

# Built to Last

～持続可能な仕組みを目指して～

欧州サイバーレジリエンス法 (CRA)  
を理解する



**Sal Kimmich**  
Policy Manager,  
OpenUK



# エグゼクティブサマリー

サイバーレジリエンス法 (CRA) は法律です。

規則 (EU) 2024/2847は2024年12月10日に発効しました。この規則は各国で対応する国内法を制定することなく、EU加盟国全体に直接適用されます。対象はEU市場で販売されるほぼすべてのハードウェアおよびソフトウェア製品です。また、デジタル製品の製造、輸入、流通、または購入を行うほとんどの組織にとって、この規則は既に実行していることがらを義務として課すものです。

このガイドが存在するのは、CRAが要求する内容と、CRAの要求としてほとんどの組織が理解している内容との間に、依然として大きな隔たりがあるためです。

規則準拠のために3つの期限が定義されています。2026年6月には、適合性評価機関への通知に関する枠組みが運用開始されました。2026年9月には、脆弱性報告義務が発効します。製造業者は、脆弱性を認識してから24時間以内に、実際に悪用されている脆弱性(AEV: Actively Exploited Vulnerability)を自国のCSIRTおよび ENISAに通知しなければなりません。この義務は、新製品だけでなく、既に市場に出回っている製品にも適用されます。2027年12月には、全面的な施行が開始され、EU市場に上市されるすべての製品に、規制が示すサイバーセキュリティに対する必須要件への適合性を証明するCEマークを付さなければなりません。

このガイドは、実務担当者、保守担当者、法務チーム、購入者が実際に抱いている10の質問を中心に構成されています。各章は独立して読めるように書かれています。必ずしも順番に読む必要はありませんが、各章の内容は互いに関連しています。

## 法的免責事項

本資料は情報提供および教育目的のみを意図したものであり、法的助言を構成するものではなく、またそのように解釈されるべきではありません。サイバーレジリエンス法 (規則 (EU) 2024/2847) は複雑な法律です。特定の組織、製品、またはサプライチェーン関係への適用は、本ガイドでは提供できない事実および法的分析に依存します。また、本ガイドで説明されている規制環境も常に変化しており、実施法、委任法、整合規格、および欧州委員会のガイダンスはすべて変更される可能性があります。読者は、関連する規制事項に基づいて行動する前に、その最新の状況を確認する必要があります。

本ガイドの内容は、著者または関連団体と読者との間に助言関係や顧客関係を生じさせるものではなく、またそのような関係を示唆するものでもありません。規制準拠に関する具体的な疑問をお持ちの組織は、EU製品規制に精通した資格のある法律顧問にご相談ください。本ガイドは、Open Source Security Foundation (OpenSSF)、Linux Foundation、欧州委員会、ENISA、およびその他の公的機関が作成した公開資料に基づいています。このガイドに記載されている見解は、著者個人のものであり、他のいかなる個人または組織の見解を反映するものではありません。

# 各章の内容

## 第1章：サイバーレジリエンス法とは何か、そしてなぜ重要なのか？

デジタル製品のすべての生産者と購入者向けの導入部分。CRAとは何か、何を規制するのか、そしてCRAが適用されないという想定がほとんどの組織にとって既に間違いなのはなぜか。

## 第2章：あなたの製品が対象範囲内にあるかどうかを知るには？

製品の階層的分類：デフォルト、重要な製品クラスIおよびII、クリティカルな製品。製品に適用される適合性評価方法を判断する方法。

## 第3章：オープンソースも例外ではない。

### CRAが実際に定めている内容とは

商業活動テスト、オープンソースソフトウェア スチュワードの概念、そして商業ユーザーが新たな疑問を投げかけ始めた今、義務を負っていないメンテナーでさえも行うべきこと。

## 第4章：セキュリティ・バイ・デザインは法的要件となったが、実際はどういうことか

附属文書Iの解説：パートIの必須製品要件とパートIIの脆弱性対応義務を、エンジニアリングチームが実施すべきことと文書化すべき内容として記す。

## 第5章：CRAに基づく脆弱性報告：実践的な解説

3段階の報告プロセス、24時間ごとの時間制約、2026年9月がSBOM準備の実施期限となる理由、そしてCRAに準拠した開示ワークフローの構築方法。

## 第6章：あなたが作ったわけではない。それでもあなたは責任を負う

輸入業者と販売業者の義務。デューデリジェンスの実践とはどのようなものか、サプライヤー契約には何を含めるべきか、そしてシステムインテグレーターが占める具体的な立場。

## 第7章：CRAに基づく適合性評価：実際のプロセス内容

適合性評価の3つの手順、認証機関の役割と必要となる時期、技術ファイルに含めるべき内容、そして整合規格の現状について。

## 第8章：CRAが優れた調達のある方を変える

購入者がCEマーキングや適合性文書を調達のためのシグナルとしてどのように活用できるか、現在標準的なベンダーからの質問事項は何か、そしてサプライヤー契約を適切に更新する方法。

## 第9章：小規模チームのためのCRAコンプライアンス：法務部門がない場合、どこから始めるべきか

中小企業向けの規定、必要最低限の文書セット、そして創業者や小規模なエンジニアリングチームにとって準拠のハードルを下げる無料の公共リソース。

## 第10章：CRAは単独で存在するものではない：EUデジタル主権フレームワークに位置付けられている

CRAがNIS2、欧州AI法、DORA、データ法とどのように関連しているか。CRA準拠を単発的な取り組みではなく、インフラストラクチャとして捉えるべき戦略的な根拠。

各章の末尾には、一次資料の参照情報が記載されています。本書全体を通して使用されている規制に関する引用は、2024年11月20日に欧州連合官報に掲載された 規則 (EU) 2024/2847の条文、およびその後採択された実施法および委任法を参照しています。

# 目次

|                                                        |    |
|--------------------------------------------------------|----|
| エグゼクティブサマリー .....                                      | 2  |
| 各章の内容.....                                             | 3  |
| 第1章：サイバーレジリエンス法とは何か、そしてなぜ重要なのか？ .....                  | 5  |
| 第2章：あなたの製品が対象範囲内にあるかどうかを知るには？ .....                    | 7  |
| 第4章：セキュリティ・バイ・デザインは法的要件となったが、実際はどういうことか .....          | 11 |
| 第5章：CRAに基づく脆弱性報告：実践的な解説 .....                          | 13 |
| 第6章：あなたが作ったわけではない。それでもあなたは責任を負う .....                  | 15 |
| 第7章：CRAに基づく適合性評価：実際のプロセス内容 .....                       | 17 |
| 第8章：CRAが優れた調達のあり方を変える .....                            | 19 |
| 第10章：CRAは単独で存在するものではない：EUデジタル主権フレームワークに位置付けられている ..... | 23 |

# 第1章：サイバーレジリエンス法とは何か、そしてなぜ重要なのか？

**要約：**CRAはEU法です。2024年12月に施行されました。EU市場で販売されるほぼすべてのハードウェアおよびソフトウェア製品が対象となります。組織がデジタル製品を製造、輸入、販売、または購入している場合は、この法律が適用されます。

数年前、ソフトウェアベンダーに製品安全法の適用を受ける予定があるかと尋ねたら、ほとんどのベンダーは「いいえ」と答えたとでしょう。ソフトウェアはトースターではありません。CEマークも付いていません。物理的な製品に関するルールは適用されませんでした。

その前提は、今は間違っています。

サイバーレジリエンス法は、2024年11月20日に規則（EU）2024/2847として正式に公布され、2024年12月10日に発効しました。これは指令（directive）ではなく、国内法の制定も不要です。EU加盟国すべてに直接適用され、多くの組織が想定していたよりも幅広い製品を対象としています。

## CRAが実際に規制しているもの

CRAは、いわゆるデジタル要素を含む製品（PDE）に適用されます。その定義は広範で、ハードウェア、ソフトウェア、それらを含む製品、およびそれらのバックエンドサービスがEU市場で提供される場合、対象となります。これには、消費者向け機器、産業用制御システム、スマートホーム製品、オペレーティングシステム、モバイルアプリ、そして企業が欧州市場で販売またはライセンス供与するソフトウェアの大部分が含まれます。

除外事項もあります。医療機器、自動車、航空機、その他独自の安全・セキュリティ基準を持つ製品カテゴリーは対象外です。しかし、一般的なソフトウェアとなにかに接続されるハードウェアのほとんどは対象範囲に含まれます。

CRAの主な目的は、データ漏洩によるコストを削減し、デジタル要素を含む製品に対する顧客の信頼を高めることです。二次的な効果として、責任の所在が大きく再調整されることになります。現在、既知の脆弱性を抱えた製品が出荷された場合、判断のコストは、その製品に依存するユーザーや組織が負担することになります。CRAはそのコストを、そもそもの判断を行ったマニュファクチャラーへ転嫁します。

## 知っておくべき3つの日付

CRAの規定は一度にすべて適用されるわけではなく、重要な3つの日付があります。

**2026年6月11日：**適合性評価機関への通知に関する枠組みが運用開始されます。あなたの製品が重要な製品またはクリティカルな製品のカテゴリーに該当する場合、この枠組みは重要となります。

**2026年9月11日：**脆弱性報告義務が開始されます。この日付以降、製品に実際に悪用されている脆弱性(AEV)がある場合、24時間以内にSRP(Single Reporting Platform: 単一報告プラットフォーム)を通じて、関連するCSIRTおよびENISAに報告する必要があります。これは、新規リリースだけでなく、既に市場に出回っている製品にも適用されます。

**2027年12月11日：**全面施行。すべての必須サイバーセキュリティ要件が適用されます。製品は、EU市場に上市される前に、適合性を証明するCEマークを取得している必要があります。

## 「自分には影響しない」という 思い込みが既に崩れ始めている理由

組織が新たな規制に対応する際のパターンには共通点があります。それは、規制の施行を待つこと、規制の範囲を実際よりも狭く見積もること、そしてコンプライアンスを初期段階の技術的な判断ではなく、最終段階の法的問題として扱うことです。

CRAは「完全な」SBOMを要求してはいないということを理解することは重要です。附属書I、パートII(1)では、少なくとも最上位の依存関係、つまり直接利用しているコンポーネントまでを網羅するSBOMを、機械可読形式で最新の状態に保つことを要求しています。これは法的最低限の要件であり、2027年12月まで強制力はありません。7段階目のログインライブラリに至るまでの推移的依存関係を列挙しなかったとしても、ペナルティを受けることはありません。

しかし、最低限の要求を目標・目的と混同すべきではありません。log4shellのシナリオでは、まさにトップレベルの可視性が問題となります。影響を受けるコンポーネントが、あなたが作成していないコードの何層も奥深くに存在する場合です。規制は表面的な部分で調査を停止することを認めていますが、効果的なインシデント対応はそうはいきません。

実質的な対応期限は、24時間以内の報告義務が発効する2026年9月です。脆弱性が開示されると、それが自社製品に影響を与えるかどうかを判断するのに1日しか猶予がありません。これは多くの場合、最上位の依存関係だけでは判断できない問題です。実際に出荷した製品の正確かつ最新の情報が必要となります。実際には、これはCRAがまだ正式に義務付けていない、より詳細なSBOMを作成することを意味します。なぜなら、それがCRAが既に要求している義務を果たす唯一の方法だからです。

## 対象となるのは誰で、どのような役割を担うのか

CRAは、マニファクチャラー、輸入業者、販売業者を区別しています。それぞれの役割には異なる義務があり、その区別は重要です。製品を設計・出荷する製造業者、つまりマニファクチャラーは最も重い義務を負います。EU域外から製品をEU市場に持ち込む輸入業者は、独自のデューデリジェンス要件を満たす必要があります。再販を行う販売業者にも義務があります。

オープンソースは原則として免除されるわけではありませんが、非営利のオープンソースは異なる扱いを受けます。オープンソースソフトウェア・スチュワードと呼ばれる新たな法的区分が設けられており、これはマニファクチャラーとして活動することなくオープンソース開発を支援する財団や組織を対象としています。

この電子書籍の残りの部分では、これらの役割それぞれについて詳しく解説しています。どの組織にとっても出発点は共通しています。それは、規制を読み、自分たちがどのような役割を担っているかを理解し、今すぐコンプライアンス作業を開始することです。

CRAは既に施行されています。期限は迫っています。問題は、それがあなたに適用されるかどうかではありません。ほとんどの組織にとって、適用されます。問題は、あなたはどれほど遅れをとってから、ようやく真剣に受け止めるつもりなのか、ということです。

参考資料：OpenSSFのEUサイバーレジリエンス法（CRA） ページ ([openssf.org/public-policy/eu-cyber-resilience-act](https://openssf.org/public-policy/eu-cyber-resilience-act)).

Linux Foundationの無料コース：LFEL1001 「EUサイバーレジリエンス法の理解」。

## 第2章：あなたの製品が対象範囲内にあるかどうかを知るには？

**要約：**CRAは段階的な製品分類システムを採用しています。ほとんどの製品は自己認証が可能です。重要な製品やクリティカルな製品はより厳しい要件を満たす必要があります。適合性評価の手順は、まず自分の製品がどの分類に属しているかを理解することから始まります。

エンジニアリングチームや製品開発チームから最もよく聞かれる質問は、「これは私たちにも適用されますか？」というものです。この質問への答えには、ほぼ必ず2つの追加質問が必要です。どのような製品を開発しているのか？そして、EU市場で誰に販売しているのか？です。

CRAは一律に適用されるわけではありません。リスクに基づいた段階的なシステムを採用しており、製品がどの段階に分類されるかによって、従うべき適合性評価の手順が決まります。

### デフォルトのカテゴリ: ほとんどの製品

デフォルトカテゴリには、デジタル製品の大部分が含まれます。メモリチップ、モバイルアプリ、スマートスピーカー、コンピュータゲーム、消費者向けデバイスなどです。製品が規則の附属書IIIまたは附属書IVに記載されていない場合、またはこれらのカテゴリの技術的説明を提供する実施規則 (EU) 2025/2392 の附属書に記載されていない場合は、デフォルトカテゴリに分類されます。

デフォルト製品は自己認証が可能です。マニファクチャラーが自ら適合性評価を実施し、必要な技術文書を作成し、CEマークを貼付します。これはプロセスが簡略化されるという意味ではありません。第三者による検証が不要になるという意味です。附属書Iに記載されている義務は引き続き適用されます。

### 重要な製品: クラスIおよびクラスII

附属書IIIでは重要な製品について説明しています。これらの製品は、サイバーセキュリティリスクに基づいて2つのクラスに分類されます。

クラスIの例としては、パスワードマネージャー、スタンドアロンブラウザ、VPN、ネットワーク管理システムなどが挙げられます。これらの製品については、マニファクチャラーが整合規格を適用していれば自己認証が可能です。整合規格を使用しない場合は、認証機関による評価が必要です。

クラスIIの例としては、オペレーティングシステム、ファイアウォール、ルーター、マイクロプロセッサ、産業用制御システムソフトウェアなどが挙げられます。クラスII製品の場合、適用される規格に関わらず、認証機関による認証が常に必要となります。

欧州委員会は、重要かつ不可欠な製品カテゴリーを構成する技術的な定義を明確にするため、2025年11月に実施規則(EU) 2025/2392を公表しました。分類作業を行う際には、この文書を読む価値があります。重要な概念はコア機能です。つまり、その製品は主にどのような機能を備えているのか、そしてその機能は附属書IIIまたは附属書IVのカテゴリに該当するのか、ということです。

### クリティカルな製品

附属書IVでは、セキュアエレメント、スマートカード、スマートメーターゲートウェイ、ハードウェアセキュリティモジュールなどのクリティカルな製品について説明しています。クリティカルな製品は、すべての場合において認証機関による評価が義務付けられています。自己認証制度はありません。

## 「上市する」とはどういう意味か

CRAは、製品がEU市場に上市されたり、EU市場で利用可能になったりした時点で適用されます。これは特定の法的概念です。つまり、製品が商業活動の一環として、有償か無償かを問わず、EU市場で初めて流通または利用可能になった時点を指します。

これはSaaSおよびサービスとしてのソフトウェアモデルにとって重要です。デジタル要素を含む製品のためのリモートデータ処理機能を提供するSaaSは対象範囲に含まれます。デジタル要素を含む製品にリモートデータ処理機能を提供しない、スタンドアロンのSaaSは前文12項に基づき対象範囲外となり、CRAではなくNIS2指令の対象となります。

委員会の**FAQ**と**ガイダンス案**がこの質問への回答すべく取り組みを始めていますが、一般的な要約に頼るのではなく、組織が具体的な法的助言を求めるべき領域であることに変わりはありません。

## EU域外の企業も免除されない

CRAは、マニファクチャラーの所在地に関わらず適用されます。EUにソフトウェアを販売する米国企業は、CRAの下ではマニファクチャラーとみなされます。EU市場にハードウェアを販売する日本企業も対象です。その適用範囲は、他のEUデジタル規制と同様です。EU市場へのアクセスを望むなら、義務を受け入れる必要があります。

これは、EU域外に拠点を置き、EU域内の顧客を持つ企業にとって、実務上重要な意味を持ちます。製品の出荷前に製品の分類を決定し、適切な適合性評価を実施し、必要な文書を準備しておく必要があります。

## 分類作業は任意ではない

適切な出発点は製品の調査・把握です。各製品または製品ラインについて、分類テストを実行します。製品にはデジタル要素がありますか？EU市場で商業活動の結果として入手可能ですか？その中核機能は附属書IIIまたは附属書IVに該当しますか？

この調査と把握を行わないと、規制にどう適合すればよいのかは分かりません。そして、適合の仕方を把握していなければ、どれだけの時間があるか、あるいはどのようなリソースを割り当てるべきかを知ることができません。

まずは製品から始めましょう。適合への道筋はそこから始まります。

参考資料：製品カテゴリーに関するEC実施規則（EU）2025/2392。EC CRA適合性評価ページ：  
[digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment](https://digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment)

## 第3章：オープンソースは適用除外ではない。 CRAが実際に定めている内容とは

**要約：**コードを収益化していない個々のオープンソース貢献者は、直接的なCRAの義務を負いません。しかし、オープンソースを商業的に利用すると、それを組み込んだマニファクチャラーに義務が発生します。財団や支援団体はスチュワードに該当する場合があります、その場合はより緩やかな義務が課せられます。

CRAが最初に提案されたとき、オープンソースコミュニティは強く、そして正当な反応を示しました。初期の草案では、メンテナーが無償で公開したコードに対して法的義務を負うのかどうかについて、大きな曖昧さが生じていました。この曖昧さにより、財団、ワーキンググループ、そして個々の貢献者からの強い関心を引き起こしました。

最終稿は以前のものから改善されています。完璧ではありませんが、初期の草稿が示唆していた内容ではなく、最終稿が実際に何を述べているのかを理解することが重要です。

### 個人の貢献者に適用される基本ルール

他者のオープンソース プロジェクトに貢献したり、収益化せずに自身のコードを公開したりする場合、CRAは適用されません。これは規則に明確に記載されています。非営利のオープンソースは対象外です。 **OpenSSF CRA Brief Guide for OSS Developers** および、 **OpenSSF CRA Guide for Maintainers** でもこの点は直接的に言及しています。

商業活動とみなされるのは何か？それは、製品に対して料金を請求すること、実際のコストを回収する以上の料金で技術サポートを提供すること（ただし、サポートサービスを提供するという事実自体は、欧州委員会のガイダンスのセクション3.2.3で明確にされているように、商業活動には該当しない）、プラットフォームを通じて収益化を意図することです。さらに、セキュリティ、互換性、相互運用性以外の理由で個人データを収集すること、コストを超える寄付を受け入れることです。

上記のいずれにも該当しない場合、あなたはマニファクチャラーとしてCRAの適用範囲外となります。

### オープンソースが商用利用されるとどうなるのか

ここから事態はさらに複雑になります。マニファクチャラーがEU市場で販売する製品にオープンソースのコンポーネントを組み込む場合、そのコンポーネントに関するコンプライアンス義務はマニファクチャラーが負うことになります。CRAでは、サードパーティ製コンポーネントやオープンソースの依存関係を含め、製品全体に対する責任がマニファクチャラーに課せられています。

これは、CRAの直接的な対象とならないメンテナーにとっても、実質的な影響を及ぼします。マニファクチャラーは、使用するコンポーネントについてデューデリジェンスを実施し、脆弱性をアップストリームのメンテナーに報告することが求められます。そのため、文書化が徹底され、明確な脆弱性開示プロセスがあり、SBOMを作成しているプロジェクトがより選ばれやすくなります。これらの要件を満たさないプロジェクトは、商用ユーザーから作成を迫られることになるでしょう。

OpenSSFのChristopher Robinsonはこの点を次のように明確に指摘しています。CRAの直接的な対象とならない開発者であっても、CRAを理解しておくべきです。なぜなら、商用ユーザーはこれまで必要としていなかったドキュメント、パッチ、成果物の提供を求めるようになるからです。

## スチュワードという区分

CRAは、オープンソースソフトウェアスチュワードという新たな法的概念を導入しました。スチュワードとは、マニファクチャラーとしての役割を担うことなく、商業活動を目的としたオープンソースソフトウェアの開発を体系的かつ継続的に支援する法人のことです。

Linux Foundation、Apache Software Foundation、Eclipse Foundationといった財団は、その代表的な例です。また、組織は、あるプロジェクトではスチュワードとしての役割を担い、別のプロジェクトではマニファクチャラーとしての役割を担う、ということもできます。

スチュワードの義務はマニファクチャラーよりも軽いものの、ゼロではありません。第24条に基づく義務には、サイバーセキュリティポリシーの提供、市場監視当局との協力および要請に応じて情報の提供、実際に悪用されている脆弱性(AEV)の報告、重大なインシデントの通知、影響を受けるユーザーへの情報提供、および緩和策の提供が含まれます。

オープンソースプロジェクトにスチュワードを設ける義務はありません。プロジェクトはスチュワードなしでも運営できます。財団や組織がスチュワードとしての役割を担うことを選択した場合、その時点でも上記の義務を引き受けることになります。

## メンテナーが今すべきこと

たとえ明らかにCRAの直接的な管轄外であることが明らかであっても、今すぐ取るべき価値のある実際的な対応がいくつかあります。

まず、プロジェクトのセキュリティ対策を文書化することです。OpenSSFのOpenSource Project Security Baselineは、3つの成熟度レベルに分かれた41項目のチェックリストを提供しています。CRAがマニファクチャラーに求める要件のほとんどは、規制の対応状況に関わらず、適切なセキュリティ対策と共通しています。

次に、脆弱性開示プロセスを確立、または正式に策定してください。CRAに基づいて事業を行う商用ユーザーは、明確なセキュリティ担当者、文書化されたサイバーセキュリティポリシー、および脆弱性報告プロセスを要求します。これらが整備されていない場合、自身のコードを利用するすべての組織から寄せられる臨時の要求に対応することに時間を費やすことになります。

また、収益化の状況を正直に理解することです。商業活動かどうかの審査は、収益化の意図だけを問うものではありません。寄付金が支出額を上回っている場合、プロジェクトを中心にビジネスモデルを構築している場合は、CRAが適用される可能性があります。OpenSSFのガイドにも明記されているように、ソフトウェアを商品として収益化しようとした途端、状況は一変します。

CRAは、EUにおけるソフトウェアセキュリティの扱い方を大きく変えるものです。オープンソースコミュニティはこの変化に関与し、最終条文に影響を与えました。そして次のステップは、最終条文の内容を理解することです。

参考資料：OpenSSF CRA Brief Guide for OSS Developers ([best.openssf.org/CRA-Brief-Guide-for-OSS-Developers.html](https://best.openssf.org/CRA-Brief-Guide-for-OSS-Developers.html)). Linux Foundation CRA Stewards Playbook ([policy.openssf.org/CRA/stewards-playbook.html](https://policy.openssf.org/CRA/stewards-playbook.html)). OpenSSF Open Source Project Security Baseline ([baseline.openssf.org](https://baseline.openssf.org)).

## 第4章：セキュリティ・バイ・デザインは法的要件となったが、実際はどういうことか

**要約：**CRAの附属書Iは、デジタル要素を含む製品に求められる必須のセキュリティ要件を定めています。これらは法的義務であり、設計上の推奨事項ではありません。実際に何が求められるかを理解できるかどうか、コンプライアンスに準拠した製品と、最初の市場監視チェックに不合格となる製品との違いを生みます。

セキュリティ・バイ・デザインは、セキュリティコミュニティでは長年にわたり原則とされてきました。CRAは、これをEU市場全体で法的要件としました。これは重要な転換点です。原則であれば柔軟に解釈される可能性がありますが、法的要件は遵守しなければなりません。

附属書Iは、エンジニアリング作業の出発点となる部分です。附属書Iでは、2つの要件群が規定されています。パートIは製品自体の特性を、パートIIは脆弱性への対処方法を規定しています。これら2つを合わせることで、セキュリティの観点からCRAに準拠した製品の姿が定義されています。

### 附属書IパートIで求めていること

パートIでは、製品を上市する際に備えるべき基本的な要件を定めています。CRAでは、リスクに基づき適切なレベルのサイバーセキュリティを確保するような、製品の設計、開発、製造が義務付けられています。

リスクベースの考え方は重要です。義務はリスクに応じて求められます。たとえば、スマートサーモスタットと産業用制御システムは、全く同じ規制を受けるわけではありません。しかし、リスク評価を実施し、適切な対策を講じる義務は、どちらにも適用されます。

パートIの主な要件：

製品は、既知の悪用可能な脆弱性がない状態で出荷されなければなりません。これは厳しい要件です。悪用可能な既知のCVEを含む製品を出荷することは、初日からコンプライアンス違反となります。

製品は、安全なデフォルト設定で出荷されなければなりません。ユーザーが製品を安全にするために再設定する必要がない状態であるべきです。セキュリティは、製品購入直後から備わっているべきです。

アクセス制御は適切に実装されなければなりません。認証、ID管理、およびアクセス制御の仕組みは、製品のリスク特性に合致していなければなりません。保存・処理・送信されるデータの機密性と完全性を保護しなければなりません。

保存・処理・送信されるデータの機密性と完全性を保護しなければなりません。

アタックサーフェスは最小限に抑える必要があります。未使用のインターフェース、ポート、サービスは、デフォルト設定に含めてはいけません。

製品は、エラーを処理し、悪用可能な状況を生み出すようなクラッシュを回避するように設計されなければなりません。

## 附属書IパートIIで求めていること

パートIIでは、製品のサポート期間中の脆弱性への対応について定めています。多くの組織が、この部分における責任範囲を過小評価しがちです。

マニファクチャラーは、少なくとも最上位の依存関係を網羅する、一般的に使用される機械可読形式でソフトウェア部品表 (SBOM) の作成も含め、脆弱性とコンポーネントを特定し、文書化する必要があります。厳密には、このSBOMの義務は2027年12月まで強制力を持ちません。しかし、第1回ブログで述べたように、製品のコンポーネントをSBOMレベルで把握していなければ、2026年9月の脆弱性報告義務を果たすことはできません。

マニファクチャラーは、脆弱性報告のための明確な連絡先を含め、CVD (Coordinated Vulnerability Disclosure) プロセスを整備しなければなりません。また、脆弱性を修正し、パッチを提供する必要があります。さらに、製品のサポート期間を明示しなければならず、製品の想定ライフサイクルがそれより短い場合を除き、少なくとも5年間とする必要があります。

サポート期間の終了日は、購入時に明確に伝えなければなりません。これは透明性確保のための義務です。ユーザーは、製品のセキュリティアップデートがいつ終了するのかを知る必要があります。

## これはエンジニアリングチームにとって何を意味するのか

CRAは組織中心ではなく、製品中心の規則です。既存の情報セキュリティ管理システムは内部ガバナンスを対象としていますが、CRAでは製品レベルでのコンプライアンスの証明が求められます。これらは関連していますが、同じものではありません。

実際には、安全なソフトウェア開発ライフサイクルを実装するには、市場監視当局が審査できる成果物を作成する必要があることを意味します。脅威モデルは文書化されなければならず、リスク評価は正当性を証明できるものでなければなりません。

標準化要求M/606に基づいて策定が進められている整合規格は、CRAの適合性に関する運用上の基準となります。ENISAの規格マッピング文書は、附属書Iの要件を理解する上で有用な背景情報を提供しますが、ISO 27001やIEC 62443などの既存の規格をCRA適合性評価の根拠として扱うべきではありません。現在、これらの基準に基づいてコンプライアンス体制を構築しているマニファクチャラーは、市場監視当局がどのような根拠を採用するかが不明確であるため、後になって対応が重複するリスクを負うことになります。それらを関連証拠として扱います。M/606関連の規格の策定動向を継続的に追跡し、整合規格がまだ利用できない分野については認証機関と連携すべきです。

CRAは実施方法を規定するものではなく、成果要件を定めるものです。その目標をどのように達成するかは、設計上の判断です。これは意図的なものであり、対象となる製品の範囲を考慮すれば適切な措置です。しかし、それはつまり、自らの選択の正当性を文書化し、説明責任を果たせるようにする必要があるということです。

まずはリスク評価から始めましょう。附属書Iに記載されているその他の事項はすべて、そこから派生するものです。

参考資料: ENISA CRA Requirements Standards Mapping. EC CRA Annex I text: [eur-lex.europa.eu/eli/reg/2024/2847/oj](https://eur-lex.europa.eu/eli/reg/2024/2847/oj). OpenSSF Concise Guide for Developing More Secure Software: [best.openssf.org](https://best.openssf.org).

## 第5章：CRAに基づく脆弱性報告：実践的な解説

**要約：**2026年9月11日以降、マニファクチャラーおよびスチュワードは、実際に悪用されている脆弱性(AEV)を24時間以内にENISAに報告し、72時間以内に完全な通知を提出しなければなりません。これは、新製品だけでなく、既に市場に出回っている製品にも適用されます。脆弱性管理プロセスがこの期限に対応できないのであれば、準備が整っているとはいえません。

2026年9月11日は、ほとんどの製品セキュリティチームが、今すぐそこから逆算して準備を進めるべき日です。この日から、CRA（サイバーレジリエンス法）に基づく脆弱性およびインシデントの報告義務が適用されます。主要な規定の適用が始まる2027年12月よりも早く、多くの組織が想定する以上に幅広い製品が対象となります。

CRA第69条第3項は、この点を明確に規定しています。第14条の報告義務は、2027年12月より前の上市も含め、市場で提供されている、デジタル要素を備えたすべての製品に適用されます。2020年に出荷した製品が現在も使用されており、その製品に実際に悪用されている脆弱性(AEV)が生じた場合、2026年9月以降は報告が必要です。

### 報告の3つのステップ

CRA第14条は、3段階の通知プロセスを定めています。すべての通知は、ENISAが運営するCRA SRP (Single Reporting Platform)を通じて行います。このプラットフォームは、2026年9月までに稼働する予定です。ENISAは、現在準備を進めている組織向けに、SRPに関するFAQを公開しています。

#### ステップ1：早期警告

マニファクチャラーは、実際に悪用されている脆弱性(AEV)を認識してから24時間以内に、管轄のCSIRT（マニファクチャラーがEU域内の主たる拠点を置く加盟国の、コンピューターセキュリティインシデント対応チーム）へ早期警告を提出し、同時にENISAにも提出しなければなりません。

#### ステップ2：完全な通知

脆弱性を認識してから72時間以内に、詳細な脆弱性通知を提出しな

ければなりません。ただし、関連情報がすでに早期警告に含まれていた場合はこの限りではありません。

#### ステップ3：最終報告

実際に悪用されている脆弱性(AEV)については、是正措置または緩和措置が利用可能になってから、遅くとも14日以内に最終報告を提出しなければなりません。重大なインシデントについては、認識してから1か月以内に提出しなければなりません。

### 「実際に悪用されている」とは実際にはどういう意味か

24時間のカウントダウンは、マニファクチャラーがその事実を認識した時点で始まります。脆弱性が公表された時点でも、CVE番号が割り当てられた時点でもありません。マニファクチャラーが知った時点です。つまり、事業者内部での認識が起点となるため、マニファクチャラーには、自社製品の構成コンポーネントの状況をリアルタイムに把握する動機が生まれます。

だからこそ、SBOMは単なるコンプライアンスのための成果物ではないのです。コンポーネント単位で構成を把握できていなければ、新たに公表されたCVEが自社製品に影響するかどうかは、誰かが手作業で調査するまで分かりません。手作業による調査には数日かかります。しかし、与えられた時間は24時間です。

2026年9月より前に、SBOMに基づく脆弱性監視の仕組みを整えた組織は、新しいCVEが公表されるたびに、脆弱性データベースとの自動照合を実施できます。この仕組みを備えていない組織は、報告期限を超過するリスクに常にさらされることになります。

## 既存のCVDプロセスとの関係

CRAの報告義務は、既存のCVDプロセスに取って代わるものではなく、並行して実施されるものです。CVEの割り当て、NVDの公開、ベンダーアドバイザリの発行は従来通り継続されます。CRAは、これらに加えて、規制に基づく義務的な報告の仕組みを設けるものです。

通知は、マニファクチャラーのEU域内の主たる拠点が所在する加盟国のCSIRTに送られます。そのCSIRTは、当該製品が入手可能であると把握されている他の加盟国のCSIRTに通知を共有し、ENISAも同時にその通知を受け取ります。

ただし、例外があります。委任規則（EU）2026/881に基づき、通知を受け取ったCSIRTは、サイバーセキュリティ上の正当な理由がある場合、他のCSIRTへの共有を遅らせることができます。例えば、72時間以内に修正パッチが提供される見込みがある場合、通知の詳細が機微な情報であり、共有すること自体が悪用を可能にしかねない場合、あるいは特定のCSIRTの情報保護能力に重大な懸念がある場合です。共有を遅らせる期間は、必要な期間に厳密に限定されなければなりません。また、共有を遅らせる決定とその理由を、直ちにENISAに知らせる必要があります。当該製品が、通知を受け取ったCSIRTの所在する加盟国内でのみ入手可能な場合は、他のCSIRTへの共有は一切必要ありません。

EU域外のマニファクチャラーについては、製品のサイバーセキュリティに関する主要な意思決定がEU域内のどこで行われているかに基づいて、主たる拠点が決定されます。EU域内に拠点を持たない製造事業者は、EU域内の代理人を指定する必要が生じる場合があります。

## 中小企業に対する制裁金の免除は、その名前の通りではない

CRAには、零細企業または小企業に該当する製造事業者について、24時間以内の報告期限を守れなかった場合に制裁金を科されないとする規定があります。一部の報道では、これが小規模企業に対する全般的な適用免除であるかのように誤解されています。

しかし、そうではありません。報告義務は引き続き適用されます。免除されるのは、24時間の期限を超過したことに対する制裁金に限られ、報告そのものを怠った場合の制裁金ではありません。小規模企業も、報告できる体制を整える必要があります。初回の報告が多少遅れた場合に、制裁金から一定の保護を受けられるにすぎません。

## CRAに準拠した脆弱性開示プロセスの構築

コンプライアンスに準拠した内部プロセスを確立するには、複数の要素を連携させる必要があります。具体的には、製品ごとのSBOMの生成・維持管理、公開データベース（EUVD、NVD、OSV、CISA KEV カタログ、GitHubアドバイザリ）と照合する自動脆弱性監視、社内で最初に認識した時点を起点として24時間以内の報告対応を開始できる明確なエスカレーション経路、そしてENISAのSRPを通じて通知を提出するための検証済みの仕組みです。

CVDに対して既にPSIRTプロセスを導入している組織は、これらを整備するための基盤があります。CRAは、その基盤の上に規制報告要件を追加するものです。PSIRTプロセスを導入していない組織は、2027年ではなく今すぐCRAを導入すべきです。

参考資料：ENISA SRPに関するFAQ ([enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp](https://enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp)). CRA第14条全文 ([european-cyber-resilience-act.com/Cyber\\_Resilience\\_Act\\_Article\\_14.html](https://european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_14.html)). ECの報告義務に関するページ ([digital-strategy.ec.europa.eu/en/policies/cra-reporting](https://digital-strategy.ec.europa.eu/en/policies/cra-reporting)).

## 第6章：あなたが作ったわけではない。それでもあなたは責任を負う

要約：CRAは、マニファクチャラーだけでなく、輸入業者や販売業者にも義務を課しています。デジタル要素を含む製品をEU市場に持ち込む場合、法令遵守の責任が生じます。デューデリジェンスは任意ではなく、「マニファクチャラーから適合していると聞いていた」という説明は、免責の理由にはなりません。

流通業者や再販業者の間では、法令への適合に関する責任は製品を製造した事業者にあると一般的に考えられています。CRAは、この前提を根本から問い直すものです。

輸入業者と販売業者には、この規則に基づく独自の義務があります。その範囲はマニファクチャラーに課される義務とは異なりますが、決して軽いものではなく、デジタル要素を含む製品をEU市場で提供するすべての組織に適用されます。

### 輸入業者の役割

CRAにおける輸入業者とは、EU域内に拠点を置き、第三国からのデジタル要素を含む製品をEU市場に上市する自然人または法人を指します。

輸入業者は、製品を上市する前に、マニファクチャラーが適切な適合性評価を実施していることを確認しなければなりません。必要な技術文書が存在することを確認する必要があります。また、製品にCEマークが付されており、EU適合宣言書が添付され、必要な取扱説明書と安全情報が記載されていることを確認しなければなりません。

輸入業者は、マニファクチャラーが脆弱性対応プロセスを確立していることを確認する必要もあります。製品を輸入し、CEマークを確認した上で、マニファクチャラーが製品のサポート期間中に実際に脆弱性を修正するかどうかという問題を無視することはできません。CRAは、この点を確認することを義務付けています。

輸入業者は、製品がCRAに適合していないと考える理由がある場合、適

合が確保されるまで、その製品を上市してはなりません。また、マニファクチャラーに通知するとともに、必要に応じて市場監視当局にも通知しなければなりません。

### 販売業者の役割

販売業者とは、マニファクチャラーまたは輸入業者以外で、デジタル要素を含む製品をEU市場で提供する、サプライチェーン上の自然人または法人を指します。

販売業者は、製品を提供する前に、CEマーキングが表示され、必要な使用説明書や情報が添付されていることを確認しなければなりません。製品がCRAの必須要件に適合していないと考える理由がある場合、その製品を提供してはなりません。

販売業者は、自社が販売した製品に脆弱性があることに気づいた場合、製造元に通知しなければなりません。製品がサイバーセキュリティ上のリスクをもたらす可能性があると判断した場合は、製造元および市場監視当局に通知しなければなりません。また、リスクの排除に関して市場監視当局に協力しなければなりません。

### サプライヤー契約にとってこれは何を意味するのか

実務上、これはサプライヤーとの契約を見直す必要があることを意味します。輸入業者または販売業者とマニファクチャラーとの間の契約には、CRAの基準への準拠について明確に規定する必要があります。

サプライヤーとの契約では、少なくとも、各製品について適切な適合性評価が実施されていることの確認、技術文書および適合宣言書へのアクセス、明示されたサポート期間中に脆弱性への対応プロセスを維持することのコミットメント、ならびにマニファクチャラーが貴社に供給した製品に影響する脆弱性を認識した場合の通知義務を定めるべきです。

さらに踏み込んで、監査権、脆弱性の通知期限に関するSLA、CRAへの不適合に伴う契約上の責任条項を求める組織もあるでしょう。契約による保護の水準は、自社が受け入れるリスクの水準に見合ったものにするべきです。

## システムインテグレーターは特定の立場を占めている

複数のマニファクチャラーのコンポーネントを組み合わせ、EU市場に上市されるシステムを構築するシステムインテグレーターは、自らの役割を慎重に検討する必要があります。統合の方法や最終製品の販売形態によっては、インテグレーターがCRA上のマニファクチャラーに該当する可能性があります。

コンポーネントを組み合わせ、ソリューションを構築し、それを製品として販売する場合、貴社はマニファクチャラーに該当する可能性が高いといえます。CRAは、個々のコンポーネントの適合性に依拠するだけでなく、統合したシステム全体の適合性評価を実施することを求めています。

これは、貴社の製品とビジネスモデルに特化した法的助言が不可欠な分野です。一般原則として、製品を上市した企業がその製品に対する責任を負います。

## まとめ

CRAはサプライチェーン全体における責任の所在を再調整するものです。これは意図的な措置です。これまで、デジタル要素を含む製品は、セキュリティに関する十分な文書がなく、明確な脆弱性対応に関するコミットメントもないまま、EU市場への参入が認められてきました。CRAは、サプライチェーン上のすべての経済事業者に義務を課すことで、そのギャップを解消します。

デジタル製品を輸入または販売している場合は、今すぐサプライヤーに対するデューデリジェンスを開始してください。サプライヤーとの契約再交渉期間を考慮すると、2027年12月という期限は、一見して感じるよりも差し迫っています。

## 第7章：CRAに基づく適合性評価：実際のプロセス内容

**要約：**ほとんどの製品はCRAの下で自己認証が可能です。クラスIの重要な製品も、整合規格が適用されれば自己認証が可能です。クラスIIの重要な製品およびすべてのクリティカルな製品は、認証機関による認証が必要です。整合規格は現在も開発中です。そのため、どの適合性評価手段を選択するかについて、即座に判断を下す必要が生じます。

ソフトウェアへのCEマーキングは、CRAが導入する最も重要な構造的変更の一つです。EU製品法の歴史の大半において、ソフトウェアにはCEマークが付されていませんでした。CRAはこの状況を変えます。そして、CEマーキングの導入に伴い、適合性評価プロセスが導入されます。

自社製品カテゴリーにおける認証手段を理解することは、コンプライアンスチームが最初に行うべき実務的な決定事項の一つです。

### 3つの適合経路

**デフォルト製品：**ほとんどのハードウェアおよびソフトウェアは、デフォルトカテゴリに分類されます。これらの製品はモジュールA（内部適合性評価）を使用し、マニファクチャラーが自社製品を附属書Iの要件に照らして評価し、技術文書を作成し、EU適合宣言書を作成し、CEマークを貼付します。認証機関は必要ありません。

**重要な製品 クラスI：**これには、パスワードマネージャー、スタンドアロンブラウザ、VPN、ネットワーク管理システムなどが含まれます。クラスI製品は、欧州の整合規格を適用している場合、モジュールAを使用できます。整合規格を使用しない場合は、モジュールB+C（EU型式審査と型式適合性試験）またはモジュールH（完全な品質保証システム評価）のいずれかを使用して、認証機関による審査を受ける必要があります。CRAの整合規格は欧州標準化機関によってまだ開発中であるため、多くのクラスIメーカーは最初の認証サイクルでは、認証機関を経由する必要があります。

**重要な製品 クラスIIおよびクリティカルな製品：**クラスIIには、オペレーティングシステム、ファイアウォール、ルーター、マイクロプロセッサが含まれます。附属書IVの重要な製品には、セキュアエレメント、スマートカード、スマートメーターゲートウェイが含まれます。どちらの製品も、適用される規格に関わらず、常に認証機関による認証が必要です。認証機関による評価は、モジュールB+CまたはモジュールHのいずれかに従って行われます。モジュールB+Cは製品レベルの型式検査を含み、安定した製品ラインに適しています。モジュールHは、完全な品質保証システム監査に基づいており、製造業者が複数の製品を扱っている場合や頻繁にアップデートを行う場合に、より柔軟に対応できます。これは、完全な型式検査を繰り返すよりも、対象範囲に新製品を追加する方が効率的であるためです。

### 認証機関の役割とは

適合性評価認証機関とは、一般的に製品の試験および認証を行う民間企業を指します。CRA（適合性評価協定）の下では、認証機関として活動するためには、設立された加盟国による評価、指定、通知、および監視を受ける必要があります。

CRAに基づく認証機関の枠組みは、2026年6月11日まで運用開始されません。加盟国は、2026年12月までに十分な数の認証機関が確保されるよう努めることが求められています。これはかなり厳しい期限です。認証機関による評価が必要な製品を扱う組織は、需要が供給を上回る前に、今すぐに潜在的な認証機関を特定しておくべきです。

CRAには、EUのサイバーセキュリティ認証制度に基づいて認証された製品は、認証機関の関与を必要としないという規定もあり、その具体的な条件は欧州委員会が定めることになっています。EUCC（共通基準に基づく欧州サイバーセキュリティ認証制度）は、高信頼性製品にとって最も関連性の高い既存の制度です。

## 技術文書の要件

内部評価を利用する場合でも、認証機関を利用する場合でも、技術ファイルが必要です。CRAは、附属書VIIにその内容を規定しています。これには、製品の説明と使用目的、適用された整合規格またはその他の規格のリスト、サイバーセキュリティリスク評価、設計および製造プロセスと監視手順の説明、EU適合宣言、および脆弱性処理の記録が含まれます。

この文書は、製品が上市されてから少なくとも10年間、またはサポート期間がそれより長い場合はその期間中、保管し、市場監視当局が閲覧できるようにしておかなければなりません。

## 整合規格とその現状

整合規格とは、適用することでCRA要件への適合が推定される技術仕様のことです。ETSI、CEN、CENELECによって開発が進められています。2026年半ばの時点で、最初の草案が出始めています。しかし、CRAの附属書Iの要件を完全に網羅した整合規格はまだ存在しません。

これは、クラスI認証取得を目指すマニュファクチャラーにとって実際的な問題です。参照できる整合規格がないため、モジュールB+CまたはモジュールHの評価を受けるには、認証機関に依頼する必要があります。

ISO 27001、IEC 62443、NISTフレームワークなどの既存の規格は代替となるものではありません。これらの規格と、欧州委員会の指令M/606に基づいて開発されているCRA固有の規格との間には正式なギャップ分析が行われていないため、これらの既存規格を根拠として適合性の推定を主張するために使用することはできません。

標準化要求M/606に基づいて策定されている整合規格は、CRA適合性評価の運用上の基準となります。ENISA規格マッピング文書は、附属書Iの要件を理解する上で有用な背景情報を提供しますが、ISO 27001やIEC 62443などの既存規格は、CRAに基づく適合性評価の基準とはならず、そのように扱うべきではありません。

これらの基準に基づいてコンプライアンスプログラムを構築しているマニュファクチャラーは、市場監視当局がそれらに関連性のあるものとして扱うかどうか不明確であるため、作業の重複のリスクを負うことになります。実務的な方法は、標準化要求M/606に基づいて策定される整合規格の策定状況を追跡し、整合規格がまだ入手できない場合は認証機関と連携することです。

参考資料：EC CRA適合性評価ページ ([digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment](https://digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment))。

BSI CRAガイダンス ([bsi.bund.de](https://bsi.bund.de))。ENISA規格マッピング。認証機関向けのEU NANDOデータベース (CRAエントリが利用可能になり次第)。

## 第8章：CRAが優れた調達のある方を変える

**要約：**CRAは、セキュリティに関する責任を生産者側にシフトさせるものです。その結果、購入者はEU域内で販売される製品に対するより強力な基本保証の恩恵を受けます。しかし、これらの保証は、調達プロセスが更新され、適合性を確認し、ベンダーに適切な質問を行う場合にのみ有効です。

CRAのあまり知られていない効果の一つは、購入者側への影響です。規制の義務の大部分は、生産者、輸入業者、販売業者に課せられています。しかし、規制全体の枠組みは、デジタル製品を利用する個人や組織のセキュリティを向上させることを中心に構築されています。購入者はこの枠組みを調達ツールとして活用できます。

CRAは、商用ソフトウェアやハードウェアを購入する企業購買担当者に対し、直接的な法的義務を課すものではありません。しかし、責任ある調達のあり方を変えるものです。

### 調達シグナルとしてのCEマーキング

2027年12月以降、EU市場で販売されるデジタル要素を含む製品には、CRAの必須要件への適合を証明するCEマークの表示が義務付けられます。このマークは、適合宣言書および技術文書によって裏付けられており、マニファクチャラーが必要なリスク評価を実施し、附属書Iの要件に対応し、宣言されたサポート期間中、脆弱性対策を維持することを約束したことを示すものです。

実際には、CEマーキングだけでは調達基準として十分ではありません。ほとんどの製品の適合性評価は自己申告です。適合宣言は、製品が要求事項を満たしているというマニファクチャラーの声明であり、独立した監査結果ではありません。特にNIS2やDORAの対象となるような高信頼性環境においては、購入者はCEマークの確認だけでなく、基礎となる技術文書や、使用された適合性評価の手順も確認すべきです。

### ベンダーに尋ねるべき質問

CRAの下での効果的な調達とは、2024年12月以前には通常回答が求められていなかった質問をベンダーに投げかけることを意味します。有用な質問には以下のようなものがあります。

この製品は、デフォルト、クラスI、クラスIIのどの製品カテゴリーに該当しますか？クラスIまたはクラスIIの場合、どのような適合性評価が採用され、どの認証機関を利用しましたか？

宣言されたサポート期間はいつで、いつ終了するのでしょうか？これはCRAに基づき、購入時点で明示されなければなりません。販売業者がこれを明確に回答できない場合、それ自体が法令遵守違反の兆候となります。

貴社におけるCVD(Coordinated Vulnerability Disclosure)プロセスとはどのようなものですか？セキュリティ担当者の連絡先はどこに公開されていますか？脆弱性の認識からパッチの提供開始までの平均所要時間はどれくらいですか？

この製品のSBOMは作成していますか？どのフォーマットで作成していますか？それらは顧客が利用できますか？

2026年9月の脆弱性報告義務をどのように履行しますか？脆弱性が発生してから24時間以内に、実際に悪用されている脆弱性(AEV)を検出できる監視インフラは整備されていますか？

これらは特別に珍しい質問ではありません。これらは、CRAが市場全体にわたって確立しようとしている注意義務の基準です。ベンダー評価プロセスにおいてこれらの質問を日常的に行う組織は、質問票に基づく自己申告のみに依存する組織よりも、より有利な立場に置かれるでしょう。

## サプライヤー契約の更新

調達契約には、CRAの義務を反映させる必要があります。少なくとも、契約には、EU市場で販売される製品がCRAに適合していること、サポート期間中に脆弱性対応を維持することのコミットメント、購入した製品で実際に悪用されている脆弱性(AEV)が発見された場合に購入者へ通知すること、そして要求に応じて技術文書へのアクセスを提供することを盛り込むべきです。

より成熟した調達フレームワークでは、脆弱性通知の期限に関するSLA、脆弱性対応プロセスに対する監査権、ならびにセキュリティインシデントにつながったCRA不適合に関連する契約上の責任条項が追加されることになります。

明確にしておくべき点が一つあります。オープンソースプロジェクトは、契約上の意味においてはサプライヤーではありません。オープンソースコンポーネントを統合するマニファクチャラーは、そのコンポーネントに関するCRAへの適合義務を自ら負います。デューデリジェンスの義務はマニファクチャラーに向けられるものであり、上流のオープンソースプロジェクトに向けられるものではありません。

オープンソースのメンテナーに対して契約上のCRA義務を負わせようとするのは、この規則を誤って解釈しているものであり、標準化に関する初期の議論で表面化した誤解を反映しています。CRAは、コンポーネントの出所にかかわらず、マニファクチャラーが出荷する製品について責任を負うことを明確にしています。

参考資料：EC CRAの概要 ([digital-strategy.ec.europa.eu/en/policies/cra-summary](https://digital-strategy.ec.europa.eu/en/policies/cra-summary))。CRA要件に関するENISAガイダンス。

DORAおよびNIS2サプライチェーンセキュリティ交差点におけるガイダンスに関する規定。

## 公共部門に関する考慮事項

公共部門の組織は、NIS2の下で重要または中核的な事業体として追加の義務を負うことがよくあります。NIS2のサプライチェーンセキュリティ要件とCRAの製品適合性が交差することで、公共部門の購入者は、調達プロセスを更新するための規制上の推進要因を二重に持つ状況になります。

CRAの透明性要件、公開された適合宣言書、明示されたサポート期間、文書化された脆弱性対応プロセスは、検証可能な情報の基盤を形成しており、公共部門の調達においては、これらを入札評価基準に組み込むことができ、また組み込むべきです。

CRAは、EUのデジタル市場の安全性を高めるために策定されました。その真のメリットは、消費者が規制で義務付けられている生産者が公開すべき情報を活用することによってのみ実現されます。今すぐ活用を始めましょう。

## 第9章：小規模チームのためのCRAコンプライアンス： 法務部門がない場合、どこから始めるべきか

**要約：**CRAは中小企業向けに特別な規定を設けていますが、義務を免除するものではありません。あくまでも障壁を軽減するものです。小規模なチームは、優先順位を明確にする必要があります。まず製品を分類し、どの適合性評価ルートに該当するかを理解し、2027年12月までに最低限必要な文書一式を整備することが重要です。

コンプライアンス遵守が容易だとは言いません。製品を出荷しようとしている3人チームにとって、CRAは確かに大きな負担となります。規制自体もこの点を認識しており、CRA第33条では、零細企業、中小企業、スタートアップ企業に対する支援策を具体的に規定しています。

しかし、負担を認識することと、それを取り除くことは別物です。義務は依然として存在します。違いは、中小企業はそれらの義務をいかに乗り越えるかにおいて構造的な優位性を持っていること、そしてその障壁を下げるために特別に設計されたリソースが存在することです。

### 中小企業向け規定の実際の内容

24時間以内の脆弱性報告期限を過ぎてしまった零細企業や小規模企業は、その特定の違反行為に対して罰金を科されることはありません。ただし、報告義務自体は依然として有効です。この免除は限定的なものであり、24時間以内の報告期限を過ぎたことに対する罰則のみを対象とし、報告義務そのものに対する罰則は適用されません。

認証機関の手数料体系は、組織の規模を考慮に入れる必要があります。製品が第三者による適合性評価を必要とする場合、認証機関は手数料を設定する際に、零細企業を含む事業体の規模を考慮しなければなりません。

加盟国は、中小企業が規制を遵守できるよう、規制サンドボックスやテスト環境を提供することが求められています。SECUREプロジェクト（EU中小企業のサイバーレジリエンス強化）は、特に中小企業がCRA（企業規制法）の遵守に取り組む際に、財政支援とガイダンスを提供します。

委員会は2025年12月に**技術的なFAQ**を、2026年3月には**ガイダンス草案**を公開した。このガイダンス案は、特に零細企業と中小企業に焦点を当てています。ガイダンス案では、適用範囲、リモートデータ処理、FOSS（フリーオープンソースソフトウェア）の取り扱い、サポート期間、および他のEU法との相互作用について取り上げています。まだ最終版ではなく、法的拘束力はありませんが、欧州委員会の最新の解釈方針を示すものであり、今すぐ読む価値があります。

### 最優先事項：製品を分類する

すべては製品分類から始まります。あなたの製品は、デフォルトカテゴリ、クラスI、それともクラスIIのどれに該当しますか？この分類一つで、適合性への道筋が決まります。

ほとんどのスタートアップ企業やインディーズ開発者にとって、製品はデフォルトカテゴリに分類されます。デフォルト製品は自己認証が可能です。つまり、体系的に取り組めば、管理しやすいプロセスとなるということです。

製品がネットワークインターフェースを使用する場合や認証を処理する場合、またはサイバーセキュリティ機能に関連する場合は、付録IIIをよく確認してください。

例えば、パスワードマネージャーはクラスIに分類されます。パスワードマネージャーを開発するスタートアップ企業は、整合規格を適用しない場合、認証機関の承認を得る必要があります。

## 最低限必要となるドキュメントセット

デフォルトカテゴリの製品の場合、CRA準拠に必要な最低限のドキュメントは以下の通りです。

まず、製品のサイバーセキュリティリスク評価があります。詳細なものである必要はありませんが、文書化され、正当性が証明され、製品が実際にもたらすリスクに見合ったものでなければなりません。

次に、附属書IパートIの要件が満たされていることを示す証拠です。これには、製品特性（デフォルトで安全であること、リリース時点で既知の悪用可能な脆弱性がないこと、攻撃対象領域が最小限であること、適切なアクセス制御、データ保護）が含まれます。

他にも、製品に組み込まれているサードパーティ製およびオープンソースのコンポーネントに関するデューデリジェンスレポートがあります。CRAは、マニファクチャラーに対し、出荷するコンポーネントについてデューデリジェンスを実施することを義務付けています。この義務の履行状況は文書化する必要があります。

また、ソフトウェア部品表、または少なくとも既知の脆弱性を追跡するために使用できるコンポーネント一覧も必要です。正式なSBOM要件は附属書IパートIIに規定されており、2027年12月から施行されます。ただし、2026年9月の脆弱性報告義務への対応には、コンポーネントの可視性が必要となります。

脆弱性開示ポリシーとセキュリティ担当者連絡先についても公開する必

要があります。自社のウェブサイトに掲載してください。

適合宣言書は、製品がCRAの要件を満たしていることを正式に表明するものです。書式は附属書Vに規定されています。

製品のサポート期間も必要です。これは、購入時に明示されます。

## 障壁を軽減する無料リソース

Linux Foundationは、無料の短期集中講座「LFEL1001: Understanding the EU Cyber Resilience Act (CRA)」を**提供しています**。基礎知識を網羅しており、デジタルバッジが付与されます。コンプライアンスに関する決定を下す前に、必ずこのコースを修了してください。

OpenSSFの“**Open Source Project Security Baseline**”は、CRAが義務付けようとしているセキュリティ対策を網羅した41項目のチェックリストを提供します。このBaselineを満たしていれば、AnnexIへの適合について、説明可能な形で整理するためのかなりの部分をカバーできます。

The **OpenSSF CRA Brief Guide for OSS Developers**は、個人開発者や小規模チーム向けに特化して書かれています。専門用語を使わずに、内容の範囲を明確に説明しています。CRAは、小規模チームをEU市場から排除することを目的としたものではありません。これは、すべての製品におけるセキュリティの基準値を引き上げることを目的としています。

本当にセキュアな製品を開発する小規模チームにとって、ドキュメント作成の負担は確かに大きいものですが、達成可能な範囲です。まずはリスク評価から始め、附属文書Iのチェックリストに沿って作業を進め、脆弱性開示ポリシーを公開しましょう。これが基礎となります。そこから構築を進めてください。

リソース: 無料の LF コース LFEL1001。OpenSSF セキュリティ ベースライン (baseline.openssf.org)。中小企業向け SECURE プロジェクト (secure4sme.eu)。EC 中小企業向けガイダンス草案 (デジタル - を参照) (strategy.ec.europa.eu に掲載)。EC 第 33 条の支援措置。

## 第10章：CRAは単独で存在するものではない： EUデジタル主権フレームワークに位置付けられている

**要約：**CRAは、より広範なEU規制体系の一部です。NIS2、AI法、データ保護法、DORAと関連しており、コンプライアンス上の重複と戦略的な機会の両方を生み出しています。これらの関連性を理解することで、CRAコンプライアンスへの投資に対する考え方が変わります。

多くの組織は、CRAを単独のコンプライアンス業務として扱っています。それは理解できます。規制は膨大で、期限も厳しいからです。しかし、CRAを単独で扱うということは、複数の規制枠組みにわたって作業が重複する可能性が高く、複数の規制義務に対応できるコンプライアンス能力を構築する機会を逃すことになります。

CRAは、必ずしも完全に整合しているとは言えないものの、一貫性のあるEUのデジタル規制体系の中に位置づけられています。他の枠組みとの関連性を理解することが、コンプライアンスへの投資を効率化するための鍵となります。

### CRAとNIS2

NIS2（指令（EU）2022/2555）は、重要かつ不可欠な事業体の組織的レジリエンスに焦点を当てています。組織レベルでのリスク管理、インシデント報告、サプライチェーンセキュリティ、および事業継続対策を要求しています。CRAは製品セキュリティに焦点を当てています。これらは、関連する義務の製品中心型と組織中心型のバージョンです。

関連性はサプライチェーンセキュリティです。NIS2は、重要かつ不可欠な事業体に対し、サプライヤーのサイバーセキュリティ対策や調達する製品・サービスのセキュリティ特性を含め、サプライチェーンのセキュリティを評価することを義務付けています。CRAは、検証可能な製品の枠組みを構築します。

具体的には、セキュリティ情報：適合性評価、適合宣言書、SBOM、脆弱性対応に関するコミットメントが含まれます。

これにより、NIS2の義務を負う組織は、評価に使用できる具体的で標準化された成果物を得ることができます。NIS2のサプライチェーンセキュリティ要件の対象となる組織は、アンケートに基づく自己申告だけに頼るのではなく、CRAへの準拠をサプライヤー評価プロセスの構造化された検証可能な要素として活用できます。

組織としては、事業体としてNIS2の適用を受け、製造業者としてはCRAの適用を受ける場合、ガバナンス、リスク評価、およびインシデント対応のプロセスは、並行して運用するのではなく、両方の枠組みに対応するように設計することができます。

### CRAとAI法

CRA第12条は、EU AI法との明確な関連性を規定しています。デジタル要素を含む製品がAI法の下で高リスクなAIシステムにも該当する場合、CRAの製品要件および附属書IIに記載されている脆弱性処理プロセスへの準拠は、第15条に基づくAI法のサイバーセキュリティ要件への準拠を証明するために利用できます。

これは実際の効率化に繋がります。AI法の下で高リスクなAIシステムに該当し、かつCRAの対象にもなるAI製品を開発する組織は、セキュリテ

ィと脆弱性管理プロセスを一度実行すれば、それを両方の規制目的に利用できます。

ただし、両者の関係は複雑です。CRAにおいて重要またはクリティカルとみなされる製品には、サイバーセキュリティ面に関してAI法（人工知能法）の内部統制規定よりも優先される独自の適合性評価要件が適用されます。両フレームワークは関連しているものの、完全に統合されているわけではありません。

## CRAとDORA

DORA（Digital Operational Resilience Act）は、金融機関およびそのICTサービスプロバイダーに適用されます。NIS2と同様に組織中心の法律ですが、ICTにおける第三者リスク管理に関する具体的な規定が含まれています。

DORAのICT第三者リスク管理要件は、デジタル製品およびサービスの供給業者に対するデューデリジェンス義務を定めています。CRAへの準拠は、そのデューデリジェンスにおける重要な要素です。

DORAの対象となる金融機関と、CRAに対応するための技術サプライヤーは、相互運用可能なコンプライアンス文書の構築において利害が一致します。

## CRAとデータ法

データ保護法（規則（EU）2023/2854）は、コネクテッド製品および関連サービスに適用されます。デジタル要素を含む製品は、データ保護法の下でコネクテッド製品として同時に該当する場合があります。両方の規制が適用される場合、マニファクチャラーはデータへのアクセス、文書化、およびユーザーへの透明性に関して重複する義務を負うことになります。

委員会はこの重複を認識しています。データ保護法の義務を最初から考慮に入れたCRAコンプライアンスプログラムは、それらを別々の作業の流れとして扱うプログラムよりも効率的です。

## 戦略的な見方

CRA、NIS2、AI法、DORA、データ法は、EUデジタル市場全体にわたるセキュリティと透明性の基本基準を確立するための、より広範な取り組みの一環です。それぞれが、安全性の低い製品、安全性の低い組織、安全性の低いAIシステム、運用上の脆弱性を抱える金融インフラ、不透明なデータ処理といった、異なる障害モードに対処しています。これは関連するEUデジタル法のすべてを網羅したリストではありませんが、CRAコンプライアンスに取り組む組織にとって、重複する義務を生み出す可能性が最も高い枠組みです。

CRAの施行期限は2027年12月です。NIS2 2024年10月から施行されています。AI法は2024年から2027年にかけて段階的に適用されます。DORAは2025年1月から金融機関に適用されています。

コンプライアンスプログラムを構築している組織は、複数のフレームワークに対応できるガバナンス、リスク管理、および文書化のインフラストラクチャを設計する絶好の機会を得ています。各期限が迫ってからでは不十分なまま、断片的なプログラムを構築することになり、コストがかさむ上に得られる効果も少なくなります。

CRAはEUのデジタル規制構築の最終段階ではなく、その第一歩に過ぎません。これを一度限りのコンプライアンス対応と捉える組織は、この作業を繰り返すことになるでしょう。しかし、今から持続的な能力を構築する組織は、そうする必要はありません。

## 参加しよう

オープンソースソフトウェアに関する規制環境は急速に変化しています。OpenSSFの[ポリシーページ](#)にアクセスして最新情報を入手してください。資料や最新情報については、こちらをご覧ください。戦略策定にご協力いただける方は、[グローバルサイバーポリシーワーキンググループにご参加ください](#)。この重要な使命に、皆様の専門知識をご提供いただくことを心よりお待ちしております。

## 著者について



**Sal Kimmich氏**は、オープンソースガバナンス、ソフトウェアサプライチェーンセキュリティ、プライバシー強化技術の交差点で活躍する開発者アドボケート兼セキュリティエンジニアです。Open Source Security FoundationのEducation SIG、BEAR WGのコントリビューターを務め、CHAOSSデータサイエンスWGの共同議長も務めています。国際的なオープンソースコミュニティリーダーとして、包括的な道筋の構築に貢献しており、初めて貢献する開発者のメンターを務め、ヨーロッパ、イギリス、北米におけるセキュアな開発プラクティスに関するポリシー策定にも携わっています。日中は、エージェント型AIシステムの最新脅威モデルのギャップを埋める作業に励み、余暇には次世代の優秀なエンジニアを育成し、オープンソースセキュリティ分野での活躍を支援しています。

参考資料：EC CRA政策ページ ([digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act](https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act))。NIS2指令 (EU) 2022/2555。  
EU AI法令規則 (EU) 2024/1689。デジタル運用レジリエンス法 (EU) 2022/2554。データ法 (EU) 2023/2854。

# 対訳表

| 和訳                                         | 英文                                                                          | 備考・説明                                                      |
|--------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------|
| マニファクチャラー                                  | manufacturer                                                                | CRA定義上のmanufacturerであることを明示するため、一般用語の製造業者と訳さずマニファクチャラーと訳した |
| サプライヤー                                     | supplier                                                                    |                                                            |
| 輸入業者                                       | importer                                                                    |                                                            |
| 販売業者                                       | distributor                                                                 |                                                            |
| 生産者                                        | producers                                                                   | CRA原文には定義がないため、一般用語の生産者と訳した                                |
| スチュワード                                     | steward                                                                     | CRA定義上のstewardであることを明示するため、一般用語の管理者と訳さずスチュワードと訳した          |
| 上市                                         | ‘placing on the market’ ‘placed on the market’<br>‘placed on the EU market’ | CRA定義上のplacing on the marketであることを明示するため、上市と訳した            |
| 重要な製品 クラスI                                 | important products ClassI                                                   | CRA定義上でのカテゴリ分類名                                            |
| 重要な製品 クラスII                                | important products ClassII                                                  | CRA定義上でのカテゴリ分類名                                            |
| クリティカルな製品                                  | critical products                                                           | CRA定義上でのカテゴリ分類名                                            |
| 整合規格                                       | harmonized standards                                                        | CRA要件への適合が推定される技術仕様<br>標準化団体(ETSI、CEN、CENELEC)によって策定       |
| 指令                                         | directive                                                                   |                                                            |
| 標準化要求                                      | mandate                                                                     | 欧州委員会が標準化団体（ETSI、CEN、CENELEC）に対して規格策定を依頼する文書               |
| 適合性評価手順、適合性評価方法                            | conformity pathway                                                          | CRA原文ではConformity assessment proceduerと表記されている             |
| SRP (Single Reporting Platform)            | Single Reporting Platform                                                   | 固有名詞のためSRPと表記                                              |
| 実際に悪用されている脆弱性(AEV)                         | actively exploited vulnerability                                            | CRA関連のドキュメントでAEVと略される事が多いので和訳に加えAEVも併記                     |
| 脆弱性対応に関するコミットメント                           | vulnerability handling commitments                                          |                                                            |
| CVD (Coordinated Vulnerability Disclosure) | coordinated vulnerability disclosure                                        | 協調的脆弱性開示。CVDと略される事が多いのでCVDと表記                              |
| 附属書                                        | Annex                                                                       |                                                            |

この資料は、OpenSSF 発行の「**Built to Last: Understanding the European Cyber Resilience Act (CRA)**」を OpenSSF Japan Working Group 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 Working Group 翻訳チーム

- ・余保 東（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）
- ・高橋 明彦（富士通）
- ・池田 宗広（サイバートラスト）



[openssf.org](https://openssf.org)