CRA対応に役立つOPC UAについて

株式会社ICS研究所

INDUSTRY CONTROL SOLUTION LABORATORY

2025.12.12

©2025 Industry Control Solution Laboratory Co.

本講演の目的

CRAが要求するセキュリティ要件に対し、OPC UAが標準機能としてどのように貢献できるかを解説します

欧州の新たなサイバーセキュリティ法「CRA (Cyber Resilience Act)」が目前に迫っています

CRAは、EU市場でデジタル製品を販売するメーカーに、設計から廃棄までのセキュリティ対応を法的に義務化するものです

このCRA対応の「技術的な拠り所」として、国際規格IEC 62443 シリーズが鍵となります

本講演では、CRAとIEC 62443の関係性、そしてOPC UAがCRA対応にどう貢献できるかを解説します

©2025 Industry Control Solution Laboratory Co.

Agenda

1 CRA (Cyber Resilience Act) とは？

2 IEC 62443シリーズの概要

3 OPC UA と IEC 62443 のマッピング

4 米国の動向（参考）とまとめ

©2025 Industry Control Solution Laboratory Co.

Agenda

1 CRA (Cyber Resilience Act) とは？

2 IEC 62443シリーズの概要

3 OPC UA と IEC 62443 のマッピング

4 米国の動向（参考）とまとめ

©2025 Industry Control Solution Laboratory Co.

1. CRA (Cyber Resilience Act) とは？

EU市場のデジタル製品に関する統一的なサイバーセキュリティ法

背景：脅威の増大と規制の空白

サイバー攻撃の増大、コネクテッドデバイスの急増に対し、既存のEU法ではデジタル製品（PDE:Products with Digital Elements）の必須セキュリティ要件を直接カバーできていませんでした

目的：PDEのセキュリティ確保

EU域内で上市される「デジタル要素を持つ製品（PDE）」のサイバーセキュリティを確保し、ライフサイクル全体でのセキュリティを確保する統一的な法的枠組みを確立する

©2025 Industry Control Solution Laboratory Co.

CRAが対処しようとする2つの主要問題

CRAは、デジタル製品市場における根本的な2つの課題を解決しようとしています

1. 製品のセキュリティレベルが低い

開発段階でセキュリティが考慮されていない

脆弱性に対処するセキュリティアップデートが、不十分

2. セキュリティ情報の不透明さ

メーカは製品の使用環境におけるセキュリティ特性の情報提供が不十分

ユーザ（消費者・企業）が、製品を安全に使用するための情報にアクセスできず、十分なセキュリティ特性を持つ製品を選択できず、また安全な使用方法もわからない

©2025 Industry Control Solution Laboratory Co.

CRAの主な要求事項（メーカーの義務）

デジタル要素を持つ製品（PDE）をEU市場で上市するメーカーは、以下が法的に義務付けられます

1. 設計・開発・生産時の義務: 製品が必須サイバーセキュリティ要件に適合していること（附属書Iパート1に定める）

2. 脆弱性対応プロセスの義務: 製品のサポート期間中（原則最低5年）、必須脆弱性ハンドリング要件に適合するプロセスを整備・運用すること（附属書Iパート2に定める）

3. 報告義務: 積極的に悪用されている脆弱性や重大なインシデントをENISAへ24時間以内に報告すること

4. 適合性評価とCEマーキング: 上記の要件への適合を評価し、「EU適合宣言書」を作成の上、CEマーキングを製品に貼付すること

©2025 Industry Control Solution Laboratory Co.

CRAの適用スケジュールと罰則

CRAはすでに発行（2024年11月）されており、適用開始が迫っています

適用スケジュール

発行：2024年11月20日

適用開始（全面）：2027年12月11日

これ以降、CRA要件を満たさない限りEU市場に出荷できません

先行適用される義務

2026年9月11日：脆弱性・インシデントの報告義務 (Article 14)

2026年6月11日：適合性評価機関に関する規定 (Chapter IV)

違反時の罰則（行政罰）

必須要件 (Annex I) 違反など:

最大 1,500万ユーロ または 全世界年間売上高の 2.5%（いずれか高い方）

その他の義務違反（情報提供など）:

最大 1,000万ユーロ または 2%

不正確・不完全な情報提供:

最大 500万ユーロ または 1%

©2025 Industry Control Solution Laboratory Co.

Agenda

1 CRA (Cyber Resilience Act) とは？

2 IEC 62443シリーズの概要

3 OPC UA と IEC 62443 のマッピング

4 米国の動向（参考）とまとめ

©2025 Industry Control Solution Laboratory Co.

CRA・IEC 62443・OPC UA の関係性

CRAという「法律」と、IEC 62443 / OPC UA という「国際規格」の関係性を整理します

©2025 Industry Control Solution Laboratory Co.

2. IEC 62443シリーズの概要

IACS（産業用オートメーション＆制御システム）セキュリティの国際標準規格

Part 1: General（一般）

コンセプト、用語、モデルを定義

Part 2: Policies & Procedures

資産所有者（ユーザー）やSier等のセキュリティプログラムを規定

Part 3: System（システム）

システム全体のセキュリティ要件とセキュリティレベル（SL）を定義

Part 4: Component（コンポーネント）

コンポーネントの開発プロセスや**技術要件**を規定

（CRA対応の核）

Part 5: Profiles（審議中）

Part 6: Conformity（セキュリティ評価手法）

©2025 Industry Control Solution Laboratory Co.

IEC 62443-4-2：IACSコンポーネントの技術要件

CRAが要求する「必須サイバーセキュリティ要件」に対応する技術仕様（7つの基礎要件）

1. IAC (識別・認証制御):ユーザー、ソフトウェア、デバイスを識別・認証する
2. UC (利用制御):認証されたエンティティの権限を強制し、アクセスを制御する
3. SI (システムインテグリティ):不正な操作や変更からシステムの完全性を保護する
4. DC (データ機密性):通信経路およびリポジトリ内の情報の機密性を確保する
5. RDF (データフロー制限):ゾーンとコンジットにより、不要なデータフローを制限する
6. TRE (イベントへのタイムリーな応答:セキュリティ違反を検知・報告し、対応する
7. RA (リソース可用性): DoS攻撃などによるサービス拒否から可用性を確保する

©2025 Industry Control Solution Laboratory Co.

その他関連するIEC 62443

CRAが要求する「必須サイバーセキュリティ要件」に対応するその他の62443シリーズ

IEC62443-4-1 製品セキュリティ開発プロセス

・セキュアバイデザイン (SD): セキュア設計原則、多層防御、設計レビュー

・セキュア実装 (SI): セキュアコーディング規約、静的コード解析

・問題管理 (DM): 脆弱性レポートの受領、トリアージ、修正、開示のプロセス

・アップデート管理 (SUM): セキュリティパッチの検証、文書化、タイムリーな配信

IEC62443-3-2　セキュリティリスクアセスメント

・初期リスク評価: SUC全体の最悪ケースのリスクを特定する

・初期リスクと許容リスクの比較: 検討したリスクが対象システムの許容範囲に収まっているか判断

・文書化: 評価結果とセキュリティ要件を文書化する

©2025 Industry Control Solution Laboratory Co.

IEC 62443　補足　適合規格取得メーカ

IEC62443-4-2　コンポーネントセキュリティ機能適合　SL１～4

セキュリティレベル	PLC/FA機器メーカー	ロボット等	機械
SL4	–	–	–
SL3	–	GE Power	–
SL2	シーメンス、ロックウェル、フェニックスコンタクト、Bosch Rexroth、BELDEN、三菱電機	ファナック（ロボット、CNC）	-
SL1		ロックウェル（インバーター）	

（2025/11　ICS研究所 調べ）

©2025 Industry Control Solution Laboratory Co.

IEC 62443　補足　適合規格取得メーカ

IEC62443-4-1　コンポーネントセキュリティ開発プロセス適合　ML１～4

成熟度	PLC/FA機器メーカー	ロボット等	機械
ML4（改善段階）	ロックウェル、シュナイダー、BELDEN	--	-
ML3（活用段階）	三菱電機、オムロン シーメンス、フェニックスコンタクト、HMS(Anybus)、ABB、	ファナック	オークマ
ML2（管理段階）	富士電機 ワイドミュラー、SICK*、Bosch Rexroth*	安川、川崎重工、セイコーエプソン	DMG森、FUJI

（2025/11　ICS研究所 調べ）

©2025 Industry Control Solution Laboratory Co.

Agenda

1 CRA (Cyber Resilience Act) とは？

2 IEC 62443シリーズの概要

3 OPC UA と IEC 62443 のマッピング

4 米国の動向（参考）とまとめ

©2025 Industry Control Solution Laboratory Co.

CRA・IEC 62443・OPC UA の関係性

CRAという「法律」と、IEC 62443 / OPC UA という「国際規格」は明確に関連付けられています

©2025 Industry Control Solution Laboratory Co.

3. OPC UA と IEC 62443-4-2 のマッピング

OPC UAは「セキュアバイデザイン」を実装した、データのやり取りの包括的な国際規格です

OPC UAは、その策定当初からセキュリティを中核機能として設計されています

OPC 10000-2 Part2 (セキュリティモデル) の附属書Aには、IEC 62443-4-2 の技術要件（CR）の多くのパートにOPC UAの標準機能が適合することが明記されています

CRAの必須要件は、IEC 62443-4-2の要件と強く関連しています（JRC/ENISAレポート）

結論: OPC UAを採用することは、CRAが要求する技術的なセキュリティ要件（附属書Iパート1）を満たす上で、非常に効率的かつ堅牢なアプローチとなります

©2025 Industry Control Solution Laboratory Co.

IEC 62443-4-2：IACSコンポーネントの技術要件

CRAが要求する「必須サイバーセキュリティ要件」に対応する技術仕様（7つの基礎要件）

1. IAC (識別・認証制御):ユーザー、ソフトウェア、デバイスを識別・認証する
2. UC (利用制御):認証されたエンティティの権限を強制し、アクセスを制御する
3. SI (システムインテグリティ):不正な操作や変更からシステムの完全性を保護する
4. DC (データ機密性):通信経路およびリポジトリ内の情報の機密性を確保する
5. RDF (データフロー制限):ゾーンとコンジットにより、不要なデータフローを制限する
6. TRE (イベントへのタイムリーな応答:セキュリティ違反を検知・報告し、対応する
7. RA (リソース可用性): DoS攻撃などによるサービス拒否から可用性を確保する

©2025 Industry Control Solution Laboratory Co.

OPC UAによる適合例 (1)：識別・認証制御 (IAC)

IEC 62443-4-2 (FR 1) は、すべてのユーザー、ソフトウェア、デバイスの識別と認証を要求

CR 1.1: ヒューマンユーザーの認証

OPC UAの対応

多様なユーザートークンをサポート：
Username/Password、X.509証明書など

CR 1.2: ソフトウェアとデバイスの認証

OPC UAの対応

X.509v3 アプリケーションインスタンス証明書による厳格なアプリケーション相互認証 (Part 2, 4, 6)

Global Security Certificate Management Service (Part 7)

©2025 Industry Control Solution Laboratory Co.

IEC 62443-4-2：IACSコンポーネントの技術要件

CRAが要求する「必須サイバーセキュリティ要件」に対応する技術仕様（7つの基礎要件）

1. IAC (識別・認証制御):ユーザー、ソフトウェア、デバイスを識別・認証する
2. UC (利用制御):認証されたエンティティの権限を強制し、アクセスを制御する
3. SI (システムインテグリティ):不正な操作や変更からシステムの完全性を保護する
4. DC (データ機密性):通信経路およびリポジトリ内の情報の機密性を確保する
5. RDF (データフロー制限):ゾーンとコンジットにより、不要なデータフローを制限する
6. TRE (イベントへのタイムリーな応答:セキュリティ違反を検知・報告し、対応する
7. RA (リソース可用性): DoS攻撃などによるサービス拒否から可用性を確保する

©2025 Industry Control Solution Laboratory Co.

OPC UAによる適合例 (2)：システムインテグリティ (SI)

IEC 62443-4-2 (FR 3) は、システム（通信、データ、ソフトウェア）の完全性（Integrity）の保護を要求

CR 3.1: 通信の完全性

OPC UAの対応

セキュアチャネル (SecureChannel) 確立プロセス (Part 2, 4)にて、メッセージのデジタル署名 (Part 6)情報を交換

Security Policy による署名アルゴリズムの指定 (Part 2)

CR 3.8: セッションの完全性

OPC UAの対応

確立されたセキュアチャネルとセッションID、認証トークンを紐付け、ハイジャックを防止 (Part 2, 4)

©2025 Industry Control Solution Laboratory Co.

IEC 62443-4-2：IACSコンポーネントの技術要件

CRAが要求する「必須サイバーセキュリティ要件」に対応する技術仕様（7つの基礎要件）

1. IAC (識別・認証制御):ユーザー、ソフトウェア、デバイスを識別・認証する
2. UC (利用制御):認証されたエンティティの権限を強制し、アクセスを制御する
3. SI (システムインテグリティ):不正な操作や変更からシステムの完全性を保護する
4. DC (データ機密性):通信経路およびリポジトリ内の情報の機密性を確保する
5. RDF (データフロー制限):ゾーンとコンジットにより、不要なデータフローを制限する
6. TRE (イベントへのタイムリーな応答:セキュリティ違反を検知・報告し、対応する
7. RA (リソース可用性): DoS攻撃などによるサービス拒否から可用性を確保する

©2025 Industry Control Solution Laboratory Co.

OPC UAによる適合例 (3)：データ機密性 (DC)

IEC 62443-4-2 (FR 4) は、通信および保存データの機密性（Confidentiality）保護を要求

CR 4.1: 情報の機密性

OPC UAの対応

セキュアチャネルサービスセットによる通信の暗号化 (Part 2,4,6)

Security Policy による署名アルゴリズムの指定 (Part 2)

CR 4.3: 暗号化の使用

OPC UAの対応

業界標準の非対称暗号（鍵交換・署名）および対称暗号（メッセージ保護）のアルゴリズムを規定 (Part 2,4,6)

安全な鍵導出（Deriving Keys）プロセス (Part 6)

©2025 Industry Control Solution Laboratory Co.

IEC 62443-4-2：IACSコンポーネントの技術要件

CRAが要求する「必須サイバーセキュリティ要件」に対応する技術仕様（7つの基礎要件）

1. IAC (識別・認証制御):ユーザー、ソフトウェア、デバイスを識別・認証する
2. UC (利用制御):認証されたエンティティの権限を強制し、アクセスを制御する
3. SI (システムインテグリティ):不正な操作や変更からシステムの完全性を保護する
4. DC (データ機密性):通信経路およびリポジトリ内の情報の機密性を確保する
5. RDF (データフロー制限):ゾーンとコンジットにより、不要なデータフローを制限する
6. TRE (イベントへのタイムリーな応答:セキュリティ違反を検知・報告し、対応する
7. RA (リソース可用性): DoS攻撃などによるサービス拒否から可用性を確保する

©2025 Industry Control Solution Laboratory Co.

OPC UAによる適合例 (4)：リソース可用性 (RA)

IEC 62443-4-2 (FR 7) は、DoS攻撃などからのリソースの可用性（Availability）確保を要求します

CR 7.1: DoS保護

OPC UAの対応

Create Session, OpenSecureChannelリクエスト数の管理、高負荷な暗号化処理を行わずにエラーを即時返却 (Part 4)

CR 7.1 RE(1): 通信負荷管理

OPC UAの対応

認証前の処理を最小化：GetEndpointsやOpenSecureChannelなど、認証前に処理するメッセージを限定し、リソース消費を抑制 (Part 4)

©2025 Industry Control Solution Laboratory Co.

Agenda

1 CRA (Cyber Resilience Act) とは？

2 IEC 62443シリーズの概要

3 OPC UA と IEC 62443 のマッピング

4 米国の動向（参考）とまとめ

©2025 Industry Control Solution Laboratory Co.

4. 米国の動向（参考）

欧州のCRAと同様、米国でもサイバーセキュリティ規制が急速に進展しています

大統領令 (EO 14028)

連邦政府のサイバーセキュリティ強化。SSDFやSBOMの導入を推進

NIST SP800シリーズ / CSF

SP800-82 (IACS) や CSF (フレームワーク) など、リスクベースのガイドラインを整備

CIRCIA (2022年)

重要インフラ事業者に対し、大規模インシデントやランサムウェア支払いのCISAへの報告を義務化

CMMC 2.0

国防総省 (DoD) のサプライチェーンに参加する企業に求めるセキュリティ認証制度

©2025 Industry Control Solution Laboratory Co.

まとめ

OPC UAの採用は、CRAの技術的要件に対応するための実証済みで効率的な選択肢となります

CRA対応は待ったなしの経営課題: デジタル製品メーカーに対し、全ライフサイクルにわたるセキュリティ対応を法的に義務化します（2027年12月適用開始）

IEC 62443が技術的ベース: CRAの技術的要件への適合性を示す「整合規格」のベースとして、IEC 62443（特に4-1と4-2）が最有力です

OPC UAはIEC 62443に適合: OPC UAは、IEC 62443-4-2が要求する「識別・認証」「完全性」「機密性」「可用性」といった技術要件の一部を標準機能として実装しています

©2025 Industry Control Solution Laboratory Co.

オンデマンドビデオ講座 eICS

時間や場所を問わず制御システムセキュリティの知見や技術、管理手法を繰り返し学べます。

制御システムセキュリティ実務能力検定

制御システムセキュリティ対策に必要な実装技術や管理手法やシステム設計技法の実務能力が身についていることを検定します。

リモートセミナー研修

社内の認識合わせから、制御システムセキュリティの知見や技術、eICSの活用法までを紹介します。

コンサルティング

認識改革や体制改善でサイバー攻撃に強い製品を送り出せる企業力を目指します。

ICS研究所による 4つの制御システムセキュリティ対策プログラム

©2025 Industry Control Solution Laboratory Co.