# 安心な社会インフラシステムに向けたセキュリティ標準規格の動向と展開

山田 勉 Yamada Tsutomu
鍛 忠司 Kaji Tadashi
中野 利彦 Nakano Toshihiko

制御システムにおけるセキュリティ向上のため，制御システムに適した標準の整備が急務となっている。制御システムのセキュリティ規格は，業界標準の整備が先行する中，国際標準規格も策定が進められており，IEC 62443規格は現在13分冊中4分冊が発行済みである。また，制御システムや制御装置のセキュリティ基準適合を認証する規格には，ISASecure※1) EDSA認証とCSMS認証がある。セキュリティに関する国際認証を迅速に取得することは，国際競争力強化の観点でも重要であり，経済産業省はそれらの認証を国内で取得可能とするパイロットプロジェクトを推進している。日立グループは，これらの規格の活用に向けた標準化活動に貢献している。

## 1. はじめに

社会インフラを支える制御システムにおいて，セキュリティ向上に向けた各国政府機関や業界における基盤的な活動が進められている。これまで社会インフラや製造現場における効率や生産性を高めるため，現場の情報が運用や経営に活用されてきた。また，情報システムとの親和性と開発効率向上のため，OS（Operating System）やネットワーク技術分野でIT（Information Technology）が多くの制御システムに導入されてきた。その中で，特定制御システム向けに作成されたコンピュータウイルスStuxnetが2010年に発見された。これは，制御システムに関係する多くの担当者，業界，政府機関が，セキュリティの必要性を再認識する契機となった。

しかし，情報システム向けセキュリティ技術の制御システムへの追加導入は困難な場合が多い。制御システムにおけるコントローラや各種装置の計算処理余力は少なく，構成変更による処理オーバーヘッドの影響が大きいことが理由である。一般に，制御システムでは守るべき資産の可用性や完全性が重視され，情報システムで重視される秘匿性の優先度が低い。また，保護対象は情報だけではなく，制御装置を含めた施設や外部環境も含まれる。

すなわち，制御システムのセキュリティを強化するには，制御システムに適した方策が必要である。また，制御システムは世界各国で使用されるため，セキュリティの対抗策やガイドラインとして国際共通的に評価可能な標準が有効である。そこで，各国政府機関や標準化団体，業界団体では，制御セキュリティに関する標準規格やガイドラインの策定を進めている。

ここでは，制御システムにおけるセキュリティの標準規格の全体概要，標準規格の代表的な取り組み，セキュリティ向上をめざす各種認証制度に関する動向と現状について述べる。

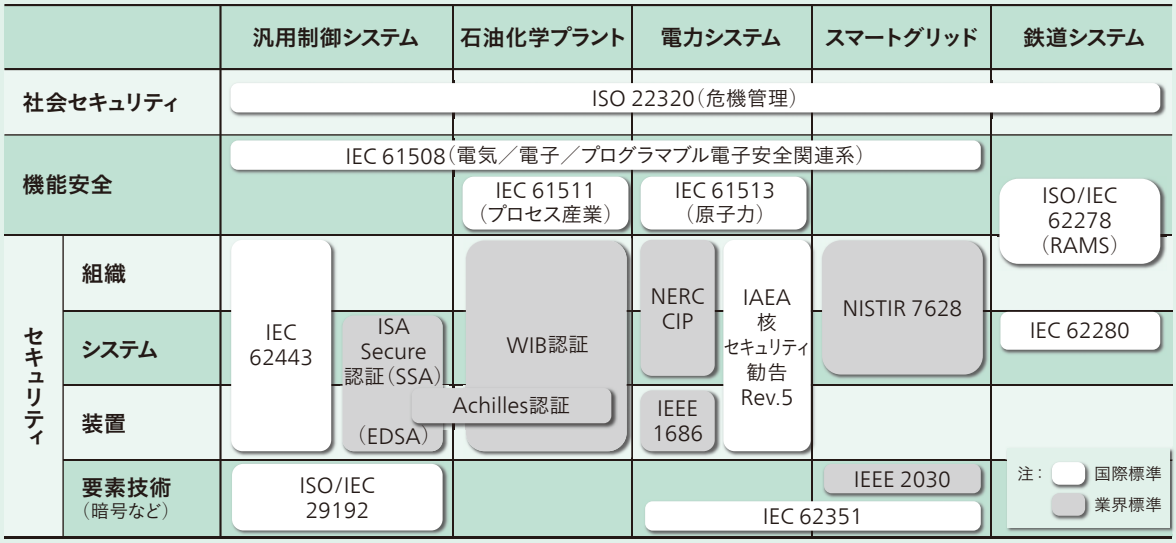
## 2. 国際標準規格・業界標準規格

### 2.1 全体概要

セキュリティの標準規格としては，IT分野における規格が先行する。例えば，コモンクライテリア（ISO/IEC 15408 [1]）はセキュリティ製品の調達に活用されている。IT分野と共通する脅威に対抗するために，制御システムにおけるセキュリティ規格の多くは，ITセキュリティ規格に加えて物理セキュリティ規格[2]も参照している。このように関連する標準規格の中で，ここでは特に制御システムにおけるセキュリティ規格の動向について述べる。

制御システムセキュリティに関する国際標準規格と業界標準の概要を**図1**に示す。同図は，分野ごとに定められている標準規格について，国際標準と業界標準の分類を示し

※1）ISASecureは，ASCIの商標である。




注：略語説明　SSA（System Security Assurance），EDSA（Embedded Device Security Assurance），NERC（North American Electric Reliability Corporation），CIP（Critical Infrastructure Protection），IAEA（International Atomic Energy Agency），NISTIR（National Institute of Standards and Technology Interagency Report），RAMS（Reliability, Availability, Maintainability and Safety）

**図1｜制御システムセキュリティ関連規格の概要**
分野ごとに定められた国際標準と業界標準を分類して示す。



ている。また，セキュリティ規格以外にも，制御システムの安全運用に関係が深い機能安全規格も含めている。

制御システムユーザーの要望に応える形で，業界ごとの標準は2000年代から比較的早くに整備されてきた。同図では，ISASecure規格[3]，WIB規格[4]，Achilles認証[5]が該当する。それらの多くは，規格と合わせて認証の枠組みを用意している。これらの企業や団体は，規格に準拠した製品が一定水準に達していることを保証するビジネスを進めている。

関連する動きとして，米国ではサイバー攻撃の脅威に対抗するために，大統領がセキュリティ防護に対する取り組みを進めている[6]。NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は，サイバーセキュリティフレームワーク[7]を発行した。このフレームワークは法的拘束力を持たないものの，企業がセキュリティを守る際の目安となるため，事実上の標準的なガイドラインとして動向を注目する必要がある。

業界標準に少し遅れて国際標準が立ち上がってきている。現在，制御システム全般を対象としてIEC 62443規格の整備が進められている。また，重要インフラである電力システムの防御のため，米国政府は電力業界に対するセキュリティ基準としてNERC（North American Electric Reliability Corporation）CIP（Critical Infrastructure Protection）[8]を用意し，すでに運用している。

日立グループは，これらの標準規格で要求される仕様を基に，制御システムをセキュアに構築するためのガイドラインを整備している。継続的にセキュリティ対策が可能となるシステムを構築するため，この特集の「社会インフラを支える制御システムセキュリティ」に述べた制御システムにおけるセキュリティの実現方針に従いながらガイドラインを活用する（本誌p.57参照）。

## 2.2　IEC 62443

IEC 62443規格は，業界で注目されている国際標準の1つである。その全体構成を**表1**に示す。

IEC 62443は全体で13分冊から成る。IEC 62443-1-xシリーズは一般向けであり，共通概念，モデル，用語を扱う。IEC 62443-2-xシリーズは制御システム保有者を想定し，セキュリティポリシーや組織・人に関わる管理システムを扱う。IEC 62443-3-xシリーズはシステムインテグレーターを想定し，制御システムの技術要件を扱う。IEC 62443-4-xシリーズは装置製造者を想定し，システムを構成する制御装置のセキュリティ要件を扱う。

IEC 62443シリーズの中で，発行済み規格の概要は以下のとおりである。

(1) IEC/TS 62443-1-1[9]

制御システムでのセキュリティ基本要件が規定されている。要件は，アクセス制御（Access control），使用制御（Use control），完全性（System integrity），データ秘匿性（Data confidentiality），データフロー制限（Restricted data flow），応答時間（Timely response to events），リソース可用性（Resource availability）の7つである。

(2) IEC 62443-2-1[10]

制御システム保有者がシステムで管理すべきリスクと，

**表1｜IEC 62443規格の全体構成**

IEC 62443規格の全体構成を示す。

| 規格番号 | 規格名 | 概要 |
|---|---|---|
| IEC/TS 62443-1-1（発行済み） | Terminology concepts and models | 用語，コンセプト，モデルの定義 |
| IEC/TR 62443-1-2 | Master glossary of terms and abbreviations | 用語・略語集 |
| IEC 62443-1-3 | System security compliance metrics | システムの安全性評価基準 |
| IEC/TR 62443-1-4 | IACS security life cycle and use case | IACSセキュリティライフサイクル・ユースケース |
| IEC 62443-2-1（発行済み） | IACS security management system - Requirements | IACSセキュリティマネジメントシステムの要件 |
| IEC 62443-2-2 | IACS security management system - Implementation guidance | IACSセキュリティマネジメントシステムの実装ガイドライン |
| IEC/TR 62443-2-3 | Patch management in the IACS environment | IACSにおけるパッチ管理方法についてのガイドライン |
| IEC 62443-2-4 | Certification of IACS supplier security policies and practices | IACS装置製造者に対するセキュリティプラクティス集 |
| IEC/TR 62443-3-1（発行済み） | Security technologies for IACS | IACSで利用可能なセキュリティ技術リスト |
| IEC 62443-3-2 | Securitiy assurance levels for zones and conduits | ゾーンやコンジットコンセプトにおける安全性保証レベル |
| IEC 62443-3-3（発行済み） | System security requirements and security assurance levels | システムのセキュリティレベルと対応する機能要件 |
| IEC 62443-4-1 | Product development requirements | コンポーネントの開発プロセス規定 |
| IEC 62443-4-2 | Technical security requirements for IACS components | コンポーネントのセキュリティ機能要件 |

注：略語説明　IACS（Industrial Automation and Control System）

サイバーセキュリティ管理システムCSMS（Cyber Security Management System）を記載している。

（3）IEC/TR 62443-3-1[11]

セキュリティ技術全般のカタログである。認証，フィルタリング・アクセス制御，暗号・データ認証，管理・監査・モニタリング，PC（Personal Computer）などソフトウェア管理，物理セキュリティを説明している。

（4）IEC 62443-3-3[12]

システムでセキュリティを守る際の詳細な機能要件を，上述の7要件それぞれに4つのセキュリティレベルで定義している。

IEC 62443は同表に示した4分冊が発行済みであり，それ以外の分冊は現在IEC（International Electrotechnical Commission）TC（Technical Committee）65/WG（Working Group）10において策定中である。日立グループは，制御システムの継続的なセキュリティ向上のため，IEC国内委員会のメンバーと共同して寄書を通じて貢献していく。

## 3.　認証規格

制御システムにセキュリティを導入するにあたっては，セキュリティの網羅度合いや強度を評価する基準が制御システム保有者に対して明確化されることが望ましい。セキュリティ機能の評価には，セキュリティ認証の枠組みが有効である。代表的な枠組みとして，ISASecure認証とCSMS認証がある。

### 3.1　ISASecure

米国に本拠を置く業界団体ISA（International Society of Automation）[13]の下部団体に，ISCI（ISA Security Compliance Institute）[3]がある。ISASecureは，ISCIが定めるセキュリティ基準を満たすことを認証する枠組みである。ISCIは認証する対象それぞれに認証プログラムを用意しており，制御装置向けにはEDSA（Embedded Device Security Assurance）認証，制御システム向けにはSSA（System Security Assurance）認証がある。EDSA認証は認証基準[14]を公開済みで認証を開始しているが，SSA認証は認証基準を準備中である。

EDSA認証は，以下の3つのカテゴリーで審査をする（**図2**参照）。

（1）CRT（Communication Robustness Testing）

制御装置の通信プロトコル［Ethernet※2），ARP（Address Resolution Protocol），IP（Internet Protocol），ICMP（Internet Control Message Protocol），TCP（Transmission Control Protocol），UDP（User Datagram Protocol）］を検証する。ISCIで認定した専用ツールで制御の正常動作を確認しながら，プロトコル検査を行う。

（2）FSA（Functional Security Assessment）

制御装置のセキュリティ機能を検証する。

（3）SDSA（Software Development Security Assessment）

制御装置が開発されているプロセスを検証する。

EDSA認証において，CRTはすべてのレベルで同一テストが検証され，FSAとSDSAは3つのレベルに応じてテスト項目が検証される。

### 3.2　CSMS

CSMSは，制御システム保有者が制御システムのリスク

※2）Ethernetおよびイーサネットは，富士ゼロックス株式会社の登録商標である。

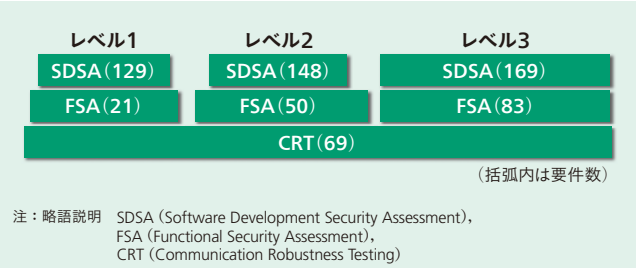
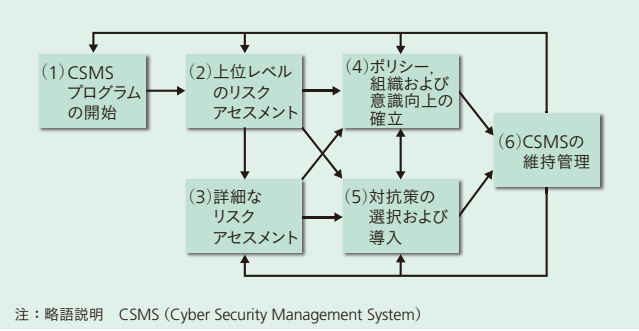



**図2｜EDSA認証の要件数**

取得認証レベルに応じたセキュリティテスト要件を規定している。




注：略語説明　CSMS（Cyber Security Management System）

**図3｜CSMSの達成フロー**

制御システムのリスクアセスメントとセキュリティの維持管理の手順を規定している。

管理を実施し，セキュリティを継続的に維持する管理システムである。情報システムにおいてISO/IEC 27001で規定されるISMS（Information Security Management System）の，制御システム版と対応づけられる。IEC 62443-2-1に基づいて認証基準が制定される見通しである。

IEC 62343-2-1 Annex B[10]に例示されているCSMSの達成フローを**図3**に示す。CSMS達成には，CSMSプログラムを経営陣に対して正当化することから始める［同図（1）参照］。その後，脅威とその実現可能性，脆（ぜい）弱性の種類，結果を提示する［同図（2），（3）参照］。さらに，組織におけるリスク許容度に基づき，対抗策を実行するための適切なポリシーと組織を確立し［同図（4）参照］，対抗策を選択・導入する［同図（5）参照］。導入後は，組織がCSMSのポリシーおよび手順に適合しているか，効果を発揮しているか，目標を変更する必要があるかを検証する［同図（6）参照］。

CSMS認証では，セキュリティを維持管理するフローが制御システム保有者で実施可能かを検証する。

## 4.　各種認証の試行

制御システムの海外展開を進めるためには，国際的に通用する認証を迅速に取得することが競争力強化の点で重要である。そこで，前述した2つの認証を日本国内で取得可能とするべく，経済産業省が主導するパイロットプロジェクトが進行している。

情報システムにおけるセキュリティ規格のISMSやISO/IEC 15408は，日本国内機関による認証枠組みが整備されたが，制御システムにおいても同様に整備をめざしている。EDSA認証に関しては，技術研究組合制御システムセキュリティセンター（CSSC）がパイロット認証を実施している。また，CSMS認証に関しては，一般財団法人日本情報経済社会推進協会（JIPDEC）がパイロット認証を推進している。

EDSA認証とCSMS認証は，いずれも認証基準やガイドラインなどの整備を進めているところである。日立グループは，これらの確立に向けて関係機関と協力していく。また，これらの規格を活用しつつ，顧客システムへのセキュリティソリューションの提供を進める。

## 5.　おわりに

制御システムにおけるセキュリティ規格の整備やその認証取得により，セキュリティレベルの底上げや一層の発展が期待できる。セキュリティ技術の基盤整備に向けて，日立グループは標準化活動へ貢献していく。

一方で，制御システムにおけるセキュリティの考え方が国際標準規格になるまでには時間を要するため，別の対策も実施する必要がある。それには，国際標準や規格への準拠と，最新のセキュリティ技術へ対応するための研究開発やソリューション提供を並行して進めることが重要になる。

**参考文献など**

1）ISO/IEC：ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security –
2）U. S. Department of Defense, DoD Manual 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives
3）ISA Security Compliance Institute, http://www.isasecure.org/
4）WIB, http://www.wib.nl/
5）Wurldtech, Wurldtech Certification, http://www.wurldtech.com/product_services/certifications/
6）President's Council of Advisors on Science and Technology, Report to the president immediate opportunities for strengthening the nation's cybersecurity（2013.11）
7）NIST, Framework for Improving Critical Infrastructure Cybersecurity（2014.2）
8）NERC, CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
9）IEC: IEC/TS 62443-1-1, Terminology, concepts and models（2009.7）
10）IEC: IEC 62443-2-1, Establishing an industrial automation and control system security program（2010.11）
11）IEC: IEC/TR 62443-3-1, Security technologies for industrial automation and control systems（2009.7）
12）IEC: IEC 62443-3-3, System security requirements and security levels（2013.8）
13）ISA, http://www.isa.org/
14）ISCI, ISASecure Program Description, http://www.isasecure.org/ISASecure-Program.aspx

**執筆者紹介**

**山田 勉**
日立製作所 日立研究所 エネルギー・環境研究センタ エネルギーマネジメント研究部 所属
現在，組込み計算機・ネットワークアーキテクチャ，制御システムにおけるセキュリティの研究開発に従事
技術士（情報工学部門）
IEEE会員，ISA会員，電子情報通信学会会員，計測自動制御学会会員

**鍛 忠司**
日立製作所 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，情報セキュリティ技術の研究開発に従事
博士（情報科学）
IEEE Computer Society会員

**中野 利彦**
日立製作所 インフラシステム社 情報制御プラットフォーム開発本部 制御プラットフォーム設計部 制御セキュリティセンタ 所属
現在，社会インフラシステムのセキュリティ開発に従事
博士（工学）