THE LINUX FOUNDATION | Research

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

balena ERICSSON REVANITE

2026 年 CRA に関する認知度と準備状況

グローバルな CRA コンプライアンスに向けた構造的な準備不足と認知の停滞 そして、そのギャップを埋めるための時間的制約

Adrienn Lawson, The Linux Foundation

Foreword by Roman Zhukov, Red Hat

2026 年 6 月

2026 年 CRA に関する認知度と準備状況

CRAが年内に施行されたにもかかわらず、**回答者の66%は依然として同法についてよく知らないまま**であり、これは2025年の水準（62%）と同様である。

EU市場で製品を販売する際にはCRAを遵守する必要があるが、**米国およびカナダの回答者の72%は同法について認識していない。**

CRAについて既に理解している組織の41%は、この規制が実際に自分たちに適用されるかどうかを**まだ判断していない。**

2027年12月に完全な遵守が求められる。目標時期として正しく認識しているのは回答者のうちわずか34%で、46%は期限自体について依然として不明確なままである。

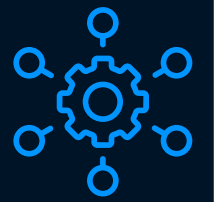
回答者の56%は、**法令違反に対する罰金が1500万ユーロ、または世界年間売上高の2.5%に達する可能性があることを認識していない。**

マニュファクチャラーのうち、全製品のSBOM（ソフトウェア部品表）を作成しているのはわずか32%で、51%は依然としてセキュリティ修正を上流のプロジェクトに受動的に依存している。

平均86個のプライベートフォークを維持するため、組織はリリースサイクルごとに約25万8000ドルの人件費を負担する必要があり、これは組織規模に比例して大幅に増加する。

2027年12月までに完全に準拠できると見込んでいるマニュファクチャラーはわずか41%で、39%はいつ準拠できるか分からないと回答している。

12,863件のプロジェクトを分析した結果、プロジェクトに貢献する組織の数はプロジェクトのセキュリティ体制を強く予測する要因となることが示され、**アップストリームへの投資が直接的なコンプライアンス戦略となること**を示している。



回答者の48%はデジタルメディアや開発者コミュニティを通じてCRAについて知った一方、EUの公式チャネルを通じてCRAを知ったのは回答者のわずか25%だった。

非営利のオープンソースソフトウェア開発者の59%は、**CRAの適用状況に関する明確なガイダンスがあれば、今後も貢献を続ける自信が持てる**と述べている。

2026年第1四半期におけるCVEの検出件数は前年同期比で394%急増し、14,000件以上のオープンソースプロジェクトにおいて、深刻度の高い脆弱性は811%増加した。

目次

序文 **4**
エグゼクティブサマリー **5**
導入 **6**
停滞した低い認識 **7**
全体的な認識は改善していない 7
具体的な知識のギャップ 9
標準規格の策定 10
広く利用可能なツールの認知度は低い 10
マニュファクチャラーの準備状況 **13**
マニュファクチャラーの準備は限定的 13
CRA時代のフォークのコスト 14
コンプライアンスのスケジュールと価格への影響 15
CRAを踏まえた中小企業の脆弱性 16
スチュワードとオープンソースプロジェクト **18**
スチュワードの準備状況 18
非営利OSSの視点 20
オープンソースプロジェクトのセキュリティ体制と脆弱性の傾向 21
結論 **26**
リソース **27**
メソドロジー **28**
アンケート対象者の属性 28
アンケートデータへのアクセス 28
著者について **30**
謝辞 **30**
付録 **31**

序文

OpenSSF Global Cyber Policy Working Group の共同議長、および欧州標準化機関（ESO）における Red Hat の代表者として、私はオープンソースコミュニティと欧州サイバーレジリエンス法（CRA）との関係性の進化を間近で見守っています。

過去数年間、OpenSSF の使命は教育とガイダンスに重点を置き、この画期的な規制が様々な組織にとって何を意味するのかをコミュニティや業界が理解できるよう支援するとともに、欧州の標準化活動に積極的に影響を与え、支援してきました。コン プライアンスへの道筋を継続的にマッピングし、生産的なワークショップの実施により、私たちは重要な基盤を築き、良好な成果を上げました。その結果、オープンソースはすべての CRA のマニュファクチャラーが頼りにする重要な技術として認識されるようになりました。

しかし、今年は方向転換が必要です。私たちは CRA の要件をすべての人にとって最も有意義で持続可能な方法でどのように実現できるかに焦点を当て、その実践にエネルギーを注ぎ込む必要があります。この実践的な取り組みの要となるのは、「責任の共有」という原則を受け入れることです。これこそが、世界全体を支える、より安全かつ持続可能なエコシステムを実現するための唯一の道だからです。Red Hat の複数の資料で強調されているように、オープンソースを利用する組織は、プロジェクトと連携して、すべての人にとって有益な、実用的で開発者中心のセキュリティ対策を採用する必要があります。

しかし、実務的な実施に向けて動き出す中で、2026 年 CRA に関する認知と準備状況のレポートは厳しい現実を明らかにしています。政策枠組みはかなり成熟しているものの、より広範なエコシステムの準備状況は完璧とは程遠いのです。2026 年 9 月の報告義務開始まであと数ヶ月、2027 年 12 月の全面施行まであとわずかという状況です。期限が迫る中、このデータは警鐘となるはずです。驚くべきことに、回答者の 66% が CRA についてまだよく知らないことです。さらに懸念されるのは、マニュファクチャラーの間で構造的な準備不足が見られることです。組織の 51% がセキュリティ修正を上流プロジェクトに受動的に依存している現状では、「消費して忘れる」という従来のモデルは、積極的なデューデリジェンスを求める CRA の要件と根本的に相容れません。

この報告書は、コンプライアンス回避策によって生み出された途方もない技術的負債を浮き彫りにしています。プライベートフォークを維持している組織は、リリースサイクルごとに平均 25 万 8000 ドルを費やしています。マニュファクチャラーにとって CRA への準拠をどのように進めるべきかはまだ不明確な点が多いものの、一つ確かなことがあります。それは、自分が依存しているオープンソースプロジェクトの多様性とセキュリティに投資することは、もはや単なる良き市民としての行動ではなく、ビジネスを行う上で不可欠な要素であるということです。

開発者、マニュファクチャラー、そしてスチュワードの方々には、ぜひこのレポートを熟読していただきたいと強く願っています。意識を高めるだけでは不十分です。CRA は、これまでに存在してきたどのコンプライアンスフレームワークとも根本的に異なります。持続不可能なプライベートフォークを捨て、標準化の場に積極的に参加し、より安全なグローバルソフトウェアサプライチェーンの構築に共に取り組んでください。

Roman Zhukov
Security Communities Lead, Red Hat Open Source and AI Program Office
Co-Chair, OpenSSF Global Cyber Policy Working Group

エグゼクティブサマリー

2026 年 CRA 認識と準備状況レポートは、世界のソフトウェアエコシステムが **欧州サイバーレジリエンス法（CRA）** にどのように備えているかを評価します。 2025 年のアンケート「**Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source**（日本語版 : **認識不足と不明確な現状：オープンソースにおけるサイバー レジリエンス法に対する準備状況の厳しい現実**）」を基にした今年のアンケートでは、回答者 数を前年比 23% 増の 843 人と拡大し、12,000 件以上のオープンソースプロジェクトのセキュリティ分析も実施しました。その結果、2027 年 12 月の完全準拠期限が近づく中、意識の停滞と構造的な準備不足が明らかになりました。

2026 年のアンケートで最も重要な発見は、業界全体の認知度の向上が見られないことです。 CRA が施行されたにもかかわらず、この規制について全く知らない、あるいは少ししか知らないと回答した人の割合は 66% に上昇しました。この認知度の低下は、特に米国とカナダなど、アンケート対象が新たな層にまで広がったことが原因と考えられます。米国とカナダでは、CRA を知らない人の割合が 72% に達しています。EU 市場に商用製品を投入するあらゆる組織はすべて CRA を遵守しなければならないことを考えると、この地域差は、グローバルサプライチェーンの大部分が依然として十分な準備ができていないことを示唆しています。CRA を認識している組織の間でも理解は深まっておらず、41% の組織は依然としてこの規制が自社に適用されるかどうかを判断していません。さらに、46% は遵守期限について確信が持てず、2027 年を目標年として正しく認識しているのはわずか 34% に過ぎません。また、56% は不遵守に対する罰則を認識していません。また、多くの組織は依然として基本的な定義の理解に苦慮しており、54% の組織は、異なる規制上の義務を負う「マニュファクチャラー」と「スチュワード」の役割の違いを整理している段階だからです。

マニュファクチャラーの準備状況は依然としてほとんど変化がなく、全製品のソフトウェア部品表（SBOM）を作成しているのはわずか 32% で、51% はセキュリティ修正を上流プロジェクトに受動的に依存し続けています。新たな重要なデータは、コンプライアンス回避策としてのプライベートフォークがもたらす経済的負担を浮き彫りにしています。平均して、組織は 86 個のプライベートフォークを維持しており、リリースサイクルごとに約 25 万 8000 ドルの人件費ががかかっています。従業員 5000 人以上の大規模な組織では、この負担は 1 サイクルあたり 1 万 1000 人時を超えます。このことは、CRA は最終的に、唯一の財政的に合理的な前進の道として、アップストリームへの貢献への移行を強制する可能性があることを示唆しています。中小企業は同時に最も影響を受けており、62% が製品の 4 分の 3 以上をオープンソースに依存しているのに対し、大規模組織では 35% にとどまっています。現在、欧州の中小企業の 51% は CRA について理解しておらず、この分野のマニュファクチャラーの 47% はコンプライアンスコストを賄うために価格を引き上げる予定です。

LFX にインデックス登録されている 12,000 件以上のオープンソースプロジェクトのデータによると、2026 年第 1 四半期に公開された CVE は前年比 394% 増加し、深刻度の高い脆弱性は 811% 増加したことが明らかになりました。この増加の要因としては、自動スキャンの改善、AI ベースのツールによる分析、CRA 対応による監査などが考えられます。この規模の増加は、マニュファクチャラーが依存するコンポーネント全体における脆弱性の実態に対する可視性が拡大していることを示しています。

LFX のデータは、プロジェクトによって回復力が異なる理由も示しています。組織の多様性はセキュリティの強力な予測因子であり、上流プロジェクトへの投資は、マニュファクチャラー自身のコンプライアンス体制への直接的な投資となります。準備のギャップを埋めるには、エコシステムは政策分析から運用ツールキットへと移行する必要があります。例えば、自動化されたコンプライアンスツールや、現在 CRA の下での自身の立場が不明確な非営利開発者の 61% に対するより明確なガイダンスなどが挙げられます。脆弱性への迅速な対応を管 理するには、管理者への財政的および法的支援も不可欠です。最終的に、成功には、公式の規制チャネルを超えて、オープンソース財団、オンラインディスカッション、ソーシャルメディアなど、実務者の大多数が学び、協力するコミュニティ主導の場へと移行することが必要となります。

導入

CRA は、欧州のサイバーセキュリティ規制における画期的な法律です。この法律は、デバイスやネットワークに接続できるあらゆるハードウェアやソフトウェアといった、幅広い製品を対象としています。スマートホーム機器や消費者向けアプリから、産業用センサー、企業向けソフトウェア、コネクテッドカーまで、市場に出回っているテクノロジー製品の大多数が対象となります。非営利のフリーソフトウェアやオープンソースソフトウェアの開発には重要な免除規定がありますが、商業サプライチェーンにおけるマニュファクチャラーだけでなく、輸入業者、販売業者には、新たな大きな義務が生じます。一方、オープンソースソフトウェア（OSS）のスチュワードは、比較的緩やかな規制体制の下に置かれ、義務も限定的です。

CRA は、これまで軽視されてきたオープンソースプロジェクトにおけるセキュリティ対策の改善に大きな推進力をもたらします。これは、この規制の影響に関する楽観的な見方です。つまり、マニュファクチャラーが依存するオープンソースコミュニティとの関わり方において、長らく必要とされていた変化を促すものです。悲観的な見方としては、移行のペースが遅すぎるという点が挙げられます。対策を講じなければ、マニュファクチャラーは規制施行時に準備不足に陥るリスクがあり、また、彼らが依存しているオープンソースプロジェクトは持続不可能な圧力に直面する可能性があります。

2026 年のアンケートは、Linux Foundation の購読者、パートナーコミュニティ、ソーシャルメディアから抽出した 843 名の回答者を対象に、2026 年初頭に実施されました。回答者は、地域、組織規模、業界を問わず、ソフトウェア業界全体にわたっています。アンケート方法は 2025 年のアンケートと同様で、前年との比較が可能となっています。

このアンケートには、一般的な認識に関するセクション（n=843）に加え、マニュファクチャラー（n=194 ～ 219）、スチュワード（n=28）、および非営利のオープンソースに関するセクション（n=109）といった役割別のモジュールが含まれていました。

スチュワードのサンプルに関する注記：スチュワードのサンプル（n=28）は、2025 年（n=34）よりも小さい。このセグメントからの知見は方向性を示す上で参考になるものの、サンプルサイズが限られているため、適切な注意を払って解釈する必要がある。

停滞した低い認識

全体的な認識は改善していない

2026 年のアンケートで最も重要な主要な発見は、図 1 に示すように、認知度の向上が見られないことです。2025 年 1 月から 2026 年 1 月にかけて、CRA が施行され、コミュニティがさまざまな教 育・啓発活動を開始した期間中に、CRA について「全く知らない」または「少ししか知らない」と回答した人の割合は 62% から 66% に増加しました。

この結果のもっともらしい説明の一つは、2026 年のサンプルには全体的に回答者が多く含まれているため、対象範囲が広がり、昨年は対象にならなかった人々も含まれているということです。他のトピック、特に AI の台頭が非常に注目を集めたため、CRA のような他の問題が埋もれてしまったのかもしれません。また、IT はこれまでこのような規制を受けたことがなかったため、規制変更の影響を全く考慮せず、また探そうともしません。他にも要因がある可能性はあるが、原因が何であれ、全体的な傾向は明らかです。業界全体の意識は過去 1 年間で向上していません。

図 2 に示すように、地域ごとの認識度は予測可能なパターンをたどっており、ヨーロッパの回答者は北米やアジア太平洋地域の回答者よりも高い認知度を示しています。ソフトウェアサプライチェーンはグローバルな性質を持つため、地域ごとの認識度の違いを理解することは重要です。北米やアジア太平洋地域の企業を含め、EU 市場に製品を投入するあらゆる組織は、CRA の規制を遵守しなければなりません。米国とカナダの回答者のうち 72% が CRA を知らないと回答していることから、ヨーロッパでソフトウェアを販売する北米企業の大多数は、2026 年 9 月の報告期限に向けて十分な準備ができていない可能性があります。これは、ほとんどの企業にとって CRA の最も早い遵守期限であり、マニュファクチャラーは悪用された脆弱性や重大なセキュリティインシデントを報告することが義務付けられています。

図 1：CRA に対する認識不足

66%

2025 年には、62% が CRA について「全く知らない」または「少ししか知らない」と回答するだろう。

62%

2026 年には、66% が CRA について「全く知らない」または「少ししか知らない」と回答するだろう。

2026 年 CRA アンケート、Q14、サンプルサイズ = 843
2025 年 CRA アンケート、Q18、サンプルサイズ = 685

詳細なデータについては、付録 A1 を参照してください。

CRA の下でのコンプライアンスのタイムライン

簡単に言うと、CRA は 3 つの段階で実施されます（CRA, 前文 126）

- **2026 年 6 月 11 日：**適合性評価機関の通知に関する規定の適用開始。加盟国は通知機関を指定する（CRA 実施文書）
- **2026 年 9 月 11 日：**マニュファクチャラーは、実際に悪用された脆弱性および重大なセキュリティインシデントの報告を開始しなければならない。
- **2027 年 12 月 11 日：**本規則が完全に適用される。

ほとんどのマニュファクチャラーにとって、2026 年 9 月は対応を求められる最初の期限となります。

図 2：地域に対する不慣れさ

サイバーレジリエンス法（CRA）について、どの程度ご存知ですか？（1 つ選択してください）

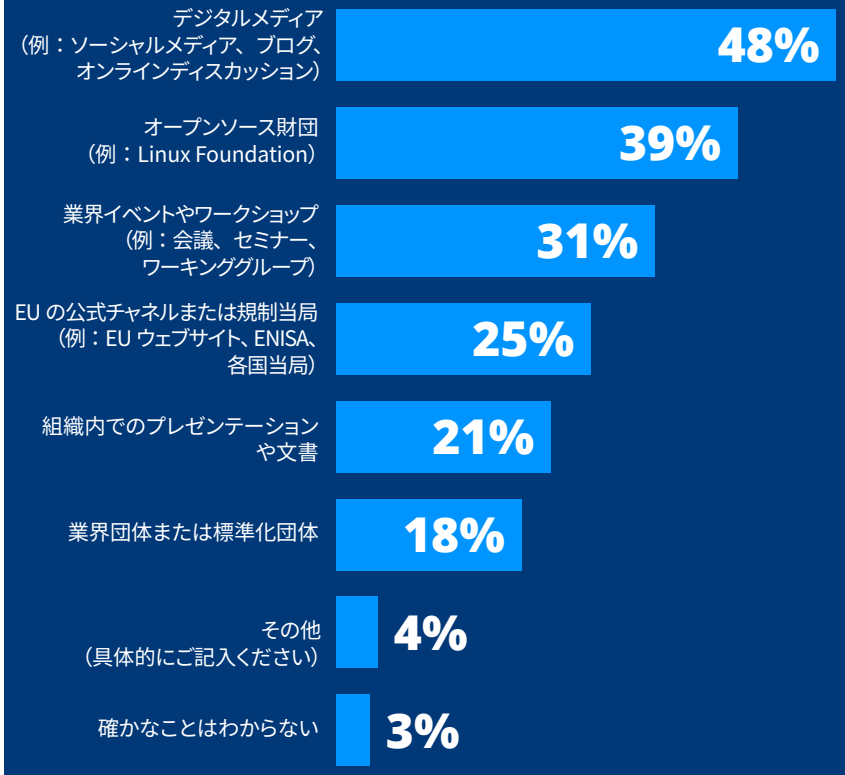
2026 年 CRA アンケート、Q14 by Q4、サンプルサイズ = 718

詳細なデータについては、付録 A2 を参照してください。

重要な点として、図 3 に示すように、CRA について知った回答者の 48% はデジタルメディア（ソーシャルメディア、ブログ、オンラインディスカッション）を通じて、39% はオープンソース財団を通じて知っています。公式の EU チャンネルが接触した割合は、アンケート対象者全体のわずか 25% にとどまっています。これは、特に技術職にある人々にとって、最も効果的な情報発信チャネルはコミュニティ主導型であることを示唆しています。オープンソース財団が情報仲介者として果たす役割は強調に値しますが、サンプルが既にオープンソースガバナンスに関わっている実務家に偏っているため、アンケート結果を一般化する際にはこの点を留意しておく必要があります。

図 3：CRA について学ぶためのチャネル

CRA についてどこで知りましたか？（該当するものをすべて選択してください）



2026 年 CRA アンケート、Q16、サンプルサイズ = 404、総回答数 = 767

アクション：コミュニティチャネルを通じたアウトリーチ活動
デジタルメディアとオープンソース財団は重要な情報発信チャネルであるため、支援エコシステムにとって高い投資対効果が得られるのは、開発者コミュニティで拡散されるコンテンツ、すなわち、短い解説動画、カンファレンスでの講演、ポッドキャストへの出演、そして CRA ガイダンスを人気の OSS ツールドキュメントに統合することである。EU の公式な情報発信だけでは十分ではない。

具体的な知識のギャップ

一般的な認知度の低さに加え、2026 年のアンケートでは、CRA を認識している回答者の間でも、具体的な知識のギャップが昨年のアンケートからほとんど変化していないことが明らかでした。これはもう一つの重要な発見である。CRA について聞いたことがある人でも、理解が深まっていません。

CRA についてある程度の知識があると回答した人々の間では、昨年と同様にいくつかの重要な知識のギャップが明らかになりました（図 4）。組織の 41% が、この規制が自社に適用されるかどうかをまだ判断していないことが分かりました。この不確実性は、実施期限が近づくにつれて、コンプライアンス上の大きな課題につながる可能性があります。

また、アンケートの結果、回答者の 46% が遵守期限について確信が持てず、完全遵守の目標年が 2027 年であることを正しく認識していたのはわずか 34% だったことが明らかでした。さらに、回答者の 56% が不遵守に対する罰則を知らないと回答しており、規制の執行メカ ニズムに関する教育が極めて重要であることが示唆されました。

回答者の間では、CRA におけるマニュファクチャラーとスチュワードの役割の区別について依然として不明瞭な点が多く、これは知識開発におけるもう一つの重要な課題となっています。現在、回答者の 54% がこれらの分類を理解しようと努めており、組織が自らの役割とそれに伴う義務を正確に判断できるよう、明確な枠組みと ガイドラインを作成する必要性が確認されています。

CRA に基づく：法令違反に対する罰則

「規定される罰則は、効果的かつ比例的であり、抑止力のあるものでなければならない。」（CRA 第 64 条 (1)）

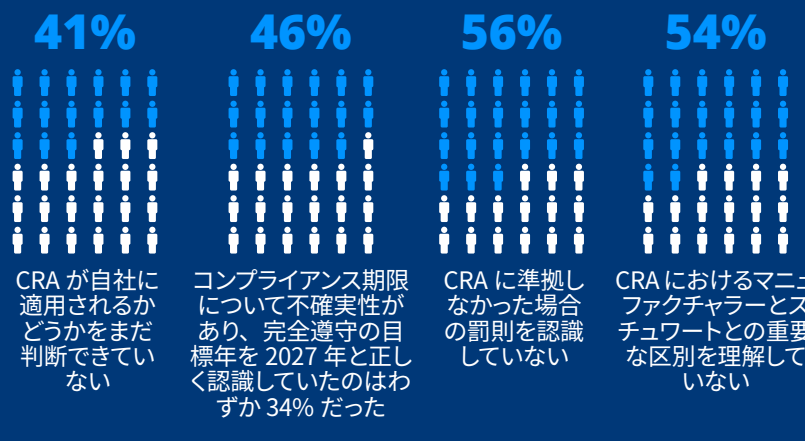
罰金額を決定する際には、当局は違反行為の性質、重大性、期間、過去に罰金が科されたことがあるかどうか、および違反組織の規模を考慮しなければならない。罰金は違反行為の種類に応じて段階的に設定されている。

- **必須のサイバーセキュリティ要件への不遵守：**最大 1,500 万ユーロまたは全世界年間売上高の 2.5%（いずれか高い方）
- **その他の義務の不履行：**その他の義務の不履行に対して、最大 1,000 万ユーロまたは全世界年間売上高の 2%の罰金
  - その他の義務については第 13、14 条に規定されている。
- **当局に不正確または誤解を招く情報を提供した場合：**最高 500 万ユーロまたは全世界年間売上高の 1%

免除（CRA 第 64 条 (10)）：

- 零細企業および小規模企業は、24 時間前の早期警告通知期限を過ぎた場合でも罰金が免除されます。
- オープンソースソフトウェアの管理者は、本規則の違反に対する罰金を免除される。

図 4：CRA を認知している回答者から得られた調査結果（前年から有意な変化なし）



2026 年 CRA アンケート、Q20、Q18、Q21、Q19、サンプルサイズ = 404

詳細なデータおよび 2025 年との比較については、付録 A3 ～ A6 を参照してください。

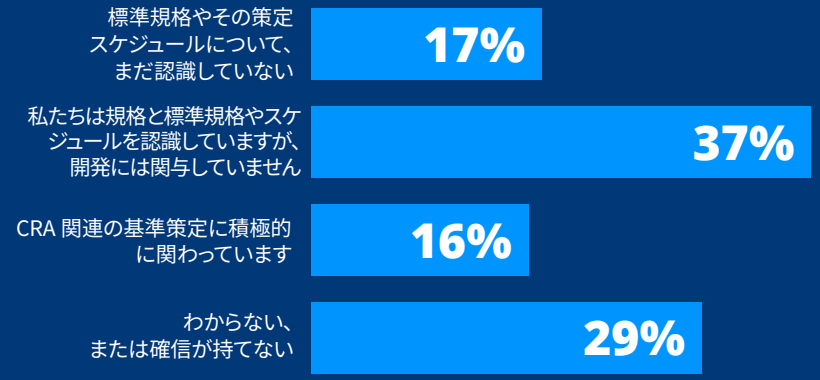
標準規格の策定

2026 年のアンケートにおける新たなデータポイントの一つは、CRA 関連の基準策定に対する認識と関与に関するものです。CRA は、とりわけ「セキュア・バイ・デザイン」が実際に何を意味するのかを定義するために、欧州および国際的な調和基準に大きく依存しています。これらの基準がなければ、組織は実際にどのような対応をすれば CRA に準拠できるのかについて、解釈上の不確実性に直面することになります。

これが重要なのは、CRA 第 19 条に基づく整合規格の策定が、製造事業者が利用できるコンプライアンス対応の道筋が直接的に決まるからです。標準化作業に携わる組織は情報面で優位に立ち、要件を形成する機会を得る可能性があります。図 5 に示すように、標準規格の策定スケジュールや自組織の関与状況について認識していない、または分からない 46%、そして標準規格について認識しているものの策定には関与していない 37% の組織は、次のような状況に直面するリスクがあります。

図 5：46%の組織が標準規格の策定を認識していない

貴組織は、CRA 関連の標準規格にどのように関わっていますか？（1 つ選択してください）



2026 年 CRA アンケート、Q22、サンプルサイズ = 194

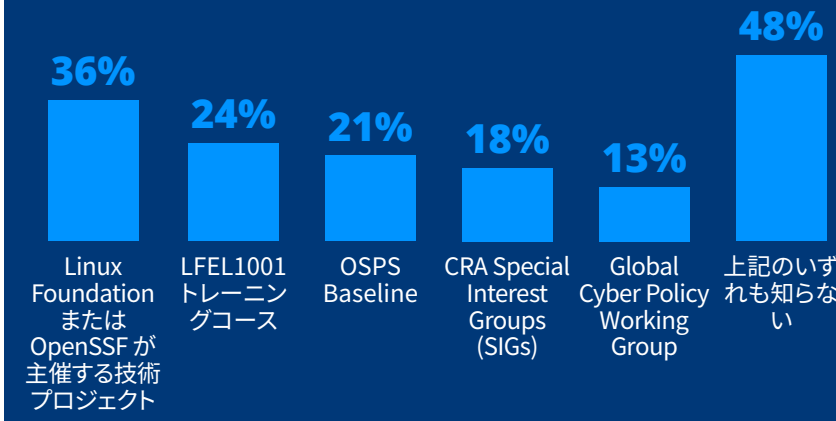
広く利用可能なツールの認知度は低い

豊富な CRA リソースが存在するにもかかわらず、対象としたコミュニティ全体で認知度は依然として大きな課題となっています（図 6）。Linux Foundation と OpenSSF の CRA 関連イニシアチブに焦点を当てており、他のリソースについては認識しているものの今回の調査には含まれていません。結果によると、回答者の 48% が Linux Foundation または OpenSSF の CRA 関連イニシアチブを全く認識しておらず、発見可能性に大きなギャップがあることが示されています（図 6）。認識していた回答者のうち、Linux Foundation または OpenSSF がホストする技術プロジェクトは認知度が最も高く 36% でした。これに続いて、**LFEL1001 Training Course** で 24%、**OSPS**

Baseline が 21% でした。さらに専門性の高いリソースになると認知度は低下し、CRA Special Interest Groups (SIGs) を認知している回答者は 18% にとどまり、Global Cyber Policy Working Group についてはわずか 13% でした。

図 6：CRA イニシアチブに対する認識（LF と OPENSSF）

Linux Foundation と OpenSSF による以下の CRA 関連の取り組みについてご存知ですか？（該当するものをすべて選択してください）



2026 年 CRA アンケート Q23、サンプルサイズ = 396、総回答数 = 634

図 7 に示すように、5 つの取り組みすべてが、5 点満点中で平均 3.78 ～ 4.19 の有用性スコアを獲得しており、その内容に触れた人々にとって明らかに役立つものであることが示されています。特に **LFEL1001 course** は無料で受講可能であり、60 ～ 90 分、有用性スコアが 5 点満点中 3.78 という、高い価値を持つ無償のリソースです。しかし、回答者の約 3 分の 1 しかその存在を知りません（**図 6**）。これは、これらのリソースを他の人々に知らせる新しい方法が必要であることを示唆しています。優れたリソースは、それを知っている人にしか役立たないのです。

図 7：CRA 関連イニシアチブの有用性評価（LF および OPENSSF）

以下のイニシアチブについて、どの程度有用だと感じたか評価してください。（各項目につき 1 つ選択）

イニシアチブ	平均有用性スコア（1 ＝まったく有用ではない、5 ＝不可欠）
OSPS Baseline	3.91
LFEL1001 トレーニングコース	3.78
CRA Special Interest Groups (SIGs)	3.93
Global Cyber Policy Working Group	3.92
Linux Foundation または OpenSSF が主催する技術プロジェクト	4.19

2026 年 CRA アンケート、Q24、サンプルサイズ = 81、94、69、51、141

さらに、「現時点では存在しないが、必要だと思う支援は何か」という自由記述の回答も収集しました。その結果からは、明確なニーズがあることがうかがえます（**図 8**）。最も多く挙げられた要望は、CRA に関する政策分析やホワイトペーパーをさらに増やすことではなく、特に中小規模の組織を対象とした、実務で活用できる段階的（ステップ・バイ・ステップ）な運用ガイダンスです。

アクション：実装ツールキットへの投資
支援エコシステムでは、CRA に関する認知を高めるための資料はすでに充実している。前述のとおり、こうした情報を影響を受ける組織へ届けるためには、異なる、あるいは追加の普及活動が必要である。次に優先して取り組むべき投資対象は、おそらく実務で活用できる運用ツールキットである。具体的には、組織規模別の CRA 準拠チェックリスト、SBOM 生成テンプレート、脆弱性開示ワークフローのテンプレート、そして CRA 第 24 条に規定されるスチュワード（Steward）の要件を満たすセキュリティポリシーの注釈付きサンプルなどが挙げられる。これらは、マニュファクチャラー、スチュワード、中小企業（SME）の各セグメントに共通して最も多く指摘された支援不足を解消するものとなる。

図 8：新たな CRA イニシアチブに対するテキスト形式

回答はテーマ別に分類され、言及回数に基づいて順位付けされています。

- **実践的な実装ガイダンス**（約 12 件の言及）- 実際のワークフロー、ステップバイステップガイド、既存の標準規格へのマッピング
- **教育リソースとトレーニング**（約 10 件の言及）- 簡略化された説明、オンラインコース、ワークショップ、ビデオ、短期集中講座
- **中小企業向けサポート**（約 8 件の言及）- リソースに制約のある組織向けの、手頃な価格のコンプライアンス対応方法、テンプレート、ツール
- **明確な文書化と要約**（約 7 件の言及）- 平易な言葉で書かれたガイド、要約版、簡潔な概要、要点
- **OSS 固有のガイダンス**（約 6 件の言及）- デューデリジェンスのフレームワーク、オープンソースのベースライン、OSS の脆弱性管理
- **SBOM およびツーリングのサポート**（約 5 件の言及）- テンプレート、VDR 規格、自動化ツール、技術フレームワーク
- **標準規格の解釈に関するヘルプ**（約 4 件の言及）- 水平 / 垂直規格の説明、改訂に関する最新情報
- **資金援助メカニズム**（約 3 件の言及）- OSS プロジェクトへの資金提供、サブスクリプションモデル、手頃な価格のソリューション
- **業界別ガイダンス**（約 3 件の言及）- 非 IT 分野（医療、化学）、教育機関
- **規制に関する認識**（約 3 件の言及）- 政策、法執行、罰則、保険への影響に関するニュースレター
- **国際協力**（約 2 回言及）- 学術提携、グローバル市場コンプライアンスガイダンス

2026 年 CRA アンケート、Q25、サンプルサイズ = 60

専門家からの情報

PHIL ROBB
Head of Ericsson
Software Technology

ERICSSON

ケンブリッジ辞典は、レジリエンス（resilience）を「問題発生後、以前の良好な状態に速やかに戻る能力」と定義している。高度に接続されたデバイスと AI による脅威が蔓延する現代において、サイバーレジリエンスは不可欠である。

エリクソンは、2022 年の CRA 草案以来、規制当局と連携し、お客様とオープンソースのエコシステムに利益をもたらすよう取り組んできました。2024 年初頭以降、CVE 修正、依存関係の強化、SBOM の公開、依存関係の自動更新、ゼロトラストの強化などを通じて、多くのオープンソースプロジェクトを強化してきました。

しかし、悪意のある行為者は活動を緩めていません。だからこそ、企業はオープンソースセキュリティ財団（OSSF）に集結しているのです。
私たちと一緒に取り組もう。レジリエンスは、チームで取り組むものなのだから。

マニュファクチャラーの準備状況

マニュファクチャラーの準備は限定的

マニュファクチャラーは、CRA の下でオープンソースソフトウェアへの依存をどのように処理するかという構造的な選択を迫られています。具体的には、フォークして独自に保守するか、エンタープライズサポートに費用を支払うか、アップストリームコミュニティに積極的に貢献するか、あるいはこれらの活動を組み合わせるかのいずれかです。データによると、多くの組織はまだこの選択を行っておらず、選択を行った組織も、技術的負債を生み出し、かつ広範なエコシステムの強化もできない独自保守パターンを選択する傾向が強いことが示唆されています。

マニュファクチャラーの行動に関する分析では、**図 9** に示すように CRA コンプライアンスへの準備において昨年と同様大きなギャップがあることが明らかに なりました。現在、すべての製品の SBOM を作成しているマニュファクチャラーはわずか 32% です。また、マニュファクチャラーの半数以上（51%）がセキュリティ修正をアップストリームプロジェクトに受動的に依存していることも判明しました。さらに調査では、OSS コンポーネントのセキュリティ対策を定期的に評価しているマニュファクチャラーはわずか 34% であり、規制で規定されているリスク管理と文書化の義務を満たしていないことも明らかになりました。今後の貢献について、マニュファクチャラーの 59% はアップストリームへの貢献計画がまだ不明確なままであり、20% は既に関与を増やさないことを決定しています。

実態：アップストリームプロジェクトへの受動的な依存
オープンソースのコンポーネントを含む製品を出荷する場合、マニュファクチャラーはそのコンポーネントが製品のセキュリティに及ぼす影響について責任を負うことになります。受動的な依存とは、マニュファクチャラーがアップストリームプロジェクトと直接的な関係を持たないことを意味します。この場合、マニュファクチャラーは修正プログラムを提供したり、プロジェクトの健全性を監視したり、脆弱性が開示された時期を追跡したりしません。単に新しいバージョンが登場するのを待ち、誰かが先に問題を発見してくれることを期待しているだけです。
CRA の下では、そのような姿勢はもはや通用しません。マニュファクチャラーは、サードパーティ製のコ ンポーネントを製品に組み込む際に、適切な注意義務を尽くし、脆弱性や開発された修正策（オープンソースのコンポーネントを含む）についてコンポーネントの提供者に通知することが義務付けられています（**CRA 第 13 条 (5) 及び (6) を参照**）。

CRA の下では：マニュファクチャラーが責任を負う
CRA は、オープンソースコンポーネントを製品に組み込むマニュファクチャラーにセキュリティ維持の責任を明確に課しています（CRA **第 13 条参照**）。 T この規制は、非営利のオープンソースプロジェクトに迅速なセキュリティ修正を提供する義務を課すものではなく、また、商用ユーザーのコンプライアンス要求を負担させるものでもありません。その代わりに、マニュファクチャラーは自社の依存関係のセキュリティに積極的に責任を負わなければならない枠組みを構築しています。CRA は、マニュファクチャラーがアップストリームでの修正に貢献したり、オープンソースプロジェクトに資金援助を提供したりすることを商業活動とみなさないと明示的に認めています（CRA **前文 18 項**）。 これはマニュファクチャラーにとって、直接的なコード貢献、セキュリティ改善、持続可能な資金調達モデルなどを通じて、オープンソースエコシステムの受動的な消費から積極的な参加へと移行する機会となります。

図 9：マニュファクチャラーと使用している OSS コンポーネント間の現在の相互作用パターン

昨年から大きな変更はみられない

自社製品すべてについて部品表（SBOM）を作成しているマニュファクチャラーは 3 社に 1 社

マニュファクチャラーの半数はセキュリティ修正をアップストリームプロジェクトに受動的に依存しており、さらに 23% は社内でコンポーネントにパッチを当てている

OSS コンポーネントのセキュリティ評価を行っているマニュファクチャラーは 34% と、依然として低い水準にとどまっている

マニュファクチャラーの 39%は今後セキュリティ修正プログラムを提供するかどうかまだ決めておらず、さらに 20%は提供しないことを既に決定している

2026 年 CRA アンケート、Q28、Q30、Q29、Q34、サンプルサイズ = 194-219

完全なデータと 2025 年との比較については付録 A6-A10 を参照してください。

CRA 時代のフォークのコスト

プライベートフォークは CRA 準拠のための短期的な回避策となり得ますが、「**ROI for Open Source Software Contribution Report**（日本語版：**オープンソース ソフトウェア貢献への投資対効果（ROI）**）」は、このアプローチが大規模になると大きなコストを伴うことを明らかにしています。同レポートの重要な洞察の一つは、プライベートフォークの維持管理が技術的負債の増大につながるという点です。平均して、組織はオープンソースコンポーネントのプライベートフォークを 86 個維持管理しており、それぞれリリースサイクルごとに保守と統合に 60 時間の作業時間が必要としています。これは、平均的な組織がプライベートフォークをリリースサイクルごとに維持するために、5,160 労働時間、つまり 258,000 米ドル [1] を費やす必要があることを意味します。

図 10 に示すように、これらのコストは組織規模に比例して急激に増加します。小規模組織（従業員数 1 ～ 249 名）では、プライベートフォークの維持にリリースサイクルあたり約 147 労働時間を要するのに対し、大規模組織（従業員数 5,000 名以上）では 11,152 時間以上を要します。この年間負担は、本来であればイノベーションやアップストリーム工程への貢献に充てられるはずの膨大なエンジニアリング時間を奪うことになります。

CRA の下では、こうしたコストは無視できなくなります。脆弱性処理、セキュリティアップデート、ソフトウェアの透明性に関する規制要件は、すべてのコンポーネントについて明確で監査可能な出所履歴を維持するという新たなプレッシャーを生み出します。これは、プライベートフォークでは本質的に複雑化します。一方、アップストリームへ修正を提供すれば、プロジェクトのユーザーコミュニティ全体でメンテナンスコストを償却し、異なるコ ードベースの管理という負担をなくすことができます。これらはすべて、CRA が要求するような透明性が高く、十分に文書化されたソフトウェアサプライチェーンの構築に役立ちます。この規制は短期的には法的複雑さをもたらしますが、最終的には経済をアップストリームへの関与へと決定的にシフトさせ、アップストリームへの貢献を単なるベストプラクティスというだけでなく、唯一経済的に合理的な道筋とする可能性もあります。これは、マニュファクチャラーの開発努力全体をアップストリームに振り向けろと言っているわけではありません。必要なのは自社製品に関連する脆弱性修正をアップストリームに提供することだけであり、これはプライベートフォークを既に維持している組織にとって十分に達成可能な目標です。

[1] このコストは、(a) 調査回答に基づくリリースサイクルごとのプライベートフォークの維持に必要な平均労働時間と、(a) Stack Overflow の年次開発者調査におけるソフトウェア開発者の世界的な回答の中央値である時給 50 米ドルの積です。出典 : https://survey.stackoverflow.co/2025/work#salary-comp-total

図 10：技術的負債としてのフォーク

組織規模	従業員数	プライベートフォークの平均数	1フォーク・1リリースあたり平均所要工数	1リリースあたり総工数	1リリースあたり総費用
小	1 ～ 249	7	21	147	$7,350
中	250 ～ 4,999	89	56	4,984	$249,200
大	5,000 以上	136	82	11,152	$557,600

2026 年 Open Source ROI アンケート、Q32 を Q13 でクロス集計、サンプルサイズ = 236

対策：プライベートフォークを監査しアップストリーム貢献へ投資する
プライベートフォークの保守は、CRA 準拠において最も顕著でありながら過小評価されているコストの一つであり、リリースサイクルごとに数千時間ものエンジニアリング工数を消費します。組織は、自社のプライベートフォークを体系的に監査し、フォークしなくてもよいコンポーネントや、アップストリーム貢献が可能なコンポーネントを特定し、構造化された貢献戦略を策定する必要があります。

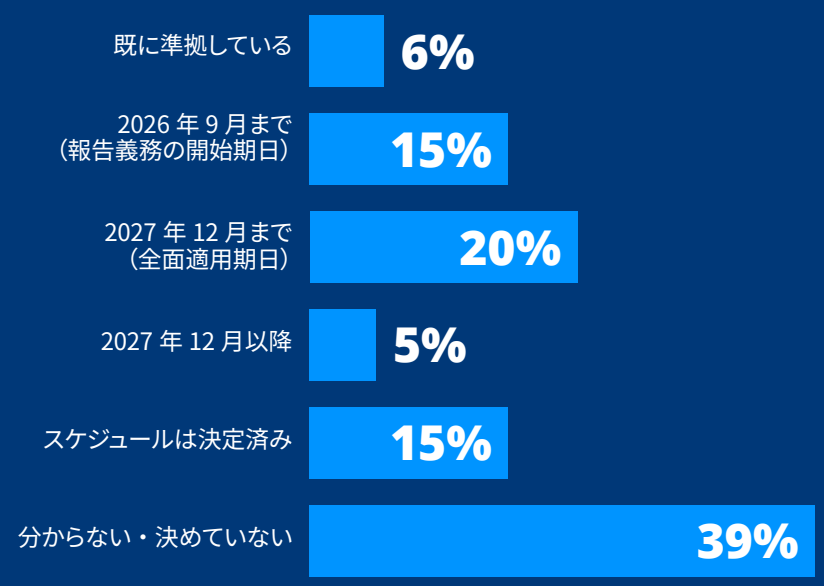
コンプライアンスのスケジュールと価格への影響

2026 年のアンケートでは、マニュファクチャラーに対して予想される法令準拠のスケジュールと価格への影響について直接質問しました。これらの回答により、不確実性の深刻さと、CRA 準拠に伴う経済的影響の可能性の両方が明らかになりました。

図 11 に示すように、2027 年 12 月までに準拠できると見込んでいるマニュファクチャラーはわずか 41% です。さらに 39% は、いつ準拠できるか分からないと回答しています。これは、完全準拠の期限まであと 2 年を切っている今時点での、業界が CRA への対応準備をどの程度整えているかを示す重要な指標です。

図 11：39%が CRA へいつ準拠できるか不明と回答

いつ CRA に完全準拠する予定ですか？（1 つ選択してください）



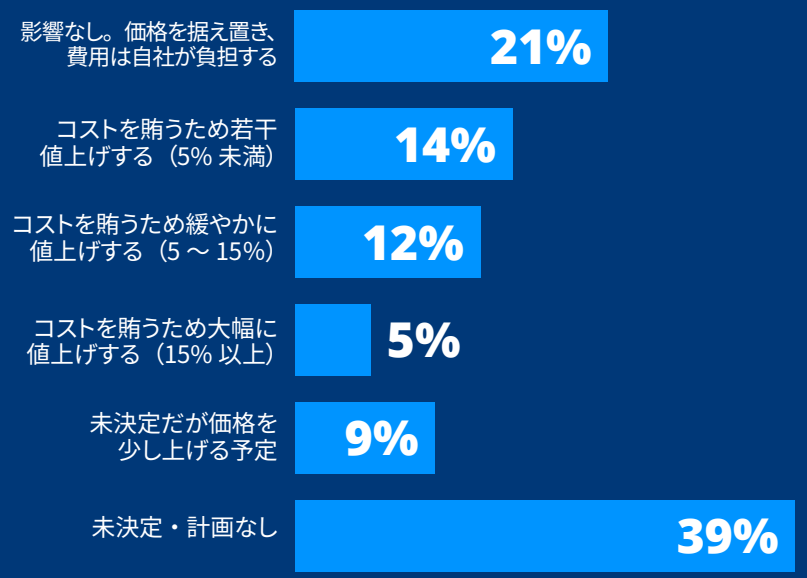
2026 年 CRA アンケート、Q38、サンプルサイズ = 194

図 12 は、コストへの影響をまとめたものです。マニュファクチャラーの 40% が、CRA 準拠のためのコストを消費者に転嫁すると回答しています。2025 年のアンケートでは、価格戦略を評価したマニュファクチャラーは平均 6% の価格上昇を予想していました。今年のデータでは、価格上昇を決定した企業の平均価格上昇率は 4% となっています。2026 年のデータでは価格への影響はやや小さくなり、回答者の 21%（2025 年のアンケートでは 14%）が影響なしと予想しています。

これは、多くの場合、多少か中程度の価格上昇が消費者に及ぶことを意味します。ただし、どの程度価格が上昇するかは企業ごとに異なり、CRA の実施が進むにつれて変化する可能性があります。CRA について既に認識しており、セキュリティに十分な注意を払っている組織にとっては、少ないコスト上昇に抑えられる可能性が高いと考えられます。影響を受けるマニュファクチャラーでさえ、CRA についてまだ認識していないマニュファクチャラーのコストがどの程度上昇するかはわかりません。

図 12：組織の 40%は CRA のコストを製品価格に反映させる

CRA 準拠のためにかかる費用は、製品またはソリューションの今後の価格設定にどのように影響しますか？（1 つ選択してください）



2026 年 CRA アンケート、Q38、サンプルサイズ = 194

2025 年のデータとの比較については 付録 A11 を参照してください。

CRA を踏まえた中小企業の脆弱性

EU の公開文書（**The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy**：EU 経済におけるオープンソース ソフトウェアとハードウェアによる技術的独立性・競争力・イノベーションに対する影響）によると、中小企業（SME）は EU の ICT セクターにおけるイノベーションと競争力の重要な推進力です。欧州委員会による最近の**事実調査**も、欧州の IT 産業における中小企業の重要性をさらに裏付けています。中小企業はオープンソースコラボレーションへの参入障壁の低さから最も恩恵を受けるセグメントであるため、CRA 準拠のための要件によるリスクも最も高くなっています。2026 年のデータによると、中小企業は（相対的に OSS への依存度が高いため）CRA の義務にさらされる度合いが高く、準拠のためのコストを吸収する能力が低い可能性があります（**図 13**）。

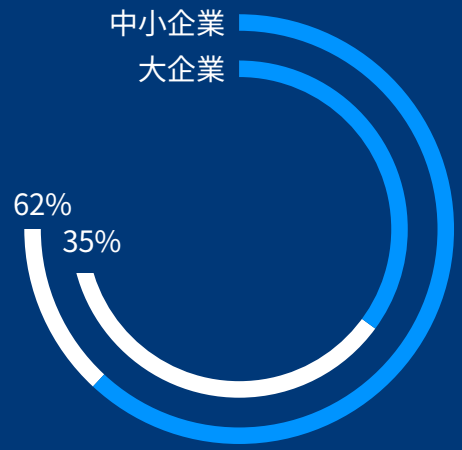
OSS への依存度が高い層に中小企業が集中しているのは、驚くべきことではありません。なぜなら小規模な組織は、独自のコンポーネントをゼロから開発するリソースを持ち合わせていない可能性が高いからです。しかしこの依存度の高さは、限られたセキュリティおよび法務の専門知識、そして多くの場合、専任のコンプライアンス部門を持たないまま、広範な OSS サプライチェーンを管理しなければならないことを意味します。

欧州の中小企業の 51% が CRA について「馴染みがない」と回答しており、これは調査対象となった中小企業の半数が CRA についてよく知らないか、ほとんど知らない状態であることを意味します。このことは、企業自身にとってだけでなく、欧州デジタル経済全体の健全性にとっても重要です。中小企業は EU のテクノロジーエコシステムの基盤であり、欧州大陸全体の企業の大多数を占め、ソフトウェアのイノベーションやサプライチェーン活動のかなりの部分を占めています。

図 14 は、中小企業が大企業よりも CRA 準拠のためのコストを消費者に転嫁する傾向が強いことを示しており、何らかの値上げを計画している企業の割合は全体で 40% なのに対して、中小企業のマニュファクチャラーでは 47% となっています。さらに、調査対象企業の 11% は 15% を超える大幅な値上げを想定しています。

図 13：中小企業の脆弱性

製品の 75% 以上が OSS に依存している組織の割合



CRA に対して馴染みのない中小企業

55%

CRA に対して馴染みのない欧州の中小企業

51%

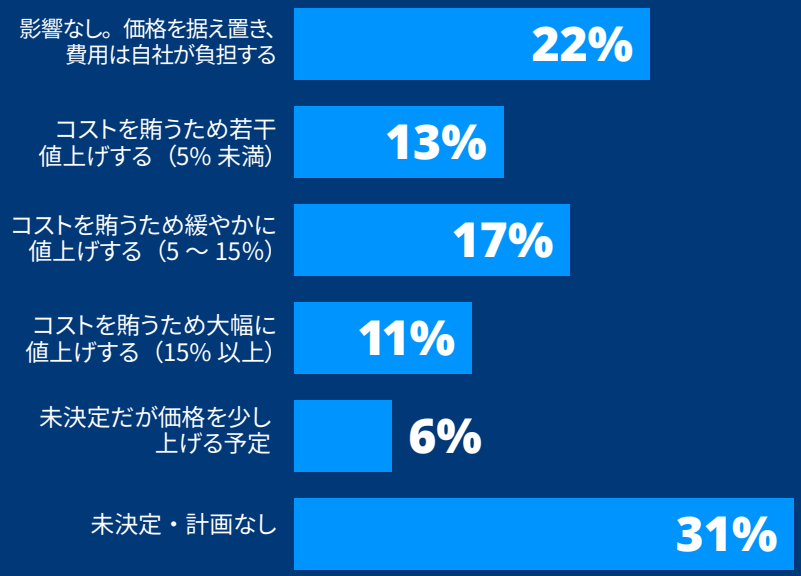
2026 年 CRA アンケート、Q27、Q14 を SME と欧州内の SME でフィルタ、サンプルサイズ = 187、162、96

完全なデータについては 付録 A12、A14 を参照してください。

同時に、中小企業は企業当たりの CRA 準拠コストが相対的に高くなっています。大企業であればセキュリティ監査、SBOM ツール、脆弱性管理インフラストラクチャのコストを、大きな収益基盤に分散できるかもしれません。しかし、IoT 製品を開発している小規模なソフトウェア企業では、それができない可能性があります。中小企業を対象とした支援策がなければ、CRA の準拠は中小企業が EU 市場に参入する際の構造的な障壁となる恐れがあります。

図 14：中小企業の 47%が CRA コストを製品価格に反映させる予定

CRA 準拠のためにかかる費用は、製品またはソリューションの今後の価格設定にどのように影響しますか？（1 つ選択してください）



2026 年 CRA アンケート、Q38、サンプルサイズ = 64 (SME マニュファクチャラーでフィルタ)

アクション：中小企業の声を CRA の議論に取り入れる
CRA の導入を形作るガイダンス、ツール、研究の多くは、法務、セキュリティ、コンプライアンス部門を専門とする大企業の視点から開発されており、中小企業が直面する現実を反映していない可能性がある。中小企業の視点を積極的に調査しそれを反映させることでほとんどのヨーロッパのソフトウェア企業が事業を展開する規模において、CRA への準拠とは実際にどのようなものなのか、より包括的に把握することができるだろう。

専門家からの情報

HARALD FISCHER
Security Aspect Lead, Balena

balena

IoT および組み込みシステム分野では、CRA に対する認識が著しく不足している状況が見られます。ユーザーは製品やソリューションの分類、責任範囲の明確化、そして実装すべき重要なサイバーセキュリティ要件の理解に苦労しています。さらに、IoT デバイスは 7 年から 10 年ものセキュリティサポートを必要とする場合が多く、そのためには単なる意識向上だけでなく、堅牢な運用ツールが不可欠です。規制対象製品におけるオープンソースソフトウェアの安全な利用に関して、業界にはより明確な実装手順が必要であるという本報告書の結論に賛同します。私たちは得られた知見を積極的に共有し、OpenSSF 内で協力しています。この規制にオープンな形で共に取り組むことが、業界全体の準備態勢を最善のものにすると確信しています。

スチュワードとオープンソースプロジェクト

スチュワードの準備状況

CRA は OSS スチュワードを次のように定義しています。

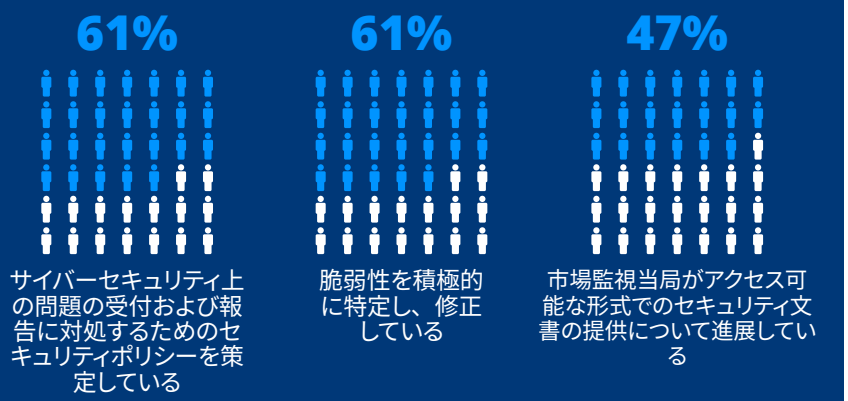
> 「オープンソース ソフトウェア スチュワード」とは、マニュファクチャラー以外の法人であって、無償かつオープンソースソフトウェアに該当し、商業活動で利用されることを意図した特定のデジタル要素を有する製品の開発を、体系的に継続的に支援することを目的とし、かつ、それらの製品の存続可能性を保証する法人をいう（CRA **第 3 条**）。

CRA に基づく OSS スチュワードは、マニュファクチャラーよりも軽い規制を受けています。スチュワードには、サイバーセキュリティポリシーを策定し、悪用されている脆弱性を当局に通知し、コミュニティ内での脆弱性情報の共有を促進するなどの要件が課されています。(CRA **第 24 条**)。

図 15 は、スチュワードが管理するプロジェクトが既に法的義務を果たす軌道に乗っていることを示しています。このデータは、正式な規制が執行される前 に、オープンソースコミュニティが正しい方向に進んでいるという心強い兆候を示しています。これは、Linux Foundation のケーススタディレポート「**Pathways to Cybersecurity Best Practices in Open Source**」によってさらに裏付けられています。このレポートでは、LF ホスト型の 3 つの成熟したプロジェクトが実際にどのように CRA の 義務を満たしているかを検証しています。Yocto Project、Zephyr Project、および Civil Infrastructure Platform: Industrial Grade Linux の経験に基づいて、より広範なオープンソース コミュニティが新しい規制要件への準備を行う際に検討すべき、具体的で実績のある方法を提示しています。

課題は依然として残っているものの、本レポートの中心的なメッセージは、セキュリティツールへの投資、コミュニティ間の連携、そして AI によるリスクなどの新たな脅威への積極的な取り組みが、CRA の義務を果たそうとするスチュワードにとって不可欠となる、ということです。

図 15：スチュワードは法的義務を果たすべく順調に進んでいる



2026 年 CRA アンケート、Q41、Q42、Q47、サンプルサイズ = 28

詳細なデータおよび 2025 年との比較については、付録 A15 ～ A17 を参照してください。

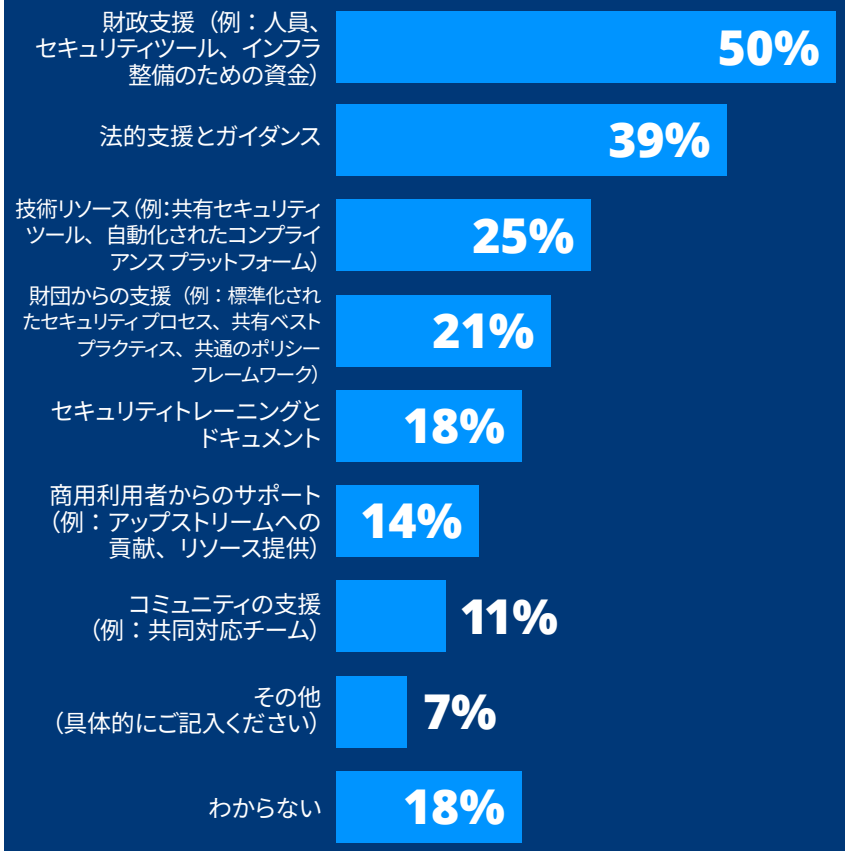
スチュワードのサンプルに関する注記：スチュワードのサンプル数（n=28）は小規模です。 今回の結果および 2025 年との比較は、あくまでも参考値として解釈されるべきであり、確定的なものではありません。

図 16 に示すように、スチュワードが挙げた上位 2 つのニーズは、財政支援と法的ガイダン スであり、これらは文書化だけでは満たすことができません。そのため、構造的な投資が必要となります。具体的には、スチュワード組織への資金提供、コンプライアンスに関するベストプラクティスの策定、そして小規模プロジェクトがゼロから構築することなく利用できる共有セキュリティ基盤の構築などが挙げられます。

財政的支援 (50%）と法的指導 (39%）に加えて、スチュワードの 4 分の 1(25%）は、共有セキュリティツールや自動化されたコンプライアンス プラットフォームといった技術リソースの必要性も挙げています。また、さらに 21% は、標準化されたセキュリティプロセスや共通のポリシーフレームワークの提供を財団に期待しています。これらの調査結果を総合すると、スチュワード コミュニティは、要件を完全に満たすためのリソース、特にスチュワードの義務に関する不確実性を 解消できるような財政的・法的支援を求めていることがうかがえます。

図 16：スチュワードに必要なもの

CRA の要件を満たすために、貴社のプロジェクトが最も必要としている支援は何ですか？（最大 3 つまで選択してください）



2026 年 CRA アンケート、Q53、サンプルサイズ = 28、総回答数 = 57

アクション：スチュワード向けの共有コンプライアンス インフラストラクチャを構築する
OpenSSF OSPS Baseline と OpenSSF Best Practices Badge は、セキュリティ保証の出発点となる。財団は、以下のサービスを提供することで、これを拡張できる。(1) CRA 上の分類区分の判断を対応している管理組織向けの法的レビューサービス、(2) スチュワードが独自のインフラストラクチャを構築することなく利用できる共有 SBOM 生成ツール、(3) CRA 要件に準拠したモデルセキュリティポリシー（SECURITY.md テンプレート、CVE トリアージワークフローなど）。

非営利 OSS の視点

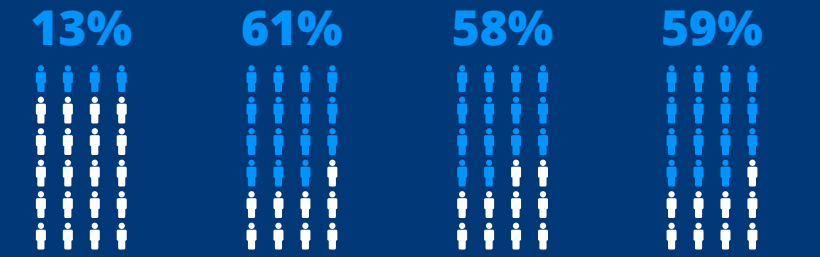
CRA は非営利の OSS 開発を適用範囲から明確に除外しているが、調査対象となった 109 名の非営利開発者の間では、この規制が自分たちに適用されるかどうかについて依然として大きな不確実性が残っています。

CRA が非営利のオープンソース貢献者を明確に適用除外していることは、制度設計の中で最も議論を呼んだ点の 1 つであり、**図 17** のデータは、この点に関する明確化が実際になぜ重要なのかを示しています。昨年の調査結果と同様に、非営利の貢献者のうち 13% は CRA が自身の貢献に適用されると考えており、61% は自分が影響を受けるかどうか確信が持てないと回答しています。また、58% はこれまで通り貢献を続けると答えていますが、かなりの割合が依然として躊躇または未決定です。
特に重要なのは、59% は明確な情報があれば安心して貢献を続けることができると答えています。これはまだ十分に活用されていないものの、容易で影響力の大きい介入策の存在を示しています。このニーズが 2025 年と同様に 2026 年も依然として切実であることは、2027 年 12 月のの適用開始までに明確な説明を提供することへの緊急性を高めるはずです。

アンケートが終了した 2026 年 3 月、欧州委員会は CRA に関する初の **包括的なガイダンス草案** を発表しました。 このガイダンスでは、フリーソフトウェアとオープンソースソフトウェアを対象としています。このガイダンス案は一般からの意見募集にかけられ、**委員会の FAQ**、と合わせて不確実性を軽減することを目的としており、最終化された後は、企業および市場監視当局の双方にとって重要な指針となるでしょう。

データから明らかなのは、非営利の貢献者が必要なのは CRA についての一般的な認識を高めることではなく、CRA が自分たちにどのように適用されるか、あるいは適用されないかについての具体的で実践的な説明であるということです。**図 18** に示すように、最も多く求められているリソースは、CRA が個人にどのように適用されるかの明確な説明（70%）と、CRA が適用される場合と適用されない場合の具体的なシナリオ例（69%）です。さらに、教育リソースと、財団または規制当局のガイダンスはそれぞれ 50% と 48% で続き、貢献者が抽象的な法的分析ではなく、権威がありアクセスしやすい情報を積極的に求めていることが裏付けられています。**OpenSSF CRA Brief Guide for OSS Developers** は、この方向への一歩ですが、データによると、このガイドのシナリオ集を拡張し、より積極的に宣伝する必要があるようです。また、本稿執筆時点では、OpenSSF が発行した、メンテナーと開発者向けのもう 1 つの貴重な資料として、**CRA Readiness Guide for Maintainers and Developers** が提供されています。

図 17：貢献者は CRA が自分たちにどのような影響を与えるのか理解していない

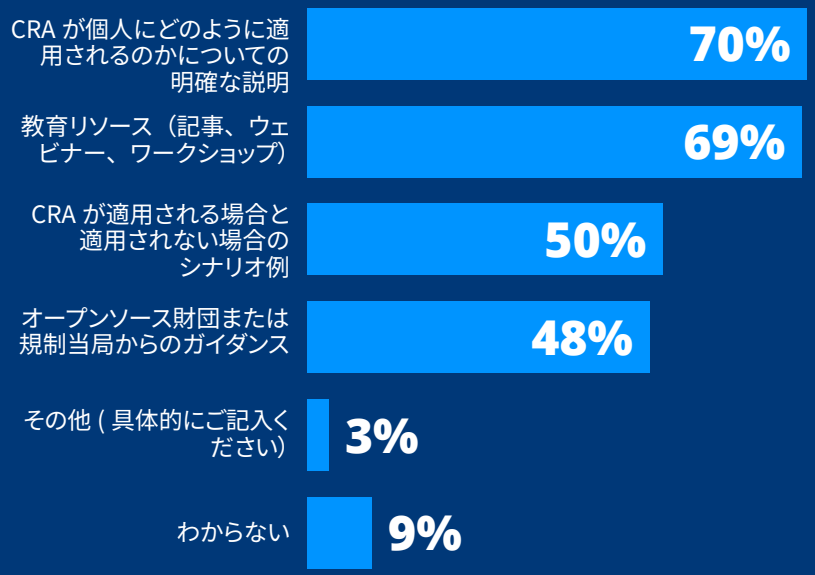


2026 年 CRA アンケート、Q54、Q55、Q56、サンプルサイズ = 1

詳細なデータおよび 2025 年との比較については、付録 A18 ～ A20 を参照してください。

図 18：OSS 貢献者向けリソース

CRA と OSS への貢献活動の影響をより深く理解するために、どのような支援が役立ちますか？（該当するものをすべて選択してください）



2026 年 CRA アンケート、Q57、サンプルサイズ = 109、総回答数 = 271

オープンソースプロジェクトのセキュリティ体制と脆弱性の傾向

本レポートは、アンケートデータに加え、**LFX プラットフォーム** に登録されている 12,863 件の重要なオープンソースソフトウェアプロジェクトのセキュリティ体制に関する知見を提供するため、別の情報源も活用しています。調査では認識、意図、自己申告に よる実践状況を把握するのに対し、LFX データは、CRA によって今後ますます要求されるセキュリティ対策に関して、オープンソースプロジェクトがどのような状況にあるかを現場レベルで把握するための情報を提供します。

セキュリティ体制と準備状況は、プロジェクトの側面によって大きく異なります。**図 19** では、上位オープンソースプロジェクトのサンプルについて、OpenSSF Scorecard[2] のチェック結果の平均スコアを示しています。**図 19** から、プロジェクトは平均的に一部のカテゴリでは優れているものの、他のカテゴリでは改善が必要であることが分かります。これは、上位オープンソースプロジェクトのセキュリティ体制には、大きな改善の余地があることを示唆しています。例えば、プロジェクトは既存の脆弱性の修正 (79%)、ライセンスの明示 (75%)、ソースツリーからバイナリ アーティファクトを排除すること (98%) に関しては概ね良好な成果を上げています。一方、危険なワークフローの回避 (45%)、コードレビュープロトコルの確立 (39%)、セキュリティポリシーの明示的な定義 (31%) に関しては、プロジェクトのセキュリティ体制はやや不十分です。リリースへの署名 (1%)、CI トークンの適切な権限設定 (5%)、依存関係の固定 (6%) といった対策を実施しているプロジェクトはさらに少ないのが現状です。

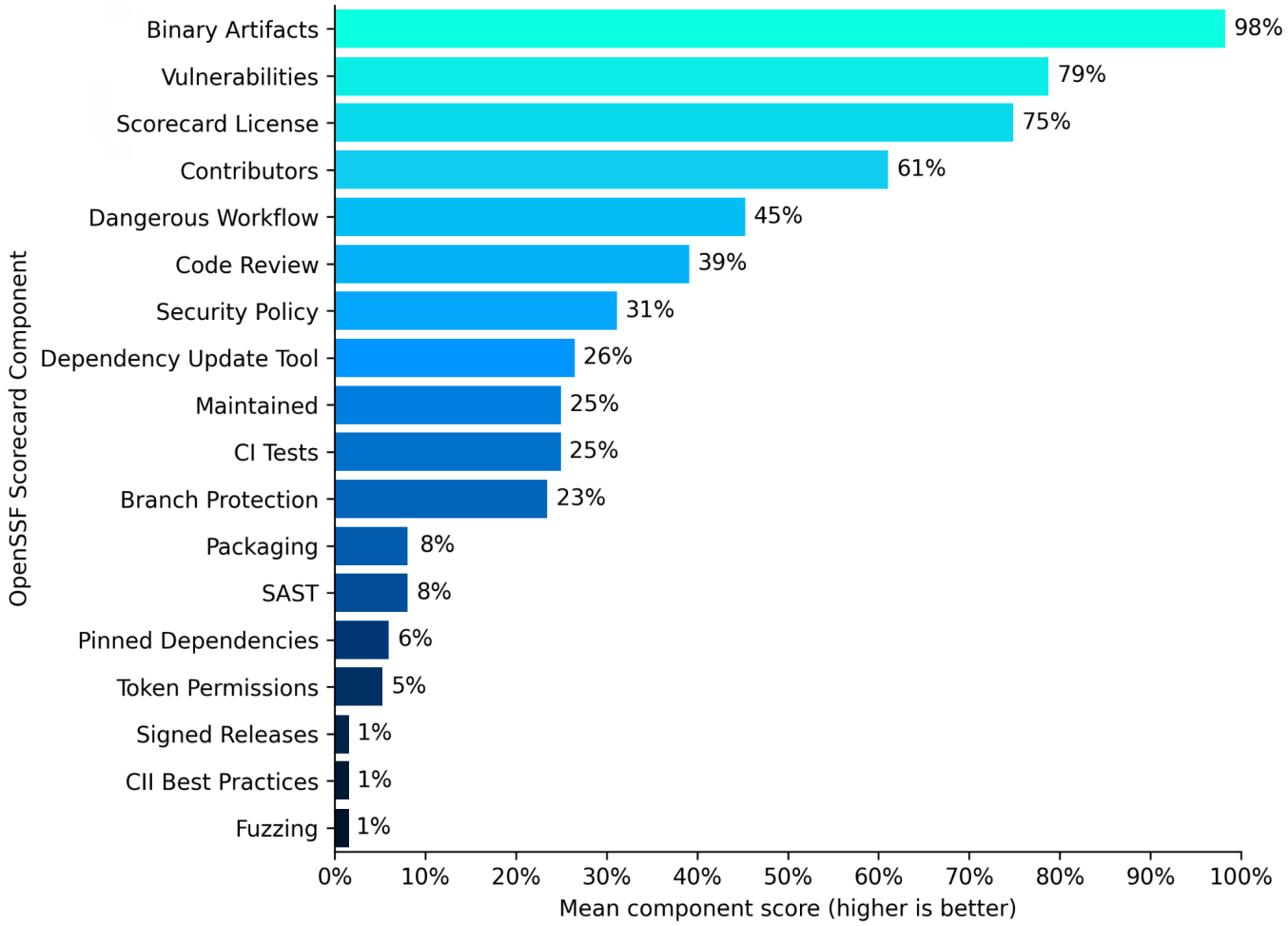
CRA のコンプライアンスという観点から最も重要なのは、リリースへの署名や CI トークンの適切な権限設定など、エコシステム全体での改善が強く求められている実践です。CRA は、こうしたサプライチェーンの完全性を確保するための管理策の導入を促進する機会となります。

図 20 は、セキュリティデータのさらなる分析結果を示しています。組織の多様性は、(1) セキュリティ体制と、(2) プロジェクトの経済的価値の両方と強い相関関係があります。プロジェクトに貢献している異なる組織の数と、CLOMonitor Security Score[3] の間には、スピアマンの相関係数が **0.57** であり、セキュリティと組織の多様性の間に強い正の相関関係があることを示しています。組織の多様性と OpenSSF Best Practices Score の相関係数は **0.40** です。さらに、組織の多様性はプロジェクトの複雑さや交換コストとも関連しており、プロジェクトの組織の多様性と COCOMO 評価の相関係数は **0.52** です。

[2] OpenSSF Scorecard とは、オープンソフトウェアのコンポーネントがセキュリティのベストプラクティスにどの程度準拠しているかを測定するための指標のフレームワーク。

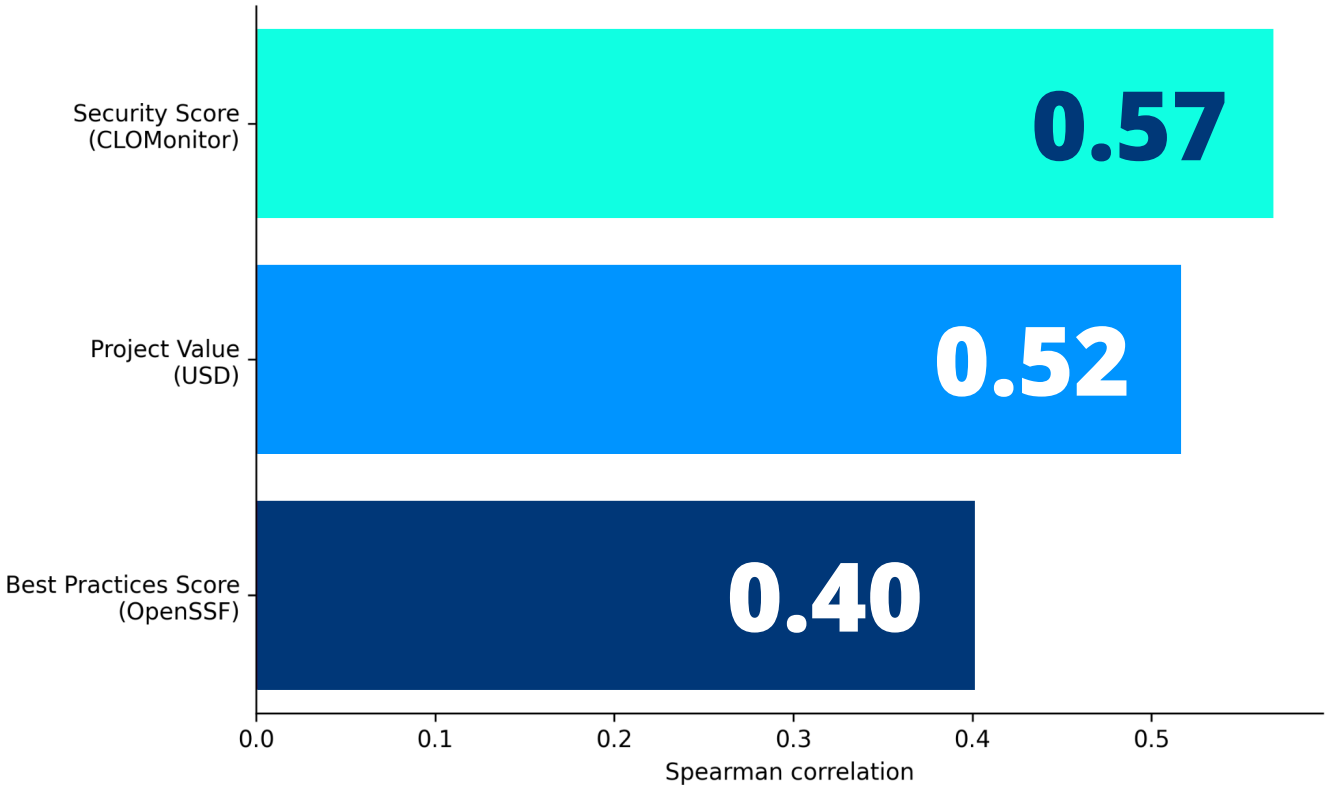
[3] Cloud Native Computing Foundation によって開発された CLOMonitor は、「オープンソースプロジェクトのリポジトリを定期的にチェックし、プロジェクトの健全性に関するベストプラクティスを満たしているかを検証するツール」。

図 19：セキュリティ体制の項目別内訳



LFX は、2024 年 3 月 8 日から 2025 年 6 月 3 日までの間に作成されたレポートに基づいてデータをキュレーションしました。

図 20：貢献組織の数は、セキュリティ体制と経済的価値の両方と関連している



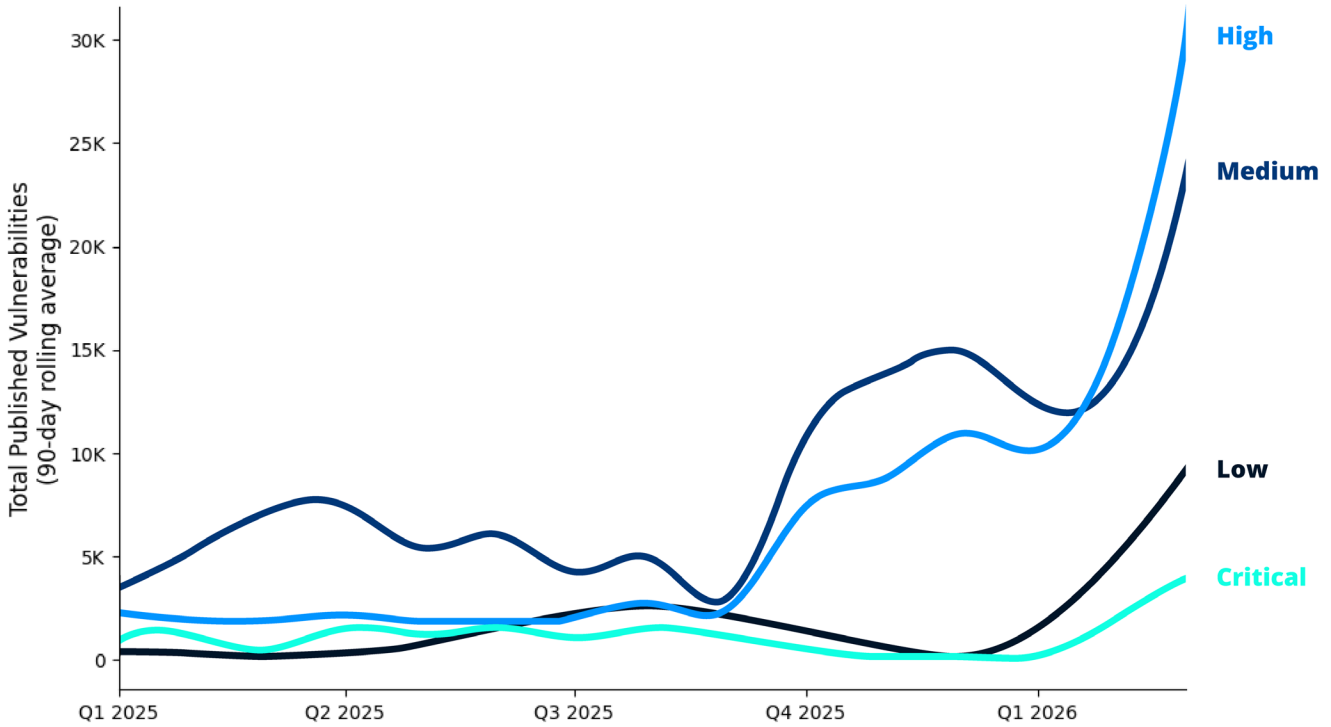
LFX は、2024 年 3 月 8 日から 2025 年 6 月 3 日までの間に作成されたレポートに基づいてデータをキュレーションしました。

アクション：活用しているオープンソースプロジェクトに投資しよう
より多くの組織がプロジェクトに貢献するほど、そのプロジェクトのセキュリティ成果は向上する傾向がある。つまり、サプライチェーン内のオープンソースプロジェクトに投資することは、自社のコンプライアンス体制への直接的な投資となる。その一方、資金不足でメンテナンスも不十分なプロジェクトに頼りながら、利用している組織の支援なしに CRA が求めるセキュリティ基準を満たすことを期待するという選択肢は、2027 年 12 月の期限が近づくにつれ、無視できないリスクとなるだろう。

図 21 は、エコシステム全体におけるセキュリティ脆弱性の発生状況を示しています。LFX に登録されている 14,204 のオープンソース ソフトウェア プロジェクトを対象に、新たに公開された脆弱性の 90 日移動平均をプロットしたものです。過去 1 年間で CVE の件数が爆発的に増加 しており、2025 年初頭からほぼ指数関数的に増加しています。2026 年 第 1 四半期には、公開された CVE が前年比で 394% という驚異的な増加をし、すべてのリポジトリを通じて 101,489 件の脆弱性が追加されました。最も憂慮すべきは、深刻度が高い 脅威 (+811%) および重大な 脅威 (+136%) の増加です。

このことは **NIST の更新情報** でも確認されています。 2026 年の最初の 3 か月間の提出件数は、前年同期比で 3 分の 1 近く増加しています。しかし、この急増については慎重に解釈する必要があります。その大部分は、AI ベースの自動脆弱性スキャンツールの急速な普及や、プロジェクトのインデックス化範囲の拡大を反映している可能性が高く、つまり、脆弱性が新たに増えたのではなく、より多くの脆弱性が発見され、報告されるようになったということを意味しています。
また、CRA による規制圧力によって、依存関係ツリーの内部監査が加速された可能性も高く、これまで記録されていなかった潜在的な問題が表面化したと考えられます。

図 21：発見された脆弱性の指数関数的増加



LFX curated data

さらに、自動検出された脆弱性のうち、実際に高いリスクをもたらすものと、誤検出を区別するためには今後さらなる分析が必要です。

真のリスクと誤検知の区別は、報告された脆弱性への対応をマニュファクチャラーに義務付けている CRA の文脈において、特に重要です。自動検出された脆弱性の大部分が誤検知であることが判明した場合、マニュファクチャラーは重大な脅威をもたらさない問題への修復義務に追われるリスクがあります。また、真に注意を払うべき脆弱性からリソースが逸れてし まう可能性もあります。

CRA にとって、このセクションの調査結果は重要な意味を持ちます。規制では、マニュファクチャラーに対しソフトウェア サプライチェーンに関するデューデリジェンスを実施する義務を課しています。しかし、マニュファクチャラーが依存するオープンソース コンポーネントのセキュリティ品質は、それらのプロジェクトがどれだけ手厚いサポートを受けているかに左右されます。単一の組織や、限られた貢献者によって支えられているプロジェクト（しばしば、たった一人のメンテナーによって維持されているプロジェクト）は、セキュリティ体制が脆弱になる可能性が高いです。

また、発見される脆弱性の数も増加しています。AI ベースの自動スキャンがこの増加の大部分を占めていると考えられますが、マニュファクチャラーがリスクに大きく晒されているのが現状です。CRA コンプライアンスが依存するコンポーネントのセキュリティ基準を引き上げるには、アップストリームへの投資と積極的な関与が最終的な現実的な手段となるでしょう。組織は、多大なコストをかけて独自のコンポーネントやコンポーネント フォークを作成・維持することもできますし、他の組織と協力して依存している OSS をより良く支援することもできます。後者の方法は、長期的に見ると組織にとってコストが低く、OSS にとっても有益であり、社会にとってもより良い選択肢となります。

専門家から

EDDIE KNIGHT
Founder, Revanite

REVANITE

公式の CRA ガイダンスと同様に、オープンソース ソリューションも常に進化しており、誰もがそのエコシステムの発展を加速させるために貢献できます。Revanite は小規模なチームながら、OpenSSF に数々の大きな貢献をしてきました。OSPS Baseline を立ち上げ、その適合状況を評価する自動スキャナーを開発し、機械可読なコンプライアンス ワークフローをエンドツーエンドで効率化する Gemara プロジェクトを立ち上げました。そして今、業界を代表する企業とともに、「CRA Baseline for Manufacturers」の策定に取り組んでいます。他の中小企業の皆様も、ぜひ私たちと共に未来を形作っていきたいと考えています。

結論

2026 年 CRA の認知と準備状況に関する報告書は、真の課題であると同時に、真の可能性の存在を記録したものです。規制は既に施行されており、期限も明示されています。そしてオープンソースコミュニティは、求められていることを実現するためのツール、人材、そして協力し合う文化が備わっています。あとは、マニュファクチャラーが行動を起こし、まだ時間があるうちに、より持続可能な道を選択するだけです。

認識のギャップは確かに存在していますが、それは恒久的な問題である必要はありません。**LFEL1001 トレーニングコース** などの既存の教材や取り組み、OpenSSF OSPS ベースラインや、Linux Foudation がホストする技術プロジェクトは、既に利用者から高い評価を得ています。課題は、その品質ではなく、これらの取り組みそのものの認知度にあります。カンファレンス、ドキュメント、ソーシャルメディア、ポッドキャストなど、開発者が実際に学習する場に情報発信の焦点を移すことが、2027 年 12 月の期限までにギャップを埋めるための明確な道筋となるでしょう。

CRA 遵守の経済性は、一見すると負担が大きく感じられますが、すべての人にとってより良いモデルを示しています。プライベートフォークの維持管理にかかる莫大なコストが明らかになれば、アップストリームへの貢献の必要性は、いかなる政策論議よりも説得力をもって示されます。組織が依存しているオープンソースプロジェクトに投資することで、コンプライアンス上の負担を軽減するだけでなく、ソフトウェアエコシステム全体が稼働する共有インフラストラクチャを強化することにもつながります。この意味において CRA は、アップストリームへの貢献がデフォルトかつ経済的に合理的な選択肢となるエコシステムを促進するインセンティブとなる可能性があります。

12,000 を超えるオープンソースプロジェクトのセキュリティ分析と脆弱性の傾向も、同様の傾向を示しています。エコシステム全体で検出された CVE は、2026 年第 1 四半期に前年同期比で 394% 増加しました。この急増は、AI ベースの自動検出の精度向上による部分もありますが、それでもなお、相当な脆弱性対応の負担を抱えていることを示しています。 こうした背景から、組織の多様性はセキュリティ体制を予測する上で重要な要素として浮上しています。つまり、オープンソースプロジェクトへの参加を拡大すること自体がコンプライアンス戦略となるのです。アップストリームに関与したり、メンテナーに資金を提供したり、セキュリティ修正を提供したりする組織はすべて、CRA が保護対象とするサプライチェーンの信頼性を直接的に向上させていることになります。

中小企業、スチュワード、非営利開発者にとって、今後の道のりは見た目ほど険しくはありません。的を絞ったサポートメカニズム、共有コンプライアンス基盤、明確なシナリオベースのガイダンスにより、単独で対応するには負担が大きい人々の負担を大幅に軽減することできます。OpenSSF の **EU サイバーレジリエンス法 (CRA) のページ**には、**Linux Foundation CRA Stewards Playbook**、**Linux Foundation のリーダーシップ CRA スチュワードワンページ**、**メンテナーと開発者向けの CRA 準備ガイド**、および**オープンソース ソフトウェア (OSS) 開発者向けのサイバー レジリエンス法 (CRA) 簡易ガイド**など、多くの OpenSSF 関連リソースへのリンクがあります。また欧州委員会が 2026 年 3 月に公表したフリーおよびオープンソースソフトウェアに関する**ガイダンス案**、および 2025 年 12 月に公開された **FAQ 文書**は、この方向性を後押しする有望な取り組みです。これらの最終版が公開されれば、現在不確実な状況にあるコミュニティの大きなセグメントが待ち望んでいた明確な指針が示されることになるでしょう。

2027 年という期限は強制的なものですが、その先には構築する価値のある未来があります。それは、現在存在するものよりも安全で、より持続可能なソフトウェアサプライチェーンです。

リソース

欧州委員会のリソース

- CRA の規制条文全文
- フリーソフトウェアおよびオープンソースソフトウェアに関するガイダンス案
- サイバーレジリエンス法の実施に関する FAQ ドキュメント

OpenSSF と Linux Foundation のリソース

- EU サイバーレジリエンス法（CRA）ページ
- Linux Foundation CRA Stewards Playbook
- Linux Foundation リーダーシップ CRA スチュワード ワンページ資料
- メンテナーおよび開発者向け CRA 準備ガイド
- サイバーレジリエンス法（CRA）オープンソースソフトウェア（OSS）開発者向け概要ガイド

グローバルサイバーポリシーワーキンググループのリソース：

- Global Cyber Policy WG GitHub
- #wg-globalcyberpolicy on Slack
- Global Cyber Policy WG Mailing List
- CRA Readiness+Awareness SIG Mailing List
- CRA Tooling+Process+Formats SIG Mailing List
- CRA Spec Standardization SIG Mailing List

脆弱性報告とガイダンス：

- LF プロジェクトおよび Foundation に特有の脆弱性報告に関するガイドライン
- Linux Foundation のプロジェクト一覧
- Linux カーネルのセキュリティ脆弱性は、Linux カーネルのセキュリティバグに関するページに記載の通り、security@kernel.org 宛てに報告
- Linux Foundation のインフラストラクチャまたはメインの LF Web サイトに特有の脆弱性を報告するには、
- security@linuxfoundation.org にメールを送信
- ソーシャルエンジニアリングによる乗っ取りに関する警告

セキュリティに関するベストプラクティスとツール：

- Alpha Omega OSS プロジェクトのメンテナーと提携して、新しい、まだ修正されていないオープンソースコードにおける未発見の脆弱性を体系的に発見し修正
- CNCF fuzzing handbook ファジングとは何か、そしてその適用方法についての説明
- OpenSSF Technical Initiatives ベストプラクティスバッジ、スコアカード、Sigstore などを含む
- システムパッケージデータ交換 (SPDX) オープン SBOM 規格（ISO/IEC 5692:2021）
- 耐量子暗号アライアンス 耐量子暗号の採用と発展のための

教育リソース：

注目の資格

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

講師主導型トレーニングコース

- 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)

実践型学習ワークショップ

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

注目の無料トレーニング

- Developing Secure Software (LFD121)
- セキュア ソフトウェア開発 (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)

無料速習コース（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)

研究

- 認識不足と不確実性：オープンソースレポートにおけるサイバーレジリエンス法への準備状況の厳しい現実 - この調査に基づく報告書は、オープンソースコミュニティが EU のサイバーレジリエンス法を遵守するための認識と準備状況を調査したものです。
- オープンソースソフトウェアへの貢献に対する投資対効果（ROI） - この研究では、LF Research は
- オープンソースへの貢献がもたらすメリットについて、アンケート調査の結果分析と貢献 ROI に関する定量的モデルを用いて考察します。
- 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 - Linux Foundation によるこのケーススタディレポートは、サイバーレジリエンス法がオープンソースソフトウェアに与える影響、特に新たなサイバーセキュリティ義務や、マニュファクチャラーおよびスチュワードの役割について調査しています。
- 2025 年 グローバルオープンソースの現状 - 継続的な「オープンソースの世界」研究シリーズの一環として、2025 年版では、オープンソースがコアテクノロジースタック全体でどのように採用されているか、また組織がセキュリティ評価の実践、正式なガバナンス構造、および本番環境におけるオープンソースのサポートをどのように活用しているかを調査します。
- 2025 年における OSPO とオープンソース管理の現状 - 2025 年版では、8 年目を迎え、OSPO（オープンソースセキュリティ組織）がコンプライアンス重視の組織から戦略的なガバナンスハブへと急速に成熟し、リスク管理、AI の監視、オープンソースのサプライチェーンセキュリティにおいて役割を拡大している様子を探ります。

メソドロジー

本調査は、Linux Foundation Research と OpenSSF が 2026 年 1 月に実施したウェブアンケートに基づいています。この調査は、政府のサイバーセキュリティ規制が OSS エコシステムに及ぼす潜在的な影響を検証することを目的としています。同様の調査は 2025 年 1 月にも実施されており、両調査の結果は前年同期比の分析を行えるよう比較可能なものとなっています。本章では、調査方法とデータ分析方法に関する背景、そして回答者の属性について説明します。

私たちは、回答者が自身または所属組織を代表して質問に正確に回答できるだけの十分な専門的経験を有していることを確認するため、徹底的な事前選別、調査質問のスクリーニング、およびデータ品質チェックを通じてデータ品質の確保に努めました。

業種別企業、IT ベンダーおよびサービスプロバイダー、非営利団体、学術機関、政府機関からアンケートデータを収集しました。回答者は、様々な業種・分野にわたり、企業規模も多岐にわたっていました。また、複数の地域・国からデータを収集しました。

このアンケートは 58 の質問で構成され、スクリーニング、回答者の属性、CRA に関する認知度、CRA における自身の役割認識などを調査しました。また、マニュファクチャラー、OSS スチュワード、非営利 OSS 開発者向けの専用セクションも設けられていました。アンケートへのアクセス方法、データセット、調査頻度については、下記のアンケートデータアクセス情報をご覧ください。

以下の基準を満たす回答者を調査対象としました。

- **OSS の概念に精通している必要がある**
- **OSS への関与を明確に示せる**
- **自身の雇用状況を明示できる**

この調査は 2025 年 1 月に実施されました。合計 685 名の回答者が、調査の認知度に関するセクションに回答しました。マニュファクチャラーのサンプル数は 194 ～ 219 件、スチュワードのサンプル数は 28 件、非営利の OSS 開発者のサンプル数は 109 件です。認知度調査のサンプル数における誤差範囲は、信頼水準 90% で± 2.8%、信頼水準 95% で± 3.4% です。

アンケートへのアクセス方法、データセット、調査頻度については、下記のアンケートデータアクセス情報をご覧ください。

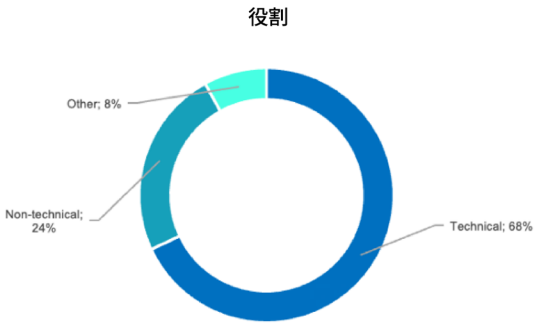
アンケート対象者の属性

図 22 は、調査対象者の最も重要な属性をまとめたものです。回答者のほとんどは技術職に従事しています。業界別では、情報技術（48%）が最も多く、次いで金融サービス（8%）、その他様々な業種となっています。組織規模は均等に分布しており、小規模組織（従業員 1 ～ 249 人）が 45%、中規模組織（従業員 250 ～ 4,999 人）が 26%、大規模組織（従業員 5,000 人以上）が 29% を占めています。地理的な分布も広く、回答者の 46% がヨーロッパ、26% が米国 / カナダ、12% がアジア太平洋地域に拠点を置いています。

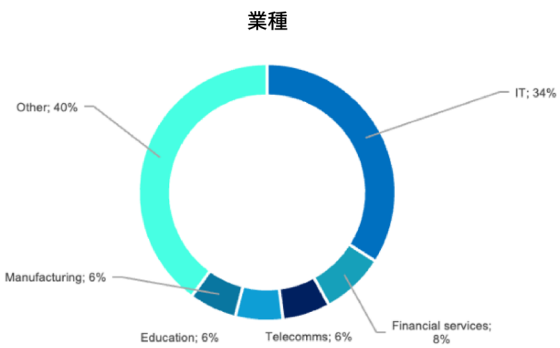
アンケートデータへのアクセス

Linux Foundation Research は、各実証プロジェクトのデータセットを Data.World で公開しています。このデータセットには、調査票、生データ、スクリーニングおよびフィルタリング基準、そしてアンケートの各質問に対する頻度グラフが含まれています。本プロジェクトを含む Linux Foundation の研究データセットは、data.world/thelinuxfoundation で入手できます。Linux Foundation のデータセットへのアクセスは無料ですが、Data.World アカウントを作成する必要があります（注：研究データは、Data.World から zenodo.org に移行しました。本レポートのデータは、**https://zenodo.org/records/21037919** にあります）。

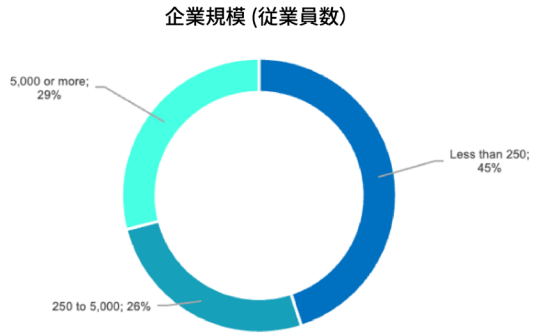
図 22：2026 年 CRA アンケート対象者の属性データ



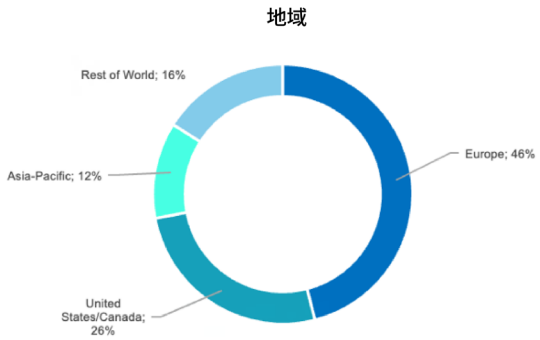
2026 年 CRA アンケート、Q5、サンプルサイズ = 843



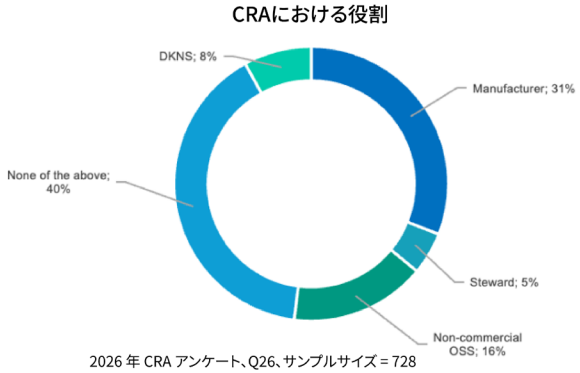
2026 年 CRA アンケート、Q9、サンプルサイズ = 638



2026 年 CRA アンケート、Q10、サンプルサイズ = 625



2026 年 CRA アンケート、Q4、サンプルサイズ = 843



2026 年 CRA アンケート、Q26、サンプルサイズ = 728

2026 年 CRA アンケート、Q26、サンプルサイズ = 728

著者について

ADRIENN LAWSON は、Linux Foundation の定量調査ディレクターとして、オープンソースのエコシステムを理解するためのデータ駆動型イニシアチブを主導しています。オックスフォード大学で社会データサイエンスの専門知識を習得し、学術研究機関と政府研究機関の両方での研究経験を持つ彼女は、分散型コラボレーションネットワークの分析において高い方法論的厳密性を発揮しています。Linux Foundation では、業界や地域を横断する横断的調査を実施するチームを率いて、オープンソースの動向に関する包括的な洞察を提供しています。彼女の研究は、規制遵守、AI の影響、持続可能な資金調達モデルに関する実証的調査を含みます。彼女は、オープンソースコミュニティにおける戦略的意思決定に役立つ、エビデンスに基づいた提言を行っています。

謝辞

アンケートにご協力いただいた皆様には、貴重なご意見やご経験を共有していただき、心より感謝申し上げます。

また、研究プロセスのさまざまな段階においてご協力いただいた査読者および Linux Foundation の同僚の皆様にも特別な感謝を表します。具体的には、Mirko Boehm、Hilary Carter、Mike Dolan、Anna Hermansen、Angelah Liu、Madalin Neag、Christopher（CRob）Robinson、Kate Stewart、David A. Wheeler、Steve Winslow の皆様です。

LFX のセキュリティおよび CVE データの分析、そして本レポートにおけるセキュリティ調査結果への貢献に対し、Sam Boysel に心より感謝申し上げます。

LF Research は、二次資料の集約、データ分析、レポート作成支援、校正、翻訳など、研究関連の業務において、生成型 AI ツールを様々な形で活用しています。AI によって生成されたコンテンツは、すべて人による確認を行い、必要に応じて修正しています。

最後に、本調査を支援してくださったスポンサーの皆様に感謝申し上げます。

付録

A1：CRAに関する全体的な理解度

サイバーレジリエンス法（CRA）について、どの程度ご存知ですか？（1つ選択してください）

	2026	2025
全く知らない	42%	36%
少し知っている	24%	26%
ある程度知っている	16%	17%
知っている	9%	12%
よく知っている	6%	5%
非常によく知っている	**3%**	**4%**

2026年 CRA アンケート、Q114、サンプルサイズ＝843; 2025年 CRA アンケート、Q18、サンプルサイズ＝685

A2：地域別CRA認知度

サイバーレジリエンス法（CRA）についてどの程度ご存知ですか？（1つ選択してください） 主にどの国または地域にお住まいですか？（1つ選択してください）

	合計	ヨーロッパ	アメリカ／カナダ	アジア太平洋
全く知らない	40%	36%	52%	31%
少し知っている	25%	26%	20%	30%
ある程度知っている	16%	16%	14%	21%
知っている	9%	10%	7%	11%
よく知っている	7%	8%	4%	5%
非常によく知っている	**3%**	**4%**	**3%**	**2%**

2026年 CRA アンケート、Q14 by Q4、サンプルサイズ＝718

A3：組織的なCRAコンプライアンス

あなたまたはあなたの組織がCRAの規制を遵守する必要があるかどうかご存知ですか？（1つ選択してください）

	2026	2025
はい	59%	58%
いいえ	41%	42%

2026年 CRA アンケート、Q20、サンプルサイズ = 404; 2025年 CRA アンケート、Q24、サンプルサイズ = 384

A4：CRA導入タイムラインに関する知識

組織はいつからCRA規制を完全に遵守しなければならなくなりますか？（1つ選択してください）

	2026	2025
2025	5%	11%
2026	12%	6%
2027	34%	28%
2028	3%	4%
わからない、または確信が持てない	46%	51%

2026年 CRA アンケート、Q18、サンプルサイズ = 404; 2025年 CRA アンケート、Q22、サンプルサイズ = 384

A5：CRAの法令遵守違反に対する潜在的な罰則についての理解度

CRAの規制に違反した場合の罰則についてご存知ですか？（1つ選択してください）

	2026	2025
はい	44%	41%
いいえ	56%	59%

2026年 CRA アンケート、Q21、サンプルサイズ = 404; 2025年 CRA アンケート、Q25、サンプルサイズ = 384

A6：マニュファクチャラーとOSSスチュワード間の違いに関する知識のギャップ

CRAにおけるマニュファクチャラーとオープンソースソフトウェアスチュワードの区別についてご存知ですか？（1つ選択してください）

	2026	2025
はい	46%	43%
いいえ	54%	57%

2026年 CRA アンケート、Q19、サンプルサイズ = 404; 2025年 CRA アンケート、Q23、サンプルサイズ = 384

A7：SBOMSを用いた製造業者の依存度追跡

貴社は、製品やソリューションで使用されるソフトウェアについてソフトウェア部品表（SBOM）の作成を行っている、あるいは予定していますか？（1つ選択してください）

	2026	2025
はい、すべての製品についてSBOMを作成している	32%	34%
一部の製品にはSBOMを作成しているが、すべての製品ではない	29%	25%
どの製品についても作成していないが、作成する計画がある	8%	6%
私の組織はSBOMの存在は認識しているが、現時点では作成しておらず、まだ作成する計画もない	8%	9%
私の組織はSBOMについて全く認識していない	5%	4%
わからない、または確信が持てない	18%	21%

2026年 CRA アンケート、Q28、サンプルサイズ = 219; 2025年 CRA アンケート、Q28、サンプルサイズ = 205

A8：マニュファクチャラーにおけるOSS脆弱性対応戦略

製品に含まれるオープンソースソフトウェア（OSS）コンポーネントに脆弱性が見つかった場合、通常どのように対処しますか？（1つ選択してください）

	2026	2025
OSSプロジェクトが修正プログラムをリリースするのを待ちます	51%	46%
内部的にコンポーネントにパッチを適用します	23%	20%
コンポーネントをより安全な代替品に交換します	9%	11%
サポート対象/エンタープライズ版のコンポーネントを使用しています	5%	9%
お客様に問題を通知しますが、直接対処はいたしません	0%	0%
対処しません	1%	1%
わからない、または確信が持てない	**11%**	**12%**

2026年 CRA アンケート、Q30、サンプルサイズ = 219; 2025年 CRA アンケート、Q30、サンプルサイズ = 205

A9：マニュファクチャラーにおけるOSSセキュリティ可視化の実践

使用しているオープンソースソフトウェア（OSS）コンポーネントのセキュリティ状況を把握できていますか？（1つ選択してください）

	2026	2025
はい、OSSプロジェクトのセキュリティ対策を定期的に評価しています	34%	38%
ある程度は把握しています、公開されたアップデートやコミュニティからの報告に頼っています	47%	44%
いいえ、利用しているオープンソースプロジェクトのセキュリティ対策を監視していません	11%	9%
わからない、または確信が持てない	**9%**	**9%**

2026年 CRA アンケート、Q29、サンプルサイズ = 19; 2025年 CRA アンケート、Q29、サンプルサイズ = 205

A10：CRAに基づくアップストリームサイバーセキュリティ貢献計画

CRAの発効後、上流工程でサイバーセキュリティ対策をアップストリームに提供する計画をお持ちですか？（1つ選択してください）

	2026	2025
はい	22%	22%
いいえ	20%	19%
既に、依存しているプロジェクトにセキュリティ修正（パッチ）をアップストリームに提供しています	19%	16%
わからない、または確信が持てない	**39%**	**44%**

2026年 CRA アンケート、Q34、サンプルサイズ = 194; 2025年 CRA アンケート、Q34、サンプルサイズ = 180

A11：CRAの価格への影響

今後、CRAのコンプライアンス導入にかかる費用は、貴社の製品またはソリューションの価格設定にどのように影響しますか？（1つ選択してください）

	2026	2025
影響はありません。価格は据え置きとなり、費用は弊社が負担します	21%	14%
コストを賄うための価格の若干の値上げ（5%未満）	14%	13%
コストを賄うための価格の緩やかな値上げ（5〜15%）	12%	12%
コストを賄うための大幅な値上げ（15%以上）	5%	8%
まだ決定していませんが、価格を少し上げる予定です	9%	6%
まだ決定しておらず、計画もありません	39%	47%

2026年 CRA アンケート、Q38、サンプルサイズ = 194; 2025年 CRA アンケート、Q38、サンプルサイズ = 180

A12：組織規模別のOSS依存度

貴社製品のうち、オープンソースソフトウェアに依存している割合はどのくらいですか？（1つ選択してください）

	中小企業	大企業
25%未満	5%	12%
25%～50%	14%	22%
51%～75%	14%	16%
75%以上	62%	35%
わからない、または確信が持てない	5%	14%

2026年 CRA アンケート、Q27、サンプルサイズ = 187

A13：中小企業の認知度レベル

サイバーレジリエンス法（CRA）についてどの程度ご存知ですか？（1つ選択してください）中小企業向けに絞り込み

全く知らない	30%
少し知っている	25%
ある程度知っている	18%
知っている	12%
よく知っている	11%
非常によく知っている	**5%**

2026年 CRA アンケート、Q14、サンプルサイズ = 162

A14：欧州の中小企業に関する認知度レベル

サイバーレジリエンス法（CRA）についてどの程度ご存知ですか？（1つ選択してください）中小企業向け（ヨーロッパ）

全く知らない	25%
少し知っている	26%
ある程度知っている	17%
知っている	13%
よく知っている	14%
非常によく知っている	**6%**

2026年 CRA アンケート、Q14、サンプルサイズ = 96

A15：サイバーセキュリティポリシーの提供に関するスチュワードの準備状況、第（24条(1)）

貴社のOSSプロジェクトには、サイバーセキュリティ問題の受付と報告に効果的に対応するためのセキュリティポリシーがありますか？（1つ選択してください）

	2026	**2025**
はい	61%	74%
いいえ	25%	18%
わからない、または確信が持てない	**14%**	**9%**

2026年 CRA アンケート、Q41、サンプルサイズ = 28; 2025年 CRA アンケート、Q40、サンプルサイズ = 34

A16：脆弱性修正に関するスチュワードの準備状況

OSSプロジェクトにおける脆弱性を特定し、対処するためのプロセスを確立していますか？（1つ選択してください）

	2026	**2025**
はい、積極的に脆弱性を特定し、修正します	61%	68%
はい、しかし脆弱性への対応はユーザーからの報告があった場合のみ行います	21%	21%
いいえ、問題解決は外部の貢献者やユーザーに頼っています	11%	6%
わからない、または確信が持てない	**7%**	**6%**

2026年 CRA アンケート、Q42、サンプルサイズ = 28; 2025年 CRA アンケート、Q41、サンプルサイズ = 34

A17：スチュワードによる書類提供の準備状況、第24条(2)

貴社のOSSプロジェクトは、市場監視当局が容易に理解できる形式で、セキュリティ対策に関する文書を提供できますか？（1つ選択してください）

	2026	2025
はい、文書は準備済	7%	9%
一部文書は準備済	29%	24%
準備中	11%	12%
文書は準備されていません	29%	26%
わからない、または確信が持てない	25%	29%

2026年 CRA アンケート、Q47、サンプルサイズ = 28, 2025年 CRA アンケート、Q46、サンプルサイズ = 34

A18：CRAがOSS開発者に与える影響

あなたのオープンソースへの貢献にCRAが適用されると思いますか？（1つ選択してください）

	2026	2025
いいえ、当てはまらないと思う	27%	24%
可能性はあるが、確信はない	61%	59%
はい、貢献者として影響を受ける可能性があると思う	13%	17%

2026年 CRA アンケート、Q54、サンプルサイズ = 109; 2025年 CRA アンケート、Q53、サンプルサイズ = 126

A19：CRAがOSS貢献に与える影響

CRAの潜在的な影響を考慮して、OSSへの貢献を再検討しますか？（1つ選択してください）

	2026	2025
いいえ、これまで通り貢献を続ける	58%	58%
多少は心配ですが、今のところは貢献を続ける	22%	25%
Yはい、貢献を減らすか、あるいは停止することを考えている	6%	5%
わからない、または確信が持てない	15%	16%

2026年 CRA アンケート、Q55、サンプルサイズ = 109; 2025年 CRA アンケート、Q54、サンプルサイズ = 126

A20：明確な情報の必要性		
CRAに関する説明が明確になれば、OSSへの貢献を続ける自信が持てるようになりますか？（1つ選択してください）		
	2026	**2025**
はい、明確な情報があれば安心できます	59%	75%
いいえ、まだ不安を感じます	6%	6%
よくわかりません。提供されるガイダンスによります	**36%**	**20%**
2026年 CRA アンケート、 Q56、サンプルサイズ = 109; 2025年 CRA アンケート、Q55、サンプルサイズ = 126		

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Open Source Security Foundation（OpenSSF）は、Linux Foundation 傘下の業界横断型組織であり、業界で最も重要なオープンソースセキュリティ関連の取り組みと、それらを支援する個人や企業を結集しています。OpenSSF は、あらゆる人々のためのオープンソースセキュリティの推進を目指し、上流コミュニティおよび既存コミュニティとの連携に尽力しています。詳細については、**openssf.org** をご覧ください。

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation Research** は 、オープンソースにおけるコラボレーションの規模拡大を探り、新たな技術動向、ベストプラクティス、そしてオープンソースプロジェクトが世界に与える影響についての知見を提供しています。Linux Foundation Research は、プロジェクトのデータベースとネットワークを活用し、定量的および定性的な手法におけるベストプラクティスに取り組むことで、世界中の組織にとって有益なオープンソースに関する知見を得るための中核的な情報基盤（ライブラリ）の構築を進めています。

この資料は、OpenSSF 発行の「2026 CRA Awareness and Readiness」を OpenSSF Japan Chapter の有志メンバーで日本語に翻訳したものです。
日本語版翻訳協力：OpenSSF Japan Chapter 翻訳チーム
- 余保 束（ルネサスエレクトロニクス）
- 清海 佑太（本田技術研究所）
- 川名 のん（日立製作所）
- 池田 宗広（サイバートラスト）

本著作物を引用する場合は、以下の形式で引用してください。
Adrienn Lawson, “2026 CRA Awareness and Readiness Report,” foreword by Roman Zhukov, The Linux Foundation, June 2026.

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/TheLinuxFoundation