今日の焦点

システム安全性検証のすすめ

デジタル化が進展することによって、システムの安全性にソフトウェアが寄与するだけでなく、ソフトウェアの障害がシステムの安全性に対する欠陥原因となって、大きな影響を及ぼすようになってきた。たとえば、最近注目されている自動車の自動運転技術では、事故を起こさないように障害物を自動的に検知して安全に停車するためのソフトウェアが必要である。このようなソフトウェアに欠陥があれば、障害物の検知ができず、安全に停止できないことになる。また、悪意を持つ個人が自動車や道路信号システムのソフトウェアに侵入して遠隔操作するような事態を回避する必要がある。

最近の自動車に搭載されるコンピュータである電子制御ユニット（ECU）は50個以上になり、ソフトウェア開発規模は1000万行に達している。このため、自動車の機能安全規格であるISO26262では、自動車のソフトウェア開発の安全性を保証するために、安全性ケースと呼ばれるドキュメントを、製品だけでなく、開発プロセスについても、整備することが求められている。

米国で発生した自動車のアクセル制御ソフトウェアの妥当性が問われた事件では、事件発生後に第三者機関による独立な妥当性確認によって、ソフトウェアには欠陥がないと判断されたにもかかわらず、自動車会社が900億円以上の和解金を支払う事態となった。安全性ケースをソフトウェアの開発段階で適切に作成して、ソフトウェアの安全性を事前に検証した証拠としての安全性ケースを提示して説明責任を果たしていれば、このような事後対応にはならなかったと思われる。

医療機器分野でも、IEC 62304規格（医療機器ソフトウェア- ソフトウェアライフサイクルプロセス）に適合するため、第三者認証機関によるソフトウェアライフサイクル監査を実施することが米国では義務付けられている。

三菱航空機（MITAC）が開発している国産の最新鋭ジェット旅客機であるMRJでは、ほぼすべてのサブシステムにソフトウェアが組込まれている。これらのソフトウェアでは、飛行安全に影響を与えることから、高い安全性要求が求められている。したがって、航空機分野のソフトウェア開発ライフサイクル規格であるDO178Bに従って、MRJのソフトウェアが開発されていることを審査当局に説明する責任がMITACにはある。このためMITACでは、世界中のパートナー企業との間でTraceability、Validation& Verficationによって、要求に抜けもれがなく正しい内容であることを証明するとともに、要求追跡の妥当性を確認している。

国立大学法人　名古屋大学
情報連携統括本部　情報戦略室
教授　工学博士
山本 修一郎氏

通信分野では、携帯電話会社などが通信障害を起こしたときに、原因究明や再発防止策の提案などを担う第三者機関について、2014年の通常国会に向けた検討を総務省が進めている。この理由は、スマートフォンの普及に伴うデータ量の増大と高機能アプリケーションの登場によって通信障害の影響が増大する傾向にあるだけでなく、通信障害の原因も複雑になってきたことにある。たとえば、2013年4月の携帯メールの不具合では影響が約300万人にも及んだ。この第三者機関では、専門的な観点から障害を起こした通信会社の設備保全体制を点検することにより、原因究明と再発防止策の妥当性を検証するようである。

上述した米国の事例にみるように、障害後に原因究明と再発防止策を第三者機関によって実施するだけでなく、通信会社が事前に通信サービスの安全性を検証して適切な証拠を用意することができていれば、障害の未然防止につながるだけでなく、障害原因究明の迅速化が期待できる。

最近の通信機器やアプリケーションは、グローバル化、多様化しており、国内の通信会社だけですべての責任を負うには酷な面もある。この点で、MRJの事例が参考になる。たとえば、通信会社が通信サービスの安全性のために必要となる通信機器の安全性要求を定義する。パートナー企業では、提示された安全性要求を通信機器が満足することを証明するドキュメントを開発段階で作成する。これらを用いて、パートナー企業の通信機器が安全性要求を満たすことを通信会社が監査できるようになる。このようなシステムの安全性を社会的に説明するためには、オープンな安全性標準が前提になる。この理由は、企業固有の安全性の取組みでは、オープン標準よりもなぜその取組みがより安全であるかを改めて説明する必要があるからであり、さらにそれを立証するために第三者による監査が求められるからである。

社会基盤的システムが安全であることを客観的に示すために、パートナー企業も含めた一貫性のあるシステム安全性の検証能力をより一層高めていく必要がある。