ハイライトレポート

2026. 2. 27

迫るEU CRA規制
– IoT/OTデバイスメーカーが今すぐ備えるべきセキュリティ対応と最新動向 Day 1

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、サイバー攻撃の手法は高度化・巧妙化しており、製造業を含む幅広い業界に対し、**より強固なセキュリティ対策**が求められています。2027年のサイバーレジリエンス法（CRA）完全施行をはじめ、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おり、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。

すでに施行までのタイムラインが明確となった今、企業は法規制への適応、**サイバー攻撃に耐えうる事業基盤の構築**を目指し、早急にセキュリティ戦略を策定・実行することが求められます。

CRAの全体構成と主な内容

CRAは、デジタル要素を含む製品のサイバーセキュリティ確保を目的とし、本編と附属書で構成されます。本編では目的や定義、製造者・輸入業者の義務、ライフサイクル全体のセキュリティ要件、CEマーキング手続きなどを規定。附属書では要求事項・製品分類・適合評価手順の詳細が示されています。技術的要件は整合規格として策定が進められ、2027年の全面適用を目指し標準化が進行中です。

CRAの義務内容の全体像

CRAは、製品の**ライフサイクル全体でサイバーセキュリティを確保**するため、製造から上市（製品の発売）後まで一貫した義務を課します。開発段階では、暗号化・認証などのセキュリティ仕様の実装、リスク評価、脆弱性低減策、攻撃耐性の検証が求められ、製品クラス判定や適合性評価の準備も必要です。

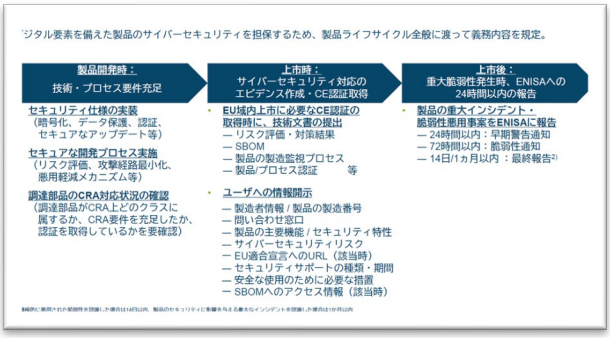
上市前には、CE認証取得や技術文書・リスク評価結果の提出が義務化。上市後は、重大脆弱性発生時の**24時間以内のENISA報告**、72時間以内の通知、14日以内の最終報告など迅速な対応が必要です。さらに更新期間やSBOMなど、ユーザーへの情報提供も求められます。

CRA準拠に向けたアプローチ

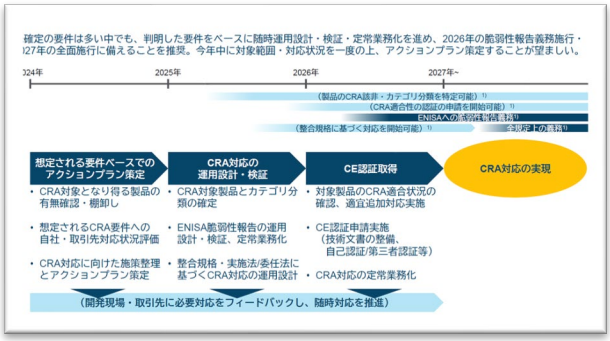
CRA対応は、判明している要求を基に**対象製品の把握とアクションプランを策定**し、設計段階からセキュリティ要件の反映や脆弱性管理の体制整備を進める必要があります。その後、運用設計・検証を実施し、適合性評価を経てCE認証取得、2027年の全面適用に向け、随時アップデートを反映しながら一連の対応を段階的に進めることが重要となります。

■ 本日の登壇者 ■

Covalent株式会社
Managing Director
小林 弘樹 氏



CRAの義務内容の全体像
出所：投影資料より一部抜粋



CRA準拠に向けたアプローチ
出所：投影資料より一部抜粋

他記事、ウェビナ、お問い合わせはこちら

リョーサン テクラボ
エンジニアによりそうマガジンサイト