一般財団法人 日欧産業協力センター　レポート
欧州デジタル政策　EU Policy Insights

Vol.11　2024 年 8 月
「EU のサイバー・レジリエンス法-初の分野横断的 IOT サイバーセキュリティ」

■ 本資料は、当センターの公式見解を示すものではありません。
■ 本レポートの内容は別途記載がない限り執筆時点で入手している情報に基づくものであり、その後の状況変化や追加政策発表により変わる場合があります。
■ 本レポートへのご意見、取り上げて欲しいトピック等、お寄せください。
eujp-info@eu-japan.or.jp

一般財団法人 日欧産業協力センター
〒108-0072　東京都港区白金 1-27-6　白金高輪ステーションビル 4 階
TEL: 03-6408-0281　FAX: 03-6408-0283
E-MAIL : eujp-info@eu-japan.or.jp

欧州デジタル政策 EU Policy Insights vol.11

「EU のサイバー・レジリエンス法-初の分野横断的 IOT サイバーセキュリティ」

1. 概要

- サイバー・レジリエンス法（以下、CRA）は、他の機器やネットワークに直接または間接的に接続される幅広い製品に適用される。これには、機器に組み込まれたソフトウェア、デジタル要素を持つ製品、インターネット通信に依存する製品などが含まれる。特に、家電製品、産業機器、ヘルスケア機器などが含まれる。

- 製造業者とサービス・プロバイダーは、重大なサイバーセキュリティ・インシデントを認知してから 24 時間以内に関係当局に報告しなければならない。これにより、ユーザーやネットワークへの潜在的な影響を軽減するための迅速な対応と調整が保証される。

- CRA は、製品ライフサイクルを通じて適切なセキュリティ対策を実施することを組織に義務付けている。これには、設計、開発、製造、配送、メンテナンスが含まれる。製造業者は、定期的なセキュリティ評価を実施し、最新の文書を維持し、脆弱性の継続的な監視とパッチ適用を確実に行わなければならない。

- CRA は、サイバーセキュリティを考慮した製品の設計を要求している。これには、データ保護の確保、不正アクセスの防止、悪意のある干渉に対する保護などが含まれる。製品は市場に出回る前にテストと認証を受け、定められたセキュリティ基準を満たしていることを確認しなければならない

- CRA を遵守しない場合、罰金や市場制限を含む罰則の対象となる。CRA は、各国当局にコンプライアンスを強制し、監査を実施し、是正措置を課す権限を与えている。継続的なコンプライアンス違反は、製品回収や EU 市場での販売禁止につながる可能性がある。

- 日本企業への影響については 11 章にて言及。

2．サイバー・レジリエンス法の概要

CRA はコネクテッドデバイスとデジタル製品のためのサイバーセキュリティを強化する EU の戦略において、立法上の大きな前進である。CRA は、セキュリティ上の要求および厳しいコンプライアンスの規格を定めることで、増大するサイバーセキュリティの脆弱性と脅威に対処し、製品がそのデザインからプロダクトライフサイクル全体に至るまで安全であることを保障するものである。

CRA の対象は、家電製品、産業用制御システム、医療機器、組み込みソフトウェアなど多岐に渡る。こうしたデジタル的要素を持つ製品をめぐっては、サイバー脅威を軽減するためにセキュリティの基準を守らなければならない。

鍵となる規定は、インシデントの報告に関するものであり、製造業者とサービス・プロバイダーは、重大なサイバーセキュリティ・インシデントが発生した場合、24 時間以内に、インシデントの詳細と影響およびその是正措置を含めた届出を当局に行なうことが義務付けられている。