

加藤 肇彦*

On its Rapid Progress and Proliferation in the Field of Information Industry

by

Hatsuhiko Kato*

Key words : Reliability, Dependability, Information Industry, Fault Avoidance, Fault Tolerance

1 はじめに

近年の情報産業の進展には目覚ましいものがある。当初は「計算する機械」とだけ位置づけられていたコンピュータが、現在は社会に不可欠なインフラストラクチャの地位を得るまでに浸透してきている。そしてこの情報産業を支える基盤は計算機関連技術を中心とする情報工学である。にもかかわらず情報工学は明確に一つの技術分野を形成して認知されるようになってから高々30数年しか経ておらず、他の工学分野に比べて体系化が遅れている。そして情報工学の中での信頼性工学もまた未分化である。この問題を解決するため、情報産業における信頼性向上技術の体系化への努力が続けられ、往時に他分野での信頼性工学がたどった軌跡をなぞりながら急速に発展を遂げつつある。今回は情報産業分野における信頼性工学の現状と課題について述べる。

2 情報産業における信頼性の捉え方

情報工学においては従来「信頼性」という日本語に相当する英文用語として「reliability」を充てていた。そしてより広くRASIS(reliability, availability, serviceability, integrity, security)という言葉で概念を包括的に捉えていた。さらに最近では「dependability」という用語が、人間から見た情報処理システムの「頼りがい」の定性的あるいは定量的尺度を表すために使用されている。これは単に情報処理機器が物理的な故障や誤動作に対して強固であるだけでなく、人為的な誤操作や悪意による破壊活動に対しても、周囲に悪影響を及ぼさない健全性を保障することを要求する概念である。特に最近では security (安全性)の面が強調されている。

3 情報産業における信頼性工学応用の二局面

情報産業における信頼性工学応用を論じるときには、二つの局面から考察する必要がある。第一の局面は情報産業自身の信頼性の維持向上である。往時のような数値計算や機器制御への応用にとどまらず、現在は情報処理システムが社会

のインフラストラクチャとして浸透しているため、偶発的な誤動作や誤操作が重大な事故につながるおそれがある。さらにコンピュータウィルスのような悪意による情報システムの攪乱が日常的に頻発している。このような事情から、情報産業が産み出す製品である情報機器の信頼性が重要な要素となる。情報機器の高信頼化技術は現在独立の分野として存立し、関連学会でも研究活動が活発に行なわれている。

今ひとつの局面は、信頼性向上そのものを情報産業の重要な応用分野として捉える見方である。従来人手あるいは機械・電気的な手段で行なってきた機器やシステムの操作を、コンピュータによって代替するだけでなく、従来手段に比した信頼性の飛躍的向上を付加価値として積極的にアピールするという姿勢である。当然信頼性向上の手段であるコンピュータ自身に信頼性が要求されるため、この第二の局面は必然的に第一の局面を内包する。

4 情報産業における信頼性の階層

情報産業における信頼性工学応用は複数の階層で捉えることにより把握が容易になり、また階層毎に事業分野や要求される要素技術も異なる。ここでは階層を以下の5層に分けて考察する。

(1) 社会レベル

社会レベルでの信頼性保証は、政府により各種対策が打ち出されている。主要な例として2000年に設置された「内閣官房情報セキュリティ対策推進室」がある。これは中長期的な助言を行なう専門調査チームと、サイバーテロのような事案に対処するための緊急対策支援チームから構成されている。この他に迷惑メールの防止を目的とした「特定電子メールの送信と適正化等に関する法律」が2002年に公布・施行された。1994年に公布されて1995年に施行された「製造物責任法」は、計算機/ソフトウェア単体では適用対象としていないものの、機器に内蔵されて一体となっているソフトウェアは適用対象に

* 正 会 員 湘南工科大学情報工学科 〒251-8511 藤沢市辻堂西海岸 1・1・25, Dept. of Information Science,
Shonan Institute of Technology, 1-1-25 Tsujido Nishikaigan Fujisawa 251-8511

含むという解釈が一般的である。

信頼性向上に不可欠な要件として規格の制定があるが、国際標準化機構ではソフトウェアの信頼性に関する規格として ISO9003-3 を制定し、国内においても各種団体ならびに企業がこれを推進している。

(2) 組織・団体レベル

官公庁・企業・学校等の組織・団体では、情報管理体制の整備が信頼性向上の要件となる。内規の整備と遵守、各構成員のモラル向上が情報漏洩や不正参照の防止に必要であり、これらは社会に対する道義的義務であるとともに、組織・団体の自己防衛にもつながる。

(3) 家庭・個人レベル

社会・組織・団体の情報の信頼性の維持向上には、構成員たる各個人の問題意識が重要である。パスワードの秘匿と更新、ウィルスの予防、バックアップファイルの保存等の配慮が必要である。これは各個人の社会的活動にとどまらず、私的行動にまで及ばなければならない。

(4) 装置・機器レベル

装置・機器の信頼性は平均故障間隔時間 (MTBF)、平均修理時間 (MTTR) ならびに平均稼働率 $MTBF/(MTBF+MTTR)$ で表される。稼働率の高い装置・機器は信頼性が高いと考えられ、MTBF を長く MTTR を短くすることが信頼性向上をもたらす。このほか情報機器はただ稼働するだけでなく、正しい結果を出力するという指標を達成しなければならない。

MTBF を長くする技術はフォールトアボイダンス (故障回避) と呼ばれ、堅牢な材料・部品を使用したり、設計・検査を周到に行なったりすることによって実現できる。出力の正しさの指標として、フォールトレナンス (耐故障性) が挙げられる。これはたとえ故障が発生してもその影響を局所的に限定して外部に及ぼさない機能である。

MTTR を短縮する技術はフォールトリカバリ (故障復帰) と呼ばれ、障害の特定と分離、保守用データの収集、保守用ツールと部品の整備、要員の教育、設計時における保守性の作りこみ等である。

5 事業としての信頼性工学応用

従来人手による操作に頼ってきた分野を計算機で自動化することによって人為ミスが排除されて信頼性が向上できる。プラントや製造ラインの制御、金融や発券窓口、放送・通信・交通・上下水・電力のインフラ制御、自動車・家電品のような民生品の制御は情報化による信頼性向上が実現されている分野である。以下にこれらを階層別に考察する。

(1) 素子・材料レベル

各素子の使用条件を事前に検討し、過酷な条件下でも長時間にわたって安定に動作することを確認する。耐環境試験を実施することはもちろんであるが、定格を安全側に割り引いて使うデレーティングが一般的に行なわれている。

(2) 部品・回路レベル

多重化した部品に同一機能を実行させて出力を比較する冗

長構成は、この分野では広く採用されている。また、故障検出時の待機系への切り替えや、自己診断機能も重要な技術である。反射や誘導による誤動作を防止するために、実装上の配慮も必要である。

(3) 装置・機器レベル

局所的な誤動作からの回復には誤り検出・訂正符号が有力である。また、集中的に発生するバーストエラーに対しては、定期的に受け取った信号により診断プログラムを起動して結果を返すウォッチドッグタイマが有効である。また、このレベルでも自己診断機能が使用される。

(4) システムレベル

システム全体の高信頼化には、上述の各技術を有機的に組合せ、全体として正常に機能させることだけでなく、レベル間でのトレードオフが必要である。正常動作が保障できなくなった場合は、縮退運転機能、出力が異常であることを外部に知らせる、フォールトシキユア機能、安全側出力を出して停止するフェイルソフト機能が要求される。

(5) 広域情報インフラストラクチャ

広域に利用される情報インフラストラクチャには通信回線が介在し、これが信頼性の要となる。物理的な伝送品質の保証だけでなく、端末制御や通信規約のような方式面での信頼性向上技術が必要である。

(6) ソフトウェアの信頼性向上

ソフトウェアはハードウェアと異なり、間歇的障害、定常的障害、固定的障害という消長を取らないで、処理の流れがプログラムの固定的障害部分を間歇的に通過するときに発生する。従ってソフトウェアの信頼性向上の要諦は設計製作時に固定的障害 (バグ) を作りこまないことにある。設計文書の可視化、モジュール分割、構造的維持、テストの網羅性の保障のための各種技術が適用されている。とりわけ最近では機械語よりは自然言語に近い高水準言語が多用されている。

6 情報保護の観点での信頼性技術

不正参照と改ざんの防止のために、離散数学を応用した暗号技術が利用されている。また、指紋・虹彩紋・顔・声紋・等の人体の特徴を判別に利用する、バイオメトリクス技術が実用化されている。近年問題になっているコンピュータウィルスに対しては、ウィルスの特徴であるシグネイチャを検出して除去するワクチンソフトが使用される。

7 今後の課題

以上から明らかなように、情報産業における信頼性工学の要素技術は極めて多岐にわたっている。そしてこれらの各技術は現在ではまだ体系化されているとはいいがたく、雑多な技術の集成でしかない。今後は階層間の整合をとり有機的に一体となった技術体系を確立する必要がある。また、設計技術の進歩により信頼性の阻害要因が回路や機器の物理的レベルから組織や社会の人為的レベルに移行してきている現状にかんがみ、経済学、社会学、心理学、教育学、行動科学等の非自然科学分野の知見を利用していく必要もある。