THE LINUX FOUNDATION | Research

OpenSSF OPEN SOURCE SECURITY FOUNDATION

THE LINUX FOUNDATION | Europe

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

Adrienn Lawson, The Linux Foundation
Stephen Hendrick, The Linux Foundation

序文、Christopher (CRob) Robinson, Open Source Security Foundation (OpenSSF)

2025年3月

CRAの全体的な認識度は低く、62%がCRAについて「まったく認識してない」または「ほんの少し認識している」と回答しています。

51%がCRAの期限について不確かであり、全面遵守の目標年が2027年であることを正しく認識していたのは、わずか28%でした。

システム インテグレーター、コンサルタント、および学術関係者は、CRAによって割り当てられた役割や責任に完全には適合しません。

製造業社のほぼ半数（46%）は、セキュリティ修正のために**上流のOSSプロジェクトに受動的に依存**しています。

OSSプロジェクトに積極的に関与している組織は、受動的なOSSユーザーと比較して、**オープンソース プロジェクトのセキュリティ実践を約2倍高く評価**しています。

スチュワードの74%は、セキュリティ ポリシーを定めて、サイバーセキュリティの問題に取り込み、報告しています。

SBOMを作成しているスチュワードは32%に過ぎませんが、**59%は自動依存関係追跡を使用しています。**

非営利のOSS開発を行う開発者のうち、17%が自分の貢献にCRAが適用されると誤って認識しており、59%が影響を受けるかどうか分からないと回答しています。

CRAは**平均6%の価格上昇**を促進すると予想されていますが、製造業者の53%はまだ価格への影響を評価しています。

製造業者にとって最大の懸念事項は、**法的な複雑さと**、サプライヤーやOSSプロジェクトからの**コンポーネントの安全性確保**です。

スチュワードの62%は、迅速にインシデント対応するための**専任の人員やリソースが不足**しています。

経済的支援（50%）、**法的指導**（47%）、および**技術リソース**（44%）は、スチュワードのCRA要件を満たすために最も必要です。

※CRA：Cyber Resilience Act（サイバー レジリエンス法）

序文

サイバーレジリエンス法は、最近制定されたサイバー セキュリティ規制の中で最も重要なものの1つであり、今後何年にもわたってオープンソース エコシステムに広範な影響を与えるでしょう。欧州連合（EU）域内で生活し、そこで働き、またはコンピュータ関連の商品やサービスを販売するほとんどの人は、準備と行動をとる必要がありますが、世界中の他の政府は、CRAを自国民を保護するための潜在的な立法課題のモデルと見ています。

この法律の内容と要件のほとんどは、長年にわたってサイバーセキュリティに携わってきた人にとって、目新しいものではありません。本当にユニークなのは、規制当局が、フリー ソフトウェアやオープンソース ソフトウェアに大きく依存しているか、またはこれらを内包しているハードウェアおよびソフトウェア製品で、望ましいセキュリティ ハイジーン（IT環境を健康・健全に維持する衛生管理）と責任ある使用およびサポートを強制するために取り組んでいることです。オープンソース ソフトウェアは、グローバルなイノベーションの原動力です。CRAは、法曹界にオープンソース ソフトウェアのスチュワードという新しい役割を生み出し、下流の人々が商用サービスの一部として使用するプロジェクトやコミュニティのサポートにもっと関与することを強く奨励しています。

ソフトウェア サプライ チェーン内での誰かの役割（製造者、スチュワード、開発者、消費者など）が何であれ、2027年12月に法律が施行されるまでの今後数年間で、法律に準拠するための変更が必要になる可能性が高くなります。このレポートで詳述されている調査結果は、開発者と組織のCRAに対する準備と認識の現状を示しており、私たち自身、コミュニティ、下流の準備をするために私たち全員が協力して始める必要があるいくつかの重要な領域を浮き彫りにしています。

私たちは、このデータを皆さんと一緒に探求し、この新たな課題に立ち向かうために、コミュニティと利害関係者を支援するために協力することを楽しみにしています。

Christopher (CRob) Robinson, Chief Architect, OpenSSF

目次

序文 3
エグゼクティブ サマリー 5
はじめに 6
セクション1：CRAに対する認識： 知識のギャップから行動へ 7
1.1 認識の現状 7
1.2 特定の知識ギャップ 8
セクション2：CRA分類は現実世界の複雑さに対応 9
セクション3：製造元とOSS依存関係 10
3.1 現在の相互作用パターン 11
3.2 協調的セキュリティの好例として 積極的に関与する製造業者 12
セクション4：CRAスチュワードの 準備状況 13
4.1 既存のOSSセキュリティ実践が CRAコンプライアンスの基礎となる 13
4.2 改善すべき領域 14
セクション5：非営利OSS開発への影響 15
セクション6：課題と今後の取り組み 17
6.1 製造業者にとっての戦略的意味合い 17
6.2 スチュワードのリソース制約 18
セクション7：推奨事項 19
リソース 20
調査方法 21
調査における人口統計 22
調査データへのアクセス 23
著者について 24
付録 25

エグゼクティブ サマリー

サイバー レジリエンス法（Cyber Resilience Act：CRA）は、ソフトウェア セキュリティ規制の画期的な転換であり、欧州連合（EU）でリリースされるデジタル要素を含む製品に対して、包括的なサイバーセキュリティ要件を導入します。この調査は、ソフトウェア業界全体の参加者からの調査回答に基づいており、CRAの認識と準備の現状に関する重要な洞察を明らかにし、特にOSSエコシステムへの影響に焦点を当てています。

私たちの調査では、業界全体で大きな知識のギャップがあることが明らかになっています。回答者の62%がCRAについてあまり詳しくないと回答し、51%が法規制遵守の期限について確信が持てないと回答、2027年を完全な法規制遵守の目標年として正しく特定したのはわずか28%でした 。さらに、回答者の59%が非遵守に対する罰則を認識しておらず、56%が規制における製造業者とスチュワードの重要な違いを理解するのに苦労しており、より明確なガイダンスが緊急に必要であることが浮き彫りになっています。

この調査では、準備のレベルが異なる3つのステークホルダーのグループを特定しています。CRAの下で主要な責任を負う製造業者は、その準備状況に懸念すべきギャップがあります。包括的なソフトウェア部品表（SBOM）を作成しているのはわずか34%で、46%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ますが、一方、依存しているOSSコミュニティに積極的に関与している製造業者は、より成熟した実践を示しています。

彼らは、セキュリティ評価と上流への貢献率が高く、業界の適応モデルを提供しています。

スチュワードは、回答者の8%を占める少数派ですが、セキュリティ実践の導入レベルは高く、74%がセキュリティ ポリシーを整備し、79%が自主的な報告メカニズムを保持しています。しかし、リソースの制約は依然として大きく、62%が専用のインシデント対応能力を欠いています。

重要な発見は、商業活動の過程外で発生したOSSに対する規制の意図しない影響に関するものです。非営利のOSS開発に携わる開発者のうち、17%がこの規制が自分のOSS貢献に適用されると誤って想定していることがわかりました。さらに59%は、自分たちが影響を受けるかどうか分からないと答えています。CRAは非営利の開発を明示的に除外することを目指していますが、この不確実性は OSS開発者の貢献パターンに影響を及ぼす可能性があります。

調査では、規制遵守による経済的影響も明らかになり、影響を評価した製造業者は平均6%の価格上昇を予想しています。ただし、53%の製造業者は、まだこれらのコストを評価中であり、規制の経済的影響について大きな不確実性があることを示しています。

はじめに

CRAは、欧州連合でリリースされるデジタル要素を含む製品に対して包括的なサイバーセキュリティ要件を導入し、ソフトウェア製品のサプライヤー、製造業者、輸入業者、販売業者に新たな義務を課します。この規制は、ソフトウェアおよびハードウェア業界全体で統一されたサイバーセキュリティ標準を確立する最初の大きな試みであり、特にOSSの開発と展開に影響を及ぼします。

OSSエコシステムの現在の不均衡を考えると、この規制のタイミングは重要です。一般に、製造業者の半数は、製品の半分以上がOSSコンポーネントに依存しているにもかかわらず、OSSの受動的、間接的、または限定的なユーザーのままです（付録A1）。

私たちの調査では、ソフトウェア業界全体のCRAに対す認識と準備の現状を評価するとともに、この規制がオープンソースにおける長年にわたる持続可能性の課題にどのように対処できるかを検証しています。詳細な調査回答と分析を通じて、CRAが完全に施行する前に対処する必要がある理解、実装上の課題、およびリソースの制約における重大なギャップを特定しました。

セクション1：CRAに対する認識：知識のギャップから行動へ

1.1 認識の現状

私たちの調査では、ソフトウェア業界のすべてのセグメントでCRAの認識にギャップがあることが明らかになりました。全体的な認識度は著しく低く、回答者の62%が規制について「まったく認識していない」または「ほんの少し認識している」と回答しています。この認識の欠如は、地理的に地域をまたがっていますが、顕著な違いがあります。

62%

図１： 全体的なCRA認識レベル

全体的な認識度は低く、62%がCRAに「まったく認識していない」または「ほんの少し認識している」と回答しています。

2025 CRA調査、Q18。サンプル数 = 685、全チャートは付録A2

地域別分析では、米国/カナダ（40%）とアジア太平洋地域（37%）で、欧州（29%）と比較して、不認識のレベルが高いことが明らかになりました（付録A3）。ソフトウェア サプライ チェーンのグローバルな性質と、ヨーロッパ市場にソフトウェアを提供する組織に対するCRAの潜在的な影響を考えると、この地理的な格差は特に懸念されます。CRAは、主に、ヨーロッパにおける立法の取り組みであるため、地域による認識度の差は予想外ではありません。ただし、サプライ チェーンのグローバルな性質とCRAの域外への適用を考慮すると、ヨーロッパ以外の組織は、市場へのアクセスを維持し、製品がEUに出荷される際に潜在的な法規制の影響を回避するために、法規制に対する理解と遵守を強化する必要があります。

興味深いことに、組織の規模と認識度には限定的な相関関係が見られます（付録A4）。ただし、スチュワードは製造業者（28%）と比較して認識度が著しく高く（42%が「認識している」から「非常に認識している」）、オープンソースの維持・保守に重点を置く組織では、規制の進展に積極的に関与していることが分りました （付録A5）。

[1]本稿執筆時点では、医療機器、自動車、民間航空製品、海洋機器、軍事機器の業界と製品はCRAの対象外です。欧州健康データ空間（EDHS）もCRAを改正してEHRシステムを含める予定です。

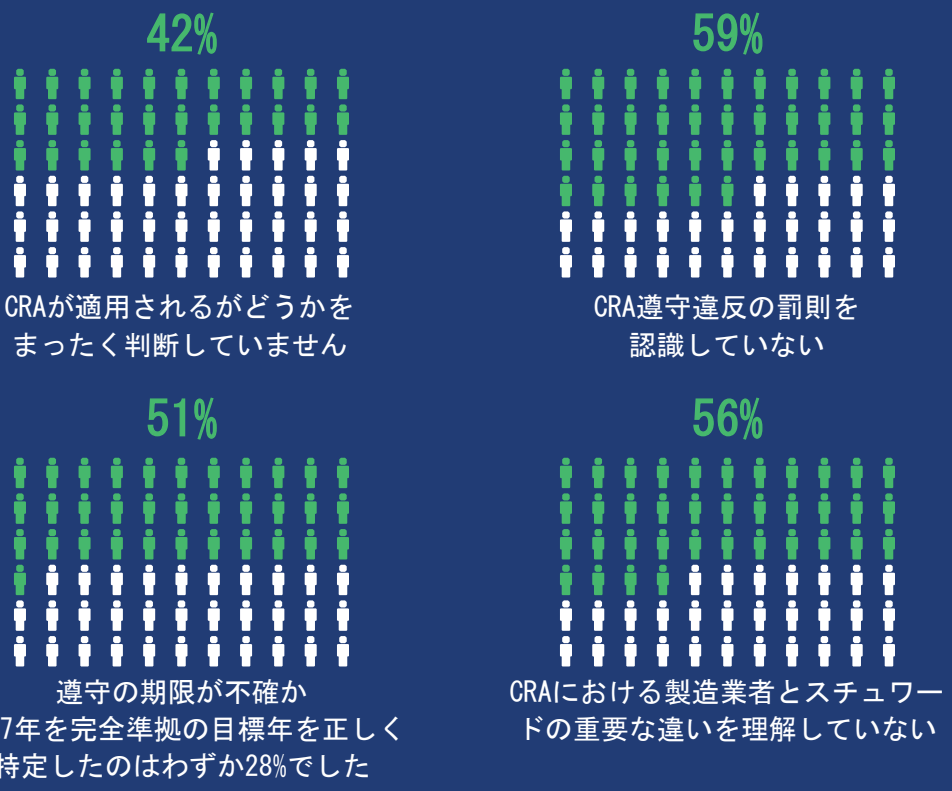
1.2 特定の知識ギャップ

CRAについてある程度の知識があると回答した回答者の中には、いくつかの重大な知識ギャップが明らかになりました（図2）。組織の42%は、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ませんでした。この見通しの不確実性は、導入期限が近づくにつれて、重大な遵守上の課題につながる可能性があります。

また、この調査では、回答者の51%が遵守の期限について確信が持てず、2027年を完全遵守の目標年として正しく認識していたのは、わずか28%であることも明らかになりました。さらに、回答者の59%が、遵守しなかった場合の罰則について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必要であることが示唆されています（図 2）。

CRAにおける製造業者とスチュワードの区別は、知識開発のもう 1つの重要な分類です。現在、回答者の56%がこれらの分類の理解に取り組んでおり、組織が役割とそれに伴う義務を正確に判断できるように、明確なフレームワークとガイドラインを作成することの重要性を強調しています。この知識ギャップは、実際に実装シナリオを検討するとき、特に顕著になります。CRAの規制フレームワークでは、さまざまな種類のソフトウェア プロバイダーに明確なカテゴリが確立されていますが、私たちの調査では、これらの分類を実際の組織構造に適用する際に大きな課題があることが明らかになりました。

図2：特定の知識ギャップ：CRAを認識している回答者からの調査結果



2025 CRA調査、Q24、Q22、Q25。サンプル数 = 384、全チャートは付録A6-A9

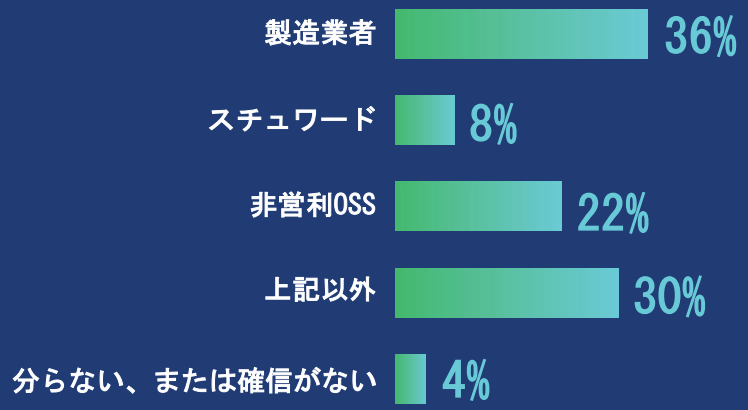
セクション2：CRA分類は現実世界の複雑さに対応

CRA規制の枠組みは、ソフトウェア プロバイダーをはっきりと区別できるカテゴリとして確立し、基本的に、製造業者とOSSスチュワードを区別しています。製造業者はCRAの規制責任を全面的に負いますが、OSSスチュワードはより緩やかな規制体制の下で活動しています。これは、セキュリティ要件とOSS開発のユニークな貢献性とのバランスを取るために設計された意図的なアプローチです。CRAは、商業目的を持たずにソフトウェアを作成する開発者は、規制の対象外となるべきであると、意図に関しても根本的な区別を試みています。

これらのカテゴリは、理論上は明確に見えるかもしれませんが、これらの区別を実際に実装することは、特に組織や個人がオープンソース エコシステム内で複数の役割を果たす場合には、かなり複雑であることが分かっています。

図3：CRAの役割の自己識別

OSSの使用と貢献に関して、この調査に回答する際に最も適していると思われる視点は次のうちどれですか？（1つを選択してください）



2025 CRA調査、Q23。サンプル数 = 384

製造業者 = "私は、欧州連合（EU）市場で商用利用を目的としたデジタル要素（例えば、ソフトウェア、IoTデバイス、コネクテッド製品など）を備えた製品を製造または開発する会社に勤務しており、これらの製品にはOSSコンポーネントが組み込まれています。"

スチュワード = "私は、EU市場での商用利用を目的とした OSSプロジェクトまたはコンポーネントを開発する組織で働いています（または、その組織から支援を受けています）。"

非営利OSS = "私は、利益を期待せず、商用利用を目的とせずに、（単独で、もしくはチームやコミュニティの一員として）自主的にOSSプロジェクトを開発しています。"

図3に示すように、調査結果によると、回答者の3分の2（66%）がCRAの役割に自分自身を分類することができ、36%が製造業者、8%がスチュワード、22%が非営利開発者として働いていると認識しています。調査でスチュワードであると回答した回答者の数が限られているのは、予想されるエコシステムの人口統計と一致しています。オープンソース エコシステムには個々のメンテナーが多数存在しますが、CRAの定義に基づいて正式に管理責任を担う組織は、より厳選された

グループであり、通常はオープンソース財団や重要なプロジェクトをサポートする専任の維持・管理組織で構成されています。

「上記以外」または「分からない、または確信がない」を選択した残り3分の1の回答者の多くは、システム インテグレーター、コンサルタント、学術関係者など、CRAカテゴリに明確に一致しない組織で働くITプロフェッショナルでした（48%）（付録A31）。IT業界には、従来のソフトウェア プロデューサー以外にもさまざまな関係者がいます。組織は、システム インテグレーター、マネージド サービス プロバイダー、コンサルタント、付加価値再販業者として同時に活動しながら、クライアント向けのカスタム ソフトウェア開発にも携わる場合があります。学術機関は、主に商業市場をターゲットにせずに、研究、ツール開発、オープン ソース プロジェクトを通じて貢献しています。

さらに複雑になるのは、オープンソース プロジェクトが独自のガバナンスとメンテナンス モデルを持つ個別のエンティティとして存在するメーカー組織自体です。大手テクノロジー企業は、多くの場合、商用製品と並行して重要なOSSプロジェクトをホストおよび維持することが多く、メーカーとスチュワードの役割の間にネストされた関係が生まれます。

セクション3：製造元とOSS依存関係

CRAはメーカーにソフトウェア開発業務全般にわたる広範な義務を課していますが、私たちの分析は特にオープンソース依存関係との関係に焦点を当てています。これは、オープンソース エコシステムへの影響を理解するという私たちの調査の主な目的を反映しています。CRAがセキュリティ評価とソフトウェア依存関係の維持に関する新しい要件を導入しているため、製造業者とオープンソース コンポーネントの関係は特に重要です。

私たちの調査結果は、セキュリティに対する姿勢の評価から上流への貢献まで、製造業者とオープンソース プロジェクトとの関わりに関する現在のパターンを調査し、効果的な共同作業の例を取り上げています。これらの動性を理解することは、オープンソース エコシステムの持続可能性をサポートしながらセキュリティを向上させるアプローチを開発する上で非常に重要です。

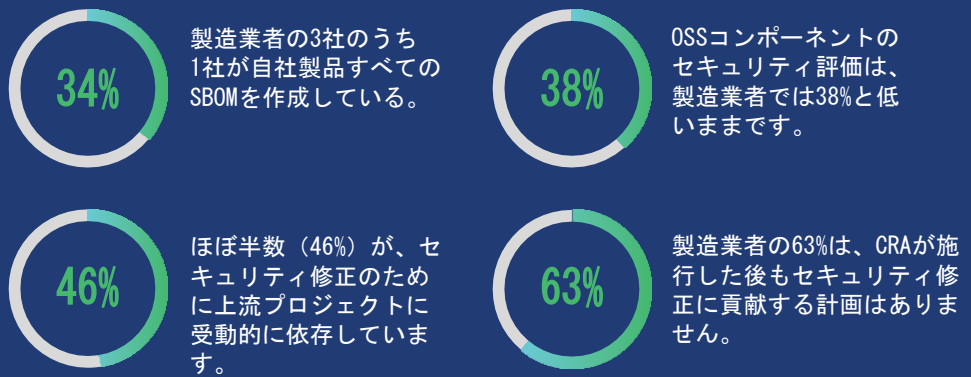
3.1 現在の相互作用パターン

製造業者の実践を分析すると、図4に示すように、CRAコンプライアンスの準備に大きなギャップがあることが明らかになりました。現在、すべての製品に対してSBOMを作成している製造業者はわずか34%であり、CRAの依存関係追跡要件にもかかわらず、ソフトウェア サプライ チェーンの可視性が限られていることが示されています。このギャップは、この規制がサプライ チェーンの透明性、報告、セキュリティ管理が重視されていることを考えると、大きな課題となります。

また、製造業者のほぼ半数（46%）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ことも判明しました。上流プロジェクトにリソースが割り当てられない限り、このアプローチは、CRAの厳格な脆弱性対応時間軸の下では不十分である可能性があります。また、調査では、OSSコンポーネントのセキュリティ対策を定常的に評価している製造業者はわずか38%であり、規制で定められた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（図4）。

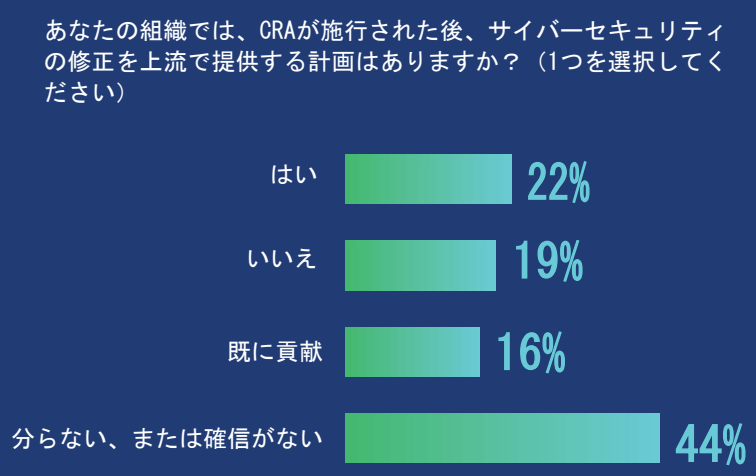
将来の貢献について、製造業者の44%は上流プロジェクトへの貢献計画について、依然として不確実であり、19%はすでに関与を増やすことを否定しています（図5）。この躊躇は、多くの組織が自社製品で使用されるオープンソース コンポーネントの長期的な存続可能性に関するCRAの暗黙的要件をまだ十分に理解しておらず、長期的な規制遵守に課題が生じる得ることを示唆しています。

図4：メーカーと使用中のOSSコンポーネントとの間の現在の相互作用パターン



2025 CRA調査、Q28、Q30、Q29、Q34。サンプル数 = 180-205、全チャートは付録A10-A13w

図5：CRAに基づく上流のサイバーセキュリティ貢献計画



2025 CRA調査、Q34。サンプル数 = 180

CRAでは、オープンソース コンポーネントを製品に統合する製造業者に、セキュリティ維持の責任を全面的に課していることを指摘しておくことが重要です。この規制は、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、商用ユーザーの法規制遵守要件の負担を負うことも求めていません。それどころか、製造業者が依存関係のセキュリティに対して積極的に責任を負わなければならないフレームワークを作成します。CRAは、製造業者が上流の修正に貢献し、オープンソース プロジェクトに資金援助を提供することを、商業活動として分類されることなく明示的に許可しています。これにより、製造業者は、直接的なコード貢献、セキュリティの改善、持続可能な資金調達モデルなどを通じて、受動的な消費からオープンソース エコシステムへの積極的な参加へと移行する機会が得られます。

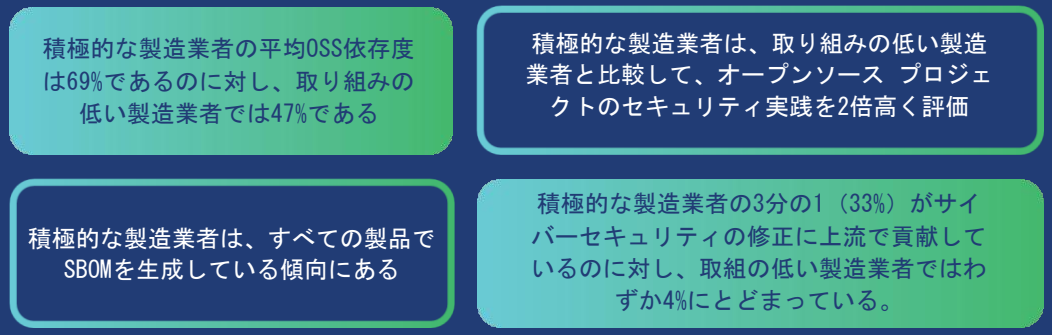
3.2 協調的セキュリティの好例として積極的に関与する製造業者

OSSへの依存に積極的に取り組んでいる製造業者は、積極的な貢献と維持を通じたオープンソースコミュニティとの緊密な統合が、製造業者とエコシステム全体の両方にどのような利益をもたらすかを実証しています。対照的に、私たちの分析では、あまり関与していない組織は、（OSSコンポーネントの管理をサード パーティに依存している）OSSの間接的、限定的、または受動的なユーザーのままである製造業者を表しています。図6にまとめられているように、関与度の高い組織はCRA要件に対する準備がより整っています。

さらに、より積極的な製造業者は、平均69%のOSS依存度を示しています。取り組みの低い製造業者は47%で、取り組みが低いにもかかわらず、深く統合しており、製品のほぼ半分をオープンソース コンポーネントに依存していることを示しています。

私たちの調査によると、積極的な製造業者は、受動的な製造業者と比較して、製品ライン全体にわたって包括的なSBOMを作成しており、オープンソース プロジェクトのセキュリティ実践を2倍高く評価していることがわかりました。

図6：協調的セキュリティの好例としての積極的に関与する製造業者



2025 CRA調査、Q27、Q28、Q29、Q32により分割されたQ34。サンプル数 = 173、全チャートは付録A14-A17

さらに、これらの組織は、上流への貢献率が著しく高いことを示しています（図6）。包括的なオープンソースへの取り組みは、野心的な目標ではなく、達成可能な現実であることを示しています。

これらの組織の既存の実践は、オープンソースのセキュリティと遵守に対する姿勢を強化したいと考えている組織にとって、実証済みのモデルとなります。

セクション4：CRAスチュワードの準備状況

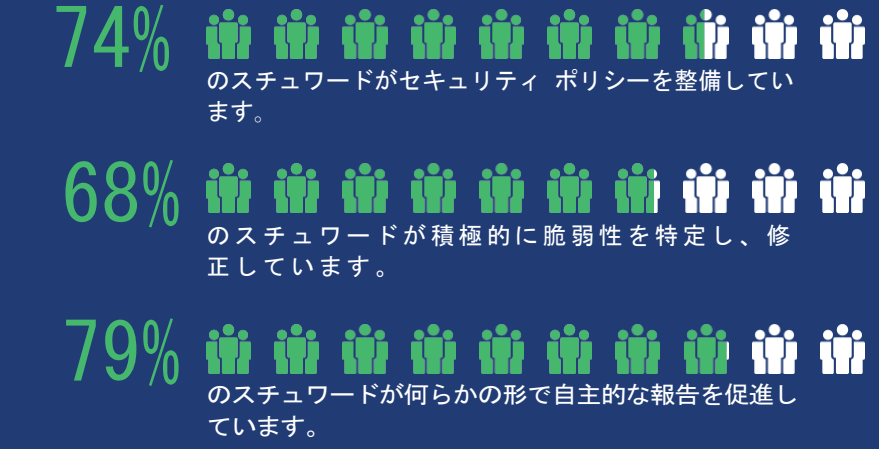
CRAにおけるスチュワードは、営利目的かどうかにかかわらず、ビジネス環境でOSSを開発する特定の財団や団体を含む、商用利用を目的としたOSSをサポートする組織を網羅する明確なカテゴリを表します。この規制は、スチュワードに対してより軽いタッチを適用し、いくつかの重要な義務に焦点を当てています。それは、文書化されたサイバーセキュリティ ポリシーの確立、頻繁に悪用されている脆弱性の当局への通知、オープンソース コミュニティ内での脆弱性情報の共有の促進です。

スチュワードの準備状況に関する私たちの評価は、34名の回答者という限られたサンプルに基づいています。これは、オープンソースのサポートと維持・管理を中心として正式に組織化されている組織の数が、比較的少ないことを反映しています。この専門グループは、調査で合計325のプロジェクトへの貢献を報告しており、重要な洞察を提供しています。しかし、CRAの導入が、最終的に正式なスチュワードの役割を導入する組織の数に影響を与える可能性があります。

4.1 既存のOSSセキュリティ実践がCRAコンプライアンスの基礎となる

調査では、CRAでスチュワードと分類される多くの組織が、規制の要件に沿った主要なセキュリティ実践をすでに実施していることが明らかになりました（図7）。約74%のスチュワードがセキュリティ ポリシーを導入していると報告し、68%が脆弱性を積極的に特定して修正していると述べています。さらに、79%のスチュワードが何らかの形の自主的な報告機能（例えは、専用のセキュリティ報告チャネルなど）を確立しており、CRAが義務付ける透明性のあるセキュリティ実践の基礎が確立されていることを示しています。

図7：既存スチュワードセキュリティ実践



2025 CRA調査、Q40、Q41、Q45。サンプル数 = 34、全チャートは付録A18-A20

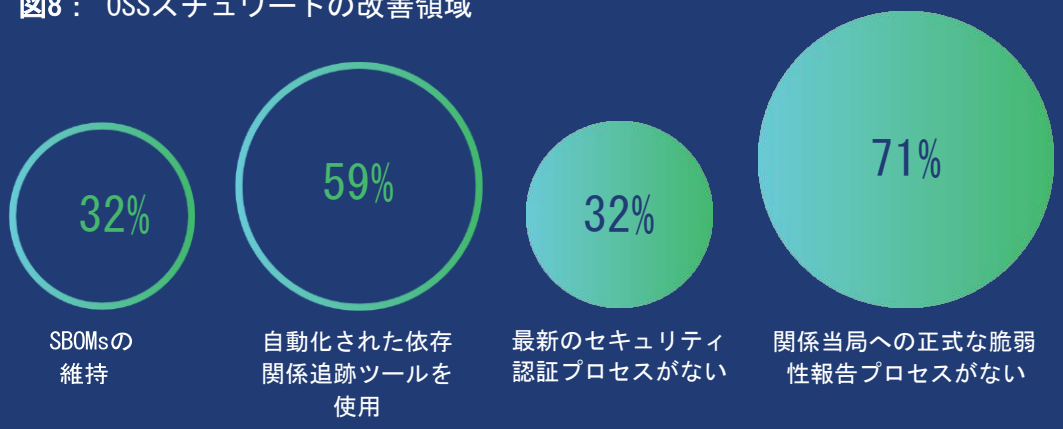
これらの既存の実践は、CRAコンプライアンスの強力な基礎となります。規制の要件に完全に適合するには、これらのメカニズムの標準化と改良が必要になる可能性がありますが、これらの基本的なセキュリティ実践は、スチュワードのコミュニティ全体でほぼ実施されているようです。

4.2 改善すべき領域

これらの肯定的な指標にもかかわらず、より広範なソフトウェア・エコシステムのセキュリティを強化できるような、スチュワードの準備状況には依然としてギャップが残っています。現在、包括的なSBOMを維持しているスチュワードはわずか32%ですが、59%が自動化された依存関係追跡ツールを使用しています（図8）。これらのツールは依存関係管理の基盤を提供しますが、標準化されたSBOMにはさらなる利点があります。例えば、プロジェクト間でシステム コンポーネントとライセンスの透明性を実現し、自動化された脆弱性追跡を容易にし、メーカーにサプライ チェーンの依存関係の明確なドキュメントを提供します。

製造業者の貢献やユーザーとのコミュニケーションプロセスに関する文書化にも顕著な限界があり、これらの分野の標準化の必要性を示唆しています。調査によると、スチュワードの32%は正式なセキュリティ認証プロセスを欠いており、71%はCRA要件に準拠した正式な脆弱性報告手順をまだ確立していません（図8）。しかし、これらのギャップは、基本的なセキュリティ対策ではなく、主にCRAの具体的な文書化要件に関係しており、手順の簡単な更新によって対処できる可能性があります。

図8： OSSスチュワードの改善領域



2025 CRA調査、Q43、Q49、Q47、サンプル数 = 34、全チャートは付録A21-A23

さらに、ほとんどのスチュワードは、市場監視当局への文書提出の準備がほとんど整っていないと回答しており、遵守に向けてこの側面について十分な準備ができていると回答したのはわずか9%でした（付録A24）。これらの要件はCRAの規制枠組みに特有のものであり、EU当局による法令の施行でさらに詳細化されることを考えると、この低い割合は驚くべきことではありません。これらの要件が明確化されるにつれて、スチュワードは既存のセキュリティ文書作成プロセスを遵守の要件に合わせて調整できるようになるはずです。

セクション5：非営利OSS開発への影響

このセクションでは、商業活動の範囲外にあるオープンソース開発に対するCRAの影響について検討します。CRAは開発者自身ではなく活動に焦点を当てていることに留意することが重要です。調査では必然的に個人から回答を収集しましたが、質問は彼らが行う活動を理解することを目的としていました。なぜなら、CRAは個々の開発者ではなく開発活動を規制するからです。

私たちの調査では、参加者にこの調査で最も代表する資格がある観点を選択するよう依頼することで、これがどのOSS開発者に影響を与えるかを特定しました。

これらの開発者は、図3に示したように、利益を期待せず、商用利用の意図もなく、自発的にOSSプロジェクトを開発していると回答しました。

調査結果から、CRAが商用の文脈以外で開発されたOSSにどのような影響を与えるかについては、不確実性が広がっていることがわかります。開発者の17%が、この規制が自分たちのOSS貢献に適用されると誤って想定していることが分かりました。さらに59%は、自分たちが影響を受けるかどうか確信が持てていません（図10）。これは、開発者の4人の内3人が、CRAが自分たちのOSS貢献に適用されると誤って想定している可能性があることを意味します（図9）。

図9：CRAがOSSの貢献に適用されるかどうかに関する不確実性

76%

オープンソース開発者の4人に3人は、CRAがOSSへの貢献に適用されると誤って想定している可能性がある

2025 CRA調査、Q53。サンプル数 = 126、全チャートは付録A25

図10：商業活動の範囲外でコードを提供する開発者に対するCRAの影響

17%は、CRAがOSS貢献に適用されると考えており、さらに59%は、影響を受けるかどうか分からないと回答しています

主たる懸念は、脆弱性に対する責任と、何が商業作業と見なされるかについての混乱に焦点を当てています

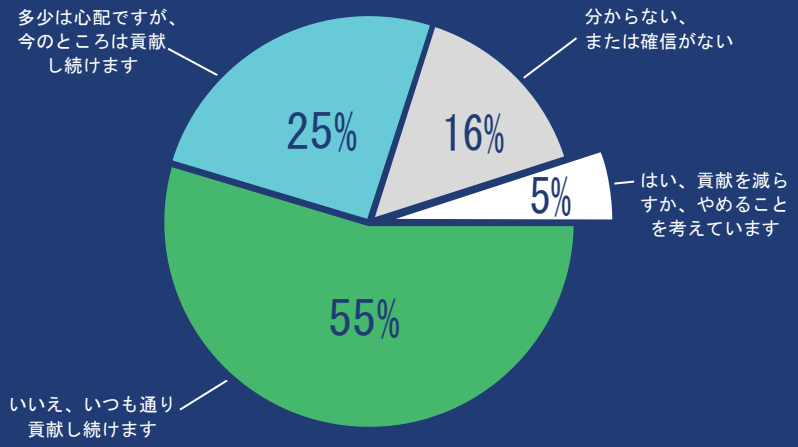
75%が明確な説明・指導が信頼を高めるのに役立つと回答

開発者は、CRAが個人にどのように適用されるか、およびシナリオ例について明確な説明を求めています

2025 CRA調査、Q53、Q57、Q55、Q56。サンプル数 = 126、全チャート付録A25-A28

図11：CRAがオープンソースの貢献に与える潜在的な影響

CRAの潜在的な影響により、OSSへの貢献を再考することはありますか？（１つを選択してください）



2025 CRA調査、Q54。サンプル数 = 126

この不確実性に対する開発者の反応は、さまざまで、5%が貢献を減らすことを検討し、25%が現在の関与レベルを継続しながらも懸念を表明しています（図11）。これらの結果は、規制の予期せぬ結果を示しています。CRAは、商業活動の範囲外にあるオープンソース開発を規制の対象から除外することを明確に目的としていましたが、明確さが欠けており、妨げられることなく作業を継続できるはずの開発者の間で躊躇が生じています。

ありがたいことに、非営利開発者の75%が、より明確なガイダンスがあれば、オープンソース作業を継続する信頼が増すだろうと回答しています（図10）。

この明確化への強い要望は、規制当局による的を絞ったコミュニケーションが、現在の不確実性に効果的に対処できることを示唆しています。CRAが個人と組織にどのような影響を与えるかに焦点を当てた明確で分かりやすいガイダンスと、規制が適用される場合と適用されない場合の実例が、特に役立ちます。これらの現実世界のシナリオは、非営利開発者が規制に対する自分の立場をより良く理解し、自信を持ってオープンソース エコシステムへの貴重な貢献を継続するのに役立つでしょう。

セクション6：課題と今後の取り組み

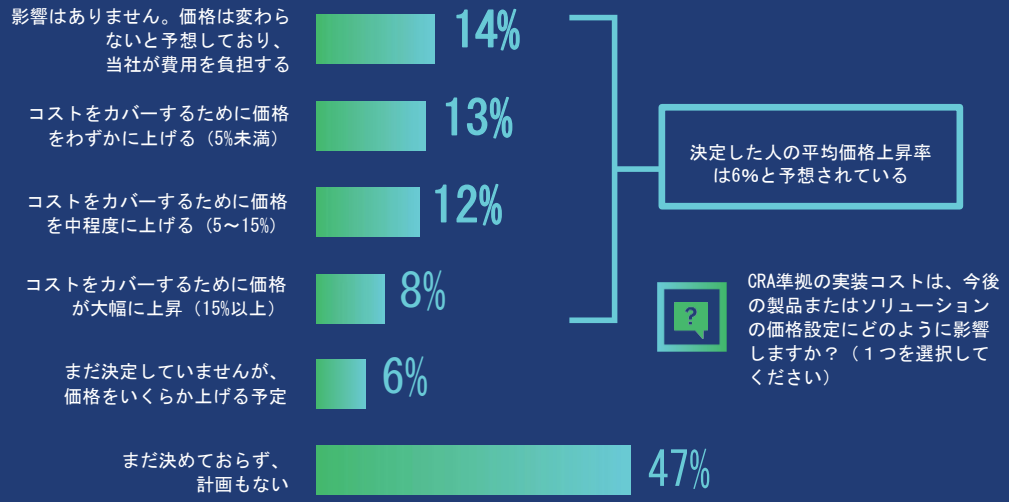
6.1 製造業者にとっての戦略的意味合い

製造業者は、CRAに準拠するための準備において、いくつかの重大な課題に直面しています。調査では、法的な複雑さと遵守の理解が主な懸念事項として挙げられ、次にサプライヤーとOSSプロジェクトのコンポーネントの安全性を確保することが課題であるとされました（付録A29）。この後者の課題が意味するところは重大です。製造業者は、オープンソース コンポーネント管理へのアプローチを根本的に見直し、受動的な消費から依存関係への積極的な関与へと移行する必要があるかもしれません。

組織は、ドキュメント要件とCRAのコストへの影響についても大きな懸念を表明しました。製造業者の53%は、まだこれらの追加要件が価格戦略にどのような影響を与えるかを判断していませんが、予備評価を行った製造業者は平均6%の価格上昇を予想しています（図12）。これは、市場がCRAに準拠するための経済的な影響全体をまだ評価中であり、ソフトウェアの価格設定とアクセシビリティに潜在的な影響があることを示しています。

CRA準備の当面の優先事項について尋ねられたとき、製造業者は、3つの主要な重点分野を特定しました（図13）。回答者の41%が挙げた最優先事項は、包括的なギャップ分析を実施して、現在の慣行をCRA要件に照らして評価することです。それに続いて、製造業者の38%が、SBOM生成、脆弱性スキャン、遵守追跡に不可欠なツールの導入を優先しています。回答者の35%が挙げた3番目の優先事項は、サイバーセキュリティの考慮事項を開発ライフサイクルとサプライチェーンのワークフローに組み込むことに重点を置いています。

図12： CRAが製品価格に及ぼす潜在的な影響



2025 CRA調査、Q38、サンプル数 = 173

6.2 スチュワードのリソース制約

この調査では、CRAエコシステムに課題をもたらす可能性があるオープンソース プロジェクト間における重大なリソース制約があることが明らかになりました（図14）。スチュワード組織の32%がインシデント対応の専用リソースを持っていると報告していますが、大多数はリソースの制約に直面しています。56%は専任の人員または資金が不足しており、6%はセキュリティ インシデントに迅速に対応できないと明確に述べています。これらの結果は、製造業者の46%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という前述の製造業者の期待と対比すると、特に重要になります。

このデータがより構造化されたサポートを受けているスチュワード支援プロジェクトのみを反映していることを考慮すると、状況はさらに複雑になります。製造業者も頼りにしている独立したコミュニティベースのプロジェクトは、迅速なセキュリティ対応能力がさらに低い可能性があります。この調査は、これらのリソース ギャップに対処するための明確な優先事項を明らかにしました。調査では、これらのリソース ギャップに対処するための明確な優先事項が明らかになりました。プロジェクトの50%が、人材、セキュリティ ツール、インフラストラクチャへの財政支援を主なニーズとして挙げており、法的支援とガイダンス（47%）、共有セキュリティ ツールや自動化コンプライアンス プラットフォームなどの技術リソース（44%）がそれに続いています（付録A31）。

製造業者の期待とオープンソース プロジェクトのリソースの現実との間のこの不一致は、製造業者が、社内能力を開発するか、依存しているプロジェクトにリソースと修正を提供するか、いずれかの方法による脆弱性の修復において、より積極的な役割を果たす必要があると示唆しています。

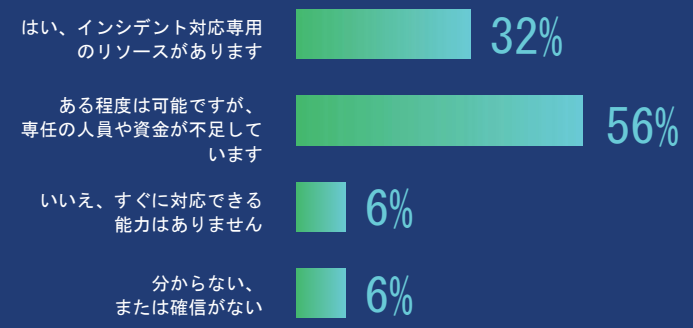
図13：製造業者のCRA要件に対処するための3つの優先事項

1. **ギャップ分析**：CRA要件に対する実践の現状評価（41%）
2. **ツールと自動化**：SBOM生成、脆弱性スキャン、コンプライアンス追跡のためのツールを導入する（38%）
3. **プロセス統合**：開発ライフサイクルとサプライ チェーンのワークフローにサイバーセキュリティを組み込む（35%）

2025 CRA調査、 Q37。サンプル数 = 180、 有効数 = 180、総言及数 = 386、全チャートは付録A30

図14：オープンソースソフトウェアプロジェクトのインシデントへの迅速な対応能力

あなたのプロジェクトには、OSSプロジェクトにおけるセキュリティ インシデントやコンプライアンスの問題に迅速に対応する能力がありますか？（1つを選択してください）



2025 CRA調査、Q50。サンプル数 = 34

セクション7：推奨事項

調査結果から、CRA導入準備における課題と機会の両方が明らかになりました。製造業者、スチュワード、OSS開発者からの回答に基づき、オープンソース エコシステムの協調性を維持しながらセキュリティ対策を強化するための戦略的取り組みとして以下を推奨します。

まず、製造業者は、CRAに基づき、依存しているOSSのセキュリティ維持について主要な責任を負うため、受動的なOSS利用者から積極的な貢献者へと変革する必要があります。現在、46%が上流の修正に依存していますが、この規制がより積極的なアプローチを求めると考えています。この変革により、メーカーは社内のセキュリティ能力を強化し、正式な貢献プロセスを確立し、依存しているプロジェクトをサポートするためのリソースを割り当てることが求められます。

第二に、セキュリティ担当者、特に確立されたセキュリティ実践とリソースを持つスチュワードは、OSSエコシステム全体にわたるセキュリティ実践の拡大と標準化に貢献できます。Open Source Security Foundation（OpenSSF）などの組織は、OpenSSFのBest Practices Badge program、OpenSSF Scorecard、SBOM生成ツールと標準、脆弱性開示フレームワークといった取り組みを通じて、スチュワードがどのように価値を提供できるかを実証しています。

第三に、規制当局と業界団体は、セキュリティ目標の達成を確保しつつ、商用活動の範囲外のものも含め、明白にOSS開発を保護する明確なCRAガイダンスの策定を優先すべきです。OSS開発者の76%がCRAの影響について不確実であることから、規制対象活動と非規制対象活動を区別する明確な事例とシナリオが不可欠です。このガイダンスには、簡素化された準拠に関わる文書と、非営利プロジェクトに対する明確な適用範囲の制限を含める必要があります。

最後に、財団や同様の組織は、商業とコミュニティの利益の間の戦略的な橋渡し役を果たすことができます。プロジェクトの26%が標準化されたセキュリティ プロセスに対する財団の支援を具体的に要請していることから、これらの組織は製造業者とコミュニティの連携を促進し、共有のインフラストラクチャとツールを提供し、すべての利害関係者に利益をもたらす標準化の取り組みを支援する上で有利な立場にあります。OpenSSFは、ソフトウェア開発者がCRAをより深く理解できるようにするためのコース（LFEL1001）を開発中です。

CRAコンプライアンスの主な責任は製造業者にありますが、リソースが豊富な関係者によるこれらの補完的な取り組みは、より回復力があり安全なオープンソース エコシステムの構築に役立ちます。

リソース

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

脆弱性のレポートとガイダンス：

- Guidelines on reporting vulnerabilities specific to LF projects and foundations.
- List of Linux Foundation projects
- Linux kernel security vulnerabilities should be reported to security@kernel.org as described in the Linux kernel security bugs page.
- Report vulnerabilities specific to Linux Foundation infrastructure or the main LF website by emailing security@linuxfoundation.org
- Alert on social engineering takeovers

セキュリティのベストプラクティスとツール：

- Alpha Omega partners with OSS project maintainers to systematically find and fix new, as-yet-undiscovered vulnerabilities in open source code
- CNCF fuzzing handbook describes what fuzzing is and how to apply it
- OpenSSF Technical Initiatives, including Best Practices Badge, Scorecard, Sigstore and more
- System Package Data Exchange (SPDX) open SBOM standard (ISO/IEC 5692:2021)
- Post Quantum Cryptography Alliance for the adoption and advancement of post quantum cryptography

教育リソース：

注目の認定資格

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

講師による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)

ハンズオン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)
- Developing Secure Software - Japanese version (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)

無料の短時間学習（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)

研究

- Empirically driven, security-specific insights from LF Research

調査方法

本調査は、Linux Foundation ResearchとOpenSSFが2025年1月に実施したWeb調査に基づいています。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調査することを目的としています。本セクションでは、調査方法とデータの分析方法、そして回答者の人口統計について説明します。

調査の観点からは、サンプル バイアスの認識を排除し、高いデータ品質を確保することが重要でした。サンプル バイアスについては、Linux Foundationの加入者、メンバー、パートナー コミュニティ、ソーシャル メディアから利用可能なサンプルを収集し、サンプル バイアスの排除に努めました。データ品質については、徹底した事前スクリーニング、アンケートのスクリーニング質問、データ品質チェックを実施し、回答者が所属組織を代表して質問に正確に回答できる十分な専門的経験を有していることを確認しました。

調査データは、業界特化型の企業、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、政府機関から収集しました。回答者は、様々な業種、規模の企業にまたがり、複数の地域からデータを収集しました。

調査は58の質問で構成され、スクリーニング、回答者の人口統計、CRAの認識度、CRAの役割の自己認識について問われ、製造業者、OSSスチュワード、非営利OSS開発者向けのセクションも設けられています。調査へのアクセス、データセット、調査頻度については、以下の調査データアクセス情報をご覧ください。

対象者には、以下の条件を満たす回答者が含まれていました。

- **OSSの概念に精通している必要があります**
- **OSSへの関与を識別できる必要があります**
- **雇用形態を識別できる必要があります**

Linux Foundation Researchによる調査は2024年12月と2025年1月に実施され、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識度セクションに回答しました。製造業者のサンプル数は180～205、スチュワードは34、OSS開発者は126です。認識度のサンプル数の誤差は、90%信頼度で±3.2%、95%信頼度で±3.8%です。

調査における人口統計

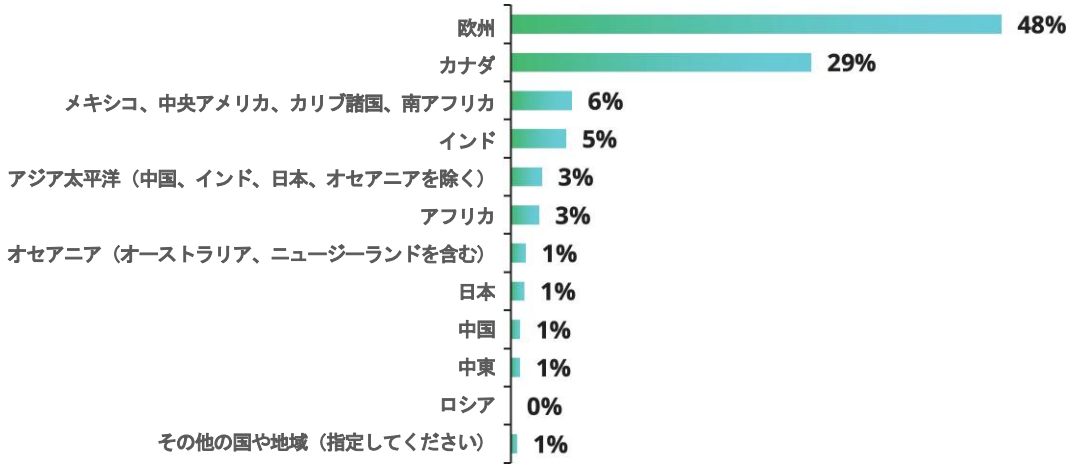
図15に示すように、本調査は幅広い地理的分布を示しており、回答者の48%がヨーロッパ、29%が米国／カナダ、10%がアジア太平洋地域に拠点を置いています。回答者のほとんどは技術職に就いています。

図16に示すように、業界別では情報技術（38%）が圧倒的に多く、次いで金融サービス（8%）とその他の様々なセクターが続いています。組織規模は分散しており、小規模組織（従業員1～249名）が41%、中規模組織（従業員250～4,999名）が29%、大規模組織（従業員5,000名以上）が28%となっています。

人口統計 I

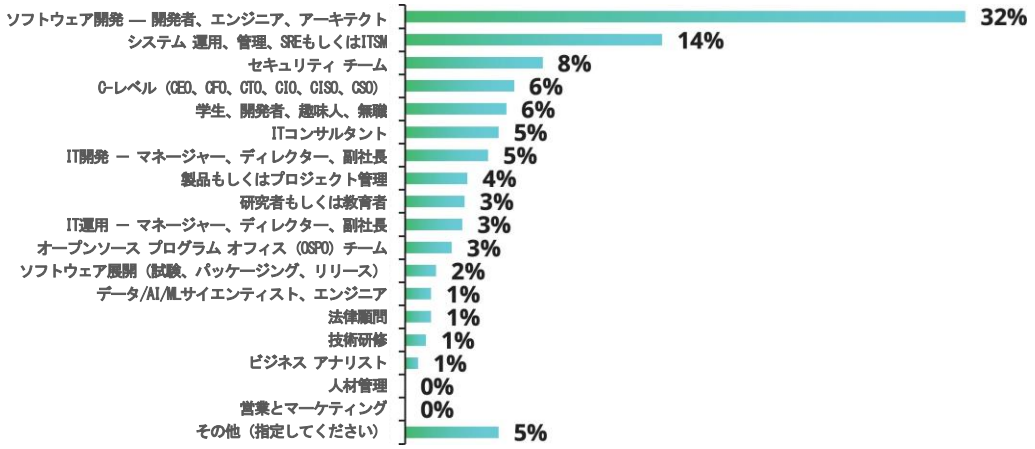
図15：2025年CRA調査で選ばれた人口統計

主にどの国や地域に住んでいますか？（1つを選択してください）



2025 CRA調査、Q6、サンプル数 = 685

職業上、あなたの役割または分野に最も近いのはどれですか？（1つを選択してください）



2025 CRA調査、Q7、サンプル数 = 685

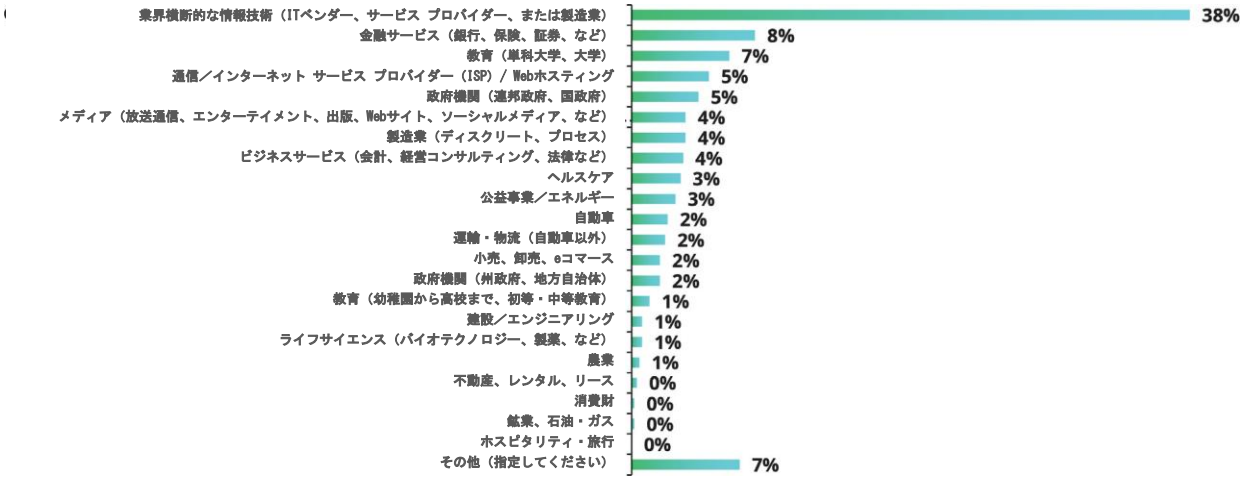
調査データへのアクセス

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、生の調査データ、スクリーニングおよびフィルタリング基準、そして調査の各質問の頻度チャートが含まれています。本プロジェクトを含むLinux Foundation Researchのデータセットは、data.world/thelinuxfoundationでご覧いただけます。Linux Foundationデータセットへのアクセスは無料ですが、Data.Worldアカウントの作成が必要です。

人口統計II

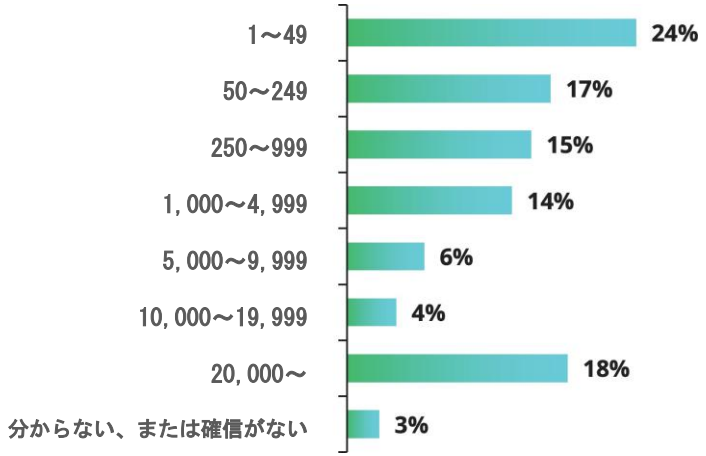
図16：2025年CRA調査で選ばれた人口統計

あなたの組織の主要産業を最もよく表すものはどれですか？（1つを選択してください）



2025 CRA調査、Q14、サンプル数 = 570

あなたが勤務する会社または団体の従業員総数の概算値を教えてください。（1つ選択してください）



2025 CRA調査、Q7、サンプル数 = 685

著者について

ADRIENN LAWSON氏は、Linux Foundationのデータアナリストです。彼女は、Oxford大学で社会データ サイエンスの修士号を取得しました。彼女は、調査の開発、分析、レポート作成を担当しています。彼女はこれまでに、Oxford大学、Budapest Institute for Policy Analysis（ブダペスト政策分析研究所）、英国Office for National Statistics（国家統計局）で研究活動に従事した経験があります。彼女は、地理的に分散したコミュニティにおけるオープンソースのコラボレーションの集合的な力に強い関心を持っています。また、彼女は、OSSの資金調達と持続可能性に関する課題の傾向と解決策の調査し、責任ある技術進歩を目指す開発者の支援に強い関心を持っています。

STEPHEN HENDRICK氏は、Linux Foundationの研究担当副社長です。Linux Foundationが、OSSがITの生産者と消費者にとってイノベーションの原動力となる仕組みを理解する上で、中核となる様々な研究プロジェクトの主任研究員を務めています。HENDRICK氏は、ソフトウェア業界アナリストとして30年以上にわたり培ってきた基礎的な研究手法を専門としています。DevOps、アプリケーション管理、意思決定分析など、アプリケーション開発と展開に関するテーマの専門家です。HENDRICK氏は、市場の動向を深く理解するための様々な定量的および定性的な研究手法の経験を持ち、多くのアプリケーション開発と導入分野における研究の先駆者となっています。HENDRICK氏は1,000以上の出版物を執筆し、シンジケート調査やカスタムコンサルティングを通じて、世界の大手ソフトウェア ベンダーや注目度の高いスタートアップ企業に市場ガイダンスを提供しています。

謝辞

調査にご協力いただき、貴重なご意見とご経験を惜しみなく共有いただいた皆様に感謝申し上げます。特に、Mirko Boehm氏、Elizabeth Bushard氏、Hilary Carter氏、Sally Cooper氏、Mia Chaszeyka氏、Mike Dolan氏、Anna Hermansen氏、Christian (fukami) Horchert氏、Angelah Liu氏、Todd Moore氏、Christina Oliviero氏、David A. Wheeler氏、Christopher (CRob) Robinso氏をはじめとする、調査プロセスの様々な段階にご協力いただいた査読者の皆様とLinux Foundationの関係者の皆様に感謝申し上げます。

付録

A1：OSS従事形態に対する製品依存関係のマッピング	
あなたの知る限り、あなたの製品の何パーセントがオープンソースソフトウェアに依存していますか？（1つ選択してください） また、あなたが依存しているOSSプロジェクトに対するあなたの組織の関与を最もよく表すものはどれですか？（1つ選択してください）	
OSS貢献レベル	**OSS依存度の平均%**
合計	**61%**
非常に積極的：依存している主要プロジェクトのコードを保守したり、定期的に提供しています	74%
中程度：時折、コードを提供したり、バグを報告したり、ドキュメントを改善したりしています	67%
限定的な関与：主に問題の報告と議論への参加を行っています	50%
間接的：上流への関与は商用サプライヤー/ベンダーに依存しています	54%
消極的：ソフトウェアは使用していますが、積極的に貢献していません	54%
2025 CRA調査、Q27～Q32、サンプル数 = 183	

A2：CRAに対する全体的な認識度	
サイバーセキュリティ レジリエンス法（CRA）についてどのくらいご存知ですか？（１つを選択してください）	
まったく認識していない	36%
ほんの少し認識している	26%
幾分認識している	17%
認識している	12%
とても認識している	5%
非常に認識している	4%
2025 CRA調査、Q18, サンプル数 = 685	

A3：地域別CRAの認識度

サイバーセキュリティ レジリエンス法（CRA）についてどの程度ご存知ですか？（1つを選択してください）主にお住まいの国または地域は？（1つを選択してください）

	総合	欧州	米国/カナダ	アジア太平洋地域
まったく認識していない	**34%**	29%	40%	37%
ほんの少し認識している	**27%**	27%	26%	27%
幾分認識している	**17%**	18%	14%	17%
認識している	**13%**	14%	10%	14%
とても認識している	**5%**	5%	7%	1%
非常に認識している	**5%**	6%	2%	4%

2025 CRA調査、Q18～Q6、サンプル数 = 615

A4：企業規模別CRAの認識度

サイバーセキュリティ レジリエンス法（CRA）についてどの程度ご存知ですか？（1つを選択してください）企業規模で分類してください。

	総合	小規模（1～249従業員）	中規模（250～4,999従業員）	大規模（5000以上従業員）
まったく認識していない	**33%**	32%	36%	32%
ほんの少し認識している	**25%**	21%	30%	27%
幾分認識している	**18%**	20%	15%	18%
認識している	**13%**	16%	12%	9%
とても認識している	**6%**	6%	2%	10%
非常に認識している	**5%**	6%	4%	4%

2025 CRA調査、Q18～Q15、サンプル数 = 555

A5：ペルソナ別CRAの認識度

サイバーセキュリティ レジリエンス法（CRA）についてどの程度ご存知ですか？（1つを選択してください）ペルソナで分類してください

	総合	製造業	スチュワード	非営利OSS
まったく認識していない	**30%**	30%	20%	34%
ほんの少し認識している	**25%**	23%	13%	33%
幾分認識している	**19%**	21%	24%	14%
認識している	**15%**	15%	24%	13%
とても認識している	**6%**	9%	7%	2%
非常に認識している	**5%**	4%	11%	4%

2025 CRA調査、Q18～Q26、サンプル数 = 389

A6：CRA準拠：組織は影響を受けているかどうか認識していますか？

あなたまたはあなたの組織がCRA規制に準拠する必要があるかどうかご存知ですか？（1つを選択してください）

はい	58%
いいえ	42%

2025 CRA調査、Q24、サンプル数 = 384

A7：CRA実装時期：重要な日付の理解が不十分

組織はいつCRA規制に完全に準拠する必要がありますか？（１つを選択してください）

2025	11%
2026	6%
2027	28%
2028	4%
分からない、または確信がない	51%

2025 CRA調査、Q22、サンプル数 = 384

A8：CRA違反の潜在的な罰則に関する認識度	
CRA規制に違反していることが判明した場合の潜在的な罰則についてご存知ですか？（１つを選択してください）	
はい	41%
いいえ	59%
2025 CRA調査、Q25、サンプル数 = 384	

A9：製造業とOSSスチュワードの違いに関する認識ギャップ	
CRAにおける製造業者とオープンソース ソフトウェア スチュワードの違いをご存知ですか？（１つを選択してください）	
はい	43%
いいえ	57%
2025 CRA調査、Q2、サンプル数 = 384	

A10：SBOMSによる製造業者の依存度追跡	
あなたの組織では、製品やソリューションで使用しているソフトウェアのソフトウェア部品表（SBOM）を作成中、または作成の準備をしていますか？（１つを選択してください）	
はい、すべての製品で対応しています	34%
一部の製品では対応していますが、すべての製品ではありません	25%
すべての製品で対応しているわけではありませんが、対応を計画しています	6%
私の組織はSBOMを認識していますが、現在は導入しておらず、計画もありません	9%
私の組織はSBOMについて全く認識していません	4%
分からない、または確信がない	21%
2025 CRA調査、Q28、サンプル数 = 205	

A11：製造業者におけるOSS脆弱性対応戦略	
製品のOSSコンポーネントに脆弱性がある場合、通常はどのように対処していますか？（1つを選択してください）	
OSSプロジェクトによる修正プログラムの提供に頼っています	46%
自分たちでコンポーネントにパッチを適用しています	20%
より安全な代替コンポーネントに置き換えています	11%
サポート対象バージョンまたはエンタープライズバージョンのコンポーネントを使用しています	9%
顧客に問題を通知していますが、直接対処していません	0%
対処をしていません	1%
分からない、または確信がない	12%
2025 CRA調査、Q30、サンプル数 = 205	

A12：メーカーにおけるOSSセキュリティ可視化の取り組み	
あなたの組織では、使用しているOSSコンポーネントのセキュリティ状況を可視化していますか？（1つを選択してください）	
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	38%
ある程度、公開されているアップデートやコミュニティ レポートに依存しています	44%
いいえ、使用しているOSSプロジェクトのセキュリティ対策を監視していません	9%
分からない、または確信がない	9%
2025 CRA調査、Q29、サンプル数 = 205	

A13：CRAに基づく上流サイバーセキュリティ貢献計画	
あなたの組織は、CRA施行後、サイバーセキュリティ修正を上流に提供する計画をお持ちですか？（いずれか1つを選択）	
はい	22%
いいえ	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）を上流に提供しています	16%
分からない、または確信がない	44%
2025 CRA調査、Q29、サンプル数 = 205	

A14：OSS貢献レベル別OSS依存度

あなたの知る限りにおいて、貴社製品のうち、オープンソース ソフトウェアにどのくらいの割合で依存ししていますか？（1つを選択してください）OSSへの関与レベルで分類してください。

	総合	高関与者	低関与者
25%未満	**13%**	5%	21%
25%～50%	**21%**	18%	23%
51% to 75%	**20%**	17%	22%
75%以上	**41%**	58%	26%
分からない、または確信がない	**5%**	1%	9%
平均		69%	47%

2025 CRA Survey, Q27 by Q32, Sample Size = 193

A15：OSS貢献レベル別SBOM作成状況

あなたの組織では、製品またはソリューションで使用されているソフトウェアについて、ソフトウェア部品表（SBOM）を作成、または作成準備中ですか？（1つを選択してください）OSS関与レベルで分類してください。

	高関与者	低関与者
はい、すべての製品で作成中です	43%	26%
はい、一部の製品で作成中です	27%	25%
すべての製品で作成中ではありませんが、作成を計画しています	8%	5%
SBOMについては認識しているが、現在は作成しておらず、計画もまだありません	8%	12%
SBOMについて全く認識していません	0%	9%
分からない、または確信がない	14%	24%

2025 CRA調査、Q28～Q32, サンプル数 = 193

A16：OSS貢献レベル別OSSセキュリティの可視性

あなたの組織では、使用しているOSSコンポーネントのセキュリティ状況を可視化していますか？（1つを選択してください）OSS関与レベルで分類してください。

	総合	高関与者	低関与者
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	38%	51%	26%
ある程度は、公開されているアップデートやコミュニティレポートに依存しています	46%	36%	55%
いいえ、私たちが利用するOSSプロジェクトのセキュリティ対策を監視していません	9%	7%	12%
分からない、または確信がない	7%	7%	7%

2025 CRA調査、Q34～Q32、サンプル数 = 173

A17：OSS貢献レベル別上流へのサイバーセキュリティ修正への貢献計画

CRA施行後、あなたの組織は、上流のサイバーセキュリティの修正に貢献する計画をお持ちですか？（1つ選択してください）
OSS貢献レベルで分類してください。

	総合	高関与者	低関与者
はい	21%	27%	16%
いいえ	20%	10%	28%
既に、依存しているプロジェクトの上流にセキュリティ修正（パッチ）を貢献しています	16%	30%	4%
分からない、または確信がない	43%	33%	51%

2025 CRA調査、Q29～Q32、サンプル数 = 193

A18：第24条（1）サイバーセキュリティ ポリシーに対応するスチュワードの準備状況、

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を効果的に処理するためのセキュリティ ポリシーがありますか？（1つを選択してください）

はい	74%
いいえ	18%
分からない、または確信がない	9%

2025 CRA調査、Q40、サンプル数 = 34

A19：脆弱性の修正に関するスチュワードの準備	
OSSプロジェクトの脆弱性を特定して対処するプロセスはありますか？（1つを選択してください）	
はい、脆弱性を積極的に特定し、修正しています	68%
はい。ただし、脆弱性への対応はユーザーから報告があった場合のみ行っています	21%
いいえ、問題の解決は外部の貢献者やユーザーに依存しています	6%
分からない、または確信がない	6%
2025 CRA調査、Q41、サンプル数 = 34	

A20：第24条（1）に対する自主的な報告を促進するためのスチュワードの準備	
あなたのプロジェクトでは、脆弱性の自主的な報告をどのように奨励していますか？（該当するものをすべて選択してください）	
専用のセキュリティ報告チャネルを提供しています（例：security@email、非公開の脆弱性報告）	65%
解決済みのセキュリティ問題に関する勧告をコミュニティと共有しています	56%
報告ガイドラインを定めたセキュリティ ポリシー（例：SECURITY.md）を整備しています	53%
機密性の高いセキュリティ報告を処理するための明確なプロセスがあります	50%
セキュリティ報告用のテンプレートまたはガイドラインを提供しています	24%
具体的な対策はまだ実施していません	12%
その他（具体的にご記入ください）	9%
分からない、または確信がない	9%
2025 CRA調査、Q45、サンプル数 = 34, 有効数 = 34, 総言及数 = 94	

A21：スチュワード組織における依存関係の追跡	
プロジェクト内の依存関係をどのように追跡していますか？（該当するものをすべて選択してください）	
自動化された依存関係追跡ツールを使用している	59%
SBOMを維持・管理している	32%
依存関係リストを手動で管理している	26%
セキュリティ上重要な依存関係を個別に追跡している	15%
現在、依存関係を体系的に追跡していない	9%
分からない、または確信がない	12%
2025 CRA調査、Q43、サンプル数 = 34、有効数 = 34, 総言及数 = 52	

A22：自主的なセキュリティ認証におけるスチュワードの準備状況（第25条）	
セキュリティ認証のプロセスには何が含まれていますか？（該当するものをすべて選択してください）	
自動化されたセキュリティ スコアリング ツールを使用しています	21%
公開された文書を通じてセキュリティ対策を自己証明しています	18%
定期的に第三者によるセキュリティ監査を受けています	18%
コミュニティのレビュープロセスを通じてセキュリティに関する要求を検証しています	18%
正式なセキュリティ認証プログラムに参加しています（例：OpenSSFベスト プラクティス バッジ）	15%
特定のセキュリティ標準への準拠を維持しています	12%
標準化された形式でセキュリティ対策を文書化しています	9%
財団／プロジェクトには、すべてのプロジェクトのセキュリティ対策を担当する一元化された脆弱性管理チームがあります	9%
現在、セキュリティ認証プロセスはありません	32%
その他（具体的にご記入ください）	6%
分からない、または確信がない	12%
2025 CRA調査、Q49、サンプル数 = 34、有効数 = 34、総言及集 = 57	

A23：既知の現在悪用されている脆弱性の報告／重大なインシデントの通知に関するスチュワードの準備状況（第24条（3）） OSSプロジェクトでは、既知の脆弱性／現在悪用されている脆弱性をどのように報告していますか？（1つを選択してください）	
関係当局への報告プロセスが確立されている	29%
誰に報告すればよいかはわかっていますが、正式なプロセスがありません	18%
報告要件／プロセスが不明である	35%
報告メカニズムが整備されていない	18%
2025 CRA調査、Q47、サンプル数 = 34	

A24：市場監視への協力/文書提供に関するスチュワードの準備状況（第24条（2）） 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？（いずれか1つを選択してください）	
はい、文書は準備できています	9%
一部の文書は準備できています	24%
現在、準備中です	12%
文書は準備されていません	26%
分からない、または確信がない	29%
2025 CRA Survey, Q46, Sample Size = 34	

A25：CRA によるOSS開発者への影響 CRAがあなたのオープンソースへの貢献に適用される可能性があると思いますか？（1つを選択してください）	
いいえ、自分に適用されるとは思っていません	24%
適用される可能性はありますが、確信はありません	59%
はい、貢献者として影響を受ける可能性があると思います	17%
2025 CRA調査、Q53、サンプル数 = 126	

A26：OSS開発者にとって最も懸念されるシナリオ	
CRA規制に関して、具体的にどのようなシナリオに懸念されますか？（該当するものをすべて選択してください）	
知らないうちに脆弱性を生じさせ、責任を問われる可能性があります	54%
趣味の貢献と専門的な仕事の区別がついていません	44%
企業が自社製品に使用した場合、自分のプロジェクトが商用として認められるかどうか不明です	40%
OSSプロジェクトが仕事で使われると、商業活動のように思われるかもしれない	33%
その他（具体的にご記入ください）	6%
心配していません	13%
分からない、または確信がない	6%
2025 CRA調査、Q46、サンプル数 = 34	

A27：明確な情報の必要性	
CRAに関する明確な説明があれば、OSSへの貢献を継続する上でより自信を持てるようになりますか？（いずれか1つを選択してください）	
はい、明確な情報があれば安心できます	75%
いいえ、それでも不安を感じます	6%
不明です。提供されるガイダンス次第です	20%
2025 CRA調査、Q55、サンプル数 = 126	

A28：OSS貢献者を支援する方法	
CRAとそのOSS貢献への影響について理解を深めるのに役立つものは何ですか？（該当するものをすべて選択してください）	
CRAが個人にどのように適用されるかについての明確な説明	81%
CRAが適用される、または適用されないシナリオの例	81%
オープンソース財団または規制当局からのガイダンス	60%
教育資材（記事、ウェビナー、ワークショップ）	52%
その他（具体的に記入してください）	6%
分からない、または確信がない	2%
2025 CRA調査、Q56、サンプル数 = 126、有効数 = 126、総言及数 = 356	

A29：製造業者にとっての主な課題	
CRAの製造業者への要件への対応に対して、どのような課題があると考えていますか？（該当するものをすべて選択してください）	
規制の複雑さと法的責任に関する懸念	47%
サプライヤーとOSSプロジェクトのコンポーネントがCRA基準に準拠していることの確認	46%
CRA規制への準拠を証明する文書の提供	42%
CRA遵守にかかるコスト	40%
SBOMの生成、更新、およびサードパーティの依存関係の追跡	39%
CRA要件と他の国際規制の整合	39%
安全なソフトウェア開発ライフサイクルの実装	36%
脆弱性管理の実装：監視、パッチ管理、および脆弱性報告	32%
サイバーセキュリティ スタッフの追加採用とトレーニングのニーズへの対応	28%
その他（具体的に記入してください）	2%
課題なし	1%
分からない、または確信がない	19%
2025 CRA調査、Q36、サンプル数 = 180、有効数 = 180、総言及数 = 669	

A30：製造業者の最優先事項	
製造業者に対するCRA要件に対応する上で、最優先事項として挙げている項目は以下のどれですか？（最大3つ選択してください）	
ギャップ分析：CRA要件に対する現在の実践の評価する	41%
ツールと自動化：SBOM生成、脆弱性スキャン、コンプライアンス追跡のためのツールを導入する	38%
プロセス統合：開発ライフ サイクルとサプラ イチェーンのワークフローにサイバーセキュリティを組み込む	35%
人材育成：CRA要件とベスト プラクティスについてチームをトレーニングする	26%
コラボレーション：サプライヤー、オープンソース プロジェクト、規制当局と連携し、整合性を確保する	24%
予算配分：必要な技術面および運用面のアップグレードのための資金を確保する	18%
分からない、または確信がない	32%
2025 CRA調査、Q37、サンプル数 = 180、有効数 = 180、総言及数 = 386	

A31：スチュワードにとって最も必要なリソース	
CRA要件を満たすために、プロジェクトに最も必要なサポートは何ですか？（最大3つ選択してください）	
財政的支援（例：人員、セキュリティツール、インフラへの資金提供）	50%
法的支援とガイダンス	47%
技術的リソース（例：共有セキュリティツール、自動化コンプライアンス プラットフォーム）	44%
財団からの支援（例：標準化されたセキュリティ プロセス、共有ベスト プラクティス、共通ポリシー フレームワーク）	26%
商用ユーザーからの支援（例：アップストリームへの貢献、リソース）	24%
セキュリティト レーニングとドキュメント	18%
コミュニティ サポート（例：共同対応チーム）	6%
その他（具体的にご記入ください）	3%
分からない、または確信がない	12%
2025 CRA調査、Q52、サンプル数 = 34, 有効数 = 34、総言及数 = 78	

A32：CRAの役割を特定できない人の分布	
どのような種類の企業または団体に勤務していますか？（1つを選択してください）	
業界特有の製品またはサービスを提供している	25%
IT製品またはサービスを提供している（SI、ITコンサルタントを含む）	20%
政府機関（地方自治体、郡、州、地域、または国）	10%
非営利団体または財団	4%
学術機関	8%
その他の団体（具体的に記入してください）	6%
学生、趣味で開発を行っている人、失業者、新卒者、退職者（または類似）	27%
2025 CRA調査、Q12とQ7、サンプル数 = 196	

facebook.com/
TheLinuxFoundation

x.com/linuxfoundation

linkedin.com/company/
TheLinuxFoundation

この研究を参照するには、次のように引用してください：Adrienn Lawson、Stephen Hendrick、「Unaware and Uncertain: The Stark Realities of Cyber Resilience Act Readiness in Open Source」、Christopher (CRob) Robinsonによる序文、The Linux Foundation、2025年3月。

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：天満尚二

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Open Source Security Foundation（OpenSSF）は、Linux Foundationによる業界横断的なイニシアチブであり、業界で最も重要なオープンソース セキュリティ イニシアチブと、それらを支援する個人や企業を結集しています。OpenSSFは、オープンソース セキュリティの推進に向け、上流や既存コミュニティとの連携・協力に尽力しています。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、拡大するオープンソース コラボレーションの規模を調査し、新興技術のトレンド、ベスト プラクティス、そしてオープンソース プロジェクトの世界的な影響に関する洞察を提供しています。Linux Foundation Researchは、プロジェクト 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 プラクティスへのコミットメントを通じて、世界中の組織に役立つオープンソースに関する洞察を提供する頼りになるライブラリを構築しています。