高信頼車載電子システムの安全性とソフトウェア

株式会社デンソー
電子基盤システム開発部
先行技術開発室 担当課長
東道　徹也

株式会社デンソー
電子基盤技術本部
DP 情報セキュリティ開発室 課長
花木　孝史

株式会社デンソー
技監
村山　浩之

近年、自動車の電子化が進み、その安全性の確保が重要な課題となってきている。本稿ではソフトウェアの観点から車載電子システムの安全性を捉え、不具合をなくす努力に加えて安全構想や設計思想を明確に伝えるアーキテクチャの重要性を解説する。

1 車載電子システムの状況

近年、自動車の電子化が進み、車載電子システムの役割はますます大きくなってきている。省燃費をはじめとする環境負荷の軽減や、交通事故を軽減するための安全技術の進化には、電子制御によるところが大きい。また最近では従来の ITS（Intelligent Transportation System：高度道路交通システム）に加えて、電気自動車やプラグインハイブリッド車の電力系との接続もはじまり、車両とインフラ環境の間で様々な情報がやりとりされるようになってきている。

電子制御を実現する装置は ECU（Electronic Control Unit）と呼ばれる車載コンピュータである。1970 年代初めに米国で施行されたマスキー法と呼ばれる排ガス規制を契機に、エンジン制御で電子化が進み、きめ細かな制御を実現するためにコンピュータが導入された。その後、技術の発展に伴い、多くの機構がメカニカル制御から電子制御に代替されてきた。1990 年代には ECU をつなぐ車載ネットワークが導入された結果、個別の制御だけでなく車載システム全体を協調させる制御が可能となり、従来にはなかった安全性や利便性が実現できるようになってきた（図 1 ）。

2 車載電子システムに求められる信頼性と安全性

車載電子システムに「高信頼」の形容詞が用いられるのは、従来のメカニカルな機構に比べて電子制御やソフトウェアが「見えにくい」状況にあるからと考えられる。とくにソフトウェアを用いることで設計者の意図にしたがった柔軟な動作を実現することが可能となる反面、詳細は ECU というブラックボックスの内部に実現されるため、設計ミスや不具合を ECU の挙動のみから見つけ出すことは難しくなってきている。

パーソナルコンピュータや情報家電として身近な存在になってきたコンピュータであるが、ときおりフリーズするような現象を経験することも少なくない。このような不具合はソフトウェアのバグや考慮漏れによって起きるものと考えられるが、再現条件などが分からない場合も少なくない。仮に走行中の車の「走る」、「曲がる」、「止まる」機能にかかわる電子制御において類似の現象が起これば、生命や人体に危害を加える事故につながりかねない。このため、電子制御やソフトウェアの信頼性や安全性を確保することが重要な課題となってくるわけである。

信頼性と安全性は異なる概念とされる [Mukaidono2010]。信頼性はいかに動作不良がないかを表し、安全性はいかに危害リスクがないかを表す概念である。例えば、エンジンが故障して走行できない車両の信頼性はゼロであるが安全性は高く、ステアリングが故障して曲がれない車両は信頼性が低く安全性も低い。このように信頼性と安全性の間には密接な関連性があるものの必ずしも同一ではない。安全性はシステムが機能している間だけでなく、機能が失われた後も対象となる。そのためシステムの機能中は信頼性と安全性は同じ意味を持つことが多いが、故障などにより機能を失った場合であっても、システムを安全な状態に保てるように安全設計（フェールセーフ設計）を行うことが重要となってくる。

3 品質と「高信頼性」

2011 年に機能安全の国際規格 ISO26262 が制定されるまでは、車載電子システムの信頼性と安全性は品質マネジ

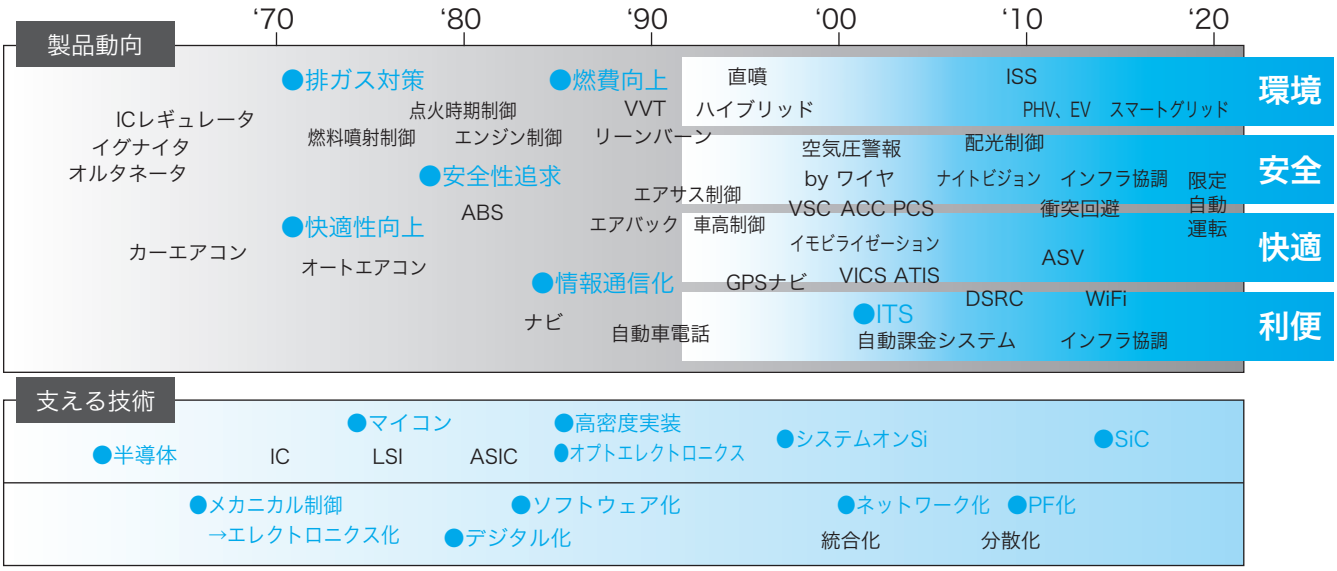

図１　車載電子システムの発展

メント体系（TQM）の中で構築されてきた。品質管理では伝統的にプロセスを重視しており、改善を通じて向上させていくという考え方が根強い。不具合が発生した際には、単なる対策にとどまらず検査方法を改善するなどして再発防止を図り、設計時点で問題そのものを作り込まないよう未然防止を図る。このようなサイクルを回して行くことにより、製品の信頼性や安全性を向上させてきた。現在では、自動車産業界では部品の品質を共通の考え方で管理できるように、ISO/TS16949 として品質マネジメント体系の満たすべき要求事項を定義している。

ソフトウェアの信頼性とは理想的には不具合（バグ）がないことに相当する。しかしながら、不具合が全くないことを保証することは難しい。「高信頼性」が要求されないソフトウェアであれば、バグ収束曲線などの定量的な評価方法を用いて出荷判断することも可能であろうが、安全性が要求される車載電子制御のソフトウェアについては、不具合の存在可能性を残したまま出荷することは考えられない。品質マネジメントの観点からは不具合をゼロにするための最大限の努力を行うことと、不具合が発生してしまった場合には修正を行うだけでなくソフトウェア開発プロセスそのものを改善することで信頼性を向上させることになる。このように車載電子システムの組込みソフトウェアは、不具合抑制の実績と改善を積み重ねることでその信頼性を向上させてきた。品質マネジメントは安全で動作不良のない製品を作り上げる点で最も重要な基盤の一つであるといえよう。

4　機能安全規格

機能安全規格 ISO26262 の制定により、車載電子システムの安全に関する標準的な考え方が確立された [ISO 26262]。機能安全とは危害リスクを許容できるレベルに抑制するという考え方である。これに対して危害を起こす要因を低減するという考え方は本質安全と呼ばれる。

ISO26262 は、車載電子システムを対象に適用される規格である。自動車は様々な危険の可能性を考慮して安全設計がなされるが、ISO26262 が適用されるのはそのうちの電子制御にかかわる部分にのみ適用される。つまり、電子システムが要因となって危険につながるリスクのみが適用の対象となる。

ISO26262 では「モノが壊れること」（偶発的故障）と「人がミスをすること」（系統的故障）の２点を前提に安全対策を行わなければならない。偶発的故障はハードウェアの通常の意味での故障であるため、故障率を許容レベル以下に抑える（信頼性をあげる）か、安全装置や安全機構を追加することで危害の発生確率を抑制するといった設計上の対策を取る必要がある。ISO26262-Part5（ハードウェア開発）の中で安全水準に従った抑制レベルが記載されている。一方で系統故障は設計上の考慮漏れや設計ミスなどに起因するために、開発プロセスの中で必要な対策を行うことになる。

品質マネジメント体系（ISO/TS16949）に基づく車載電子システムの安全性は、安全性の作り込みを行うことを重視してきたが、ISO26262 では安全性を規格に照らし合わせて説明できることが問われている。

5　ソフトウェアの安全性

ISO26262 の立場からは、ソフトウェアの不具合（バグ）は系統的故障に分類されることになる。それでは ISO26262 に従って開発プロセスさえ整備すれば、ソフトウェアに対する安全対策が十分であるかといえば、必ずしもそうでは

ない。ISO26262-Part6 はソフトウェアの安全性分析を行うことを要求している。つまりソフトウェアに対しても安全設計を行うこととその検証を行うことが要求されているのである。

ソフトウェアの安全性を説明することは難しい。小規模なソフトウェアに対してはレビューを十分に行うことでバグの不在を確認できるかも知れないが、近年のようにソフトウェアが大規模化する場合には、レビューのみによる対処方法は十分なものとして納得することは難しいであろう。このような複雑なシステムに対しては、アーキテクチャレベルで安全構想を基本設計に落とし込んでおくことが重要となる。アーキテクチャレベルで安全対策を行うためには、安全要件とその安全対策を明確にすることと、安全機能とそれ以外の非安全機能（主制御など）を明確に分離しておくことなどがポイントである。

ソフトウェア不具合のうちメモリ破壊や暴走につながるものは、その影響の解析が一般には難しいが、保護機構若しくは監視機構などを用いて非安全機構の不具合からの干渉を受けない構成を取ることで、安全機構を分離することができる（図２）。この場合には、干渉に関する安全性解析

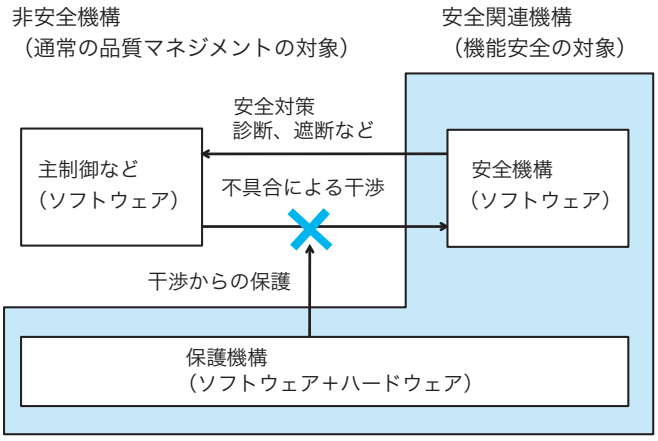

図２　ソフトウェア安全性の設計への織り込み

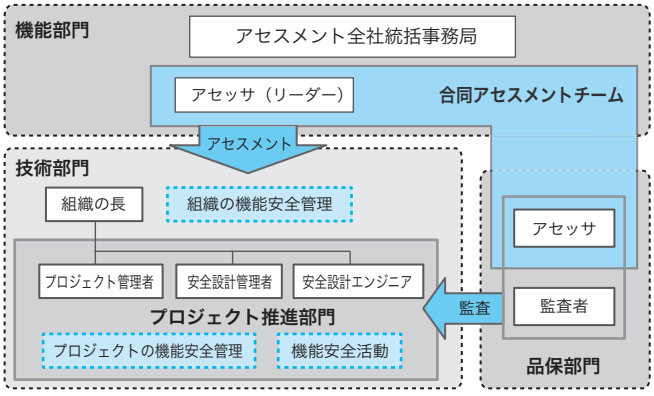

図３　機能安全への組織的対応

を安全機構に対して行うことで、非安全機構も含めた安全性の確認ができる [Jaspar2013]。

このようにソフトウェアであっても、安全構想から基本設計に落とすレベルで対策を考慮しておくことで十分に安全性の説明が可能なのである。

6 安全マネジメント

ISO26262 は安全設計、開発プロセスだけでなく、製品ライフサイクル全体の観点から、組織面やマネジメント面での要件も規定している。そのため機能安全に対応するためには企業活動の広範囲に渡った対応が必要となってくる。弊社の事例で実際に必要となる対応を簡単に紹介する。

デンソーの品質マネジメント体系は初期流動管理と呼ばれる仕組みを中心に構築されている。これは製品の企画段階から、設計、生産の立ち上げまでの節目を定義し、品質管理のための組織や社内ルールを体系化したものである [Fukaya2014]。機能安全への対応のため ISO26262 で規定されている役割や手順を初期流動管理の仕組みの上に追加した（図３）。

この仕組みを実際に運用するために、社内教育や文書テンプレートなどを整備した。その上で製品開発部門がそれぞれの現場において ISO26262 に対応させるため活動を開始した。

7 更なる安心安全に向けて（情報セキュリティ）

自動車は情報系技術を取り込みながら社会とつながる存在に変貌をとげようとしている。車載電子システムがネットワークに常時接続することにより、今後、様々な利便性をサービスとして実現できるようになって行く（図４）。

社会インフラに接続される自動車は、社会の安心という側面からは、情報セキュリティが重要となる。情報システムの脆弱性につけいるサイバー攻撃は、単なる情報資産の

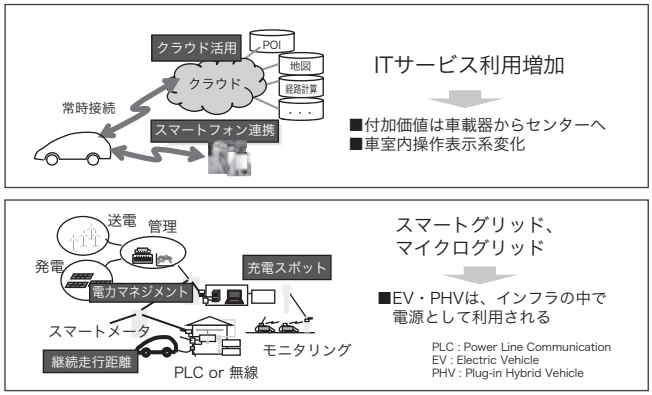

図４　社会とつながる自動車

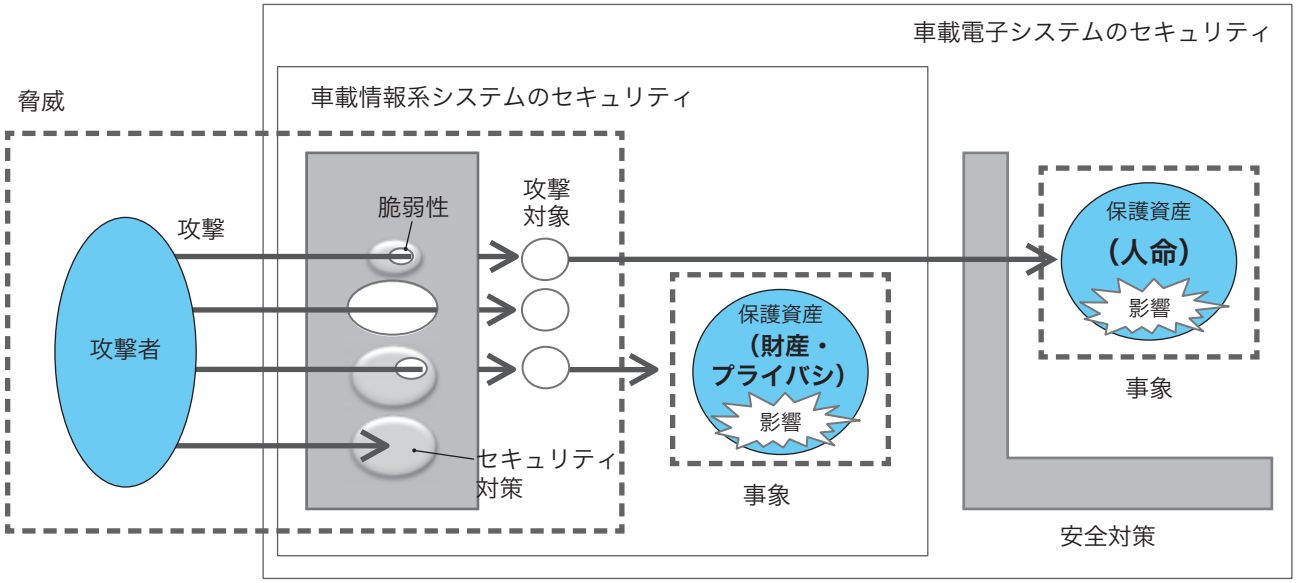

図５　車載電子システムのセキュリティ

流出だけではなく、社会インフラを不全に陥れる可能性も懸念されている。自動車に関しては、外部からネットワークを介して走行中の運転機能を阻害するような攻撃がなされた場合には、人命にかかわる危険性が高く安全の観点からも重要な問題である。

安全性と情報セキュリティはどちらも危害リスクを最小化する考え方ではあるが、相違点も多い。安全性は生命の危険や人体への損傷といった危害を対象にするのに対し、情報セキュリティは盗難、プライバシーなどリスクの対象が加わり、幅広く多岐にわたる。 安全性が故障をはじめとしたリスク要因を特定することが前提となるのに対して、情報セキュリティにおける脅威は外部からの攻撃も想定しなければならず特定そのものが難しい。更に情報システムのセキュリティには ISO/IEC15408 をはじめとする規格や基準が既に整備されてきているため、これからの社会インフラにつながる車載電子システムは情報システムの観点と安全性の観点の双方から対応していく必要がある。

現実的なアプローチは、安全設計を中核として情報セキュリティの基準を取り込んでいくというものであろう。具体的には情報セキュリティの観点から行う脅威分析段階において、財産やプライバシーなどの従来の観点に加えて人命を考慮した分析を行うことと、人命にかかわる危害シナリオが識別できた際には、ISO26262 の観点から安全性の検証を行うことである（図５）。

機能安全の立場から見ると、情報セキュリティ上の脅威は、安全に関連しない機構からの干渉そのものである。ソフトウェアの安全性で例示したように、安全機構の外からの系統的故障からの保護をアーキテクチャレベルで作り込んでおけば、この部分にセキュリティ固有の対策（暗号化など）を必要に応じて追加すれば良く、外部からの攻撃に対して安全性を確保することも容易になる。

8　終わりに

本稿では車載電子システムの分野におけるソフトウェアの安全性の解説を試みた。 ISO26262 がこの分野に与えた最も大きな影響の一つが説明責任であろう。それ以前は品質という枠組みの中で各社の実力が安全をささえてきており、その源泉がプロセスを重視した改善にあった。しかし、今や安全は社会の受容という基準に変わり、安全構想や設計思想を明確に伝えるアーキテクチャがプロセスと同様に重要となってきている。車載や安全に限らず、今後ますます複雑化する電子システムを構築・運用して行く上で、いかに良いアーキテクチャを構築するかが問われている。この観点から、ソフトウェア工学にはまだ開拓すべき分野があるのではないかと筆者らは考える。今後は、ソフトウェアだけを対象にするのではなく、安全工学や制御工学など関連する分野を含めた知見を体系化していくことが重要であろう。

【参考文献】

[Mukaidono2010] 向殿政男：コンピュータ安全と機能安全 , Fundamentals Review Vol.4 No.2, 電子情報通信学会 , 2010（12 月 1 日）

[ISO26262] ISO/TC22/SC3：ISO 26262:2011 Road vehicles - Functional Safety, ISO, 2011

[Jaspar2013] 一般社団法人 JASPAR：機能安全対応のための解説書【ソフトウェアパーティショニング編】Ver1.0, 一般社団法人 JASPAR, 2011（2 月 28 日）

[Fukaya2014] 深谷紘一：会社を育て人を育てる品質経営―先進、信頼、総智・総力 , 日本規格協会 , 2014

[Meti2011] 経済産業省：サイバーセキュリティと経済 研究会 報告書 中間とりまとめ , 経済産業省 , 2011（8 月 5 日）