ハイライトレポート

2025. 2. 25　セッション1

法規制対応が急務に！
IoT/OTデバイスを製造する組織に求められるセキュリティ対応とは
～CRAの最新動向とその対応～

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。

EUサイバーセキュリティ規制のタイムライン

2022年に草案が発表されたCyber Resilience Act（CRA）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日に完全施行となる予定です。

CRAのポイント

CRAは、技術的対策だけでなく、法的・組織的な対応も求められる包括的な規制です。製造業者には、設計・開発段階からのセキュリティ確保、販売後の脆弱性対応、アップデート提供などが求められ、脆弱性への悪用を認知した場合はEUサイバーセキュリティ庁（ENISA）へ報告する必要があります（第14条）。対応の遅れは重大なリスクとなるため、組織的な対応体制の構築が不可欠です。

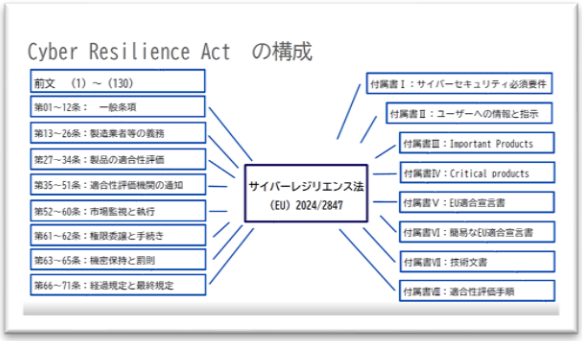
また、輸入業者・販売業者も、取り扱う製品がCRA準拠であることを確認する義務があり、規制対応はサプライチェーン全体に及びます。企業は自社だけでなく取引先のセキュリティ基準を見直し、管理体制を構築する必要があります。違反した場合、大きな罰則が科される可能性があり、特に製造業者にとっては重大な経営リスクとなります。企業は、早急に規制内容を理解し、脆弱性対応プロセスやサプライチェーンリスク管理を強化する必要があります。

CRA準拠に向けたアプローチ

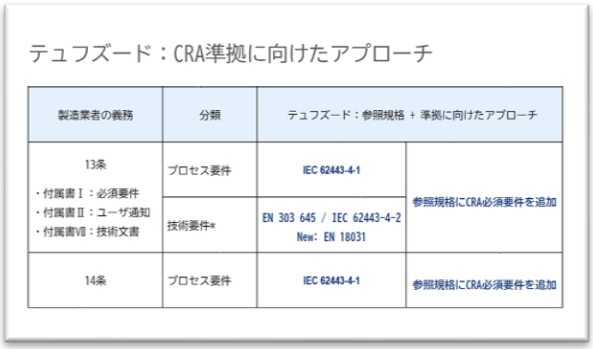
CRAに準拠するためには、製品の設計・開発から運用・保守までのライフサイクル全体でのセキュリティ対策を確立することが求められます。そのため、産業分野の国際的なセキュリティ規格であるIEC 62443を活用し、実効性のある対策を講じることが有効です。

■ 本日の登壇者 ■

テュフズードジャパン株式会社
COM事業部　IEP部
シニアセールスエクゼクティブ
登山 慎一　氏



Cyber Resilience Act の構成
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