❷ 機能安全と制御セキュリティの標準化動向

神余浩夫（三菱電機（株）先端技術総合研究所）

社会インフラの安全・安心

電力・上下水，鉄道・交通，ビル・地下街，工場・プラントなどの社会インフラは，その運行・運転状況を監視制御するために高度な制御システムが導入されている．制御システムは，電力系統設備や交通網に張り巡らされた多数のセンサから電力や車両の状況を把握し，プログラムされた制御機器あるいは中央制御室からの（人の）指令により，確実・快適なサービスを提供する．図 -1 は，発電所の中央制御室の例であり，大画面表示とインタラクティブ操作が特徴である．制御システムの故障やトラブルは，社会インフラの停止や事故に繋がるため，制御システムには高い信頼性，可用性そして安全性が要求される．

まだ情報処理技術が発達していない時代，これらの信頼性や安全性を確保するために，制御システム関連各社は十分検証された独自技術を適用した製品開発を行った．製品提供，システム構築から保全までをその 1 社が担当することで，制御システムの安全性を含む品質を保証していた．

1990 年代になると，制御システムは接続機器の拡大と監視制御の複雑化に対応するためにより多くのソフトウェアやネットワークが必要になった．当時，市販品として入手可能な UNIX や Windows などの汎用ソフトウェア，および Ethernet や TCP/IP などの汎用プロトコルが，制御システムに導入されるようになった．このようなオープンな情報処理技術を導入することで制御システムは性能向上・高機能化したが，その反面，ソフトウェアに潜む不具合が引き起こす影響や，システムの改修や部分更新における信頼性が懸念されるようになってきた．

図 -1　発電所の中央制御室の例（三菱電機）

いま，あらゆるモノが繋がる時代において，各国の研究者・技術者は，社会インフラを支える制御システムの安全・安心を保証する技術の確立を緊急課題として取り組んでいる．その中核となる技術が，機能安全（Functional Safety）技術と制御セキュリティ（Cyber Security）である．

機能安全とは，車の自動ブレーキの「障害物を検知して止まる」といった安全を担保する安全機能を実現する技術である．1999 年に発行された IEC 61508 機能安全規格に，安全関連部のハードウェアおよびソフトウェアが遵守すべき項目（要求）が規定されている．本規格は，ソフトウェアによって安全機能を実現できることを示した最初の規格である [1]．

制御セキュリティとは，一般的な情報セキュリティ技術の適用がむつかしい制御機器や監視装置を，ネットワーク経由（USB やワイヤレスの場合もある）の脅威から守ることである．国際計測自動制御学会（ISA）が 2002 年に ISA99 制御セキュリティ規格の開発に着手し，後に IEC 62443 制御セキュリティ規格として発行された [2]．

社会インフラの安全・安心を保証するには，制御システムの安全とセキュリティの 2 つの側面を同時に検討しなければならない．とりわけ，事故を回避する最後の砦となる安全機能部にセキュリティ脆弱性があると，

外部から安全機能を無効化されて大事故が起きる危険性がある．制御システムのリモート監視は慎重に分析および対策されなければならない．ところが，安全やセキュリティに関する用語，概念や要求事項が，機能安全規格と制御セキュリティ規格で異なっており，制御システムに 2 つの規格を同時に適用することは容易でないことが分かってきた．

各国の制御システム専門家が集まってこの問題について議論を行い，2016 年に日本の提案で「IEC TR 63069 機能安全と制御セキュリティのためのフレームワーク」委員会が設立された．現在，本委員会は技術仕様の策定を進めている．また，機械や原子力発電の分野でも，機能安全と制御セキュリティの両立に向けた標準化が進んでいる．

本稿は，現在進行中の制御システムにおける機能安全と制御セキュリティの連携に関する標準化動向について解説する．

安全制御システム

まず，対象となる制御システムの概略を理解しよう．図 -2 は，ロボットの安全制御システム（Safety Control System）を含む工場の制御システムの構成図を示している [3]．

フィールドネットワーク（図中の CC-Link IE）は，上流レベル（エンタープライズ層），コントローラレベル，および安全通信を含むフィールドレベルで使用される多目的ネットワークである．安全制御システム（図中実線囲み部）は生産工程 C の安全機能を担っており，人がロボットに接近するとロボット速度を低速にする「安全速度制限」，およびより接近した場合の「非常停止」を実現している．

人がロボットに接近したことや非常状態は，安全制御システム内の安全スイッチとライトカーテンにより検知する．検知結果は安全リモート I/O ユニットから安全フィールドネットワーク（CC-Link IE）経由で安全 CPU に送られる．安全 CPU の制御プログラムのロジック（アルゴリズム）により，検知した状態から安全確保のためにロボットをどのように制御するかを判断し，ロボットに指示する．ロボットに内蔵された安全制御回路は，安全 CPU から受けた指示にしたがって，ロボットの動力とモーターを「安全速度制限」または「非常停止」となるように制御する．

制御システムのセキュリティ分析の対象は，図 -2 のすべてのコンピュータ，ネットワーク，および機器である．これらは内部／外部ネットワーク，シリアル通信，ワイヤレスおよび USB 経由の脅威を伴う．安全制御システムには，図中のエンタープライズ，コントローラレベ

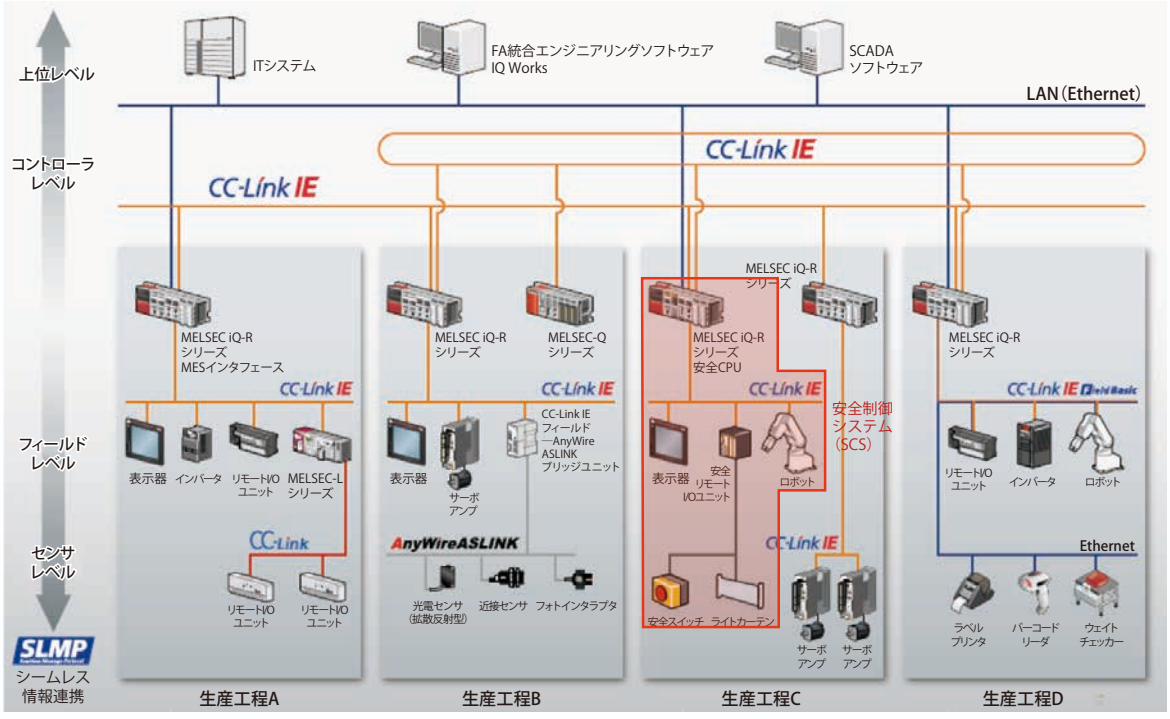

図 -2　安全制御システムを含む工場の制御システムの例（三菱電機）

ルのすべての機器からネットワークを経由してアクセス可能である．もちろん，生産工程 C の安全制御システムの内部は相互にアクセス可能である．

セキュリティリスクの評価は，事故による被害の大きさとその発生確率（脅威と脆弱性）に基づく．被害の大きな事故の発生確率が高いほど，そのセキュリティ脅威のリスクは高くなる．一般に安全制御システムのセキュリティリスクは，一般制御システムよりも高くなる．工場の操業データの漏洩，生産設備の一時停止（チョコ停）は，作業者がロボットや機械に負傷させられることに比べれば，大きな被害ではないからである．安全制御システムのセキュリティ対策が，ほかよりも優先される理由である．

機能安全規格

1999 年に発行された IEC 61508 機能安全規格は，機能安全の考え方と実現方法を規定した初めての規格である．

機能安全とは，制御システムによる安全機能で安全状態を維持する考え方である．たとえば，車がぶつかっても乗員は大丈夫なのがフェールセーフで，障害物を検知して衝突回避するように自動ブレーキがかかるのが機能安全である．機能安全は，状態検知のセンサと判断部と安全状態への移行動作から構成される制御システムで実現されるが，故障やバグに対する対策や信頼性がなければ安全とはいえない．

機能安全規格は，対象システムのリスク分析を行い，必要となる安全機能の性能を 4 レベルの SIL（Safety Integrity Level）で表す．SIL1 は軽微なリスクで，SIL4 は多数の死傷事故がしばしば起こり得るリスクである．そして，ソフトウェア開発プロセス，設計と検証技術，自己診断や安全機能に対する要求事項が SIL ごとに詳細に決められている．設計者は，要求された安全レベルをどう達成するか，達成したことの証明をどうするかが課題となり，また，過剰な「より安全に」を追求する必要はなくなった．

IEC 61508 はハードウェア，ソフトウェアに対する具体的な要求を詳細に決めていたため，この規格を利用して分野規格を作りやすかった．図 -3 に示すように，自動車，鉄道，原子力，プロセス，ロボットなどの分野規格が開発された[4]．さらに，その後の技術革新の反映と，オフラインツールなど周辺技術を取り込んだ第 2 版が 2010 年に発行され，現在第 3 版の改定作業が進められている．

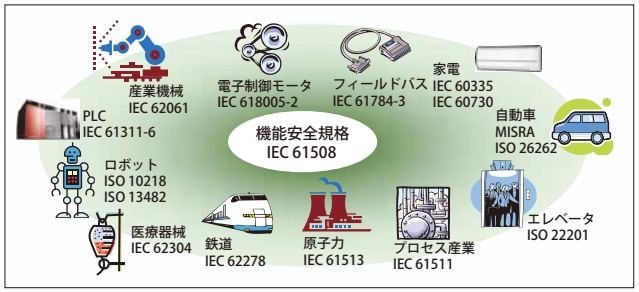

図 -3　いろいろな分野の機能安全規格

制御セキュリティ規格

一方，制御セキュリティ規格の策定には時間を要した．情報セキュリティが機密情報や個人情報の漏洩・流出を高リスクと考えるのに対し，制御セキュリティは作業員の死傷および工場・プラントの操業停止を高リスクと考える．当初，BS 7799（後の ISO 27001）など既存の情報システムセキュリティ規格を適用しようとしたが，以下の制御システムに特有の課題のために難航した．

― 長期間の連続運転
― 簡単に停止／リセットできない
― 多くの独自技術を適用（制御用言語など）
― セキュリティ専門家が現場にいない
― 深刻な社会的影響に及ぶ可能性

これらの課題は，制御システム専門家でなければ解決できない．そこで，米国の国際計測制御学会（ISA：The International Society of Automation）は，2002 年に制御セキュリティの標準を作成する ISA99 委員会を発足した．本稿冒頭で述べたように，当時はまだ各社の独自技術に基づいた制御システムが主流であり，脅威はインターネット経由で市販品の OS やコンピュータが狙われるとしか考えられていなかった．つまり，独自プロトコルの制御ネットワークや独自ソフトウェアの制御装置に脆弱性があるとは考えていなかった．このため，ISA99 が発行されたにもかかわらず，一般に注目されることはなかった．

しかし，2010 年にイランの核燃料濃縮プラントを操

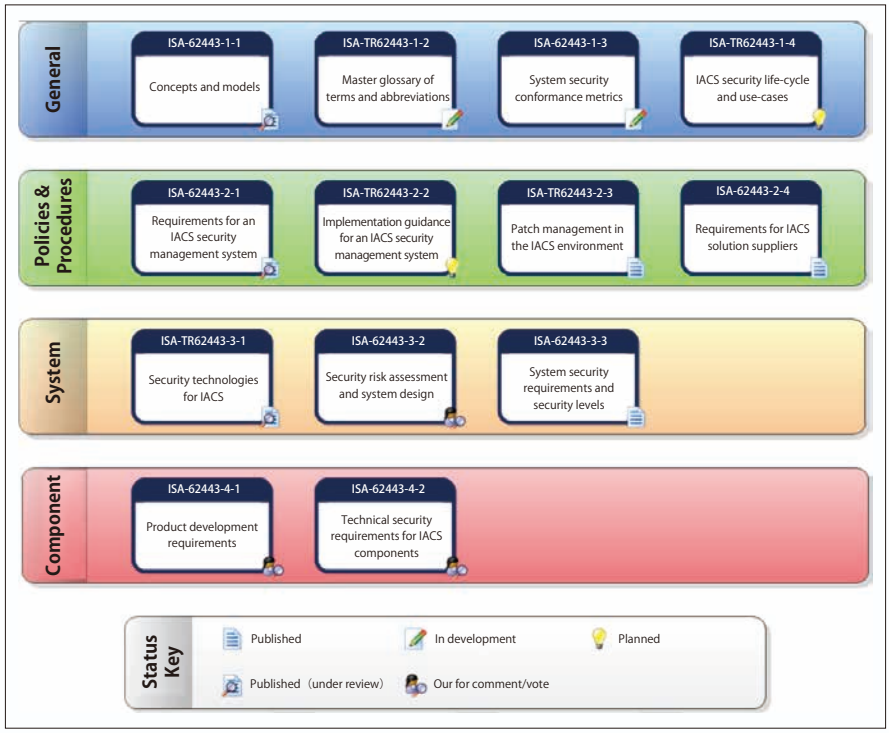

図 -4　IEC 62443 シリーズの構成（ISA99 委員会，©ISA）

機能安全	項目	制御セキュリティ
人	保護対象	データ，プログラム（間接的に人）
機械の危険源 装置の故障・不具合	原因	外部からの攻撃（マルウェア，改ざん，DoS など）
人的死傷	損害	人，操業妨害，企業価値
損害×発生確率	リスク	損害×発生確率
（危険源への）暴露時間，アクセス頻度	発生確率	脅威の程度，脆弱性の量
リスク分析 安全対策	分析・対策	リスク分析 セキュリティ対策
機能安全マネジメント（IEC 61508-1）	管理手法	セキュリティ保証マネジメント（IEC 62443-2-1,4-1）
自己診断 定期点検	検知	侵入検知 マルウェア監視
定期点検 改造・無効化の確認	運用・保全	パッチ管理 侵入・改ざんの確認

表 -1　機能安全と制御セキュリティの比較

業妨害したマルウェア Stuxnet は，独自技術による制御ネットワークや制御機器でも直接攻撃できることを示した．USB メモリから核燃料濃縮プラントに侵入した Stuxnet は，濃縮装置の制御装置のプログラミング端末に感染し，遠心分離装置の回転数を書き換えることで遠心分離装置を破損させた．独自技術の制御装置がセキュリティ攻撃を受けた世界初の事件であった．

Stuxnet 事件を引き金に，各国政府および関連団体は制御システムのセキュリティ対策に乗り出した．2010 年に ISA99 は IEC 62443（正確には ISA/IEC 62443）シリーズとして再編することになった[5]．図 -4 に示すように，IEC 62443 シリーズは 4 部から構成され，第 1 部は用語・概念，第 2 部は事業者（ユーザ），第 3 部はシステムインテグレータ，第 4 部は制御機器提供者向けの内容で，13 編（うち，6 編が発行済み）の規格を含む．

機能安全と制御セキュリティの相違点

機能安全も制御セキュリティも，重大事故・事件を回避または被害を抑制することが目的であり，被害と確率に基づいたリスク分析の結果であるリスクレベルに応じた適切な対策を実施する．設計者は，システムに不具合や脆弱性がなく，信頼性と可用性が十分に低いことを証明しなければならない．場合によっては，第三者に客観的評価（適合性評価）を受ける．したがって，全体的にみると両者間に類似点は多い．

表 -1 に機能安全と制御セキュリティの比較を示す．また，両者間の大きな相違点について，以下で論じる．

機能安全のリスクは，設計時の使い方に関する想定が運用時においてもほぼ一致するので，設計以後リスクが変化することは少ない．したがって，設計時の安全対策が以後も有効である．一方，制御セキュリティのリスクは，新たな脅威や脆弱性の発見によって，使用中も変動する．ユーザがパッチ対策を怠ると，リスクはさらに増大する．Stuxnet への対応がその一例である．すなわち，制御セキュリティのリスク分析は，ユーザが適宜実施しなければならない．また，リスク分析をやり直そうとしても，その時点の脅威と脆弱性による事故・事件の発生確率が分からない．制御セキュリティの普及が進んでいない理由の 1 つである．

運用・保全に関しても，両者間の相違がある．機能安全では，安全制御システムの定期点検による寿命劣化部品の交換と，現場で安全機能を無効化するような改造がないかを確認する．当初と同じ構成と状態を維持するように務める．一方，制御セキュリティでは，新

たに見つかった脆弱性を塞ぐために，制御機器にセキュリティパッチを当てなければならない．では，安全関連部の制御装置にセキュリティパッチを当てたとき，機能安全的には問題ないだろうか．たとえば，暗号強化したセキュリティパッチを当てたところ，CPU の演算負荷が増えて機械の停止時間が長くなるなら，機能安全的には NG である．また，機能安全では長年使い込んだサブシステムやソフトウェアは，「実績による証明（proven-in-use）」で安全とみなすことができる．これにパッチを当てると安全性を証明できなくなる．

表 -1 には記載していない仔細な相違点もいくつかある．ソフトウェア（C 言語）のコーディングルールが機能安全（MISRA-C）と制御セキュリティ（CERT-C）で異なる．試験のカバレッジが，機能安全はすべて（100%）であるが，制御セキュリティは想定できる組合せは膨大なので一部範囲（ファジング）とする，などである．

安全制御システムは，事故を防ぐために，システムの不具合と脆弱性を排除し，故障や脅威・攻撃に対して適切な対策を講じる．そのために，機能安全と制御セキュリティの両方に適合しなければならない．ところが，2 つの規格の要求事項には多くの相違点があるため，安全かつセキュアな制御システムを構築することは容易ではない．

機能安全と制御セキュリティの連携規格

上記の問題の解決に向けて，オートメーション全般の技術標準化を担当する IEC/TC65 委員会は，2016 年に IEC TR 63069 - Framework for functional safety and security（以下，安全・セキュリティ連携規格）を設立した．IEC/TC65 委員会は，これに先立ち 2014 年から機能安全と制御セキュリティの連携技術について調査・検討を進め，新たな標準の必要性を認めていた．そこで，日本が提案国となり安全・セキュリティ連携規格の開発に着手した．

IEC TR 63069 安全・セキュリティ連携規格は，機能安全と制御セキュリティに跨る用語，概念，ライフサイクルなどの共通的な定義を目的とするので，広い分野に影響を与える．IEC 61508 機能安全規格も IEC 62443 制御セキュリティ規格も IEC/TC65 傘下であり，3 つの標準化委員会は連携して規格の作成・改定を進めている．

安全・セキュリティ連携規格が意欲的に取り組んでいる技術課題の 1 つが，安全とセキュリティのリスク分析から安全・セキュリティの要求定義，安全・セキュリティ対策を含むシステム設計に至るフローである．安全チームとセキュリティチームは，それぞれ並行してリスク分析を行い，何を何から守るべきか，そのリスクレベルを求める．このリスク分析結果に基づいて，安全機能仕様，セキュリティ機能仕様をそれぞれ設計する．ただし，安全チームが設計した安全制御システムは，まだセキュリティ分析されていないので，追加の分析を行う．最終的に，安全とセキュリティのシステム仕様を統合し，もし矛盾・競合があれば両者で議論して解決し，実装する（図 -5a）．たとえば，安全 CPU のプログラム書込みのパスワードは，安全でもセキュリティでも用いられる．両者が両立するように，パスワードの管理方法を決めなければならない．

一方，ファクトリーオートメーションの IEC/TC44 は，IEC 63074 Security aspects related to functional safety of safety-related control systems（以下，安全制御のセキュリティ規格）を 2016 年に立ち上げた．主に機械製造者が安全制御システムのセキュリティ分析・対策をどのように進めるかについて要求事項を示している．

こちらは，セキュリティ分析対象を安全制御システムに限定しているので，まず安全チームが安全リスク分析と安全制御システム設計を行う．次にセキュリティチームが，安全制御システムをセキュリティ分析し，セキュリティ対策を追加する．人に危害を与えるのは機械の物理的な危険源だけなので，サイバー攻撃が新たな危険源を生み出すことはない．せいぜい，暴走などの発生確率が増えるくらいであるが，これはセキュリティ対

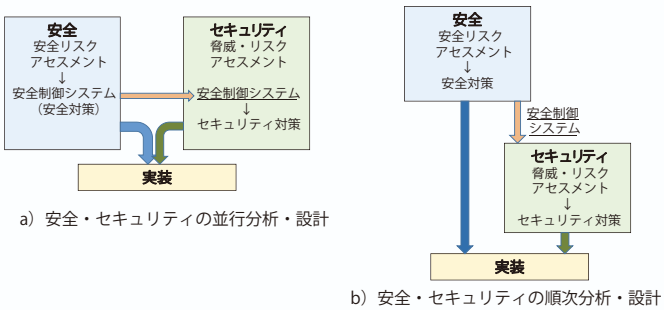

図 -5　制御系の安全とセキュリティの設計フロー

分野	安全規格	安全セキュリティ規格	セキュリティ規格
プロセス	IEC 61508	IEC TR 63069	IEC 62443
機械	ISO 13849 IEC 62061	IEC 63074	IEC 62443
原子力	IEC 61513	IEC 62859	IEC 62645
自動車	ISO 26262	ISO 26262	J-3061
航空	DP-178C	——	DO 326A
鉄道	IEC 62278	——	IEC 62280

表 -2　各分野における安全とセキュリティ規格

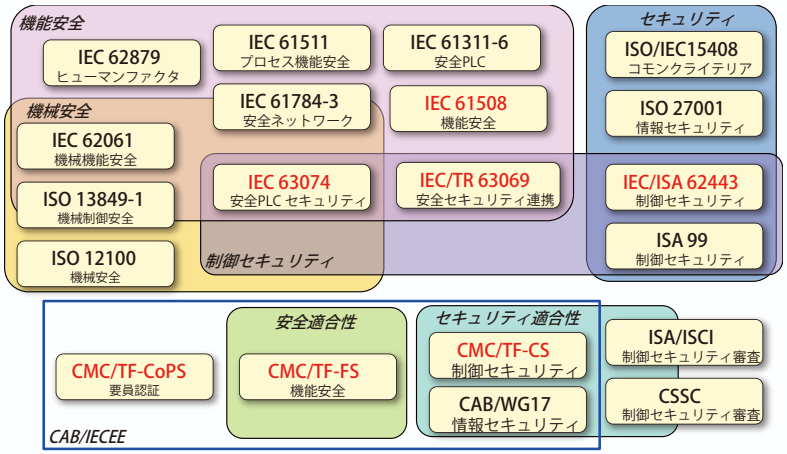

図 -6　安全とセキュリティ規格の関連図

策で抑制できる．すなわち，安全仕様とセキュリティ仕様が競合することはないので，そのまま実現に移行する（図 -5b）．安全制御システム以外の制御システムのセキュリティ分析および対策は含まれていない．

同時期に開発されている類似の規格であっても，対象範囲が異なると，安全とセキュリティを独立並行に分析・設計し両者間で矛盾・競合解消を図る規格と，安全設計とセキュリティ設計を直列に実施する規格がある．今後，2 つの標準化委員会の間で意見交換，議論が活発化するであろう．

安全・セキュアな社会に向けて

機械，オートメーション分野以外でも，原子力発電，自動車分野で機能安全と制御セキュリティを連携するための標準化が検討されている．その状況を表 -2 に示す．いくつかの分野では，ようやく機能安全と制御セキュリティの調査･検討が始まったばかりであり，安全･セキュリティ連携規格の開発状況を注目している．分野固有の課題もあるが，これから規格開発は加速していくだろう．

図 -6 に，機械安全，機能安全，セキュリティ規格の関連性を示す．機能安全とセキュリティの境界に IEC TR 63069，機械安全とセキュリティの境界に IEC 63074 が位置する．下部の CAB/IECEE は，IEC の適合性評価委員会（Conformity Assessment Board）であり，製品／システム／マネジメント等の認証手順を規定している．2016 年末に，機能安全と制御セキュリティのタスクフォース（TF-FS，TF-CS）が設立された．また，安全関連部の開発・運用にかかわる要員認証のタスクフォース（TF-CoPC）も，日本提案により 2017 年に立ち上がった．安全・セキュアな制御システムは，第三者による適合性認証を受けることが商慣習として多いので，CAB の認証手順の標準化の動きも重要である．

安全・セキュアな社会インフラを支える制御システムの標準化動向について解説してきた．安全もセキュリティも重要性は理解されているが，規格が難しいまたは適合に手間がかかるなどの理由から普及しているとは言い難い．しかし，国際標準化が進む中で，日本製品の安全・安心を世界に認めさせるためにも，取り組むべき技術課題である．安全・セキュリティ連携規格は，技術的にも分野的にも幅広い経験と知見が必要なので，1 人でも多くの方に興味を持って参画いただけたら我が国にとって幸いである．

参考文献

1) IEC 61508 series - Functional safety of E/E/PE safety-related systems
2) IEC 62443 series - Industrial communication networks-Network and system security
3) 汎用シーケンサ MELSEC iQ-R 総合カタログ，三菱電機（2016）.
4) 神余浩夫：目で見る機能安全，日本規格協会 (2017).
5) 福田敏博：工場・プラントのサイバー攻撃への対策と課題がよ〜くわかる本，秀和システム (2015).

（2017 年 7 月 24 日受付）

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

1987 年大阪大学大学院原子力工学専攻修士修了，同年三菱電機（株）中央研究所入社．名古屋製作所を経て，2011 年より先端技術総合研究所主席技師長．制御システムの機能安全とセキュリティの開発，標準化，認証などに従事．