IoT時代の安全安心に向けて

制御システム セーフティ・セキュリティ検討活動

SEC調査役 石田 茂　SEC研究員 細目 紀子　SEC専門委員 中谷 博司

1 はじめに

プラント、鉄道、電力など社会の重要インフラを担う制御システムは、障害発生時に人命や環境に与える影響の大きさから、ライフサイクル全般にわたる安全性(セーフティ)を重視した"ものづくり"が行われてきた。

一方、2020年に予定されている東京オリンピック／パラリンピック開催に向け日本全体としてのサイバーセキュリティ対策が急がれている今日、重要インフラを手がけるものづくり企業では以下のような課題がある。

- 重要インフラのサイバーセキュリティ対応の重要性は理解しているが、セーフティ、セキュリティ双方に精通した技術者は極めて限られる
- セキュリティ要件を実現した場合、セーフティに及ぼす影響を評価する上での手がかりが欲しい
- セーフティに比べてセキュリティの歴史は新しく、対応が後手になりがち
- セーフティシステムに対するセキュリティ脅威分析の具体的な進め方が分からない

上記の課題は、いずれも容易には解決できない内容だが、IPA/SECでは変化する時代の要請に対応した活動が必要であると考え、課題を共有し、セーフティとセキュリティが連携し双方の要件をすり合わせる枠組みを提示することを目的とした「制御システムセーフティ・セキュリティ検討WG」を設立した(なお、WG名称は昨年度「組込みシステムセーフティ・セキュリティ検討WG」としていたが、検討対象システム及び活動内容を端的に示すため、本年度からは「制御システムセーフティ・セキュリティ検討WG」としている)。

2 活動経緯

2017年度からの本格検討に先立ち、2016年度は、その準備段階として、IEC 61508※1若しくはISO 26262などの国際機能安全または、セキュリティ認証取得(例えばEDSA認証※2、Achilles認証※3)の実務経験を有する企業の方々、学術機関の専門家の方々11名に委員として参加いただき、本検討を円滑に進めるための叩き台となる資料を作成し、2017年度以降の進め方についてディスカッションを行ってきた。

3 活動方針の策定

3.1 活動方針

以下のような方針で進めることとした。

(1) セーフティファースト
セーフティとセキュリティの要件検討は、セーフティゴール(安全性、可用性などの確保)を前提としてセキュリティを考える

(2) グローバルスタンダード(国際規格)準拠
プラント、鉄道、自動車など、重要インフラ、製品における各国及び、国際的な動向を踏まえ、ISO/IEC国際規格及び業界スタンダード(IEC 61508、IEC 62443※4)に基づき、上流プロセスにおける要件のすり合わせ検討を行う

(3) 国際標準化活動との連携
IEC/TC65/WG20※5など国際的な検討活動との連携を意識した活動を推進する

3.2 目標成果物

以下のような内容が反映された「制御システム セーフティ・セキュリティ要件検討のためのガイド(仮称)」を作成することを2017年度の目標に設定した。

- IEC 61508をベースに、セーフティプロセスにセキュリティ要件、運用上の留意事項などを関連付ける
- 上記プロセスを用いて検討を行う際の手順例
- 参考となるような検討フォーマット、サンプル例

4 WG活動の概要

2017年度に進めるWG活動内容について検討した。ここではその中から幾つかのポイントを示す。

4.1 検討対象システム

検討の具体性を確保するために架空のFAシステムを想定した。これは架空の事業者製造工場内に構築された、組み立て生産を行うための架空の設備である。本WGでもよりどころとしているセキュリティ国際規格IEC 62443との関係を含め図1にその全体像について示す。

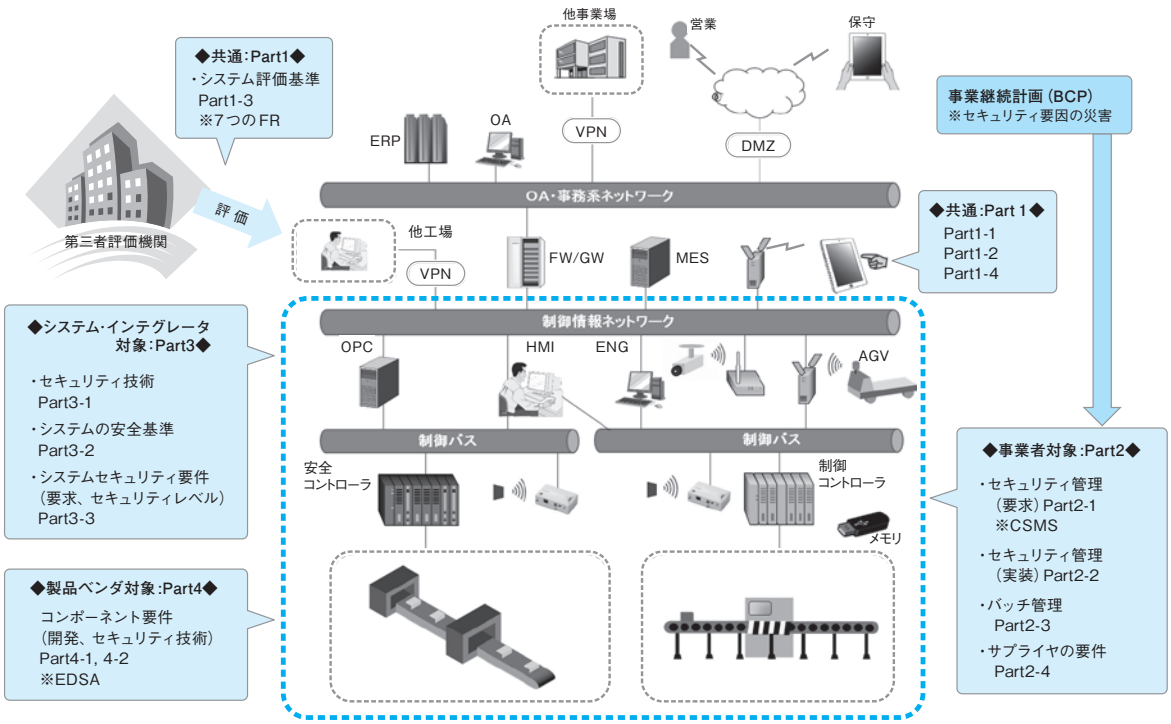

図1　制御システムとIEC 62443の関係

4.2　セーフティな制御コントローラ

前掲の製造工程で使用される制御システムコントローラは、当該製造工程の安全性要求に鑑みてIEC 61508に適合済みと想定している。具体的には、図2に示される安全ライフサイクルに基づく設計、製造、運用が適切になされているとの前提に立っている。

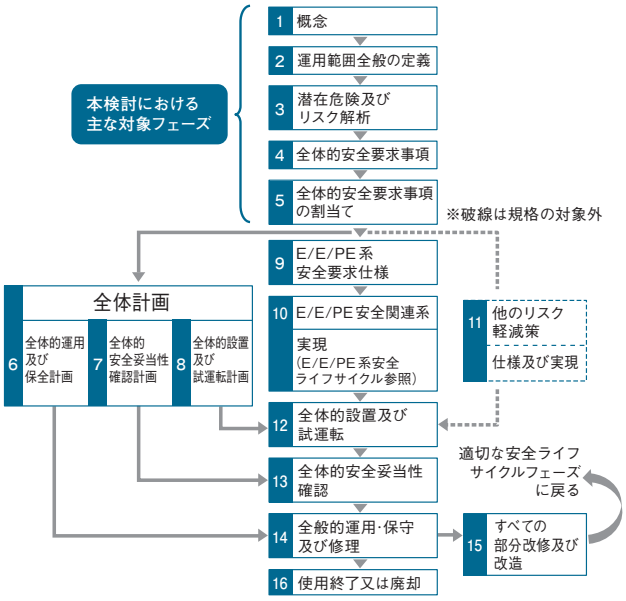

図2　IEC 61508 安全ライフサイクル

4.3　IEC 62443によるセキュリティ要件検討

セキュリティ脅威が識別され、セキュリティ対策が検討・立案された場合に、既存のセーフティ機能、運用に及ぼす影響の抽出と対策の検討が重要となる。

そのため、プラントなどの産業制御用コントロールシステムのためのセキュリティ国際規格で、米国で発行されているNIST SP800-82などでも参照されているIEC 62443に基づくサイバーセキュリティ分析を試行し、セーフティ要件への関連性、影響を検討する。

4.4　国際認証取得経験者の知見を活かす

WGではIEC 61508、EDSA認証などの国際機能安全、セキュリティ対応の実務を経験した方々の知見を得ると共に、開発現場目線を意識したより実践的な活動とすることを目指す。

5　今後の取り組み

制御システムを実際に開発・運用している現場の方々の課題を共有しつつ、同様の課題を抱える多くの企業の問題解決の糸口とできるよう検討を進め、2017年度末に成果物リリースを行う予定である。

脚注

※1 IEC 61508：IEC(国際電気標準会議)が制定した基本安全規格。プロセス産業における電気・電子・プログラマブル電子(E/E/PE)機能安全に関する国際規格。

※2 EDSA認証：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。

※3 Achilles認証：Achilles Certification。ネットワーク接続装置(コントローラ等)の認証。

※4 IEC 62443：制御システムセキュリティの事業者、インテグレータ、装置ベンダを対象とした汎用的な国際標準規格。

※5 IEC/TC 65 Industrial-process measurement, control and automation WG20 Framework to bridge the requirements for safety and security