第 2 章　ソフトウェア危機の例

ソフトウェア危機についての報告

第 1 章で、現時点でのソフトウェア危機の症状は、次の 4 つの形で表れると述べた。

- 開発した製品の品質が悪い。
- 開発が、当初に立てたスケジュールから遅れる。
- 開発費用が、当初の予算を超過する。

さらに、

- 開発プロジェクトが、最終の製品を作り出す前に解散させられる。

これらが原因となって、結果としてうまくゆかなかったソフトウェア開発の数は、残念ながら非常に多い。そしてそれらについての報告も、数多く発表されている。

例えば日経コンピュータ誌では、創刊以来断続的に「動かないコンピュータ」と銘打った記事が掲載されている。ここに掲載される全てのものが、ソフトウェア工学の立場での失敗例ではない。しかし、この立場から反省するべきものは多い。その主なものをまとめた単行本も、発行されている［NIK02b］。2002 年（平成 14 年）4 月に起きたみずほ銀行のシステム障害についての報告もある[NIK02a]。2005 年 12 月に起きた東京証券取引所の注文取消に関わるケースは、当時マスコミなどに大きく取り上げられた[1]。

アメリカでも、ACM（Association for Computing Machinery）というコンピュータ関係の学会が発行する雑誌の 1 つである「Software Engineering Notes」誌にも、毎号同様の記事が掲載されている。さらにそれから抽出した記事をまとめた単行本もある。この本には、これらのコンピュータの障害で次のようなことが起きたと報告されている[NUE95]。

- 列車が正面衝突した。
- 飛行機が墜落した。
- 人工衛星が行方不明になった。
- 原子炉から放射能漏れが発生した。
- 建物が倒壊した。
- 医療機器のトラブルで人が死んだ。

インターネットでも、そのような事例が掲載されたサイトを簡単に探すことができる[2]。

デンバー国際空港の手荷物取り扱いシステム

それらの多くの失敗事例の中で、このほとんど全てのソフトウェア危機の症状が表れた典型的な例が 1 つある。アメリカのデンバー国際空港の手荷物取り扱いシステムである。第 2 章では、このシステムの開発の経緯を追うことで、現時点でのソフトウェア危機がどういうもので

---

[1] この件は裁判になり、2009 年（平成 21 年）12 月に東証に 100 億円強の支払いを命じる東京地裁の判決が出た。しかし原告側が判決を不服として上告し、2013 年（平成 25 年）7 月 24 日に東京高裁の判決が出た。結果は、地裁の判決を支持するというものだった。そのため原告側がその判決も不服として最高裁に上告し、2015 年 9 月 3 日に最高裁の判決が出た。高裁の判決を踏襲するという内容だった。これで 10 年に及んだ裁判が決着した。しかし私はソフトウェア技術者として、この一連の裁判所の判断は間違いであると考えている。

[2] 例えば、google を使って「システム障害」というキーワードで「日本語のページ」を検索すると、約 433 万件件がヒットする。「system trouble」をキーワードにしてウェブ全体で検索すると、なんと 2 億 9200 万件がヒットする。（2017 年 1 月 3 日現在）

あるかを、改めて確認しておきたい。

ソフトウェア開発の失敗が、その経緯や内容まで詳細に公表されることは、たいへん珍しい。ソフトウェアの開発がうまく行かなかったということは、当事者にとって恥ずべき事柄であって、胸を張って世間に公表するようなものではない。だからこのシステムが一企業内のシステムであったなら、ここまでその内容がオープンになることはなかっただろう。しかしこのシステムは国際空港という公の設備に関連したものであり、このシステムの完成が遅れたために空港の開港も大幅に遅れてしまった。そのためマスコミも地方公共団体も、このシステムに大きな関心を寄せた。それがこのシステムの開発について、詳細な内容や経緯を入手できることにつながっている。

この章の基になる情報を、私はインターネットで入手した。何の検索エンジンを使ったかは忘れたが、「DIA（Denver International Airport）」をキーワードにして検索し、その結果をチェックしている間にこの情報を見つけた。これは、アメリカのカリフォルニア・ポリテクニック州立大学（California Polytechnic State University）で、ダニエル・スターンズ（Daniel Stearns）先生の下で勉強していたコンピュータ・サイエンス学部の学生マイケル・シュロー（Michael Schloh）氏の卒業論文のように見える[SCH96]。

以下は、その論文の要約である。インターネットで公表されている資料であるから、ここでの引用にシュロー氏の許可を必要とするとは、私は考えていない。それでもシュロー氏には、私が行おうとしていることを伝えたいと考えた。しかしシュロー氏への直接のコンタクトの方法が分からないため、ここにその要約を引用することについての連絡を、私はスターンズ先生に電子メールで行った。先生からの返事は、届いていない。

計画の発端

アメリカ中西部のコロラド州にあるデンバー市には、スタプレトン（Stapleton）国際空港があった。しかし 1980 年代半ばに、新しいデンバー国際空港の建設プロジェクトがスタートした。スタプレトン空港は構造上の問題を持っており、それを改善するより新しい空港を作る方が容易と考えられたこと、21 世紀に向けての航空機による旅客需要の増大に対応するためには、スタプレトン空港は適切ではないと考えられたこと、などがその理由だった。つまり新しいデンバー国際空港建設は、「21 世紀のための空港建設で、国家にとっての欠くべからざる投資」と考えられていた。

手荷物取り扱いシステムの自動化

建設プロジェクトのスタートからまだ間がない 1991 年に、ユナイテッド航空はデンバー国際空港での同社の手荷物取り扱いシステムを自動化するため、BAE 社[3]と契約を交わした。自動化された手荷物取り扱いシステムはこれが世界最初のものというわけではなく、それまでにサンフランシスコ国際空港、フランクフルト国際空港、ミュンヘン空港ですでに稼働していた。ユナイテッド航空はその後、このシステムを同社単独のものとするのではなく、デンバー国際空港全体をカバーするものにすることを提案した。

デンバー市当局は当初、この空港を使う全ての航空会社はそれぞれのニーズに基づいて、独自の手荷物取り扱いシステムを構築するだろうと考えていた。しかし各航空会社のその後の動

[3] 本社はテキサス州キャロルトン（Carrollton）に所在。以前は Boeing Airport Equipment という社名だった。

きを見、さらにしばらくの検討の時間をとって、空港全体に自動化された手荷物取り扱いシステムを導入することが他の航空会社にもメリットをもたらすと考え、ユナイテッド航空の提案に同意した。デンバー市当局は BAE 社の力を借りて、このシステムの仕様を作成した。

手荷物取り扱いシステム自動化の必要性

デンバー国際空港で手荷物取り扱いシステムを自動化することが必要な理由として、以下のものをあげることができる。

まず一般的な理由として、タグ（動力付きの車。連結した多数のカートを引っ張り、人が運転して先頭を走る）とカート（手荷物を乗せて運ぶ車。タグに引かれる）を使った従来型の手作業によるシステムは労働集約的であり、運用の費用が割高なものにつくことがあげられる。

さらにデンバー国際空港独自の理由として、以下のようなものがある。

手荷物取り扱いシステムの対応方法が決まる前に、空港全体の構造や、ビルディングなどの主な建造物とそれらをつなぐトンネルの概要などが決まってしまい、手荷物取り扱いシステムはそのトンネルをそのまま使わざるを得なかった。タグにはディーゼル・エンジンが付いているが、この排気ガスのために空調のよくないトンネル内で運転者や他の作業者を窒息させる恐れがあった。さらに狭いトンネルの中に多くのタグやカートが集まると、ひどい渋滞を引き起こす恐れもあった。

またこの空港は他の空港と比べてたいへんに大きく、ものを運ぶスピードが何にも増して重要だった。空港のエプロンに従来のタグとカートで手荷物を運ぶのに、50 分が必要と考えられた。航空会社は、飛行機が地上で手荷物を待っていることで利益を上げるのではなく、大空を飛ぶことで利益を上げる。ユナイテッド航空をはじめ航空各社は、この自動化システムに期待した。

BAE 社が作成した概念と仕様

BAE 社が作成したシステムの概念は、以下のようなものであった。

- 「狭くて長いトンネル」というような、上で述べたデンバー国際空港での制約下で稼働し、人手の作業をほとんど必要としない。
- 手荷物が移動中でも、その所在を常に明確にすることができる。
- 完全に自動化されるので、ほとんどの場合手荷物は、飛行機から降ろされた後手荷物引き取り所でその持ち主に会うまで人間を見ることがない。
- さらにシステムのスピードは空港内の高速列車をしのぎ、旅行者が手荷物引き取り所に着いたとき、手荷物はすでにそこで持ち主を待っている。

このシステムは、他の空港の自動化された手荷物取り扱いシステムと比べて、たいへん規模が大きく、複雑であるという特徴を持っていた。サンフランシスコのシステムと比べると、デンバーのシステムは規模で 10 倍、スピードで 14 倍の違いがあった。フランクフルトと比較しても、デンバーは規模で 3 倍大きかった。

デンバーのシステムでは、従来のコンベア・ベルトに代えて「遠隔操縦の車（テレカー）」を使うことになった。テレカーは直列モータで動き、荷物を乗せたものは時速 4.5 マイル（7.2km）、何も乗せていないものの中には時速 19 マイル（30.4km）のスピードで動くものもあった。各線路は 1 分間に 60 台のテレカーを通過させることができ、各空港ターミナルと 3 つあるコンコースの間を 9 分以内に結ぶことができた。その結果、1 分間に 1,000 個の手荷物を取り扱う

ことができた。

このシステムは、8 つのコントロールルームに設置された 486[4]ベースのコンピュータ 300 台と、光ケーブルを使った高速イーサーネット、そのための 1,400 万フィートのワイアリング、56 台のレーザー読みとり装置、3,100 台の普通のテレカーと、450 台の大型のテレカー、10,000 個のモータなどから構成され、その規模はパナマ運河や英仏海峡トンネルに匹敵するといわれた。

手荷物取り扱いのプロセスは、以下のようになっている。

- チェックインの時係員は、持ち主の氏名、航空会社と最終目的地、フライトナンバーなどを記入したバーコードラベルを手荷物に貼り付け、その手荷物をコンベア・ベルトに乗せる。
- システムにはテレカーの所在を管理／制御する機能があり、システムが必要な場所に空のテレカーを送り込む。
- 空のテレカーが到着するとコンベア・ベルトは手荷物を前に進め、テレカーのファイバーガラス製のトレイがそれを受け止める。
- 手荷物を乗せるときと下ろすとき、デンバーのテレカーはスピードを緩めるだけで、停止はしない。この方式を使うことで手荷物の取扱量を増やし、消費するエネルギーを節約することができる。
- テレカーがスピードを上げて走り始める前に、レーザースキャナーは手荷物に張られたバーコードラベルを読む。
- この情報は分類用のコンピュータに送られ、フライトナンバーから適切なゲイトを選んで、追跡用のコンピュータがそのテレカーを目的地まで誘導する。
- テレカーは途中で他のテレカーの流れに合流したり、荷下ろしステーションに分岐したりする。1 秒間に何百万のメッセージが移動中の全てのテレカーと追跡用のコンピュータとの間で無線を通してやりとりされて、追跡用のコンピュータは全てのテレカーの動きを把握している。
- 飛行機が出発するゲイトが変更されると、コンピュータは新しい目的地にテレカーを誘導する。

デンバー国際空港では、標準サイズのテレカーに加えて大型のテレカーを用意した。これはスキーやゴルフバッグを運ぶためのものである。

このシステムは、毎日 18 時間、全ての設備が 99.5 パーセントの稼働率で動くように設計された。将来の拡張や予測しない問題に対応するため、必要な冗長性も付加された。手荷物の流れが止まることで空港全体が閉鎖されることがないように、コンピュータは鉄のドアに厳重に鍵をかけた部屋に設置されるなど、厳格な安全対策が施された。

このシステムはオブジェクト指向技法で設計され、OS／2 の下で開発されて、稼働することになっていた。分散処理の方式をとっているので、空港全体の情報システムとは独立して稼働することができた。このシステムが関係を持つシステムは、各航空会社の予約システムだけである。

問題点

[4] インテル社製のマイクロプロセッサの一種。80386 と最初のペンティアムの間に位置するもの。

デンバー国際空港の手荷物取り扱いシステムの開発では、「起こる可能性がある悪いことが全部起きた」といえるような状態になった。問題は広範囲にわたり、深刻だった。

まず、スケジュールの問題があった。当初空港のオープンは、1993 年 10 月 31 日と決められた。この決定はきわめて「政治的」色彩の強いもので、現実的なものではなかった。手荷物取り扱いシステムも、この日までに完成しなければならなかった。BEA は後で「開発期間として、当初のスケジュールで与えられたものの 2 倍が必要だった」と述べている。ミュンヘンの当局はデンバーに、「テストのために充分な時間と資源を確保する」ようにアドバイズした。ミュンヘンのアドバイズは、彼らがテストの期間に 2 年をとり、開港前にシステムの 24 時間フル稼働を 6 ヶ月間続けた実績に裏打ちされていた。しかしこのアドバイズは、聞き入れられなかった。このタイトなスケジュールが、システム全体の複雑さについての理解不足や基本的な部分での計算間違い、開発の仕事を小さく見積もったこと、などに結びついた。

次に、当初の仕様についての妥当性の問題があった。BAE 社の仕様は、技術的にたいへん進んだものだった。手荷物取り扱いシステムとして、「次の世代のもの」というより、第 3 世代からいきなり第 5 世代にジャンプしたようなものだった。BAE 社は、この進んだ技術ですばらしいパフォーマンスも実現できると考えた。しかし不幸なことに、これは間違いだった。

仕様変更の問題もあった。BEA は、当初の仕様が固まった後は、仕様変更はないものと考えていた。しかし開発が始まってから、デンバー市当局は BAE 社や航空会社に相談することなく計画や予定を変え、仕様を変更した。航空会社からの仕様変更も続出した。システムの一部を変更した場合に、その影響が及ぶ範囲の把握も不十分だった。

1994 年 3 月に、BAE 社はパフォーマンステストのために手荷物取り扱いシステムを初めて動かした。この試行は、テレビや新聞社に公開されていた。1994 年 3 月とは、1993 年 10 月の当初の開港予定日からさらに半年近く遅延している。しかしその結果は、惨憺たるものだった。スーツケースはテレカーから投げ出されて壊れ、折り重なって線路を塞いだ。衣類や個人の持ち物が空を飛び、多くのテレカーも脱線して、お互いを壊しあった。間違った場所に手荷物を降ろしたテレカーもあった。

この結果について、5 月はじめに BAE 社の社長は、「システムが壊れたわけではない。テストがまだ充分になされていないだけだ」と述べた。8 月になってもシステムは、まだひどい状態だった。従来方式のタグとカートによる代替システムの計画が進んでいる間も、テレカーは衝突し、脱線を繰り返していた。BAE 社は、プログラミングに関わる事項に充分な注意を払っていなかったと非難された。問題を発見し、それを修正し、再テストする時間を過小見積りしたことが、開港を遅らせた主な原因といわれた。

それに対して BAE 社の社長は、「ソフトウェアが主な問題ではない。電気的なものがもっと大きな問題だ」と述べた。実際そちらにも大きな問題が続出した。486 ベースのコンピュータは、ハードウェアもソフトウェアも信頼性が低かった。レーザー・スキャン装置はよくバーコードを読み間違えた。タグのプリンターにも問題があった。テレカーとコンピュータの間の無線通信にも、信頼性の問題があった。さらに、空港全体に電気を供給する電源装置にも問題が発生した。電源の不安定さが、システム全体をシャット・ダウンすることもあった。

既存のシステムとの接続でも問題が出た。ユナイテッド航空の座席予約システムである「アポロ」との情報伝達がうまくゆかなかった。この情報伝達の失敗は、タイミングに起因する。この結果ユナイテッド航空の乗客の手荷物を乗せたテレカーが自動的に行き先を決められず、人間が手作業で送り先を決めるステーションに送られることになった。

1994 年 7 月には、「ライン・バランスの問題」が新たに発生した。これはシステムの負荷が均等に分布せず、システムの一部に集中することから発生する問題である。この問題の特徴は、関連する要素の数が増えるに従って難しさが指数関数的に増えることにある。

システムのパフォーマンスも悪かった。

デンバー国際空港の手荷物取り扱いシステムでは、このように問題が山積した。

解決方法

1994 年 9 月に、BAE 社の親会社はこのシステムをチェックし、当初の設計を見直すために英国のコンサルタントを雇い、自社の技術者も派遣した。さらにデンバー市当局も、悪いところを的確に指摘し、修正に必要な期間を提示できるコンサルタントを捜して、ドイツのコンサルタント会社ログプラン社と契約を結んだ。ログプラン社はフランクフルト国際空港のシステムで、このような仕事の経験を持っていた。デンバー市当局とユナイテッド航空はログプラン社の報告書に従って、このシステムの一部を稼働させるために必要な事項の実施を取り決めた。

まずこのシステム構築の推進が、デンバー市当局からユナイテッド航空に戻された。ユナイテッド航空はシステムの複雑さを軽減し、パフォーマンスを改善することで、このシステムを「稼働」させられるものに変えた。

その過程で、いろんな変更がなされた。まず、各線路は毎分 60 台のテレカーを通過させることになっていたが、これを 30 台に変えた。

システムの対象範囲の縮小もはかられた。当初このシステムが対象としたものは、３つのコンコースでの全ての手荷物だった。これらは、デンバーから出てゆくもの、デンバーに到着するもの、及び単にデンバー国際空港を通過するだけのものに分類できる。最終的にこのシステムが対象としたものは、ユナイテッド航空が使用するコンコース B のみで、しかもデンバーから送り出されるものだけになった。コンコース A と C を含むそれ以外のものは、従来型の手作業によるタグとカートのシステムを新たに構築して、それで対応した。このシステムの構築に、7,100 万ドルを要した。

電気関係の障害も、順次解決された。

開港の延期

すでに述べたとおり、当初デンバー国際空港は 1993 年 10 月 31 日に開港する予定が立てられていた。しかし実際の開港は 1995 年 2 月 28 日になった。16 ヶ月の遅れである。この間の経過は、以下の通りである。

1993 年 3 月 2 日に、デンバー市のウェブ市長は、最初の「開港の遅れ」を発表した。遅延の理由は「多くのシステムのデバッグに要する期間を確保するため」として、新たな開港日として、当初の予定日から 7 週間遅れの 1993 年 12 月 19 日が決められた。

1993 年 10 月 25 日になって、ウェブ市長は 2 回目の遅れを発表した。理由は「航空会社からの変更要求に対応し、クリティカルな空港の情報システムをテストし、さらに航空会社の従業員に充分なトレーニングの機会を与え、消防とセキュリティのシステムを導入するため」とした。新たな開港日は、1994 年 3 月 9 日に決められた。

1994 年 3 月 1 日に、ウェブ市長は 3 回目の遅延を発表した。理由は「手荷物取り扱いシステムのトラブルシュートのため」で、新たな開港日として 1994 年 5 月 15 日が決められた。

1994 年 5 月 2 日に、ウェブ市長は 4 回目の遅れを発表した。「手荷物システムで発生した多

くの問題を解決するため」というのが延期の理由で、今回は開港予定日は示されなかった。

1994 年 8 月 4 日に、ウェブ市長は、新たに空港全体を対象とした従来型のタグとカートによる手作業の手荷物システムを導入すると発表した。

そして 1994 年 8 月 22 日に、ウェブ市長は「デンバー国際空港は 1995 年 2 月 28 日に開港する」と発表した。この期限は守られた。

費用の問題など

この空港全体の建設費は、当初 17 億ドルと見積もられた。しかし実際は、45 億ドルを要した[5]。デンバー市は初めから、この空港の建設費を税金からまかなうことはせず、全額債券を発行して調達した。大幅な予算超過の結果債券市場でのデンバー市の格付けは急落し、デンバー市はジャンクボンド並の利率でなければ資金を調達できないという事態が発生した。デンバー市の破産も心配され、SEC（米国証券取引委員会）などがデンバー市に調査員を派遣した。この負債を返還するため、デンバー国際空港は空港使用料として、各旅客から 20 ドルを徴収している。これは米国の空港の中で、もっとも高い金額である。

システムの開発費は、当初 1 億 93 百万ドルと見積もられていた。最終的にはこれが 3 億 11 百万ドルになった[6]。この費用には、従来型の手荷物取り扱いシステムの構築費も含まれている。

どうすれば良かったのか

前述の通り、1994 年 5 月 2 日にウェブ市長は 4 回目の遅れを発表した。この時、開港予定日は示されなかった。そして 8 月 22 日にウェブ市長は「デンバー国際空港は 1995 年 2 月 28 日に開港する」と発表し、この期限は守られた。

ここからは私の想像だが、1994 年 5 月頃からの 4 ヶ月ぐらいの間、現存する問題点の洗い出し、その解決方法の検討と手順の確定、作業をどの組織が担当するかなどについての検討と調整、決定が精力的に進められただろう。そしてその解決のために 1995 年 2 月までの時間が必要という結論を出して、8 月 22 日の発表につながったと考える。

8 月から開港までの半年間にも、実際はいろんな問題や遅れがあったはずである。しかしそれらを一切表に出さずに宣言通りに開港を実現したことは素晴らしいことであり、その裏にはたいへん有能な SE の存在を感じさせる。リスク管理も、適切になされていたに違いない[7]。

この開発の遅れについての個別の原因を探せば、要件定義のレビューの不充分さ、仕様凍結がなされていないこと、プロジェクトの進捗管理の不充分さなど、多くの項目を挙げることができる。テストも、もっとシステマティックに進めることができた。しかしこのような個別の問題よりも、プロジェクトのマネジメントの問題を提起したい。仮に最後の局面で登場した彼、あるいは彼女が最初からこのプロジェクトの責任者を務めていたなら、スケジュールの遅延や予算の超過といった問題は起きず、平穏無事に手荷物取り扱いシステムの開発が進み、それが原因となって開港が遅れるということはなかったに違いない。

私はこのスーパ SE の名前も所属もしらない。しかしその人に私は改めて、大いなる敬意を表したい。

---

[5] これは当初予算の、265%に当たる。つまり 165%の予算超過が発生したことになる。

[6] これは当初予算の、161%に当たる。つまり手荷物取り扱いシステム開発の予算超過は、空港全体の建設費の予算超過より、率でも遙かに小さかった。

[7] リスク管理については、第 51 章で述べる。

キィワード

ソフトウェア危機、オブジェクト指向技法、デンバー国際空港、手荷物取り扱いシステム、分散処理、リスク管理

略語

ACM：Association for Computing Machinery

参考文献とリンク先

[NIK02a]　日経コンピュータ編、「システム障害はなぜ起きたか みずほの教訓」、日経 BP 社、2002 年.

[NIK02b]　日経コンピュータ編、「動かないコンピュータ 情報システムに見る失敗の研究」、日経 BP 社、2002 年.

[NUE95]　ピーター・ニューマン著、滝沢徹他訳、「危ないコンピュータ 頻発するコンピュータ事故からの教訓」、ピアソン・エデュケーション、1999 年.

この本の原書は、以下のものである。

Peter G. Nuemann, “Computer Related Risks,” ACM Press, 1995.

[SCH96]　http://www.csc.calpoly.edu/~mshloh/senior/title.html （今この URL を検索すると “Not Found”になって、情報を得ることができない（確認日：2017 年（平成 29 年）1 月 3 日）。）

（2003 年（平成 15 年）9 月 22 日　初稿作成）
（2007 年（平成 19 年）10 月 2 日　一部追加）
（2008 年（平成 20 年）7 月 23 日　一部修正）
（2010 年（平成 22 年）7 月 15 日　一部修正）
（2013 年（平成 25 年）11 月 5 日　一部修正）
（2016 年（平成 28 年）1 月 13 日　一部修正）
（2017 年（平成 29 年）1 月 3 日　一部修正）