一般社団法人 日本電気計測器工業会

産業 IoT 分野における「機能安全とセキュリティ」の認証制度に関する調査報告書

２０２０年６月

一般社団法人　日本電気計測器工業会

目次

1. はじめに

1.1 概要

本書は、産業 IoT 分野における機能安全とセキュリティの認証制度に関する、国内国外の状況と、標準化の動向についてヒアリング調査結果を報告するものである。

1.2 目的

産業 IoT の導入が進みつつあるが、これに適用する機器／システムへのセキュリティ脅威による産業保安が課題となっている。産業 IoT のリスクを低減する方法はふたつあり、ひとつは脆弱性を塞ぎ脅威の可能性を低減するセキュリティ対策(IEC 62443：産業通信ネットワーク／ネットワークとシステムのセキュリティ)であり、もうひとつは被害を抑えるセーフティ（安全）対策(IEC 61508：電気・電子・プログラマブル電子安全関連系の機能安全)である。産業 IoT 機器/システム購入者は、購買対象がこれらの規格の両方あるいはいずれかに適合することを求める。購入者が独自に機器のセキュリティ性や安全性を判断することが技術的に難しいからである。

ここで、2 点の課題がある。一点目が規格適合性認証のグローバルにおける日本の不利な状況、二点目がセーフティとセキュリティの両立性の達成である。一点目の規格適合性認証について、欧米の認証機関が市場を占有しており、国内企業は文書翻訳や審査において工数とコストの点で不利を受けている。国内企業の海外市場進出を拡大するためには、国内認証機関の育成とともに、規格適合性の認証手順の標準化および国内展開が課題となる。二点目のセーフティとセキュリティの両立性については、 IEC TR 63069（機能安全とセキュリティのフレームワーク）でようやく規格化が端緒についたところであり、認証のベースとなる IS 化や認証基準の策定は、世界的にも今後の課題として残されている。セーフティとセキュリティは前提条件の異なる技術的課題の難しさも相まって、これまでの認証とは異なる要件となると考えられる。

本報告書は、セーフティとセキュリティを両立できる産業 IoT 機器／システムの規格を日本主導で策定し、その認証体制を日本主導で育成することを目的とする。

1．3　内容

上記課題に対して、産業用 IoT 分野におけるセーフティとセキュリティに関連する下記項目を調査し、関連技術と認証制度の提案可能性について検討する。

①　国際標準化の動向

以下の調査候補を対象に、規格適合認証方法の国際標準化の動向について、委員会等への参加またはヒアリング等により調査する。

調査候補：IECEE/CMC/WG32(安全認証)、IECEE/CMC/WG31(セキュリティ認証)、IEC/TC65/WG20（安全セキュリティ両立）、IEC/CAB/WG17(サイバーセキュリティ)、ISA 84(プロセス安全)、ISA 99(制御セキュリティ)等

②　各国認証制度の動向

以下の調査候補を対象に、各国認証制度の動向（CB スキームへの対応、審査手順と期間、審査体制と審査官資格と審査実績等）について、参加またはヒアリング等により調査する。この調査結果を踏まえて、認証制度の日本での展開方法等について検討する。

調査候補：政府系機関、業界団体（NAMUR,ARC 等）、認証機関、海外産業分野展示会（SPS Drive、Automation week 等）等

③　国内の関連技術・認証制度の動向

以下の国内の調査候補を対象に、国内の関連技術および認証制度の特徴を調査する。この調査結果を踏まえて、国内の関連技術や、既に国内にて運用されている制度について、それらを国際標準に提案できるか、その可能性を検討する。なお、提案先は、既存 WG または新規 WG のいずれかであり、海外調査の結果をもって判断する。

調査候補：NECA のセーフティアセッサ制度、および CMC/CoPC(要員認証)の状況、CSSC の EDSA 認証制度、IPA の独自認証制度(情報処理安全確保支援士)、CSMS(制御セキュリティマネジメントシステム)等

2. 実施内容

2. 1 実施概要

① 国際標準化の動向

安全とセキュリティに関連する規格と規格適合性認証を規定する規格団体と業界団体、認証機関（規格団体 IEC/TC65、IEC/CAB、業界団体 ISA 等）等に関して調査した。規格適合認証は認証機関独自の方法に基づいているが、この標準化の動きについて調査した。

調査対象：

a) IEC/CAB/IECEE/CMC/WG31 標準化委員会

b) IEC/CAB/IECEE/CMC/WG32 標準化委員会

c) IEC/TC65/WG20 標準化委員会

d) ISA S84 標準化委員会

e) ISA S99 標準化委員会

② 各国認証制度の動向

規格適合認証は国・分野によって状況が異なる。規格適合認証に関連する規制当局、業界団体、認証機関等の状況について調査した。

調査対象：

a) 政府系機関 A

b) 業界団体 A

c) NAMUR

d) ARC

e) Exida

f) 認証機関 A

g) SPS Drive Show 展示会

h) 2019 International Conference on the EU Cybersecurity Act

③ 国内の関連技術・認証制度の動向

日本の状況（認証機関 CSSC、業界団体 NECA 等）について各国との違いを調査し、日本から提案できる技術等を検討した。

CSSC、NECA、認証機関 B 等にて既に実施している認証制度の状況を調査した。

調査対象：

a) （研究組合）制御システムセキュリティセンター(CSSC)

b) （一社）日本電気制御機器工業会（NECA）

c) 認証機関 B

d) （独法）情報処理推進機構（IPA）

e) 経済産業省サイバーセキュリティ課

2．2 実施詳細

① 国際標準化の動向

a) IEC/CAB/IECEE/CMC/WG31 標準化委員会

調査日：2020 年 2 月 3 日、LakeForest, CA, USA

内容：IECEE/CMC/WG31 では IEC62443 の認証スキーム（OD-2061）の改定を行っている。また、サイバーセキュリティに関する要員認証の必要性評価もスコープとなっている。

CAB/WG17 の解散に伴い、WG17 で行っていた活動を WG31 が引き継ぐこととなった。また、CBTL となるための要件について、IECEE 02-2 では 10 のプロジェクトが要求されているが、IEC62443 についてはこれを緩和させる方向で引き続き議論することとなった。

b) IEC/CAB/IECEE/CMC/WG32 標準化委員会

調査日：2019 年 10 月 16-17 日、大阪

内容：IECEE/CMC/WG32 では、機能安全関連製品の認証方法について議論を行っている。メンバーは、TUV, UL, CSA などに加えて、メーカーも 3 社参加している。機能安全の規格適合審査手順が共通化されれば、複数の認証機関を相手にするにも、国内認証機関にテコ入れするのも有益である。

2019 年 1 月の会議から議論が加速している。5 月の CMC 会議で WG32 に対して出された指摘事項への対応を主に議論した。特に、Test Report form/Evaluation Test Form)の共通化、OD-2064 の修正、工場監査の必要性、本 WG 広報のためのワークショップ、試験装置への要求などが議論された。いずれも NCB/SPTL 視点からの共通化を探っている。

調査日：2020 年 2 月 10-11 日、LakeForest, USA

内容：10 月の大阪会議の合意を踏まえての議論が継続された。

Test Report Form と Evaluation Report Form も承認された。NCB/SPTL の FS エンジニアについても原案作成する。また、関係者(審査機関)対象の Technical Workshop も計画しており、内容と担当の議論があった。製品認証に関しては、既にビジネスが存在しているので、各認証機関は現状から制度を大きく変えずに妥協点を見つけようとしている。

c)　IEC/TC65/WG20 標準化委員会

調査日：2020 年 2 月 10-12 日、LakeForest, USA

内容：IEC/TC65/WG20 は Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security、すなわち制御システムの機能安全とセキュリティの両立を目的とする。

同 WG は 2019 年に TR 63069 を発行した。その後、同じスコープにおいて技術的詳細を示すために、2020 年より新たな TS(技術仕様)を作成する方針で議論を進めている。今回の会議では、今後の方針、現状 TR へのコメント回答、標準に盛り込みたい技術内容について議論が行われた。今後 Web 会議を重ねて内容を詰める予定である。

d)　ISA S84 標準化委員会

調査日：2019 年 10 月 25-28 日、SanDiego, USA

内容：ISA(International Society of Automation)は北米中心の計測自動制御学会であり、オートメーションに関する各種規格(S84 機能安全、S99 セキュリティ)の策定、出版・トレーニングなどの事業を行っている。ISA の年次総会において、主要な標準化活動の報告があり、S84 プロセス機能安全の Paul Gruham 議長(ISA 会長)に適合性評価に関する質問を行った。ISA はエンジニアの教育・認定制度に力を入れているが、製品認証は認証機関に任せている。

e)　ISA S99 標準化委員会

調査日：2019 年 10 月 25-28 日、SanDiego, USA

内容：Leader's Meeting は、ISA の総会、各種戦略委員会および支部長会議・トレーニングを実施する。報告者は、ISA 日本支部長として本会議に出席できるので、ISA 戦略について調査を行った。

ISA84 プロセス機能安全は IEC61511 と連携しており、製品認証は外部企業(Exida)が実施している。ISA99 サイバーセキュリティは、ISCI(ISA Security Compliance Institute)が CSA (Component Security Assurance)認証のスキームオーナーとして認証を推進している。特記すべきは、ISA99 の Eric Cosman が ISA 次期会長であり技術者教育と認定に力を入れるとの発表である。

調査日：2019 年 11 月 22-24 日、Manheim, Germany

内容：ISA(International Society of Automation)の委員会である ISA99 は、産業オートメーションと制御システムのセキュリティに関する議論を行い、IEC TC65/WG10 とのリエゾンを組んで規格文書 ISA/IEC 62443 を策定している。参加メンバーは特定の組織を代表せず、セキュリティ標準策定の専門家として任意に参加・議論する。本ミーティングでは ISA99 の目的や活動・議論の進め方のイントロダクション、課題の議論、および各 WG の活動について活発な議論がされた。今回の参加者はベンダー、コンサルタントおよび BSI(ドイツ), NIST(アメリカ)などの公的機関のメンバー等。主な課題は、62443 文書の有効活用（IECEE 認証ほか）、利用を促進するためにシンプルさや一貫性が求められること、62443 に登場する各ロールの明確な定義が必要であること等。

ISA/IEC 62443 のさらなる利用を促進するために、今後 62443-2-1 で見直される要件項目と従来の 62443-3-3, 4-2 の技術要件および 62443-2-4, 4-1 の組織要件との整合性や、セキュリティ評価指標としての SL(Security Level), ML(Maturity Level), SPE(Security Program Elements)の整理等が必要であり、引き続き議論が継続される。また 62443 の普及促進・他組織連携を行う団体である ISA GCA(ISA Global Cybersecurity Alliance)が発足している。ISA GCA は ENISA との関係構築をしようとしているが現段階での影響力は不明。

② 各国認証制度の動向

規格適合認証は国・分野によって状況が異なる。規格適合認証に関連する規制当局、業界団体、認証機関等の状況について調査した。

調査対象：

a) 政府系機関 A

調査日：2019 年 11 月 18 日、欧州

内容： 欧州サイバーセキュリティ認証制度は産業セクター毎にスキームが作成されるが、第一弾として SOG-IS をベースにした認証制度の開発が進められており、今後 1 年以内に完成予定である。どの基準を採用するかはスキームのデザイナーによるところであるが、IEC62443 も産業用制御機器分野の候補の一つとのコメントも聞かれた。

b) 業界団体 A

調査日：2019 年 11 月 20 日、欧州

内容：業界団体 A は非営利民間組織。サイバーセキュリティに関するステイクホルダーが参加し、既存の認証制度に関する調査や欧州サイバーセキュリティ認証制度の提案を行っている。

業界団体 A が公開しているレポートは EC がサイバーセキュリティ認証フレームワークを提案する際のサポートとして作成したものであり、これ自体が EU サイバーセキュリティ認証スキームになるというものではない。現在、コモンクライテリアをベースに認証制度が議論されているが、現在、SOG-IS MRA に入っていない EU Member States にはコモンクライテリアに基づく評価キャパシティがない為、ラボの評価能力をどのように揃えていくのかといった課題がある。

c) NAMUR

調査日:2019 年 11 月 21 日、Mannheim, Germany

内容:産業用制御機器のユーザーを主体とした団体で、1949 年に発足し、現在 165 の企業・組織が加入している。ユーザー以外にもシステムインテグレーターや政府系組織（BSI(ドイツ情報セキュリティ庁)）が加入している。加入企業・組織のうち、ドイツからは 132 社（団体）と最も多い。また、中国からは 8 社（団体）が参加している。40 の WG があり、ガイドラインの作成や脆弱性のデータ交換等を行っている。今回のミーティングには米国 NIST からも参加があり、NIST Cybersecurity Framework についての説明を行っていた。

NAMUR は基本的に特定バージョン製品に対する認証を好まない。現状では規制で認証を求められていないので、ベンダーに対して認証取得を要求あるいは推進しているという訳ではない。また、欧州サイバーセキュリティ認証については、当局がエキスパートを集めて議論を始めたところと認識されているが、現段階では詳しいことは把握できなかった。

d) ARC (ARC Advisory Group)

調査日：2019 年 12 月 11 日、Austin, USA

内容：ARC は米国に本部を置く産業界および社会基盤を対象とする調査／提言を行う企業であり、ビジネスシステムから製品／設備ライフサイクル管理・サプライチェーン管理・操業管理・エネルギ管理・先進オートメーションシステムまでを幅広くカバーしている。

米国においても IEC62443 が受け入れられてきている一方で、その他の認証（UL CAP やアキレス認証）についてはプレゼンスが低下している。また、ISASecure は IEC 62443 をベースとしたセキュリティ人材に関する認証制度があり、この要員認証制度を国際的に広めたいとは思うが、IEC では要員認証がない。そのため、国際的に認められる制度にしたい、との事であった。

e) Exida

調査日：2019 年 12 月 12 日、Philadelphia, USA

内容：Exida は 1999 年に設立された米国の試験認証機関であり、機能安全及びサイバーセキュリティに関する試験認証サービスを行っている。IEC62443 をベースとした ISASecure 認証の認証機関として登録されている。

ISASecure に要員認証制度があるが、Exida でも CACE,CACS といった類似の要員認証制度がある。US だけでなくアジアでも採用が増えている。（日本だけ取り残されているという状況）

TR63069 は使っていないがセキュリティとセーフティの同時評価は行っている。同時に評価してほしいというニーズは存在する。

f) 認証機関 A

調査日：2019 年 11 月 25 日、欧州

内容：認証機関 A は欧州に本部を置く認証機関。産業インフラ、セキュリティ、機能安全、ロボティックス、産業機械など数多くの製品安全試験、検査、および認証サービスを提供している。

サイバーセキュリティ認証について関心が高まる中、IEC62443 に関する評価・認証サービスを行っている。

g) SPS Drive Show 展示会

調査日：2019 年 11 月 27 日、Nurnberg, Germany

内容：SPS Drive Show は、オートメーション関連でドイツ最大の展示会であり、Industry4.0 関連で盛り上がりを見せている。

多くの企業が IEC62443(3-3, 4-1, 4-2)の認証取得を始めている。大手企業が IEC62443 シリーズの認証取得・規格適合を進めているところ、サプライチェーンの中で中小企

業にも IEC62443 認証取得の動きが進んでいる。現在のところ規制では認証を求められないが、顧客からの要求により規格適合を進めている企業が多い。

h)　2019 International Conference on the EU Cybersecurity Act

調査日：2019 年 11 月 18-19 日、Brussel, Belgium

内容：ENISA や ECSO 等の公的機関、HP や HUAWEI 等のメーカー、SGS や TUViT 等の認証機関から約 200 名が参加し、欧州における基準認証制度の現状や欧州 Cybersecurity Act の方向性に関するプレゼンテーションが行われた。

欧州 Cybersecurity Act の下で作成される認証スキームについては、第一弾としてコモンクライテリア（ISO/IEC 15408）をベースとしたスキームの開発が進んでいる。産業・自動制御システム向けの規格としては IEC 62443 にも言及されており、今後作成される認証スキームの一部として扱われる可能性がある。他方、認証スキームについてはまだ議論が始まったばかりで、現状において確たる方向性が見えているものではない。認証スキームはそれ単独でとらえられるものではなく、NIS Directive のコンテキストの中で動くべきとのコメントも聞かれ、欧州のサイバーセキュリティ政策全体の中の一つの柱として認証制度をとらえる必要がある。

③ 国内の関連技術・認証制度の動向

日本の状況（認証機関 CSSC、業界団体 NECA 等）について各国との違いを調査し、日本から提案できる技術等を検討した。

CSSC、NECA、認証機関 B 等にて既に実施している認証制度の状況を調査した。

調査対象：

a)　（研究組合）制御システムセキュリティセンター(CSSC)

調査日：2019 年 9 月 10 日、多賀城

内容：CSSC は制御システムのセキュリティ対策の研究組合であり、ISCI の EDSA (Embedded Device Security Assurance)認証スキームに基づいた製品認証を行っている。

審査部門は ISO 17025 審査機関の認証を受けており、国内唯一の制御セキュリティ製品認証機関である。現在、4 社 5 製品の認証実績がある。
注)EDSA は 2019 年に改訂され、CSA(Component Security Assurance)認証となった。

b)　（一社）日本電気制御機器工業会（NECA）

調査日：2020 年 1 月 17 日、浜松町

内容：NECA は電気制御機器の工業会であり、特に ISO/IEC に適合した機械安全の啓もう普及に力を入れている。機械安全の要員認証制度であるセーフティアセッサ制度のスキームオーナーであり、同制度の JIS B 9971 化および IECEE/CMC/WG34 要員認証のコンビナを務めている。

セーフティアセッサ制度は 16 年かけて約 18000 人規模となり、アジア中心に海外展開も行っている。同制度は学会発表を通じて欧米にも知られており、IEC と共同で国際標準化を進めている。IECEE/CMC/WG34 は機械安全だけでない幅広い要員認証スキームを開発しており、機能安全やセキュリティ要員も視野に入れている。

c)　認証機関 B

調査日：2019 年 10 月 15 日

内容：認証機関 B は製品やマネジメントシステムの認証機関であり、IEC 62443-2-1 をベースにした CSMS (Control-system Security Management System)認証を行っている。同制度は、アセットオーナーのためのセキュリティマネジメント認証制度である。

認証機関 B から CSMS 認証を取得しているのは数社である。

c)　（独法）情報処理推進機構（IPA）

調査日：2019 年 9 月 20 日、丸の内

内容：IPA 産業サイバーセキュリティセンターは、社会インフラ等へのサイバー攻撃対策に向けた、攻撃情報の調査、模擬プラントを用いた演習や人材育成を進めている。

これまでも制御システムサイバーセキュリティの中核人材育成プログラムおよび国家資格である情報処理安全確保支援士の試験運用などを進めてきた。これに加えて、11

月より「製造・生産分野の管理監督者層向けプログラム」を実施することになった。職場・現場におけるセキュリティ対策に当たる人材は決定的に不足しており、分野と職制に適したカリキュラムの開発が望まれている。

d)　METI

調査日：2019 年 11 月 6 日、霞ヶ関

内容：METI サイバーセキュリティ課に、IoT や制御システムのセキュリティ対策に関する取り組みや制度についてヒアリングを行った。

同課では IT 人材モデルのセキュリティ拡張(ITSS+)や、情報処理安全確保支援士制度などのサイバーセキュリティ人材強化政策を進めている。今後、産業分野の IoT 活用が本格化する中、IoT や安全分野も踏まえたセキュリティ人材を、IPA や教育機関と連携して育成していく。また、欧州セキュリティ法や米国規制との対応についても検討中である。

2．3　その他

今回の調査対象外であるが、関連する IEC/CAB の動きがあったので、ここに記す。

a)　ACSEC(Advisory Committee on Information security and data privacy)委員会

調査日：2019 年 10 月 22 日、上海

内容：ACSEC は ISO/IEC のセキュリティとデータプライバシーに関するアドバイサリー委員会であり、ISO/IEC のセキュリティ関連規格を横通しで管轄している。

これまでサイバーセキュリティの適合性を議論していた CAB/WG17 を解散し、IECEE/CMC/WG31 サイバーセキュリティに統合する。また、ENISA との連携を進めるとの決定を下した。結果、IECEE/CMC/WG31 の役割はさらに重要となる。

3. 考察

本報告書は、安心できる産業 IoT 機器／システムの規格を日本主導で策定し、その認証体制を育成することを目的とする。そのための課題は２点あり、一点目が規格適合性認証のグローバルにおける日本の不利な状況、二点目がセーフティとセキュリティの両立性の達成である。

（1）各国と国内の認証制度の動向

２．２②と③が対応する調査内容となる。欧州でも米国でも、IEC 規格等に適合する制御機器やシステムの製品認証および開発・運用組織認証スキームが開発済みあるいは運用済みであり、さらに新しい制度が検討されつつある。特に、セキュリティに関しては欧州サイバーセキュリティ法、米国カリフォルニア州などの法整備により強制化の見通しがある。

他方、日本では世界に先駆けて IEC 62443-2-1 をベースにした CSMS 認証制度が開発されたが、企業からは認証取得に対するインセンティブ（法的要求・取引先からの要求・税制優遇等）がないとの声が聞かれており、認証は普及していない。

また、要員力量の認証は、日本（NECA）がリードして IECEE/CMC/WG34 で手順書の開発を進めている。NECA は機械安全（セーフティアセッサ）であったが、WG34 は機能安全とセキュリティを含む汎用性のあるスキームを策定している。さらに、セキュリティ人材については IPA において国家資格「情報処理安全確保支援士」や中核人材、製造・生産分野の管理監督者層のプログラムを開発済みである。しかし、現在のところ世界的に普及している要員認証制度はない。いま、IECEE が機能安全、セキュリティ等の認証手順の検討を進めているので、日本からも国内のこれらの認証制度を紹介するべきである。

（2）セーフティとセキュリティの両立性の国際標準化動向

２．２①と②の一部が対応する調査内容となる。機能安全は IEC 61508、サイバーセキュリティは IEC 62443 が基本規格として多く参照されており、米国の ISA S84 と S99 も IEC と連携している。制御システム、とくに重要インフラを支える制御システムは安全・安心が求められ、日本の制御システムはこの点で高く評価されている。従って、機能安全とサイバーセキュリティの標準化は注視し続けるべきである。

機能安全とサイバーセキュリティの両立に関して、日本提案の IEC TR 63069 が 2019 年に発行された。さらに多くの技術要求を盛り込んだ技術仕様(TS)の策定を開始することになった。日本的な制御システムの安全・セキュリティの考え方や方式が認められ、大きな改修や設計変更なく展開できるように、安全とセキュリティの両立の標準化を推進すべきである。

4. 今後の課題

社会インフラや産業システムを支える制御システムの機能安全とセキュリティは、IoT 時代にますます重要となる。そのため、両者の基本規格である IEC 61508 機能安全と IEC 62443 サイバーセキュリティが世界的に注目されている。また、両者を統合する IEC TR 63069 機能安全とサイバーセキュリティの両立規格も、日本提案で進めている。社会インフラや製造業などの制御システムの安全とセキュリティの両立性は、それらの製品に強い日本企業にとって重要であり、今後も標準化に積極的に関与すべきである。

調査結果からは、安全やセキュリティ規格の適合性評価、とくに CB スキームが世界的に注目されており、この標準化と各国の法整備状況も注視しなければならない。機能安全やサイバーセキュリティの認証制度は、ISO/CASCO よりも IEC/CAB/IECEE が積極的であることが調査により明らかになった。

制度化が先行することや過去からの商習慣から、欧米においては日本に先んじて認証の普及が始まっている。このまま日本での認証活用が後手に回ってしまうと、日本企業においても欧米認証機関の活用が進み、欧米認証機関が認証市場を独占することとなる。そのような状況となると、費用面などで企業の負担が増すだけでなくルール形成においても不利な状況となりかねない。そのため、IEC62443 を始めとした国際標準の法規制等への活用を進め、国内での普及を進めると同時に、国内の認証体制の整備を進める必要がある。併せて、中小企業にも規格・認証を活用しやすい環境を整える観点から、当該規格の JIS 化が必要である。

制御システムの機能安全とセキュリティの標準化、および認証体制の整備は、日本が世界に取り残されないために積極的に推進すべき課題である。

一般社団法人 日本電気計測器工業会

---------禁無断転載----------

産業 IoT 分野における「機能安全とセキュリティ」の認証制度に関する調査報告書

本件についてのお問合せ先

〒103-0014　東京都中央区日本橋蛎殻町２-１５-１２

一般社団法人 日本電気計測器工業会

TEL：03-3662-8183

政策課題グループ