コンピュータシステムB -ソフトウェアを中心に -

#9 バグ・ソフトウェア工学

Yutaka Yasuda

ソフトウェア開発

- 願望

  正しく動作するソフトウェアをなるべく容易に安定して作成し、利用したい

- 問題

  バグ：正しく動作しない

  要求仕様を満たせない

  開発計画の見積もり失敗

“Software Factories に関する陳述”

- Jack Greenfield, Microsoft corp., July 2004
- The Standish Group. The Chaos Report. (1994) によれば、

  米国では毎年17 万 5000 のプロジェクトに約 2500 億ドルのソフトウェア開発費が投じられる

  僅か16%がスケジュールと予算の枠内に収まった

  31% が品質の問題によりキャンセル（810 億ドル相当）

  53% が予算超過（平均 189%）し、損失 590 億ドル

- ソフトウェア開発産業は工業化の段階としては未成熟と言わざるを得ない

ソフトウェアの安全性

参考：相次ぐシステム障害（日経 ITPro）
http://itpro.nikkeibp.co.jp/trouble/index.html

- 事例

  みずほ銀行システムトラブル（2002/4, バグ）

  JR 東日本 Suica 改札トラブル（2006/12, バグ）

  NTT東西 ひかり電話接続不良（2006/9,10, 複合）

  東証 TOPIX システムトラブル（2008.7, バグ）

  JAL チェックイン・システム障害（2009.6, バグ）

- ウィルス問題（各社, セキュリティホール等）

Software Update

- 事例：Microsoft のソフトウェア・アップデート

  ほとんどがトラブルまたは安全上の対策（バグ）

  減る気配なし

Software Update　(ex. Microsoft)

Update ごとの一覧

MS09-068 : Word の重要な更新 (976307) (2009/11/11)
MS09-067 : Excel の重要な更新 (972652) (2009/11/11)
MS09-065 : Windows の重要な更新 (969947) (2009/11/11)
MS09-063 : Windows の重要な更新 (973565) (2009/11/11)
MS09-062 : Windows の重要な更新 (957488) (2009/10/14)
MS09-061 : Windows の重要な更新 (974378) (2009/10/14)
MS09-060 : Office の重要な更新 (973965) (2009/10/14)
MS09-059 : Windows の重要な更新 (975467) (2009/10/14)
MS09-058 : Windows の重要な更新 (971486) (2009/10/14)
MS09-057 : Windows の重要な更新 (969059) (2009/10/14)
MS09-056 : Windows の重要な更新 (974571) (2009/10/14)
MS09-055 : Windows の重要な更新 (973525) (2009/10/14)
MS09-054 : Internet Explorer の重要な更新 (974455) (2009/10/14)
MS09-052 : Windows Media Player の重要な更新 (974112) (2009/10/14)
MS09-051 : Windows の重要な更新 (975682) (2009/10/14)
MS09-050 : Windows の重要な更新 (975517) (2009/10/14)

月ごとの Update 件数

年	月	件	年	月	件
2009/	12	-	2008/	12	7
2009/	11	4	2008/	11	2
2009/	10	12	2008/	10	10
2009/	9	5	2008/	9	4
2009/	8	7	2008/	8	11
2009/	7	5	2008/	7	2
2009/	6	8	2008/	6	7
2009/	5	1	2008/	5	4
2009/	4	7	2008/	4	6
2009/	3	2	2008/	3	4
2009/	2	2	2008/	2	8
2009/	1	1	2008/	1	2

つづく… (資料は2009/12/5 現在)

http://www.microsoft.com/japan/security/bulletins/visual_list.mspx
Microsoft, Inc. 絵で見るセキュリティ情報から抽出

バグ

- ソフトウェア障害の 3/4 が既知の初歩的なプログラミングの誤りによる - Eugene H. Spafford
- なぜバグは発生するのか？無くならないのか？

  「注意深く設計すれば良かった」だけか？

- コンピュータが本来持つ構造問題として理解していきましょう

ソフトウェアとバグの関係

バグ

- プログラムに含まれる「間違い」
- データは意味をもたない
- コンピュータは意味を扱わない
- バグ

  無意味な（矛盾した）処理でも指示通り動作する

  例えば「金利と残高を加算する」ところを間違えて
  「年齢と金額を加算」させてしまうかもしれない

- なぜ間違えた指示が最後まで？

プログラミング

- 「1から10までの数を足した結果を出せ」

  これはコンピュータにとって「難しすぎる」指示

- 手順の明記

  「Xを 1 から 10 まで変化させ、毎回 Y に繰り込め」

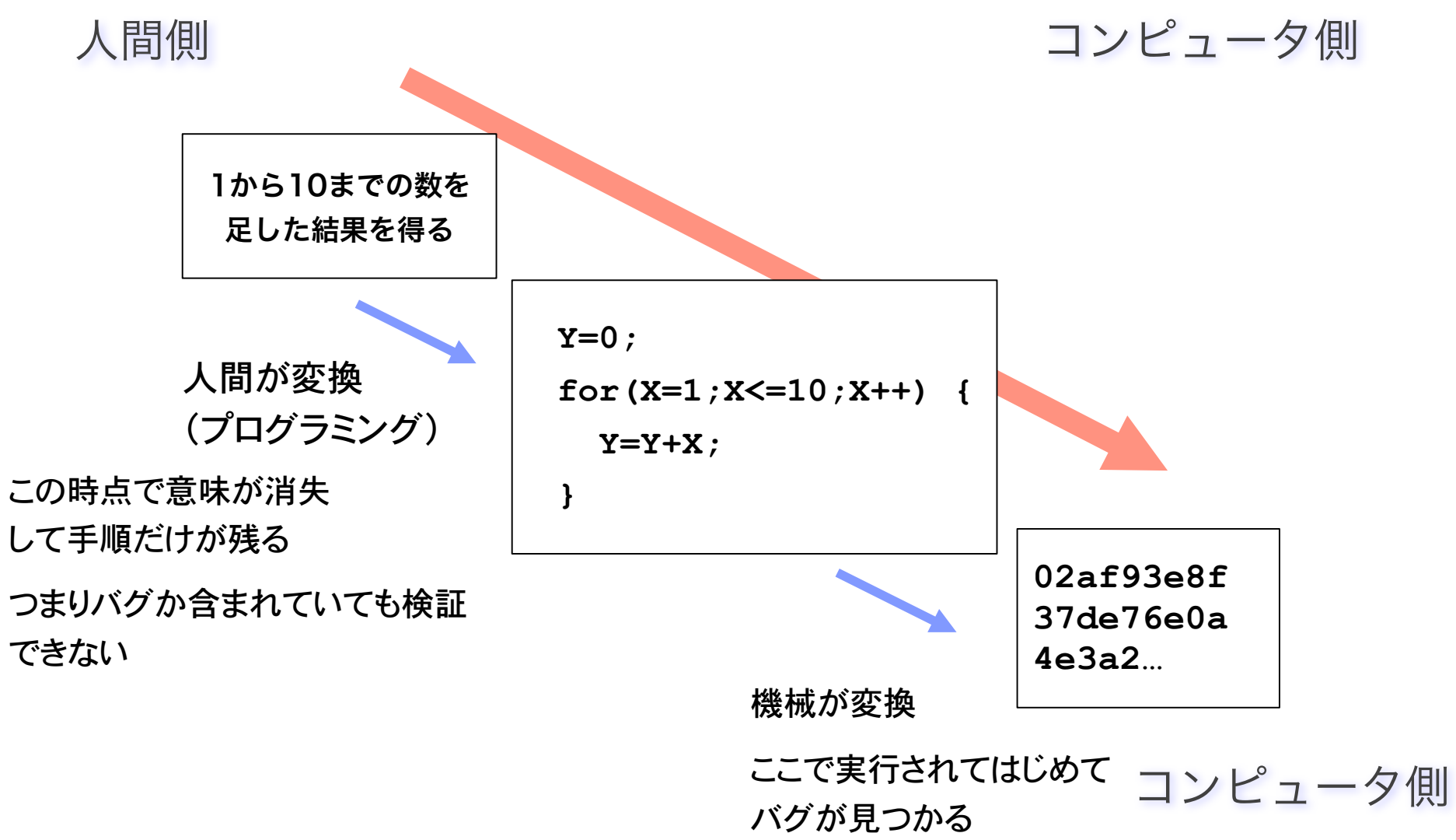
- プログラムとは何か

  目的に対して「何をどう処理するか」を詳述したもの

- 意味の消失

  「コンピュータはデータの意味を理解しないのと同様に、プログラムの意味も知らない」
  （ただ手順だけを知っている）

二つの変換過程


人間側
コンピュータ側
1から10までの数を
足した結果を得る
人間が変換
（プログラミング）
この時点で意味が消失
して手順だけが残る
つまりバグか含まれていても検証
できない
Y=0;
for(X=1;X<=10;X++) {
Y=Y+X;
}
02af93e8f
37de76e0a
4e3a2...
機械が変換
ここで実行されてはじめて
バグが見つかる
コンピュータ側

失われれる意味

- プログラミングの過程で、プログラムから意味は失われる

  そのプログラムの目的を知るのはプログラマだけ

- コンピュータは情報ではなくデータだけを扱う

  データが表現する情報は入出力の前後にいる人間が扱う

- ソフトウェアは作業から意味を抜いた手順だけを扱う

  その意味（内容）は結果を受け取る人間だけが知る

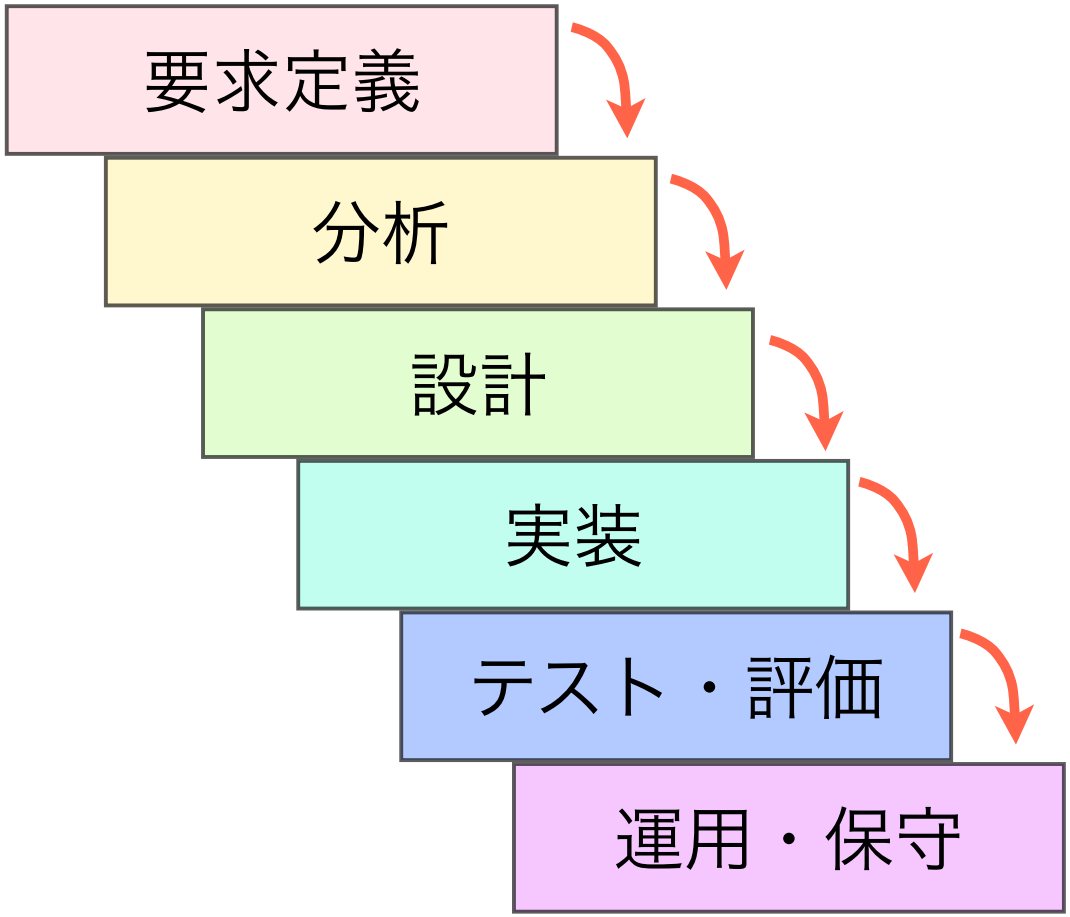
- バグ（意図しないプログラムの振る舞いをひきおこす不具合）が発生する根本的要因のひとつ

大規模システム開発の問題

Brooks に学ぶ

Water Fall model

- 古典的ソフトウェア開発手法
- ユーザの要求からはじめて段階を踏んで開発
- 各工程が完了すると次の行程に進む
- 家を建てる場合を想像せよ



人月の神話

- Brooks Jr., Frederick P.
  "The Mythical Man-Month: Essays on Software Engineering”, 1975
- IBM System 360 開発の経験から
- Water Fall model の限界
- 人月という考え方は適切でない

ブルックスの法則

- 人間と月（工数）は交換可能である、というのは幻想だ
- 遅れているプロジェクトへの要員追加はさらに進捗を遅らせるだけだ
- 優秀なプログラマは平均的なプログラマより１桁以上生産性が高い
- 工数はプログラムの規模の累乗になる
- プログラマがプログラミングとテストに費やす工数は、全工数の半分以下に過ぎない

「人月の神話」における主張

- ソフトウェア開発では作業員間のコミュニケーションの比重が（非常に）大きい
- 人数増はその比重を更に上げる
- 30年経ったいまでも予言として残っている
- エンジニアリングといっても社会工学的な側面であり、技術から離れている

銀の銃弾などない

- 1986年発表
- ソフトウェアの生産性をひとりでに高めるようなプログラミング手法は今後10年間登場しない
- ある程度は今も当てはまる（らしい）

まとめと対策

- なぜトラブル・バグはなくならないか？
- 情報とデータの相違

  コンピュータは情報でなくデータを扱う

  情報処理機械≠自動データ処理機械
- ソフトウェア工学の価値

  ソフトウェア開発に工学的手法を適用したい

  高度で安全なシステムを確実に開発できるように
- 脆弱なソフトウェア基盤からの脱却を

参考：Y2K 問題を思い出せ（or 調べてみよ）

- 坂東俊矢（京都産業大学法務研究科）
  「IT2001 なにが問題か」から

  「どこにあるかも知らないコンピュータの誤動作によるライフラインの断絶に備えて、半信半疑で風呂に水をため、当面の食料品を購入したりもしたが最後まで具体的な情報は消費者には伝わってこなかった」

  「消費者は情報社会が滑稽なほど不完全であって、それが自らの生活に直接の影響を与えるものであることだけは理解できたに違いない」

- 参照：首相官邸「コンピュータ西暦2000年問題」
  http://www.kantei.go.jp/jp/pc2000/

参考：様々なアプローチ

- 新しいプログラミング言語・環境・アイディア

  いかにして抽象化するか、また抽象化されたままプログラミングするか

  オブジェクト指向プログラミング
- アジャイルソフトウェア開発

  XP (eXtreme Programming) / Kent Beck ら

  ペアプログラミング / 頻繁なリリース / 完成という概念を廃し、期限までに顧客の要求を最大限採り入れる

  小さなテストを繰り返し、修正を繰り返す
- より良いプログラミング、システム開発へのアプローチはまだまだ続く