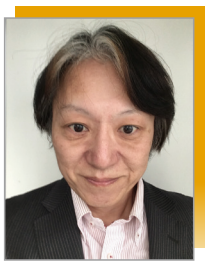
特集
Special Feature

［DX（デジタル・トランスフォーメーション）時代のサプライチェーン・セキュリティ］

4 制御機器のセキュリティ認証制度

基 応 専 般




神余浩夫　三菱電機（株）

山田　勉　（株）日立製作所

制御システムへのサイバー脅威と対策

制御システムへのサイバー脅威

2010 年以降, 社会インフラおよび産業システムを狙ったサイバーセキュリティ・インシデントが増加している. 表 -1 に, 過去に話題となった制御システム関連のセキュリティ・インシデントを示す [1].

各国の専門家は，緊急課題として産業制御システムのセキュリティ対策に取り組みを開始し，国際標準や分野別ガイドラインの開発を進めている [2]．その対策の骨子は，まず，対象システムの守るべき資産・人命についてリスクアセスメントを実施し，それらをいかなる脅威からどれくらいの堅牢さ（セキュリティレベル）で守るのかを評価する．そして，それぞれのセキュリティレベルに十分なリスク低減対策を講じて，リスクを許容できる程度に抑えることである.

ここで重要なのは，産業制御システムを構成する制御機器，監視装置やネットワーク装置等が求められるセキュリティレベルを満足していなければ，セキュアなシステムを構築できないことである．後付けでファイアウォールや侵入検知装置を追加しても，肝心の制御機器に脆弱性があっては，システムが停止するようなインシデントにとどまらず人身事故や爆発事故まで起こり得る. したがって，制御機器市場において，制御機器のセキュリティ規格適合が注目を集めている.

制御機器のセキュリティ認証とサプライチェーン

欧州 CE マーキングのように，製品供給者が規格適合性を自ら表明する自己宣言は，製品のセキュリティ対応を示す簡便な方法である．問題は，その自己宣言の質が製品供給者を信用できるかに依存することにある．やはり，製品を調達するシステム構築者が，自身の責任で製品の規格適合性を評価するべきだろうか. だが，制御機器のセキュリティ規格適合性評価は技術的難易度も，必要な試験機材も，評価の工数も多大であり，調達者側の負担が大きい.

信頼できる第三者による製品の規格適合性評価は，自己宣言と調達者評価の利点を併せ持つ．然るべき審査機関がセキュリティ規格適合性を認証した製品であれば，調達者は安心して購入および使用できる．また，同一製品の評価を繰り返す，何度も自己宣言評

■表 -1　最近の制御システムのセキュリティ・インシデント

年	名称	インシデント
2010	Stuxnet	イランのウラン濃縮工場の遠心分離装置を破壊
2015	BlackEnergy	ウクライナの電力システムを停止＝停電
2016	Industroyer	ウクライナの電力開閉器を操作＝停電
2017	HatMan (Triton)	サウジアラビア石油プラントの安全計装制御装置を異常停止 ＝プラントシャットダウン
2020	EKANS	アルゼンチンの配電会社のカスタマサービスに障害

価データを提供することもないので，供給者と調達者の双方の労力も軽減できる．いま，いくつかの国際標準化団体が，セキュリティ規格適合性評価の枠組み（スキーム）の開発および運用を始めつつある☆1．

制御機器のセキュリティ証明のためには，製品を構成するハードウェア，ソフトウェア部品についても，セキュリティ保証しなければならない．脆弱性のある怪しい部品は使えないし，脆弱性が見つかった際には迅速にセキュリティパッチが開示されなければ，その部品は採用できない．すなわち，制御機器製品の供給者と調達者を中心に，部品から社会システムまで巨大なサプライチェーンをセキュリティ保証することが，求められている．

本稿では，セキュアな産業制御システムを構築するためのセキュリティ製品認証の国際標準の動向について解説する．さらに，部品や製品のセキュリティを保証するためのセキュア・サプライチェーンの状況についても述べる．

制御システムのサイバーセキュリティ標準

ISA99

制御システムのサイバーセキュリティ標準の草分けは，国際制御学会（ISA：The International Society of Automation）の「ISA99産業自動制御システムのセキュリティ」である☆2．ISA99は，情報漏洩や機密流出を扱う情報セキュリティとは異なり，サイバー脅威から産業オートメーション制御システム（IACS）の操業妨害や事故を防ぐことを目的に開発された．2001年の米国テロにおいて社会インフラがサイバー攻撃を受けたことから，この標準化が急務となった．

ISA99の初版は2004年に発行されたが，当時はUNIXやインターネットなどのオープン技術の脆弱性が狙われることはあっても，各社独自のコントローラやプロトコルが攻撃を受けることはないと考えられていた．そのため，情報セキュリティと同じ製品や技術で制御システムも守れるとして，制御システムに特化した技術開発は進まなかった．ところが，2010年にイランのウラン濃縮工場の遠心分離装置を破壊したマルウェアStuxnet以降，各社独自のコントローラやプロトコルの脆弱性がサイバー脅威に直接狙われるようになり，ISA99が再評価されることになった．

IEC 62443

もともと，情報セキュリティ技術の標準化は，「ISO/IEC/JTC1/SC 27 情報セキュリティと個人情報保護」にて議論されていた．しかし，制御システムおよび組込みシステムは，情報セキュリティ専門家にとって未知の分野であり，制御機器各社固有の技術の壁にも阻まれて，議論は進まなかった．

2010年，ISAとIECは産業制御システムのサイバーセキュリティ標準を共同開発することで合意し，ISA99をベースとして「ISA/IEC 62443 産業通信ネットワーク－ネットワークシステムセキュリティ」を制定することになった．ISA99はANSI規格でもあったが，IEC国際標準になったことで多くの標準や団体組織との整合性を求められるようになった．

表-2にISA/IEC 62443シリーズの構成を示す☆3．標準は読者想定によって，共通，アセットオーナ，インテグレータ，制御機器に分類される．斜字は現在開

☆1 SP800-82, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

☆2 ISA99, https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

☆3 IEC/TC65 work program, https://www.iec.ch/dyn/www/f?p=103:23:25380131696612::::FSP_ORG_ID,FSP_LANG_ID:1250,25

■表-2　ISA/IEC 62443 シリーズの構成（斜字は開発中）

対象	副番	規格名
共通	1-1	Concepts & models
	1-2	*Glossary of terms*
	1-3	*Conformance metrics*
	1-4	*Lifecycle & use case*
アセットオーナ	2-1	Requirements for IACS asset owners
	2-2	*Security protection ratings*
	2-3	Patch management
	2-4	Requirements for service providers
	2-5	*Implementation guidance*
インテグレータ	3-1	Security technologies
	3-2	Security risk assessment
	3-3	Security requirements & levels
制御機器	4-1	Product development life cycle
	4-2	Requirements for IACS components

発中であり，発行済みのいくつかも改訂を進めている．表 -2 以外にも，分野共通規格，分野ごとの標準，規格適合性評価のための基準など，新しい開発提案が続いている．これらの開発提案は国際投票による承認を要するため，現在手続きを進めている．

NIST

NIST（National Institute of Standards and Technology）は，米国商務省に属する組織であり，サイバーセキュリティに関して多数の技術文書を発行している．主な文書を表 -3 に示す．

特に，「SP 800-82 産業制御システムのセキュリティガイド」は，政府機関に産業制御システムを納入する際のセキュリティ要件を規定した文書であり，産業制御システムを構成する分散制御システム，プログラマブルコントローラ，監視システムなどの機能や設定について言及している[3]．技術的に，ISA99 との関係性が深い．

経済産業省サイバーフィジカルセキュリティ対策フレームワーク（CPSF）

経済産業省が策定した CPSF（Cyber Physical Security Framework）は技術標準ではないが，産業システムやサービスのセキュリティ確保のための参照モデルとして国際的に知られている．CPSF の概念モデルを図 -1 に示す[4]．CPSF は，サービスをフィジカル空間の企業間の繋がり（第 1 層）と，サイバー空間のデータの繋がり（第 3 層），およびその両者間の「転写」機能による繋がり（第 2 層）から構成される．第 1 層はモノの動きすなわちサプライチェーン，第 3 層はデータの動きすなわちバリューチェーン，そして第 2 層は IoT とみなすことができる．各層が適切な信頼性確保の対策を講じることで，現実のサービスの信頼性（セキュリティ含む）が保証できる．

たとえば，制御システムに使われる制御機器，およびその部品（ハードウェア，ソフトウェア）は，第 1 層の取引により組み立てられる．調達者は，購入する制御機器およびその部品のセキュリティレベルや脆弱性について第 3 層の情報により調査する．ここで，制御機器の型名やバージョンがセキュリティ情報と正しく紐ついているか，虚偽や誤りがないかは，第 2 層が保証する．すなわち，すべての層が信頼できてこそ，セキュアな部品調達およびシステム構築ができる．

すでに技術蓄積のある第 1 層と第 3 層に比べて，第 2 層 IoT 転写機能の信頼性技術は，いまだ検討開発段階にあり，今後の発展が望まれる．

■表 -3　制御システムのセキュリティに関する NIST 標準

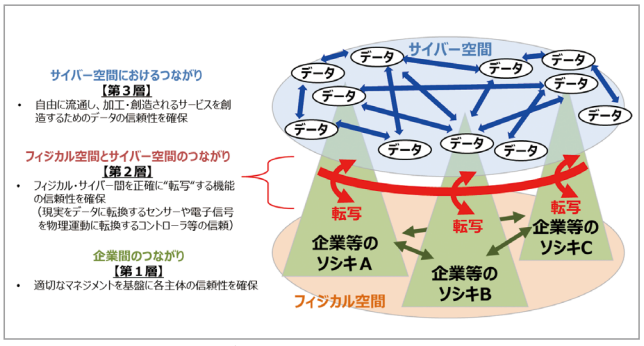
文書	表題
SP800-30	Guide for Conducting Risk Assessments
SP800-40	Creating a Patch and Vulnerability Management Program
SP800-53	Recommended Security Controls for Federal Information Systems
SP800-61	Computer Security Incident Handling Guide
SP800-64	Security Considerations in the System Development Life Cycle
SP800-82	**Guide to Industrial Control Systems (ICS) Security**
SP800-83	Guide to Malware Incident Prevention and Handling
SP800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

制御機器のセキュリティ認証

自己宣言と第三者認証

製品やサービスが法令や標準等の品質を満足することを保証する方法は，誰が規格適合性を試験および証明するかによって 3 つに大別される．

第 1 は，製造者または供給者による自己宣言である．



■図 -1　CPSF の 3 層モデル

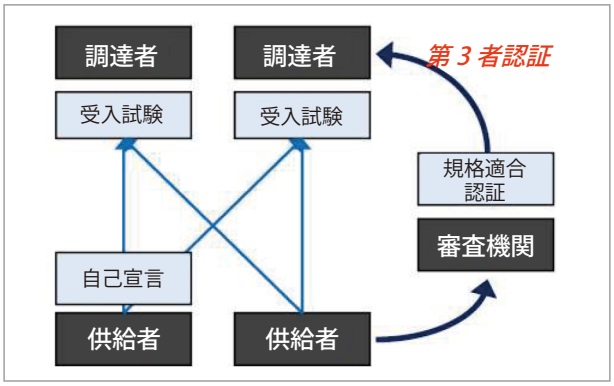
製造者は品質保証のために，基準に従った試験を実施するので，それを根拠に規格適合の自己宣言を行う．供給者は，求めに応じて規格適合の根拠や試験結果を開示する．自己宣言は，供給者が信用できるかどうかが鍵となる．

第 2 は，調達者が自らの基準で製品を指定する方法である．セキュリティ規格適合性は，技術的にも難しく，試験機材も高価であり，評価の工数も多く要する傾向にある．調達者に大きな負担がかかるため，余裕のある調達者にしか選択できない．

第 3 は，信用できる第三者機関による規格適合性試験および認証である．一般に，ISO 17025 試験所および校正機関の能力を有する試験所が，客観的に信用できる条件となる．以上 3 方式の対比を図 -2 に示す．

環境条件のように試験が簡単な場合，供給者による試験結果を再現追試できるため，自己宣言でも十分信用できる．しかし，技術的にも高度なセキュリティ規格適合性評価は，再試験が容易ではないことに加えて，供給者の評価が不適切な場合もある．調達者評価も，対象製品すべての脆弱性を調べるのは困難である．したがって，第三者評価が，供給者と調達者にとって評価の労力とコストの点でバランスが良い．特に，複数の調達者が同じ製品の評価を繰り返さなくてよい，供給者が高度なセキュリティ試験機材を揃えなくてもよいので，市場全体での規格適合性評価のコストは抑制できる．

技術的に高度かつ認証の信憑性も求められる制御機器のセキュリティ認証は，第三者認証が主流になると思われる．以下では，制御機器のセキュリティ認証制度の状況について述べる．



■図 -2　規格適合性評価の方式の対比

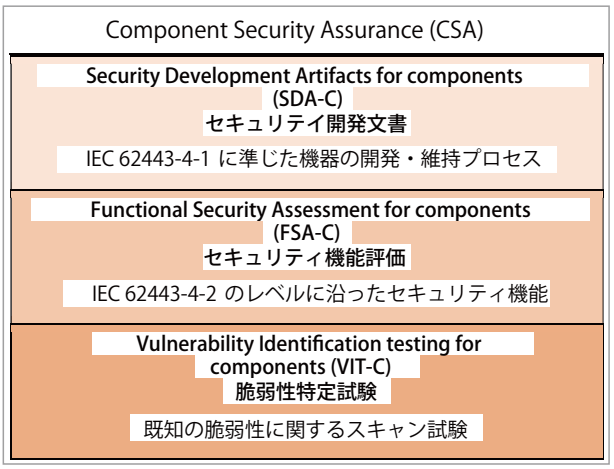
ISAsecure

前述の ISA は，2011 年に審査機関である ISCI（ISA Security Compliance Institute）を立ち上げ，ISAsecure 認証スキームに基づく制御機器のセキュリティ認証を運用している．現在の認証制度は，制御機器の製品認証 CSA（Component Security Assurance，旧 EDSA 認証），システム認証 SSA（System Security Assurance）および開発組織認証 SDLA（Security Development Lifecycle Assurance）である☆4．

CSA 認証の試験項目を図 -3 に示す．まず，開発プロセスが IEC 62443-4-1 セキュリティ製品開発プロセス要求に適合しているか，開発文書等が揃っているかを確認する（SDA-C）．開発組織が SDLA 取得済みの場合，この試験の一部が免除される．次に，IEC 62443-4-2 制御機器のセキュリティ機能が要求に応じて実現されているかを評価する（FSA-C）．最後に，既知の脆弱性が塞がれているかを試験により確認する（VIT-C）．

ISAsecure 認証は，ISA/IEC 62443 に忠実かつ分野汎用的であるため，分散制御システム（DCS）や

☆4　ISCI, https://www.isasecure.org/en-US/Certification



■図 -3　CSA 認証（製品認証）の試験項目

安全計装システム (SIS) など 42 機種 (2020 年 10 月時点) が認証を受けている．日本でも,(技術研究組合) 制御システムセキュリティセンター (CSSC：Control System Security Center) が，ISCI のライセンスを受けて EDSA 認証を実施している☆5．CSSC は現在国内唯一のセキュリティ製品認証機関であり，日本語で審査できる点が，国内供給者から支持されている．

Achilles

Achilles Communications Certification 制度は，米国 Wurldtech 社 (現在は GE Digital 社の傘下) が，2008 年から開始した制御機器のセキュリティ認証制度である☆6．ISAsecure が規格に忠実なため審査に時間がかかるのに対して，審査期間を短縮するために通信堅牢性に注目した試験プログラム Achilles Test Platform を採用している．Achilles Test Platform の対応プロトコルを図 -4 に示す．MODBUS/TCP や OPC UA など制御システムの代表的なプロトコルに対応している．Achilles Test Platform は代表的なファジングテスト；想定外の異常データを送信して対象機器の動作を確認するツールであり，多くの審査機関でも使われている．

Achilles 認証には，脆弱性対策の強度によって 2 段階のレベルがあり, Level2 はより厳しい要件となっている．レベル 1 認証 276 機種，レベル 2 認証 528 機種 (2020 年 10 月時点) が公表されている．

☆5 CSSC 認証ラボラトリ，http://www.cssc-cl.org/
☆6 Achilles Communication Certification, https://www.ge.com/digital/applications/achilles-communications-certified-products

	SCADA	IT
Application	DNP3 Ethernet/IP FF-HSE MMS MODBUS/TCP SES-92 OPC -UA	FTP HTTP NTP RDP RPC SNMP Telnet
Presentation		
Session		
Transport	TCP, UDP	
Networks	ICMP, IGMP, IP	
Data Link	LLDP, ARP, Ethernet	

■図 -4　Achilles test platform の対応プロトコル

WIB

WIB (Werkgroup voor Instrument Beoordeling) は，主にオランダとベルギーのプロセス産業エンドユーザが参加する団体である．欧州各国の類似団体と連携して，制御機器のセキュリティ認証制度を運営している．そのために，前述の ISA や NIST などの国際的な標準化組織と連携をとり，標準化案について互換性や試験容易性について相互レビューを行っている [5]．

WIB 認証の特徴は，ユーザ主導でセキュリティ要件を明確にして，供給者に適合する制御機器やシステムを開発させたことにある．供給者は，ユーザ要求が明確であり，実現性やコストの点で無理がなく，かつ調達条件となっていることから，制御機器の WIB 認証を推進した．WIB 認証には，ゴールド，シルバー，ブロンズの 3 つのレベルがあり，最初からゴールドを狙うのではなく，導入計画に従って段階的にレベルを高めていくことができる．

WIB 認証は石油化学などプロセス産業に特化しており，他分野をカバーする汎用的な認証制度としては認められていない．WIB を含む分野と標準化の関係を表 -4 に示す．

IEC/CAB/IECEE

IEC/CAB (Conformity Assessment Board) 適合性評価評議会は，製品や組織が IEC 標準に適合するか評価方法や手順を規定し，関連する認証制度を

■表 -4　産業分野と標準化状況

対象	汎用	石油化学	電力	スマートグリッド
組織	IEC 62443-2		NERC CIP	NIST IR7628
システム	IEC 62443-3	WIB	IEC 61850	
機器	IEC 62443-4		IEEE 1686	-

とりまとめる．その下部組織の電気機器製品を担当するIECEE（IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components）において，IEC 62443に基づいた制御機器のセキュリティ認証制度の開発を進めている．

2010年頃より，IEC/CABの複数の組織において，さまざまな分野の制御機器セキュリティ認証スキームの議論が並列して始まった．2019年にそれらの議論はIECEE/CMC（Certification Management Committee）のWG 31サイバーセキュリティに一本化され，製品，システムおよび組織についてIEC 62443規格適合性評価が議論されている[☆7]．筆者（山田）も，このWGに参加している．

ISAとIECが標準化を共同で進めることになったため，ISAsecureスキームをIECEEスキームに統合する案も検討された．しかし，IECの認証スキームとの整合やISAsecure認証済み製品の扱いなど調整がつかず，IECは独自スキーム（OD-2061）を策定した[☆8]．IECEE認証スキームは，国際的な認証制度の本命であり，引き続き改訂議論が進められている．

ENISA

ENISA（European Network and Information Security Agency, 欧州ネットワーク情報セキュリティ機関）は，2004年に設立されたEUの専門機関である．名前の通り，EU内のネットワークと情報セキュリティ問題を取り扱う．

2019年に成立したEUサイバーセキュリティ法によると，EU域内で活動する企業は，情報機器，関連サービスおよび開発プロセスについて認証を受け，取引においてその認証書を開示しなければならないとある[☆9]．ENISAは，認証書に関する欧州共通のサイバーセキュリティ認証フレームワークを提供する．このフレームワークは，対象製品やサービスの分類，サイバーセキュリティ技術要件，評価の種類（自己宣言または第三者評価），および保証レベル（3段階）を指定している．

ただし，現時点ですべての製品・サービスの認証手順が完成しておらず，重要分野から順次整備していく計画となっている．

その他

ドイツのTUV，米国のULなどがIEC 62443に基づくプライベート認証を開始している．第三者認証は，供給者と調達者の双方にとって納得できる審査機関を選択することが重要である．そのため，その市場地域において実績のある審査機関が選ばれる傾向にある．

幸い，多くの有力審査機関がIECEEスキーム策定に参加しており，将来的には彼らのプライベート認証制度がIECEEスキームに合流および統合していくと予想される．

セキュアサプライチェーン

産業制御システムのアセットオーナあるいはインテグレータは，その制御システムをセキュアにするために，要求するセキュリティレベルに十分な制御機器や情報機器を調達しなければならない．調達者が，個々の製品のセキュリティ規格適合およびセキュリティレベルを評価するのは技術的，コスト的に困難であり，第三者認証に向けたセキュリティ認証スキームの開発が急務となっている．

ところで，アセットオーナやインテグレータと同様の問題が，制御機器供給者にも存在する．コントローラや監視システムは，プロセッサなど多くのハードウェアとソフトウェアの部品から構成されている．それらの部品はバックドア等がなく，既知の脆弱性が塞がれたセキュアな部品でなければならない．もし，新規に脆弱性が見つかった場合は，迅速に対策（パッチ等）が提供され，エンドユーザにまで届かなければならない．すなわち，すべての部品からエンドユーザまでの巨大なサプラ

☆7 IEC/CAB/IECEE/CMC/WG 31, https://www.iecee.org/dyn/www/f?p=106:46:0::::FSP_ORG_ID:19409
☆8 IECEE OD-2061, https://www.iecee.org/documents/refdocs/downloads/od-2061_ed.2.0.pdf
☆9 Regulation EU No.526/2013, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

特集
Special Feature

イチェーンにセキュリティを要求するようになった.

特に昨年から，大企業から中小企業に至るまで，サプライチェーンの弱点を狙ったサイバー攻撃が顕在化し，政府は政策として対策を進めている[6]．企業は，自らの事業継続の観点だけでなく，社会的責任としてセキュリティ確保や管理を求められる．具体的には，表 -5 に示す「共有」「報告」「公表」の 3 つのアクションであり，これらにより企業のセキュリティ対策への取り組みの可視化を行う．さらに，各分野のセキュリティ対策の取り組みと連動することで，産業界全体のセキュリティ推進につなげる.

前述の NIST や ENISA もセキュアなサプライチェーンに注目しており，認証制度とリスク管理を彼らのフレームワークに取り込んでいる.

将来に向けて

産業制御システムがセキュリティ国際標準に適合していることを客観的に示すことで，システムのセキュリティ性を証明できる．そのためには，セキュリティ標準の第三者認証を得た制御機器やソフトウェアを適用することが，市場原理としても効果的・効率的である．しかし，話は制御機器にとどまらず，制御機器が採用したプロセッサやソフトウェア等の部品まで，脆弱性対応が求められる．すなわち，部品からエンドユーザまでの巨大なセキュア・サプライチェーンが求められている.

セキュア・サプライチェーンは国内問題でなく，国際経済連携，技術共同開発，安全保障など多くの側面を持つ．難問ではあるが緊急課題であり，関係者のご協力をお願いしたい.

■表 -5　サプライチェーン全体のセキュリティ確保のために求められる行動

共有 (Share)	報告 (Report)	公表 (Announcement)
①サプライチェーン共有主体間での高密度な情報共有	②機微技術情報の流出懸念時の経産省への報告	③適切な場合の公表
重要なサプライチェーンを共有する企業間で，サイバー攻撃を受けて影響が及んでいる可能性がある場合には，お互いに高密度な情報共有をすることが望ましい.	軍事転用可能性のある技術情報（輸出管理対象を目安）の流出は安全保障環境に影響を与えるおそれ．流出の可能性がある場合は，経済産業省への報告が望ましい.	サイバー攻撃による被害が甚大で影響する範囲の特定が難しく，広く関係者を巻き込んでしまう可能性があり，情報共有では被害拡大の抑制を図ることが難しいと考えられる場合には，速やかにサイバー事案について公表をすることが望ましい.
中小企業を含めたサプライチェーン全体のサイバーセキュリティ対策の強化 **→サイバーセキュリティ対策の取り組みを可視化**		

参考文献

1) 宮地：制御システムセキュリティの現在と展望―この 1 年間を振り返って―，JPCERT/CC 制御システムセキュリティカンファレンス 2020.
2) 神余：機能安全と制御セキュリティの標準化動向，情報処理 Vol.58, No.11 (Nov. 2017).
3) SP 800-82 Rev.2：Guide to Industrial Control Systems (ICS) Security, CSRC, NIST (May 2015).
4) サイバー・フィジカル・セキュリティ対策フレームワーク，経済産業省商務情報政策局サイバーセキュリティ課，2019 年 4 月.
5) WIB Plant Security Working Group：Process Control Domain Security Requirements for Vendors, Report: M2784-X-10 ver2.0 (Oct. 2010).
6) 昨今の産業を巡るサイバーセキュリティに係る状況の認識と，今後の取組の方向性について，経済産業省商務情報政策局サイバーセキュリティ課，令和 2 年 6 月 12 日.

(2020 年 11 月 3 日受付)

■神余浩夫　Kanamaru.Hiroo@db.mitsubishielectric.co.jp

三菱電機（株）先端技術総合研究所主席技師長．産業制御システムの研究開発に従事．IEC 61508 機能安全，IEC 62443 サイバーセキュリティ，IEC TR 63069 機能安全とサイバーセキュリティ両立性，IEC/CAB/ IECEE/CMC/WG 32 機能安全認証の国際エキスパート．ISA 日本支部長.

■山田　勉　tsutomu.yamada.bs@hitachi.com

（株）日立製作所 制御プラットフォーム統括本部 制御セキュリティ設計部所属．制御システムのセキュリティコンサルティングに従事．IEC 62443 サイバーセキュリティ規格，IEC/CAB/IECEE/CMC/WG 31 サイバーセキュリティ認証の国際エキスパート.