モノづくり現場におけるセキュリティリスクと知っておきたい重要ポイント -欧州サイバーレジリエンス法編

オムロン株式会社 インダストリアルオートメーションビジネスカンパニー 商品事業本部

欧州サイバーレジリエンス法（EU Cyber Resilience Act、EU-CRA）は、通信機能を持つデジタル製品を対象に、EU 市場で共通のサイバーセキュリティ要求を定める規制です。本規制は、製品に残存しがちな脆弱性、不十分なセキュリティアップデートの提供、利用者への情報提供の不足といった課題を解消し、製品の廃棄に至るまでのライフサイクル全体にわたって、一定レベルのセキュリティと情報の透明性を確保することを目的としています。本書では、EU-CRA および関連する規格の概要と、これらに対するオムロンの取組について紹介します。

1. EU-CRA とは

近年、インターネットを含む外部ネットワークとの接続拡大やサプライチェーンの複雑化に伴い、通信機器が扱うデータの重要性は、製品の安全性や品質の観点からも一層高まっています。一方で、セキュリティ対策が不十分なサプライチェーン上の機器を狙ったサイバー攻撃が増加しており、製造業者やサプライヤは以下のようなリスクに直面しています。

- 生産ライン停止や重大な事故：サイバー攻撃により、工場制御が乗っ取られる、あるいは情報資産が漏洩し、生産ラインの停止、不良品の製造、重大な事故につながる可能性があります。
- 事業中断や信頼失墜：事業を中断せざるを得ない状況に追い込まれ、経済的損失を被り、法的責任も問われるなど、企業の存続に大きな影響が生じます。
- 環境汚染や健康被害：サイバー攻撃により、意図しない有害物質の流出など、環境汚染や健康被害に発展する可能性があります。

EU-CRA（Regulation (EU) 2024/2847）は、EU 市場で流通する「通信機能を持つデジタル製品」を対象に、横断的（水平的）なサイバーセキュリティ要求を設け、EU 市場における統一的なルールとして整備する規制です。規制の背景には、通信機器の急増に伴うサイバー攻撃面の拡大、製品に存在する脆弱性の広がり、セキュリティ更新の提供が不十分または不統一であること、さらに利用者が適切に設定・使用するための情報を得にくく、安全な製品の選択や運用が難しいことがあります。

EU-CRA が目指すのは、製品を「出荷時点でより安全に」することに留まらず、製造業者が製品ライフサイクル全体を通じて、セキュリティサポートを継続的に担保することです。具体的には、セキュア・バイ・デザインの実践、セキュリティ更新を継続的な提供、サポート期間の透明性を高めることで、利用者が製品選定や運用の際にサイバーセキュリティを考慮できる環境の整備を求めています。

また EU-CRA は、業界別規制に存在していたサイバーセキュリティ要求の“つぎはぎ”による法的不確実性や、製造業者の追加的な対応負担を軽減することも目的としています。CE マークを通じて適合を示す枠組みを提供することで、EU 市場での信頼性と流通の円滑化を促進します。その結果、調達側（ユーザ）にとっては「更新が継続され、情報が提供される製品」を選択しやすくなり、供給側（製造業者）にとっては要求が共通化され、説明責任を果たしやすくなります。

2. EU-CRA に求められること

2.1. EU-CRA 要件

以下は EU-CRA で製造業者に求められる要求事項の概要です。

- 通信機能を持つデジタル製品は、2027 年 12 月 11 日までに法律に適合しなければ EU(欧州連合)に出荷できなくなります。
- 適合したものだけが CE マークを付けることができます。
- 違反時は 1,500 万ユーロまたはグローバル年間総売上高の 2.5%のいずれか高い方を上限とする罰金が科せられます。
- 販売後のセキュリティサポートの義務があるため、製造業者には継続的な対応体制の整備が求められます。
- 機能要件、セキュア開発プロセス要件、脆弱性ハンドリング要件、製品サポート要件などの要件があります。

2.2. スケジュール

2024 年 12 月 11 日：発効　移行期間開始
2026 年 8 月 30 日：脆弱性管理要件に対する整合規格公開
2026 年 9 月 11 日：実際に悪用された脆弱性の当局への報告義務開始
2026 年 10 月 30 日：クラス Ⅰ / Ⅱ /クリティカル製品に対する整合規格公開
2027 年 10 月 30 日：その他の製品に対する整合規格公開
2027 年 12 月 11 日：適用開始

2.3. 対象商品と分類

ハードウェア／ソフトウェアを含む「通信機能を持つデジタル製品」が対象になります。対象商品はリスクにより、下記の通り分類されます。製品分類は原則として製造業者がリスク評価に基づいて自己判定し、必要に応じて第三者評価を行います。

カテゴリ		内容
「基本的な」デジタル製品（低リスク）		「重要な」デジタル製品以外のデジタル製品。比較的リスクが低い、スマート家電など市場に流通する 90%程度の製品
「重要な」デジタル製品	クラス Ⅰ（中リスク）	ユーザの個人情報やネットワークへの影響が懸念される製品
	クラス II（高リスク）	他のシステムやネットワーク全体へのセキュリティ影響が大きい製品
「クリティカルな」デジタル製品（最高リスク）		特に国家インフラや安全保障に深く関わる製品

2.4. 製造業者の義務

製造業者は、セキュアな製品を開発・提供することに加え、製品ライフサイクルを通してセキュリティをサポートできる仕組みやフロー・プロセスの整備、適合の正当性・妥当性を示す技術文書やユーザ向け文書を求められます。

附属書	**概要**
製品特性	適切なレベルのサイバーセキュリティを確保するように設計、開発、製造**セキュアプロセス**を実施すること
	製品ごとに脅威分析・要件定義・実現性検討・商品開発を行い、**セキュリティ要件を実現**すること （悪用可能な脆弱性なし、**デフォルトセキュア**、セキュリティアップデート、不正アクセス保護、監査ログ　など）
脆弱性処理	**ソフトウェアの部品表(SBOM)**を作成・運用し、当局から要求があった際に提出できること
	セキュリティテスト/レビューを実施し、文書化する。当局から要求があった際に文書を提出できること
	セキュリティアップデート/脆弱性に関するアドバイザリを、無償で提供できること ● 提供にあたっては、改ざん防止や提供元の真正性が確保された方法であることが求められる ● 市場からの報告受付窓口を設置し、悪用された脆弱性や重大インシデントは以下の 3 段階で当局に報告する 　● 初動通知（影響を受ける可能性のある重大な脆弱性）：24 時間以内 　● 詳細情報の追加報告：72 時間以内 　● 是正状況・最終報告：14 日または 1 か月以内
技術文書	脅威分析結果、テストレポート等の適合性/正当性を説明する文書を作成・更新。文書は最低 10 年間保管し、当局から要求があった際に提出できること
ユーザ向け文書	マニュアル/ガイドラインなどで、製品情報/セキュリティサポート期間/セキュリティアップデート方法などの**情報をユーザにわかりやすく提供**できること

3. EU-CRA に対するオムロンの取組

3.1. セキュア・バイ・デザインの実践

オムロンは、産業用オートメーションおよび制御システムで使用される制御機器のセキュアな開発に必要なプロセスおよび組織要件を規定する国際規格 IEC 62443-4-1 の第三者認証を取得しています。この認証に基づく開発プロセスの下、セキュア・バイ・デザインの原則に沿って、多くの FA 製品について EU-CRA への適合を見据えた対応を進めています。

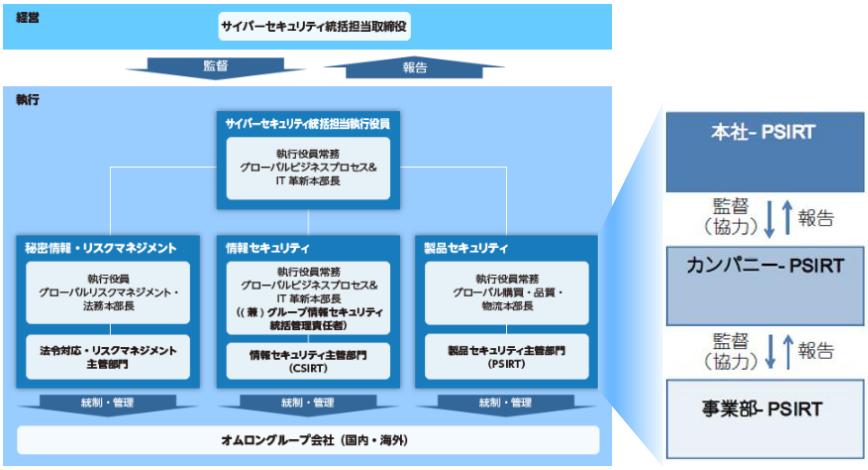
一方、既存製品については、ハードウェア構成や技術的制約により、EU-CRA で求められる要件への対応が困難な場合があります。そのた

め、製品の用途やリスク、ライフサイクルを踏まえ、可能な範囲での対応や、後継製品での対応を含めた検討を進めています。

3.2. 脆弱性・インシデント管理

お客様の安全、安心のため、セキュリティを考慮したオムロンの製品、サービスの提供に努めます。そのため、オムロングループ全体で、サイバー攻撃に対するセキュリティ対策を講じるための製品セキュリティ活動に取り組んでいます。

オムロンは、製品セキュリティの活動を推進するため、本社および各事業部で連携体制を整えています。その中で、製品、サービスの脆弱性管理では、本社および各事業部にオムロン PSIRT[1]体制を構築し、対応を行っています。



オムロンは、セキュリティの脆弱性に関する国際的な取り組みである CVE[2]プログラムにおいて、脆弱性識別子（CVE ID[3]）を自社で採番できる CVE 採番機関（CNA[4]）として認定されています。CNA 認定により、オムロングループの製品・サービスに影響する脆弱性について、従来は外部機関に依頼していた CVE ID の採番を自社で行うことが可能となり、脆弱性情報をより迅速に公開できる体制を整えています。当社製品の脆弱性情報は以下の Web サイトで公開しており、RSS 配信により最新情報をタイムリーに取得することができます。

https://www.fa.omron.co.jp/product/security/vulnerability/

オムロン社内では、国際標準に準拠した SBOM を活用した脆弱性管理の自動化を進めており、当社製品で使用しているソフトウェア部品（OSS[5]/商用ソフトなど）に関する脆弱性を継続的に監視しています。

3.3. セキュリティガイドライン

オムロンでは、当社 FA 製品におけるセキュリティの考え方や取組内容をご理解いただくとともに、製品をご利用いただく際に実施していただきたいセキュリティ対策を示すことを目的として、セキュリティガイドラインを公開しています。本ガイドラインは、お客様の装置における EU-CRA への対応や、システム全体のセキュリティ対策を検討・実施する際の参考資料として活用いただけます。

https://www.fa.omron.co.jp/data_pdf/mnu/sbca-140c_fa_system_security_guideline.pdf

4. 終わりに

本書では、EU-CRA の概要と、これに対するオムロンの考え方および取組を紹介しました。欧州市場における製品・装置の安全性と信頼性を確保するための一助として、本内容をご活用いただければ幸いです。

---

[1] Product Security Incident Response Team。製品の脆弱性報告の受付・評価、修正、情報公開、更新提供などを担う製品セキュリティ対応チーム。

[2] Common Vulnerabilities and Exposures。米国の非営利団体 MITRE Corporation が運営する、国際的に広く利用されている脆弱性識別の枠組み。

[3] 個別製品内のソフトウェアやハードウェアに存在する脆弱性に一意の識別番号を付与することで、別団体が公開している情報との相互参照や関連付けを可能にする標準化された識別子。

[4] CVE Numbering Authority。CVE プログラムの中で CVE ID を割り当て、CVE レコード（脆弱性情報）を公開できる権限を持つ。

[5] Open Source Software。