レベルの「高（high）」が「AVA_VAN level 3, 4 or 5」に相当することを定めている。それゆえ，実質的に見た場合，「低（low）」を除き，少なくとも 5 段階の保証レベルが存在することになる。
「AVA_VAN level」の定義は，同実装規則の第 2 条第 8 号で定められている。

Critical dependencies, critical dependency

この参考訳においては，「critical dependency (critical dependencies)」を「不可欠の依存関係」と訳すことにした。

既出の参考訳の中では別異に訳出したこともあるが，改める。

Bug bounty programme

「bug bounty programme」（＝米語では「bug bounty program」）は，一般に，「バグ報奨金制度」と訳される。しかし，個々の企業等が国家制度（system）を任意に設計・構築することはできないので，「bug bounty programme」における「programme」を「制度」と訳すことは，明確に誤訳である。

ここでいう「programme」は，情報セキュリティのマネジメントシステムの中において脆弱性情報を取扱うために，当該管理主体によって個別具体的に様式化された管理策（control）の一種として理解すべきものなので，「対処計画」または「対処手順」等と訳すのが妥当である。

以前は別異に訳出したことあるが，再検討の上で，訳語を改めるべきだと判断した。

以上を踏まえた上で，この参考訳においては，とりあえず，「bug bounty programme」を「バグ報償対処計画」と訳すことにした。

Notified body（notified bodies）

「notified body（notified bodies）」は，職務権限のある国内機関（competent national authorities）によって指定を受け，かつ，欧州委員会に対して通知された適合性評価組織である。

「notified body」は，構成国の行政機関の一種であり得るけれども，民間の特殊な能力をもつ評価組織または監査組織が「notified body」となることが想定されている。
ただし，企業の会計監査や情報セキュリティ上の監査とはかなり異なり，得意分野とする部門別に区分された指定が行われることが想定されている。現時点においては，全ての種類のデジタルの要素をもつ製品及びその応用製品と応用サービスに関して，技術上の要求事項及び法律上の要件と義務の充足の有無を単一の監査法人等が完全に審査・評価・判断することは，ほぼ不可能である。
少なくとも，現時点の日本国内において，規則(EU) 2024/2847 に示された必須の要件を充足する業務遂行能力と中立性と公平性を満たす民間組織は，1 つも存在しないし，今後もビジネスとして成立する見込みはほとんどない。
それゆえ，日本国においては，民間企業ではなく，国の厳格な管理の下にある特別の研究組織等が個人情報保護委員会と協力しながら「notified body」としての役割を果たさざるを得ないのではないかと考えられる。

「notified body（notified bodies）」は，直訳では「被通知組織」または「通知された組織」と訳すことになる。しかし，このような訳語を用いる場合，「notified body」に期待されている極めて重要な任務と機能を反映するものではないという意味で適切な訳語ではないと考えられる。
そこで，この参考訳においては，その意味を反映させるため，「notified body（notified bodies）」を「指定組織」と意訳することにした。

ただし，「the New Approach Notified and Designated Organisations (NANDO) information system」の「Notified」は，直訳により「被通知」と訳すことにした（前文 103 参照）。
その結果，この参考訳の中には「notified」に関して異なる訳が混在している。

Proprietary rights

一般に，「proprietary rights」は，特許権，商標権，著作権，営業秘密のような独占権としての知的財産

権を指す総称である。

規則(EU) 2024/2847（サイバー回復力法）の中においても同じ意味をもつ語として使用されている（第 39 条第 10 項参照）。
規則(EU) 2024/2847（サイバー回復力法）の第 63 条第 1 項(a)は，同規則における「proprietary rights」の概念内容を理解する上で参考になる。

以上の諸点を踏まえた上で，この参考訳においては，慣例に従い，「proprietary rights」を「専有権」と訳すことにした。

Data, personal or other,

別紙 I の中にある「data, personal or other」との表現は，「personal data or non-personal data」を意味するものと解される。

一般に，デジタルの要素をもつ製品において処理されるデータには GDPR が適用される「個人データ（personal data）」と GDPR が適用されない「非個人データ（non-personal data）」とが存在し得るが，個人データと非個人データが混在している場合には GDPR が適用される。

非個人データに関して定める EU の基本的な法令は，規則(EU) 2018/1807（OJ L 303, 28.11.2018, p. 59–68）である。

このような解釈を踏まえた上で，この参考訳においては，「data, personal or other」を「個人データまたはそれ以外のデータ」と訳すことにした。

4. 関連参考訳等

規則(EU) 2019/881（Cybersecurity Act）の参考訳・改訂版は，法と情報雑誌 4 巻 8 号 16～86 頁にある。
指令(EU) 2022/2555（NIS2 指令）の参考訳は，法と情報雑誌 8 巻 4 号 1～206 頁にある。

規則(EU)2022/2065（デジタルサービス法）の参考訳は，法と情報雑誌 8 巻 2 号 1～299 頁にある。

規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は，法と情報雑誌 3 巻 5 号 1～114 頁にある。データローカライゼーション規則(EU) 2018/1807 の参考訳は，法と情報雑誌 4 巻 1 号 82～100 頁にある。電子識別規則(EU) No 910/2014 の参考訳は，法と情報雑誌 2 巻 10 号 147～196 頁にある。

製造物責任に関する理事会指令 85/374/EEC の参考訳は，法と情報雑誌 2 巻 10 号 278～291 頁にある。製造物責任指令改正指令案の参考訳は，法と情報雑誌 8 巻 1 号 81～161 頁にある。製造物責任指令報告書 COM(2018) 246 final の参考訳は，法と情報雑誌 3 巻 9 号 269～280 頁にある。
営業秘密指令(EU) 2016/943 の参考訳は，法と情報雑誌 2 巻 9 号 489～514 頁にある。

規則(EU) No 182/2011 の参考訳は，法と情報雑誌 3 巻 5 号 168～179 頁にある。

この参考訳の校正等に関し，唐亀侑久氏（株式会社ラック）の助力を得た。

＊＊＊

デジタルの要素をもつ製品の横断的なサイバーセキュリティ要件に関する並びに規則(EU) No 168/2013 及び規則 (EU) 2019/1020 並びに指令 (EU) 2020/1828 を改正する欧州議会及び理事会の 2024 年 10 月 23 日の規則(EU) 2024/2847（サイバー回復力法）

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024
on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013
and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

（EEA に適用される正文）
(Text with EEA relevance)

欧州議会及び欧州連合の理事会は,
欧州連合の機能に関する条約, とりわけ, 同条約の第 114 条に鑑み,
欧州委員会からの提案に鑑み,
立法案を国内議会に送付した後,
欧州経済社会委員会の意見書に鑑み[1],
地域委員会からの意見聴取を経た後,
通常の立法手続に従って審議し[2],

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,
Having regard to the proposal from the European Commission,
After transmission of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee[(1)],
After consulting the Committee of the Regions,
Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) サイバーセキュリティは, 欧州連合にとって鍵となる検討課題の一つである。ネット接続された機器の数及び種類は, 今後数年間に飛躍的に増加する。サイバー攻撃が欧州連合の経済に対してだけではなく, 民主主義及び消費者の安全と健康に対しても重大な影響をもつことから, サイバー攻撃は, 公共の利益のある事柄を表している。それゆえ, サイバーセキュリティに対する欧州連合のアプローチを強化し, 欧州連合レベルでサイバー回復力に対処し, そして, デジタルの要素をもつ製品を欧州連合の市場に置くことに関する必須のサイバーセキュリティ要件に関する統一的な法的枠組

[1] OJ C 100, 16.3.2023, p. 101.
[2] 欧州議会の 2024 年 3 月 12 日付け意見書（官報未搭載）及び理事会の 2024 年 10 月 10 日付け決定。
Position of the European Parliament of 12 March 2024 (not yet published in the Official Journal) and decision of the Council of 10 October 2024.

みを定めることによって域内市場の稼働を向上させる必要がある。利用者及び社会に対してコストを付加する 2 つの主要な問題が対処されるべきである：すなわち，広範に拡散する脆弱性及び当該脆弱性に対処するためのセキュリティアップデートの不十分かつ一貫性のない提供によって反映される，デジタルの要素をもつ製品の低レベルのサイバーセキュリティであり，また，利用者に対し，適切なサイバーセキュリティ特性をもつ製品を選択することを妨げまたは当該製品を安全な態様で利用することを妨げている，利用者による不十分な理解と情報への不十分なアクセスである。

Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

(2) この規則は，より少ない脆弱性をもつ状態でハードウェア製品とソフトウェア製品が市場に置かれることを確保することにより，及び，製造者が，製品のライフサイクル全体を通じてセキュリティを真剣に受け止めることを確保することにより，デジタルの要素をもつ安全な製品の開発に関する境界条件を設定することを狙いとしている。この規則は，例えば，市場において利用できるようにされたデジタルの要素をもつ製品のサポート期間に関する透明性を向上させることにより，デジタルの要素をもつ製品を選択する際及び利用する際，利用者がサイバーセキュリティを考慮に入れることができるようにする条件をつくり出すことも狙いとしている。

This Regulation aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements, for example by improving transparency with regard to the support period for products with digital elements made available on the market.

(3) 現在発効している適格な欧州連合法は，デジタルサプライチェーンの防護を向上させるための措置を含め，異なる角度からサイバーセキュリティと結び付けられた一定の側面に対処する幾つかの横断的な規定のセットによって構成されている。しかしながら，欧州議会及び理事会の規則(EU) 2019/881[3]並びに欧州議会及び理事会の指令(EU) 2022/2555[4]を含め，サイバーセキュリティと関係する

[3] ENISA（欧州連合サイバーセキュリティ局）に関する及び情報通信技術のサイバーセキュリティ認証に関する並びに規則(EU) No 526/2013 を廃止する欧州議会及び理事会の 2019 年 4 月 17 日の規則(EU) 2019/881（サイバーセキュリティ法）(OJ L 151, 7.6.2019, p. 15).

欧州連合の現行の欧州連合法は，直接的には，デジタルの要素をもつ製品の防護に関する強制的な要件を包摂していない。

Relevant Union law in force comprises several sets of horizontal rules that address certain aspects linked to cybersecurity from different angles, including measures to improve the security of the digital supply chain. However, existing Union law related to cybersecurity, including Regulation (EU) 2019/881 of the European Parliament and of the Council[3] and Directive (EU) 2022/2555 of the European Parliament and of the Council [4], does not directly cover mandatory requirements for the security of products with digital elements.

(4) 欧州連合の現行法はデジタルの要素をもつ一定の製品に対して適用されるものの，デジタルの要素をもつ全ての製品に関する包括的なサイバーセキュリティ要件を設ける欧州連合の横断的な法制枠組みは存在しない。欧州連合レベル及び国内レベルでこれまで行われてきた様々な活動及び取組みは，発見されたサイバーセキュリティと関連する問題及びリスクに対して部分的に対処するだけであり，域内市場内において立法上のパッチワークをつくり出し，当該製品の製造者と利用者の両者に対して法的な不確実性を増加させ，そして，類似のタイプの製品に関する多数の要件及び義務を遵守するための無用の負担を企業及び組織に対して付加している。ある構成国または第三国で製造されたデジタルの要素をもつ製品は，しばしば，域内市場全体にわたる組織及び消費者によって利用されるので，それらの製品のサイバーセキュリティは，とりわけ強力な国境を越える局面をもつ。このことは，整合化された法制枠組みを確保するため，そして，委員会勧告 2003/361/EC[5]の別紙に定義するマイクロ企業，小企業及び中規模企業を含め，利用者，組織及び企業にとっての法的確実性を確保するため，その分野を欧州連合レベルで規制すべき必要性を生じさせている。欧州連合の法制の様相は，デジタルの要素をもつ製品に関する横断的なサイバーセキュリティ要件を導入することによって整合化されるべきである。加えて，経済取引主体及び利用者にとっての法的確実性，並びに，域内市場への参入を狙いとする経済運営主体のためのより実行可能な条件をつくり出す，単一市場のより良い整合化と，マイクロ企業，小企業及び中規模企業のための比例性が，欧州連合全域にわたって確保されるべきである。

While existing Union law applies to certain products with digital elements, there is no horizontal Union regulatory

---

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

[4] 欧州全域の共通の高いレベルのサイバーセキュリティのための措置に関する，規則(EU) No 910/2014 及び指令(EU)2018/1972 を改正し，並びに，指令(EU)2016/1148 を廃止する欧州議会及び理事会の 2022 年 12 月 14 日の指令(EU)2022/2555（NIS2 指令）(OJ L 333, 27.12.2022, p. 80).

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

[5] マイクロ企業，小企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告 2003/361/EC (OJ L 124, 20.5.2003, p. 36).

Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

framework establishing comprehensive cybersecurity requirements for all products with digital elements. The various acts and initiatives taken thus far at Union and national levels only partially address the identified cybersecurity-related problems and risks, creating a legislative patchwork within the internal market, increasing legal uncertainty for both manufacturers and users of those products and adding an unnecessary burden on businesses and organisations to comply with a number of requirements and obligations for similar types of products. The cybersecurity of those products has a particularly strong cross-border dimension, as products with digital elements manufactured in one Member State or third country are often used by organisations and consumers across the entire internal market. This makes it necessary to regulate the field at Union level to ensure a harmonised regulatory framework and legal certainty for users, organisations and businesses, including microenterprises and small and medium-sized enterprises as defined in the Annex to Commission Recommendation 2003/361/EC[5]. The Union regulatory landscape should be harmonised by introducing horizontal cybersecurity requirements for products with digital elements. In addition, legal certainty for economic operators and users, as well as a better harmonisation of the internal market and proportionality for microenterprises and small and medium-sized enterprises, creating more viable conditions for economic operators aiming to enter that market, should be ensured across the Union.

(5) マイクロ企業並びに小企業及び中規模企業に関して，ある企業が該当する類型を決定する際，勧告 2003/361/EC の別紙の条項が全面的に適用されるべきである。それゆえ，企業類型を決定する従業員数及び資金上の上限値を計算する際，パートナー企業または連携企業のような特定のタイプの企業を考慮に入れて企業のデータを確定することに関する勧告 2003/361/EC の別紙の第 6 条の条項も適用されるべきである。

As regards microenterprises and small and medium-sized enterprises, when determining the category an enterprise falls into, the provisions of the Annex to Recommendation 2003/361/EC should be applied in their entirety. Therefore, when calculating the staff headcount and financial ceilings determining the enterprise categories, the provisions of Article 6 of the Annex to Recommendation 2003/361/EC on establishing the data of an enterprise in consideration of specific types of enterprises, such as partner enterprises or linked enterprises, should also be applied.

(6) 欧州委員会は，この規則の適用において経済取引主体，とりわけマイクロ企業並びに小企業及び中規模企業を補助するためのガイドを提供すべきである。そのようなガイドは，就中，この規則の適用範囲を包摂すべきであり，とりわけ無料でオープンソースのソフトウェア開発者にとってのリモートのデータ処理とその意味，デジタルの要素をもつ製品のサポート期間を決定するために使用される基準の適用，この規則と他の欧州連合法との間の相互作用並びに大きな修正の概念を含めるべきである。

The Commission should provide guidance to assist economic operators, in particular microenterprises and small and medium-sized enterprises, in the application of this Regulation. Such guidance should cover, inter alia, the scope of this Regulation, in particular remote data processing and its implications for free and open-source software developers, the application of the criteria used to determine support periods for products with digital elements, the interplay between this Regulation and other Union law and the concept of substantial modification.

(7) 欧州連合レベルにおいて，「EU のデジタル 10 年のためのサイバーセキュリティ戦略」と題する 2020

年 12 月 16 日の欧州委員会並びに外務及び安全保障基本方針に関する欧州連合上級代表の共同通知と，ネット接続された機器のサイバーセキュリティに関する 2020 年 12 月 2 日の理事会決議及び欧州連合のサイバー態勢の構築に関する 2022 年 5 月 23 日の理事会決議並びにデジタル 10 年のための EU のサイバーセキュリティ戦略に関する 2021 年 6 月 10 日の欧州議会決議[6]のような様々な計画文書及び政治文書は，当該第三国の自発によりこの問題に対処するための措置を導入する幾つかの第三国に対し，デジタル製品またはネット接続された製品に関する欧州連合の個別のサイバーセキュリティ要件を求めてきた。欧州の未来に関する会議の最終報告書の中で，市民は，「サイバーセキュリティ上の脅威への対抗における EU のより強力な役割」を求めた。サイバーセキュリティの分野において欧州連合が主導的な国際的役割を果たすため，意欲的な法制枠組みを確立することが重要である。

At Union level, various programmatic and political documents, such as the Joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 16 December 2020, entitled 'The EU's Cybersecurity Strategy for the Digital Decade', the Council Conclusions of 2 December 2020 on the cybersecurity of connected devices and of 23 May 2022 on the development of the European Union's cyber posture and the European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade[6], have called for specific Union cybersecurity requirements for digital or connected products, with several third countries introducing measures to address this issue on their own initiative. In the final report of the Conference on the Future of Europe, citizens called for 'a stronger role for the EU in countering cybersecurity threats'. In order for the Union to play a leading international role in the field of cybersecurity, it is important to establish an ambitious regulatory framework.

(8) 域内市場に置かれたデジタルの要素をもつ全ての製品のサイバーセキュリティの全体的なレベルを向上させるため，デジタルの要素をもつ製品に関する横断的に適用され，目的指向でありかつ技術的中立があるサイバーセキュリティの必須要件を導入する必要がある。

To increase the overall level of cybersecurity of all products with digital elements placed on the internal market, it is necessary to introduce objective-oriented and technology-neutral essential cybersecurity requirements for those products that apply horizontally.

(9) 一定の条件の下において，より大きな電子情報システムの中に組み込まれまたはより大きな電子情報システムに接続されているデジタルの要素をもつ全ての製品は，悪意ある行為者のための攻撃ベクトルとして奉仕し得る。その結果として，より重要ではないと判断されているハードウェア及びソフトウェアでさえ，機器またはネットワークの最初の弱体化を容易にでき，悪意ある行為者が，システムに対する特権アクセスを獲得できるようにし，または，システム間を横断して移動できるようにする。それゆえ，製造者は，デジタルの要素をもつ全ての製品が，この規則の中で定められた必須のサイバーセキュリティ要件に従って設計されかつ開発されることを確保すべきである。同義務は，ハードウェアインタフェイスを介して物理的に接続され得る製品と，ネットワークソケット，パイプ，ファイル，アプリケーションプログラミングインタフェイスまたはそれら以外のタイプのソフトウェアインタフェイスを介する

[6] OJ C 67, 8.2.2022, p. 81.

場合のように，論理的に接続されている製品の両者と関連している。サイバー脅威は，例えば，脆弱性の多角的な悪用を互いに結びつけることによって，ある標的に到達する前に，デジタルの要素をもつ様々な製品を介して伝播し得るので，製造者は，別の機器またはネットワークと間接的にのみ接続されているデジタルの要素をもつ製品のサイバーセキュリティも確保すべきである。

Under certain conditions, all products with digital elements integrated in or connected to a larger electronic information system can serve as an attack vector for malicious actors. As a result, even hardware and software considered to be less critical can facilitate the initial compromise of a device or network, enabling malicious actors to gain privileged access to a system or to move laterally across systems. Manufacturers should therefore ensure that all products with digital elements are designed and developed in accordance with the essential cybersecurity requirements laid down in this Regulation. That obligation relates to both products that can be connected physically via hardware interfaces and products that are connected logically, such as via network sockets, pipes, files, application programming interfaces or any other types of software interface. As cyber threats can propagate through various products with digital elements before reaching a certain target, for example by chaining together multiple vulnerability exploits, manufacturers should also ensure the cybersecurity of products with digital elements that are only indirectly connected to other devices or networks.

(10) デジタルの要素をもつ製品を市場に置くことに関するサイバーセキュリティ要件を定めることにより，消費者のため及び企業のための当該デジタルの要素をもつ製品のサイバーセキュリティが同様に拡大されることが意図されている。同要件は，サイバーセキュリティが，デジタルの要素をもつ最終製品及び当該製品のコンポーネントをより安全にすることを，サプライチェーン全体を通して考慮に入れることも確保することになる。このことは，玩具やベビー監視システムのような，脆弱性のある消費者向けを意図したデジタルの要素をもつ消費者向け製品を市場に置くための要件も含める。デジタルの要素をもつ重要な製品としてこの規則の中で類型化されたデジタルの要素をもつ消費者向け製品は，そのリスクの強度の面における負の影響，及び，そのような製品の利用者の健康，防護または安全を損なう能力の面における負の影響という大きなリスクのある機能を遂行することによる，サイバーセキュリティ上のより高度なリスクを示しており，より厳格な適合性評価手続を受けるべきである。この手続は，スマートドアロックを含め，セキュリティ機能をもつスマートホーム製品，ベビー監視システムと警報システム，ネット接続した玩具，及び，個人向けウェアラブル医療技術のような製品に対して適用される。更に，デジタルの要素をもつ重要な製品または不可欠な製品としてこの規則の中で類型化されたデジタルの要素をもつその他の製品が受けることを要求されるより厳格な適合性評価手続は，脆弱性の悪用という消費者に対する潜在的な負の影響を防止するために寄与することになる。

By laying down cybersecurity requirements for placing on the market products with digital elements, it is intended that the cybersecurity of those products for consumers and businesses alike be enhanced. Those requirements will also ensure that cybersecurity is taken into account throughout supply chains, making final products with digital elements and their components more secure. This also includes requirements for placing on the market consumer products with digital elements intended for vulnerable consumers, such as toys and baby monitoring systems. Consumer products with digital elements categorised in this Regulation as important products with digital elements present a higher cybersecurity risk by performing a function which carries a significant risk of adverse effects in terms of its intensity and

ability to damage the health, security or safety of users of such products, and should undergo a stricter conformity assessment procedure. This applies to such products as smart home products with security functionalities, including smart door locks, baby monitoring systems and alarm systems, connected toys and personal wearable health technology. Furthermore, the stricter conformity assessment procedures that other products with digital elements categorised in this Regulation as important or critical products with digital elements are required to undergo, will contribute to preventing potential negative impacts on consumers of the exploitation of vulnerabilities.

(11) この規則の目的は，デジタルの要素をもつ製品及び当該製品に組み込まれたリモートのデータ処理ソリューションの高いレベルのサイバーセキュリティを確保することにある。そのようなリモートのデータ処理ソリューションは，その処理のために関係するデジタルの要素をもつ製品の製造者によってまたはその代わりの者によってソフトウェアが指定されまたは開発される隔地のデータ処理であって，そのデータ処理が欠けるときは，そのデジタルの要素をもつ製品が，その製品の機能のいずれかを遂行することが妨げられるようなものとして定義されるべきである。このアプローチは，データが利用者の機器上でローカルに処理もしくは記録保存されるか，または，その製造者によってリモートで処理もしくは記録保存されるかに拘わらず，そのような製品が，当該製品の全体について，当該製品の製造者によって適切に防護されることを確保する。それと同時に，隔地の処理または記録保存は，デジタルの要素をもつ製品にとって，当該製品の機能を遂行するために必要な限りにおいて，この規則の適用範囲内にある。そのような隔地の処理または記録保存は，モバイルアプリケーションが，その製造者によって開発されたサービスから提供されるアプリケーションプログラミングインタフェイスまたはデータベースへのアクセスを要求する状況を含む。そのような場合においては，そのサービスは，リモートのデータ処理ソリューションとして，この規則の適用範囲内にある。それゆえ，この規則の適用範囲内にあるリモートのデータ処理ソリューションと関係する諸要件は，製造者のネットワーク及び情報システム全体の防護に対して呈されるリスクを管理することを狙いとする技術上の措置，運営管理上の措置及び組織上の措置を伴わない。

The purpose of this Regulation is to ensure a high level of cybersecurity of products with digital elements and their integrated remote data processing solutions. Such remote data processing solutions should be defined as data processing at a distance for which the software is designed and developed by or on behalf of the manufacturer of the product with digital elements concerned, the absence of which would prevent the product with digital elements from performing one of its functions. That approach ensures that such products are adequately secured in their entirety by their manufacturers, irrespective of whether data is processed or stored locally on the user's device or remotely by the manufacturer. At the same time, processing or storage at a distance falls within the scope of this Regulation only in so far as it is necessary for a product with digital elements to perform its functions. Such processing or storage at a distance includes the situation where a mobile application requires access to an application programming interface or to a database provided by means of a service developed by the manufacturer. In such a case, the service falls within the scope of this Regulation as a remote data processing solution. The requirements concerning the remote data processing solutions falling within the scope of this Regulation do therefore not entail technical, operational or organisational measures aiming to manage the risks posed to the security of a manufacturer's network and information systems as a whole.

クラウドソリューションは，当該クラウドソリューションがこの規則の中で定められた定義に適合する場

合に限り，この規則の意味におけるリモートのデータ処理ソリューションを構成する。例えば，その利用者が隔地でその機器の管理をできるようにするスマートホーム機器の製造者から提供されるクラウドが実現可能化する機能は，この規則の適用範囲内にある。他方において，デジタルの要素をもつ製品の機能を支えない Web サイト，または，デジタルの要素をもつ製品の製造者の責任の外で設計及び開発されたクラウドサービスは，この規則の適用範囲内にはない。指令(EU) 2022/2555 は，ソフトウェアアズアサービス（SaaS），プラットフォームアズアサービス（PaaS）またはインフラストラクチャアズアサービス（IaaS）のような，クラウドコンピューティングサービス及びクラウドサービスのモデルに対して適用される。欧州連合内でクラウドコンピューティングサービスを提供する法主体であって，勧告 2003/361/EC の別紙の第 2 条の下において中規模企業としての適格性のある法主体，または，同条の第 1 項の中で定められた中規模企業の上限値を超過する法主体は，同指令の適用範囲内にある。

Cloud solutions constitute remote data processing solutions within the meaning of this Regulation only if they meet the definition laid down in this Regulation. For example, cloud enabled functionalities provided by a manufacturer of smart home devices that enable users to control the device at a distance fall within the scope of this Regulation. On the other hand, websites that do not support the functionality of a product with digital elements, or cloud services designed and developed outside the responsibility of a manufacturer of a product with digital elements do not fall within the scope of this Regulation. Directive (EU) 2022/2555 applies to cloud computing services and cloud service models, such as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). Entities providing cloud computing services in the Union which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, fall within the scope of that Directive.

(13) デジタルの要素をもつ製品の支障のない移動を妨げる障碍を除去するためのこの規則の目的に沿って，構成国は，この規則によって包摂される事項に関し，この規則を遵守するデジタルの要素をもつ製品を市場において利用できるようにすることを妨げてはならない。それゆえ，この規則によって整合化される事項に関し，構成国は，デジタルの要素をもつ製品を市場において利用できるようにするための付加的なサイバーセキュリティ要件を課し得ない。ただし，公的な法主体または民間の法主体は，当該法主体の個別の目的のためのデジタルの要素をもつ製品の調達または利用のための，この規則の中で定められた要件への付加的な要件を設けることができ，また，それゆえ，この規則の下で市場において利用できるようにするために適用されるサイバーセキュリティ要件よりも厳格で，かつ，より個別的なサイバーセキュリティ要件に適合するデジタルの要素をもつ製品を利用することを選択できる。欧州議会及び理事会の指令 2014/24/EU[7]及び指令 2014/25/EU[8]を妨げることなく，

[7] 公共調達に関する及び指令 2004/18/EC を廃止する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/24/EU (OJ L 94, 28.3.2014, p. 65).
Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

[8] 水，エネルギー，輸送及び郵便サービスの各部門において業務運営する法主体による調達に関する及び指令 2004/17/EC を廃止する欧州議会及び理事会の 2014 年 2 月 26 日の指令 2014/25/EU (OJ L 94, 28.3.2014, p. 243).
Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in

脆弱性の取扱いと関連する要件を含め，この規則の中で定められた必須のサイバーセキュリティ要件を遵守しなければならないデジタルの要素をもつ製品を調達するときは，構成国は，その公共調達の過程においてそのような要件が考慮に入れられること，そして，サイバーセキュリティ上の方策を実効的に適用するため及びサイバー脅威を管理するための製造者の能力も考慮に入れられることを確保すべきである。更に，指令(EU) 2022/2555 は，この規則の中で定められたサイバーセキュリティ要件よりも厳格なサイバーセキュリティ要件に適合するデジタルの要素をもつ製品のそのような法主体による利用を要求するサプライチェーンのセキュリティ措置を伴い得る，同指令の第 3 条に示す基礎法主体及び重要法主体に関するサイバーセキュリティ上のリスク管理措置を定めている。それゆえ，指令(EU) 2022/2555 に従って，かつ，同指令のミニマムの整合化という基本原則に沿って，構成国は，そのような要件が欧州連合法の中で定められた構成国の義務と一貫性があることを条件として，より高いレベルのサイバーセキュリティを確保するため，同指令によって，基礎法主体または重要法主体による情報通信技術（ICT）製品の利用に関する付加的なサイバーセキュリティ要件を課し得る。この規則の適用のない事項は，デジタルの要素をもつ製品及びその製造者と関連する非技術的な諸要素を含め得る。それゆえ，構成国は，デジタルの要素をもつ製品またはそのような製品の供給者に対する制限を含め，非技術的な諸要素を考慮に入れる国内措置を定め得る。そのような諸要素と関連する国内措置は，欧州連合法を遵守することを要する。

In line with the objective of this Regulation to remove obstacles to the free movement of products with digital elements, Member States should not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply with this Regulation. Therefore, for matters harmonised by this Regulation, Member States cannot impose additional cybersecurity requirements for the making available on the market of products with digital elements. Any entity, public or private, can however establish additional requirements to those laid down in this Regulation for the procurement or use of products with digital elements for its specific purposes, and can therefore choose to use products with digital elements that meet stricter or more specific cybersecurity requirements than those applicable for the making available on the market under this Regulation. Without prejudice to Directives 2014/24/EU[7] and 2014/25/EU[8] of the European Parliament and of the Council, when procuring products with digital elements, which must comply with the essential cybersecurity requirements laid down in this Regulation, including those relating to vulnerability handling, Member States should ensure that such requirements are taken into consideration in the procurement process and that the manufacturers' ability to effectively apply cybersecurity measures and manage cyber threats are also taken into consideration. Furthermore, Directive (EU) 2022/2555 sets out cybersecurity risk-management measures for essential and important entities as referred to in Article 3 of that Directive that could entail supply chain security measures that require the use by such entities of products with digital elements meeting stricter cybersecurity requirements than those laid down in this Regulation. In accordance with Directive (EU) 2022/2555 and in line with its minimum harmonisation principle, Member States can therefore impose additional cybersecurity requirements for the use of information and communications technology (ICT) products by essential or important entities pursuant to that Directive in order to ensure a higher level of cybersecurity, provided that such requirements are consistent with Member States' obligations laid down in Union law. Matters not covered by this Regulation can include non-technical factors relating to products with digital elements and the manufacturers thereof.

---

the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243).

Member States can therefore lay down national measures, including restrictions on products with digital elements or suppliers of such products that take account of non-technical factors. National measures relating to such factors are required to comply with Union law.

(14) この規則は，欧州連合法を遵守して，国家安全保障を安全確保することに関する構成国の責任を妨げてはならない。そのような措置が欧州連合法の中で定められた構成国の義務と一貫性があることを条件として，構成国は，国家安全保障の目的または国防の目的のために調達または利用されるデジタルの要素をもつ製品を付加的な措置に服させ得るべきである。

This Regulation should be without prejudice to the Member States' responsibility for safeguarding national security, in compliance with Union law. Member States should be able to subject products with digital elements that are procured or used for national security or defence purposes to additional measures, provided that such measures are consistent with Member States' obligations laid down in Union law.

(15) この規則は，市場において利用できるようにされたデジタルの要素をもつ製品との関係においてのみ，従って，商業活動の過程において欧州連合の市場で流通または利用のために供給されたデジタルの要素をもつ製品との関係においてのみ，経済取引主体に対して適用される。商業活動の過程における供給は，デジタルの要素をもつ製品に対する対価の請求によって特徴づけられるだけではなく，実費の回収のためにのみ奉仕するのではない技術支援のサービスに対する対価の請求によって，例えば，そのプラットフォームを介して製造者が別のサービスを収益化するソフトウェアプラットフォームを提供することによる，収益化の意図によっても，専らそのソフトウェアのセキュリティ，互換性もしくは相互運用性を向上させるためという理由以外の理由により個人データの処理を利用するための条件を要求することによっても，または，デジタルの要素をもつ製品の設計，開発及び提供と関係する費用を超過する寄付を受けることによっても特徴づけられ得る。利益を得る意図なく寄付を受けることは，商業活動であると判断されてはならない。

This Regulation applies to economic operators only in relation to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. Supply in the course of a commercial activity might be characterised not only by charging a price for a product with digital elements, but also by charging a price for technical support services where this does not serve only the recuperation of actual costs, by an intention to monetise, for instance by providing a software platform through which the manufacturer monetises other services, by requiring as a condition for use the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, or by accepting donations exceeding the costs associated with the design, development and provision of a product with digital elements. Accepting donations without the intention of making a profit should not be considered to be a commercial activity.

(16) 行政機関である法主体から提供される一定のデジタルの要素をもつ製品がそのような場合であり得るように，当該サービスの運用と直接に関連する実費の回収のためにのみ当該サービスに関して手数料が請求されるサービスの供給の一部として提供されるデジタルの要素をもつ製品は，この規則の目的のために，そのことのみを根拠として商業活動であると判断されてはならない。更に，専ら当

該法主体の利用のために行政機関である法主体によって開発または改修されるデジタルの要素をもつ製品は，この規則の意味において市場において利用できるようにされていると判断されてはならない。

Products with digital elements provided as part of the delivery of a service for which a fee is charged solely to recover the actual costs directly related to the operation of that service, such as may be the case with certain products with digital elements provided by public administration entities, should not be considered on those grounds alone to be a commercial activity for the purposes of this Regulation. Furthermore, products with digital elements which are developed or modified by a public administration entity exclusively for its own use should not be considered to be made available on the market within the meaning of this Regulation.

(17) オープンに共有されており，かつ，利用者が，その場では無料で，当該ソフトウェア及びデータにアクセスし，それを使用し，修正及び再配布し，または，そのバージョンを変更できるソフトウェア及びデータは，市場における調査研究及び技術革新に寄与し得る。とりわけ，スタートアップを含め，マイクロ企業，小企業及び中規模企業による，並びに，個人，非営利組織及び学術上の調査研究組織による，無料でオープンソースのソフトウェアの開発及び配置を育成するため，商業活動の過程における流通または利用のために供給される無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品に対するこの規則の適用は，無料でオープンソースのソフトウェアの利用許諾の下において配布及び開発されるソフトウェアの異なる開発モデルの性質を考慮に入れるべきである。

Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. To foster the development and deployment of free and open-source software, in particular by microenterprises and small and medium-sized enterprises, including start-ups, individuals, not-for-profit organisations, and academic research organisations, the application of this Regulation to products with digital elements qualifying as free and open-source software supplied for distribution or use in the course of a commercial activity should take into account the nature of the different development models of software distributed and developed under free and open-source software licences.

(18) 無料でオープンソースのソフトウェアは，当該ソフトウェアのソースコードがオープンに共有されており，かつ，そのソースコードを，無料でアクセス可能にし，利用可能にし，修正可能にし，そして，再配布可能にするための全ての権利を当該ソフトウェアの利用許諾が提供しているソフトウェアとして理解されている。無料でオープンソースのソフトウェアは，オンラインプラットフォームを介する場合を含め，オープンに開発され，維持管理され，そして，配布される。この規則の適用のある経済取引主体との関係においては，市場において利用できるようにされ，そして，それゆえに商業活動の過程において流通または利用のために供給された無料でオープンソースのソフトウェアのみが，この規則の適用範囲内にあるべきである。それゆえ，その状況の下でそのデジタルの要素をもつ製品が開発された単なる状況，または，その開発がどのように資金提供を受けたかは，当該活動の商業上の性質または非商業上の性質を判定する際に考慮に入れられてはならない。より具体的には，この規則の目的のために，かつ，この規則の適用範囲内にある経済取引主体との関係において，開発段階と供

給段階との間に明確な区分が存在することを確保するため，そのソフトウェアの製造者によって収益化されていない無料でオープンソースのソフトウェアとして適格なデジタルの要素をもつ製品の提供は，商業活動であると判断されてはならない。更に，別の製造者によって当該別の製造者自身のデジタルの要素をもつ製品の中に組み込まれることが意図されている無料でオープンソースのソフトウェアのコンポーネントとして適格なデジタルの要素をもつ製品の供給は，そのコンポーネントの最初の製造者によってそのコンポーネントが収益化されているときに限り，市場において利用できるようにされていると判断されるべきである。例えば，デジタルの要素をもつオープンソースのソフトウェア製品が製造者から資金上の支援を受けているということ，または，製造者がそのような製品の開発に寄与しているということは，そのことだけでは，その活動が商業的な性質をもつものであると判定してはならない。加えて，定期的なリリースが存在するということは，そのことだけでは，デジタルの要素をもつ製品が商業活動の過程において供給されているという結論を導いてはならない。最後に，この規則の目的のために，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品の非営利団体による開発は，費用控除後の収益の全てが非営利の目的を達成するために使用されることが確保される方法でその団体が設立されていることを条件として，商業活動であると判断されてはならない。この規則は，当該の者の責任の下にはない無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品のためにソースコードを寄付する自然人または法人に対しては適用されない。

Free and open-source software is understood as software the source code of which is openly shared and the licensing of which provides for all rights to make it freely accessible, usable, modifiable and redistributable. Free and open-source software is developed, maintained and distributed openly, including via online platforms. In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity, should fall within the scope of this Regulation. The mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial or non-commercial nature of that activity. More specifically, for the purposes of this Regulation and in relation to the economic operators that fall within its scope, to ensure that there is a clear distinction between the development and supply phases, the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity. Furthermore, the supply of products with digital elements qualifying as free and open-source software components intended for integration by other manufacturers into their own products with digital elements should be considered to be making available on the market only if the component is monetised by its original manufacturer. For instance, the mere fact that an open-source software product with digital elements receives financial support from manufacturers or that manufacturers contribute to the development of such a product should not in itself determine that the activity is of commercial nature. In addition, the mere presence of regular releases should not in itself lead to the conclusion that a product with digital elements is supplied in the course of a commercial activity. Finally, for the purposes of this Regulation, the development of products with digital elements qualifying as free and open-source software by not-for-profit organisations should not be considered to be a commercial activity provided that the organisation is set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives. This Regulation does not apply to natural or legal persons who contribute with source code to products with digital elements qualifying as free and open-source software that are not

under their responsibility.

(19) 発行されているけれども，この規則の意味における市場において利用できるようにされていない無料でオープンソースとしての適格のあるデジタルの要素をもつ多数の製品のサイバーセキュリティに関する重要性を考慮に入れ，そのような商業活動を意図する製品の開発のための持続的な基盤に対する支援を提供する法人であって，当該製品の存続を確保する上での主要な役割を果たす者（「オープンソースソフトウェアスチュワード」）は，軽いタッチで個別対応の法制度に服するべきである。オープンソースソフトウェアスチュワードは，非営利の法主体を含め，企業活動の過程において無料でオープンソースのソフトウェアを開発及び発行する一定の財団及び法主体を含む。その法制度は，当該法主体の個別の性質，及び，課される義務のタイプとの互換性を考慮に入れるべきである。その法制度は，商業サービスへの統合またはデジタルの要素をもつ収益化製品への統合のような，最終的には商業活動を意図している無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品のみを包摂すべきである。同法制度の目的のために，デジタルの要素をもつ収益化製品に組み込む意図は，当該製造者自身のデジタルの要素をもつ製品の中にコンポーネントを組み込む製造者が当該コンポーネントの開発に対して定期的に寄付する場合またはソフトウェア製品の継続性を確保するために定期的な資金支援を提供する場合を含む。デジタルの要素をもつ製品の開発への持続的な支援の提供は，ソフトウェアの共同開発プラットフォームのホスティング及び運営管理，ソースコードまたはソフトウェアのホスティング，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品の統治または運営管理，並びに，そのような製品の開発の舵取りを含むが，それらに限定されない。軽いタッチで個別対応の法制度が，オープンソースソフトウェアスチュワードとして活動している者をこの規則の下にある製造者として活動している者と同一の義務に服させていないことに鑑み，オープンソースソフトウェアスチュワードは，当該オープンソースソフトウェアスチュワードがその開発を支援するデジタルの要素をもつ製品に対して CE マークを付すことを認められてはならない。

Taking into account the importance for cybersecurity of many products with digital elements qualifying as free and open-source software that are published, but not made available on the market within the meaning of this Regulation, legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities. The regulatory regime should take account of their specific nature and compatibility with the type of obligations imposed. It should only cover products with digital elements qualifying as free and open-source software that are ultimately intended for commercial activities, such as for integration into commercial services or into monetised products with digital elements. For the purposes of that regulatory regime, an intention for integration into monetised products with digital elements includes cases where manufacturers that integrate a component into their own products with digital elements either contribute to the development of that component in a regular manner or provide regular financial assistance to ensure the continuity of a software product. The provision of sustained support to the development of a product with digital elements includes but is not limited to the hosting and managing of software development collaboration platforms, the hosting of source code or software, the governing or managing of products

with digital elements qualifying as free and open-source software as well as the steering of the development of such products. Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.

(20) パッケージマネジャーを介する場合または共同開発プラットフォーム上の場合を含め，オープンなリポジトリ上においてデジタルの要素をもつ製品をホスティングしているという行為は，その行為だけでは，デジタルの要素をもつ製品を市場において利用できるようにしていることを構成しない。そのようなサービスの提供者は，当該提供者がそのようなソフトウェアを市場において利用できるようにしており，従って，商業活動の過程において，流通または利用のために，欧州連合の市場にそのソフトウェアを提供している場合に限り，流通業者であると判断されるべきである。

The sole act of hosting products with digital elements on open repositories, including through package managers or on collaboration platforms, does not in itself constitute the making available on the market of a product with digital elements. Providers of such services should be considered to be distributors only if they make such software available on the market and hence supply it for distribution or use on the Union market in the course of a commercial activity.

(21) この規則の中で定められた必須のサイバーセキュリティ要件に服さない無料でオープンソースのソフトウェアのコンポーネントを当該製造者のデジタルの要素をもつ製品の中に組み込む製造者のデューディリジェンスを支援及び促進するため，欧州委員会は，この規則を補完する委任される行為により，または，規則(EU) 2019/881 の第 48 条による無料でオープンソースのソフトウェア開発モデルの特性を考慮に入れる欧州サイバーセキュリティ認証制度を要求することにより，任意のセキュリティ証明書発行プログラムを設け得るべきである。そのセキュリティ証明書発行プログラムは，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品を開発している自然人もしくは法人またはその開発に寄与している自然人もしくは法人だけではなく，当該製造者自身のデジタルの要素をもつ製品の中にそのような製品を組み込む製造者，利用者または欧州連合の行政機関及び国内行政機関のような第三者もまた，セキュリティ証明書発行を開始し，または，その発行に資金提供し得るような方法で検討されるべきである。

In order to support and facilitate the due diligence of manufacturers that integrate free and open-source software components that are not subject to the essential cybersecurity requirements set out in this Regulation into their products with digital elements, the Commission should be able to establish voluntary security attestation programmes, either by a delegated act supplementing this Regulation or by requesting a European cybersecurity certification scheme pursuant to Article 48 of Regulation (EU) 2019/881 that takes into account the specificities of the free and open-source software development models. The security attestation programmes should be conceived in such a way that not only natural or legal persons developing or contributing to the development of a product with digital elements qualifying as free and open-source software can initiate or finance a security attestation but also third parties, such as manufacturers that integrate such products into their own products with digital elements, users, or Union and national public administrations.

(22) この規則のサイバーセキュリティ上の公共の目的を考慮し，かつ，ソフトウェアコンポーネントに対す

る欧州連合の依存に関する，とりわけ，潜在的に無料でオープンソースのソフトウェアのコンポーネントに対する欧州連合の依存に関する構成国の状況認識を向上させるため，この規則によって設けられる行政協力専門グループ（ADCO）は，欧州連合の依存性評価を共同して行うことを決定できるべきである。市場監視当局は，ADCO によって策定される類型のデジタルの要素をもつ製品の製造者に対し，この規則により当該製造者が生成したソフトウェア素材表（SBOMs）を提出することを要請できるべきである。SBOMs の機密性を保護するため，市場監視当局は，ADCO に対し，匿名化されかつ集約された態様で，依存性に関する適格な情報を提出すべきである。

In view of the public cybersecurity objectives of this Regulation and in order to improve the situational awareness of Member States as regards the Union's dependency on software components and in particular on potentially free and open-source software components, a dedicated administrative cooperation group (ADCO) established by this Regulation should be able to decide to jointly undertake a Union dependency assessment. Market surveillance authorities should be able to request manufacturers of categories of products with digital elements established by ADCO to submit the software bills of materials (SBOMs) that they have generated pursuant to this Regulation. In order to protect the confidentiality of SBOMs, market surveillance authorities should submit relevant information about dependencies to ADCO in an anonymised and aggregated manner.

(23) この規則の実装の実効性もまた，適切なサイバーセキュリティ技能の可用性に依存することになる。欧州連合レベルにおいて，EU の競争力，成長及び回復力を加速するためにサイバーセキュリティの人材格差を縮小させることに関する 2023 年 4 月 18 日の委員会通知並びに EU のサイバー防衛政策に関する 2023 年 5 月 22 日の理事会決議を含め，様々な計画文書及び政治文書は，公的部門と民間部門の両者において，欧州連合内におけるサイバーセキュリティ技能の格差及びそのような検討課題に対して優先事項として対処すべき必要性を認めた。この規則の実効的な実装を確保するという観点から，構成国は，市場監視当局及び適合性評価組織が，この規則の中で定められたそれら当局及び組織の職務を遂行するための適切な職員配置のために十分な資源を利用できることを確保すべきである。それらの措置は，サイバーセキュリティの分野における労働力の流動性及び当該労働者が関係するキャリアパスを拡大すべきである。構成国は，ジェンダーの面においても，サイバーセキュリティの労働力をより回復力がありかつ包摂的にすることにも貢献すべきである。それゆえ，構成国は，それらの職務が，必要なサイバーセキュリティ技能をもち，十分に訓練を受けた職業人によって遂行されることを確保するための措置を講ずるべきである。同様に，製造者は，当該製造者の職員が，この規則の中で定められた製造者の義務を遵守するために必要となる技能をもつことを確保すべきである。構成国及び欧州委員会は，構成国及び欧州委員会の特権及び職務権限並びにこの規則によって付与された個々の職務に沿って，技能開発のような分野においても，この規則の中で定められた製造者の義務を遵守するため，製造者，並びに，とりわけ，スタートアップを含め，マイクロ企業，小企業及び中規模企業を支援するための措置を講ずるべきである。更に，指令(EU) 2022/2555 は，構成国に対し，構成国の国内サイバーセキュリティ戦略の一部として，サイバーセキュリティに関する訓練及びサイバーセキュリティ技能を促進及び開発する基本方針を採択することを要求しているので，構成国は，そのような戦略を採択する際，技能の再習得及び技能向上と関連する需要を含め，この規則から生ずるサイバーセキュリティ技能の需要に対処することも検討できる。

The effectiveness of the implementation of this Regulation will also depend on the availability of adequate cybersecurity skills. At Union level, various programmatic and political documents, including the Commission communication of 18 April 2023 on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience and the Council Conclusions of 22 May 2023 on the EU Policy on Cyber Defence acknowledged the cybersecurity skills gap in the Union and the need to address such challenges as a matter of priority, in both the public and private sectors. With a view to ensuring an effective implementation of this Regulation, Member States should ensure that adequate resources are available for the appropriate staffing of the market surveillance authorities and conformity assessment bodies to perform their tasks as laid down in this Regulation. Those measures should enhance workforce mobility in the cybersecurity field and their associated career pathways. They should also contribute to making the cybersecurity workforce more resilient and inclusive, also in terms of gender. Member States should therefore take measures to ensure that those tasks are carried out by adequately trained professionals, with the necessary cybersecurity skills. Similarly, manufacturers should ensure that their staff has the necessary skills to comply with their obligations as laid down in this Regulation. Member States and the Commission, in line with their prerogatives and competences and the specific tasks conferred upon them by this Regulation, should take measures to support manufacturers and in particular microenterprises and small and medium-sized enterprises, including start-ups, also in areas such as skill development, for the purposes of compliance with their obligations as laid down in this Regulation. Furthermore, as Directive (EU) 2022/2555 requires Member States to adopt policies promoting and developing training on cybersecurity and cybersecurity skills as part of their national cybersecurity strategies, Member States may also consider, when adopting such strategies, addressing the cybersecurity skills needs resulting from this Regulation, including those relating to re-skilling and up-skilling.

(24) 安全なインターネットは，不可欠インフラの稼働のために，そして，社会全体のために，欠かすことができない。指令(EU) 2022/2555 は，オープンなインターネットのコア機能を支え，インターネットアクセスを確保し及びインターネットサービスを提供するデジタルインフラのプロバイダを含め，同指令の第 3 条に示す基本法主体及び重要法主体から提供されるサービスの高いレベルのサイバーセキュリティを確保することを狙いとしている。それゆえ，インターネットの稼働を確保するためにデジタルインフラのプロバイダにとって必要なデジタルの要素をもつ製品が安全な態様で開発されること，そして，デジタルインフラのプロバイダがインターネットのセキュリティの確立された技術標準を遵守することが重要である。ネット接続可能な全てのハードウェア製品及びソフトウェア製品に適用されるこの規則は，当該プロバイダのサービスの提供のために当該プロバイダが使用するデジタルの要素をもつ製品が安全な態様で開発されることを確保すること，及び，そのような製品のセキュリティアップデートに対して当該プロバイダが適時のアクセスをもつことを確保することによって，デジタルインフラのプロバイダによる指令(EU) 2022/2555 の下にあるサプライチェーンの要件の遵守を容易にすることも狙いとしている。

A secure internet is indispensable for the functioning of critical infrastructures and for society as a whole. Directive (EU) 2022/2555 aims at ensuring a high level of cybersecurity of services provided by essential and important entities as referred to in Article 3 of that Directive, including digital infrastructure providers that support core functions of the open internet, ensure internet access and provide internet services. It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the internet are developed in a secure

manner and that they comply with well-established internet security standards. This Regulation, which applies to all connectable hardware and software products, also aims at facilitating the compliance of digital infrastructure providers with the supply chain requirements under Directive (EU) 2022/2555 by ensuring that the products with digital elements that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

(25) 欧州議会及び理事会の規則(EU) 2017/745[9]は，医療機器に関する規定を定めており，また，欧州議会及び理事会の規則(EU) 2017/746[10]は，体外診断用医療機器に関する規定を定めている。それらの規則は，サイバーセキュリティ上のリスクに対応しており，かつ，この規則の中においても対処されている特別のアプローチに従っている。より具体的には，規則(EU) 2017/745 及び規則(EU) 2017/746 は，電子システムを介して機能する医療機器またはそれ自体としてソフトウェアである医療機器に関する必須の要件を定めている。一定の非組込ソフトウェア及び全ライフサイクルのアプローチもまた，それらの規則によって包摂されている。それらの要件は，製造者に対し，リスクマネジメントの基本原則を適用することによって，そして，IT セキュリティの措置と関係する要件及びそれと対応する適合性評価手続を設けることによって，当該製造者の製品を開発及び構築することを命じている。更に，2019 年 12 月以降，医療機器のサイバーセキュリティに関する個別のガイドが定められており，体外診断用医療機器を含め，医療機器の製造者に対し，サイバーセキュリティと関連してそれらの規則の別紙 I の中で定められた適格な必須の要件の全てをどのようにして満たすかに関するガイドを提供している。それゆえ，それらの規則のいずれかが適用されるデジタルの要素をもつ製品は，この規則に服してはならない。

Regulation (EU) 2017/745 of the European Parliament and of the Council[(9)] lays down rules on medical devices and Regulation (EU) 2017/746 of the European Parliament and of the Council [(10)] lays down rules on in vitro diagnostic medical devices. Those Regulations address cybersecurity risks and follow particular approaches that are also addressed in this Regulation. More specifically, Regulations (EU) 2017/745 and (EU) No 2017/746 lay down essential requirements for medical devices that function through an electronic system or that are software themselves. Certain non-embedded software and the whole lifecycle approach are also covered by those Regulations. Those requirements mandate manufacturers to develop and build their products by applying risk management principles and by setting out requirements concerning IT security measures, as well as corresponding conformity assessment procedures. Furthermore, specific guidance on cybersecurity for medical devices is in place since December 2019, providing

[9] 医療機器に関する，指令 2001/83/EC，規則(EC) No 178/2002 及び規則(EC) No 1223/2009 を改正する，並びに，理事会指令 90/385/EEC 及び理事会指令 93/42/EEC を廃止する欧州議会及び理事会の 2017 年 4 月 5 日の規則(EU) 2017/745 (OJ L 117, 5.5.2017, p. 1).

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).

[10] 体外診断用医療機器に関する，並びに，指令 98/79/EC 及び委員会決定 2010/227/EU を廃止する欧州議会及び理事会の 2017 年 4 月 5 日の規則(EU) 2017/746 (OJ L 117, 5.5.2017, p. 176).

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

manufacturers of medical devices, including in vitro diagnostic devices, with guidance on how to fulfil all the relevant essential requirements set out in Annex I to those Regulations with regard to cybersecurity. Products with digital elements to which either of those Regulations apply should not therefore be subject to this Regulation.

(26) 専ら国家安全保障の目的もしくは国防の目的のために開発されもしくは修正されているデジタルの要素をもつ製品または機密情報の処理のために特別に設計された製品は，この規則の適用範囲の外にある。構成国は，それらの製品に関し，この規則の適用範囲内にある製品と同一のレベルまたはそれ以上のレベルの保護を確保することが推奨される。

Products with digital elements that are developed or modified exclusively for national security or defence purposes or products that are specifically designed to process classified information fall outside the scope of this Regulation. Member States are encouraged to ensure the same or a higher level of protection for those products as for those falling within the scope of this Regulation.

(27) 欧州議会及び理事会の規則(EU) 2019/2144[11]は，車両の型式承認及び車両のシステムとコンポーネントの型式承認の要件を定めており，認証を受けたサイバーセキュリティマネジメントシステムの運用に関する要件を含め，ソフトウェアのアップデートに関する一定のサイバーセキュリティ要件を導入し，技術仕様及びサイバーセキュリティに関する適用可能な国連の規則，とりわけ，国連規則第 155 号ーサイバーセキュリティ及びサイバーセキュリティマネジメントシステムと関連する車両の承認に関する統一条項[12]を遵守する車両，機器及びサービスの全ライフサイクルと関連するサイバーセキュリティリスクに関する組織の基本方針及び処理を包摂し，そして，個別の適合性評価手続を定めている。航空の分野において，欧州議会及び理事会の規則(EU) 2018/1139[13]の主たる目的は，欧州連合にお

[11] 車両等の一般的な安全及び車両の乗員と脆弱性のある道路利用者の保護と関連する，自走車両，自走車両の運搬車両，そのような車両に使用されることが意図されたシステム，コンポーネント及び個別の技術ユニットの型式承認の要件に関する，並びに，欧州議会及び理事会の規則(EU) 2018/858 を改正し，欧州議会及び理事会の規則(EC) No 78/2009，規則(EC) No 79/2009 及び規則(EC) No 661/2009，委員会規則(EC) No 631/2009，委員会規則(EU) No 406/2010，委員会規則(EU) No 672/2010，委員会規則(EU) No 1003/2010，委員会規則(EU) No 1005/2010，委員会規則(EU) No 1008/2010，委員会規則(EU) No 1009/2010，委員会規則(EU) No 19/2011，委員会規則(EU) No 109/2011，委員会規則(EU) No 458/2011，委員会規則(EU) No 65/2012，委員会規則(EU) No 130/2012，委員会規則(EU) No 347/2012，委員会規則(EU) No 351/2012，委員会規則(EU) No 1230/2012 及び委員会規則(EU) 2015/166 を廃止する欧州議会及び理事会の 2019 年 11 月 27 日の規則(EU) 2019/2144 (OJ L 325, 16.12.2019, p. 1).
Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

[12] OJ L 82, 9.3.2021, p. 30.

[13] 民間航空の分野における共通規定に関する，欧州連合航空安全局を設置する，並びに，欧州議会及び理事

ける統一的かつ高いレベルの民間航空の安全性を確立すること及び維持することである。同規則は，ソフトウェアを含め，航空用の製品，部品，装置の耐空性に関し，情報セキュリティ上の脅威に抗して保護すべき義務を含む必須の要件の枠組みを創設している。規則(EU) 2018/1139 の下にある認証過程は，この規則によって狙いとされている保証のレベルを確保している。それゆえ，規則(EU) 2019/2144 が適用されるデジタルの要素をもつ製品及び規則(EU) 2018/1139 に従って認証される製品は，この規則の中で定められた必須のサイバーセキュリティ要件及び適合性評価手続に服さない。

Regulation (EU) 2019/2144 of the European Parliament and of the Council [11] establishes requirements for the type-approval of vehicles, and of their systems and components, introducing certain cybersecurity requirements, including on the operation of a certified cybersecurity management system, on software updates, covering organisations' policies and processes for cybersecurity risks related to the entire lifecycle of vehicles, equipment and services in compliance with the applicable United Nations regulations on technical specifications and cybersecurity, in particular UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [12] and providing for specific conformity assessment procedures. In the area of aviation, the principal objective of Regulation (EU) 2018/1139 of the European Parliament and of the Council [13] is to establish and maintain a high uniform level of civil aviation safety in the Union. It creates a framework for essential requirements for airworthiness for aeronautical products, parts and equipment, including software, that includes obligations to protect against information security threats. The certification process under Regulation (EU) 2018/1139 ensures the level of assurance aimed for by this Regulation. Products with digital elements to which Regulation (EU) 2019/2144 applies and products certified in accordance with Regulation (EU) 2018/1139 should not therefore be subject to the essential cybersecurity requirements and conformity assessment procedures set out in this Regulation.

(28) この規則は，部門または一定のデジタルの要素をもつ製品を限定しない横断的なサイバーセキュリティの規定を定めている。それにも拘わらず，この規則の中で定められた必須のサイバーセキュリティ要件が適用されるリスクの全部または幾つかに対処する要件を定める，部門別のまたは製品に特化した欧州連合の規定が導入され得る。そのような場合において，そのような制限または適用除外が当該デジタルの要素をもつ製品に対して適用される法制枠組み全体と一貫性をもつ場合，及び，その部門別の規定が，少なくとも，この規則によって定められた保護と同一のレベルの保護を達成している場合，この規則の中で定められた必須のサイバーセキュリティ要件が適用されるリスクの全部または幾つかに対処する要件を定める他の欧州連合の規定によって包摂されるデジタルの要素をもつ製品に対するこの規則の適用は，制限を受けまたは適用除外され得る。欧州委員会は，そのよ

会の規則(EC) No 2111/2005，規則(EC) No 1008/2008，規則(EU) No 996/2010，規則(EU) No 376/2014 並びに指令 2014/30/EU 及び指令 2014/53/EU を改正し，欧州議会及び理事会の規則(EC) No 552/2004 及び規則(EC) No 216/2008 並びに理事会規則(EEC) No 3922/91 を廃止する欧州議会及び理事会の 2018 年 7 月 4 日の規則(EU) 2018/1139 (OJ L 212, 22.8.2018, p. 1).

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

うな製品及び規定を特定することによってこの規則を補完するための委任される行為を採択する権限が与えられるべきである。そのような制限または適用除外が適用されるべきである既存の欧州連合法に関し，この規則は，この規則と当該欧州連合法との間の関係を明確にするための細目的な条項を含んでいる。

This Regulation lays down horizontal cybersecurity rules which are not specific to sectors or to certain products with digital elements. Nevertheless, sectoral or product-specific Union rules could be introduced, laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in this Regulation. In such cases, the application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in this Regulation may be limited or excluded where such limitation or exclusion is consistent with the overall regulatory framework applying to those products and where the sectoral rules achieve at least the same level of protection as the one provided for by this Regulation. The Commission should be empowered to adopt delegated acts to supplement this Regulation by identifying such products and rules. For existing Union law where such limitation or exclusion should apply, this Regulation contains specific provisions to clarify its relation with that Union law.

(29) 市場において利用できるようにされたデジタルの要素をもつ製品が，実効的に修理され得ること及び当該製品の耐久性が拡張され得ることを確保するため，交換部品に関しては，適用除外が定められるべきである。その適用除外は，この規則の適用の日よりも前に利用できるようにされた旧式の製品を修理する目的をもつ交換部品及びこの規則による適合性評価手続を既に受けた交換部品の両者を包摂すべきである。

In order to ensure that products with digital elements made available on the market can be repaired effectively and their durability extended, an exemption should be provided for spare parts. That exemption should cover both spare parts that have the purpose of repairing legacy products made available before the date of application of this Regulation and spare parts that have already undergone a conformity assessment procedure pursuant to this Regulation.

(30) 委員会委任規則(EU) 2022/30[14]は，ネットワーク上の危害及びネットワーク資源の濫用，個人データとプライバシー並びに詐欺と関連して欧州議会及び理事会の指令 2014/53/EU[15]の第 3 条第 3 項の(d), (e)及び(f)の中で定められた多数の必須の要件を一定の無線機器に対して適用することを定めてい

[14] 欧州議会及び理事会の指令 2014/53/EU の第 3 条第 3 項の(d), (e)及び(f)に示す必須の要件の適用と関連して同指令を補完する 2021 年 10 月 29 日の委員会委任規則(EU) 2022/30 (OJ L 7, 12.1.2022, p. 6).
Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (OJ L 7, 12.1.2022, p. 6).

[15] 無線機器を市場において利用できるようにすることと関連する構成国の法律の整合化に関する及び指令 1999/5/EC を廃止する欧州議会及び理事会の 2014 年 4 月 16 日の指令 2014/53/EU (OJ L 153, 22.5.2014, p. 62).
Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

る。欧州標準化委員会及び電気技術の標準に関する欧州の委員会に対する標準化の要請に関する 2022 年 8 月 5 日の委員会実装決定 C(2022) 5637 は，それらの必須の要件がどのように対処されるべきかを別に定める個々の技術標準の策定のための要件を定めている。この規則の中で定められた必須のサイバーセキュリティ要件は，指令 2014/53/EU の第 3 条第 3 項の(d), (e)及び(f)の中で示された必須の要件の全ての要素を含んでいる。更に，この規則の中で定められた必須のサイバーセキュリティ要件は，同標準化の要請の中に含められる個々の技術標準の要件の対象と揃えられている。それゆえ，欧州委員会が委任規則(EU) 2022/30 を廃止し，または，この規則に服する一定の製品に対する同委員会委任規則の適用を終了する結果となる改正をするときは，欧州委員会及び欧州の標準化組織は，この規則の実装を容易にするための整合化された技術標準の準備及び策定において，実装決定 C(2022)5637 の文脈において実施される標準化作業を考慮に入れるべきである。この規則の適用のための移行期間の間に，欧州委員会は，この規則に服し，委任規則(EU) 2022/30 にも服する製造者に対し，2 つの規則の遵守を示すことを容易にするためのガイドを提供すべきである。

Commission Delegated Regulation (EU) 2022/30[14] specifies that a number of essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU of the European Parliament and of the Council[15], relating to network harm and misuse of network resources, personal data and privacy, and fraud, apply to certain radio equipment. Commission Implementing Decision C(2022) 5637 of 5 August 2022 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation lays down requirements for the development of specific standards further specifying how those essential requirements should be addressed. The essential cybersecurity requirements set out in this Regulation include all the elements of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU. Furthermore, the essential cybersecurity requirements set out in this Regulation are aligned with the objectives of the requirements for specific standards included in that standardisation request. Therefore, when the Commission repeals or amends Delegated Regulation (EU) 2022/30 with the consequence that it ceases to apply to certain products subject to this Regulation, the Commission and the European standardisation organisations should take into account the standardisation work carried out in the context of Implementing Decision C(2022) 5637 in the preparation and development of harmonised standards to facilitate the implementation of this Regulation. During the transitional period for the application of this Regulation, the Commission should provide guidance to manufacturers subject to this Regulation that are also subject to Delegated Regulation (EU) 2022/30 to facilitate the demonstration of compliance with the two Regulations.

(31) 欧州議会及び理事会の指令(EU) 2024/2853[16]は，この規則を補完している。同指令は，欠陥のある製品に関し，欠陥のある製品によって損害が生じた場合に被害者が弁償を請求できるようにする法的責任の規定を定めている。同指令は，製品の製造者が，過失の有無に拘わらず，当該製造者の製品の中にある安全性の欠如によって生じた損害に関し法的責任を負うという基本原則（「厳格責任」）

[16] 欠陥のある製品の法的責任に関する及び理事会指令 85/374/EEC を廃止する欧州議会及び理事会の 2024 年 10 月 23 日の指令(EU) 2024/2853 (OJ L, 2024/2853, 18.11.2024).
Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (OJ L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

を定めている。そのような安全性の欠如が，その製品が市場に置かれた後のセキュリティアップデートの欠如を組成しており，かつ，そのことが損害を発生させている場合においては，その製造者の法的責任が発生し得る。そのようなセキュリティアップデートの提供と関係する製造者の義務は，この規則の中で定められるべきである。

Directive (EU) 2024/2853 of the European Parliament and of the Council[16] is complementary to this Regulation. That Directive sets out liability rules for defective products so that injured persons can claim compensation when a damage has been caused by defective products. It establishes the principle that the manufacturer of a product is liable for damages caused by a lack of safety in their product irrespective of fault (strict liability). Where such a lack of safety consists in a lack of security updates after the placing on the market of the product, and this causes damage, the liability of the manufacturer could be triggered. Obligations for manufacturers that concern the provision of such security updates should be laid down in this Regulation.

(32) この規則は，管理者及び処理者による処理の業務運用が欧州議会及び理事会の規則(EU) 2016/679[17]を遵守していることを示す目的のためのデータ保護認証の仕組みの設置に関する条項並びにデータ保護シール及びデータ保護マークに関する条項を含め，同規則を妨げてはならない。そのような業務運用は，デジタルの要素をもつ製品の中に組み込まれ得る。バイデザイン及びバイデフォルトによるデータ保護並びに一般的なサイバーセキュリティは，規則(EU) 2016/679 の鍵となる要素である。サイバーセキュリティ上のリスクから消費者と組織を保護することにより，この規則の中で定められた必須のサイバーセキュリティ要件は，個人データ及び個人のプライバシーの保護を拡大することにも貢献する。欧州委員会，欧州の標準化組織，欧州連合サイバーセキュリティ局（ENISA），規則(EU) 2016/679 によって設けられた欧州データ保護委員会及び国内データ保護監督当局の間における協力を通じて，サイバーセキュリティの標準化の側面及び認証の側面の両者に対する波及効果が検討されるべきである。市場監視及び執行の分野においても，この規則と欧州連合のデータ保護法との間の波及効果がつくり出されるべきである。その目的のために，この規則の下において指定される国内市場監視当局は，欧州連合のデータ保護法の適用を監視する当局と協力すべきである。後者の当局は，当該当局の職務の遂行のために適格な情報へのアクセスももつべきである。

This Regulation should be without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council[17], including to provisions relating to the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance of processing operations by controllers and processors with that Regulation. Such operations could be embedded in a product with digital elements. Data protection by design and by default, and cybersecurity in general, are key elements of Regulation (EU) 2016/679. By protecting

---

[17] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する，並びに，指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）(OJ L 119, 4.5.2016, p. 1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

consumers and organisations from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation are also to contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification of cybersecurity aspects should be considered through the cooperation between the Commission, the European standardisation organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board established by Regulation (EU) 2016/679, and the national data protection supervisory authorities. Synergies between this Regulation and Union data protection law should also be created in the area of market surveillance and enforcement. To that end, national market surveillance authorities designated under this Regulation should cooperate with authorities supervising the application of Union data protection law. The latter should also have access to information relevant for accomplishing their tasks.

(33) 当該提供者の製品がこの規則の適用範囲内にある範囲において，欧州議会及び理事会の規則(EU) No 910/2014[18]の第 5 条 a の第 2 項に示す欧州デジタル識別子ウォレットの提供者は，この規則の中で定められた横断的で必須のサイバーセキュリティ要件と規則(EU) No 910/2014 の第 5 条 a の中で定められた個別のセキュリティ要件の両者を遵守すべきである。遵守を容易にするため，規則(EU) 2019/881 の下で設けられており，かつ，その認証に関して委任される行為によって欧州委員会がこの規則の遵守の推定を定める欧州サイバーセキュリティ認証制度の下において当該提供者の製品の認証を受けることによって，その認証またはその一部がそれらの諸要件を包摂する限りにおいて，ウォレット提供者は，この規則の中で定められた要件と規則(EU) No 910/2014 の中で定められた要件の両者それぞれを欧州デジタル識別子ウォレットが遵守していることを示すことができるべきである。

To the extent that their products fall within the scope of this Regulation, providers of European Digital Identity Wallets as referred to in Article 5a(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council[(18)], should comply with both the horizontal essential cybersecurity requirements set out in this Regulation and the specific security requirements set out in Article 5a of Regulation (EU) No 910/2014. In order to facilitate compliance, wallet providers should be able to demonstrate the compliance of European Digital Identity Wallets with the requirements set out in this Regulation and in Regulation (EU) No 910/2014, respectively, by certifying their products under a European cybersecurity certification scheme established under Regulation (EU) 2019/881 and for which the Commission has specified, by means of delegated acts, a presumption of conformity with this Regulation, in so far as the certificate, or parts thereof, covers those requirements.

(34) 設計及び開発の各段階の間においてデジタルの要素をもつ製品の中に第三者から由来するコンポーネントを組み込むときは，製造者は，この規則の中で定められた必須のサイバーセキュリティ要件に従って製品が設計，開発及び製造されることを確保するため，市場において利用できるようにされなかった無料でオープンソースのソフトウェアのコンポーネントを含め，当該コンポーネントと関連

18 域内市場における電子的なやりとりのための電子識別及び信頼サービスに関する並びに指令 1999/93/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の規則(EU) No 910/2014 (OJ L 257, 28.8.2014, p. 73).
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

するデューディリジェンスを実施すべきである。デューディリジェンスの適切なレベルは，当のコンポーネントと関係するサイバーセキュリティ上のリスクの性質及びレベルによって異なり，かつ，その目的のために，以下の 1 または複数の活動が考慮に入れられるべきである：すなわち，そのコンポーネントに CE マークが既に付されているかどうかを検査することを含め，コンポーネントの製造者がこの規則との適合性を示したことをしかるべく検査すること；セキュリティアップデートの履歴を検査することによる場合のように，コンポーネントが定期的なセキュリティアップデートを受けていることを検査すること；コンポーネントが，指令(EU) 2022/2555 の第 12 条第 2 項により設けられた欧州脆弱性データベースもしくはそれ以外の公衆がアクセス可能な脆弱性データベースに登録された脆弱性をもたないことを検査すること；または，付加的なセキュリティ試験を実施すること。この規則の中で定められた脆弱性の取扱い義務であって，製造者がデジタルの要素をもつ製品を市場に置く際及びサポート期間内に遵守しなければならない義務は，組み込まれた全てのコンポーネントを含め，デジタルの要素をもつ製品の全体に適用される。デューディリジェンスを実施する際，デジタルの要素をもつ製品の製造者が，無料でオープンソースのコンポーネントを含め，コンポーネント内の脆弱性を発見したときは，当該製造者は，そのコンポーネントを製造または維持管理する個人または法主体に対して連絡し，その脆弱性に対処し，及び，その脆弱性を解消し，かつ，それが適切なときは，当該の個人または法主体に対し，適用されたセキュリティ修正を提供すべきである。

When integrating components sourced from third parties in products with digital elements during the design and development phase, manufacturers should, in order to ensure that the products are designed, developed and produced in accordance with the essential cybersecurity requirements set out in this Regulation, exercise due diligence with regard to those components, including free and open-source software components that have not been made available on the market. The appropriate level of due diligence depends on the nature and the level of cybersecurity risk associated with a given component, and should, for that purpose, take into account one or more of the following actions: verifying, as applicable, that the manufacturer of a component has demonstrated conformity with this Regulation, including by checking if the component already bears the CE marking; verifying that a component receives regular security updates, such as by checking its security updates history; verifying that a component is free from vulnerabilities registered in the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555 or other publicly accessible vulnerability databases; or carrying out additional security tests. The vulnerability handling obligations set out in this Regulation, which manufacturers have to comply with when placing a product with digital elements on the market and for the support period, apply to products with digital elements in their entirety, including to all integrated components. Where, in the exercise of due diligence, the manufacturer of the product with digital elements identifies a vulnerability in a component, including in a free and open-source component, it should inform the person or entity manufacturing or maintaining the component, address and remediate the vulnerability, and, where applicable, provide the person or entity with the applied security fix.

(35) この規則の適用のための移行期間経過後直ちに，当該コンポーネントもまたこの規則に服する第三者から由来する 1 または複数のコンポーネントを組み込んでいるデジタルの要素をもつ製品の製造者は，当該製造者のデューディリジェンス義務の一部として，例えば，そのコンポーネントに CE マークが既に付されているかどうかを検査することによって，当該コンポーネントの製造者がこの規則の適合性を示したことを検査できないかもしれない。当該コンポーネントの製造者に対してこの規則が適

用可能となる前に，そのコンポーネントが組み込まれた場合がその場合であり得る。そのような場合においては，そのようなコンポーネントを組み込む製造者は，別の手段によってデューディリジェンスを実施すべきである。

Immediately after the transitional period for the application of this Regulation, a manufacturer of a product with digital elements that integrates one or several components sourced from third parties which are also subject to this Regulation may not be able to verify, as part of its due diligence obligation, that the manufacturers of those components have demonstrated conformity with this Regulation by checking, for instance, if the components already bear the CE marking. This may be the case where the components have been integrated before this Regulation becomes applicable to the manufacturers of those components. In such a case, a manufacturer integrating such components should exercise due diligence through other means.

(36) デジタルの要素をもつ製品は，当該製品が域内市場の中で支障なく移動できるようにするため，当該製品のこの規則の適合性を視認的，読解可能かつ恒久的に表示する CE マークが付されるべきである。構成国は，この規則の中で定められた要件を遵守しており，かつ，CE マークを付しているデジタルの要素をもつ製品を市場に置くことを妨げる正当な理由のない障碍をつくり出してはならない。更に，見本市，展示会及び説明会またはそれらと類似のイベントの際，構成国は，その製品がこの規則を遵守していないこと及びその製品がこの規則を遵守するまではその製品が市場で利用できるようにされないことを明確に表示する視認可能な徴憑がその製品に表示されていることを条件として，当該製品の試作品を含め，この規則を遵守しないデジタルの要素をもつ製品の展示または利用を妨げてはならない。

Products with digital elements should bear the CE marking to visibly, legibly and indelibly indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market of products with digital elements that comply with the requirements laid down in this Regulation and bear the CE marking. Furthermore, at trade fairs, exhibitions and demonstrations or similar events, Member States should not prevent the presentation or use of a product with digital elements which does not comply with this Regulation, including its prototypes, provided that the product is presented with a visible sign clearly indicating that the product does not comply with this Regulation and that it is not to be made available on the market until it does so.

(37) 製造者が，当該製造者のデジタルの要素をもつ製品を適合性評価に服させる前に，試験の目的でソフトウェアをリリースできることを確保するため，構成国は，当該未完成ソフトウェアを試験し及びフィードバックを収集するために必要な期間だけその未完成ソフトウェアが利用できるようにされることを条件として，アルファ版，ベータ版またはリリース候補版のような未完成のソフトウェアを利用できるようにすることを妨げてはならない。製造者は，それらの諸条件の下で利用できるようにされるソフトウェアがリスク評価を受けた後にのみリリースされること，及び，そのソフトウェアが，この規則の中で定められたデジタルの要素をもつ製品の特性と関連するセキュリティ要件を可能な範囲内で遵守することを確保すべきである。製造者は，可能な範囲内で，脆弱性の取扱いの要件も実装すべきである。製造者は，試験の目的のみのためにリリースされた版にアップグレードすることを利用者に対して強い

てはならない。

In order to ensure that manufacturers can release software for testing purposes before subjecting their products with digital elements to conformity assessment, Member States should not prevent the making available of unfinished software, such as alpha versions, beta versions or release candidates, provided that the unfinished software is made available only for the time necessary to test it and gather feedback. Manufacturers should ensure that software made available under those conditions is released only following a risk assessment and that it complies to the extent possible with the security requirements relating to the properties of products with digital elements laid down in this Regulation. Manufacturers should also implement the vulnerability handling requirements to the extent possible. Manufacturers should not force users to upgrade to versions only released for testing purposes.

(38) 市場に置かれる際，デジタルの要素をもつ製品が個人及び組織に対してサイバーセキュリティ上のリスクを呈しないことを確保するため，そのような製品に関し，必須のサイバーセキュリティ要件が定められるべきである。脆弱性管理取扱い要件を含め，それらの必須のサイバーセキュリティ要件は，そのデジタルの要素をもつ製品が単体として製造されているかシリーズのものとして製造されているかに拘わらず，市場に置かれる際，個々の個別のデジタルの要素をもつ製品に対して適用される。製品のタイプに関しては，例えば，個々の個別のデジタルの要素をもつ製品は，そのデジタルの要素をもつ製品が市場に置かれる時点における適格なセキュリティ上の問題に対処するために利用可能な全てのセキュリティパッチまたはアップデートを受けているべきである。物理的な手段またはデジタルの手段によって，当初のリスク評価においては製造者によって想定されておらず，かつ，適格な必須のサイバーセキュリティ要件に当該の製品が適合しなくなっていることを意味し得る方法で，デジタルの要素をもつ製品が事後的に修正されるときは，その修正は，大きなものとして判断されるべきである。例えば，当該修理が，適用可能な要件の遵守が影響を受け得る方法または評価を受けた製品に関する所期の目的が変更され得る方法では既に市場に置かれた製品を修正しないことを条件として，修理は，維持管理業務と同視され得る。

In order to ensure that products with digital elements, when placed on the market, do not pose cybersecurity risks to persons and organisations, essential cybersecurity requirements should be set out for such products. Those essential cybersecurity requirements, including vulnerability management handling requirements, apply to each individual product with digital elements when placed on the market, irrespective of whether the product with digital elements is manufactured as an individual unit or in series. For example, for a product type, each individual product with digital elements should have received all security patches or updates available to address relevant security issues when it is placed on the market. Where products with digital elements are subsequently modified, by physical or digital means, in a way that is not foreseen by the manufacturer in the initial risk assessment and that may imply that they no longer meet the relevant essential cybersecurity requirements, the modification should be considered to be substantial. For example, repairs could be assimilated to maintenance operations provided that they do not modify a product with digital elements already placed on the market in such a way that compliance with the applicable requirements may be affected, or that the intended purpose for which the product has been assessed may be changed.

(39) ソフトウェアアップデートが当該製品の所期の目的を修正し，かつ，その修正が当初のリスク評価に

おいては製造者によって想定されていなかった場合，または，そのソフトウェアアップデートのゆえに危険の性質が変更された場合もしくはサイバーセキュリティ上のリスクのレベルが増加した場合であって，当該アップデートされた版の製品が市場において利用できるようにされている場合においては，物理的な修理または修正の場合となるので，デジタルの要素をもつ製品は，ソフトウェアの変更によって大きく修正されたと判断されるべきである。デジタルの要素をもつ製品のサイバーセキュリティ上のリスクのレベルを低下させるために設計されているセキュリティアップデートが，デジタルの要素をもつ製品の所期の目的を修正しないときは，それは，大きな修正であるとは判断されない。このことは，通常，セキュリティアップデートがソースコードの小規模な補正のみを伴う状況を含む。例えば，サイバーセキュリティ上のリスクのレベルを低下させる目的のみのためにデジタルの要素をもつ製品の機能または遂行能力を修正することによる場合を含め，セキュリティアップデートが既知の脆弱性に対処する場合がその場合であり得る。同様に，視覚面の強化，ユーザインタフェイスへの新たな絵文字または言語の追加のような，機能性の小規模なアップデートは，一般的には，大きな修正であると判断されてはならない。反対に，機能のアップデートが，当初の所期の機能またはデジタルの要素をもつ製品の型式もしくは遂行能力を修正するものであり，かつ，上述の基準に適合するときは，付加される新機能が攻撃対象面の拡大を導き，それによってサイバーセキュリティ上のリスクを増加させるので，それは，大きな修正であると判断されるべきである。例えば，製造者に対して適切な入力の検証を確保することを要求する新たな入力要素がアプリケーションに付加される場合がその場合であり得る。機能のアップデートが大きな修正であると判断されるかどうかの評価において，それが個別のアップデートとして提供されるか，または，セキュリティアップデートと組み合わされて提供されるかは，関係がない。欧州委員会は，何が大きな修正を構成するかをどのようにして判定するかに関するガイドを発行すべきである。

As is the case for physical repairs or modifications, a product with digital elements should be considered to be substantially modified by a software change where the software update modifies the intended purpose of that product and those changes were not foreseen by the manufacturer in the initial risk assessment, or where the nature of the hazard has changed or the level of cybersecurity risk has increased because of the software update, and the updated version of the product is made available on the market. Where a security update which is designed to decrease the level of cybersecurity risk of a product with digital elements does not modify the intended purpose of a product with digital elements, it is not considered to be a substantial modification. This usually includes situations where a security update entails only minor adjustments of the source code. For example, this could be the case where a security update addresses a known vulnerability, including by modifying functions or the performance of a product with digital elements for the sole purpose of decreasing the level of cybersecurity risk. Similarly, a minor functionality update, such as a visual enhancement or the addition of new pictograms or languages to the user interface, should not generally be considered to be a substantial modification. Conversely, where a feature update modifies the original intended functions or the type or performance of a product with digital elements and meets the above criteria, it should be considered to be a substantial modification, as the addition of new features typically leads to a broader attack surface, thereby increasing the cybersecurity risk. For example, this could be the case where a new input element is added to an application, requiring the manufacturer to ensure adequate input validation. In assessing whether a feature update is considered to be a substantial modification it is not relevant whether it is provided as a separate update or in combination with a security update. The Commission should issue guidance on how to determine what constitutes a substantial modification.

(40) ソフトウェア開発の反復的な性質を考慮に入れた上で，後に行われた当該製品の大きな修正の結果として，後の版のソフトウェア製品を市場に置いた製造者は，当該製造者が直近に市場に置いた版のソフトウェア製品に関してのみ，サポート期間内，セキュリティアップデートを提供できるべきである。当該製造者は，適格な従前の版の製品の利用者が，直近に市場に置かれた版の製品に対して無料のアクセスをもち，かつ，当該利用者がその製品を運用するハードウェアまたはソフトウェアの環境を補正するための付加的な費用がかからない場合に限り，そのようにできるべきである。例えば，デスクトップのオペレーティングシステムのアップグレードが，より高速の中央演算処理ユニットまたはより多くのメモリのような新たなハードウェアを要求しない場合は，その場合であり得る。それにも拘わらず，製造者は，後に大きく修正された全ての版の市場に置かれたソフトウェア製品の潜在的な脆弱性に関する情報の共有を容易にするための調整された脆弱性の開示または措置に関する基本方針をもつことのように，サポート期間内，他の脆弱性取扱の要件を遵守し続けるべきである。製造者は，大きく修正されなかったソフトウェア製品の直近の版またはサブバージョンに関してのみ，大きな修正を組成しない小規模なセキュリティアップデートまたは機能性のアップデートを提供できるべきである。それと同時に，スマートフォンのようなハードウェア製品が，当該製品と共に当初出荷された直近の版のオペレーティングシステムと互換性がない場合，その製造者は，サポート期間内，少なくとも直近の互換性のある版のオペレーティングシステムのセキュリティアップデートの提供を継続すべきである。

Taking into account the iterative nature of software development, manufacturers that have placed subsequent versions of a software product on the market as a result of a subsequent substantial modification of that product should be able to provide security updates for the support period only for the version of the software product that they have last placed on the market. They should be able to do so only if the users of the relevant previous product versions have access to the product version last placed on the market free of charge and do not incur additional costs to adjust the hardware or software environment in which they operate the product. This could, for instance, be the case where a desktop operating system upgrade does not require new hardware, such as a faster central processing unit or more memory. Nonetheless, the manufacturer should continue to comply, for the support period, with other vulnerability-handling requirements, such as having a policy on coordinated vulnerability disclosure or measures in place to facilitate the sharing of information about potential vulnerabilities for all subsequent substantially modified versions of the software product placed on the market. Manufacturers should be able to provide minor security or functionality updates that do not constitute a substantial modification only for the latest version or sub-version of a software product that has not been substantially modified. At the same time, where a hardware product, such as a smartphone, is not compatible with the latest version of the operating system it was originally delivered with, the manufacturer should continue to provide security updates at least for the latest compatible version of the operating system for the support period.

(41) 欧州連合整合化立法によって規律される製品に関する大きな修正という共通に確立された概念に沿って，大きな修正が，デジタルの要素をもつ製品のこの規則の遵守に対して影響を与え得る場合または当該製品の所期の目的を変更する場合においては，デジタルの要素をもつ製品の遵守が検査されることが適切であり，また，それが適用可能なときは，新たな適合性評価を受けることが適切である。それが適用可能なときは，第三者が関与する適合性評価を製造者が行うのであれば，大きな修正を導いたかもしれない変更を当該第三者に対して通知すべきである。

In line with the commonly established concept of substantial modification for products regulated by Union harmonisation legislation, where a substantial modification occurs that may affect the compliance of a product with digital elements with this Regulation or when the intended purpose of that product changes, it is appropriate that the compliance of the product with digital elements is verified and that, where applicable, it undergoes a new conformity assessment. Where applicable, if the manufacturer undertakes a conformity assessment involving a third party, a change that might lead to a substantial modification should be notified to the third party.

(42) デジタルの要素をもつ製品が，欧州議会及び理事会の規則(EU) 2024/1781[19]の第 2 条第 18 号，第 19 号及び第 20 号に定義する「再生」，「維持管理」及び「修理」に服するときは，例えば，所期の目的及び機能性が変更されておらず，リスクのレベルが影響を受けないままであれば，製品の大きな修正を導くとは限らない。ただし，製造者によるデジタルの要素をもつ製品のアップグレードは，当該製品の設計及び開発への変更を導いたかもしれず，また，それゆえ，当該製品の所期の目的及びこの規則の中で定められた要件のその製品の遵守に影響を与えたかもしれない。

Where a product with digital elements is subject to 'refurbishment', 'maintenance' and 'repair' as defined in Article 2, points (18), (19) and (20), of Regulation (EU) 2024/1781 of the European Parliament and of the Council[19], this does not necessarily lead to a substantial modification of the product, for instance if the intended purpose and functionalities are not changed and the level of risk remains unaffected. However, an upgrade of a product with digital elements by the manufacturer might lead to changes in the design and development of that product and might therefore affect its intended purpose and compliance with the requirements set out in this Regulation.

(43) 就中，サイバーセキュリティと関連する機能性のゆえに，または，ネットワーク管理，設定管理，仮想化もしくは個人データの処理を含め，中枢的なシステム機能のような，そのリスクの強度の面における負の影響，及び，直接的な操作を介して，デジタルの要素をもつ他の非常に多数の製品に対しもしくは当該製品の利用者の健康，防護もしくは安全に対し，それを破壊し，支配しもしくはそれに対して損害を生じさせる能力の面における負の影響という大きなリスクをもつ機能のゆえに，製品内の潜在的な脆弱性の濫用という負の影響が深刻化し得る場合，デジタルの要素をもつ製品は，重要と判断されるべきである。とりわけ，ブートマネジャのような，サイバーセキュリティと関連する機能性をもつデジタルの要素をもつ製品の中にある脆弱性は，サプライチェーン全体にわたるセキュリティ上の問題の伝播を導き得る。インシデントの影響の深刻度は，その製品が，ネットワーク管理，設定管理，仮想化または個人データの処理を含め，中枢的なシステム機能を主として遂行する場合にも増加し得る。

---

[19] 持続可能な製品に関するエコデザイン要件を定めるための枠組みを設ける，指令(EU) 2020/1828 及び規則(EU) 2023/1542 を改正する，並びに，指令 2009/125/EC を廃止する欧州議会及び理事会の 2024 年 6 月 13 日の規則(EU) 2024/1781 (OJ L, 2024/1781, 28.6.2024).

Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (OJ L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

Products with digital elements should be considered to be important if the negative impact of the exploitation of potential vulnerabilities in the product can be severe due to, inter alia, the cybersecurity-related functionality or a function carrying a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data. In particular, vulnerabilities in products with digital elements that have a cybersecurity-related functionality, such as boot managers, can lead to a propagation of security issues throughout the supply chain. The severity of the impact of an incident may also increase where the product primarily performs a central system function, including network management, configuration control, virtualisation or processing of personal data.

(44) 一定の類型のデジタルの要素をもつ製品は，比例的なアプローチを維持しつつ，より厳格な適合性評価手続に服するべきである。その目的のために，デジタルの要素をもつ重要な製品は，当該類型の製品と結び付けられたサイバーセキュリティ上のリスクのレベルを反映する 2 つのクラスに分別されるべきである。クラス Ⅱ の下にあるデジタルの要素をもつ重要な製品を含んでいるインシデントは，例えば，当該製品のサイバーセキュリティと関連する機能の性質のゆえに，または，負の影響の大きなリスクをもつ別の機能の遂行能力のゆえに，クラス Ⅰ の下にあるデジタルの要素をもつ重要な製品を含んでいるインシデントよりも大きな負の影響を導くかもしれない。そのようなより大きな負の影響の指標として，クラス Ⅱ の下にあるデジタルの要素をもつ製品は，クラス Ⅰ の中に列挙される製品または上述の基準の両者に適合する製品の負の影響よりも高い負の影響という大きなリスクをもつサイバーセキュリティと関連する機能性または別の機能のいずれかを遂行し得る。それゆえ，クラス Ⅱ の下にあるデジタルの要素をもつ重要な製品は，より厳格な適合性評価手続に服するべきである。

Certain categories of products with digital elements should be subject to stricter conformity assessment procedures, while keeping a proportionate approach. For that purpose, important products with digital elements should be divided into two classes, reflecting the level of cybersecurity risk linked to those categories of products. An incident involving important products with digital elements that fall under class II might lead to greater negative impacts than an incident involving important products with digital elements that fall under class I, for instance due to the nature of their cybersecurity-related function or the performance of another function which carries a significant risk of adverse effects. As an indication of such greater negative impacts, products with digital elements that fall under class II could either perform a cybersecurity-related functionality or another function which carries a significant risk of adverse effects that is higher than for those listed in class I, or meet both of the aforementioned criteria. Important products with digital elements that fall under class II should therefore be subject to a stricter conformity assessment procedure.

(45) この規則に示すデジタルの要素をもつ重要な製品は，この規則の中で定められているデジタルの要素をもつ重要な製品の類型のコア機能性をもつ製品として理解されるべきである。例えば，この規則は，クラス Ⅱ の中において，ファイアウォール，侵入検知システムまたは侵入防止システムとしての当該製品の機能性によって定義されているデジタルの要素をもつ重要な製品の類型を定めている。その結果として，ファイアウォール，侵入検知システムまたは侵入防止システムは，強制的な第三者適合性評価に服する。それ以外の，ファイアウォール，侵入検知システムまたは侵入防止システムを組み込み得るデジタルの要素をもつ重要な製品として類型化されないデジタルの要素をもつ製品は，

その場合に該当しない。欧州委員会は，この規則に定めるクラス I 及びクラス II の下にあるデジタルの要素をもつ重要な製品の類型の技術上の記述の細目を定めるための実装行為を採択すべきである。

Important products with digital elements as referred to in this Regulation should be understood as products which have the core functionality of a category of important products with digital elements that is set out in this Regulation. For example, this Regulation sets out categories of important products with digital elements which are defined by their core functionality as firewalls or intrusion detection or prevention systems in class II. As a result, firewalls and intrusion detection or prevention systems are subject to mandatory third-party conformity assessment. This is not the case for other products with digital elements not categorised as important products with digital elements which may integrate firewalls or intrusion detection or prevention systems. The Commission should adopt an implementing act to specify the technical description of the categories of important products with digital elements that fall under classes I and II as set out in this Regulation.

(46) この規則の中で定められたデジタルの要素をもつ不可欠な製品の類型は，サイバーセキュリティと関連する機能性をもち，かつ，当該リスクの強度の面における負の影響，及び，直接的な操作を介して，デジタルの要素をもつ他の非常に多数の製品を破壊し，支配しもしくはそれに対して損害を生じさせる能力の面における負の影響という大きなリスクをもつ機能を遂行する。更に，それらのデジタルの要素をもつ不可欠な製品の類型は，指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体にとって不可欠の依存関係であると理解されている。この規則の別紙の中で定められるデジタルの要素をもつ不可欠な製品の類型は，同類型の不可欠性のゆえに，様々な形態の認証において既に広範に使用されており，また，委員会実装規則(EU) 2024/482[20]の中で定められた共通基準ベースの欧州サイバーセキュリティ認証制度（EUCC）によっても包摂されている。それゆえ，欧州連合内におけるデジタルの要素をもつ不可欠な製品のサイバーセキュリティ上の共通の適切な保護を確保するため，それらの製品を包摂する適格な欧州サイバーセキュリティ認証制度が既に設けられており，かつ，予定されている強制的な認証の市場に対する潜在的な影響の評価が欧州委員会によって実施されたときは，委任される行為により，そのような類型の製品を，強制的な欧州サイバーセキュリティ認証に服させることが適切かつ比例的であり得る。その影響の評価は，関係するデジタルの要素をもつ製品に対する構成国及び利用者の両者からの，欧州サイバーセキュリティ認証が要求されることへの十分な需要があるかどうか，並びに，指令(EU) 2022/2555 第 3 条第 1 項に示す基礎法主体によるそれらの製品に対する不可欠の依存関係を含め，利用されることが意図されているデジタルの要素をもつ製品のその目的を含め，供給側と需要側の両者を検討すべきである。その評価は，域内市場における当該製品の可用性に対する強制的な認証の潜在的な影響並びに適格な欧州サイ

[20] 共通基準ベースの欧州サイバーセキュリティ認証制度（EUCC）の採択と関連する欧州議会及び理事会の規則(EU) 2019/881 の適用のための規定を定める 2024 年 1 月 31 日の委員会実装規則(EU) 2024/482 (OJ L, 2024/ 482, 7.2.2024).
Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) (OJ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

バーセキュリティ認証制度の実装のための構成国の実現能力及び準備態勢も分析すべきである。

The categories of critical products with digital elements set out in this Regulation have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation. Furthermore, those categories of products with digital elements are considered to be critical dependencies for essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. The categories of critical products with digital elements set out in an annex to this Regulation, due to their criticality, already widely use various forms of certification, and are also covered by the European Common Criteria-based cybersecurity certification scheme (EUCC) set out in Commission Implementing Regulation (EU) 2024/482[20]. Therefore, in order to ensure a common adequate cybersecurity protection of critical products with digital elements in the Union, it could be adequate and proportionate to subject such categories of product, by means of a delegated act, to mandatory European cybersecurity certification where a relevant European cybersecurity certification scheme covering those products is already in place and an assessment of the potential market impact of the envisaged mandatory certification has been carried out by the Commission. That assessment should consider both the supply and demand side, including whether there is sufficient demand for the products with digital elements concerned from both Member States and users for European cybersecurity certification to be required, as well as the purposes for which the products with digital elements are intended to be used, including the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. The assessment should also analyse the potential effects of the mandatory certification on the availability of those products on the internal market and the capabilities and the readiness of the Member States for the implementation of the relevant European cybersecurity certification schemes.

(47) 強制的な欧州サイバーセキュリティ認証を要求する委任される行為は，この規則の中で定められたデジタルの要素をもつ不可欠の製品であって強制的な認証に服すべき製品の類型のコア機能性をもち，かつ，少なくとも「十分」であるべき要求される保証レベルをもつデジタルの要素をもつ製品を決定すべきである。要求される保証レベルは，デジタルの要素をもつ製品と関係するサイバーセキュリティ上のリスクのレベルと比例しているべきである。例えば，デジタルの要素をもつ製品が，この規則の中で定められたデジタルの要素をもつ不可欠の製品の類型のコア機能性をもち，かつ，指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体の利用が意図されている製品のような機微の環境または不可欠な環境における利用を意図している場合，最高度の保証レベルを要求することがあり得る。

Delegated acts requiring mandatory European cybersecurity certification should determine the products with digital elements that have the core functionality of a category of critical products with digital elements set out in this Regulation that are to be subject to mandatory certification, as well as the required assurance level, which should be at least ‘substantial’. The required assurance level should be proportionate to the level of cybersecurity risk associated with the product with digital elements. For instance, where the product with digital elements has the core functionality of a category of critical products with digital elements set out in this Regulation and is intended for the use in a sensitive or critical environment, such as products intended for the use of essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555, it may require the highest assurance level.

(48) この規則の中で定められたデジタルの要素をもつ不可欠な製品の類型のコア機能性をもつデジタルの要素をもつ製品の欧州連合内における共通の適切なサイバーセキュリティ上の保護を確保するため，欧州委員会は，その製品に関してこの規則の遵守を示すために規則(EU) 2019/881 による欧州サイバーセキュリティ認証制度の下における欧州サイバーセキュリティ証明書を得ることを製造者が要求され得るデジタルの要素をもつ不可欠の製品の類型を追加することまたは取消すことによりこの規則を改正するための委任される行為を採択する権限も与えられるべきである。指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体の当該製品への不可欠の依存関係が存在する場合，または，インシデントによる影響を受けると，もしくは，悪用された脆弱性を含んでいると，そのことが不可欠なサプライチェーンの破壊を導き得る場合においては，デジタルの要素をもつ不可欠な製品の新たな類型は，同類型に付加され得る。委任される行為によるデジタルの要素をもつ不可欠な製品の類型を追加することまたは取消すことの必要性を評価する際，欧州委員会は，指令(EU) 2022/2555 の第 3 条第 1 条に示す基礎法主体の回復力にとって不可欠の役割をもち，かつ，重大で破壊的な潜在的影響をもつサプライチェーンのサイバー攻撃に直面することが増加しているデジタルの要素をもつ製品を構成国が国内レベルで識別したかどうかを考慮に入れ得るべきである。更に，欧州委員会は，指令(EU) 2022/2555 の第 22 条に従って実施された不可欠なサプライチェーンの欧州連合レベルで調整されたセキュリティリスク評価の結果を考慮に入れ得るべきである。

In order to ensure a common adequate cybersecurity protection in the Union of products with digital elements that have the core functionality of a category of critical products with digital elements set out in this Regulation, the Commission should also be empowered to adopt delegated acts to amend this Regulation by adding or withdrawing categories of critical products with digital elements for which manufacturers could be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 to demonstrate conformity with this Regulation. A new category of critical products with digital elements can be added to those categories if there is a critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555 or, if affected by incidents or when containing exploited vulnerabilities, this could lead to disruptions of critical supply chains. When assessing the need for adding or withdrawing categories of critical products with digital elements by means of a delegated act, the Commission should be able to take into account whether the Member States have identified at national level products with digital elements that have a critical role for the resilience of essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555 and which increasingly face supply chain cyberattacks, with potential serious disruptive effects. Furthermore, the Commission should be able to take into account the outcome of the Union level coordinated security risk assessment of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555.

(49) この規則の実装のための措置を準備する際，欧州委員会は，幅広い適格な利害関係者が構造化されかつ定期的な態様で意見聴取されることを確保すべきである。とりわけ，デジタルな要素をもつ重要な製品または不可欠な製品の類型のリストの潜在的なアップデートの必要性を欧州委員会が評価する場合，適格な製造者が意見聴取を受けるべきであり，かつ，サイバーセキュリティ上のリスク及びそのような製品の類型を重要または不可欠として指定することの費用と利益の均衡を分析するため，当該製造者の見解が考慮に入れられるべき場合がそれに該当すべきである。

The Commission should ensure that a wide range of relevant stakeholders are consulted in a structured and regular manner when preparing measures for the implementation of this Regulation. This should particularly be the case where the Commission assesses the need for potential updates to the lists of categories of important or critical products with digital elements, where relevant manufacturers should be consulted and their views taken into account in order to analyse the cybersecurity risks as well as the balance of costs and benefits of designating such categories of products as important or critical.

(50) この規則は，的を絞った態様で，サイバーセキュリティ上のリスクに対処している。ただし，デジタルの要素をもつ製品は，常にサイバーセキュリティと関連するとは限らないが，セキュリティ侵害の結果であり得る別の安全性リスクを呈することがあり得る。それらのリスクは，この規則以外の適格な欧州連合整合化立法によって規律され続けるべきである。この規則以外の欧州連合整合化立法が適用可能ではない場合，当該製品は，欧州議会及び理事会の規則(EU) 2023/988[21]に服するべきである。それゆえ，当該製品が，規則(EU) 2023/988 の第 3 条第 27 号の意味におけるこの規則以外の欧州連合整合化立法の中で定められた個別の要件に服さないときは，この規則の的を絞った性質に照らし，規則(EU) 2023/988 の第 2 条第 1 項第 3 副項(b)からの特例として，規則(EU) 2023/988 の第 III 章第 1 節，第 V 章及び第 VII 章並びに第 IX 章ないし第 XI 章が，この規則の適用のない安全性リスクとの関係において，デジタルの要素をもつ製品に対して適用されるべきである。

This Regulation addresses cybersecurity risks in a targeted manner. Products with digital elements might, however, pose other safety risks, that are not always related to cybersecurity but can be a consequence of a security breach. Those risks should continue to be regulated by relevant Union harmonisation legislation other than this Regulation. If no Union harmonisation legislation other than this Regulation is applicable, they should be subject to Regulation (EU) 2023/988 of the European Parliament and of the Council [(21)]. Therefore, in light of the targeted nature of this Regulation, as a derogation from Article 2(1), third subparagraph, point (b), of Regulation (EU) 2023/988, Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of Regulation (EU) 2023/988 should apply to products with digital elements with respect to safety risks not covered by this Regulation, if those products are not subject to specific requirements laid down in Union harmonisation legislation other than this Regulation within the meaning of Article 3, point (27), of Regulation (EU) 2023/988.

(51) 欧州議会及び理事会の規則(EU) 2024/1689[22]の第 6 条により高リスク AI システムとして分類され，この規則の適用範囲内にあるデジタルの要素をもつ製品は，この規則の中で定められた必須のサイバ

---

21 製品の一般的な安全性に関する，欧州議会及び理事会の規則(EU) No 1025/2012 及び欧州議会及び理事会の指令 (EU) 2020/1828 を改正する，並びに，欧州議会及び理事会の指令 2001/95/EC 及び理事会指令 87/357/EEC を廃止する欧州議会及び理事会の 2023 年 5 月 10 日の規則(EU) 2023/988 (OJ L 135, 23.5.2023, p. 1).

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).

22 人工知能に関する整合化された規定を定める，並びに，規則(EC) No 300/2008，規則(EU) No 167/2013，規則(EU) No 168/2013，規則(EU) 2018/858，規則(EU) 2018/1139 及び規則(EU) 2019/2144 並びに指令 2014/90/EU，指令

ーセキュリティ要件を遵守すべきである。当該高リスク AI システムがこの規則の中で定められた必須のサイバーセキュリティ要件を満たすときは，当該高リスク AI システムは，規則(EU) 2024/1689 の第 15 条の中で定められたサイバーセキュリティ要件がこの規則の下において発される EU 適合宣言書または同宣言書の一部に含められている限り，同要件を遵守しているとみなされるべきである。その目的のために，規則(EU) 2024/1689 により高リスク AI システムとして分類されたデジタルの要素をもつ製品と関係するサイバーセキュリティ上のリスクであって，この規則の下において要求されるように，そのような製品の企画，設計，開発，製造，流通及び維持管理の各段階を通じて考慮に入れられるべきリスクの評価は，規則(EU) 2024/1689 に従い，データポイズニング攻撃または敵対的攻撃のような AI 特有の脆弱性を含め，当該 AI システムの利用，ふるまいまたは遂行能力を改変するための無権限の第三者による試みと関連する AI システムのサイバー回復力を妨げるリスク，並びに，それが関連するときは，基本的な権利を妨げるリスクが考慮に入れられるべきである。この規則の適用範囲内にありかつ高リスク AI システムとして分類されているデジタルの要素をもつ製品の必須のサイバーセキュリティ要件と関連する適合性評価手続に関し，規則(EU) 2024/1689 の第 43 条は，この規則の適格な条項の代わりの規定として適用されるべきである。ただし，同規定は，この規則に示すデジタルの要素をもつ重要な製品または不可欠な製品に関する必要な保証のレベルを低下させることを帰結してはならない。それゆえ，同規定からの特例により，規則(EU) 2024/1689 の適用範囲内にある高リスク AI システムであって，この規則に示すデジタルの要素をもつ重要な製品または不可欠の製品でもあり，かつ，当該製品に対して規則(EU) 2024/1689 の別紙 VI に示す内部統制を基礎とする適合性評価手続が適用される高リスク AI システムは，この規則の中で定められた必須のサイバーセキュリティ要件が関係する範囲内において，この規則の中で定められた適合性評価手続に服するべきである。そのような場合において，規則(EU) 2024/1689 によって包摂される他の全ての側面に関し，同規則の別紙 VI の中で定められた内部統制を基礎とする適合性評価に関する適格な条項が適用されるべきである。

Products with digital elements classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689 of the European Parliament and of the Council[22] which fall within the scope of this Regulation should comply with the essential cybersecurity requirements set out in this Regulation. Where those high-risk AI systems fulfil the essential cybersecurity requirements set out in this Regulation, they should be deemed to comply with the cybersecurity requirements set out in Article 15 of Regulation (EU) 2024/1689 in so far as those requirements are covered by the EU declaration of conformity or parts thereof issued under this Regulation. For that purpose, the assessment of the cybersecurity risks associated with a product with digital elements classified as a high-risk AI system pursuant to Regulation (EU) 2024/1689 that is to be taken into account during the planning, design, development, production, delivery and maintenance phases of such product, as required under this Regulation, should take into account risks to the

---

(EU) 2016/797 及び指令(EU) 2020/1828 を改正する欧州議会及び理事会の 2024 年 6 月 13 日の規則(EU) 2024/1689（人工知能法）(OJ L, 2024/1689, 12.7.2024).

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights, in accordance with Regulation (EU) 2024/1689. As regards the conformity assessment procedures relating to the essential cybersecurity requirements for a product with digital elements that falls within the scope of this Regulation and that is classified as a high-risk AI system, Article 43 of Regulation (EU) 2024/1689 should apply as a rule instead of the relevant provisions of this Regulation. However, that rule should not result in a reduction of the necessary level of assurance for important or critical products with digital elements as referred to in this Regulation. Therefore, by way of derogation from that rule, high-risk AI systems that fall within the scope of Regulation (EU) 2024/1689 which are also important or critical products with digital elements as referred to in this Regulation and to which the conformity assessment procedure based on internal control referred to in Annex VI to Regulation (EU) 2024/1689 applies, should be subject to the conformity assessment procedures provided for in this Regulation in so far as the essential cybersecurity requirements set out in this Regulation are concerned. In such a case, for all the other aspects covered by Regulation (EU) 2024/1689 the relevant provisions on conformity assessment based on internal control set out in Annex VI to that Regulation should apply.

(52) 域内市場に置かれたデジタルの要素をもつ製品の防護を向上させるため，そのような製品に対して適用可能な必須のサイバーセキュリティ要件を定める必要がある。それらの必須のサイバーセキュリティ要件は，指令(EU) 2022/2555 の第 22 条の中で定められ，技術的な要素を考慮に入れ，及び，それが適格なときは，供給者に対する第三国からの不適正な影響のような非技術的なリスク要素を考慮に入れる，不可欠なサプライチェーンの欧州連合レベルで調整されたセキュリティリスク評価を妨げてはならない。更に，それらの必須のサイバーセキュリティ要件は，5G ネットワークのサイバーセキュリティの EU の調整されたリスク評価において，及び，指令(EU) 2022/2555 の第 14 条により設けられた協力グループによって同意された 5G サイバーセキュリティに関する EU ツールボックスにおいて，委員会勧告(EU) 2019/534[23]の中で定義された諸要素を含め，高いレベルの回復力を確保する目的のために非技術的な諸要素を考慮に入れる付加的な要件を定めるための構成国の特権を妨げてはならない。

In order to improve the security of products with digital elements placed on the internal market it is necessary to lay down essential cybersecurity requirements applicable to such products. Those essential cybersecurity requirements should be without prejudice to the Union level coordinated security risk assessments of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555, which take into account both technical and, where relevant, non-technical risk factors, such as undue influence by a third country on suppliers. Furthermore, they should be without prejudice to the Member States' prerogative to lay down additional requirements that take account of non-technical factors for the purpose of ensuring a high level of resilience, including those defined in Commission Recommendation (EU) 2019/534[(23)], in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555.

[23] 2019 年 3 月 26 日の委員会勧告(EU) 2019/534 5G ネットワークのサイバーセキュリティ (OJ L 88, 29.3.2019, p. 42).
Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks (OJ L 88, 29.3.2019, p. 42).

(53) この規則に定義するデジタルの要素をもつ製品でもある欧州議会及び理事会の規則(EU) 2023/1230[24]の適用範囲内にある製品の製造者は，この規則の中で定められた必須のサイバーセキュリティ要件及び規則(EU) 2023/1230 の中で定められた必須の健康と安全の要件の両者を遵守すべきである。この規則の中で定められた必須のサイバーセキュリティ要件及び規則(EU) 2023/1230 の中で定められた一定の必須の要件は，類似のサイバーセキュリティ上のリスクに対応できるかもしれない。それゆえ，この規則の中で定められた必須のサイバーセキュリティ要件の遵守は，規則(EU) 2023/1230 の中で定められたような一定のサイバーセキュリティ上のリスク，並びに，とりわけ，同規則の別紙 Ⅲ の 1.1.9 節及び 1.2.1 節の中で定められた破壊に抗する保護と関連するリスク並びに制御システムの安全性及び信頼性と関連するリスクをも包摂している必須の要件の遵守を容易にし得る。そのような波及効果は，例えば，それが利用可能なときは，それらのサイバーセキュリティ上のリスクを包摂するリスク評価の後，適格な必須のサイバーセキュリティ要件を包摂する整合化された技術標準またはそれ以外の技術仕様を適用することにより，その製造者によって示されなければならない。製造者は，この規則及び規則(EU) 2023/1230 に定める適用可能な適合性評価手続にも従うべきである。欧州委員会及び欧州の標準化組織は，この規則及び規則(EU) 2023/1230 の実装を支える準備作業並びに関連する標準化の過程において，サイバーセキュリティ上のリスクがどのように評価されるか，及び，適格な必須の要件と関連する整合化された技術標準によってそれらのリスクがどのように包摂されるかにおける一貫性を向上させるべきである。とりわけ，欧州委員会及び欧州の標準化組織は，規則(EU) 2023/1230 の別紙 Ⅲ の 1.1.9 節及び 1.2.1 節の中で定められた破壊に抗する保護並びに制御システムの安全性及び信頼性と関連するサイバーセキュリティ上の側面と特に関連し，同規則の実装を容易にするための整合化された技術標準の準備及び開発において，この規則を考慮に入れるべきである。欧州委員会は，この規則に服しかつ規則(EU) 2023/1230 にも服する製造者を支援するためのガイド，並びに，とりわけ，この規則及び規則(EU) 2023/1230 の中で定められた適格な必須の要件を遵守していることの説明を容易にするためのガイドを提供すべきである。

Manufacturers of products falling within the scope of Regulation (EU) 2023/1230 of the European Parliament and of the Council[24] which are also products with digital elements as defined in this Regulation should comply with both the essential cybersecurity requirements set out in this Regulation and the essential health and safety requirements set out in Regulation (EU) 2023/1230. The essential cybersecurity requirements set out in this Regulation and certain essential requirements set out in Regulation (EU) 2023/1230 might address similar cybersecurity risks. Therefore, the compliance with the essential cybersecurity requirements set out in this Regulation could facilitate the compliance with the essential requirements that also cover certain cybersecurity risks as set out in Regulation (EU) 2023/1230, and in particular those regarding the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. Such synergies have to be demonstrated by the manufacturer, for instance by applying, where available, harmonised standards or other technical specifications covering relevant essential cybersecurity requirements following a risk assessment covering those cybersecurity risks. The manufacturer should

[24] 機械に関する，並びに，欧州議会及び理事会の指令 2006/42/EC，理事会指令 73/361/EEC を廃止する欧州議会及び理事会の 2023 年 6 月 14 日の規則(EU) 2023/1230 (OJ L 165, 29.6.2023, p. 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 (OJ L 165, 29.6.2023, p. 1).

also follow the applicable conformity assessment procedures set out in this Regulation and in Regulation (EU) 2023/1230. The Commission and the European standardisation organisations, in the preparatory work supporting the implementation of this Regulation and of Regulation (EU) 2023/1230 and the related standardisation processes, should promote consistency in how the cybersecurity risks are to be assessed and in how those risks are to be covered by harmonised standards with regard to the relevant essential requirements. In particular, the Commission and the European standardisation organisations should take into account this Regulation in the preparation and development of harmonised standards to facilitate the implementation of Regulation (EU) 2023/1230 as regards in particular the cybersecurity aspects related to the protection against corruption and safety and reliability of control systems set out in sections 1.1.9 and 1.2.1 of Annex III to that Regulation. The Commission should provide guidance to support manufacturers subject to this Regulation that are also subject to Regulation (EU) 2023/1230, in particular to facilitate the demonstration of compliance with relevant essential requirements set out in this Regulation and in Regulation (EU) 2023/1230.

(54) デジタルの要素をもつ製品が市場に置く時点とそのデジタルの要素をもつ製品が利用されると予想される期間内との両時点においてデジタルの要素をもつ製品が安全であることを確保するため，脆弱性の取扱いに関する必須のサイバーセキュリティ要件及びデジタルの要素をもつ製品の特性と関係する必須のサイバーセキュリティ要件を定める必要がある。製造者は，サポート期間を通じて脆弱性の取扱いに関する全ての必須のサイバーセキュリティ要件を遵守すべきであるが，製造者は，関係するデジタルの要素をもつ製品のタイプにとって，製品の特性と関連する他のどの必須のサイバーセキュリティ要件が適格であるかを判定すべきである。その目的のために，製造者は，当該製品の防護に対する影響をもつかもしれない既知の悪用可能な脆弱性なしにその製造者のデジタルの要素をもつ製品を利用できるようにするために適格なリスク及び適格な必須のサイバーセキュリティ要件を特定するため，並びに，適切に整合化された技術標準，共通仕様または欧州の技術標準もしくは国際的な技術標準を適切に適用するため，デジタルの要素をもつ製品と関係するサイバーセキュリティリスク評価を行うべきである。

In order to ensure that products with digital elements are secure both at the time of their placing on the market as well as during the time the product with digital elements is expected to be in use, it is necessary to lay down essential cybersecurity requirements for vulnerability handling and essential cybersecurity requirements relating to the properties of products with digital elements. While manufacturers should comply with all essential cybersecurity requirements related to vulnerability handling throughout the support period, they should determine which other essential cybersecurity requirements related to the product properties are relevant for the type of product with digital elements concerned. For that purpose, manufacturers should undertake an assessment of the cybersecurity risks associated with a product with digital elements to identify relevant risks and relevant essential cybersecurity requirements in order to make available their products with digital elements without known exploitable vulnerabilities that might have an impact on the security of those products and to appropriately apply suitable harmonised standards, common specifications or European or international standards.

(55) デジタルの要素をもつ製品に対して一定の必須のサイバーセキュリティ要件が適用可能ではない場合，製造者は，技術文書の中に含められるサイバーセキュリティリスク評価の中に，明確な正当化事

由を含めるべきである。必須のサイバーセキュリティ要件が，デジタルの要素をもつ製品の性質と適合していない場合がその場合であり得る。例えば，デジタルの要素をもつ製品の所期の目的が，その製造者に対し，当該技術標準のセキュリティ機能が最新のものであるとは判断されなくなっているとしても，広範に承認された相互運用性の技術標準に従うことを要求することがあり得る。同様に，他の欧州連合法は，製造者に対し，特定の相互運用性の要件を適用すること要求する。必須のサイバーセキュリティ要件がデジタルの要素をもつ製品に対して適用可能ではないが，当該必須のサイバーセキュリティ要件と関係するサイバーセキュリティ上のリスクをその製造者が発見した場合，その製造者は，別の手段によって，例えば，その製品の所期の目的を信頼できる環境に限定することによって，または，利用者に対し，当該リスクに関して連絡することによって，当該リスクに対処するための方策をとるべきである。

Where certain essential cybersecurity requirements are not applicable to a product with digital elements, the manufacturer should include a clear justification in the cybersecurity risk assessment included in the technical documentation. This could be the case where an essential cybersecurity requirement is incompatible with the nature of a product with digital elements. For example, the intended purpose of a product with digital elements may require the manufacturer to follow widely recognised interoperability standards even if its security features are no longer considered to be state of the art. Similarly, other Union law requires manufacturers to apply specific interoperability requirements. Where an essential cybersecurity requirement is not applicable to a product with digital elements, but the manufacturer has identified cybersecurity risks in relation to that essential cybersecurity requirement, it should take measures to address those risks by other means, for instance by limiting the intended purpose of the product to trusted environments or by informing the users about those risks.

(56) 当該利用者のデジタルの要素をもつ製品をサイバー攻撃から保護するためにとる利用者にとっての最も重要な手段の 1 つは，可能な限り速やかに，利用可能な最新のセキュリティアップデートをインストールすることである。それゆえ，とりわけ，消費者向けの製品の場合において，製造者は，デジタルの要素をもつ製品が，セキュリティアップデートの自動的な通知，配布，ダウンロード及びインストールを実現可能化する機能を含むことを確保するために，その製造者の製品を設計し，かつ，そのためのプロセスを設けるべきである。製造者は，最後の手立てとして，セキュリティアップデートのダウンロードとインストールを承認できることも提供すべきである。利用者は，利用者がどのようにしてオプトアウトできるかに関する明瞭な指示によって支えられた明瞭で利用しやすい仕組みにより，自動的なアップデートを非アクティブ化する能力を保持すべきである。この規則の別紙に定める自動的なアップデートと関連する要件は，コンポーネントとして別の製品の中に組み込まれることを基本的に意図するデジタルの要素をもつ製品に対しては適用可能ではない。その要件は，専門的な ICT ネットワークにおいて，特に，自動的なアップデートが運用管理に支障を生じさせ得るような不可欠な環境及び産業上の環境において利用されることが意図されたデジタルの要素をもつ製品を含め，その製品に関して自動的なアップデートを利用者が合理的に期待していないようなデジタルの要素をもつ製品に対しても適用されない。デジタルの要素をもつ製品が自動的なアップデートを受けるように設計されているかどうかに拘わらず，デジタルの要素をもつ製品の製造者は，利用者に対し，脆弱性に関して連絡すべきであり，かつ，遅滞なく，セキュリティアップデートを利用できるようにすべきである。デジタルの要素をもつ製品が，当該製品の利用者との間で直接のやりとりをできるようにするユ

ーザインタフェイスまたは類似の技術的手段をもつときは，その製造者は，当該製造者のデジタルの要素をもつ製品がサポート期間の終了に至ったことを利用者に対して連絡するために，そのような機能を活用すべきである。通知は，この連絡の実効的な受領を確保するために必要なところに制限されるべきであり，かつ，デジタルの要素をもつ製品の利用者の経験に対して負の影響をもってはならない。

One of the most important measures for users to take in order to protect their products with digital elements from cyberattacks is to install the latest available security updates as soon as possible. Manufacturers should therefore design their products and put in place processes to ensure that products with digital elements include functions that enable the notification, distribution, download and installation of security updates automatically, in particular in the case of consumer products. They should also provide the possibility to approve the download and installation of the security updates as a final step. Users should retain the ability to deactivate automatic updates, with a clear and easy-to-use mechanism, supported by clear instructions on how users can opt out. The requirements relating to automatic updates as set out in an annex to this Regulation are not applicable to products with digital elements primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic updates, including products with digital elements intended to be used in professional ICT networks, and especially in critical and industrial environments where an automatic update could cause interference with operations. Irrespective of whether a product with digital elements is designed to receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay. Where a product with digital elements has a user interface or similar technical means allowing direct interaction with its users, the manufacturer should make use of such features to inform users that their product with digital elements has reached the end of the support period. Notifications should be limited to what is necessary in order to ensure the effective reception of this information and should not have a negative impact on the user experience of the product with digital elements.

(57) 脆弱性取扱のプロセスの透明性を向上させるため，そして，利用者が，最新のセキュリティアップデートを受ける目的のみのために新たな機能のアップデートのインストールを要求されないことを確保するため，製造者は，それが技術的に利用可能なときは，新たなセキュリティアップデートが，機能性のアップデートとは別に提供されることを確保すべきである。

To improve the transparency of vulnerability handling processes and to ensure that users are not required to install new functionality updates for the sole purpose of receiving the latest security updates, manufacturers should ensure, where technically feasible, that new security updates are provided separately from functionality updates.

(58) 欧州委員会並びに欧州連合の外務及び安全保障政策上級代表の「欧州経済安全保障戦略」と題する 2023 年 6 月 20 日の共同通知は，欧州連合が，欧州連合の経済安全保障に関する共通の戦略枠組みを介して，高リスクのベンダへの経済的依存からのリスクをミニマム化させつつ，欧州連合の経済的オープン性からの受益を最大化させる必要があると述べた。デジタルの要素をもつ製品の高リスクな供給者への依存は，そのデジタルの要素をもつ製品が指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体による利用を意図する場合においては特に，欧州連合レベルで対応される必

要のある戦略上のリスクを呈し得る。そのようなリスクは，製造者に対して適用可能な裁判管轄権，当該製造者の会社保有の特性，並びに，その会社の拠点のある地の第三国政府との支配上の牽連性，とりわけ，第三国が経済上のスパイ活動またはサイバー空間における無責任な国家行動に従事している地，その第三国の立法が，商業上の機微のデータを含め，全ての種類の会社運営またはデータへの恣意的なアクセスの許容を許容している地，及び，民主的なチェックとバランス，監視の仕組み，デュープロセスまたは独立の裁判所もしくは審判廷への不服申立ての権利のない，諜報目的のための義務を課すことができる地の第三国政府との支配上の牽連性と結びつき得るが，それらに限定されない。この規則の意味におけるサイバーセキュリティ上のリスクの大きさを判定する際，欧州委員会及び市場監視当局は，この規則の中に定める欧州委員会及び市場監視当局の職責に従い，非技術的なリスク要素，とりわけ，指令(EU) 2022/2555 の第 22 条に従って実施された不可欠なサプライチェーンの欧州連合レベルで調整されたセキュリティリスク評価の結果として確認された諸要素も検討すべきである。

The joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 20 June 2023 entitled 'European Economic Security Strategy' stated that the Union needs to maximise the benefits of its economic openness while minimising the risks from economic dependencies on high-risk vendors, through a common strategic framework for Union economic security. Dependencies on high-risk suppliers of products with digital elements may pose a strategic risk that needs to be addressed at Union level, especially where the products with digital elements are intended for the use by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555. Such risks may be linked, but not limited, to the jurisdiction applicable to the manufacturer, the characteristics of its corporate ownership and the links of control to a third-country government where it is established, in particular where a third country engages in economic espionage or irresponsible state behaviour in cyberspace and its legislation allows arbitrary access to any kind of company operations or data, including commercially sensitive data, and can impose obligations for intelligence purposes without democratic checks and balances, oversight mechanisms, due process or the right to appeal to an independent court or tribunal. When determining the significance of a cybersecurity risk within the meaning of this Regulation, the Commission and the market surveillance authorities, as per their responsibilities as set out in this Regulation, should also consider non-technical risk factors, in particular those established as a result of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555.

(59) 当該製品が市場に置かれた後におけるデジタルの要素をもつ製品の防護を確保する目的のために，製造者は，サポート期間を決定すべきであり，その期間は，そのデジタルの要素をもつ製品が利用に供されると予想される期間を反映すべきである。サポート期間を決定する際，製造者は，とりわけ，合理的な利用者の期待，その製品の性質及びデジタルの要素をもつ製品の耐用年数を決定する適格な欧州連合法を考慮に入れるべきである。製造者は，他の適格な諸要素も考慮に入れ得るべきである。基準は，サポート期間の決定における比例性を確保する態様で適用されるべきである。要請に応じて，製造者は，市場監視当局に対し，デジタルの要素をもつ製品のサポート期間を決定するために考慮に入れられた情報を提供すべきである。

For the purpose of ensuring the security of products with digital elements after their placing on the market,

manufacturers should determine the support period, which should reflect the time the product with digital elements is expected to be in use. In determining a support period, a manufacturer should take into account in particular reasonable user expectations, the nature of the product, as well as relevant Union law determining the lifetime of products with digital elements. Manufacturers should also be able to take into account other relevant factors. Criteria should be applied in a manner that ensures proportionality in the determination of the support period. Upon request, a manufacturer should provide market surveillance authorities with the information that was taken into account to determine the support period of a product with digital elements.

(60) その期間内はその製造者が脆弱性の実効的な取扱いを確保するサポート期間は，デジタルの要素をもつ製品の耐用年数が 5 年よりも短い場合を除き，5 年よりも短くてはならない。5 年よりも短い場合においては，製造者は，当該耐用年数の間について，脆弱性の取扱いを確保すべきである。マザーボードまたはマイクロプロセッサのようなハードウェアのコンポーネント，ルータ，モデムまたはスイッチのようなネットワーク機器，及び，オペレーティングシステムまたはビデオ編集ツールのようなソフトウェアがしばしばその場合に該当するが，デジタルの要素をもつ製品が利用に供されると合理的に予想される期間が 5 年よりも長い場合，製造者は，しかるべく，より長いサポート期間を確保すべきである。とりわけ，産業用制御システムのような，産業上の設定における利用を意図するデジタルの要素をもつ製品は，しばしば，相当に，より長い期間にわたって利用に供される。製造者は，関係するデジタルの要素をもつ製品の性質によって正当化される場合であり，かつ，当該製品が 5 年よりも短い期間利用に供されると予想される場合に限り，5 年よりも短いサポート期間を決定できるべきである。その場合においては，そのサポート期間は，予想される利用期間に対応すべきである。例えば，パンデミックの期間内の利用を意図する接触追跡アプリの耐用年数は，パンデミックの間に限定され得る。それに加えて，幾つかのソフトウェアアプリケーションは，とりわけ，サブスクリプションの期間が満了すると，そのアプリケーションが利用者にとって利用できないものとなり，その結果として，利用に供されなくなる場合においては，その性質上，サブスクリプションのモデルを基礎としてのみ利用できるようにされ得る。

The support period for which the manufacturer ensures the effective handling of vulnerabilities should be no less than five years, unless the lifetime of the product with digital elements is less than five years, in which case the manufacturer should ensure the vulnerability handling for that lifetime. Where the time the product with digital elements is reasonably expected to be in use is longer than five years, as is often the case for hardware components such as motherboards or microprocessors, network devices such as routers, modems or switches, as well as software, such as operating systems or video-editing tools, manufacturers should accordingly ensure longer support periods. In particular, products with digital elements intended for use in industrial settings, such as industrial control systems, are often in use for significantly longer periods of time. A manufacturer should be able to define a support period of less than five years only where this is justified by the nature of the product with digital elements concerned and where that product is expected to be in use for less than five years, in which case the support period should correspond to the expected use time. For instance, the lifetime of a contact tracing application intended for use during a pandemic could be limited to the duration of the pandemic. Moreover, some software applications can by nature only be made available on the basis of a subscription model, in particular where the application becomes unavailable to the user and is consequently not in use anymore once the subscription expires.

(61) デジタルの要素をもつ製品が当該製品のサポート期間の終了に至ったときは，サポート期間の終了後においても脆弱性が取り扱われ得ることを確保するため，製造者は，脆弱性取扱サービスの提供を延長することを約束している別の事業者に対しまたは公衆に対し，そのようなデジタルの要素をもつ製品のソースコードをリリースすることを検討すべきである。製造者が別の事業者に対してソースコードをリリースするときは，当該製造者は，例えば，契約上の手立てを通じて，そのデジタルの要素をもつ製品の保有を保護し，また，そのソースコードの公衆への配布を防止できるべきである。

When products with digital elements reach the end of their support periods, in order to ensure that vulnerabilities can be handled after the end of the support period, manufacturers should consider releasing the source code of such products with digital elements either to other undertakings which commit to extending the provision of vulnerability handling services or to the public. Where manufacturers release the source code to other undertakings, they should be able to protect the ownership of the product with digital elements and prevent the dissemination of the source code to the public, for example through contractual arrangements.

(62) 欧州連合全域の製造者が，同等のデジタルの要素をもつ製品に関して類似のサポート期間を決定することを確保するため，ADCO は，デジタルの要素をもつ製品の類型毎の製造者によって決定された平均サポート期間に関する統計を刊行すべきであり，また，そのような類型毎の適切なサポート期間を示すガイドを発行すべきである。加えて，域内市場全域にわたる整合化されたアプローチを確保するという観点から，欧州委員会は，製造者によって決定されたサポート期間が，この規則の中で定められたサポート期間の決定のための基準に体系上で沿っていないこと，または，異なる構成国の製造者が，正当事由なく，異なるサポート期間を決定していることを市場監視当局から提供されたデータが示唆している場合において，個々の製品類型毎のミニマムのサポート期間の細目を定めるため，委任される行為を採択できるべきである。

In order to ensure that manufacturers across the Union determine similar support periods for comparable products with digital elements, ADCO should publish statistics on the average support periods determined by manufacturers for categories of products with digital elements and issue guidance indicating appropriate support periods for such categories. In addition, with a view to ensuring a harmonised approach across the internal market, the Commission should be able to adopt delegated acts to specify minimum support periods for specific product categories where the data provided by market surveillance authorities suggests that the support periods determined by manufacturers are either systematically not in line with the criteria for determining the support periods as laid down in this Regulation or that manufacturers in different Member States unjustifiably determine different support periods.

(63) 製造者は，デジタルの要素をもつ製品の脆弱性を報告する目的の場合またはその情報を受ける目的のための場合を含め，利用者が当該製造者との間で容易に通信できるようにする単一連絡場所を設けるべきである。製造者は，単一連絡場所を，利用者にとって容易にアクセス可能であり，かつ，その可用性を明確に表示するようにし，その情報が最新のものに保たれるようにすべきである。製造者が，例えば，チャットボックスを介して，自動化されたツールを提供することを選択するときは，その製造者は，電話番号，または，電子メールアドレスもしくは問合せフォームのような別のデジタル連絡手段も提供すべきである。単一連絡場所は，自動化されたツールだけに依拠してはならない。

Manufacturers should set up a single point of contact that enables users to communicate easily with them, including for the purpose of reporting on and receiving information about the vulnerabilities of the product with digital element. They should make the single point of contact easily accessible for users and clearly indicate its availability, keeping this information up to date. Where manufacturers choose to offer automated tools, e.g. chat boxes, they should also offer a phone number or other digital means of contact, such as an email address or a contact form. The single point of contact should not rely exclusively on automated tools.

(64) 製造者は，当該製造者のデジタルの要素をもつ製品を，デフォルト設定により安全に市場において利用できるようにすべきであり，かつ，利用者に対し，無料でセキュリティアップデートを提供すべきである。製造者は，特定の企業利用者の特定の目的に適合している個別対応の製品と関係する場合であり，かつ，当該製造者及び当該利用者が異なるセットの契約条件に明示で合意している場合に限り，その必須のサイバーセキュリティ要件を免れることができるべきである。

Manufacturers should make their products with digital elements available on the market with a secure by default configuration and provide security updates to users free of charge. Manufacturers should only be able to deviate from the essential cybersecurity requirements in relation to tailor-made products that are fitted to a particular purpose for a particular business user and where both the manufacturer and the user have explicitly agreed to a different set of contractual terms.

(65) 製造者は，調整者として指定されたコンピュータセキュリティインシデント対応チーム（CSIRT）及び ENISA の両者に対し，単一報告プラットフォームを介して同時に，デジタルの要素をもつ製品の中に含まれている能動的に悪用された脆弱性及び当該製品の防護に対する影響をもつ重大なインシデントを通知すべきである。その通知は，調整者として指定された CSIRT の電子通知終点を使用して提出されるべきであり，かつ，ENISA が同時にアクセス可能であるべきである。

Manufacturers should notify simultaneously via the single reporting platform both the computer security incident response team (CSIRT) designated as coordinator as well as ENISA of actively exploited vulnerabilities contained in products with digital elements, as well as severe incidents having an impact on the security of those products. The notifications should be submitted using the electronic notification end-point of a CSIRT designated as coordinator and should be simultaneously accessible to ENISA.

(66) 調整者として指定されている CSIRT 及び ENISA が，そのような脆弱性について十分な概要把握をもち，かつ，指令(EU) 2022/2555 に定める CSIRT 及び ENISA の職務を満たすために必要となる情報の提供を受け，また，同指令の第 3 条に示す基礎法主体及び重要法主体のサイバーセキュリティのレベル全体を向上させることを確保するため，並びに，市場監視当局の実効的な稼働を確保するため，製造者は，能動的に悪用された脆弱性を通知すべきである。デジタルの要素をもつ製品の大半が域内市場全体にわたって取引されているので，デジタルの要素をもつ製品の中にある悪用された脆弱性は，域内市場の稼働を妨げる脅威であると判断されるべきである。ENISA は，製造者と合意した上で，指令(EU) 2022/2555 の第 12 条第 2 項により設置される欧州脆弱性データベースに対して，解決された脆弱性を開示すべきである。安全な製品が市場において利用できるようにされることを確

保するため，欧州脆弱性データベースは，製造者の製品の中にある既知の悪用可能な脆弱性の検出において，製造者を補助することになる。

Manufacturers should notify actively exploited vulnerabilities to ensure that the CSIRTs designated as coordinators, and ENISA, have an adequate overview of such vulnerabilities and are provided with the information necessary to fulfil their tasks as set out in Directive (EU) 2022/2555 and raise the overall level of cybersecurity of essential and important entities as referred to in Article 3 of that Directive, as well as to ensure the effective functioning of market surveillance authorities. As most products with digital elements are marketed across the entire internal market, any exploited vulnerability in a product with digital elements should be considered to be a threat to the functioning of the internal market. ENISA should, in agreement with the manufacturer, disclose fixed vulnerabilities to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555. The European vulnerability database will assist manufacturers in detecting known exploitable vulnerabilities in their products, in order to ensure that secure products are made available on the market.

(67) 製造者は，調整者として指定された CSIRT 及び ENISA に対し，デジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントも通知すべきである。当該製造者のデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントに対して利用者が迅速に対処できることを確保するため，製造者は，当該製品の利用者に対しても，そのようなインシデントに関して連絡すべきであり，また，それが適用可能なときは，例えば，当該製造者の Web サイト上で適格な情報を公表することにより，または，製造者が利用者と連絡をとることが可能であり，かつ，そのサイバーセキュリティ上のリスクによって正当化されるときは，利用者と直接に連絡をとることにより，そのインシデントの影響を緩和するために利用者が配置可能な解消の方策に関して連絡すべきである。

Manufacturers should also notify any severe incident having an impact on the security of the product with digital elements to the CSIRT designated as coordinator and ENISA. In order to ensure that users can react quickly to severe incidents having an impact on the security of their products with digital elements, manufacturers should also inform their users about any such incident and, where applicable, about any corrective measures that the users can deploy to mitigate the impact of the incident, for example by publishing relevant information on their websites or, where the manufacturer is able to contact the users and where justified by the cybersecurity risks, by reaching out to the users directly.

(68) 能動的に悪用された脆弱性は，その製造者によって市場において利用できるようにされたデジタルの要素をもつ製品の欠陥を悪意ある行為者が利用したことから，当該製造者の利用者またはそれ以外の自然人もしくは法人に対して影響を与えるセキュリティ侵害が生じたということを製造者が確認したような場合と関係している。そのような脆弱性の例は，製品の識別と認証の機能の中にある弱点であり得る。悪意ある意図のない，システムの保有者及びそのシステムの利用者の防護または安全を向上させるための誠実な試験，調査，是正または開示の目的のために発見される脆弱性は，強制的な通知に服させてはならない。他方において，デジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントは，サイバーセキュリティ上のインシデントが，利用者またはそれ以外の個人に対するサイバーセキュリティ上のリスクの増加を帰結し得るような方法により，その製造者の開発，製造または維持管理の過程に対して影響を与える状況のことを指す。そのような重大なインシ

デントは，その経路を介して製造者が利用者に対してセキュリティアップデートをリリースするリリース経路の中に，攻撃者が悪意あるコードを導入することに成功した状況を含み得る。

Actively exploited vulnerabilities concern instances where a manufacturer establishes that a security breach affecting its users or any other natural or legal persons has resulted from a malicious actor making use of a flaw in one of the products with digital elements made available on the market by the manufacturer. Examples of such vulnerabilities could be weaknesses in a product's identification and authentication functions. Vulnerabilities that are discovered with no malicious intent for purposes of good faith testing, investigation, correction or disclosure to promote the security or safety of the system owner and its users should not be subject to mandatory notification. Severe incidents having an impact on the security of the product with digital elements, on the other hand, refer to situations where a cybersecurity incident affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons. Such a severe incident could include a situation where an attacker has successfully introduced malicious code into the release channel via which the manufacturer releases security updates to users.

(69) 調整者として指定された適格な全ての CSIRT に対して通知が迅速に伝達され得ること，及び，通知過程の各段階において製造者が単一の通知のみを提出できるようにすることを確保するため，国内電子通知終点をもつ単一の報告プラットフォームが ENISA によって構築されるべきである。その単一の報告プラットフォームの日々の運用は，ENISA によって運営管理及び維持管理されるべきである。調整者として指定された CSIRT は，当該 CSIRT それぞれの市場監視当局に対し，通知された脆弱性またはインシデントを連絡すべきである。単一の報告プラットフォームは，特に，その脆弱性に関してセキュリティアップデートがまだ利用可能ではない脆弱性と関連する通知の機密性を確保するような方法によって設計されるべきである。加えて，ENISA は，防護されかつ機密の態様で情報を取扱うための手続を設けるべきである。ENISA が収集した情報を基礎として，ENISA は，デジタルの要素をもつ製品の中にあるサイバーセキュリティ上のリスクと関連する最新動向に関する隔年の技術報告書を準備すべきであり，かつ，指令(EU) 2022/2555 の第 14 条によって設けられた協力グループに対し，同報告書を提出すべきである。

To ensure that notifications can be disseminated quickly to all relevant CSIRTs designated as coordinators and to enable manufacturers to submit a single notification at each stage of the notification process, a single reporting platform with national electronic notification end-points should be established by ENISA. The day-to-day operations of the single reporting platform should be managed and maintained by ENISA. The CSIRTs designated as coordinators should inform their respective market surveillance authorities about notified vulnerabilities or incidents. The single reporting platform should be designed in such a way that it ensures the confidentiality of notifications, in particular as regards vulnerabilities for which a security update is not yet available. In addition, ENISA should put in place procedures to handle information in a secure and confidential manner. On the basis of the information it gathers, ENISA should prepare a biennial technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555.

(70) 例外的な状況下において，かつ，とりわけ，製造者からの要請に応じて，通知を最初に受領する調

整者として指定された CSIRT は，サイバーセキュリティと関連する根拠によって正当化され得る場合，かつ，厳格に必要な期間内，単一報告プラットフォームを介する調整者として指定された他の適格な CSIRT に対する通知の伝達を遅延させることを決定できるべきである。その調整者として指定された CSIRT は，直ちに，ENISA に対し，遅延させる決定及びその根拠に関し，並びに，当該 CSIRT が更に伝達することを予定している時機を連絡すべきである。欧州委員会は，委任される行為により，サイバーセキュリティと関連する根拠が適用され得るための条件に関する仕様を開発すべきであり，かつ，当該委任される行為案の準備において，指令(EU) 2022/2555 の第 15 条により設けられた CSIRT ネットワーク及び ENISA と協力すべきである。サイバーセキュリティと関連する根拠の例は，進行中の調整された脆弱性開示手続，または，製造者が直ちに解消の方策を提供することを期待され，かつ，単一報告プラットフォームを介する即時の伝達のサイバーセキュリティ上のリスクがその伝達の利益を上回っている状況を含む。調整者として指定された CSIRT から要請を受けたときは，ENISA は，当該サイバーセキュリティと関連する根拠に関する通知を保留する決定に関する当該 CSIRT から ENISA が受領した情報を基礎として通知の伝達を遅延させることとの関係におけるサイバーセキュリティと関連する根拠の適用に関し，当該 CSIRT を支援できるべきである。更に，特別に例外的な状況下においては，ENISA は，能動的に悪用された脆弱性の通知の詳細の全てを同時の態様で受領してはならない。製造者が，その製造者の通知の中で，通知される脆弱性が悪意ある行為者によって能動的に悪用されたこと，及び，利用可能な情報に従い，その製造者がその脆弱性を通知した調整者として指定された CSIRT の構成国以外のいかなる構成国においてもその脆弱性が悪用されなかったことを明記した場合，または，通知された脆弱性を即時に更に伝達することにより，その情報の開示が当該構成国の必須の利益に反し得るような情報を供給することを帰結することとなりかねない場合，または，通知された脆弱性が，更に伝達することから派生するサイバーセキュリティ上の差し迫った高度のリスクを呈している場合がその場合に該当し得るだろう。そのような場合，ENISA は，その製造者によって通知が行われたという情報，関係するデジタルの要素をもつ製品に関する一般的な情報，その悪用の一般的な性質に関する情報，並びに，当該セキュリティ上の根拠がその製造者から提起されたこと，それゆえ，その通知の内容全部が保留されることに関する情報に対する同時のアクセスのみを受けることになる。そして，通知を最初に受領する調整者として指定された CSIRT が，この規則の中で定められた特別に例外的な状況を反映する当該セキュリティ上の根拠が消滅したと判断する時に，ENISA 及び調整者として指定された他の適格な CSIRT にとって，通知の全文が利用可能となるべきである。利用可能な情報を基礎として，域内市場の防護に対して影響を与えるシステミックリスクが存在すると ENISA が判断するときは，ENISA は，通知受領者である CSIRT に対し，調整者として指定された他の CSIRT 及び ENISA 自身に対して通知の全文を伝達することを勧告すべきである。

In exceptional circumstances and in particular upon request by the manufacturer, the CSIRT designated as coordinator initially receiving a notification should be able to decide to delay its dissemination to the other relevant CSIRTs designated as coordinators via the single reporting platform where this can be justified on cybersecurity-related grounds and for a period of time that is strictly necessary. The CSIRT designated as coordinator should immediately inform ENISA about the decision to delay and on which grounds, as well as when it intends to disseminate further. The Commission should develop, through a delegated act, specifications on the terms and conditions for when cybersecurity-related grounds could be applied and should cooperate with the CSIRTs network established pursuant to

Article 15 of Directive (EU) 2022/2555, and ENISA in preparing the draft delegated act. Examples of cybersecurity-related grounds include an ongoing coordinated vulnerability disclosure procedure or situations in which a manufacturer is expected to provide a mitigating measure shortly and the cybersecurity risks of an immediate dissemination via the single reporting platform outweigh its benefits. If requested by the CSIRT designated as coordinator, ENISA should be able to support that CSIRT on the application of cybersecurity-related grounds in relation to delaying the dissemination of the notification based on the information ENISA has received from that CSIRT on the decision to withhold a notification on those cybersecurity-related grounds. Furthermore, in particularly exceptional circumstances, ENISA should not receive all the details of a notification of an actively exploited vulnerability in a simultaneous manner. This would be the case when the manufacturer marks in its notification that the notified vulnerability has been actively exploited by a malicious actor and that, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability, when any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State, or when the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination. In such cases, ENISA will only receive simultaneous access to the information that a notification was made by the manufacturer, general information about the product with digital elements concerned, the information about the general nature of the exploit and information about the fact that those security grounds were raised by the manufacturer and that the full content of the notification is therefore withheld. The full notification should then be made available to ENISA and other relevant CSIRTs designated as coordinators when the CSIRT designated as coordinator initially receiving the notification finds that those security grounds, reflecting particularly exceptional circumstances as established in this Regulation, cease to exist. Where, based on the information available, ENISA considers that there is a systemic risk affecting the security of the internal market, ENISA should recommend to the recipient CSIRT to disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

(71) 能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントを製造者が通知する場合，その製造者は，通知される情報がどのように機微であるとその製造者が考えるかを示すべきである。通知を最初に受領する調整者として指定された CSIRT は，サイバーセキュリティと関連する正当な根拠を基礎として調整者として指定された他の適格な CSIRT に対する通知の伝達の遅延を正当化する例外的な状況を当該通知が生じさせているかどうかを評価する際，その情報を考慮に入れるべきである。当該 CSIRT は，通知の全文が ENISA に対して同時に利用できるようにされないことを正当化する特別に例外的な状況を，能動的に悪用された脆弱性の通知が生じさせるかどうかを評価する際においても，その情報を考慮に入れるべきである。最後に，調整者として指定された CSIRT は，そのような脆弱性及びインシデントから派生するリスクを緩和するための適切な措置を決定する際，その情報を考慮に入れることができるべきである。

When manufacturers notify an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, they should indicate how sensitive they consider the notified information to be. The CSIRT designated as coordinator initially receiving the notification should take this information into account when assessing whether the notification gives rise to exceptional circumstances that justify a delay in the dissemination of the notification to the other relevant CSIRTs designated as coordinators based on justified cybersecurity-related grounds. It

should also take that information into account when assessing whether the notification of an actively exploited vulnerability gives rise to particularly exceptional circumstances that justify that the full notification is not made available simultaneously to ENISA. Finally, CSIRTs designated as coordinators should be able to take that information into account when determining appropriate measures to mitigate the risks stemming from such vulnerabilities and incidents.

(72) 規則(EU) 2016/679, 欧州議会及び理事会の規則(EU) 2022/2554[25], 欧州議会及び理事会の指令 2002/58/EC[26]並びに指令(EU) 2022/2555 のような欧州連合法の中で定められた他の補完的な報告の要件を考慮して, この規則の下で要求される情報の報告を簡素化するため, また, 法主体にかかる行政上の負担を軽減するため, 構成国は, そのような報告の要件のための国内レベルの単一始点を提供することを検討することが推奨される。規則(EU) 2016/679 及び指令 2002/58/EC の下におけるセキュリティ上のインシデントの報告のためのそのような国内単一始点の利用は, 規則(EU) 2016/679 及び指令 2002/58/EC の条項の適用に対し, とりわけ, 規則(EU) 2016/679 及び指令 2002/58/EC に示す機関の独立性と関連する条項に対し, 影響を与えてはならない。この規則に示す単一報告プラットフォームを設ける際, ENISA は, この規則に示す国内電子通知終点が, 欧州連合法の下において要求される別の通知も統合し得る国内単一始点に統合され得るという可能性も考慮に入れるべきである。

In order to simplify the reporting of information required under this Regulation, in consideration of other complementary reporting requirements laid down in Union law, such as Regulation (EU) 2016/679, Regulation (EU) 2022/2554 of the European Parliament and of the Council[25], Directive 2002/58/EC of the European Parliament and of the Council[26] and Directive (EU) 2022/2555, as well as to decrease the administrative burden for entities, Member States are encouraged to consider providing at national level single entry points for such reporting requirements. The use of such national single entry points for the reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. When establishing the single reporting platform referred to in this Regulation, ENISA should take into account the possibility for the national electronic notification end-points referred to in this Regulation to be integrated into national single entry points that may also integrate other notifications required under Union law.

(73) この規則に示す単一報告プラットフォームを設置するときは, かつ, 過去の経験を活かすために,

---

[25] 金融部門におけるデジタルの運用上の回復力に関する並びに規則(EC) No 1060/2009, 規則(EU) No 648/2012, 規則 (EU) No 600/2014, 規則(EU) No 909/2014 及び規則(EU) 2016/1011 を改正する欧州議会及び理事会の 2022 年 12 月 14 日の規則(EU) 2022/2554 (OJ L 333, 27.12.2022, p. 1).
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

[26] 電子通信部門における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC (OJ L 201, 31.7.2002, p. 37).
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).

ENISA は，自由，保安及び法務の領域における欧州連合大規模 IT システム運用管理局（eu-LISA）のような，厳格なセキュリティ要件に服するプラットフォームまたはデータベースを運営管理している欧州連合の他の機関または部局からも意見聴取すべきである。ENISA は，指令(EU) 2022/2555 の第 12 条第 2 項によって設置される欧州脆弱性データベースの潜在的な補完性も分析すべきである。

When establishing the single reporting platform refered to in this Regulation and in order to benefit from past experience, ENISA should consult other Union institutions or agencies that are managing platforms or databases subject to stringent security requirements, such as the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). ENISA should also analyse potential complementarities with the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.

(74) 製造者及びそれ以外の自然人及び法人は，調整者として指定された CSIRT または ENISA に対し，デジタルの要素をもつ製品の中に含まれている脆弱性，デジタルの要素をもつ製品のリスクプロファイルに対して影響を与え得るサイバー脅威，デジタルの要素をもつ製品の防護に対する影響をもつインシデント並びにそのようなインシデントを帰結した可能性のあるニアミスに関し，任意で通知できるべきである。

Manufacturers and other natural and legal persons should be able to notify to a CSIRT designated as coordinator or ENISA, on a voluntary basis, any vulnerability contained in a product with digital elements, cyber threats that could affect the risk profile of a product with digital elements, any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident.

(75) 構成国は，国内法に従い，脆弱性の調査研究者が刑事上の法的責任の危険に潜在的に晒されていることを含め，脆弱性の調査研究者が直面する検討課題に対して可能な範囲内で対処することを狙いとすべきである。幾つかの構成国において，脆弱性を調査研究する自然人及び法人が刑事及び民事の法的責任に晒され得ることに鑑み，構成国は，情報セキュリティの調査研究者の不訴追及び当該の者の行為に対する民事上の法的責任の免除に関するガイドを採択することが推奨される。

Member States should aim to address, to the extent possible, the challenges faced by vulnerability researchers, including their potential exposure to criminal liability, in accordance with national law. Given that natural and legal persons researching vulnerabilities could in some Member States be exposed to criminal and civil liability, Member States are encouraged to adopt guidelines as regards the non-prosecution of information security researchers and an exemption from civil liability for their activities.

(76) デジタルの要素をもつ製品の製造者は，当該製造者に対して直接にまたは間接に，及び，匿名によることが求められるときは，指令(EU) 2022/2555 の第 12 条第 1 項に従った調整された脆弱性開示の目的のために調整者として指定された CSIRT を介して，個人または法主体から脆弱性を報告することを容易にするため，調整された脆弱性開示の基本方針を設けるべきである。製造者の調整された脆弱性開示の基本方針は，第三者に対してまたは公衆に対して詳細な脆弱性情報が開示される

前に，当該製造者がそのような脆弱性を診断及び解消できるようにする態様で，そのプロセスを介して製造者に対して脆弱性が報告される構造化されたプロセスの細目を示すべきである。更に，製造者は，当該製造者のセキュリティ基本方針を機械読取可能なフォーマットで刊行することも検討すべきである。広範に利用されているデジタルの要素をもつ製品の中にある悪用され得る脆弱性に関する情報が闇市場において高額で販売され得ることに鑑み，そのような製品の製造者は，当該製造者の調整された脆弱性開示の基本方針の一部として，個人または法主体が当該の者の努力に対する承認及び報償を受けることを確保することによって脆弱性の報告に対してインセンティブを与える計画を利用できるべきである。この計画は，いわゆる「バグ報償対処計画」と呼ばれる。

Manufacturers of products with digital elements should put in place coordinated vulnerability disclosure policies to facilitate the reporting of vulnerabilities by individuals or entities either directly to the manufacturer or indirectly, and where requested anonymously, via CSIRTs designated as coordinators for the purposes of coordinated vulnerability disclosure in accordance with Article 12(1) of Directive (EU) 2022/2555. Manufacturers' coordinated vulnerability disclosure policy should specify a structured process through which vulnerabilities are reported to a manufacturer in a manner allowing the manufacturer to diagnose and remedy such vulnerabilities before detailed vulnerability information is disclosed to third parties or to the public. Moreover, manufacturers should also consider publishing their security policies in machine-readable format. Given the fact that information about exploitable vulnerabilities in widely used products with digital elements can be sold at high prices on the black market, manufacturers of such products should be able to use programmes, as part of their coordinated vulnerability disclosure policies, to incentivise the reporting of vulnerabilities by ensuring that individuals or entities receive recognition and compensation for their efforts. This refers to so-called 'bug bounty programmes'.

(77) 脆弱性の分析を容易にするため，製造者は，SBOM を作成することによる場合を含め，デジタルの要素をもつ製品の中に含まれるコンポーネントを特定及び文書化すべきである。SBOM は，ソフトウェアを製造し，購入し及び運用する者に対し，当該の者らのサプライチェーンの理解を拡大する情報を提供できる。その情報は，多角的な利益をもち，とりわけ，その情報は，製造者及び利用者が，既知の新たに出現した脆弱性及びサイバーセキュリティ上のリスクを追跡することを助ける。当該製造者のデジタルの要素をもつ製品が第三者によって開発された脆弱性のあるコンポーネントを含んでいないことを製造者が確保することは，とりわけ重要なことである。製造者は，SBOM を公表することを強いられてはならない。

In order to facilitate vulnerability analysis, manufacturers should identify and document components contained in the products with digital elements, including by drawing up an SBOM. An SBOM can provide those who manufacture, purchase, and operate software with information that enhances their understanding of the supply chain, which has multiple benefits, in particular it helps manufacturers and users to track known newly emerged vulnerabilities and cybersecurity risks. It is of particular importance that manufacturers ensure that their products with digital elements do not contain vulnerable components developed by third parties. Manufacturers should not be obliged to make the SBOM public.

(78) オンライン販売と結び付けられた新たな複雑なビジネスモデルの下において，オンラインで運営され

る企業は，様々なサービスを提供できる。当のデジタルの要素をもつ製品との関係において提供されるサービスの性質の相違により，同一の法主体は，異なる類型のビジネスモデルまたは経済取引主体の範疇の中にあり得る。法主体が，当のデジタルの要素をもつ製品のためのオンラインの中間介在サービスのみを提供しており，かつ，規則(EU) 2023/988 の第 13 条第 14 号に定義するオンライン市場の提供者に過ぎない場合，その法主体は，この規則の中で定義されたタイプの経済取引主体の 1 つとしての適格性があるとは評価されない。同一の法主体が，オンライン市場のプロバイダであり，かつ，デジタルの要素をもつ特定の製品の販売に関してこの規則に定義する経済取引主体としても行動している場合，その法主体は，当該タイプの経済取引主体に関してこの規則の中で定められた義務に服するべきである。例えば，オンライン市場のプロバイダがデジタルの要素をもつ製品を流通させてもいるときは，当該製品の販売に関し，そのプロバイダは，流通業者として判断されることになるだろう。同様に，当の法主体が自己ブランドのデジタルの要素をもつ製品を販売するときは，その法主体は，製造者として適格であると評価されることになり，そして，適用可能な製造者の要件を遵守しなければならないだろう。また，当該法主体がそのようなサービスを提供する場合，幾つかの法主体は，欧州議会及び理事会の規則(EU) 2019/1020[27]の第 3 条第 11 号に定義するフルフィルメントサービスのプロバイダとしての適格性があり得る。そのような場合，ケースバイケースで評価される必要があるだろう。電子商取引を実現可能化する上でオンライン市場がもつ顕著な役割に鑑み，オンライン市場を介して購入されるデジタルの要素をもつ製品がこの規則の中で定められたサイバーセキュリティ要件を遵守することを確保することを助けるため，その法主体は，構成国の市場監視当局との協力に努めるべきである。

Under the new complex business models linked to online sales, a business operating online can provide a variety of services. Depending on the nature of the services provided in relation to a given product with digital elements, the same entity may fall within different categories of business models or economic operators. Where an entity provides only online intermediation services for a given product with digital elements and is merely a provider of an online marketplace as defined in Article 3, point (14), of Regulation (EU) 2023/988, it does not qualify as one of the types of economic operator defined in this Regulation. Where the same entity is a provider of an online marketplace and also acts as an economic operator as defined in this Regulation for the sale of particular products with digital elements, it should be subject to the obligations set out in this Regulation for that type of economic operator. For instance, if the provider of an online marketplace also distributes a product with digital elements, then, with respect to the sale of that product, it would be considered to be a distributor. Similarly, if the entity in question sells its own branded products with digital elements, it would qualify as a manufacturer and would thus have to comply with the applicable requirements for manufacturers. Also, some entities can qualify as fulfilment service providers as defined in Article 3, point (11), of Regulation (EU) 2019/1020 of the European Parliament and of the Council[27] if they offer such services. Such cases would need to be assessed on a case-by-case basis. Given the prominent role that online marketplaces have in enabling

---

[27] 市場監視及び製品の法令遵守に関する，並びに，指令 2004/42/EC，規則(EC) No 765/2008 及び規則(EU) No 305/2011 を改正する欧州議会及び理事会の 2019 年 6 月 20 日の規則(EU) 2019/1020 (OJ L 169, 25.6.2019, p. 1).
Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

electronic commerce, they should strive to cooperate with the market surveillance authorities of the Member States in order to help ensure that products with digital elements purchased through online marketplaces comply with the cybersecurity requirements laid down in this Regulation.

(79) この規則の中で定められた要件の適合性の評価を容易にするため，この規則の中で定められた必須のサイバーセキュリティ要件を詳細な技術仕様に翻訳しており，かつ，欧州議会及び理事会の規則(EU) No 1025/2012[28]に従って採択されている整合化された技術標準に適合しているデジタルの要素をもつ製品に関し，適合性の推定があるべきである。同規則は，当該技術標準がこの規則の中で定められた要件を全く満たしていない場合，整合化された技術標準に対して異議を述べるための手続を定めている。標準化の過程は，バランスのとれた利益代表，及び，消費者団体を含め，民間の社会的な利害関係者の実効的な参加を確保すべきである。整合化された技術標準の開発及びこの規則の実装を容易にするため，そして，会社の遵守を容易にするため，とりわけ，マイクロ企業，小企業及び中規模企業並びにグローバルに活動している企業の遵守を容易にするため，この規則の中で定められた必須のサイバーセキュリティ要件によって狙いとされているレベルのサイバーセキュリティ上の保護に沿っている国際的な技術標準もまた考慮に入れられるべきである。

In order to facilitate assessment of conformity with the requirements laid down in this Regulation, there should be a presumption of conformity for products with digital elements which are in conformity with harmonised standards, which translate the essential cybersecurity requirements set out in this Regulation into detailed technical specifications, and which are adopted in accordance with Regulation (EU) No 1025/2012 of the European Parliament and of the Council[28]. That Regulation provides for a procedure for objections to harmonised standards where those standards do not entirely satisfy the requirements set out in this Regulation. The standardisation process should ensure a balanced representation of interests and effective participation of civil society stakeholders, including consumer organisations. International standards that are in line with the level of cybersecurity protection aimed for by the essential cybersecurity requirements set out in this Regulation should also be taken into account, in order to facilitate the development of harmonised standards and the implementation of this Regulation, as well as to facilitate compliance for companies, in particular microenterprises and small and medium-sized enterprises and those operating globally.

(80) この規則の適用のための移行期間の間における整合化された技術標準の適時の開発及びこの規則の適用の日よりも前の当該技術標準の可用性は，この規則の実効的な実装にとってとりわけ重要なこととなる。このことは，クラス I の下にあるデジタルの要素をもつ重要な製品に関しては，特にそう

[28] 欧州の標準化に関する，理事会指令 89/686/EEC 及び理事会指令 93/15/EEC，欧州議会及び理事会の指令 94/9/EC，指令 94/25/EC，指令 95/16/EC，指令 97/23/EC，指令 98/34/EC，指令 2004/22/EC，指令 2007/23/EC，指令 2009/23/EC 及び指令 2009/105/EC を改正する，並びに，理事会決定 87/95/EEC，欧州議会及び理事会の決定 No 1673/2006/EC を廃止する欧州議会及び理事会の 2012 年 10 月 25 日の規則(EU) No 1025/2012 (OJ L 316, 14.11.2012, p. 12).

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

である。整合化された技術標準の可用性は，そのような製品の製造者が，内部統制手続を介して適合性評価を遂行することを実現可能にすることとなり，それゆえ，適合性評価組織の活動の隘路と遅延を回避できる。

The timely development of harmonised standards during the transitional period for the application of this Regulation and their availability before the date of application of this Regulation will be particularly important for its effective implementation. This is, in particular, the case for important products with digital elements that fall under class I. The availability of harmonised standards will enable manufacturers of such products to perform the conformity assessments via the internal control procedure and can therefore avoid bottlenecks and delays in the activities of conformity assessment bodies.

(81) 規則(EU) 2019/881 は，ICT 製品，ICT プロセス及び ICT サービスのための任意の欧州サイバーセキュリティ認証の枠組みを設けている。欧州サイバーセキュリティ認証制度は，この規則の適用範囲内にあるデジタルの要素をもつ製品を利用するための利用者の信頼の共通枠組みを提供する。その結果として，この規則は，規則(EU) 2019/881 との間の波及効果をつくり出すべきである。この規則の中で定められた要件の適合性の評価を容易にするため，認証されているデジタルの要素をもつ製品，または，当該製品に関して規則(EU) 2019/881 による欧州サイバーセキュリティ認証制度の下において適合宣言書が発されたデジタルの要素をもつ製品であって，実装行為の中で欧州委員会によって特定された製品は，欧州サイバーセキュリティ証明書もしくは適合宣言書またはそれらの一部がそれらの要件を包摂している限り，この規則の中で定められた必須のサイバーセキュリティ要件を遵守していると推定されるべきである。デジタルの要素をもつ製品のための新たな欧州サイバーセキュリティ認証制度の必要性は，規則(EU) 2019/881 に従って欧州連合がとりまとめる作業計画の準備の際を含め，この規則に照らして評価されるべきである。この規則の遵守を容易にするための場合を含め，デジタルの要素をもつ製品を包摂する新たな制度の必要性が存在するときは，欧州委員会は，ENISA に対し，規則(EU) 2019/881 の第 48 条に従って制度候補を準備することを要請できる。そのようなデジタルの要素をもつ製品を包摂する将来の欧州サイバーセキュリティ認証制度は，この規則に定める必須のサイバーセキュリティ要件及び適合性評価手続を考慮に入れるべきであり，かつ，この規則の遵守を容易にすべきである。この規則の発効よりも前に発効する欧州サイバーセキュリティ認証制度に関しては，適合性の推定がどのようにして適用され得るのかという細部の側面に関し，更に細目を定めることが必要かもしれない。欧州委員会は，委任される行為により，当該条件の下でこの規則の中で定められた必須のサイバーセキュリティ要件に適合していることを示すために欧州サイバーセキュリティ認証制度が利用され得る条件の細目を定める権限を与えられるべきである。更に，不適切な行政上の負担を避けるため，そのような欧州サイバーセキュリティ認証制度の下において，少なくとも「十分」のレベルで欧州サイバーセキュリティ証明書が発行された場合における対応する諸要件に関し，この規則の中で定められた第三者適合性評価を実施する義務を製造者に対して負わせてはならない。

Regulation (EU) 2019/881 establishes a voluntary European cybersecurity certification framework for ICT products, ICT processes and ICT services. European cybersecurity certification schemes provide a common framework of trust for users to use products with digital elements that fall within the scope of this Regulation. This Regulation should

consequently create synergies with Regulation (EU) 2019/881. In order to facilitate the assessment of conformity with the requirements laid down in this Regulation, products with digital elements that are certified or for which a statement of conformity has been issued under a European cybersecurity scheme pursuant to Regulation (EU) 2019/881 that has been identified by the Commission in an implementing act, shall be presumed to be in compliance with the essential cybersecurity requirements set out in this Regulation in so far as the European cybersecurity certificate or statement of conformity or parts thereof cover those requirements. The need for new European cybersecurity certification schemes for products with digital elements should be assessed in the light of this Regulation, including when preparing the Union rolling work programme in accordance with Regulation (EU) 2019/881. Where there is a need for a new scheme covering products with digital elements, including in order to facilitate compliance with this Regulation, the Commission can request ENISA to prepare candidate schemes in accordance with Article 48 of Regulation (EU) 2019/881. Such future European cybersecurity certification schemes covering products with digital elements should take into account the essential cybersecurity requirements and conformity assessment procedures as set out in this Regulation and facilitate compliance with this Regulation. For European cybersecurity certification schemes that enter into force before the entry into force of this Regulation, further specifications may be needed on detailed aspects of how a presumption of conformity can apply. The Commission, by means of delegated acts, should be empowered to specify under which conditions the European cybersecurity certification schemes can be used to demonstrate conformity with the essential cybersecurity requirements set out in this Regulation. Furthermore, to avoid undue administrative burdens, there should be no obligation for manufacturers to carry out a third-party conformity assessment as provided for in this Regulation for corresponding requirements where a European cybersecurity certificate has been issued under such European cybersecurity certification schemes at least at level 'substantial'.

(82) ハードウェアセキュリティモジュール及びマイクロプロセッサのような，この規則の適用範囲内にある製品に関する実装規則(EU) 2024/482 の発効の後，欧州委員会は，委任される行為により，この規則に定める必須のサイバーセキュリティ要件またはその一部の適合性の推定を EUCC がどのように提供するかの細目を定め得るべきである。更に，そのような委任される行為は，対応する要件に関してこの規則によって要求される第三者評価を実施すべき製造者の義務を，EUCC の下で発行される証明書がどのように解消するかの細目を定め得る。

Upon entry into force of Implementing Regulation (EU) 2024/482 which concerns products that fall within the scope of this Regulation, such as hardware security modules and microprocessors, the Commission should be able to specify, by means of a delegated act, how the EUCC provides a presumption of conformity with the essential cybersecurity requirements as set out in this Regulation or parts thereof. Furthermore, such a delegated act may specify how a certificate issued under the EUCC eliminates the obligation for manufacturers to carry out a third-party assessment as required pursuant to this Regulation for corresponding requirements.

(83) 技術的な整合化及び技術標準への新たなアプローチに関する 1985 年 5 月 7 日の理事会決議の中で定められた新たなアプローチ原則並びに規則(EU) No 1025/2012 を基礎とする現行の欧州の標準化枠組みは，この規則の中で定められた適格な必須のサイバーセキュリティ要件の適合性の推定を定める技術標準を練るためのデフォルトの枠組みを表現している。欧州の技術標準は，公共の利益を考慮に入れ，また，欧州の 1 または複数の標準化組織に対して，定められた期限内に，かつ，

合意を基礎として，整合化された技術標準を起草することを求める欧州委員会の要請の中で明確に述べられている政策目的を考慮に入れた上で，市場駆動型であるべきである。ただし，整合化された技術標準への適格な参照がない場合においては，実装行為を採択する際において欧州の標準化組織の役割と機能を欧州委員会が適正に尊重することを条件として，標準化の過程が行き詰まっている場合または適切な整合化された技術標準の策定の遅延が存在する場合における当該必須のサイバーセキュリティ要件を遵守すべき製造者の義務を容易にするための例外的な代替手段として，欧州委員会は，この規則の中で定められた必須のサイバーセキュリティ要件に関する共通仕様を定める実装行為を採択できるべきである。そのような遅延が，当の技術標準の技術上の複雑性によるときは，共通仕様を定めるかどうかを検討する前に，欧州委員会によってそのことが判断されるべきである。

The current European standardisation framework, which is based on the New Approach principles set out in Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards and on Regulation (EU) No 1025/2012, represents the framework by default to elaborate standards that provide for a presumption of conformity with the relevant essential cybersecurity requirements set out in this Regulation. European standards should be market-driven, take into account the public interest, as well as the policy objectives clearly stated in the Commission's request to one or more European standardisation organisations to draft harmonised standards, within a set deadline, and be based on consensus. However, in the absence of relevant references to harmonised standards, the Commission should be able to adopt implementing acts establishing common specifications for the essential cybersecurity requirements set out in this Regulation, provided that in doing so it duly respects the role and functions of European standardisation organisations, as an exceptional fall back solution to facilitate the manufacturer's obligation to comply with those essential cybersecurity requirements, where the standardisation process is blocked or where there are delays in the establishment of appropriate harmonised standards. If such delay is due to the technical complexity of the standard in question, this should be considered by the Commission before considering whether to establish common specifications.

(84) この規則の中で定められた必須のサイバーセキュリティ要件を包摂する共通仕様を最も効率的な方法で定めるという観点から，欧州委員会は，関連する利害関係者をその過程の中に含めるべきである。

With a view to establishing, in the most efficient way, common specifications that cover the essential cybersecurity requirements set out in this Regulation, the Commission should involve relevant stakeholders in the process.

(85) 「合理的な期間」は，規則(EU) No 1025/2012 に従った EU 官報の中における整合化された技術標準への参照の公示との関係において，その技術標準への参照の EU 官報上の公示，その訂正またはその改正が期待され，かつ，規則(EU) No 1025/2012 に従って欧州技術標準が起草される期限の後 1 年を超過してはならない期間という意味をもつ。

'Reasonable period' has the meaning, in relation to the publication of a reference to harmonised standards in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012, of a period during which the publication in the *Official Journal of the European Union* of the reference to the standard, its corrigendum or its

amendment is expected and which should not exceed one year after the deadline for drafting a European standard set in accordance with Regulation (EU) No 1025/2012.

(86) この規則の中で定められた必須のサイバーセキュリティ要件の適合性評価を容易にするため，同要件の詳細な技術仕様を表現する目的のためにこの規則によって欧州委員会により採択される共通仕様に適合しているデジタルの要素をもつ製品の適合性の推定が存在すべきである。

In order to facilitate the assessment of conformity with the essential cybersecurity requirements set out in this Regulation, there should be a presumption of conformity for products with digital elements that are in conformity with the common specifications adopted by the Commission pursuant to this Regulation for the purpose of expressing detailed technical specifications of those requirements.

(87) デジタルの要素をもつ製品に対して適用可能な必須のサイバーセキュリティ要件との関係における適合性の推定を提供する整合化された技術標準，共通仕様または規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度の適用は，製造者による適合性の評価を容易にすることになる。ある要件に関してそのような手段を適用しないことを製造者が選択するときは，その製造者は，別の方法によって遵守がどのように達成されているかに関するその製造者の技術文書を示さなければならない。更に，製造者による適合性の推定を提供する整合化された技術標準，共通仕様または規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度の適用は，市場監視当局によるデジタルの要素をもつ製品の遵守の点検を容易にすることだろう。それゆえ，デジタルの要素をもつ製品の製造者は，そのような整合化された技術標準，共通仕様または欧州サイバーセキュリティ認証制度を適用することが推奨される。

The application of harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 providing presumption of conformity in relation to the essential cybersecurity requirements applicable to products with digital elements will facilitate the assessment of conformity by the manufacturers. If the manufacturer chooses not to apply such means for certain requirements, it has to indicate in their technical documentation how the compliance is reached otherwise. Furthermore, the application of harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 providing presumption of conformity by manufacturers would facilitate the check of compliance of products with digital elements by market surveillance authorities. Therefore, manufacturers of products with digital elements are encouraged to apply such harmonised standards, common specifications or European cybersecurity certification schemes.

(88) 製造者は，デジタルの要素をもつ製品の，この規則の中で定められた必須のサイバーセキュリティ要件の適合性に関し，また，それが適用可能なときは，当該デジタルの要素をもつ製品が包摂されている他の適格な欧州連合整合化立法の必須のサイバーセキュリティ要件の適合性に関し，この規則の下において要求される情報を提供するための EU 適合宣言書を作成すべきである。製造者は，欧州連合の他の法行為毎に EU 適合宣言書を作成することを要求されることもあり得る。市場監視の目的のための情報への実効的なアクセスを確保するため，欧州連合の他の全ての適格な法行為

の遵守との関係において単一の EU 適合宣言書が作成されるべきである。経済取引主体の行政上の負担を削減するため，当該単一の EU 適合宣言書を，適格な個別の適合宣言書によってつくられる合綴書類とすることが可能であるべきである。

Manufacturers should draw up an EU declaration of conformity to provide information required under this Regulation on the conformity of products with digital elements with the essential cybersecurity requirements set out in this Regulation and, where applicable, of the other relevant Union harmonisation legislation by which the product with digital elements is covered. Manufacturers may also be required to draw up an EU declaration of conformity by other Union legal acts. To ensure effective access to information for market surveillance purposes, a single EU declaration of conformity should be drawn up in respect of compliance with all relevant Union legal acts. In order to reduce the administrative burden on economic operators, it should be possible for that single EU declaration of conformity to be a dossier made up of relevant individual declarations of conformity.

(89) 製品の適合性を示す CE マークは，広い意味での適合性評価を構成する全過程の可視的な結果である。CE マークを規律する一般原則は，欧州議会及び理事会の規則(EC) No 765/2008[29]の中で定められている。デジタルの要素をもつ製品に CE マークを付すことを規律する規定は，この規則の中で定められるべきである。CE マークは，デジタルの要素をもつ製品がこの規則の中で定められた要件を遵守していることを保証するだけのマークであるべきである。

The CE marking, indicating the conformity of a product, is the visible consequence of a whole process comprising conformity assessment in a broad sense. The general principles governing the CE marking are set out in Regulation (EC) No 765/2008 of the European Parliament and of the Council[29]. Rules governing the affixing of the CE marking on products with digital elements should be laid down in this Regulation. The CE marking should be the only marking which guarantees that products with digital elements comply with the requirements set out in this Regulation.

(90) 経済取引主体が，この規則の中で定められた必須のサイバーセキュリティ要件の適合性を示すことができるようにするため，また，市場監視当局が，市場において利用できるようにされたデジタルの要素をもつ製品がそれらの要件を遵守することを確保できるようにするため，適合性評価手続を定める必要がある。欧州議会及び理事会の決定 No 768/2008/EC[30]は，包含されているリスクのレベル及び要求される防護のレベルと比例する適合性評価手続のためのモジュールを設けている。諸部門間の一貫性を確保するため，及び，アドホックな変異を避けるため，デジタルの要素をもつ製品のこの規則の中で定められた必須のサイバーセキュリティ要件の適合性を検証することのために適切な適

[29] 適格性認定のための要件を定める及び規則(EEC) No 339/93 を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の規則(EC) No 765/2008 (OJ L 218, 13.8.2008, p. 30).
Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

[30] 製品のマーケティングの共通枠組みに関する及び理事会決定 93/465/EEC を廃止する欧州議会及び理事会の 2008 年 7 月 9 日の決定 No 768/2008/EC (OJ L 218, 13.8.2008, p. 82).
Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

合性評価手続は，それらのモジュールを基礎とすべきである。適合性評価手続は，デジタルの要素をもつ製品の企画，設計，開発または製造，試験及び維持管理を含め，デジタルの要素をもつ製品の全ライフサイクルにおいて適用される製品の要件とプロセス関連の要件の両者を審査及び検査すべきである。

In order to allow economic operators to demonstrate conformity with the essential cybersecurity requirements set out in this Regulation and to allow market surveillance authorities to ensure that products with digital elements made available on the market comply with those requirements, it is necessary to provide for conformity assessment procedures. Decision No 768/2008/EC of the European Parliament and of the Council [30] establishes modules for conformity assessment procedures in proportion to the level of risk involved and the level of security required. In order to ensure inter-sectoral coherence and to avoid ad-hoc variants, conformity assessment procedures adequate for verifying the conformity of products with digital elements with the essential cybersecurity requirements set out in this Regulation should be based on those modules. The conformity assessment procedures should examine and verify both product and process-related requirements covering the whole lifecycle of products with digital elements, including planning, design, development or production, testing and maintenance of the product with digital elements.

(91) この規則の中においてデジタルの要素をもつ重要または不可欠な製品として列挙されていないデジタルの要素をもつ製品の適合性評価は，この規則に従い，決定 No 768/2008/EC のモジュール A を基礎とする内部統制手続により，製造者自身の責任の下において，当該製造者によって実施され得る。このことは，製造者が，適用可能な整合化された技術標準，共通仕様または欧州サイバーセキュリティ認証制度の全部または一部を適用しないことを選択する場合に対しても適用される。その製造者は，第三者が関与するより厳格な適合性評価手続を選択するための柔軟性を保持する。内部統制の適合性評価手続の下において，製造者は，デジタルの要素をもつ製品及びその製造の過程がこの規則の中で定められた適用可能な必須のサイバーセキュリティ要件に適合していることをその製造者の単独の責任に基づいて確保しかつ宣言する。デジタルの要素をもつ重要な製品がクラス I の下にあるときは，この規則の中で定められた必須のサイバーセキュリティ要件の適合性を示すために，付加的な保証が要求される。製造者がその製造者自身の責任の下において適合性評価を実施することを望むときは（モジュール A），その製造者は，整合化された技術標準，共通仕様または規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度であって，実装行為の中で欧州委員会により特定されたものを適用すべきである。製造者がそのような整合化された技術標準，共通仕様または欧州サイバーセキュリティ認証制度を適用しないときは，その製造者は，（モジュール B 及び C を基礎としまたはモジュール H を基礎とする）第三者が関与する適合性評価を受けるべきである。製造者にかかる行政上の負担を考慮に入れ，かつ，デジタルの要素をもつ有形及び無形の製品の設計及び開発の各段階においてサイバーセキュリティが重要な役割を演じていることを考慮に入れた上で，デジタルの要素をもつ重要な製品の遵守を比例的かつ実効的な態様で評価するために最も適切であるとして，決定 No 768/2008/EC のモジュール B 及び C を基礎としまたはモジュール H を基礎とする適合性評価手続が選ばれた。第三者適合性評価を実施する製造者は，その製品の設計及び製造過程に最も適する手続を選択できる。クラス II の下にあるデジタルの要素をもつ重要な製品の利用と結び付けられるより大きなサイバーセキュリティ上のリスクに鑑み，適合性評価は，当該製品が整合化された技術標準，共通仕様または欧州サイバーセキュリティ

認証制度を全面的または部分的に遵守している場合であっても，常に第三者が関与すべきである。無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ重要な製品の製造者は，当該製造者が技術文書を公衆に利用可能にすることを条件として，モジュール A を基礎とする内部統制手続によることができるべきである。

Conformity assessment of products with digital elements that are not listed as important or critical products with digital elements in this Regulation can be carried out by the manufacturer under its own responsibility following the internal control procedure based on module A of Decision No 768/2008/EC in accordance with this Regulation. This also applies to cases where a manufacturer chooses not to apply in whole or in part an applicable harmonised standard, common specification or European cybersecurity certification scheme. The manufacturer retains the flexibility to choose a stricter conformity assessment procedure involving a third party. Under the internal control conformity assessment procedure, the manufacturer ensures and declares on its sole responsibility that the product with digital elements and the processes of the manufacturer meet the applicable essential cybersecurity requirements set out in this Regulation. If an important product with digital elements falls under class I, additional assurance is required to demonstrate conformity with the essential cybersecurity requirements set out in this Regulation. The manufacturer should apply harmonised standards, common specifications or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 which have been identified by the Commission in an implementing act if it wants to carry out the conformity assessment under its own responsibility (module A). If the manufacturer does not apply such harmonised standards, common specifications or European cybersecurity certification schemes, the manufacturer should undergo conformity assessment involving a third party (based on modules B and C or module H). Taking into account the administrative burden on manufacturers and the fact that cybersecurity plays an important role in the design and development phase of tangible and intangible products with digital elements, conformity assessment procedures based on modules B and C or module H of Decision No 768/2008/EC have been chosen as most appropriate for assessing the compliance of important products with digital elements in a proportionate and effective manner. The manufacturer that carries out the third-party conformity assessment can choose the procedure that best suits its design and production process. Given the even greater cybersecurity risk linked with the use of important products with digital elements that fall under class II, the conformity assessment should always involve a third party, even where the product complies fully or partly with harmonised standards, common specifications or European cybersecurity certification schemes. Manufacturers of important products with digital elements qualifying as free and open-source software should be able to follow the internal control procedure based on module A, provided that they make the technical documentation available to the public.

(92) デジタルの要素をもつ有形の製品の創作は，通常，設計，開発及び製造の各段階を通じて，製造者に対して大きな努力を払うことを要求するが，ソフトウェアの形態のデジタルの要素をもつ製品の創作は，製造の段階が小さな役割を演じる一方で，ほとんど専ら設計及び開発に焦点が当てられている。それにも拘わらず，多くの場合において，ソフトウェア製品は，依然として，市場に置かれる前に，コンパイルされ，構築され，パッケージ化され，ダウンロードできるようにされ，または，物理媒体上に複製される必要がある。これらの行為は，設計，開発及び製造の各段階を横断してこの規則の中で定められた必須のサイバーセキュリティ要件の当該製品の遵守を検証するための適格な適合性評価モジュールを適用する際には，製造に該当する行為として判断されるべきである。

While the creation of tangible products with digital elements usually requires manufacturers to make substantial efforts throughout the design, development and production phases, the creation of products with digital elements in the form of software almost exclusively focuses on design and development, while the production phase plays a minor role. Nonetheless, in many cases software products still need to be compiled, built, packaged, made available for download or copied onto physical media before being placed on the market. Those activities should be considered to be activities amounting to production when applying the relevant conformity assessment modules to verify the compliance of the product with the essential cybersecurity requirements set out in this Regulation across the design, development and production phases.

(93) マイクロ企業及び小企業との関係においては，比例性を確保するため，この規則の適用範囲内にあるデジタルの要素をもつ製品のサイバーセキュリティ上の保護のレベルまたは製造者間の平等な競争の場を損なうことなく，行政上の費用負担を緩和することが適切である。それゆえ，マイクロ企業及び小企業の需要に的を絞った簡易化された技術文書の書式を，欧州委員会が策定することが適切である。欧州委員会によって採択される簡易化された技術文書の書式は，この規則の中で定められた技術文書と関連する全ての適用可能な要素を包摂すべきであり，かつ，マイクロ企業または小企業が，デジタルの要素をもつ製品の設計，開発及び製造の説明のような，どのようにすれば要求される要素を簡潔な方法で提供できるかの細目を示すべきである。そのようにして，その書式は，関係する企業に対し，提供される情報の範囲及び詳細度に関する法的確実性を提供することにより，行政上の遵守の負担を緩和することに寄与するだろう。マイクロ企業及び小企業は，拡張された書式の技術文書と関連する適用可能な要素を提供すること，そして，当該企業にとって利用可能な簡易化された技術文書の書式を利用しないことを選択できるべきである。

In relation to microenterprises and small enterprises, in order to ensure proportionality, it is appropriate to alleviate administrative costs without affecting the level of cybersecurity protection of products with digital elements that fall within the scope of this Regulation or the level playing field among manufacturers. It is therefore appropriate for the Commission to establish a simplified technical documentation form targeted at the needs of microenterprises and small enterprises. The simplified technical documentation form adopted by the Commission should cover all the applicable elements related to technical documentation set out in this Regulation and specify how a microenterprise or a small enterprise can provide the requested elements in a concise way, such as the description of the design, development and production of the product with digital elements. In doing so, the form would contribute to alleviating the administrative compliance burden by providing the enterprises concerned with legal certainty about the extent and detail of information to be provided. Microenterprises and small enterprises should be able to choose to provide the applicable elements related to technical documentation in extensive form and not take advantage of the simplified technical form available to them.

(94) 技術革新を促進及び保護するため，マイクロ企業または小企業もしくは中規模企業である製造者の利益，とりわけ，スタートアップを含め，マイクロ企業及び小企業の利益が特に考慮に入れられることが重要である。この目標のために，構成国は，訓練，認識向上，情報通信，試験及び第三者適合性評価の諸活動並びにサンドボックスの設置に関するものを含め，マイクロ企業または小企業である製造者に的を絞った取組みを発展させ得る。この規則によって要求される技術文書のような強制的な

文書，利用者に対する情報提供及び指示並びに当局との間の通信と関連する翻訳の費用は，製造者にとって，とりわけ小規模な製造者にとって，大きな費用負担を構成し得る。それゆえ，構成国は，適格な製造者の文書に関し及び製造者との間の通信に関し，構成国によって決定及び承認された言語の一つが，可能な限り多数の利用者によって広く理解される言語であると判断することができるべきである。

In order to promote and protect innovation, it is important that the interests of manufacturers that are microenterprises or small or medium-sized enterprises, in particular microenterprises and small enterprises, including start-ups, are taken into particular account. To that end, Member States could develop initiatives which are targeted at manufacturers that are microenterprises or small enterprises, including on training, awareness raising, information communication, testing and third-party conformity assessment activities, as well as the establishment of sandboxes. Translation costs related to mandatory documentation, such as the technical documentation and the information and instructions to the user required pursuant to this Regulation, and communication with authorities, may constitute a significant cost for manufacturers, in particular those of a smaller size. Therefore, Member States should be able to consider that one of the languages determined and accepted by them for relevant manufacturers' documentation and for communication with manufacturers is one which is broadly understood by the largest possible number of users.

(95) この規則の円滑な適用を確保するため，構成国は，この規則の適用の日よりも前に，十分な数の指定組織が第三者適合性評価を実施できることを確保するよう努めるべきである。製造者にとっての市場参入を妨げる隘路と障碍を避けるため，欧州委員会は，この取組みにおいて構成国及びそれ以外の適格な関係者を補助することに努めるべきである。欧州委員会の支援を得ることが適切な場合を含め，構成国によって主導される的を絞った訓練活動は，この規則の下における指定組織の活動を支援することを含め，熟練の職業人の可用性に貢献できる。更に，第三者適合性評価に伴うかもしれない費用負担を考慮し，マイクロ企業及び小企業に関してそのような費用負担を緩和することを企図する欧州連合レベル及び国内レベルの資金提供の取組みが検討されるべきである。

In order to ensure a smooth application of this Regulation, Member States should strive to ensure, before the date of application of this Regulation, that a sufficient number of notified bodies is available to carry out third-party conformity assessments. The Commission should seek to assist Member States and other relevant parties in this endeavour, in order to avoid bottlenecks and hindrances to market entry for manufacturers. Targeted training activities led by Member States, including where appropriate with the support of the Commission, can contribute to the availability of skilled professionals including to support the activities of notified bodies under this Regulation. Furthermore, in light of the costs that third-party conformity assessment may entail, funding initiatives at Union and national level that seek to alleviate such costs for microenterprises and small enterprises should be considered.

(96) 比例性を確保するため，適合性評価組織は，適合性評価手続の手数料を設定する際，スタートアップを含め，マイクロ企業並びに小企業及び中規模企業の個別の利益と需要を考慮に入れるべきである。とりわけ，適合性評価組織は，リスクベースのアプローチによることが適切でありかつそれのアプローチによる場合に限り，この規則の中で定められた適格な審査手続及び試験を適用すべきである。

In order to ensure proportionality, conformity assessment bodies, when setting the fees for conformity assessment procedures, should take into account the specific interests and needs of microenterprises and small and medium-sized enterprises, including start-ups. In particular, conformity assessment bodies should apply the relevant examination procedure and tests provided for in this Regulation only where appropriate and following a risk-based approach.

(97) 法制サンドボックスの目標は，デジタルの要素をもつ製品を市場に置く前に，管理された試験環境を設けることにより，事業者の技術革新と競争力を育成することであるべきである。法制サンドボックスは，この規則の適用範囲内にある全ての関係者にとっての法的確実性を向上させることに寄与し，並びに，とりわけ，スタートアップを含め，マイクロ企業及び小企業から提供される場合，デジタルの要素をもつ製品のための欧州連合の市場へのアクセスを容易にしかつ加速させることに寄与すべきである。

The objectives of regulatory sandboxes should be to foster innovation and competitiveness for businesses by establishing controlled testing environments before the placing on the market of products with digital elements. Regulatory sandboxes should contribute to improve legal certainty for all actors that fall within the scope of this Regulation and facilitate and accelerate access to the Union market for products with digital elements, in particular when provided by microenterprises and small enterprises, including start-ups.

(98) デジタルの要素をもつ製品に対する第三者適合性評価を実施するため，適合性評価組織は，当該組織が要件のセットを遵守すること，とりわけ，独立性，職務遂行能力及び利益相反の不存在に関する要件を遵守することを条件として，欧州委員会及び他の構成国に対する国内通知元当局から通知を受けるべきである。

In order to carry out third-party conformity assessment for products with digital elements, conformity assessment bodies should be notified by the national notifying authorities to the Commission and the other Member States, provided they comply with a set of requirements, in particular on independence, competence and absence of conflicts of interest.

(99) デジタルの要素をもつ製品の適合性評価の業務遂行における一貫性のあるレベルの品質を確保するため，その評価に関与する通知元当局及びそれ以外の組織，通知及び指定組織の監察に関する要件を定める必要もある。この規則の中で定められた制度は，規則(EC) No 765/2008 の中で定められた認定制度によって補完されるべきである。認定は，適合性評価組織の職務遂行能力の検査の必須の手段なので，通知の目的のためにも使用されるべきである。

In order to ensure a consistent level of quality in the performance of conformity assessment of products with digital elements, it is also necessary to lay down requirements for notifying authorities and other bodies involved in the assessment, notification and monitoring of notified bodies. The system set out in this Regulation should be complemented by the accreditation system provided for in Regulation (EC) No 765/2008. Since accreditation is an essential means of verifying the competence of conformity assessment bodies, it should also be used for the purposes of notification.

(100) 規則(EU) 2019/881 によって採択された欧州サイバーセキュリティ認証制度に関して通知を受けまたは委任規則(EU) 2022/30 の下で通知を受けた適合性評価組織のような，この規則の中で定められた要件と類似の要件を定めている欧州連合法の下で認定されかつ通知された適合性評価組織は，この規則の下において，改めて評価されかつ通知されるべきである。ただし，資金上及び行政上の無用の負担を避けるため，そして，円滑かつ適時の通知プロセスを確保するため，重複する要件に関しては，適格な当局によって相互の影響が定義され得る。

Conformity assessment bodies that have been accredited and notified under Union law laying down requirements similar to those laid down in this Regulation, such as a conformity assessment body that has been notified for a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 or notified under Delegated Regulation (EU) 2022/30, should be newly assessed and notified under this Regulation. However, synergies can be defined by relevant authorities regarding any overlapping requirements in order to prevent an unnecessary financial and administrative burden and to ensure a smooth and timely notification process.

(101) 必要なレベルの適合性証明書の信頼性を確保する規則(EC) No 765/2008 の中で定められた透明性認定は，適合性評価組織の技術上の能力を示す好ましい手段であるものとして欧州連合全域にわたり国内行政機関によって検討されるべきである。ただし，国内当局は，当該当局自身でその評価を実施する適切な手段を当該当局がもつことを検討できる。そのような場合，別の国内機関によって実施された評価の適切なレベルの信頼性を確保するため，当該国内当局は，欧州委員会及び他の構成国に対し，適格な法制上の要件による評価を受けた適合性評価組織の法令遵守を示す必要な文書化された証拠を提供すべきである。

Transparent accreditation as provided for in Regulation (EC) No 765/2008, ensuring the necessary level of confidence in certificates of conformity, should be considered by the national public authorities throughout the Union to be the preferred means of demonstrating the technical competence of conformity assessment bodies. However, national authorities may consider that they possess the appropriate means of carrying out that evaluation themselves. In such cases, in order to ensure the appropriate level of credibility of evaluations carried out by other national authorities, they should provide the Commission and the other Member States with the necessary documentary evidence demonstrating the compliance of the conformity assessment bodies evaluated with the relevant regulatory requirements.

(102) 適合性評価組織は，適合性の評価と結びついた当該組織の活動の一部を下請けさせ，または，子組織に頼ることが頻繁にある。市場に置かれるデジタルの要素をもつ製品に対して要求される保護のレベルを防護するため，適合性評価の下請業者及び子組織が，適合性評価の職務の遂行との関係において，指定組織と同一の要件を満たすことが不可欠である。

Conformity assessment bodies frequently subcontract parts of their activities linked to the assessment of conformity or have recourse to a subsidiary. In order to safeguard the level of protection required for a product with digital elements to be placed on the market, it is essential that conformity assessment subcontractors and subsidiaries fulfil the same requirements as notified bodies in relation to the performance of conformity assessment tasks.

(103) 適合性評価組織の通知は，新アプローチ被通知団体及び被指定団体（NANDO）情報システムを介して，通知元当局から，欧州委員会及び他の構成国に対して送付されるべきである。NANDO 情報システムは，通知された全ての組織のリストが見つけられ得る欧州委員会によって開発及び維持管理される電子的な通知ツールである。

The notification of a conformity assessment body should be sent by the notifying authority to the Commission and the other Member States via the New Approach Notified and Designated Organisations (NANDO) information system. The NANDO information system is the electronic notification tool developed and managed by the Commission where a list of all notified bodies can be found.

(104) 指定組織は，欧州連合全域にわたり当該組織のサービスを提供し得るので，他の構成国及び欧州委員会に対し，指定組織と関係する異議を述べる機会を与えることが適切である。それゆえ，当該組織が指定組織として業務運営を開始する前に，適合性評価組織の能力に関する疑問または懸念が解決され得る期間を定めることが重要である。

Since notified bodies may offer their services throughout the Union, it is appropriate to give the other Member States and the Commission the opportunity to raise objections concerning a notified body. It is therefore important to provide for a period during which any doubts or concerns as to the competence of conformity assessment bodies can be clarified before they start operating as notified bodies.

(105) 競争力の利益において，経済取引主体に対して無用の負担をつくり出すことなく，指定組織が適合性評価手続を適用することが重要である。同じ理由により，かつ，経済取引主体の平等な取扱いを確保するため，適合性評価手続の技術上の適用の一貫性が確保される必要がある。その確保は，指定組織間の適切な調整と協力を通じて最善に達成されるべきである。

In the interests of competitiveness, it is crucial that notified bodies apply the conformity assessment procedures without creating unnecessary burden for economic operators. For the same reason, and to ensure equal treatment of economic operators, consistency in the technical application of the conformity assessment procedures needs to be ensured. That should be best achieved through appropriate coordination and cooperation between notified bodies.

(106) 市場監視は，欧州連合法の適正かつ統一的な適用を確保する上で不可欠の手段である。それゆえ，当該枠組み内において適切な態様で市場監視が実施され得る法的枠組みを設けることが適切である。規則(EU) 2019/1020 の中で定められた欧州連合の市場監視及び欧州連合の市場に参入する製品の監督に関する規定は，この規則の適用範囲内にあるデジタルの要素をもつ製品に対して適用される。

Market surveillance is an essential instrument in ensuring the proper and uniform application of Union law. It is therefore appropriate to put in place a legal framework within which market surveillance can be carried out in an appropriate manner. The rules on Union market surveillance and control of products entering the Union market provided for in Regulation (EU) 2019/1020 apply to products with digital elements that fall within the scope of this Regulation.

(107) 規則(EU) 2019/1020 に従い，市場監視当局は，当該市場監視当局を指定する構成国の領土内において市場監視を実施する。この規則は，構成国が，市場監視の職務を実施する職務権限のある機関を選ぶことを妨げてはならない。各構成国は，その構成国の領土内における 1 または複数の市場監視当局を指定すべきである。構成国は，指令(EU) 2022/2555 の第 8 条により指定されもしくは設置される職務権限のある機関または規則(EU) 2019/881 の第 58 条により指定された国内サイバーセキュリティ認証機関または指令 2014/53/EU の目的のために指定された市場監視当局を含め，市場監視当局として行動する既存の当局または新たな当局を指定することを選択できるべきである。経済取引主体は，市場監視当局及びそれ以外の職務権限のある機関と全面的に協力すべきである。各構成国は，欧州委員会及び他の構成国に対し，その構成国の市場監視当局及び当該当局それぞれの職務権限分野を連絡すべきであり，また，この規則と関連する市場監視の職務を実施するために必要となる資源及び技能を確保すべきである。規則(EU) 2019/1020 の第 10 条第 2 項及び第 3 項により，各構成国は，就中，市場監視当局の調整された立場を代表すること，及び，異なる構成国の市場監視当局間の協力を補助することについて職責を負うべき単一連絡部署を指定すべきである。

In accordance with Regulation (EU) 2019/1020, a market surveillance authority carries out market surveillance in the territory of the Member State that designates it. This Regulation should not prevent Member States from choosing the competent authorities to carry out market surveillance tasks. Each Member State should designate one or more market surveillance authorities in its territory. Member States should be able to choose to designate any existing or new authority to act as market surveillance authority, including competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555, national cybersecurity certification authorities designated pursuant to Article 58 of Regulation (EU) 2019/881 or market surveillance authorities designated for the purposes of Directive 2014/53/EU. Economic operators should fully cooperate with market surveillance authorities and other competent authorities. Each Member State should inform the Commission and the other Member States of its market surveillance authorities and the areas of competence of each of those authorities and should ensure the necessary resources and skills to carry out the market surveillance tasks relating to this Regulation. Pursuant to Article 10(2) and (3) of Regulation (EU) 2019/1020, each Member State should appoint a single liaison office that should be responsible, inter alia, for representing the coordinated position of the market surveillance authorities and assisting in the cooperation between market surveillance authorities in different Member States.

(108) 規則(EU) 2019/1020 の第 30 条第 2 項により，この規則の統一的な適用のため，デジタルの要素をもつ製品のサイバー回復力に関する専門の ADCO が設置されるべきである。ADCO は，指定された市場監視当局の代表，及び，それが適切なときは，単一連絡部署の代表によって構成されるべきである。欧州委員会は，規則(EU) 2019/1020 の第 29 条により設置され，同規則の第 10 条に示す各単一連絡部署の代表及びオプションの国内専門家を含め，各構成国の代表，ADCO の議長，並びに，欧州委員会からの代表によって構成される欧州連合製品法令遵守ネットワークを通じた市場監視当局間の協力を支援及び推進すべきである。欧州委員会は，欧州連合製品法令遵守ネットワーク，ネットワークのサブグループ及び ADCO の各会合に参加すべきである。欧州委員会は，技術上及び事務処理上の支援を提供する事務局により，ADCO の補助もすべきである。ADCO は，独立の専門家を参加のために招請することもでき，また，指令 2014/53/EU の下で設置された ADCO のような別の ADCO と連絡をとることもできる。

A dedicated ADCO for the cyber resilience of products with digital elements should be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. ADCO should be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of the single liaison offices. The Commission should support and encourage cooperation between market surveillance authorities through the Union Product Compliance Network established pursuant to Article 29 of Regulation (EU) 2019/1020 and comprising representatives from each Member State, including a representative of each single liaison office as referred to in Article 10 of that Regulation and an optional national expert, the chairs of ADCOs, and representatives from the Commission. The Commission should participate in the meetings of the Union Product Compliance Network, its sub-groups and ADCO. It should also assist ADCO by means of an executive secretariat that provides technical and logistic support. ADCO may also invite independent experts to participate, and liaise with other ADCOs, such as that established under Directive 2014/53/EU.

(109) 市場監視当局は，この規則の下で設置される ADCO を介して，緊密に協力すべきであり，また，ベストプラクティスを発展させることによる場合のような国内レベルの市場監視活動を促進するためのガイド文書を開発し，及び，デジタルの要素をもつ製品のこの規則の遵守を実効的に検査するための指標を開発できるべきである。

Market surveillance authorities, through ADCO established under this Regulation, should cooperate closely and should be able to develop guidance documents to facilitate market surveillance activities at national level, such as by developing best practices and indicators to effectively check the compliance of products with digital elements with this Regulation.

(110) サイバーセキュリティ上の大きなリスクを示しているデジタルの要素をもつ製品との関係における適時の，比例的かつ実効的な措置を確保するため，そのような製品と関連して講じられることが意図されている措置について利害関係者が連絡を受ける欧州連合の安全確保手続が定められるべきである。その手続は，市場監視当局が，関連する経済取引主体と協力して，それが必要なときはより早い段階で活動できるようにもすべきである。不遵守が，整合化された技術標準の欠点に起因し得る場合を除き，構成国によって講じられる措置の正当性に関して構成国と欧州委員会が合意しているときは，欧州委員会のそれ以上の関与が要求されてはならない。

In order to ensure timely, proportionate and effective measures in relation to products with digital elements presenting a significant cybersecurity risk, a Union safeguard procedure under which interested parties are informed of measures intended to be taken with regard to such products should be provided for. This should also allow market surveillance authorities, in cooperation with the relevant economic operators, to act at an earlier stage where necessary. Where the Member States and the Commission agree as to the justification of a measure taken by a Member State, no further involvement of the Commission should be required, except where non-compliance can be attributed to shortcomings of a harmonised standard.

(111) 一定の場合において，この規則に準拠するデジタルの要素をもつ製品が，そうであるにも拘わらず，サイバーセキュリティ上の大きなリスクを示し，または，個人の健康もしくは安全，基本的な権利を保護することを意図する欧州連合法もしくは国内法の下にある義務の遵守，指令(EU) 2022/2555 の第 3

条第 1 項に示す基礎法主体によって電子情報システムを用いて提供されるサービスの可用性，真正性，完全性もしくは機密性または公共の利益の保護の他の側面に対するリスクを呈することがあり得る。それゆえ，それらのリスクの緩和を確保する規定を設ける必要がある。その結果として，市場監視当局は，経済取引主体に対し，当該製品が当該リスクを示さなくなっていることを確保すること，または，当該リスクの別に応じて，当該製品をリコールしもしくは回収することを要求するための措置を講ずるべきである。そのような方法によって市場監視当局がデジタルの要素をもつ製品の支障のない移動を制限または禁止するときは直ちに，その構成国は，欧州委員会及び他の構成国に対し，遅滞なく，その決定の理由及び正当化事由を示して，その暫定措置を通知すべきである。市場監視当局が，リスクを示しているデジタルの要素をもつ製品に対するそのような措置を採択する場合，欧州委員会は，遅滞なく，その構成国及び 1 または複数の適格な経済取引主体との間で意見聴取に入るべきであり，かつ，その国内措置を評価すべきである。同評価の結果を基礎として，欧州委員会は，その国内措置が正当化されるか否かを決定すべきである。欧州委員会は，全ての構成国宛にその決定書を発出すべきであり，かつ，直ちに，全ての構成国及びその適格な 1 または複数の経済取引主体に対し，同決定を通知すべきである。その措置が正当であると判断される場合，欧州委員会は，適格な欧州連合法を改訂するための提案を採択するかどうかも検討すべきである。

In certain cases, a product with digital elements which complies with this Regulation can nonetheless present a significant cybersecurity risk or pose a risk to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights, to the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555 or to other aspects of public interest protection. Therefore it is necessary to establish rules which ensure mitigation of those risks. As a result, market surveillance authorities should take measures to require the economic operator to ensure that the product no longer presents that risk, or to recall or withdraw it, depending on the risk. As soon as a market surveillance authority restricts or forbids the free movement of a product with digital elements in such way, the Member State should notify without delay the Commission and the other Member States of the provisional measures, indicating the reasons and justification for the decision. Where a market surveillance authority adopts such measures against products with digital elements presenting a risk, the Commission should enter into consultation with the Member States and the relevant economic operator or operators without delay and should evaluate the national measure. On the basis of the results of this evaluation, the Commission should decide whether the national measure is justified or not. The Commission should address its decision to all Member States and immediately communicate it to them and the relevant economic operator or operators. If the measure is considered to be justified, the Commission should also consider whether to adopt proposals to revise the relevant Union law.

(112) サイバーセキュリティ上の大きなリスクを示しているデジタルの要素をもつ製品に関し，かつ，当該製品がこの規則を遵守していないと信ずる理由が存在する場合において，または，この規則を遵守しているけれども，個人の健康もしくは安全，基本的な権利を保護することを意図している欧州連合法もしくは国内法の下における義務の遵守を妨げるリスク，または，指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体から電子情報システムを用いて提供されるサービスの可用性，真正性，完全性もしくは機密性を妨げるリスクのような，サイバーセキュリティ上の大きなリスク以外の大きなリスクを示す製品に関し，欧州委員会は，ENISA に対し，評価を実施することを要請できるべきである。その

評価を基礎として，欧州委員会は，実装行為により，そのリスクの性質に応じて，関係するデジタルの要素をもつ製品が合理的な期間内に市場から回収されることまたはリコールされることを要求することを含め，欧州連合レベルの是正措置または制限措置を採択できるべきである。欧州委員会は，域内市場の適正な稼働を保持するための即時の介入を正当化する例外的な状況下においてのみ，かつ，その状況を解消するために，市場監視当局によって実効的な措置が何ら講じられなかった場合に限り，そのような介入に依ることができるべきである。そのような例外的な状況は，例えば，含有されている既知の脆弱性が悪意ある行為者によって悪用されつつありながら，不遵守のデジタルの要素をもつ製品が，製造者によって複数の構成国内で広範に利用できるようにされており，指令(EU) 2022/2555 の適用範囲内にある法主体によって鍵となる部門においても利用されており，かつ，当該脆弱性に関し，その製造者が利用可能なパッチを提供しない場合においては，緊急の状況であり得る。欧州委員会は，その例外的な状況の間に限り，かつ，この規則の不遵守または大きなリスクが持続的に示されている限り，そのような緊急の状況に介入できるべきである。

For products with digital elements presenting a significant cybersecurity risk, and where there is reason to believe that they do not comply with this Regulation, or for products that comply with this Regulation, but that present other important risks, such as risks to the health or safety of persons, to compliance with obligations under Union or national law intended to protect fundamental rights or to the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555, the Commission should be able to request ENISA to carry out an evaluation. Based on that evaluation, the Commission should be able to adopt, by means of implementing acts, corrective or restrictive measures at Union level, including requiring the products with digital elements concerned to be withdrawn from the market or recalled, within a reasonable period, commensurate with the nature of the risk. The Commission should be able to have recourse to such intervention only in exceptional circumstances that justify an immediate intervention to preserve the proper functioning of the internal market, and only where no effective measures have been taken by market surveillance authorities to remedy the situation. Such exceptional circumstances may be emergency situations where, for example, a non-compliant product with digital elements is widely made available by the manufacturer throughout several Member States, used also in key sectors by entities that fall within the scope of Directive (EU) 2022/2555 while containing known vulnerabilities that are being exploited by malicious actors and for which the manufacturer does not provide available patches. The Commission should be able to intervene in such emergency situations only for the duration of the exceptional circumstances and if non-compliance with this Regulation or the important risks presented persist.

(113) 複数の構成国内においてこの規則の不遵守の兆候が存在するときは，市場監視当局は，デジタルの要素をもつ製品の遵守を検査しかつサイバーセキュリティ上のリスクを特定するという観点から，他の当局との間の共同活動を実施できるべきである。

Where there are indications of non-compliance with this Regulation in several Member States, market surveillance authorities should be able to carry out joint activities with other authorities, with a view to verifying compliance and identifying cybersecurity risks of products with digital elements.

(114) 調整された同時監督活動（「スウィープ」）は，製品の安全性を更に拡大できる市場監視当局による

特別の執行活動である。スウィープは，とりわけ，市場動向，消費者からの苦情またはそれら以外の兆候が，一定の類型のデジタルの要素をもつ製品がしばしばサイバーセキュリティ上のリスクを示していることを示唆している場合に実行されるべきである。更に，スウィープに服する製品類型を決定する際，市場監視当局は，非技術的なリスク要素と関連する諸事情も考慮に入れるべきである。その目的のために，市場監視当局は，非技術的なリスク要素と関連する諸事情を含め，指令(EU) 2022/2555 の第 22 条に従って実施された不可欠なサプライチェーンの欧州連合レベルで調整されたセキュリティリスク評価の結果を考慮に入れることができるべきである。ENISA は，市場監視当局に対し，就中，ENISA が受けた脆弱性及びインシデントの通知を基礎として，その製品に関してスウィープが開始準備され得るデジタルの要素をもつ製品の類型に関する提案書を提出すべきである。

Simultaneous coordinated control actions (sweeps) are specific enforcement actions by market surveillance authorities that can further enhance product security. Sweeps should, in particular, be conducted where market trends, consumer complaints or other indications suggest that certain categories of products with digital elements are often found to present cybersecurity risks. Furthermore, when determining the product categories to be subjected to sweeps, market surveillance authorities should also take into account circumstances relating to non-technical risk factors. To that end, market surveillance authorities should be able to take into account the results of Union level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555, including circumstances relating to non-technical risk factors. ENISA should submit proposals for categories of products with digital elements for which sweeps could be organised to the market surveillance authorities, based, inter alia, on the notifications of vulnerabilities and incidents it receives.

(115) ENISA の専門知識及び任務に照らし，ENISA は，この規則の実装の過程を支援できるべきである。とりわけ，ENISA は，デジタルの要素をもつ製品の複数の構成国にわたるこの規則の潜在的な不遵守と関連する兆候または情報を基礎として，市場監視当局によって実施される共同活動を提案できるべきであり，または，その製品に関してウィープが開始準備されるべき製品の類型を特定すべきである。例外的な状況下において，域内市場の適正な稼働を保持するために迅速な介入が求められるときは，ENISA は，欧州委員会からの要請に応じて，サイバーセキュリティ上の大きなリスクを示すデジタルの要素をもつ特定の製品との関係における評価を実施できるべきである。

In light of its expertise and mandate, ENISA should be able to support the process for implementation of this Regulation. In particular, ENISA should be able to propose joint activities to be conducted by market surveillance authorities based on indications or information regarding potential non-compliance with this Regulation of products with digital elements across several Member States or identify categories of products for which sweeps should be organised. In exceptional circumstances, ENISA should be able, at the request of the Commission, to conduct evaluations in respect of specific products with digital elements that present a significant cybersecurity risk, where an immediate intervention is required to preserve the proper functioning of the internal market.

(116) この規則は，ENISA に対し，ENISA が当該職務を実効的に実施できるようにするための専門知識及び人的資源の両者の面における十分な資源を要求する一定の職務を与える。欧州委員会は，欧州連合の一般予算案を準備する際，規則(EU) 2019/881 の第 29 条の中で定められた手続に従い，

ENISA 設置計画のための必要な予算上の資源を提案することになる。その過程において，欧州委員会は，この規則により ENISA に対して与えられた職務を含め，ENISA がその職務を満たすことができるようにするための ENISA の資源全体を検討することになる。

This Regulation confers certain tasks upon ENISA which require appropriate resources in terms of both expertise and human resources in order to enable ENISA to carry out those tasks effectively. The Commission will propose the necessary budgetary resources for ENISA's establishment plan, in accordance with the procedure set out in Article 29 of Regulation (EU) 2019/881, when preparing the draft general budget of the Union. During that process, the Commission will consider ENISA's overall resources to enable it to fulfil its tasks, including those conferred on ENISA pursuant to this Regulation.

(117) それが必要なときは法制枠組みが採択され得ることを確保するため，デジタルの要素をもつ重要な製品を列挙しているこの規則の別紙のアップデートとの関係において，欧州連合の機能に関する条約（TFEU）の第 290 条に従って法行為を採択する権限は，欧州委員会に対して委任されるべきである。この規則と同一のレベルの保護を達成する欧州連合の別の規定の適用のあるデジタルの要素をもつ製品を識別するため，この規則の適用範囲の制限または適用除外が必要となり得るかどうか，及び，それが適用可能なときは，当該制限の適用範囲の細目を定め，同条に従って法行為を採択する採択する権限は，欧州委員会に対して委任されるべきである。この規則の別紙に定めるデジタルの要素をもつ不可欠な製品の欧州サイバーセキュリティ認証制度の下にある認証を潜在的に強制にすることに関し，並びに，この規則の中で定められた不可欠性の基準を基礎とするデジタルの要素をもつ不可欠な製品のリストのアップデートに関し，そして，この規則の別紙の中で定められたような必須のサイバーセキュリティ要件またはその一部の適合性を示すために用いられ得る規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度の細目を定めることに関し，同条に従って法行為を採択する権限もまた，欧州委員会に対して委任されるべきである。市場監視データが不適切なサポート期間を示唆する場合において，特定の製品類型に関するミニマムのサポート期間の細目を定めるため，並びに，能動的に悪用された脆弱性の通知の伝達を遅延させることとの関係におけるサイバーセキュリティと関連する根拠を適用するための条件の細目を定めるため，法行為を採択する権限もまた，欧州委員会に対して委任されるべきである。更に，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品の，この規則の中で定められた必須のサイバーセキュリティ要件またはそれ以外の義務の全部または一定部分の適合性の評価のための任意のセキュリティ証明書発行プログラムを設けるため，並びに，EU 適合宣言書のミニマムの内容の細目を定めるため，及び，技術文書の中に含められる要素を補完するため，法行為を採択する権限もまた，欧州委員会に対して委任されるべきである。欧州委員会が，その準備作業の間，専門家レベルのものを含め，適切な意見聴取を実施すること，及び，当該意見聴取が，より良い立法に関する 2016 年 4 月 13 日の機関間合意[31]の中で定められた基本原則に従って実施されることは，特に重要なことである。とりわけ，委任される行為の準備への平等な参加を確保するため，欧州議会及び理事会は，構成国の専門家と同時に全ての文書を受領し，かつ，それらの専門家は，自動的に，委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。この規則によ

[31] OJ L 123, 12.5.2016, p. 1.

る委任される行為を採択する権限は，2024 年 12 月 10 日から 5 年間，欧州委員会に対して与えられるべきである。欧州委員会は，遅くとも，その 5 年間の満了日よりも 9 か月前に，権限の委任と関係する報告書を作成すべきである。遅くとも各期間の満了日よりも 3 か月前に欧州議会または理事会がそのような延長に対して異議を唱えない限り，権限の委任は，同一の長さの期間により黙示で延長されるべきである。

In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union (TFEU) should be delegated to the Commission in respect of updating an annex to this Regulation listing the important products with digital elements. Power to adopt acts in accordance with that Article should be delegated to the Commission to identify products with digital elements covered by other Union rules which achieve the same level of protection as this Regulation, specifying whether a limitation or exclusion from the scope of this Regulation would be necessary as well as the scope of that limitation, if applicable. Power to adopt acts in accordance with that Article should also be delegated to the Commission in respect of the potential mandating of certification under a European cybersecurity certification scheme of the critical products with digital elements set out in an annex to this Regulation, as well as for updating the list of critical products with digital elements based on criticality criteria set out in this Regulation, and for specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity with the essential cybersecurity requirements or parts thereof as set out in an annex to this Regulation. Power to adopt acts should also be delegated to the Commission to specify the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods, as well as to specify the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications of actively exploited vulnerabilities. Furthermore, power to adopt acts should be delegated to the Commission to establish voluntary security attestation programmes for assessing the conformity of products with digital elements qualifying as free and open-source software with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation, as well as to specify the minimum content of the EU declaration of conformity and to supplement the elements to be included in the technical documentation. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making[31]. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts. The power to adopt delegated acts pursuant to this Regulation should be conferred on the Commission for a period of five years from 10 December 2024. The Commission should draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power should be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

(118) この規則の実装のための統一的な条件を確保するため，この規則の別紙の中で定められたデジタルの要素をもつ重要な製品の類型の技術上の記述の細目を定めるため，SBOM の書式及び要素の細目を定めるため，製造者から提出される能動的に悪用された脆弱性及びデジタルの要素をも

つ製品の防護に対する影響をもつ重大なインシデントの通知の書式及び手続を別に定めるため，この規則の別紙の中で定められた必須のサイバーセキュリティ要件の遵守のための手段を提供する技術上の要件を包摂する共通仕様を設けるため，デジタルの要素をもつ製品の防護，当該製品のサポート期間及び当該製品の利用を促進するため及びデジタルの要素をもつ製品の防護に関する公衆の認識を向上させるための仕組みと関連するラベル，絵文字またはそれ以外の記号の技術仕様を定めるため，マイクロ企業及び小企業の需要に的を絞った簡易化された文書書式の細目を定めるため，並びに，域内市場の適正な稼働を保持するための即時の介入を正当化する例外的な状況の下における欧州連合レベルの是正措置または制限措置を決定するための実装権限は，欧州委員会に対して与えられるべきである。それらの権限は，欧州議会及び理事会の規則(EU) No 182/2011[32]に従って行使されるべきである。

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to specify the technical description of the categories of important products with digital elements set out in an annex to this Regulation, specify the format and elements of the SBOM, specify further the format and procedure of the notifications of actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements submitted by manufacturers, establish common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements set out in an annex to this Regulation, lay down technical specifications for labels, pictograms or any other marks related to the security of the products with digital elements, their support period and mechanisms to promote their use and to increase public awareness about the security of products with digital elements, specify the simplified documentation form targeted at the needs of microenterprises and small enterprises, and decide on corrective or restrictive measures at Union level in exceptional circumstances which justify an immediate intervention to preserve the proper functioning of the internal market. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[32].

(119) 欧州連合レベル及び国内レベルにおける市場監視当局の信頼及び建設的な協力を確保するため，この規則の適用に関与する全ての関係者は，当該の者の職務を実施する上で入手した情報及びデータの機密性を尊重すべきである。

In order to ensure trusting and constructive cooperation of market surveillance authorities at Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.

(120) この規則の中で定められた義務の実効的な執行を確保するため，各市場監視当局は，行政上の制

---

[32] 欧州委員会の実装権限の行使の構成国による管理のための仕組みに関する規定及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011 (OJ L 55, 28.2.2011, p. 13).
Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

裁金を科す権限またはそれを科すことを要求する権限をもつべきである。それゆえ，この規則の中で定められた義務の不遵守に関して国内法の中で定められる行政上の制裁金の上限が設けられるべきである。個々の具体的な案件において行政上の制裁金の額を決定する際，個別の状況における全ての適格な諸事情が考慮に入れられるべきであり，また，ミニマムのものとして，製造者が，スタートアップを含めマイクロ企業または小企業もしくは中規模企業であるかどうか，及び，類似の違反行為に関して同一の経済取引主体に対し同じ市場監視当局または別の市場監視当局によって既に行政上の制裁金が適用されているかどうかを含め，この規則の中において明示で設けられている諸事情が考慮に入れられるべきである。そのような諸事情は，行政上の制裁金が既に適用された構成国以外の構成国の領土上において同じ経済取引主体による違反行為が持続している状況下においては加算的であり得るし，または，同じ経済取引主体に関してもしくは同じタイプの違反行為に関して別の市場監視当局によって検討された別の行政上の制裁金が，他の適格な個別事情に沿って，別の構成国内で科された制裁及び当該制裁の重さを予め考慮に入れるべきであることを確保する上では，減額的であり得る。そのような全ての案件において，同一の経済取引主体に対して同一のタイプの違反行為に関して複数の構成国の市場監視当局によって適用され得る累積的な行政上の制裁金は，比例性の原則の尊重を確保すべきである。能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントの早期警戒通知のための 24 時間の期限に適合しないことを理由にマイクロ企業及び小企業に対しては行政上の制裁金を適用せず，また，この規則の違反行為を理由にオープンソースソフトウェアスチュワードに対しても行政上の制裁金を適用しないことに鑑み，かつ，制裁は実効的であり，比例的でありかつ抑止力があるべきであるという基本原則に従い，構成国は，それらの法主体に対し，金銭的な性質をもつ別の種類の制裁を科してはならない。

In order to ensure effective enforcement of the obligations laid down in this Regulation, each market surveillance authority should have the power to impose or request the imposition of administrative fines. Maximum levels for administrative fines to be provided for in national law for non-compliance with the obligations laid down in this Regulation should therefore be established. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation should be taken into account and, as a minimum, those explicitly established in this Regulation, including whether the manufacturer is a microenterprise or a small or medium-sized enterprise, including a start-up, and whether administrative fines have been already applied by the same or other market surveillance authorities to the same economic operator for a similar infringement. Such circumstances could be either aggravating, in situations where the infringement by the same economic operator persists on the territory of Member States other than that where an administrative fine has already been applied, or mitigating, in ensuring that any other administrative fine considered by another market surveillance authority for the same economic operator or the same type of infringement should already take account, along with other relevant specific circumstances, of a penalty and the quantum thereof imposed in other Member States. In all such cases, the cumulative administrative fine that could be applied by market surveillance authorities of several Member States to the same economic operator for the same type of infringement should ensure the respect of the principle of proportionality. Given that administrative fines do not apply to microenterprises or small enterprises for a failure to meet the 24-hour deadline for the early warning notification of actively exploited vulnerabilities or severe incidents having an impact on the security of the product with digital elements, nor to open-source software stewards for any infringement of this Regulation, and subject to the principle that penalties

should be effective, proportionate and dissuasive, Member States should not impose other kinds of penalties with pecuniary character on those entities.

(121) 事業者ではない者に対して行政上の制裁金が科される場合，職務権限のある機関は，適切な額の制裁金を検討する際，その構成国の一般的な所得レベル及び当該の者の経済状態を考慮に入れるべきである。行政機関が行政上の制裁金に服すべきかどうか及びその範囲を決定するのは、構成国であるべきである。

Where administrative fines are imposed on a person that is not an undertaking, the competent authority should take account of the general level of income in the Member State as well as the economic situation of the person when considering the appropriate amount of the fine. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines.

(122) 構成国は，国内状況を考慮に入れた上で，就中，資格をもつサイバーセキュリティの職業人の数を増加させること，マイクロ企業及び小企業と中規模企業のための能力構築を強化すること，並びに，サイバー脅威についての公衆の認識を向上させることによって，サイバーセキュリティの基本方針を支持するために及び欧州連合内のサイバーセキュリティのレベルを向上させるためにこの規則の中で定られた制裁金からの収入または制裁金の金銭的等価物からの収入を用い得る可能性を検討すべきである。

Member States should examine, taking into account national circumstances, the possibility of using the revenues from the penalties as provided for in this Regulation or their financial equivalent to support cybersecurity policies and increase the level of cybersecurity in the Union by, inter alia, increasing the number of qualified cybersecurity professionals, strengthening capacity building for microenterprises and small and medium-sized enterprises and improving public awareness of cyber threats.

(123) 欧州連合と第三国との間の関係において，欧州連合は，規律される製品の国際的な取引を促進することに努める。規律される製品の適合性評価及びマークを付すことに関する二国間（政府間）の相互承認協定（MRAs）のような複数の法律文書を含め，貿易を促進するために，広範な種類の措置が適用され得る。同等の技術開発レベルを基礎とし，かつ，適合性評価に関して互換性のあるアプローチを持つ MRAs は，欧州連合と第三国との間で設けられる。それらの協定は，相手方当事国の立法と適合する当事国双方の適合性評価組織から発行される証明書，適合性のマーク及び試験報告書の相互承認を基礎としている。現在，MRAs は，複数の第三国との間において設けられている。それらの MRAs は，多数の特定の部門において締結されており，それらは，ある第三国と別の第三国とでは異なるものであり得る。貿易を更に促進するため，かつ，デジタルの要素をもつ製品のサプライチェーンがグローバルなものであることを認識しつつ，適合性評価と関係する MRAs は，TFEU の第 218 条に従い，欧州連合によって，この規則の下において規律される製品に関して締結され得る。サイバー回復力は長期間にわたって欧州連合内と欧州連合外の両者において強化されたサイバーセキュリティの枠組みに貢献することになるので，サイバー回復力をグローバルに強化するため，パートナーである第三国との間の協力も重要である。

In its relationships with third countries, the Union endeavours to promote international trade in regulated products. A broad variety of measures can be applied in order to facilitate trade, including several legal instruments such as bilateral (inter-governmental) Mutual Recognition Agreements (MRAs) for conformity assessment and marking of regulated products. MRAs are established between the Union and third countries which are on a comparable level of technical development and have a compatible approach concerning conformity assessment. Those agreements are based on the mutual acceptance of certificates, marks of conformity and test reports issued by the conformity assessment bodies of either party in conformity with the legislation of the other party. Currently, MRAs are in place with several third countries. Those MRAs are concluded in a number of specific sectors, which might vary from one third country to another. In order to further facilitate trade, and recognising that supply chains of products with digital elements are global, MRAs concerning conformity assessment can be concluded for products regulated under this Regulation by the Union in accordance with Article 218 TFEU. Cooperation with partner third countries is also important, in order to strengthen cyber resilience globally, as in the long term this will contribute to a strengthened cybersecurity framework both within and outside of the Union.

(124) 消費者は，欧州議会及び理事会の指令(EU) 2020/1828[33]による代表訴訟を介して，この規則の下にある経済取引主体に対して課される義務との関係における消費者の権利を行使する資格をもつべきである。その目的のために，この規則は，消費者の集団的な利益を害しまたは害し得るこの規則の違反行為に関する代表訴訟に対して指令(EU) 2020/1828 が適用可能であることを定めるべきである。それゆえ，同指令の別紙 I は，しかるべく改正されるべきである。その点に関する国内法化措置を採択することはそれらの代表訴訟に対する同指令の適用のための条件とはなっていないが，同指令によって採択される国内法化措置の中において同改正が反映されることを確保するのは，構成国である。消費者の集団的な利益を害しまたは害し得るこの規則の条項の経済取引主体による違反行為に関して提起される代表訴訟に対する同指令の適用可能性は，2027 年 12 月 11 日から開始となるべきである。

Consumers should be entitled to enforce their rights in relation to the obligations imposed on economic operators under this Regulation through representative actions pursuant to Directive (EU) 2020/1828 of the European Parliament and of the Council[33]. For that purpose, this Regulation should provide that Directive (EU) 2020/1828 is applicable to the representative actions concerning infringements of this Regulation that harm or can harm the collective interests of consumers. Annex I to that Directive should therefore be amended accordingly. It is for the Member States to ensure that those amendments are reflected in the transposition measures adopted pursuant to that Directive, although the adoption of national transposition measures in that regard is not a condition for the applicability of that Directive to those representative actions. The applicability of that Directive to the representative actions brought with regard to infringements of provisions of this Regulation by economic operators that harm or could harm the collective interests of consumers should start from 11 December 2027.

---

33 消費者の集団的利益の保護のための代表訴訟に関する及び指令 2009/22/EC を廃止する欧州議会及び理事会の 2020 年 11 月 25 日の指令(EU) 2020/1828 (OJ L 409, 4.12.2020, p. 1).

Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

(125) 欧州委員会は，とりわけ，社会，政治，技術または市場の状態の変化に照らして修正の必要性の有無を判断するという観点から，定期的に，関連する利害関係者から意見聴取し，この規則を評価し及び見直すべきである。この規則は，規則(EU) 2022/2554 及び指令(EU) 2022/2555 の適用範囲内にあり，デジタルの要素をもつ製品を利用する法主体のサプライチェーン防護義務の遵守を促進することになる。欧州委員会は，その定期的な見直しの一部として，欧州連合のサイバーセキュリティの枠組みの複合効果を評価すべきである。

The Commission should periodically evaluate and review this Regulation, in consultation with relevant stakeholders, in particular with a view to determining the need for modification in the light of changes to societal, political, technological or market conditions. This Regulation will facilitate the compliance with supply chain security obligations of entities that fall within the scope of Regulation (EU) 2022/2554 and Directive (EU) 2022/2555 that use products with digital elements. The Commission should evaluate, as part of that periodic review, the combined effects of the Union cybersecurity framework.

(126) 経済取引主体は，この規則の中で定められた要件に適応するための十分な時間を提供されるべきである。この規則は，2026 年 9 月 11 日から適用されるべき能動的に悪用された脆弱性及びデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントに関する報告義務，並びに，2026 年 6 月 11 日から適用されるべき適合性評価組織の通知に関する条項を除き，2027 年 12 月 11 日から適用されるべきである。

Economic operators should be provided with sufficient time to adapt to the requirements set out in this Regulation. This Regulation should apply from 11 December 2027, with exception of the reporting obligations concerning actively exploited vulnerabilities and severe incidents having an impact on the security of products with digital elements, which should apply from 11 September 2026 and of the provisions on notification of conformity assessment bodies, which should apply from 11 June 2026.

(127) この規則の実装において，スタートアップを含めマイクロ企業並びに小企業及び中規模企業に対し支援を提供すること，市場における知識及び専門知識の欠如から帰結する実装のリスクをミニマム化すること，そして，この規則の中で定められた製造者の義務を製造者が遵守することを容易にすることが重要である。デジタル欧州計画及びそれ以外の欧州連合の適格な諸計画は，それらの企業が，欧州経済の成長に寄与すること及び欧州連合におけるサイバーセキュリティの共通のレベルを強化することを実現可能化する資金上及び技術上の支援を提供する。欧州連合レベルまたは国内レベルで欧州委員会及び構成国によって設置された欧州サイバーセキュリティ能力センター及び国内調整拠点並びに欧州デジタル技術革新ハブもまた，企業と公的部門の組織を支援でき，また，この規則の実装に寄与し得る。それらの組織それぞれの任務及び能力分野の範囲内において，それらの組織は，マイクロ企業並びに小企業及び中規模企業に対し，試験活動及び第三者適合性評価に関するもののような技術上及び自然科学上の支援を提供し得る。それらの組織は，この規則の実装を容易にするためのツールの配置も育成し得る。

It is important to provide support to microenterprises and small and medium-sized enterprises, including start-ups, in the

implementation of this Regulation and to minimise the risks to the implementation resulting from lack of knowledge and expertise in the market, as well as in order to facilitate compliance of manufacturers with their obligations laid down in this Regulation. The Digital Europe Programme and other relevant Union programmes provide financial and technical support that enable those enterprises to contribute to the growth of the Union economy and to the strengthening of the common level of cybersecurity in the Union. The European Cybersecurity Competence Centre and National Coordination Centres as well as European Digital Innovation Hubs established by the Commission and the Member States at Union or national level could also support companies and public sector organisations and could contribute to the implementation of this Regulation. Within their respective missions and fields of competence, they could provide technical and scientific support to microenterprises and small and medium sized enterprises, such as for testing activities and third-party conformity assessments. They could also foster the deployment of tools to facilitate the implementation of this Regulation.

(128) 更に，構成国は，法制サンドボックス及び専用通信経路の設置のような，マイクロ企業並びに小企業及び中規模企業に対するガイド及び支援の提供を狙いとする補完的な活動を行うことを検討すべきである。欧州連合内におけるサイバーセキュリティのレベルを強化するため，構成国は，デジタルの要素をもつ製品のサイバーセキュリティと関連する実現能力及び技能を発展させることへの支援を提供すること，経済取引主体，とりわけ，マイクロ企業並びに小企業及び中規模企業のサイバー回復力を向上させること，そして，デジタルの要素をもつ製品のサイバーセキュリティに関する公衆の認識を育成することも検討し得る。

Furthermore, Member States should consider taking complementary action aiming to provide guidance and support for microenterprises and small and medium-sized enterprises, such as the establishment of regulatory sandboxes and dedicated channels for communication. In order to strengthen the level of cybersecurity in the Union, Member States may also consider providing support to develop capacity and skills related to cybersecurity of products with digital elements, improving the cyber resilience of economic operators, in particular of microenterprises and small and medium-sized enterprises, and fostering public awareness about the cybersecurity of products with digital elements.

(129) この規則の目的は構成国によっては十分に達成され得ず，その活動の効果のゆえに，欧州連合レベルでより良く達成され得るので，欧州連合は，欧州連合条約の第 5 条に定める補完性の原則に従い，措置を採択できる。同条に定める比例性の原則に従い，この規則は，その目的を達成するために必要なところを超えることがない。

Since the objective of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(130) 欧州データ保護監督官は，欧州議会及び理事会の規則(EU) 2018/1725[34]の第 42 条第 1 項に従って意見聴取を受け，2022 年 11 月 9 日にその意見書を伝達した[35]，

The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[34] and delivered an opinion on 9 November 2022[35],

HAVE ADOPTED THIS REGULATION:

以上のとおりであるので, この規則を採択する:

[34] 欧州連合の機関, 組織, 事務局及び部局による個人データの処理と関連する自然人の保護並びにそのデータの支障のない移動に関する, 並びに, 規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725 (OJ L 295, 21.11.2018, p. 39).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

[35] OJ C 452, 29.11.2022, p. 23.

第 I 章 総則的な条項
Chapter I **General Provisions**

第 1 条 対象事項
Article 1 **Subject matter**

この規則は，以下のことを定める:

This Regulation lays down:

(a) デジタルの要素をもつ製品のサイバーセキュリティを確保するため，そのような製品を市場において利用できるようにすることに関する規定;

rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;

(b) デジタルの要素をもつ製品の設計，開発及び製造に関する必須のサイバーセキュリティ要件並びにそれらの製品との関係における経済取引主体のサイバーセキュリティと関係する義務;

essential cybersecurity requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;

(c) その製品が利用に供されると予想される期間内におけるデジタルの要素をもつ製品のサイバーセキュリティを確保するための，製造者によって設けられる脆弱性取扱のプロセスに関する必須のサイバーセキュリティ要件並びに同プロセスとの関係における経済取引主体の義務;

essential cybersecurity requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the time the products are expected to be in use, and obligations for economic operators in relation to those processes;

(d) 監察を含め，市場監視に関する規定並びに本条の中に示す規定及び要件の執行。

rules on market surveillance, including monitoring, and enforcement of the rules and requirements referred to in this Article.

第 2 条 適用範囲
Article 2 **Scope**

1. この規則は，市場において利用できるようにされたデジタルの要素をもつ製品であって，当該製品の

所期の目的または合理的に予想可能な利用が，直接または間接に機器またはネットワークと論理的または物理的なデータ接続を含んでいるものに対して適用される。

This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

2. この規則は，当該製品に対して以下の欧州連合の法行為が適用されるデジタルの要素をもつ製品に対しては適用されない：

This Regulation does not apply to products with digital elements to which the following Union legal acts apply:

(a) 規則(EU) 2017/745；

Regulation (EU) 2017/745;

(b) 規則(EU) 2017/746；

Regulation (EU) 2017/746;

(c) 規則(EU) 2019/2144。

Regulation (EU) 2019/2144.

3. この規則は，規則(EU) 2018/1139 に従って認証されたデジタルの要素をもつ製品に対しては適用されない。

This Regulation does not apply to products with digital elements that have been certified in accordance with Regulation (EU) 2018/1139.

4. この規則は，欧州議会及び理事会の指令 2014/90/EU[36]の適用範囲内にある機器に対しては適用されない。

This Regulation does not apply to equipment that falls within the scope of Directive 2014/90/EU of the European Parliament and of the Council[36].

[36] 船舶用機器に関する及び理事会指令 96/98/EC を廃止する欧州議会及び理事会の 2014 年 7 月 23 日の指令 2014/90/EU (OJ L 257, 28.8.2014, p. 146).
Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

5. 別紙 I の中で定められた必須のサイバーセキュリティ要件の適用のあるリスクの全部または幾つかに対処する要件を定めている欧州連合の別の規定の適用のあるデジタルの要素をもつ製品に対するこの規則の適用は，以下の場合においては，制限を受けまたは適用除外され得る：

The application of this Regulation to products with digital elements covered by other Union rules laying down requirements that address all or some of the risks covered by the essential cybersecurity requirements set out in Annex I may be limited or excluded where:

(a) そのような制限または適用除外が，当該製品に対して適用される法制枠組み全体と一貫性があり；かつ

such limitation or exclusion is consistent with the overall regulatory framework that applies to those products; and

(b) 部門別の規定が，この規則によって定められている規定と同じまたはそれ以上のレベルの保護を達成している。

the sectoral rules achieve the same or a higher level of protection as that provided for by this Regulation.

欧州委員会は，そのような制限または適用除外が必要かどうか，関係する製品及び規定，並びに，それが適格なときは，その制限の適用範囲の細目を定めることによってこの規則を補完するため，第 61 条に従って委任される行為を採択する権限を与えられる。

The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying whether such limitation or exclusion is necessary, the products and rules concerned, as well as the scope of the limitation, if relevant.

6. この規則は，デジタルの要素をもつ製品の中にある同一のコンポーネントを交換するために市場において利用できるようにされており，かつ，交換が意図されているコンポーネントと同じコンポーネント仕様に従って製造されている交換部品に対しては，適用されない。

This Regulation does not apply to spare parts that are made available on the market to replace identical components in products with digital elements and that are manufactured according to the same specifications as the components that they are intended to replace.

7. この規則は，専ら国家安全保障の目的もしくは国防の目的のために開発されもしくは修正されているデジタルの要素をもつ製品，または，機密情報の処理のために特別に設計された製品に対しては適用されない。

This Regulation does not apply to products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information.

8. この規則の中で定められた義務は，当該情報の開示が構成国の国家安全保障，公共の保安または国防という必須の利益に反するような情報の供給を伴ってはならない。

The obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.

第 3 条 定義

Article 3 **Definitions**

この規則の目的のために，以下の定義が適用される：

For the purposes of this Regulation, the following definitions apply:

(1) 「デジタルの要素をもつ製品」とは，分別されて市場に置かれるソフトウェアまたはハードウェアのコンポーネントを含め，ソフトウェアまたはハードウェアの製品及び当該製品のリモートのデータ処理ソリューションのことを意味し；

'product with digital elements' means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

(2) 「リモートのデータ処理」とは，当該処理のために製造者によってまたは製造者の責任の下においてソフトウェアが設計及び開発され，かつ，その処理がなければ，そのデジタルの要素をもつ製品がその製品の機能のいずれかを遂行することが妨げられるような隔地のデータ処理のことを意味し；

'remote data processing' means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions;

(3) 「サイバーセキュリティ」とは，規則(EU) 2019/881 の第 2 条第 1 号に定義するサイバーセキュリティのことを意味し；

'cybersecurity' means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;

(4) 「ソフトウェア」とは，電子情報システムの一部であって，コンピュータコードで組成されるもののことを意味し；

'software' means the part of an electronic information system which consists of computer code;

(5) 「ハードウェア」とは，デジタルデータを処理すること，記録保存することまたは伝送することが可能な物理的な電子情報システムまたはその一部のことを意味し；

‘hardware’ means a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data;

(6) 「コンポーネント」とは，電子情報システムの中に組み込まれることを意図されたソフトウェアまたはハードウェアのことを意味し；

‘component’ means software or hardware intended for integration into an electronic information system;

(7) 「電子情報システム」とは，電気機器または電子機器を含め，デジタルデータを処理すること，記録保存することまたは伝送することを実現可能にするシステムのことを意味し；

‘electronic information system’ means a system, including electrical or electronic equipment, capable of processing, storing or transmitting digital data;

(8) 「論理的な接続」とは，ソフトウェアインタフェイスを介して実装されたデータ接続の仮想的な表現のことを意味し；

‘logical connection’ means a virtual representation of a data connection implemented through a software interface;

(9) 「物理的な接続」とは，電気的インタフェイス，光インタフェイスもしくは機械的インタフェイス，有線または電波を介する場合を含め，電子情報システム間またはコンポーネント間の物理的な手段を使用して実装された接続のことを意味し；

‘physical connection’ means a connection between electronic information systems or components implemented using physical means, including through electrical, optical or mechanical interfaces, wires or radio waves;

(10) 「間接的な接続」とは，機器またはネットワークへの接続であって，直接的にではなく，そのような機器またはネットワークに対して直接に接続可能なより大きなシステムの一部として接続が起きるもののことを意味し；

‘indirect connection’ means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network;

(11) 「終点」とは，ネットワークに接続されており，かつ，当該ネットワークへの始点を提供する機器のことを意味し；

‘end-point’ means any device that is connected to a network and serves as an entry point to that network;

(12) 「経済取引主体」とは，製造者，権限のある代理者，輸入業者，流通業者またはそれら以外の自然人もしくは法人であって，デジタルの要素をもつ製品の製造と関係する義務に服する者，または，この規則に従ってデジタルの要素をもつ製品を市場において利用できるようにしていることと関係する義務に服する者のことを意味し；

‘economic operator’ means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of products with digital elements or to the making available of products with digital elements on the market in accordance with this Regulation;

(13) 「製造者」とは，デジタルの要素をもつ製品を開発もしくは製造し，または，デジタルの要素をもつ製品を設計させ，開発させもしくは製造させ，かつ，有料であるか，収益化であるかまたは無料であるかの別を問わず，その者の名前または商標の下で当該製品を市場に出す自然人または法人のことを意味し；

‘manufacturer’ means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge;

(14) 「オープンソースソフトウェアスチュワード」とは，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ特定の製品の開発のために継続的な支援を自動的に提供することを目的または目標としてもち，かつ，商業活動を意図する製造者以外の法人であって，当該製品の存続を確保する者のことを意味し；

‘open-source software steward’ means a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products;

(15) 「権限のある代理者」とは，欧州連合内に拠点をもつ自然人または法人であって，製造者から，特定の仕事との関係においてその製造者の代わりに行為することの書面による委任を受けている者のことを意味し；

‘authorised representative’ means a natural or legal person established within the Union who has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks;

(16) 「輸入業者」とは，欧州連合内に拠点をもつ自然人または法人であって，欧州連合の外に拠点をもつ自然人または法人の名前または商標を表示しているデジタルの要素をもつ製品を市場に置く者のことを意味し；

‘importer’ means a natural or legal person established in the Union who places on the market a product with

digital elements that bears the name or trademark of a natural or legal person established outside the Union;

(17) 「流通業者」とは，当該製品の性質に影響を与えることなく，欧州連合の市場においてデジタルの要素をもつ製品を利用できるようにする，製造者または輸入業者以外の，サプライチェーン内の自然人または法人のことを意味し；

'distributor' means a natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a product with digital elements available on the Union market without affecting its properties;

(18) 「消費者」とは，当該の者の取引，事業，技能または職業の外にある目的のために行動する自然人のことを意味し；

'consumer' means a natural person who acts for purposes which are outside that person's trade, business, craft or profession;

(19) 「マイクロ企業」，「小企業」及び「中規模企業」とは，それぞれ，勧告 2003/361/EC の別紙に定義するマイクロ企業，小企業及び中規模企業のことを意味し；

'microenterprises', 'small enterprises' and 'medium-sized enterprises' mean, respectively, microenterprises, small enterprises and medium-sized enterprises as defined in the Annex to Recommendation 2003/361/EC;

(20) 「サポート期間」とは，当該期間中，デジタルの要素をもつ製品の脆弱性が実効的かつ別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に従って取り扱われることを確保することを製造者が要求される期間のことを意味し；

'support period' means the period during which a manufacturer is required to ensure that vulnerabilities of a product with digital elements are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I;

(21) 「市場に置く」とは，欧州連合の市場において，デジタルの要素をもつ製品を最初に利用できるようにすることを意味し；

'placing on the market' means the first making available of a product with digital elements on the Union market;

(22) 「市場において利用できるようにする」とは，対価を得るか無料であるかの別を問わず，商業活動の過程において，デジタルの要素をもつ製品を流通または利用のために欧州連合の市場に供給することを意味し；

'making available on the market' means the supply of a product with digital elements for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(23) 「所期の目的」とは，使用説明書，宣伝広告または販売用の素材及び文言の中において並びに技術文書の中において製造者から供給された情報の中で指示されているような，個別の文脈及び利用条件を含め，デジタルの要素をもつ製品に関してその製造者によって意図されている利用のことを意味し；

‘intended purpose’ means the use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(24) 「合理的に予想可能な利用」とは，使用説明書，宣伝広告または販売用の素材及び文言の中において並びに技術文書の中においてその製造者から供給された所期の目的であるとは限らない利用ではあるけれども，合理的に予想可能な人間の行動または技術上の操作もしくは相互作用から帰結する見込みのある利用のことを意味し；

‘reasonably foreseeable use’ means use that is not necessarily the intended purpose supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation, but which is likely to result from reasonably foreseeable human behaviour or technical operations or interactions;

(25) 「合理的に予想可能な濫用」とは，当該製品の所期の目的に従っていない方法によるデジタルの要素をもつ製品の利用であるが，合理的に予想可能な人間の行動または別のシステムとの間の相互作用から帰結し得るもののことを意味し；

‘reasonably foreseeable misuse’ means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(26) 「通知元当局」とは，適合性評価組織の評価，指定及び通知のために必要な手続並びに適合性評価組織の監視のために必要な手続を設け及び実施する職責を負う国内当局のことを意味し；

‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(27) 「適合性評価」とは，別紙 I の中で定められた必須のサイバーセキュリティ要件が満たされているか否かを検証する過程のことを意味し；

‘conformity assessment’ means the process of verifying whether the essential cybersecurity requirements set out in Annex I have been fulfilled;

(28) 「適合性評価組織」とは，規則(EU) No 765/2008 の第 2 条第 13 号に定義する適合性評価組織のことを意味し；

‘conformity assessment body’ means a conformity assessment body as defined in Article 2, point (13), of Regulation (EC) No 765/2008;

(29) 「指定組織」とは，この規則の第 43 条及び他の適格な欧州連合整合化立法に従って指定された適合性評価組織のことを意味し；

‘notified body’ means a conformity assessment body designated in accordance with Article 43 and other relevant Union harmonisation legislation;

(30) 「大きな修正」とは，当該製品が市場に置かれる後におけるデジタルの要素をもつ製品に対する変更であって，そのデジタルの要素をもつ製品の，別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件の遵守に影響を与える変更またはその所期の目的に関して当該デジタルの要素をもつ製品が評価された所期の目的に対する修正を帰結する変更のことを意味し；

‘substantial modification’ means a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I or which results in a modification to the intended purpose for which the product with digital elements has been assessed;

(31) 「CE マーク」とは，当該マークによって，デジタルの要素をもつ製品及び当該製造者により設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件及び CE マークを付すことを定めている他の適用可能な欧州連合整合化立法に適合していることを製造者が表示するマークのことを意味し；

‘CE marking’ means a marking by which a manufacturer indicates that a product with digital elements and the processes put in place by the manufacturer are in conformity with the essential cybersecurity requirements set out in Annex I and other applicable Union harmonisation legislation providing for its affixing;

(32) 「欧州連合整合化立法」とは，規則(EU) 2019/1020 の別紙 I の中で列挙された欧州連合の立法及び同規則が適用される製品のマーケティングに関する条件を整合化する他の欧州連合の立法のことを意味し；

‘Union harmonisation legislation’ means Union legislation listed in Annex I to Regulation (EU) 2019/1020 and any other Union legislation harmonising the conditions for the marketing of products to which that Regulation applies;

(33) 「市場監視当局」とは，規則(EU) 2019/1020 の第 3 条第 4 号に定義する市場監視当局のことを意味し；

‘market surveillance authority’ means a market surveillance authority as defined in Article 3, point (4), of Regulation (EU) 2019/1020;

(34) 「国際的な技術標準」とは，規則(EU) No 1025/2012 の第 2 条第 1 号(a)に定義する国際的な技術標準のことを意味し；

‘international standard’ means an international standard as defined in Article 2, point (1)(a), of Regulation (EU) No 1025/2012;

(35) 「欧州の技術標準」とは，規則(EU) No 1025/2012 の第 2 条第 1 号(b)に定義する欧州の技術標準のことを意味し；

‘European standard’ means a European standard as defined in Article 2, point (1)(b), of Regulation (EU) No 1025/2012;

(36) 「整合化された技術標準」とは，規則(EU) No 1025/2012 の第 2 条第 1 号(c)に定義する整合化された技術標準のことを意味し；

‘harmonised standard’ means a harmonised standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012;

(37) 「サイバーセキュリティ上のリスク」とは，インシデントによって生じる損失または破壊の可能性であり，かつ，そのような損失または破壊の大きさ及びそのインシデントの発生の蓋然性の組合せとして表現されるべきもののことを意味し；

‘cybersecurity risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

(38) 「サイバーセキュリティ上の大きなリスク」とは，そのリスクの技術上の特性を基礎として，物的または非物的な大きな損失または破壊を生じさせることによる場合を含め，重大な負の影響を導き得るインシデントの高い蓋然性をもつと評価され得るサイバーセキュリティ上のリスクのことを意味し；

‘significant cybersecurity risk’ means a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption;

(39) 「ソフトウェア素材表」とは，デジタルの要素をもつ製品のソフトウェア要素の中に含まれているコンポーネントの詳細及びサプライチェーンとの関係を含んでいる正式の記録のことを意味し；

‘software bill of materials’ means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements;

(40) 「脆弱性」とは，デジタルの要素をもつ製品の，サイバー脅威によって悪用され得る弱点，感受性または欠陥のことを意味し；

‘vulnerability’ means a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat;

(41) 「悪用可能な脆弱性」とは，実際に運用可能な条件の下において，敵対者によって実効的に使用される可能性をもつ脆弱性のことを意味し；

‘exploitable vulnerability’ means a vulnerability that has the potential to be effectively used by an adversary under practical operational conditions;

(42) 「能動的に悪用された脆弱性」とは，その脆弱性に関し，悪意ある行為者が，そのシステムの保有者の許可なく，システムの中にある脆弱性を悪用したことの信頼できる証拠が存在する脆弱性のことを意味し；

‘actively exploited vulnerability’ means a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner;

(43) 「インシデント」とは，指令(EU) 2022/2555 の第 6 条第 6 号に定義するインシデントのことを意味し；

‘incident’ means an incident as defined in Article 6, point (6), of Directive (EU) 2022/2555;

(44) 「デジタルの要素をもつ製品の防護に対する影響をもつインシデント」とは，データまたは機能の可用性，真正性，完全性または機密性を保護するためのデジタルの要素をもつ製品の能力に対して負の影響を与えるインシデントまたは負の影響を与えることが可能なインシデントのことを意味し；

‘incident having an impact on the security of the product with digital elements’ means an incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions;

(45) 「ニアミス」とは，指令(EU) 2022/2555 の第 6 条第 5 号に定義するニアミスのことを意味し；

‘near miss’ means a near miss as defined in Article 6, point (5), of Directive (EU) 2022/2555;

(46) 「サイバー脅威」とは，規則(EU) 2019/881 の第 2 条第 8 号に定義するサイバー脅威のことを意味し；

‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;

(47) 「個人データ」とは，規則(EU) 2016/679 の第 4 条第 1 号に定義する個人データのことを意味し；

‘personal data’ means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(48) 「無料でオープンソースのソフトウェア」とは，そのソフトウェアのソースコードがオープンに共有されており，かつ，そのソースコードに無料でアクセスでき，それを利用でき，修正できかつ再配布できるようにするための全ての権利を提供する無料でオープンソースの利用許諾の下で利用できるようにされているソフトウェアのことを意味し；

‘free and open-source software’ means software the source code of which is openly shared and which is made available under a free and open-source licence which provides for all rights to make it freely accessible, usable, modifiable and redistributable;

(49) 「リコール」とは，規則(EU) 2019/1020 の第 3 条第 22 号に定義するリコールのことを意味し；

‘recall’ means recall as defined in Article 3, point (22), of Regulation (EU) 2019/1020;

(50) 「回収」とは，規則(EU) 2019/1020 の第 3 条第 23 号に定義する回収のことを意味し；

‘withdrawal’ means withdrawal as defined in Article 3, point (23), of Regulation (EU) 2019/1020;

(51) 「調整者として指定された CSIRT」とは，規則(EU) 2022/2555 の第 12 条第 1 項により調整者として指定された CSIRT のことを意味する。

‘CSIRT designated as coordinator’ means a CSIRT designated as coordinator pursuant to Article 12(1) of Directive (EU) 2022/2555.

第 4 条 支障のない移動

Article 4 **Free movement**

1. 構成国は，この規則によって包摂されている事柄のために，この規則を遵守しているデジタルの要素をもつ製品を市場において利用できるようにすることを阻害してはならない。

Member States shall not impede, for the matters covered by this Regulation, the making available on the market of products with digital elements which comply with this Regulation.

2. 見本市，展示会，説明会またはそれらと類似のイベントの際，構成国は，その製品がこの規則を遵守していないこと及びその製品がこの規則を遵守するまではその製品が市場で利用できるようにされないことを明確に表示する視認可能な徴憑がその製品に表示されていることを条件として，その製品の試作品を含め，この規則を遵守していないデジタルの要素をもつ製品の展示または利用を妨げてはならない。

At trade fairs, exhibitions, demonstrations or similar events, Member States shall not prevent the presentation or use of a product with digital elements which does not comply with this Regulation, including its prototypes, provided that the product is presented with a visible sign clearly indicating that it does not comply with this Regulation and that it is not to be made available on the market until it does so.

3. 構成国は，この規則を遵守していないことを明確に表示する視認可能な徴憑により試験の目的のために要求される限定された期間だけそのソフトウェアが利用できるようにされること及び試験以外の目的のためにはそのソフトウェアが市場において利用できるようにされないことを条件として，この規則を遵守しない未完成のソフトウェアを市場において利用できるようにすることを妨げてはならない。

Member States shall not prevent the making available on the market of unfinished software which does not comply with this Regulation, provided that the software is made available only for a limited period required for testing purposes with a visible sign clearly indicating that it does not comply with this Regulation and that it will not be available on the market for purposes other than testing.

4. 第 3 項は，この規則以外の欧州連合整合化立法に示す安全性コンポーネントに対しては適用されない。

Paragraph 3 does not apply to safety components as referred to in Union harmonisation legislation other than this Regulation.

第 5 条 デジタルの要素をもつ製品の調達または利用

Article 5 Procurement or use of products with digital elements

1. この規則は，構成国が，デジタルの要素をもつ製品を，そのような要件が欧州連合法の中で定められた構成国の義務と一貫性があること，かつ，当該目的の達成のためにそれらの要件が必要かつ比例的であることを条件として，国家安全保障の目的または国防の目的で当該製品が調達または利用される場合を含め，特別の目的のためのそれらの製品の調達または利用に関する付加的なサイバーセキュリティ要件に服させることを妨げてはならない。

This Regulation shall not prevent Member States from subjecting products with digital elements to additional cybersecurity requirements for the procurement or use of those products for specific purposes, including where those products are procured or used for national security or defence purposes, provided that such requirements are consistent with Member States' obligations laid down in Union law and that they are necessary and proportionate for the achievement of those purposes.

2. 指令 2014/24/EU 及び指令 2014/25/EU を妨げることなく，この規則の適用範囲内にあるデジタルの要素をもつ製品が調達される場合，構成国は，脆弱性を実効的に取扱うための製造者の能力を含め，この規則の別紙 I の中で定められた必須のサイバーセキュリティ要件の遵守がその調達手続の中で考慮に入れられることを確保する。

Without prejudice to Directives 2014/24/EU and 2014/25/EU, where products with digital elements that fall within the scope of this Regulation are procured, Member States shall ensure that compliance with the essential cybersecurity requirements set out in Annex I to this Regulation, including the manufacturers' ability to handle vulnerabilities effectively, are taken into consideration in the procurement process.

第 6 条 デジタルの要素をもつ製品に関する要件

Article 6 **Requirements for products with digital elements**

デジタルの要素をもつ製品は，以下の場合に限り，市場において利用できるようにされる：

Products with digital elements shall be made available on the market only where:

(a) 当該製品の所期の目的のためにまたは合理的に予測可能な条件の下において適正にインストールされ，維持管理され，利用されていることを条件として，当該製品が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件に適合しており，かつ，それが適用可能なときは，必要なセキュリティアップデートがインストールされていること；かつ，

they meet the essential cybersecurity requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed; and

(b) 製造者によって設けられたプロセスが，別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件を遵守していること。

the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

第 7 条　デジタルの要素をもつ重要な製品

Article 7 Important products with digital elements

1. 別紙 Ⅲ の中で定められた製品類型のコア機能性をもつデジタルの要素をもつ製品は，デジタルの要素をもつ重要な製品であると判断され，かつ，第 32 条第 2 項及び第 3 項に示す適合性評価手続に服する。別紙 Ⅲ の中で定められた製品類型のコア機能性をもつデジタルの要素をもつ製品を組み込むことは，それ自体としては，当該製品が組み込まれている製品を第 32 条第 2 項及び第 3 項に示す適合性評価手続に服させてはならない。

Products with digital elements which have the core functionality of a product category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3). The integration of a product with digital elements which has the core functionality of a product category set out in Annex III shall not in itself render the product in which it is integrated subject to the conformity assessment procedures referred to in Article 32(2) and (3).

2. 別紙 Ⅲ の中で定められたクラス Ⅰ とクラス Ⅱ に分割された本条の第 1 項に示すデジタルの要素をもつ製品の類型は，以下の基準の少なくとも 1 つに適合するものとする：

The categories of products with digital elements referred to in paragraph 1 of this Article, divided into classes I and II as set out in Annex III, meet at least one of the following criteria:

(a) そのデジタルの要素をもつ製品は，認証とアクセスを安全にすること，侵入の防止と検出，終点の防護またはネットワークの保護を含め，他の製品，ネットワークまたはサービスのサイバーセキュリティにとって不可欠な機能を主として遂行する；

the product with digital elements primarily performs functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, end-point security or network protection;

(b) そのデジタルの要素をもつ製品は，当該リスクの強度の面における負の影響という大きなリスクをもち，かつ，ネットワークの運営管理，設定管理，仮想化または個人データの処理を含め，中枢システムの機能のような，直接の操作を介して多数の他の製品に対しまたはその製品の利用者の健康，防護もしくは安全を破壊し，支配し，または，損害を生じさせる能力をもつ機能を遂行する。

the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

3. 欧州委員会は，デジタルの要素をもつ製品の各クラスの類型の中に新たな類型のリストを含めること及びその定義の細目を定めることによって，製品の類型を一方のクラスから他方のクラスへと移動することによって，または，同リストから既存の類型を撤去することによって別紙 Ⅲ を改正するため，第 61 条に従って委任される行為を採択する権限を与えられる。別紙 Ⅲ の中で定められたリストの改正の必要性を評価する際，欧州委員会は，サイバーセキュリティと関連する機能性または機能及び本条の第 2 項に示す基準によって定められるようなデジタルの要素をもつ製品によって呈されるサイバーセキュリティ上のリスクのレベルを考慮に入れる。

The Commission is empowered to adopt delegated acts in accordance with Article 61 to amend Annex III by including in the list a new category within each class of the categories of products with digital elements and specifying its definition, moving a category of products from one class to the other or withdrawing an existing category from that list. When assessing the need to amend the list set out in Annex III, the Commission shall take into account the cybersecurity-related functionalities or the function and the level of cybersecurity risk posed by the products with digital elements as set out by the criteria referred to in paragraph 2 of this Article.

本項の第 1 副項に示す委任される行為は，それが適切なときは，とりわけ，別紙 Ⅲ の中で定められたクラス Ⅰ もしくはクラス Ⅱ にデジタルの要素をもつ重要な製品の新たな類型が付加され，または，クラス Ⅰ もしくはクラス Ⅱ からデジタルの要素をもつ重要な製品の類型が移動されるときは，第 32 条第 2 項及び第 3 項に示す適格な適合性評価手続が適用を開始する前に，緊急性という優越する理由によってより短い移行期間が正当化される場合を除き，12 か月のミニマムの移行期間を定める。

The delegated acts referred to in the first subparagraph of this paragraph shall, where appropriate, provide for a minimum transitional period of 12 months, in particular where a new category of important products with digital elements is added to class I or II or is moved from class I to II as set out in Annex III, before the relevant conformity assessment procedures as referred to in Article 32(2) and (3) start applying, unless a shorter transitional period is justified on imperative grounds of urgency.

4. 2025 年 12 月 11 日までに，欧州委員会は，別紙 Ⅲ に定めるクラス Ⅰ 及びクラス Ⅱ の下にあるデジタルの要素をもつ製品の類型の技術上の記述並びに別紙 Ⅳ に定めるデジタルの要素をもつ製品の類型の技術上の記述の細目を定める実装行為を採択する。その実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。
By 11 December 2025, the Commission shall adopt an implementing act specifying the technical description of the categories of products with digital elements under classes I and II as set out in Annex III and the technical description of the categories of products with digital elements as set out in Annex IV. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 62(2).

第 8 条　デジタルの要素をもつ不可欠な製品

Article 8 **Critical products with digital elements**

1. 規則(EU) 2019/881 によって当該デジタルの要素をもつ製品の類型を包摂している欧州サイバーセキュリティ認証制度が採択されており，かつ，製造者にとって利用可能であることを条件として，欧州委員会は，この規則の別紙 Ⅳ の中で定められている製品類型のコア機能性をもつどのデジタルの要素をもつ製品が，この規則の別紙 Ⅰ の中で定められた必須のサイバーセキュリティ要件またはその一部に適合していることを示すために規則(EU) 2019/881 によって採択された欧州サイバーセキュリティ認証制度の下において少なくとも「十分」の保証レベルの欧州サイバーセキュリティ証明書を獲得することを要求されるかを決定するため，この規則を補完するために第 61 条に従って委任される行為を採択する権限を与えられる。それらの委任される行為は，デジタルの要素をもつ製品と関係するサイバーセキュリティ上のリスクのレベルと比例して要求される保証レベルの細目を定め，かつ，指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体による当該製品への不可欠の依存関係を含め，それらの製品の所期の目的を考慮に入れる。

The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation to determine which products with digital elements that have the core functionality of a product category that is set out in Annex IV to this Regulation are to be required to obtain a European cybersecurity certificate at assurance level at least ‘substantial’ under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, to demonstrate conformity with the essential cybersecurity requirements set out in Annex I to this Regulation or parts thereof, provided that a European cybersecurity certification scheme covering those categories of products with digital elements has been adopted pursuant to Regulation (EU) 2019/881 and is available to manufacturers. Those delegated acts shall specify the required assurance level that shall be proportionate to the level of cybersecurity risk associated with the products with digital elements and shall take account of their intended purpose, including the critical dependency on them by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555.

そのような委任される行為を採択する前に，欧州委員会は，予定されている措置の市場に対する潜在的な影響の評価を実施し，かつ，規則(EU) 2019/881 の下において設けられた欧州サイバーセキュリティ認証グループを含め，適格な利害関係者の意見聴取を実施する。その評価は，適格な欧州サイバーセキュリティ認証制度の実装のための構成国の準備態勢及び実現能力のレベルを考慮に入れる。本項の第 1 副項に示す委任される行為が採択されなかった場合，別紙 Ⅳ に定める製品類型のコア機能性をもつデジタルの要素をもつ製品は，第 32 条第 3 項に示す適合性評価手続に服する。

Before adopting such delegated acts, the Commission shall carry out an assessment of the potential market impact of the envisaged measures and shall carry out consultations with relevant stakeholders, including the European Cybersecurity Certification Group established under Regulation (EU) 2019/881. The assessment shall take into account the readiness and the capacity level of the Member States for the implementation of the relevant European cybersecurity certification scheme. Where no delegated acts as referred to in the first subparagraph of this paragraph have been adopted, products with digital elements which have the core functionality of a product category as set out in Annex IV shall be subject to the conformity assessment procedures referred to in Article 32(3).

第 1 副項に示す委任される行為は，緊急性という優越する理由によってより短い移行期間が正当化

される場合を除き，6か月のミニマムの移行期間を定める。

The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency.

2. 欧州委員会は，デジタルの要素をもつ不可欠な製品の類型を付加することまたは撤去することによって別紙 IV を改正するため，第 61 条に従って委任される行為を採択する権限を与えられる。本条の第 1 項に従ってデジタルの要素をもつ不可欠の製品のそのような類型及び要求される保証レベルを決定する際，欧州委員会は，第 7 条第 2 項に示す基準を考慮に入れ，かつ，デジタルの要素をもつ製品の類型が以下の基準の少なくとも 1 つと適合することを確保する：

The Commission is empowered to adopt delegated acts in accordance with Article 61 to amend Annex IV by adding or withdrawing categories of critical products with digital elements. When determining such categories of critical products with digital elements and the required assurance level, in accordance with paragraph 1 of this Article, the Commission shall take into account the criteria referred to in Article 7(2) and ensure that the categories of products with digital elements meet at least one of the following criteria:

(a) デジタルの要素をもつ製品の類型に対する指令(EU) 2022/2555 の第 3 条に示す基礎法主体の不可欠の依存関係が存在すること；

there is a critical dependency of essential entities as referred to in Article 3 of Directive (EU) 2022/2555 on the category of products with digital elements;

(b) デジタルの要素をもつ製品の類型と関係するインシデント及び悪用された脆弱性が域内市場全域にわたる不可欠なサプライチェーンに対して深刻な破壊を導き得ること。

incidents and exploited vulnerabilities concerning the category of products with digital elements could lead to serious disruptions of critical supply chains across the internal market.

そのような委任される行為を採択する前に，欧州委員会は，第 1 項に示すタイプの評価を実施する。

Before adopting such delegated acts, the Commission shall carry out an assessment of the type referred to in paragraph 1.

第 1 副項に示す委任される行為は，緊急性という優越する理由によってより短い移行期間が正当化される場合を除き，6か月のミニマムの移行期間を定める。

The delegated acts referred to in the first subparagraph shall provide for a minimum transitional period of six months, unless a shorter transitional period is justified for imperative reasons of urgency.

第 9 条 利害関係者の意見聴取

Article 9 **Stakeholder consultation**

1. この規則の実装のための措置を準備する際, 欧州委員会は, 適格な構成国の機関, マイクロ企業並びに小企業及び中規模企業を含め, 民間部門の事業者, オープンソースソフトウェアのコミュニティ, 消費者団体, 学術団体, 並びに, 欧州連合の適格な部局及び組織, 並びに, 欧州連合レベルで設けられた専門家グループのような, 適格な利害関係者から意見聴取し, かつ, その見解を考慮に入れる。とりわけ, 欧州委員会は, 以下の場合において, それが適切であるときは, 構成された態様でそれらの利害関係者から意見聴取し, かつ, その見解を求める:

When preparing measures for the implementation of this Regulation, the Commission shall consult and take into account the views of relevant stakeholders, such as relevant Member State authorities, private sector undertakings, including microenterprises and small and medium-sized enterprises, the open-source software community, consumer associations, academia, and relevant Union agencies and bodies as well as expert groups established at Union level. In particular, the Commission shall, in a structured manner, where appropriate, consult and seek the views of those stakeholders when:

(a) 第 26 条に示すガイドを準備する場合;

preparing the guidance referred to in Article 26;

(b) 第 61 条を妨げることなく, 第 7 条第 4 項に従って別紙 III の中で定められた製品類型の技術上の記述を準備する場合, 第 7 条第 3 項及び第 8 条第 2 項に従って製品類型のリストの潜在的なアップデートの必要性を評価する場合, または, 第 8 条第 1 項に示す市場に対する潜在的な影響の評価を実施する場合;

preparing the technical descriptions of the product categories set out in Annex III in accordance with Article 7(4), assessing the need for potential updates of the list of product categories in accordance with Article 7(3) and Article 8(2), or carrying out the assessment of the potential market impact referred to in Article 8(1), without prejudice to Article 61;

(c) この規則の評価及び見直しのための準備作業を行う場合。

undertaking preparatory work for the evaluation and review of this Regulation.

2. 欧州委員会は, この規則の実装に関し, 第 1 項に示す利害関係者の見解を収集するため, 少なくとも年 1 回, 定期的な意見聴取及び情報収集の会合を開始準備する。

The Commission shall organise regular consultation and information sessions, at least once a year, to gather the views of the stakeholders referred to in paragraph 1 on the implementation of this Regulation.

第 10 条　サイバー回復力のあるデジタル環境における技能の拡大

Article 10 **Enhancing skills in a cyber resilient digital environment**

この規則の目的のために，かつ，この規則の実装を支援する職業人の需要に対応するため，構成国は，それが適切なときは，欧州委員会，欧州サイバーセキュリティ能力拠点及び ENISA の支援を得て，教育分野における構成国の職責を全面的に尊重しつつ，以下のことを狙いとする措置及び戦略を促進する：

For the purposes of this Regulation and in order to respond to the needs of professionals in support of the implementation of this Regulation, Member States with, where appropriate, the support of the Commission, the European Cybersecurity Competence Centre and ENISA, while fully respecting the responsibility of the Member States in the education field, shall promote measures and strategies aiming to:

(a) 市場監視当局及び適合性評価組織の活動を支援するための技能をもつ職業人の十分な可用性を確保するため，サイバーセキュリティの技能を開発すること並びに組織上のツール及び技術上のツールをつくり出すこと；

develop cybersecurity skills and create organisational and technological tools to ensure sufficient availability of skilled professionals in order to support the activities of the market surveillance authorities and conformity assessment bodies;

(b) 民間部門，製造者の従業者の技能の再獲得または技能向上を含め，経済取引主体，消費者，訓練プロバイダ及び行政機関の間における共働を増加させること，それによって，サイバーセキュリティ部門の中にある職にアクセスするための若い人々の選択肢を拡大すること。

increase collaboration between the private sector, economic operators, including via re-skilling or up-skilling for manufacturers' employees, consumers, training providers as well as public administrations, thereby expanding the options for young people to access jobs in the cybersecurity sector.

第 11 条　一般的な製品の安全性

Article 11 **General product safety**

規則(EU) 2023/988 の第 2 条第 1 項第 3 副項(b)からの特例により，当該製品が規則(EU) 2023/988 の第 3 条第 27 号に定義する他の「欧州連合整合化立法」の中で定められた個別の安全性要件に服さないときは，同規則の第 III 章第 1 節，第 V 章及び第 VII 章並びに第 IX 章ないし第 XI 章は，この規則によって包摂されない側面及びリスクまたはリスク類型との関係において，デジタルの要素をもつ製品に対して適用される。

By way of derogation from Article 2(1), third subparagraph, point (b), of Regulation (EU) 2023/988, Chapter III, Section 1, Chapters V and VII, and Chapters IX to XI of that Regulation shall apply to products with digital elements with respect

to aspects and risks or categories of risks that are not covered by this Regulation where those products are not subject to specific safety requirements laid down in other 'Union harmonisation legislation' as defined in Article 3, point (27), of Regulation (EU) 2023/988.

第 12 条 高リスク AI システム

Article 12 **High-risk AI systems**

1. 規則(EU) 2024/1689 の第 15 条の中で定められた正確性及び堅牢性と関連する要件を妨げることなく，この規則の適用範囲内にありかつ規則(EU) 2024/1689 の第 6 条により高リスク AI システムとして分類されているデジタルの要素をもつ製品は，以下のとおりであるときは，同規則の第 15 条の中で定められたサイバーセキュリティ要件を遵守していると推定される:

Without prejudice to the requirements relating to accuracy and robustness set out in Article 15 of Regulation (EU) 2024/1689, products with digital elements which fall within the scope of this Regulation and which are classified as high-risk AI systems pursuant to Article 6 of that Regulation shall be deemed to comply with the cybersecurity requirements set out in Article 15 of that Regulation where:

(a) 当該製品は，別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を満たしている;

those products fulfil the essential cybersecurity requirements set out in Part I of Annex I;

(b) 製造者によって設けられたプロセスは，別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件を遵守している;かつ

the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I; and

(c) 規則(EU) 2024/1689 の第 15 条の下において要求されるサイバーセキュリティ上の保護のレベルが達成されていることが，この規則の下において発行される EU 適合宣言書の中で示されている。

the achievement of the level of cybersecurity protection required under Article 15 of Regulation (EU) 2024/1689 is demonstrated in the EU declaration of conformity issued under this Regulation.

2. 本条の第 1 項に示すデジタルの要素をもつ製品及びサイバーセキュリティ要件に関し，規則(EU) 2024/1689 の第 43 条の中で定められた適格な適合性評価手続が適用される。その評価の目的のために，規則(EU) 2024/1689 の下にある高リスク AI システムの適合性を監督する職務権限のある指定組織は，この規則の第 39 条の中で定められた要件を当該指定組織が遵守していることが規則(EU)

2024/1689 の下にある通知手続の過程で評価されることを条件として，この規則の適用範囲内にある高リスク AI システムのこの規則の別紙 I の中で定められた要件の適合性を監督するための職務権限ももつ。

For the products with digital elements and cybersecurity requirements referred to in paragraph 1 of this Article, the relevant conformity assessment procedure provided for in Article 43 of Regulation (EU) 2024/1689 shall apply. For the purposes of that assessment, notified bodies which are competent to control the conformity of the high-risk AI systems under Regulation (EU) 2024/1689 shall also be competent to control the conformity of high-risk AI systems which fall within the scope of this Regulation with the requirements set out in Annex I to this Regulation, provided that the compliance of those notified bodies with the requirements laid down in Article 39 of this Regulation has been assessed in the context of the notification procedure under Regulation (EU) 2024/1689.

3. 本条の第 2 項からの特例により，この規則の別紙 III に列挙するデジタルの要素をもつ重要な製品であって，この規則の第 32 条第 2 項(a)及び(b)並びに第 32 条第 3 項に示す適合性評価手続に服する製品，並びに，この規則の別紙 IV に列挙するデジタルの要素をもつ不可欠な製品であって，この規則の第 8 条第 1 項により欧州サイバーセキュリティ証明書を得ることが要求される製品，または，その証明書がないときは，この規則の第 32 条第 3 項に示す適合性評価手続に服する製品であり，かつ，規則(EU) 2024/1689 の第 6 条により高リスク AI システムとしても分類されており，当該製品に対して，規則(EU) 2024/1689 の別紙 VI に示す内部統制を基礎とする適合性評価手続が適用される製品は，この規則の中で定められた必須のサイバーセキュリティ要件と関係する範囲内において，この規則の中で定められた適合性評価手続に服する。

By way of derogation from paragraph 2 of this Article, important products with digital elements as listed in Annex III to this Regulation, which are subject to the conformity assessment procedures referred to in Article 32(2), points (a) and (b), and Article 32(3) of this Regulation and critical products with digital elements as listed in Annex IV to this Regulation which are required to obtain a European cybersecurity certificate pursuant to Article 8(1) of this Regulation or, absent that, which are subject to the conformity assessment procedures referred to in Article 32(3) of this Regulation, and which are classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689, and to which the conformity assessment procedure based on internal control as referred to in Annex VI to Regulation (EU) 2024/1689 applies, shall be subject to the conformity assessment procedures provided for in this Regulation in so far as the essential cybersecurity requirements set out in this Regulation are concerned.

4. 本条の第 1 項に示すデジタルの要素をもつ製品の製造者は，規則(EU) 2024/1689 の第 57 条に示す AI 法制サンドボックスに参加できる。

Manufacturers of products with digital elements as referred to in paragraph 1 of this Article may participate in the AI regulatory sandboxes referred to in Article 57 of Regulation (EU) 2024/1689.

第II章　経済取引主体の義務及び無料でオープンソースのソフトウェアと関係する条項
Chapter Ⅱ **Obligations of Economic Operators and Provisions in relation to Free and Open-Source Software**

第 13 条　製造者の義務
Article 13 **Obligations of manufacturers**

1. デジタルの要素をもつ製品を市場に置く際，製造者は，別紙Ⅰのパート Ⅰの中で定められた必須のサイバーセキュリティ要件に従ってその製品が設計，開発及び製造されていることを確保する。

When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.

2. 第 1 項を遵守する目的のために，製造者は，サイバーセキュリティ上のリスクをミニマム化し，インシデントを防止し，及び，利用者の健康及び安全との関係を含め，そのインシデントの影響をミニマム化するという観点から，デジタルの要素をもつ製品と関係するサイバーセキュリティ上のリスクの評価を行い，かつ，そのデジタルの要素をもつ製品の企画段階，設計段階，開発段階，製造段階，流通段階及び維持管理の段階の間，当該評価の結果を考慮に入れる。

For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

3. サイバーセキュリティ上のリスク評価は，文書化され，かつ，本条の第 8 項に従って決定されるサポート期間内，しかるべくアップデートされる。そのサイバーセキュリティ上のリスク評価は，当該製品が利用に供されると予想される期間を考慮に入れた上で，少なくとも，所期の目的及び合理的に予測可能な利用並びに運用環境または保護される資産のような，デジタルの要素をもつ製品の利用条件を基礎とするサイバーセキュリティ上のリスクの分析によって組成される。サイバーセキュリティ上のリスク評価は，別紙Ⅰのパート Ⅰの第 2 号の中で定められたセキュリティ要件が適格なデジタルの要素をもつ製品に対して適用可能であるかどうか及びそれが適用可能なときはどのような態様で適用可能なのかを示し，また，サイバーセキュリティ上のリスク評価によって報告されるものとして，当該要件がどのように実装されるのかを示す。その評価は，その製造者が，別紙Ⅰのパート Ⅰの第 1 号及び別紙Ⅰのパート Ⅱの中で定められた脆弱性取扱の要件をどのように適用することになるのかも示す。

The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether

and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.

4. デジタルの要素をもつ製品を市場に置く際，その製造者は，第 31 条及び別紙 VII によって要求される技術文書の中に，本条の第 3 項に示すサイバーセキュリティ上のリスク評価を含める。第 12 条に示すデジタルの要素をもつ製品であって，他の欧州連合の法行為にも服する製品に関しては，そのサイバーセキュリティ上のリスク評価は，当該欧州連合の法行為によって要求されるリスク評価の一部であり得る。デジタルの要素をもつ製品に対して一定の必須のサイバーセキュリティ要件が適用可能ではない場合，その製造者は，当該技術文書の中に，その趣旨の明確な正当事由を含める。

When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in paragraph 3 of this Article in the technical documentation required pursuant to Article 31 and Annex VII. For products with digital elements as referred to in Article 12, which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.

5. 第 1 項を遵守する目的のために，製造者は，商業活動の過程で市場において利用できるようにされていない無料でオープンソースのソフトウェアのコンポーネントを組み込む場合を含め，当該コンポーネントがデジタルの要素をもつ製品のサイバーセキュリティを損ねることのないよう，第三者から由来したコンポーネントを組み込む際にデューディリジェンスを尽くす。

For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.

6. 製造者は，オープンソースのコンポーネントを含め，デジタルの要素をもつ製品の中に組み込まれているコンポーネントの中の脆弱性を発見したときは，そのコンポーネントを製造または維持管理している個人または法主体に対してその脆弱性を報告し，かつ，別紙 I のパート II の中で定められた脆弱性取扱の要件に従ってその脆弱性に対処し及びそれを解消する。当該コンポーネント内の脆弱性に対処するためのソフトウェアまたはハードウェアの修正を製造者が開発したときは，その製造者は，それが適切なときは機械読取り可能なフォーマットにより，そのコンポーネントを製造または維持管理している個人または法主体との間で適格なコードまたは文書を共有する。

Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling

requirements set out in Part II of Annex I. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.

7. 製造者は，性質及びサイバーセキュリティ上のリスクと比例する態様で，その製造者が気づいた脆弱性及び第三者から提供された適格な情報を含め，デジタルの要素をもつ製品と関係するサイバーセキュリティ上の適格な側面を体系的に文書化し，かつ，それが適用可能なときは，その製品のサイバーセキュリティ上のリスク評価をアップデートする。

The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.

8. 製造者は，デジタルの要素をもつ製品を市場に置く際及びサポート期間中，当該製品のコンポーネントを含め，当該製品の脆弱性が，実効的にかつ別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に従って取り扱われることを確保する。

Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I.

製造者は，とりわけ，合理的な利用者の期待，その製品の所期の目的を含め，その製品の性質，及び，デジタルの要素をもつ製品の耐用年数を決定する適格な欧州連合法を考慮に入れた上で，そのサポート期間がその製品が利用に供されると予想される期間の長さを反映するように，そのサポート期間を決定する。サポート期間を決定する際，製造者は，別の製造者によって市場に置かれた類似の機能性を提供しているデジタルの要素をもつ製品のサポート期間，運用環境の可用性，コア機能を提供しかつ第三者から由来する組み込まれたコンポーネントのサポート期間，並びに，第 52 条第 15 項により設けられる行政協力専門グループ（ADCO）及び欧州委員会から提供される適格なガイドも考慮に入れ得る。サポート期間を決定するために考慮に入れられる諸事項は，比例性を確保する態様で検討される。

Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the support

period shall be considered in a manner that ensures proportionality.

第 2 副項を妨げることなく，サポート期間は，少なくとも 5 年間とする。当該デジタルの要素をもつ製品が 5 年未満の期間で利用に供されると予想される場合，そのサポート期間は，予想される利用期間に対応するものとする。

Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.

第 52 条第 16 項に示す ADCO の勧告を考慮に入れた上で，欧州委員会は，市場監視データが不適切なサポート期間を示唆している場合，特定の製品類型のためのミニマムのサポート期間の細目を定めることによってこの規則を補完するため，第 61 条に従って委任される行為を採択し得る。

Taking into account ADCO recommendations as referred to in Article 52(16), the Commission may adopt delegated acts in accordance with Article 61 to supplement this Regulation by specifying the minimum support period for specific product categories where the market surveillance data suggests inadequate support periods.

製造者は，別紙 VII の中で定められた技術文書の中に，デジタルの要素をもつ製品のサポート期間を決定するために考慮に入れられた情報を含める。

Manufacturers shall include the information that was taken into account to determine the support period of a product with digital elements in the technical documentation as set out in Annex VII.

製造者は，別紙 I のパート II の第 5 号に示す調整された脆弱性開示の基本方針を含め，内部または外部の情報源から報告されたデジタルの要素をもつ製品の中にある潜在的な脆弱性を処理及び解消するための適切な基本方針及び手続をもつ。

Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Part II, point (5), of Annex I to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.

9. 製造者は，別紙 I のパート II の第 8 号に示す個々のセキュリティアップデートであって，そのサポート期間中は利用者に対して利用できるようにされたものが，そのセキュリティアップデートが発行された後，ミニマムの 10 年の期間内またはそのサポート期間の残期間のいずれか長い方の期間内はそのまま利用できることを確保する。

Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.

10. 製造者が，後に大きく修正された版のソフトウェア製品を市場に置いたときは，当該事業者は，従前に市場に置かれた版の利用者が，直近に市場に置かれた版に対する無料のアクセスをもち，かつ，当初の版の当該製品を当該利用者が利用するハードウェア及びソフトウェアの環境を補正するための追加的な費用がかからないことを条件として，その製造者が直近に市場に置いた版に限定して，別紙 I のパート II の第 2 号の中で定められた必須のサイバーセキュリティ要件の遵守を確保できる。

Where a manufacturer has placed subsequent substantially modified versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product.

11. 製造者は，過去の版への利用者のアクセスを拡張する公開のソフトウェアアーカイブを維持管理できる。その場合，利用者は，サポートされないソフトウェアの利用と関係するリスクに関し，容易にアクセス可能な態様で，明確に情報提供を受ける。

Manufacturers may maintain public software archives enhancing user access to historical versions. In those cases, users shall be clearly informed in an easily accessible manner about risks associated with using unsupported software.

12. デジタルの要素をもつ製品を市場に置く前に，製造者は，第 31 条に示す技術文書を作成する。

Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 31.

製造者は，第 32 条に示す適合性評価手続を選択して実施し，または，それを実施させる。

They shall carry out the chosen conformity assessment procedures as referred to in Article 32 or have them carried out.

当該デジタルの要素をもつ製品が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を遵守していること及びその製造者によって設けられた手続が別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件を遵守していることが当該適合性評価手続によって示されたときは，製造者は，第 28 条に従って EU 適合宣言書を作成し，かつ，第 30 条に従って CE マークを付す。

Where compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.

13. 製造者は，デジタルの要素をもつ製品が市場に置かれた後少なくとも 10 年間またはサポート期間

のいずれか長い方の期間内は，その技術文書及び EU 適合宣言書を市場監視当局が自由に利用できるように保管する。

Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.

14. 製造者は，あるシリーズの生産の一部であるデジタルの要素をもつ製品に関し，この規則の適合性を維持するための手続が設けられることを確保する。そのデジタルの要素をもつ製品の適合性が宣言されていることの参照によって，または，その製品の適合性が検証されることを申請することによって，製造者は，そのデジタルの要素をもつ製品の開発及び製造の過程における変更または設計もしくは特性の変更，並びに，第 27 条に示す整合化された技術標準，欧州サイバーセキュリティ認証制度または共通仕様の変更を適切に考慮に入れる。

Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity with this Regulation. Manufacturers shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or common specifications as referred to in Article 27 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.

15. 製造者は，その製造者のデジタルの要素をもつ製品が，型式番号，バッチ番号もしくはシリアル番号またはそれ以外のその製品の識別をできるようにする要素が記されることを確保し，または，それが可能ではないときは，その製品のパッケージ上で，もしくは，そのデジタルの要素をもつ製品に添付されている文書の中で当該情報が提供されることを確保する。

Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, that that information is provided on their packaging or in a document accompanying the product with digital elements.

16. 製造者は，デジタルの要素をもつ製品上に，その製品の包装上に，または，そのデジタルの要素をもつ製品に添付される文書中で，その製造者の名称，登録商号または登録商標及び郵便住所，電子メールアドレスまたはそれ以外のデジタルの連絡先，並びに，それが適用可能なときは，その製造者と連絡をとり得る Web サイトを表示する。その情報は，別紙 II の中で定められた利用者に対する情報提供及び指示の中にも含められる。その連絡先は，利用者及び市場監視当局によって容易に理解され得る言語によるものとする。

Manufacturers shall indicate the name, registered trade name or registered trademark of the manufacturer, and the postal address, email address or other digital contact details, as well as, where applicable, the website where the manufacturer can be contacted, on the product with digital elements, on its packaging or in a document accompanying the product

with digital elements. That information shall also be included in the information and instructions to the user set out in Annex II. The contact details shall be in a language which can be easily understood by users and market surveillance authorities.

17. この規則の目的のために，製造者は，デジタルの要素をもつ製品の脆弱性に関する報告を容易にするための場合を含め，利用者が製造者との間で直接かつ迅速に連絡をとることを可能にするための単一連絡先を指定する。

For the purposes of this Regulation, manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, including in order to facilitate reporting on vulnerabilities of the product with digital elements.

製造者は，単一連絡先が利用者によって容易に発見され得ることを確保する。製造者は，別紙 II の中で定められた利用者に対する情報提供及び指示の中にも単一連絡先を含める。

Manufacturers shall ensure that the single point of contact is easily identifiable by the users. They shall also include the single point of contact in the information and instructions to the user set out in Annex II.

単一連絡先は，利用者が利用者の好む通信手段を選択できるようにし，かつ，そのような手段を自動化されたツールに限定してはならない。

The single point of contact shall allow users to choose their preferred means of communication and shall not limit such means to automated tools.

18. 製造者は，デジタルの要素をもつ製品が，紙または電子的な方式で，別紙 II の中で定められた利用者に対する情報提供及び指示が添付されることを確保する。そのような情報提供及び指示は，利用者及び市場監視当局によって容易に理解され得る言語で提供される。その情報提供及び指示は，明確であり，理解可能であり，意味をとりやすく，かつ，判読しやすいものとする。その情報提供及び指示は，デジタルの要素をもつ製品の安全なインストール，運用及び利用ができるようにする。製造者は，デジタルの要素をもつ製品が市場に置かれた後少なくとも 10 年間またはサポート期間のいずれか長い方の期間内は，別紙 II の中で定められた利用者に対する情報提供及び指示を利用者及び市場監視当局が自由に利用できるように保つ。そのような情報提供及び指示がオンラインで提供される場合，製造者は，デジタルの要素をもつ製品が市場に置かれた後少なくとも 10 年間またはサポート期間のいずれか長い方の期間内は，その情報提供及び指示がアクセス可能であり，ユーザフレンドリでありかつオンラインで利用可能であることを確保する。

Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions to the user set out in Annex II, in paper or electronic form. Such information and instructions shall be provided in a language which can be easily understood by users and market surveillance authorities. They shall be clear, understandable, intelligible and legible. They shall allow for the secure installation, operation and use of products with

digital elements. Manufacturers shall keep the information and instructions to the user set out in Annex II at the disposal of users and market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. Where such information and instructions are provided online, manufacturers shall ensure that they are accessible, user-friendly and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.

19. 製造者は，少なくとも月及び年を含め，第 8 項に示すサポート期間の終了日が，その購入の時点において，容易にアクセス可能な態様で，かつ，それが適用可能なときは，そのデジタルの要素をもつ製品上で，その製品のパッケージ上でまたはデジタルの手段により，明確かつ理解可能なように示されることを確保する。

Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means.

デジタルの要素をもつ製品の性質に照らして技術的に利用可能なときは，製造者は，その製造者のデジタルの要素をもつ製品がその製品のサポート期間の最終時点に至ったことを利用者に対して連絡する利用者宛の通知を表示する。

Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period.

20. 製造者は，デジタルの要素をもつ製品の EU 適合宣言書のコピーまたは簡易化された EU 適合宣言書のいずれかを提供する。簡易化された EU 適合宣言書が提供される場合，その簡易化された EU 適合宣言書は，EU 適合宣言書の全文にアクセスできる正確なインターネットアドレスを含める。

Manufacturers shall either provide a copy of the EU declaration of conformity or a simplified EU declaration of conformity with the product with digital elements. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address at which the full EU declaration of conformity can be accessed.

21. 市場に置く時点から及びサポート期間内，デジタルの要素をもつ製品またはその製造者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していないことを知っている製造者またはそのように信ずる合理的な理由をもつ製造者は，直ちに，当該デジタルの要素をもつ製品もしくはその製造者によって設けられたプロセスを適合させるため，または，それが適切なときは，その製品を回収するためもしくはリコールするために必要となる解消の方策をとる。

From the placing on the market and for the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, or to withdraw or recall the product, as

appropriate.

22. 製造者は，市場監視当局からの理由を付した要請があるときは，当該当局に対し，当該当局によって容易に理解され得る言語により，紙または電子的な方式で，そのデジタルの要素をもつ製品及びその製造者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していることを示すために必要となる全ての情報及び文書を提供する。製造者は，当該当局の要請があるときは，その製造者が市場に置いたデジタルの要素をもつ製品によって呈されているサイバーセキュリティ上のリスクを解消するためにとられる方策に関し，当該当局と協力する。

Manufacturers shall, upon a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by that authority, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Annex I. Manufacturers shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements which they have placed on the market.

23. その製造者の業務運営を停止させ，その結果として，この規則を遵守できない製造者は，その業務運営の停止が発効する前に，適格な市場監視当局に対し，また，利用可能な手段により及び可能な範囲内で，市場に置かれた適格なデジタルの要素をもつ製品の利用者に対し，切迫している業務運営の停止を連絡する。

A manufacturer that ceases its operations and, as a result, is not able to comply with this Regulation shall inform, before the cessation of operations takes effect, the relevant market surveillance authorities as well as, by any means available and to the extent possible, the users of the relevant products with digital elements placed on the market, of the impending cessation of operations.

24. 欧州委員会は，欧州の技術標準または国際的な技術標準及びベストプラクティスを考慮に入れた上で，実装行為により，別紙 I のパート II の第 1 号に示すソフトウェア素材表の書式及び要素の細目を定め得る。同実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

The Commission may, by means of implementing acts taking into account European or international standards and best practices, specify the format and elements of the software bill of materials referred to in Part II, point (1), of Annex I. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

25. ソフトウェアのコンポーネントに対する，及び，とりわけ，無料でオープンソースのソフトウェアとしての適格のあるコンポーネントに対する構成国及び欧州連合の全体的な依存性を評価するため，ADCO は，特定の類型のデジタルの要素をもつ製品に関する欧州連合全域の依存性評価を行うことを決定できる。当該の目的のために，市場監視当局は，そのような類型のデジタルの要素をもつ製品の製造者に対し，別紙 I のパート II 第 1 号に示す関連ソフトウェア素材表を提供することを要請できる。そのような情報を基礎として，市場監視当局は，ADCO に対し，ソフトウェアの依存性に関す

る匿名化され集約された情報を提供できる。ADCO は，指令(EU)2022/2555 の第 14 条により設けられた協力グループに対し，依存性評価の結果に関する報告書を提出する。

In order to assess the dependence of Member States and of the Union as a whole on software components and in particular on components qualifying as free and open-source software, ADCO may decide to conduct a Union wide dependency assessment for specific categories of products with digital elements. For that purpose, market surveillance authorities may request manufacturers of such categories of products with digital elements to provide the relevant software bills of materials as referred to in Part II, point (1), of Annex I. On the basis of such information, the market surveillance authorities may provide ADCO with anonymised and aggregated information about software dependencies. ADCO shall submit a report on the results of the dependency assessment to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555.

第 14 条　製造者の報告義務

Article 14 **Reporting obligations of manufacturers**

1. 製造者は，本条の第 7 項に従って調整者として指定された CSIRT に対し及び ENISA に対し，同時に，その製造者が気づいたデジタルの要素をもつ製品に含まれている能動的に悪用された脆弱性を通知する。その製造者は，第 16 条により設置される単一報告プラットフォームを介して，当該能動的に悪用された脆弱性を通知する。

A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.

2. 第 1 項に示す通知の目的のために，製造者は，以下のものを提出する：

For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit:

(a) 不適切な遅滞なく，かつ，いかなる場合においてもその製造者がそれに気づいてから 24 時間以内に，それが適用可能なときは，その領土上においてその製造者のデジタルの要素をもつ製品が利用できるようにされたことをその製造者が気づいている構成国を示して，能動的に悪用された脆弱性の早期警戒通知；

an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) 適格な情報が既に提供されていない限り，不適切な遅滞なく，かつ，いかなる場合においても

その製造者がその能動的に悪用された脆弱性に気づいてから 72 時間以内に，それが利用可能なときは，関係するデジタルの要素をもつ製品，その悪用の一般的な性質及び関係する脆弱性の一般的な性質，並びに，とられた解消の方策または緩和の方策，及び，利用者がとることのできる解消の方策または緩和の方策に関する一般的な情報を提供し，また，それが適用可能なときは，通知される情報がどの程度まで機微であるとその製造者が判断しているかも示して，脆弱性の通知；

unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) 適格な情報が既に提供されていない限り，解消の方策または緩和の方策が利用可能となってから遅くとも 14 日以内に，少なくとも以下の事項を含む最終報告書：

unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following:

(i) その脆弱性の深刻度及び影響を含め，その脆弱性の記述；

a description of the vulnerability, including its severity and impact;

(ii) それが利用可能なときは，その脆弱性を悪用したまたは悪用している悪意ある行為者に関する情報；

where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability;

(iii) その脆弱性を解消するために利用できるようにされているセキュリティアップデートまたはそれ以外の解消の方策の詳細。

details about the security update or other corrective measures that have been made available to remedy the vulnerability.

3. 製造者は，本条の第 7 項に従って調整者として指定された CSIRT に対し及び ENISA に対し，同時に，その製造者が気づいたデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントを通知する。その製造者は，第 16 条により設置される単一報告プラットフォームを介して，当該インシデントを通知する。

A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.

4. 第 3 項に示す通知の目的のために，製造者は，以下のものを提出する：

For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit:

(a) 不適切な遅滞なく，かつ，いかなる場合においてもその製造者がそれに気づいてから 24 時間以内に，それが適用可能なときは，その領土上においてその製造者のデジタルの要素をもつ製品が利用できるようにされたことをその製造者が気づいている構成国を示して，少なくとも，そのインシデントが違法な行為または悪意ある行為に起因している疑いがあるかどうかを含め，デジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントの早期警戒通知；

an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available;

(b) 適格な情報が既に提供されていない限り，不適切な遅滞なく，かつ，いかなる場合においてもその製造者がそのインシデントに気づいてから 72 時間以内に，それが利用可能なときは，そのインシデントの性質，そのインシデントの初期評価，並びに，とられた解消の方策または緩和の方策，及び，利用者がとることのできる解消の方策または緩和の方策に関する一般的な情報を提供し，また，それが適用可能なときは，通知される情報がどの程度まで機微であるとその製造者が判断しているかも示して，インシデントの通知；

unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be;

(c) 適格な情報が既に提供されていない限り，(b)の下にあるインシデント通知の提出後 1 か月以内に，少なくとも以下の事項を含む最終報告書：

unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following:

(i) そのインシデントの深刻度及び影響を含め，そのインシデントの詳細な記述；

a detailed description of the incident, including its severity and impact;

(ii) そのインシデントの引き金となった蓋然性のある脅威のタイプまたは根本原因；

the type of threat or root cause that is likely to have triggered the incident;

(iii) 適用された緩和の方策及び進行中の緩和の方策。

applied and ongoing mitigation measures.

5. 第 3 項の目的のために，以下の場合においては，デジタルの要素をもつ製品の防護に対する影響をもつインシデントは，重大であると判断される：

For the purposes of paragraph 3, an incident having an impact on the security of the product with digital elements shall be considered to be severe where:

(a) そのインシデントが，デジタルの要素をもつ製品の，機微のデータもしくは重要なデータまたは機能の可用性，真正性，完全性または機密性を保護するための能力に対して負の影響を与えている場合または負の影響を与えることが可能な場合；または

it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or

(b) そのインシデントが，デジタルの要素をもつ製品の中においてまたはそのデジタルの要素をもつ製品の利用者のネットワーク及び情報システムの中における悪意あるコードの導入または実行を導いた場合またはそれを導くことが可能な場合。

it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

6. それが必要なときは，通知を最初に受領する調整者として指定された CSIRT は，製造者に対し，能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントに関する適格な状態のアップデートに関し，中間報告書を提供することを要求できる。

Where necessary, the CSIRT designated as coordinator initially receiving the notification may request manufacturers to provide an intermediate report on relevant status updates about the actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements.

7. 本条の第 1 項及び第 3 項に示す通知は，第 16 条に示す単一報告プラットフォームを介して，第 16 条第 1 項に示す電子通知終点のいずれかを用いて提出される。その通知は，製造者がその製造者の欧州連合内の主たる拠点をもつ構成国の調整者として指定された CSIRT の電子通知終点を用いて提出され，かつ，ENISA が同時にアクセス可能であるものとする。

The notifications referred to in paragraphs 1 and 3 of this Article shall be submitted via the single reporting platform referred to in Article 16 using one of the electronic notification end-points referred to in Article 16(1). The notification shall be submitted using the electronic notification end-point of the CSIRT designated as coordinator of the Member State where the manufacturers have their main establishment in the Union and shall be simultaneously accessible to ENISA.

この規則の目的のために，製造者は，その製造者のデジタルの要素をもつ製品のサイバーセキュリティと関連する決定が主として行われる構成国において，その製造者の欧州連合内の主たる拠点をもつと判断される。そのような構成国が決定され得ない場合，その主たる拠点は，関係する製造者が，欧州連合内における最多従業者数の拠点をもつ構成国にあると判断される。

For the purposes of this Regulation, a manufacturer shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the manufacturer concerned has the establishment with the highest number of employees in the Union.

製造者が欧州連合内に主たる拠点をもたない場合，その製造者は，以下の順序により，かつ，その製造者にとって利用可能な情報を基礎として決定される構成国において調整者として指定された CSIRT の電子通知終点を用いて，第 1 項及び第 3 項に示す通知を提出する：

Where a manufacturer has no main establishment in the Union, it shall submit the notifications referred to in paragraphs 1 and 3 using the electronic notification end-point of the CSIRT designated as coordinator in the Member State determined pursuant to the following order and based on the information available to the manufacturer:

(a) 当該製造者の最多のデジタルの要素をもつ製品に関してその製造者の代わりに行動する権限のある代理者が拠点をもつ構成国；

the Member State in which the authorised representative acting on behalf of the manufacturer for the highest number of products with digital elements of that manufacturer is established;

(b) 当該製造者の最多のデジタルの要素をもつ製品を市場に置いている輸入業者が拠点をもつ構成国；

the Member State in which the importer placing on the market the highest number of products with digital

elements of that manufacturer is established;

(c) 当該製造者の最多のデジタルの要素をもつ製品を利用できるようにしている流通業者が拠点をもつ構成国；

the Member State in which the distributor making available on the market the highest number of products with digital elements of that manufacturer is established;

(d) 当該製造者のデジタルの要素をもつ製品の最多の利用者が所在している構成国。

the Member State in which the highest number of users of products with digital elements of that manufacturer are located.

第 3 副項(d)との関係において，製造者は，その製造者が最初に報告したのと同一の調整者として指定された CSIRT に対し，その後の能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントと関連する通知を提出できる。

In relation to the third subparagraph, point (d), a manufacturer may submit notifications related to any subsequent actively exploited vulnerability or severe incident having an impact on the security of the product with digital elements to the same CSIRT designated as coordinator to which it first reported.

8. 能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントに気づいた後，その製造者は，そのデジタルの要素をもつ製品の影響を受けた利用者に対し，及び，それが適切なときは，全ての利用者に対し，それが適切なときは，構造化され，容易に自動的に処理可能な機械読取り可能なフォーマットにより，当該脆弱性またはインシデントを連絡し，また，それが必要なときは，当該脆弱性またはインシデントの影響を緩和するために利用者が配置できるリスクの緩和の方策及び解消の方策を連絡する。製造者がそのデジタルの要素をもつ製品の利用者に対して適時の態様で連絡しない場合，通知を受領した調整者として指定された CSIRT は，当該脆弱性またはインシデントの影響を防止または緩和するために比例的かつ必要であると判断するときは，利用者に対し，そのような情報を提供できる。

After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.

9. 2025 年 12 月 11 日までに，欧州委員会は，この規則の第 16 条第 2 項に示す通知の伝達の遅延と関係するサイバーセキュリティと関連する根拠の適用のための条件の細目を定めることによってこの規則を補完するため，この規則の第 61 条に従って委任される行為を採択する。欧州委員会は，その委任される行為案を準備する際，指令(EU) 2022/2555 の第 15 条により設けられる CSIRT ネットワーク及び ENISA と協力する。

By 11 December 2025, the Commission shall adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the terms and conditions for applying the cybersecurity-related grounds in relation to delaying the dissemination of notifications as referred to in Article 16(2) of this Regulation. The Commission shall cooperate with the CSIRTs network established pursuant to Article 15 of Directive (EU) 2022/2555 and ENISA in preparing the draft delegated acts.

10. 欧州委員会は，実装行為により，本条並びに第 15 条及び第 16 条に示す通知の書式及び手続の細目を別に定め得る。同実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。欧州委員会は，同実装行為案を準備する際，CSIRT ネットワーク及び ENISA と協力する。

The Commission may, by means of implementing acts, specify further the format and procedures of the notifications referred to in this Article as well as in Articles 15 and 16. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2). The Commission shall cooperate with the CSIRTs network and ENISA in preparing those draft implementing acts.

第 15 条 任意の報告

Article 15 **Voluntary reporting**

1. 製造者及びそれ以外の自然人または法人は，任意で，調整者として指定された CSIRT または ENISA に対し，デジタルの要素をもつ製品の中に含まれている脆弱性及びデジタルの要素をもつ製品のリスクプロファイルに対して影響を与え得るサイバー脅威を通知できる。

Manufacturers as well as other natural or legal persons may notify any vulnerability contained in a product with digital elements as well as cyber threats that could affect the risk profile of a product with digital elements on a voluntary basis to a CSIRT designated as coordinator or ENISA.

2. 製造者及びそれ以外の自然人または法人は，任意で，調整者として指定された CSIRT または ENISA に対し，デジタルの要素をもつ製品の防護に対する影響をもつインシデント及びそのようなインシデントにおいて帰結し得たニアミスを通知できる。

Manufacturers as well as other natural or legal persons may notify any incident having an impact on the security of the product with digital elements as well as near misses that could have resulted in such an incident on a voluntary basis to a CSIRT designated as coordinator or ENISA.

3. 調整者として指定された CSIRT または ENISA は，第 16 条の中で定められた手続に従って，本条の第 1 項及び第 2 項に示す通知を処理する。

The CSIRT designated as coordinator or ENISA shall process the notifications referred to in paragraphs 1 and 2 of this Article in accordance with the procedure laid down in Article 16.

調整者として指定された CSIRT は，任意の通知よりも強制的な通知の処理を優先できる。

The CSIRT designated as coordinator may prioritise the processing of mandatory notifications over voluntary notifications.

4. 製造者以外の自然人または法人が第 1 項または第 2 項に従って能動的に悪用された脆弱性またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントを通知する場合，調整者として指定された CSIRT は，不適切な遅滞なく，その製造者に対して連絡する。

Where a natural or legal person other than the manufacturer notifies an actively exploited vulnerability or a severe incident having an impact on the security of a product with digital elements in accordance with paragraph 1 or 2, the CSIRT designated as coordinator shall without undue delay inform the manufacturer.

5. 調整者として指定された CSIRT 及び ENISA は，通知元である自然人または法人から提供された情報の機密性及び適切な保護を確保する。犯罪行為の防止，捜査，検知及び訴追を妨げることなく，任意の報告は，その者がその通知を提出しなかったとすればその者が服することがなかったような付加的な義務を通知元である自然人または法人に対して課する結果となってはならない。

The CSIRTs designated as coordinators as well as ENISA shall ensure the confidentiality and appropriate protection of the information provided by a notifying natural or legal person. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon a notifying natural or legal person to which it would not have been subject had it not submitted the notification.

第 16 条 単一報告プラットフォームの設置

Article 16 **Establishment of a single reporting platform**

1. 第 14 条の第 1 項及び第 3 項並びに第 15 条の第 1 項及び第 2 項に示す通知の目的のために，かつ，製造者の報告義務を簡素化するため，ENISA によって単一報告プラットフォームが設置される。その単一報告プラットフォームの日々の運用は，ENISA によって運営管理及び維持管理される。単一報告プラットフォームのアーキテクチャは，構成国及び ENISA が，それら自身の電子通知終点を設けることができるようにする。

For the purposes of the notifications referred to in Article 14(1) and (3) and Article 15(1) and (2) and in order to simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall allow Member States and ENISA to put in place their own electronic notification end-points.

2. 通知を受けた後，通知を最初に受領する調整者として指定された CSIRT は，その領土上においてそのデジタルの要素をもつ製品が利用できるようにされていることをその製造者が示した構成国の調整者として指定された CSIRT に対し，遅滞なく，単一報告プラットフォームを介して，その通知を伝達する。

After receiving a notification, the CSIRT designated as coordinator initially receiving the notification shall, without delay, disseminate the notification via the single reporting platform to the CSIRTs designated as coordinators on the territory of which the manufacturer has indicated that the product with digital elements has been made available.

脆弱性が指令(EU) 2022/2555 の第 12 条第 1 項に示す調整された脆弱性開示手続に服する場合を含め，例外的な状況において，かつ，とりわけ，製造者からの要請に応じて，かつ，この規則の第 14 条の第 2 項(a)の下において製造者から示されたようなその通知された情報の機微性のレベルに照らし，通知の伝達は，それが厳格に必要な期間だけ，正当な理由のあるサイバーセキュリティと関連する根拠を基礎として遅延され得る。CSIRT が伝達を保留することを決定する場合，その CSIRT は，直ちに，ENISA に対し，その決定に関して連絡し，かつ，その通知を保留することの正当化事由及び本項の中で定められた伝達手続に従ってその CSIRT がその通知を伝達するのがいつになるかの表示の両者を提供する。ENISA は，その通知の伝達を遅延させることとの関係において，サイバーセキュリティと関連する根拠の適用に関し，その CSIRT を支援できる。

In exceptional circumstances and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the notified information as indicated by the manufacturer under Article 14(2), point (a), of this Regulation, the dissemination of the notification may be delayed based on justified cybersecurity-related grounds for a period of time that is strictly necessary, including where a vulnerability is subject to a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555. Where a CSIRT decides to withhold a notification, it shall immediately inform ENISA about the decision and provide both a justification for withholding the notification as well as an indication of when it will disseminate the notification in accordance with the dissemination procedure laid down in this paragraph. ENISA may support the CSIRT on the application of cybersecurity-related grounds in relation to delaying the dissemination of the notification.

特別に例外的な状況において，第 14 条第 2 項(b)に示す通知の中で，製造者が：

In particularly exceptional circumstances, where the manufacturer indicates in the notification referred to in Article 14(2), point (b):

(a) 通知された脆弱性が悪意ある行為者によって能動的に悪用されたこと，及び，利用可能な情

報によれば，その製造者がその脆弱性を通知した調整者として指定された CSIRT の構成国以外のいずれの構成国内においても悪用されなかったこと；

that the notified vulnerability has been actively exploited by a malicious actor and, according to the information available, it has been exploited in no other Member State than the one of the CSIRT designated as coordinator to which the manufacturer has notified the vulnerability;

(b) 通知された脆弱性を即時に更に伝達すると，その情報の開示がその構成国の必須の利益に反するような情報の提供を帰結することとなりかねないこと；または

that any immediate further dissemination of the notified vulnerability would likely result in the supply of information the disclosure of which would be contrary to the essential interests of that Member State; or

(c) 通知された脆弱性が，更に伝達することから派生するサイバーセキュリティ上の差し迫った高度のリスクを呈していること；

that the notified vulnerability poses an imminent high cybersecurity risk stemming from the further dissemination;

を示しているときは，関係する CSIRT 及び ENISA に対して通知の全文が伝達されるまでの間，その製造者から通知が行われたという情報，その製品に関する一般的な情報，その悪用の一般的な性質に関する情報，並びに，セキュリティと関連する根拠が提起されているという情報のみが，ENISA に対して同時に利用できるようにされなければならない。当該情報を基礎として，域内市場の防護に影響を与えるシステミックなリスクが存在すると ENISA が判断するときは，ENISA は，受領者である CSIRT に対し，他の調整者として指定された CSIRT 及び ENISA 自身に対してその通知の全文を伝達することを勧告する。

only the information that a notification was made by the manufacturer, the general information about the product, the information on the general nature of the exploit and the information that security related grounds were raised are to be made available simultaneously to ENISA until the full notification is disseminated to the CSIRTs concerned and ENISA. Where, based on that information, ENISA considers that there is a systemic risk affecting security in the internal market, it shall recommend to the recipient CSIRT that it disseminate the full notification to the other CSIRTs designated as coordinators and to ENISA itself.

3. デジタルの要素をもつ製品の中にある能動的に悪用された脆弱性の通知またはデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントの通知を受領した後，その調整者として指定された CSIRT は，その CSIRT それぞれの構成国の市場監視当局に対し，この規則の下にあるその市場監視当局の義務を満たすためにその市場監視当局にとって必要な通知された情報を提供する。

After receiving a notification of an actively exploited vulnerability in a product with digital elements or of a severe incident having an impact on the security of a product with digital elements, the CSIRTs designated as coordinators shall provide the market surveillance authorities of their respective Member States with the notified information necessary for the market surveillance authorities to fulfil their obligations under this Regulation.

4. ENISA は，単一報告プラットフォームの防護に対して呈されたリスク及び単一報告プラットフォームを介して提出または伝達された情報を管理するための適切かつ比例的な技術上，運営管理上及び組織上の措置を講ずる。ENISA は，不適切な遅滞なく，CSIRT ネットワーク及び欧州委員会に対し，単一報告プラットフォームに対して影響を与えるセキュリティ上のインシデントを通知する。

ENISA shall take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of the single reporting platform and the information submitted or disseminated via the single reporting platform. It shall notify without undue delay any security incident affecting the single reporting platform to the CSIRTs network as well as to the Commission.

5. ENISA は，CSIRT ネットワークと協力して，少なくとも，単一報告プラットフォームの設置，運営管理及び維持管理と関連するセキュリティ上の手立てを含め，第 1 項に示す単一報告プラットフォームの設置，維持管理及び安全な運用と関連する技術上，運用上及び組織上の措置に関する仕様を提供しかつ実装し，また，通知された脆弱性が利用可能な解消の方策または緩和の方策をもたないときは厳格なセキュリティ手順に沿ってかつ知る必要性ベースで当該脆弱性に関する情報が共有されることを確保するための手続上の側面を含め，国内レベルでは調整者として指定された CSIRT によって及び欧州連合レベルでは ENISA によって設置される電子通知終点の仕様を提供しかつ実装する。

ENISA, in cooperation with the CSIRTs network, shall provide and implement specifications on the technical, operational and organisational measures regarding the establishment, maintenance and secure operation of the single reporting platform referred to in paragraph 1, including at least the security arrangements related to the establishment, operation and maintenance of the single reporting platform, as well as the electronic notification end-points set up by the CSIRTs designated as coordinators at national level and ENISA at Union level, including procedural aspects to ensure that, where a notified vulnerability has no corrective or mitigating measures available, information about that vulnerability is shared in line with strict security protocols and on a need-to-know basis.

6. 調整者として指定された CSIRT が，指令(EU) 2022/2555 の第 12 条第 1 項に示す調整された脆弱性開示手続の一部として能動的に悪用された脆弱性に気づいたときは，通知を最初に受領する調整者として指定された CSIRT は，それが厳格に必要な期間だけ，かつ，調整された脆弱性開示に関与した関係者から開示の同意が与えられるまで，正当な理由のあるサイバーセキュリティと関連する根拠を基礎として，単一報告プラットフォームを介する適格な通知の伝達を遅延させ得る。この要件は，製造者が，任意で，本条の中で定められた手続に従ってそのような脆弱性を通知することを妨げてはならない。

Where a CSIRT designated as coordinator has been made aware of an actively exploited vulnerability as part of a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555, the CSIRT designated as coordinator initially receiving the notification may delay the dissemination of the relevant notification via the single reporting platform based on justified cybersecurity-related grounds for a period that is no longer than is strictly necessary and until consent for disclosure by the involved coordinated vulnerability disclosure parties is given. That requirement shall not prevent manufacturers from notifying such a vulnerability on a voluntary basis in accordance with the procedure laid down in this Article.

第 17 条　報告と関係するその他の条項

Article 17 **Other provisions related to reporting**

1. ENISA は，そのような情報が大規模なサイバーセキュリティ上のインシデント及び運営レベルの危機の調整された管理運営にとって適格であるときは，指令(EU) 2022/2555 の第 16 条の下において設置された欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）に対し，この規則の第 14 条の第 1 項及び第 3 項並びに第 15 条の第 1 項及び第 2 項により通知された情報を提出できる。そのような適格性を決定する目的のために，ENISA は，それが利用可能なときは，CSIRT ネットワークによって遂行される技術分析を検討できる。

ENISA may submit to the European cyber crisis liaison organisation network (EU-CyCLONe) established under Article 16 of Directive (EU) 2022/2555 information notified pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation if such information is relevant for the coordinated management of large-scale cybersecurity incidents and crises at an operational level. For the purpose of determining such relevance, ENISA may consider technical analyses performed by the CSIRTs network, where available.

2. デジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントを防止もしくは緩和するため，または，現在進行中のインシデントを取扱うために公衆の認識が必要な場合，または，そのインシデントの開示が何らかの意味で公共の利益となる場合においては，適格な構成国の調整者として指定された CSIRT は，関係する製造者の意見聴取を経た上で，かつ，それが適切なときは ENISA と協力して，公衆に対してそのインシデントに関して連絡でき，または，その製造者に対してそのようにすることを要求できる。

Where public awareness is necessary to prevent or mitigate a severe incident having an impact on the security of the product with digital elements or to handle an ongoing incident, or where disclosure of the incident is otherwise in the public interest, the CSIRT designated as coordinator of the relevant Member State may, after consulting the manufacturer concerned and, where appropriate, in cooperation with ENISA, inform the public about the incident or require the manufacturer to do so.

3. ENISA は，24 か月毎に，この規則の第 14 条の第 1 項及び第 3 項並びに第 15 条の第 1 項及び第 2 項により受領した通知を基礎として，デジタルの要素をもつ製品の中にあるサイバーセキュリティ上

のリスクと関連する最新動向に関する技術報告書を準備し，かつ，指令(EU) 2022/2555 の第 14 条により設けられた協力グループに対し，その報告書を提出する。そのような最初の報告書は，この規則の第 14 条の第 1 項及び第 3 項の中で定められた義務の適用の日から 24 か月以内に提出される。ENISA は，指令(EU) 2022/2555 の第 18 条による欧州連合内のサイバーセキュリティの状態に関する ENISA の報告書の中に，ENISA の技術報告書からの適格な情報を含める。

ENISA, on the basis of the notifications received pursuant to Article 14(1) and (3) and Article 15(1) and (2) of this Regulation, shall prepare, every 24 months, a technical report on emerging trends regarding cybersecurity risks in products with digital elements and submit it to the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555. The first such report shall be submitted within 24 months of the date of application of the obligations laid down in Article 14(1) and (3) of this Regulation. ENISA shall include relevant information from its technical reports in its report on the state of cybersecurity in the Union pursuant to Article 18 of Directive (EU) 2022/2555.

4. 第 14 条の第 1 項及び第 3 項または第 15 条の第 1 項及び第 2 項に従った通知行為があったということだけでは，通知元である自然人または法人を，加重された法的責任に服させてはならない。

The mere act of notification in accordance with Article 14(1) and (3) or Article 15(1) and (2) shall not subject the notifying natural or legal person to increased liability.

5. セキュリティアップデートまたはそれ以外の形態の解消の方策もしくは緩和の方策が利用可能となった後，ENISA は，関係するデジタルの要素をもつ製品の製造者の同意を得た上で，指令(EU) 2022/2555 の第 12 条第 2 項によって設置される欧州脆弱性データベースの中に，この規則の第 14 条第 1 項または第 15 条第 1 項により通知された公知の脆弱性を加える。

After a security update or another form of corrective or mitigating measure is available, ENISA shall, in agreement with the manufacturer of the product with digital elements concerned, add the publicly known vulnerability notified pursuant to Article 14(1) or Article 15(1) of this Regulation to the European vulnerability database established pursuant to Article 12(2) of Directive (EU) 2022/2555.

6. 調整者として指定された CSIRT は，製造者に対し，及び，とりわけ，マイクロ企業または小企業もしく中規模企業としての適格性のある製造者に対し，第 14 条による報告義務との関係における相談窓口の支援を提供する。

The CSIRTs designated as coordinators shall provide helpdesk support in relation to the reporting obligations pursuant to Article 14 to manufacturers and in particular manufacturers that qualify as microenterprises or as small or medium-sized enterprises.

第 18 条　権限のある代理者

Article 18 **Authorised representatives**

1. 製造者は，書面による委任により，権限のある代理者を指定できる。

A manufacturer may, by a written mandate, appoint an authorised representative.

2. 第 13 条第 1 項ないし第 11 項，第 13 条第 12 項第 1 副項及び第 13 条第 14 項の中で定められた義務は，権限のある代理者の任務の一部を組成してはならない。

The obligations laid down in Article 13(1) to (11), Article 13(12), first subparagraph, and Article 13(14) shall not form part of the authorised representative's mandate.

3. 権限のある代理者は，製造者から受領した委任状の中で定められた職務を遂行する。権限のある代理者は，要請に応じて，市場監視当局に対し，委任状のコピーを提供する。委任状は，権限のある代理者が少なくとも以下のことをできるようにする：

An authorised representative shall perform the tasks specified in the mandate received from the manufacturer. The authorised representative shall provide a copy of the mandate to the market surveillance authorities upon request. The mandate shall allow the authorised representative to do at least the following:

(a) デジタルの要素をもつ製品が市場に置かれた後少なくとも 10 年間またはサポート期間のいずれか長い方の期間内は，第 28 条に示す EU 適合宣言書及び第 31 条に示す技術文書を，市場監視当局が自由に利用できるように保つこと；

keep the EU declaration of conformity referred to in Article 28 and the technical documentation referred to in Article 31 at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer;

(b) 市場監視当局からの理由を付した要請に応じて，当該当局に対し，デジタルの要素をもつ製品の適合性を示すために必要となる全ての情報及び文書を提供すること；

further to a reasoned request from a market surveillance authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the product with digital elements;

(c) 市場監視当局の要請があるときは，権限のある代理者の委任に包摂されているデジタルの要素をもつ製品によって呈されているリスクを解消するためにとられる行動に関し，当該当局と協力すること。

cooperate with the market surveillance authorities, at their request, on any action taken to eliminate the risks posed

by a product with digital elements covered by the authorised representative's mandate.

第 19 条 輸入業者の義務

Article 19 **Obligations of importers**

1. 輸入業者は，別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を遵守するデジタルの要素をもつ製品のみを，かつ，製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件を遵守している場合に限り，市場に置く。

Importers shall place on the market only products with digital elements that comply with the essential cybersecurity requirements set out in Part I of Annex I and where the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Part II of Annex I.

2. デジタルの要素をもつ製品を市場に置く前に，輸入業者は，以下のことを確保する:

Before placing a product with digital elements on the market, importers shall ensure that:

(a) 第 32 条に示す適切な適合性評価手続が製造者によって実施されたこと;

the appropriate conformity assessment procedures as referred to in Article 32 have been carried out by the manufacturer;

(b) 製造者が技術文書を作成したこと;

the manufacturer has drawn up the technical documentation;

(c) そのデジタルの要素をもつ製品が，第 30 条に示す CE マークを付していること，第 13 条第 20 項に示す EU 適合宣言書並びに利用者及び市場監視当局によって容易に理解され得る言語による別紙 II に定める利用者に対する情報提供及び指示を添付していること;

the product with digital elements bears the CE marking referred to in Article 30 and is accompanied by the EU declaration of conformity referred to in Article 13(20) and the information and instructions to the user as set out in Annex II in a language which can be easily understood by users and market surveillance authorities;

(d) 製造者が，第 13 条第 15 項，第 16 項及び第 19 項に定める要件を充足したこと。

the manufacturer has complied with the requirements set out in Article 13(15), (16) and (19).

本項の目的のために，輸入業者は，本条の中で定められた要件の充足を証明する必要文書を提供できる。

For the purposes of this paragraph, importers shall be able to provide the necessary documents proving the fulfilment of the requirements set out in this Article.

3. 輸入業者が，デジタルの要素をもつ製品または製造者によって設けられたプロセスがこの規則に適合していないと判断するとき，または，そのように信ずる理由をもつときは，その輸入業者は，当該製品または製造者によって設けられたプロセスがこの規則に適合させられるようになるまでは，その製品を市場に置いてはならない。更に，そのデジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを示しているときは，その輸入業者は，その製造者及び市場監視当局に対し，その旨を連絡する。

Where an importer considers or has reason to believe that a product with digital elements or the processes put in place by the manufacturer are not in conformity with this Regulation, the importer shall not place the product on the market until that product or the processes put in place by the manufacturer have been brought into conformity with this Regulation. Furthermore, where the product with digital elements presents a significant cybersecurity risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

輸入業者が，非技術的なリスク要素に照らし，デジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを示しているかもしれないと信ずる理由をもつときは，その輸入業者は，市場監視当局に対し，その旨を連絡する。そのような情報を受領した後，その市場監視当局は，第 54 条第 2 項に示す手続に従う。

Where an importer has reason to believe that a product with digital elements may present a significant cybersecurity risk in light of non-technical risk factors, the importer shall inform the market surveillance authorities to that effect. Upon receipt of such information, the market surveillance authorities shall follow the procedures referred to in Article 54(2).

4. 輸入業者は，そのデジタルの要素をもつ製品上に，その製品の包装上に，または，そのデジタルの要素をもつ製品に添付される文書中で，その輸入業者の名称，登録商号または登録商標，郵便住所，電子メールアドレスまたはそれ以外のデジタルの連絡先，及び，それが適用可能なときは，その輸入業者と連絡をとり得る Web サイトを表示する。その連絡先は，利用者及び市場監視当局によって容易に理解され得る言語によるものとする。

Importers shall indicate their name, registered trade name or registered trademark, the postal address, email address or other digital contact as well as, where applicable, the website at which they can be contacted on the product with digital elements or on its packaging or in a document accompanying the product with digital elements. The contact details shall be in a language easily understood by users and market surveillance authorities.

5. 当該輸入業者が市場に置いたデジタルの要素をもつ製品がこの規則に適合していないことを知っている輸入業者またはそのように信ずる理由をもつ輸入業者は，直ちに，そのデジタルの要素をもつ製品をこの規則に適合させられることを確保するため，または，それが適切なときは，その製品を回収するためもしくはリコールするために必要となる解消の方策をとる。

Importers who know or have reason to believe that a product with digital elements which they have placed on the market is not in conformity with this Regulation shall immediately take the corrective measures necessary to ensure that the product with digital elements is brought into conformity with this Regulation, or to withdraw or recall the product, if appropriate.

デジタルの要素をもつ製品の中にある脆弱性に気づいた後，輸入業者は，不適切な遅滞なく，その製造者に対し，当該脆弱性に関して連絡する。更に，そのデジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを示しているときは，輸入業者は，直ちに，そのデジタルの要素をもつ製品をその輸入業者が市場において利用できるようにした構成国の市場監視当局に対し，とりわけ，不適合であることの詳細及びとられた解消の方策の詳細を提供して，その旨を連絡する。

Upon becoming aware of a vulnerability in the product with digital elements, importers shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, importers shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of non-compliance and of any corrective measures taken.

6. 輸入業者は，デジタルの要素をもつ製品が市場に置かれた後少なくとも 10 年間またはサポート期間のいずれか長い方の期間内は，EU 適合宣言書のコピーを市場監視当局が自由に利用できることを保ち，かつ，要請に応じて，その技術文書を市場監視当局が利用できるようにされることを確保する。

Importers shall, for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities, upon request.

7. 輸入業者は，市場監視当局からの理由を付した要請に応じて，当該当局に対し，当該当局によって容易に理解され得る言語により，紙または電子的な方式で，そのデジタルの要素をもつ製品が，別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件に適合していること及び製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合していることを示すために必要となる全ての情報及び文書を提供する。その輸入業者は，当該当局の要請があるときは，その輸入業者が市場に置いたデジタルの要素をもつ製品によって呈されているサイバーセキュリティ上のリスクを解消するためにとられる方策に関し，当該当局と協力する。

Importers shall, further to a reasoned request from a market surveillance authority, provide it with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I as well as of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to

eliminate the cybersecurity risks posed by a product with digital elements, which they have placed on the market.

8. デジタルの要素をもつ製品の輸入業者が，当該製品の製造者がその製造者の業務運営を停止させたこと，及び，その結果として，この規則の中で定められた義務を遵守できないことに気づいたときは，その輸入業者は，適格な市場監視当局に対し，その状況に関して連絡し，また，利用可能な手段により及び可能な範囲内で，市場に置かれたデジタルの要素をもつ製品の利用者に対し，連絡する。

Where the importer of a product with digital elements becomes aware that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the importer shall inform the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

第 20 条 流通業者の義務

Article 20 **Obligations of distributors**

1. デジタルの要素をもつ製品を市場において利用できるようにする際，流通業者は，この規則の中で定められた要件との関係において適正に注意を払って行動する。

When making a product with digital elements available on the market, distributors shall act with due care in relation to the requirements set out in this Regulation.

2. デジタルの要素をもつ製品を市場において利用できるようにする前に，流通業者は，以下のことを検査する:

Before making a product with digital elements available on the market, distributors shall verify that:

(a) そのデジタルの要素をもつ製品が CE マークを付していること;

the product with digital elements bears the CE marking;

(b) 製造者及び輸入業者が，第 13 条第 15 項，第 16 項，第 18 項，第 19 項及び第 20 項並びに第 19 条第 4 項の中で定められた義務を充足したこと，並びに，その流通業者に対し，必要な全ての文書が提供されたこと。

the manufacturer and the importer have complied with the obligations set out in Article 13(15), (16), (18), (19) and (20) and Article 19(4), and have provided all necessary documents to the distributor.

3. 流通業者が，その流通業者が保有する情報を基礎として，デジタルの要素をもつ製品または製造

者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していないと判断するとき，または，そのように信ずる理由をもつときは，その流通業者は，当該製品またはその製造者によって設けられたプロセスがこの規則に適合させられるようになるまでは，そのデジタルの要素をもつ製品を市場において利用できるようにしてはならない。更に，そのデジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを呈しているときは，その流通業者は，不適切な遅滞なく，製造者及び市場監視当局に対し，その旨を連絡する。

Where a distributor considers or has reason to believe, on the basis of information in its possession, that a product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I, the distributor shall not make the product with digital elements available on the market until that product or the processes put in place by the manufacturer have been brought into conformity with this Regulation. Furthermore, where the product with digital elements poses a significant cybersecurity risk, the distributor shall inform, without undue delay, the manufacturer and the market surveillance authorities to that effect.

4. 当該流通業者が保有する情報を基礎として，その流通業者が市場において利用できるようにしたデジタルの要素をもつ製品またはその製品の製造者によって設けられたプロセスがこの規則に適合していないことを知っている流通業者またはそのように信ずる理由をもつ流通業者は，当該デジタルの要素をもつ製品もしくはその製品の製造者によって設けられたプロセスを適合させるため，または，それが適切なときは，その製品を回収するためまたはリコールするために必要となる解消の方策がとられることを確実にする。

Distributors who know or have reason to believe, on the basis of information in their possession, that a product with digital elements, which they have made available on the market, or the processes put in place by its manufacturer are not in conformity with this Regulation shall make sure that the corrective measures necessary to bring that product with digital elements or the processes put in place by its manufacturer into conformity, or to withdraw or recall the product, if appropriate, are taken.

デジタルの要素をもつ製品の中にある脆弱性に気づいた後，流通業者は，不適切な遅滞なく，製造者に対し，当該脆弱性に関して連絡する。更に，そのデジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを示しているときは，流通業者は，直ちに，その流通業者がそのデジタルの要素をもつ製品を市場において利用できるようにした構成国の市場監視当局に対し，とりわけ，不適合であることの詳細及びとられた解消の方策の詳細を提供して，その旨を連絡する。

Upon becoming aware of a vulnerability in the product with digital elements, distributors shall inform the manufacturer without undue delay about that vulnerability. Furthermore, where the product with digital elements presents a significant cybersecurity risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they have made the product with digital elements available on the market to that effect, giving details, in particular, of the non-compliance and of any corrective measures taken.

5. 流通業者は，市場監視当局からの理由を付した要請に応じて，当該当局によって容易に理解され

得る言語により，紙または電子的な方式で，そのデジタルの要素をもつ製品及び当該製造者によって設けられたプロセスがこの規則に適合していることを示すために必要となる全ての情報及び文書を提供する。その流通業者は，当該当局の要請があるときは，その流通業者が市場において利用できるようにしたデジタルの要素をもつ製品によって呈されているサイバーセキュリティ上のリスクを解消するためにとられる方策に関し，当該当局と協力する。

Distributors shall, further to a reasoned request from a market surveillance authority, provide all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and the processes put in place by its manufacturer with this Regulation in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by a product with digital elements which they have made available on the market.

6. デジタルの要素をもつ製品の流通業者が，その流通業者が保有する情報を基礎として，当該製品の製造者がその製造者の業務運営を停止させたこと，及び，その結果として，この規則の中で定められた義務を遵守できないことに気づいたときは，その流通業者は，適格な市場監視当局に対し，不適切な遅滞なく，その状況に関して連絡し，また，利用可能な手段により及び可能な範囲内で，市場に置かれたデジタルの要素をもつ製品の利用者に対し，連絡する。

Where the distributor of a product with digital elements becomes aware, on the basis of information in its possession, that the manufacturer of that product has ceased its operations and, as result, is not able to comply with the obligations laid down in this Regulation, the distributor shall inform, without undue delay, the relevant market surveillance authorities about this situation, as well as, by any means available and to the extent possible, the users of the products with digital elements placed on the market.

第 21 条　製造者の義務が輸入業者及び流通業者に対して適用される場合

Article 21 **Cases in which obligations of manufacturers apply to importers and distributors**

当該輸入業者または流通業者が，その名前または商標の下でデジタルの要素をもつ製品を市場に置く場合，または，既に市場に置かれたデジタルの要素をもつ製品の大きな修正を実施する場合，輸入業者または流通業者は，この規則の目的のために製造者であると判断され，かつ，第 13 条及び第 14 条に服する。

An importer or distributor shall be considered to be a manufacturer for the purposes of this Regulation and shall be subject to Articles 13 and 14, where that importer or distributor places a product with digital elements on the market under its name or trademark or carries out a substantial modification of a product with digital elements already placed on the market.

第 22 条　製造者の義務が適用される上記以外の場合

Article 22 **Other cases in which obligations of manufacturers apply**

1. デジタルの要素をもつ製品の大きな修正を実施し，かつ，当該製品を市場において利用できるようにする製造者以外の自然人もしくは法人，輸入業者または製造者は，この規則の目的のために製造者として判断される。

A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of a product with digital elements and makes that product available on the market, shall be considered to be a manufacturer for the purposes of this Regulation.

2. 本条の第 1 項に示す者は，大きな修正によって影響を受けている部分のデジタルの要素をもつ製品に関し，または，その大きな修正がそのデジタルの要素をもつ製品全体のサイバーセキュリティに対して影響をもつときは製品全体に関し，第 13 条及び第 14 条の中で定められた義務に服する。

The person referred to in paragraph 1 of this Article shall be subject to the obligations set out in Articles 13 and 14 for the part of the product with digital elements that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product.

第 23 条　経済取引主体の特定

Article 23 **Identification of economic operators**

1. 経済取引主体は，要求に応じて，市場監視当局に対し，以下の情報を提供する:

Economic operators shall, on request, provide the market surveillance authorities with the following information:

(a) 当該経済取引主体に対してデジタルの要素をもつ製品を供給した経済取引主体の名称及び住所;

the name and address of any economic operator who has supplied them with a product with digital elements;

(b) それが利用可能なときは，当該経済取引主体がデジタルの要素をもつ製品を供給した経済取引主体の名称及び住所。

where available, the name and address of any economic operator to whom they have supplied a product with digital elements.

2. 経済取引主体は，当該経済取引主体がデジタルの要素をもつ製品の供給を受けた後の 10 年間，及び，当該経済取引主体が当該デジタルの要素をもつ製品を供給した後の 10 年間，第 1 項に示

す情報を提示できるものとする。

Economic operators shall be able to present the information referred to in paragraph 1 for 10 years after they have been supplied with the product with digital elements and for 10 years after they have supplied the product with digital elements.

第 24 条 オープンソースソフトウェアスチュワードの義務

Article 24 **Obligations of open-source software stewards**

1. オープンソースソフトウェアスチュワードは，デジタルの要素をもつ安全な製品の開発及び当該製品の開発者による脆弱性の実効的な取扱いを育成するためのサイバーセキュリティ上の基本方針を，検証可能な態様で設けかつ文書化する。その基本方針は，当該製品の開発者による第 15 条に定める脆弱性の任意の報告も育成し，また，オープンソースソフトウェアスチュワードの特性及びそのオープンソースソフトウェアスチュワードが服する法律上の手立て及び組織上の手立てを考慮に入れる。その基本方針は，とりわけ，脆弱性の文書化，対応及び解消と関連する側面を含めるものとし，かつ，オープンソースコミュニティ内における発見された脆弱性に関する情報の共有を促進する。

Open-source software stewards shall put in place and document in a verifiable manner a cybersecurity policy to foster the development of a secure product with digital elements as well as an effective handling of vulnerabilities by the developers of that product. That policy shall also foster the voluntary reporting of vulnerabilities as laid down in Article 15 by the developers of that product and take into account the specific nature of the open-source software steward and the legal and organisational arrangements to which it is subject. That policy shall, in particular, include aspects related to documenting, addressing and remediating vulnerabilities and promote the sharing of information concerning discovered vulnerabilities within the open-source community.

2. オープンソースソフトウェアスチュワードは，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品によって呈されているサイバーセキュリティ上のリスクを解消するという観点から，市場監視当局の要請があるときは，当該当局と協力する。

Open-source software stewards shall cooperate with the market surveillance authorities, at their request, with a view to mitigating the cybersecurity risks posed by a product with digital elements qualifying as free and open-source software.

市場監視当局からの理由を付した要請に応じて，オープンソースソフトウェアスチュワードは，当該当局に対し，当該当局によって容易に理解され得る言語により，紙または電子的な方式で，第 1 項に示す文書を提供する。

Further to a reasoned request from a market surveillance authority, open-source software stewards shall provide that authority, in a language which can be easily understood by that authority, with the documentation referred to in paragraph 1, in paper or electronic form.

3. 第 14 条第 1 項の中で定められた義務は，オープンソースソフトウェアスチュワードがデジタルの要素をもつ製品の開発に関与している範囲内において，そのオープンソースソフトウェアスチュワードに対して適用される。第 14 条第 3 項及び第 8 項の中で定められた義務は，そのような製品の開発のためにオープンソースソフトウェアスチュワードから提供されたネットワーク及び情報システムに対してデジタルの要素をもつ製品の防護に対する影響をもつ重大なインシデントが影響を与える範囲内において，そのオープンソースソフトウェアスチュワードに対して適用される。

The obligations laid down in Article 14(1) shall apply to open-source software stewards to the extent that they are involved in the development of the products with digital elements. The obligations laid down in Article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products.

第 25 条 無料でオープンソースのソフトウェアのセキュリティ証明書

Article 25 **Security attestation of free and open-source software**

とりわけ，当該製造者のデジタルの要素をもつ製品の中に無料でオープンソースのソフトウェアのコンポーネントを組み込む製造者に関し，第 13 条第 5 項の中で定められたデューディリジェンス義務の履行を容易にするため，欧州委員会は，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品の開発者または利用者及びそれらの者以外の第三者が，この規則の中で定められた必須のサイバーセキュリティ要件またはそれ以外の義務の全部または一部へのそのような製品の適合性を評価できるようにする任意のセキュリティ証明書の計画を設けることによってこの規則を補完するため，第 61 条に従って委任される行為を採択する権限を与えられる。

In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components in their products with digital elements, the Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by establishing voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements or other obligations laid down in this Regulation.

第 26 条 ガイド

Article 26 **Guidance**

1. 実装を容易にし，かつ，そのような実装の一貫性を確保するため，欧州委員会は，マイクロ企業並びに小企業及び中規模企業による遵守を容易にすることに特に焦点を当て，この規則の適用において経済取引主体を補助するためのガイドを発行する。

In order to facilitate implementation and ensure the consistency of such implementation, the Commission shall publish guidance to assist economic operators in applying this Regulation, with a particular focus on facilitating compliance by microenterprises and small and medium-sized enterprises.

2. 欧州委員会が第 1 項に示すガイドの提供を意図するときは，欧州委員会は，少なくとも，以下の諸側面に対処する：

Where it intends to provide guidance as referred to in paragraph 1, the Commission shall address at least the following aspects:

(a) リモートのデータ処理ソリューション及び無料でオープンソースのソフトウェアに特に焦点を当て，この規則の適用範囲；

the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;

(b) 特別の類型のデジタルの要素をもつ製品との関係におけるサポート期間の適用；

the application of support periods in relation to particular categories of products with digital elements;

(c) この規則に服しており，この規則以外の欧州連合整合化立法またはそれ以外の適格な欧州連合の法行為にも服している製造者に的を絞ったガイド；

guidance targeted at manufacturers subject to this Regulation that are also subject to Union harmonisation legislation other than this Regulation or to other related Union legal acts;

(d) 大きな修正の概念。

the concept of substantial modification.

欧州委員会は，この規則によって採択される委任される行為及び実装行為の容易にアクセス可能なリストを維持管理する。

The Commission shall also maintain an easy-to-access list of the delegated and implementing acts adopted pursuant to this Regulation.

3. 本条によるガイドを準備する際，欧州委員会は，適格な利害関係者から意見聴取する。

When preparing the guidance pursuant to this Article, the Commission shall consult relevant stakeholders.

第III章 デジタルの要素をもつ製品の適合性
Chapter Ⅲ **Conformity of the product with digital elements**

第 27 条 適合性の推定
Article 27 **Presumption of conformity**

1. その参照が EU 官報上で公示された整合化された技術標準またはその一部に適合しているデジタルの要素をもつ製品及び製造者によって設けられたプロセスは，それらの技術標準またはその一部によって包摂されている別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していると推定される。

Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those standards or parts thereof.

欧州委員会は，規則(EU)No 1025/2012 の第 10 条第 1 項に従い，1 または複数の欧州の標準化組織に対し，この規則の別紙 I の中で定められた必須のサイバーセキュリティ要件に関する整合化された技術標準を起草することを要請する。この規則のための標準化要請を準備する際，欧州委員会は，規則(EU)No 1025/2012 に従い，整合化された技術標準の開発を簡素化するため，実施されているまたは開発中のサイバーセキュリティに関する既存の欧州の技術標準及び国際的な技術標準を考慮に入れるよう努める。

The Commission shall, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards for the essential cybersecurity requirements set out in Annex I to this Regulation. When preparing standardisation requests for this Regulation, the Commission shall strive to take into account existing European and international standards for cybersecurity that are in place or under development in order to simplify the development of harmonised standards, in accordance with Regulation (EU) No 1025/2012.

2. 欧州委員会は，この規則の適用範囲内にあるデジタルの要素をもつ製品に関する別紙 I の中で定められた必須のサイバーセキュリティ要件を遵守するための手段を提供する技術上の要件を包摂する共通仕様を定める実装行為を採択できる。

The Commission may adopt implementing acts establishing common specifications covering technical requirements that provide a means to comply with the essential cybersecurity requirements set out in Annex I for products with digital elements that fall within the scope of this Regulation.

同実装行為は，以下の条件が満たされる場合に限り，採択される：

Those implementing acts shall be adopted only where the following conditions are fulfilled:

(a) 欧州委員会が，規則(EU)No 1025/2012 の第 10 条第 1 項により，1 または複数の欧州の標準化組織に対し，この規則の別紙 I の中で定められた必須のサイバーセキュリティ要件に関する整合化された技術標準を起草することを要請しており，かつ：

the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the essential cybersecurity requirements set out in Annex I and:

(i) その要請が受諾されなかった場合；

the request has not been accepted;

(ii) 規則(EU)No 1025/2012 の第 10 条第 1 項に従って定められた期限内に，当該要請に対応する整合化された技術標準が伝達されなかった場合；または，

the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or

(iii) その整合化された技術標準が当該要請を遵守していない場合であり；かつ，

the harmonised standards do not comply with the request; and

(b) この規則の別紙 I の中で定められた適格な必須のサイバーセキュリティ要件を包摂する整合化された技術標準への参照が規則(EU)No 1025/2012 に従って EU 官報上で公示されていない場合であり，かつ，合理的な期間内にそのような参照が公示される見込みがない場合。

no reference to harmonised standards covering the relevant essential cybersecurity requirements set out in Annex I to this Regulation has been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012 and no such reference is expected to be published within a reasonable period.

同実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

3. 本条の第 2 項に示す実装行為案を準備する前に，欧州委員会は，規則(EU) No 1025/2012 の第 22 条に示す委員会に対し，本条の第 2 項に示す条件が満たされたと欧州委員会が判断している旨を連絡する。

Before preparing the draft implementing act referred to in paragraph 2 of this Article, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers that the conditions in paragraph 2 of this Article have been fulfilled.

4. 本条の第 2 項に示す実装行為案を準備する際，欧州委員会は，適格な組織の見解を考慮に入れ，かつ，全ての適格な利害関係者から適正に意見聴取する。

When preparing the draft implementing act referred to in paragraph 2, the Commission shall take into account the views of relevant bodies and shall duly consult all relevant stakeholders.

5. 本条の第 2 項に示す実装行為によって定められた共通仕様またはその一部に適合するデジタルの要素をもつ製品及び製造者によって設けられたプロセスは，当該共通仕様またはその一部によって包摂されている別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していると推定される。

Products with digital elements and processes put in place by the manufacturer which are in conformity with the common specifications established by implementing acts referred to in paragraph 2 of this Article, or parts thereof, shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I covered by those common specifications or parts thereof.

6. 整合化された技術標準が欧州の標準化組織によって採択され，EU 官報上においてその参照を公示する目的のために欧州委員会に対して提案されたときは，欧州委員会は，規則(EU) No 1025/2012 に従い，その整合化された技術標準を評価する。整合化された技術標準への参照が EU 官報上で公示される際，欧州委員会は，当該整合化された技術標準によって包摂されている必須のサイバーセキュリティ要件と同一の必須のサイバーセキュリティ要件を包摂している本条の第 2 項に示す実装行為またはその一部を廃止する。

Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the purpose of publishing its reference in the *Official Journal of the European Union*, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When a reference of a harmonised standard is published in the *Official Journal of the European Union*, the Commission shall repeal the implementing acts referred to in paragraph 2 of this Article, or parts thereof which cover the same essential cybersecurity requirements as those covered by that harmonised standard.

7. 共通仕様がこの規則の別紙 I の中で定められた必須のサイバーセキュリティ要件を全部満たしていないと構成国が判断するときは，その構成国は，欧州委員会に対し，詳細な説明書を提出することによって，そのことを連絡する。欧州委員会は，当該当該詳細な説明書を評価し，かつ，それが適切なときは，当の共通仕様を定める実装行為を改正できる。

Where a Member State considers that a common specification does not entirely satisfy the essential cybersecurity

requirements set out in Annex I, it shall inform the Commission thereof by submitting a detailed explanation. The Commission shall assess that detailed explanation and may, if appropriate, amend the implementing act establishing the common specification in question.

8. 規則(EU) 2019/881 によって採択された欧州サイバーセキュリティ認証制度の下において EU 適合宣言書または証明書が発行されたデジタルの要素をもつ製品及び製造者によって設けられたプロセスは，その EU 適合宣言書もしくは欧州サイバーセキュリティ証明書またはそれらの一部がこの規則の別紙 I の中で定められた必須のサイバーセキュリティ要件を包摂している範囲内において，同要件に適合していると推定される。

Products with digital elements and processes put in place by the manufacturer for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881 shall be presumed to be in conformity with the essential cybersecurity requirements set out in Annex I in so far as the EU statement of conformity or European cybersecurity certificate, or parts thereof, cover those requirements.

9. 欧州委員会は，デジタルの要素をもつ製品の，この規則の別紙 I の中に定める必須のサイバーセキュリティ要件またはその一部に適合性を示すために利用され得る規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度の細目を定めることによってこの規則を補完するため，この規則の第 61 条に従って委任される行為を採択する権限を与えられる。更に，そのような制度の下において発行され，少なくとも「十分」の保証レベルのサイバーセキュリティ証明書の発行は，この規則の第 32 条第 2 項(a)及び(b)並びに第 32 条第 3 項(a)及び(b)に定める対応する諸要件に関する第三者適合性評価を実施すべき製造者の義務を解消させる。

The Commission is empowered to adopt delegated acts in accordance with Article 61 of this Regulation to supplement this Regulation by specifying the European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 that can be used to demonstrate conformity of products with digital elements with the essential cybersecurity requirements or parts thereof as set out in Annex I to this Regulation. Furthermore, the issuance of a European cybersecurity certificate issued under such schemes, at least at assurance level 'substantial', eliminates the obligation of a manufacturer to carry out a third-party conformity assessment for the corresponding requirements, as set out in Article 32(2), points (a) and (b), and Article 32(3), points (a) and (b), of this Regulation.

第 28 条　EU 適合宣言書

Article 28 **EU declaration of conformity**

1. EU 適合宣言書は，第 13 条第 12 項に従って製造者によって作成され，かつ，別紙 I の中で定められた適用可能な必須のサイバーセキュリティ要件の充足が示された旨を述べる。

The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 13(12) and state that the fulfilment of the applicable essential cybersecurity requirements set out in Annex I has been demonstrated.

2. EU 適合宣言書は，別紙 V の中で定められたモデル構造をもち，かつ，別紙 VIII の中で定められた適格な適合性評価手続の中で細目が定められている諸要素を包含する。そのような宣言書は，しかるべくアップデートされる。EU 適合宣言書は，デジタルの要素をもつ製品が市場に置かれまたは市場において利用できるようにされた構成国から要求される言語で利用できるようにされる。

The EU declaration of conformity shall have the model structure set out in Annex V and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VIII. Such a declaration shall be updated as appropriate. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.

第 13 条第 20 項に示す簡易化された EU 適合宣言書は，別紙 VI の中で定められたモデル構造をもつ。簡易化された EU 適合宣言書は，デジタルの要素をもつ製品が市場に置かれまたは市場において利用できるようにされた構成国から要求される言語で利用できるようにされる。

The simplified EU declaration of conformity referred to in Article 13(20) shall have the model structure set out in Annex VI. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available on the market.

3. デジタルの要素をもつ製品が EU 適合宣言書を要求する複数の欧州連合の法行為に服するときは，そのような欧州連合の法行為の全てとの関係において単一の EU 適合宣言書が作成される。同宣言書は，その法行為の公示の参照を含め，関係する欧州連合の法行為の識別子を含める。

Where a product with digital elements is subject to more than one Union legal act requiring an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all such Union legal acts. That declaration shall contain the identification of the Union legal acts concerned, including their publication references.

4. EU 適合宣言書を作成することにより，製造者は，そのデジタルの要素をもつ製品の遵守に関する責任を負う。

By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the product with digital elements.

5. 欧州委員会は，技術上の発展を考慮に入れるために別紙 V の中で定められた EU 適合宣言書のミニマムの内容に要素を付加することによってこの規則を補完するため，第 61 条に従って委任される行為を採択する権限を与えられる。

The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by adding elements to the minimum content of the EU declaration of conformity set out in Annex V to take account of technological developments.

第 29 条　CE マークの総則的な基本原則
Article 29 **General principles of the CE marking**

CE マークは，規則(EC) No 765/2008 の第 30 条の中で定められた総則的な基本原則に服する。

The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

第 30 条　CE マークを付すことに関する規定及び条件
Article 30 **Rules and conditions for affixing the CE marking**

1. CE マークは，デジタルの要素をもつ製品に対し，視認的，読解可能かつ恒久的に付される。そのデジタルの要素をもつ製品の性質を考慮すると，そのことが不可能であるか保証されないときは，CE マークは，包装に付され及びそのデジタルの要素をもつ製品に添付される第 28 条に示す EU 適合宣言書に付される。ソフトウェア形態のデジタルの要素をもつ製品に関しては，CE マークは，第 28 条に示す EU 適合宣言書上またはソフトウェア製品を伴う Web サイト上のいずれかに付される。後者の場合，その Web サイトの適格なセクションは，消費者にとって容易かつ直接にアクセス可能なものとする。

   The CE marking shall be affixed visibly, legibly and indelibly to the product with digital elements. Where that is not possible or not warranted on account of the nature of the product with digital elements, it shall be affixed to the packaging and to the EU declaration of conformity referred to in Article 28 accompanying the product with digital elements. For products with digital elements which are in the form of software, the CE marking shall be affixed either to the EU declaration of conformity referred to in Article 28 or on the website accompanying the software product. In the latter case, the relevant section of the website shall be easily and directly accessible to consumers.

2. デジタルの要素をもつ製品の性質を考慮し，CE マークが視認的かつ読解可能なままであることを条件として，デジタルの要素をもつ製品に付される CE マークの高さは，5mm 未満であることが可能である。

   On account of the nature of the product with digital elements, the height of the CE marking affixed to the product with digital elements may be lower than 5 mm, provided that it remains visible and legible.

3. CE マークは，デジタルの要素をもつ製品が市場に置かれる前に付される。CE マークは，第 6 項に示す実装行為の中で定められる特別のサイバーセキュリティ上のリスクまたは利用を表示する絵文字またはそれ以外のマークを伴うことが可能である。

   The CE marking shall be affixed before the product with digital elements is placed on the market. It may be followed by a pictogram or any other mark indicating a special cybersecurity risk or use set out in the implementing acts referred to in paragraph 6.

4. 当該指定組織が第 32 条に示す（モジュール H を基礎とする）完全な品質保証を基礎とする適合性評価手続に関与するときは，CE マークは，その指定組織の識別番号を伴う。

The CE marking shall be followed by the identification number of the notified body, where that body is involved in the conformity assessment procedure based on full quality assurance (based on module H) referred to in Article 32.

指定組織の識別番号は，その組織自身によって付され，または，その組織の指示の下において，製造者もしくは製造者の権限のある代理者によって付される。

The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the manufacturer or the manufacturer's authorised representative.

5. 構成国は，CE マークを規律する制度の正確な適用を確保するため，既存の仕組みを基礎とし，かつ，同マークの不適正な利用の際には適切な行動をとる。デジタルの要素をもつ製品が，この規則以外の欧州連合整合化立法であって，その立法もまた CE マークを付すこと定めている立法に服するときは，その CE マークは，その製品がそのような別の欧州連合整合化立法の中で定められた要件も満たしていることを表示する。

Member States shall build upon existing mechanisms to ensure correct application of the regime governing the CE marking and shall take appropriate action in the event of improper use of that marking. Where the product with digital elements is subject to Union harmonisation legislation, other than this Regulation, which also provides for the affixing of the CE marking, the CE marking shall indicate that the product also fulfils the requirements set out in such other Union harmonisation legislation.

6. 欧州委員会は，実装行為により，デジタルの要素をもつ製品の防護，それらの製品のサポート期間，及び，それらの利用を向上させるための仕組み及びデジタルの要素をもつ製品の防護に関する公衆の認識を向上させる仕組みと関連するラベル，絵文字またはそれ以外の記号に関する技術仕様を定め得る。実装行為案を準備する際，欧州委員会は，適格な利害関係者から意見聴取し，また，第 52 条第 15 項により ADCO が既に設置されているときは，ADCO から意見聴取する。同実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

The Commission may, by means of implementing acts, lay down technical specifications for labels, pictograms or any other marks related to the security of the products with digital elements, their support periods and mechanisms to promote their use and to increase public awareness about the security of products with digital elements. When preparing the draft implementing acts, the Commission shall consult relevant stakeholders, and, if it has already been established pursuant to Article 52(15), ADCO. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

第 31 条 技術文書

Article 31 **Technical documentation**

1. 技術文書は，デジタルの要素をもつ製品及びその製造者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件を遵守することを確保するためにその製造者によって使用される全ての適格なデータまたは手段の詳細を含める。技術文書は，少なくとも，別紙 VII の中で定められた諸要素を含める。

   The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Annex I. It shall at least contain the elements set out in Annex VII.

2. 技術文書は，デジタルの要素をもつ製品が市場に置かれる前に作成され，かつ，それが適切なときは，少なくともサポート期間内は，継続的にアップデートされる。

   The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, at least during the support period.

3. 第 12 条に示すデジタルの要素をもつ製品であって，技術文書を定めている他の欧州連合の法行為にも服する製品に関しては，この規則の別紙 VII に示す情報及び当該別の欧州連合の法行為によって要求される情報を含めて，単一のセットの技術文書が作成される。

   For products with digital elements as referred to in Article 12, which are also subject to other Union legal acts which provide for technical documentation, a single set of technical documentation shall be drawn up containing the information referred to in Annex VII and the information required by those Union legal acts.

4. 技術文書及び適合性評価手続と関連する対応文書は，指定組織が拠点をもつ構成国の公用語または当該組織にとって受容可能な言語で作成される。

   The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.

5. 欧州委員会は，技術上の発展及びこの規則の実装過程において直面した発展を考慮に入れるために別紙 VII の中で定められた技術文書の中に付加的な諸要素が含められることによってこの規則を補完するため，第 61 条に従って委任される行為を採択する権限を与えられる。その目的のために，欧州委員会は，マイクロ企業並びに小企業及び中規模企業にかかる行政上の負担が比例的なものであることを確保することに努める。

   The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation by

adding elements to be included in the technical documentation set out in Annex VII to take account of technological developments, as well as developments encountered in the implementation process of this Regulation. To that end, the Commission shall strive to ensure that the administrative burden on microenterprises and small and medium-sized enterprises is proportionate.

第 32 条 デジタルの要素をもつ製品の適合性評価手続

Article 32 **Conformity assessment procedures for products with digital elements**

1. 製造者は，別紙 I の中で定められた必須のサイバーセキュリティ要件に適合しているかどうかを判定するため，デジタルの要素をもつ製品及びその製造者によって設けられたプロセスの適合性評価を遂行する。その製造者は，以下の諸手続のいずれかを用いることにより，必須のサイバーセキュリティ要件との適合性を示す：

The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential cybersecurity requirements set out in Annex I are met. The manufacturer shall demonstrate conformity with the essential cybersecurity requirements by using any of the following procedures:

(a) 別紙 VIII の中で定められた（モジュール A を基礎とする）内部統制手続；

the internal control procedure (based on module A) set out in Annex VIII;

(b) 別紙 VIII の中で定められた（モジュール C を基礎とする）内部製造管理を基礎とする EU 型式の適合性を伴う別紙 VIII の中で定められた（モジュール B を基礎とする）EU 型式審査手続；

the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII;

(c) 別紙 VIII の中で定められた（モジュール H を基礎とする）完全な品質保証を基礎とする適合性評価；または

a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or

(d) それが利用可能かつ適用可能なときは，第 27 条第 9 項による欧州サイバーセキュリティ認証制度。

where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9).

2. 別紙 III の中で定められたクラス I の中に含まれているデジタルの要素をもつ重要な製品及びその

製品の製造者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件を遵守していることを評価する際において，その製造者が，第 27 条に示す整合化された技術標準，共通仕様または少なくとも「十分」の保証レベルの欧州サイバーセキュリティ認証制度を適用せず，もしくは，それらの一部のみを適用した場合，または，そのような整合化された技術標準，共通仕様または欧州サイバーセキュリティ認証制度が存在しない場合，関係するデジタルの要素をもつ製品及びその製造者によって設けられたプロセスは，それらの必須のサイバーセキュリティ要件に関して，以下のいずれかの手続に付される：

Where, in assessing the compliance of an important product with digital elements that falls under class I as set out in Annex III and the processes put in place by its manufacturer with the essential cybersecurity requirements set out in Annex I, the manufacturer has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes at assurance level at least 'substantial' as referred to in Article 27, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential cybersecurity requirements to either of the following procedures:

(a) 別紙 VIII の中で定められた（モジュール C を基礎とする）内部製造管理を基礎とする EU 型式の適合性を伴う別紙 VIII の中で定められた（モジュール B を基礎とする）EU 型式審査手続；または

the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; or

(b) 別紙 VIII の中で定められた（モジュール H を基礎とする）完全な品質保証を基礎とする適合性評価。

a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII.

3. その製品が，別紙 III に定めるクラス II の範囲内にあるデジタルの要素をもつ重要な製品である場合，その製造者は，以下の手続のいずれかを用いて， 別紙 I の中で定められた必須のサイバーセキュリティ要件の適合性を示す：

Where the product is an important product with digital elements that falls under class II as set out in Annex III, the manufacturer shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using any of the following procedures:

(a) 別紙 VIII の中で定められた（モジュール C を基礎とする）内部製造管理を基礎とする EU 型式の適合性を伴う別紙 VIII の中で定められた（モジュール B を基礎とする）EU 型式審査手続；

EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type

based on internal production control (based on module C) set out in Annex VIII;

(b) 別紙 VIII の中で定められた（モジュール H を基礎とする）完全な品質保証を基礎とする適合性評価；または

a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or

(c) それが利用可能かつ適用可能なときは，規則(EU) 2019/881 による少なくとも「十分」の保証レベルで，この規則の第 27 条第 9 項による欧州サイバーセキュリティ認証制度。

where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9) of this Regulation at assurance level at least 'substantial' pursuant to Regulation (EU) 2019/881.

4. 別紙 IV の中で列挙されたデジタルの要素をもつ不可欠な製品は，以下の手続のいずれかを用いて，別紙 I の中で定められた必須のサイバーセキュリティ要件の適合性を示す：

Critical products with digital elements listed in Annex IV shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the following procedures:

(a) 第 8 条第 1 項に従って，欧州サイバーセキュリティ認証制度；または

a European cybersecurity certification scheme in accordance with Article 8(1); or

(b) 第 8 条第 1 項の条件に適合しないときは，本条の第 3 項に示すいずれかの手続。

where the conditions in Article 8(1) are not met, any of the procedures referred to in paragraph 3 of this Article.

5. 別紙IIIの中で定められた類型の下にあり，無料でオープンソースのソフトウェアとしての適格のあるデジタルの要素をもつ製品の製造者は，当該製品が市場に置かれる時点において第 31 条に示す技術文書が公衆に利用できるようにされていることを条件として，本条の第 1 項に示すいずれかの手続を用いることによって，別紙 I の中で定められた必須のサイバーセキュリティ要件の適合性を示し得る。

Manufacturers of products with digital elements qualifying as free and open-source software, which fall under the categories set out in Annex III, shall be able to demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using one of the procedures referred to in paragraph 1 of this Article, provided that the technical documentation referred to in Article 31 is made available to the public at the time of the placing on the market of those products.

6. 適合性評価手続の手数料を設定する際，スタートアップを含め，マイクロ企業並びに小企業及び中規模企業の個別の利益と需要が考慮に入れられ，かつ，それらの手数料は，それらの企業の個別の利益と需要に比例して減額される。

The specific interests and needs of microenterprises and small and medium-sized enterprises, including start-ups, shall be taken into account when setting the fees for conformity assessment procedures and those fees shall be reduced proportionately to their specific interests and needs.

第 33 条 スタートアップを含め，マイクロ企業並びに小企業及び中規模企業のための支援措置

Article 33 **Support measures for microenterprises and small and medium-sized enterprises, including start-ups**

1. 構成国は，それが適切なときは，マイクロ企業及び小企業の需要に個別対応して，以下の活動を行う:

Member States shall, where appropriate, undertake the following actions, tailored to the needs of microenterprises and small enterprises:

(a) この規則の適用に関し，個別の認識向上及び訓練の活動を開始準備すること;

organise specific awareness-raising and training activities about the application of this Regulation;

(b) この規則の実装に関し，助言を提供し及び質問に応答するための，マイクロ企業及び小企業との間の，及び，しかるべく地方行政機関との間の，専用通信経路を設置すること;

establish a dedicated channel for communication with microenterprises and small enterprises and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation;

(c) 欧州サイバーセキュリティ能力拠点の支援と関係する場合を含め，試験及び適合性評価の活動を支援すること。

support testing and conformity assessment activities, including where relevant with the support of the European Cybersecurity Competence Centre.

2. 構成国は，それが適切なときは，サイバー回復力の法制サンドボックスを設置できる。そのような法制サンドボックスは，市場に置く前の限定された期間内，この規則を遵守する目的のために当該製品の開発，設計，検証及び試験を容易にするためのデジタルの要素をもつ革新的な製品の管理された試験環境を提供する。欧州委員会，及び，それが適切なときは，ENISA は，法制サンドボックスの設置及び運用のための技術上の支援，助言及びツールを提供できる。法制サンドボックスは，市場監視当局の直接の監督，ガイド及び支援の下で設置される。構成国は，欧州委員会及び他の市場

監視当局に対し，ADCO を介して，法制サンドボックスの設置を連絡する。法制サンドボックスは，職務権限のある機関の監督権限及び是正権限に影響を与えてはならない。構成国は，法制サンドボックスへのオープンで、公正かつ透明性のあるアクセスを確保し，また，とりわけ，スタートアップを含め，マイクロ企業及び小企業によるアクセスを容易にする。

Member States may, where appropriate, establish cyber resilience regulatory sandboxes. Such regulatory sandboxes shall provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before the placing on the market. The Commission and, where appropriate, ENISA, may provide technical support, advice and tools for the establishment and operation of regulatory sandboxes. The regulatory sandboxes shall be set up under the direct supervision, guidance and support by the market surveillance authorities. Member States shall inform the Commission and the other market surveillance authorities of the establishment of a regulatory sandbox through ADCO. The regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. Member States shall ensure open, fair, and transparent access to regulatory sandboxes, and in particular facilitate access by microenterprises and small enterprises, including start-ups.

3. 第 26 条に従い，欧州委員会は，この規則の実装との関係において，マイクロ企業並びに小企業及び中規模企業のためのガイドを提供する。

In accordance with Article 26, the Commission shall provide guidance for microenterprises and small and medium-sized enterprises in relation to the implementation of this Regulation.

4. 欧州委員会は，とりわけ，マイクロ企業及び小企業にかかる資金負担を緩和するため，既存の欧州連合の計画の法制枠組み内において，利用可能な資金支援を周知する。

The Commission shall advertise available financial support in the regulatory framework of existing Union programmes, in particular in order to ease the financial burden on microenterprises and small enterprises.

5. マイクロ企業及び小企業は，簡易化された書式を用いて，別紙 VII の中で細目が定められた技術文書の全ての要素を提供できる。その目的のために，欧州委員会は，実装行為により，別紙 VII の中で定められた要素がどのようにして提供されるべきかを含め，マイクロ企業及び小企業の需要に的を絞って，簡易化された技術文書の書式の細目を定める。マイクロ企業または小企業が，簡易化された態様により別紙 VII の中で定められた情報を提供することを選択する場合，その企業は，本項に示す書式を使用する。指定組織は，適合性評価の目的のためにその書式を認める。

Microenterprises and small enterprises may provide all elements of the technical documentation specified in Annex VII by using a simplified format. For that purpose, the Commission shall, by means of implementing acts, specify the simplified technical documentation form targeted at the needs of microenterprises and small enterprises, including how the elements set out in Annex VII are to be provided. Where a microenterprise or small enterprise opts to provide the information set out in Annex VII in a simplified manner, it shall use the form referred to in this paragraph. Notified

bodies shall accept that form for the purposes of conformity assessment.

同実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

第 34 条　相互承認の協定

Article 34 **Mutual recognition agreements**

技術発展のレベル及び第三国の適合性評価に関するアプローチを考慮に入れた上で，国際取引を促進しかつ容易にするため，欧州連合は，TFEU の第 218 条に従い，第三国との間で相互承認協定を締結できる。

Taking into account the level of technical development and the approach on conformity assessment of a third country, the Union may conclude Mutual Recognition Agreements with third countries, in accordance with Article 218 TFEU, in order to promote and facilitate international trade.

第IV章 適合性評価組織の通知
Chapter IV **Notification of Conformity Assessment Bodies**

第 35 条 通知
Article 35 **Notification**

1. 構成国は，欧州委員会及び他の構成国に対し，この規則に従って適合性評価を実施することが認められた組織を通知する。

   Member States shall notify the Commission and the other Member States of bodies authorised to carry out conformity assessments in accordance with this Regulation.

2. 構成国は，2026 年 12 月 11 日までに，市場参入を妨げる隘路と障碍を避けるため，適合性評価を実施するための十分な数の指定組織が欧州連合内に存在することを確保するよう努める。

   Member States shall strive to ensure, by 11 December 2026 that there is a sufficient number of notified bodies in the Union to carry out conformity assessments, in order to avoid bottlenecks and hindrances to market entry.

第 36 条 通知元当局
Article 36 **Notifying authorities**

1. 各構成国は，適合性評価組織の評価，指定及び通知のために必要となる手続を設けること及び遂行すること，並びに，第 41 条の遵守を含め，それらの組織を監視することに関して職責を負う通知元当局を指定する。

   Each Member State shall designate a notifying authority that shall be responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and their monitoring, including compliance with Article 41.

2. 構成国は，第 1 項に示す評価及び監視が，規則(EC) No 765/2008 の意味における国内認定組織によって，かつ，同規則に従って実施されることを決定できる。

   Member States may decide that the assessment and monitoring referred to in paragraph 1 shall be carried out by a national accreditation body within the meaning of and in accordance with Regulation (EC) No 765/2008.

3. 通知元当局が，政府の法主体ではない組織に対し，本条の第 1 項に示す評価，通知または監視を委任しまたは委任以外の委託をする場合，当該組織は，法人であるものとし，かつ，第 37 条を*準用*して遵守する。加えて，通知元当局は，その通知元当局の活動から生ずる法的責任に適用される手立てを設ける。

Where the notifying authority delegates or otherwise entrusts the assessment, notification or monitoring referred to in paragraph 1 of this Article to a body which is not a governmental entity, that body shall be a legal entity and shall comply *mutatis mutandis* with Article 37. In addition, it shall have arrangements in place to cover liabilities arising from its activities.

4. 通知元当局は，第 3 項に示す組織によって遂行される職務に関し，全面的に職責を負う。

The notifying authority shall take full responsibility for the tasks performed by the body referred to in paragraph 3.

第 37 条　通知元当局と関連する要件

Article 37 **Requirements relating to notifying authorities**

1. 通知元当局は，適合性評価組織との間で利益相反が発生しないような方法で設置される。

A notifying authority shall be established in such a way that no conflict of interest with conformity assessment bodies occurs.

通知元当局は，その通知元当局の活動の客観性及び公平性を守るように組織構成され，かつ，そのように稼働する。

A notifying authority shall be organised and shall function so as to safeguard the objectivity and impartiality of its activities.

2. 通知元当局は，当該評価を実施する者とは別の職務権限のある者によって適合性評価組織の通知と関連する個々の決定が行われるような方法で組織構成される。

A notifying authority shall be organised in such a way that each decision relating to notification of a conformity assessment body is taken by competent persons different from those who carried out the assessment.

3. 通知元当局は，適合性評価組織が遂行する活動またはコンサルタントサービスを商業ベースまたは競争ベースで提示または提供してはならない。

A notifying authority shall not offer or provide any activities that conformity assessment bodies perform or consultancy services on commercial or competitive basis.

4. 通知元当局は，その通知元当局が入手する情報の機密性を守る。

A notifying authority shall safeguard the confidentiality of the information it obtains.

5. 通知元当局は，その通知元当局の職務の適正な遂行のためにその通知元当局が自由に使うことのできる十分な員数の職務権限のある者をもつ。

A notifying authority shall have a sufficient number of competent personnel at its disposal for the proper performance of its tasks.

第 38 条 通知元当局に関する情報提供義務

Article 38 **Information obligation on notifying authorities**

1. 構成国は，欧州委員会に対し，適合性評価組織の評価及び通知並びに指定組織の監視に関するその構成国の手続を連絡し，また，その後の変更を連絡する。

Member States shall inform the Commission of their procedures for the assessment and notification of conformity assessment bodies and the monitoring of notified bodies, and of any changes thereto.

2. 欧州委員会は，第 1 項に示す情報を公表する。

The Commission shall make the information referred to in paragraph 1 publicly available.

第 39 条 指定組織と関連する要件

Article 39 **Requirements relating to notified bodies**

1. 通知の目的のために，適合性評価組織は，第 2 項ないし第 12 項の中で定められた要件に適合するものとする。

For the purposes of notification, a conformity assessment body shall meet the requirements laid down in paragraphs 2 to 12.

2. 適合性評価組織は，国内法の下において設立され，かつ，法人格をもつ。

A conformity assessment body shall be established under national law and have legal personality.

3. 適合性評価組織は，その適合性評価組織が評価する組織またはデジタルの要素をもつ製品から独立の第三者組織であるものとする。

A conformity assessment body shall be a third-party body independent of the organisation or the product with digital elements it assesses.

当該適合性評価組織が評価するデジタルの要素をもつ製品の設計，開発，製造，提供，組立て，使用または維持管理に関与する事業者を代表する事業者団体または職業人協会に所属する組織は，当該組織の独立性及び利益相反の不存在が示されることを条件として，そのような第三者組織であると判断され得る。

A body belonging to a business association or professional federation representing undertakings involved in the design, development, production, provision, assembly, use or maintenance of products with digital elements which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered to be such a third-party body.

4. 適合性評価組織，その適合性評価組織の最上位の経営陣及びその適合性評価の職務の遂行に関して職責を負う者は，それらの者が評価するデジタルの要素をもつ製品の設計者，開発者，製造者，供給者，輸入業者，流通業者，設置者，購入者，保有者，利用者または維持管理者であってはならず，また，それらの関係者の権限のある代理者であってもならない。このことは，その適合性評価組織の運用のために必要な被評価製品の利用またはそのような製品の私的目的のための利用を排除してはならない。

A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be the designer, developer, manufacturer, supplier, importer, distributor, installer, purchaser, owner, user or maintainer of the products with digital elements which they assess, nor the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

適合性評価組織，その適合性評価組織の最上位の経営陣及びその適合性評価の職務の遂行に関して職責を負う者は，それらの者が評価するデジタルの要素をもつ製品の設計，開発，製造，輸入，流通，マーケティング，設置，利用または維持管理に直接に関与してはならず，または，それらの活動に従事する者を代理してはならない。当該の者は，その活動に関してその適合性評価組織が通知された適合性評価活動との関係において，当該の者の判断の独立性または完全性と抵触し得るいかなる活動にも従事してはならない。このことは，とりわけ，コンサルタントサービスに対して適用される。

A conformity assessment body, its top level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, development, production, import, distribution, the marketing, installation, use or maintenance of the products with digital elements which they assess, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall in particular apply to consultancy services.

適合性評価組織は，その適合性評価組織の子組織または下請業者の活動が，その適合性評価組織の適合性評価活動の機密性，客観性または公平性に対して影響を与えないことを確保する。

Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

5. 適合性評価組織及び当該組織の者は，職業人としての最高度の完全性及び個別の分野において必要な技術上の能力をもって適合性評価活動を実施し，かつ，特に，当該評価活動の結果に利害のある個人または個人のグループに関し，当該の者の判断または当該の者の適合性評価活動の結果に対して影響を及ぼすかもしれない全ての圧力及び誘惑，特に金銭的な圧力及び誘惑を受けないものとする。

Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, particularly financial, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

6. 適合性評価組織は，当該職務がその適合性評価組織自身によって実施されるかまたはその適合性評価組織の責任の下においてその適合性評価組織の代わりの者によって実施されるかを問わず，別紙 VIII に示す全ての適合性評価の職務を，かつ，通知されたこととの関係において実施できるものとする。

A conformity assessment body shall be capable of carrying out all the conformity assessment tasks referred to in Annex VIII and in relation to which it has been notified, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

常に，並びに，通知されたこととの関係において個々の適合性評価手続及び個々の種類または類型のデジタルの要素をもつ製品に関し，適合性評価組織は，必要な以下のものを自由に利用できるものとする：

At all times and for each conformity assessment procedure and each kind or category of products with digital elements in relation to which it has been notified, a conformity assessment body shall have at its disposal the necessary:

(a) 適合性評価の職務を遂行するための技術上の知識及び十分かつ適切な経験をもつ者；

personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) それに従って適合性評価が実施され，その手続の透明性及び再利用の能力を確保する手続説明書。その手続説明書は，当該適合性評価組織が指定組織として実施する職務とそれ以外の職務との間を分別する適切な基本方針及び手続をもつ；

descriptions of procedures in accordance with which conformity assessment is to be carried out, ensuring the transparency of and ability to reproduce those procedures. It shall have appropriate policies and procedures in place that distinguish between tasks it carries out as a notified body and other activities;

(c) 事業者の規模, 事業者が業務運用する部門, 事業者の組織構造, 当の製造技術の複雑性の程度及び製造過程の大量的な性質または連続的な性質を適正に考慮に入れた活動遂行のための手続。

procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the product technology in question and the mass or serial nature of the production process.

適合性評価組織は, 適合性評価の活動と関係をもつ技術上の職務及び行政上の職務を適切な態様で遂行するために必要となる手段をもち, かつ, 必要な全ての機器または施設へのアクセスをもつ。

A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner and shall have access to all necessary equipment or facilities.

7. 適合性評価の活動を実施することに関して職責を負う者は, 以下のものもつ:

The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) その適合性評価組織が通知されたこととの関係において全ての適合性評価活動を包摂する良好な技術上の訓練及び職業訓練;

sound technical and vocational training covering all the conformity assessment activities in relation to which the conformity assessment body has been notified;

(b) 当該の者が実施する評価の要件についての十分な知識及び当該評価を実施するための適切な権限;

satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) 別紙Ⅰの中で定められた必須のサイバーセキュリティ要件, 適用可能な整合化された技術標準及び共通仕様並びに欧州連合整合化立法の適格な条項及び実装行為についての適切な知識と理解;

appropriate knowledge and understanding of the essential cybersecurity requirements set out in Annex I, of the applicable harmonised standards and common specifications, and of the relevant provisions of Union harmonisation legislation and implementing acts;

(d) 当該評価が実施されたことを示す証明書，記録及び報告書を作成する能力。

the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

8. 適合性評価組織，適合性評価組織の最上位経営陣及び評価者の公平性は，保証される。

The impartiality of the conformity assessment bodies, their top level management and of the assessment personnel shall be guaranteed.

適合性評価組織の最上位経営陣及び評価者の報酬は，実施された評価の数またはその評価の結果に依ってはならない。

The remuneration of the top level management and assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

9. 適合性評価組織は，国内法に従ってその適合性評価組織の構成国が法的責任を負わない限り，または，その構成国自身が適合性評価に関して直接に職責を負わない限り，損害賠償責任保険に加入する。

Conformity assessment bodies shall take out liability insurance unless liability is assumed by their Member State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

10. 適合性評価組織の者は，その適合性評価組織の活動が実施される構成国の市場監視当局との関係における場合を除き，別紙 VIII の下にあるその適合性評価組織の職務またはその職務に有効性を与える国内法の条項の下にあるその適合性評価組織の職務を遂行する際に入手した全ての情報に関し，職業上の秘密を尊重する。専有権は，保護される。適合性評価組織は，本項の遵守を確保するための文書化された手続をもつ。

The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under Annex VIII or any provision of national law giving effect to it, except in relation to the market surveillance authorities of the Member State in which its activities are carried out. Proprietary rights shall be protected. The conformity assessment body shall have documented procedures ensuring compliance with this paragraph.

11. 適合性評価組織は，適格な標準化活動及び第 51 条の下で設置される指定組織調整グループの活動に参加し，または，その適合性評価組織の者がそれらの活動の連絡を受けることを確保し，ま

た，一般的なガイドとして，行政上の判断及び同グループの作業の結果として作成された文書を適用する。

Conformity assessment bodies shall participate in, or ensure that their assessment personnel are informed of, the relevant standardisation activities and the activities of the notified body coordination group established under Article 51 and apply as general guidance the administrative decisions and documents produced as a result of the work of that group.

12. 適合性評価組織は，とりわけ，手数料との関係においてマイクロ企業並びに小企業及び中規模企業の利益を考慮に入れた上で，経済取引主体に対する無用の負担を避けつつ，一貫性があり，公正であり，比例的かつ合理的な利用条件のセットに従って業務運営する。

Conformity assessment bodies shall operate in accordance with a set of consistent, fair, proportionate and reasonable terms and conditions, while avoiding unnecessary burden for economic operators, in particular taking into account the interests of microenterprises and small and medium-sized enterprises in relation to fees.

第 40 条　指定組織の適合性の推定

Article 40 **Presumption of conformity of notified bodies**

適合性評価組織が，その参照が EU 官報上で公示された適格な整合化された技術標準またはその一部の中で定められた基準へのその適合性評価組織の適合性を示すときは，その適合性評価組織は，適用可能な整合化された技術標準が当該要件を包摂している範囲内において，第 39 条の中で定められた要件を遵守していると推定される。

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* it shall be presumed to comply with the requirements set out in Article 39 in so far as the applicable harmonised standards cover those requirements.

第 41 条　指定組織の下部組織及び指定組織による再委託

Article 41 **Subsidiaries of and subcontracting by notified bodies**

1. 指定組織が適合性評価と関係する個別の職務を再委託し，または，下部組織に任せるときは，その指定組織は，その再委託先または下部組織が第 39 条の中で定められた要件に適合することを確保し，かつ，通知元当局に対し，しかるべく連絡する。

Where a notified body subcontracts specific tasks connected with conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements set out in Article 39 and shall inform the notifying authority accordingly.

2. 指定組織は，再委託先または下部組織が設けられているときはいつでも，再委託先または下部組織によって遂行された職務に関する職責を全面的に負う。

Notified bodies shall take full responsibility for the tasks performed by subcontractors or subsidiaries wherever they are established.

3. 活動は，製造者の同意があるときに限り，再委託され，または，下部組織によって実施され得る。

Activities may be subcontracted or carried out by a subsidiary only with the agreement of the manufacturer.

4. 指定組織は，再委託先または下部組織の資格の評価に関する適格な文書及びこの規則の下において再委託先または下部組織によって実施された仕事に関する適格な文書を通知元当局が自由に利用できるように保つ。

Notified bodies shall keep at the disposal of the notifying authority the relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation.

第 42 条 通知の申請

Article 42 **Application for notification**

1. 適合性評価組織は，その適合性評価組織が拠点をもつ構成国の通知元当局に対し，通知の申請書を提出する。

A conformity assessment body shall submit an application for notification to the notifying authority of the Member State in which it is established.

2. 同申請書は，適合性評価活動，1 または複数の適合性評価手続及びその適合性評価組織が能力をもつと主張する 1 または複数のデジタルの要素をもつ製品の説明書が添付され，また，それが適用可能なときは，当該適合性評価組織が第 39 条の中で定められた要件を満たしていることを証明する国内認定組織から発行された認定書が添付される。

That application shall be accompanied by a description of the conformity assessment activities, the conformity assessment procedure or procedures and the product or products with digital elements for which that body claims to be competent, as well as, where applicable, by an accreditation certificate issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 39.

3. 関係する適合性評価組織が認定書を提供できないときは，その適合性評価組織は，通知元当局に対し，第 39 条の中で定められた要件をその適合性評価組織が遵守していることの検証，承認及び定期的な監視のために必要となる全ての文書化された証拠を提供する。

Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 39.

第 43 条 通知手続

Article 43 **Notification procedure**

1. 通知元当局は，第 39 条の中で定められた要件を満たした適合性評価組織のみを通知する。

Notifying authorities shall notify only conformity assessment bodies which have satisfied the requirements laid down in Article 39.

2. 通知元当局は，欧州委員会及び他の構成国に対し，欧州委員会によって開発され及び運営管理されている新アプローチの被通知団体及び被指定団体情報システムを用いて通知する。

The notifying authority shall notify the Commission and the other Member States using the New Approach Notified and Designated Organisations information system developed and managed by the Commission.

3. 通知は，適合性評価活動の詳細全部，1 または複数の適合性評価モジュール及び 1 または複数の関係するデジタルの要素をもつ製品並びに適格な能力証明書を含める。

The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and product or products with digital elements concerned and the relevant attestation of competence.

4. 通知が第 42 条第 2 項に示す認定書を基礎としないときは，通知元当局は，欧州委員会及び他の構成国に対し，その適合性評価組織の能力を証明する文書化された証拠及び当該組織が定期的に監視され，かつ，第 39 条の中で定められた要件を満たし続けることを確保するために設けられる手立てを提供する。

Where a notification is not based on an accreditation certificate as referred to in Article 42(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the conformity assessment body's competence and the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 39.

5. 関係する組織は，認定書が使用される場合には通知から 2 週間以内に，または，認定書が使用されない場合には通知から 2 か月以内に，欧州委員会または他の構成国から異議が提起されない場合に限り，指定組織の活動を遂行できる。

The body concerned may perform the activities of a notified body only where no objections are raised by the

Commission or the other Member States within two weeks of a notification where an accreditation certificate is used or within two months of a notification where accreditation is not used.

そのような組織のみが，この規則の目的のための指定組織であると判断される。

Only such a body shall be considered to be a notified body for the purposes of this Regulation.

6. 欧州委員会及び他の構成国は，通知に対するその後の適格な変更の通知を受ける。

The Commission and the other Member States shall be notified of any subsequent relevant changes to the notification.

第 44 条　指定組織の識別番号及びリスト

Article 44 **Identification numbers and lists of notified bodies**

1. 欧州委員会は，指定組織に対し，識別番号を割当てる。

The Commission shall assign an identification number to a notified body.

欧州委員会は，欧州連合の複数の法行為の下において当該組織が通知されている場合であっても，単一の識別番号を割当てる。

It shall assign a single such number even where the body is notified under several Union legal acts.

2. 欧州委員会は，当該組織に割当てられた識別番号及び当該組織に関して通知された活動を含めて，この規則の下において通知された組織のリストを公表する。

The Commission shall make publicly available the list of the bodies notified under this Regulation, including the identification numbers that have been allocated to them and the activities for which they have been notified.

欧州委員会は，同リストを最新の状態に保つ。

The Commission shall ensure that that list is kept up to date.

第 45 条　通知の変更

Article 45 **Changes to notifications**

1. 指定組織が第 39 条の中で定められた要件を満たさなくなったことまたは当該組織がその組織の義務を満たしていないことを通知元当局が確認した場合またはそのことの連絡を受けた場合，その通

知元当局は，当該要件に適合していないことまたは当該義務を満たしていないことの重大性の程度に応じて，しかるべく，通知を制限し，停止しまたは取消す。その通知元当局は，欧州委員会及び他の構成国に対し，直ちに，しかるべく連絡する。

Where a notifying authority has ascertained or has been informed that a notified body no longer meets the requirements laid down in Article 39, or that it is failing to fulfil its obligations, the notifying authority shall restrict, suspend or withdraw notification as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

2. 通知の制限，停止もしくは取消が発生する場合または指定組織がその組織の活動を停止させた場合，通知元構成国は，当該組織の記録が，別の指定組織によって処理されること，または，職責を負う通知元当局及び市場監視当局の要請に応じて，それらの当局が利用できることを保つことを確保するための適切な手立てを講ずる。

In the event of restriction, suspension or withdrawal of notification, or where the notified body has ceased its activity, the notifying Member State shall take appropriate steps to ensure that the files of that body are either processed by another notified body or kept available for the responsible notifying and market surveillance authorities at their request.

第 46 条　指定組織の能力の疑義

Article 46 **Challenge of the competence of notified bodies**

1. 欧州委員会は，指定組織が服している要件及び職責に適合するための指定組織の能力または指定組織によってその要件及び職責が継続して満たされていることに欧州委員会が疑問をもつときは，または，それらに関する疑義に欧州委員会が注意を向けるときは，全ての案件を調査する。

The Commission shall investigate all cases where it doubts, or where doubt is brought to its attention regarding, the competence of a notified body to meet, or the continued fulfilment by a notified body of, the requirements and responsibilities to which it is subject.

2. 通知元構成国は，欧州委員会に対し，求めに応じて，その通知の根拠または関係する組織の能力が維持されていることと関連する全ての情報を提供する。

The notifying Member State shall provide the Commission, on request, with all information relating to the basis for the notification or the maintenance of the competence of the body concerned.

3. 欧州委員会は，欧州委員会の調査の過程において入手した全ての機微の情報が機密に扱われることを確保する。

The Commission shall ensure that all sensitive information obtained in the course of its investigations is treated

confidentially.

4. 指定組織がその指定組織の通知のための要件に適合していないことまたは適合しなくなっていることを欧州委員会が確認したときは，欧州委員会は，通知元構成国に対し，しかるべく連絡し，かつ，通知元構成国に対し，必要があるときは通知の失効を含め，必要な是正措置を講ずることを求める。

Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including de-notification if necessary.

第 47 条　指定組織の業務運営上の義務

Article 47 **Operational obligations of notified bodies**

1. 指定組織は，第 32 条及び別紙 VIII の中で定められた適合性評価手続に従って適合性評価を実施する。

Notified bodies shall carry out conformity assessments in accordance with the conformity assessment procedures provided for in Article 32 and Annex VIII.

2. 適合性評価は，経済取引主体の無用の負担を避ける比例的な態様で実施される。適合性評価組織は，とりわけマイクロ企業並びに小企業及び中規模企業に関し，事業者の規模，事業者が業務運営する部門，事業者の組織構造，当のデジタルの要素をもつ製品と技術の複雑性及びサイバーセキュリティ上のリスクのレベル並びに製造過程の大量的な性質または連続的な性質を適正に考慮に入れた上で，その適合性評価組織の活動を遂行する。

Conformity assessments shall be carried out in a proportionate manner, avoiding unnecessary burdens for economic operators. Conformity assessment bodies shall perform their activities taking due account of the size of undertakings, in particular as regards microenterprises and small and medium-sized enterprises, the sector in which they operate, their structure, their degree of complexity and the cybersecurity risk level of the products with digital elements and technology in question and the mass or serial nature of the production process.

3. ただし，指定組織は，デジタルの要素をもつ製品のこの規則の遵守のために要求される厳格さの程度及び保護のレベルを尊重する。

Notified bodies shall however respect the degree of rigour and the level of protection required for the compliance of products with digital elements with this Regulation.

4. 別紙 I の中で定められた要件または第 27 条に示す整合化された技術標準もしくは共通仕様と対応する要件が製造者によって適合されていなかったと指定組織が判断するときは，その指定組織は，

当該製造者に対し，適切な解消の方策をとることを要求し，かつ，適合性証明書を発行しない。

Where a notified body finds that the requirements set out in Annex I or in corresponding harmonised standards or common specifications as referred to in Article 27 have not been met by a manufacturer, it shall require that manufacturer to take appropriate corrective measures and shall not issue a certificate of conformity.

5. 証明書の発行後の適合性監視の過程において，デジタルの要素をもつ製品がこの規則の中で定められた要件を遵守しなくなったと指定組織が判断するときは，その指定組織は，その製造者に対し，適切な解消の方策をとることを要求し，かつ，必要があれば，その証明書を停止しまたは取消す。

Where, in the course of the monitoring of conformity following the issuance of a certificate, a notified body finds that a product with digital elements no longer complies with the requirements laid down in this Regulation, it shall require the manufacturer to take appropriate corrective measures and shall suspend or withdraw the certificate if necessary.

6. 解消の方策がとられない場合，または，要求された効果をもたない場合，指定組織は，しかるべく，証明書を制限し，停止しまたは取消す。

Where corrective measures are not taken or do not have the required effect, the notified body shall restrict, suspend or withdraw any certificates, as appropriate.

第 48 条　指定組織の判定に対する不服申立て

Article 48 **Appeal against decisions of notified bodies**

構成国は，指定組織の判定に対する不服申立て手続が利用できることを確保する。

Member States shall ensure that an appeal procedure against decisions of the notified bodies is available.

第 49 条　指定組織が負う情報提供義務

Article 49 **Information obligation on notified bodies**

1. 指定組織は，通知元当局に対し，以下のことを連絡する：

Notified bodies shall inform the notifying authority of the following:

(a) 証明書の拒否，制限，停止または取消し；

any refusal, restriction, suspension or withdrawal of a certificate;

(b) 通知の適用範囲及び通知のための条件に影響を与える事情；

any circumstances affecting the scope of and conditions for notification;

(c) 適合性評価活動と関連して市場監視当局から当該指定組織が受けた情報提供を求める要請；

any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

(d) 求めに応じて，国境を越える活動及び再委託を含め，当該指定組織の通知の適用範囲内で遂行された適合性評価活動及びそれ以外の遂行された活動。

on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. 指定組織は，同じデジタルの要素をもつ製品を包摂する類似の適合性評価活動を実施しており，この規則の下において通知された他の組織に対し，否定的な適合性評価結果と関連する問題，及び，要請に応じて，積極的な適合性評価結果と関連する問題に関する適格な情報を提供する。

Notified bodies shall provide the other bodies notified under this Regulation carrying out similar conformity assessment activities covering the same products with digital elements with relevant information on issues relating to negative and, upon request, positive conformity assessment results.

第 50 条 経験の交換

Article 50 **Exchange of experience**

欧州委員会は，通知の基本方針に関して職責を負う構成国の国内当局の間において経験を交換する組織を定める。

The Commission shall provide for the organisation of the exchange of experience between the Member States' national authorities responsible for notification policy.

第 51 条 指定組織の調整

Article 51 **Coordination of notified bodies**

1. 欧州委員会は，指定組織間の適切な調整及び協力が，指定組織の部門横断のグループという形態で設けられかつ適正に運用されることを確保する。

The Commission shall ensure that appropriate coordination and cooperation between notified bodies are put in place and properly operated in the form of a cross-sectoral group of notified bodies.

2. 構成国は，その構成国によって通知された組織が，直接にまたは指定された代理者により，同グループの作業に参加することを確保する。

Member States shall ensure that the bodies notified by them participate in the work of that group, directly or by means of designated representatives.

第V章 市場の監視及び執行
Chapter V **Market Surveillance and Enforcement**

第 52 条 欧州連合の市場におけるデジタルの要素をもつ製品の市場監視及び監督
Article 52 **Market surveillance and control of products with digital elements in the Union market**

1. 規則(EU) 2019/1020 は，この規則の適用範囲内にあるデジタルの要素をもつ製品に対して適用される。

   Regulation (EU) 2019/1020 shall apply to products with digital elements that fall within the scope of this Regulation.

2. 各構成国は，この規則の実効的な実装を確保する目的のために，1 または複数の市場監視当局を指定する。構成国は，この規則のための市場監視当局として活動するために，既存の当局または新たな当局を指定できる。

   Each Member State shall designate one or more market surveillance authorities for the purpose of ensuring the effective implementation of this Regulation. Member States may designate an existing or new authority to act as market surveillance authority for this Regulation.

3. 本条の第 2 項の下において指定された市場監視当局は，第 24 条の中で定められたオープンソースソフトウェアスチュワードの義務との関係においても，市場監視活動を実施することに関する職責を負う。オープンソースソフトウェアスチュワードが同条の中で定められた義務を遵守していないと市場監視当局が判断するときは，その市場監視当局は，そのオープンソースソフトウェアスチュワードに対し，全ての適切な是正の活動が行われることを確保することを要求する。オープンソースソフトウェアスチュワードは，この規則の下にあるオープンソースソフトウェアスチュワードの義務の関係における全ての適切な是正の活動が行われることを確保する。

   The market surveillance authorities designated under paragraph 2 of this Article shall also be responsible for carrying out market surveillance activities in relation to the obligations for open-source software stewards laid down in Article 24. Where a market surveillance authority finds that an open-source software steward does not comply with the obligations set out in that Article, it shall require the open-source software steward to ensure that all appropriate corrective actions are taken. Open-source software stewards shall ensure that all appropriate corrective action is taken in respect of their obligations under this Regulation.

4. それが適格なときは，市場監視当局は，規則(EU) 2019/881 の第 58 条により指定された国内サイバーセキュリティ認証機関と協力し，かつ，定期的に情報交換する。この規則の第 14 条による報告義務の実装の監督に関しては，指定された市場監視当局は，調整者として指定された CSIRT 及び ENISA と協力し，かつ，定期的に情報交換する。

   Where relevant, the market surveillance authorities shall cooperate with the national cybersecurity certification

authorities designated pursuant to Article 58 of Regulation (EU) 2019/881 and exchange information on a regular basis. With respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, the designated market surveillance authorities shall cooperate and exchange information on a regular basis with the CSIRTs designated as coordinators and ENISA.

5. 市場監視当局は，調整者として指定された CSIRT または ENISA に対し，この規則の実装及び執行と関連する事項に関し，技術上の助言を提供することを要請できる。第 54 条の下において調査を実施する際，市場監視当局は，調整者として指定された CSIRT または ENISA に対し，デジタルの要素をもつ製品の遵守の評価を支えるための分析を提供することを要請できる。

The market surveillance authorities may request a CSIRT designated as coordinator or ENISA to provide technical advice on matters related to the implementation and enforcement of this Regulation. When conducting an investigation under Article 54, market surveillance authorities may request the CSIRT designated as coordinator or ENISA to provide an analysis to support evaluations of compliance of products with digital elements.

6. それが適格なときは，市場監視当局は，この規則以外の欧州連合整合化立法を基礎として指定された他の市場監視当局と協力し，かつ，定期的に情報を交換する。

Where relevant, the market surveillance authorities shall cooperate with other market surveillance authorities designated on the basis of Union harmonisation legislation other than this Regulation, and exchange information on a regular basis.

7. 市場監視当局は，しかるべく，欧州連合のデータ保護法の執行を監督する機関と協力する。そのような協力は，そのようなガイド及び助言が個人データの処理と関係するときは第 10 項によるガイド及び助言を発行する際を含め，当該機関に対し，その機関の職務権限を満たすことのために適格な判定結果を連絡することを含む。

Market surveillance authorities shall cooperate, as appropriate, with the authorities supervising Union data protection law. Such cooperation includes informing those authorities of any finding relevant for the fulfilment of their competences, including when issuing guidance and advice pursuant to paragraph 10 if such guidance and advice concerns the processing of personal data.

欧州連合のデータ保護法の執行を監督する機関は，その機関の職務を満たすための当該文書へのアクセスが必要なときは，この規則の下において作成または維持管理された文書を要求する権限及びそれらの文書にアクセスする権限をもつ。その機関は，関係する構成国の指定された市場監視当局に対し，そのような要求を連絡する。

Authorities supervising Union data protection law shall have the power to request and access any documentation created or maintained under this Regulation when access to that documentation is necessary for the fulfilment of their tasks. They shall inform the designated market surveillance authorities of the Member State concerned of any such request.

8. 構成国は，指定された市場監視当局が，それが適切なときは自動化ツールによる処理を含め，資金上及び技術上の十分な資源の提供を受けること，並びに，この規則の下にある市場監視当局の職務を満たすために必要となるサイバーセキュリティ上の技能をもつ人的資源の提供を受けることを確保する。

Member States shall ensure that the designated market surveillance authorities are provided with adequate financial and technical resources, including, where appropriate, processing automation tools, as well as with human resources with the necessary cybersecurity skills to fulfil their tasks under this Regulation.

9. 欧州委員会は，指定された市場監視当局の間における経験の交換を推進しかつ促進する。

The Commission shall encourage and facilitate the exchange of experience between designated market surveillance authorities.

10. 市場監視当局は，欧州委員会の支援を得て，また，それが適切なときは CSIRT 及び ENISA の支援を得て，経済取引主体に対し，この規則の実装に関し，ガイド及び助言を提供できる。

Market surveillance authorities may provide guidance and advice to economic operators on the implementation of this Regulation, with the support of the Commission and, where appropriate, CSIRTs and ENISA.

11. 市場監視当局は，消費者に対し，規則(EU) 2019/1020 の第 11 条に従って，この規則の不遵守を示し得る苦情をどこに提出するかについて情報提供し，また，消費者に対し，デジタルの要素をもつ製品に対して影響を与えるかもしれない脆弱性，インシデント及びサイバーな脅威の通報を容易にするための仕組みがどこにあるのか，その仕組みに対してどのようにアクセスするのかに関する情報も提供する。

Market surveillance authorities shall inform consumers of where to submit complaints that could indicate non-compliance with this Regulation, in accordance with Article 11 of Regulation (EU) 2019/1020, and shall provide information to consumers on where and how to access mechanisms to facilitate reporting of vulnerabilities, incidents and cyber threats that may affect products with digital elements.

12. 市場監視当局は，それが適格なときは，科学技術の団体，調査研究の団体及び消費者団体を含め，適格な利害関係者との間の協力を促進する。

Market surveillance authorities shall facilitate, where relevant, the cooperation with relevant stakeholders, including scientific, research and consumer organisations.

13. 市場監視当局は，欧州委員会に対し，年次で，適格な市場監視活動の結果を報告する。指定された市場監視当局は，欧州委員会及び適格な国内競争当局に対し，遅滞なく，欧州連合の競争法の適用に対して潜在的に利害をもつかもしれない市場監視活動の過程で発見した情報を報告する。

The market surveillance authorities shall report to the Commission on an annual basis the outcomes of relevant market surveillance activities. The designated market surveillance authorities shall report, without delay, to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union competition law.

14. この規則の適用範囲内にあるデジタルの要素をもつ製品であって，規則(EU) 2024/1689 の第 6 条によって高リスク AI システムとして分類される製品に関し，同規則の目的のために指定された市場監視当局は，この規則の下において要求される市場監視活動に関する職責を負う機関であるものとする。規則(EU) 2024/1689 により指定された市場監視当局は，しかるべく，この規則により指定された市場監視当局と協力し，また，この規則の第 14 条による報告義務の実装の監視に関しては，調整者として指定された CSIRT 及び ENISA と協力する。規則(EU) 2024/1689 により指定された市場監視当局は，この規則により指定された市場監視当局に対し，とりわけ，この規則の実装との関係における当該当局の職務を満たすことのために適格な判定結果を連絡する。

For products with digital elements that fall within the scope of this Regulation which are classified as high-risk AI systems pursuant to Article 6 of Regulation (EU) 2024/1689, the market surveillance authorities designated for the purposes of that Regulation shall be the authorities responsible for market surveillance activities required under this Regulation. The market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 shall cooperate, as appropriate, with the market surveillance authorities designated pursuant to this Regulation and, with respect to the supervision of the implementation of the reporting obligations pursuant to Article 14 of this Regulation, with the CSIRTs designated as coordinators and ENISA. Market surveillance authorities designated pursuant to Regulation (EU) 2024/1689 shall in particular inform market surveillance authorities designated pursuant to this Regulation of any finding relevant for the fulfilment of their tasks in relation to the implementation of this Regulation.

15. 規則(EU) 2019/1020 の第 30 条第 2 項により，この規則の統一的な適用のため，ADCO が設けられる。ADCO は，指定された市場監視当局の代表，及び，それが適切なときは，単一連絡部局の代表によって構成される。ADCO は，オープンソースソフトウェアスチュワードに課される義務の関係において市場監視活動に関連する個別の事項にも対処する。

ADCO shall be established for the uniform application of this Regulation, pursuant to Article 30(2) of Regulation (EU) 2019/1020. ADCO shall be composed of representatives of the designated market surveillance authorities and, if appropriate, representatives of single liaison offices. ADCO shall also address specific matters related to the market surveillance activities in relation to the obligations placed on open-source software stewards.

16. 市場監視当局は，製造者が，当該製造者のデジタルの要素をもつ製品のサポート期間を決定する際に第 13 条第 8 項に示す基準をどのように適用したかを監視する。

Market surveillance authorities shall monitor how manufacturers have applied the criteria referred to in Article 13(8) when determining the support period of their products with digital elements.

ADCO は，公衆がアクセス可能でありかつユーザフレンドリな方式により，第 13 条第 8 項により製造者によって決定される平均サポート期間を含め，デジタルの要素をもつ製品の類型に関する適格な統計を公表し，また，デジタルの要素をもつ製品の類型の指標化されたサポート期間を含むガイドを提供する。

ADCO shall publish in a publicly accessible and user-friendly form relevant statistics on categories of products with digital elements, including average support periods, as determined by the manufacturer pursuant to Article 13(8), as well as provide guidance that includes indicative support periods for categories of products with digital elements.

特定の類型のデジタルの要素をもつ製品に関して，不適切なサポート期間であることをデータが示唆している場合，ADCO は，市場監視当局に対し，そのような類型のデジタルの要素をもつ製品に対してその市場監視当局の活動の焦点を当てることの勧告書を発行できる。

Where the data suggests inadequate support periods for specific categories of products with digital elements, ADCO may issue recommendations to market surveillance authorities to focus their activities on such categories of products with digital elements.

第 53 条　データ及び文書へのアクセス

Article 53 **Access to data and documentation**

デジタルの要素をもつ製品及びその製品の製造者によって設けられたプロセスの，別紙 I の中で定められた必須のサイバーセキュリティ要件の遵守を評価するために必要な場合において，市場監視当局は，理由を付した要請に応じて，適格な経済取引主体の関連内部文書を含め，そのような製品の設計，開発，製造及び脆弱性の取扱いを評価するために要求されるデータに対するその市場監視当局によって容易に理解可能な言語によるアクセスが与えられる。

Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential cybersecurity requirements set out in Annex I, the market surveillance authorities shall, upon a reasoned request, be granted access to the data, in a language easily understood by them, required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the relevant economic operator.

第 54 条　サイバーセキュリティ上の大きなリスクを示しているデジタルの要素をもつ製品に関する国内レベルの手続

Article 54 **Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk**

1.　構成国の市場監視当局が，当該製品の脆弱性の取扱いを含め，デジタルの要素をもつ製品がサイ

バーセキュリティ上の大きなリスクを示していると判断する十分な理由をもつときは，その市場監視当局は，不適切な遅滞なく，かつ，それが適切なときは，適格な CSIRT と協力して，この規則の中で定められた全ての要件のその製品の遵守との関係において，関係するデジタルの要素をもつ製品の評価を実施する。適格な経済取引主体は，必要に応じて，当該市場監視当局に協力する。

Where the market surveillance authority of a Member State has sufficient reason to consider that a product with digital elements, including its vulnerability handling, presents a significant cybersecurity risk, it shall, without undue delay and, where appropriate, in cooperation with the relevant CSIRT, carry out an evaluation of the product with digital elements concerned in respect of its compliance with all the requirements laid down in this Regulation. The relevant economic operators shall cooperate with the market surveillance authority as necessary.

市場監視当局が，当該評価の過程において，デジタルの要素をもつ製品がこの規則の中で定められた要件を遵守していないと判断するときは，その市場監視当局は，遅滞なく，適格な経済取引主体に対し，その市場監視当局が定め得るように，そのサイバーセキュリティ上のリスクの性質に応じて，そのデジタルの要素をもつ製品が当該要件を遵守するようにさせるための全ての適切な解消の方策を講ずること，合理的な期間内に，その製品を市場から回収することまたはその製品をリコールすることを要求する。

Where, in the course of that evaluation, the market surveillance authority finds that the product with digital elements does not comply with the requirements laid down in this Regulation, it shall without delay require the relevant economic operator to take all appropriate corrective actions to bring the product with digital elements into compliance with those requirements, to withdraw it from the market, or to recall it within a reasonable period, commensurate with the nature of the cybersecurity risk, as the market surveillance authority may prescribe.

市場監視当局は，適格な指定組織に対し，しかるべく連絡する。規則(EU) 2019/1020 の第 18 条は，解消の方策に対して適用される。

The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the corrective actions.

2. 本条の第 1 項に示すサイバーセキュリティ上のリスクの大きさを判定する際，市場監視当局は，非技術的なリスク要素，とりわけ，指令(EU) 2022/2555 の第 22 条に従って実施された不可欠なサプライチェーンの欧州連合レベルの調整されたセキュリティリスク評価の結果として確定されたリスク要素も判断する。非技術的なリスク要素に照らしてデジタルの要素をもつ製品がサイバーセキュリティ上の大きなリスクを示していると判断する十分な理由を市場監視当局がもつときは，その市場監視当局は，指令(EU) 2022/2555 の第 8 条によって指定されまたは設置された職務権限のある機関に対して連絡し，かつ，必要に応じてそれらの機関と協力する。

When determining the significance of a cybersecurity risk referred to in paragraph 1 of this Article, the market surveillance authorities shall also consider non-technical risk factors, in particular those established as a result of Union

level coordinated security risk assessments of critical supply chains carried out in accordance with Article 22 of Directive (EU) 2022/2555. Where a market surveillance authority has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary.

3. 不遵守が当該市場監視当局の国内領土に限定されていないと市場監視当局が判断するときは，その市場監視当局は，欧州委員会及び他の構成国に対し，その評価の結果及びその市場監視当局が当該経済取引主体に対して行うように要求した行動を連絡する。

Where the market surveillance authority considers that non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States of the results of the evaluation and of the actions which it has required the economic operator to take.

4. 経済取引主体は，当該経済取引主体が欧州連合全域にわたって市場において利用できるようにした関係する全てのデジタルの要素をもつ製品との関係において，全ての適切な解消の方策をとることを確保する。

The economic operator shall ensure that all appropriate corrective action is taken in respect of all the products with digital elements concerned that it has made available on the market throughout the Union.

5. 第 1 項第 2 副項に示す期間内に経済取引主体が適切な解消の方策をとらないときは，市場監視当局は，当該デジタルの要素をもつ製品を当該市場監視当局の国内市場において利用できるようにすることを禁止もしくは制限し，同市場からその製品を回収しまたはその製品をリコールするための全ての適切な暫定措置を講ずる。

Where the economic operator does not take adequate corrective action within the period referred to in paragraph 1, second subparagraph, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict that product with digital elements from being made available on its national market, to withdraw it from that market or to recall it.

その当局は，遅滞なく，欧州委員会及び他の構成国に対し，当該措置を通知する。

That authority shall notify the Commission and the other Member States, without delay, of those measures.

6. 第 5 項に示す情報は，利用可能な全ての詳細情報を含めるものとし，とりわけ，不遵守のデジタルの要素をもつ製品の識別のために必要となるデータ，当該デジタルの要素をもつ製品の原産地，主張された不遵守の性質及び包含されているリスク，講じられた国内措置の性質及び期間並びに適格な経済取引主体から提出された主張を含めるものとする。とりわけ，市場監視当局は，その不遵守が以下の 1 または複数の事由によるものかどうかを示す：

The information referred to in paragraph 5 shall include all available details, in particular the data necessary for the identification of the non-compliant product with digital elements, the origin of that product with digital elements, the nature of the alleged non-compliance and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant economic operator. In particular, the market surveillance authority shall indicate whether the non-compliance is due to one or more of the following:

(a) そのデジタルの要素をもつ製品またはその製造者によって設けられたプロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件に適合していないこと;

a failure of the product with digital elements or of the processes put in place by the manufacturer to meet the essential cybersecurity requirements set out in Annex I;

(b) 第 27 条に示す整合化された技術標準, 欧州サイバーセキュリティ認証制度または共通仕様の中にある欠点。

shortcomings in the harmonised standards, European cybersecurity certification schemes or common specifications, as referred to in Article 27.

7. 手続を開始する構成国の市場監視当局以外の構成国の市場監視当局は, 遅滞なく, 欧州委員会及び他の構成国に対し, 採択された措置及び関係するデジタルの要素をもつ不遵守製品と関連してその市場監視当局が自由に利用できる付加的な情報を連絡し, また, 通知された国内措置に不同意のときは, その市場監視当局の異議を連絡する。

The market surveillance authorities of the Member States other than the market surveillance authority of the Member State initiating the procedure shall without delay inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the product with digital elements concerned, and, in the event of disagreement with the notified national measure, of their objections.

8. 本条の第 5 項に示す通知の受領から 3 か月以内に, 構成国によって講じられた暫定措置に関して構成国または欧州委員会からいかなる異議も提起されなかったときは, 当該措置は, 正当なものとみなされる。このことは, 規則(EU) 2019/1020 の第 18 条に従った関係経済取引主体の手続上の権利を妨げない。

Where, within three months of receipt of the notification referred to in paragraph 5 of this Article, no objection has been raised by either a Member State or the Commission in respect of a provisional measure taken by a Member State, that measure shall be deemed to be justified. This is without prejudice to the procedural rights of the economic operator concerned in accordance with Article 18 of Regulation (EU) 2019/1020.

9. 全ての構成国の市場監視当局は, 関係するデジタルの要素をもつ製品との関係において, 当該製品のその構成国の市場からの回収のような適切な制限措置が遅滞なく講じられることを確保する。

The market surveillance authorities of all Member States shall ensure that appropriate restrictive measures are taken in respect of the product with digital elements concerned, such as withdrawal of that product from their market, without delay.

第 55 条 欧州連合の安全確保手続

Article 55 **Union safeguard procedure**

1. 第 54 条第 5 項に示す通知の受領から 3か月以内に, 他の構成国によって講じられた措置に反対し構成国から異議が提起される場合, または, その措置が欧州連合法に反すると欧州委員会が判断する場合, 欧州委員会は, 遅滞なく, 適格な構成国及び 1 または複数の経済取引主体からの意見聴取に入り, かつ, その国内措置を評価する。同評価の結果を基礎として, 欧州委員会は, 第 54 条第 5 項に示す通知から 9 か月以内に, その国内措置が正当化されるか否かを決定し, かつ, 関係する構成国に対し, 当該決定を通知する。

Where, within three months of receipt of the notification referred to in Article 54(5), objections are raised by a Member State against a measure taken by another Member State, or where the Commission considers the measure to be contrary to Union law, the Commission shall without delay enter into consultation with the relevant Member State and the economic operator or operators and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not within nine months from the notification referred to in Article 54(5) and notify that decision to the Member State concerned.

2. 国内措置が正当であると判断されるときは, 全ての構成国は, デジタルの要素をもつ不遵守製品がその構成国の市場から回収されることを確保するために必要となる措置を講じ, かつ, 欧州委員会に対し, しかるべく連絡する。国内措置が正当ではないと判断されるときは, 関係する構成国は, その措置を取消す。

If the national measure is considered to be justified, all Member States shall take the measures necessary to ensure that the non-compliant product with digital elements is withdrawn from their market, and shall inform the Commission accordingly. If the national measure is not considered to be justified, the Member State concerned shall withdraw the measure.

3. 国内措置が正当であると判断され, かつ, そのデジタルの要素をもつ製品の不遵守が整合化された技術標準の中にある欠点に起因するときは, 欧州委員会は, 規則(EU) No 1025/2012 の第 11 条の中で定められた手続を適用する。

Where the national measure is considered to be justified and the non-compliance of the product with digital elements is attributed to shortcomings in the harmonised standards, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

4. 国内措置が正当であると判断され，かつ，そのデジタルの要素をもつ製品の不遵守が第 27 条に示す欧州サイバーセキュリティ認証制度の中にある欠点に起因するときは，欧州委員会は，第 27 条第 9 項により採択された同認証制度と関係する適合性の推定の細目を定める委任される行為を改正または廃止するかどうかを判断する。

Where the national measure is considered to be justified and the non-compliance of the product with digital elements is attributed to shortcomings in a European cybersecurity certification scheme as referred to in Article 27, the Commission shall consider whether to amend or repeal any delegated act adopted pursuant to Article 27(9) that specifies the presumption of conformity concerning that certification scheme.

5. 国内措置が正当であると判断され，かつ，そのデジタルの要素をもつ製品の不遵守が第 27 条に示す共通仕様の中にある欠点に起因するときは，欧州委員会は，第 27 条第 2 項により採択された当該共通仕様を定めている実装行為を改正または廃止するかどうかを判断する。

Where the national measure is considered to be justified and the non-compliance of the product with digital elements is attributed to shortcomings in common specifications as referred to in Article 27, the Commission shall consider whether to amend or repeal any implementing act adopted pursuant to Article 27(2) setting out those common specifications.

第 56 条 サイバーセキュリティ上の大きなリスクを示しているデジタルの要素をもつ製品に関する欧州連合レベルの手続

Article 56 **Procedure at Union level concerning products with digital elements presenting a significant cybersecurity risk**

1. ENISA から提供された情報を基礎とする場合を含め，サイバーセキュリティ上の大きなリスクを示すデジタルの要素をもつ製品がこの規則の中で定められた要件を遵守していないと判断する十分な理由を欧州委員会がもつときは，欧州委員会は，適格な市場監視当局に対して連絡する。デジタルの要素をもつ製品のこの規則の中で定められた要件の遵守との関係において，サイバーセキュリティ上の大きなリスクを示しているかもしれない当該製品の評価を市場監視当局が実施するときは，第 54 条及び第 55 条に示す手続が適用される。

Where the Commission has sufficient reason to consider, including based on information provided by ENISA, that a product with digital elements that presents a significant cybersecurity risk does not comply with the requirements laid down in this Regulation, it shall inform the relevant market surveillance authorities. Where the market surveillance authorities carry out an evaluation of that product with digital elements that may present a significant cybersecurity risk in respect of its compliance with the requirements laid down in this Regulation, the procedures referred to in Articles 54 and 55 shall apply.

2. デジタルの要素をもつ製品が非技術的なリスク要素に照らしてサイバーセキュリティ上の大きなリスクを示していると判断する十分な理由を欧州委員会がもつときは，欧州委員会は，適格な市場監視当

局に対し，及び，それが適切なときは，指令(EU) 2022/2555 の第 8 条によって指定または設置された職務権限のある機関に対して連絡し，かつ，必要に応じて，それらの機関と協力する。指令(EU) 2022/2555 の第 22 条の中で定められた不可欠なサプライチェーンの欧州連合レベルの調整されたセキュリティリスク評価と関連する欧州委員会の職務を考慮して，当該デジタルの要素をもつ製品に関して発見されたリスクの適格性も判断し，かつ，必要に応じて，指令(EU) 2022/2555 の第 14 条によって設けられた協力グループ及び ENISA から意見聴取する。

Where the Commission has sufficient reason to consider that a product with digital elements presents a significant cybersecurity risk in light of non-technical risk factors, it shall inform the relevant market surveillance authorities and, where appropriate, the competent authorities designated or established pursuant to Article 8 of Directive (EU) 2022/2555 and cooperate with those authorities as necessary. The Commission shall also consider the relevance of the identified risks for that product with digital elements in view of its tasks regarding the Union level coordinated security risk assessments of critical supply chains provided for in Article 22 of Directive (EU) 2022/2555, and consult, as necessary, the Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and ENISA.

3. 域内市場の適正な稼働を維持するための即時の介入が正当化される状況下において，かつ，第 1 項に示すデジタルの要素をもつ製品がこの規則の中で定められた要件を不遵守のままであり，かつ，適格な市場監督当局によって実効的な措置が何ら講じられなかったと判断する十分な理由を欧州委員会がもつときは，欧州委員会は，遵守の評価を実施し，また，ENISA に対し，その評価を支援するための分析を提供することを要請できる。欧州委員会は，適格な市場監督当局に対し，しかるべく連絡する。適格な経済取引主体は，必要に応じて ENISA と協力する。

In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 1 remains non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the relevant market surveillance authorities, the Commission shall carry out an evaluation of compliance and may request ENISA to provide an analysis to support it. The Commission shall inform the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate with ENISA as necessary.

4. 第 3 項に示す評価を基礎として，欧州委員会は，欧州連合レベルで是正措置または制限措置が必要であると決定できる。その目的のために，欧州委員会は，遅滞なく，関係する構成国及び適格な 1 または複数の経済取引主体から意見聴取する。

Based on the evaluation referred to in paragraph 3, the Commission may decide that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

5. 本条の第 4 項に示す意見聴取を基礎として，欧州委員会は，そのリスクの性質に応じて，合理的な期間内に，関係するデジタルの要素をもつ製品が市場から回収されることまたはリコールされることを要求することを含め，欧州連合レベルの是正措置または制限措置を定めるための実装行為を採

択できる。それらの実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

On the basis of the consultation referred to in paragraph 4 of this Article, the Commission may adopt implementing acts to provide for corrective or restrictive measures at Union level, including requiring the products with digital elements concerned to be withdrawn from the market or recalled, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

6. 欧州委員会は，直ちに，適格な 1 または複数の経済取引主体に対し，第 5 項に示す実装行為を通知する。構成国は，遅滞なく，それらの実装行為を実装し，かつ，欧州委員会に対し，しかるべく連絡する。

The Commission shall immediately communicate the implementing acts referred to in paragraph 5 to the relevant economic operator or operators. Member States shall implement those implementing acts without delay and shall inform the Commission accordingly.

7. 第 3 項ないし第 6 項は，欧州委員会の介入が正当化される例外的な状況の間だけ，関係するデジタルの要素をもつ製品がこの規則を遵守するようにされてないことを条件として，適用される。

Paragraphs 3 to 6 shall be applicable for the duration of the exceptional situation that justified the Commission's intervention, provided that the product with digital elements concerned is not brought in compliance with this Regulation.

第 57 条　サイバーセキュリティ上の大きなリスクを示すデジタルの要素をもつ遵守製品

Article 57 **Compliant products with digital elements which present a significant cybersecurity risk**

1. 構成国の市場監視当局は，第 54 条の下にある評価を遂行した上で，デジタルの要素をもつ製品及びその製造者によって設けられたプロセスがこの規則を遵守しておりながら，それでもサイバーセキュリティ上の大きなリスク及び以下の事柄に対するリスクを示しているとその市場監視当局が判断するときは，経済取引主体に対し，全ての適切な方策をとることを要求する：

The market surveillance authority of a Member State shall require an economic operator to take all appropriate measures where, having performed an evaluation under Article 54, it finds that although a product with digital elements and the processes put in place by the manufacturer are in compliance with this Regulation, they present a significant cybersecurity risk as well as a risk to:

(a) 個人の健康もしくは安全；

the health or safety of persons;

(b) 基本的な権利を保護することを意図する欧州連合法もしくは国内法の下における義務の遵守；

the compliance with obligations under Union or national law intended to protect fundamental rights;

(c) 指令(EU) 2022/2555 の第 3 条第 1 項に示す基礎法主体から電子情報システムを用いて提供されるサービスの可用性，真正性，完全性もしくは機密性；または

the availability, authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities as referred to in Article 3(1) of Directive (EU) 2022/2555; or

(d) それら以外の側面の公共の利益の保護。

other aspects of public interest protection.

第 1 副項に示す方策は，関係するデジタルの要素をもつ製品及びその製造者によって設けられたプロセスが，市場において利用できるようにされる際には当該リスクを示さなくなっていることを確保するための措置，関係するデジタルの要素をもつ製品の市場から回収することまたはその製品をリコールすることを含み得るものとし，かつ，当該リスクの性質に対応するものとする。

The measures referred to in the first subparagraph may include measures to ensure that the product with digital elements concerned and the processes put in place by the manufacturer no longer present the relevant risks when made available on the market, withdrawal from the market of the product with digital elements concerned, or recalling of it, and shall be commensurate with the nature of those risks.

2. 製造者またはそれ以外の適格な経済取引主体は，第 1 項に示す構成国の市場監視当局によって定められた期限内に，その製造者またはそれ以外の経済取引主体が欧州全域にわたり市場において利用できるようにしたデジタルの要素をもつ製品との関係において，解消の方策がとられることを確保する。

The manufacturer or other relevant economic operators shall ensure that corrective action is taken in respect of the products with digital elements concerned that they have made available on the market throughout the Union within the timeline established by the market surveillance authority of the Member State referred to in paragraph 1.

3. 構成国は，直ちに，欧州委員会及び他の構成国に対し，第 1 項によりとられた方策に関して連絡する。その情報は，全ての利用可能な詳細情報を含めるものとし，とりわけ，関係するデジタルの要素をもつ製品の特定のために必要となるデータ，当該デジタルの要素をもつ製品の原産地及びサプライチェーン，包含されているリスクの性質並びに講じられた国内措置の性質及び期間を含めるものとする。

The Member State shall immediately inform the Commission and the other Member States about the measures taken pursuant to paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the products with digital elements concerned, the origin and the supply chain of those products with digital elements, the nature of the risk involved and the nature and duration of the national measures taken.

4. 欧州委員会は，遅滞なく，構成国及び適格な経済取引主体からの意見聴取に入り，かつ，講じられた国内措置を評価する。同評価の結果を基礎として，欧州委員会は，その措置が正当化されるか否かを決定し，かつ，それが必要なときは，適切な措置を提案する。

The Commission shall without delay enter into consultation with the Member States and the relevant economic operator and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified or not and, where necessary, propose appropriate measures.

5. 欧州委員会は，構成国宛に第 4 項に示す決定を発出する。

The Commission shall address the decision referred to in paragraph 4 to the Member States.

6. ENISA から提供された情報を基礎とする場合を含め，デジタルの要素をもつ製品がこの規則を遵守しておりながら，それでも本条の第 1 項に示すリスクを示していると判断する十分な理由を欧州委員会がもつときは，欧州委員会は，1 または複数の適格な市場監視当局に対して連絡し，かつ，評価を実施すること，また，第 54 条並びに本条の第 1 項，第 2 項及び第 3 項に示す手続に従うことを要求できる。

Where the Commission has sufficient reason to consider, including based on information provided by ENISA, that a product with digital elements, although compliant with this Regulation, presents the risks referred to in paragraph 1 of this Article, it shall inform and may request the relevant market surveillance authority or authorities to carry out an evaluation and follow the procedures referred to in Article 54 and in paragraphs 1, 2 and 3 of this Article.

7. 域内市場の適正な稼働を維持するための即時の介入が正当化される状況下において，かつ，第 6 項に示すデジタルの要素をもつ製品が第 1 項に示すリスクを示し続けており，かつ，適格な国内市場監督当局によって実効的な措置が講じられなかったと判断する十分な理由を欧州委員会がもつときは，欧州委員会は，当該デジタルの要素をもつ製品によって示されているリスクの評価を実施し，また，ENISA に対し，その評価を支援するための分析を提供することを要請でき，かつ，適格な市場監督当局に対してしかるべく連絡する。適格な経済取引主体は，必要に応じて ENISA と協力する。

In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the product with digital elements referred to in paragraph 6 continues to present the risks referred to in paragraph 1, and no effective measures have been taken by the relevant national market surveillance authorities, the Commission shall carry out an evaluation of the risks presented by that product with digital elements and may request ENISA to provide an analysis to support that evaluation and shall inform

the relevant market surveillance authorities accordingly. The relevant economic operators shall cooperate with ENISA as necessary.

8. 第 7 項に示す評価を基礎として，欧州委員会は，欧州連合レベルで是正措置または制限措置が必要であると決定できる。その目的のために，欧州委員会は，遅滞なく，関係する構成国及び適格な 1 または複数の経済取引主体から意見聴取する。

Based on the evaluation referred to in paragraph 7, the Commission may establish that a corrective or restrictive measure is necessary at Union level. To that end, it shall without delay consult the Member States concerned and the relevant economic operator or operators.

9. 本条の第 8 項に示す意見聴取を基礎として，欧州委員会は，そのリスクの性質に応じて，合理的な期間内に，関係するデジタルの要素をもつ製品が市場から回収されることまたはリコールされることを要求することを含め，欧州連合レベルの是正措置または制限措置を決定するための実装行為を採択できる。それらの実装行為は，第 62 条第 2 項に示す審議手続に従って採択される。

On the basis of the consultation referred to in paragraph 8 of this Article, the Commission may adopt implementing acts to decide on corrective or restrictive measures at Union level, including requiring the products with digital elements concerned to be withdrawn from the market, or recalled, within a reasonable period, commensurate with the nature of the risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 62(2).

10. 欧州委員会は，直ちに，適格な 1 または複数の経済取引主体に対し，第 9 項に示す実装行為を通知する。構成国は，遅滞なく，それらの実装行為を実装し，かつ，欧州委員会に対し，しかるべく連絡する。

The Commission shall immediately communicate the implementing acts referred to in paragraph 9 to the relevant economic operator or operators. Member States shall implement those implementing acts without delay and shall inform the Commission accordingly.

11. 第 6 項ないし第 10 項は，欧州委員会の介入が正当化される例外的な状況の間だけ，かつ，関係するデジタルの要素をもつ製品が第 1 項に示すリスクを示している間だけ，適用される。

Paragraphs 6 to 10 shall apply for the duration of the exceptional situation that justified the Commission's intervention and for as long as the product with digital elements concerned continues to present the risks referred to in paragraph 1.

第 58 条　形式的な不遵守

Article 58 **Formal non-compliance**

1. 構成国の市場監視当局が以下のいずれかの判断を行うときは，その市場監視当局は，適格な製造者に対し，関係する不遵守を終了させることを要求する:

Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant manufacturer to put an end to the non-compliance concerned:

(a) 第 29 条及び第 30 条に違反して CE マークが付された;

the CE marking has been affixed in violation of Articles 29 and 30;

(b) CE マークが付されなかった;

the CE marking has not been affixed;

(c) EU 適合宣言書が作成されなかった;

the EU declaration of conformity has not been drawn up;

(d) EU 適合宣言書が正確に作成されなかった;

the EU declaration of conformity has not been drawn up correctly;

(e) それが適用可能なときは，適合性評価手続に関与する指定組織の識別番号が付されなかった;

the identification number of the notified body which is involved in the conformity assessment procedure, where applicable, has not been affixed;

(f) 技術文書が利用できないまたは完全ではない。

the technical documentation is either not available or not complete.

2. 第 1 項に示す不遵守が持続するときは，関係する構成国は，そのデジタルの要素をもつ製品が市場において利用できるようにされることを制限もしくは禁止するための全ての適切な措置を講じ，または，その製品がリコールされもしくは市場から回収されることを確保する。

Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the product with digital elements from being made available on the market or ensure that it is recalled or withdrawn from the market.

第 59 条 市場監視当局の共同活動

Article 59 **Joint activities of market surveillance authorities**

1. 市場監視当局は，他の適格な当局との間で，市場に置かれているまたは市場において利用できるようにされている個々のデジタルの要素をもつ製品に関し，とりわけ，サイバーセキュリティ上のリスクを示しているとしばしば判断されるデジタルの要素をもつ製品に関し，サイバーセキュリティ及び消費者保護を確保することを狙いとする共同活動を実施することを合意できる。

Market surveillance authorities may agree with other relevant authorities to carry out joint activities aimed at ensuring cybersecurity and the protection of consumers with respect to specific products with digital elements placed on the market or made available on the market, in particular products with digital elements that are often found to present cybersecurity risks.

2. 欧州委員会または ENISA は，この規則の適用範囲内にあるデジタルの要素をもつ製品の，この規則の中で定められた要件の複数の構成国にわたる潜在的な不遵守の兆候または情報を基礎として市場監視当局によって実施されるこの規則の遵守の点検のための共同活動を提案する。

The Commission or ENISA shall propose joint activities for checking compliance with this Regulation to be conducted by market surveillance authorities based on indications or information of potential non-compliance across several Member States of products with digital elements that fall within the scope of this Regulation with the requirements laid down in this Regulation.

3. 市場監視当局，及び，それが適用可能なときは，欧州委員会は，共同活動を実施するための合意が，経済取引主体間の不公正な競争を導かないこと，また，その合意への参加者の客観性，独立性及び公平性に対して負の影響を与えないことを確保する。

The market surveillance authorities and, where applicable, the Commission, shall ensure that the agreement to carry out joint activities does not lead to unfair competition between economic operators and does not negatively affect the objectivity, independence and impartiality of the parties to the agreement.

4. 市場監視当局は，その市場監視当局が行う調査の一部として実施された共同活動の結果として得られた情報を利用できる。

A market surveillance authority may use any information obtained as a result of the joint activities carried out as part of any investigation that it undertakes.

5. 関係する市場監視当局，及び，それが適用可能なときは，欧州委員会は，関与する関係者の名称を含め，共同活動に関する合意を公表する。

The market surveillance authority concerned and, where applicable, the Commission, shall make the agreement on

joint activities, including the names of the parties involved, available to the public.

第 60 条 スウィープ
Article 60 **Sweeps**

1. 市場監視当局は，この規則の遵守を点検するため，または，この規則の違反を検知するため，特定のデジタルの要素をもつ製品またはその類型の調整された同時監督活動（「スウィープ」）を行う。それらのスウィープは，識別子が隠された状態で入手されたデジタルの要素をもつ製品の検査を含め得る。

Market surveillance authorities shall conduct simultaneous coordinated control actions (sweeps) of particular products with digital elements or categories thereof to check compliance with or to detect infringements to this Regulation. Those sweeps may include inspections of products with digital elements acquired under a cover identity.

2. 関与する市場監督機関によって別異に合意されていない限り，スウィープは，欧州委員会によって調整される。スウィープの調整者は，それが適切なときは，集約された結果を公表する。

Unless otherwise agreed upon by the market surveillance authorities involved, sweeps shall be coordinated by the Commission. The coordinator of the sweep shall, where appropriate, make the aggregated results publicly available.

3. 第 14 条第 1 項及び第 3 項によって受領した通知を基礎とする場合を含め，ENISA の職務の遂行において，それに対してスウィープが準備され得る類型のデジタルの要素をもつ製品を発見したときは，ENISA は，市場監視当局の検討のため，本条の第 2 項に示す調整者に対し，スウィープを求める提案書を提出する。

Where, in the performance of its tasks, including based on the notifications received pursuant to Article 14(1) and (3), ENISA identifies categories of products with digital elements for which sweeps may be organised, it shall submit a proposal for a sweep to the coordinator referred to in paragraph 2 of this Article for the consideration of the market surveillance authorities.

4. スウィープを行う際，関与する市場監視当局は，第 52 条ないし第 58 条に定める調査権限及び国内法によってその市場監視当局に対して与えられているその他の権限を用い得る。

When conducting sweeps, the market surveillance authorities involved may use the investigation powers set out in Articles 52 to 58 and any other powers conferred upon them by national law.

5. 市場監視当局は，スウィープへの参加のため，欧州委員会の官吏，及び，欧州委員会によって権限を与えられた官吏以外の随行者を招請し得る。

Market surveillance authorities may invite Commission officials, and other accompanying persons authorised by the Commission, to participate in sweeps.

第 VI 章　委任される権限及び委員会の手続
Chapter VI **Delegated Powers and Committee Procedure**

第 61 条　委任の実行
Article 61 **Exercise of the delegation**

1. 委任される行為を採択する権限は，本条の中で定められた条件に従い，欧州委員会に対して与えられる。

   The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. 第 2 条第 5 項第 2 副項，第 7 条第 3 項，第 8 条第 1 項及び第 2 項，第 13 条第 8 項第 4 副項，第 14 条第 9 項，第 25 条，第 27 条第 9 項，第 28 条第 5 項及び第 31 条第 5 項に示す委任される行為を採択する権限は，2024 年 12 月 10 日から 5 年間，欧州委員会に対して与えられる。欧州委員会は，遅くともその 5 年間の最終日よりも 9 か月前までに，権限の委任と関係する報告書を作成する。各期間の最終日から遅くとも 3 か月前までに欧州議会または理事会がそのような延長に異議を述べない限り，権限の委任は，黙示で，同じ期間で延長される。

   The power to adopt delegated acts referred to in Article 2(5), second subparagraph, Article 7(3), Article 8(1) and (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(5) shall be conferred on the Commission for a period of five years from 10 December 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. 第 2 条第 5 項第 2 副項，第 7 条第 3 項，第 8 条第 1 項及び第 2 項，第 13 条第 8 項第 4 副項，第 14 条第 9 項，第 25 条，第 27 条第 9 項，第 28 条第 5 項及び第 31 条第 5 項に示す権限の委任は，いつでも，欧州議会または理事会によって取消され得る。取消しの決定は，同決定の中で指示される権限の委任を終了させる。その決定は，EU 官報上でその決定が公示された翌日に発効し，または，その決定の中で指定された後の日に発効する。その決定は，既に発効している委任される行為の有効性に影響を与えてはならない。

   The delegation of power referred to in Article 2(5), second subparagraph, Article 7(3), Article 8(1) and (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) and Article 31(5) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. 委任される行為を採択する前に，欧州委員会は，より良い立法に関する 2016 年 4 月 13 日の機関間合意の中で定められた基本原則に従い，各構成国から指定された専門家から意見聴取する。

Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

5. 欧州委員会が委任される行為を採択したときは直ちに，欧州委員会は，欧州議会及び理事会に対し，同時に通知する。

As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. 第 2 条第 5 項第 2 副項，第 7 条第 3 項，第 8 条第 1 項または第 2 項，第 13 条第 8 項第 4 副項，第 14 条第 9 項，第 25 条，第 27 条第 9 項，第 28 条第 5 項または第 31 条第 5 項によって採択された委任される行為は，欧州議会及び理事会に対する当該行為の通知から 2 か月以内に欧州議会もしくは理事会のいずれからも異議が表明されないとき，または，その期間が満了する前に，欧州議会及び理事会の両者が欧州委員会に対して異議を述べない旨を連絡したときに限り発効する。その期間は，欧州議会の発意または理事会の発意により，2 か月まで延長される。

A delegated act adopted pursuant to Article 2(5), second subparagraph, Article 7(3), Article 8(1) or (2), Article 13(8), fourth subparagraph, Article 14(9), Article 25, Article 27(9), Article 28(5) or Article 31(5) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

第 62 条 委員会の手続

Article 62 **Committee procedure**

1. 欧州委員会は，委員会による補佐を受ける。同委員会は，規則(EU) No 182/2011 の意味における委員会である。

The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. 本項に対する参照があるときは，規則(EU) No 182/2011 の第 5 条が適用される。

Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. 委員会の意見が書面手続によって得られるべき場合において，当該手続は，意見伝達のための期限内に，委員会の議長がそのように決定し，または，委員会の構成員がそのように要請したときは，結論を得ないで結了する。

Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.

第 VII 章 機密性及び制裁
Chapter VII **Confidentiality and Penalties**

第 63 条 機密性
Article 63 **Confidentiality**

1. この規則の適用に関与する全ての関係者は，とりわけ，以下の事柄を保護するような態様で，当該関係者の職務及び活動を実施する際に入手した情報及びデータの機密性を尊重する：

   All parties involved in the application of this Regulation shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

   (a) 知的財産権，並びに，欧州議会及び理事会の指令(EU) 2016/943[37]の第 5 条に示す場合を除き，ソースコードを含め，自然人または法人の機密の企業情報または営業秘密；

   intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive (EU) 2016/943 of the European Parliament and of the Council[37];

   (b) とりわけ検査，調査または監査の目的のための，この規則の実効的な実装；

   the effective implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;

   (c) 公共の保安上及び国家安全保障上の利益；

   public and national security interests;

   (d) 刑事手続及び行政手続の完全性。

   integrity of criminal or administrative proceedings.

2. 第 1 項を妨げることなく，市場監視当局間及び市場監視当局と欧州委員会との間において機密ベースで交換される情報は，情報源である市場監視当局の事前の同意なく開示されてはならない。

---

[37] 当該情報の違法な入手，利用及び開示に抗する非開示のノウハウ及び企業情報（営業秘密）の保護に関する欧州議会及び理事会の 2016 年 6 月 8 日の指令(EU) 2016/943 (OJ L 157, 15.6.2016, p. 1).
Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

Without prejudice to paragraph 1, information exchanged on a confidential basis between the market surveillance authorities and between market surveillance authorities and the Commission shall not be disclosed without the prior agreement of the originating market surveillance authority.

3. 第 1 項及び第 2 項は，情報の交換及び警報の伝達と関連する欧州委員会，構成国及び指定組織の権利及び義務に影響を与えてはならず，また，構成国の刑事法の下において情報を提供する関係者の義務に影響を与えてもならない。

Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the persons concerned to provide information under criminal law of the Member States.

4. 欧州委員会及び構成国は，それが必要なときは，欧州委員会及び構成国が二国間または多国間の十分なレベルの保護を保証する機密保持協定を締結した第三国の適格な当局との間において，機微の情報を交換できる。

The Commission and Member States may exchange, where necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.

第 64 条 制裁

Article 64 **Penalties**

1. 構成国は，この規則の違反行為に対して適用可能な制裁に関する規定を定め，かつ，同規定が実装されることを確保するために必要となる全ての措置を講ずる。定められる制裁は，実効的であり，比例的であり，かつ，抑止力のあるものとする。構成国は，遅滞なく，欧州委員会に対し，当該規定及び当該措置を通知し，かつ，遅滞なく，欧州委員会に対し，当該規定及び当該措置に対して影響を与えるその後の改正を通知する。

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, without delay, notify the Commission of those rules and measures and shall notify it, without delay, of any subsequent amendment affecting them.

2. 別紙 I の中で定められた必須のサイバーセキュリティ要件並びに第 13 条及び第 14 条の中で定められた義務の不遵守は，上限を 1500 万ユーロとする額，または，当該違反者が事業者であるときは，前会計年における当該事業者の全世界の年次総売上の 2.5%を上限とする額のいずれか高い方の額の行政上の制裁金に服する。

Non-compliance with the essential cybersecurity requirements set out in Annex I and the obligations set out in Articles 13 and 14 shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.

3. この規則の第 18 条ないし第 23 条, 第 28 条, 第 30 条第 1 項ないし第 4 項, 第 31 条第 1 項ないし第 4 項, 第 32 条第 1 項, 第 2 項及び第 3 項, 第 33 条第 5 項, 並びに, 第 39 条, 第 41 条, 第 47 条, 第 49 条及び第 53 条の中で定められた義務の不遵守は, 上限を 1000 万ユーロとする額, または, 当該違反者が事業者であるときは, 前会計年における当該事業者の全世界の年次総売上の 2%を上限とする額のいずれか高い方の額の行政上の制裁金に服する。

Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

4. 要求に対する返答において, 指定組織及び市場監視当局に対し, 不正確, 不完全または誤解を招く情報を提供することは, 上限を 500 万ユーロとする額, または, 当該違反者が事業者であるときは, 前会計年における当該事業者の全世界の年次総売上の 1%を上限とする額のいずれか高い方の額の行政上の制裁金に服する。

The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities in reply to a request shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

5. 個々の具体的な案件において行政上の制裁金の額を決定する際, 個別の状況の適格な全ての事情が考慮に入れられ, かつ, 以下の事情に対して適正な考慮が払われる:

When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

(a) 違反行為及びその結果の性質, 重大性及び持続期間;

the nature, gravity and duration of the infringement and of its consequences;

(b) 類似の違反行為に関して同一の取引主体に対し同一または別の市場監視当局によって既に行政上の制裁金が適用されたかどうか;

whether administrative fines have been already applied by the same or other market surveillance authorities to the same economic operator for a similar infringement;

(c) とりわけ，スタートアップを含め，マイクロ企業並びに小企業及び中規模企業と関連して，違反行為を実行している経済取引主体の規模及び市場占有率。

the size, in particular with regard to microenterprises and small and medium sized-enterprises, including start-ups, and the market share of the economic operator committing the infringement.

6. 行政上の制裁金を適用する市場監視当局は，規則(EU) 2019/1020 の第 34 条に示す情報及び通信システムを介して，別の構成国の市場監視当局に対し，当該適用を通知する。

Market surveillance authorities that apply administrative fines shall communicate that application to the market surveillance authorities of other Member States through the information and communication system referred to in Article 34 of Regulation (EU) 2019/1020.

7. 各構成国は，当該構成国内に設置されている行政機関及び行政組織に対し，行政上の制裁金が科されるかどうか及びどの範囲で科されるかに関する規定を定める。

Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and public bodies established in that Member State.

8. 構成国の法制度の相違に対応して，行政上の制裁金に関する規定は，当該構成国内において国内レベルで定められた職務権限に従い，職務権限のある国内裁判所またはそれ以外の組織によって制裁金が科されるような態様で適用され得る。それらの構成国内におけるそのような規定の適用は，均等な効果をもつ。

Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or other bodies according to the competences established at national level in those Member States. The application of such rules in those Member States shall have an equivalent effect.

9. 個々の具体的な案件の状況の相違に応じて，行政上の制裁金は，同一の違反行為に関し市場監視当局によって適用された他の是正措置または制限措置に付加して科され得る。

Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement.

10. 本条の第 3 項ないし第 9 項からの特例により，以下の者に対しては，それらの各項に示す行政上の制裁金を適用してはならない：

By way of derogation from paragraphs 3 to 9, the administrative fines referred to in those paragraphs shall not apply to the following:

(a) 第 14 条第 2 項(a)または第 14 条第 4 項(a)に示す期限に適合しないことに関し，マイクロ企業または小企業として適格な製造者；

manufacturers that qualify as microenterprises or small enterprises with regard to any failure to meet the deadline referred to in Article 14(2), point (a), or Article 14(4), point (a);

(b) オープンソーススチュワードによるこの規則の違反行為。

any infringement of this Regulation by open-source software stewards.

第 65 条 代表訴訟

Article 65 **Representative actions**

指令(EU) 2020/1828 は，経済取引主体によるこの規則の条項の違反行為であって，消費者の集団的な利益を害する行為または害するかもしれない行為に対して提起される代表訴訟に適用される。

Directive (EU) 2020/1828 shall apply to the representative actions brought against infringements by economic operators of provisions of this Regulation that harm, or may harm, the collective interests of consumers.

第 VIII 章　移行措置条項及び最終規定
Chapter VIII **Transitional and Final Provisions**

第 66 条　規則(EU) 2019/1020 の改正
Article 66 **Amendment to Regulation (EU) 2019/1020**

規則(EU) 2019/1020 の別紙 I において，以下の号が付加される：
「72. 欧州議会及び理事会の規則(EU) 2024/2847 (*)

――――――――

(*)　デジタルの要素をもつ製品の横断的なサイバーセキュリティ要件に関する並びに規則(EU) No 168/2013 及び規則 (EU) 2019/1020 並びに指令 (EU) 2020/1828 を改正する欧州議会及び理事会の 2024 年 10 月 23 日の規則(EU) 2024/2847（サイバー回復力法）(OJ L, 2024/2847, 20.11.2024)」。

In Annex I to Regulation (EU) 2019/1020, the following point is added:
‘72. Regulation (EU) 2024/2847 of the European Parliament and of the Council (*)

――――――――

(*) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU)No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).’.

第 67 条　指令(EU) 2020/1828 の改正
Article 67 **Amendment to Directive (EU) 2020/1828**

指令(EU) 2020/1828 の別紙 I において，以下の号が付加される：
「69. 欧州議会及び理事会の規則(EU) 2024/2847 (*)

――――――――

(*)　デジタルの要素をもつ製品の横断的なサイバーセキュリティ要件に関する並びに規則(EU) No 168/2013 及び規則 (EU) 2019/1020 並びに指令 (EU) 2020/1828 を改正する欧州議会及び理事会の 2024 年 10 月 23 日の規則(EU) 2024/2847（サイバー回復力法）(OJ L, 2024/2847, 20.11.2024)」。

In Annex I to Directive (EU) 2020/1828, the following point is added:
‘69. Regulation (EU) 2024/2847 of the European Parliament and of the Council (*)

――――――――

(*) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU)No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).’.

第 68 条 規則(EU) No 168/2013 の改正

Article 68 **Amendment to Regulation (EU) No 168/2013**

欧州議会及び理事会の規則(EU) No 168/2013[38]の別紙 II のパート C1 において，表の中に以下のエントリが付加される:

「

16	18	サイバー攻撃に対する自動車の保護		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

」。

In Part C1, in the table, of Annex II to Regulation (EU) No 168/2013 of the European Parliament and of the Council [38], the following entry is added:

`

16	18	protection of vehicle against cyberattacks		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

`.

第 69 条 移行措置条項

Article 69 **Transitional provisions**

1. この規則以外の欧州連合の別の整合化立法に服するデジタルの要素をもつ製品に関するサイバーセキュリティ上の要件と関連して発された EU 型式審査証明書及び承認決定書は，2028 年 6 月 11 日までに失効しない限り，または，そのような欧州連合の別の立法の中で別異に定められていない限り，同日まではその有効性を維持し，別異に定められている場合においては，その EU 型式審査証明書及び承認決定書は，その欧州連合の別の立法の中に示すように有効性を維持する。

EU type-examination certificates and approval decisions issued regarding cybersecurity requirements for products with digital elements that are subject to Union harmonisation legislation other than this Regulation shall remain valid until 11 June 2028, unless they expire before that date, or unless otherwise specified in such other Union harmonisation legislation, in which case they shall remain valid as referred to in that legislation.

2. 2027 年 12 月 11 日よりも前に市場に置かれたデジタルの要素をもつ製品は，その製品が，同日から，大きな変更に服する場合に限り，この規則の中で定められた要件に服する。

---

[38] 2 輪または 3 輪の車両及び 4 輪自転車の承認及び市場監視に関する欧州議会及び理事会の 2013 年 1 月 15 日の規則(EU) No 168/2013 (OJ L 60, 2.3.2013, p. 52).

Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

Products with digital elements that have been placed on the market before 11 December 2027 shall be subject to the requirements set out in this Regulation only if, from that date, those products are subject to a substantial modification.

3. 本条の第 2 項からの特例により，第 14 条の中で定められた義務は，2027 年 12 月 11 日よりも前に市場に置かれたこの規則の適用範囲内にある全てのデジタルの要素をもつ製品に対して適用される。

By way of derogation from paragraph 2 of this Article, the obligations laid down in Article 14 shall apply to all products with digital elements that fall within the scope of this Regulation that have been placed on the market before 11 December 2027.

第 70 条 評価及び見直し

Article 70 **Evaluation and review**

1. 2030 年 12 月 11 日までに及びその後は 4 年毎に，欧州委員会は，欧州議会及び理事会に対し，この規則の評価及び見直しに関する報告書を提出する。同報告書は，公表される。

By 11 December 2030 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. Those reports shall be made public.

2. 2028 年 9 月 11 日までに，欧州委員会は，ENISA 及び CSIRT ネットワークからの意見聴取を経た上で，欧州議会及び理事会に対し，第 16 条の中で定められた単一報告プラットフォームの実効性を評価し，かつ，受領した通知の適格な他の CSIRT への適時の伝達と関連して，同プラットフォームの実効性に対する調整者として指定された CSIRT による第 16 条第 2 項に示すサイバーセキュリティと関連する根拠の適用の影響を評価する報告書を提出する。

By 11 September 2028, the Commission shall, after consulting ENISA and the CSIRTs network, submit a report to the European Parliament and to the Council, assessing the effectiveness of the single reporting platform set out in Article 16, as well as the impact of the application of the cybersecurity-related grounds referred to Article 16(2) by the CSIRTs designated as coordinators on the effectiveness of the single reporting platform as regards the timely dissemination of received notifications to other relevant CSIRTs.

第 71 条 発効及び適用

Article 71 **Entry into force and application**

1. この規則は，EU 官報上のその公示の 20 日後に発効する。

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. この規則は，2027 年 12 月 11 日から適用される。

This Regulation shall apply from 11 December 2027.

ただし，第 14 条は，2026 年 9 月 11 日から適用され，また，第 IV 章（第 35 条ないし第 51 条）は，2026 年 6 月 11 日から適用される。

However, Article 14 shall apply from 11 September 2026 and Chapter IV (Articles 35 to 51) shall apply from 11 June 2026.

この規則は，その全体について拘束力があり，かつ，全ての構成国において直接に適用される。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

2024 年 10 月 23 日にストラスブールにおいて行われた。

Done at Strasbourg, 23 October 2024.

欧州議会として	理事会として
For the European Parliament	For the Council
長 R. METSOLA	長 ZSIGMOND B. P.
The President R. METSOLA	The President ZSIGMOND B. P.

別紙 I

必須のサイバーセキュリティ要件
Essential Cybersecurity Requirements

パート I デジタルの要素をもつ製品の特性と関連するサイバーセキュリティ要件
Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) デジタルの要素をもつ製品は，リスクを基礎とする適切なレベルのサイバーセキュリティをその製品が確保するような方法で設計され，開発され及び製造される；

Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) 第 13 条第 2 項に示すサイバーセキュリティリスク評価を基礎として，かつ，それが適用可能なときは，デジタルの要素をもつ製品は：

On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) 既知の悪用可能な脆弱性なしに市場において利用できるようにされ；

be made available on the market without known exploitable vulnerabilities;

(b) 個別対応のデジタルの要素をもつ製品との関係において，その製品をその製品の初期状態にリセットできることを含め，製造者と企業利用者との間で別異に合意されていない限り，デフォルトで安全な設定をもって市場において利用できるようにされ；

be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) それが適用可能なときは，明瞭で利用しやすいオプトアウトの仕組みをもち，デフォルト設定として実現可能な適切な時間枠内にインストールされる自動的なセキュリティアップデートによる場合，利用者にとって利用可能なアップデートの通知による場合，及び，アップデートを一時的に遅延させるオプションの場合を含め，セキュリティアップデートによって脆弱性が対処され得ることを確保し；

ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting,

with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) 認証，識別子管理システムまたはアクセス管理システム及び可能的な無権限アクセスに関する報告を含むがこれらに限定されない適切な管理の仕組みによって，無権限アクセスからの保護を確保し；

ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) 保存中または通過中の適格なデータを最新の仕組みによって暗号化することによる場合，及び，それら以外の技術手段を用いることによる場合のように，記録保存され，伝送されまたはそれら以外の処理をされる個人データまたはそれ以外のデータの機密性を保護し；

protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) 記録保存され，伝送されまたはそれら以外の処理をされる個人データまたはそれ以外のデータ，命令，プログラム及び設定の完全性を，利用者から権限が与えられていない操作または改変に抗して保護し，かつ，破壊を報告し；

protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

(g) デジタルの要素をもつ製品の所期の目的との関係において十分であり，適格でありかつ必要なところに限定された個人データまたはそれ以外のデータのみを処理し（「データのミニマム化」）；

process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) サービス拒否攻撃に抗する回復措置及び緩和措置を用いる場合を含め，インシデントの後においても，必須機能及び基本機能の可用性を保護し；

protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) 他の機器またはネットワークから提供されるサービスの可用性に対するその製品それ自体または接続された機器による負の影響をミニマム化し；

minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

(j) 外部のインタフェイスを含め，攻撃対象領域を限定するために設計され，開発され及び製造され；

be designed, developed and produced to limit attack surfaces, including external interfaces;

(k) 悪用を緩和する適切な仕組み及び技術を用いてインシデントの影響を削減するために設計され，開発され及び製造され；

be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

(l) データ，サービスまたは機能へのアクセスまたはその改変の記録化及び監視を含め，利用者のためのオプトアウトの仕組みをもつ適格な内部活動を記録すること及び監視することにより，セキュリティと関連する情報を提供し；

provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) 全てのデータ及び設定を利用者が恒久的，安全かつ容易に削除できることを提供し，かつ，そのようなデータが別の製品またはシステムに移転され得るときは，安全な態様でそれが行われることを確保する。

provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

パート II 脆弱性取扱の要件
Part II **Vulnerability handling requirements**

デジタルの要素をもつ製品の製造者は：

Manufacturers of products with digital elements shall:

(1) 最少でもその製品のトップレベルの依存性を包摂し，一般に使用されておりかつ機械読取り可能なフォーマットによるソフトウェア素材表を作成することによる場合を含め，デジタルの要素をもつ製品の中に包含されている脆弱性及びコンポーネントを特定し及び文書化し；

identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) デジタルの要素をもつ製品に対して呈されているリスクとの関係において，セキュリティアップデートを提供することによる場合を含め，遅滞なく，脆弱性に対処し及びそれを解消し；それが技術的に利用可能なときは，新たなセキュリティアップデートが，機能性のアップデートとは別に提供され；

in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) デジタルの要素をもつ製品のセキュリティの実効的かつ定期的な試験及び見直しを適用し；

apply effective and regular tests and reviews of the security of the product with digital elements;

(4) セキュリティアップデートが利用できるようにされた後，その脆弱性の説明を含め，手当てされた脆弱性に関する情報，影響を受けるデジタルの要素をもつ製品を利用者が識別できるようにする情報，その脆弱性の影響，脆弱性の深刻度に関する情報及びその脆弱性を解消するために利用者を助ける明瞭かつアクセス可能な情報を共有し及び公衆に開示し；適正に正当化される場合において，公表することのセキュリティ上のリスクがセキュリティ上の利益を上回ると製造者が判断するときは，その製造者は，適格なパッチを適用する可能性を利用者が与えられた後になるまで，手当てされた脆弱性に関する情報を公表することを遅延させることができ；

once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) 調整された脆弱性開示に関する基本方針を設け及び執行し；

put in place and enforce a policy on coordinated vulnerability disclosure;

(6) デジタルの要素をもつ製品の中で発見された脆弱性の報告のための連絡先を提供することによる場合を含め，その製造者のデジタルの要素をもつ製品の中にある潜在的な脆弱性及び当該製品内に含まれている第三者のコンポーネントの中にある潜在的な脆弱性に関する情報の共有を容易にするための方策をとり；

take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) 適時の態様で，かつ，セキュリティアップデートに適用可能なときは，自動的な態様で，脆弱性が手当てされまたは緩和されることを確保するためのデジタルの要素をもつ製品のアップデートを安全に伝達するための仕組みを定め；

provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

(8) 発見されたセキュリティ上の問題に対処するためにセキュリティアップデートが利用可能なときは，遅滞なく，かつ，個別対応のデジタルの要素をもつ製品との関係において製造者と企業利用者との間で別異に合意されていない限り，無料で，とられるべき潜在的な行動を含め，適格な情報を利用者に対して提供する助言メッセージを伴って，そのアップデートが伝達されることを確保する。

ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

別紙Ⅱ

利用者に対する情報提供及び指示
Information and Instructions to the User

ミニマムのものとして，デジタルの要素をもつ製品には，以下のものが付される：

At minimum, the product with digital elements shall be accompanied by:

1. その製造者の名称，登録商号または登録商標，郵便住所，電子メールアドレスまたはそれ以外のデジタルの連絡先，並びに，それが利用可能なときは，その製造者と連絡をとり得る Web サイト；

   the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;

2. デジタルの要素をもつ製品の脆弱性に関する情報が報告され及び受領され得る，かつ，調整された脆弱性開示に関するその製造者の基本方針をみつけることができる単一連絡先；

   the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;

3. そのデジタルの要素をもつ製品の唯一無二の識別をできるようにする名称及び型式並びに付加的な情報；

   name and type and any additional information enabling the unique identification of the product with digital elements;

4. その製造者から提供されるセキュリティ環境を含め，そのデジタルの要素をもつ製品の所期の目的及びその製品の基本的な機能性並びにセキュリティ特性に関する情報；

   the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;

5. その製品の所期の目的に従ったまたは合理的に予測可能な濫用という条件の下におけるデジタルの要素をもつ製品の利用との関係において，サイバーセキュリティ上の大きなリスクを導くかもしれない既知の状況または予測可能な状況；

   any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

6. それが適用可能なときは，EU 適合宣言書がアクセスされ得るインターネット上のアドレス；

where applicable, the internet address at which the EU declaration of conformity can be accessed;

7. その製造者から提供される技術上のセキュリティサポートのタイプ，及び，脆弱性が取り扱われ及びセキュリティアップデートを受領することを利用者が期待できるサポート期間の最終日；

the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

8. 以下の事項に関する詳細な指示，または，そのような詳細な指示及び情報を示すインターネット上のアドレス；

detailed instructions or an internet address referring to such detailed instructions and information on:

(a) そのデジタルの要素をもつ製品の導入期間中及び耐用年数の間にわたる，そのデジタルの要素をもつ製品の安全な利用を確保するために必要となる方策；

the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;

(b) そのデジタルの要素をもつ製品に対する変更がどのようにデータのセキュリティに影響を与え得るか；

how changes to the product with digital elements can affect the security of data;

(c) セキュリティと関係するアップデートがどのようにインストールされるか；

how security-relevant updates can be installed;

(d) 利用者のデータがどのようにして安全に削除され得るかに関する情報を含め，そのデジタルの要素をもつ製品の安全な廃止；

the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;

(e) 別紙 I のパート I の第 2 号(c)によって要求されるセキュリティアップデートの自動的なインストールをできるようにするデフォルトの設定がどのようにして停止され得るか；

how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of

Annex I, can be turned off;

(f) そのデジタルの要素をもつ製品がデジタルの要素をもつ別の製品の中に組み込まれることが意図されている場合，別紙 I の中で定められた必須のサイバーセキュリティ要件及び別紙 VII の中で定められた文書の要件を遵守するために，その組込みをする者にとって必要な情報。

where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.

9. その製造者が，利用者に対してソフトウェア素材表を利用できるようにすることを決定する場合，そのソフトウェア素材表がアクセスされ得る場所に関する情報。

If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.

別紙 III

デジタルの要素をもつ重要な製品
Important Products with Digital Elements

クラス I

1. 認証を含め，識別子管理システム及び特権アクセス管理のソフトウェアとハードウェア，並びに，生体要素読取装置を含め，アクセス管理用読取装置

   Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

2. スタンドアロンのブラウザ及び組み込まれたブラウザ

   Standalone and embedded browsers

3. パスワードマネジャ

   Password managers

4. 悪意あるソフトウェアを探索し，除去しまたは検疫するソフトウェア

   Software that searches for, removes, or quarantines malicious software

5. 仮想プライベートネットワーク（VPN）の機能のあるデジタルの要素をもつ製品

   Products with digital elements with the function of virtual private network (VPN)

6. ネットワーク管理システム

   Network management systems

7. セキュリティ情報及びイベント管理（SIEM）システム

   Security information and event management (SIEM) systems

8. ブートマネジャ

   Boot managers

9. 公開鍵インフラ及びデジタル証明書発行ソフトウェア

   Public key infrastructure and digital certificate issuance software

10. 物理的なネットワークインタフェイス及び仮想的なネットワークインタフェイス

    Physical and virtual network interfaces

11. オペレーティングシステム

    Operating systems

12. ルータ，インターネットへの接続を意図するモデム及びスイッチ

    Routers, modems intended for the connection to the internet, and switches

13. セキュリティと関係する機能性をもつマイクロプロセッサ

    Microprocessors with security-related functionalities

14. セキュリティと関係する機能性をもつマイクロコントローラ

    Microcontrollers with security-related functionalities

15. セキュリティと関係する機能性をもつ特定用途向け集積回路（ASIC）及び現場でプログラム可能なゲートアレイ（FPGA）

    Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities

16. スマートホームの一般的な目的の仮想アシスタント

    Smart home general purpose virtual assistants

17. スマートドアロック，セキュリティカメラ，ベビー監視システム及び警報システムを含め，セキュリティ上の機能性をもつスマートホーム製品

    Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems

18. ソーシャルインタラクティブ機能（例：会話もしくは動画撮影）をもちまたは位置追跡機能をもつ，欧州議会及び理事会の指令 2009/48/EC[1]の適用のあるインターネットに接続された玩具

Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council [(1)] that have social interactive features (e.g. speaking or filming) or that have location tracking features

19. 人間の身体上で着用もしくは装着され，（追跡のような）健康状態監視の目的をもち，かつ，その製品に対して規則(EU) 2017/745 もしくは規則(EU) 2017/746 が適用されない個人向けウェアラブル製品，または，児童による使用もしくは児童のための使用を意図する個人向けウェアラブル製品。

Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

クラス II

1. オペレーティングシステム及び類似の環境の仮想実行を支えるハイパービジョン及びコンテナランタイムシステム

Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments

2. ファイアウォール，侵入検知システム及び侵入防止システム

Firewalls, intrusion detection and prevention systems

3. 耐タンパーマイクロプロセッサ

Tamper-resistant microprocessors

4. 耐タンパーマイクロコントローラ

Tamper-resistant microcontrollers

---

[1] 玩具の安全性に関する欧州議会及び理事会の 2009 年 6 月 18 日の指令 2009/48/EC (OJ L 170, 30.6.2009, p. 1).
Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1).

別紙 IV

デジタルな要素をもつ不可欠な製品
Critical Products with Digital Elements

1. セキュリティボックスをもつハードウェア機器

   Hardware Devices with Security Boxes

2. 欧州議会及び理事会の指令(EU) 2019/944[1]の第 2 条第 23 号に定義す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，安全な暗号処理の目的を含め，高度なセキュリティの目的のためのその他の機器

   Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing

3. 安全の要素を含むスマートカードまたは類似の機器

   Smartcards or similar devices, including secure elements

---

[1] 電力の域内市場のための共通規定に関する及び指令 2012/27/EU を改正する欧州議会及び理事会の 2019 年 6 月 5 日の指令(EU) 2019/944 (OJ L 158, 14.6.2019, p. 125).
Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (OJ L 158, 14.6.2019, p. 125).

別紙 V

EU 適合宣言書
EU Declaration of Conformity

第 28 条に示す EU 適合宣言書は，以下の情報の全てを含める：

The EU declaration of conformity referred to in Article 28, shall contain all of the following information:

1. デジタルの要素をもつ製品の唯一無二の識別ができるようにする名称及び型式並びに付加的な情報

   Name and type and any additional information enabling the unique identification of the product with digital elements

2. 製造者の名称及び住所またはその製造者の権限のある代理者；

   Name and address of the manufacturer or its authorised representative

3. 提供者の単独の責任の下において EU 適合宣言書が発行される旨の文言；

   A statement that the EU declaration of conformity is issued under the sole responsibility of the provider

4. 宣言の対象（トレーサビリティを可能にするデジタルの要素をもつ製品の識別子。それが適切なときは，写真を含め得る）；

   Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)

5. 上述の宣言の対象が適格な欧州連合整合化立法に適合している旨の文言；

   A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation

6. 使用された適格な整合化された技術標準もしくはそれ以外の共通仕様または適合性が宣言されていることとの関係におけるサイバーセキュリティ証明書への参照；

   References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared

7. それが適用可能なときは，指定組織の名称及び番号，遂行された適合性評価手続の記述及び発

行された証明書の識別子；

Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued

8. 付加的な情報：

Additional information:

の代わりに署名された：

Signed for and on behalf of:

（発行の場所及び日付）

(place and date of issue):

（名称，職位）（署名）

(name, function) (signature):

別紙 VI

簡易化された EU 適合宣言書
Simplified EU Declaration of Conformity

第 13 条第 20 項に示す簡易化された EU 適合宣言書は，以下のように提供される：

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

ここに，…[製造者の名称]は，デジタルの要素をもつ製品の型式…[デジタルの要素をもつ製品の型式指定]が規則(EU) 2024/2847[1] を遵守していることを宣言する。

Hereby, … [name of manufacturer] declares that the product with digital elements type … [designation of type of product with digital element] is in compliance with Regulation (EU) 2024/2847[(1)].

EU 適合宣言書の全文は，以下のインターネット上のアドレスで利用できる：

The full text of the EU declaration of conformity is available at the following internet address: …

[1] OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj

別紙 VII

技術文書の内容
Content of the Technical Documentation

第 31 条に示す技術文書は，適格なデジタルの要素をもつ製品に適用可能な，少なくとも以下の情報を含める:

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements:

1. 以下の事項を含め，そのデジタルの要素をもつ製品の一般的な説明:

   a general description of the product with digital elements, including:

   (a) そのデジタルの要素をもつ製品の所期の目的;

   its intended purpose;

   (b) 必須のサイバーセキュリティ要件の遵守に影響を与えるソフトウェアの版;

   versions of software affecting compliance with essential cybersecurity requirements;

   (c) そのデジタルの要素をもつ製品がハードウェア製品である場合，外形上の特徴，目印及び内部配置を示す写真またはイラスト;

   where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;

   (d) 別紙 II に定める利用者に対する情報提供及び指示;

   user information and instructions as set out in Annex II;

2. 以下の事項を含め，そのデジタルの要素をもつ製品の設計，開発及び製造並びに脆弱性取扱手続の説明:

   a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:

   (a) それが適用可能なときは，ソフトウェアコンポーネントがどのように構築されているかまたは相互

に利用し合っているか，また，処理全体の中にどのように組み込まれているかを解説するシステムアーキテクチャの図及びスキームまたは説明を含め，そのデジタルの要素をもつ製品の設計及び開発に関する必要な情報；

necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;

(b) ソフトウェア素材表，調整された脆弱性開示の基本方針，脆弱性報告のための連絡先の提供の証拠及びアップデートの安全な伝達のために選択された技術ソリューションの説明を含め，その製造者によって設けられた脆弱性取扱プロセスの必要な情報及び仕様；

necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;

(c) そのデジタルの要素をもつ製品の製造及び監視のプロセス並びに同プロセスの検証の必要な情報及び仕様；

necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;

3. 別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件がどのように適用され得るかを含め，そのデジタルの要素をもつ製品が第 13 条によって設計され，開発され，製造され，流通され及び維持管理されることを損ねるサイバーセキュリティ上のリスクの評価；

an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;

4. そのデジタルの要素をもつ製品の第 13 条第 8 項によるサポート期間を決定するために考慮に入れられた適格な情報；

relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;

5. その全部または一部が適用され，その参照が EU 官報上で公示された整合化された技術標準，この規則の第 27 条に定める共通仕様またはこの規則の第 27 条第 8 項による規則(EU) 2019/881 により採択された欧州サイバーセキュリティ認証制度のリスト，及び，それらの整合化された技術標準，共

通仕様または欧州サイバーセキュリティ認証制度が適用されなかったときは，それら以外の適用された適格な技術仕様のリストを含め，別紙 I のパート I 及びパート II の中で定められた必須のサイバーセキュリティ要件に適合するために採用されたソリューションの記述。整合化された技術標準，共通仕様または欧州サイバーセキュリティ認証制度が部分的に適用された場合においては，その技術文書は，適用された部分を示す；

a list of the harmonised standards applied in full or in part the references of which have been published in the *Official Journal of the European Union*, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;

6. そのデジタルの要素をもつ製品及び脆弱性取扱プロセスの，別紙 I のパート I 及びパート II の中で定められた適用可能な必須のサイバーセキュリティ要件への適合性を検証するために実施された試験の結果報告；

reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;

7. EU 適合宣言書のコピー；

a copy of the EU declaration of conformity;

8. それが適用可能なときは，当該市場監視当局が別紙 I の中で定められた必須のサイバーセキュリティ要件の遵守を点検できるようにするためにそれが必要であることを条件として，市場監視当局からの理由を付した要求に応じて，ソフトウェア素材表。

where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.

別紙 VIII

適合性評価手続
Conformity Assessment Procedures

パート I（モジュール A を基礎とする）内部統制を基礎とする適合性評価手続

Part I **Conformity assessment procedure based on internal control (based on module A)**

1. 内部統制は，それによって，製造者が本パートの第 2 号，第 3 号及び第 4 号の中で定められた義務を満たし，かつ，そのデジタルの要素をもつ製品が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件の全てを満たすこと，及び，その製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合することを当該製造者の単独の責任に基づいて確保しかつその旨を宣言する適合性評価手続である。

   Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2, 3 and 4 of this Part, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements set out in Part I of Annex I and the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

2. 製造者は，別紙 VII に示す技術文書を作成する。

   The manufacturer shall draw up the technical documentation described in Annex VII.

3. デジタルの要素をもつ製品の設計，開発，製造及び脆弱性取扱

   Design, development, production and vulnerability handling of products with digital elements

   製造者は，製造されまたは開発されたデジタルの要素をもつ製品及びその製造者によって設けられたプロセスが別紙 I のパート I 及びパート II の中で定められた必須のサイバーセキュリティ要件を遵守することを，設計，開発，製造及び脆弱性取扱プロセス並びにそれらの監視によって確保するようにするために必要となる全ての措置を講ずる。

   The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Parts I and II of Annex I.

4. 適合マーク及び適合宣言

Conformity marking and declaration of conformity

4.1. 製造者は，この規則の中で定められた適用可能な要件を満たすデジタルの要素をもつ個々の具体的な製品に CE マークを付す。

The manufacturer shall affix the CE marking to each individual product with digital elements that satisfies the applicable requirements set out in this Regulation.

4.2. 製造者は，第 28 条に従い，個々のデジタルの要素をもつ製品に関し，書面による EU 適合宣言を作成し，かつ，そのデジタルの要素をもつ製品が市場に置かれた後 10 年間またはサポート期間のいずれか長い方の期間，技術文書と共にその EU 適合宣言書を国内当局が自由に利用できるように保つ。EU 適合宣言書は，その EU 適合宣言書が作成されたデジタルの要素をもつ製品を特定する。要求に応じて，EU 適合宣言書のコピーを適格な当局が利用できるようにされる。

The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 28 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.

5. 権限のある代理者

Authorised representatives

第 4 号の中で定められた製造者の義務は，委任状の中で適格な義務が定められていることを条件として，その製造者の代わりに，かつ，その製造者の責任の下において，その製造者の権限のある代理者によって満たされ得る。

The manufacturer's obligations set out in point 4 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

パート II（モジュール B を基礎とする）EU 型式審査

Part II **EU-type examination (based on module B)**

1. EU 型式審査は，その手続内において，デジタルの要素をもつ製品の技術上の設計及び開発並びにその製造者によって設けられた脆弱性取扱プロセスを指定組織が審査し，かつ，デジタルの要素をもつ製品が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件に適合しているこ

と，及び，その製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合していることを証明する適合性評価手続の一部である。

EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

2. EU 型式審査は，第 3 号に示す技術文書及び補助証拠の審査を通じてデジタルの要素をもつ製品の技術上の設計及び開発の十分性を評価すること，及び，その製品の 1 または複数の不可欠部分の仕様を審査すること（製造型式と設計型式の組合せ）によって実施される。

EU-type examination shall be carried out by assessing the adequacy of the technical design and development of the product with digital elements through the examination of the technical documentation and supporting evidence referred to in point 3, and the examination of specimens of one or more critical parts of the product (combination of production type and design type).

3. 製造者は，その製造者が選択する単一の指定組織に対し，EU 型式審査の申請を申立てる。

The manufacturer shall lodge an application for EU-type examination with a single notified body of its choice.

申請書は，以下の事項を含める：

The application shall include:

3.1. その製造者の名称及び住所，また，権限のある代理者によって申請が申立てられたときは，当該権限のある代理者の名称及び住所；

the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

3.2. 同一の申請が別の指定組織に対して申立てられなかったことの書面による宣言；

a written declaration that the same application has not been lodged with any other notified body;

3.3. デジタルの要素をもつ製品が別紙 I のパート I の中で定められた適用可能な必須のサイバーセキュリティ要件及び別紙 I のパート II の中で定められた製造者の脆弱性取扱プロセスを遵守していることを評価できるようにするものとし，かつ，リスクの適切な分析及び評価を含めるものとする技術文書。技術文書は，適用される要件を示し，かつ，評価のために適格である限り，そのデジタルの要素をもつ製品の設計，製造及び運用を包摂する。技術文書は，それが適用

可能なときはいつでも，少なくとも別紙 VII の中で定められた諸要素を含める；

the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer's vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;

3.4. 技術上の設計及び開発ソリューション並びに脆弱性取扱プロセスの十分性に関する補助証拠。この補助証拠は，とりわけ，適格な整合化された技術標準または技術仕様が全面的には適用されなかった場合において，使用された文書に言及する。補助証拠は，それが必要なときは，その製造者の適切な研究施設によって実施された試験の結果またはその製造者の代わりにかつその製造者の責任の下において別の試験施設によって実施された試験の結果を含める。

the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on its behalf and under its responsibility.

4. 指定組織は：

The notified body shall:

4.1. デジタルの要素をもつ製品の技術上の設計及び開発が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を遵守していること及びその製造者によって設けられた脆弱性取扱プロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件を遵守していることの十分性を評価するため，技術文書及び補助証拠を審査し；

examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I;

4.2. 検体が技術文書に適合するように開発または製造されたことを検証し，また，適格な整合化された技術標準または技術仕様の適用可能な条項に従って設計及び開発された諸要素と，当該技術標準の適格な条項を適用することなく設計及び開発された諸要素とを識別し；

verify that specimens have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;

4.3. 製造者が，別紙 I の中で定められた諸要件のために，適格な整合化された技術標準または技術仕様の中にあるソリューションを適用することを選択した場合においては，そのソリューションが正確に適用されたか否かを点検するため，適切な審査及び試験を実施し，または，その審査及び試験を実施させ；

carry out appropriate examinations and tests, or have them carried out, to check that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I, they have been applied correctly;

4.4. 製造者が，別紙 I の中で定められた要件のために，適格な整合化された技術標準または技術仕様の中にあるソリューションが適用されなかった場合においては，その製造者によって採用されたソリューションが対応する必須のサイバーセキュリティ要件に適合するか否かを点検するため，適切な審査及び試験を実施し，または，その審査及び試験を実施させ；

carry out appropriate examinations and tests, or have them carried out, to check that, where the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential cybersecurity requirements;

4.5. 審査及び試験が実施されることになる場所に関し，その製造者と合意する。

agree with the manufacturer on a location where the examinations and tests will be carried out.

5. 指定組織は，第 4 号に従って行われた活動及び当該活動の結果を記録する評価報告書を作成する。それぞれの通知元当局との間における指定組織の義務を妨げることなく，指定組織は，製造者の同意がある場合に限り，同報告書の内容の全部または一部を公開する。

The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.

6. 型式及び脆弱性取扱プロセスが別紙 I の中で定められた必須のサイバーセキュリティ要件に適合しているときは，指定組織は，その製造者に対し，EU 型式審査証明書を発行する。同証明書は，その製造者の名称及び住所，審査の結論，（もしそれがあるときは）当該証明書の有効性の条件及び承認された型式及び脆弱性取扱プロセスの識別のために必要となるデータを含める。証明書は，1 または複数の別紙を添付し得る。

Where the type and the vulnerability handling processes meet the essential cybersecurity requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached.

証明書及びその別紙は，製造または開発されたデジタルの要素をもつ製品が，審査された型式及び脆弱性取扱プロセスを遵守していることが評価されるようにするため及び稼働中の監督に供することができるようにするための全ての適格な情報を含める。

The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with digital elements with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.

型式及び脆弱性取扱プロセスが別紙 I の中で定められた適用可能な必須のサイバーセキュリティ要件を満たさないときは，指定組織は，EU 型式審査証明書の発行を拒否し，かつ，その申請者に対してしかるべく連絡し，その申請の拒否の詳細な理由を与える。

Where the type and the vulnerability handling processes do not satisfy the applicable essential cybersecurity requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

7. 指定組織は，承認された型式及び脆弱性取扱プロセスが別紙 I の中で定められた適用可能な必須のサイバーセキュリティ要件を遵守しなくなったことを示唆する一般的に承認されている最新技術の変化に知覚する状態を保ち，かつ，そのような変化が更なる調査を要求するかどうかを判定する。もしそうであるときは，指定組織は，製造者に対し，しかるべく連絡する。

The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential cybersecurity requirements set out in Annex I, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.

製造者は，EU 型式審査証明書と関連する技術文書を保管している指定組織に対し，別紙 I の中で定められた必須のサイバーセキュリティ要件の適合性またはその証明書の有効性の条件に対して影響を与えるかもしれない，承認された型式及び脆弱性取扱プロセスに対する全ての修正を連絡する。そのような修正は，当初の EU 型式審査証明書に付記する方式による追加の承認を要求する。

The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the conditions for validity of the

certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.

8. 指定組織は，別紙 I のパート II の中で定められた脆弱性取扱プロセスが適切に実装されることを確保するため，定期的な監査を実施する。

The notified body shall carry out periodic audits to ensure that the vulnerability handling processes as set out in Part II of Annex I are implemented adequately.

9. 各指定組織は，その指定組織の通知元当局に対し，その指定組織が発行または取消した EU 型式審査証明書及びその証明書への付記に関して連絡し，また，定期的にまたは要請に応じて，その指定組織の通知元当局が，拒否され，停止されまたはそれ以外の制限が行われた証明書及び同証明書への付記のリストを利用できるようにする。

Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and any additions thereto refused, suspended or otherwise restricted.

各指定組織は，他の指定組織に対し，その指定組織が拒否し，取消し，停止しまたはそれ以外の制限を行った EU 型式審査証明書及び同証明書への付記に関して連絡し，また，要請に応じて，その指定組織が発行した証明書及び同証明書への付記に関して連絡する。

Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and additions thereto which it has issued.

欧州委員会，構成国及び他の指定組織は，要請により，EU 型式審査証明書及び同証明書への付記のコピーを入手できる。要請により，欧州委員会及び構成国は，技術文書のコピー及びその指定組織によって実施された審査の結果を入手できる。指定組織は，証明書の有効性が失効するまで，EU 型式審査証明書，その別紙及び付記のコピー並びに製造者から提出された文書を収納している技術ファイルを保管する。

The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and any additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.

10. 製造者は，デジタルの要素をもつ製品が市場に置かれた後 10 年間またはサポート期間のいずれか長い方の期間，技術文書と共に EU 型式審査証明書，その別紙及び同証明書への付記のコピ

ーを，国内当局が自由に利用できるように保管する。

The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.

11. 製造者の権限のある代理者は，委任状の中で適格な義務が定められていることを条件として，第 3 号に示す申請を申立て，また，第 7 号及び第 9 号の中で定められた義務を満たし得る。

The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 10, provided that the relevant obligations are specified in the mandate.

パート III （モジュール C を基礎とする）内部製造管理を基礎とする型式の適合性

Part III **Conformity to type based on internal production control (based on module C)**

1. 内部製造管理を基礎とする型式の適合性は，それによって，製造者が本パートの第 2 号及び第 3 号の中で定められた義務を満たし，また，関係するデジタルの要素をもつ製品が EU 型式審査証明書の中で示されている型式に適合していること，及び，別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を満たしていること，並びに，その製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合していることを確保しかつその旨を宣言する適合性評価手続の一部である。

Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 3 of this Part, and ensures and declares that the products with digital elements concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

2. 製造

Production

製造者は，その製造及びその製造の監視が，製造されたデジタルの要素をもつ製品の，EU 型式審査証明書の中で示されている承認された型式及び別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件の適合性を確保するようにし，かつ，その製造者によって設けられたプロセスが別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合することを確保するようにするために必要となる全ての方策を講ずる。

The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the

manufactured products with digital elements with the approved type described in the EU-type examination certificate and with the essential cybersecurity requirements as set out in Part I of Annex I and ensures that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

3. 適合マーク及び適合性の宣言

Conformity marking and declaration of conformity

3.1. 製造者は，EU 型式審査証明書の中で示されている型式に適合しており，かつ，この規則の中で定められた適用可能な要件を満たしている個々の具体的なデジタルの要素をもつ製品に対し，CE マークを付す。

The manufacturer shall affix the CE marking to each individual product with digital elements that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements set out in this Regulation.

3.2. 製造者は，製品モデルに関する書面による適合宣言を作成し，かつ，そのデジタルの要素をもつ製品が市場に置かれた後 10 年間またはサポート期間のいずれか長い方の期間，国内当局が自由に利用できるようにその適合宣言書を保管する。適合宣言書は，宣言書が作成された製品モデルを特定する。要求に応じて，その適合宣言書のコピーを適格な当局が利用できるようにされる。

The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

4. 権限のある代理者

Authorised representative

第 3 号の中で定められた製造者の義務は，委任状の中で適格な義務が定められていることを条件として，その製造者の代わりに，かつ，その製造者の責任の下において，その製造者の権限のある代理者によって満たされ得る。

The manufacturer's obligations set out in point 3 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

パート IV （モジュール H を基礎とする）完全な品質保証を基礎とする適合性
Part IV C**onformity based on full quality assurance (based on module H)**

1. 完全な品質保証を基礎とする適合性は，それによって，製造者が本パートの第 2 号及び第 5 号の中で定められた義務を満たし，かつ，関係するデジタルの要素をもつ製品または製品類型が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を満たしていること，及び，その製造者によって設けられた脆弱性取扱プロセスが別紙 I のパート II の中で定められた要件に適合していることをその製造者の単独の責任に基づいて確保しかつその旨を宣言する適合性評価手続である。

   Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 5 of this Part, and ensures and declares on its sole responsibility that the products with digital elements or product categories concerned satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Part II of Annex I.

2. デジタルの要素をもつ製品の設計，開発，製造及び脆弱性取扱

   Design, development, production and vulnerability handling of products with digital elements

   製造者は，関係するデジタルの要素をもつ製品の設計，開発及び最終製品検査と試験に関し及び脆弱性の取扱いに関し，本パートの第 3 号の中で細目が定められた承認された品質システムを運用し，サポート期間を通じて同品質システムの実効性を維持し，かつ，本パートの第 4 号の中で細目が定められた調査に服する。

   The manufacturer shall operate an approved quality system as specified in point 3 for the design, development and final product inspection and testing of the products with digital elements concerned and for handling vulnerabilities, maintain its effectiveness throughout the support period, and shall be subject to surveillance as specified in point 4.

3. 品質システム

   Quality system

   3.1. 製造者は，関係するデジタルの要素をもつ製品に関し，その製造者が選択する指定組織に対し，その製造者の品質システムの評価の申請を申立てる。

      The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned.

      申請書は，以下の事項を含める：

The application shall include:

(a) 製造者の名称及び住所，また，権限のある代理者によって申請が申立てられたときは，当該権限のある代理者の名称及び住所；

the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

(b) 製造されまたは開発されることが意図されたデジタルの要素をもつ製品の個々の類型の 1 つのモデルに関する技術文書。その技術文書は，それが適用可能なときはいつでも，少なくとも別紙 VII の中で定められた諸要素を含める；

the technical documentation for one model of each category of products with digital elements intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex VII;

(c) その品質システムに関する文書；及び

the documentation concerning the quality system; and

(d) 同一の申請が別の指定組織に対して申立てられなかったことの書面による宣言。

a written declaration that the same application has not been lodged with any other notified body.

3.2. 品質システムは，デジタルの要素をもつ製品が別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件を遵守することを確保し，かつ，その製造者によって設けられた脆弱性取扱プロセスが別紙 I のパート II の中で定められた要件を遵守することを確保する。

The quality system shall ensure compliance of the products with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Part II of Annex I.

製造者によって採用された全ての要素，要件及び条項は，体系的かつ順序立てられた態様により，書面による基本方針，手続及び指示の書式の中で文書化される。当該品種システム文書は，品質管理計画，企画書，マニュアル及び記録の一貫性のある解釈を許容する。

All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.

品質システムは，とりわけ，以下に関する適切な記述を含める：

It shall, in particular, contain an adequate description of:

(a) 品質目標，並びに，設計，開発，製品の品質及び脆弱性取扱と関連する運営管理の組織構造，責任及び権限；

the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;

(b) 技術標準を含め，適用されることになる技術上の設計及び開発の仕様，また，適格な整合化された技術標準または技術仕様が全面的には適用されないときは，そのデジタルの要素をもつ製品に適用されることになる別紙 I のパート I の中で定められた必須のサイバーセキュリティ要件に適合することを確保するために使用されることになる手段；

the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part I of Annex I that apply to the products with digital elements will be met;

(c) 技術標準を含め，適用されることになる手続の仕様，また，適格な整合化された技術標準または技術仕様が全面的には適用されないときは，その製造者によって設けられたプロセスに適用されることになる別紙 I のパート II の中で定められた必須のサイバーセキュリティ要件に適合することを確保するために使用されることになる手段；

the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part II of Annex I that apply to the manufacturer will be met;

(d) 設計及び開発の管理策，並びに，設計及び開発を検証する技術，適用される製品類型に含まれるデジタルの要素をもつ製品を設計及び開発する際に使用されることになる処理及び組織的活動；

the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products with digital elements pertaining to the product category covered;

(e) 対応する生産，品質管理及び品質保証の技術，使用されることになる処理及び組織的活動；

the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;

(f) 生産前，生産中及び生産後に実施されることになる審査及び試験，並びに，その審査及び試験が実施されることになる頻度；

the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;

(g) 検査報告書及び試験データのような品質記録，校正データ，関係者の資格報告書；

the quality records, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned;

(h) 要求される設計及び生産の品質の達成を監視する手段，並びに，品質システムの実効的な運用。

the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.

3.3. 指定組織は，品質システムが第 3.2 号に示す要件を満たしているかどうかを判定するため，その品質システムを評価する。

The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.

適格な整合化された技術標準または技術仕様を実装する国内技術標準の対応する仕様を遵守する品質システムの諸要素との関係において，当該要件の適合性が推定される。

It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard or technical specification.

品質管理システムにおける経験に加え，監査チームは，適格な製品分野及び関係する製品技術における評価者としての経験を積んだ少なくとも 1 名の構成員がおり，かつ，この規則の中で定められた適用可能な要件の知識をもつものとする。その監査は，そのような施設が存在するときは，製造者の施設の評価訪問を含める。監査チームは，この規則の中で定められた適用可能な要件を識別するための製造者の能力を検証するため，及び，デジタルの要素をもつ製品が当該要件を遵守することを確保するために必要となる審査を実施するため，第 3.1 号の(b)に示す技術文書を見直す。

In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and shall have knowledge of the applicable requirements set out in this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1 (b), to verify the manufacturer's ability to identify the applicable requirements set out in this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with digital elements with those requirements.

製造者及びその製造者の権限のある代理者は，その判定の通知を受ける。

The manufacturer or its authorised representative shall be notified of the decision.

その通知は，監査の結論及び理由を付した評価判定を含める。

The notification shall contain the conclusions of the audit and the reasoned assessment decision.

3.4. 製造者は，承認されたものとしての品質システムから生ずる義務を履行すること，及び，その品質システムが適切性と効率性を維持するように同システムを維持管理することを約束する。

The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

3.5. 製造者は，品質システムを承認した指定組織が，その品質システムに対する意図的な変更について連絡を受けることを保つ。

The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system.

指定組織は，提案された変更を評価し，かつ，修正された品質システムが第 3.2 号に示す要件を満足させ続けるかどうか，または，再評価が必要であるかどうかを判定する。

The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

その指定組織は，その製造者に対し，同指定組織の判定を通知する。その判定は，審査の結論及び理由を付した評価判定を含める。

It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

4. 指定組織の職責の下にある調査

Surveillance under the responsibility of the notified body

4.1. 調査の目的は，製造者が，承認された品質システムから生ずる義務を適正に満たすことを確実にすることにある。

The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.

4.2. 製造者は，評価の目的のために，指定組織が設計，開発，製造，検査，試験及び貯蔵の場所に対してアクセスすることを許容し，かつ，指定組織に対し，必要な全ての情報，とりわけ，以下の情報を提供する:

The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:

(a) 品質システムの文書;

the quality system documentation;

(b) 分析結果，計算結果及び試験結果のような，品質システムの設計のフェーズによって定められる品質記録;

the quality records as provided for by the design part of the quality system, such as results of analyses, calculations and tests;

(c) 検査報告書及び試験データのような品質システムの製造部分によって定められる品質記録，校正データ及び関係者の資格報告書。

the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned.

4.3. 指定組織は，製造者が品質システムを維持管理及び適用することを確実にするための定期監査を実施し，かつ，当該製造者に対し，監査報告書を提供する。

The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

5. 適合マーク及び適合宣言書

Conformity marking and declaration of conformity

5.1. 製造者は，別紙 I のパート I の中で定められた要件を満たす個々の具体的な製品に対し，CE マークを付し，かつ，第 3.1 号に示す指定組織の責任の下において，当該指定組織の識別番号を付す。

The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product with digital elements that satisfies the requirements set out in Part I of Annex I.

5.2. 製造者は，個々の製品モデル毎に書面による適合宣言を作成し，かつ，当該製品が市場に置かれた後 10 年間またはサポート期間のいずれか長い方の期間，国内当局が自由に利用できるように保管する。適合宣言書は，同宣言書が作成された製品モデルを特定する。

The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up.

要求に応じて，適合宣言書のコピーを関連当局が利用できるようにされる。

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

6. 製造者は，当該製品が市場に置かれた後 10 年間またはサポート期間のいずれか長い方の期間，国内当局が自由に利用できるように，以下の文書を保管する：

The manufacturer shall, for a period ending at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep at the disposal of the national authorities:

(a) 第 3.1 号に示す技術文書；

the technical documentation referred to in point 3.1;

(b) 第 3.1 号に示す品質システムに関する文書；

the documentation concerning the quality system referred to in point 3.1;

(c) 承認されたものとしての第 3.5 号に示す変更書；

the change referred to in point 3.5, as approved;

(d) 第 3.5 号及び第 4.3 号に示す指定組織の判定書及び報告書。

the decisions and reports of the notified body referred to in points 3.5 and 4.3.

7. 各指定組織は，その指定組織の通知元当局に対し，品質システムの承認の発行または取消しを連絡し，かつ，その指定組織の通知元当局に対し，定期的にまたは要請に応じて，拒否され，停止されまたはそれ以外の制限が行われた品質システムの承認のリストを利用できるようにする。

Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

各指定組織は，他の指定組織に対し，その指定組織が拒否し，取消し，停止しまたはそれ以外の制限を行った品質システムの承認を連絡し，また，要請に応じて，その指定組織が発行した品質システムの承認を連絡する。

Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

8. 権限のある代理者

Authorised representative

第 3.1 号，第 3.5 号，第 5 号及び第 6 号の中で定められた製造者の義務は，委任状の中で適格な義務が定められていることを条件として，その製造者の代わりに，かつ，その製造者の責任の下において，その製造者の権限のある代理者によって満たされ得る。

The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

2025 Printed in Japan
ISSN 2432-6089
法と情報雑誌　第 10 巻第 2 号（通巻第 63 号）
The Law and Information Magazine vol.10 no.2 (consecutive no.63)

2025 年 2 月 24 日発行
2025 年 3 月 31 日誤記等修正版発行
発行者　夏井高人
発行所　法と情報研究会（代表 夏井高人）
東京都千代田区神田駿河台 1－1
学校法人明治大学研究棟
（非売品）