

安全とは初期の目的を達成してなおかつ別に害毒を伴わないこと

2011年の30日以内死者数は、5405人になっています（警察庁, 2012）。交通事故による死者数です。この数字から、その当事者になる確率を出すと、 4.2×10^{-5} 人/年となります（人口が127,510千人としています）。この数字を他のリスクと比較した上で、社会的にこのリスクは容認されているとするのは誤りです。容認というのは選択ですから、選択がない場合には（即ち自己責任ではなく）危害を受けることは一般的に容認されないということになります。この数字には、犠牲者には選択の余地がない事故が多数含まれています。

さて、ISO 26262が目指すのは、機能安全を通じた事故の減少になります。すなわち、安全性を担保する機能の故障により、結果として事故を減らすということになります（プロセスの開始点となるアイテム定義のアイテムはあくまで車両レベルであることに注意が必要です）。しかし、そもそも交通事故と呼ばれるもののなかで、故障に起因するものはどの程度あるのでしょうか。

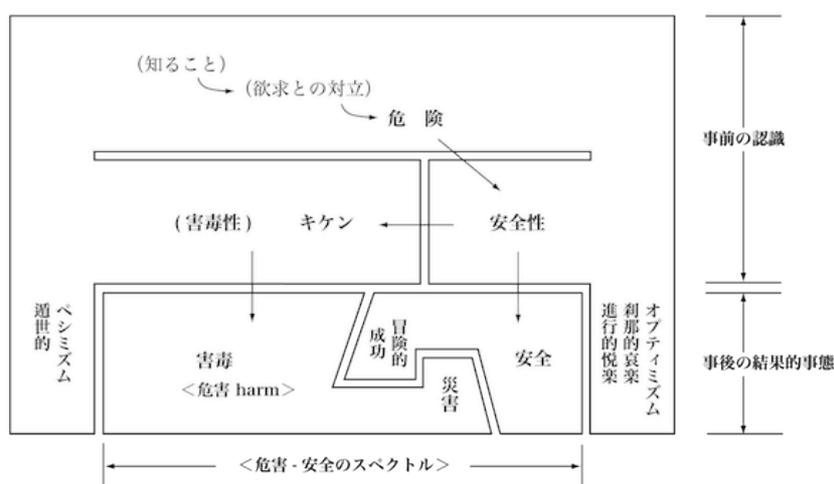
ごく簡単にですが、調べてみることにしたいと思います。警察庁の統計だとほとんどが交通法規の違反にカウントされてしまいます（違反不明が0.1%）。行政機関として法規を遵守すれば事故は起きないという立場なのでしょう。或いは、実際に車両故障に起因するかどうかを毎回調べられないということかもしれません。

次に商業車の統計を見てみます¹。こちらは、ISO 26262のスコープから外れています（商業車であり、かつコンテナ落下といった事故も含まれます）。運送事業者からの報告で構成されていますから、どこまで客観性が担保されているか分かりません。しかし、事業者は事故に対して大きな関心を持っているので、ある程度正確な数字であることが期待できます。5520件の事故のうち、車両故障が占める割合は意外に大きく42.8%となっています。ただ、原因としての整備不良もここに含まれますし、乗務員というより車両の問題としたいというバイアスが掛かっているかもしれません。

別の統計としては、同じく国交省でメーカーからの届け出の記録があります²。この件数は少なく、平成22年で193件となっています。細かな分類をみると、特定できず/点検・整備の問題/調査中が3大要因で、設計製造の問題とするのはごくわずかです（全原因のうち10%程度）。こちらは、メーカー（OEM）のバイアスがかかるであろうことは想像できます。

結局、機能安全により、最終的なアウトカムとしての事故減少がどの程度期待できるかは不明です。警察庁の統計だとほとんどが人間の問題ということになりますし、国交省の統計だと、おおむね5%程度ということになります（42.8%の10%ということかなり乱暴な計算です）。特に商業車の場合は、プロのドライバーによる運行であることを差し引いて考える必要があるかとも思います。そうすると、ISO26262のスコープで対象となる機能安全に起因する事故は、5%より更に小さな数字になるということが想像できます。もちろん小さいと云っても生死に関わる数字に対しては、十分な関心を持つべきであることは間違いありません。

「安全学策隠」³という本があります。そのタイトルが示すように、安全の意味について探究した読み応えのある本です。この本の中に以下の図が書かれています（p.89）。少しだけ改変しているのですが、ぜひ図書館等で本にあたって頂いて、オリジナルの図と本全体に含まれる滋味を感じて頂けたらと思います。



安全の現れ方として、一つには欲求がある。典型的には身を守りたいということでしょう（もちろん起因としては、身体的なものだけではなく単に素早く目的地に着きたいという欲求もあります。ただ「危険」を惹起するには身体的な欲求へと変化する必要があります）。一方で、知ることがある。ある物質がありその成分と身体への因果が分かると、それは身体の維持という欲求に対立して危険という意識を生む。もちろん、知ることが知識に限定されず経験という言葉が適切な身体性を持つ「知」の場合もあります。この場合は、欲求との対立というよりは、直接的に「危険」が意識に上ります。

危険の意識は、次に「安全性」と「キケン」という相反する二項を生みだし、その境界を考える上での契機となります。これらは必ず不確実性を持ちます。結果は実

行後にしか分からない。そのため、ここでは不確実性を意味として含むように「安全性」と「キケン」という用語になっています。「安全性」とは、システムの特性というよりは、いま想定し考える安全の度合いといった意味ですし、カタカナの「キケン」も同様に危険ではなく受けるであろう危害の度合いです。著者は危害に代わり害毒を用い、また安全に対立する害毒の（生じる）程度ということで、「害毒一性」を用語としては適切としています。私は、ここでは標準的な「危害」と「キケン」を用いることにします。

さて、事後的に、（危険源が顕現することで）実際に危害が加わったか、安全かが分かります。このときに、当初は安全性が高いと見なしたことに對して生じた突発的な「災害」による危害もありますし、キケンとみなしてもやり遂げ結果的に問題がなかった「冒険的成功」もあります。ここでの「災害」や「冒険的成功」は文字通りの場合もありますし、象徴的ないい方でもあります。例えば、「災害」というのは、実際に地震や台風ということもあるでしょうが、それが計算されているのであれば、地震・台風といえども「災害」には入らない。今考えている系の外側から突発的に到来するものといったことになります。

もちろん、反省的に安全性・キケンを考えない場合、オプティミズムやペシミズムの態度を取ることになります。ここまで見た経路の最初のトリガーとなる（経験を含めた）「知」が働かないと、オプティミズムに近くなるでしょうし、「知」が働いても、「危険」から「安全性」へのギャップを超えられないと、ペシミズムに落ちていくということになります。

ISO 26262 は、その上位の規格である IEC 61508 と基本的な点での違いを感じます。IEC 61508 は、安全を確保するための機能の故障により（プラント等の事故から）人や環境に危害を加えることを防ぎたいというのが前提になっています⁴。ISO 26262 では、乗用車と運転者を含めた系が事故を起こさないということが主眼で、単に安全に関わる機能の故障と云うよりも、車を運行する運転手まで含めたより広い範囲を扱っています（典型的には、SILの算出において運転者の制御可能性を含んでいることに注意が必要です）。このことが（主としてプラントか車かという）対象の違いで生じているとすると、本来の規格における上下関係が実は左右の関係ということになります。規格の構成としてはあくまで上下なのですが、同一レベルであるという要素も大きいかと思えます。

ところで、どこまでを系として含むか、即ち安全とは誰にとっての安全かというの

は、安全に関わる機能の故障と同様に、重要な問題です。最初に書いた交通事故を例に取ります。交通事故で危害を受けるのは、運転者や同乗者に限りません。比率では歩行者が一番高い(36.6%)。もし、「交通事故」ということを意識するのだとすると、安全に関して考えるべき範疇は、車一運転者という系に対して、更に広くとらなくてははいけないということになります。

先の図では、安全性とキケンの中にギャップがあります。安全性とキケンの間は滑らかに移行するのですが、実際には行動するための判断があるので、ギャップを越える必要があるということになります。法的な基準があるとしても、日常生活においては、これは個々に判断することになります。少し簡単な例を考えます。私の住んでいる場所の近くに少し変則の交差点があります。ここは左折車の見通しが悪く、信号が青でも歩行者は横断時によほど注意しない限り、キケンという場所です。歩いて渡る私にとって、キケンー安全性を区別する線はかなり右側にとる必要があります。一方で、この交差点をよく知らない人にとっては、安全性が確保されている位置で考えています。従って、危害を受ける・与える可能性はずいぶんと高くなるということになります。事故があった場合、法的には、これは交差点安全進行違反ということになるのでしょうかけれど、そうしたところで事故に遭った人が救われるわけではありません。車両における今のプリクラッシュセーフティ等の予防安全はおおむね運転者の安全確保に重点を置いています。歩行者を含めた社会という系の中ではないということ、より一層「安全」という用語を使うときに注意しなくてはならないこととなります。

今回の表題は、先に紹介した辛島さんの本にあるものです(p.38)。安全は事後的に定まる！ということと、安全が議論に上るのは、何らかの有益と思える行為があるからということになります。「無益では問題にならない(前述.注1)」。

(nil)