4

制御システムのセキュリティを対象とした評価・検証技術と標準化動向 専応

小林偉昭
技術研究組合制御システムセキュリティセンター

制御システムの脅威の動向

2010年イランにおける核施設がStuxnetと呼ばれるマルウェアにより攻撃された事件は，その後制御システムに対するサイバー攻撃が広く意識され始めるきっかけとなった．今日（こんにち），プラント設備（生産ライン制御等）における標準ネットワーク・汎用製品使用オープン化の割合は，外部ネットワーク接続が36.8%，設備内の汎用OS利用状況としてWindowsが88.9%，UNIX系が13.7%と報告されている．この制御システムにおける標準ネットワーク・汎用製品の普及により，従来情報システムで起きていたサイバー攻撃の脅威が制御システムでも増大してきている．

本稿では，世界各国で使用される制御システムを対象とし，国際的に共通なセキュリティに対する要件とその評価を可能とする国際標準や認証の動向および，技術研究組合制御システムセキュリティセンターCSSC☆1の取り組みを解説する．

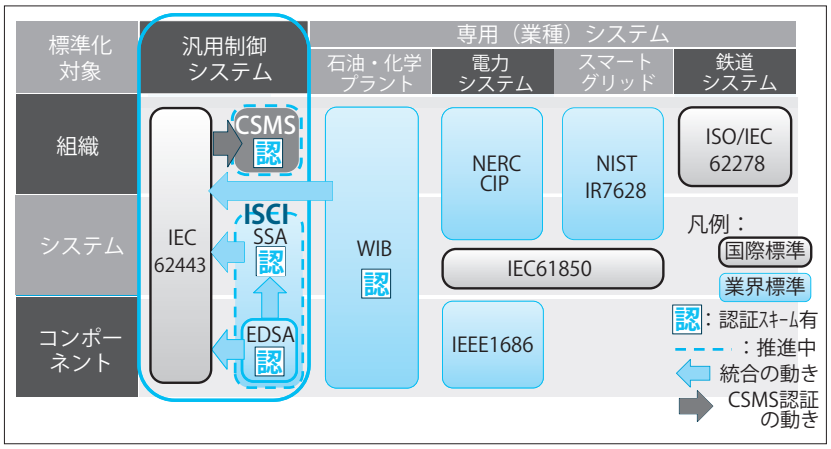


図-1　制御システム分野での標準化の動向

制御システムセキュリティの標準化と認証の動向

国際標準IEC62443☆2の採用

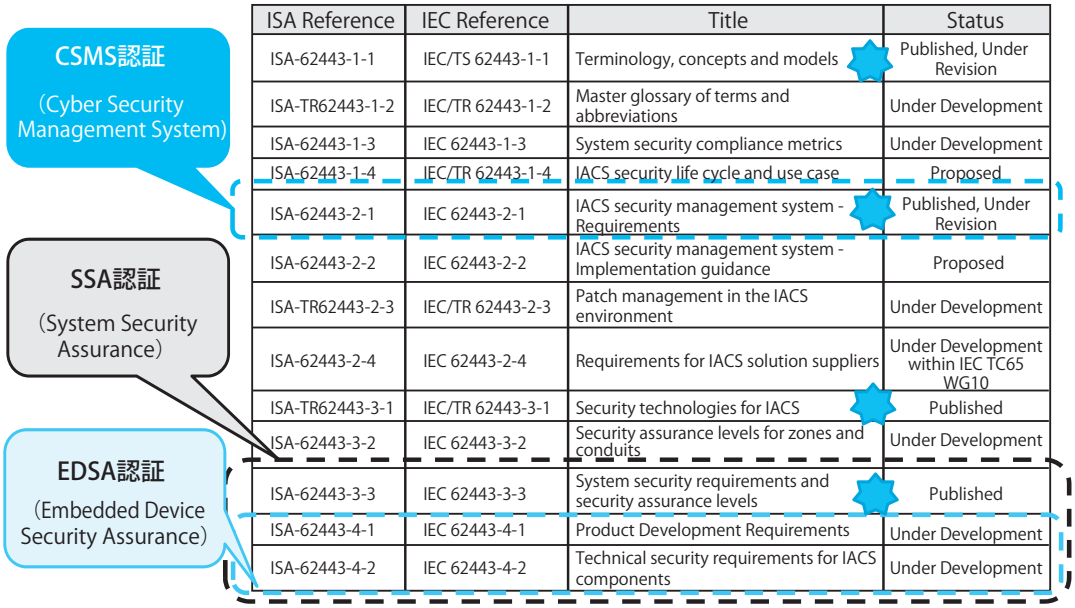
図-1に制御システム分野における標準化の動向を示す．業界向けとして，石油・化学プラントではWIB☆3，電力システムではNERC☆4のCIP☆5，スマートグリッドではNIST☆6IR7628☆7や鉄道ではISO/IEC62278☆8等がある．

現在，IEC62443が，制御システムのセキュリティにおいて製品はじめシステム，組織の各レベルなど全レイヤ／プレイヤをカバーする標準であり，シェル，シェブロン等石油関連の国際的大企業の調達要件にも含まれ，将来汎用的な国際標準として選択されるようになると予想されている．

そこで経済産業省，（独）情報処理推進機構IPA☆9とCSSCは，日本で推進する制御システムのセキュリティ標準を選択するにあたり，① トータルなセキュリティ，② すべての関係者に適用可，③ 汎用性・一般性，④ 国際標準，⑤ 評価認証スキームおよび第三者認証等の要件を検討した．この検討から当初の目標を次のように定め，推進している．

- IEC62443を汎用的な国際標準として選択

☆1 CSSC : Control System Security Center.
☆2 IEC62443 : Industrial Network and System Security.
☆3 WIB : International Instrument User's Association（国際装置ユーザ協会）.
☆4 NERC : North American Electric Reliability Corporation（北米電力信頼性評議会）.
☆5 CIP : Critical Infrastructure Protection.
☆6 NIST : National Institute of Standards and Technology（米国標準技術研究所）.
☆7 IR7628 : Interagency Report Guidelines for Smart Grid Cyber Security.
☆8 ISO/IEC62278 : Railway applications - Specification and demonstration of reliability, availability, maintainability and safety.
☆9 IPA : Information-technology Promotion Agency, Japan.



ISA Reference	IEC Reference	Title	Status
ISA-62443-1-1	IEC/TS 62443-1-1	Terminology, concepts and models	Published, Under Revision
ISA-TR62443-1-2	IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Under Development
ISA-62443-1-3	IEC 62443-1-3	System security compliance metrics	Under Development
ISA-62443-1-4	IEC/TR 62443-1-4	IACS security life cycle and use case	Proposed
ISA-62443-2-1	IEC 62443-2-1	IACS security management system - Requirements	Published, Under Revision
ISA-62443-2-2	IEC 62443-2-2	IACS security management system - Implementation guidance	Proposed
ISA-TR62443-2-3	IEC/TR 62443-2-3	Patch management in the IACS environment	Under Development
ISA-62443-2-4	IEC 62443-2-4	Requirements for IACS solution suppliers	Under Development within IEC TC65 WG10
ISA-TR62443-3-1	IEC/TR 62443-3-1	Security technologies for IACS	Published
ISA-62443-3-2	IEC 62443-3-2	Security assurance levels for zones and conduits	Under Development
ISA-62443-3-3	IEC 62443-3-3	System security requirements and security assurance levels	Published
ISA-62443-4-1	IEC 62443-4-1	Product Development Requirements	Under Development
ISA-62443-4-2	IEC 62443-4-2	Technical security requirements for IACS components	Under Development

■ 13標準中，4つが標準化済み
■ 装置ベンダ向けEDSA認証は米国で先行，事業・運用者向けCSMS認証は国内で先行

図 -2 ISA/IEC62443 標準化および評価・認証の状況 [1)]

- 標準確立，評価認証を一体で推進する
- IEC62443 対応の認証標準として，ISCI[☆10] で先行している標準に対応する

国際標準 ISA/IEC62443 の概要

IEC[☆11] は標準作成作業が完了しないと標準案を一般に公開しない．一方 ISA[☆12] は国際的学会で，検討中の標準原案も公開している．本稿では ISA の標準化作業中の標準原案をベースに記載している．以降標準について説明するときは，ISA/IEC62443 と記す．

図 -2 に ISA/IEC62443 標準化および評価・認証の状況を示す．現在，1 ～ 4 のシリーズに分けて，13 種の標準の策定を進めている [2)]．

▌ISA/IEC62443-1 シリーズ

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等すべての関係者が共通して参照する標準である．

1）ISA/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．用語の解説，制御システムの動向や状況，セキュリティ概念等を記載している．7 つの基礎的な要件（Foundational Requirement：FR）が規定されている．初版は 2009 年 7 月に発行済であるが，2014 年現在，第 2 版が策定中である．

2）ISA/IEC62443-1-2

制御システムのセキュリティに関連する用語・略語集を記した技術報告書（TR）である．草案（Documents for Committee）の策定中である．

3）ISA/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．評価基準（metrics）策定等を記載している．2014 年現在，草案の策定中である．

4）ISA/IEC62443-1-4

制御システムのライフサイクルとユースケースを記載予定で，WG も今後決める予定である．

▌ISA/IEC62443-2 シリーズ

事業者や運用者等の組織を対象としたセキュリティ要求事項等を規定した標準である．

1）ISA/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[☆13] というセキュリティマネジメントプログラムの標準と

☆10 ISCI：ISA Security Compliance Institute（ISA セキュリティ適合性協会）．
☆11 IEC：International Electrotechnical Commission（国際電気標準会議）．
☆12 ISA：International Society of Automation（国際計測制御学会）．
☆13 CSMS：Cyber Security Management System.

なっており，これはISMS[☆14]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月に発行済みであるが，2014年現在，第2版が策定中である．

2）ISA/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について，セキュリティポリシー，組織，資産管理，人的資源セキュリティ，物理環境セキュリティ等を記載している．2014年現在，草案の策定中である．

3）ISA/IEC62443-2-3

制御システムにおける脆弱性対策用パッチの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等について記載している．2014年現在，草案の策定中である．

4）ISA/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等を規定した文書（IS）である．業界で先行している認証を基に，事業者が制御機器やシステムを調達する際に必要な要件等が提案されている．2014年現在，草案の策定中である．

ISA/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標準である．

1）ISA/IEC62443-3-1

一般的なセキュリティ技術のうち，制御システムに適用可能なものについて解説等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，人的セキュリティ等を記載している．初版は2009年7月に発行済である．

2）ISA/IEC62443-3-2

同一のセキュリティポリシーを適用する範囲（ゾーン）やゾーン間を連結する範囲（コンジット：導管の意味）に関するセキュリティについて規定する文書（IS）である．ゾーンおよびコンジットやセキュリティ要求事項の定義等が規定され，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．2014年現在，草案の策定中である．

3）ISA/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文書（IS）である．62443-1-1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（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．初版は2013年8月に発行済み．

ISA/IEC62443-4シリーズ

制御システムの一部であるコンポーネントが対象となる標準である．

1）ISA/IEC62443-4-1

コンポーネントの開発要件を規定した文書（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，ISASecure[☆15]のEDSA[☆16]（SDSA[☆17]）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．2014年現在，草案の策定中である．

2）ISA/IEC62443-4-2

コンポーネントのセキュリティ要件を規定した文書（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している．ISASecureのEDSA（FSA[☆18]）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．2014

☆14 ISMS：Information Security Management System.

☆15 ISCIが推進する制御システムと制御機器の認証制度名.

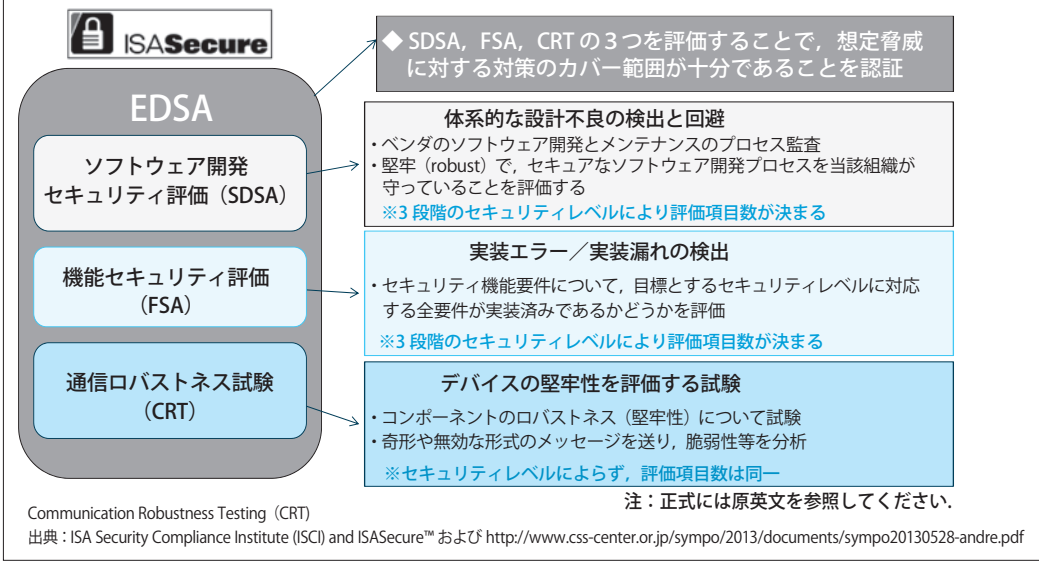
☆16 EDSA：Embedded Device Security Assurance．制御機器（組込み機器）のセキュリティ保証に関する認証制度.

☆17 SDSA：Software Development Security Assessment.

☆18 FSA：Functional Security Assessment.

認証プログラム	ISASecure	Achilles	WIB
対象	制御機器・システム（コンポーネント／システム）	制御機器（コンポーネント）	制御システム（システム）
標準	業界標準（ISA/ISCI）	業界標準	業界標準
形態	国際学会主導（ISA/ISCI）	Wurldtech 社（カナダ）	民間団体（シェル他）
提供方法	標準準拠評価型＋ツール提供型（通信ロバストネステスト）	ツール提供型（通信ロバストネステスト）	標準準拠評価型＋ツール提供型（通信ロバストネステスト）
内容	国際学会 ISA 配下の ISCI が作成した制御システムにおけるコンポーネント（EDSA），システム（SSA）に関する国際学会認証プログラム	Wurldtech 社（カナダ）が提供している制御機器の民間認証プログラム．認証に Wurldtech 社の Achilles Test Platform を使用	欧州石油メジャが中心となり，制御機器，システムベンダに対するセキュリティ調達要件を規定した標準．認証に Wurldtech 社の Achilles Test Platform を使用
特長	IEC62443 へ取り込まれる見込み	遠隔地からのリモートテストが可能	IEC62443-2-4 として国際標準化の見込み

表 -1　主な制御システムの認証プログラム



注：正式には原英文を参照してください．
Communication Robustness Testing（CRT）
出典：ISA Security Compliance Institute (ISCI) and ISASecure™ および http://www.css-center.or.jp/sympo/2013/documents/sympo20130528-andre.pdf

図 -3
制御機器に対する EDSA 認証

年現在，草案の策定中である．

制御システム・機器の認証の動向

▌セキュリティ認証の動向

制御機器の民間でのセキュリティ認証として，Wurldtech 社の Achilles 認証が普及している．制御機器・システム供給者に対するセキュリティ調達要件を規定した業界標準としての WIB が欧州の石油メジャーを中心に利用されている．現在，国際的な第三者認証の ISASecure 認証が，上記を含めた統合的な認証制度として進展中である．各組織が進める認証プログラムを**表 -1** に示した．

▌国際的な制御システムのセキュリティ認証標準 ISA/ISCI の EDSA/SSA☆19, 3)

セキュアな制御システムを実現するためには，制御システムを構成する各制御機器や制御システムがセキュアで安全かつ安定的に利用できることが重要である．そこで制御機器ベンダや制御システム供給者は，セキュリティ強靭化に向け，ISA/IEC62443 の制御システムセキュリティ標準を参照してセキュリティ機能の実装を進めている．セキュリティ機能の実装に対して制御機器や制御システムが，国際標準の要求に適合しているかの評価を実施し，評価結果を判定する認証が必要である．国際的には ISCI が進めている ISASecure 認証が注目されている．この認証は第三者の認証機関で実施される．

ISCI とは，制御システム事業者，サプライヤや業界組織からなるコンソーシアムで，2007 年に設置された．ISCI は，**図 -3** の制御機器の認証から取り組んでいる．これが EDSA と呼ばれるものである．EDSA 以外の取り組みには，SSA や SDLA☆20 と呼ばれる認証標準がある．SSA は 2014 年 2 月に公開され，SSA 認証が近々開始される状況にある．SDLA は，現在開発中である．

▌国際的な相互承認に基づいた認証フレームワーク

日本の制御機器ベンダが日本で取得した認証が，海外でも通用することは海外輸出などでの競争力を確保するために重要である．経済産業省主導のも

☆19 SSA : System Security Assurance.

☆20 SDLA : Security Development Lifecycle Assurance.

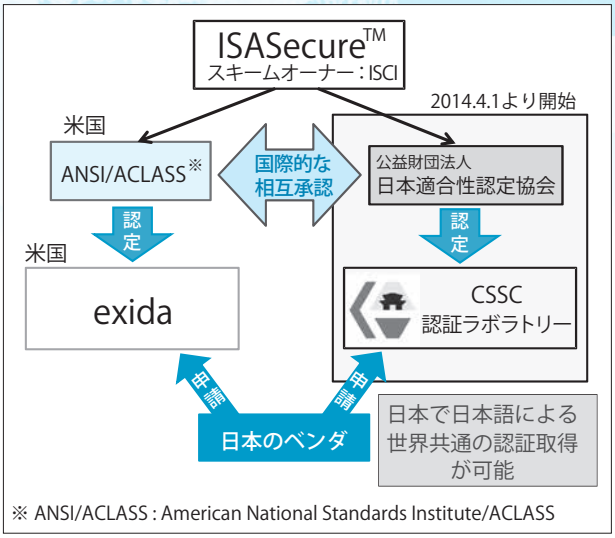


図 -4　ISASecure EDSA 認証と国際的な相互承認

と，CSSC 内に独立した CSSC 認証ラボラトリーを 2013 年 8 月に設立し，ISASecure 認証を推進している．この ISASecure EDSA 認証は，国際的な相互承認の認証フレームワークで，**図 -4** に示すように海外の認証機関で認証取得をする必要がなく，日本で日本語により EDSA 認証が受審できる [4]．

セキュリティ認証に関する評価・検証技術の具体例

ISASecure EDSA 認証は 3 つの標準で構成されている．それぞれの評価，テストについて以下説明する．

ソフトウェア開発セキュリティ評価（SDSA）

対象とする制御機器のソフトウェア開発プロセスを評価するのが SDSA である．EDSA-312 の要求事項に沿って，開発ドキュメント（計画／成果物）とレビュー記録（PDCA プロセスの妥当性と記録確認）を評価する．

SDSA では，たとえば，**図 -5** に示す V 字モデルに従ったセキュリティ活動フェーズが組み込まれていることの監査を実施する．認証機関の監査人は，認証を受けるために提出されたドキュメントと開発者へのインタビューを含む現地訪問を実施する．

機能セキュリティ評価（FSA）

対象とする制御機器のセキュリティ機能の評価をするのが，FSA である．EDSA-311 の要求事項に沿って，対象とする制御機器の機能や初期設定等の確認を行い，適合／不適合を評価する．一部の要求事項については，実機を用いて実際に動作を確認する．

認証機関の監査人は，ユーザ向けや設計用ドキュメント，監査のために特別に提出されたドキュメントおよび制御機器のテスト結果に基づいて監査を実施する．監査の主な要求事項を**表 -2** に示す．

通信堅牢性（ロバストネス）テスト（CRT）

図 -6 に示す ISCI 認定の試験デバイスにより試験パケットを試験対象 DUT（DeviceUnder Test）に対して送信し，サービスの維持を確認するテストが CRT である．EDSA-310 ほかに従って，**図 -7** に示す 6 つの必須サービスの維持が合否判定の基準となる．このときコントローラだけではなく，事実上 HMI 側の用意も必要となる．

認証機関の監査人は，制御機器に対して上記の通信堅牢性テストを実施する．現在の通信堅牢性テストの対象となる通信プロトコルは次の 6 種類である．

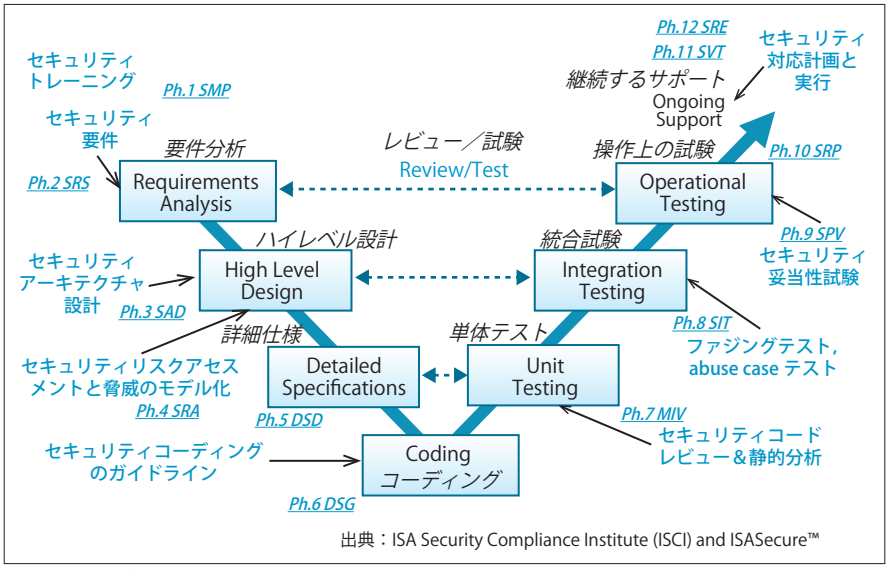


図 -5　開発プロセスの V 字モデルに従ったセキュリティ活動フェーズ

EDSA-401：IEEE 802.3（Ethernet），ARP, IPv4, ICMPv4, UDP, TCP

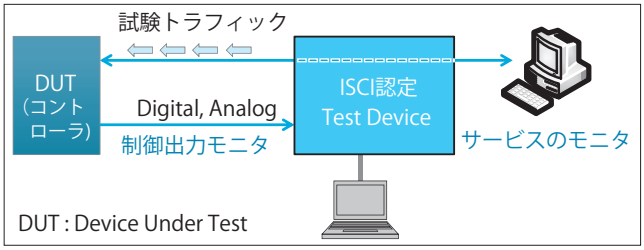
セキュアな制御システムを目指して

制御機器の標準化と認証は今後ますます重要になってくる．今後は制御システムのセキュリティ標準と認証という新しい分野に対して，評価技術の研究開発が必要になってくると思う．この分野についても，CSSC は組合員企業と連携して研究を進めていく所存である．

CSSC は，発足時の組合員は 8 組織だったが，2014 年 3 月末現在 23 組織に拡大している．さらに賛助会員制も立ち上げて，研究開発成果の普及に努めている．重要インフラ事業者を始めとする制御システム関係者の CSSC への参画を期待している．また，CSSC の認証実証事業などを多賀城市の宮城復興パークで実施し，復興支援にも貢献していく所存である．今後とも CSSC は，「セキュアな制御システムを世界へ未来へ」という目標を掲げてグローバルに活動を進める計画である．

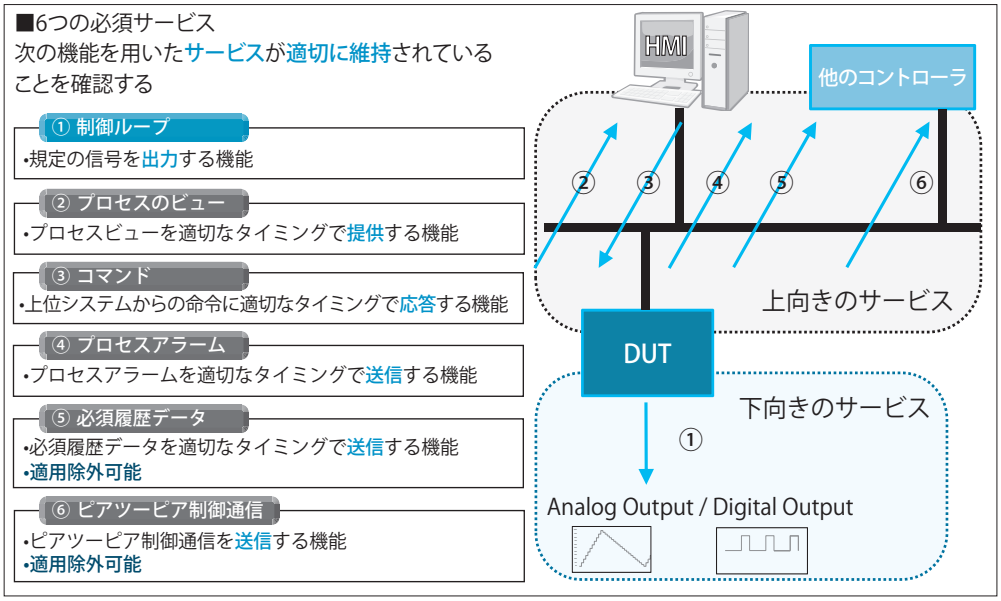
アクセスコントロール (AC : Access Control)	ユーザ承認，ユーザ認証，システム使用通知，セッションロック／終了 User Authorization, User Authentication, System Use Notification, Session Locking / Termination
使用コントロール (UC : Use Control)	デバイス認証，監査証跡 Device Authentication, Audit Trail
データの完全性 (DI : Data Integrity)	転送中のデータ，保管中のデータ Data in Transit, Data at Rest
データの機密性 (DC : Data Confidentiality)	転送中のデータ，保管中のデータ，暗号化 Data in Transit, Data at Rest, Crypto
データフロー制限 (RDF : Restrict Data Flow)	情報フロー実施，適用パーティッショニング，機能分離 Information Flow Enforcement, Application Partitioning, Function Isolation
イベントへのタイムリーなレスポンス (TRE : Timely Response to Event)	インシデント応答 Incident Response
ネットワークリソースの可用性 (NRA : Network Resource Availability)	サービス不能攻撃防御，バックアップと回復 Denial of Service Protection, Backup & Recovery

▲表 -2　セキュリティ機能評価の主な要求事項



◀図 -6　CRT 試験環境のイメージ

▼図 -7　CRT 試験の内容…6 つの必須サービス



参考文献

1) ISA99 Committee Work Product List, http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx
2) IPA : SEC journal, p.182（2014 年 1 月 31 日発行），https://www.ipa.go.jp/files/000036644.pdf
3) ISCI ISASecure Program, http://www.isasecure.org/
4) CSSC 認証ラボラトリー，http://www.cssc-cl.org/

（2014 年 4 月 5 日受付）

小林偉昭　hideaki.kobayashi@css-center.or.jp

1972 年日立入社，ネットワークとセキュリティ経験，2006 年より IPA 情報セキュリティ技術ラボラトリー長，脆弱性関連業務と自動車や制御システムのセキュリティ．2013 年から CSSC 専務理事，研究開発，認証事業に従事し，現在へ．