5. 欧州サイバーレジリエンス法(EU Cyber Resilience Act)の発効

要約

- EU 理事会の正式採択、官報への掲載を経て欧州サイバーレジリエンス法(CRA)が発効した。
- 厳しいセキュリティ要件に対応するため、サプライチェーン全体での対応と責任分担が必要。
- 規則の本格適用までに SBOM を活用した脆弱性管理体制や、迅速な報告体制の構築が必須。

欧州サイバーレジリエンス法成立の背景と目的

2024 年 12 月 11 日に欧州サイバーレジリエンス法(CRA)が正式発効し、2027 年 12 月に完全適用されるまでのタイムラインが確定しました(*1)。

CRA はデジタル製品やサービスのセキュリティを強化し、消費者をデジタルリスクから保護することを目的とし、欧州市場で製品を提供する事業者(製造者、輸入者、販売者)に対し、企画・設計、販売、保守の製品ライフサイクル全般にわたるサイバーセキュリティの確保を義務付けた EU 規則です。

今日、デジタル製品の普及と日常生活への浸透により、サイバーセキュリティのリスクは一般消費者にとっても身近なリスクとなっています。一方で、多くのコンシューマー向け製品では、ライフサイクルにわたるセキュリティが十分に確保されないことが問題と考えられています。

たとえばスマートフォンなどのセキュリティアップデートが製品寿命より短期間に提供終了してしまうことや、安価な IoT ガジェット製品で、セキュリティ機能が提供されないことなどがあります。

CRA では、製品のセキュリティレベルに応じた第三者認証の利用など、定められた方法により、セキュリティ性能を検証し、CE マークを表示することを求めています。CRA が適用されることで、消費者は購入時点だけでなく、法で定める利用期間を通じてサイバーリスクに対してセキュアな製品を利用できます。

また、NIS2 指令(*2)の対象となる重要インフラやサービスを提供する組織においては、CRAに対応する製品・サービスを利用することで、NIS2 指令で求めるサプライチェーンを含めたシステムのセキュリティ確認を容易にできることが期待されます。

具体的かつ高い基準と強力な罰則規定

CRA の要件には既存のセキュリティ標準に規定されているものも多く、対応するセキュリティ標準をマッピングした資料が公開されています(*3)。CRA はこれまでの標準に不足する要件や推奨であった項目も要件に加え、EU の法規として強力な罰則を伴い運用します。以下に CRA の特徴的な要求事項を示します。

- 製品ライフサイクル全体を通じたセキュリティ確保
  販売されてから最低 5 年間、または製品の寿命が短い場合はその期間、セキュリティを担保します
- リスクベース・アプローチによる製品分類と認証要件
  自己宣言から第三者認証制度必須化まで製品のリスクレベルで分類し、CE マークを表示します
- 脆弱性報告義務と迅速なセキュリティアップデート
  発見から 24 時間以内の ENISA(*4)報告義務や、サードパーティ製品を含めた SBOM の整備義務
- 厳格な罰金制度による規制遵守の強化
  1,500 万ユーロまたは企業の年間売上高の 2.5%のいずれか高い方が罰金として科される

(*1) EUR-Lex「REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL」

(*2) EUR-Lex「DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL」

(*3) europa.eu「Cyber resilience act requirements standards mapping」

(*4) ENISA(欧州連合サイバーセキュリティ機関):EU のサイバーセキュリティ政策の支援、脅威インテリジェンスの共有、インシデント対応支援などを通じ、EU 全体のネットワークおよび情報セキュリティの向上に取り組む EU の専門機関

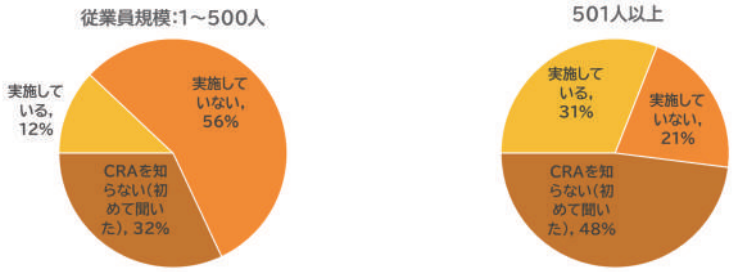
サプライチェーン全体での対応と責任分担

CRA は、サプライチェーンを構成する企業にも対応を求める構造となっています。

CRA では最終製品を製造する事業者に対し、製品を構成するコンポーネントなどのサードパーティ製品を活用する際に、セキュリティ品質の確認を求めます。この手段として、事業者が整備する SBOM を活用した脆弱性管理体制に各サプライヤーが参加するなど、サプライチェーンで情報を連携する仕組みが必要となります。

また、CRA に抵触する事案が生じた場合には非常に高額な罰金を科される可能性があるため、企画段階から明確にセキュリティの要求仕様を定め、契約に示すことで、責任の所在を明確にすることも大切です。

このように多くの企業に取り組みが求められる一方で、昨年 PwC が日本の製造業関連企業を対象に実施した調査によると、従業員規模 500 人以下の企業の半数超が、CRA 対応に取り組めておらず、1/3 の回答者は CRA を認識していなかったという状況が報告されています。



日本企業の CRA 対応状況（2023 年 10 月, n＝580）

出典: PwC 2024 年 4 月「日本企業の欧州サイバーレジリエンス法対応実態調査」（*1）に基づき大和総研作成

CRA の適用スケジュールが確定したため、サプライチェーンオーナーとなる企業は、中小企業を含むサプライチェーン全体で CRA 対応の必要性を共有し、認識する必要があります。

欧州主要企業では、すでに CRA の取り組みが進んでいますが、ENISA への脆弱性報告義務やサプライチェーンでの SBOM 対応は高水準の要求と見なされており、多くの企業でこれをチャレンジングな目標としています。

日本では、IoT 製品を対象に「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が整備され、将来 CRA との相互認証も計画されています（JC-STAR については、本冊子 P.5 で紹介していますのでご参照ください）。日本の大企業は、国内外の制度対応を総合的に見据え、自社だけでなくサプライチェーン全体でサイバーセキュリティを構築するために、中小サプライヤーを含めた一体的な対応を計画し、推進する必要があります。

まとめ

今回、CRA 完全適用までのタイムラインが次のように確定しました。

2024 年　12 月 11 日:　CRA 正式発効
2026 年　 6 月 11 日:　評価機関（ノーティファイドボディ）の届出開始
2026 年　 9 月 11 日:　脆弱性報告の義務化
2027 年　12 月 11 日:　猶予期間終了、全 CRA 要件の完全適用

企業は、「自社に影響がありうる」という前提に CRA 違反による巨額の罰金や欧州市場喪失のリスクを経営課題と認識し、確認や対応を進めていくことが賢明です。

特に、完全適用に先行して義務化される製品の脆弱性報告義務に関する対応は、早期に着手し、平時より脆弱性情報を収集し、速やかに公開・報告できる体制とプロセスを整備していくことが求められます。

完全適用に向けては、企業の中長期的な戦略の一部として、国内外の制度動向にも留意しながら、サプライチェーンで一体となったセキュリティ対応を推進していくことが望まれます。

（渋谷　篤）

（*1）PwC「PSIRT が認知すべき海外法規制解説 / 日本企業の欧州サイバーレジリエンス法対応実態調査」