サイバーレジリエンス法におけるオープンソース・スチュワードの義務とその履行

山中倫太郎（D1）

はじめに

サイバーレジリエンス法（以下、CRA）とは、欧州連合でリリースされるデジタル要素を含む製品に対して包括的なサイバーセキュリティ要件を導入し、ソフトウェア製品のサプライヤ ー、製造業者、輸入業者及び販売業者に新たな義務を課すものである。同法の規制は、ソフトウェア業界及びハードウェア業界に統一的なサイバーセキュリティ標準を導入しようとするもので、本稿が特に対象とするオープンソースソフトウェアスチュワード（以下、OSS スチュワード）の開発及び展開にも多大な影響を及ぼすものである。

本稿では、この法律で規律されている事項のうち、特に OSS スチュワードの義務とその履行について紹介し、解説を加える[1]。

１．CRA が適用される製品

CRA が適用される製品は、デジタル要素を備えた製品（Product with Digital Elements[PDE]）である。これは、ソフトウェア又はハードウェア製品及びその遠隔データ処理ソリューションをいい、別個に上市されるソフトウェア・ハードウェアコンポーネントを含む（３条１号)。例えば、IoT 機器、スマートデバイス、通信機器がこれに該当することになる。但し、PDE の意図された目的や合理的に予見される使用が、デバイスやネットワークへの直接的又は間接的な論理的・物理的なデータ接続を含む場合にのみ、CRA が適用される（２条１項)。

本稿のテーマとの関係で特に関心を引くのは、オープンソースソフトウェア（以下、OSS）が PDE に該当するか否かである。CRA では、フリー・OSS（Free and Open-Source Software[FOSS]）とは、ソースコードがオープンに共有され自由にアクセスし、使用し、改変し、再配布できるようにする、すべての権利を提供するフリー・オープンライセンスの下で利用できるようにされたソフトウェア（３条４８号）をいう。この意味における OSS も PDE に含まれ、原則的に CRA の規制対象となる。というのは、PDE は、その定義からして、デバイスやネットワーク接続性を備えたソフトウェアを含むのであって、そのソースコードがオープンになっているかどうかは問わないからである。

２．PDE の商業的提供

もっとも、およそ PDE であれば、すべてが CRA の適用の対象となるわけではない。そこには限定があり、PDE の商業的提供について規制がかかることになる。

---

[1] なお、本稿は、情報セキュリティ大学院大学の博士課程での学修の過程において作成された文書であり、この分野の法律の専門家としての立場で作成されたものではない。そのため、その内容について本稿筆者が法的な責任を負いかねることに留意されたい。

PDE の商業的提供とは、商業活動の一環として PDE を供給すること（「市場への提供」）（３条２２項）を指している。商業活動の例として、例えば、①PDE の料金を請求する、②テクニカルサポートサービスに対して実際の費用を超えて請求、③製造業者が他のサービスを収益化するためのソフトウェアプラットフォームを提供することによって収益化する、④非常に狭い理由(ソフトウェアのセキュリティ、互換性、又は相互運用性の向上)以外の理由で個人データを要求する、⑤費用を上回る寄付を受け付けるといった行為を挙げることができる[2]。これらの行為は、直接のマネタイズ行為のみならず、間接のマネタイズ行為を含んでいるといえるだろう。これに対して、利益を目的としない寄付の受入は、商業活動とはみなされない（前文１５）。

このように CRA の規制対象を商業的な提供に限定する見地からして、商業的な提供ではない PDE は、CRA の規制対象にはならないことになる。OSS のうち商業活動の過程で頒布又は使用されるために市場に提供されたものでないものが、CRA の適用から除外（前文１８号）されていることも、そのことの帰結である。このことは、非商業的なオープンソースコミュニティへの貢献を CRA の規制の対象外とすることによって非商業的なオープンソースコミュニティの自律的な発展を CRA が妨げないようにするために重要である。

OSS の商業的性質の問題については、CRA 自身が次のように詳説している点も踏まえる必要があろう。「より具体的には、この規則の目的上、およびその範囲に該当する経済事業者に関連して、開発段階と供給段階を明確に区別するために、メーカーによって収益化されていない無料の OSS として適格なデジタル要素を備えた製品の提供は、商業活動と見なすべきではありません。さらに、他のメーカーがデジタル要素を備えた自社製品に統合することを目的とした、無料の OSS コンポーネントとして認定されるデジタル要素を備えた製品の供給は、コンポーネントが元のメーカーによって収益化されている場合にのみ、市場で利用可能であると見なす必要があります。たとえば、デジタル要素を備えた OSS 製品がメーカーから財政的支援を受けているという事実、またはメーカーがそのような製品の開発に貢献しているという事実自体は、その活動が商業的な性質を持っていると判断するものではありません。さらに、定期的なリリースが存在するだけでは、デジタル要素を含む製品が商業活動の過程で供給されるという結論につながるべきではありません。最後に、この規則の目的上、非営利団体によるフリーおよび OSS として認定されるデジタル要素を備えた製品の開発は、その組織が費用を差し引いたすべての収益が非営利目的の達成に使用されることを保証する方法で設立されている限り、商業活動とは見なすべきではありません。この規則は、その責任下にないフリーおよび OSS として認定されるデジタル要素を含む製品にソースコードを提供する自然人または法人には適用されません。」（前文１８号）

---

[2] Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers（https://best.openssf.org/CRA-Brief-Guide-for-OSS-Developers）

３．CRA における主体と義務（全体像）

CRA は、主体の違いごとに、これに異なった義務を課している。OSS スチュワードの義務を明らかにする上で、この主体の区別が意味をもつので、ここでその区別について明らかにしておくことにしよう。

（１）製造業者（manufacturer）

CRA において最も中心的な地位を占めるのは、製造業者である。製造業者とは、デジタル製品を開発若しくは製造する、又はデジタル製品を設計、開発若しくは製造させ、有償、収益化、無償を問わず、その名称又は商標の下で販売する自然人又は法人を指している（３条１３号)。CRA では、製造業者の他に、輸入業者、流通業者にもそれぞれ一定の義務が課されているが、CRA では、製造業者に最も厳格な義務を課されており、OSS スチュワードの義務を理解する上でも、まずは製造業者に焦点を当てることが必要であるので、本稿では、以下、製造業者の義務を概説した後に、これとの関係で OSS スチュワードの義務を概観する。

製造業者の主な義務として次の内容がある。まず、上市前の義務である。サイバーセキュリティ要件[3]を満たすように[4]デジタル製品が設計、開発及び製造されていることを保証することである（１３条１項)。このために、①サイバーセキュリティアセスメントの実施及び文書化（１３条２項、３項)、②技術文書の作成（１３条１２項、３１条)、③CE マークのデジタル製品への貼付（１３条１２項、２９条、３０条）などが具体的に求められることになる。第三者のコンポーネント（OSS を含む）を組み込む場合には、当該製品についてデューディリジェンスを実施する。その製品がセキュリティリスクを高めるものではないことを確認する必要がある（１３条５項)。次に、上市時及び上市後の義務である。これには、①デジタル製品がセキュリティ要件に適合した状態を維持するための手続の確保（１３条１４項)、②脆弱性情報等の体系的文書化、最低５年間の「サポート期間」（１３条８項）にわたるサイバーセキュリティリスクアセスメント結果のアップデート（１３条３項）などが求められる。さらに、報告・通知義務である。これには、①脆弱性を認識した場合に CSRT 及び ENISA への報告（１４条１項、２項)、②重大インシデントを認識した場合における報告（１４条３項、４項）である。

（２）OSS スチュワード

CRA において製造業者とは区別される主体が、OSS スチュワードである。OSS スチュワードとは、製造業者以外の法人であり、商業活動を目的とした特定のデジタル要素を備えた製品の開発を持続的に支援し、その製品の存続可能性を確保することを目的または目標とするもの（CRA３条１４号）を指している。OSS スチュワードは、製造業者に提供さ

---

[3] サイバーセキュリティ要件は、セキュリティ要件と脆弱性対応要件に分かれる。

[4] サイバーセキュリティ要件への適合性評価の手続きは、デジタル製品のカテゴリーによって異なる。①クリティカルなデジタル製品、②重要なデジタル製品、③通常のデジタル製品。

れる OSS の開発を体系的に支援するが、自身は収益化しているわけではない。

CRA において OSS スチュワードとして予定されているのは、その定義にもみられるように、製造業者以外の「法人（legal person）」―「自然人（natural person）」と対比される―であり（３条１４号）、Git Hub 上の FAQ にもそのような考えが示されている[5]。通常はオープンソース財団や重要なプロジェクトをサポートする専任の維持・管理組織で構成されている[6]。OSS スチュワードとして立法者が念頭においていた組織の例は、特定の FOSS プロジェクトを支援する財団、FOSS を自社で構築しているが、公開している企業、FOSS を開発する非営利団体である[7]。一つの組織が、あるプロジェクトにとって製造業者とみなされ、別のプロジェクトにとって、OSS スチュワードとみなされることがあることも指摘される[8]。

OSS スチュワードは、製造業者に比してより軽い義務を負うにとどまる。スチュワード自身は、製造業者とは異なって、OSS コンポーネントを商業提供せず、寄附や会費によって運営資金をまかなう。OSS スチュワード自身がセキュリティに関して責任を負うことが不可能である。にもかかわらず、CRA が厳しい責任を課すと、OSS コミュニティの発展が阻害される恐れがあるからである。このように製造業者と区別される OSS スチュワードには、より軽減された責任を負わせるにとどまるようにすることは、「セキュリティ要件と OSS 開発のユニークな貢献性とのバランスを取るために設計された意図的なアプローチ」[9]である。

OSS スチュワードが CRA に基づいて負う義務の概要は、次の通りである。まず、サイバーセキュリティポリシーの策定及び文書化がある。このポリシーには脆弱性の文書化、対処及び修正に関する内容を含める必要がある。次に、市場監視当局（MSA）との協力、及びサイバーセキュリティリスクに対応するための文書提供がある。例えば、 法的通知や問い合わせに対応する責任者を明確化すること、MSA の要請に応じて技術文書やセキュリティ情報を提出できる体制を整備することがこれに該当する。さらに、既知の脆弱性の報告、重大インシデントの報告、影響を受けたユーザーへの通知、緩和策の提供がある。これは、製造業者の報告・通知義務がセキュリティに影響を与える重大なインシデントが、OSS の管理者が提供するネットワーク及び情報システムに影響を与える範囲で適用される。例えば、脆弱性報告窓口の設置、脆弱性の評価・修正・公開のプロセス整備、欧州ネットワーク・情報セキュリティ機関（ENISA）や製品製造業者からの報告に対応できる体制構築が挙げられる。また、任意のセキュリティ認証プログラムの設立も挙げることが

---

[5] Git Hub サイト（https://github.com/orcwg/cra-hub/blob/main/faq.md#faq-tmp-124）

[6] Adrienn Lawson, Stephen Hendrick, Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source, 2025, p.10.

[7] 2024 年 FOSDEM における Benjamin Bögel のスライド（https://archive.fosdem.org/2024/events/attachments/fosdem-2024-3683-the-regulators-are-coming-one-year-on/slides/22201/Slides_CRA_FOSDEM_v3_ukPnQUG.pdf）; Git Hub サイト（https://github.com/orcwg/cra-hub/blob/main/faq.md#faq-tmp-11）

[8] 欧州委員会 Benjamin Bögel の説明。

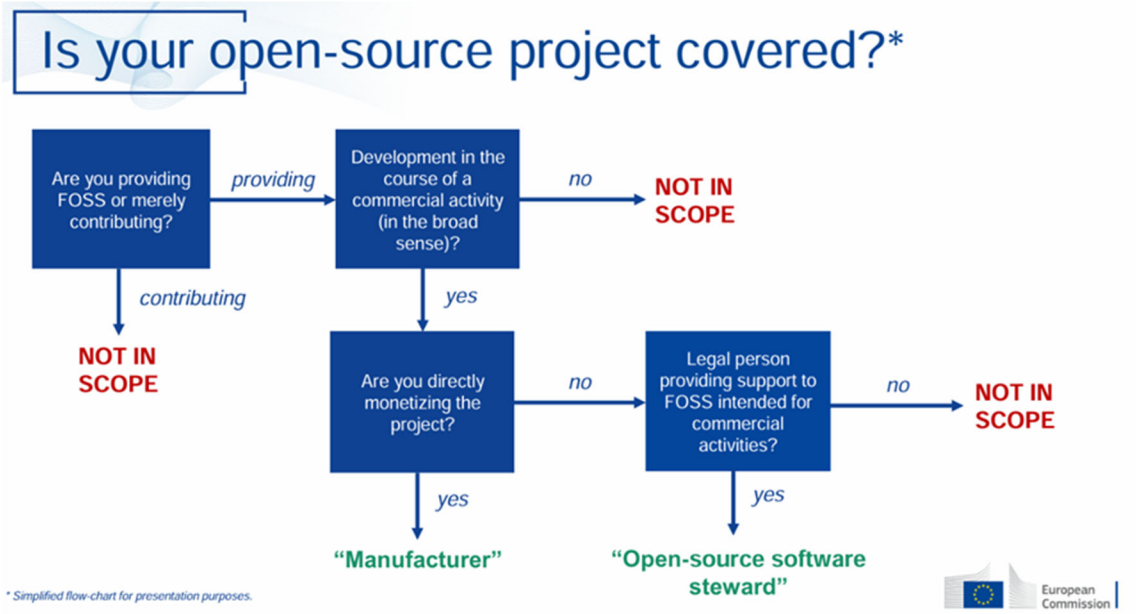
[9] Lawson, Hendrick, Unaware and Uncertain, p.9.

できる。

（３）CRA の射程外の主体

CRA において製造業者でもないし、OSS スチュワードでもない主体は、CRA の規制の対象外となる。このような主体は、報告書『認識不足と不明確な現状』（２０２５年）において「非営利開発者」とカテゴライズされている。同報告書は、これに該当するかどうかを判定するために、「私は、利益を期待せず、商用利用を目的とせずに、（単独で、もしくはチームや コミュニティの一員として）自主的に OSS プロジェクトを開発しています。」という問いを用いており、わかりやすいイメージを提供している。

＜各主体を識別するためのフロー＞



出典：2024 年 FOSDEM における Benjamin Bögel のスライド[10]

４．製造業者と OSS スチュワードの協力関係の形成

OSS スチュワード自身の義務とは別に、製造業者が CRA の義務を履行する際に OSS スチュワードが製造業者とどのような協力関係が必要となるか、その結果として、CRA の制定によってどのような協力関係が形成されるようになるかという問題がある。

製造業者の側からみると、OSS スチュワードが提供する OSS が製品に統合される場合、製造業者は、そのセキュリティ品質や脆弱性管理の体制が問われる（デューディリジェンスの履行（１３条５項））。このことから、製品に統合する OSS のセキュリティ品質が厳格に問われ、よりセキュアな OSS が選好されるようになるだろう。他方、OSS　スチュワードの側からみると、OSS スチュワードは、製造業者のデューディリジェンスの履行を

[10] 2024 年 FOSDEM における Benjamin Bögel のスライド（https://archive.fosdem.org/2024/events/attachments/fosdem-2024-3683-the-regulators-are-coming-one-year-on/slides/22201/Slides_CRA_FOSDEM_v3_ukPnQUG.pdf）

支援することが求められ、たとえば、SBOM の提供の支援を実施すること、OSS のバージョン、依存関係、ライセンス情報等の情報を機械可読形式で提供することが求められるかもしれない。また、OSS スチュワードは OSS の保守者として脆弱性報告の受け手となる可能性があり（１３条６項参照)、報告を受けた後に、対応責任が生じるかもしれない。こういった支援は、CRA において OSS スチュワードの義務ではないが、製造業者と OSS スチュワードの契約関係によっては、契約上の義務とされることも考えられるだろう。

このように CRA の製造業者への規制が OSS スチュワードへと波及する影響については、次のような的確な指摘が参考になる。「この規制の影響は、文書化や脆弱性報告にとどまらず、上流のオープンソースプロジェクトと下流の商業的採用者との関係を根本的に変え、持続可能なセキュリティ維持のためにより大きな協力を求めています。製造業者もスチュワードも、CRA の要件を単独で満たすことはできません。製造業者はオープンソースコンポーネントを統合する際に適切なデューディリジェンスを行う必要があり、スチュワードはセキュアな開発を促進するサイバーセキュリティポリシーを実施し、文書化しなければなりません。」[11]。それは、また、CRA による OSS のエコシステムの転換という視点からは、次のようにいうこともできよう。「CRA は、製造業者が上流の修正に貢献し、オープンソースプロジェクトに資金援助を提供することを、商業活動として分類されることなく明示的に許可している。これにより、製造業者は、直接的なコード貢献、セキュリティの改善、持続可能な資金調達モデルなどを通じて、受動的な消費からオープンソースエコシステムへの積極的な参加へと移行する機会が得られる。」[12]

５．OSS スチュワードに該当する組織・団体

ここまでの CRA に関する一般論を踏まえて、個別具体的な組織・団体やそれによってホストされた OSS プロジェクトと CRA の関係について検討することにしよう。この問題は、CRA の適用の問題である。

ここで再度、OSS スチュワードの定義を確認しておくと、OSS スチュワードとは、製造業者以外の法人であり、商業活動を目的とした特定のデジタル要素を備えた製品の開発を持続的に支援し、その製品の存続可能性を確保することを目的または目標とするもの（CRA３条１４号）を指す。また、そのソフトウェアは、「最終的に商業活動を目的」としていなければならない（recital 19)。

この定義にあてはまるのは、具体的に実在する、どのような組織・団体であろうか。管見の限りであるが、この点について EU の公的機関が公権的な判断を下したものが見当たらないため、ここでは、本稿筆者なりの評価が示されるにとどまる。

（１）OSS スチュワードに該当する組織・団体

[11] Anna Hermansen, Pathways to Cybersecurity Best Practices in Open Source: How Three Linux Foundation Projects are Leading the Way in CRA Compliance, 2025, p.5.
[12] Lawson, Hendrick, Unaware and Uncertain, p.12.

① Linux Foundation

Linux Foundation は、アメリカ（カリフォルニア州）に本拠を置く非営利団体である。米国の連邦税法に基づく 501(c)(6)という分類に該当する。このタイプの団体は、主に業界やビジネスの発展を目的として設立されている。企業メンバーには、Intel、IBM、SAMSUNG、Microsoft、FUJITSU、HITACHI などがある。企業が商業活動に OSS を活用できるよう、技術基盤、教育、標準化、コミュニティ支援を包括的に提供している。Linux Foundation は、800 以上の OSS プロジェクトをホストしており、代表的なプロジェクトには、Open SSF、Yocto Project、Zephyr Project、Civil Infrastructure Platform がある。

Linux Foundation は、法人であり、その目的も、商業目的のために OSS を開発を持続的に支援し、その製品に存続可能性を確保することを目的としており、プロジェクトによっては、そのソフトウェアが最終的に商業活動を目的としているといえる。そのようなプロジェクトとの関係で、Linux Foundation は OSS スチュワードに該当するといえよう。実際、Linux Foundation 自体、そのような自己認識の下に、積極的に CRA に適合的なプラクティスを模索している。

② Eclipse Foundation

Eclipse Foundation は、ベルギーに拠点を置く非営利国際団体（AISBL）であり、企業メンバーには、IBM、HUAWEI、Microsoft、FUJITSU、ORACLE などがある。「オープンソースプロジェクトを成功に導くための環境を作り、Eclipse 技術が商業およびオープンソースの解決策として採用されるよう促進すること」に焦点を置き、「オープンソースソフトウェアのコラボレーションとイノベーションのためのビジネスフレンドリーな環境を、個人や組織から成るグローバルなコミュニティに提供」[13]している。また、コミュニティ主導で産業向けのオープンソースイノベーションを可能にしてきた実績がある。また、Adoptium、Software Defined Vehicle、Jakarta EE、Eclipse IDE など、410 以上のオープンソースプロジェクトをホストしている[14]。

Eclipse Foundation も、法人であって、その目的も、商業目的のために OSS を開発を持続的に支援し、その製品に存続可能性を確保することにあるといえる。プロジェクトによっては、そのソフトウェアが最終的に商業活動を目的としているといえよう。

（2）OSS スチュワードに該当しない組織・団体

① Software in the Public Interest (SPI)

SPI は、アメリカ（ニューヨーク州）で登録された非営利団体である。その使命は、「大規模かつ重要なオープンソースプロジェクトを支援することで、非技術的な管理業務を引き受け、彼らが独自の法的実体を運営する必要がないようにすること」[15]にある。目的

---

[13] Eclipse Foundation のサイト（https://www.eclipse.org/org/）

[14] 同上

[15] Software in the Public Interest のサイト（https://www.spi-inc.org/）

は、一般利用可能なソフトウェアやシステムの提供と品質向上を目指すこと、教育活動やワークショップを開催すること、また、コンピューターやソフトウェアの適切な使用促進すること、資金調達を通じてこれらの目標を実現するために、公共・教育・政府組織と協力することなどがある[16]。寄付は SPI に対して行われるため、寄付の受付窓口として機能する。プロジェクトとして、Debian、LibreOffice、PostgreSQL などがある。

SPI は、法人ではあるが、その目的は、商業目的の OSS を開発する点にあるとはいえない。このことからして、SPI は OSS スチュワードには該当しないと考えられる。

② Free Software Foundation (FSF)

FSF は、アメリカ（マサチューセッツ州）に本拠を有する非営利団体であり、「コンピューター利用者の自由を推進する世界的な使命を持ち、全てのソフトウェア利用者の権利を擁護」することを目的とし、「コンピューター利用者の自由を守るために、自由（ここで「自由」とは、自由な権利を意味する）のソフトウェアやドキュメントの開発と使用を推進している[17]。２６カ国に５０００人のアクティブメンバーが所属している[18]。プロジェクトとして、GNU プロジェクトなどがある。

FSF も、法人ではあるが、その目的は、商業目的の OSS を開発する点にあるとはいえず、むしろ主に啓蒙団体としての性格がみられる。このことからして、FSF は OSS スチュワードには該当しないと考えられる。

６．OSS スチュワードとプロジェクトの関係

CRA において OSS スチュワードトプロジェクトはどのような関係にあるのであろうか。この点も、CRA における OSS スチュワード該当性の問題において一つの問題となる。

まず、すべての OSS プロジェクトが OSS スチュワードをもつわけではない[19]ことに注意が必要であろう。CRA においても、すべてのプロジェクトがスチュワードをもたなければならないこととはされていない。実際、収益化の意図がない者や趣味で OSS 開発をしている者によって運営されているプロジェクトは、スチュワードをもたない状態で OSS をリリースされることがある。このような OSS を製品に利用する場合にも、製造業者は、OSS のセキュリティ品質等についてデューディリジェンスを果たさなければならない。

では、あるホスト団体によって OSS プロジェクトがホストされている場合に、CRA 上の責任を負うのは、プロジェクトなのであろうか、それともホスト団体なのであろうか。この点、CRA 法における位置づけは、いくぶん不明確であり、明確なガイダンスの必要性が認識されることもあるようである。

---

[16] 同上

[17] The Free Software Foundation のサイト（https://www.fsf.org/about/）

[18] 同上

[19] Git Hub のサイト（https://github.com/orcwg/cra-hub/blob/main/faq.md#faq-tmp-11）

ここでは、Linux Foundation（ホスト団体）と Civil Infrastructure Platform（OSS プロジェクト）の関係をみる。CIP は、OSS のスチュワードとして機能しており、企業が自社の PDE やサービスを開発するために使用する OSS をリリースしている[20]。CIP 自体は PDE や商業サービスをリリースすることはなく、OSS を補完する商業的な提供も行っていない。CIP につき、Linux Foundation の側では、次のような理解が示されている。いわく、「CIP の場合、我々の理解では、プロジェクトをホストする法人としての Linux Foundation がスチュワードとなり、CRA 関連のコンプライアンス活動を CIP に委任する形になると考えられます。」[21]。CRA の責任は、ホスト団体に課せられ、その履行を実際に担うのはプロジェクトということであろう。

７．CRA における OSS スチュワードの義務の履行の実際上の困難

CRA における OSS スチュワードの義務が実効的に果たされるためにいくつかの支障が指摘されている。以下、二点のみ挙げておく。

（１）OSS スチュワード該当性判断の困難

一つ目に、製造業者、OSS スチュワード、非営利 OSS の間の区別を実際に適用することが困難であることがある。CRA における OSS スチュワードの定義は、いくぶん抽象的であるのに対して、実際に存在している OSS 組織・団体は、その目的、メンバーシップ、組織形態等、極めて多様である。そのような事情を前にして、OSS スチュワードの定義にあてはまる組織・団体とは何かを判断するのは、場合によっては容易ではない。「これらカテゴリーは、理論上は明確に見えるかもしれませんが、これらの区別を実際に実装することは、特に組織や個人がオープンソースエコシステム内で複数の役割を果たす場合には、かなり複雑であることが分かっています。」[22]というように指摘されることもある。

このような難しさに直面して、CRA 自体に対して懐疑的な意見もみられる。また、より明確なガイドラインの制定を要求する向きもあるようである。

（２）OSS スチュワードのリソースの制約

二つ目に、OSS スチュワードのリソースの制約の問題がある。OSS スチュワードが ORA の義務を果たすためには、相応の人員及び資金が必要となるが、次のような実態があることが報告されている。「スチュワード組織の３２％がインシデント対応の専用リソースを持っていると報告していますが、大多数はリソースの制約に直面しています。５６％は専任の人員または資金が不足しており、６％はセキュリティインシデントに迅速に対応できないと明確に述べています。」[23]

このような問題を克服するための一つの策は、OSS を組み込むことによって収益化を図り、かつ、その製品のセキュリティについて責任を負っている製造業者から OSS スチュワ

---

[20] Hermansen, Pathways to Cybersecurity Best Practices in Open Source, p.14.
[21] Ibid.
[22] Lawson, Hendrick, Unaware and Uncertain, p.9.
[23] Lawson, Hendrick, Unaware and Uncertain, p.18.

ードに資源を割り当てることである。そのためには、「製造業者は、CRA に基づき、依存している OSS のセキュリティ維持について主要な責任を負うため、受動的な OSS 利用者から積極的な貢献者へと変革する必要がある」[24]。CRA が、そのような変革によって OSS のエコシステムを実際に転換しうるかどうか、今後の CRA の運用のあり方が注目されよう。

８．OSS スチュワードの義務の履行のベストプラクティス

（１）Zephyr Project の例

Zephyr Project とは、Linux Foundation がホストする OSS プロジェクトであり、リソース制約のあるデバイス向けに最適化された、優れた小型でスケーラブルなリアルタイムオペレーティングシステムの構築に焦点を当てたオープンソースプロジェクトである[25]。

Zephyr Project は、GitHub を基盤としたリリース管理に中心を置いた構造的な開発実践を実施し、セキュリティの概要、セキュアコーディングガイド、センサー機器の脅威モデルを含む豊富なドキュメントを提供をしている。

Zephyr が CVE 番号付与機関（CVE Numbering Authority）としての地位を有していることにより、PSIRT 当局との脆弱性通知に関する直接的なやり取りが可能となっている。プロジェクトは直接報告された情報を積極的に監視しており、セキュリティ関連のリクエストには通常 1～2 日で対応する、レスポンスの良いボランティアベースの体制を維持している。また、任意参加の信頼性検証プログラムに参加している[26]。

（２）Civil Infrastructure Platform の例

Civil Infrastructure Platform は、Linux Foundation がホストする OSS プロジェクトであり、基礎インフラプロジェクトにおけるソフトウェア構成要素の利用と実装を可能にする、産業グレードのコアとなる OSS コンポーネントの基盤層を確立することに焦点がある[27]。

CIP は確立されたオープンソースインフラを活用した開発プラクティスを実施しており、すべてのソフトウェアのソースコードを kernel.org と GitLab 上で公開している。リリースプロセスは CIP のウェブサイト上で詳細に文書化されており、公開監査が可能であり、産業オートメーションおよび制御システムの安全な開発に関する IEC 62443-4-1:2018 の要件に準拠している[28]。

CIP のサイバーセキュリティポリシーは GitLab 上で管理されており、IEC 62443-4-1 の要件に準拠している。脆弱性の報告は公開チャネルを通じて行われるが、責任ある開示のための非公開メールアドレスも用意されている。報告メカニズムとしては主にメーリングリストが使用され、Linux カーネルや Debian コミュニティで確立されたプロセスと統

---

[24] Lawson, Hendrick, Unaware and Uncertain, p.19.
[25] Hermansen, Pathways to Cybersecurity Best Practices in Open Source, p.20.
[26] Ibid.
[27] Hermansen, Pathways to Cybersecurity Best Practices in Open Source, p.14.
[28] Hermansen, Pathways to Cybersecurity Best Practices in Open Source, p.15.

合されている。CIP は契約したメンテナーを保持し、メンバー企業からの重要なコミットメントを得ており、その結果、リクエストに対する迅速かつ慎重な対応が可能である[29]。

おわりに

CRA の規制自体、今後 EU のガイドラインや法の適用例等を通じて、より具体的かつ明確なものへと発展していくことが予想される。その意味で、本稿の検討もまた、暫定的なものに過ぎない。今後の展開を踏まえて、アップデートされるべきものであるといえるだろう。

[29] Ibid.