障害事例に学ぶソフトウェアの品質とリスク

平成25年6月29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

本日の話題

- 航空における情報・通信技術(ICT)
  (ICT: Information & Communication Technology)
- 情報・通信システムのソフトウェア
- ソフトウェアの品質
- システム障害の類型
- 事例研究
- 「失敗学」の視点
- システム障害のリスク
- まとめ

航空における情報・通信技術

- 現在、情報・通信技術は、多くの航空システムで利用されている。
  - 航空機搭載システム:
    - 組込型制御システム (例:エンジン制御、飛行制御、等)
    - 管理システム (例:飛行管理 (FMS), 通信管理(CMU), エア・データ計算 (ADC), 等)
    - 通信/航法/監視 (CNS) システム
  - 地上系システム:
    - 運航支援システム (例:運航管理、整備保守、等)
    - 航空交通業務 (例:情報、交通管制/管理、気象、捜索救難、等)
    - 通信ネット (例:ATN, 対空通信(音声/データ)、衛星通信等)

操縦室

航空交通管制

エンジン制御

飛行管理
システム(FMS)

航空交通管理

衛星通信

情報・通信システムのソフトウェア

- 情報・通信システムは次の３種類で構成される。
  - ハードウェア: 処理装置, メモリ、入出力装置
    - 「蓄積プログラム」方式 (von Neumann型)デジタルコンピュータ
    - 超LSI(Very Large Scale Integration : VLSI)を使用（超小型、安価）
    - VLSI上のトランジスタ数は18カ月毎に2倍になる（ムーアの法則）
  - ソフトウェア: プログラム、データ、運用マニュアル等
  - ネットワーク: 高速デジタル通信
- プログラム・コード数は「天文学的」に増加。
  - 自動車: 7,000,000 (カーナビを除く)
  - 携帯電話: 10,000,000
  - 都市銀行: 100,000,000

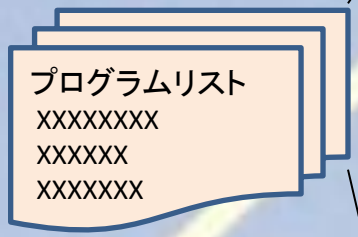
ハードウェア

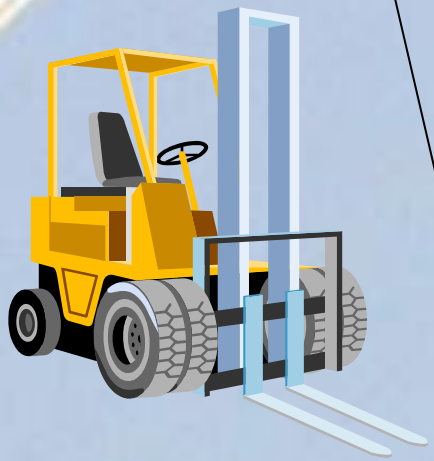
プリント基板上
のVLSI

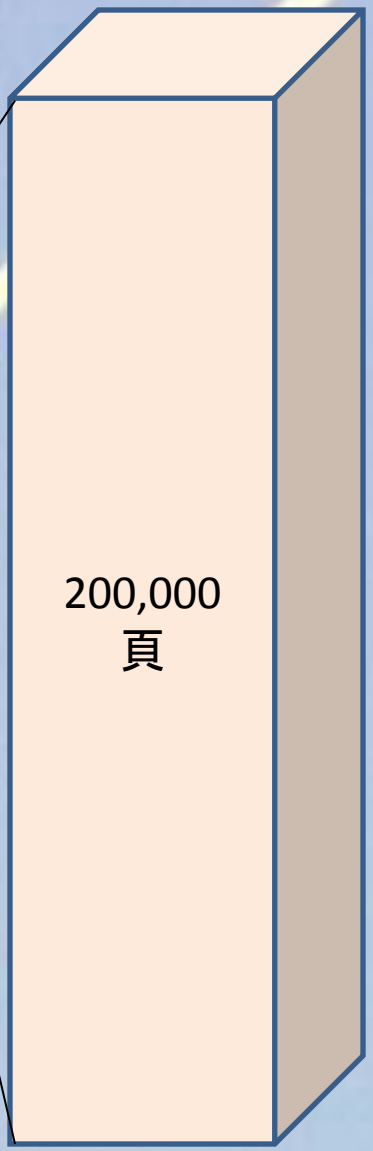
プリント基板用コネクタ

ソフトウェア

1，000万ステップの
プログラム・リストを
50行/頁で印刷すると







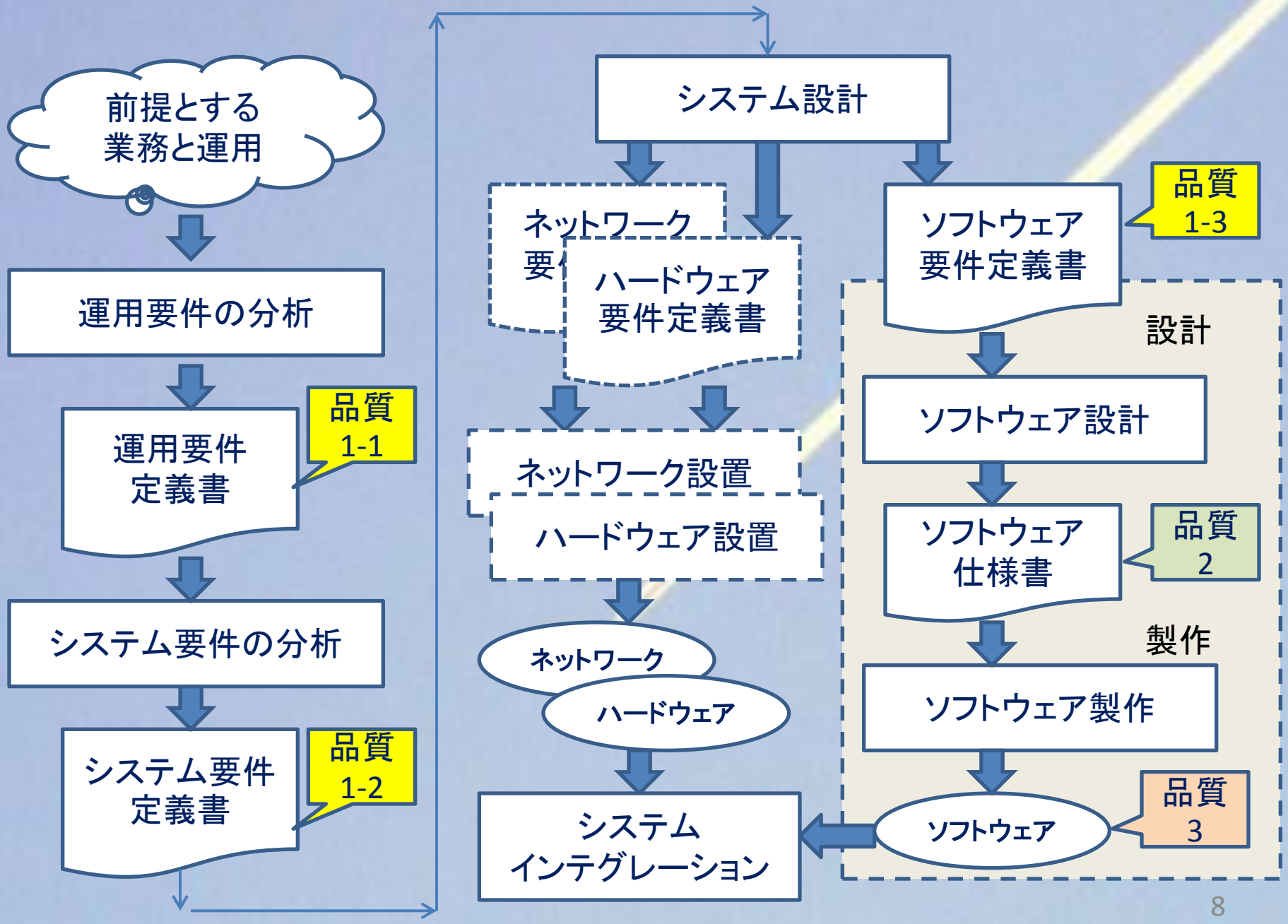
ソフトウェアの品質

- ソフトウェア品質には次の3つの側面がある。
  1. 「要件定義」品質
  2. 「設計」品質
  3. 「製造」品質
- ソフトウェアは他とは全く異なる製品である。
  - アルゴリズム（演算論理）とデータから成る（形も重さもない）
  - 柔軟。MTBFや MTTRなどの指標はふさわしくない
- ソフトウェアは複雑すぎて全ての検証は困難。

  n個からm個を取り出す場合の組合せの数

$$ {}_nC_m = \frac{n \times (n-1) \times \cdots \times (n-m+1)}{m \times (m-1) \times \cdots \times 1} $$

- 「誤りを犯す」人間が要件を定義し、設計し、製作するため、「完璧」なソフトウェアはあり得ない。


前提とする
業務と運用
運用要件の分析
運用要件
定義書
品質
1-1
システム要件の分析
システム要件
定義書
品質
1-2
システム設計
ネットワーク
要
ハードウェア
要件定義書
ネットワーク設置
ハードウェア設置
ネットワーク
ハードウェア
システム
インテグレーション
ソフトウェア
要件定義書
品質
1-3
設計
ソフトウェア設計
ソフトウェア
仕様書
品質
2
製作
ソフトウェア製作
ソフトウェア
品質
3

システム障害の類型

- 公開情報により、典型的なICTシステム障害事例を定性的に分析した。
- 参考になる他業界の事例も含む。
- 事例は原因により次の類型に分類した。

  タイプ-1: 単純なソフトウェアの「バグ」

  タイプ-2: 設計時の考慮不足（ソフトウェア単独）

  タイプ-3: 設計時の考慮不足（ハードウェアが関係）

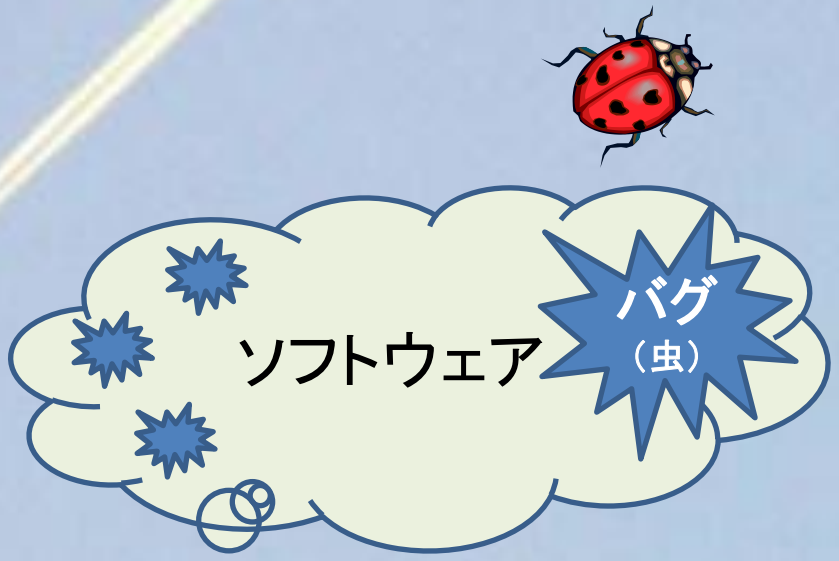
  タイプ-4: 不十分なシステム要件定義

  タイプ-5: 不適切な運用条件の想定

  タイプ-6: その他 (操作ミス、インフラ障害、等)

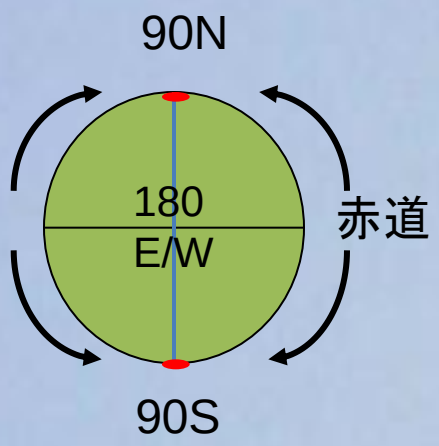
タイプ-1: 単純なソフトウェアの「バグ」(1)

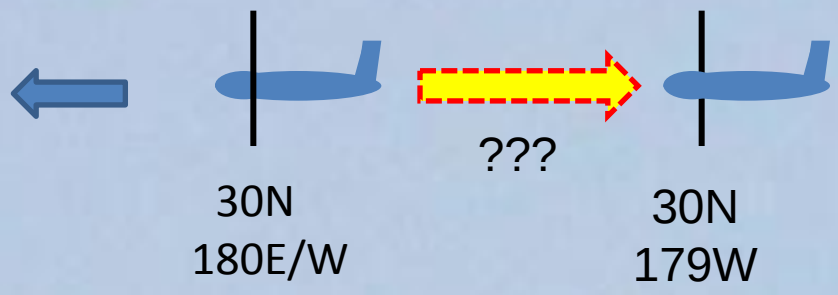
- 航空路管制レーダー・データ処理 (RDP)システムが障害により停止した(2004年4月8日19:11JST)。
  - 国内線の130便が30分以上遅延した。
  - 原因は飛行計画の異常データ処理に関するソフトウェアの不具合。



タイプ-1: 単純なソフトウェアの「バグ」(2)

- 西行フライトで180E/Wを通過した際、FMSが現在位置を　180S180W　と表示した。
  - この誤った値はプログラムの初期値で、原因はプログラムのミス。
- 西行フライトで180E/Wを通過した際、FMSが現在位置を 30N179W と表示した。
  - 内部的な計算結果は 30.00N179.99W　であった。
  - 原因は「度⇒分」の換算ミスで、0.99 度分が脱落した。





タイプ-2: 設計時の考慮不足（ソフトウェア単独）

- ニュージーランドのアルミ工場で、全ての溶融炉が停止した（1996年12月31日）。
  - 原因は「うるう年」の 366日目が考慮されていなかった。
  - 約100万ニュージーランド・ドルの損害が発生した。

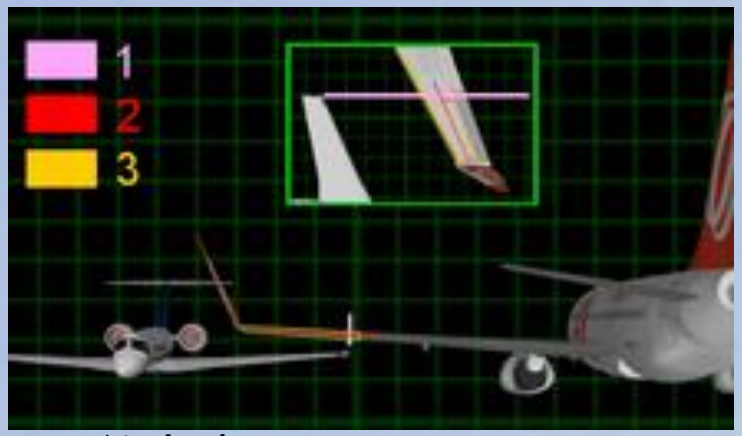
- 航空管制飛行計画データ処理(FDP)システムが停止した（2003年3月１日　0700 JST）。
  - 215 便が欠航し、1,500 便が大幅に遅れ、30万人の乗客に影響。
  - 原因は、統計プログラムと防衛庁通信プログラムの競合。
  - 設計段階でこの種の競合の可能性を想定していなかった。

タイプ-3: 設計時の考慮不足（ハードウェアが関係）

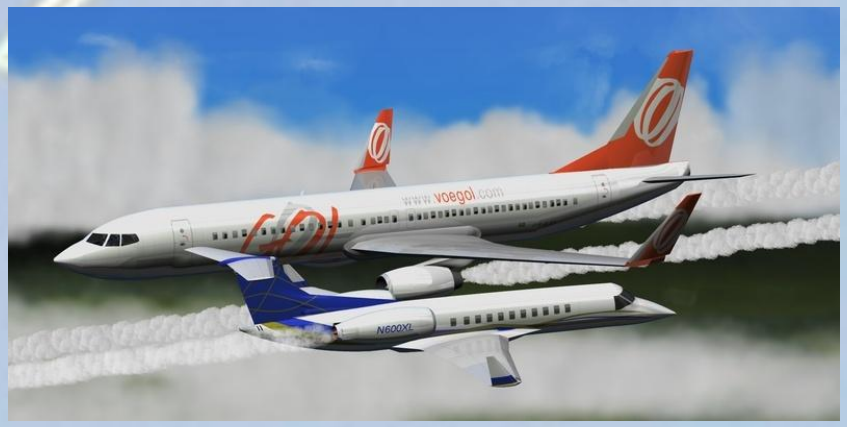
- 東京証券取引所の金融派生商品取引システムが停止した（2012年8月7日）。
  - 最初の原因はネットワーク切替装置（スイッチ）の障害。
  - 予備スイッチへの切替ソフトウェアに不具合があった。
- KDDIの交換システムの性能が大幅に低下し、携帯電話がつながらなくなった（2012年1月25日）。
  - 最初の原因はメモリ不足の検出（実際には十分な予備メモリが残っていたのに警報が出た）。
  - 予備メモリを使うためのソフトウェア機能が準備されていなかった。

タイプ-4: システム要件の不適切な定義(1)

- ゴア航空のB737-800とエクセル航空のエンブライエル・レガシー 600が空中衝突（2006年9月29日）。
  - 両機はブラジル上空の同じ経路を同じフライトレベルで飛行。
  - エンブライエルは近くの空港に緊急着陸したが、B737-800 は空中分解して落下。乗員乗客154名は全員死亡した。
  - 原因のひとつの可能性として、管制システムの混同されやすい高度（FL）表示が指摘されている（飛行計画の要求FLと管制官の指示高度）が指摘されている）。



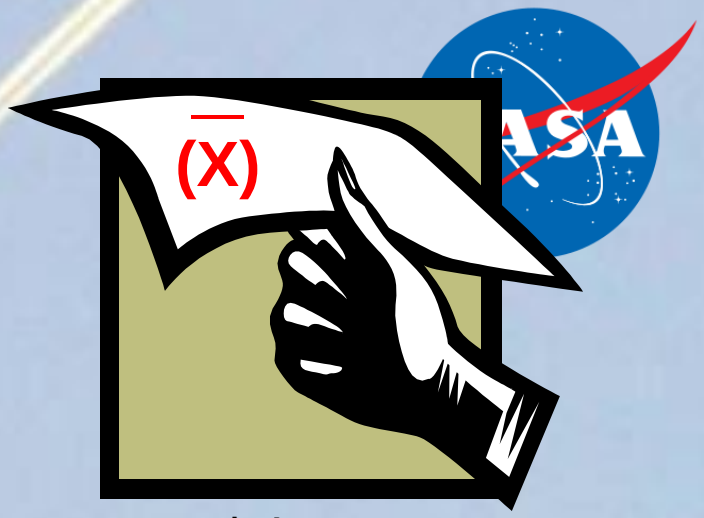
衝突時のシミュレーション


空中衝突時の想像図

タイプ-4: システム要件の不適切な定義(2)

- マリナー1号ロケットは打上げ後にコースを外れ、293秒後に指令爆破された（1962年7月22日）。
  - ロケット設計者は、飛行コース制御の計算式を手書きのメモでプログラマに渡した。そこには、レーダ測距データ“x “は平準化して使うようにと、“x “の上に「バー」が書いてあった。
  - プログラマは「バー」の意味を理解せず、平準化処理なしの間違ったFORTRANプログラムを書いてしまった。

マリナー1号の打上



手書きのメモ

タイプ-5:不適切な運用要件の想定 (1)

- みずほ銀行の勘定系システムが停止し、ATMが3日間使えなくなった（2011年3月19～21日）。
  - 東日本大震災の被災者に対する膨大な数の見舞金が特定口座に集中して振り込まれた。
  - システムは振込件数を無意味な小さな数に制限していた（それを誰も知らなかった）ため、多数の未処理データが滞留し全体が停止した。
  - 膨大な手作業が必要で、復旧処理が翌朝までに終了できなかった。
  - 未処理データがあると時間的な前後関係が保てないため、翌朝のオンライン処理が開始できなかった。未処理データはさらに蓄積した。

ATM サービス

多数の見舞金の振込

前後関係の制約

タイプ-5:不適切な運用要件の想定 (2)

- 東京証券取引所のシステムがオーバーフローして取引ができなくなった（2006年1月18日）。
  - システムの処理容量が過小で、拡張性もなかった。
  - ライブドア株が額面金額を1/100に分割したため株数が増え、話題性もあったため売買が急増した。

1 株

分割

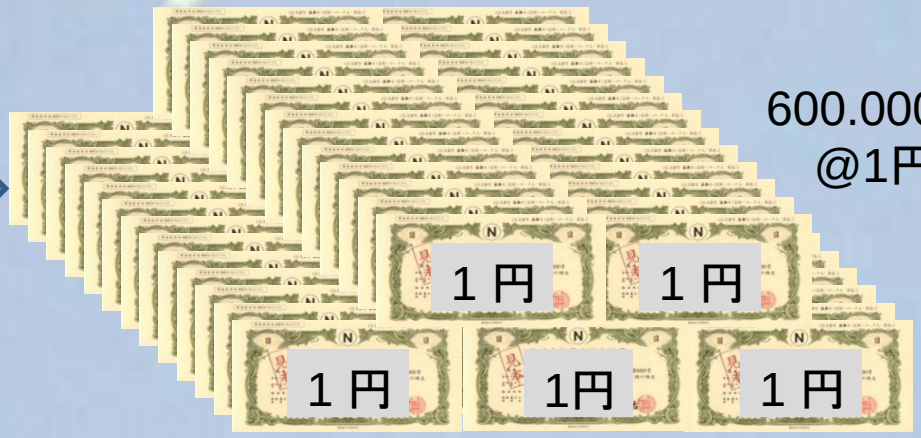
100 株

タイプ-6: その他 (誤入力、インフラ障害等-1)

- 売り注文の入力ミスで東京証券取引所(TSE)のシステムがオーバーフローし、多額の損失を出した(2006年12月8日)。
  - みずほ証券が、1株を600,000円でという売り注文を、600,000 株を1円でと誤入力した。システムの確認要求メッセージは無視された。
  - この超格安の売りに対して膨大な数の買い注文が殺到し、TSE のシステムがオーバーフローした。そのため、みずほ証券は誤入力に気付いたが訂正できなかった。電話での取消要求は拒否された。
  - みずほ証券は414億円の損害賠償訴訟を起こし、係争中。TSEは責任の一部を認め、みずほ証券に132億円を仮払い済み。

1株を
600,000円で

誤入力



600.000株を
@1円で

タイプ-6: その他 (誤入力、インフラ障害等-2)

- 東京国際空港（当時。現在は羽田国際空港）の管制システムに対する電力供給が停止した（2005年8月2日）。
  - 定期保守時に切替えミスで電源が蓄電池に接続され、完全に放電した時点で供給が停止した。その後、業務手順が改善された。
- 気象衛星センターでスーパーコンピュータの冷却系統に不具合が発生し、温度上昇で全機能を停止（2013年2月5日）。
  - 原因は冷却系統の制御システムの設定ミスで、誤って系統全体に停止命令を送ってしまった。

羽田国際空港の管制塔
新 (左) & 旧 (右: 当時)

気象衛星センターの
新スーパーコンピュータ

演算性能:
847TFLOPS

「失敗学」の視点

- 「失敗学」は工学／経営学を網羅する新しい学問
  - 2000年代初期に畑村洋太郎教授が提唱し、学会を設立。
- 「失敗学」は、多くの学生が実験室で似たような失敗を繰り返すという現象の解明から始まった。
- 「失敗学」では、
  - 織込済み、チャレンジの結果、回避可能な失敗に大別。
  - 同じような原因で同じような失敗が繰り返される場合は予測と回避が可能であると考える。
  - 次の3つから構成されている。
    - 原因分析（Cause Analysis：CA）
    - 失敗予防（Failure Prevention：FP）
    - 知識配布（Knowledge Distribution：KD）

システム障害のリスク

- システム障害リスクの種類
  - 直接的損害： 生命、財産の喪失
  - 間接的損害： 業務の混乱／遅延、機会損失、リコール、営業停止
  - 無形の損害： 信用失墜、顧客離反
- 的確な想定が難しく、あまり行われていない。
  - 定性的な想定： どのような損害が起こり得るか
  - 定量的な想定： どの位の損害が発生するか
- 事業継続計画（Business Continuity Plan: BCP）
  - 起こり得る事故/災害の種類と損害規模の想定
  - 具体的な対応策の立案。ただし無限大の対策は求められない。
- 結果が予知可能で対応なければ刑事責任？
  - 意図的に「控え目な想定」に抑えている場合が多い？

まとめ

- 障害原因の多くに共通性があり、過去に度々繰り返され、単純で初歩的で修正が容易なものが多い。
- 過去の同様の事例を知っていれば予測し、回避できたと思われる障害が多い。
  - 「想定外とは無知と怠惰の言い訳である」（吉村　昭）
- 他分野を含め、もっと過去から学ぶべきでは？
  - 古い事例も新技術システムの似たような障害の予防に役に立つ。
  - 他分野の事例の多くは航空システムにも良い参考になる。
- 利用者と技術者はもっとコミュニケーションを！
  - 「専門家は自分の分野の全てを知っているが、他は何も知らない」
- 起こりそうなことは可能な限り想定しておこう！

ご清聴ありがとうございました。