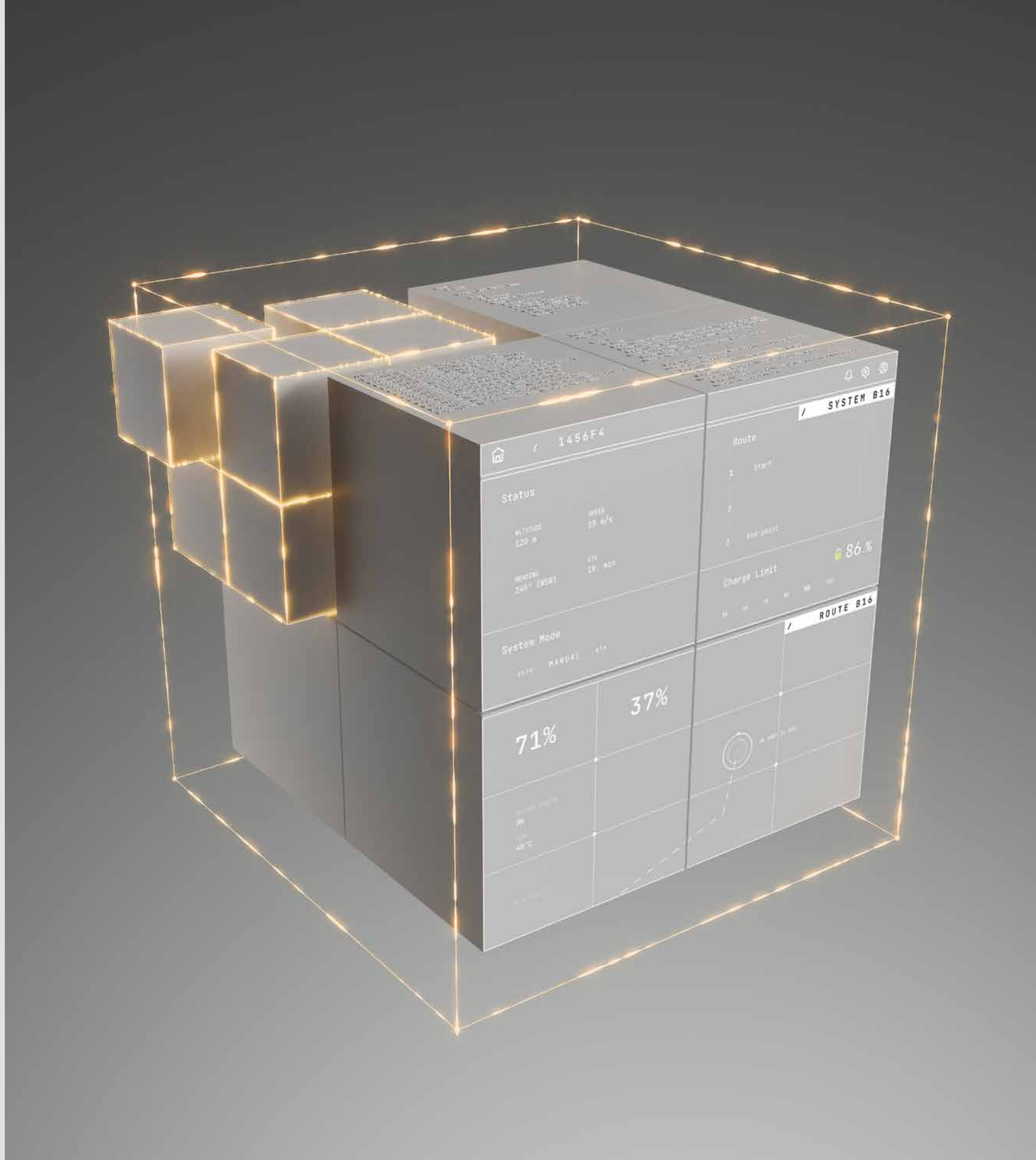
Qt Group

# EUサイバーレジリエンス法

CRA 対応、今こそ準備を加速するとき

2025



Qt Group

第 1 章

# CRA - 共通ルールの整備へ

EUサイバーレジリエンス法（CRA）は、今後のデジタル要素を含む製品の開発方法に大きな影響を与える新たな規制です。

現在、セキュリティ脆弱性による損害は年間で数千億ユーロ規模にのぼると言われています。CRAは、こうした損害の発生を抑えるための仕組みであり、製造者自身を守るとともに、製品のエンドユーザーにとっても安全な世界を実現することを目指しています。

Qt Groupは、厳格な規制環境下にある産業分野で長年培った経験を活かし、CRAを共通の土台を築く重要な動きと捉えています。これまで、サイバーセキュリティ対策は企業ごとの努力に委ねられる部分が多くありましたが、CRAの登場により、すべての製品に共通するセキュリティ要件の土台が整いつつあります。
EUサイバーセキュリティ法やNIS-2指令といった既存の規制で一部カバーされていた領域もありますが、CRAはさらにその上に、すべてのデジタル要素を持つ製品・デバイスを対象とした包括的なセキュリティ対策を求めています。

本ビジョンペーパーでは、Qt Groupがデジタル要素を含む製品の製造者にとってのCRAの影響を整理し、CRA要件への対応を競争優位へとつなげるための戦略的ロードマップを提示します。

## 異なる視点から見るCRA

新しい法規制の導入にはつきものですが、CRAについても一部では懸念の声が上がっています。

「なぜまた新しい規制が?」「開発のスピードが落ちるのでは?」

こうした声は珍しくありません。これまで、多くの組織では新製品の市場投入を急ぎ、その後に脆弱性対策を“後追い”で行う、あるいは行わないままというケースも少なくありませんでした。CRAは、そうした状況を根本から変えるものです。

しかし、開発が遅くなることは本当に悪いことなのでしょうか?

CRAが求めているのは、製造者がサイバーセキュリティ全体に責任を持つという姿勢です。これは、「短期的な市場投入の速さ」から、「長期的な安全性と信頼性」へとマインドセットを変えることを意味します。スピードの問題にとらわれすぎるのではなく、セキュリティを軸にプロセスや組織体制そのものを進化させることが、企業全体のレベルアップにもつながるという観点で捉えることが重要です。

CRAの導入は、製造者にとって競争優位性を築くためのチャンスにもなり得るのです。

Qt Group

**「CRAは、製品をEU市場で販売するための最低限の基準を定めています。これを満たせなければ、市場に参入することすらできません。”信頼できるベンダー”とみなされるための前提条件なのです。」**

- Öykü Işık 氏, IMDビジネススクール デジタル戦略およびサイバーセキュリティ担当教授

第 2 章

# EUサイバーレジリエンス法（CRA）とは？

CRAは、欧州連合（EU）の規制枠組みに加わった最新の法令です。EU市場で販売されるすべてのデジタル要素を備えた製品（PDE）に対して、そのライフサイクル全体にわたるセキュリティとサイバー脅威への耐性を確保することを目的とした包括的な法規制です。

PDEとは、産業用センサーから家庭用電子機器、組み込みUIまで、デジタルコンポーネントを含むハードウェアおよびソフトウェア製品を指します。CRAは、こうした製品の製造業者すべてに共通して適用される基準を定めています。ただし、すでに同様の規制が存在する医療、自動車、航空といった産業については、CRAの対象外となる場合が多くなっています。

CRAは指令ではなく規則であるため、各国での個別な立法手続きを経ることなく直接的に法的拘束力を持つ点が特徴です。すでに存在するEUサイバーセキュリティ法や、クラウド基盤（SaaSなど）のサイバーセキュリティに焦点を当てたNIS-2指令と補完的な関係にあります。一定の重複はありますが、CRAはこれまで十分にカバーされてこなかった「製品そのもの」を対象とする新たな規制です。

「CRAは“セキュア・バイ・デザイン”な製品を求める規則であり、NIS-2指令は組織としてのレジリエンスを求めるものです。両者は補完し合う関係にあります。」

- Öykü Işık 氏, IMDビジネススクール デジタル戦略およびサイバーセキュリティ担当教授

CRAは2024年12月10日に発効しましたが、製造業者などの関係者には、段階的に準備を進め規制に対応するための3年間の猶予期間が設けられています。
現在、重要な2つの実施マイルストーンが間近に迫っています：

### 2026 年 9 月 11 日

深刻なサイバーセキュリティインシデントや悪用された脆弱性に関する報告義務が適用開始となります。これは、新たに市場に投入される製品だけでなく、すでにEU市場に出回っているすべての製品が対象となります。


### 2027 年 12 月 11 日

すべてのCRAの基本要件が、新たにEU市場に投入される製品に対して適用されます。これには、設計段階から製品ライフサイクル全体にわたるセキュリティの確保、適合性評価の実施、および必要な技術文書の提供などが含まれます。

期限が迫る中、製造業者には、セキュリティリスクの分析、開発・報告プロセスの見直し、製品ライフサイクル全体にわたるセキュリティアップデート体制の構築が求められています。対応を怠れば、最大で1,500万ユーロまたは全世界年間売上高の2.5%という多額の罰金が科される可能性があるほか、EU市場へのアクセスを失うリスクもあります。

「CRAの最大の利点は、製品を開発するすべての企業に共通の基準を設けたことです。これまでは、セキュリティ対応は企業ごとの個別対応に頼っていました。CRAがなければ、セキュリティは今でも“後回し”になっていた企業もあったはずです。しかし今では、すべての企業が同じ要件や認証基準に従う必要があります。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター

第 3 章

# セキュリティ・バイ・デザインの時代が始まる

CRAは、セキュリティ対策を製品開発のごく初期段階から考慮することを明確に求めています。既知の悪用可能な脆弱性が存在する製品は、EU市場で販売することができません。

知っておくべき重要ポイント：

**サイバーセキュリティリスクの評価**

製造業者は、自社製品ごとにサイバーセキュリティ評価を実施する必要があります。評価では、製品の意図された使用方法や誤使用の可能性、データの取り扱い、インシデント発生時のリスクや影響などを検討します。その結果をもとに、製造業者はリスクを事前にコントロールするための対策を講じる必要があります。

「アイデアをいち早く市場に出すか、それともリスクを最小限に抑えるために開発を急がないという選択をするか。そのどちらかを選ぶ必要があります。自分たちの価値観と、何を生み出しているのかを明確に意識し、『最初から正しくやろう』と判断することが重要です。たとえば、設計段階からセキュリティエンジニアを関与させるといったことです。」

- Öykü Işık 氏, IMDビジネススクール デジタル戦略およびサイバーセキュリティ担当教授

「実は、これによってイテレーションのスピードが上がるのです。製品開発サイクルの中に“セキュリティ・ファースト”の考え方を組み込んでいれば、セキュリティ上の問題で後の開発が滞ることはありません。セキュリティがデフォルトで管理されるようなプロセスがあれば、製品のイノベーションにより集中できるようになります。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター

**セキュアな初期設定の確保**

CRAでは、「セキュア・バイ・デフォルト」の構成で製品を出荷することが求められています。たとえば、セキュリティアップデートはデフォルトで自動インストールされる必要があります。ユーザーが意図的にセキュリティレベルを下げない限り、脆弱な設定になることはなく、ITに詳しくないユーザーでもリスクにさらされる可能性を軽減できます。

**強固なセキュリティ機能の組み込み**

CRAは、未承認アクセスからの保護（たとえば強力な認証の導入）や、暗号化やデータ最小化の原則に基づく機密データの保護など、基本的なセキュリティ要件を定めています。また、ユーザーが安全にデータを削除・移行できる機能も必須です。

**TIP :** Qtには、CRAが求めるこれらの技術的要件を簡単に満たすための構成要素（ビルディングブロック）がそろっています。

第 4 章

# ライフサイクル全体での対応が必須に

CRAは、「リリースして終わり」という時代の終焉を意味します。製品のライフサイクル全体、特に販売後フェーズにおけるサイバーセキュリティ対応を怠ると、規制違反による多額の罰金だけでなく、ブランドイメージの毀損、そしてそれに伴う経済的損失にもつながりかねません。

知っておくべき重要ポイント：

### 定期的なテストとモニタリング体制の構築

製造業者は、製品におけるサイバーセキュリティ上の脆弱性を継続的に検出し、発見された課題に対応する社内体制を整備する必要があります。これにより、既存のプロセスの見直しや、新たなセキュリティテスト体制の構築が求められることもあります。

### 製品ライフタイムに対応したセキュリティサポートの提供

CRAでは、ほとんどの製品に対して、5年間または製品ライフサイクル期間のいずれか長い方の期間にわたり、セキュリティアップデートおよびサポートを提供することが求められます。製造業者は、脆弱性を可能な限り自動的に製品アップデートを通じて修正できるようにしなければなりません。

**TIP:** Qtの5年間の長期サポート(LTS)のリリースは、Qt部分のCRA準拠を強力に支援します。

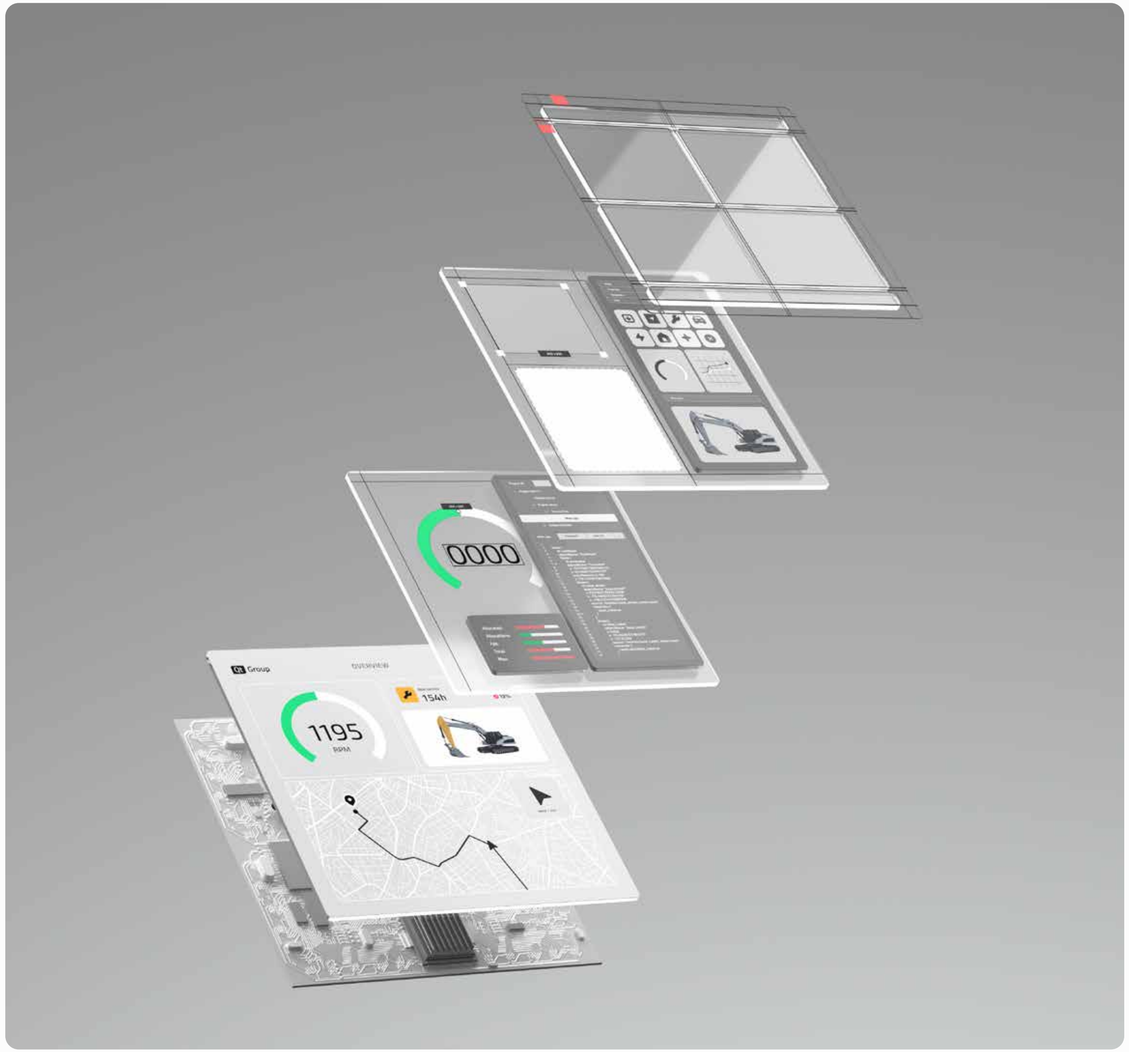
### 脆弱性は24時間以内に報告

CRAでは、製品にセキュリティ上の欠陥やインシデントが発見された場合、その存在を開示するだけでなく、迅速な報告も義務付けています。製造者は、発見された脆弱性のうち、すでに悪用されているものや重大なセキュリティインシデントについて、24時間以内に規制当局へ「早期警告」として通知し、ユーザーにも速やかに情報提供しなければなりません。

**TIP:** Qtの商用ユーザーは、Customer PortalからQt Early Warning List (EWL)に登録することで、重要な脆弱性情報を早期に受け取ることができます。

「CRAは、アップデートの方法について厳密な指針を示しているわけではありません。むしろ、脆弱性に関する情報提供における共通の基準を定めているのです。つまり製造者は、この機会を活かして自社にとって最適なプロセスを整備し、どれだけ迅速にセキュリティ対応ができるかを示すことで、ユーザー体験の向上や信頼の構築につなげることができます。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター



第 5 章

# 適合宣言と証明の提供

CRAでは、製品のライフサイクル全体を通じてセキュリティが確実に維持されていることを証明可能な形で示すために、プロセス重視の要件が定められています。

以下に、その概要を紹介します：

### 適合性評価の実施

CRAは、製品のリスクレベルに応じて「デフォルトカテゴリ」と「クリティカルカテゴリ」に分類し、それぞれに求められるセキュリティ対策を定めています。多くの製品は「デフォルトカテゴリ」に該当し、製造業者自身が仕様に基づいて要件への適合性を確認する「自己適合評価」が認められています。
一方、「クリティカルカテゴリ」に該当する製品については、第三者認証機関による適合性評価が必要となります。

### 技術文書の作成

製造業者は、各製品ごとに包括的な技術文書を作成する必要があります。その内容には、リスクアセスメントレポート、要件をどのように満たしているかの説明、適用される規格の参照、脆弱性評価の結果、ユーザー向けの使用説明書などが含まれます。

**TIP:** Qtは、製品の一部として使用される際に必要な技術文書があらかじめ整備されている点で高く評価されています。

### 適合宣言の作成

製造業者は、CRAに準拠していることを証明するEU適合宣言を作成する必要があります。これは、定められた技術仕様に基づいて作成されます。
この適合宣言は、規制当局によって10年間または定義されたサポート期間のいずれか長い方の期間、参照可能な状態で保持されなければなりません。

### 製品へのCEマーキングの貼付

適合が宣言された後、CEマーキングを製品に明確かつ視認可能な形で表示する必要があります。これにより、その製品がCRAの基準を満たしていることが示され、EU域内での自由な販売が可能になります。

**TIP:** Qt Framework CommercialはCEマーキング取得予定のため、お客様の製品におけるQt部分のCRA対応を後押しします。

「セキュリティを最初から意識して開発サイクルを設計すれば、後のイテレーションでセキュリティの問題に足を引っ張られることがなくなります。つまり、セキュリティがデフォルトで管理された状態のプロセスを構築できるため、より製品のイノベーションに集中できるようになるのです。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター

第 6 章

# CRA時代のイノベーションとの向き合い方

CRAを、また新たな規制のひとつと捉え、テクノロジー分野のイノベーションに対してネガティブな影響を与えるのではないかという懸念の声もあります。

そして、その懸念は決して的外れとは言えません。新たな法規制は常に、初期段階での追加的な作業負担を生みますし、要求に適応するには、製造者側での時間と労力を要します。これは、機能開発だけでなく、プロセスや運用方法、さらには組織全体の体制の見直しを含むものです。

やるべきことは確かに多くあります。
けれども、前向きに捉えてみてはどうでしょうか？

CRAには、理想主義的な側面もあります。すなわち、製造者が自社製品と統合されたすべてのコンポーネントに責任を持つこと。それは、どのみち「正しいこと」であるはずです。

「本質的には価値観に基づいたアプローチです。規制の枠の中でも、イノベーションは十分に可能です。」

- Öykü Işık 氏, IMDビジネススクール デジタル戦略およびサイバーセキュリティ担当教授

「イノベーションとサイバーセキュリティは、決して相反するものではありません。開発プロセスをきちんと整備してセキュリティ対応を組み込めば、開発スピードを落とすことなく、同時にイノベーションを進めることができます。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター

次に、外部のガバナンス機関が期待値を設定することは、イノベーションを妨げることを意味するものではありません。医療業界や自動車業界のように、厳しく規制された分野においても、優れたイノベーションが実現されている好例があります。これらの事例は、規制によって足かせになるのではという懸念を乗り越えるためのインスピレーションとなり、むしろ既存の、そして今後導入される規制の枠組みの中で、どのようにイノベーションを起こしていくかを考えるきっかけとなるはずです。

もうひとつ興味深い視点として、「サイバーセキュリティにおけるイノベーション」があります。たとえば、セキュリティインシデントが発生した際に、デバイスをアップデートするプロセス（OTAによる更新や、自動車の場合は整備工場に持ち込んでのアップデートなど）は、現在でも決して簡単とは言えません。こうした課題に対して、製品ライフサイクル全体を通じたサイバーセキュリティの管理方法において、企業がどのように革新を進めていけるのか。アップデートをいかにシームレスかつ効率的に行うかという観点で、新たな取り組みが求められています。この分野で先行する企業は、今後大きな競争優位を築くことができるかもしれません。

## サードパーティ管理の重要性が加速

製品には、ソフトウェアやハードウェアの複雑なサプライチェーンが関わることが多く、1つの製品に多数のサードパーティ製モジュール（オープンソースライブラリやクラウドAPIなど）が使用されることも珍しくありません。CRAでは、こうした外部調達のコンポーネントも含めて製造業者に責任が課されるため、製品全体のセキュリティを損なうことがないよう、外部コンポーネントの管理が重要な関心事項となります。

**TIP:** Qtのサードパーティソフトウェアに関する考慮事項一覧もぜひご参照ください。

また、サードパーティに関連して、製造業者は製品に含まれるすべてのコンポーネントを機械可読形式で一覧化した ソフトウェア部品表（SBOM）の作成も義務付けられています。

## オープンソースはどうなる？

CRAに関する重要な論点の一つが、オープンソースソフトウェア（OSS）への影響です。CRAでは、製品に組み込まれているすべてのコンポーネント（OSSを含む）について製造業者が責任を負う必要があるため、サードパーティの選定はこれまで以上に慎重に行う必要があります。つまり、「そのOSSコンポーネントのCRA準拠に対して、自社が責任を負えるか？」が問われているのです。

Qt Groupでは、デュアルライセンスモデルを採用しています。世界中にいる150万人以上のQtユーザーのうち、多くの方がオープンソースライセンスでQtを利用しており、日々その安定性とセキュリティの検証に貢献しています。

さらに Qt 商用版をご利用のお客様は、長期的なリリースサイクルや拡張サポートといった付加価値を活用することで、CRA対応の達成およびその継続に大きく貢献することができます。

第 7 章

# CRAへの対応とその先を見据えたステップガイド


商用版のQtフレームワークは CE マーキング取得予定。Qtが担う製品部分のCRA対応を支援します。

Qt 6.8以降では、SBOMを自動生成できます。

Qt Group、CVE番号採番機関（CNA）として正式認定

「早く始めれば始めるほど、備えは万全になります。最初の重要なステップは“自己評価”です。まずは、自社の現在のセキュリティプロセスがCRAの要件にどれだけ対応できているのかを把握すること。そして次に、コンプライアンスを達成するために何をすべきか、具体的なステップを明確にすることが重要です。」

- Maurice Kalinowski 氏, Qt Group フレームワーク担当プロダクトディレクター

# まとめ

確かに、CRAには現在もなお、認証プロセスや早期警告の運用方法など、いくつか未解決の課題が残されています。しかし、時間が刻一刻と迫る中で、製造業者にとって重要なのは、「今すぐに」CRA対応に着手することです。すでに取り組むべき要件は数多く存在しています。

CRAは開発チームだけの話ではありません。「この製品をCRA対応にして」とエンジニアに指示するだけでは不十分であり、これは企業全体で取り組むべき課題です。すでに多くの製造業者が、自社の組織体制や業務プロセスのあり方を見直す必要に迫られています。製品管理体制は適切に整備されているか？セキュリティ対応に関するカスタマーサポートの仕組みはどうか？社内ITインフラはどうなっているか？限られたリソースの中で、最適なアプローチは何か？そして、組織内のさまざまな部門をどう連携させ、真に協力体制を築けるか？

つまり、CRAとは技術面の変更ではありません。単なるプロセスの見直しでもありません。

これは、「文化の変革」です。

そして、文化の変革にはそもそも時間がかかるものです。


「とにかく始めてみてください。まずはドキュメント化することから。脅威分析を始めてみましょう。そして、自社でどう評価できるかを考え始めてください。どのみち、それは良い投資になります。」

- Öykü Işık 氏, IMDビジネススクール デジタル戦略およびサイバーセキュリティ担当教授

Qt Group

Qt Group（キュートグループ）は、クロスプラットフォームのソフトウェア開発ライフサイクル全体をカバーするソリューションを提供しています。

Qt Group（Nasdaq Helsinki: QTCOM）は、世界のリーダー企業や150万人以上の開発者から信頼されるグローバルなソフトウェア企業として、ユーザーに愛されるアプリケーションやスマートデバイスの開発を進めるお客様をサポートしています。また、UIデザインからソフトウェア開発、品質管理・展開に至るまで、製品開発ライフサイクル全体を通して、お客様の生産性向上を支援しています。

Qt Groupは、180カ国以上、70を超える業界のお客様へソリューションを提供。フィンランドのエスポーに本社を置き、世界中に約900人の従業員を擁しています。