**EUサイバーレジリエンス法のパブコメについて**

**現在、EUが法令整備中のサイバーレジリエンス法（Cyber Resilience Act）がパブリック・コンサルテーションを実施中。**

**＜パブコメ締め切り＞：2022年5月25日**

※上記ページの「Go to consultation>」と書かれた黄色いボタンをクリック。→「Respond to the questionnaire>」をクリック。ログインして回答。

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services\_en

**＜パブコメ質問内容＞**

**●セクション１：デジタル製品や使用者のためのサイバーセキュリティ**

**Section 1: Cybersecurity of digital products and the users of digital products**

**This section contains questions on the state of cybersecurity of digital products marketed in the European Union and users’ ability to choose secure products and use them in a secure manner, and the role that vendors can play in securing products and providing cybersecurity related information on their products.**

*Sub-section 1.a. – The state of cybersecurity of digital products*

**Q1:** In your view, what is the overall level of cybersecurity of digital products marketed within the European Union (on a scale from 1 to 5 with 5 indicating a very high level of cybersecurity)?

EU域内で販売されているデジタル製品のサイバーセキィリティレベル全体について、5段階で示して下さい。（１～５で）

**Q2:** In your view, during the last five years, how has the level of risk of cybersecurity incidents affecting digital products evolved?

過去５年間に、デジタル製品に影響するサイバーセキュリティインシデントのレベルについて、どのようになったと感じますか。５段階で示して下さい。

*Sub-section 1.b. – Consequences of cyber incidents and non-secure digital products*

**Q3:** How would you evaluate the actual impact of cybersecurity incidents affecting digital products on you or your organisation (on a scale from 1 to 5 with 5 indicating a very high negative impact)?

あなた自身やあなたの組織のデジタル製品に影響を与えるサイバーインシデントの実際のインパクトを以下の表の中で表して下さい。（１～５の５段階で）



**Q4:** In your view, if a digital product is not cyber secure, how does it impact the user (on a scale from 1 to 5 with 5 indicating that you fully agree)?

　デジタル製品がセキュアでない場合、ユーザーにとってどのようなインパクトを与えると思いますか。



*Sub-section 1.c. – Trust, cybersecurity awareness and capabilities of users*

Q5: To what extent do you agree with the following statements as regards your awareness and understanding of cybersecurity properties of digital products (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

　デジタル製品のサイバーセキュリティ特性についての認識と理解に関して、以下の記載内容にどの程度、賛同しますか。（１～５の5段階で）



 Sub-section 1.d - The role of vendors in providing secure digital products

**Q6:** To what extent do you agree with the following statements on the role of the vendors? Please rate the following statements on a scale from 1 to 5 (with 5 indicating that you strongly agree).

　ベンダーの役割に関する以下の記載について、どの程度、賛同しますか。（１～５の5段階で）



**Q7:**If you are a vendor: which of the following aspects have the biggest impact on your decision related to cybersecurity of your digital product?

　　もし、あなたがベンダーの場合、あなたのデジタル製品におけるサイバーセキュリティに関する意見に最も影響を与える要因は以下のうちどれですか？



**Q8:**To what extent are hardware manufacturers and software developers taking the cybersecurity of their digital products into account in each of the following phases of the product lifecycle (on a scale from 1 to 5 with 5 indicating that cybersecurity is taken very seriously)?

　ハードウェア製造者やソフトウェア開発者は、製品のライフサイクルにおける以下の各フェーズにおいてどの程度デジタル製品におけるサイバーセキュリティを考慮していますか。（１～５の5段階で）



**●セクション２：デジタル製品におけるサイバーセキュリティの改善**

**Section 2: Improving the cybersecurity of digital products**

**This section explores various policy options to improve the cybersecurity of digital products. This includes also questions on the types of products to be covered by an intervention, on other relevant legislation, on security requirements, on risk as well as ways to assess the conformity of manufacturers.**

*Sub-section 2.a. – Exploring ways to make digital products more secure*

**Q9:** To what extent do you think that the following measures could be effective in raising the level of cybersecurity of digital products marketed in the Union (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

　EU域内で販売されているデジタル製品におけるサイバーセキュリティのレベルを向上させる点で以下の方法がどの程度効果的だと思いますか。（１～５の５段階で）



**Q10:**How would you assess the impact of the following measures on the level of cybersecurity of digital products and of the consumers/organisations using such products (on a scale from 1 to 5 with 5 indicating that a measure would have a very high impact)?

　デジタル製品やそれを使用する消費者/組織のサイバーセキュリティレベルに関して、以下の方法をどの程度のインパクトがあると評価しますか。



*Sub-section 2.b. – Exploring ways to make users more aware*

**Q11:** How would you assess the relevance of the following measures for the users’ ability to evaluate the cybersecurity properties of a digital product and to make better informed purchase or usage decisions (on a scale from 1 to 5 with 5 indicating that a measure is very relevant)?

デジタル製品のサイバーセキュリティ特性を評価し、十分な情報に基づいて購入又は使用する点におけるユーザーの能力に対し、以下の方法がどの程度関連すると思いますか。（１～５の5段階で）



*Sub-section 2.c. – Digital products to be covered by a European initiative*

**Q12:** To what extent do you agree that subjecting certain products marketed in the Union to cybersecurity requirements would be effective (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

　EU域内で販売されている以下の製品をサイバーセキュリティ要件に遵守させることが効果的であるという点にどの程度賛同しますか。（１～５の5段階で）



*Sub-section 2.d. – Existing legislation on the cybersecurity of digital products*

**Q13:** To what extent do you agree with the following statements about how cybersecurity is addressed in existing EU legislation (e.g. the [General Product Safety Directive](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0095) and the [Machinery Directive](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006L0042-20190726), both currently under review; the [Delegated Regulation of 29 October 2021 under the Radio Equipment Directive](https://ec.europa.eu/growth/news/commission-strengthens-cybersecurity-wireless-devices-and-products-2021-10-29_en)) (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?

既存のEU法令におけるサイバーセキュリティの扱いについて、以下の記載にどの程度賛同しますか。（例：現在レビュー中の一般製品安全指令、機械指令、及び無線機器指令に基づく2021年10月29日の委任規則）（１～５の5段階で）



**Q14:** In the absence of horizontal cybersecurity requirements at European level, Member States could adopt national laws placing certain requirements on vendors. To what extent do you agree that there is a risk of increasing costs and legal uncertainty for market stakeholders, in the absence of an EU initiative? (on a scale from 1 to 5 with 5 indicating you fully agree)?

欧州レベルでの水平的なサイバーセキュリティ要件がない場合、EU加盟国はベンダーに特定の要件を課す国内法を採用する可能性があります。このようなEUのイニシアティブがない場合、市場のステークホルダーにとって、コストの増加や法的不確実性が生じるリスクがあることにどの程度賛同しますか。（１～５の５段階で）

**Q15:** If you are a vendor: are your digital products subject to legal requirements as regards their cybersecurity? In your answer, please take into account European, national but also legislation stemming from third countries.

　もし、あなたがベンダーの場合、あなたのデジタル製品は、EU法令・国内法・第三国の法令のサイバーセキュリティに関する法的要件を遵守していますか。（Yes/No）

*Sub-section 2.e. – Cybersecurity requirements for digital products*

**Q16:** Should hardware manufacturers and software developers be responsible for the full life cycle of a digital product (such as by being required to provide updates)?

ハードウェア製造者やソフトウェア開発者はデジタル製品のライフサイクル全てに責任を負うべきと思いますか？（例えば、更新を提供する必要性など）（Yes/No）

**Q17:** To what extent can the following approaches contribute to the cybersecurity of a digital product (on a scale from 1 to 5 with 5 indicating that a measure would be very effective)?

デジタル製品におけるサイバーセキュリティのために、以下のアプローチがどの程度貢献すると思いますか。（１～５の５段階で）



*Sub-section 2.f. – The role of risk*

**Q18:** Under this initiative, hardware manufacturers and software developers would need to demonstrate their compliance with cybersecurity requirements. Should digital products with a higher risk be subject to a stricter process of demonstrating conformity with these requirements?

　本イニシアティブでは、ハードウェア製造者とソフトウェア開発者は、サイバーセキュリティ要件への準拠を実証する必要があります。リスクの高いデジタル製品は、これらの要件への適合を実証するためにより厳格なプロセスの対象とすべきと思いますか。（Yes/No）

*Sub-section 2.g. – Demonstrating compliance with security requirements*

**Q19:** How would you assess the following statement regarding self-declaration as a way for hardware manufacturers and software developers to demonstrate compliance with security requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree)?

ハードウェア製造者とソフトウェア開発者がセキュリティ要件への準拠を実証する方法として、自己宣言に関する以下の記載をどのように評価しますか。（１～５の5段階で）



**Q20:** If you consider that self-declaration is not enough to demonstrate compliance with security requirements, do you think that the involvement of a third party should be required under certain circumstances?

セキュリティ要件への準拠を実証する方法として、自己宣言が不十分であると考える場合、特定の状況下では第三者機関の関与が必要だと思いますか。（Yes/No）

**●セクション３：潜在的な規制措置のステークホルダーへの影響**

**Section 3: Stakeholder impact of potential regulatory measures**

**This section focuses on the EU added value and estimated impacts of potential measures on stakeholders.**

*Sub-section 3.a. – Relevance of horizontal requirements for digital products at European level*

**Q21:** To what extent do you agree with the following statements that look into the potential effectiveness of an EU initiative on horizontal (cross-sectoral) cybersecurity requirements?

水平的（分野横断的）なサイバーセキュリティ要件に関するEUのイニシアティブの潜在的な有効性を検討するための以下の記述にどの程度賛同しますか。



**Q22:** The [EU Action Plan on synergies between civil, defence and space industries](https://ec.europa.eu/info/files/action-plan-synergies-between-civil-defence-and-space-industries_en) underlines the importance of promoting and applying common standards across sectors and the increased relevance of digital products that are used both in a civilian and military context (‘dual-use products’). To what extent could horizontal requirements applying to digital dual-use products contribute to moving the security performance of such products closer to the needs of the defense community and to raising the overall level of cybersecurity in civilian uses (on a scale from 1 to 5 with 5 indicating a very positive contribution)?

　民間・防衛・宇宙産業間の相乗効果に関するEU行動計画は、分野横断の共通の基準を推進/適用することの重要性と、民間・軍事の両方の文脈で使用されるデジタル製品（デュアル・ユース製品）の関連性の向上を強調しています。デジタルデュアルユース製品に適用される水平的要件は、そのような製品のセキュリティパフォーマンスを防衛業界のニーズに近づけ、民間用途のサイバーセキュリティの全体的なレベル向上にどの程度貢献できると思いますか。（１～５の5段階で）

*Sub-section 3.b. – Impact on your organisation in terms of cost*

**Q23:** How would you assess the impact of the following types of intervention on the costs of your organisation (on a scale from 1 to 5 with 5 indicating that the intervention would be very costly)?

以下のタイプの介入について、組織のコストに与える影響をどのように評価しますか。（１～５の5段階で）



*Sub-section 3.c. – Regulatory burden and costs for small and medium-sized companies*

**Q24: Which of the following approaches would in your view ensure that small and medium-sized hardware manufacturers and software developers, including individual entrepreneurs, are subject to proportionate obligations (balance between administrative burden and compliance costs on the one hand and a high level of cybersecurity on the other hand) under a European legislation introducing mandatory horizontal cybersecurity requirements (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?**

サイバーセキュリティにおける水平的な強制要件を取り入れたEU法令において、個人起業家を含む中小のハードウェア製造者やソフトウェア開発者がどの程度の義務を負うべきと考えますか。（行政的な負荷やコンプライアンスコストと高レベルでのサイバーセキュリティとをバランスさせる意味で）（１～５の5段階で）



*Sub-section 3.d. – Impact on competition*

**Q25: An EU initiative laying down mandatory horizontal cybersecurity requirements would apply to all vendors placing products on the internal market, irrespective of their origin and location. To what extent would you agree with the following statements regarding the impact on competition of such an initiative (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?**

サイバーセキュリティにおける水平的な強制要件を規定するEUイニシアティブは、製品の原産地や場所に関わらず、製品を国内市場に上市する全てのベンダーに適用されます。そのようなイニシアティブが競争環境にどの程度影響を与えると思いますか。（１～５の5段階で）



*Sub-section 3.e. – Impact on fundamental rights*

**Q26: To what extent to you agree with the following statements regarding the impact of horizontal cybersecurity requirements on fundamental rights (on a scale from 1 to 5 with 5 indicating that you strongly agree with a statement)?**

　基本的権利に関し、水平的なサイバーセキュリティ要件の影響について、次の記載にどの程度賛同しますか。（１～５の５段階で）



●**セクション４：その他**

**Section 4: Other issues**

**This section focuses on cybersecurity challenges for the internal market other than those related to digital products.**

**Q27:** In addition to the issues above, are there other cybersecurity related challenges not directly linked to the cybersecurity of products that you think the Cyber Resilience Act should include to enhance the cyber resilience of the internal market? Please elaborate

上記の内容に加えて、製品のサイバーセキュリティに直接は関係しないもののサイバーレジリエンス法に含めるべき課題はありますか。