制御システムセキュリティへの対応

独立行政法人情報処理推進機構（IPA）
情報セキュリティ技術ラボラトリー 研究員
入澤　康紀

産業分野や重要インフラ分野などに用いられる制御システムのセキュリティへの対応の重要性を、脅威の高まりと、米国をはじめとした国際動向を背景に解説。制御システムのセキュリティに関する国際基準である IEC62443 の構成と内容、独立行政法人情報処理推進機構（IPA）の提案・推進する本基準を用いた認証制度の確立に向けたパイロットプロジェクトについて解説。

1　はじめに

1.1　制御システムの概要

制御システムは、生産工程やプロセスの制御の自動化など、様々な用途で工数の低減や生産性の向上を目的に利用されている。

最近の制御システムは、情報系のシステムとはファイアウォールなどで分離されている。制御システムのエリアでは、下記の図 1 に示すように、アプリケーションや管理システムなどが動作する上位のレイヤに Windows や UNIX 系の汎用のサーバやパソコンなどで構成されており、標準プロトコルが利用されている。実際の制御にかかわるコントローラやセンサーなどの下層部分は独自のプロトコルやハードウェア、OS などが利用される割合が高く固有の仕様により構成されている。

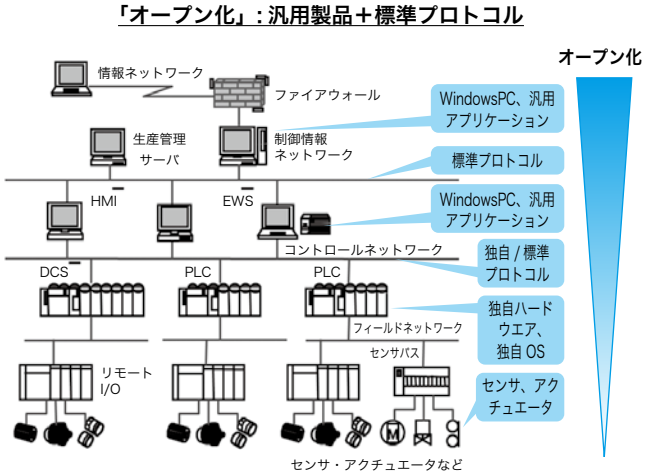


図 1　オープン化が進む制御システムの構成※ 1

1.2　制御システムセキュリティの課題

従来、制御システムは事業者ごとに固有の仕様部分が多く、詳細な内部仕様などを把握しない限り、外部からの攻撃は難しいものと考えられていた。しかし、近年、汎用プラットフォームや標準プロトコルが採用され、更にメンテナンスや管理の目的で外部ネットワークに接続されるなど、事業者及びシステム開発企業の利便性向上やコスト低減が図られている反面で、攻撃対象になりやすいという課題に直面している。さらに、攻撃の糸口となり得る産業用制御システムのソフトウェアの脆弱性の報告件数は大幅に増加している（図 2）。

加えて、これらの産業用制御システムに用いられるソフトウェアの脆弱性については、その特性から、他の一般のソフトウェアに比べて深刻度レベル※ 2（CVSS※ 3 による分類）の高い脆弱性が多くを占めているという特徴があり、対応の必要性が高いと考えられる（図 3）。

1.3　制御システムセキュリティの動向と国内の取り組み

エネルギー、水道、生産ライン、化学プラント、輸送・通信など、重要インフラの制御システムに影響を

【脚注】
※ 1　計測展 2011 TOKYO テクニカルセミナー資料 http://www.ipa.go.jp/security/vuln/documents/TechnicalSeminar2011.pdf
※ 2　CVSS を用いた、脆弱性の深刻度を同一の基準の下で定量的に比較。CVSS については次脚注参照。
※ 3　共通脆弱性評価システム CVSS(Common Vulnerability Scoring System) は、情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法を提供している。
共通脆弱性評価システム CVSS 概説
http://www.ipa.go.jp/security/vuln/CVSS.html

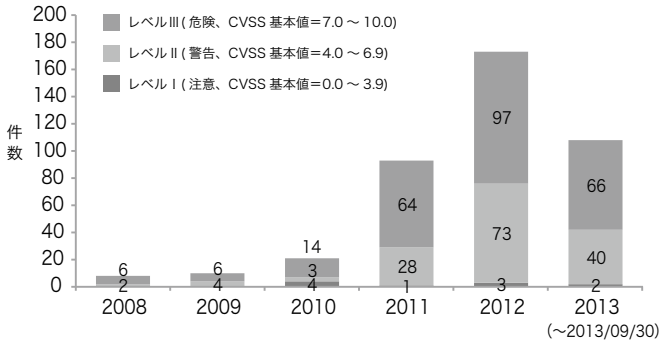


図２　産業用制御システムに関するソフトウェアの脆弱性の深刻度別件数

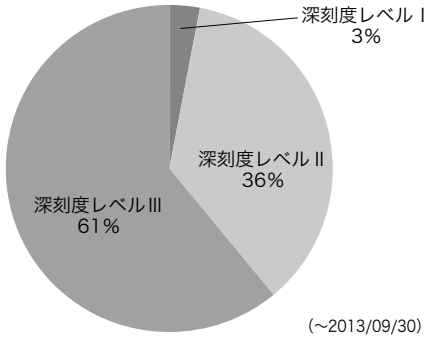


図３　産業用制御システムに用いられるソフトウェアの脆弱性の深刻度別の割合

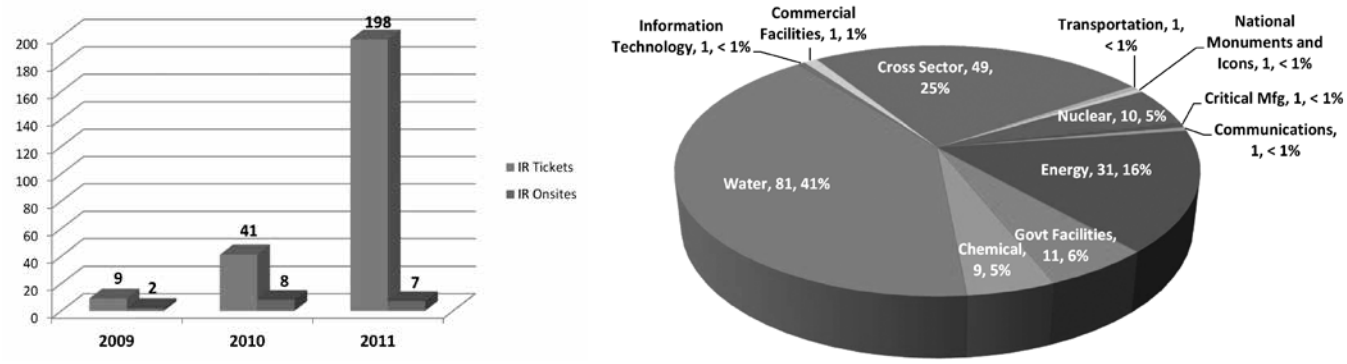


図４　ICS-CERT の 2009-2011 年インシデントレスポンス件数及び 2011 年の分野別報告割合

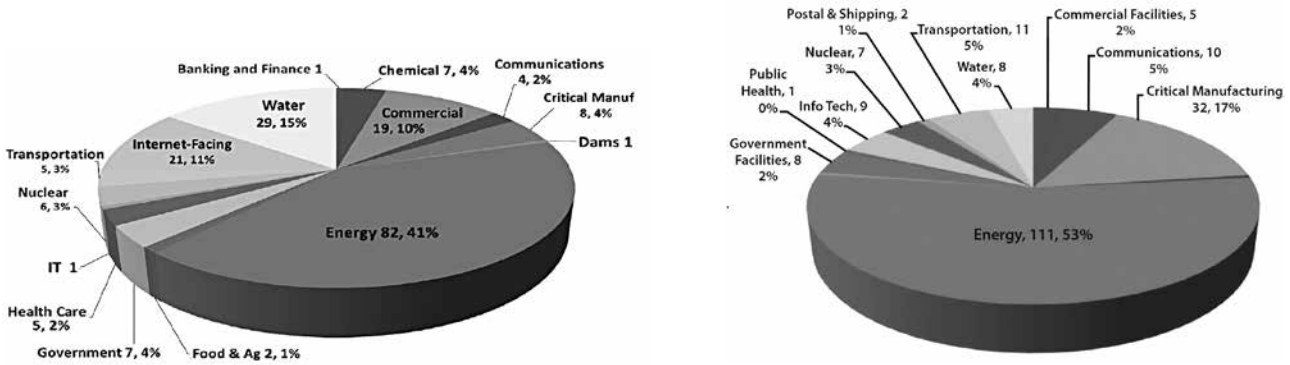


図５　2012 年（FY）及び 2013 年（10 月～翌 5 月）における分野別インシデントレスポンス件数

与えるインシデントが増加傾向にある。米国土安全保障省（Department of Homeland Security：DHS）の公表によると、過去 3 年間の米国内の制御システムインシデントの報告件数は、2009 年が 9 件、2010 年は 41 件、2011 年は 198 件と、急激な増加傾向にあることが報告されている※4（図 4）。

この報告の中では、水道、エネルギー分野でのインシデント報告件数が特に高い割合となっている。さらに、2012 年においても、インシデント報告件数は 198 件※5（※ 10 月～翌 9 月）と、依然として高い水準にあり、特にエネルギー分野において著しい増加が見られる（図 5）。また、2013 年においても 5 月末時点で既に 204 件※6（10 月～翌 5 月）が報告されている。

【脚注】

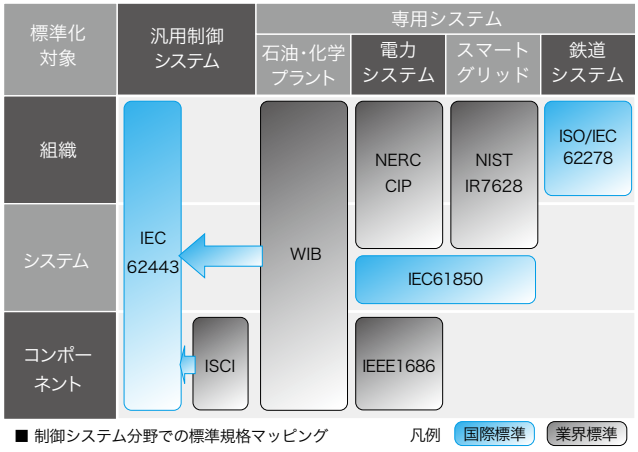
※ 4　http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT Incident Response Summary Report (2009-2011).pdf

※ 5　http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf

※ 6　http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

このような状況下において、制御システムへのサイバーセキュリティ対策は国家の安全保障、危機管理上重要な課題となってきている。

重要インフラの一端を担う制御システムが攻撃された場合、システムの停止や誤作動などにより、社会インフラへ大きな影響を及ぼす危険性がある。海外では、制御システムセキュリティに関する国際規格の整備が進むとともに、規格に基づく認証制度が確立されてきており、制御システムの輸出の際の要件にも加わり始めている。このような状況を鑑み、2010 年に経済産業省で実施された「サイバーセキュリティと経済研究会」の提言として「制御システムの安全性確保」が挙げられた※7。それを受け、2011 年には同省の下で「制御システム情報セキュリティ検討タスクフォース」が実施され、標準化や評価認証などの実現が検討されてきた※8。



■ 制御システム分野での標準規格マッピング

図 6　制御システム分野での標準規格マッピング

表 1　IEC62443 の構成及び標準化のステータス

分類	規格	現状ステータス	リリース
General	62443-1-1	Ed.1：発行済 Ed.2：ドラフト（CD）	Ed.1：2009.07 —
	62443-1-2	ドラフト（DC）	—
	62443-1-3	ドラフト（DC）	—
	62443-1-4	ドラフト（CD）	—
Asset owner	62443-2-1	Ed.1：発行済 Ed.2：1stDC リリース	Ed.1：2010.10 Ed.2：—
	62443-2-2	提案段階（NP）	—
	62443-2-3	ドラフト（DC）	—
	62443-2-4	ドラフト（CD）	—
System integrator	62443-3-1	発行済	2009.07
	62443-3-2	ドラフト（DC）	—
	62443-3-3	発行済	2013.08
Component Provider	62443-4-1	ドラフト（DC）	—
	62443-4-2	ドラフト（DC）	—

※ CD：Committee Draft、DC：Document for Comments、NP：New Work Item Proposal、FDIS：Final Draft for International Standard

2 制御システム分野に関連する標準規格について

制御システムのセキュリティの標準・基準には、組織やシステムのレイヤに対応したもの、業種や業界に対応したもの等、様々な標準・基準が提案されている。このような状況下において、汎用的な標準・基準として IEC62443 が注目され、一部事業者の調達要件に挙がってきている。一方で、制御システム分野では、既存の業界標準を用いた評価認証が ISCI※9、WIB※10 などで実施されている。ISCI では 2010 年より制御システムを構成する個々のコントローラなどのコンポーネントに相当する製品の認証制度を運用している。WIB では、事業者によるシステムの調達の際のセキュリティ要件を広く規定しており、石油・化学など一部の業界でその認証が利用されてきている。一方で、この評価認証で先行していた ISCI や WIB の要求事項（評価基準）が、IEC62443 のシリーズに標準案として提案される動きとなっている（図 6）。換言すると、組織からコンポーネントまでのレイヤをカバーする汎用の制御システムセキュリティに対する国際標準が、評価認証スキームを兼ね備えることになり、その適用や普及が推進されるものと考えられる。次項では、この IEC62443 の構成と内容について解説する。

3 工業用プロセス計測制御のセキュリティ規格（IEC 62443）

国際電気標準会議（International Electrotechnical Commission：IEC）では、電気、電子技術分野の国際標準・規格を作成し、その普及を図ることを目的としている。

【脚注】

※ 7　http://www.meti.go.jp/press/2011/08/20110805006/20110805006.html

※ 8　http://www.meti.go.jp/committee/kenkyukai/shoujo/controlsystem_security/report01.html

※ 9　ISCI：ISA Security Compliance Institute（米国の ISA セキュリティ適合性協会）の略称。ISA のメンバのコンソーシアムにより創設された EDSA 認証の制度運営元（スキームオーナ）である。http://www.isasecure.org/

※ 10　Working-party on Instrument Behaviour の略称、1982 年以降は International Instrument Users' Association と呼称。欧州石油メジャーが中心となり、制御機器ベンダに対するセキュリティ調達要件を規定している。

IEC を構成する専門委員会（Technical Committee：TC）の一つである TC65 では、工業用プロセス計測制御に関する標準化を行っている。TC65 の配下にある WG10 では、ネットワーク及びシステムのセキュリティに関する標準化を推進している。本稿では、WG10 において策定中の規格である「IEC62443」の標準化活動について解説する。

IEC62443 は大別して 4 つの分類があり、発行済み、策定中の規格を合わせて総計 12 の規格が存在する（表 1 [ドラフト段階のステータスは 2012 年時点の参考値]。

[IEC62443-1 シリーズ]

IEC62443 の中で用いられる用語の解説や、制御システムのセキュリティ動向、SCADA モデルの一般論などを記載している。このシリーズは事業者や、システムインテグレータ、コンポーネントプロバイダなど、すべての関係者が共通して参照する規格となっており 4 つの規格から構成されている。現在は、IEC62443-1-1 のみが発行済みであり、他は現在策定中となっている。IEC62443-1-1 では、7 つの基礎的な要件（Foundational Requirement：FR）を規定している。

＜ IEC62443-1-1 ＞

用語、コンセプト、モデルの定義について記した技術仕様書（Technical Standard：TS）である。これには、IEC62443 に用いられる用語の解説や、制御システムの動向や状況、セキュリティ概念、及び SCADA モデルの一般論などを記載している。初版は 2009 年 7 月に発行済であるが、2013 年現在、第二版が策定中である。

＜ IEC62443-1-2 ＞

用語、略語について記した技術報告書（Technical Report：TR）である。IEC62443 に用いられる制御システムのセキュリティに関連する用語・略語集となっている。2013 年現在、草案段階であるが用語を 243 個、略語（Abbreviated terms and acronyms）を 117 個登録している。草案（Documents for Committee）の策定中である。

＜ IEC62443-1-3 ＞

システムの安全性評価基準の規定について記した文書（International Standard：IS）である。これには、評価基準（metrics）策定や利用のためのフレームワークなどを記載している。2013 年現在、草案（Documents for Committee）の策定中である。

[IEC62443-2 シリーズ]

事業者や運用者などの組織を対象としたセキュリティ要求事項などを規定した規格である。このシリーズは 4 つの規格から構成されており、現在 IEC62443-2-1 が発行済みとなっている。このほか、IEC62443-2-2、IEC62443-2-3、IEC62443-2-4 についてはドラフトの策定中となっている。

＜ IEC62443-2-1 ＞

制御システムのセキュリティプログラム確立方法について規定した文書（IS）である。CSMS（Cyber Security Management System）というセキュリティマネジメントプログラムの規格となっており、これは既存規格である ISMS をベースに制御システムのセキュリティに関する要求事項が記載されている。初版は 2010 年 10 月に発行済であるが、2013 年現在、第二版が策定中である。

＜ IEC62443-2-2 ＞

制御システムのセキュリティプログラムの運用ガイドラインについて規定した文書（IS）である。運用する際に必要となる対策ついて、セキュリティポリシー、組織（Organization of security）、資産管理（Asset Management）、人的資源セキュリティ（Human Resources Security）、物理環境セキュリティ（Physical and Environmental Security）など、を記載している。2013 年現在、草案（Documents for Committee）の策定中である。

＜ IEC62443-2-3 ＞

制御システムにおけるパッチ管理方法に関するガイドラインについて記した技術報告書（TR）である。制御システムへのパッチ適用に関する問題点を導入とし、事業者の要件、製品提供者の要件、パッチ情報交換時の要件などについて記載している。Annex としてパッチ報告の書式やパッチについての制御システムの事業者のガイドラインも含んでいる。2013 年現在、草案（Documents for Committee）の策定中である。

＜ IEC62443-2-4 ＞

制御システムの提供者に対するセキュリティ要求事項

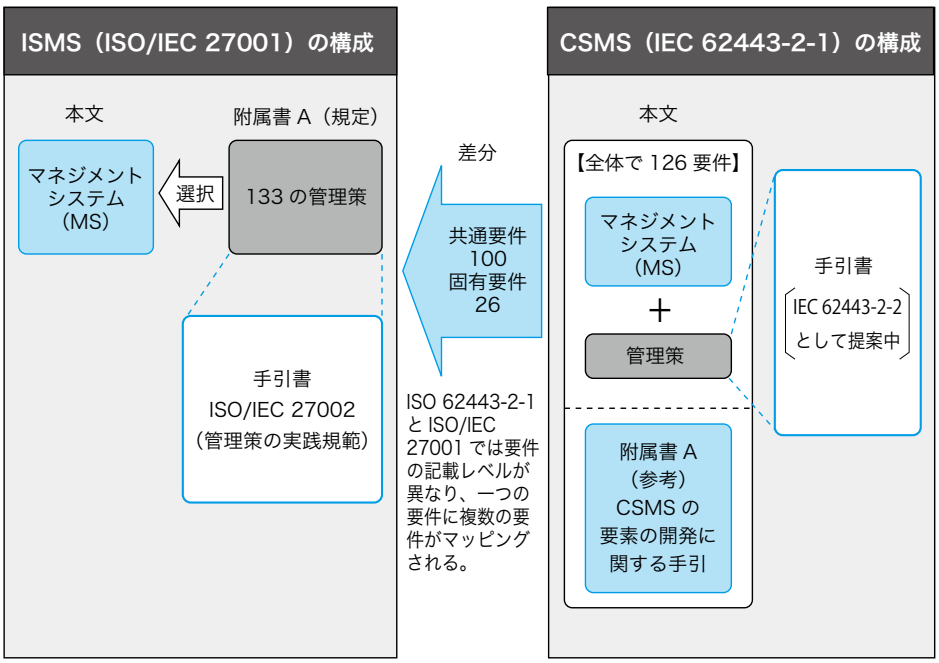
などを規定した文書（IS）である。業界で先行している認証を基に、事業者が制御システムのコンポーネントやシステムを調達する際に必要な要件などが本規格に提案されている。2013 年現在、草案（Committee Draft）の策定中である。

[IEC62443-3 シリーズ]

複数の機能や製品を組み合わせて運用している制御システムを対象とした規格である。このシリーズは 3 つの規格から構成されており、IEC62443-3-1 及び IEC62443-3-3 が発行され、IEC62443-3-2 はドラフト案の策定中である。IEC62443-3-3 については、IEC62443-1-1 で規定されている 7 つの基礎的な要件（FR1 から FR7）に対応する形で技術的なシステム要件を規定している。システム要件は、基本的な要件（System Requirement：SR）と強化策（Requirement Enhancement：RE）から構成されている。それぞれの要件には、セキュリティレベル（Security Level：SL）が割り当てられている。SL は、各要件を満たした場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階のレベルが規定されており、最も高度な要件を満たすものをレベル 4 としている。

表 2　セキュリティレベル（SL）の定義

SL	対策可能な攻撃（攻撃者）の特徴				
	悪意の有無	攻撃手段	使用リソース	スキルレベル	動機
1	無	-	-	-	-
2	有	単純	低	一般的	低
3	有	洗練	中	システム固有	中
4	有	洗練	高	システム固有	高



出典 :IPA「制御システムにおけるセキュリティマネジメントシステムの構築に向けて」2012 年 10 月

図 7　ISMS と CSMS の関係

＜ IEC62443-3-1 ＞

一般的なセキュリティ技術のうち、制御システムで適用可能なものについて、解説などを記載した技術報告書（TR）である。セキュリティ技術の解説書という位置づけであり、認証、フィルタリング／ブロッキング／アクセス制御、暗号／データ保護、管理・監査・証跡、ソフト管理（脆弱性対応を含む）、物理セキュリティ、人的セキュリティなどを記載している。初版は既に 2009 年 7 月に発行済である。

＜ IEC62443-3-2 ＞

ゾーン（領域）やそれらを連結するコンジットに関するセキュリティについて規定する文書（IS）である。ゾーン及びコンジットやセキュリティ要求事項の定義などが規定されている規格である。ゾーンやコンジットを適切に確立することに目的としている。2013 年現在、草案（Documents for Committee）の策定中である。

＜ IEC62443-3-3 ＞

制御システムのセキュリティ機能要件を規定した国際標準（IS）である。IEC62443-1-1 で規定されている 7 つの基礎的な要件（FR1 から FR7）に対応する形で技術的なシステム要件を規定している。システム要件は、基本的な要件（System Requirement：SR）と強化策（Requirement Enhancement：RE）から構成されており、SR や RE ごとにセキュリティレベル（Security Level：SL）が割り当てられている。SL は、各要件を満足した場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階のレベルが規定されており、巧妙で大

規模な攻撃にも対処可能なレベルをレベル 4 としている。この SL の定義を表 2 に示す。初版は 2013 年 8 月に発行済。

[IEC62443-4 シリーズ]

制御システムの一部である個別のコンポーネント単位が準拠の対象となる規格である。このシリーズの規格として、現在 IEC62443-4-1 及び IEC62443-4-2 の 2 つが存在するが、いずれもドラフト案の策定中となっている。

＜ IEC62443-4-1 ＞

コンポーネントの開発要件を規定した国際標準（IS）である。セキュアなコンポーネントを開発するための方法を規定しており、ISA Secure の EDSA（SDSA）をベースにしている。内容は、ソフトウェア開発のライフサイクルを 12 の段階に分けて、それぞれのセキュリティに関する要求事項を記載している。2013 年現在、草案（Documents for Committee）の策定中である。

＜ IEC62443-4-2 ＞

コンポーネントのセキュリティ要件を規定した国際標準（IS）である。デバイスに搭載されるセキュリティ機能を規定。ISA Secure の EDSA（FSA）をベースにしており、セキュリティ機能の実装評価に関する要求事項を記載している。2013 年現在、草案（Documents for Committee）の策定中である。

なお、既に発行済みの規格（IEC62443-1-1、2-1、3-1）に対しては、IPA により作成された英日対訳版が、日本規格協会から発刊されている※ 11。

4 我が国の評価認証への取り組み

4.1 日本発のセキュリティマネジメントの認証プログラム「CSMS」のパイロットプロジェクトの開始

制御システムにおけるセキュリティ対策の必要性の高まりに対応するため、制御システムを利用する事業者のセキュリティマネジメントシステムの確立が非常に重要となってくる。本規格の IEC62443-2-1^{ed1} は、制御システムのセキュリティマネジメントを規定しており、CSMS※ 12 と定義している。IPA では前述の「制御システム情報セキュリティ検討タスクフォース」において、この CSMS に基づく認証制度の実現を提案してきた。現在、経済産業省及び一般財団法人日本情報経済社会推進協会（JIPDEC）において、日本発の制御システム向けセキュリティマネジメントシステム適合性評価制度の確立が進められている。本制度では、CSMS（IEC62443-2-1^{ed1}）規格の要求事項を用いて、世界的にも突出して高い認証実績を有する ISMS 適合性評価スキームに沿った評価認証を実施することが予定されている。また、既に ISMS を取得している事業者等においては、認証の重複を省くなどの効率的な認証スキームの推進も今後検討していくことで、制御システム分野にセキュリティマネジメントシステムを普及、浸透させるきっかけとなる事が期待される。

経済産業省は、「グローバル認証基盤整備事業」による政策に基づき、JIPDEC を主体とした CSMS のパイロットプロジェクトを 2013 年度に実施している。本パイロットプロジェクトでは、認証機関が審査に用いる認証基準、及びこれに基づく認証機関に対する認定基準を策定し、これらを用いて実証実験を目的とした試行の受審となるパイロット認証を実施している。このパイロット認証においては、CSMS の認証機関候補が制御システムを利用する事業者（受審企業候補）に対して実際に CSMS への適合性を評価し、実証実験としてその結果を認証基準やスキームへフィードバックすることが盛り込まれている。本パイロットプロジェクトは ISMS 創設時に実施された「ISMS パイロット事業」と同等の位置付けとして実施されており、本プロジェクトにおいて抽出された課題などを解消した上で、2014 年度を目途に正式な認証制度が施行される見込みとなっている。

ISMS は、準拠する標準である ISO/IEC27000 シリーズが ISO によって改正が進められているところであり、IEC62443-2-1 の標準化においても、これに沿った整合が図られる見込みである（図 7）。IEC62443-2-1^{ed2} の案では、ISMS の箇条体系に沿った形式でのリリースが予定されており、認証制度についてもこれに伴って改正されていくことによって、より一層、ISMS と親和性の高い CSMS 認証が確立、普及していくことが期待される。

【脚注】

※ 11　一般財団法人日本規格協会 http://www.jsa.or.jp/

※ 12　CSMS：Cyber Security Management System の略称。制御システムにおけるセキュリティマネジメントに関する要求事項を規定している。

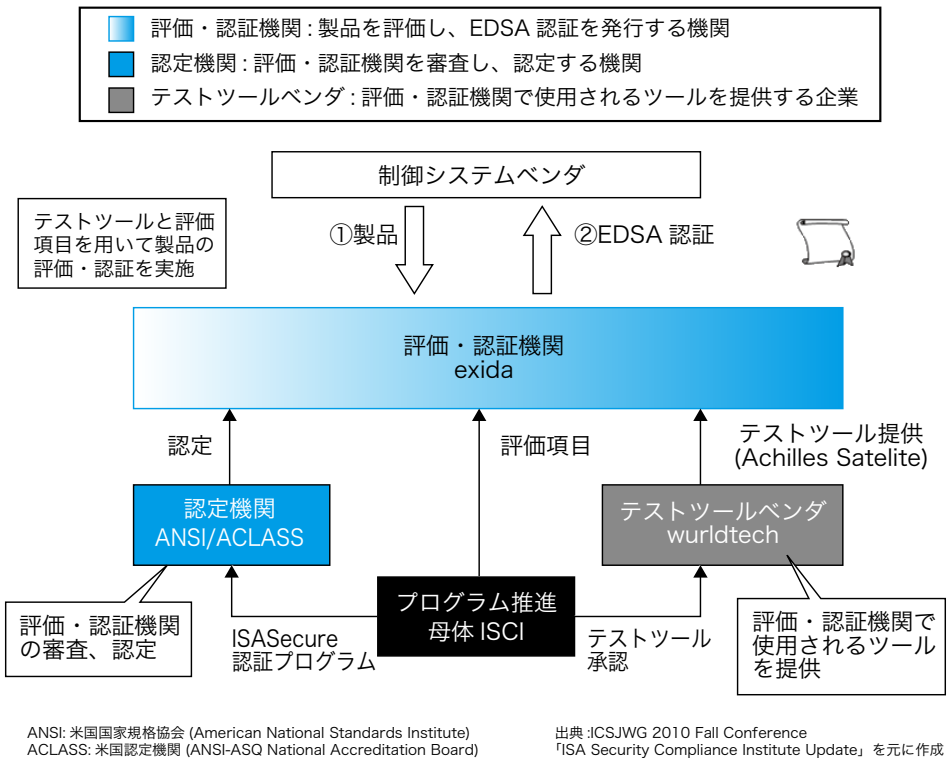


図 8　EDSA スキームの概念図

4.2　組込み機器のセキュリティ保証プログラム「EDSA」の国内導入

ISCI がスキームオーナを担っている組込み機器のセキュリティを保証する認証プログラムである EDSA は、IEC62443-4（制御システムセキュリティ）シリーズの標準化の場へその要求事項が提案され、承認される見込みとなっている。EDSA 認証は ISA※13 のメンバー（民間企業主体）により創設された ISCI がスキームオーナとなり、運営されている認証スキームである。EDSA 認証の主な評価項目は「通信の堅牢性試験（CRT※14）」、「セキュリティ機能の実装評価（FSA※15）」、「ソフトウェア開発のライフサイクルの各フェーズにおけるセキュリティ評価（SDSA※16）」に大別される。なお、SDSA の要求事項には IEC61508（電気 / 電子 / プログラム可能電子安全関連システムの機能安全）、ISO/IEC15408（IT セキュリティの評価基準）などが引用されている。EDSA 認証において、現状は米国 ANSI※17 のみが唯一の認定機関となっており、同じく米国の exida.com, LLC が唯一の評価・認証機関を担っている。EDSA スキームにおいて、評価・認証機関は、スキームオーナの認可する評価ツールを用いることとされている。現状、スキームオーナより認可されているツールは wurldtech 社ツール（Achilles Test Platform）及び Codenomicon 社ツール（Codenomicon Defensics）がある。現状の EDSA スキームの概念図を図 8 に示す。

現状の EDSA 認証スキームは北米主体で先行しているが、北米だけでなく国際的な製品の調達要件に挙げられ始めている。このため、国内の企業からも EDSA 認証取得に関する要望があるため、国内においても認証が可能となるよう取り組んでいる。ISCI のメンバである IPA では、2012 年 10 月から、日本の JAB※18 を EDSA 認証スキームの認定機関として登録するための活動を実施しており、2013 年 3 月には米国 ISCI、ANSI、JAB、IPA の 4 者会合にて IPA より交渉を行い、正式に日本スキームの確立が承認された※19。これにより、国内での認証機関の認定、及び製品認証取得が実現する見込みとなった（図 9）。IPA は、国内での認証制度の実現計画を策定し、国内に同スキームの認定機関及び認証機関の設置を提案及びその支援を実施した。この結果、2012 年に設立された技術研究組合制御システムセキュリティセンター（CSSC）内に、同制度の認証機関が設置され、現在その正式な認定を取得する作業が推進されている。

【脚注】

※ 13　ISA：International Society of Automation（国際計測制御学会）の略称。
※ 14　Communication Robustness Testing
※ 15　Functional Security Assessment
※ 16　Software Development Security Assessment
※ 17　ANSI：American National Standards Institute（米国国家規格協会）の略称。米国内の工業製品の規格を策定する団体。EDSA 認証スキームにおける認定機関を担っている。http://www.ansi.org/
※ 18　JAB：Japan Accreditation Board（公益財団法人 日本適合性認定協会）の略称。適合性評価制度全般に関わる認定機関としての役割を担う組織。http://www.jab.or.jp/
※ 19　制御機器認証プログラム「EDSA」国内認証制度の確立および規格書対訳版の公開について http://www.ipa.go.jp/about/press/20130415.html

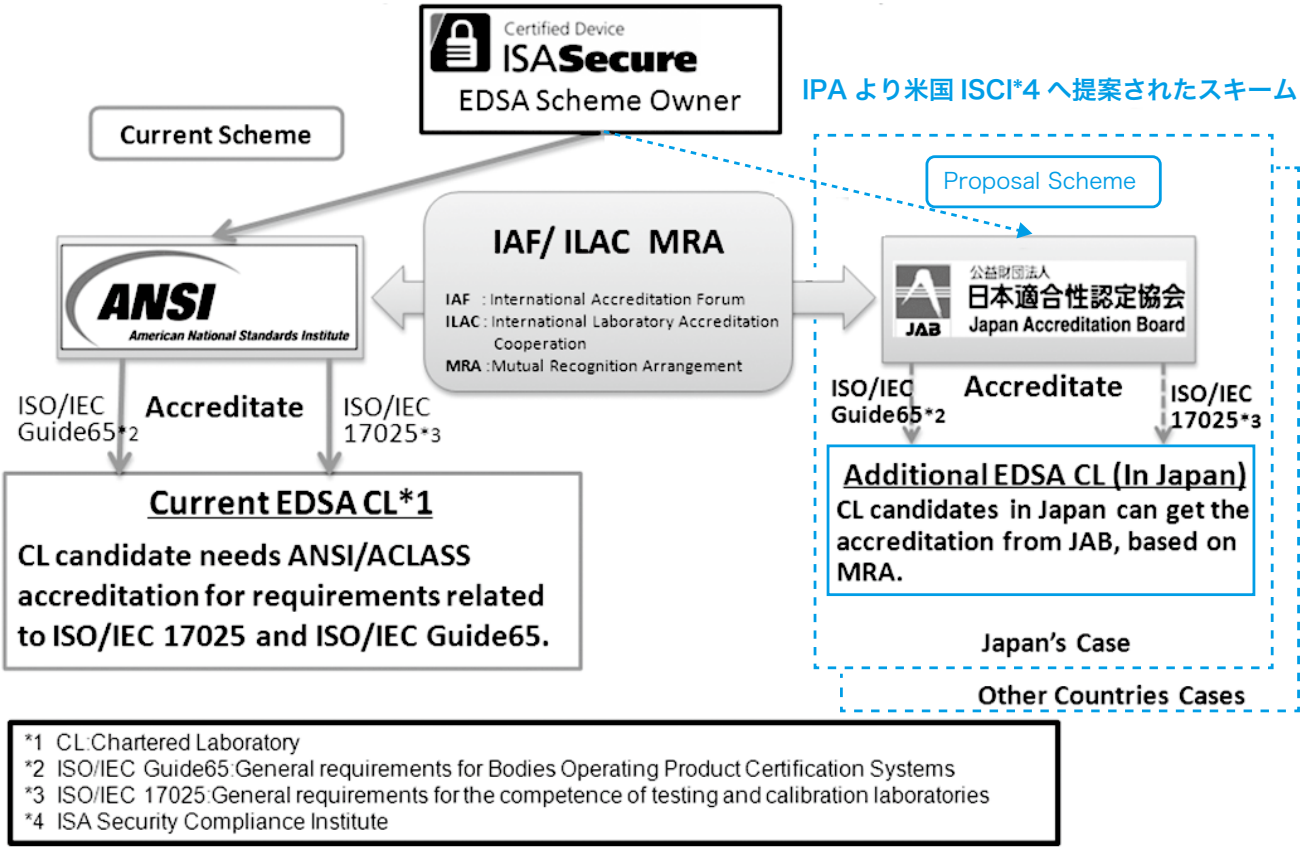


図 9　EDSA 認証スキームへの日本参画構想

5 今後の展望

我が国内では、制御システムのセキュリティへの対応として、IEC62443 の活用を軸に、その普及啓発が進められていく見通しである。これをベースに、日本発の制御システムのセキュリティマネジメントシステムの評価認証制度が開始され、制御機器などの個別のコンポーネントに関しても米国に次ぐ形で同じく評価認証制度が開始される予定である。これらはいずれも 2014 年度から施行される見込みとなっており、今後のセキュリティ対策の発展が期待される。マネジメントシステムについて、制御システムを用いる各分野に共通で汎用的な要求事項が求められており、これに適合するための指針となるガイドの策定が併せて進んでいる。また、将来的には業界ごとにその指針を詳細化したガイドが策定及び普及されることが望まれる。一方で、「システム」のレイヤに対応した IEC62443-3-3 が発行されており、これを用いた認証制度として SSA（System Security Assurance）の策定が ISCI により進められている。こちらも我が国として、その導入の可否が検討段階に入っている。

制御システムへの脅威、業界・国際規格の動向とこれに基づく認証制度の策定状況については流動的となっているため、引き続き、関係業界・各国などと連携を保ちながら、我が国として国内の制御システムのセキュリティ向上と制御システム製品の国際競争力の強化の観点から、タイムリーに標準の活用と評価認証制度の拡充を図っていくことが望まれる。

【参考文献】

[1] IPA,"CSMS/EDSA 認証導入に向けたパイロットプロジェクト ", http://www.ipa.go.jp/security/fy24/reports/ics_sec/ics_annex.pdf
[2] 入澤康紀 , IPA," 制御システムセキュリティ標準「IEC62443」 ", http://techon.nikkeibp.co.jp/article/FEATURE/20130130/263280/
[3] 入澤康紀 , IPA," 政府による制御システムのセキュリティへの取組み ", http://techon.nikkeibp.co.jp/article/FEATURE/20130128/262781/
[4] IPA," 制御システムにおけるセキュリティマネジメントシステムの構築に向けた解説書の公開 ", http://www.ipa.go.jp/security/fy24/reports/ics_management/index.html
[5] 入澤康紀 , IPA,"EDSA の認証プログラム ", http://techon.nikkeibp.co.jp/article/FEATURE/20130130/263302/
[6] 入澤康紀 , IPA," 制御システムのセキュリティマネジメントシステム ", http://techon.nikkeibp.co.jp/article/FEATURE/20130130/263303/