# ハイライトレポート

2025. 2. 25　セッション2

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。

## CRAにおいて特に注目すべき技術要件

Cyber Resilience Act（CRA）は、製品の設計から運用までの安全性を確保するため、高度なセキュリティ対策を求めています。通信の暗号化やアクセス制御の強化、静的解析ツールを活用した開発段階での脆弱性検出が不可欠です。また、リスクを把握するために、自動スキャンツールによる監査、ソフトウェア部品の追跡管理、脅威の事前評価が推奨されます。さらに、ソフトウェアの構成要素を可視化し、更新プロセスを自動化することで、脆弱性対応の迅速化が可能になります。

## CRAにおいて対応が必要となる文書

CRAに対応するには、技術的対策に加え、適切な文書整備が不可欠です。設計・開発、運用、保守の各フェーズでセキュリティ基準を明確にし、文書化することで規制要件への準拠を証明する必要があります。リスク評価や設計ポリシーを記録し、脆弱性対策の基準を明文化するとともに、定期的なチェックを実施し、報告書として整理することが重要です。また、ユーザ向けガイドラインを作成し、安全な利用方法を示すとともに、脆弱性の報告や修正対応の手順を整備し、迅速な対応を可能にする必要があります。

## CRA対応における連携の重要性

CRAへの対応には、体制強化・連携が不可欠です。企業は、サイバーセキュリティ担当を確保し、明確な役割分担を定めることで、規制要件への適応をスムーズに進める必要があります。また、リスク評価チームやインシデント対応チームを結成し、脅威の特定から対応までの流れを明確化することが重要です。これに加え、定期的な研修や実践的なトレーニングを通じ、従業員の対応力を向上させることが求められます。CRA準拠には、専門チームの整備と継続的なスキル向上を通じた、社内全体のセキュリティ意識の強化が不可欠です。

### ■ 本日の登壇者 ■

Trellix
プロフェッショナルサービス
プリンシパルコンサルタント
麓 広大 氏



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