第７回「情報システムのあり方と人間活動」研究会　開催報告

開催日時 平成２２年５月２２日（土） 午後１時３０分～
場所　　慶應義塾大学日吉キャンパス協生館６階 大会議室
参加人数　１６名

研究会を開催しましたので概要をご報告します。研究会に学生諸君の参加もあり活発な研究会となりました。途中、慶応義塾大学ＳＤＭ研究科長狼教授より情報システム学会研究会の開催を歓迎しますとのご挨拶がありました。

第１部 午後１時３０分～３時　質疑３０分
題目　　「システムの安全性を脅かす人間活動の落とし穴」
講演者　電気通信大学　大学院情報システム学研究科教授　田中 健次氏

【講演概要】

安全情報社会は、高信頼性技術のみで実現可能であるのかの観点から論ずる。最近の製品・システムには、安全装置や仕組みが組み込まれているが、本当の安全装置はあるのか？ 瞬間湯沸し器での死亡事故を考えた場合、改造が原因であったことから Human-Machine の観点から問題点と対応の現状、今後の期待、つまり使う側の問題に踏み込んで考えたい。

信頼性と安全性の関係であるが、正常に動いていた製品が故障し安全であった使用者に危険･損害が生じることが一般的に考えられる。又、製品が正常に動いていたが、人間のエラーで使用者が危険・損害を被ることが生じる。これらのことを考えていきたい。

１　情報セキュリティをベースとしたシステムセキュリティ

安心な情報社会は、情報セキュリティの高信頼性技術のみでは実現可能ではなく人間系も含めた全体で実現できると考える。

情報システムのリスクは、どこに存在するのかを点検し、情報伝達のサイクル：情報伝達の６要件（田中,1999）として分析した。

①発信情報 ②発信者 ③通信機器 ④受信者 ⑤受信者行為 ⑥情報の恩恵 の６サイクルである。これに対応したリスクは、①間違った情報 ②入力ミス・不在 ③情報不正利用と故障・災害対策 ④不在リスク ⑤不法行為 ⑥確認欠如 が対応している。対応策は、①情報の信頼性確保 ②容易な操作、又は、ミスの顕在化と訂正処理 ③暗号使用、又は、冗長化（バックアップ） ④受信者の確保 ⑤社内監査、法整備 ⑥対応したシステム が考えられる。事例として、２００４年１０月に台

風２３号の被害を受けた豊岡市の水害防災システム（工費４１億円）で、実際に水害が発生したにも拘らず防災システムの画面には何も表示されなかったというトラブルがあった。このトラブルでは、情報システムは完成していたが、水害被災地では水害時に防災システムへ状況入力する人がいないことが顕在化したことで、手段はあっても人間活動の観点が忘れられていたことが最大の原因であった。従って、システムを人間活動も入れてトータルで考える必要性が明らかになった。

次にシステム・製品への不信が生じる場合について考える。

２　システム・製品への不信

不信に陥ると何が問題となるのか？

（１） 余計な操作により、止める、壊す

（２） スイッチを切る

不信に陥る理由は以下の通り。

（１） プロセスの不透明性・意図の不一致（処理過程を明示し不信を防ぐ）

（２） リスクレベルが高い(何回もの少々の損害より１回の大損害への感度が高い)

（３） トラブルの発生パターン（飛行機事故の方が自動車事故より不信感大）

（４） 対応が遅い（乳製品の食中毒事故での対応のまずさ）

３　システム・製品（装置）への過信

過信に陥ると何が問題か？

（１） リスクを意識しなくなる

（２） 危険な状況の判断に遅れが生じる

過信に陥る理由は以下の通り。

（１） 便利のみが表面に出た結果、リスク感覚が欠如してしまう
過信と警戒心の欠如となり、実感の無い操作で犯罪となるケースがある

（２） 安全装置の限界や盲点を知らない
車にエアバッグを装備したがこの結果、車の速度を上昇するケースが増えた。
そこで、車の運転方法として、手動・警報装置＋手動装置・警戒装置・手動＋警戒装置＋自動ブレーキ装置の３種類を実験した結果、この中で１番安全なのは、「警報装置＋手動操作」の結果となった。自動ブレーキ装置がついている場合、人間は装置に頼り速度を上昇させる傾向が見られた（リスク恒常性の発現）。従って、安全性を決めるのは安全装置でなく人の行動である点が明確になった。又、警報装置が欠報を引き起こす場合には、状況から異常を発見することが難しくなると言える。
最近、低速ＡＣＣ（Adaptive CC:車間一定追従装置）が装備される車が出てきているが、前方車の急停止にはブレーキ操作が必要であることを忘

れてしまうのではないかと危惧している。又、人間活動に関する「多重防護の落とし穴」の実験によると、多重の人間による残存エラー検出率は、２名の場合が一番高いという結果になっている。多くの人間がエラー検出するからと言っても、エラー検出を多くの人間が行うと当該グループで認識している場合には、前の人がエラー検出しているとの安心感から残存エラー検出率が極めて低くなる、４番目以降は０となる傾向が出た。

（３）長期間トラブルが発生しない

安全経験が事故を招くことになる

４　グレーゾーンでのトラブル対応

安全保障設計が重要と考えているので紹介したい。この定義は、グレーゾーン（安全領域と危険領域の間）を含めた危険を回避することを意図した設計を行うことを指している。以下、グレーゾーン＝ＧＺと呼称。

危険回避設計と言われるものは、ＧＺを含めず明らかな危険のみを回避することを意図した設計である。事例として、高気圧酸素治療での火傷事故が上げられる。高気圧酸素治療装置に、「化繊のパジャマは危険」、つまり危険情報表示がしてあったが、５％化繊のパジャマを着た患者が火傷をした件である。以降、安全情報表示に変更となり「１００％木綿のパジャマのみ可」へ変更された。

安全保障型のフールプルーフ設計が日本では多くなって来ているが、果たして安心は得られるのかを論じる。安全にしか使えない製品の増加、つまりＧＺ回避の対応は、言わば“ぽかよけ”を多くし“ぽか人間の生成”となると考える。

安全な製品・システムを作るというより、ＧＺでも安全に使える人を作る考え方が最近、生じている。「使用者自らが危険を認識し回避できる仕組みを組み込む」考え方で、状況認識の容易な設計・危険の透明化を行うものである。

これは、受動的安全から獲得する安全へと考え方を方向転換するもので、リスク認知の工夫を行うことで、情報システムの真のリスクを全ユーザに正しく認知させるべきであると考える。このためには、①リスク情報の明示 ②事故・トラブルのＤＢ公開を行うことにより実現可能と考える。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

第２部 午後３時４０分～５時　 質疑 ３０分

題目「建築学から学ぶ情報システム学の基盤（２）」

講演者　 みずほ情報総研株式会社　伊藤 重隆氏

【講演概要】

西洋建築史を紀元前のピラミッド、パルテノン神殿から現代建築までをたどる。

建築学では、建築史を重要なテーマとして位置づけているが、情報システム学に取り情報システム史を確立することは意味を持つものと期待される。

建築の定義が、「人間が活動するための空間を内部に持った構造物を、計画・設計、施工そして使用するに至るまでの行為の過程全体、あるいは一部のこと」とされているので、情報システムの定義を建築の定義からのアナロジーとして、下記の様にする。

人間が活動するための、ある情報空間を計画、設計、製造そして使用するに至るまでの行為の過程全体、あるいは一部のこと。情報空間＝情報システムと考える。

建築にとって、建築家は大きな役割を持っている。西洋では、建築家は、プロフェッションと看做され、弁護士・医師と同格の公益を増進する中立な社会的に認められた地位となっている。又、計画・設計と施工は職業として分離している。ローマ時代の偉大な建築家、ウィトルウィトスは、建築家は、理論と実技に精通するものとしている。一方、日本においては、建築士といえども西洋での位置づけとは異なり、有名な建築家に依頼する場合を除いて計画・設計と施工を一括請負する場合が大半で、これが構造設計問題（手抜き）を引き起こした遠因とも言える。情報システム構築時には、プロジェクトマネージャー（ＳＥ経験者）とＳＥが中心となり情報システムを設計・施工（製造）しているが、仕事として建築家の様な位置づけの職業は無い。情報システム社会の到来に従い社会的に重要な情報システムが増加しているので、情報システム構築時に、西洋でいう建築家のポジションを設定し中立な立場で情報システムを完成させることが社会的に要求されると考える。

建築学は、学際的な「壮大な総合学問」と考えられている。情報システム学についても工学、理学、経済・経営学、社会学等も包含する総合学として考えられる。

建築の場合には、計画・設計に要する期間は、一般的には全工期の１－２割であるが、情報システム構築の場合には、約４割程度でかなり多い。この事由は、情報システムの場合には、企業等の業務機能を細部にわたり明確にする、又は、ユーザが機能要件を決定するのに時間を要すること、要件が複雑なことから、ベンダーと発注者の間でコミュニケーションに多くの時間を要するのが主要因である。なお、建築の場合、設計図は標準化されて、どの施工者も理解できるが、情報システムの場合は当たらない。情報システム開発の場合には、開発途中であっても仕様変更、要件変更が生ずる場合が普通となっているが、建築の場合には、施工以降での設計変更は、工程のやり直しのコストが大幅増で納期遅延となるので現実的には、まず有り得ない。建築は、設計図に材質、工法等を指定し設計時に構造シミュレーション等を行い、施工は設計図に従い行う。又、情報システム構築と異なり建築には、構造物が完成した時にテストの様な検証するプロセスは無い。つまり建築の場合には、設計図を完成した時点で施工の条件が明確、又、施工方法も施工業者に取り実績があるものとしている点が異なる。又、情報システムの場合には完成時にすぐ利用できるが、一方、建築の場合、建築物が完成しても設備、内装、インテリア、家具等が家主に選択され設置されてから使用可能となる。この点から類推

して、情報システムについて基本構造物と追加構造物に階層を別にして考え、ユーザの持つ固有の条件は追加階層にして全体の構造物を完成させる方式を考えることを提案したい。

（伊藤重隆）

以上