ハイライトレポート

2025. 8. 22

対応が急務に！
IoT/OTデバイスに求められるセキュリティ対応とは
～JC-STAR、CRAの最新動向とその対応～　パート2

セキュリティ対策に乗り遅れないために

産業制御機器のIoT化が進む中、サイバー攻撃はますます高度かつ巧妙になっています。製造業を含む幅広い業界では、より強固なセキュリティ対策が求められています。

日本のJC-STAR、欧州のサイバーレジリエンス法（CRA）をはじめ、サイバーセキュリティを義務化する動きが世界的に加速しています。これらへの対応の遅れは、市場競争力の低下や法的リスクの増大につながる可能性があります。

企業は、製品やソフトウェアに求められるサイバーセキュリティ要件を明確化し、法規制への適応、サイバー攻撃に耐えうる事業基盤の構築をめざし、セキュリティ戦略を策定・実行することが求められます。

EUサイバーセキュリティ規制のポイント

2022年に草案が発表されたサイバーレジリエンス法は、EU市場で販売されるデジタル製品に対し、サイバーセキュリティ要件の順守を義務化する規制です。2026年9月11日に一部施行（第14条：製造業者の報告義務）、2027年12月11日に完全施行される予定です。対象製品をEU市場に投入する際には、セキュリティ要件を満たすことを承認するために適合性評価手続きを実施し、CEマークを取得する必要があります。または、代替として、CEマークに準じた整合規格の認証が必要となります。

脆弱性の報告義務の解説

製造業者には、設計・開発段階からのセキュリティ確保や販売後の脆弱性対応、アップデート提供などが求められます。特に、製品の脆弱性の悪用を認知した場合、CSIRT及びENISAへの報告が必要です（第14条）。

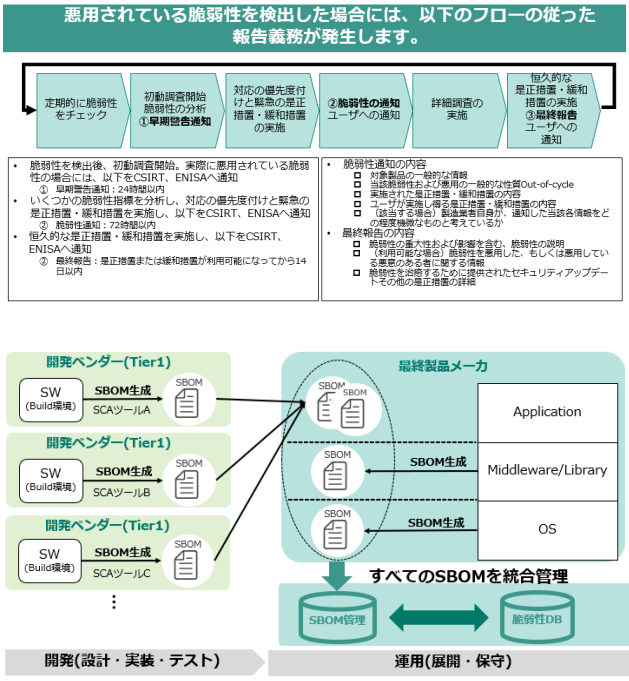
脆弱性検出後、初動調査を開始し、悪用の可能性がある場合は24時間以内にCSIRT・ENISAへ早期警告通知を行います。脆弱性指標を分析し、優先度を判断したうえで72時間以内に脆弱性通知を行います。恒久的な是正・緩和措置が整い次第、14日以内に最終報告を提出する必要があります。

脆弱性処理要件とSBOM

CRA対応では、附属書Ⅰの2に基づき、アプリケーション内のコンポーネントを適切に識別するため、最上位レベル（1階層）の依存関係を含むSBOMの作成が求められます。しかし、実際には製品の脆弱性を適切に管理するために、製品内のソフトウェアのすべてに対してSBOMを作成し、定期的な脆弱性管理を実施する必要があります。開発部門は各自のツールでSBOMを作成、製品管理部門はそのSBOMを受け取り、実行環境のSBOMと統合、全体を一元管理する必要があります。

■ 本日の登壇者 ■

サイバートラスト株式会社
フィールドマーケティング部
富田 佑実 氏



出所：投影資料より一部抜粋