Sécurité fonctionnelle

セーフティケースによくにた概念にアシュアランスケースがあります．アシュアランス自身は，規格化されています（ISO/IEC 15026）．この中で，アシュアランスは，システムのプロパティに対して適用されるとしています．このプロパティを定義するものとして代表的なものに SQuaRE（Systems and software Quality Requirements and Evalution，以下ではシリーズのうちISO/IEC 25010についてみてみます）と呼ばれるシステム及びソフトウェア品質モデルがあります．

ソフトウェアライフサイクルの議論も含め，いかにソフトウェアのモデルや議論・規格がシステムレベルの同等のものに影響を及ぼしているかを記憶して頂くだけにとどめて，詳細は別の機会にしたいと思います．

ここでは，ISO/IEC 25010の中から，単に安全性とセキュリティをとりあげます．

***

安全性とセキュリティと単に対比してみると，基本的に違った概念のように見えます．しかし，「このシステムはセキュリティがしっかりしているので，お客様のデータは安全です」という云い方も可能ですから，関係がないわけではありません．

先の ISO/IEC 25010から，安全性とセキュリティに関して少し抜き出してみます．なかなか日本語にするのは難しいのですが，ちょっとトライしてみます．

> 【安全性を含む場所】(4.1, Table 3)
> 定義場所：利用時の品質
> 特性　　：リスク緩和性
> 副特性　：経済的リスク緩和，健康及び安全リスク緩和，環境リスク緩和
> 【セキュリティを含む場所】(3.3, Figure 4)
> 定義場所：システム／ソフトウェア製品品質
> 特性　　：保障性（security）
> 副特性　：機密性，完全性，行為証明性(non-repudiation)，行為追跡性（accountability），真正性

こうすると，セキュリティというのは，何らかの保障を行うこと，すなわち正しく認められた人が，正しいデータに確実にアクセスできるといったことを指しています．データという財産を守っているのだと考えても良いのだろうと思います．セ

キュリティはシステムの保障であり，一方で，安全は，直接的に人の生命を守るという，それぞれ狭い範囲に閉じ込められています．ここには，そういコンテキストがあるのだと理解しておきます．

別の視点から考えてみます．例えば，ホームセキュリティという場合，そのセキュリティは，家の財産，住人の生命を守ることを目標としています．先のリスク緩和性の経済的リスク緩和であり安全リスク緩和なわけです．ここでは，（人および財産への毀損がない）安全確保の手段としてのセキュリティがあります．

一般化すると，安全とは，人及び財産への毀損がない状態を指しており，そのための手段が保障（セキュリティ）だと考えることができます．ISO/IEC 25010 に戻ると，コンテキストは違うとはいえ，セキュリティが製品品質であり，安全性が利用時品質なのも，前者は手段であり，後者はそれによる結果だとすれば，一応の理解を得ることができます．

***

しかし，それでもなお，不満は残ります．利用時品質の安全は，システムのプロパティとしてはどこに相当するのかということです．特性のうち，機能性や信頼性などに分散しているという説明しかないことになります（c.f. ライフサイクル上の利用時品質の定義からシステム品質への展開）．あるいは「安全はシステムとその外部との関係によって定まるために純粋なプロパティとしては措定できない」ということかもしれません（cf. Context coverage — 利用時品質の一つ）．確かにここで定義されている狭義のセキュリティは，ほぼシステムに閉じています．それを破る可能性のあるものは，システムから排除することもできます．しかし，そうだとすると，「このシステムは安全である」という言明は意味をなさないということなります．

ウルリッヒ・ベックが指摘するように，安全の問題にはつねに「非知」を伴います．誰もある化学物質が環境にそして人間にいかなる影響を与えるかを指摘することはできないのと同様に，その構造として全てを知ることはできない（まして，二者間取引とはことなるコンシューマ向けシステムにおいて，ユーザは更に構造的に強化された「非知」の状況におかれています．ここでいう「構造的」というのは，抗菌薬とそれをすり抜ける真菌やウィルスとの相互的関係に似ています．いくらがんばっても最終的な「知」には達することができない）．だとすると，利用時品質->製品品質->利用時品質というプロセスの中で安全性を評価できるとする主張は，素朴すぎて，あまり意味を持たない気がします．

さて，最初にもどるとアシュアランス概念は，これら品質特性によって示されるシステムの様々なプロパティを同時に扱えることになっているのですが，さて，それが果たして可能かはまた考えたいと思います．

***

さて，今回のタイトルは，機能安全（functional safety)のフランス語訳です．安全ですが，英語のsecurity に近い（なるべく近いカタカナで書き表すと）セキュリテが使われています．Sécurité の語源は，securitasaで，これは，心配がないという意味になります．語源としては，日本語で言う安心に近いでしょうか．さて，ここでは，安全という用語にセキュリティが使われているので，では，セキュリティという意味のフランス語はなにかというと，（ISO/IEC 2510 規約は仏訳がないので分からないのですが）sûreté あたりが使われるのかなと思います．この単語にも安心という意味がありますが，chaîne de sûretéといえば防犯チェーンのことですから，日本語で言うセキュリティに近いかも知れません．

用語は，難しくもあり，面白くもあり．

(nil)