欧州サイバーレジリエンス法（CRA）概要と対策（ダイジェスト版）

シーメンス株式会社　デジタルインダストリーズ　プロセスオートメーション事業部
大島　正嗣（シーメンス認定IEC62443スペシャリスト）

SIEMENS

CRA概要と国内装置メーカーへの影響

	Cyber Resilience Act （CRA）
コンセプト	ユーザーにサイバーリスクを与え得るデジタル製品のセキュリティ確保について、 製品ライフサイクル全体を通じて製造業者が責任を負う
適用開始時期	• 一部規定は2026年9月11日（重大な脆弱性やインシデントの報告義務） • 全規定は2027年12月11日
対象	デジタル要素を有する製品 ➢ ソフトウェア、デジタルデータを処理・保存・伝送可能なハードウェア、および遠隔データ処理ソリューション ➢ ユーザーネットワークやインターネットへの接続有無は無関係 ➢ 医療・航空・自動車・船舶・軍事関連業界は対象外
主な義務化内容	• セキュリティ特性要件の遵守（デジタル製品が有するべき技術要件） • 脆弱性処理要件の遵守（製造業者として備えるべきプロセス要件） • 報告義務（24時間以内の早期警告通知など）
適合性の評価	一般的な産業用制御システムは自己適合宣言で対応可能となる可能性が高い
罰則	最大1500万ユーロまたはグローバル全売上高の2.5%のうち、高い方
国内装置メーカーへの影響	• CRA準拠がCEマーキングに影響 • 未対応の場合、EUでの製品販売が不可

CRAへの対応の遅れは、欧州ビジネスを丸ごと喪失するリスクに直結します

SIEMENS

CRAの主な要件と対策について

CRAは対策が急務ですが整合規格がいまだ定められておらず、完璧な対策の手本が無いことが大きな問題です。しかし、CRA要件の内容は産業用サイバーセキュリティの国際標準であるIEC62443と共通性が高く、これに基づいて準備を進める事が現時点で最も効率の良い手段であると言えます。また、脆弱性対処要件や報告義務を遵守することは既存部門（品質保証や設計、開発部門など）の追加業務としては困難である場合も多く、自社製品セキュリティの専門チーム（PSIRT）を組織し運用することも検討する必要があります。

主な要件と対策の方向性

セキュリティ特性要件（技術要件）：CRA施行後の上市製品が対象 ➢ 不正アクセスからの保護を確保すること ➢ 既知の悪用可能な脆弱性が含まれていないこと　・・・等	▶ IEC62443-3-3に基づく対策
脆弱性対処要件（プロセス要件）：CRA施行後の上市製品が対象 ➢ 脆弱性開示ポリシーを導入し実施すること ➢ 悪用可能な脆弱性が適時に修正・緩和される仕組みを提供すること　・・・等	▶ IEC62443-4-1に基づく対策
報告義務：過去に上市したものも含め全製品が対象 ➢ 製品に重大な脆弱性やインシデントが発生した場合、指定機関に報告 ➢ 認識から24時間以内の初期警告通知、72時間以内の本通知、14日または1か月以内の最終報告	▶ PSIRTを社内に組織し運用

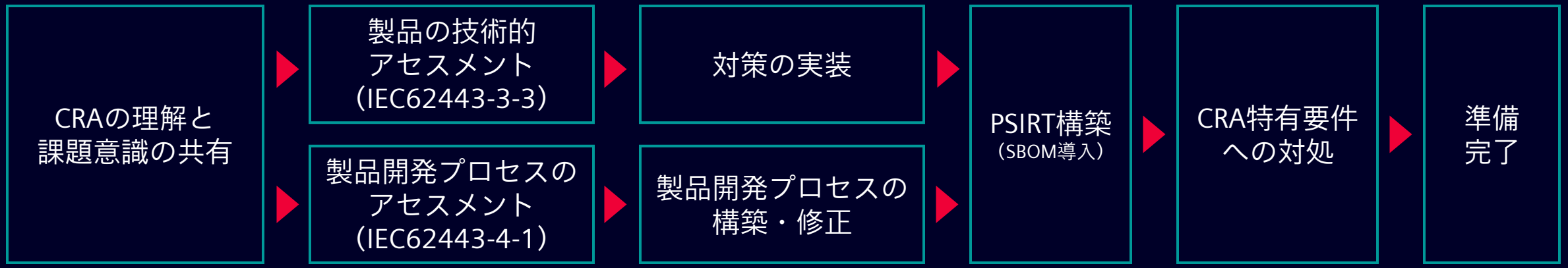
なお、シーメンスでは上記の３つの主要対策に関し、IEC62443要件と御社の現状の差分を測定し対策案を提示する「アセスメントサービス」および、PSIRTの構築支援サービスを提供可能です。

SIEMENS

CRA対策のステップについて

CRA対策の第一歩として最も重要な事は、CRAの内容、そして対策の必要性と方向性を全社で部署横断的に理解・共有することです。なぜならばCRAはデジタル製品のライフサイクル全体に関わる法律であり、設計・開発・製造・調達・サービスといった様々な部門が何らかの形で関わることになるためです。また、PSIRTのような新部署を創設する必要性にも関連することから、経営陣のCRAに対する理解も必須となります。

CRA対策はゼロベースからの開始であれば30か月程度を要するという試算が認証機関等によって出されています。2024年中に法律が発効され、2026年中に報告義務が適用開始、2027年中に全規定が適用開始となることを考慮すると、対策を今すぐ開始する必要があります。シーメンスでは、普段サイバーセキュリティに馴染みのない方も含め全社でこの問題を理解・共有して頂ける有償セミナーもご用意しています。



シーメンスから提供可能なサービス・製品

目的	サービス	概要
CRAの理解と社内での課題共有	CRA解説セミナー	2時間のプライベートセミナーでCRA概要と対策の必要性・方向性を解説します。普段サイバーセキュリティに馴染みのない部門や経営層の方にも分かりやすい内容となっており、社内で課題共有し対策の第一歩を踏み出すきっかけとして最適です。
セキュリティ特性要件対策	IEC62443-3-3アセスメントサービス	IEC62443-3-3要件に基づいて御社の装置・システムを診断し、クリアすべき課題をレポートするサービスです。また、それらの課題をクリアするための具体的かつ現実的な対策の議論をお客様と入念に行い、対策に使える製品もご提案します。
	各種セキュリティ関連製品	産業用ファイアウォールをはじめとして、様々なOTセキュリティ関連製品をご提案可能です。アセスメント結果に基づいて、最もコストパフォーマンスの高い技術的対策をご提案します。
脆弱性処理要件／報告義務対策	IEC62443-4-1アセスメントサービス	IEC62443-4-1要件に基づいて御社の製品開発プロセスのセキュリティレベルを診断し、今後必要となる開発プロセスについてレポートするサービスです。
	プロセス構築・修正支援サービス	アセスメント結果に基づき、御社の製品開発プロセスをIEC62443-4-1が求める水準に改善するための構築・修正支援を行います。セキュア開発プロセスの構築に必要となる様々なドキュメントのテンプレート提供なども含まれます。
	PSIRT構築支援サービス	PSIRTを社内で構築する際にも様々なノウハウが必要です。このサービスではCRAに対応するための必要最低限の要素に絞って、御社PSIRTを最短で運用軌道に乗せるための支援を実施します。
	SBOM導入支援サービス	SBOMは脆弱性管理ツールとしてCRAでも言及されており、PSIRT効果的に機能するためには必要不可欠なツールです。一方でその運用にはノウハウが必要であり、このサービスでは御社PSIRTがSBOMを使いこなし脆弱性管理を行うための導入支援を実施します。
その他	リスク分析サービス	CRA第13条「製造業者の義務」では製品のリスクアセスメントを実施し、その結果を技術文書に記載することが求められています。このリスクアセスメントを代行するサービスとなります。

Contact

Published by Siemens K.K
シーメンス株式会社
デジタルインダストリーズ
プロセスオートメーション事業部　ビジネスディベロップメントGr.

グループマネージャー
シーメンス認定IEC62443スペシャリスト

大島正嗣
E-mail: masashi.oshima@siemens.com
〒141-8641
東京都品川区大崎1-11-1　ゲートシティ大崎ウエストタワー

LinkedInでCRA関連情報を発信しています。
お気軽にフォローください！