THE LINUX FOUNDATION | Europe

THE LINUX FOUNDATION | Research

オープンソースにおけるサイバーセキュリティ ベストプラクティスへの道

Civil Infrastructure Platform、
Yocto Project、Zephyr Project は
どのようにしてサイバーレジリエンス法の
要件を満たすためのギャップを埋めているか

2025年3月

Mirko Boehm, PhD, The Linux Foundation
Hilary Carter, The Linux Foundation
Cailean Osborne, PhD, The Linux Foundation

序文：Miriam Seyffarth,
Open Source Business Alliance

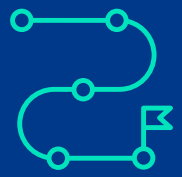
SPONSORED BY:

CIVIL INFRASTRUCTURE PLATFORM
OpenSSF OPEN SOURCE SECURITY FOUNDATION
yocto PROJECT
Zephyr™

CRA は、**デジタル要素を含む製品（PDE）に対して規制による監督**を導入しており、関係者グループ全体にわたってOSS の開発に重要な影響を及ぼします。

CRA では、**OSS スチュワード**という新たな役割が定義されており、これは自ら収益化していないオープンソース技術の開発を体系的に支援する組織を指します。

CRA の下では、**OSS スチュワードはサイバーセキュリティ ポリシー、脆弱性の取り扱いや報告のためのプロセス、市場監視機関（MSA）**との連携、そして自主的な**セキュリティ宣言**に対して責任を負います。

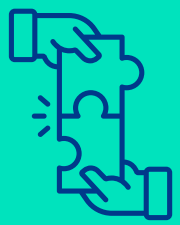


オープンソース プロジェクトは、CRA のタイムライン要件に備えるために、PSIRT チームやセキュリティ ポリシーへの投資を行いながら、**5 年間のセキュリティ ロードマップ**を策定する必要があります。

標準化されたセキュリティ ツールは CRA への準拠を加速させており、**SPDX 3.0、OpenSSF Scorecard、OpenChain** の各フレームワークが、プロジェクトによるセキュリティのベストプラクティスの実装を支援します。

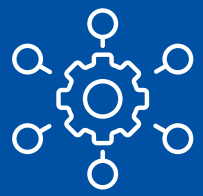
セマンティック バージョニングは、重大な変更、軽微な更新、バグ修正を明確なバージョン管理に対応させることで、製造業者が CRA への準拠状況を追跡するのに役立ちます。

SBOM はより高い粒度での情報提供が求められており、ファイルレベルでの追跡によって、製造業者にとってセキュリティの可視性、リスク評価、脆弱性対応が向上します。



オープンソースの**セキュリティには業界横断的な協力が必要**であり、製造業者、政府、プロジェクトが共同でポリシーを開発し、セキュリティに資金を提供し、長期的なソフトウェアのメンテナンスを確保します。

CRA は、セキュリティの実践、文書化、そしてエコシステム全体での協力を改善することによって、オープンソース ソフトウェアのセキュリティを強化する**機会**を提供します。



AI は新たなセキュリティ リスクをもたらし、AI 生成コードや汚染されたトレーニング データセットからの脅威を軽減するためのフレームワークが必要です。

リーダーシップはオープンソースのレジリエンスを推進します。プロジェクトのメンテナー、ディレクター、そして運営委員会のメンバーは、積極的にセキュリティ文化を構築するために、啓蒙活動や広報活動を通じて取り組まなければなりません。

Linux Foundation と **OpenSSF** は、開発者、製造業者、スチュワードがサイバーセキュリティ規制に適合できるよう、協力とベストプラクティスを通じて CRA への準備をサポートしています。

Copyright © 2025 **The Linux Foundation** | March 2025. This report is licensed under the **Creative Commons Attribution-NoDerivatives 4.0 International Public License**

目次

序文

2023 年にサイバー レジリエンス法（CRA）の規制が策定された際、当時のオープンソース開発者の間で共通していた懸念は、新しい規制が意図せずにグローバルなオープンソース プロジェクトに害を及ぼす可能性があるというものでした。その後、オープンソースの支持者や立法者が生産的な対話に参加し、オープンソースエコシステムの複雑さについて相互理解を深めました。この取り組みは最終的に成功を収め、CRA は現在、オープンソース エコシステム内の異なる商業的およびボランティアの関係者を考慮に入れています。そしてオープンソース コミュニティは、再び一緒に力を合わせることで物事を実現できることを学びました。

多くのオープンソース組織は、この勢いを維持し、オープンソース ビジネス、財団、コミュニティを CRA 対応にするための取り組みに変えています。多くの人々は、2018 年の春、当時新たに施行された一般データ保護規則（GDPR）の完全な遵守が一夜にして義務付けられたことを覚えています。ほとんどの組織は、その日までに準備を整えて遵守するための時間を活用していませんでした。オープンソース コミュニティ全体は、CRA において同じ過ちを繰り返さないことを決意しているようです。

Linux Foundation や Open Source Business Alliance、そしてその他多くの組織は現在、それぞれのコミュニティのメンバーが CRA に準拠するために何をすべきかを理解できるように、ガイダンス資料を作成しています。

この共通の取り組みは非常に重要です。なぜなら、CRA には課題とともに機会も含まれているからです。例えば、CRA はオープンソース ソフトウェア スチュワードといった新しい役割を導入しています。オープンソース開発者は、これらの新しい概念に取り組み、製造業者とソフトウェア スチュワードの要件がどのように異なり、どの役割が自分たちに該当するのかを理解しなければなりません。Linux Foundation の新しいレポート「オープンソースにおけるサイバーセキュリティのベストプラクティスへの道筋」は、CRA に対する理解を深め、オープンソース コミュニティにおける広まった懸念や不確実性を軽減する手助けをしています。

これらの課題や不確実性にもかかわらず、新しい規制を活用してオープンソースの利点を自信を持って指摘することも重要です。一般的に言えば、オープンソース ソフトウェアは透明性の面で他のソフトウェアに大きな優位性を持っており、CRA の要件を満たす可能性を秘めています。実際、すでにいくつかのオープンソース プロジェクトは CRA が求める以上の取り組みを行っており、このレポートに掲載された事例がその証拠となっています。

CRA が 2027 年に完全施行されるまでには、まだ多くのことを行わなければなりません。いくつかのオープンソース プロジェクトはすでに CRA に対応していますが、他のプロジェクトはまだその要件を満たす準備ができていません。したがって、私たちが得意とすることを行うべきです。それは、協力し、知識を共有し、互いに支援することです。共に、ソフトウェア開発と配布をより安全にするための世界的な取り組みを先導できるでしょう。

このレポートはこの大きな取り組みに貢献し、認識を広め、貴重な提言を提供します。私は、読者が取り上げられたプロジェクトとそのリーダーシップ チームから刺激を受け、それぞれのオープンソース コミュニティに参加してオープンソースのセキュリティと持続可能性を確保することを願っています。

さあ、CRA 対応に向けて進みましょう！

MIRIAM SEYFFARTH
HEAD OF POLITICAL COMMUNICATIONS
OPEN SOURCE BUSINESS ALLIANCE

エクゼクティブ サマリー：オープンソースにおけるサイバー レジリエンス

欧州連合のサイバー レジリエンス法（CRA）は、オープンソース エコシステムにとって転機となる瞬間であり、EU で商業化されるデジタル要素を含む製品（PDE）に対して厳格なサイバーセキュリティ要件を課しています。この規制は 2027 年 12 月まで完全には適用されませんが、いくつかの条項はそれ以前に発効する予定です。規制違反に対するペナルティは、最大で 1500 万ユーロまたは世界全体の年間売上高の 2.5% に達する可能性があり、その影響は非常に大きいです。

Linux Foundation による三つの主要プロジェクト、Civil Infrastructure Platform（CIP）、Yocto Project、Zephyr Project の分析は、新しい規制枠組みの下でオープンソース ソフトウェア スチュワードが直面する準備状況と課題を明らかにしています。CRA は、製品の遵守に対して主要な責任を負う商業的製造業者と、収益化せずにオープンソース ソフトウェアを開発・維持するオープンソース ソフトウェア スチュワードとの間に新たな区別を導入しています。この区別は、オープンソース コンポーネントが現代のソフトウェアの最大 96% を占める現実を認識し、開発モデルの基本的なオープン性を尊重しています。

各プロジェクトは、CRA の要件に大きく一致する高度なセキュリティ対策を示しています。例えば、CIP は IEC 62443-4-1 産業サイバーセキュリティ規格の採用を先駆けて行いました。Yocto Project は、ソースからバイナリ コードへの独立して検証可能な経路を作成する再現可能なビルドを提供しています。Zephyr は、確立された製品セキュリティ インシデント対応チームを持つ CVE 番号付与機関として機能しています。3 つのプロジェクトすべてが強力な脆弱性管理プロセスを実施していますが、必須の 5 年間のサポート期間は、一部のプロジェクトの現在の長期サポートのコミットメントを超えています。

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。

課題は依然として重大です。一部の産業システムは 30 年から 50 年にわたるライフサイクルを持ち、典型的なソフトウェアのサポート期間を大きく超えています。標準化のギャップは依然として存在しており、特にソフトウェア部品表（SBOM）の形式や脆弱性追跡のための一貫した命名規則に関して問題があります。また、この規制は、どの組織がスチュワードとして認定され、どのように市場監視機関（MSA）の要求を処理すべきかについて、かなりの不確実性をもたらしています。

Linux Foundation と Open Source Security Foundation は、これらの課題に対処するためのイニシアチブを立ち上げ、標準の開発、認識の向上、ツールの改善に焦点を当てています。主な推奨事項には、重要な修正が新たな適合性評価を引き起こす際にそのことを伝えるためにセマンティック バージョニングを採用すること、開発ワークフローにセキュリティ対策を統合すること、標準化された SBOM を生成すること、そして自動化されたセキュリティ スキャンを実施することが含まれます。

技術的な解決策を超えて、リーダーシップはサイバーセキュリティの準備において重要な要素として浮かび上がります。目に見える形で積極的に支援するリーダーを持つプロジェクトは、長期的なセキュリティ改善に必要な注目、リソース、そして組織的なサポートを引き寄せます。規制がより厳しい運営環境を作り出す中で、そのようなリーダーシップが、どのプロジェクトが成功するかを決定します。

CRA は単なるコンプライアンスの負担ではなく、デジタル エコシステム全体のサイバーセキュリティを強化する機会を提供します。初期の実施課題があるものの、セキュリティが任意の考慮事項ではなく明確な優先事項となる枠組みを確立します。製造業者、スチュワード、規制当局が適切に協力して実施すれば、「サイバーセキュリティの分野で国際的に先導的な役割を果たす」という野心的な目標を達成し、オープンソース開発が代表するイノベーションの原動力を維持することができるかもしれません。

はじめに：政策課題がオープンソース エコシステムを活性化させる

現在、オープンソース ソフトウェアを開発するコミュニティと、そのソフトウェアを利用するダウンストリームのユーザーとの間で、より強固な連携を求める新たな推進力が生まれています。その推進力とは、欧州連合（EU）の最近の法制度であるサイバー レジリエンス法（CRA）[1] です。これは製造業者、メンテナー、オープンソース スチュワードに対して大きな影響を与えるものです。本レポートは、変化するグローバルなサイバーセキュリティ政策の状況に向けて、関係者が備えるための Linux Foundation による数多くの取り組みの一つです。

CRA の目的は、EU で商業化されるデバイスおよびソフトウェアに対してサイバーセキュリティ要件を確立することです。CRA の文言には一部わかりにくい箇所もありますが、すでに法制化されており、2026 年には一部条項が、2027 年には完全な適用が開始されます。CRA に違反した場合の制裁は非常に厳しく、最大で 1,500 万ユーロ、または全世界の年間売上高の 2.5% のいずれか高い方が科されます。CRA の適用対象者にとって、いわゆるタイムリミットが迫る中、今こそコンプライアンスを強化する時です。しかし、コンプライアンスのために何が必要で、関係者はどこから取り組むべきなのでしょうか。

CRA の下では、製品、特にデジタル要素を含む製品（PDE）のサイバーセキュリティおよび適合性の責任は、下流の製造業者に課されます。[2] 多くの PDE はオープンソース コンポーネントを基盤としており、それらは時にデバイス内ソフトウェアの大部分、報告によっては最大 96% [3] を占めることもあります。PDE 内のソフトウェアを効率的かつ柔軟に保守するには、製造業者は上流のオープンソース コミュニティが提供するドキュメント、コラボレーション プロセス、その他の支援策に依存し、それらを活用する必要があります。CRA は下流の製造業者と上流のオープンソース プロジェクトの関係についてあまり具体的には定めていませんが、CRA が課す長期サポートや迅速なサイバーセキュリティ対応の要件を満たすためには、この関係が極めて重要になります。さらに状況を複雑にするのは、リリースの周期、品質保証の手法、データ形式、その他ソフトウェア サプライチェーンに関わる多くの側面が、オープンソース プロジェクトごとや製造業者のプロセスごとに異なっていることです。

朗報として、広く利用されている多くのオープンソース プロジェクトは、以前からサイバーセキュリティを重要視してきました。多くのプロジェクトは、信頼性が高く、十分に文書化された開発およびコラボレーションの慣行を確立しており、下流の利用者が自らの製品にそのソフトウェアを導入する際の支援にも多大な努力を注いできました。これらすべての取り組みがオープンソース環境で実施されているため、下流の利用者はそれらを優れた実践例として調査したり、自らの開発に同様の、あるいは同様の実績あるツールやプロセスを取り入れたりすることが可能です。これは特に、オペレーティング システムやデバイス ソフトウェアの構築キットなど、デバイスや製品を構築するための競争前段階のレイヤーとして設計されたオープンソース プロジェクトにおいて顕著です。

本レポートでは、Linux Foundation がホストする広く利用されている 3 つのオープンソース プロジェクトに焦点を絞りました。これらはいずれもセキュリティ対策において高く評価されており、体系的な調査プロセスを経て、CRA の下でもそれ以降でも効果的な OSS スチュワードの事例として取り上げられています。1 つ目は、Civil Infrastructure Platform: Industrial Grade Linux（CIP）プロジェクトです。これは、現代の社会インフラや産業オートメーションの安全性、信頼性などの要件を満たす Linux ベースの組み込みシステムを構築するための、産業グレードの中核的なオープンソース ソフトウェア コンポーネント、ツール、および手法のベース レイヤーを提供します。2 つ目は、Yocto Project です。これはハードウェア アーキテクチャに依存せず、カスタムの組み込み Linux オペレーティング システムを構築するための業界標準的な「ツールキット」として知られています。3 つ目は、Zephyr Project で、これは複数のコンピューター アーキテクチャをサポートする、リソース制約のあるデバイス向けに最適化されたリアルタイム オペレーティング システムです。

本レポートでは、Linux Foundation がホストする広く利用されている 3 つのオープンソース プロジェクトに焦点を絞りました。これらはいずれもセキュリティ対策において高く評価されており、体系的な調査プロセスを経て、CRA の下でもそれ以降でも効果的な OSS スチュワードの事例として取り上げられています。1 つ目は、Civil Infrastructure Platform: Industrial Grade Linux（CIP）プロジェクトです。これは、現代の社会インフラや産業オートメーションの安全性、信頼性などの要件を満たす Linux ベースの組み込みシステムを構築するための、産業グレードの中核的なオープンソース ソフトウェア コンポーネント、ツール、および手法のベースレイヤーを提供します。2 つ目は、Yocto Project です。これはハードウェア アーキテクチャに依存せず、カスタムの組み込み Linux オペレーティング システムを構築するための業界標準的な「ツールキット」として知られています。3 つ目は、Zephyr Project で、これは複数のコンピューター アーキテクチャをサポートする、リソース制約のあるデバイス向けに最適化されたリアルタイム オペレーティング システムです。

これらの知見が、他のオープンソース プロジェクトやリーダーたちにとって、CRA の要件に照らした自らのサイバーセキュリティ態勢をより深く理解し、それを改善するための必要なアクションを取るきっかけとなることを願っています。理解と協調を深めることで、CRA への準拠を実現する道が開けるだけでなく、オープンソース ソフトウェアの強靭性、持続可能性、そしてセキュリティを一層高める絶好の機会ともなるのです。

方法論

このレポートは、実務者、製造業者、およびオープンソース ソフトウェアの管理者に対し、全体的なサイバーセキュリティの姿勢を改善し、CRA への準備を整えるための指針、ガイダンス、推奨事項、そしてインスピレーションを提供することを目的としています。具体的には、CRA のテキストの分析、主要なオープンソース プロジェクトのサイバーセキュリティ実践のレビュー、3 つの Linux Foundation がホストするプロジェクトの関係者へのインタビューから得た定性的なインサイト、および 2024 年 12 月の「管理者と製造業者のワークショップ」のようなワークショップや利害関係者との意見交換から得た知見を組み合わせています。各内容については以下で詳細に説明します。

CRA のテキストの分析

CRA の分析は、2024 年 10 月 23 日[4] に EU 理事会が公表した CRA のテキストに基づいています。それは、オープンソース エコシステムの運営に関連する法内で言及されている経済主体の役割について議論し、それらの間の関係をレビューします。特に、この分析は、経済主体間の明示的および暗示的な関係を調査します。

CRA は、製造者と消費者、製造者と市場監視機関 (MSA)、およびオープンソース ソフトウェアの管理者と MSA 間の関係を明示的に説明しています。CRA は、オープンソース ソフトウェアの管理者と製造者間の関係については暗示しているものの、詳細には規定していません。また、未法人化のオープンソース コミュニティ、個々のメンテナーや貢献者と、ソフトウェアの下流の製造者やユーザーとの関係については、あまり詳細が提供されていません。可能な限り、私たちは Linux Foundation プロジェクトで通常適用される実践やガバナンスの規範に基づいて、これらのギャップを埋めることを試みています。

テキスト分析は、CRA によって課せられた異なる関係者の義務の簡単な概要で締めくくられます。これには、CRA の対象となる活動と対象外となる活動の概略も含まれています。

CIP、Yocto Project、Zephyr Project のリーダーとの定性的インタビュー

次に、主要な貢献者との定性的インタビューを通じて、3 つの重要なオープンソース プロジェクト（Civil Infrastructure Platform、Yocto Project、Zephyr Project）のサイバーセキュリティ プラクティスをレビューしました。定性的インタビューは、以下の主要な研究課題に基づいて進められました。

1. あなたのオープンソース プロジェクトで、CRA の範囲に該当する製品で一般的に使用されているサイバーセキュリティのベストプラクティス、ドキュメント、およびサポート プロセスの現状はどうですか？

2. CRA で定義された役割と義務は、オープンソース コミュニティと下流の製造業者との関係におけるサイバーセキュリティのベストプラクティスにどのように関連していますか？

3. オープンソースの管理者と製造業者は、効率的な CRA 準拠を実現するために、どのような組織的および技術的措置を講じるべきですか？

Linux Foundation 傘下の多くのプロジェクトはサイバーセキュリティのベストプラクティスを優先してきましたが、これらの特定のプロジェクトは、オープンソース コミュニティが開発ライフサイクルにセキュリティを組み込む方法の代表的な例として、Linux Foundation の大規模なポートフォリオから選ばれました。これにより、セキュリティ態勢の向上だけでなく、CRA に基づく管理者の要件を満たすための手段として機能しています。サイバーセキュリティ、品質保証、ドキュメントの実践に多大な労力を費やし、強力なサイバーセキュリティ態勢と長期的なセキュリティ ベストプラクティスへの取り組みで広く認識されています。さらに、各プロジェクトは数多くの下流製品の基盤となっており、そのため、世界中のサイバーセキュリティの状態に特別な影響を与えています。重要なことに、各プロジェクトの主要な貢献者が利用可能であり、このレポートに協力する意欲があり、彼らのセキュリティ戦略に関する直接的な洞察を提供してくれました。これらの理由から、ケーススタディとして選ばれたことにより、他のプロジェクトや業界の管理者が採用を検討できる具体的な実践と教訓を強調し、この研究から導かれた推奨事項がサイバーセキュリティのベストプラクティスの最先端を代表するものであるという確信を持っています。

これらの 3 つのプロジェクトは貴重な視点を提供していますが、サイバーセキュリティのベストプラクティスに関する結論は簡単に一般化できないことに注意する必要があります。なぜなら、これらの 3 つのプロジェクトはオープンソース エコシステム全体をそのすべてのニュアンスで代表するものではなく、またオープンソースのセキュリティ アプローチの全スペクトルを網羅しているわけではないからです。さらに、これらは CRA コンプライアンスに強い立場を持つ唯一の LF プロジェクトでもありません。例えば、これらの 3 つのプロジェクトは、オペレーティング システムのコンポーネントやオペレーティング システム カーネルを提供する低レベルのプラットフォームを代表しています。Kubernetes、SPDX、OpenSSF の取り組みなど、別の視点で CRA の準備状況を示すプロジェクトもあったかもしれません。それにもかかわらず、私たちのサンプルは、オープンソース ソフトウェア開発におけるサイバーセキュリティとコンプライアンスへのアプローチの有意義な断面を提供しています。これらがさまざまなオープンソース コミュニティの利害関係者にとって出発点として有用なガイダンスを提供することを期待しています。

それぞれのプロジェクトのケーススタディでは、CRA に基づく分類、現在の実践が CRA で要求される内容とどのように比較されるか、現在の実践と CRA の義務とのギャップを埋めるために必要なステップ、そして現在の実践が CRA で参照されていないサイバーセキュリティのニーズをどのようにカバーしているか、または CRA の基本要件を超えているかを分析します。

スチュワードおよび製造業者を含むステークホルダーとのワークショップから得られた洞察

Linux Foundation は、主要なオープンソース ソフトウェアの管理者としての役割を担い、CRA の実施において製造業者やオープンソースプロジェクトと積極的に連携しています。コミュニティの管理者と製造業者それぞれの役割と責任についての理解を深めるために、Open Source Security Foundation（OpenSSF）と Linux Foundation Europe は、CRA の公式発表後の 2024 年 12 月に「オープンソース ソフトウェア スチュワードと製造業者ワークショップ」を共同で開催しました。このワークショップには、Linux Foundation、他の上流のオープンソース財団、コミュニティの専門家、政府関係者[5] から 50 名のリーダーが参加しました。参加者は、製造業者と管理者それぞれの義務についての理解を共有し、CRA が最終的に発効するまでの 3 年間の間におけるさらなる協力の機会を模索しました。

全体会議とワークショップ セッションでは、参加者が CRA 実施に向けたロードマップを 3 つのテーマ別作業フローを通じて策定しました。

1. **認知 :** CRA、そのタイムライン、要件、そして立法が施行される際の全体的な準備状況についての認知を高めるための道筋を探る。

2. **標準 :** コミュニティのベストプラクティスを認められた仕様に形式化・標準化し、プロセスを開発すること。

3. **ツール化 :** ソフトウェア サプライチェーンのフローをサポートするフォーマットやツールを特定し、より大きな影響を与える機会を見つけること。

このワークショップは、OpenSSF の下で Global Cyber Policy working group を設立するきっかけとなり、また、定性的インタビューで取り上げられた多くのテーマを裏付ける役割も果たしました。この情報は最終的に、報告書の推奨事項に影響を与え、強化することになりました。

上記の実証的アプローチを通じて、本報告書の結果は、オープンソースプロジェクト コミュニティが CRA の必須要件を実施するための必要な行動を加速させるとともに、すべてのソフトウェアをより安全にするベストプラクティスに対する認識を広めることを目的としています。

EU サイバー レジリエンス法：オープンソース関係者が知っておくべきこと

CRA は、EU 内部市場および世界規模でのサイバーセキュリティ向上を目指す画期的な法案です。この法案は、次の 3 つの政策目標を達成することを目指しています（前文 2）。

1. デジタル製品の脆弱性の数と深刻度を減らすこと。

2. 製品のライフサイクル全体を通じてサイバーセキュリティが維持されることを確保すること。

3. デジタル製品を選択・運用する際に、ユーザーがサイバーセキュリティ基準を参考にして情報に基づいた意思決定を行えるようにすること。

これらの要件は、ソフトウェア、ハードウェア、またはその両方を含むデジタル要素を持つすべての製品に適用され、EU 市場で商業的に提供される場合に該当します。国際的な製造業者が E に製品を提供できるよう、より強化されたサイバーセキュリティの実践を導入することを前提として、この法律は世界的なサイ U 市場バーセキュリティの基準を向上させることを目指しています。

この横断的かつ義務的なアプローチにより、EU は、EU 市場で商業的に提供されるすべてのデジタル要素を持つ製品が最低限のサイバーセキュリティ基準を遵守することを求め、広範な脆弱性報告要件を導入し、通常は 5 年以上のセキュリティ修正サポート期間を義務付けています。CRA の適用範囲は明確に EU 内部市場に関するものですが、その野心はヨーロッパを超えて広がっています。法律の序文第 7 条では、「サイバーセキュリティ分野で国際的に主導的な役割を果たすことを目指す」[6] と述べています。CRA は、他の法域が同様の目標を持ったサイバーセキュリティ規制を実施しているという、世界的なトレンドに合致しています。たとえば、米国のサイバー トラスト マークプログラムや IoT サイバーセキュリティ改善法、シンガポールのサイバーセキュリティ ラベリング制度、日本のサイバーセキュリティ戦略、オーストラリアの重要インフラ セキュリティ法などは、デジタル製品とインフラのセキュリティ強化に向けた国際的な取り組みの拡大を反映しています。

2024 年 12 月 11 日に施行されると、3 年間の実施期間が始まり、その間に追加のガイダンスが伝えられる予定です。特に、欧州規格が採用され、一般的なサイバーセキュリティ要件や特定の製品に対する要件が詳述されます。製造業者はこれらの規格を参照し、自社製品が CRA の要件に適合していることを示すために CE マークを使用します。第 71 条に記載されているように、CRA によって導入されたほとんどの義務は 2027 年 12 月 11 日から適用されますが、製造業者は、積極的に悪用されている脆弱性や重大なインシデントに関する報告義務が 2026 年 9 月 11 日から、適合性評価機関の通知に関する規定が 2026 年 6 月 11 日から適用されることを認識しておく必要があります。

サイバー レジリエンス法（CRA）の理解：主要な定義とフレームワーク

CRA はサイバーセキュリティ規制にいくつかの新しいアプローチを導入しており、これらはデジタル サプライチェーンに大きな影響を与える可能性があります。その中には、デジタル要素を備えた製品という概念のように、従来の規制とは異なる新しいアイデアも含まれています。また、オープンソース ソフトウェア開発によってもたらされた変化に対応するため、ソフトウェア開発の新しい動向を反映した概念もあります。この章では、製造業者とオープンソース プロジェクトが認識しておくべき CRA から選んだ概念について説明します。

デジタル要素を備えた製品

「デジタル要素を備えた製品（PDE）」は、CRA[7] が適用される製品の範囲を定義します。PDE には、ソフトウェアやハードウェア製品が含まれ、これらがソフトウェアとハードウェアを統合したデバイスとして市場に出される場合でも、別々に販売される場合でも関係ありません（第 3 条第 1 項）。CRA は、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または間接的な論理的・物理的なデータ接続を含む場合にのみ適用されます（第 2 条第 1 項）。しかし、これは多くの製品に該当します。PDEs には、これらの機能に必要な範囲で、リモートデータ処理ソリューションも含まれます（第 3 条第 2 項）。ソフトウェアはコンピューター コードに基づいた製品の一部として定義されます（第 3 条第 4 項）、一方、ハードウェアはすべての物理的なコンポーネントを含みます（第 3 条第 5 項）。PDE の定義は、オープンソース ソフトウェアと他の製品を区別しません。その代わり、義務は PDE が商業的な意図で市場に提供されるかどうかに基づいて異なり、この点については以下で詳細に説明されます。

製品を商業的に提供すること

CRA は「市場への提供」を商業活動の一環として PDE を供給することと定義しています（第 3 条第 22 項）。さらに「市場への配置」を PDE の初回の提供と定義しています（第 3 条第 21 項）。デジタルの世界では、「市場への配置」は新しい製品の初回リリースや導入として理解できますが、その後のソフトウェアやハードウェアのアップデートは「提供される」となります。この用語を製造者やオープンソース プロジェクトの開発慣行に関連付けることが必要になるかもしれません。

前文において、商業活動の一環としての供給は製品に対して価格を設定することに限らず、消費者データの取得やその他のメカニズムを通じた間接的なマネタイズも含まれることが明確にされています。また、CRA が導入するもう一つの重要な概念は、商業的意図のないソフトウェアの提供であり、この記事に定義はありませんが、オープンソース ソフトウェアが収益化されていない場合は商業活動とは見なされないとされています（前文 18）。これに対して、「製品の提供」とは、商業活動の一環として製品を配布または使用のために供給することを意味します。この区別は、供給されるものの性質、すなわちクローズドソースやオープンソース製品または関連サービスの違いには影響を与えません。むしろ、商業活動の性質に基づいて製造者（および一部の他の関係者）に役割と責任を割り当てています。

マネタイズには、ソフトウェア ライセンスやデバイスに対して価格を設定する直接的なマネタイズと、無料で提供されるソフトウェアの使用からユーザー データを取得するような間接的なマネタイズが含まれます。間接的なマネタイズが何を意味するかについては議論の余地があると予想されますが、例えばソフトウェア開発環境やウェブ ブラウザをユーザー アカウントのサブスクリプション販売のチャネルとして提供するような、現在一般的な慣行はこれに該当すると考えられます。また、間接的なマネタイズには、デジタル製品の設計、開発、提供に関わる費用を上回る寄付を受け入れることも含まれます。ただし、利益を目的としない寄付の受け入れは商業活動とは見なされません（前文 15）。

製造業者およびオープンソース ソフトウェア スチュワード

CRA は、製造業者とオープンソース ソフトウェア スチュワードの役割を明確に区別した初めての EU 規制です。製造業者は、EU 市場でデジタル要素を含む製品を商業的に提供する責任がある主体です。オープンソース ソフトウェア スチュワード(略して「スチュワード」) は、オープンソース製品の開発を体系的に支援し、その実行可能性を確保する組織です。

製造業者は、デジタル要素を含む製品を開発または製造するか、またはそれらの設計、開発、製造を委託します。オープンソース ソフトウェア スチュワード (別名「スチュワード」) は、製造業者以外の組織で、特定のオープンソース製品の開発を体系的に支援し、その実行可能性を確保します。

この区別は重要な市場の現実を反映しています。スチュワードはオープンソース ソフトウェアを誰にでも、どんな目的でも利用できるように提供しますが、製品のユーザーと直接関わるわけではありません。スチュワードは通常、自分たちのソフトウェアがどの程度広く利用されているかを完全には把握していませんが、それでも多くの現代的なデジタル製品のコードの大部分を構成する基本的なオープンソース ソフトウェアのビルディング ブロックを提供しています。オープンソース エコシステムの重要な礎となるのは、ソフトウェアのユーザーが上流のソフトウェア コミュニティから使用許可を求めたり、使用の登録をしたりする必要がないことです。また、スチュワードが提供するオープンソース ソフトウェア コンポーネントは、彼ら自身によって収益化や商業化されることはありません。代わりに、スチュワードは通常、寄付や会費によって運営資金を賄い、その運営自体がソフトウェアの使用の対価として支払われることはありません。この点を踏まえると、無料で提供されるソフトウェアのサイバーセキュリティ機能に対して、スチュワードが責任を負うことはほぼ不可能です。CRA はこの課題を認識し、特定の商業製品におけるオープンソース コンポーネントの目的適合性について適切なデューデリジェンス評価を行う責任を、その製品の製造業者に明確に課しています。

オープンソース開発プロセスの典型的な形態と同様に、製造業者とスチュワードの間の意図された関係は、ボランティアによる参加と協力に基づいています。製造業者は、自社の製品に対して長期間にわたるセキュリティ更新を提供するという要件を通じて、自社のオープンソース依存関係の維持可能性を確保することが奨励されています。スチュワードは、彼らの製品にリリースおよび脆弱性に関するドキュメントを提供することが奨励されています。CRA は、この製造業者とスチュワードの関係の未来を市場に委ねることが多いですが、製造業者が自社のオープンソース依存関係の維持と管理に対する共通の責任を負うべきだとほのめかしています。

CRA におけるオープンソース ソフトウェアの範囲

Recital 18 では、デジタル要素を備えた製品が無料およびオープンソース ソフトウェア (FOSS) に該当する場合について言及しています。これらの製品は、製造者が商業活動の一環として収益化し、提供される場合のみ、CRA の適用対象となります。オープンソース ソフトウェアの開発、維持、配布への参加は、開発がどのように資金提供されているかや構造がどうであれ、商業活動とは見なされません。また、他者の責任で行われるオープンソース プロジェクトへの貢献や、オープンソース ソフトウェアを開発する非営利団体の活動も商業活動には該当しません。この重要な条項は、オープンソース プロジェクトやコミュニティへの貢献が CRA の対象外であることを明確にし、既存のオープンソース プロジェクトへの貢献に対する障壁を生じさせないことを保証します。

明示的なオープンソースの免除はない

オープンソース ソフトウェアに対する広範な免除を提供するのではなく、CRA は商業的意図なしで提供されるソフトウェアに対して免除を導入しています。この区別には重要な影響があります。例えば、単一ベンダーのオープンソース企業は、「商業的意図なしで提供」という概念に該当しない可能性があります。なぜなら、通常のビジネス活動のすべては商業的目的によって推進されていると考えられるからです。さらに、同じ企業が開発・所有するオープンソース コンポーネントに関連するコンサルティングやその他のサービスを提供することは、間接的な収益化の形態と解釈される可能性があり、その場合、そのような企業は CRA の要件の範囲に含まれることになります。

CRA は、Open Source Initiative が維持するオープンソースの定義を参照していません。[8] オープンソース ソフトウェアは、一般的に次の 4 つの自由を可能にするライセンスのもとでソースコードが公開されているソフトウェアとして理解されています。ソースコードを研究する自由、ソースコードを使用する自由、ソースコードを変更する自由、および再配布する自由です。第 3 条第 48 項で、CRA は「ソースコードが公開されており、自由にアクセス、使用、変更、再配布できるすべての権利を提供する無料およびオープンソース ライセンスのもとで提供されるソフトウェア」として、無料およびオープンソース ソフトウェアを定義しています。[9]

CRA における
オープンソース ソフトウェア スチュワードの役割

CRA は、オープンソース ソフトウェア スチュワードを、無料でオープンソース ソフトウェアの持続的な開発を体系的にサポートし、その存続可能性を確保する組織として定義しています。CRA は、スチュワードが「製造業者以外の法人」であることを明示的に要求することによって、スチュワードが製造業者に課せられたサイバーセキュリティ義務から保護されるとともに、スチュワードの活動に対する制約も定義しています。これらの制約は、オープンソース ソフトウェアの開発に役立つものであり、収益化を構成するものではありません。個人も法人と見なされるため、スチュワードとして認められる可能性はありますが、欧州委員会の代表者は、スチュワードは法人格を持つ組織であるべきだと期待していることを示しています。

オープンソース ソフトウェア スチュワードには、CRA の下でいくつかの重要な義務があります。これらの義務は、事例研究の利害関係者との質的調査で提示された質問に影響を与えました。CRA の下では、オープンソース ソフトウェア スチュワードは、セキュアな開発慣行を促進し、効果的な脆弱性の取り扱いや脆弱性の自主的な報告を行うサイバーセキュリティ ポリシーを実施し、文書化することが求められています（第 24 条第 1 項）。また、市場監視当局からの要請に応じて協力し、サイバーセキュリティ リスクに対応するために必要な文書を提供しなければなりません（第 24 条第 2 項）。さらに、スチュワードは、既知の積極的に悪用されている脆弱性を報告し、重大なインシデントを通知し、影響を受けたユーザーに対して通知を行い、緩和策を提供する必要があります（第 24 条第 3 項）。オープンソース コンポーネントを統合する製造業者を支援するために、CRA は任意のセキュリティ認証プログラムの設立を可能にし、開発者やユーザーがサイバーセキュリティ要件への適合性を評価できるようにしています（第 25 条）。

オープンソース コンポーネントを商業製品に統合する際のデューデリジェンス

商業製品にオープンソース コンポーネントを組み込む製造業者は、依存するオープンソース製品のサイバーセキュリティ慣行に依存していると言えます。オープンソース コンポーネントのセキュリティ、維持管理性、およびコンプライアンスは、セマンティック バージョニング、継続的インテグレーション / 継続的デプロイメント（CI/CD）、分散バージョン管理システム（DVCS）などの確立されたオープンソース開発慣行によって形成されます。さらに、上流のコンポーネントに加えられた変更の範囲は、最終製品のセキュリティ体制やタイムリーなアップデートを受け取る能力に影響を与えます。

このため、製造業者は、オープンソース ソフトウェアを含む第三者のコンポーネントを統合する際に適切なデューデリジェンスを行わなければなりません（第 13 条第 5 項）。また、コンポーネントの脆弱性が発見された場合、製造業者はそれをコンポーネントのメンテナーに報告しなければなりません（第 13 条第 6 項）。オープンソース依存関係管理に関するデューデリジェンスの重要性は、次の重要な研究課題の形成に影響を与えました。「選ばれたプロジェクトは、下流の製造業者をどの程度サポートできる準備ができているか？」

ケーススタディ：CRA への準拠とサイバーセキュリティのベストプラクティスにおける先進プロジェクト

Civil Infrastructure Platform

Civil Infrastructure Platform（CIP）は、Linux Foundation がホストするオープンソース ソフトウェア 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オープンソース ソフトウェア コンポーネントの基盤層を確立することに焦点を当てています。CIP プロジェクトは、安全性、信頼性、その他の産業・基礎インフラ分野に特有の要件を満たす再利用可能なソフトウェア構成要素の作成を目指しています。さらに、CIP はそのソフトウェア コンポーネントに対して長期サポート（LTS）を提供することをコミットしており、こうしたシステムに一般的な長いライフサイクルに対応するため、最低 10 年間の保守期間を目標としています。CIP のガバニングボードは、プロジェクトに関連する財務面を担当し、テクニカル ステアリング コミッティ（TSC）はプロジェクトの技術的な方向性を監督しています。

分類

CIP は、製造業者ではなくオープンソース ソフトウェアのスチュワードとして活動しており、企業が自社の PDE やサービスを開発するために利用するオープンソース ソフトウェアをリリースしています。CIP は、タグを通じて更新（すなわち大幅に変更されたバージョン）を提供しています。CIP 自身は、収益化された PDE やサービスをリリースしておらず、オープンソース ソフトウェアを補完する商業的な提供も行っていません。しかしながら、プロジェクトのリーダーシップへのインタビューでは、CIP がスチュワードに該当するかどうかについて不確実性があることが明らかになりました。この不確実性は CRA に関するより明確なガイダンスの必要性を浮き彫りにしています。たとえば、スチュワードとしての責任を担うのはプロジェクト自体なのか、それともプロジェクトをホストする財団なのかという点です。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。

CRAの本質的要件への準拠

開発プラクティス

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** 上で公開しています。プロジェクトは、リリース通知のための購読ベースのメーリングリストを通じてユーザーとのコミュニケーションを維持しています。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ます。実際、プロジェクト リーダーの知る限り、CIP は IEC 62443-4-1 のサイバーセキュリティ要件を採用した最初の OSS プロジェクトでした。「この点において私たちは先駆者です」と述べるのは、本報告書のインタビュー対象の一人であり、CIP の技術指導委員会およびセキュリティ ワーキング グループのメンバーである Stefan Schroeder です。この **IEC 規格**は、産業用オートメーションおよび制御システムで使用される製品の安全な開発のためのプロセス要件を定めています。加えて、CIP はタグとブランチ システムを通じて開発版とリリース版を明確に区別しており、開発は main ブランチおよび専用のフィーチャー ブランチで継続的に行われています。

サイバーセキュリティ ポリシー

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ます。脆弱性の報告は公開チャネルを通じて行われますが、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ます。報告メカニズムとしては主にメーリングリストが使われており、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合されています。インタビューの中で、Schroeder は文書は常に進化しており、ソフトウェアと文書を同時にバージョン管理する必要があるかもしれないという懸念を示しました。加えて、リリースはソフトウェアと文書を含んだ包括的なバンドルとして扱うべきであり、そうすることでユーザーが特定のリリース時点で適用された文書を明確に把握できるようになると主張しています。

MSA との協力

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す。しかし、Schroeder は、分散型コミュニティ構造内での対応調整に課題があることを認めており、MSA（市場監視当局）からのリクエストに対応するために、専任の従業員を雇うことが有益かもしれないと示唆しています。彼はまた、プロジェクトのセキュリティ状態を効果的に伝えるために、**OpenSSF スコアカード**と **security.txt** ファイルの採用を強く推奨しています。

任意参加のサイバーセキュリティ信頼性検証プログラム

CIP のインテグレーターとしての立場は、特に上流の依存関係を管理する際にユニークな課題を提示します。上流プロジェクトのセキュリティプラクティスを強制できないため、CIP はこの制限を補うために上流プロジェクトに対して適切なデューデリジェンスを実施しています。現在、リリース時に SBOM を提供していませんが、この機能については議論されています。脆弱性開示については、CIP はカーネルに関しては kernel.org を、その他については Debian を番号付け機関として依存しています。しかし、CIP は特定のパッケージセットをリリースしていないため、この結びつきはさらに緩やかです。多くのケースで、CIP のアプローチは追加のサードパーティの証明によって CRA の要求を超えており、しかし、オープンソース ソフトウェア プロジェクトが通常、コミュニティ主導の開発モデルに依存しているため、サイバーセキュリティ証明プログラムにどのようにアプローチすべきかについては依然として大きな不確実性があります。役割、責任、および実際の実施に関する明確なガイダンスの欠如は、CIP のようなプロジェクトにとって課題となっています。

CRAの要求事項を上回るサイバーセキュリティ プラクティス

CIP は CRA の要件を超える高度なセキュリティ慣行を実施しており、特にカーネル作業グループでは、すべてのリリース タグと tarball が暗号的に署名される必要があります。この非否認の原則は、コミットの整合性とコミッターの識別を明確に保証しますが、プロジェクトは、開発者が個別の秘密鍵を使用することに関して、より標準化されたアプローチが望ましいと懸念を示しています。さらに、CIP はソフトウェア コンポーネントの長期サポート（LTS）を提供することを目指しており、最小で 10 年間の保守期間をターゲットにしています。この取り組みは、民間インフラ システムが長期間にわたり安全かつ信頼性を保ちながら運用できることを保証するのに役立ちます。すべてのオープンソースと同様に、開発やソースコードの成果は公開されており、他の人々が欠陥を見つけて報告することが容易になります。

さらなる洞察

CIP は、特にオープンソース ソフトウェア開発と産業用途の特有の特徴に関して、CRA にいくつかの重要なギャップがあることを指摘しています。

主な懸念点は、規制がオープンソース エコシステム内のオープンソース プロジェクトのガバナンス モデルの多様性を十分に認識していないことです。CRA が想定する構造（例：オープンソース ファウンデーションのスチュワードとしての役割）を実施していないプロジェクトは、必要なサポート組織なしで、サイバーセキュリティの姿勢に関して同様の期待を抱かれる可能性があります。多くの主要なオープンソース ソフトウェア プロジェクトは、スチュワードとして機能するオープンソース ファウンデーションによってホストされていますが、そうでないものもあります。例えば、Debian プロジェクトは、2024 年に 1600 人以上の貢献者がいる広く使用されている Linux ディストリビューションを開発しており、スチュワードとして資格のあるホスティング組織はありません。

さらに、OSS の貢献者は特定の時期に OSS プロジェクトに対して機能やパッチを提供する義務がないため、産業ユーザーは特定の OSS プロジェクトに依存する製品のロードマップを計画することができません。ユーザーは OSS プロジェクトに貢献することはできますが、典型的な中規模プロジェクトは少なくとも数千の OSS ライブラリやコンポーネントを使用しており、これらの依存関係を管理し、ライセンスを監視するだけでも手間がかかります。どの産業ユーザーも、自分たちが恩恵を受けているすべての OSS プロジェクトを支援することはできません。従来の IT ワークフローやビジネス慣行がオープンソースの方法に転送できないもう一つの例は、OSS プロジェクトのサンセット（寿命終了、EOL）の問題です。OSS においてこれは複雑なトピックであり、リード メンテナーが OSS を EOL と宣言しても、他の人々がそれをフォークして維持することができるからです。新たな規制は産業ユーザーに脆弱性からの自由を確保することを求めていますが、規制が期限を設定し始めると、その期限を守らせることが困難になるでしょう。

さらに、産業システムの非常に長いライフサイクルに関して、CRA のサポート要件（第 13 条）について懸念があります。具体的には、CRA はサポート期間が「製品が使用されると予想される期間」を反映することを要求しています。しかし、鉄道システムは通常 30 ～ 50 年の間運用され、その他のシステムも長寿命です。このため、CRA が要求する製品の合理的なライフサイクル全体にわたる無料のセキュリティパッチの提供は、ビジネスの観点から持続不可能となる可能性があります。特に、こうした長期間にわたる無料のセキュリティ パッチを提供する義務は、組織が数十年にわたるメンテナンス活動の予算を立てる必要があるため、持続不可能なビジネス計画のシナリオを生み出します。この規制要件と、長寿命の産業システムの実際的な現実との不一致は、長期的な運用期間を持つ分野で CRA のセキュリティ メンテナンス規定を実施する上での重要な課題を浮き彫りにしています。

また、CRA のセキュリティ要件と高度に規制された業界の現実との間に潜在的な不一致がある可能性もあります。例えば、Schroeder は、これらの業界における製品の評価および承認プロセスが通常数ヶ月を要し、その間に新たな脆弱性が発生する可能性があることを説明しています。Schroeder は、セキュリティ管理に対してより柔軟なアプローチを提案しており、異なるコンポーネントに対しては、その攻撃面や重要性に基づいて異なるセキュリティ対応プロセスを適用するべきだと述べています。例えば、カーネルのような重要なコンポーネントには、より厳格な認証プロセスを適用し、その他のシステム コンポーネントは定期的な月次更新サイクルに従うという方法です。しかし、プロジェクトは、このようなアプローチを受け入れるためには業界の慣行や期待が進化する必要があると指摘しています。

多くの産業メーカーは主に OSS の利用者であり、貢献者ではないため、長期的なメンテナンスに対する資金が不足しています。この不均衡は、しばしば半導体ベンダーなどの上流の開発者に不相応な負担をかけ、重要なオープンソース インフラの持続可能性を損なうリスクを生じさせています。

Yocto Project

Yocto Project は、Linux Foundation がホストするオープンソース ソフトウェア プロジェクトであり、開発者がハードウェア アーキテクチャに依存せずにカスタム Linux ベースのシステムを作成できるようにするものです。これは、カスタム組み込み Linux オペレーティング システムを構築するための業界標準的な「ツールキット」として広く使用されています。このプロジェクトは柔軟なツール群を提供し、組み込み開発者が世界中でテクノロジー、ソフトウェア スタック、設定、ベストプラクティスを共有できる場を提供しています。これにより、組み込み機器や IoT デバイス、あるいはカスタム Linux OS が必要とされるあらゆる場面で使用可能な、特化された Linux イメージを作成することができます。Yocto Project は、メンテナーによって主導され、Yocto Governance Board によって調整される階層的なガバナンス構造のもとで運営されています。

分類

Yocto Project はオープンソース ソフトウェアのスチュワードとして運営されており、企業が自社の PDE やサービスを開発するために利用するオープンソース ソフトウェアを提供しています。プロジェクト自体は、収益化された PDE やサービスをリリースしておらず、オープンソース ソフトウェアを補完する商用製品も提供していません。

Yocto Project はスチュワードとして運営されているにもかかわらず、CRA の条項 13 における製造者の義務に沿った複数のサイバーセキュリティ プラクティスを実装しています。具体的には、共通脆弱性識別子（CVE）の体系的な監視を通じてサイバーセキュリティ リスク評価を実施しており、ビルド時に CVE チェックを行っています。このアプローチは、Yocto Project を基にオペレーティング システム環境を構築することが多い下流の製造者にとって、セキュリティ管理の基盤を提供するものです。プロジェクトでは、バグ報告と修正のためにバグ追跡システムである Bugzilla を使用しており、CVE チェッカーは機械可読な形式で提供されています。長期的なセキュリティ サポートに関しては、Yocto Project の現在の 4 年間の LTS（Long Term Support）サポート期間は、CRA が定めるセキュリティ更新の最低 5 年間、および 10 年間の利用可能期間という要件には満たない状況です。ただし、最近 LTS 期間を 2 年から 4 年に延長したことは、長期的なセキュリティ サポートを求める組織にとってプロジェクトへの関与を促進する要因となり得ます。プロジェクトはこのギャップを認識しており、5 年の基準を満たすように LTS 期間をさらに延長する用意があると述べています。Yocto Project は「コ トラベラー モデル（co-traveller model）」を支援しており、このモデルでは、プラットフォームを利用する製造者が共通のツール、データ、更新および修正を通じてセキュリティに協調的に取り組みます。この協力的アプローチにより、単一の製造者からの脆弱性報告や修正であっても、ユーザー ベース全体にセキュリティ上の恩恵がもたらされます。

CRA の本質的要件への準拠

開発プラクティス

Yocto Project の既存のサイバーセキュリティ プラクティスは、CRA の要件とよく一致しており、同プロジェクトが長年にわたり堅牢なセキュリティ プラクティスに取り組んできた姿勢を反映しています。この一致は偶然ではありません。Yocto Project はもともと、ソフトウェアのカスタマイズ プロセスに秩序をもたらすことを目的に、製造者やエコシステム全体の下流ユーザーからのインプットを得ながら、設計・文書化されたビルド手順を通じて構想されたプロジェクトです。

Yocto Project は体系的なリリース サイクルを維持しており、主に 2 つのリリース タイプを採用しています。標準リリースは毎年 4 月と 10 月に実施され、6 か月間のサポートが提供されます。長期サポート(LTS) リリースは 2 年ごとに行われ、プロジェクトから 4 年間のサポートを受けます。更新は Git ベースのワークフローで管理されており、機能更新とセキュリティ更新が区別されています。機能更新は通常、6 か月ごとのリリースに含まれ、セキュリティ更新は必要に応じてリリース間に提供されます。プロジェクトでは、各リリースが安定ブランチとなるブランチおよびタグシステムを採用しており、明確な保守ポリシーに基づいて運用されています。すべての開発は master ブランチで行われ、継続的インテグレーション テストが適用されることで、堅牢な品質保証体制が確保されています。更新に関する情報は、IRC、メーリングリスト、ブログ投稿、メンバー ミーティングなど、複数のコミュニティ チャネルを通じて発信されます。

このプロジェクトでは、包括的な開発手法が Git ベースのワークフローを中心に展開されており、明確なリリース管理プロセスが整備されています。ソフトウェアのリリースは、電子メールによるアナウンス リストや週次のステータス レポートなど、複数のチャネルを通じて通知され、下流の利用者が今後のリリースに備えられるよう配慮されています。リリース手順は、プロジェクトの Wiki や docs.yoctoproject.org に詳細に記録されており、透明性と監査可能性が確保されています。Yocto Project のドキュメントはリリースに対応してバージョン管理されており、特定のリリースに関連するドキュメントを容易に照合できます。また、タグ付けシステムを通じて開発版と正式リリース版を明確に区別しており、タグが付けられたバージョンのみが公式リリースと見なされます。特に、Yocto Project のビルド プロセスには、統合された上流コンポーネントのカスタマイズに関する詳細なドキュメントが含まれており、そのソフトウェア サプライチェーンの透明性が担保されています。

サイバーセキュリティ ポリシー

サイバーセキュリティ ガバナンスは、いくつかの主要な要素を中心に構成されています。プロジェクトでは、Bugzilla を用いたバグトラッカーを運用しており、セキュリティ関連のタグ付け機能も備えています。また、ドイツの Sovereign Tech Fund による監査を通じて、セキュリティ対応プロセスが強化されています。CVE スキャンツールも提供されており、これはプロジェクトの中核部分および下流の製造業者の双方にとって有益です。セキュリティに関するコミュニティの関与は、定期的なバグ トリアージ会議を通じて行われており、優先事項が共同で特定・対処されています。脆弱性に関する情報はメーリング リストを通じてコミュニティと共有されており、バグ報告のためのベストプラクティスも文書化されています。これには、すべてのレイヤーに「セキュリティ ファイル」を用意することも推奨事項として含まれています。実際に悪用されている脆弱性の対応において、Yocto Project は技術指導委員会（Technical Steering Committee）によって調整された体系的な手法を採用しています。対応プロセスは、脆弱性がユーザーが追加したコードに起因するのか、それともプロジェクト レイヤーに起因するのかを特定することから始まり、その後、オープンソースの手段を通じた修正の共同開発へと進みます。このような透明性の高い脆弱性管理の手法により、セキュリティの改善が下流ユーザー全体のエコシステムに波及する仕組みが実現されています。

MSAとの協力

Yocto Project は、創設者であり Linux Foundation フェローの Richard Purdie を含むセキュリティ チームを維持しています。このチームは米国 NIST が管理する National Vulnerability Database（NVD）と緊密に連携しています。セキュリティ対応については、専任スタッフ 1 名と複数の契約者で対応可能ですが、Purdie は、技術的には対応可能でも、リソース不足のため迅速かつ丁寧な対応には限界があると述べており、より迅速な対応には追加の人員を雇用するための資金が必要であると説明しています。

任意参加のサイバーセキュリティ信頼性検証プログラム

Yocto Project は、再現可能なビルドやコンプライアンス検証を重視しながら、そのプロセスの体系的な文書化と明文化を通じてアテステーションに取り組んでいます。ただし、Purdie は、CRA におけるアテステーションの用語が不明確であり、アテステーション プログラム自体がまだ確立されておらず任意である点を指摘しています。また、Yocto Project は **OpenSSF のシルバーバッジを保持しており**、脆弱性データベースに対する定期的なチェックや自動化されたコンプライアンス モニタリングを含む堅牢なセキュリティ検証を実施しています。ビルドプロセスの一環として、**SPDX**（System Package Data Exchange）3.0 SBOM 標準に準拠したソフトウェア部品表（SBOM）を生成しており、SPDX を採用した理由は、CRA のトレーサビリティおよび透明性要件を満たすための効率的な手段であると判断したからです。さらに、Yocto Project は CVE 分析のツールを提供しており、**Valkyrie という自動テストシステム**を通じて定期的にレポートを生成しています。これらのツールは、コアプロジェクトおよびメタレイヤーの両方に関する詳細なパッチメトリクスを提供し、包括的なセキュリティ監視を可能にしています。現時点では、Yocto Project はリリース時に **VEX（Vulnerability Exploitability eXchange）や CSAF（Common Security Advisory Framework）**といった脆弱性開示情報を提供していませんが、これまでは必要とされてこなかったためであり、提供は可能であると述べています。さらに、Yocto Project はビルド時に実行可能な CVE チェック機能を備えており、セキュリティ ステータスを追跡するための公開リソースを Wiki 上で提供しています。

CRA の要求事項を上回るサイバーセキュリティ プラクティス

Yocto Project は、CRA の要件を超える高度なサイバーセキュリティ実践をいくつか導入しています。これらの実践の中核となっているのが、再現可能ビルドへの包括的な取り組みです。ビルドが再現可能であるとは、同一のソースコード、ビルド環境、ビルド手順が与えられた場合に、任意の関係者がすべての指定された成果物をビット単位で同一に再構築できることを意味します。再現可能ビルドは、ソースからバイナリ コードへの独立した検証可能な経路を提供することで、多くの攻撃に対抗します。[10] Yocto Project は、任意のホストシステム上でのソースベース ビルドに対して再現可能ビルドを提供する数少ないプロジェクトの一つであり、ビルド場所に依存しません。この再現性の機能は、ソフトウェアの完全性を徹底的に検証できるようにし、特定のビルド変更を通じてセキュリティがどのように損なわれる可能性があるかについての詳細な分析を支援する、重要なセキュリティ メカニズムとして機能します。さらに、Yocto Project の積極的なセキュリティ姿勢は、SPDX 3.0 への完全対応や、ビルド監査可能性の重視にも表れています。現行の CRA 要件を超えて、Yocto Project のメンテナーは、ソフトウェア マニフェストにオー

プンソース ソフトウェア層の再ビルドを可能にする十分な情報を含めることを要件とするよう提案しています。これは、より広範な「ソフトウェアの修復可能性」というビジョンと一致しており、特に製造元がすでに存在しない状況においても、ユーザーがソフトウェアを独自に再ビルド・修復できる能力を保持すべきであるという考え方です。加えて、CVE処理においては標準化されたコンポーネント命名が必要であると指摘し、この標準化は EU にとどまらず、NVD などのグローバルな脆弱性データベースと整合する形で、国や業界を超えたより統一的な脆弱性管理アプローチを構築すべきだとしています。

Zephyr Project

Zephyr Project（Zephyr）は、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（RTOS）の構築に焦点を当てたオープンソース プロジェクトです。これは、シリコン ベンダー、OEM、ODM、ISV、OSV が技術を提供して、コスト削減と市場投入までの時間の短縮を図ることができる、ベンダー ニュートラルなプロジェクトです。そのコミュニティ メンバーは、新しいハードウェア、開発ツール、センサー、およびデバイス ドライバーのサポートを行っています。セキュリティ、デバイス管理機能、接続スタック、ファイル システムの強化が頻繁に行われています。Zephyr の運営委員会は、プロジェクトに関する財務問題を担当し、技術指導委員会はプロジェクトの技術的方向性を監督しています。

分類

Zephyr はオープンソース ソフトウェアのスチュワードとして機能しており、企業が自社の PDE（製品開発環境）やサービスを開発するために使用するオープンソース ソフトウェアをリリースしています。Zephyr 自体は PDE や商業サービスをリリースすることはなく、オープンソース ソフトウェアを補完する商業的な提供も行っていません。プロジェクトのソフトウェアは、プロジェクトのウェブ サイトから無料でダウンロード可能で、GitHub 上でオープンに開発されています。

CRA の本質的要件への準拠

開発プラクティス

Zephyr 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ています。新しいバージョンは 4 ヶ月ごとにリリースされ、各リリースにはサポート期間が設けられています。また、2.5 年ごとに長期安定版がリリースされ、2.5 年間サポートされます。ソフトウェアのリリースは、リポジトリのタグ付け、メーリング リストの発表、Discord の通知、専用の Q&A セッションなど、複数のチャネルを通じて伝えられます。リリース プロセスはプロジェクトのオンライン ドキュメントに包括的に記録されており、透明性と監査可能性が確保されています。プロジェクトは、メイン ブランチでの開発アプローチ、セマンティック バージョニングの実践、および新しい貢献者向けの詳細な「はじめに」ガイドを通じて、開発版とリリース版の明確な区別を維持しています。

サイバーセキュリティ ポリシー

このプロジェクトは成熟したサイバーセキュリティ態勢を備えており、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しています。特に、Zephyr は CVE 番号付与機関(CVE Numbering Authority) として堅牢なセキュリティ管理体制を維持しており、確立された製品セキュリティ インシデント対応チーム（PSIRT）を有しています。専用のメールアドレスを通じた脆弱性の自主報告用の明確なチャネルを提供し、是正情報を含む脆弱性レジストリを維持しています。この包括的なセキュリティ枠組みにより、コミュニティおよび下流の利用者との効果的な脆弱性情報の共有が実現されています。

MSAとの協力

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ます。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ます。

必須とされる 5 年間のサポート期間に関して、Zephyr の Kate Stewart は、サードパーティの保守組織との関係性に変化が生じると予想していますが、スチュワードと製造業者との間の関係性には大きな変化はないと見ています。より具体的には、Stewart は、サポート期間の延長があったとしても、製造業者がオープンソース開発への直接的な関与を増やす可能性は低いと主張しています。Zephyr の特定バージョンのサポートは 2.5 年間であり、それを超えて利用する製造業者にとっての選択肢は、より新しいバージョンの Zephyr へアップグレードすることです。そのためには、製造業者がアップグレードに備えるとともに、自社アプリケーションのためのテスト インフラを整備しておく必要があります。

任意参加のサイバーセキュリティ信頼性検証プログラム

Zephyr はすでに任意参加の信頼性検証プログラムに参加しています。プロジェクトは OpenSSF Scorecard を活用しており、OpenSSF Best Practices Badge プログラムにおいてゴールドステータスを達成しており、年次レビューによって継続的な準拠が確認されています。プロジェクトでは、SPDX 形式でビルドごとの SBOM を簡単に生成できるようになっています。多くのビルド ターゲットに対応した SBOM を掲載した公開ダッシュボードは、プロジェクト メンバーによって提供されており、SBOM の生成がビルド プロセスの一環としてシームレスに実現できることを示しています。

CRA の要求事項を上回るサイバーセキュリティ プラクティス

Zephyr は、CRA 要件を超えるいくつかの高度なサイバーセキュリティ対策を実施しています。その中核となるのがプロジェクトのエンバーゴポリシーであり、単独の責任者に依存しない体制を意図的に構築した組織的な PSIRT（プロダクト セキュリティ インシデント対応チーム）によって補完されています。このプロジェクトは、OpenSSF スコアカードから新たに登場するポリシーの定期的な評価と自己証明を通じて、セキュリティ標準への積極的な取り組みを維持しています。Kate Stewart は、セキュリティのベストプラクティスが進化し続けるものであることを認識し、それに伴いプロジェクトの PSIRT プロセスも継続的に更新していく必要があると強調しています。これは、CVE や National Vulnerability Database（NVD）のインフラの変化に対応するためでもあります。さらに Stewart は、Motor Industry Software Reliability Association（MISRA）スキャンによるセキュリティ リグレッションの自動防止や、コントリビューター向けの専用セキュア プラクティス トレーニングなど、継続的なセキュリティ改善のためのさまざまな手段を強調しています。このような包括的なアプローチにより、開発プロセス全体にセキュリティの観点が組み込まれ、同時にコントリビューターコミュニティ内におけるセキュリティ専門性の育成も実現されています。

さらなる洞察

CRA の規制枠組みにおける潜在的なギャップについて、Stewart は 2 つの重要な懸念を提起しています。第一に、SBOM に関するガイダンスが加盟国に委ねられている点が、標準化の機会を逸していると見なされています。加盟国ごとに異なる SBOM のバリアントが出現する可能性があり、セキュリティ文書やコンプライアンスに不必要な複雑さを生むおそれがあります。第二に、ソフトウェアの来歴に関するリスク評価が十分に扱われていないというギャップがあります。現在の規制では、オープンソースのスチュワードがコードの信頼性を評価・確保する上で直面する課題、特にリポジトリ汚染攻撃やコード投稿の制御に関する課題が十分にカバーされていません。

スチュワードおよび製造業者との関与から得られた知見

2024 年 12 月にアムステルダムで開催されたスチュワードおよび製造業者向けワークショップは、Linux Foundation Europe および OpenSSF が主催した招待制のフォーラムであり、オープンソース関係者が CRA 準拠への準備を促進することを目的としていました。議論は、標準、認知、ツール化という 3 つの重要なワークストリームを中心に構成され、それぞれがオープンソース ソフトウェアの開発と統合におけるサイバーセキュリティのベストプラクティスを支援するための具体的なステップの定義、および今後 3 年間で CRA を実装する支援に焦点を当てていました。これらのワークストリームは、オープンソースのガバナンスを規制要件に沿わせるための協働努力、業界全体のより広範な認知の必要性、脆弱性管理およびコンプライアンスのための標準化されたプロセスとツールの開発の重要性についての洞察を提供しました。このワークショップは、CRA の義務を実践的でコミュニティ主導の取り組みに翻訳するための重要な場となり、スチュワードおよび製造業者が進化する規制環境を乗り越える支援となりました。以下に、それぞれのワークストリームからの要点を示します。

認知ワークストリーム

認知ワークストリームは、オープンソース プロジェクト、製造業者、そして広範なエコシステムにおいて CRA の理解を深める必要性に取り組んでいます。主な取り組みとしては、CRA の認知度を評価するための世界規模の調査の実施、組織が自らの規制分類を決定するためのインタラクティブな意思決定ツリーの開発、そして Linux Foundation が提供する CRA に関するガイダンスの更新と改善が含まれます。参加者は、OpenSSF が教育資料を作成する取り組みをリードする必要性を強調しました。これには、「CRA 101」コース、企業向けのトレーニング モジュール、および製造業者、市場監視当局、オープンソース ソフトウェアのスチュワードなどの異なる利害関係者に向けたペルソナ ベースのガイドラインが含まれます。その他の計画された活動には、CRA に特化したイベント、ワークショップ、そして用語の標準化と一般的な懸念事項に対応するための包括的な FAQ と用語集の作成が含まれています。

標準ワークストリーム

標準ワークストリームは、オープンソース コミュニティで開発されたベストプラクティスに基づいて、CRA に準拠した認識されたサイバーセキュリティ標準を確立するという緊急の必要性に焦点を当てています。参加者は、既存の ISO プロセスを活用して、CRA に対応する標準を作成し、広範な採用と規制遵守を確保する方法について議論しました。厳しいタイムラインを考慮し、CRA に関連する標準は CRA が完全に適用される前（2027 年 12 月 11 日）に発効する必要があるため、参加者は

これらの標準化機関との協力の迅速化と、標準の加速された開発に伴うリスクについて強調しました。ヨーロッパの規制団体との関係構築と、国内機関との連絡担当者の地位を確保することが重要なステップとして挙げられました。最終的な目標は、オープンソースのスチュワードと製造業者に明確さを提供し、業界全体でのコンプライアンス努力を効率化する広く受け入れられた標準を開発することです。

ツール化ワークストリーム

ツール化ワークストリームは、オープンソース プロジェクトと製造業者が CRA の義務を果たすために必要なリソースを提供することに焦点を当てました。OpenSSF は他の Linux Foundation プロジェクトと共に、標準化されたサイバーセキュリティ ポリシーと脆弱性報告テンプレートを開発し、オープンソース プロジェクトが安全な開発と開示のための明確なガイドラインを持つことを確保します。さらに、市場監視当局（MSA）との協力のためのコミュニケーション チャネルの確立と、MSA からのリクエストに対応するためのベストプラクティスの文書化も行われます。また、このグループは、オープンソース ソフトウェアのセキュリティに対する製造業者の信頼を高めるために、任意参加のサイバーセキュリティ信頼性検証プログラムの可能性を探りました。このイニシアチブには、OpenChain とのコラボレーションにより、標準化された適合証明書を開発し、プロジェクトがセキュリティのベストプラクティスと規制要件に従っていることを示すための支援が含まれる可能性があります。

ワークショップの成果

アムステルダムでのワークショップでは、CRA の要件を満たすためにオープンソースのスチュワードと製造業者の協力が不可欠であることが強調されました。参加者は、認識された標準の確立、認知度の向上、そしてコンプライアンスを確保するための実用的なツールの開発の重要性を強調しました。

しかし、長期的な課題は依然として存在し、特に規制アプローチが異なる管轄区域間（EU 外）の間での不一致が、グローバルなオープンソース開発に摩擦を生む可能性があるという点です。オープンソース ソフトウェアは国境を越えて運用されているため、サイバーセキュリティに関する規制の断片化は、プロジェクトや製造業者に対して矛盾した要件を課すリスクがあります。オープンソースが革新とセキュリティの柱として引き続き繁栄するためには、規制フレームワークがより高い調和を目指すべきであり、コンプライアンスの努力が断片化するのではなく、一致する環境を促進する必要があります。このワークショップで得られた教訓と特定された行動は、急速に進化する規制環境の中で、セキュアで持続可能なオープンソース開発のベストプラクティスを形成するうえで重要な役割を果たすでしょう。

スチュワードと製造業者のワークショップの議論を具体的な成果として、Linux Foundation Europe と OpenSSF は最近、CRA および世界中で進展するサイバーセキュリティ関連の立法に備えるため、メンテナー、製造業者、オープンソースのスチュワード向けの**グローバル イニシアチブ**を立ち上げました。このイニシアチブは、コミュニティ主導のサイバーセキュリティ標準の開発、コンプライアンス ガイダンスの提供、および必要なプロセスやツールの実装に焦点を当てています。さらに、このイニシアチブは、ステークホルダー グループ間での CRA に対する認知度を実証的に評価するために行われた研究を基に情報提供されます。これらの努力を CRA の目標と調和させることにより、このイニシアチブは、オープンソース コミュニティが進化する規制環境を効果的にナビゲートできるよう支援することを目的としています。詳細については、本文書のリソースセクションにある「Global Cyber Policy Working Group Resources」を参照してください。

結論 : オープンソースのセキュリティ強化と CRA 準備の整備

本報告では、オープンソース プロジェクトが CRA の要件を満たすための主要な課題と機会を、3 つの主要な Linux Foundation（LF）プロジェクトのサイバーセキュリティ体制を通じて探求しました。これらのケーススタディ、および LF およびコミュニティ主導のワークショップの洞察、CIP、Yocto Project、Zephyr Project におけるベストプラクティスの分析を通じて、CRA への準拠は単に規制フレームワークに従うことだけではなく、セキュリティ実践を積極的に改善し、セキュリティ ワークフローを標準化し、オープンソース エコシステム全体での協力を強化するための機会であることが明確になりました。

CRA はオープンソース コミュニティにとって大きな変革を意味し、規制の監視が導入され、上流と下流のネットワーク構造に長期的かつ広範な影響を与えることになります。これまでの規制アプローチが主にライセンスに関する考慮に焦点を当てていたのとは異なり、CRA はオープンソース ソフトウェアがどのように提供され、維持され、セキュリティが確保されるかに注目します。CRA はオープンソースのスチュワードの役割を製造業者とは異なるものとして正式に認識し、商業活動とは直接関係のないオープンソース プロジェクトを維持・開発する者に対して専任の責任を定めています。ライセンスだけでなく、オープンソース ソフトウェアの非商業的な提供に焦点を当てることで、CRA は現代のソフトウェアがどのように構築され、統合され、維持されるかの複雑さを認識しています。

さらに、CRA はオープンソース コミュニティにおける長年の課題にも取り組んでいます。それは、名前だけはオープンソースであるが実際にはそうでないプロジェクトです。多くのソフトウェア コンポーネントはライセンス上は技術的にオープンソースですが、意味のあるコミュニティの協力や透明なセキュリティ プロセスが欠けています。CRA は、重要なソフトウェア コンポーネントを提供するプロジェクトに対してサイバーセキュリティ要件の基準を課すことによって、オープンソース エコシステム全体でセキュリティ基準を引き上げ、広く使用されているソフトウェアが単にオープンソース ライセンスの下で共有されるだけでなく、積極的に安全かつ責任を持って維持されることを確実にしようとしています。

依然として多くの課題が残っています。例えば規制アプローチの断片化、リソースの制約、進化するセキュリティの脅威などが挙げられます。しかし、オープンソース プロジェクト、政府、企業が準備態勢を整えるために取るべき明確なステップもあります。これらのステップには、セキュリティの持続可能性に向けた長期的な計画、教育と訓練への投資、標準化されたセキュリティ ツールの採用、共同組織や標準開発へのより深い関与、そして何よりもプロジェクトを推進する強力な公共向けリーダーシップが含まれます。

推奨

持続可能なセキュリティ ロードマップの構築

この報告書からの重要なポイントの一つは、オープンソース プロジェクトにおけるセキュリティ計画のための長期的で体系的なアプローチの必要性です。特に、大規模なプロジェクトは短期的なコンプライアンス目標にとどまらず、5 年間のセキュリティ戦略を策定し、積極的な脆弱性管理、セキュリティ担当者への持続的な資金提供、そして下流のユーザーや規制当局との関わり方に関する明確なプロセスを含める必要があります。

セキュリティの透明性も非常に重要です。オープンソース プロジェクトは、既存のセキュリティ能力や必要なリソースについて明確にコミュニケーションを行い、ユーザーやステークホルダーがその強みとリソースのギャップを理解できるようにすべきです。専任の製品セキュリティ インシデント対応チーム（PSIRT）の設立は、大規模なプロジェクトにとって重要なステップであり、脆弱性が効果的に処理され、セキュリティ インシデントが体系的に対処されることを保証します。個々のメンテナーによる即席の対応に頼るのではなく、組織的な対応が求められます。

教育も重要な要素です。オープンソース プロジェクトやメンテナーは、CRA のコンプライアンスや脆弱性開示、セキュアな開発手法のベストプラクティスに関するより良いトレーニングを受ける必要があります。また、オープンソース ソフトウェアを統合する製造業者や企業も、サプライチェーン全体のセキュリティを強化する方法で上流のプロジェクトと連携する方法について、チームの教育を担当すべきです。

オープンソース エコシステム全体からの広範な協力によって開発されたサイバーセキュリティのベストプラクティスを採用することは、セキュリティとサプライチェーン管理の基本レベルを確立するための実績あるアプローチです。これには、**OpenSSF スコアカード**の適用や **security.txt ファイル**の維持、さらに **OpenChain 自己認証評価**の実施が含まれます。サイバーセキュリティは、明確に定義されたサプライチェーン プロセスに依存しているためです。

さらに、ライセンスの透明性も優先事項であるべきです。セキュリティがソフトウェア開発における重要な課題であるのと同様に、明確で一貫したライセンス管理の実践が強調されるべきです。OpenSSF のベストプラクティス認証を追求することは、セキュリティ姿勢の改善と業界で認められたセキュリティ フレームワークとの整合を図るための第一歩となります。

適切な場合には、開発プラクティスをCRAの概念に整合させる

実質的な変更が PDE に加えられた場合、適合性評価を更新する必要があるかもしれません。そのため、プロジェクトは自分たちのリリースが実質的な変更なのか、軽微な機能更新やバグ修正にすぎないのかを明示する必要があります。これを実現する方法の一つは、セマンティック バージョニングを使用して、CRA に基づく実質的な変更をメジャー バージョン、軽微な機能更新をマイナー バージョン、バグやセキュリティ修正をパッチ バージョンにマッピングすることです。この慣行は、ソフトウェアの下流のユーザーに対して、適合性評価の更新が必要となる場合を示すことができます。プロジェクトのメイン ブランチに基づいてローリング リリースが行われる場合、未完成のソフトウェア（前文 37）としてラベル付けすることが役立つかもしれません。そうしないと、下流のユーザーは実質的な変更と軽微な変更を区別するのが難しくなります。

プロジェクトのサイバーセキュリティ ポリシーや脆弱性管理手順に関する文書は時間とともに変更される可能性があるため、文書はバージョン管理され、プロジェクトにタグ付けされるべきです（可能であれば、ソースコードと同じリポジトリ内で管理されることが望ましい）。これにより、採用者は使用しているソフトウェア バージョンに一致する文書を識別できるようになります。

CRA によって義務付けられた長期サポート要件や、鉄道輸送や航空業界のようなさらに長期間のサポート期間は、適切に維持されているソフトウェア プロジェクトでさえ、その寿命を超える可能性があります。こうした状況では、組織は重要な依存関係が有効であり続けるように開発コミュニティに積極的に参加するだけでなく、寿命終了（EOL）コンポーネントを新しい技術に置き換えるための専門知識と能力を維持しなければなりません。

CRA は、個々の貢献者や法人化されていない緩く組織されたコミュニティを対象としていません。また、ソフトウェアを公開する公共部門の組織が規制の下で製造業者またはスチュワードとして該当するかどうかについても不確実性があります。それにもかかわらず、これらの組織は、製造業者およびスチュワードの義務をガイドラインとして自発的に遵守することから利益を得る可能性があります。このアプローチは、エコシステムのベストプラクティスと一致し、サイバーセキュリティの基準を確立し、組織が将来の規制要件に備える手助けとなります。

コンプライアンスとセキュリティのためのツールへの投資

セキュリティのベストプラクティスを効果的に運用するためには、セキュリティ ツールをソフトウェア開発プロセスにライセンスのベストプラクティスと同様にシームレスに統合する必要があります。GitHub が新しいプロジェクトを開始する際に開発者に OSI 準拠のライセンスを選択するよう促すのと同様に、セキュリティのベストプラクティス、例えば構造化された脆弱性報告、セキュリティ ポリシーの採用、標準化されたソフトウェア コンポーネント レジストリの利用に関しても、同様の促しや推奨が必要です。実用的であれば、それらをデフォルトで有効にすることで、採用における摩擦をなくすことができます。

SBOM（ソフトウェア部品表）の作成、例えば SPDX 3.0 の使用は、CRA の要件を満たすために重要となります。SPDX 3.0 は、プロジェクトがコンポーネント依存関係を文書化し、脆弱性を追跡し、製造業者がリスク評価に必要なデータを提供するのを容易にします。しかし、SBOM には、コンポーネント レベルの依存関係のみを追跡するのではなく、展開されたソフトウェア イメージに含まれる特定のソースファイルについての可視性を向上させるために、さらなる粒度が必要です。

SBOM を超えて、オープンソース プロジェクトは、脆弱性追跡、依存関係スキャン、サプライチェーンのセキュリティ監視など、自動化されたセキュリティ ツールを開発パイプラインに統合すべきです。これらのツールは、プロジェクトが規制要件を満たすのを助けるだけでなく、セキュリティ脅威に対するプロジェクトのレジリエンスを向上させることにも繋がります。

コストを削減したり、可能な限り自動化する努力は、特に小規模な OSS プロジェクトにとって非常に重要です。数百行程度のコードしかない 1 人で運営されているプロジェクトでは、時間やお金の面で高額な投資を維持することは通常不可能です。より大規模な OSS プロジェクトでもリソースは限られており、これらの取り組みを開発プロセス自体に「デフォルトでオン」にすることができれば、広範な改善がもたらされるでしょう。

政府や企業は、オープンソースのセキュリティ ツール開発に投資し、広く使用されているセキュリティ フレームワークがアクセス可能で、十分に文書化され、メンテナーが採用しやすいようにすることで、これらの取り組みを支援できます。

標準の開発と業界横断的な協力

セキュリティとコンプライアンスは、孤立して解決できる問題ではありません。オープンソース プロジェクトは、他のプロジェクト、政府、企業、非営利団体と積極的に連携し、業界全体でセキュリティの標準化と調和を推進する必要があります。CRA はセキュリティの期待値を世界的に一致させる機会を提供しますが、それはオープンソース コミュニティが協力し、ソフトウェア開発の現実を反映した規制とベストプラクティスを共に形作る場合に限られます。

早急に対処が必要な分野の一つは、ソフトウェアおよびコンポーネントの命名規則の標準化です。脆弱性データベース、パッケージ マネージャ、コンプライアンス ツール間でコンポーネントの識別方法に一貫性がなければ、セキュリティ リスクの追跡は不必要に複雑になります。従来は Common Platform Enumeration（CPE）が使用されてきましたが、CPE の中央集権的な割り当てシステムは、現代のソフトウェア エコシステムにはスケーラブルではありません。pURL（package URL）などの代替手段は大きな改善をもたらす可能性がありますが、それも合意されて使用される場合に限られます。プロジェクト間で協力し、CVE/NVD などの業界で認識されている脆弱性追跡フレームワークと整合する統一的な命名スキーマを確立すべきです。

さらに、CRA の用語、特に「ソフトウェアを市場に出す（placing software on the market）」ことと「市場でソフトウェアを利用可能にする(making software available on the market）」ことの違いについて、より明確な定義が求められています。これらの定義は、オープンソースプロジェクトおよびそのダウンストリームの採用者にとって、コンプライアンス要件に大きな影響を与えるため、オープンソース関係者と規制当局との協力により、実用的かつ現実的な解釈を確立することが必要です。

オープンソース プロジェクトは、セキュリティ標準化団体、政策に関する議論、業界横断的なセキュリティ イニシアチブに積極的に参加し、サイバーセキュリティ規制においてオープンソースの現実が適切に反映されるようにすべきです。こうした活動の資金調達は困難な場合もありますが、企業や製造業者も、自らが利用しているオープンソース ソフトウェアに対して、単に消費するだけでなく、そのセキュリティと持続可能性の向上に貢献する形で協力すべきです。

各国で規制が断片化するのを防ぐために、政府は業界のリーダーだけでなく、広範なオープンソース コミュニティとも連携し、サイバーセキュリティ要件の調和を図る必要があります。セキュリティ規制に関する世界的に整合性の取れたアプローチは、コンプライアンスの負担を軽減し、セキュリティの成果を向上させ、オープンソース開発の長期的な持続可能性を支えることにつながります。

新たに生じるセキュリティ課題への対応

多くのセキュリティのベストプラクティスは確立されていますが、現在のセキュリティ枠組みでは完全には対応しきれていない新たな課題も出現しています。中でも特に差し迫った懸念の一つは、AI モデルのセキュリティおよび、トレーニングデータセットが汚染されるリスクです。AI が支援・生成するコードがオープンソース開発において一般的になりつつある中で、悪意ある攻撃者がモデルのトレーニング段階で脆弱性を仕込もうとする可能性があり、その結果としてセキュリティ検証がはるかに複雑化する恐れがあります。

オープンソースのセキュリティ フレームワークは、AI 生成コードを考慮に入れて進化し、AI でトレーニングされたモデルの完全性を評価するための仕組みを提供する必要があります。これには、データセットの来歴に関するガイドラインの確立、改ざんの可能性を検出するための検証プロセスの導入、そして AI による貢献がセキュリティのベストプラクティスに準拠していることを確認するための新たな監査メカニズムの開発が含まれます。

政府、企業、そしてセキュリティ研究者は、オープンソース コミュニティと連携し、AI 支援による開発の安全性を確保するための新たな戦略を策定する必要があります。これにより、オープンソース ソフトウェアが引き続き、安全で信頼できるイノベーションの基盤であり続けることが保証されます。

オープンソース ソフトウェア セキュリティの推進力としてのリーダーシップ

セキュリティ ツール化、教育、そして標準の開発はすべて重要ですが、これらの取り組みが成功するためには、強力な公的リーダーシップが必要です。最もセキュリティ成熟度の高いオープンソース プロジェクトには共通点があります。それは、リーダーが積極的に自分たちのニーズを訴え、外部のステークホルダーと関わり、実際の変化を推進していることです。これにより、プロジェクト全体にセキュリティ文化を根付かせ、プロジェクト間や業界横断的な協力を生み出しています。

CIP、Yocto Project、Zephyr のようなプロジェクトのリーダーは、単なる技術の専門家ではありません。彼らはセキュリティのアンバサダーです。ブログを書いたり、数えきれないほどのプレゼンテーションを行ったり、ウェビナーを開催したりして、セキュリティ改善の重要性を訴えています。彼らの活動は政策立案者、資金提供者、業界のステークホルダーから注目を集め、協力や投資の機会を生み出しています。

オープンソースのセキュリティを前進させるためには、より多くのプロジェクトがこのリーダーシップのモデルを採用する必要があります。オープンソースのメンテナーは解決策が自分たちの元に来るのを待っていてはいけません。彼らは積極的に助成金を求め、規制当局に働きかけ、企業パートナーと関わり、そのセキュリティ ニーズを広めるべきです。たとえば、Richard Purdie の Yocto Project が直面する課題に関するブログ投稿は、ドイツの Sovereign Tech Fund からの資金提供につながり、どのように見える形で積極的なリーダーシップが具体的なセキュリティ改善を生むかを示しています。[11] Zephyr での彼女の活動を超えて、Kate Stewart の SPDX プロジェクトの共同リーダーとしての仕事は、それを国際的に認められた ISO 規格にしました。[12] そして CIP のリーダーたちは、セキュリティに関するトピックで定期的に発言しており、最近では Yoshitake Kobayashi と Dinesh Kumar によるウェビナーが、国際的な規格と規制の文脈において、安全で堅牢なインフラを提供するプロジェクトの価値を示しています。[13]

政府や企業は、このリーダーシップを支援するために、オープンソースのセキュリティ イニシアチブに資金を提供し、協力の機会を創出し、ポリシーやコンプライアンスの枠組みを作成する際に、オープンソースのメンテナー、ディレクター、その他の主要なステークホルダーの声に耳を傾ける必要があります。

オープンソースのセキュリティの未来は、CRA のような規制への準拠だけでなく、セキュリティのリーダーシップ、長期的な投資、そしてグローバルな協力を優先する文化的変革にかかっています。今日、オープンソース プロジェクト、企業、政府がこれらのステップを踏むことで、将来に向けてより強固で、よりレジリエントで、よりセキュアなソフトウェア エコシステムを共に築くことができます。

リソース

Global Cyber Policy ワーキング グループのリソース：

- Global Cyber Policy WG GitHub
- Slack の #wg-globalcyberpolicy
- Global Cyber Policy WG メーリングリスト
- CRA Readiness+Awareness SIG メーリングリスト
- CRA Tooling+Process+Formats SIG メーリングリスト
- CRA Spec Standardization SIG メーリングリスト

脆弱性の報告とガイダンス：

- LF プロジェクトおよび財団に特有の脆弱性報告に関するガイドライン
- Linux Foundation プロジェクトの一覧
- Linux カーネルのセキュリティ脆弱性は、Linux カーネルセキュリティバグページに記載された通り、security@kernel.org に報告すること
- Linux Foundation インフラストラクチャやメインの LF ウェブサイトに特有の脆弱性は、security@linuxfoundation.org に報告すること
- ソーシャル エンジニアリングによる乗っ取りへの警告

セキュリティのベストプラクティスとツール：

- Alpha Omega は、オープンソース ソフトウェア プロジェクトのメンテナーと提携し、オープンソース コード内の新たに発見されていない脆弱性を体系的に見つけ、修正する
- CNCF のファジング ハンドブックは、ファジングとは何か、そしてそれをどのように適用するかを説明している
- OpenSSF の技術的イニシアチブには、ベストプラクティス バッジ、スコアカード、Sigstore などが含まれる
- System Package Data Exchange（SPDX）オープン SBOM 標準（ISO/IEC 5692:2021）
- ポスト量子暗号アライアンスは、ポスト量子暗号の採用と進展を目指している
- Safer Languages は、セキュリティを考慮して設計されたプログラミング言語の利点について論じている（NIST）
- セキュアバイデザインの原則は、顧客のセキュリティをコアビジネス要件として優先する（CISA）

教育用リソース：

認定

- **Kubernetes and Cloud Native Security Associate** (KCSA)
- **Certified Kubernetes Security Specialist** (CKS)

インストラクター主導コース

- **Security and the Linux Kernel** (LFD441)
- **Kubernetes Security Fundamentals** (LFS460)
- **Zero Trust Security with SPIFFE and SPIRE** (LFS482)
- **Security Coding Fundamentals** (WSKF601)
- **Understanding Vulnerabilities and Security Threats** (WSKF603)

ハンズオン ワークショップ

- **Securing Coding Fundamentals** (WSKF601)
- **Understanding Vulnerabilities and Security Threats** (WSKF603)

無料コース

- **Developing Secure Software** (LFD121)
- **セキュア ソフトウェア開発 - 日本語版** (LFD121-JP)
- **Securing Your Software Supply Chain with Sigstore** (LFS182)
- **Understanding the OWASP® Top 10 Security Threats** (SKF100)
- **Introduction to DevSecOps for Managers** (LFS180)
- **Introduction to Zero Trust** (LFS183)
- **Cybersecurity Essentials** (A Must-Have for ALL Employees) (LFC108)

無料速習 (60-90分)

- **Security Self-Assessments for Open Source Projects** (LFEL1005)
- **Securing Projects with OpenSSF Scorecard** (LFEL1006)
- **Automating Supply Chain Security: SBOMs and Signatures** (LFEL1007)

eラーニング コース

- **Kubernetes Security Essentials** (LFS260)
- **Mastering Kubernetes Security with Kyverno** (LFS255)
- **Modern Air Gap Software Delivery** (LFS281)
- **Implementing DevSecOps** (LFS262)
- **Mastering Infrastructure Security: Strategies, Tools, and Practices** (SKF200)
- **Cloud Native Fuzzing Fundamentals** (LFS251)
- **Detecting Cloud Runtime Threats with Falco** (LFS254)

Research

- **Empirically-driven, security-specific insights from LF Research**

後注

1 **https://eur-lex.europa.eu/eli/reg/2024/2847/oj**
2 CRA は、その目的や予見される使用がデータ接続に関連する場合にのみ PDE に適用され、いくつかのケース（例えば医療機器）では別の規制が存在しますが、実際にはこの法律はほとんどの商業用ソフトウェアに適用されます。
3 Frank Nagle, Kate Powell, Richie Zitomer, and David A. Wheeler, “Census III of Free and Open Source Software: Application Libraries,” The Linux Foundation, December 2024. **https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_censusiii_120424a.pdf?hsLang=en**
4 **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02024R2847-20241120**
5 **https://openssf.org/blog/2024/12/23/cra-stewards-and-manufacturers-workshop-key-takeaways-and-next-steps/**
6 **https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847**
7 **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847 p. 29**
8 **https://opensource.org/osd**
9 **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847 p.31**
10 **https://reproducible-builds.org/**
11 **https://www.yoctoproject.org/blog/2024/03/28/maintainer-confidential-challenges-and-opportunities-one-year-on/**
12 **https://www.linuxfoundation.org/press/featured/spdx-becomes-internationally-recognized-standard-for-software-bill-of-materials**
13 **https://www.linuxfoundation.org/webinars/enhancing-cyber-resilience-with-cip**

謝辞

著者は、このレポートの公開を可能にしたすべてのプロジェクト コミュニティと、貴重な意見や指導を提供してくださったすべての方々に感謝しています。特に、以下の方々に感謝いたします。

Dan Applequist
Gabriele Columbro
Marion Deveaud
Mike Dolan
Esther Garcia
Urs Gleim
Anna Hermansen
Christian“ fukami” Horchert
Takehisa Katayama
Jan Kiszka
Megan Knight
Clara Kowalsky
Yoshitake Kobayashi
Todd Moore
Federica Nocerino
Richard Purdie
Christopher “CRob” Robinson
Stefan Schroeder
Kate Stewart
Christian Storm
Andrew Wafaa
David A. Wheeler

著者について

Mirko Boehm, PhD

Mirko Boehm は、フリーおよびオープンソース ソフトウェア（OSS）の貢献者、コミュニティ マネージャー、ライセンスの専門家、研究者であり、KDE デスクトップ（1997 年から、KDE e.V. 理事会での数年間を含む）、Open Invention Network、Open Source Initiative などの主要なオープンソース プロジェクトに貢献しています。彼はベルリン工科大学でフリーおよび OSS に関する客員講師および研究者としても活動しています。Mirko Boehm は、起業家、企業マネージャー、ソフトウェア開発者、ドイツ空軍の軍人として幅広い経験を有しています。2023 年 6 月には LF（Linux Foundation）に加入し、LF ヨーロッパのコミュニティ開発担当シニア ディレクターとして、ヨーロッパのすべてのオープンソース関係者とのエンゲージメントおよびコラボレーションの推進に注力しています。Mirko は英語とドイツ語を話し、ベルリン近郊に住んでいます。

Hilary Carter

カナダに拠点を置き、アイルランドとカナダの二重国籍を持つ Hilary Carter は、2021 年 3 月に Linux Foundation に加入し、LF Research を立ち上げて指導しています。オープンソース コミュニティ全体の関係者と広範囲にわたり連携しながら活動してきました。LF Research はその創設以来、規模での大規模な協力のパラダイムとしてのオープンソースに関する実証的洞察の決定的なコレクションを発表しており、オープンソース ソフトウェア、オープンハードウェア、オープンスタンダード、オープンデータの影響を体系的に測定し、個別のプロジェクトコミュニティ、企業、政府、そして社会全体に対して意思決定に役立つデータを提供しています。Linux Foundation に参加する前は、ブロックチェーン技術に特化したグローバルなシンジケート型リサーチ機関をリードしており、マネジメント コンサルティング、コミュニケーション、金融サービスの分野でのプロフェッショナルな経験を持っています。彼女は London School of Economics で経営学修士（MSc）を取得しています。

Cailean Osborne, PhD

Cailean Osborne は Linux Foundation のシニア リサーチャーで、オープンソースの資金調達の影響からオープンソース AI ガバナンスに至るまで、さまざまなオープンソースのトレンドと政策に関する研究プロジェクトをリードしています。Cailean はオックスフォード大学インターネット研究所で社会データ科学の博士号を取得しており、2023 年から 2024 年には中国・北京の北京大学オープンソース ソフトウェア データ分析ラボで客員研究員として活動していました。以前は、イギリス政府で AI 政策に従事し、OECD の AI に関するグローバル パートナーシップおよび欧州評議会の AI に関する特別委員会で UK 政府の代表を務めました。Cailean は多言語話者で、ドイツ・ベルリンを拠点にしています。

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation Research** は、拡大するオープンソース コラボレーションを調査し、新たな技術トレンド、ベストプラクティス、オープンソース プロジェクトのグローバルな影響に関する洞察を提供してい ます。プロジェクトのデータベースやネットワークを活用し、定量的・定性的手法のベストプラクティスに取り組むことで、Linux Foundation Research は、世界中の組織にとって有益なオープンソースの知見を提供するライブラリを構築しています。

CIVIL INFRASTRUCTURE PLATFORM
INDUSTRIAL GRADE LINUX

CIP は、**Linux Foundation** がホストするオープンソース プロジェクトで、民間インフラシステム向けの持続可能な産業グレードのソフトウェア プラットフォームを開発・維持することを目的としています。CIP の使命は、世界中の重要なシステムを支える安全で信頼性が高く、長期間にわたって機能するソリューションを提供することです。詳細については、**www.cip-project.org** をご覧ください。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Open Source Security Foundation (OpenSSF) は、Linux Foundation が主導する業界横断的なイニシアチブで、業界で最も重要なオープンソース セキュリティの取り組みと、それらをサポートする個人や企業を結集させています。OpenSSF は、オープンソース セキュリティを推進するために、上流のプロジェクトや既存のコミュニティと協力して取り組むことにコミットしています。詳細については、**openssf.org** をご覧ください。

yocto PROJECT

Yocto Project は、接続されたエッジデバイス、サーバー、または仮想環境における組み込みシステムの展開のために、カスタムの Linux ベースのシステムを作成するためのテンプレート、ツール、および手法を提供するオープンソースのコラボレーション プロジェクトです。ハードウェア アーキテクチャに関係なく、これらのシステムをサポートします。詳細については、**yoctoproject.org** をご覧ください。

Zephyr®

Zephyr® Project は、複数のハードウェア アーキテクチャをサポートするオープンソースの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（RTOS）です。詳細については、**zephyrproject.org** をご覧ください。

CC BY ND

Copyright © 2025 **The Linux Foundation**

このレポートは **Creative Commons Attribution-NoDerivatives 4.0 International Public License** にてライセンスされています。

参照する場合は、次のように引用してください。
Mirko Boehm, Hilary Carter, and Cailean Osborne,“ Pathways to Cybersecurity Best Practices in Open Source: How the Civil Infrastructure Platform, Yocto Project, and Zephyr Project are Closing the Gap to Meeting the Requirements of the Cyber Resilience Act,” foreword by Miriam Seyffarth, The Linux Foundation, March 2025.

この日本語文書は、上記レポートの参考訳として The Linux Foundation Japan が提供するものです。
翻訳協力：小笠原徳彦