情報システムの障害リスクとは何か

2016年7月23日（土）

航空運航システム研究会（TFOS.SG）
航空システム部会＋リスク部会　合同勉強会

航空システム部会　松田　宏

自己紹介

（略　歴）

- 昭和22年生　山形市出身　山形大学理学部物理学科卒業
- 運輸省東京航空交通管制部　航空管制官（専修科41期）
- 日本電気　システムエンジニア（航空管制システム開発）
- 三菱総合研究所　主任研究員／室長（宇宙開発システム開発など）
- 日本ヒューレットパッカード　シニアコンサルタント／人材開発部長
- コンサルティング会社自営（航空管制／情報システム／人材開発）
- 現在：隠居生活（個人事務所として委員、執筆など限定的に活動）

（所属団体等）

- 非営利活動法人　日本シンクタンクアカデミー（JTTA）　正会員
- 一般財団法人　航空交通管制協会（ATCAJ）　賛助会員
- 非営利活動法人　航空・鉄道安全推進機構（ARSaP）　正会員
- 航空運航システム研究会（TFOS）　会員
- 航空安全報告分析委員会　委員
- 異分野交流サロン　主宰

背景：航空機の情報システム依存度が高まった
⇒ソフトウェア比重が高いので品質が重要

＜最初の飛行機＞
＝機体＋エンジン

＜大昔の飛行機＞
＝機体＋エンジン＋電気系
＋通信／航法装置（ADF等）

＜昔の飛行機＞
＝機体＋エンジン＋電気系
＋通信／航法／監視装置
＋自動制御装置（アナログ）

＜今の飛行機＞
＝機体＋エンジン＋電気系
＋通信／航法／監視
システム（FANS-CNS)
＋自動制御装置（デジタル）
（情報システム化）

＜地上の支援システム＞
運航管理、航空管制、
空港・旅客、etc

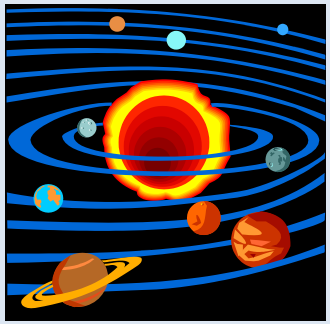
本日のテーマ

1. 情報システムとは何か
2. 情報システムの信頼性
3. 情報システムの障害パターン
4. 航空システムの障害事例
5. 人工知能の動向と将来像

Part-1　情報システムとは何か
①システムとは何か

- 個々の要素が相互に影響しあいながら、全体として機能するまとまりや仕組み

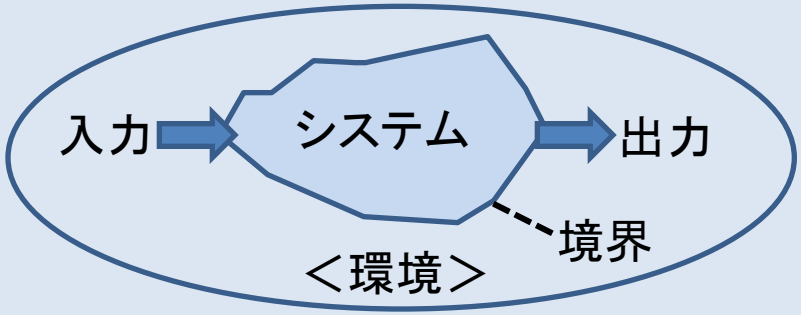
（系、体系、制度、方式、機構、組織など）

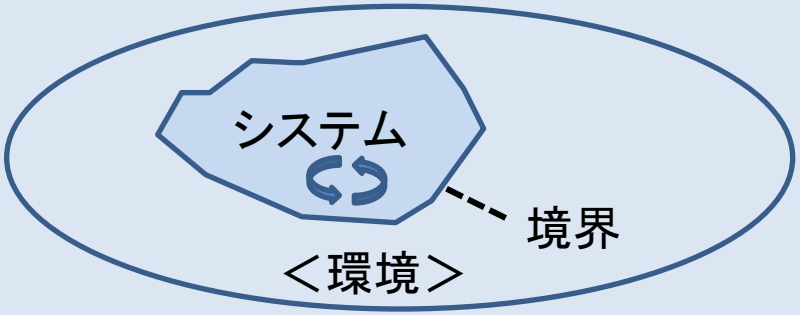


（例）
太陽系（Solar System）、生体系（Biological System）、
循環器系（Circulatory System）、呼吸器系（Respiratory System）、
力学系（Dynamical System)、代数系（Algebraic System)、
社会構造（Social System）、年金制度（Pension System）、
法体系（Legal System）、メートル法（Metric System）、
輸送システム（Delivery System)、鉄道システム（Railway System)、
計測システム（Instrumentation System)、制御システム（Control System）、
データ処理システム（Data Processing System)、
情報システム（Information System）、・・・

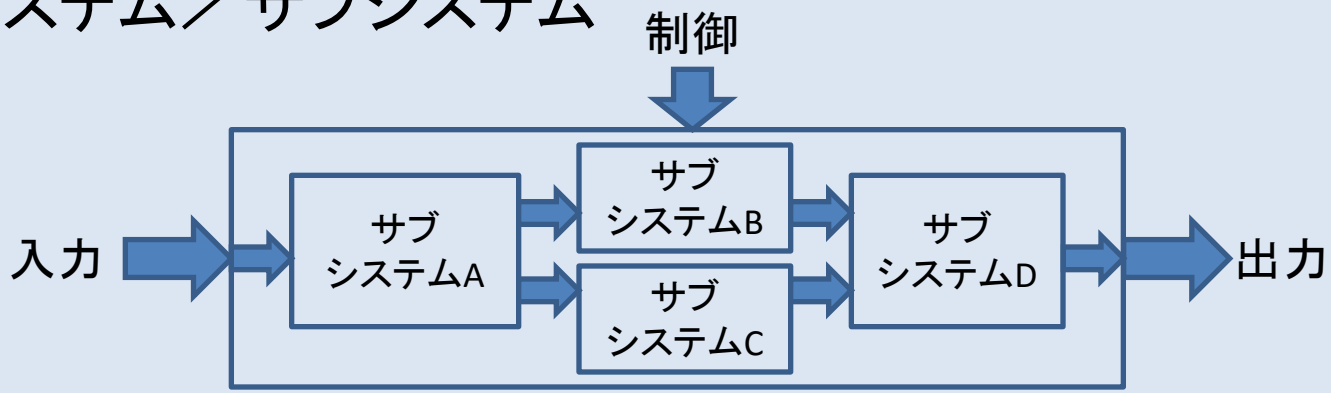
Part-1　情報システムとは何か
②システムの構造

- 開かれたシステム（オープンなシステム）
  閉じたシステム（クローズドなシステム）



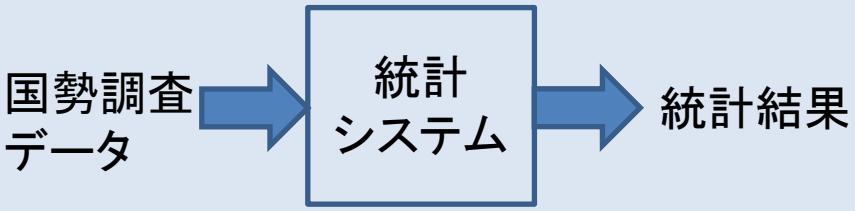


- システム／サブシステム

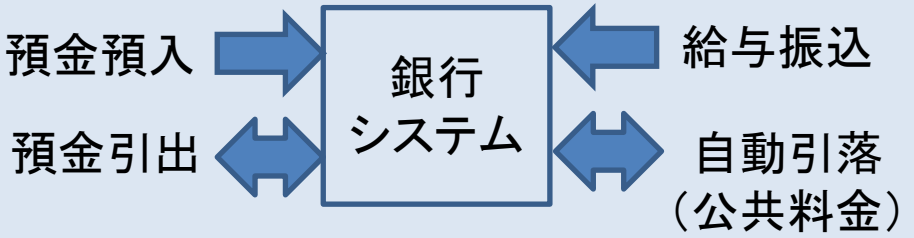


全体システム

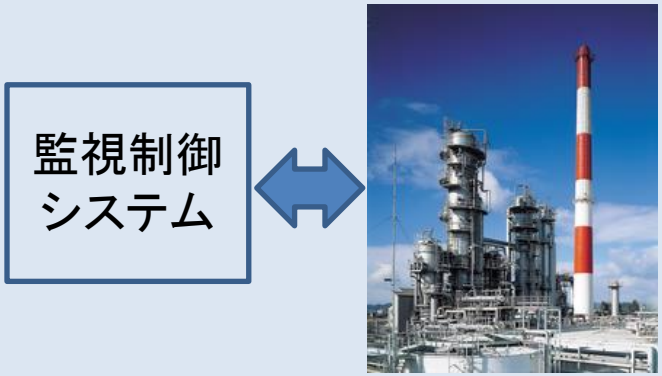
Part-1　情報システムとは何か
③情報システムの種類



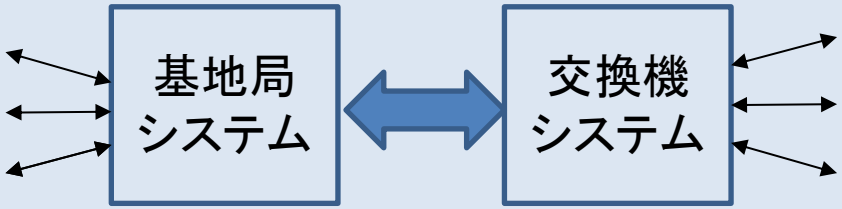
データ処理型



データ更新型

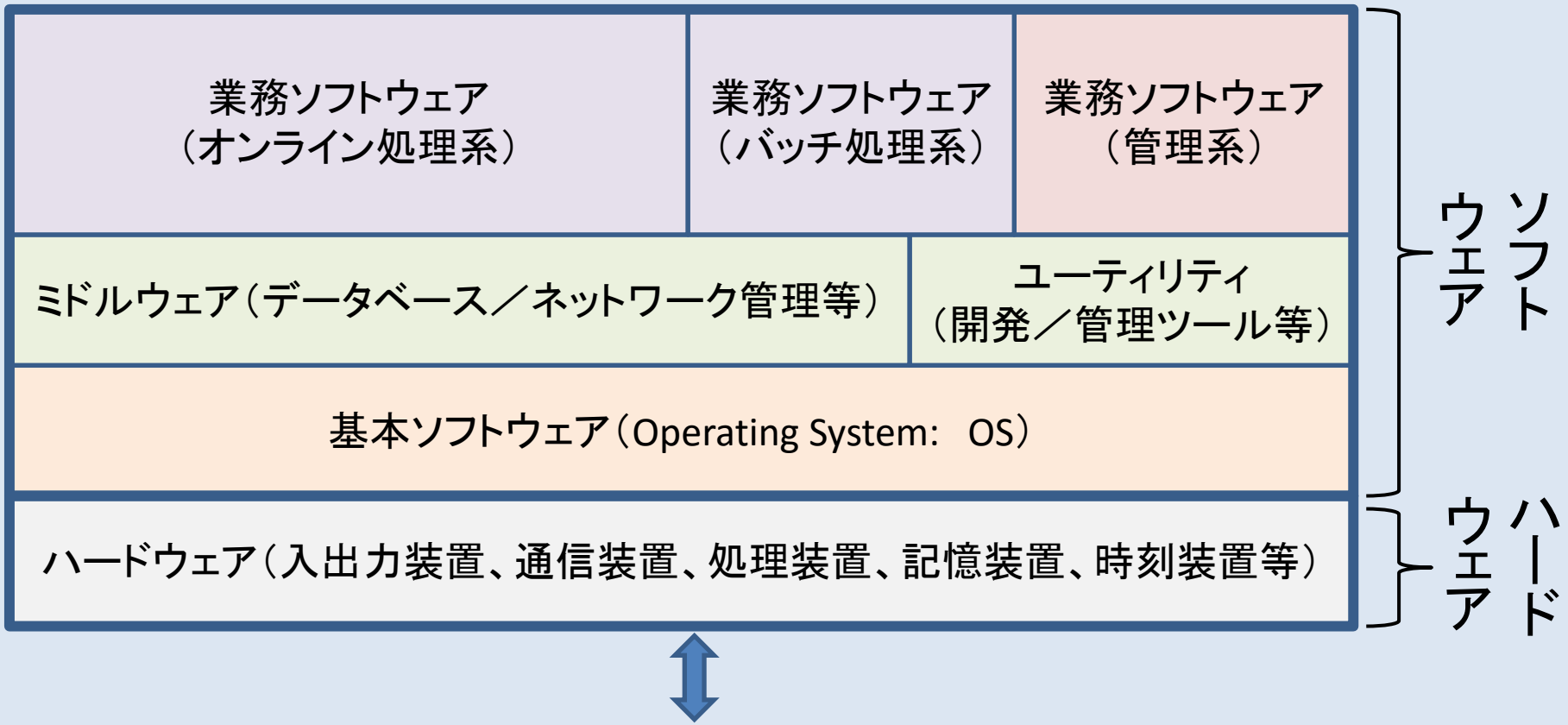


計測制御型



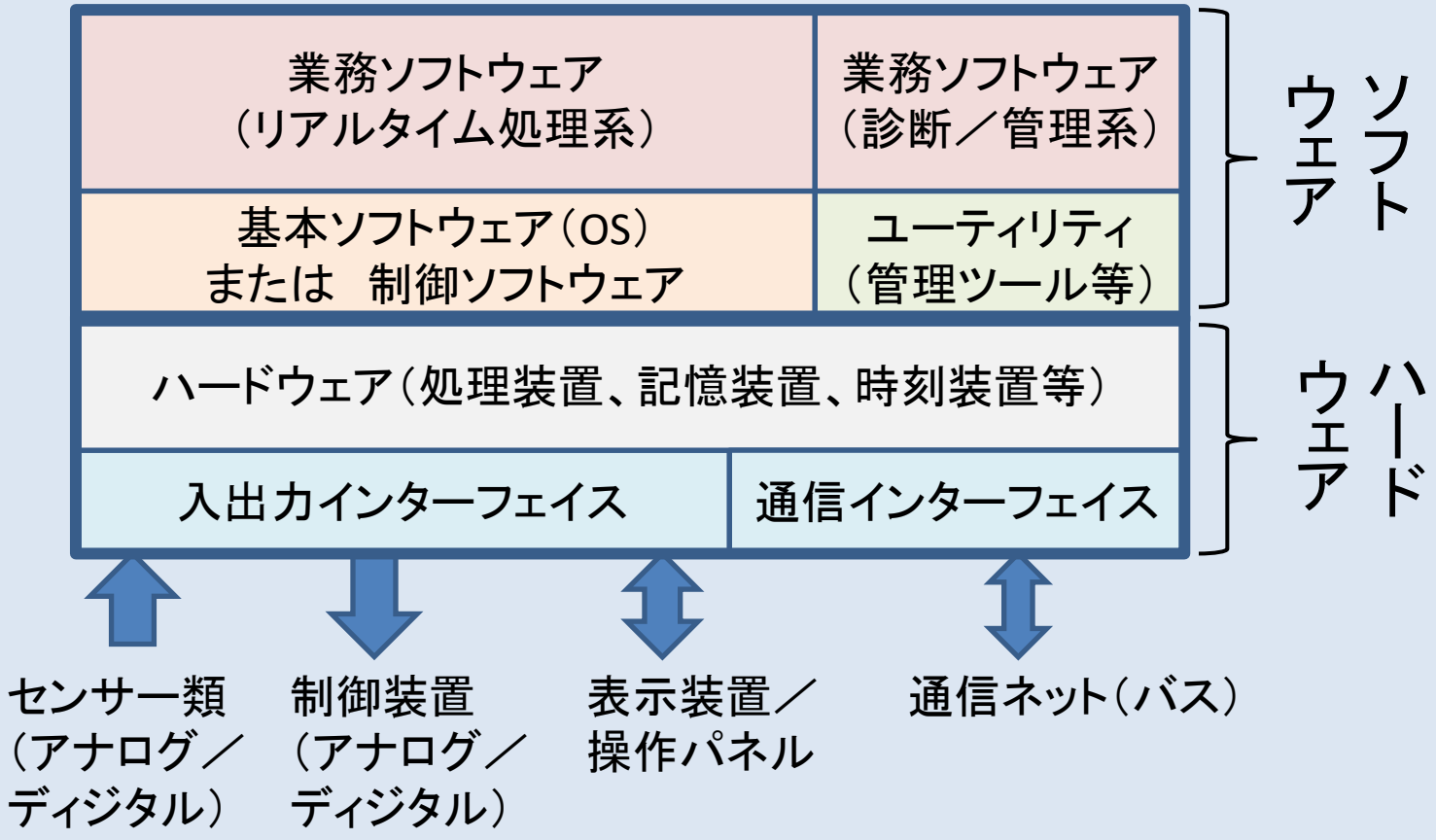
データ通信型

Part-1　情報システムとは何か
④一般的情報システムの構成



特徴：ソフトの比率が高い。汎用ソフトを多用。

Part-1　情報システムとは何か
⑤計測制御型システムの構成



特徴：専用ソフトが多い。アナログデータはデジタル変換。

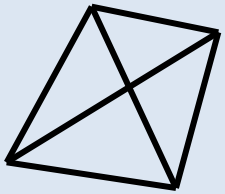
Part-2　情報システムの信頼性
①よく使われる信頼性指標

- 平均故障間隔
  （Mean Time Between Failure: MTBF)
- 平均修復時間
  （Mean Time To Repair：MTTR)
- 稼働率（Availability)

（例）99．9%　　1年間で8時間46分間停止
　　99．99%　　1年間で　　53分間停止
　　99．999%　　1年間で　　5分36秒間停止
　　99．9999%　1年間で　　32秒間停止
　　99．99999%　1年間で　　3秒間停止

（注）1年間＝3,600秒／時間×24時間／日×365．25日／年
　　＝31,557,600秒

Part-2　情報システムの信頼性
②多重化による信頼性向上



- ハードウェアの多重化

（例）航空機のエンジン／航法計器／通信機器
　　航空路監視レーダー／対空通信設備
　　金融機関など重要な情報システム機器

- ネットワークの多重化

（例）予備回線／複数回線
　　インターネット（冷戦時代の核攻撃対策として開発された！）
　　２系統の商用電源

- 代替手段による業務機能の維持

（例）DARC（Direct Access Radar Channel：予備用簡易レーダー表示装置）
　　管制塔のライトガン／バッテリー方式の非常用無線機
　　UPS（無停電電源装置）／非常用発電機

余談1：一回り小さな予備システム

- 侍は大小二本の刀を持ち歩いた。小刀は大刀が折れた場合に戦い続けるための予備となる。
- 船舶は遭難に備え、最小限の水と食料、通信機を搭載した救命ボートを準備している。
- 金融機関は、夜間や週末に機能を限定した予備システムを運用している。

Part-2　情報システムの信頼性
③障害時の影響の最小化

- フェイルセーフ（Fail Safe)

  故障などにより障害が発生しても、常に安全側に制御する設計手法

  （例）鉄道車両はブレーキ故障時に非常ブレーキがかかる
  　　鉄道信号は異常時や停電時は必ず「赤」となる

- フェイルソフト（Fail Soft)

  故障個所を切り離して被害を最小限に抑え、機能は低下してもシステムを停止させず、主要機能を維持する設計方式

- フォールトトレラント（Fault Tolerant)

  一部に問題が生じても、全体が機能停止せず動作し続けるような設計手法（≒構成要素の多重化＋動作継続制御）

  （例）フォールトトレラント・コンピュータ／ノンストップ・コンピュータ

Part-2　情報システムの信頼性
①ソフトウェアとは何か

ソフトウェア
Software
軟件（軟體）

金物屋の金物（ハードウェア）の反対語（造語）

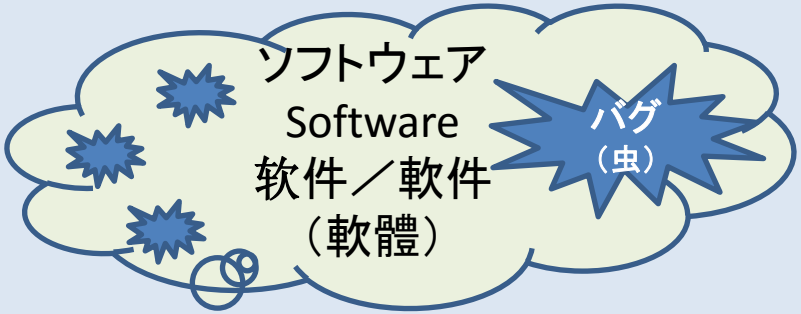
- ソフトウェア設計書（基本設計書、詳細設計書、変更記録など）
- **プログラムのソースコード（プログラム言語で記述）**
  標題等の基本情報、データ定義、実行コード、コメント
- **プログラムのオブジェクト（実行可能な機械語形式）**
- **プログラムの実行に必要なパラメータ類**
- **プログラムが参照するデータテーブル**
- **ジョブ制御情報（JCL）／リンク情報**
- 試験仕様（試験の方法、データ、結果など）
- 保守履歴（障害記録、仕様変更／修正記録、運用記録など）
- 保守マニュアル／保守ツール
- 運用管理マニュアル／運用管理上のノウハウ
- 利用者用操作マニュアル／利用上のノウハウ

狭義のソフト

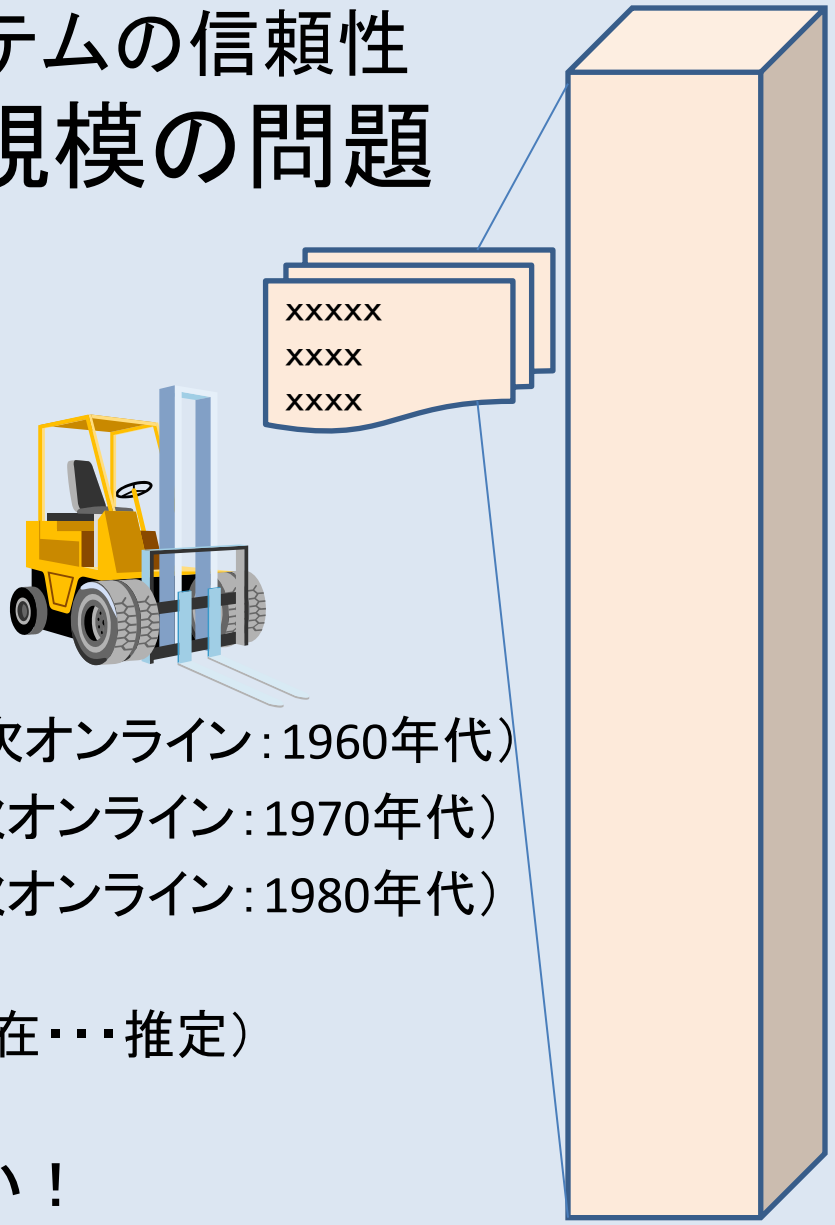
広義のソフト

Part-2　情報システムの信頼性
②品質の高いソフトウェアとは

- システムが停止しない
  （無限ループ、メモリ不正アクセス、入出力異常、不正演算などで停止）
- 必要なときに確実に動作する
- データが正しく入出力される
- 正しい処理結果が得られる（数値計算では一定の誤差範囲）
- 正しいタイミングで処理される
- 例外処理が適切に行われる
- データが無くならない
- データが正しく蓄積／更新される
- 操作／設定が容易
- 適切なチェックポイント／リカバリポイントが設定されている
- 機能の追加／変更、容量拡大などが容易（構造、論理、表現、・・・）



Part-2　情報システムの信頼性
③プログラム規模の問題



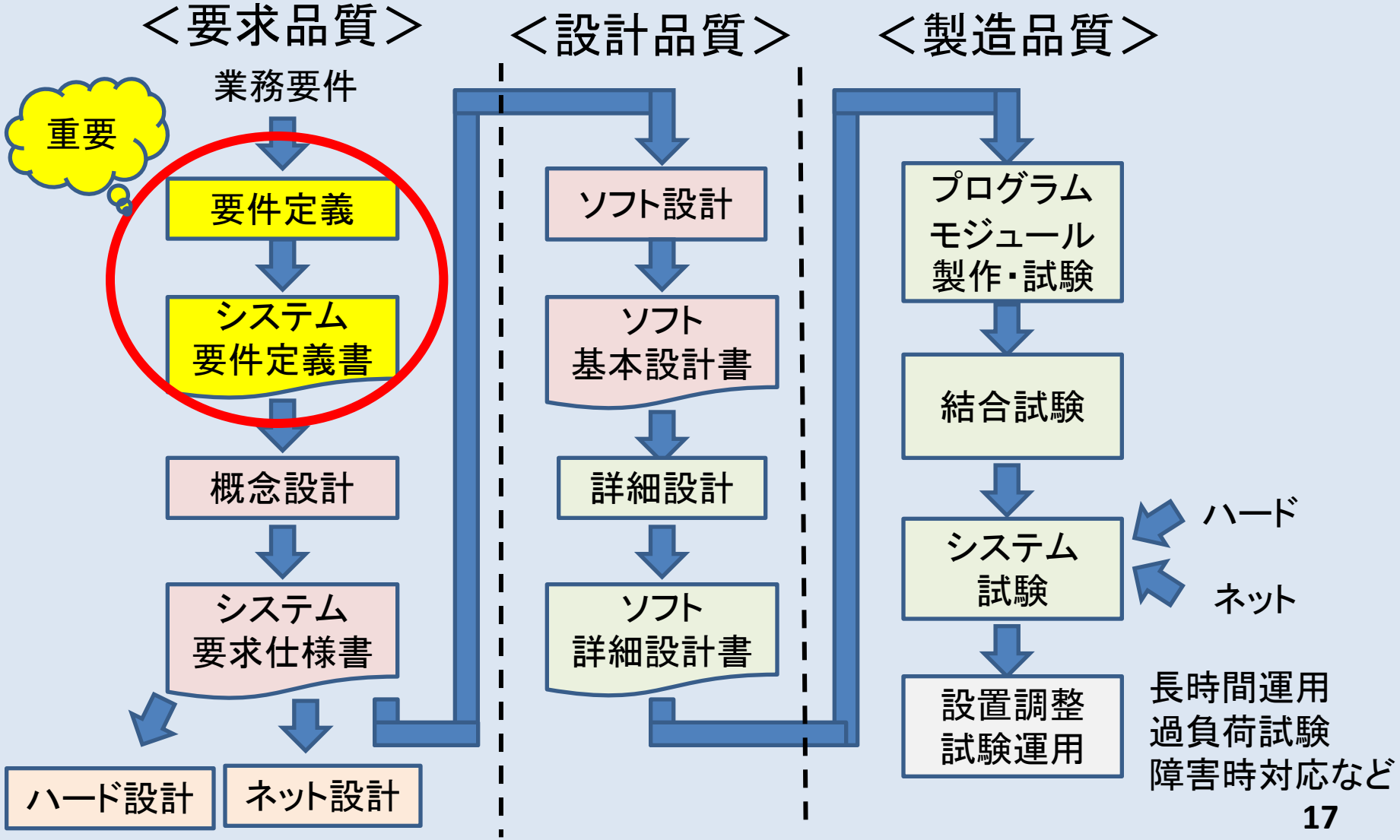
- 自動車　700万ステップ
  （カーナビは除く）
- 携帯電話　1,000万ステップ
- 社会保険庁　2,100万ステップ
- MS-Windows XP　4,000万ステップ
- ゆうちょ　5,130万ステップ
- 銀行システム　50万ステップ（1次オンライン：1960年代）
  200万ステップ（2次オンライン：1970年代）
  700万ステップ（3次オンライン：1980年代）
  ・・・・・・
  10,000万ステップ（現在・・・推定）

＊人為的間違いがないはずがない！

大銀行合併時のプロジェクト・・・6,000人（4,000億円）

Part-2　情報システムの信頼性

④設計品質と製造品質



Part-2　情報システムの信頼性
⑤運用管理の品質

- 操作ミス⇒システム停止／データ喪失
  - 運用管理方式が未確立
  - 要員の教育訓練が不十分 （特に異常時対応）
- 不適切なインフラ管理⇒システム停止／データ喪失
  - 電源喪失
  - 空調停止
  - ネットワーク
- 不適切なソフト保守⇒システム停止／誤処理
  - バージョン管理
  - 試験範囲

Part-3　情報システムの障害
①典型的な発生パターン

- システムが停止する
  - 短時間で復旧できる（データは保持される）
  - 再起動できるが、データが失われる
  - 再起動してもまたすぐ停止する
  - 全く動かなくなる
- データが入力されない
- 処理結果（出力）が得られない
- 処理結果が正しくない
- 処理タイミングが正しくない
- 処理が遅い
- データの破損／喪失

Part-3　情報システムの障害
②設計ミス／想定漏れに起因

- スペースシャトル初号機（コロンビア）は飛行制御システムのソフト不具合により打上げが1カ月遅れた（1981年4月）。
  多数決方式の複数コンピュータ間で初期タイミングが合わず無限にやり直し続けたため。
  （主：4台＋予備：1台＝合計：5台）

- うるう年（1996年）の大晦日に、ニュージーランドのAluminum Smelter社のアルミ精錬工場ですべての溶解炉が停止した。
  制御システムのプログラムが366日目を想定していなかった。損害額は100万NZドル。

Part-3　情報システムの障害
③想定以上の過負荷に起因

- 2006年1月18日に、東京証券取引所の売買システムがライブドア事件に伴う大量の売注文を処理できず、全銘柄の取引停止。
  システムが旧式で拡張性がなく、処理能力を増強した新システムへの移行は2010年１月まで4年もかかった。

- 2011年3月19～21日の3連休に、みずほ銀行のすべてのATMが停止。
  大震災の義捐金振込が特定口座に集中。夜間バッチ処理が翌朝のオンライン処理開始に間に合わなくなった。データ容量設定ミスや操作ミスも重なった。

Part-3　情報システムの障害
④操作ミスの複合に起因

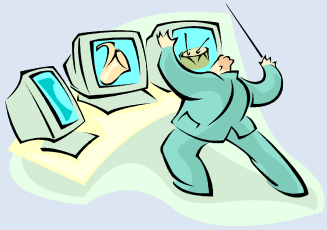
- 2005年12月8日、みずほ証券が新規上場のジェイコム株の売注文を誤入力：「61万円で1株」⇒「1円で61万株」買注文の殺到で東証の売買システムがパンク。注文の取消に手間取っている間に多額の損害が発生。
  - みずほ証券は414億円の損害賠償を請求。
  - 地裁は東証に約107億円の支払を命じた。
  - みずほ証券はこれを不服として控訴。
  - 最高裁により東証の107億円の支払が確定

- 2012年6月20日、ファーストサーバ社のレンタルサーバに預けられていた5698社分のWEBデータが完全消失した。データバックアップを取っていなかったため、大部分が復旧できなかった。原因は作業ミス（詳細は未公表）。

Part-3　情報システムの障害
④障害処理の不具合に起因

- 2012年8月7日、東証の派生商品（デリバティブ）売買システムの障害により全銘柄の取引を停止した。
  原因：デリバティブ取引システムと構内ネットの間のL3スイッチ（２重化）の障害。
  自動切替ソフトに不具合。
- 2012年1月25日、KDDIのau携帯電話、固定通信、法人系サービスが東京都西部で利用しずらい状態になった。

  原因：制御基板のメモリ処理容量不足で動作異常となったが、冗長切替機能（ソフトウェア）に不備があった。



Part-3　情報システムの障害
⑤運用管理上の不作為に起因

- 2005年8月2日に、羽田空港の管制施設への電源供給が止まりレーダー等が使えなくなった。
  商用2系統、予備発電機があるにも関わらず、保守時の切替ミスで無停電電源装置のバッテリーを使い果たしたため。
- インターネットプロバイダA社のデータセンターで突然停電。
  サーバーを次々に増設し、電力消費量が限度を超えたため。管理者は容量の問題を全く意識していなかった。
- クレジット会社B社でシステム操作記録ファイルがパンクし、システムが停止。
  記憶装置の容量は十分にあるのに上限値の設定が不適切だったため。

Part-3　情報システムの障害
⑥バックアップセンターによる復旧

- 1989年10月のサンフランシスコ大地震で通販会社の受注システムが停止。

⇒　電話オペレータ約200人を飛行機でシカゴに移動させ、オヘア空港隣接のバックアップセンターで業務を継続。

- 1996年5月にパリのクレディ・リヨネ銀行本店で火災が起き、金融商品取引システムが焼失。

⇒　システムはブリュッセルとロンドンで相互バックアップされていたので、担当者が移動して翌日から業務を再開。

クレディ・リヨネ銀行の正面入口

Part-3　情報システムの障害
⑦事業継続計画（BCP）による対策

- 2001年9月11日のアメリカ同時多発テロ事件でニューヨークの世界貿易センター入居企業は壊滅的な被害を受けた。

⇒　大手金融機関はバックアップシステムを含む事業継続計画（BCP)が義務付けられていたため、業務機能もデータも喪失せず、代替要員により別な場所で業務継続できた。

＊中小企業は事業データを喪失し、多くが倒産した。

BCP：Business Continuity Planning

Part-3　情報システムの障害
⑧人的対応による代替

- 1969年7月20日、アポロ11号の月着陸船イーグルが月面降下中に、飛行制御システムがオーバーフローした。
  ⇒　オルドリン飛行士は飛行制御システムの電源を切り、手動操縦により無事月面に着陸した。
- NASAの研究所の廊下に「いざという時はこれを使え」と算盤（そろばん）が展示。
- NASAにAbacus Technology（「算盤技術！」）という関連企業がある（同社製解析ソフト：Abacus）。

2008年にスペースシャトル「ディスカバリー号」に搭乗した宇宙飛行士星出彰彦さん携帯のアルミ製「宇宙ソロバン」（NASA認定の記念品）

万一の障害時に備え、原始的な航法も使えるように練習しておきましょう。

余談2：アポロ月着陸船操縦訓練シミュレーター

NASAのAMES研究所（カリフォルニア州サニーベイル）に稼働状態で保存されている

アポロ11号・月着陸船の誘導システムのソース

アポロ月着陸船）

［余談の余談］
同所のMoffet飛行場には海軍の飛行船用巨大なハンガーが残っている（解体費用が巨額なため）

Part-4　航空システムの障害事例
①管制システム障害でコンフリクト

- 1975年頃、羽田空港のARTSシステムと東京管制部のFDPシステムとの間のデータ交換開始直後、ARTS側から未定義の文字コードが送信されたためFDPシステムが停止。

⇒　たまたま新潟上空でシベリア方面行、札幌行、福岡行の3機が飛行しており、管制官が障害に気をとられている間にコンフリクト（規定の管制間隔が無くなる状況）が発生した。

［原因］

ARTSシステムとFDPシステムの間にあるデータ伝送システムの文字コード変換テーブルに誤りがあった。

Part-4　航空システムの障害事例
②管制システムの障害で欠航･遅延

- 2003年3月1日午前7時頃、東京航空交通管制部が運用する飛行計画情報処理システム（FDP）が障害で停止。欠航215便、大幅な遅延1500便、足止めされた客30万人。

- 午前1時に防衛庁と東京航空交通管制部で飛行計画をやり取りする「防衛庁システム対応プログラム」が追加され稼働。

- 午前7時に「オンライン統計処理プログラム」が自動起動され、「防衛庁システム対応プログラム」と矛盾が発生した。

- 原因はメーカーの仕様があいまいで、起こりうる競合状況が想定されていなかったため。

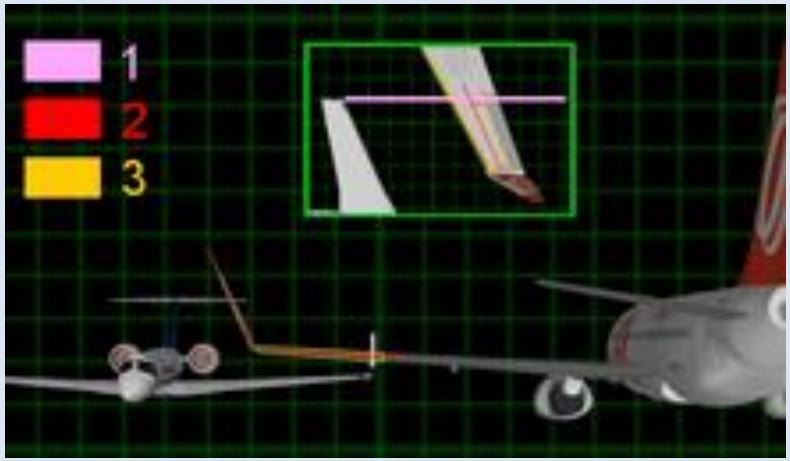
Part-4　航空システムの障害事例
③管制システムの障害で遅延

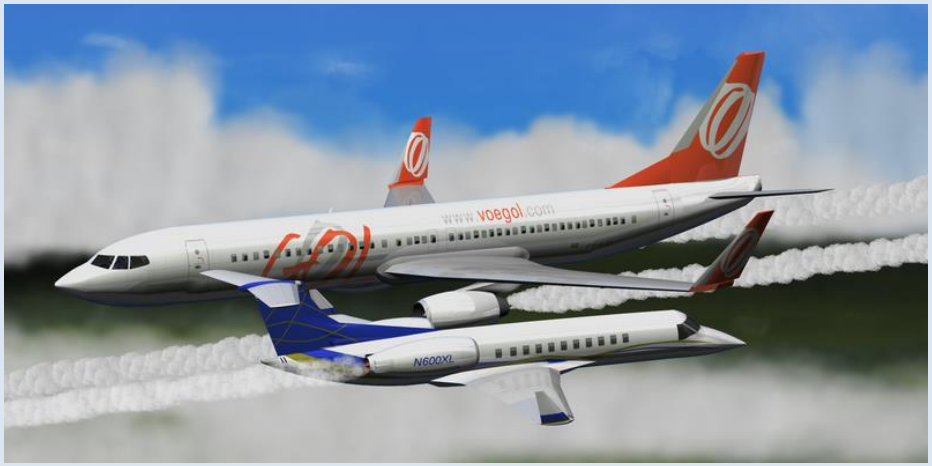
- 2004年4月8日19時11分に航空路レーダー情報処理システム（RDP）がダウンした。
- 名古屋発福岡行きの便の飛行計画情報にあり得ない経由地が含まれていたため、異常処理として自動再起動したがデータが残っていたためダウンと再起動を繰り返した。
- 予備系システムが稼働したが、業務の一部を人手で行ったため、国内便だけで130便に30分以上の遅れが出た。

- 国土交通省は、「FDPが持つデータや、RDPのハードディスクに書き込まれたデータの中に、不正なデータはなかった。メモリにデータを展開した際にソフトウエアを原因とする不具合が起こったと考えている」とした。

Part-4　航空システムの障害事例
④管制システムの不具合で空中衝突？

- 2006年9月29日にブラジル内陸部でブラジル・ゴル航空のB737-800と米エクセルエアのエンブライエル・レガシー600が、同一経路を同一高度で飛行して空中衝突。
- エンブライエルは近くの空港に緊急着陸したが、B737-800は空中分解して墜落。乗員乗客154名全員が死亡。
- 原因は調査中。管制システムが管制官の指示高度と航空機の飛行計画高度を混同した仕様だった、という説もある。





Part-4　航空システムの障害事例
⑤ソフトウェアのバグにより急降下

- 2008 年 10 月 7 日、豪カンタス航空のエアバス A330 が 急降下し、39 人が病院に運ばれ、うち 12 人が重傷を負った。オーストラリア交通安全局の調査報告書によれば、事故の原因は速度計の不具合と飛行操縦システムのバグ。

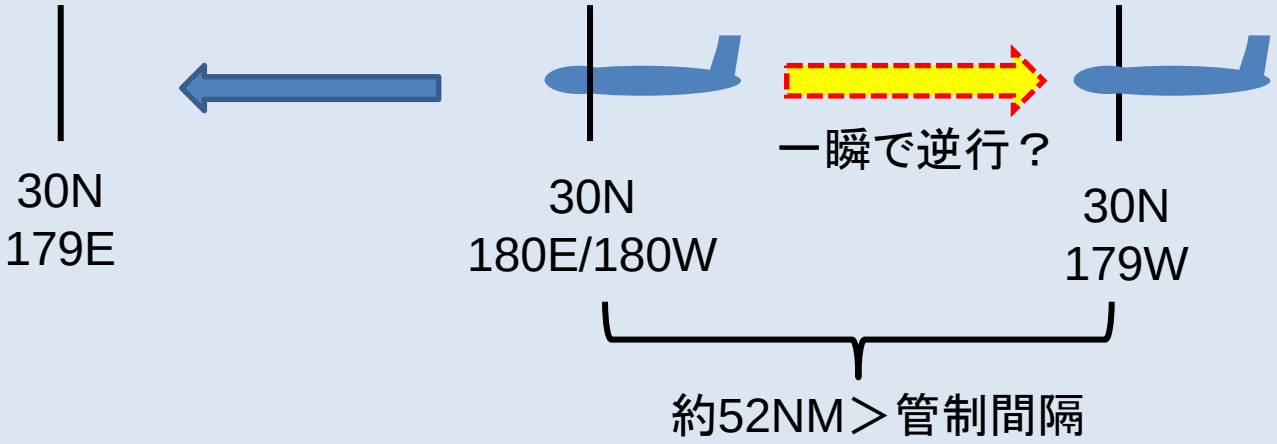
  http://it.slashdot.org/story/11/12/20/0127215/software-bug-caused-qantas-airbus-a330-to-nose-dive?sdsrc=rel
- 不具合を起こしたのは 3 つある速度計のうちの 1 つ。断続的に誤ったデータを飛行管理システム（FMS）に送信し続けていた。プログラムは 1990 年代に書かれたもので、速度計からの誤ったデータにより急降下を起こす可能性があった。

Air Data Computer

Part-4　航空システムの障害事例
⑥FMSが現在位置を誤表示

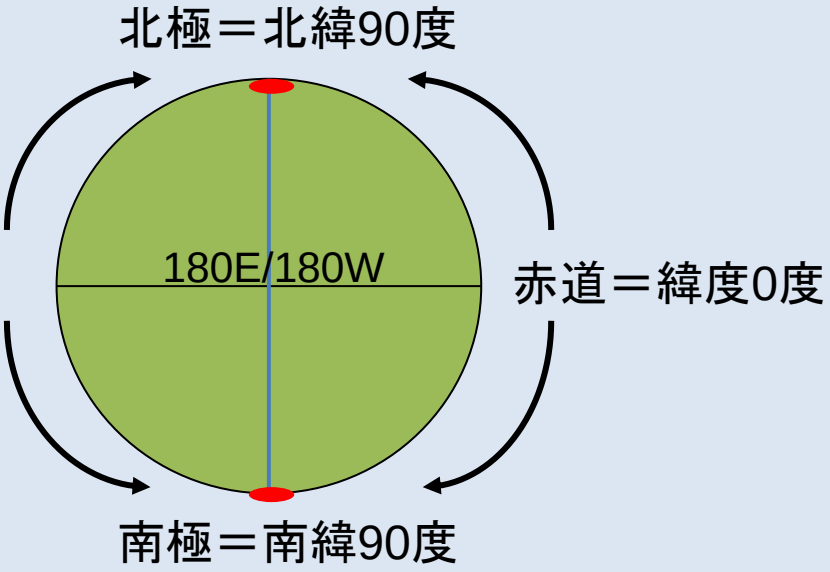
中部太平洋を西に飛行中の旅客機が180°に近づいたら、FMSが現在位置をW179°00′00″と表示した。

計算結果が179.9998度となったのを179度00分00秒と誤処理した？
パイロットは表示が異常であることに気付いたため問題なかった。



Part-4　航空システムの障害事例
⑦FMSが地球上にない位置を表示

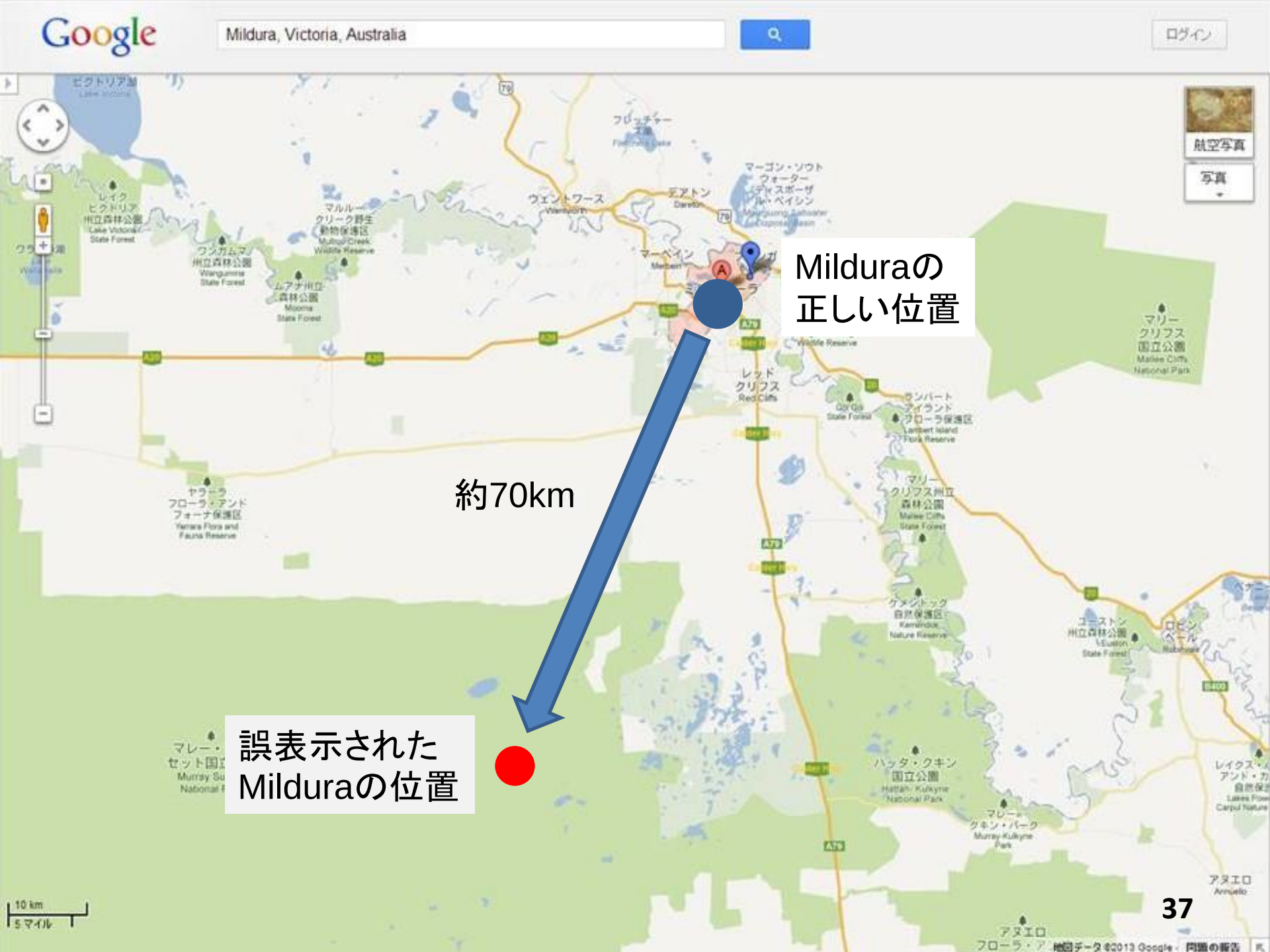
- 飛行中の旅客機が経度180度を通過した際、FMSが現在位置を“S180W180”と表示した。
- そんな場所は地球上にはないので、パイロットは異常に気がつき、問題は起きなかった（開発時のデフォルト値だった）。



S180（南緯180度）という場所は地球上にはない！

余談3：間違ったスマホ地図で遭難

- 【2012年12月10日 AFP】
  オーストラリアの警察当局は、地図の間違いで死亡する危険があるとして、米アップルのiPhoneの新しい地図アプリApple Mapsを使用しないようドライバーに警告。
- ビクトリア州内陸部の町ミルデューラ（Mildura）へ行こうとした車が「道を外れ」、約70キロ離れたマレー・サンセット国立公園の中央部へナビゲートされる事態が続出したため。
- 救出されたドライバーはこの数週間で6人。うち何人かは食料も水もない状態で最長24時間さまよった。公園内は気温が摂氏46度に達することもある過酷な環境だった。
- この事件でアップル社の幹部2名が辞職した。


Google
Mildura, Victoria, Australia
ログイン
航空写真
写真
Milduraの
正しい位置
約70km
誤表示された
Milduraの位置
10 km
5 マイル
37

Part-4　航空システムの障害事例
⑧国産哨戒機P-1の全エンジン停止

（第１報：平成25年6月20日　防衛省）

固定翼哨戒機Ｐ－１（５号機・６号機）の納入の遅延について

- 本年（2013年）5月13日、川崎重工業株式会社において製造中の固定翼哨戒機P-１の5号機について社内飛行試験の際、通常の運用では想定されない、高高度における高速度での急激な機動を行ったところ、エンジンが停止するという事象が発生しました。
- 原因究明の結果、同不具合はP-１の量産化にあたりエンジンの形状を一部変更したため、前述の急激な機動を行った際に、エンジンの燃焼が一時的に不安定となり発生したと判明しました。
- これを受け、Ｐ－１の量産機（注：３号機以降が量産機に該当）に対して不具合対応策を講じることとなったことから、今月末に納入される予定であった５号機及び６号機について、納入が遅延することとなりました。
- 既に厚木基地に配備されている量産機２機（３号機及び４号機）については、現在、飛行を停止しておりますが、更なる原因究明を進めるとともに不具合対応策を講じた後、飛行を再開する予定です。

国産哨戒機P-1の全エンジン停止（続）

（第2報：平成25年9月27日　防衛省）

固定翼哨戒機Ｐ－１のエンジン不具合への対応について

- 本年５月１３日、川崎重工業株式会社において製造中の固定翼哨戒機Ｐ－１の５号機について、社内飛行試験の際、通常の運用では想定されない、高高度における高速度での急激な機動を行ったところ、エンジン４発が停止するという事象が発生しました。
- 原因究明の結果、同不具合は、Ｐ－１の量産化にあたりエンジンの燃料噴射弁の肉厚を増加したことが原因となって、急激な機動を行なった際、エンジンの燃焼が一時的に不安定となったために発生したことが判明しました。
- これを受け、防衛省は、このような急激な機動を行った場合においてもエンジンの燃焼が不安定になることがないよう、エンジン制御ソフトウェアを改修することとしました。
- 今後、川崎重工業株式会社で製造中の量産機２機（５号機及び６号機）及び既に厚木基地に配備されている量産機２機（３号機及び４号機）について、上の改修を実施する予定です。これらの機体は、地上運転試験などを経て、飛行を再開する予定です。

国産哨戒機P-1のエンジン停止（考察）
（ソフト障害では機器多重化の意味がない！）

（経緯と考察）

- 発生は5月13日、公式発表は6月20日。単に「エンジンが停止」と発表。
- 記者会見では「複数エンジン」とし、台数は答えなかったが、その後の取材で「4基あるエンジン全部」の停止であったことを認めた。
- 不具合の発生状況は、愛知県沖の太平洋上で高度10,000mから8,000mに急降下後、エンジン出力を急激に下げながら飛行姿勢を立てなおしたところ、エンジンが止まった。乗員が再起動し、無事着陸したというもの。（2013年6月21日　毎日新聞、他）
- 防衛省の公式発表および記者会見を踏まえた報道を見る限り、直接的原因はソフトウェアの「バグ」（製造上のミス）ではないと思われる。
- 可能性が高いのは、エンジン形状（詳細不明）変更に伴う燃焼特性の変化を十分に確認（シミュレーションや実際の燃焼試験等で）せず、制御ソフトを変更しなかったソフト仕様の変更管理の問題と思われる。

IHI社製
XF7-10エンジン

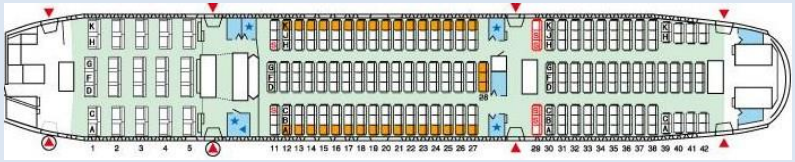
Part-4　航空システムの障害事例
⑨エンジンが起動しない

B787のエンジンが起動せず欠航、山口

- 2013/6/12 12:47 (2013/6/12 13:30更新)　12日午前9時ごろ、山口宇部空港で羽田行き全日空692便のボーイング787が駐機場を出発しようとした際、右エンジンが起動せず欠航した。乗客約140人は次の便や他社便に乗り換えた。

- 全日空によると、エンジン起動の際、電気を供給する機体の補助動力装置（APU）がうまく機能せず、地上電源からケーブルをつないでエンジンを起動しようとしたがかからなかった。
- APUの不具合とエンジントラブルの関連は不明でエンジン制御のコンピューターに問題があった可能性もあるという。
- 全日空787は10日にも、福岡空港で地上走行中にコックピットでエンジンの不具合が表示され、駐機場に引き返すトラブルがあった。〔共同〕

Part-4　航空システムの障害事例
⑩誤操作で座席指定10万席分が消失



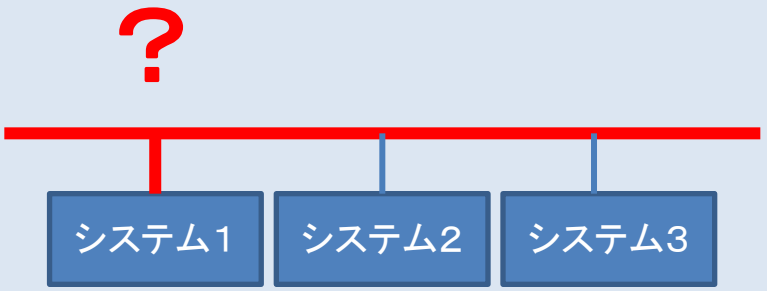
- 2012年11月、全日空国内線2013年2月分の座席指定約10万席分が、予約システムの不具合で取り消されていた。対象は11月26日午後6時までに購入した国内線航空券のうち2013年2月の搭乗分。

- 航空券の予約そのものには影響がなく、事前の座席指定情報のみが取り消されていた。ホームページ、国内線予約・案内センター、特設コールセンターで改めて座席を指定した。
- 原因は、営業担当者の操作ミス。2人でダブルチェックする体制にもかかわらず、予約システムの時刻表情報を更新する際に手順を守らず、誤って予約情報を消去してしまった。

Part-4　航空システムの障害事例
⑪成田空港で出国システムなど障害

- 2013年7月11日午前7時過ぎ、成田空港第2旅客ターミナルの出国審査場や荷物検査場のシステムに障害が発生し、出発ロビーは保安検査を待つ乗客約600名が行列を作るなど、一時混乱した。

- 障害が発生したのは出国審査場の出入国管理システムの一部と、航空機に積み込む受託手荷物の爆発部物を検査するシステム。
- 互いのシステムは独立しており、いずれも通信に不具合があった。



Part-4　航空システムの障害事例
⑫米航空会社でもシステム障害が頻発

- 2013年4月16日にアメリカン航空の予約システムで障害が発生し、1,950便が欠航ないし遅延。
- 2012年にユナイテッド航空とコンチネンタル航空が業務提携し、システム統合したが、機能不全が発生。米国全土の空港で大混乱が起きた。
- 2011年にユナイテッド航空の予約システムがネット接続の不具合で停止。大規模な欠航と遅延が発生。
- 2005年にUSエアウェイズとアメリカウェスト航空が合併した際も、ソフト統合で同様のトラブルが発生。

（出典：Wired）

Part-4　航空システムの障害事例
⑬ネット予約で航空券をタダで販売

- 米ユナイテッド航空が9月12日にインターネットを通じた予約販売で約１５分間、国内線の航空券を税別で無料、または10ドルの超格安で売り出す珍事がおきた。
- 原因は同社の手違いによるもの。ユナイテッド航空は「予約時に表示された価格で航空券を提供する」と説明。

(2013.9.15　日本経済新聞）

- 損害額は公表されていないが、ユナイテッド航空の対応は、法的な義務（錯誤による取引契約は取消し可能）を超える。
- 日々変動する運賃の単純な入力ミスが原因と思われる。
- 事務手順にチェックプロセスがなかったか省略した？
- 機械系に妥当性チェックの機能がなかった？

余談4：ハイフンひとつでロケットが爆発？

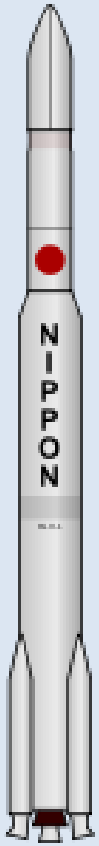
- 1962年7月に打上げられたNASAの金星探査衛星を搭載したマリナー1号は打上直後に軌道をそれ、指令破壊により爆破された。

マリナー1号の打上
（293秒後に爆破）

- ロケット設計者は速度測定レーダーのデータ“R”の値をスムージング処理して使うよう、“R”に”¯”(bar)をつけた計算式を手書きメモでプログラマに渡した。
- プログラマは計算式の意味を理解できず、スムージング処理なしの制御プログラムを書いたため速度データが正しく処理されず、ロケットは予定の軌道から外れた。
- 後年、この話が「“－”（ハイフン）のミス」と誤って伝えられ、ソフト業界の伝説になった。

$$\overline{R} \neq R$$

余談5：人工衛星運用管制システムのソフト障害



1回目の打上が失敗し、ソフト開発グループは解散。1年後に2回目の打上のためのリハーサル中に問題が発見されたが、原因不明。問題の現象が起きたら自動的にリセットする「姑息な」方法で暫定解決。
（B787のリチウムイオン電池の火災事故で、原因不明のまま対症療法で安全を確保し、飛行再開したのと同様の対応）

郵政省電波研究所鹿島支所にて(1978年)
（現・独立行政法人　情報通信研究所　鹿島宇宙技術センター）

Part-5　人工知能の動向と将来像
①人工知能とは何か

人間の知能と心の現象を
コンピューター上で実現
（さまざまな定義がある）

または

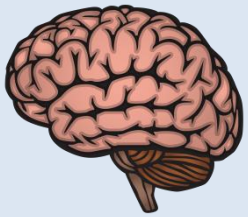
知能機械　　人間

交信

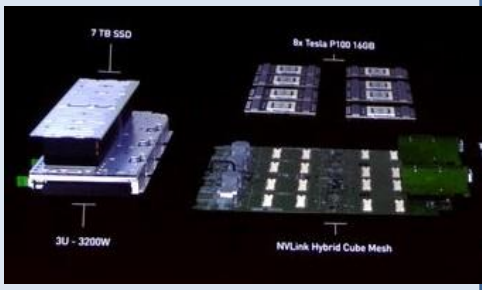
相手が人間か
機械か、区別
がつかない

知識（例：法則、ルールなど）
推論（例：ゲームの対戦など）
学習（例：知識の習得など）

人工知能（Artificial Intelligence）の二つの立場
①人間の知能そのものを持つ機械を作る
②人間が知能を使ってすることを機械にさせる
（研究の大部分が②の立場）



Part-5　人工知能の動向と将来像
②人工知能の歴史と最新動向



深層学習用スパコン
DGX-1

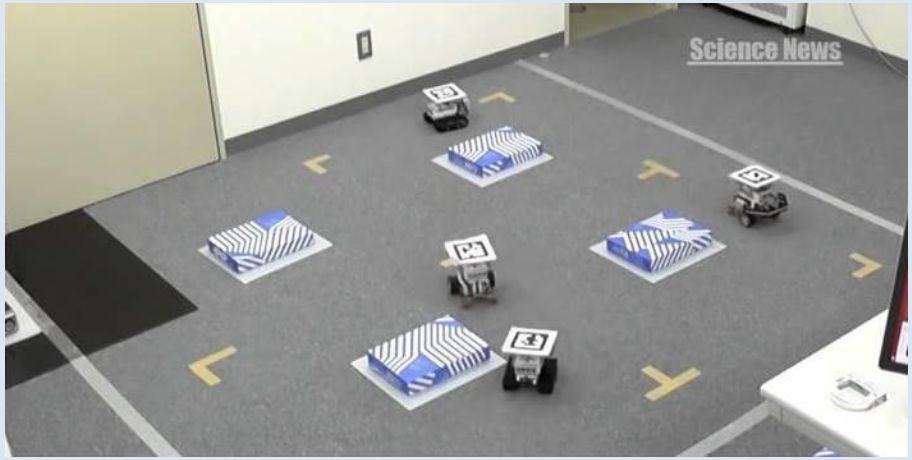
- 人工知能の歴史
  - ニューラルネットワークの研究（1940年代）
  - 人工知能の概念。プログラム言語LISP（1950年代）
  - 推論機能。プログラム言語PROLOG（1960-70年代）
  - 第五世代のコンピューター開発プロジェクト（1980年代）
    （知識ベース＋推論マシン「Ψ（プサイ）」によるエキスパートシステム）
  - チェスで「ディープブルー」が世界チャンピオンに勝利（1997）
- 最新動向：深層学習(Deep Learning)により急激に発達
  - 証券取引、金融商品説明、報道記事執筆等、様々な分野で実用化。
  - 国立情報学研究所の人工知能が東大入学問題に挑戦（2013～）
  - Google開発の無人運転自動車の公道実験開始（2015）
  - Google開発の人工知能AlphaGoが碁の名人に勝利（2016）
  - Ponanzaがプロ棋士に勝利。羽生名人が「叡王戦」出馬表明（2016）

Part-5　人工知能の動向と将来像
③最先端の人工知能技術（ビデオ）

https://www.youtube.com/watch?v=JGaHwOubY4Q

[Science News 2016]　ディープラーニング

最新の人工知能アルゴリズム（2016年1月）　4分59秒



- ブロック崩しゲーム
- 機械学習／ディープラーニング
- 画像分類コンテスト
- ニューラルネットワーク
- 自動運転の自動車
- 強化学習
- 交通システムの研究：モデルカーのシミュレーション
- ディープラーニングを使った作業ロボット

Part-5　人工知能の動向と将来像

④人工知能の将来像

（私見：超便利だが怖いリスクも一杯！）

- 人工知能は人間を超えるか・・・Yes！
  - 人間が教える限り名人レベルが上限
  - 機械学習により人工知能どうしが競えば無限
- 人間は不要になるか・・・No！
  - システム要件の定義
  - 機械学習結果の良否（判定基準）を示す
  - 「ロボット三原則」の遵守状況を監視する
- 人工知能のリスク（SF映画が現実に）
  - 倫理的に問題のある内容を学習
  - 人間に危害を加える兵器への応用
  - 「ビッグブラザー」になり大衆を支配
  - 人工知能（ロボット）が人類に反逆

余談6：航空機の信頼性の究極の向上策

資料：米国運輸省ボルペ研究所

＜ご静聴ありがとうございました＞