航空機のネットワーク化と搭載システムソフトウェアの認証

２０１４年１０月４日（土）

航空運航システム研究会（TFOS.SG)
航空システム部会　　松田　宏

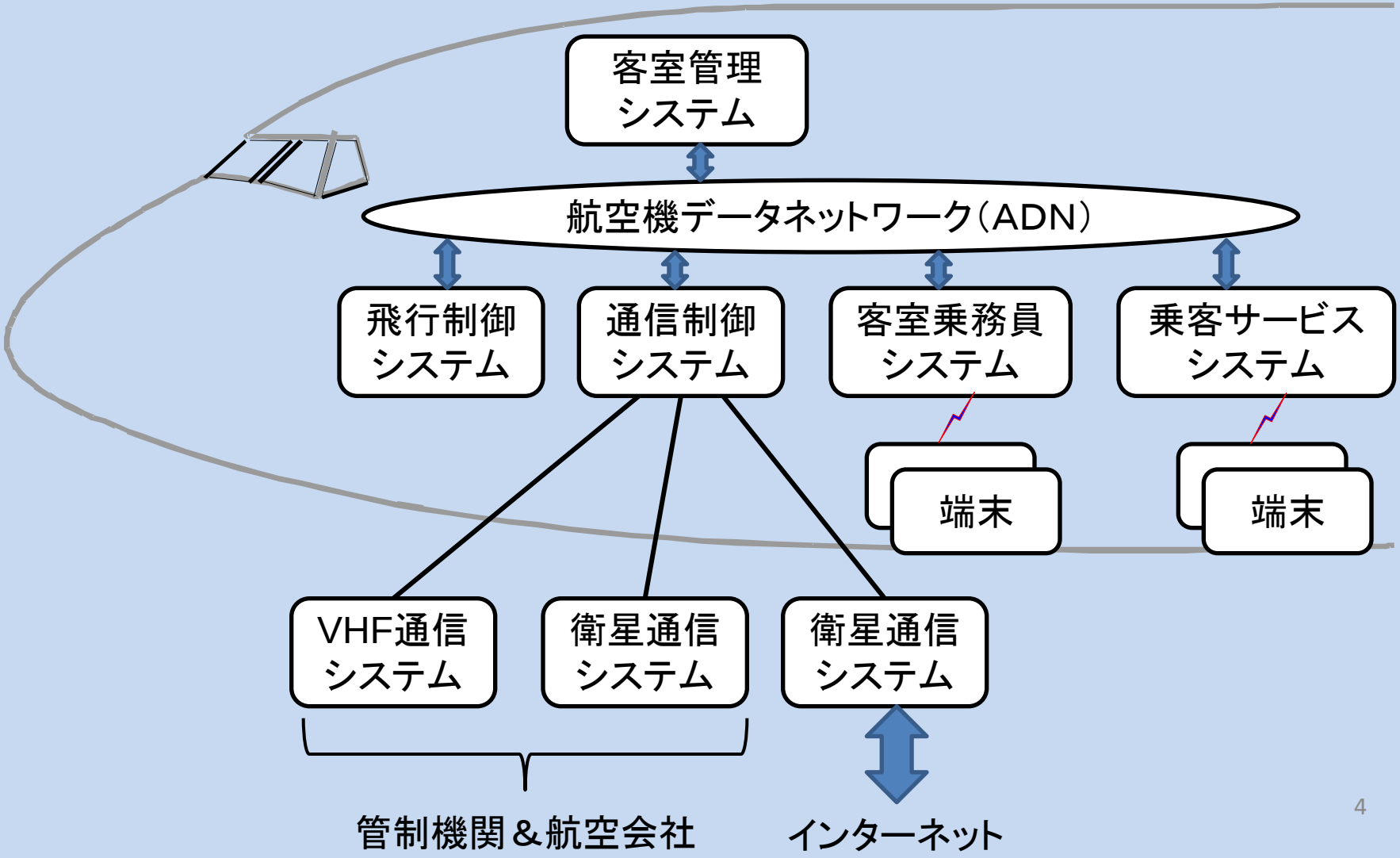
今日のテーマ

- 航空機のネットワーク化に伴う問題
  - 機内データネットワーク(AND)のセキュリティ
  - 搭載システムのソフトウェア更新
- 搭載システムのソフトウェア認証に関する規定
  - RTCA DO-178C / EUROCAE ED-12C
  - FAA AC 20-115C

航空機データネットワーク（ADN）

- 特殊ミッションの軍用機では、通信ケーブル類の重量削減のため、古くから機内情報通信を統合しネットワーク化してきた。
  - 早期警戒管制機
  - 大統領専用機エアフォース・ワン
  - C-130Jスーパーハーキュリーズなどの新世代機
- 民間機でもB787やA380／350からインターネット技術による航空機データネットワーク（Aircraft Data Network：ADN）を導入した。
- 客室内でWifi無線LANによるブロードバンド・インターネットやスマホ通話サービスを提供するようになった。

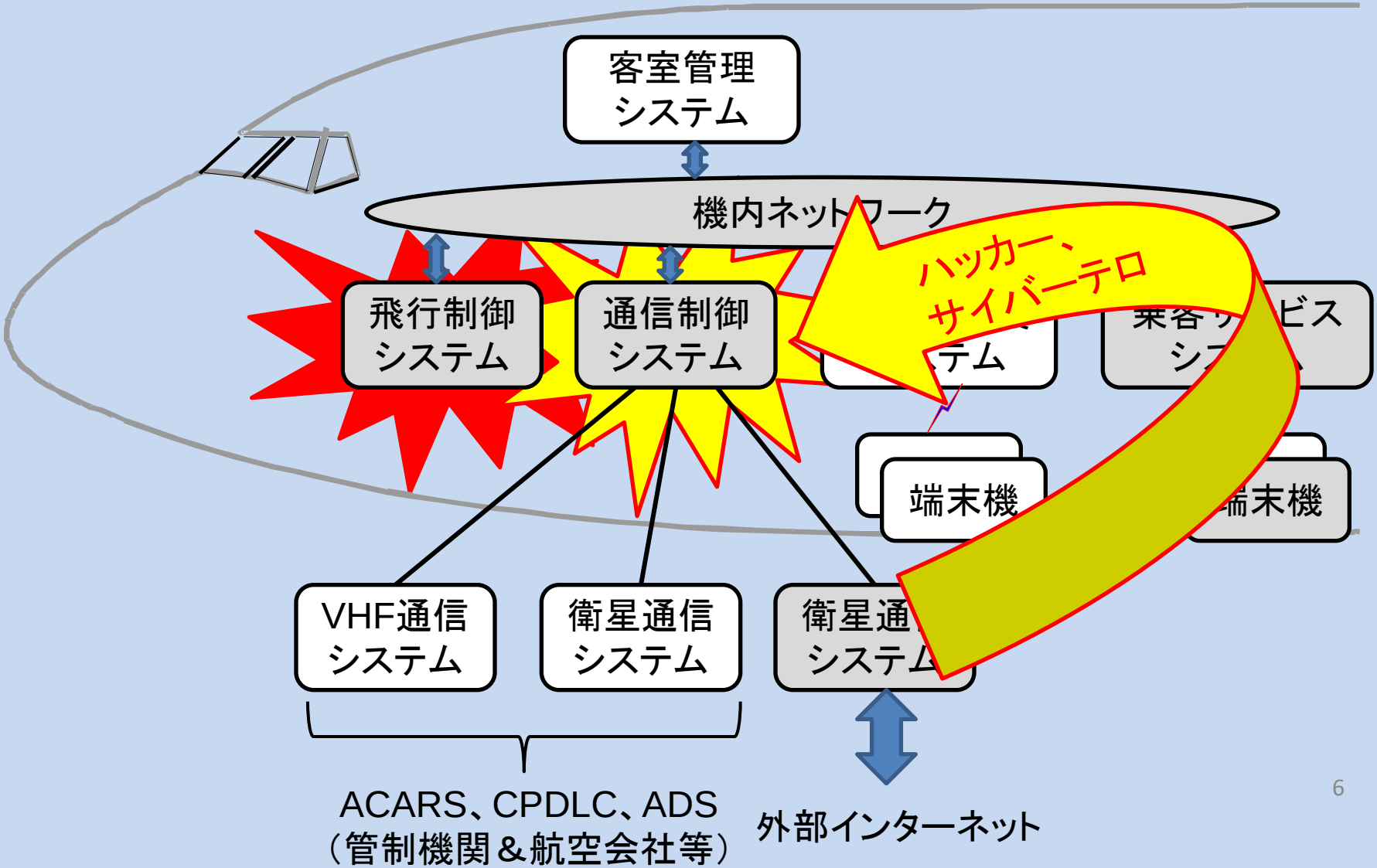
航空機データネットワークの構成



機内データネットワークのセキュリティ

- 航空機運航の安全性にかかわる重要な情報と、乗客サービスのインターネット等の情報がネット上で混在する。
- 航空機は、機内データネットワーク経由で地上の多数の組織や個人と常時接続されているので、脆弱な部分が多い。
  - 航空機製造会社、エンジン製造業者
  - 運航会社、整備業者、空港サービス業者など
  - 管制機関／航空通信会社
  - インターネットサービス業者／電話会社など
  - 地上のインターネット／電話の利用者
- 地上または機内からのハッカー、サーバー犯罪、テロなどに対するセキュリティ対策が不十分なのでは？

航空機データネットワークの脆弱性



搭載システムのソフトウェア更新問題

- 搭載システムのソフトウェア更新を整備時に限定せず、空港ゲートで高速無線ネットワークによって行うことが可能に。
- ソフトウェアは飛行管理システム（FMS）や電子飛行バッグ（EFB)のデータベースと比較すると、はるかに重要。
- FMSの飛行計画データや気象データは量的に少ないので、伝送速度の遅いACARSやCPDLCで更新されている。
- 対象となる航空機は世界中を飛び回っている。最新のソフトウェアが正しく実装されるには、次のような対策が必要。
  - 種類やバージョンの確認と誤りの検出
  - 伝送途中での誤配、喪失、破損などの検出と再送
  - 悪意の改竄、すり替え、攻撃などの検出と防止

資料：セキュリティ向上活動の歴史（1）

Secure Aircraft Data Network（SADN）Researches

- FAA
  - Network Security and Safety Aircraft LAN Study
  - Automated Airborne Flight Alert System (AAFAS)
  - Boeing 787 Security Issue Papers
  - Airborne Internet（A.I.）
- 業界
  - ARINC/AEEC Subcommittees (ADN & SEC)
  - ATA E-Biz's Digital Security Working Group (DSWG)
  - EUROCAE WG-72 Aeronautical System Security WG
- 国防総省
  - USAF Airborne Network (AN) Project
  - USAF Multi-sensor Command & Control Aircraft
  - JPDO Global Information Grid

資料：米運輸省ボルペ研究所

資料：セキュリティ向上活動の歴史（2）

Secure Aircraft Data Network（SADN）Researches

- FAA
  - GCNSS Network-enabled Operations (NEO) Airspace Security Demo
  - ISS R&D Program Planning Team (PPT)
- NASA
  - Mobile Communications Network Architecture (MCNA)
  - ADS-B Security Project
  - Aircraft Centric Data and Information Communications Systems Security
    - Assessment report
    - Policy report
- 業界
  - Transatlantic Secure Collaboration Program-TSCP
  - Wireless Communications Consortium
- 国防総省
  - TWIC (& HPSD-12) - logical access smart cards
  - Computer Security Information Assurance (CSIA) R&D Working Group

資料：米運輸省ボルペ研究所

民間機搭載ソフトウェアの認証規定

- 搭載システムのソフトウェア認証に関する規定はない？
- Federal Aviation Regulation (FAR) では、Part 33 “Accessory Attachment”のSection 28 “Electrical and electronic engine control systems”が「ソフトウェア」という言葉が出てくる唯一のセクション?

  ［規定内容］ 正常な運航のため、電気的または電子的な手段に依存する各制御システムは、
  - エンジン出力／推力の喪失、安全でない状況をもたらすエラーが起きないようソフトウェアを設計・実装しなければならない。
  - また、ソフトウェアの設計・実装は、FAAから認定された方法で行わなければならない。

資料：FAR　Part 33　Section 28

Electrical and electronic engine control systems

FAR　Part 33　Section 28

Each control system which relies on electrical and electronic means for normal operation must:

(a) Have the control system description, the percent of available power or trust controlled in both normal operation and failure conditions, and the range of control of other controlled functions, specified in the instruction manual required by §33.5 for the engine;

(b) Be designed and constructed so that any failure of aircraft-supplied power or data will not result in an unacceptable change in power or thrust, or prevent continued safe operation of the engine;

(c) Be designed and constructed so that no single failure or malfunction, or probable combination of failures of electrical or electronic components of the control system, results in an unsafe condition;

(d) Have environmental limits, including transients caused by lightning strikes, specified in the instruction manual; and

(e) Have all associated software designed and implemented to prevent errors that would result in an unacceptable loss of power or thrust, or other unsafe condition, and have the method used to design and implement the software approved by the Administrator.

[Doc. No. 24466, 58 FR 29095, May 18, 1993]

RTCAの搭載ソフトウェアに関する文書

DO-178C 航空機搭載システムおよび機器の認証におけるソフトウェア考察

RTCA（Radio Telecommunication Commission for Aviation）

DO-178C “Software Consideration in Airborne Systems and Equipment Certification（2012）

- FAAはDO-178B(2001)の妥当性を認識し、承認基準としたが、関係者からは定義や対象範囲の明確化を求められた。
- RTCAとEUROCAE（European Organization for Civil Aviation Equipmentが共同委員会を組織して改定作業を行った。
  - RTCA特別委員会　SC-205
  - EUROCAE作業部会　WG-71
- EUROCAE発行の欧州基準ED-12B(2001)およびED-12C(2012)の内容は、RTCAのDO-178BおよびDO-178Cと同じである。

RTCA DO-178Cの概要（1）
位置づけと発行経緯

- *R*TCA DO-178C（＝EUROCAE ED-12C）は、FAA、EASA、カナダ運輸省などの航空当局が民間航空機のソフトウェアベース・システムを承認するための重要文書。
- RTCAとEUROCAEによる共同作業で旧版の*R*TCA DO-178B（＝EUROCAE ED-12B）の改定版として作成され、2012年1月に発行された。
- FAAは2012年7月にAC 20-115Cを承認し、DO-178Cを「航空機搭載システムのソフトウェアの側面に関して適用すべき耐空性規則として遵守する」という見解を明らかにした。

AC 20-115C　Airborne Software Assurance

（航空機搭載ソフトウェアの保証）

RTCA DO-178Cの概要（2）
委員会の構成

- 委員会は次の7分科会（Subgroup)から構成された。

SG1：　委員会（SC＆WG)の文書構成
SG2:　課題と理論的根拠
SG3:　ツールの品質評価
SG4:　モデルベースの開発と検証
SG5：　オブジェクトオリエンテッド技術
SG6：　公式な方式
SG7：　安全に関連する考慮点

RTCA DO-178Cの概要（3）
ソフトウェアレベルの区分

- A（壊滅的） 障害が複数の致命的事態、通常は航空機の喪失に至るもの
- B（危険な） 障害が安全性や性能、乗務員の身体的疲労や過大な負荷、乗客の重大／致命的な怪我など、大きな負の影響を与えるもの
- C（大きな） 障害が安全性の余裕の著しい減少や乗務員の多大な負担増をもたらすもの。乗客の不快感や軽傷など。
- D（小さな） 障害が若干の安全性の余裕の減少や乗務員の負担増をもたらすもの。例えば乗客に不便をもたらしたり日常的な飛行計画の変更をしたりすること。
- E（無害な） 障害が安全性、航空機の運航、乗員の負荷に影響を与えないもの。

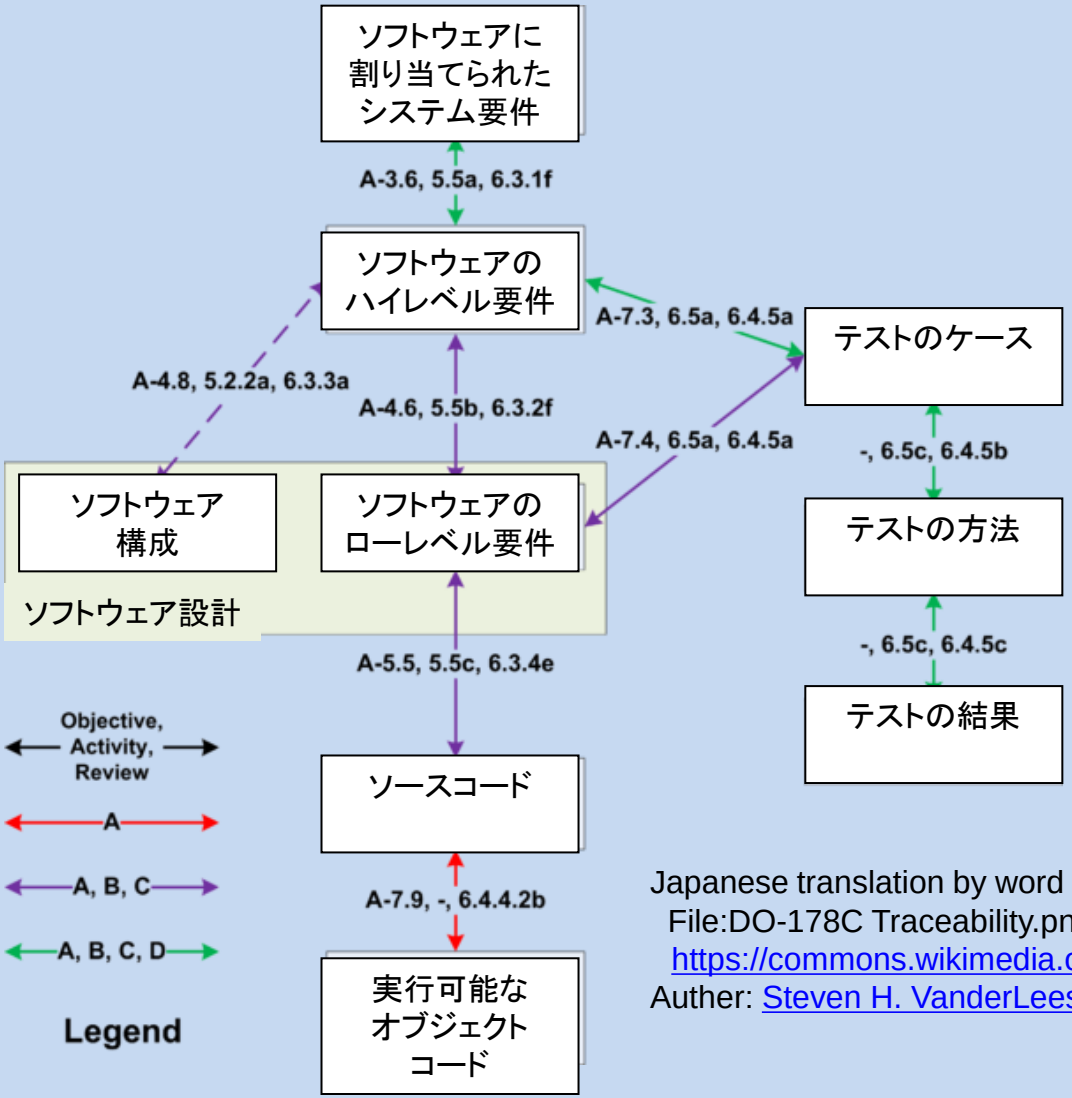
RTCA DO-178Cの概要（4）

障害レベル毎の目標項目数

レベル	障害条件	目標項目数	独自項目数
A	壊滅的（Catastrophic）	71	33
B	危険な（Hazardous）	69	21
C	大きな（Major）	62	8
D	小さな（Minor）	26	5
E	無害な（No Safety Effect）	0	0

RTCA DO-178Cの概要（5）

システム要件⇒実行オブジェクトコードのトレーサビリティ



Japanese translation by word to word from the following:
File:DO-178C Traceability.png
https://commons.wikimedia.org/wiki/File:DO-178C_Traceability.png
Auther: Steven H. VanderLeest

RTCA DO-178Cの概要（6）
DO-178Bとの主な相違点

- より明確で統一された表現と用語
- 目標項目を追加 (レベル A, B,および C)
- 「隠れた目標」の明確化

  例：DO-178Bの6.4.4.2b項に記述されているのに付録Aの表から抜けている項目。この目標は現在、DO－178C,付録Aの表A-7、目標9「ソースコードからでは判別できない新しいコード追加の検証が行われること」にリストアップされている。
- パラメータデータ項目ファイル：　実行形式のオブジェクトコードに影響を与えないよう分離された情報を提供。

  例：分割されたオペレーティングシステムのスケジュールと主要時間枠に設定される構成ファイルがある。このパラメータデータ項目ファイルは、実行オブジェクトコードと一緒に検証され、またはパラメータデータ項目のすべての範囲がテストされなければならない。

RTCA DO-178Cの概要（7）
関連する技術情報（Technology supplement）

- DO-330 “Software Tool Qualification Considerations” – ソフトウェア・ツールとアビオニクス・ツールの適格性評価方法を明らかにする

- DO-331 “Model-Based Development and Verification Supplement to DO-178C and DO-278” – モデリング方式につきものの落とし穴を予防し、開発・検証を改善するためのモデルベース開発 (MBD) と検証、モデリング技術の使用能力の解説

- DO-332 “Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A” – オブジェクトオリエンテッドなソフトウェア技術とその使用条件を解説

- DO-333 “Formal Methods Supplement to DO-178C and DO-278A” – テストを補完する（置換えるのではなく）公式な方法を解説

FAA　AC 20-115Cの概要
搭載ソフトウェアの保証

- ”AC 20-115C Airborne Software Assurance（搭載ソフトウェアの保証）”は、FAA のAviation Safety - Aircraft Certification Service, Aircraft Engineering Division（AIR-120）が2013年7月に発行したAdvisory Circular（AC）
- このACは、航空機搭載システム／機器のソフトウェアに関する耐空性規則の適用について、適合のひとつの方法（唯一の方法ではなく）として記述している。
- FAAはこのACをRTCAの次の文書を認可して書いている。
  DO-178C、DO-330、DO-331、DO-332,DO-333
- このACは、RTCAのDO-178Cの適用方法を説明している。
- このACは、RTCAの参照文書に記載されたいかなるデータや活動も、FAAの承認を義務付けるものではない。

ご清聴ありがとうございました。

余談：究極の航空機信頼性向上策？

資料：米運輸省ボルペ研究所