

東証における誤発注問題に関する提言

情報システム学会 東証問題検討プロジェクト

代表 上野南海雄

東証における証券会社からの誤発注にともなう巨額の損害発生問題は、証券会社と東証との間の7ヶ月以上にわたる交渉の末、10月27日東京地裁に提訴がなされた。社会的影響の非常に大きな事件であるにもかかわらず、提訴に至るまで、当事者である証券会社、東証、ソフトウェア開発業者が、事件に関して十分な説明責任を果たしていないことは、きわめて問題である。

どのような分野においても専門家が関わる業務において、技術者倫理など専門家の倫理規範にもとづいて業務を推進すべきことは、今や国際的な常識になっている。専門家の倫理において最も重要な規範の1つが説明責任を果たすことである。特に今回当事者となったのは、いずれもわが国で指導的立場にある企業・組織であり、倫理的にも他の企業・組織に対して範を示すべきであった。

金融分野の情報システムトラブルで、説明責任が果たされた優れた事例として数年前に起きたある金融機関の基幹オンラインシステム障害がある。^[1]この事故では、約半日の間コンピュータを使った一切の金融取引が不可能になった。

これに対しこの金融機関では「今回の障害を自社だけの問題に止めず、障害原因をはじめこの障害で得られた数々の教訓について金融界はもとより広く社会に公表し、他においても二度とこのような事態の発生がないよう障害を発生させた者の責務として努めていく」として、障害の内容、原因、顧客などへの影響とそれへの対応、マニュアルの整備状況と今回の運用状況、再発防止策などを19ページにまとめて、インターネットで公開した。

金融の情報システム分野において、すでにこれだけの実績があるのだから、東証問題の当事者も上記金融機関をベンチマークにして説明責任を果たしていくべきであろう。今後裁判が終息後、各当事者から明確な説明がなされることを期待している。

すでに主要な雑誌・新聞などを通じて報道されている内容から、今回巨額の損害が発生したプロセスは、添付の連関図のようであったと考えられる。現在伝えられている範囲内でも、今回事件の当事者には次のような問題・課題が存在していることが推定される。

(1) 証券会社

- ・異常注文警告のメッセージが出たにもかかわらず、発注を行なった原因は、どのように分析されているか。
- ・誤入力をした担当者は、若手で経験が少なかったと伝えられている。会社として、情報システムの利用者教育はどのように行なわれていたのか。事件のあと、利用者

教育はどのように改善されたのか。

- ・システムの異常注文警告のメッセージを出す基準はどのように設定されていて、事件後どう改善されたのか。基準の決定と徹底の社内的なプロセスについてはどうか。

- ・誤入力は、2分後にアシスタントにより発見されており、今回結果的には人によるチェック機構が働いた。この発見がなかったら、損害はさらに著しく拡大していたはずである。これはアシスタントの個人的な資質によったものか、それとも業務の標準的なプロセスだったのか。業務標準として、当時チェックプロセスはどのように設定されていて、それは事件後どう改善されたか。

- ・証券会社の中で誤入力をした部署から東証に対する窓口部署に報告がなく、窓口部署が東証から連絡を受けたとき混乱があった。今回に限れば誤入力をした部署の注文取り消し開始と東証からの連絡がほぼ同時刻だったため、結果的に大きな影響は生じなかったが、本来は入力部署の異常が直ちに東証に対する窓口部署に伝えられる体制がとられるべきだろう。この点はどのように改善されているのか。

(2) ソフトウェア開発業者

今回、誤入力に対する取り消し操作は、入力の2分後に行なわれている。損害額が拡大したのは、取り消しができなかったためである。

取り消しができなかった原因は、ソフトウェアの欠陥にある。取り消したい銘柄が連続的に約定処理中であり、みなし処理がかかった注文への取り消しの場合、未約定の注文が残っていても取り消しができないようにソフトウェアが組まれていた。

ソフトウェア欠陥の原因としては、要求仕様・設計・製作の誤り、およびそれらをテストの過程で発見できなかったことが可能性として挙げられる。

一般的に、要求仕様・設計・製作は、システム機能および構造に関する段階的詳細化のプロセスになっている。要求仕様書では、設計・製作段階ほど粒度的に細かく機能や構造が記述されるわけではない。

事件発生当時のソフトウェアは、注文の取り消し操作に対し、連続的な約定処理の有無、みなし処理の有無が重なった4つのケースに対して、3ケースに対して正しく取り消し処理をしているが、両者ともに有という1ケースのみ未約定の注文が残っていても取り消しをできないようになっていた。^[2]

今回要求仕様書には分岐条件の判断基準の明記がなかったとされている。しかし結果的には4ケースに正しく分岐し、そのうち1ケースのみ処理を誤っているのであるから、設計・製作者は分岐条件を理解しており、詳細設計または製作の過程でミスがあったと推定される。当時の東証の関係者も「取り消しができない仕様で開発を依頼するはずがない」と語っている。

また、一般的に金融関係の基幹システムでは、プログラムの全パスをテストで確認するのが通例であるが、今回特定の1パスで必要な機能がもれているのであるか

ら、全パスのテストがどのような手順で行われたのかということも問題として挙げられる。名古屋証券取引所では、東証と同じソフトウェアをカスタマイズして使っているが、今回の事件後調査をしたところ、東証と同じ不具合が存在し、また東証の不具合と同じ条件下でのテストが抜けていた、と名証関係者が言っている。^[3]東証においてもテストもれの可能性が高い、という見方は妥当であろう。

今回の事件につき、今後の賠償の問題は別として、大きな損害がソフトウェアに起因して起きたのであるから、開発業者はプロジェクト・マネジメントにおいて、プロダクトプロセス管理と品質管理をどのように進めたのか、可能な限り残された資料を分析し証言を集めて、問題の構造を明らかにすべきである。またソフトウェア開発業者は1社ではなく、協力会社が参加している可能性が高い。その場合、調達管理はどのように進められたか、ということも併せて問題になる。

今回の事件後、証券会社および東証に対しては金融庁から業務改善命令が出され、概括的ではあるがそれぞれから報告書が公表されている。それに対しソフトウェア開発業者は、巨額の損害の原因を作りこんだにもかかわらず、まったく説明責任を果たしていない。オープンな情報開示こそ優れた企業の資格であると理解して対応すべきである。

(3) 東証

ソフトウェア欠陥の原因がソフトウェア開発業者にあったとしても、この問題に関して東証の企業としての社会的責任(CSR)が減じられるわけではない。東証には、情報システムの発注者として、またオーナーとしての役割がある。

東証がシステムの受け入れに際し、プログラムの全パスを確認するのはむしろかしいだろう。東証の役割は、ソフトウェア開発業者がプロジェクト・マネジメント、すなわちプロダクトプロセスや品質、調達の管理を適切に行なっているか、発注者としてチェックすることにある。このチェックが十分行なわれていたかどうかの問題になる。もしそれがなされてなかったならば、どうしてそのような状態になったのか分析しなければならない。

ソフトウェア開発業者がプロジェクト・マネジメントを十分に行ない、東証がそのチェックを十二分に行なったとしても、システムトラブル発生の確率をゼロにすることはできない。そのため、東証としてはトラブル発生に備えて危機対応計画を作成し、その体制を整えておかなければならない。今回の事件発生の時点でこのような計画や体制がどのように作られていたかが問題である。

東証は2000年問題以降、コンティンジェンシー・プランを作成し、システム障害における対応策を明確にし、体制整備も進めてきたとされている。一方、今回の事件発生時、「売買状況の異常を理由とする停止の経験もマニュアルもなかった」という東証幹部の発言がある。^[4]コンティンジェンシー・プランは具体的にはどのように作られ、徹底・運用が図られてきたのだろうか。

今回の場合、東証は証券会社の誤入力 of 2 分後には証券会社に注文の妥当性について問い合わせを行っており、入力の監視体制と機能は優れたものだったと言える。これはどのような業務システムにもとづいていたのだろうか。内容によっては今後築いていくべきもっと広範な業務システムの基盤にできる可能性がある。

実際には、発行済み株数 14,500 株に対して 61 万株の売り（しかも 1 円の指値）という、明らかに異常な注文に対して、取引の停止が発動されることはなかったし、注文の取り消しが不可能と判明した時点でもなお、取引の停止が意思決定されることはなかった。

東証のある幹部は、事件発生 of 4 時間後、海外出張から帰国直後の空港で報告を受けたが、その瞬間「どうしてすぐに取引中止にしなかったのか」と問い返している。⁵このことは、今回の場合、取引の停止が当業者に容易に判断できる処置であることを表わしている。誤入力の発見自体は 2 分以内にできていたのであるから、問題はそのときの処置基準がどのように標準化され、また徹底が図られていたかということになる。

今回起きたような株数と株価の誤入力は、珍しい事例ではない。数年前に数 10 億円の損害を出した事例があるし、それ以下の損害の事例なら頻発している。今回の事件を契機に、東証では上場株式数の 30% を超える注文を受付けない、などの処置をとったが、遅きに失したと言ふべきだろう。数年前の事件で、すでに上場株数の 40% を超える誤入力が行なわれている。

今回の東証問題は、当初総額 61 万円の予定で始めたビジネスが、わずか 10 分余りで 407 億円（実に 67000 倍）の損害をもたらすという、人間とコンピュータのかかわる今日の情報システムに潜むリスクの大きさを象徴的に示す事件だった。

情報社会においては、このようなリスクが至るところに存在していると考えられる。われわれはこのようなリスクを回避しなければならないし、万一発生したときの影響を軽減する対策も、今後検討していかなければならない。このためには何よりもまず、事件が起きたとき各当事者が上に述べたような諸問題に対して説明責任を果たし、その上でそれらの情報にもとづいて総合的に問題の構造を明らかにする必要がある。

今回事件が起きたとき、最初に東証より「取り消しができなかった原因は証券会社の取り消し方法に問題があったのではないか」という発言があり、その後「東証のシステムに原因があった。ソフトウェア開発業者にも責任があると言わざるを得ない」と修正がなされた。事件の 8 ヶ月後、証券会社は東証に 404 億円の損失負担を求め、東証がこれに対して拒否を続けたため、先述のとおり提訴に至っている。

各当事者が説明責任を果たさず、総合的に問題構造を明らかにしないままに、

責任と損失負担の転嫁のみが活発に行なわれている現状自体、きわめて問題である。特にソフトウェア開発業者に対する責任の追及に対して「現場の志気がダウンする」「人間は神ではない。過ちを犯す存在だ」「賠償の恐れがあるのならシステム開発は請け負えない」など、感情的ともいえる反発が生じている。しかし、ソフトウェア開発業界が社会のインフラを形成するかけがえのない産業として、今後インダストリ・アイデンティティを確立していくためには、冷静にこの事件を分析して、一段と品質水準の高い製品づくりに取り組むことこそ必要だろう。ソフトウェア開発業者は、まず今回ソフトウェアの欠陥がなぜ生じたのか明らかにした上で、このような事件を二度と起こさないための自らの施策と、発注者に求める対策を提示すべきである。

今回の事件で407億円の損害が発生したことは、人間とコンピュータのかかわる今日の情報システムがいかに重要な、価値のある存在であるかということを示している。また上記のような数多くの問題が重なって事件が発生したことは、それらの問題のいずれかでも事前に改善されていれば、損害が大幅に軽減された可能性があることも示している。対策がそれだけ多角的に存在しているということは、今回の問題の解決がきわめて現実的に可能なものであることを意味する。

各当事者には、何よりもまず説明責任を果たし、総合的に問題の構造を明らかにして頂きたい。そして今回の事件を当事者だけの問題に止めず、二度とこのような事件の発生がないよう、金融界・ソフトウェア開発業界はもとより広く社会全体にこの事件からの教訓を伝えて頂きたい。そのことを強く要望し、情報システム学会東証問題検討プロジェクトからの提言としたい。

参考文献

[1]<http://www.fukuokabank.co.jp/news/h200003-02/index.htm>

[2]日経コンピュータ, No.646, pp.16-17, 2006年2月20日.

[3]<http://itpro.nikkeibp.co.jp/article/COLUMN/20051227/226805/>

[4]<http://www.mainichi-msn.co.jp/keizai/kigyuu/news/20051218k0000m020093000c.html>

[5]日経コンピュータ, No.646, pp.18, 2006年2月20日

東証・誤発注損害発生問題 連関図

