2010 年 10 月 12 日

大規模システム化した自動車の安全性向上策
～プリウス・ブレーキのリコール問題考察からの提言～

情報システム学会企画委員会
「社会への提言」検討チーム

2010 年（平成 22 年）2 月 9 日に、トヨタ自動車株式会社（以下では、単に「トヨタ」と記す）は 3 代目のプリウスを含む 4 つの車種のリコールを国土交通省に届け出た。その日の午後に東京都内で行われた記者会見でトヨタの副社長（品質担当）の佐々木眞一氏は、このリコールの原因は「ABS（Antilock Brake System）の制御のコンピュータに入っているプログラムの不具合である」と述べた。

しかしこのプログラムには、「プログラムの不具合」という言葉から容易に想像されるような、普通の意味でのプログラムの「バグ」は無かった。このプログラムは、当初の仕様通りに的確に機能していた。それにも関わらず、そのプログラムを搭載したコンピュータでブレーキを制御していた自動車が、リコールの対象になった。

以下で、そのリコールの原因を明らかにし、このようなことが起きた問題の構造を解明し、その上でこれからトヨタを初めとする自動車業界と所管官庁および学界等の関係者が、どのような考え方で大規模システム化した自動車の安全性向上を図っていくべきかについて、我々の意見を述べたい。

今回のリコールの原因

3 代目のプリウスのリコールの原因は、雪道などの滑りやすい道路を低速で走っていて、その状態でブレーキをかけると一瞬「ブレーキが抜ける」ような状態になり、ドライバがヒヤッとする、ということが多発したことにあった。

プリウスのブレーキの構造は、プリウスがハイブリッド車であることから、かなり複雑である。プリウスのブレーキには、これまでの「油圧ブレーキ」に加えて、自動車を止めたり、自動車の速度を落とす時に自動車が持っている運動エネルギーを回収して電気に変える「回生ブレーキ」があり、その上で凍結した道路などでも的確に自動車を止めるための ABS が付いている。

ハイブリッド車の特徴の 1 つは、この「回生ブレーキ」が付いていることである。その「回生ブレーキ」だけでドライバが必要とする制動力が得られない場合、従来の油圧ブレーキをこの回生ブレーキと併用する。このような仕組みを、「回生協調ブレーキ」と呼ぶ。この回生協調ブレーキの働きを、図 1 に示す。

この回生ブレーキと ABS の相性が、実は良くない。例えばブレーキをかける時、回生ブレーキは左右両輪に同じようにブレーキをかけようとする。しかし ABS は、滑っている車輪を見つけるとその車輪だけブレーキを外そうとする。このように、ある場合には双方の対応方法が異なってしまう。したがってプリウスでは ABS の機能が必要になると、回生協調ブレーキの回生ブレーキの機能を止める方式を採用している。

しかし、単純に回生ブレーキを止めてしまうと制動力が不足する。そのため 2 代目までのプリウスは、ここで電動の油圧ポンプを稼働させて油圧ブレーキの制動力を強化し、全体の制動力不足を補う方法を採っていた。この電動ポンプが稼働する時に、独特の「音」が発生する。静寂性を含めた自動車の室内の快適さを重視しているトヨタは、この「音」の発生を嫌った。

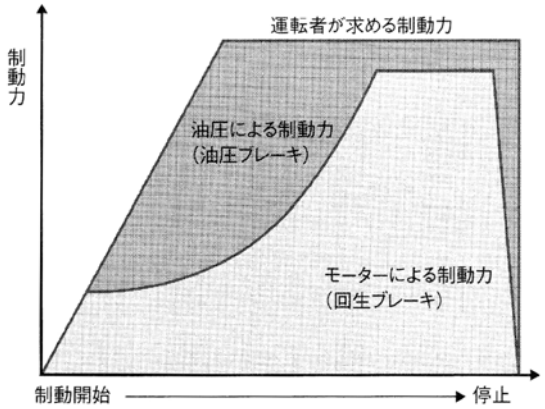

図 1　回生協調ブレーキの働き（[NIK10]より）

このため 3 代目のプリウスはこの電動ポンプを稼働させる方式を止めて、ドライバが踏んでいるペダルからの力をそのまま制動力の一部として使う方式に切り替えた。この動力源が切り替わる時に、低速時などブレーキペダルを軽く踏んでいるケースでブレーキの油圧が下がってしまい、そのため制動力が減って、ドライバに空走感を感じさせることになった。その上その減速度は元の大きさには戻らずにそのまま継続し、制動距離を伸ばすことにもなった[NIK10]。

これが、今回のリコールの原因である。トヨタはこのリコールの対策として、3 代目のプリウスのプログラムを 2 代目で使用していたものに変えた。プログラムを変えるだけで 3 代目のプリウスのブレーキのシステムは、2 代目までのプリウスのものと全く同じように機能できるように、メカニカルな部分は用意されていた。

余談になるが、この度のプリウスのリコールに関するトヨタの対応について、ここで 1 つコメントをしておきたい。リコールとは、「自動車が道路運送車両の保安基準に適合しなくなるおそれ」がある場合に適用するものである[HON]。当初トヨタは、「プリウスのブレーキはこの保安基準に合致している」として、リコールとはしなかった。しかしその後、「保安基準には堅牢要件（自動車の安全な運行を確保するための要件）というものもあって、その立場を考慮してリコールとして届け出た」という趣旨のことを、佐々木副社長は述べている。

具体的には、豊田社長が「お客様第一で考えろ」と指示をされ、それを受けて「この時までに 3 代目のプリウスを購入した 20 万人の人が、この後 10 年間このままの状態でずっと安心して乗り続けて貰えるのか」を考えてリコールに踏み切った、とのことである[NIK10]。このリコールの届け出を行った頃、対応が遅いとして、トヨタのマスコミ評判は悪かった。しかしここで会社としての考え方を変えてリコールとして届け出たことは、

もっと評価されてよいと我々は考える。我々はこのトヨタの対応を、問題の発生とは別に、高く評価したい。

「回帰テストのセンス」の必要性

トヨタは3代目のプリウスを開発するに当たって、ABS制御用のプログラムについては、2代目のプリウスで使っていたプログラムの一部に手を入れることによって対応した。

この新しく書き直した部分について、トヨタは必要と考えたテストを実施している。つまりこの新しいプログラムを使って、高速から適切に停止できることについての確認を充分に行っている。2月9日の記者会見で、佐々木副社長は次のような趣旨のことを述べている[NIK10]。

「ブレーキという性質上、技術者がシステムを構築する時に一番留意するのは本当に止まれるのかということである。つまり、最大減速度はどのへんまで出せるのか、それをコントロールできるのか、といったことが一番気になるところである。そういう試験は、充分にやった。しかし低速で、低減速度というところについての注目は、しっかりとはできていなかった。」

情報システムでは、回帰テストという種類のテストを実施することがある。この回帰テストは、情報システムの新規開発でのシステム・テスト以降の局面や、本番作業が開始された後の保守の局面で実施されるものである。例えば保守の場合、既に稼働しているソフトウェアに、何らかの理由で手を加える。仮に、新しい機能を追加することになったとしよう。その新しい機能を追加する際に、既存の機能を損なってしまうことがある。そのため、新しく追加した機能が当初想定したとおりに正しく稼働することを確認することは当然として、既存の、今回変更の対象にはしていなかった機能が損なわれていないことも、併せて確認しなければならない。この後者の目的で行うテストが、回帰テストである。新しく追加した部分のテストは、回帰テストとは呼ばない。

今回のプリウスのケースでは、新しく手を入れた部分にテスト不充分なところがあったわけで、これは回帰テストの領域ではない。しかし回帰テストを行う時の「これまで持っており、今後も必要である機能が今回の変更で損なわれていないか」を確認するというスタンスが、今回のテストでは不充分だった。このスタンスを、「回帰テストのセンス」と呼んでおこう。

組み込みシステムで今どの程度回帰テストが行われているのかについて、我々は残念ながら情報を持っていない。しかしソフトウェアの開発では先輩格に当たるビジネス・アプリケーションで、その中で最重要とされる「重要インフラ情報システム」でも、回帰テストの実施率が余り高く無いという調査結果が出ている[JUA10]。安全性を重視する組み込みシステムでは、回帰テストの実施率は充分に高いものが要求されると我々は考える。

このソフトウェアを変更した時の回帰テストの実施、あるいは「回帰テストのセンス」を持ったテストの実施を、ここでの最初の提言としたい。

プリウスは自動車の機能を持った情報システム

以前の自動車は、全てメカニカルに作られていた。つまりアクセルペダルは燃料を気化させるキャブレターと直接つながっており、ドライバがアクセルペダルを踏むと、その力でそのままスロットルバルブ（エンジンのシリンダーに入る空気量を調整する弁）が開いて、エンジンの出力を変える仕組みになっていた。ブレーキも同様で、ドライバがブレーキペダルを踏む力が、油圧ブレーキを介してそのまま制動力になっていた。

しかしプリウスを始めとする今の一部の自動車は、まるで様変わりしている。例えばアクセルは既に一種のスイッチになっており、ドライバがアクセルペダルを踏む時の踏み方や踏み込んだ量をセンサーが検出して、この部分を制御するコンピュータにそのデータを入力し、そのコンピュータの出力がモータの回転やスロットルバルブを調整する形に変わっている。ブレーキも、全く同様の仕組みになっている。

つまりドライバとのインタフェースの部分は、これまでの自動車と全く変わってはいない。しかし自動車に関わる基本的な「走る」、「止まる」、「曲がる」といった機能は既に、完全にコンピュータで制御されるようになっている。単に基本的な機能だけでなく、室内の空調やオーディオ、カーナビ、ドアのロックなどの補助的な機能まで、今や全てコンピュータ・コントロールに変わった。

このため 3 代目のプリウスには多くのマイクロコンピュータが搭載されていて、コストに占める電子部品の金額は、全体の 50%を超えたと推察されている。3 代目のプリウスに、いくつのコンピュータが搭載されているかという情報はない。しかしクラウンでは既に 50～100 個のマイクロコンピュータが搭載されているとのことであるから、3 代目のプリウスにはこれと同等か、場合によるとこれ以上のコンピュータが搭載されていると推察される。そしてそれらのコンピュータを稼働させるためのソフトウェアの量が、既に 1,000 万ステートメントを超えたという。1,000 万ステートメントのソフトウェアというのは、1990 年頃に第三次オンラインシステムの開発を終えた時の、日本の都市銀行各社がそれぞれ持っていたソフトウェアの量に匹敵する。

これまで組み込みシステムでは、それぞれのコンピュータは、エンジンはエンジンだけ、ブレーキはブレーキだけ、というように、個々の機能の制御だけを行っていた。これが、組み込みシステムの 1 つの特徴だった。

自動車以外の家電製品で、既に徹底的にコンピュータで制御されているものが多くある。全自動の炊飯器や洗濯機などがそうである。これらは既に制御のレベルがたいへん高くなっており、今やコンピュータで制御された機器というより、それぞれの機能を持った情報システムと考えた方がよい。

自動車でも、例えばブレーキの制御機能では、ペダルの踏み込み方や踏み込んだ量を検出して、制動力を回生ブレーキと油圧ブレーキでどのように受け持つべきか計算して配分したり、さらにスリップを検出したら回生ブレーキを切り離して油圧を高め、必要に応じてこの油圧を高めたり低めたりするなど、複雑な仕組みができている。これだけですでに、情報システムを形成していると見てよい。

ここで「情報システム」とは、当学会が提唱する情報システムであって[ISS09]、単純なソフトウェアによる一部の機能のコンピュータ・コントロールの域を超え、人間の意思をインタフェースを通して情報として受け取り、その情報に基づいた高度な、あるいは複雑な、場合によれば複合した機能の制御をつかさどる、人間系を含めたシステムを意味している。

さらに今の自動車では、ネットワークを通して複数のコンピュータが相互に情報をやりとりして、複数の機能を制御することが既に始まっている [NIK10]。例えば、今年(2010 年／平成 22 年)初めの一連のリコールへの対応の中で、トヨタが採用を決めた「ブレーキオーバーライド機能（アクセルとブレーキが両方同時に踏まれている状態では、ブレーキを優先させる機能）」は、この相互に連携を取り、複数の機能を制御することによって、初めて実現が可能に

なるものである。このようなソフトウェアの使い方は、企業がビジネスで使用している情報システムの形に近いということができる。つまり組み込みシステムも、一部のものは既に情報システムになったと言える。

このように考えると、プリウスは既に自動車という、一群の専用の機能を持った「情報システム」であると捉えるべきである。仮にプリウスを「情報システム」と考えても、「走る」、「止まる」、「曲がる」という、自動車が持っている基本的な機能は引き続き重要である。したがってこの部分の技術は、自動車がメカニカルな製品だった頃からの技術を継承し、発展させることが肝要である。

一方プリウスを 1 つの情報システムであると考えると、そのコンピュータを稼働させるためのソフトウェアを通して、いかにその情報システムとしての機能を発展／拡大させ、品質を維持し、向上させるか、生産性の向上を通して価格を低下させるか、個々の機能をうまく連携させて全体としての効果を出すか、という新しい方向へのテーマが見えてくる。

例えば今多くの自動車に、既に EDR（Event Data Recorder）という機器が搭載されている。これは飛行機のフライトレコーダと同じように自動車のドライブに関する情報を記録するもので、「ドライブレコーダ」とも呼ばれる。今回の一連のリコールへの対応のなかでトヨタは、今後このデータを活用してゆくことを決めた。

この EDR には、各ドライバの自動車の操作についての特徴や癖など、「個性」とも言えるデータも書き込まれる。東京農工大学の永井正夫教授は自動車の情報システムに柔軟性を持たせて、このデータを活用して各人の「個性」に合うように自動車の動きなどを変えることによって、自動車の安全性と快適さを一層向上させることができると述べている[NIK10]。これは、自動車の情報システムとしての側面の将来方向についての、重要な示唆である。我々は、こうした自動車単体としての情報システムが、近い将来人間活動とネットワークを通じて結合されて、情報システムの範囲を更に拡げると予測する。

先般のトヨタの記者会見の記録を読むと、トヨタの社長と副社長のスタンスには、プリウスが「自動車」であり、その機能をいかに維持し、発展・拡大させるかということについての強烈な意識を感じることができる。しかし残念なことに、プリウスは既に「情報システム」であり、その情報システムとしていかにそれを発展させ、拡大して、使用者の安全性と利便性を向上させるか、という立場からの意識は、必ずしも充分ではないと我々は考える。

さらにトヨタは 2010 年（平成 22 年）7 月 12 日に、トヨタが日科技連（財団法人日本科学技術連盟）に委託して評価してもらったトヨタの品質保証体制の評価報告書をウェブで公開した[JUS10] 。16 ページに及ぶ報告書であるが、この評価報告書にもやはり「プリウスが情報システムである」というスタンスはない。

従来の「メカニカルに作られた自動車」と現在の「情報システムに置き換えられた自動車」では、品質や安全性などについて、初期不良、劣化、耐用年数などといった面で、根本的な違いがあると思われる。そして実際に設計などの現場で仕事をしている技術者は、既にこの「プリウスは情報システム」というスタンスを持って仕事に取り組んでいると推察する。しかし社長、副社長という上層部から販売店でプリウスを売っている営業担当者に至るまで、まだこの認識は充分ではないように思われる。したがってまずトヨタの社内で、この意識変革を成し遂げて頂きたい。その上で、トヨタが変わることを通して、業界全体や監督官庁まで変えて頂くことを期待する。これが我々の、2 つ目の提言である。

信頼性と安全性

システムの信頼性は、次のように定義される[LEV95]。

信頼性：ある品目が、与えられた期間と指定された、または想定された条件の下で、指定された方法で、それに求められた機能を実行する確率によって表される特性

この信頼性とは別に、安全性という概念がある。その安全性の定義は、以下の通りである[LEV95]。

安全性：事故や故障がないこと

つまり、信頼性と安全性は異なる。信頼性が高くても安全でないことがあり、逆に信頼性がそれほど高くなくても安全な場合がある。そして利用者の立場で、自動車で重要なのは安全性の方である。信頼性は、それによって安全性を高めることができる場合に意味がある。この信頼性と安全性の関係を、図 2 に示す。

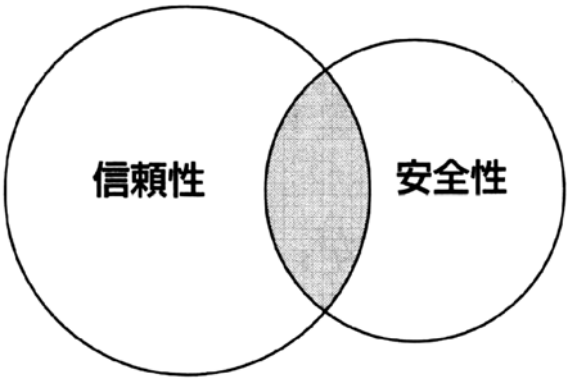

図 2　信頼性と安全性（[LEV95]より）

ソフトウェアの世界についていえば、これまで「信頼性をいかに向上させるか」が主要なテーマになっていた。例えば経済産業省は、2006 年（平成 18 年）6 月 18 日に「情報システムの信頼性向上に関するガイドライン」を発表し、さらにその 3 年後の 2009 年（平成 21 年）3 月 24 日にそれを第 2 版にバージョンアップして、情報システムの信頼性を向上させることの必要性を強調し、その実現のための具体的な考え方と方法を提示した[MET09]。しかし安全性については、やっと最近ビジネス・アプリケーションについて日本情報システム・ユーザー協会で議論が始まったばかりであり[JUA09]、国内にはまだこのようなガイドラインや指針はない。

この安全性に関するガイドラインを作っている団体に、世界にはすでに MISRA（The Motor Industry Software Reliability Association）という、英国をベースにした団体がある。MISRA は信頼性を向上させる立場から、自動車で使用するソフトウェアと電子機器の製造についてのガイドラインを作って、発表している[WIKa]。

その MISRA の具体的な成果の 1 つが、MISRA-C と呼ばれるものである。これは、元は自動車業界のための C 言語のソフトウェア開発標準規格で、ISO 規格に基づく C 言語で記述された組み込みシステムで、安全性と移植性と信頼性を確保することを目的としたものだった。これが今や、他業界にも広く普及して適用されている。さらにこの MISRA-C の後継の MISRA-C : 2004 は「Guidelines for the use of the C language in critical systems (クリティカル・システムで C 言語を利用するためのガイドライン) 」と呼ばれ、クリティカルなシステムにまで適用範囲を広げて、安全性の確保に一段の配慮をしている [WIKb]。

この MISRA に、「自動車分野の機能安全規格に対処する実務ガイドライン（The Motor Industry Software Reliability Association – Safety Analysis : MISRA-SA）」という、今議論しているプリウスの情報システム開発に直接結びつくガイドラインがある。そして今、このガイドラインを基にして ISO で国際規格化の作業が進んでおり、ごく近い将来 ISO 26262 として発行される予定になっている[FUT07]。

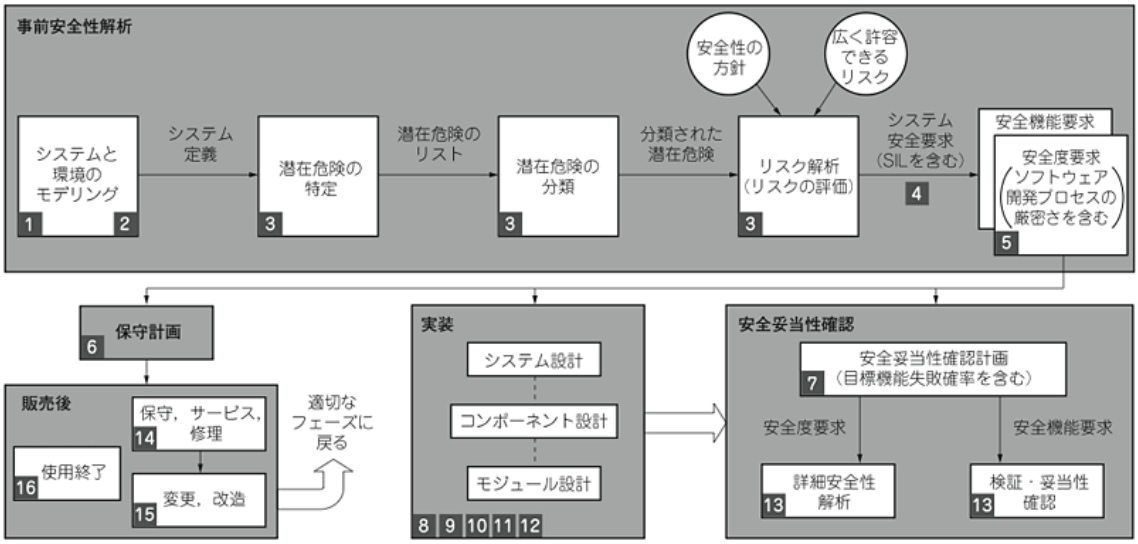

図 3　MISRA-SA のライフ・サイクル（ドラフト版）（[FUT07]より）

この MISRA-SA は、会社としての方針を取り込んだ安全性の解析から始まり、その解析の結果を基にした安全性に関わる機能の要求、その要求を実現するための製品の設計、設計された製品の安全面での妥当性の確認から、製造された製品の保守計画までを、広くカバーしている[FUT07]。つまり MISRA-SA は、MISRA-C のような極めて限られた範囲での規格とは異なり、安全性を実現するために製品のライフ・サイクル全てをカバーしているものである。そのためこれを企業の中で適切に適用するためには、単に現場の技術者だけがカバーすればよいというものではなく、トップを含めて全社で対応する必要がある。

この ISO 規格（ISO 26262）が発行された場合、その ISO 規格を速やかに JIS 化するなどして、経済産業省は日本国内で「安全性」に関わる議論を高めて頂きたい。そして日本の自動車産業の各社は、安全性に関して全社で対応する形を作って頂きたい。これが、我々の 3 つ目の提言の前半部分である。

トヨタはMISRA-SAについて、設計の現場などで既に充分に調査をし、技術者たちはこれを上回るガイドラインを社内に用意して、トヨタの自動車の安全性を確固たるものにしてゆきたいという想いで取り組んでおられるものと推察する。それを、我々にも目に見える形に完成させて頂きたい。トヨタは品質に関する規格であるISO 9001 で、過去にこれと同じようなことを実現した実績がある。その再現を、我々はMISRA-SAで期待している。

しかしここで、2つ目の提言に関連した留意事項がある。前述の通りMISRA-SAは、現場の技術者たちだけが対応すれば「それでよい」というものではない。TQC／TQM やISO 9001と同様、トップを含む全社で一体となって対応して、始めて充分な効果が現れるものである。トヨタはこのMISRA-SAを上回るガイドラインを社内に設定し、トップは情報システムで対応するべき範囲にこのような領域もあることを強く認識して、これを活かす全社的な体制を早急に構築して頂きたい。さらに将来この規格が改訂される場合などには、世界のリーディング・カンパニーとして、トヨタはここでも国際貢献という観点から世界をリードする立場に立って頂きたい。これが、我々の3つ目の提言の後半部分である。

提言のまとめ

以上我々の今回の提言をまとめると、以下の通りである。

1. ソフトウェアに手を入れた時には、回帰テストそのもの、あるいは「回帰テストのセンス」を持ったテスト（これまで持っており、今後も必要である機能が今回のプログラム変更で損なわれていないかを確認するテスト）の実施が必要である。
2. プリウスに限らず今の自動車は、既に「情報システム」である。したがってそれをメカニカルな自動車として捉えるだけでなく、情報システムとして今後それをいかに発展させ、使用者の安全性と利便性を向上させるか、という立場からのアプローチが必要である。さらにこれを効果的に進めるために、トップを初めとする自動車メーカ全社での意識改革が必要である。
3. MISRA-SAという英国の自動車の機能安全規格に対処するガイドラインを基に、今ISO規格化が進められているが、国際規格として発行された場合、そのISO規格を速やかにJIS化するなどして、経済産業省は日本国内で「安全性」の議論を高めて頂きたい。さらに日本の自動車業界の各社は、安全性の問題に的確に対応できるようにして頂きたい。

   併せてトヨタは、MISRA-SA（またはISO 26262）を上回るガイドラインを社内に設定し、それを活用できる全社的な体制を構築して頂きたい。また将来この規格の改訂時などでは、世界をリードする立場に立って頂きたい。

参考文献とリンク先

[FUT07] 二上貴夫、「自動車分野の機能安全規格に対処する実務ガイドライン「MISRA-SA」を知る ― 自動車業界の要請はCコーディング・ガイドラインから安全性解析へ」.
この資料は、以下のURLからダウンロードできる。（確認日：2010年9月2日）
http://www.kumikomi.net/archives/2007/03/21misr.php

[HON] 本田技研工業株式会社、「リコール制度・改善対策制度とは」.
この資料は、以下のURLからダウンロードできる。（確認日：2010年9月2日）

http://www.honda.co.jp/recall/

[ISS09] 情報システム学会、学会紹介小冊子「情報システム学会について」、情報システム学会、2009 年 11 月.

[JUA09] 日本情報システム・ユーザー協会、「障害を発生させない、被害を拡大させないシステム対策ガイド」、日本情報システム・ユーザー協会、2009 年 6 月.

[JUA10] 日本情報システム・ユーザー協会、「2009 年度版 企業 IT 動向調査 2010」、日本情報システム・ユーザー協会、2010 年 6 月.

[JUS10] 日本科学技術連盟、「外部専門家による品質保証体制評価報告書」、日本科学技術連盟、2010 年 6 月 30 日.

この資料は、以下の URL からダウンロードできる。（確認日：2010 年 9 月 2 日）

http://www2.toyota.co.jp/jp/news/10/07/nt10_0708b.pdf

[LEV95] ナンシー・G. レブソン著、松原友夫監訳、片平真史他訳、「セーフウェア 安全・安心なシステムとソフトウェアを目指して」、翔泳社、2009 年 10 月 29 日.

[MET09] 経済産業省商務情報政策局情報処理振興課、「情報システムの信頼性向上に関するガイドライン 第 2 版」、平成 21 年 3 月 24 日.

この資料は、以下の URL からダウンロードできる。（確認日：2010 年 9 月 2 日）

http://www.meti.go.jp/press/20090324004/20090324004.html

[NIK10] 日経 BP 社トヨタリコール問題取材班、「不具合連鎖 「プリウス」リコールからの警鐘」、日経 BP 社、2010 年 3 月 23 日.

[WIKa] Wikipedia の“Motor Industry Software Reliability Association”より。

この資料は、以下の URL からダウンロードできる。（確認日：2010 年 9 月 2 日）

http://en.wikipedia.org/wiki/MISRA

[WIKb] 日本版 Wikipedia の「MISRA-C」より。

この資料は、以下の URL からダウンロードできる。（確認日：2010 年 9 月 2 日）

http://ja.wikipedia.org/wiki/MISRA-C

以上