委員会活動報告

国際標準化活動報告
IEC/TC65/WG20
安全とセキュリティの架け橋のフレームワーク

IEC/TC65国内委員会

1. はじめに

IEC TC65の担当分野である「工業用プロセス計測制御及びオートメーション(Industrial-process measurement, control and automation)」（以下「産業分野」と呼ぶことにする）の安全については機能安全規格IEC 61508が1999年-2000年にかけて制定され、現在では水平規格として他の分野でも幅広く参照されている。また、「産業分野」のセキュリティについてもIEC62443が2009年に基本規格が制定され、４つの区分別（全般、ポリシー・手順、システム、デバイス・製品）にシリーズ規格化が進み、各国の政策に取り入れられ普及してきている。

これらの規格では、安全、セキュリティそれぞれ単独の目的を達成するための方法論について明確に定められている。安全を実現するための安全関連系のセキュリティを強化することにより安全性を向上させられるように、多くの場合には安全とセキュリティは両立するものである。しかし時には、安全とセキュリティが両立せずに背反する場合も起こりえる。例えば、システムの脆弱性が発見されたときに、セキュリティの見地からは一刻も早くセキュリティパッチという対策を施すことが求められるが、安全の見地からはセキュリティパッチの安全性の検証が求められ、重要な用途ほど検証により多くの時間、工数が必要となる。また、両者が両立する場合であっても両方の技術を有機的に融合させることにより、更に安全なシステムを構築できる可能性もある。こうした時こそ、安全、セキュリティ両方の分野の専門家の協力が必要となるが、両方の分野の専門家の間ではアプローチどころか用語定義も異なるのが現状である。そこで両者の間の橋渡しをして不整合を解決して両立させるための方法論が待たれていた。

以上のような背景のもと、2014年4月に開催されたドイツハンブルクでのTC65総会にて「産業分野における安全とセキュリティに関連する枠組み作り」についてアドホックグループ（ahG）が日本主導で設立されることが決定し、IEC TC65/ahG1として活動を開始した。2015年10月中国 大連にて開催されたTC65の総会においては、ahG1より新たな標準文書開発を行うことが提案され、これを受けて日本から提出された新業務項目提案（NP: New work item Proposal, 65/622/NP）が投票の結果、22ヶ国中21ヶ国の賛成で承認され、出町公二氏（横河電機株式会社）をコンベナー（作業グループ主査）にしてTC65/WG20（Framework to bridge the requirements for safety and security：安全とセキュリティのフレームワーク）がスタートした。

以下本稿では安全とセキュリティのフレームワークに関する国際標準化活動を紹介する。

注１：機能安全とは、コンピュータを用いる操業における予期せぬ故障等による事故を防ぐため多重的な防護策を講じてリスクを許容可能なレベルに低減する考え方

注2：産業分野のセキュリティは情報分野とは異なり安全との協調が求められる。

2. 安全、セキュリティ関連のTC65国際標準化体制とWG20

TC65の下では、図１に示すようにシステム一般を担当分野とするSC65Aの下に機能安全規格IEC 61508のメインテナンスを担当するMT61508-1/2 (Part 1, 2, 4, 5, 6, 7を担当)とMT61508-3 (Part 3, 4, 6, 7を担当、なおPart 4, 6, 7は両方のMT (Maintenance Team)が担当)があり、2010年にはED2を発行している。また、「産業分野」のネットワークとシステムセキュリティを担当するWG10はIEC 62443シリーズを順次発行し、各国で普及してきている。

新たに設置されたWG20で作成しているTR (Technical Report)、IEC TR 63069はそのスコープによれば、「産業分野」へIEC 61508とIEC 62443を共に適用するためのガイダンスを説明、提供することを目的としている。なお、スコープでは、「IEC 61508とIEC 62443を適用できるほかの産業分野にも適用可能である。」

としており、現在は適用分野を「産業分野」と限定しているものの、将来は水平規格にと「小さく生んで大きく育てる」と言うWG20メンバーの願いが込められている。

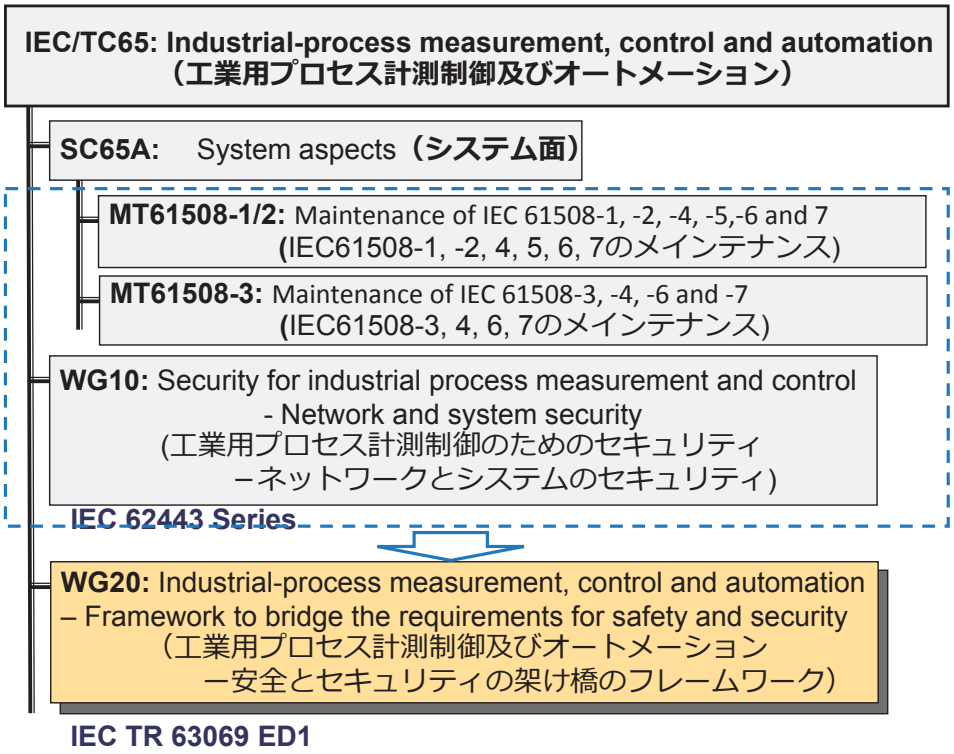

図１．TC65の安全、セキュリティ関連の体制

3. IEC TR 63069 構成と概要

IEC TR 63069（ドラフト）は、シングルパート構成で、イントロダクションに始まり、第1章で先に述べた通りスコープを示し、第2章では参照すべき規格文書としてIEC 61508、IEC 62443全パートを挙げている。

第3章では用語の定義、記号、略号について述べている。特に、IEC 61508, IEC 62443で異なる定義がなされている用語について表に対比しながら纏められている。これらの異なる定義がなされている用語については文中では〈safety〉、〈security〉とブラケットを付してどちらの定義によるものかを区別している。これらの分野間の用語の定義の対比が、今後安全とセキュリティという異なる分野間の共同作業の一助となれば幸いである。

第4章ではセキュリティ上の脆弱性のために安全関連系の動作が阻害されるという、機能安全に関連したセキュリティの背景について説明し、第5章では上位の推奨事項として、ガイディングプリンシプル1（安全性の実装の保護）、ガイディングプリンシプル2（セキュリティの実装の保護）、ガイディングプリンシプル3（両者の実装の両立）を挙げている。さらに、第6章ではライフサイクルに亘る両分野の協働についての推奨事項について述べており、図2（DTRではFigure 4）に安全とセキュリティの協働について概念的に図示し、各ライフサイクル段階での推奨される活動内容について表にまとめられてある。

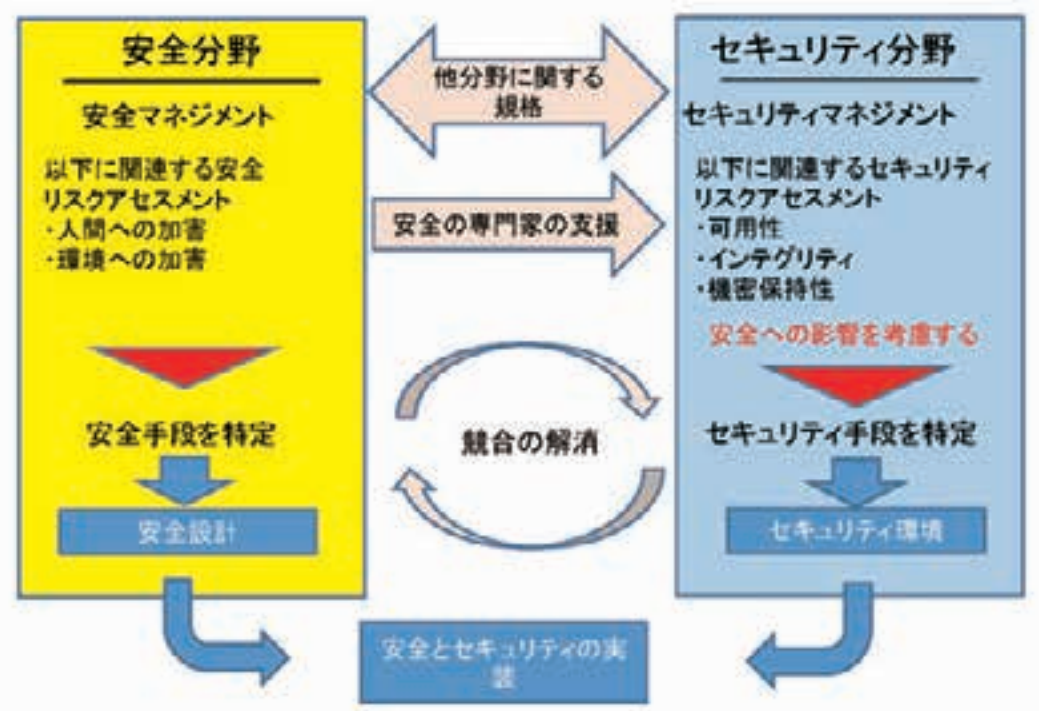

図２　安全とセキュリティの統合化

第7章でリスクアセスメント上考慮すべき点について纏められており、最後の第8章でインシデント対応準備と対応方法について纏められている。

4. 現在までの主要イベント

表１に現在までの国際会議、主要な遠隔会議(Teleconference)、文書発行を含む主要イベントの一覧を示す。なお表中、国際会議の回次と遠隔会議を含めた通算での回次を併記している。

キックオフになる第1回国際会議はフィンランドのヘルシンキで開催された。65/622/NPに対する投票結果の報告に始まり、65/622/NPに対するコメントへのリゾリューション（対応方針）についても話し合われ、スコープ、文書の構成についても話し合われた。

第2回国際会議はドイツのブリューエルで開催され、65/622/NPに対するコメントへのリゾリューションに加えて、WGの方針について話し合われた。

第3回国際会議は（一社）電気計測器工業会の本部である東京の計測会館で開催された。スコープと、文書のタイプについてキックオフ会議以来議論が続けられていたが、以下の3点についてWGとして最終決定された。これらの決定事項は、翌5月に開催されたTC65プレナリ会議に諮られ、承認された。

・スコープを「『産業分野』へIEC 61508とIEC 62443を共に適用するためのガイダンスを説明、提供すること。」とし更に先に述べたように将来は水平規格にというメンバーの願いを込めて、「IEC 61508とIEC 62443を適用できるほかの産業分野にも適用可能である。」とすること
・文書のタイプをTR (Technical Report)とすること
・文書のタイトルをよりシンプルに“Framework for functional safety and security”とすること

第4回国際会議は米国レイクフォーレストで開催され、IEC 61508とIEC 62443を同時に適用するための推奨事項について議論された。先に述べた安全とセキュリティの協働について概念的に示した図（Figure 4）と、ライフサイクル段階での推奨される活動内容を纏めた表（Table 2）について合意された。特にFigure 4は合意に至るまで、安全とセキュリティの協働を密接にすべきという派と、密接にすべきでないという派の間で激論が交わされ、報告者の提案した修正案をベースに何度も書き直された。第4回国際会議での決定事項を受けて、2回の遠隔会議での最終準備を経て、2017年8月6日にCD(65/678/CD)が発行された。

その後、オーストリアのウィーンで開催された第5回国際会議、フランスのグルノーブルで開催された第6

回国際会議、及び通算32回目までの7回に亘る遠隔会議においてCDに対して各国委員会より寄せられたコメントに対するリゾリューションが議論された。コメントに対するリゾリューションの議論に際しては、議論の難易度ごとに分類して、難易度の高い（面と向かった議論が必要な）コメントについては国際会議で、低いコメントについては遠隔会議でリゾリューションについて議論された。以上のプロセスを経て、通算32回目の遠隔会議での最終準備、確認を経て、2018年6月15日にDTR(65/698/DTR)が発行され、8月10日に賛成多数で可決された。

今後は、DTRへのコメントへの対応を含め、TR発行後の次のステップについて議論が行われていく見通しである。

表１：現在までの主要イベント（国際会議、主要な遠隔会議、文書発行）

回	通算回	開催場所	時期	主な内容
1	1	ヘルシンキ、フィンランド	2016/6/7-10	キックオフ、 65/622/NPへのコメント対応方針 スコープ、文書の構成
2	7	ブリューエル、ドイツ	2016/10/11-14	WGの方針 ドラフトCD (WD)へのコメント対応方針
3	13	東京、日本	2017/4/14-17	スコープ、文書の種類 →5月のTC65総会で承認される
4	20	レイクフォーレスト、米国	2017/6/26-29	IEC 61508 とIEC62443 を同時に適用するための推奨事項
	22(Telecon)		*2017/7/27*	*CD最終準備*
			2017/8/4	65/678/CD発行
5	24	ウィーン、オーストリア	2017/10/9 - 12	65/678/CDへのコメント対応方針
6	28	グルノーブル、フランス	2018/2/6 - 9	65/678/CDへのコメント対応方針
	32(Telecon)		*2018/5/18*	*DTR最終準備*
			2018/6/15	65/698/DTR発行
	33(Telecon)		*2018/6/21*	*次のステップについての議論*
			2018/8/10	65/698/DTRが賛成多数で可決される

写真１：第1回国際会議（フィンランド　ヘルシンキ、2016/6/7-10）出席者集合写真
（散歩中の犬（写真中央）の飼い主に撮影をお願いした。）

写真２：第3回国際会議（東京　計測会館、2017/4/14-17）出席者集合写真

5. おわりに

TC65国内委員会の活動として、安全とセキュリティのフレームワークの国際標準化の最新状況を紹介した。冒頭で述べたとおり、「産業分野」への安全、セキュリティの要求は年々高まってきており、それに応えるように技術も進化している。さらに安全、セキュリティの両立のための両分野の専門家の協働の必要性も高まってきている。TC65国内委員会は、本稿で紹介したWG20の国際標準化活動を通して、日本の意見を国際標準に盛り込み、Connected industries政策に貢献すると共に、最新技術動向や規制制度の動向に関する情報提供や新規格の提案などにより、JEMIMA会員企業のビジネスの拡大に貢献していく所存である。

執筆
IEC/TC65/WG20国内委員会 幹事
IEC/TC65/WG20国際エキスパート
金川　信康（株式会社日立製作所）