自動改札システム障害事例のD-Caseを書いてみる

2014/1/27

ICカード改札サービスと自動改札システムの大規模障害の歴史

2001.04.08　JR東日本Suica試験利用開始（常磐線上野-勝田間）

2001.11.18　JR東日本Suica利用開始（首都圏全駅）

2006.12.01　日付が変わった時点で日本信号製の自動改札機（エリア内184駅）で「Suica定期券」「VIEW Suica」「モバイルSuica」の通過を拒否する誤判定障害が発生した。JR東日本は終電まで全改札機を開放し、とりあえずの混乱を回避した。4時38分にプログラム修正作業を完了し、5時10分までに全駅で復旧した。Suicaシステムの大規模障害は初めて。

2007.03.18　PASMOと相互利用開始

2007.10.12　日本信号製の自動改札機が、始業時起動処理を進めたが、正常起動しないというトラブルが発生した。JR東日本およびPASMO関係鉄道事業者は混乱を避けるため同社製以外のものも含め首都圏の全改札機を午前6時ごろから開放した。午前7時50分ごろから、個別の自動改札機の電源を入れることで機能の一部が古いままで動作が可能なことが明らかになり、午前10時ごろまでにすべて再起動された。始発から午前6時ごろまでの利用者の一部に影響が及んだが、開放した事により、ラッシュ時の混乱は避けられた。原因究明に時間を要し、10.15になってようやく原因の発表がなされ、修正が施された。

2013.03.23　全国10種類のICカードと相互利用開始

自動改札システムのD-Caseを書いてみる

2006.12.01および2007.10.12の自動改札機障害の事例を参考に、事後ではあるがD-Caseを記述して、JR東日本およびPASMO関係鉄道事業者の事故に際しての対応策が、DEOSのコンセプトに照らし合わせて、似通っていたかどうかを検証する。

DEOSコンセプトと相通ずる点

2006.12.01および2007.10.12の自動改札機障害に際して、改札機を開放して混乱を避けると言うとりあえずの対応が取られていたので、おそらく、D-Caseの一つの分岐木にあるように、組織として緊急に対応すると言う計画は立てられており、実施指示書もあり、何度か訓練はされていたのではないかと推察される。

とりあえずの混乱を避けた後、さらに迅速な原因究明のアクションが取られており、原因究明後は、順次修正がなされた事からも、変化対応も計画されており、実施指示書もあり、何度か訓練はされていたのではないかと推察される。

以上から、この事業者においては、DEOSプロセスにきわめて近いプロセスが回っていたと考えられる。

追記

2007年10月18日木曜日の早朝、首都圏の私鉄や地下鉄5事業者において、PASMOとSuicaの精算など窓口処理ができなくなった。日本信号製の窓口処理機に不具合が発生したためだという。

原因は10月12日に発生した、自動改札機と同様だった。プログラムの不具合によって、センターからの配信データの読み込みに失敗するというもの。自動改札機とは一部プログラムを共用しており、配信データのうち自動改札機と同様に盗難や紛失で無効にしたICカードの「ネガ・データ」の読み込みで問題が発生している。

約1週間の時間差について日本信号は「窓口処理機と自動改札機のデータ配信フォーマットが異なり、不具合を発生させるデータの件数が異なるため」と説明している。

鉄道事業者では当面の間、プログラムの修正や検証ができるまで、問題を起こしたデータの配信を停止した。なお、12日の自動改札機の問題が発生した際、窓口処理機もチェックしたが問題を見つけることはできなかったという。

障害が発生した窓口処理機の内訳は、埼玉高速鉄道15台、東京メトロ12台、東武鉄道56台、東葉高速鉄道11台、ゆりかもめ7台。読み取り部分にICカードをかざしても、処理ができない状態となった。窓口処理機器を単体で立ち上げ直すことで、午前11時に復旧した。約400人の乗客に影響があった。

追記を踏まえての原因究明の徹底の重要性への考察

2006.12.01の事故を起こした後、同様なソフトウェアの潜在バグの探索が行われたかどうかは不明である。なぜなら、2007.10.12の事故も同じ日本信号製の改札機でのみ、しかもソフトウェアが原因で起きているからである。適切なバウンダリー条件をリストアップし、しらみつぶしでテストしていれば、後者のバグは事前に修正出来ていたかもしれない。

また追記にあるように、2007.10.12の事故の6日後の2007.10.18に、同じソフトウェアが使われている日本信号製の窓口処理機でも同じ障害が起きており、2007.10.12の事故後、窓口処理機もチェックされたと述べられているが、残念ながら障害が起きたと言う事は探索・チェックが足りなかったと考えられる。

原因究明のためにはいろんな手法がすでに確立されており、D-Case手法を適用するまでもないかもしれないが、D-Caseを書く事により、関係者が究明の目標や方法論を議論し理解を深めるためであったり、説明責任遂行時にシステマチックな説明にD-Caseが使えそうだと感じられたら、原因究明の活動に入る前にその活動のD-Caseを書いてみる価値はあると思う。