# 組込みシステム セーフティ・セキュリティ 検討WGの取り組み

SEC調査役　石田 茂

## 1 はじめに

社会の重要インフラを担う組込み製品・システムでは、障害発生時に及ぼす人命並びに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を重視したものづくりが行われてきた。一方、急速に進む事業のグローバル化は国際機能安全規格認証などの新たな対応を要求しており、またネットワークによる相互接続の進展により日々増大し続けるセキュリティ脅威への対処といった新たな取り組みが必要不可欠となってきた。

例えば近年話題となっている自動車の自動運転などに代表されるような新しい機能、サービスの実現に際してはインターネットを介したシステム連携が欠かせないが、同時に車載システムのハッキングなど、セキュリティ上の脅威がセーフティに及ぼすリスクへの対応が危急の命題となっている。

## 2 セーフティとセキュリティの課題

従来のセキュリティ対策は情報システム部門が担い手となり、企業が内部で利用するITインフラへの対応を中心に進められてきたが、個別の組込み製品・システムのものづくりにおいてはどうなのか、開発の現場ではどのようなニーズがあるのか把握する必要があると感じ、2015年度より社会の重要インフラに使用されるセーフティな制御システムの開発製造を行っている国内メーカ並びにこうした事情に明るい大学等の総数20以上の組織よりヒアリングを行いつつ、業界を取巻く技術動向などの調査を行ってきた。この結果、

- セキュリティ対応の必要性は理解しているが、従来セーフティとセキュリティの接点はなく、開発・運用の組織やエンジニア同士のコミュニケーションも図られていない。

- セーフティに比べセキュリティの歴史は新しく、脅威の拡大スピードにその対応が追い付いていない。

などの状況にあることが分かってきた。（詳細は図1を参照）

| | Safety | Security |
|---|---|---|
| 動向・要件 | プロセスなど確立しているが、IoT時代に向けた新たなサービスや機能への対応が必要になっている（自動運転、生産系と事務系システム連携など） | セキュリティ脅威は日々増加、変化しており、将来にわたる脅威の全体像をあらかじめ網羅することは不可能である |
| 規格 | IEC61508を親としたドメインごとの子規格が存在している | 組込みシステムのセキュリティ規格は現在ドメインごとに作成中である |
| プロセス | ドメインごとに確立されたプロセスが定義されている | モデルとなるようなプロセスは現状未定義である |
| 課題（国内企業、大学よりヒアリング） | 事業の国際化を考えるとグローバルスタンダードへの適合が不可欠だが、Safetyの認証取得同様にSecurityでも多大なコスト、工数が必要となると負担は大きい | |
| | Safety, Securityの双方に詳しい技術者はおらず、Security要件がSafetyに及ぼす影響を同時に評価・すり合わせてゆくことが難しく、連携させる枠組みもない | |
| | Security要件の抽出において、脅威分析の具体的なやり方などが規格にも明示されていないため、人による差が大きくなり網羅性が十分であるかどうか判断できない | |
| | Security脅威を定量的に把握、評価することが難しく、また年々新たな脅威が発生するため対応の十分性がはっきりしない | |

図1　セーフティ・セキュリティ状況

## 3 活動の狙いと進め方

これらはいずれも難しい課題でありそのすべてへの対処は容易ではないことを承知しつつ、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、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「組込みシステムセーフティ・セキュリティ検討WG」を設立した。この際、以下のような考え方をベースとした。

**【活動方針】**

- **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）からセキュリティを考える。

- **グローバルスタンダードとの連動**

  プラント、鉄道、自動車など重要インフラの国際市場展開状況に照らし、ISO/IEC国際規格及び業界スタンダードの動向、日本を含む国際的な検討活動との連携性などを念頭に置く。（例. IEC/TC65/WG20※1活動）

- **本格検討に先立つ準備フェーズの設定**

  2017年からの本格検討に向けた準備段階として、2016年度はフレーム（検討のための叩き台）を検討する。

**【進め方】**

- **仮想システム**

  検討にあたってはターゲットシステム（検討のための仮想システム）を想定する。

- **国際規格準拠**

  機能安全はIEC61508※2、セキュリティはIEC62443※3を用い、上流プロセスを検討する。

- **実務者レベルの検討**

  国際機能安全、組込みシステムセキュリティ対応が特に重要となる分野の実務経験メンバーによる現場目線を意識した検討を行う。

## 4 今後の取り組み

前述の通り2016年度は本格検討に先立つ準備フェーズとして、フレームの作成を目標に数回の検討活動を行う予定である。

**脚注**

※1　IEC/TC 65 Industrial-process measurement, control and automationの中で安全とセキュリティのフレームワークをWG20で検討中。
※2　IECが制定した基本安全規格であり、電気・電子・プログラマブル電子にかかわる国際規格。
※3　IECが制定を進めている制御システムにおけるセキュリティに関する国際標準規格。