ソフトウェアの品質とリスク（続編）

2013年8月17日（土）

航空運航システム研究会（TFOS.SG)
航空システム部会　　松田　宏

紹介した事例のその後の動き
（東証株1円売りによる損害賠償裁判）

- H17年12月、みずほ証券は東証マザーズ新規上場のジェイコム株の「61万円で1株売り」を「1円で61万株売り」と誤入力。
- 買い注文が殺到してシステム障害が起き、取り消し注文が受けつけられず、約10分間で400億円超の損失が出た。
- みずほ証券は東証に415億円の損害賠償を求め、H21年12月、東京地裁は東証に107億円の支払いを命じた。
- みずほ証券はこれを不服として控訴。控訴審では和解協議も行われたが合意にいたらなかった。
- 東京高裁はH25年7月24日、107億円の支払いを命じた一審判決を支持し、控訴を棄却。

（注：東証は責任を認め、利息を含む132億円を支払い済み）

本日の話題

- ソフトウェア障害の特徴
- ハードウェアの多重化
  - 参考：多重化による信頼性向上
  - ソフト障害にハード多重化は無意味
- ソフト不具合の机上シミュレーション
  - 米証券取引所でシステム障害が頻発
  - 米航空会社でもシステム障害が頻発
  - 航空機搭載システムが故障したら
  - 運航管理システムが故障したら
  - 航空管制システムが故障したら
- システム障害による損害
  - ソフト品質への投資の損得勘定
  - 航空システム開発費の問題点

ソフトウェア障害の特徴

- ハードウェア（機械系、電気系）のような予兆がなく、障害は突然起きる。
  - 異常音、温度上昇、性能低下などの機能的変化
  - 摩耗、変形、ヒビ、錆などによる外見上の変化
- 物理的な劣化がないので、定期点検や部品交換などによる予防保守ができない。
- 一定条件を満たせば必ず障害が起こる不具合が未発見のまま隠れている。
  - 特定データの組合せ
  - 処理の条件またはタイミング

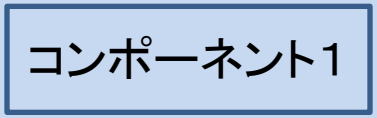
ハードウェアの多重化

（障害はランダムに発生するという前提）

- 多発式の航空機は、エンジンのひとつが故障しても残りのエンジンで飛行が可能。
- 計器飛行する航空機は、航法計器、通信装置、監視装置の２重化が義務づけられている。
- 金融機関など社会的に重要なICTシステムは、構成機器やネットワークの二重化が義務付けられている。
- 一定以上の旅客機などでは2名のパイロットの乗務が義務付けられている。
- 昔は外交使節として正使と副使の２名を派遣した。

参考：多重化による信頼性向上

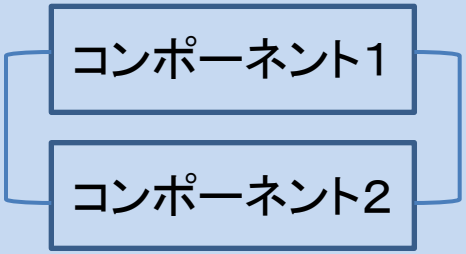
＜単一構成の場合＞



MTBF　=1,000H
MTTR　=　1H

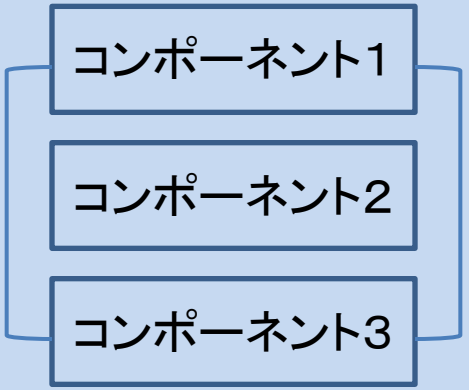
（稼働している確率）
0.999
（故障している確率）
0.001
=1,000時間に1回

＜二重化した場合＞



（少なくても一方が
稼働している確率）
0.999999
（両方同時に故障する確率）
0.000001
=100万時間に1回

＜三重化した場合＞



（最低1台が稼働
している確率）
0.999999999
（すべてが同時に
故障する確率）
0.000000001
=10億時間に1回

(注1)　故障は互いに独立で、ランダムに発生
すると仮定した場合（実際とは異なる）。
(注2)　多重化すると制御等が複雑になるため、
実際の信頼性はこれよりも低くなる。

余談：一回り小さな予備システムも

- 侍は大小二本の刀を持ち歩いた。小刀は大刀が折れた場合などに戦い続けるための予備となる。

- 遭難時に備え船舶は最小限の水と食料、通信機を搭載した救命ボートを準備している。
- 金融機関は、週末や夜間に機能を限定した予備システムを運用している。

ソフト障害にハード多重化は無意味

- ソフト不具合による障害はすべてのハードで同じように起きるので、ハードの多重化は無意味である。
  - 事例1： スペースシャトル初号機は制御コンピュータを5台も搭載していたが、ソフト障害で打上を1カ月延期した。
  - 事例2： 新規開発した航空機の試験飛行中、4基のエンジンが同時に停止した。制御ソフトの変更が関係か？
- ソフトの多重化は費用と時間の関係で困難だが、ハードの信頼性が向上すれば必要性が高まる。
- 障害時には修正前の古いソフトに戻すという方法は広く採用されている。修正直後の障害が多いため。

ソフト不具合の机上シミュレーション

- 米証券取引所でシステムの障害が増え、稼働前の試験が不十分だと問題になっている（詳細後述）。
- 米航空会社で合併時に予約システムの障害が多発し、欠航などで多額の損失を出している（詳細後述）。
- 航空運航関係でもソフト依存度が高まっており、ソフト不具合による障害の可能性が高まっている。
  - 航空機搭載システム（装置制御系、情報管理系）
  - 運航管理／支援システム
  - 航空交通管理／航空管制システム

⇒ソフト障害によって何が起こるか考えてみる。

米証券取引所でシステム障害が頻発

- 2013年４月：CBOEでソフト不具合によりオプション取引が約３時間半停止。
- 2012年8月：米証券仲介ナイト・キャピタルで誤発注。損失は約４億4000万ドル。
- 2012年5月：ナスダック市場でフェイスブック上場時に取引障害。補償6,200万ドル。
- 2012年3月：BATSグルーバルでアップル株が急落。
- 2010年5月：大量の売注文でダウ平均が一時1000ドル近く下げる「フラッシュ・クラッシュ（瞬時の急落）」

（出典：日本経済新聞　2013.05.13）

米航空会社でもシステム障害が頻発

- 2013年4月16日にアメリカン航空の予約システムで障害が発生し、1,950便が欠航ないし遅延。
- 2012年にユナイテッド航空とコンチネンタル航空が業務提携し、システム統合したが、機能不全が発生。米国全土の空港で大混乱が起きた。
- 2011年にユナイテッド航空の予約システムがネット接続の不具合で停止。大規模な欠航と遅延が発生。
- 2005年にUSエアウェイズとアメリカウェスト航空が合併した際も、ソフト統合で同様のトラブルが発生。

（出典：Wired）

余談：航空機のソフト依存度が増大

最初の飛行機
＝機体＋エンジン

大昔の飛行機
＝機体＋エンジン＋電気系
＋通信／航法装置（ADF等）

昔の飛行機
＝機体＋エンジン＋電気系
＋通信／航法／監視装置
＋自動制御装置（アナログ）

今の飛行機
＝機体＋エンジン＋電気系
＋通信／航法／監視
システム（FANS-CNS)
＋自動制御装置（デジタル）
（コンピュータ＋ソフト）

航空機搭載システムが故障したら？

- エンジン/燃料停止：　エンジン停止（＝停電）、墜落
- 飛行制御（操縦系）：　飛行継続困難、失速、墜落
- 飛行管理（FMS)：　コース／高度／速度逸脱、失速、墜落、地表／障害物への衝突
- 通信(C)：　情報入手不可、空中衝突、救難捜索困難
- 航法(N)：　コース逸脱、空中衝突、地表／障害物への衝突
- 監視(S)：　コース逸脱、空中衝突、地表への衝突

⇒　<u>重大インシデント、事故</u>

運航管理システムが故障したら？

- 飛行計画作成：　手作業移行により大幅に遅延。
  不慣れな手作業により誤りの発生。
  - 重量バランスのミス
  - 燃料搭載量のミス
  - 情報伝達ミス（FMS DBなど）
- 運航状況監視：　処理能力低下により把握度低下。
  緊急時への対応能力の低下。
  - 気象条件の急変
  - 飛行中の機体トラブル

⇒　欠航、遅延、インシデント／（重大インシデント）

航空管制システムが故障したら？

- システム停止（直後）：空中待機、出発取止め、
  ニアミス、空中衝突、
  地表／障害物への衝突
  （継続）：マニュアル管制（間隔拡大）
  ⇒取扱可能機数の大幅低下
  ⇒欠航、遅延
- システム誤作動：　ニアミス、空中衝突、
  地表／障害物への衝突

⇒重大インシデント／事故

システム障害による損害

- 大幅な欠航、遅延が起きた場合
  - 旅客宿泊費など
  - 運賃収入の機会損失
  - 機材の減価償却／資産税／乗員人件費、駐機料など
- 航空事故が発生した場合
  - 人命補償　（遺族交通／宿泊費、見舞金、補償金（新ホフマン方式）、慰謝料など）
  - 医療費（入院/治療費、搬送費用、見舞金、補償金など）
  - 機体（保険金で損害補填）
  - 事故処理費用

ソフト品質への投資の損得勘定

- 携帯電話／スマホ
  　ソフト不具合が発見され、膨大な数の製品をリコールする例が後を絶たない（発火／感電の危険も）。
  ⇒　新製品開発合戦の弊害。品質向上は必須条件。
- 自動車業界
  　米国でトヨタ車のアクセル電子制御の不具合が指摘され売上が激減したが、第三者機関としてのNASAの調査で問題ないことが判明。
  ⇒ 事実よりも品質に対する信頼が収益を左右。

航空システム開発費の問題点

- 航空機は数が少なく、システム当たりの開発費負担が大きいので高価（自動車は数が多いので、カーナビやレーダー衝突防止システムを安価に提供）。
- 運航管理システムは多数の航空会社がJeppesenなど同じシステムを採用。多様な運用ノウハウを取込んだ標準システムは、コスト対効果が大きい。
- 複数の航空交通管制システムが市販され、各国で使われている。米国の規模なら開発費をペイできても、わが国では独自開発の負担は過大では？