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の概要のセキュリティ特性要件

CRAのセキュリティ特性要件は、製品の安全性を**「設計とデフォルト設定」「データ保護と完全性」「ライフサイクルとレジリエンス」**の三つの観点から確保することを求めています。

まず「設計とデフォルト設定」では、リリース時点で既知の脆弱性を含まないこと、安全な初期状態（セキュア・バイ・デフォルト）の実現が必要です。また、ハードコードされたパスワード（暗号化されていないパスワードがソースコードに埋め込まれている状態）の使用は禁止され、強固な認証やアクセス制御を備えることが求められます。

次に「データ保護と完全性」では、機密性・完全性・可用性（CIA）の確保が中心となり、暗号化、改ざん防止、DoS攻撃への耐性が必要です。加えて、不要なデータを扱わない**「データ最小化」**や、外部インターフェースを最小限に抑える対策も求められます。

最後に「ライフサイクルとレジリエンス」では、アップデート提供の仕組み、脆弱性悪用時の影響低減、ログ管理による異常検知など、運用まで含めた継続的な安全性確保が重要とされています。

CRA準拠へのロードマップ

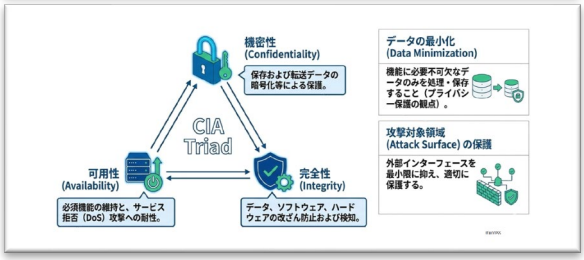
CRA準拠には、まず規制で求められる要件の把握と、対象製品の整理が必要です。次に、設計段階から**セキュリティ要件を製品仕様へ反映**し、脆弱性管理やリスク評価プロセスを整備します。

その後、製品の検証・運用設計を経て、**適合性評価とCE認証取得**へ進みます。2027年の全面適用に向け、規制や関連規格の更新を踏まえながら、継続的に対応内容を見直すことが重要です。

■ 本日の登壇者 ■

アイティアクセス株式会社
ADV事業部
セキュリティーエキスパート
大貫 良一 氏

株式会社リョーサン
デバイス第一事業本部
技術支援部 第二課
木村 友哉



CRAの概要のセキュリティ特性要件
出所：投影資料より一部抜粋