情報システムと社会安全

相原 磨世
TFOS.SG 環境部会

1. はじめに

コンピュータの処理能力の向上、インターネット通信網の発達等により、我々の生活における情報システムへの依存度は年々高まっている。そのため情報システムの障害による社会的影響の大きさもまた深刻化しており、情報システムの信頼性や安全性の向上は極めて重要な課題になっている。

航空業界においても、最近では 2009 年の日本航空チェックインシステム障害、2003 年の全日空チェックインシステム障害、同 2003 年の FDP システム障害など、情報システムへの依存度に比例して障害の影響が大規模化している。

本稿では、今後情報システムと社会安全を検討するにあたり、導入部として情報システムや障害の分類、信頼性・安全性向上に向けた基本的対策を紹介する。

2. 情報システムや障害の分類について

情報システムとは、「コンピュータを用いて構成されるソフトウェア、装置・機器等のシステム及び処理・記録されるデータ・データベース」を総称したものである。情報システムの特殊性として、「ネットワーク性」が挙げられる。通常大規模な情報システムは、多数の情報システムがネットワーク等を介して接続され、連携して機能する。このような場合は、全体を一体の情報システムと見なすことが出来る。

経済産業省が 2006 年に策定した情報システム信頼性向上に関するガイドライン[1]では、求められる信頼性・安全性の水準に応じ、情報システムを以下のように分類している。

(A) 重要インフラ等システム

国民生活・社会経済活動の基盤であり、他に代替することが著しく困難なサービスを提供するもの。その機能の低下、または利用不可能な状態が、国民生活・社会経済活動に多大な影響を及ぼす恐れが生じるもの、人命に影響を及ぼすもの。管制システム等がこれにあたると思われる。

(B) 企業基幹システム

企業活動の基盤であり、その機能が低下又は利用不可能な状態に陥ったとき、企業活動に大きな影響を及ぼし、且つ及び取引先や顧客等にも影響を及ぼすもの。エアラインのチェックインシステムはこれにあたると思われる。

(C) その他のシステム
　上記未満の水準のもの。

　社会安全の観点では、（A）と、(B)の一部を対象に、情報システムのライフサイクル全般において、求められる信頼性と安全性の水準を議論し、発生しうる障害を調査分析し、原因毎に多面的な対策を講じる必要がある。
　情報システム障害に係る原因としては、以下のようなものが挙げられる。

(1) 要件の誤り
発注仕様の誤り、システム動作環境、運用環境（前提条件等）の認識誤り、システム対象業務分析ミス、非機能要件の評価誤り、セキュリティ機能要件の誤り等

(2) ソフトウェアの誤り
機能不適合、データ加工・処理ミス、条件判定ミス、処理タイミング・ミス、情報の誤表示等、コーディング・ミス（脆弱性） 等

(3) 調達ソフトウェアの不具合
調達ライブラリの仕様不適合、ミドルウェアの不安定稼動、ドライバソフトウェアの不具合、調達ソフトウェアの脆弱性等

(4) ハードウェア故障・性能低下等
ハードウェア故障（周辺装置・機器、制御装置を含む）、故障時の代替機の調達困難、ハードウェア処理能力の低下、想定状況外での不安定動作、製造プロセスにおけるマルウェアの混入等

(5) 製品間インターフェイスの誤り
ハードウェア及びソフトウェア製品単体の機能としては問題ないが、それぞれの組合せの不整合等により発生するトラブル等

(6) 性能・容量等の不足
トランザクションや処理の集中に伴う処理速度の低下､データ量増大に伴うデータ記憶領域の不足、不正アクセス等による過負荷等

(7) 移行時の誤り
ソフトウェア修正時のデグレード発生、データ移行の失敗、機器及びソフトウェアの設定ミス等

(8)運用・保守方法・手順等の誤り
マニュアル等の誤りや過信、操作手順に関する誤解や誤り、慣れに伴う操作の誤解や誤り、脆弱性対応手順の誤り（パターンファイルの不適用等） 等

(9) 情報システム障害発生時の対応の誤り・遅れ
情報システム障害発生時の復帰手順の整備不足、復帰操作の誤解や誤り、縮退運転機能の欠落、関係者への周知不足、対応の遅れ等

特に大規模な重要インフラ等システム（以下、大規模システムと略記する）は、上記の原因を誘発するリスクを多く内在している。多くの大規模システムは類似システムが少ない特殊性を持つために(1)、(2)を引き起こす可能性を秘める。大規模システムの持つネットワーク性は、(3)、(5)、(6)のリスクを内在し、また長期間にわたり継続的に機能追加や修正を行いながら運用されるため、(7)、(8)が原因となる障害もある。

日本航空は 2009 年 6 月 3 日に発生したチェックインシステムの障害の原因について、チェックインシステムと予約発券システムのバージョンアップ作業によるものと発表した。これは上記分類の(7)にあたる。ソフトウェアの移行やバージョンアップ作業は、一般的な機能テストに対し実施できる頻度も少なく、移行のためのテスト環境自体が存在しない場合も多い。

3. 信頼性・安全性を向上させるために

上述のガイドラインでは、信頼性・安全性向上のためには情報システムの共有者や利用者だけでなく、経営層にも責任があることを明言し、経営層が情報システムのリスクと不完全性を認識すること、経営資源の投入、継続計画の策定、訓練の実施等を求めている。

また未然防止のための対策と、障害発生後に業務への影響を最小限に抑える事後対策についてもシステムの特性に応じて凹検討が必要である。

運用期間が長いいわゆる「枯れたシステム」であったとしても、どれほどの時間をかけてテストを実施しても、システム障害は起こりえる。Myers は 1976 年に、たった 100 行のプログラムでも 10 の 18 乗の実行パターンが存在しうることを述べ、完全テストの不可能性を示した。システムは人間が構築したものである。よって「人間はミスをする」ということと「システムは障害を起こす」ということは本質的に同じ意味を持つ。

情報システム業界は新しい業界である。大規模な情報インフラが社会安全に与える重要性が急速に高まっている一方で、社会安全に関する分析、現場の安全リテラシー、法整備等はまだまだ未成熟であり、その重要性とのバランスが取れているとは言い難い。

情報システムを提供する企業や開発エンジニアも、直接の顧客に対する顧客満足や仕様を満たすかのみに注力する傾向が強く、社会安全に関する意識や文化が育ってるとはいえない。

今後それらの分析を行うとともに、背後要因や根本原因の特定を円滑に行うための手順や体制についても、情報システムの特殊性を考慮した上で整備する必要があると思われる。

＜参考文献＞
[1] 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，経済産業省，2009 年
[2] システムおよびソフトウェアに課せられたリスク抑制の完全性水準（JIS X0134:1999）