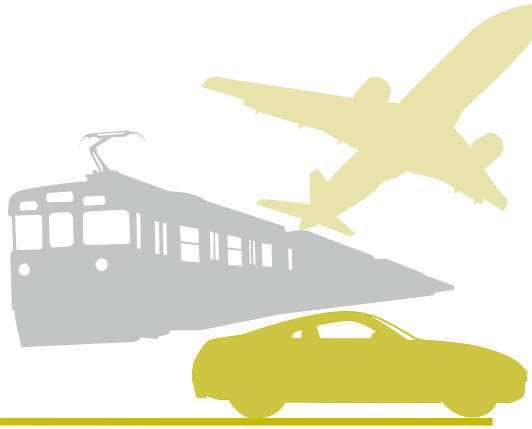
セーフティとセキュリティ

基般



大久保 隆夫（情報セキュリティ大学院大学）

セーフティの概念

Safety（セーフティ）を日本語にすると，「安全」である．また一方，security を「セキュリティ」ではなく元々ある日本語で表わそうとするとやはり「安全」ということになるだろう．同じ「安全」なのに，この 2 つは，その意味や基準，規格も異なってくる．セキュリティの方は 1 つ前の記事『情報セキュリティと乗り物』で解説したが，セーフティの概念についてもここで紹介しておく．

実は，乗り物や，制御システムなどでは，セキュリティよりもセーフティの方が重視され，保証される品質の 1 つにもなってきた．すなわち，世の中に出ている車や鉄道，飛行機はセーフティの品質において必要な基準を満たしたものである．技術的なセーフティの定義は，「受け入れ不可能なリスクが存在しないこと」となっている．また，別の定義では，「人への危害または資（機）材の損傷の危険性が，許容可能な水準に抑えられている状態」となっている．後者の定義にあるように，絶対的な安全は存在しないという前提に立ち，リスクの線引きを行い，「ここまでリスクを低減できたら安全とする」という考え方である．この考え方に基づき，リスクを基準以下に低減する機能の働きによって確保する「機能安全」の方法が近年では主流となっている．機能安全では，リスクを発生確率×被害の大きさで考えるため，リスクを見積もる手段として，自然現象やヒューマンエラーなど，確率が計算可能な事象が想定されてきた．乗り物の安全規格も，この機能安全の考え方に沿って設計されている [1]．

セーフティとセキュリティの共通点，相違

では，セーフティとセキュリティの関係はどうなっているのか，関係を**図 -1** に示す．図には，セーフティ，セキュリティにとってリスクの因子になる要素を示した．セーフティ側の，「機器の安全」「人命」「事故防止」は同じことのように見えるが，異なる場合もある．機器の安全を無故障ととらえると，機器が故障することによって，事故や人命への危害を防ぐことができる場合もある．たとえば，車の窓ガラスはハンマーなどで衝撃を与えると簡単に割れるようになっている（故障する）が，割れることで乗員の脱出を可能にすることができる．

ではまず，セーフティ，セキュリティ両者に共通する要素から考えてみよう．1 つ前の記事で挙げたような，車載ネットワークを流れる制御通信を奪うような完全性に対する脅威は，セキュリティに関係するだけでなく，制御を奪うことで機器や人命の安全を脅かすため，セーフティにも属するといえる．機密性については，このような制御情報が漏洩することが攻撃の助けになることもあるので，セーフティに関係していないとはいえないが，直接的ではない．また，前の記事で挙げたプライバシー情報の漏洩は，直接的に機器や人命に危険が及ぶ訳ではない．可用性についても，情報やサービスの可用性の確保が安全に関係する場合もあるが，可用性の要求が逆に安全性の要求と相反する場合もある．たとえば，何か問題が発生して，安全にエンジンを停止しなければならない場合．この場合は，セキュリティの可用性の要求に対しては侵害することになる．

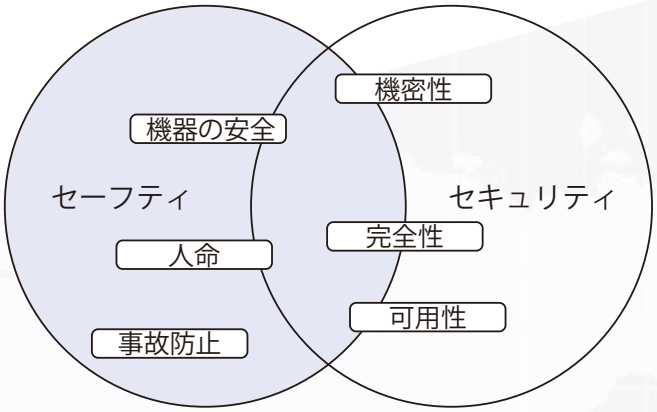


図-1　セキュリティ分析の流れ

逆に，機器安全や人命保護を，セキュリティのアプローチでリスク分析しようとした場合，機密性や完全性，可用性の検討だけでは，観点が網羅できないことになる．機密性や完全性に侵害がなくても，自然災害などによって安全が脅かされる場合がある．

また，セーフティ的分析とセキュリティ的分析の決定的な相違として，「悪意の存在の仮定の有無」がある．セキュリティでは，常に攻撃者が悪意を持って対象のシステム関係者の意図しない動作をさせることを前提にリスク分析を行う．一方，セーフティにおいては，リスクを発生確率×被害の大きさで考えるが，これを攻撃のリスクとしてとらえた場合，攻撃の「発生確率」を求めることができるだろうか？　セーフティ分野で用いられる故障の木解析（Fault Tree Analysis：FTA）においては，この確率は故障率として扱われる．この故障率は，複数の機器がかかわる場合，その和や積で表されるが，攻撃者が任意にそれぞれの故障の確率を操作できるとしたら，故障率が低い＝リスクが基準値以下だから対応不要，と言えるだろうか．また，前の記事で紹介した weakest link の概念[☆1]も，セキュリティ的攻撃が故障率の和や積で表現できないことを示している．

[☆1] システムや製品の中で最も弱い場所を攻撃者は狙うため，システムや製品の安全性は最も脆弱な場所の安全性に依存するという考え方．

規格，現場の対応状況

前述のように，セーフティ，セキュリティの一方のアプローチのみで，もう一方をカバーすることは困難である．セーフティ，セキュリティの現状の規格もそれぞれのアプローチを反映しているため，安全（セーフティ）規格を満たしただけで，セキュリティ的にも「安全」かというとそうはいえない．このため，製品の開発現場では双方のアプローチによって，双方の規格を満たすという手間がかかることになってしまっている．この問題に対して，業界ごとになんとかしようという動きは（主にセーフティ側から）あるようである．詳細はほかの記事に譲るが，自動車業界においては，ヨーロッパの EVITA（E-safety Vehicle Intrusion proTected Applications）[☆2]や，自動車技術会 JSAE の情報セキュリティ分析ガイドなどが挙げられる．

参考文献
1）ISO：ISO 26262-1:2011 Road vehicles Functional safety (2011).

（2016 年 3 月 30 日受付）

[☆2] http://www.evita-project.org/

大久保隆夫（正会員）　okubo@iisec.ac.jp
1991 年東京工業大学物理情報工学専攻修了．同年（株）富士通研究所入社．2013 年より情報セキュリティ大学院大学准教授，2014 年より同大教授．博士（情報学）．専門はソフトウェア工学，システムセキュリティ．