RMD DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

まえがき

本解説書は、国立研究開発法人新エネルギー・産業技術総合開発機構（以下 NEDO）「次世代空モビリティの社会実装に向けた実現プロジェクト（通称：ReAMo プロジェクト） ／ドローンの性能評価手法の開発／次世代空モビリティの安全認証および社会実装に求められる性能評価手法に関する研究開発」（2022年度（令和 4 年度）～2026年度（令和 8 年度））の成果の一部を公表用として作成したものである。

無人航空機は、「空の産業革命」とも言われ、すでに空撮、農薬散布、測量、インフラの点検など広く活用されている。今後、都市部も含む物流への活用など、さらに多様な分野の幅広い用途に利用され、多くの人々がその利便性を享受し、産業、経済、社会に変革をもたらすことが期待されるが、その実現には有人地帯上空における補助者なし目視外飛行（レベル 4 飛行）の実現が不可欠である。

このことから「空の産業革命に向けたロードマップ 2021」（小型無人機に係る環境整備に向けた官民協議会）や「成長戦略実行計画」（2021 年（令和 3 年）6 月 18 日閣議決定）において、安全上の観点からこれまでは飛行を認めていなかったレベル 4 飛行というリスクの高い飛行を、2022（令和 4）年度を目途に実現することが目標とされ、これに向けて官民において検討を進められてきた。この検討を踏まえた航空法などの一部を改正する法律（令和 3 年法律第 65 号、改正航空法）が第 204 回通常国会において成立、2021 年（令和 3 年）6 月に公布され、2023 年（令和 4 年）12 月 5 日に施行された。同法により、無人航空機の機体認証・型式認証制度および無人航空機操縦者技能証明制度などが創設された。

このような背景を踏まえ、本研究開発では、無人航空機の機体認証・型式認証や運航の許可・承認に必要な、安全性に関する証明/認証手法を研究開発し、航空業界の標準化のコミュニティと協調し、国内外で標準化活動を実施することを目的としている。

これらの目的を達成するため、「無人航空機の認証に対応した証明手法の事例検討 WG」を設置し、国土交通省航空局から 2022 年（令和 4 年）9 月 7 日に発行された「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領” （以降、「サーキュラーNo.8-001」と呼ぶ）」、2022 年（令和 4 年）12 月 2 日に発行された「サーキュラーNo.8-002”無人航空機の型式認証等の手続き” （以降、「サーキュラーNo.8-002」と呼ぶ）」、および「無人航空機の型式認証などの取得のためのガイドライン（以降、「航空局ガイドライン」と呼ぶ）」から、優先的に解説が必要と判断した項目について本 WG の下に当該項目ごとのサブ WG を設置し「航空局ガイドライン」を活用するための解説書の作成を行った。

本文書の主要部（第 2 章）の主執筆者は下表の通り。

本文書の主要部（第 2 章）の主執筆者

担当節	主執筆者
2.1.1	橋本　寛之（株式会社プロドローン）
2.2.1	中田　博精（AeroVXR 合同会社）
2.2.2	宮川 毅也（一般財団法人日本海事協会）
2.2.3	山崎　まりか（株式会社電通総研（旧株式会社電通国際情報サービス））
2.3.4	南　貴紘（株式会社電通総研（旧株式会社電通国際情報サービス））
2.2.5	矢口　勇一（公立大学法人会津大学）
2.2.6	兵頭 淳（株式会社東京アールアンドデー）
2.2.7	森下 尚久（イームズロボティックス株式会社）
2.2.8	河野　敬（国立研究開発法人宇宙航空研究開発機構）

目次

図 目次

表 目次

1　本文書の概要

1.1　目的

第二種型式認証／機体認証の無人航空機に求められる機体の安全性の具体的な証明方法について参考となる安全基準および型式認証プロセスの適合性証明計画について解説を行うことを目的とする。この際、本制度を所管する国土交通省航空局から発行された「サーキュラーNo.8-001」、「サーキュラーNo.8-002」および「航空局ガイドライン」にもとづき内容の解説を行う解説書の作成を行う。

1.2　型式／機体認証制度の概要

レベル 4 の実現に向けた新たな制度では、飛行のリスクの程度に応じた 3 つのカテゴリー（リスクの高いものからカテゴリーⅢ、Ⅱ、Ⅰ）が設定され、カテゴリーに応じた規制が適用されている。具体的には以下のように分類される。

- カテゴリーⅢ：特定飛行のうち、無人航空機の飛行経路下において立入管理措置を講じないで行う飛行。（＝第三者の上空で特定飛行を行う）
- カテゴリーⅡ：特定飛行のうち、無人航空機の飛行経路下において立入管理措置を講じたうえで行う飛行。（＝第三者の上空を飛行しない）
- カテゴリーⅠ：特定飛行に該当しない飛行。航空法上の飛行許可・承認手続きは不要。

第三者の上空を飛行することができるよう飛行の安全を厳格に担保しつつ、利用者利便の向上のためその他の飛行について規制を合理化・簡略化する仕組みが整備されつつある。その一環として無人航空機の安全基準への適合性について検査する機体認証制度が創設され、また型式認証を受けた量産機の機体は、同じ型式のものであれば機体ごとに行う機体認証の検査の全部または一部を省略できる。

これらの機体に対する機体認証および型式認証は、認証の対象となる無人航空機の飛行形態に応じて、機体に求められる安全性のレベルが異なることから、第三者上空を飛行する機体であるかどうかの観点から区分され、カテゴリーⅢまでの飛行を行うことを目的とする機体に対する第一種認証、カテゴリーⅡの飛行を行うことを目的とする機体に対する第二種認証に区分される。

飛行のリスクの程度に応じた各カテゴリーの飛行形態と飛行にあたっての主な要件・条件のイメージを図 1.2-1 に示す。また、飛行形態ごとのカテゴリー分類の詳細と、カテゴリーの決定フローのイメージについて、それぞれ図 1.2-2、図 1.2-3 に示し、機体認証および型式認証の区分を表 1.2-1 に、機体認証制度の概要を図 1.2-4 に示す。

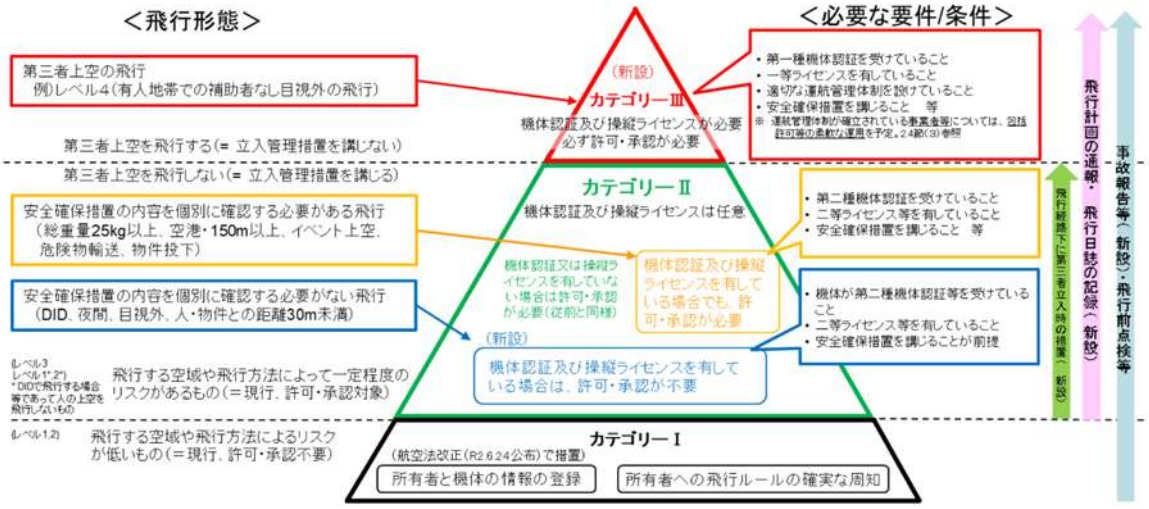


図 1.2-1 飛行のリスクの程度に応じた各カテゴリーの飛行形態と主な規制内容のイメージ

出所)国土交通省 HP 無人航空機の有人地帯における目視外飛行(レベル 4)の実現に向けた検討 小委員会 中間とりまとめ
https://www.mlit.go.jp/policy/shingikai/content/001389494.pdf (閲覧日 2022 年 11 月 16 日)

	飛行の空域		飛行の方法					
	132条第1項		132条の2第1項					
	第1号	第2号	第5号	第6号	第7号	第8号	第9号	第10号
	空港周辺・150m以上	DID	夜間	目視外	人・物件30m未満	イベント上空	危険物輸送	物件投下
第三者上空以外の飛行(= 立入管理措置を講じる飛行)		カテゴリーⅡのうち、機体認証、操縦ライセンスを有する場合に個別審査不要なもの				カテゴリーⅡのうち、機体認証、操縦ライセンスを有する場合であっても個別審査を要するもの		
第三者上空の飛行(= 立入管理措置を講じない飛行)	カテゴリーⅢ							

図 1.2-2 飛行形態ごとのカテゴリー分類の詳細

出所)国土交通省 HP 無人航空機の有人地帯における目視外飛行(レベル 4)の実現に向けた検討 小委員会 中間とりまとめ
https://www.mlit.go.jp/policy/shingikai/content/001389494.pdf (閲覧日 2022 年 11 月 16 日)

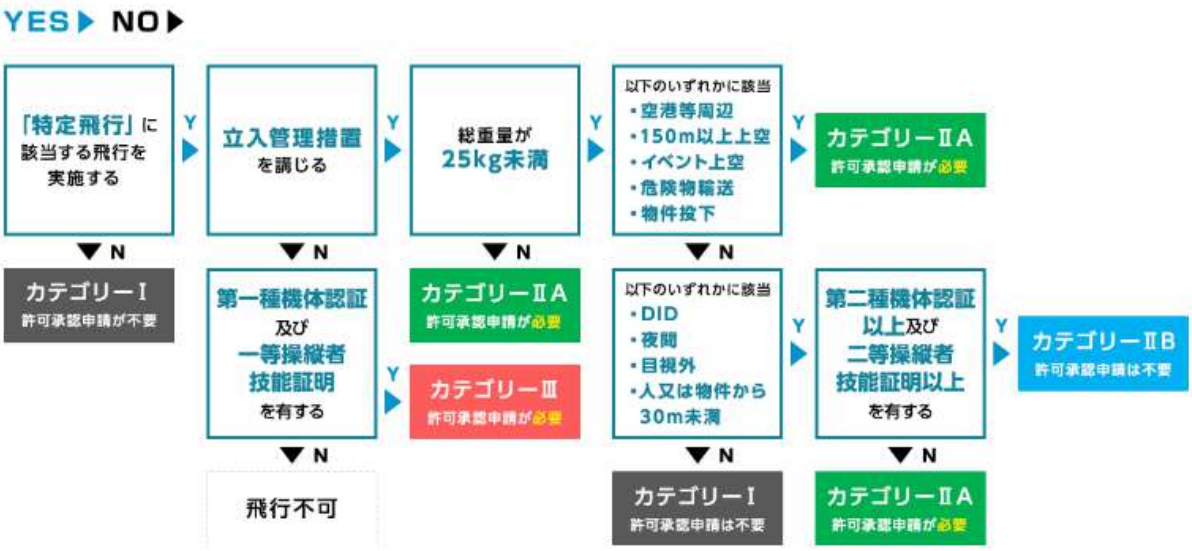


図 1.2-3 カテゴリーの決定フローのイメージ

出所)国土交通省 HP 無人航空機の飛行許可･承認手続
https://www.mlit.go.jp/koku/koku_fr10_000042.html（閲覧日 2022 年 11 月 16 日）

表 1.2-1 機体認証および型式認証の区分

	カテゴリーⅢまでの飛行	カテゴリーⅡまでの飛行
型式認証	第一種型式認証	第二種型式認証
機体認証	第一種機体認証	第二種機体認証

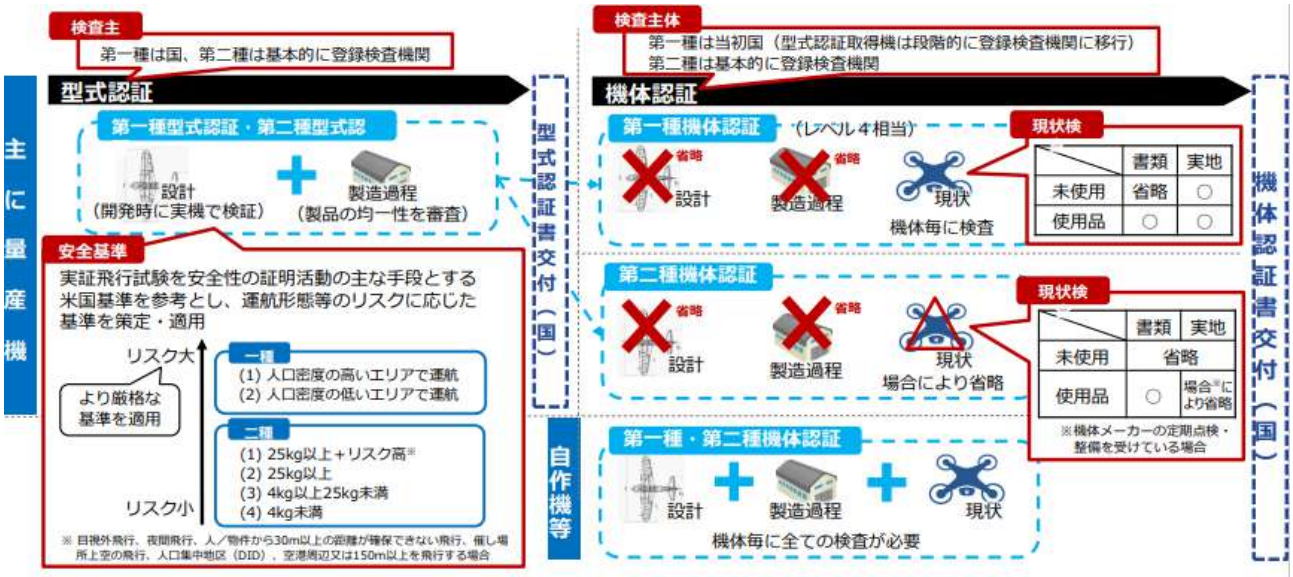


図 1.2-4 無人航空機の機体認証制度の概要

出所)https://www.kantei.go.jp/jp/singi/kogatamujinki/kanminkyougi_dai17/siryou1.pdf
（閲覧日 2022 年 11 月 16 日）

第一種の型式認証／機体認証は、立入管理措置（補助者の配置やその代替として看板の設置などにより第三者の立入りを管理する措置）を講じることなく行う特定飛行を目的とする型式に対する認証制度であり、第二種型式認証は、特定飛行のうち、無人航空機の飛行経路下において立入管理措置を講じたうえで行う飛行を目的とする型式認証／機体認証に対する認証制度である。

このうち第二種の型式認証／機体認証は、第一種の型式認証／機体認証ほどの厳格さは必要ないものの、個別の許可・承認を必要とせずに一部の特定飛行を可能とする機体に求められる基準であり、一定レベル以上の飛行の安全を担保する必要があるほか、第一種の型式認証／機体認証との連続性も必要とされる。加えて、立入管理措置を講じた上で行う特定飛行は、ホビー、農薬散布、物流などの事業まで多様な利用が見込まれ、また多くの機体の最大離陸重量が数キログラム未満と小型であることも十分に留意される必要がある。

このような背景から、国土交通省航空局では、無人航空機の型式認証等の検査要領（無人航空機及び装備品等に対する航空法施行規則第 236 条の 15 による「安全性を確保するための強度、構造及び性能についての基準」（以下、「安全基準」という）および同令第 236 条の 24 による「均一性を確保するために必要なものとして定める基準」（以降、「均一性基準」という）を制定しており※、第一種機体認証を受けようとする無人航空機または第一種型式認証を受けようとする型式の無人航空機で、人口密度が 1 平方キロメートル当たり 1.5 万人以上の区域の上空（以降、「特定空域」という）を含まない空域を飛行するものおよび第二種の型式認証／機体認証を受けようとする無人航空機、または第二種の型式認証を受けようとする型式の無人航空機は、本航空局検査要領「サーキュラーNo.8-001」にしたがって機体性能が適合していることを証明しなければならない。

認証の申請者は自ら、申請に係る無人航空機、または型式の無人航空機が安全基準の該当規定に適合することを証明する手段を検討し、国土交通省および国土交通省が登録した無人航空機登録検査機関（登録検査機関）に対して証明しなければならない。しかしながら、本制度運用開始当初には認証取得の事例が存在しないため、申請者にとって適合性証明手段検討の負荷が重く、申請をためらう可能性が懸念された。そこで、安全基準に対する適合性証明手段として活用可能な証明方法（試験方法を含む）の策定およびそれらの文書（証明手順書や事例集）化を活動の最終目標として設定したうえで、本検討では安全基準および型式認証プロセスの項目の区分のうち優先的に解説が必要と判断した安全基準項目および型式認証プロセスにおける適合性証明計画を対象に、「航空局ガイドライン」解説書を作成することとした。

1.3 「航空局ガイドライン」解説書対象項目と本文書の位置づけ

国土交通省航空局から発行された「航空局ガイドライン」に記載された項目のうち型式認証プロセスおよび安全基準から優先的に解説が必要と判断した項目から順次「航空局ガイドライン」解説書を作成した。表 1.3-1 に国土交通省航空局から発行された「航空局ガイドライン」のうち本解説書の対象とした項目を示す。表中朱塗りしている項目が本文書の検討対象である。

※「無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領」、整理番号 No.8-001、2022 年（令和 4 年）9 月 7 日 制定（国空機第 456 号）、2022 年（令和 4 年）12 月 2 日 一部改正（国空機第 645 号）、https://www.mlit.go.jp/koku/certification.html

表 1.3-1 「航空局ガイドライン」構成と検討対象項目

「航空局ガイドライン」構成	「航空局ガイドライン」項目
第１部	共通
第２部	型式認証プロセス
第３部	安全基準
第４部	均一性基準

また、「航空局ガイドライン」安全基準のうち、検討対象としたセクションについて、表 1.3-2 に国土交通省航空局から発行された安全基準区分に応じて適用される規定を示す。表中朱塗りしている区分（セクション）が本文書の検討対象である。

なお、本「航空局ガイドライン」解説書は、無人航空機の型式認証の取得を目指す機体メーカーおよび部品メーカー商社が使用する場合には、無人航空機の型式認証の申請時において「航空局ガイドライン」の内容の理解を深めると共に当該認証の検査の計画・実施に資する文書として活用されることを想定する。また、登録講習機関（ドローンスクール）、無人航空機操縦者技能証明取得者および取得予定者などが本文書を使用する場合は、無人航空機の操縦者および操縦の指導者として、型式認証制度を理解し、安全な運航に必要な機体性能などを理解するに資する文書として活用されることを想定する。

212 表 1.3-2「無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領」の
213 「第Ⅲ部 安全基準 表１ 区分に応じて適用される規定」

区分	第二種 機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機				第一種 機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機
	最大離陸重量 4kg 未満のもの	最大離陸重量 4kg 以上 25kg 未満のもの	最大離陸重量 25 ㎏以上のもの		特定空域を含まない空域を飛行するもの
			法第 132 条の 85 第１項各号に掲げる空域以外の空域を飛行し、かつ、法第 132 条の 86 第２項第１号から第４号までのいずれにも該当する方法により飛行するもの※2	その他のもの※3	
001 設計概念書（CONOPS）	✓	✓	✓	✓	✓
005 定義	✓	✓	✓	✓	✓
100 無人航空機に係る信号の監視と送信	✓※4	✓	✓	✓	✓
105 無人航空機の安全な運用に必要な関連システム	✓	✓	✓	✓	✓
110 ソフトウェア	✓※5	✓※5	✓※5	✓	✓
115 サイバーセキュリティ	✓	✓	✓	✓	✓
120 緊急時の対応計画	✓ ✓※6	✓	✓	✓	✓
125 雷	✓	✓	✓	✓	✓
130 悪天候	✓	✓	✓	✓	✓
135 重要な部品(フライトエッセンシャルパーツ)	✓	✓	✓	✓	✓
140 その他必要となる設計及び構成	✓※7	✓※7	✓※7	✓※7	✓※7
200 無人航空機飛行規程	✓	✓	✓	✓	✓
205 ICA	✓	✓	✓	✓	✓
300 耐久性及び信頼性	✓	✓	✓	✓	✓
305 起こり得る故障	✓ ✓※8	✓ ✓※8	✓	✓	✓
310 能力及び機能	✓※9	✓	✓	✓	✓
315 疲労試験	N/A	N/A	✓	✓	✓
320 制限の検証	N/A	N/A	✓	✓	✓

（凡例）✓：適用されるもの、✓✓：該当する特定飛行※1 に応じて適用されるもの、N/A：適用されないもの
※1：法第 132 条の 85 第 1 項各号に掲げる空域における飛行または法第 132 条の 86 第 2 項各号に掲げる方法のいずれかによらない飛行
※2：危険物輸送または物件投下を行う飛行が該当。ただし、いずれの飛行にあっても第三者上空を飛行しないものに限る。
※3：空港周辺、地表若しくは水面から高さ 150m 以上若しくは人口集中地区（DID）の上空を飛行するもの、夜間飛行、目視外飛行、人／物件から 30m 以上の距離が確保できない飛行または催し場所上空を飛行するものが該当。ただし、いずれの飛行にあっても第三者上空を飛行しないものに限る。
※4：100(a)項はすべての無人航空機に適用。また、目視外飛行の場合は 100(c)項および(d)項も追加適用
※5：航空局または登録検査機関による当該要件に対する適合性の検査は受けないものの、申請者自身が当該要件に対して適合していることを確認した上で、適合している旨を記載した宣言書を機体認証申請後または型式認証申請後に提出することが必要
※6：目視外飛行の場合は 120(a)項が適用。それ以外の飛行の場合は非適用
※7：140-1(a)項および(b)項ならびに 140-2(a)項はすべての無人航空機に適用。また、140-1(c)項および(d)項、140-2(b)項および(c)項、140-3 項、140-4 項ならびに 140-5 項は、該当する特定飛行や機体重量に応じて追加適用
※8：目視外飛行の場合は 305(a)項(2)、(3)および(6)がそれぞれ適用。それ以外の飛行の場合は非適用
※9：310(a)項(3)～(6)はすべての無人航空機に適用。また、目視外飛行の場合は 310(a)項(1)が、物件投下の場合は 310(c)項がそれぞれ追加適用
出所：国土交通令和 4 年 12 月 2 日制定（国空機第 645 号）サーキュラー無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領より引用し三菱総合研究所にて作成

具体的な検討項目を以下に示す。これらの項目については、欧米においても現状対応方針が定まっておらず、日本が世界に先駆けて適合性証明手段を定めることになることから、優先的に検討すべき項目と判断し選定した。

- CP（適合性証明計画）
  適合性証明計画を作成する際に参考となる「航空局ガイドライン」解説書の作成
- 001 設計概念書（CONOPS）
  無人航空機の想定される運用（CONOPS）について、「航空局ガイドライン」解説書の作成
- 105 無人航空機の安全な運用に必要な関連システム
  無人航空機の安全性に影響を与え、または無人航空機が安全基準を満たすために必要な無人航空機関連システム（AE）について、「航空局ガイドライン」解説書の作成
- 110 ソフトウェア
  無人航空機の安全な運用に影響を与えるすべてのソフトウェアについて、「航空局ガイドライン」解説書の作成
- 115 サイバーセキュリティ
  他のシステムと連携する無人航空機の機器、システムおよびネットワークに対するサイバーセキュリティについて、「航空局ガイドライン」解説書の作成
- 135　重要な部品（フライトエッセンシャルパーツ）
  無人航空機を構成する部品の内、その不具合により計画外飛行または回復できない制御不能につながる重要な部品について、「航空局ガイドライン」解説書の作成
- 300 耐久性と信頼性
  型式認証データシートおよび無人航空機飛行規程、CONOPS などに規定された運用環境の制限下で運用された場合の耐久性と信頼性について、「航空局ガイドライン」解説書の作成
- 305 起こり得る故障
  起こり得る故障によって機体の制御不能または想定飛行範囲からの逸脱を生じさせない設計について、「航空局ガイドライン」解説書の作成

- 安全基準の各セクションにおける「安全」などの用語の解釈
  安全基準の各セクションに記載されている「安全」などの用語の解釈に関する各セクションの基準で要求されている内容について、「航空局ガイドライン」解説書の作成

なお、「航空局ガイドライン」解説書を構成するセクション対象項目の文書番号と版数を以下表 1.3-3 に示す。

表 1.3-3 検討対象項目一覧

セクション	文書番号	版数
CP(適合性証明計画)	RMD-CP	Rev.01
001(CONOPS)	RMD-001	Rev.01
105(無人航空機の安全な運用に必要な関連システム)	RMD-105	Rev.01
110(ソフトウェア)	RMD-110	Rev.01
115(サイバーセキュリティ)	RMD-115	Rev.01
135(重要な部品)	RMD-135	Rev.01
300(耐久性及び信頼性)	RMD-300	Rev.01
305(起こり得る故障)	RMD-305	Rev.01
安全基準の各セクションにおける「安全」等の用語の解釈	RMD	Rev.01

1.4 更新履歴

今後新たな「航空局ガイドライン」解説項目が追加となった際は順次本項にて更新履歴を記載する。

1.5 関連文書

(1) 空の産業革命に向けたロードマップ 2021、2021 年 6 月 28 日
https://www.kantei.go.jp/jp/singi/kogatamujinki/kanminkyougi_dai16/siryou4.pdf

(2) 成長戦略実行計画、2021 年 6 月 18 日
https://www.cas.go.jp/jp/seisaku/seicho/pdf/ap2021.pdf

(3) 航空法等の一部を改正する法律(改正航空法)、令和 3 年法律第 65 号
https://www.mlit.go.jp/report/press/content/001492103.pdf

(4) サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領、2022 年 9 月 7 日(国空機第 456 号)
https://www.mlit.go.jp/koku/content/001520547.pdf

(5) サーキュラーNo.8-002 無人航空機の型式認証等の手続き、2022 年 12 月 2 日(国空機第 645 号)
https://www.mlit.go.jp/koku/content/001574424.pdf

(6) 無人航空機の型式認証等の取得のためのガイドライン、2022 年 11 月 2 日
https://www.mlit.go.jp/common/001574425.pdf

1.6　検討体制

国土交通省航空局から発行された「航空局ガイドライン」に記載された項目のうち、優先的に解説が必要な型式認証プロセスおよび安全基準の項目について議論する「無人航空機の第二種認証に対応した証明手法の事例検討 WG」を設置するとともに、本 WG 内に各項目の解説書の具体検討を行う「サブWG」を設置し、登録検査機関候補および機体メーカー、有識者などが参加して議論を行い、「航空局ガイドライン」解説書を取りまとめた。図 1.6-1 に検討体制を示す。

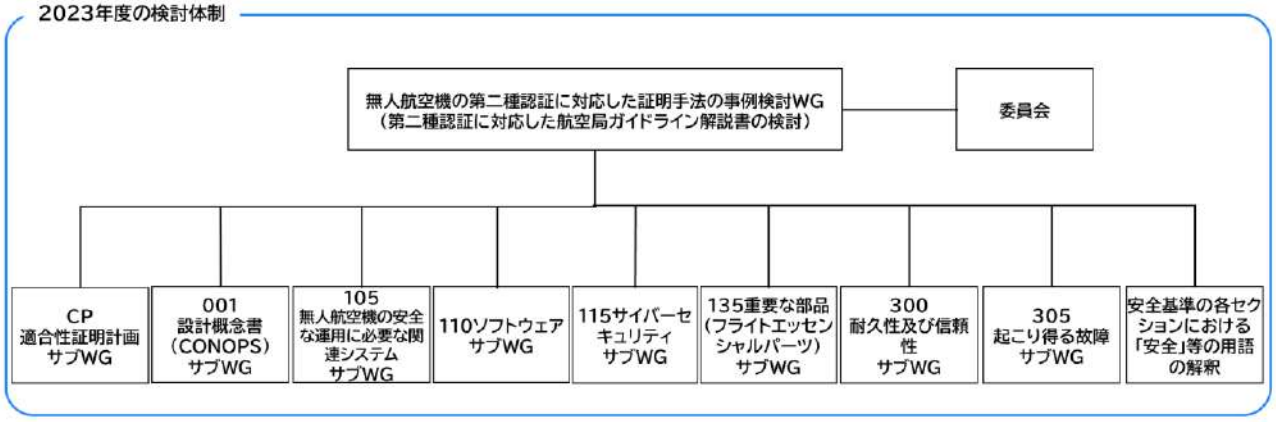


図 1.6-1　無人航空機の第二種認証に対応した証明手法の事例検討体制

2　各項目の解説概要

無人航空機の「第二種」の機体の認証（型式認証/機体認証）を円滑にするために、国土交通省航空局から発行された「航空局ガイドライン」に記載された型式認証プロセスの適合性証明計画および各安全基準の項目のうち、優先的に解説が必要な項目について順次「解説書」を検討・作成した。各セクションの「航空局ガイドライン」解説書は別紙から構成され、「航空局ガイドライン」記載内容に対する解説、検討の際の論点整理および本検討に引き続き継続的に検討が必要な課題などから構成される。

なお、各セクション解説書の記載内容・見方については Appendix-2 を参照。

2.1　認証文書

2.1.1 CP（適合性証明計画）検査要領

（1） 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、型式認証プロセスの適合性証明計画に対する解説を記載する。

（2） 文書呼び出し

RMD-CP Rev.01

2.2　安全基準

2.2.1 安全基準の各セクションにおける「安全」などの用語の解釈

（1） 背景

安全基準として具体的な内容がサーキュラーNo.8-001 に定められている。しかし、本サーキュラーは無人航空機に対する第一種認証及び第二種認証の両方に適用されているため、各認証において用語の意味を適切に解釈する必要がある。特に、第一種認証と第二種認証では求められる要求が異なる。本項では、第二種認証を対象として、安全基準の各セクションに記載されている「安全」などの用語の解釈を明確にし、各セクションの基準で要求されている内容を明確にする。

（2） 第二種型式認証/機体認証

第二種型式認証/機体認証（第二種認証）は、カテゴリーII までの飛行を行うことを目的とする機体に対して適用されている。つまり、無人航空機の飛行経路下において立入管理措置を講じたうえで特定飛

行を行う飛行に用いられることを想定している機体に対して第二種認証が適用されている。

（3） セクション 005 “定義”の解釈

安全基準セクション 005 定義 （以降、「セクション 005」と呼ぶ）には、安全基準内で用いられている「制御不能」及び「計画外飛行」の定義が記載されている。本定義を基に第二種認証という観点を考慮した際の各定義の解釈を明確にする。

セクション 005 定義

(a) 制御不能：制御不能とは、無人航空機の制御された飛行状態からの意図しない逸脱を意味する。これには、逆効き又は縦、横若しくは方向の安定性及び操縦性の過度な喪失が含まれる。また、地表面への制御不可能な衝突の可能性が高い計画外又は命令外の姿勢への変化が含まれる。制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。

(b) 計画外飛行：計画外飛行とは、無人航空機が当初計画された着陸地点まで、計画どおりに飛行を完了できないことを意味する。これには、無人航空機の制御下における地表面、障害物等への衝突又は深刻若しくは回復不可能な高度の喪失が含まれる。計画外飛行には、パラシュート等の回収系統の展開による運用者が指定したリカバリーゾーン外の計画外の着陸も含まれる。

［引用：サーキュラーNo.8-001］

1） 「制御不能」の解釈

セクション 005(a)には、「制御不能」の定義が記載されている。本定義では、「無人航空機の制御された飛行状態からの意図しない逸脱を意味する」としており、さらに「一般的には墜落につながる状態」と記載されている。一方で、第二種認証を取得している機体はカテゴリーII 飛行までの飛行を想定しており、特定飛行を実施する場合には立入管理措置を実施した上空のみを飛行する。このことを考慮すると、カテゴリーII 飛行を実施する場合には、立入管理措置区域内においては、無人航空機を飛行させる者およびこれを補助する者以外の立入りを管理していることから、運用者によって管理された飛行中断を実施することは安全性を確保するという観点から考えれば、問題ないと考えられる。

以上のことから、「制御不能」は、以下のように解釈できる。

セクション 005 定義

(a) 制御不能：制御不能とは、無人航空機の制御された飛行状態からの意図しない逸脱を意味する。これには、逆効き又は縦、横若しくは方向の安定性及び操縦性の過度な喪失が含まれる。また、地表面への制御不可能な衝突の可能性が高い計画外又は命令外の姿勢への変化が含まれる。制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。ただし、人の死傷および航空機または無人航空機との衝突または接触が生じないように管理された飛行空域および地上範囲に運用者によって意図的に実施した飛行中断は制御不能の範疇には入らない。

(b) [引用：サーキュラーNo.8-001]

2） 「計画外飛行」の解釈

セクション 005(b)には、「計画外飛行」の定義が記載されている。本定義に記載されている「当初計画された着陸地点」に関しては複数の解釈が存在する。無人航空機の飛行前に作成される飛行計画では、ミッションを完遂するために必要となる離陸場所および着陸場所を設定するのに加えて、必要に応じて緊急時に使用する可能性のある着陸場所を定める。これらの場所に関しては、「当初計画された着陸場所」と考えることができる。

以上のことから、「計画外飛行」は、以下のように解釈できる。また計画外飛行と想定飛行範囲（立入管理措置区域を含む）のイメージを図 2.2-1 に示す。

セクション 005 定義

(c) 計画外飛行：計画外飛行とは、無人航空機が当初計画された着陸地点（ミッション実施時の出発もしくは目的場所または緊急時に着陸を認めた場所（リカバリーゾーン））まで、計画どおりに飛行を完了できないことを意味する。これには、無人航空機の制御下における地表面、障害物等への衝突又は深刻若しくは回復不可能な高度の喪失が含まれる。計画外飛行には、パラシュート等の回収系統の展開による運用者が指定したリカバリーゾーン外の計画外の着陸も含まれる。

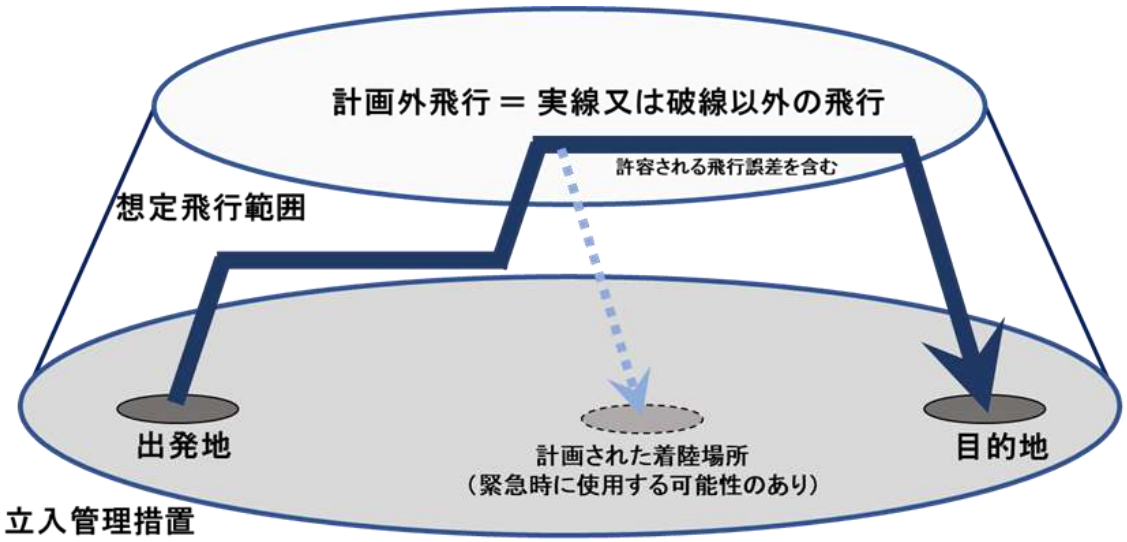


図 2.2-1 計画外飛行と想定飛行範囲（立入管理措置区域含む）のイメージ

（4） 各セクションにおける“安全”などの用語の解釈

安全基準の各セクションでは、“安全”やそれに類する用語が使用されている。カテゴリーII 飛行において安全な飛行を実施するために最低限守るべきことは、運用において人の死傷を生じないようにすることと考えられる。そのことを念頭におくと、“安全”またはそれに類する用語に関しては、「機体の制御不能または想定範囲からの逸脱を生じない」という解釈ができる。

各セクションにおける具体的な解釈は表 2.2-1 のとおりである。なお、本項では“安全”等の用語の解釈のみを明確にしたため、各セクションにおける詳細な解釈や証明方法に関しては、各セクションの航空局ガイドラインや解説書を確認しなければならない。

394 表 2.2-1 各セクションの“安全”などの用語の解釈

セクション	安全基準(該当箇所抜粋)	下線部の解釈
100	無人航空機は、**安全な飛行と運用の継続**に必要なすべての情報を監視し…	故障またはエラーが生じた場合に無人航空機が以下のいずれにもならない ● 制御不能 ● 想定飛行範囲からの逸脱
105	(a) 申請者は、**無人航空機の安全性に影響を与え**、又は…	故障またはエラーが生じた場合に無人航空機が以下のいずれかにつながる可能性がある ● 制御不能 ● 想定飛行範囲からの逸脱
110	(a) **無人航空機の安全な運用に影響を与える**すべてのソフトウェアに対して…	エラーが生じた場合に無人航空機が以下のいずれかにつながる可能性がある ● 制御不能 ● 想定飛行範囲からの逸脱
115	(a) 別のシステムと連携する無人航空機の機器、システム及びネットワークは、**無人航空機の安全性に悪影響を及ぼす**意図的で許可されていない電子的な干渉から守られなくてはならない。…	無人航空機が以下のいずれかにつながる可能性がある ● 制御不能 ● 想定飛行範囲からの逸脱
125	(a) 下記(b)項の場合を除き、無人航空機は雷撃による**計画外飛行又は制御不能がない**ような設計特性を有さなければならない。	無人航空機が以下のいずれも生じない ● 計画外飛行 ● 制御不能
130	(b) 下記(b)項の場合を除き、無人航空機はCONOPS で定義した悪天候の範囲内において**計画外飛行又は制御不能を生じることなし**に運用できるような設計特性を有されなければならない。	無人航空機が以下のいずれも生じない ● 計画外飛行 ● 制御不能
135	(a) フライトエッセンシャルパーツとは、その不具合により**計画外飛行又は回復できない制御不能につながる**部品である。	無人航空機が以下のいずれかにつながる ● 計画外飛行 ● (回復できない)制御不能
300	…。試験は、**計画外飛行、制御不能、想定飛行範囲からの逸脱又はリカバリーエリア外での非常着陸につながる不具合なく**完了しなければならない。…	無人航空機が以下のいずれにもつながる不具合がない ● 計画外飛行 ● 操縦不能 ● 想定飛行範囲からの逸脱 ● リカバリーエリア外での非常着陸
305	無人航空機は、単一の起こり得る故障によって**機体の制御不能又は想定飛行範囲からの逸脱を生じない**ように設計されなければならない。…	無人航空機が以下のいずれも生じない ● 制御不能 ● 想定飛行範囲からの逸脱
320	無人航空機飛行規程に指定される飛行エンベロープにおける機体の性能、操縦性、安定性及び制御について、最大総重量を少なくとも5%超える状態で**計画外飛行又は制御不能が生じないこと**を実証しなければならない。	無人航空機が以下のいずれも生じない ● 計画外飛行 ● 制御不能

395

2.2.2 セクション 001 設計概念書（CONOPS）

（1） 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 001 設計概念書（CONOPS）（以降、「セクション 001」と呼ぶ）における、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

（2） 文書呼び出し

RMD-001 Rev.01

2.2.3 セクション 105 無人航空機の安全な運用に必要な関連システム

（1） 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 105 無人航空機の安全な運用（以降、「セクション 105」と呼ぶ）に必要な関連システムにおける、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

（2） 文書呼び出し

RMD-105 Rev.01

2.2.4 セクション 110 ソフトウェア

（1） 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 110 ソフトウェア（以降、「セクション 110」と呼ぶ）における、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

（2） 文書呼び出し

RMD-110 Rev.01

2.2.5 セクション 115 サイバーセキュリティ

(1) 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 115 サイバーセキュリティ（以降、「セクション 115」と呼ぶ）における、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

(2) 文書呼び出し

RMD-115 Rev.01

2.2.6 セクション 135 重要な部品（フライトエッセンシャルパーツ）

(1) 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 135 重要な部品（フライトエッセンシャルパーツ）（以降、「セクション 135」と呼ぶ）における、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

(2) 文書呼び出し

RMD-135 Rev.01

2.2.7 セクション 300 耐久性と信頼性

(1) 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 300 耐久性と信頼性（以降、「セクション 300」と呼ぶ）における、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

(2) 文書呼び出し

RMD-300 Rev.01

2.2.8 セクション 305 起こり得る故障

（1） 概要

国土交通省航空局から発行された「航空局ガイドライン」に記載される、安全基準 セクション 305 起こり得る故障に（以降、「セクション 305」と呼ぶ）おける、適合性証明方法（Moc）、検査のポイント、検査者の関与度（LOI）などに関する解説を記載する。

（2） 文書呼び出し

RMD-305 Rev.01

Appendix 1 用語集(用語一覧)

#	用語/略語	説明	出所等
1	AC 20-136B	Federal Aviation Administration (FAA)が発行する Advisory Circulars(AC)であり、耐雷に関する要求について記載される。タイトルは Aircraft Electrical and Electronic System Lightning Protection。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
2	ARP5416	Society of Automotive Engineers(SAE)が発行するガイドラインであり、耐雷に関する要求について記載される。タイトルは Aircraft Lightning Test Methods。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
3	ASTM	以前は American Society for Testing and Materials の略であったが、現在は ASTM が正式名称であり、工業関連標準規格を設定・発行している米国の民間非営利標準化団体のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
4	CIR	Conformity Inspection Record の略であり、適合検査記録書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
5	CIT	Conformity Inspection Tag の略であり、適合検査票のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
6	CP	Certification Plan の略であり、適合性証明計画のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
7	D&R	Durability and Reliability の略であり、耐久性および信頼性を実証試験で証明する方法のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
8	DAL	Development Assurance Level。開発保証における厳格さの程度のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
9	Deviation	設計データ(試験方案などを含む。)から少しでも逸脱するものが認められる場合、または試験において供試体や試験装置などが破損する、あるいは試験方案の求める設定条件での試験が出来ないなどの不具合が発生した状態のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
10	Deviation シート	設計データ(試験方案などを含む。)からの逸脱または当該設計データに記載されていない事項であって明確にする必要がある場合などに、相違の内容を明確にした上で、申請者の担当部門による成立性の判定を記載し、検査者の了解を得て試験の継続を可能とする際に使用する書類のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン

11	DIPS	Drone/UAS Information Platform System の略であり、ドローン情報基盤システムのこと。申請などの機能を利用することができる。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
12	DO-160	RTCA が発行する装備品の環境試験方法。タイトルは Environmental Conditions and Test Procedures for Airborne Equipment。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
13	DO-178	RTCA が発行するソフトウェア認証のガイドライン。タイトルは Software Considerations in Airborne Systems and Equipment Certification。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
14	DOP	Dilution Of Precision。精度低下率のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
15	EMI	Erectromagnetic Interference の略であり、電磁干渉のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
16	FHA	Functional Hazard Analysis の略称であり、安全性評価の一手法。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
17	FMEA	Failure Mode and Effect Analysis の略称であり、安全性評価の一手法。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
18	FTA	Fault Tree Analysis の略称であり、安全性評価の一手法。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
19	HIRF	High Intensity Radiated Field の略であり、高強度放射電界のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
20	ICA	無人航空機などに対する点検および整備を行うための手順書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
21	IP	Issue Paper の略称であり、適合性見解書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
22	LIDAR	Light Detection And Ranging の略であり、レーザーで物体や表面を対象にして、反射光が受信機に戻るまでに時間を継続することにより、可変距離を測定するものまたは方法。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン

23	MoC	Means of Compliance の略称であり、適合性証明方法のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
24	RFC/W	Request for Conformity/Test Witnessing の略であり、適合検査／試験立会要求書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
25	RTCA	Radio Technical Commission for Aeronautics の略であり、航空に関する要求事項・技術的コンセプトの調査検討に取り組み、提言を行うことを目的とした米国の民間非営利標準化団体のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
26	RTH	Return To Home の略であり、機体の不具合発生または操縦者の指示によって、自動的に発着点に帰還飛行する機能のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
27	SAE	Society of Automotive Engineers の略であり、自動車関連および航空宇宙関連の標準規格の開発、専門家会議の開催などをおこなっている米国の民間非営利標準化団体のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
28	SOC	State Of Charge の略であり、バッテリーの充電率または充電状態を表す指標のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
29	SOC(書類名)	STATEMENT OF COMPLIANCE または Statement of Conformity の略称であり、STATEMENT OF COMPLIANCE は適合判定書、Statement of Conformity は適合報告書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
30	SOH	State Of Health の略であり、バッテリーの健全度や劣化状態を表す指標のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
31	TCDS	Type Certificate Data Sheet の略であり、型式認証データシートのこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
32	TWR	Test Witness Record の略であり、試験立会記録書のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
33	安全基準	国土交通省令で定める安全性を確保するための強度、構造および性能についての基準のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン
34	安全性	無人航空機のリスクレベルが許容できる範囲に収まっている状態のこと。	航空局発行 無人航空機の型式認証等の取得のためのガイドライン

35	員数	数量のこと。機体などへの工具などの置き忘れによる不具合や、飛行中の落下による地上への影響をなくすために、機体の製造に使用する設備（工具などを含む。）を管理する際に使用する用語。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
36	インバータ	直流電流を交流電流に変換する回路または装置のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
37	運用エンベロープ	無人航空機の運用可能な速度や荷重や高度の範囲のこと。高度と速度の関係で用いる（表す）ことが多い。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
38	加工	素材、材料または部品などに変化を与えること。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
39	型式認証試験	型式認証などにおいて、適合性証明のために試験結果を使うことを目的に、適合性判定書に検査者の承認を受けた試験方案に基づき実施する試験のこと。 申請のあった型式の無人航空機に関する試験であっても、社内の設計開発のために実施する試験であり、適合性証明のために試験結果を使うことを目的としない試験は除く。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
40	管理された墜落	無人航空機そのものに加え、墜落後の部品の飛散範囲を考慮するなどあらかじめ設計上で想定された墜落のこと。無人航空機飛行規程で操縦者（運航体制）へ別途具体的な指示を行うことを前提とした墜落が該当。 （例）部品の飛散が立入管理区画を超えないように墜落させること　など	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
41	機能検査	製造過程の成果物である製品が、設計者などが意図する機能を達成できているかについて、設計者などが指定する方法で実施する定量的検査のこと。機能試験と同義。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
42	均一性	製造された無人航空機が、型式認証を取得した型式の無人航空機の設計および製造過程とすべて同一である状態のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
43	均一性基準	無人航空機が安全基準および均一性を確保するために必要なものとして国土交通省令で定める基準のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
44	組立	いくつかの材料、部品および装備品を組み合わせて、1つの製品を作りあげる作業のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
45	ゲージマーキング	ゲージ（計器など）に、上限、下限および許容範囲などを示すための線状、帯状などの印（マーキング）のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン

46	検査者	型式認証の検査を行う者(航空局または登録検査機関)のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
47	検査要領	サーキュラーNo. 8-001「無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領」(令和4年9月7日 国空機第456号)のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
48	構成品	申請のあった型式の無人航空機を構成する主要な構造体、装備品および部品のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
49	工程	素材、部品または装備品について、それに変化を与える作業を進めていく順序・段階のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
50	サービスライフ	運用寿命、耐用年数のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
51	ジオ・フェンス機能	無人航空機の飛行範囲を制限する機能のこと。ジオ・アウェアネス機能ともいう。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
52	使用不能量	タンクの形状や配管の取り回しによって、消費できずにタンク内に残ってしまう燃料または滑油などの量のこと。当該燃料および滑油の重量は無人航空機の自重に含まれる。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
53	新技術 または 新しい技術	無人航空機の型式認証などにおいて過去に認証されていない技術のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
54	申請者	航空局により申請書が受理された後に、検査者と型式認証取得に向けた調整、検査を受検する者のこと。なお、型式認証の取得を計画する者または航空局により申請書が受理される前に、検査者と型式認証の申請に係る調整を行う申請予定者についても、ここでは申請者の定義に含めることとする。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
55	制御された非常着陸	無人航空機を制御することによって行われる安全な着陸。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
56	製造過程	無人航空機の製造の過程における素材の受け入れから加工、組立、検査および引き渡しに至るまでの全工程のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
57	製造管理要領	均一性基準について、要件に適合し続けることを確保するため、製造など業務の実施に関し、品質管理に関するプロセス(過程、仕組み)の管理が組織的かつ継続的に機能するよう申請者が作成する要領のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン

58	製造計画書	申請に係る無人航空機およびその構成品などの製造場所および主要下請製造者名ならびに申請に係る無人航空機およびその構成品などの製造の日程を記載した、型式認証申請書に添付すべき書類のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
59	製品	部品、装備品および機体のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
60	設計データ	設計者が示した機体などの仕様を確定する図面、スペックなどの基本データのこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
61	装備品	無人航空機に用いられることを目的とした部品の集合体である完成品であって、それ自体で特定の独立した機能を有するものをいう。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
62	素材	加工する前の状態、ある物を作るとき、もととして用いる原料のこと。「材料」と同義。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
63	第一種	第一種型式認証（航空法第 132 条の 16 第 2 項第 1 号）のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
64	第二種	第二種型式認証（航空法第 132 条の 16 第 2 項第 2 号）のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
65	適用基準	適用される基準、適合性証明方法、特別要件、適用除外または同等安全性を合わせて、適用基準への適合性を証明するための要領または方法のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
66	適合検査	適用される基準、適合性証明方法、特別要件、適用除外または同等安全性を合わせて、適用基準への適合性を証明するための要領または方法のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
67	ハードオーバー	舵面やアクチュエータがその限界点まで動く状態のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
68	破壊モード	破壊がどのような状態で発生するかをまとめたもの。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
69	飛行エンベロープ	無人航空機の飛行可能な速度や荷重や高度の範囲のこと。荷重と速度の関係で用いる（表す）ことが多い。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン

70	不具合(製造関連)	製造過程に起因する不具合により、施設、設備などおよび無人航空機などが適切に機能しない状態のこと。意図しない故障だけではなく、エラーに起因する事象も含まれる。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
71	不具合(設計関連)	設計に起因する不具合により、無人航空機などが適切に機能しない状態のこと。不具合には、故障およびエラーが含まれる。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
72	不適合	設計データ、製造工程を規定する書類などまたは品質管理体制などの基準からの逸脱のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
73	部品	無人航空機または装備品を構成する最小の単位であって、それ自体では特定の独立した機能を有しないものをいう。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
74	フライトモード	離陸モードや巡航モードなど運用における状態のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
75	プラカード(掲示板)	情報を提供するために機体などに施す板状の掲示物のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
76	ブラックボックステスト	内部の構造を把握することなくブラックボックスとして、アプリケーションを確認するソフトウェアテストの手法のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
77	保管	材料、部品、装備品などを適切に保存・管理すること。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
78	ホワイトボックステスト	内部の構造を把握した上で(ホワイトボックス)、アプリケーションを確認するソフトウェアテストの手法のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
79	マルチパス	無線通信において、発信源が同じである電波が建物、地形などの影響によって複数の経路を経て受信側に届く状態のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
80	ミリ波レーダー	ミリメートル波帯の周波数の電波(ミリ波)を使用し、ミリ波を対象物に照射してセンシングを行うレーダーのこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
81	乱反射	障害物に当たった際に複数の方向へ乱れて反射すること。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン

82	リカバリーゾーン	無人航空機の運用において、第三者および第三者物件に危害を与えることなく、無人航空機を回収するためにあらかじめ設定する地表の範囲のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
83	故障モード	故障がどのような状態で発生するかをまとめたもの。例えば、部品やコンポーネントの断線、短絡、折損、摩耗、特性の劣化などの構造の破壊など。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
84	主要下請製造者	申請のあった型式の無人航空機を製造する委託先のうち、構成品を製造する委託先のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン
85	製造工程を規定する書類など	素材の受け入れから、加工、組立、検査および引き渡しに至るまでの製造工程に適用されている、PIR（Production Inspection Record）、ワークシートなどの、作業・検査指示書および記録のこと。	航空局発行　無人航空機の型式認証等の取得のためのガイドライン

449

450

Appendix 2 各セクションの解説書の見方

【資料の構成】

1　目的

ここでは基準項目とスコープを記載

例：001 設計概念書（CONOPS）に対する「航空局ガイドライン」の解説書である

2　対象の基準

ここでは、サーキュラー（安全基準は「サーキュラーNo.8-001」、型式認証プロセスの適合性証明計画（CP）については「サーキュラーNo.8-002」）に記載された対象の基準を記載

例：001 設計概念書（CONOPS））

> *・001 設計概念書（CONOPS）*
>
> *申請者は、型式認証を希望する無人航空機の我が国の空域における想定される運用（Concept of Operations: CONOPS）を定義し、航空局又は登録検査機関（以下「検査者」という。）に提出すること。CONOPS には、試験及び運用限界の値と範囲を決定するために十分に詳細な以下の説明を少なくとも含むこと。*
>
> *（a）　意図する運用のタイプ*
>
> *（b）　無人航空機の仕様*
>
> *（c）　気象状態*
>
> *（d）　使用者、無人航空機を飛行させる者及び関係者の責任*
>
> *（e）　コントロールステーション（Control Station: CS）、補助機器及びその他安全基準に適合するために必要な関連システム（Associated Elements: AE）*
>
> *（f）　無人航空機の運用のために使用される無線通信機能（コマンド、コントロール及びコミュニケーション）*
>
> *（g）　人口密度、運用（地理的）の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制（Air Traffic Control: ATC）との連絡、目視内飛行又は目視外飛行の種別（目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離）、航空機との間隔等の運用パラメータ*
>
> *（h）　認証に必要な場合、衝突回避装置*

3　「航空局ガイドライン」（引用）

ここでは、「航空局ガイドライン」に記載された対象の内容を記載する。ただし安全基準については、「基準の概要」、「適合性証明方法（MoC）」、「その他参考となる情報」を引用記載し、「検査のポイント」および「検査者の関与度（LOI）」については引用記載しない。

・001 設計概念書（CONOPS）

基準の概要

本基準は、設計概念書（CONOPS）を適切に作成するために記載すべき事項をまとめたものです。

空港から空港へ定型的な運航を行い、歴史ある地上施設と手順に支えられた有人航空機とは異なり、無人航空機においては様々な運用形態が考えられます。運用形態に応じた適切な機体であることを証明することが型式認証制度の根幹となるため、CONOPS は証明活動のファーストステップとして適切に設定する必要があります。なお、CONOPS にはD&R の各試験における条件や範囲を決定するために十分に詳細な記述が求められます。

適合性証明方法（MoC）：1

(a)～(h): セクション 001 CONOPS (MoC 1)

以下の情報を含む CONOPS を作成します。

（a） 意図する運用のタイプ

航空法第 132 条の 85 第 1 項（飛行の禁止空域）及び同第 132 条の 86 第 2 項（飛行の方法）における適否

（b） 無人航空機の仕様

- 機体本体の基本仕様（機体のサイズや使用される材料等の物理的な特性、機体の最高速度やペイロード等の性能的な特性、運用環境）
- 搭載できるオプション装備品（ex.カメラ、測量装置）の仕様
- 性能特性
  飛行距離、飛行時間、ルートの複雑性、重量、重心、密度高度、速度、エネルギー貯蔵系統の容量、操縦者と無人航空機の比率（1 操縦者が同時に操縦可能な無人航空機の数）、飛行フェーズごとの自動・自律状態、推進システム（原理、種類、数、能力など）、航法センサ、飛行制御システム、逸脱防止システム（ジオフェンス、ジオアウェアネス等）
- 運用環境
  外気温度、風速、夜間運用、電磁干渉（Erectromagnetic Interference:EMI）及び高強度放射電界（High Intensity Radiated Field: HIRF）環境

(c)　気象状態

雷、雨、雪及び着氷状態など運用できる気象条件を記載
必要に応じてその他、特殊な気象現象(霧や煙で視界が確保できない場合、霧や火山灰が機体に侵入し安全な飛行に影響がある場合など)に対し運用できる気象条件を記載

(d)　運用者、操縦者及び当該無人航空機の運用に関係する者の責任

(e)　コントロールステーション(CS)、補助機器及びその他安全基準に適合するために必要な関連システム(AE)

(f)　無人航空機の運用のために使用される無線通信機能(コマンド、コントロール及びコミュニケーション)

(g)　人口密度、運用(地理的)の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制(Air Traffic Control: ATC)との連絡、目視内飛行又は目視外飛行の種別
(目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離)、航空機との間隔等の運用パラメータ

(h)　認証に必要な場合、衝突回避装置

<u>その他参考となる情報</u>

なし。

4　解説書

4.1　xxxxxxx

引用箇所の明記⇒その解説○○。

【記載方法】

「サーキュラー」および「航空局ガイドライン」“引用部分”（タイトルのみ記載）“に関する解説(「サーキュラー」にも「航空局ガイドライン」にも記載があるもの)、「サーキュラー」“引用部分(タイトルのみ記載)“に関する解説(「サーキュラー」にしか記載のないもの)、「航空局ガイドライン」“引用部分”(タイトル)“(タイトルのみ記載)“に関する解説(「航空局ガイドライン」にしか記載のないもの)などから引用箇所を明記しその解説を記載する。

5　今後の課題(未議論項目)

WG 活動で話題に上がったが未対応(今後対応予定)項目は以下の通り

5.1 xxxxxxxx

報告書本文○○。

482 5.2 xxxxxxxxxx
483 報告書本文○○
484 ○○○○○。○○
485
486 Appendix 1 証明手順例など
487 Appendix 2 各セクション特有の用語集
488 Appendix 3 関連文書
489 Appendix 4 サブ WG 構成員名簿
490

Appendix3 WG 構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG の構成員名簿（WG 主査副査およびレビュワー）を以下に示す。なお、各サブ WG の講成員名簿は別紙を参照すること。

レビュワーについては、DRAFT1 及び 2 においてレビューコメントを寄せたレビュワー情報を今後追記予定

役割	所属	氏名
WG 主査	東京大学大学院　工学系研究科　航空宇宙工学専攻	五十嵐　広希
WG 副査	株式会社 SClabAir	各務　博之
WG 副査	AeroVXR 合同会社	中田　博精
以下、レビュワー		
	○○○○株式会社	三菱　太郎
	××××大学	四菱　花子
	□□□研究所	

Appendix4 委員会 構成員名簿

「無人航空機の第二種認証に対応した証明手法の事例検討委員会」の構成員名簿を以下に示す。
（2024 年 3 月時点の委員、所属、肩書）

委員長　鈴木 真二	国立大学法人 東京大学 未来ビジョン研究センター 特任教授
委 員　野波 健蔵	一般社団法人 日本ドローンコンソーシアム 会長
委 員　佐藤 彰	一般社団法人 日本産業用無人航空機工業会 顧問
委 員　菊地 隆	一般社団法人 農林水産航空協会 航空安全・技術室長
委 員　佐々木 徹	一般社団法人 日本航空宇宙工業会 技術部 部長
委 員　高橋 教雄	一般社団法人 航空イノベーション推進協議会
	航空機装備品認証技術コンソーシアム 代表
委 員　又吉 直樹	国立研究開発法人 宇宙航空研究開発機構 航空技術部門
	航空利用拡大イノベーションハブ ハブ長
委 員　若井 洋	福島ロボットテストフィールド 副所長
関係省庁	国土交通省 航空局 安全部 航空機安全課
関係省庁	国土交通省 総合政策局 技術政策課
関係省庁	警察庁 長官官房 技術企画課
関係省庁	警察庁 警備局 警備運用部 警備第一課
関係省庁	警察庁 警備局 警備運用部 警備第三課
関係省庁	総務省 総合通信基盤局 電波部 移動通信課
関係省庁	総務省 総合通信基盤局 電波部 基幹・衛星移動通信課
関係省庁	農林水産省 大臣官房政策課 技術政策室 技術調査班
関係省庁	農林水産省 農産局 技術普及課
関係省庁	林野庁 森林整備部 研究指導課
関係省庁	防衛省 陸上自衛隊 教育訓練研究本部
関係省庁	防衛省 航空自衛隊 航空開発実験団
関係省庁	経済産業省 製造産業局 航空機武器宇宙産業課 次世代空モビリティ政策室
関係者	無人航空機の認証に対応した証明手法の事例検討 WG 構成員
オブザーバ	一般財団法人 日本規格協会 産業基盤系規格開発ユニット
オブザーバ	一般財団法人 日本海事協会
オブザーバ	IPA デジタルアーキテクチャ・デザインセンター
オブザーバ	各団体所属の企業
	一般社団法人 航空イノベーション推進協議会

一般社団法人 日本航空宇宙工業会
一般社団法人 日本産業用無人航空機工業会
一般社団法人 日本ドローンコンソーシアム
日本無人機運行管理コンソーシアム
一般社団法人日本 UAS 産業振興協議会
一般社団法人 ドローン操縦士協会
一般社団法人 農林水産航空協会
ReAMo プロジェクトを構成する各コンソーシアム関係者

以上

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

543

RMD-001 DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション001設計概念書（CONOPS） 解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン（以降、「航空局ガイドライン」と呼ぶ）」安全基準「セクション 001 設計概念書（CONOPS）（以降、「セクション 001」と呼ぶ）」についての解説書であり、第二種型式認証を対象とする。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）」の「001 設計概念書（CONOPS）」を以下に引用する。

> *・001 設計概念書（CONOPS）*
>
> *申請者は、型式認証を希望する無人航空機の我が国の空域における想定される運用（Concept of Operations: CONOPS）を定義し、航空局又は登録検査機関（以下「検査者」という。）に提出すること。CONOPS には、試験及び運用限界の値と範囲を決定するために十分に詳細な以下の説明を少なくとも含むこと。*
>
> *（a） 意図する運用のタイプ*
>
> *（b） 無人航空機の仕様*
>
> *（c） 気象状態*
>
> *（d） 使用者、無人航空機を飛行させる者及び関係者の責任*
>
> *（e） コントロールステーション（Control Station: CS）、補助機器及びその他安全基準に適合するために必要な関連システム（Associated Elements: AE）*
>
> *（f） 無人航空機の運用のために使用される無線通信機能（コマンド、コントロール及びコミュニケーション）*
>
> *（g） 人口密度、運用（地理的）の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制（Air Traffic Control: ATC）との連絡、目視内飛行又は目視外飛行の種別（目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離）、航空機との間隔等の運用パラメータ*
>
> *（h） 認証に必要な場合、衝突回避装置*

3 「航空局ガイドライン」(引用)

航空局ガイドライン 第 3 部 安全基準について 「001 設計概念書(CONOPS)」の「基準の概要」、「適合性証明方法(MoC)」、「その他参考となる情報」を以下に引用する。

・001 設計概念書(CONOPS)

基準の概要

本基準は、設計概念書(CONOPS)を適切に作成するために記載すべき事項をまとめたものです。

空港から空港へ定型的な運航を行い、歴史ある地上施設と手順に支えられた有人航空機とは異なり、無人航空機においては様々な運用形態が考えられます。運用形態に応じた適切な機体であることを証明することが型式認証制度の根幹となるため、CONOPS は証明活動のファーストステップとして適切に設定する必要があります。なお、CONOPS にはD&R の各試験における条件や範囲を決定するために十分に詳細な記述が求められます。

適合性証明方法(MoC):1

(a)~(h): セクション 001 CONOPS (MoC 1)

以下の情報を含む CONOPS を作成します。

(a) 意図する運用のタイプ

航空法第 132 条の 85 第 1 項(飛行の禁止空域)及び同第 132 条の 86 第 2 項(飛行の方法)における適否

(b) 無人航空機の仕様

- *機体本体の基本仕様(機体のサイズや使用される材料等の物理的な特性、機体の最高速度やペイロード等の性能的な特性、運用環境)*
- *搭載できるオプション装備品(ex.カメラ、測量装置)の仕様*
- *性能特性*

  飛行距離、飛行時間、ルートの複雑性、重量、重心、密度高度、速度、エネルギー貯蔵系統の容量、操縦者と無人航空機の比率(1 操縦者が同時に操縦可能な無人航空機の数)、飛行フェーズごとの自動・自律状態、推進システム(原理、種類、数、能力など)、航法センサ、飛行制御システム、逸脱防止システム(ジオフェンス、ジオアウェアネス等)
- *運用環境*

  外気温度、風速、夜間運用、電磁干渉(Erectromagnetic Interference:EMI)及び高強度放射電界(High Intensity Radiated Field: HIRF)環境

(c) 気象状態

雷、雨、雪及び着氷状態など運用できる気象条件を記載

必要に応じてその他、特殊な気象現象（霧や煙で視界が確保できない場合、霧や火山灰が機体に侵入し安全な飛行に影響がある場合など）に対し運用できる気象条件を記載

（d） 運用者、操縦者及び当該無人航空機の運用に関係する者の責任

（e） コントロールステーション（CS）、補助機器及びその他安全基準に適合するために必要な関連システム（AE）

（f） 無人航空機の運用のために使用される無線通信機能（コマンド、コントロール及びコミュニケーション）

（g） 人口密度、運用（地理的）の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制（Air Traffic Control: ATC）との連絡、目視内飛行又は目視外飛行の種別（目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離）、航空機との間隔等の運用パラメータ

（h） 認証に必要な場合、衝突回避装置

<u>その他参考となる情報</u>

なし。

79
80
81

4　解説書

注：特に断りがない限り、本解説書中の用語は、サーキュラーNo.8-001、航空局ガイドラインのほか、JIS W 0141 の定義に従うものとする。また、「無人航空機に係る規制の運用 における解釈について」（平成 27 年 11 月 17 日、国空航第 690 号、国空機第 930 号）に無人航空機の制度に関連した解釈が示されている。

4.1 CONOPS の意義

型式認証を得ようとするものは、型式認証を希望する無人航空機の我が国の空域における想定される運用（ Concept of Operations: CONOPS ）を定義し、その CONOPS には、D&R の各試験における条件や範囲（試験内容）、運用限界の値などを決定するために十分に詳細な説明を含める必要がある。なぜならば CONOPS がサーキュラーNo.8-001 の多くのセクションから呼ばれる認証活動の根幹（D&R 試験の根拠）だからである。ここでの CONOPS はシステム開発におけるユーザー視点から仕様・特性を記述する文書などの他分野での使われ方とは目的が違う可能性があることに注意が必要である。

また以下のように、サーキュラーNo.8-001 の他セクションもしくは航空局ガイドラインから明確に CONOPS を呼び出している。

セクション 120　緊急時の対応計画

> *セクション 001 CONOPS には以下を含めます。*
> *・C2 リンク喪失時の各飛行フェーズにおける機体の仕様*
> *・C2 リンクの性能低下により最低性能要件を満たさない場合の離陸時における機体の仕様*
> *［引用：航空局ガイドライン］*

セクション 130　悪天候

> *（b）下記（c）項の場合を除き、無人航空機は CONOPS で定義した悪天候の範囲内において計画外飛行又は制御不能を生じることなしに運用できるような特性を有されなければならない。*
> *「ガイドライン」CONOPS に運用可能な悪天候の定義を含めます。*
> *［引用：航空局ガイドライン］*

セクション 300　耐久性及び信頼性（以降、「セクション 300」と呼ぶ）

> *無人航空機は、CONOPS に記載され、また型式認証データシート及び無人航空機飛行規程に無人航空機運用限界として含まれる、運用環境の制限下で運用された場合に耐久性と信頼性を持つように設計されなければならない。*
> *(d) 試験では CONOPS で指定される運用タイプに応じた別々の飛行プロファイル及びルートの分布を示さなければならない。*
> *(e) 試験は、CONOPS で指定される想定環境下で行わなければならない。これには、電磁干渉(EMI)と高強度放射電界(HIRF)環境を含む。*
>
> *[引用:航空局ガイドライン]*

また明示的に記載されていないが、CONOPS に必要な情報を記載する必要があると想定されるサーキュラーNo.8-001 の他セクションとしては以下がある。

セクション 100　無人航空機に係る信号の監視と送信

> *無人航空機は、安全な飛行と運用の継続に必要なすべての情報を監視し、関連システム(AE)に送信するように設計されなければならない 。その情報には、少なくとも以下を含むこと。*
> *(a) すべてのエネルギー貯蔵系統のすべてのクリティカルパラメータの状態*
> *(b) すべての推進系統のすべてのクリティカルパラメータの状態*
> *(c) 飛行及び航法の情報(例えば、対気速度、針路、高度、位置等)*
> *(d) 緊急時の情報や状態を含む通信及び航法信号の強度並びに品質*
>
> *[引用:サーキュラーNo.8-001]*

なお、航空局ガイドラインには、「設計図面には、上記(a)～(d)に対する無人航空機の設計仕様とその詳細を記載します。」と書かれているが、CONOPS にあらかじめこれらの情報を記載し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

セクション 105　無人航空機の安全な運用に必要な関連システム

> *(a)申請者は、無人航空機の安全性に影響を与え、又は無人航空機が安全基準を満たすために必要な無人航空機システムのすべての関連システム(AE)及びインターフェース条件を特定し、検査者に提出しなければならない。この要件の一部として、以下のものが含まれる。*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインには「当該設計図面には、上記基準(a)および(b)(4)を満足する関連システムとインターフェース条件を示します。」と書かれているが、CONOPS にあらかじめこれらのシステム概要を記載し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

セクション 115 サイバーセキュリティ

> *(a)別のシステムと連携する無人航空機の機器、システム及びネットワークは、無人航空機の安全性に悪影響を及ぼす意図的で許可されていない電子的な干渉から守られなくてはならない。セキュリティ対策は、セキュリティリスクが特定され、評価され、かつ、必要により緩和されていることを示すことによって確実になされなければならない。*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインには「Threat Condition の原因となるシステムを抽出する」こととあり、CONOPS で表される全体のシステム設計から解析がスタートすることとなると考えられる。また、想定する運用に際して、「意図的で許可されていない電子的な干渉」を行う攻撃者の性質を想定する必要があるため、CONOPS にあらかじめこのようなシステム概要および運用、保護されるべきセキュリティレベルの想定を記述することが望ましいと考えられる。

セクション 125 雷

> *下記(b)項の場合を除き、無人航空機は雷撃による計画外飛行又は制御不能がないような設計特性を有さなければならない。*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインには「適合性証明方法(a): TBD 無人航空機における証明手法は未定です。」と書かれているが、当該設計特性を有する場合には、CONOPS にあらかじめ、その設計概要を記載し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

セクション 140-4 危険物輸送

> *危険物の輸送を行う無人航空機にあっては、危険物の輸送に適した装備が備えられていなければならない。*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインには「危険物輸送設計図面 (MoC 1) 危険物輸送に適した装備について、その設計が妥当であることを証明します。」と書かれているが、CONOPS にあらかじめ当該機体が危険物の輸送に用いられるものであり、輸送しようとする危険物の種類などを記載し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

セクション 305 起こり得る故障

> *無人航空機は、単一の起こり得る故障によって機体の制御不能又は想定飛行範囲からの逸脱を生じないように設計されなければならない。これは、試験により実証されなければならない。*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインには「飛行試験方案（MoC 6） 以下の故障状態を意図的に発生させて、無人航空機が制御不能または想定飛行範囲からの逸脱を起さないことを評価します。」と書かれているが、CONOPS にあらかじめ、該当する故障の検知方法や対処方法を記載し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

セクション 310 能力及び機能（以降、「セクション 310」と呼ぶ）

> *(a)無人航空機に求められる以下のすべての能力及び機能は、試験により実証されなければならない。*
> *(b)認証に必要な場合、以下の能力及び機能は、試験により実証されなければならない。*
>
> ［引用：*航空局ガイドライン*］

航空局ガイドラインには「飛行試験方案（MoC 6） 試験ケースとして以下を考慮し、試験方案を作成します。」と書かれているが、CONOPS にも当該能力および機能の作動条件などもあらかじめ記述し、検査者と共有することは認証プロセスのスムーズな実施に有益と考えられる。

以上のセクション以外においても CONOPS の内容が間接的なインプットとなりうることに注意する必要がある。そして、CONOPS に記載される重要な項目は、最終的には無人航空機飛行規程に含まれる内容であることにも注意する必要がある。 特に「無人航空機運用限界」は航空局が承認する内容であるため、運用環境の限界などの記載には留意する必要がある。

また、CONOPS は申請後ただちに提出する文書であるが、申請後も型式認証書発行まで間にその段階に応じた成熟度に更新していく必要がある Living Document（絶えず更新または編集される文書）である。一般的には以下のような段階を経て、最終形に至る（図 4.1-1）。

1. 適用基準の判断ができるレベルの CONOPS
2. 適合性証明計画合意の判断ができるレベルの CONOPS
3. 試験方案合意の判断ができるレベルの CONOPS
4. 型式認証書発行の判断ができるレベルの CONOPS

CONOPS は認証活動の根幹（型式認証試験の前提）となることから、認証の全期間をとおして常に参照・精査（認証試験結果により、必要に応じて修正）され、最終的に型式認証証明書類として検査者から適合性判定を受ける必要がある。

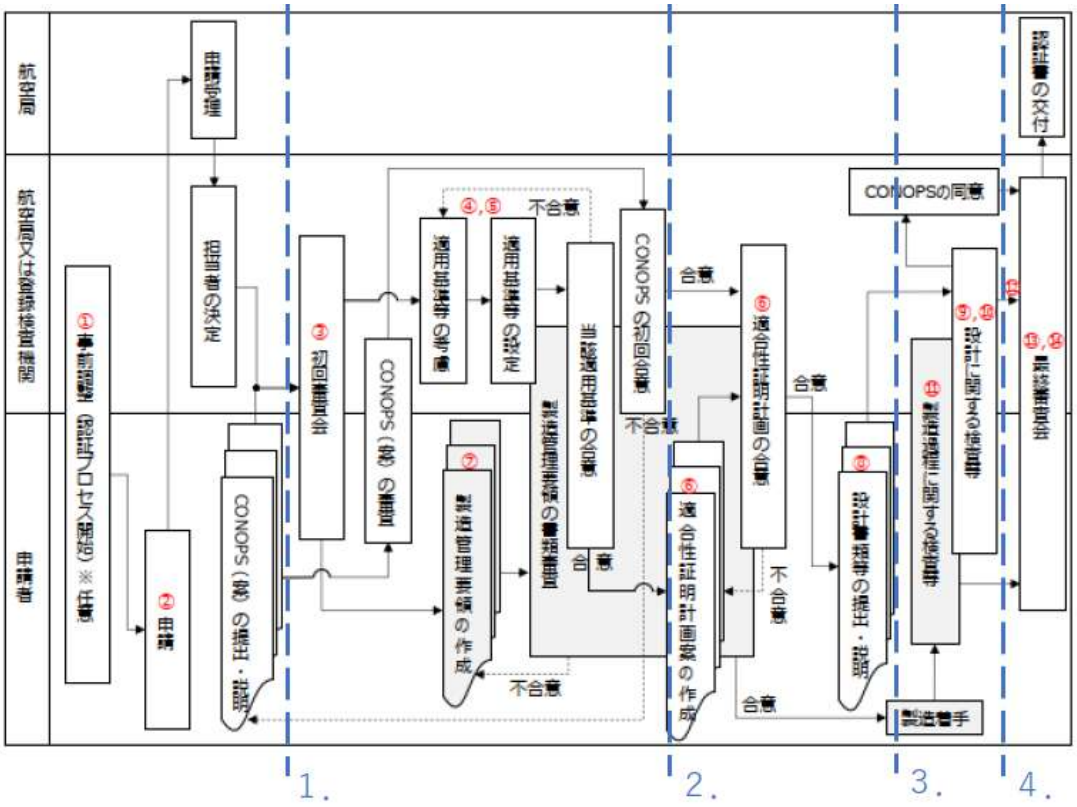


図 4.1-1 事前調整～認証書の交付まで

出所）航空局ガイドライン

以降は、サーキュラーNo.8-001 のセクション 001(a)～(h)各項に記載する内容について個別に解説を行う。

各解説は、サーキュラーNo.8-001 の記述内容、航空局ガイドラインの記述内容を引用・併記し、それらに対する解釈を記載する。なお機体のタイプはマルチコプターを想定している。

4.2 セクション 001(a) 意図する運用のタイプ

> *001 設計概念書（CONOPS）*
> *(a)意図する運用のタイプ*
>
> *FAA D&R.001 Concept of Operations（参考）*
> *(a) The intended type of operations;*
>
> *[引用:サーキュラーNo.8-001]*

> *適合性証明方法(MoC):1（設計図面 / Design/Data Review）*
> *以下の情報を含む CONOPS を作成します。*
> *(a) 意図する運用のタイプ*
> *航空法第 132 条の 85 第1項(飛行の禁止空域)及び同第 132 条の 86 第 2 項(飛行の方法)における適否*
>
> *[引用:航空局ガイドライン]*

【解説】

＜解釈＞

認証を受けようとする型式の無人航空機が、航空法第 132 条の 85 第 1 項(飛行の禁止空域)および同第 132 条の 86 第 2 項(飛行の方法)で規定されている特定飛行のうちどれに対応したものとなるのかを明確にする。(該当する特定飛行に応じて適用される規定が異なるものがある。)

＜記載内容例＞

航空法	特定飛行の内容	適用非適用の別
航空法第132条の85第1項第1号	空港等の周辺の空域、緊急用務空域又は150m以上の上空	適用・非適用
同法　同条　同項　第2号	人又は家屋の密集している地域(DID)の上空	適用・非適用
航空法第132条の86第2項第1号	夜間飛行	適用・非適用
同法　同条　同項　第2号	目視外飛行	適用・非適用
同法　同条　同項　第3号	人又は物件から30m以上の距離が確保できない飛行	適用・非適用
同法　同条　同項　第4号	催し場所上空の飛行	適用・非適用
同法　同条　同項　第5号	危険物の輸送	適用・非適用
同法　同条　同項　第6号	物件投下	適用・非適用

図 4.2-1 セクション 001(a) 意図する運用のタイプの記載例

4.3 セクション 001(b) 無人航空機の仕様

001 設計概念書（CONOPS）
(b)無人航空機の仕様

FAA D&R.001 Concept of Operations（参考）
(b) UA specifications;

[引用:サーキュラーNo.8-001]

適合性証明方法(MoC):1（設計図面 / Design/Data Review）
以下の情報を含む CONOPS を作成します。

(b) 無人航空機の仕様
□機体本体の基本仕様(機体のサイズや使用される材料等の物理的な特性、機体の最高速度やペイロード等の性能的な特性、運用環境)
□搭載できるオプション装備品(ex.カメラ、測量装置)の仕様
□性能特性
飛行距離、飛行時間、ルートの複雑性、重量、重心、密度高度、速度、エネルギー貯蔵系統の容量、操縦者と無人航空機の比率(1操縦者が同時に操縦可能な無人航空機の数)、飛行フェーズごとの自動・自律状態、推進システム(原理、種類、数、能力など)、航法センサ、飛行制御システム、逸脱防止システム(ジオ・フェンス機能、ジオ・アウェアネス機能等)
□運用環境
外気温度、風速、夜間運用、電磁干渉(Electromagnetic Interference : EMI)及び高強度放射電界(High Intensity Radiated Field : HIRF)環境

[引用:航空局ガイドライン]

【解説】

＜解釈＞

「航空局ガイドライン」の各項目(機体本体の基本仕様、搭載できるオプション装備品、性能特性、運用環境)について、セクション 300 の飛行試験における環境などの試験条件や証明すべき事項となることに留意して記述する。

＜記載内容例＞

- 機体本体の基本仕様(機体のサイズや使用される材料などの物理的な特性)

（以下は参考例）
分類:固定翼無人航空機/プロペラ推進・ジェット推進、回転翼無人航空機/ヘリコプタ・マルチロータなど
主要寸法:機体全長・全幅、全高、およびロータ直径など(マルチロータ機の場合、軸間距離も)
主要重量(最大離陸重量、機体重量など)、重心位置(許容範囲)
ロータ数および配置など
使用されている主要構造部材の材料と使用されている場所
（特に複合材などの新素材については重点的に説明することが望ましい）

- 搭載できるオプション装備品(ex.カメラ、測量装置)の仕様

（以下は参考例）
機体重量と重心位置、電気的負荷、飛行特性などに影響を与える可能性のあるオプション装備品に関する情報（重量や重心位置、大きさ、電気的負荷などの情報を含む）。

- 性能特性

無人航空機が認証を受ける運用可能な範囲を記載する。運用可能な範囲としては、無人航空機が能力的に到達可能な限界値またはそれよりも安全側の値を採用することが望ましい。
（以下は参考例）
最大速度 / 最大巡航速度 / 最大上昇速度/最大降下速度 /最大対地高度（150m など）
高地運用をする場合には、最大運用可能標高（例えば 2,000m など）と最大/最小外気温度
最大飛行距離 / 最大飛行時間 / 最大チルト角 / 最大ヨーレート

- ルートの複雑性、エネルギー貯蔵系統の容量、操縦者と無人航空機の比率（1 操縦者が同時に操縦可能な無人航空機の数）、飛行フェーズごとの自動・自律状態

  - ルートの複雑性 （以下は参考例）
    具体的に想定される、代表的なフライトプロファイル（図を用いて説明）
  - エネルギー貯蔵系統の容量（以下は参考例）
    バッテリ容量
  - 操縦者と無人航空機の比率
    1 操縦者が同時に操縦可能な無人航空機の数
  - 飛行フェーズごとの自動・自律状態（以下は参考例）
    「離陸」「上昇」「巡航」「降下」「着陸」「滞空（ロイター）」「ホバリング」などの飛行フェーズの定義をした上で、飛行フェーズごとに、例えば、「離陸」「上昇」は手動操縦、「巡航」は自動操縦などを記載（図で示すのが分かりやすい）

なお、自律飛行、自動操縦の定義は以下が考えられる。
自律飛行：（JIS W 0141 の定義、「航空局ガイドライン」にも同様の記述あり）
飛行中に遭遇するあらゆる状況に対し、地上からの指示によらず、安全を確保した自動動作を継続し得る飛行
自動操縦：（「無人航空機に係る規制の運用における解釈について」に解釈が示されているとともに JIS W 0141 に定義されている。サーキュラーNo.8-001・航空局ガイドラインに定義はない）
＜「無人航空機に係る規制の運用における解釈について」の解釈＞
プログラムにより自動的に飛行するものであるが、地上からの指示も受け入れるもの
＜JIS W 0141 の定義＞
飛行中における無人航空機の姿勢の変化または設定された飛行条件に応じて、組み込まれたプログラムによってロータ、操だ面などを自動的に作動して、無人航空機の運動（方向、高度、速度など）、姿勢などを制御すること、またはその機能飛行するものであるが、地上からの指示

も受け入れるもの

- 推進システム（原理、種類、数、能力など）
（以下は電気を用いた推進システムの参考例）

（1）バッテリからモータに至る電力供給経路を含む電源系統の詳細
（2）使用されているモータの種類、数
（3）モータの最大連続出力（W）
（4）モータの最大ピーク電力出力（W）
（5）モータの電流範囲（A）
（6）ロータブレードの仕様（ブレード長、ピッチ角）
（7）ESC（Electric Speed Controller）の仕様
（8）他系統と電力源が共用されている場合、各系統間の電力管理
（9）推進システムが複数のモータで構成される場合、各モータへの電力配分法
（10）バッテリの劣化状況および交換時期の把握手法
（11）バッテリの残量および状態の検知方法、ならびに低残量および状態の異常を監視し、操縦者に提供する方法
（12）推進システム電源喪失時にバックアップ電源が利用できる場合、以下を含むその作動原理
▸バックアップ電源から電力供給を受けるシステム
▸バックアップ電源から電力供給を受けないシステムおよびその負荷遮断法
▸バックアップ電源による運用可能時間とその算出根拠

- 航法センサ、飛行制御システム、逸脱防止システム（ジオ・フェンス機能、ジオ・アウェアネス機能など）
機体に搭載されるアビオニクスシステムについて、構成する航法機器、飛行制御機器（FCC/FMC）、センサ機器の機能について記載する

■ 航法センサ（以下は参考例）
無人航空機の位置検出センサまたは位置計測方法

■航法機器、飛行制御機器（以下は参考例）
（1）無人航空機を目的地まで、または計画された飛行経路に沿って誘導する方法
（2）主要な航法機能が失われた場合の（システムまたは操縦者による）識別方法と、失われた場合の対応
（3）飛行自動化のレベル（手動、姿勢制御、位置速度など飛行状態制御、自動などの飛行モード）および操縦者による操縦への介入方法
（4）飛行制御システムについて、制御（姿勢制御、飛行状態制御、自動）と誘導の概要
（システムブロック図などを用いて記載を推奨）

- 逸脱防止システム（ジオ・フェンス機能、ジオ・アウェアネス機能など）（以下は参考例）
  運用領域または空域からの逸脱を防止、回避システムを有する場合には、システムまたは機器の動作原理・機能概要

- 運用環境
  運用可能な、外気温度、風速、夜間運用、電磁干渉（Electromagnetic Interference：EMI）および高強度放射電界（High Intensity Radiated Field：HIRF）環境の限界を記載

  - 外気温度（以下は参考例）
    安全な運用が可能な外気温度範囲および、保管・運搬に許容される温度範囲
  - 風速（以下は参考例）
    離着陸およびホバリング時を含む、想定する運用が可能となる最大の風速とその風向
  - 夜間運用（以下は参考例）
    夜間飛行を行う無人航空機にあっては、無人航空機の姿勢および方向が正確に視認できるよう灯火を有していることを、灯火の仕様、機上の灯火配置図などを含めて記載
  - 電磁干渉および高強度放射電界環境（以下は参考例）
    これらの環境下で運用を許容する場合は、許容できる EMI レベル、HIRF レベルを記載。また、その際のそれらの環境に対する安全対策について記載。
    許容されない場合は、そのような環境に遭遇しないための手順や運用制限を記載。（この場合は、無人航空機飛行規程に制限事項として記載する必要がある）

4.4 セクション 001(c)気象条件

> *001 設計概念書（CONOPS）*
> *(c)気象状態*
>
> *FAA D&R.001 Concept of Operations（参考）*
> *(c) Meteorological conditions;*
>
> *［引用:サーキュラーNo.8-001］*

> *適合性証明方法(MoC):1（設計図面 / Design/Data Review）*
> *以下の情報を含む CONOPS を作成します。*
> *(c) 気象状態*
> *雷、雨、雪及び着氷状態など運用できる気象条件を記載*
> *必要に応じてその他、特殊な気象現象（霧や煙で視界が確保できない場合、霧や火山灰が機体に侵入し安全な飛行に影響がある場合など）に対し運用できる気象条件を記載*
> *［引用:航空局ガイドライン］*

【解説】

＜解釈＞

航空局ガイドラインの各項目（雷、雨、雪、着氷状態など）について、その環境下での運用の可否、運用可能な場合にはその条件や運用手順について記述する。運用可能な気象条件は、セクション 300 の飛行試験にて実証することが求められる。

＜記載内容例＞

- 雷、雨、雪および着氷状態など運用できる気象条件を記載
  （以下は参考例）
  - ■ 降雨、降雪下の運用の可否
    可能な場合には運用可能な閾値
  - ■ 運用が許容される最小視程
  - ■ 着氷気象状態における運用の可否
    運用が許容される場合は、防氷装置について記載する。
    許容されない場合は、そのような気象に遭遇しないための機能または手順を記載する。（この場合、無人航空機飛行規程に制限事項として記載する必要がある。）
  - ■ 雷撃の可能性がある気象状態における運用の可否
    運用が許容される場合は、雷撃に対する安全対策について記載する。
    許容されない場合は、そのような気象に遭遇しないための機能または手順を記載する。（この場合、無人航空機飛行規程に制限事項として記載する必要がある。）
  - ■ 特殊な気象現象（霧や煙で視界が確保できない場合や、霧や火山灰が機体に侵入する可能性がある場合など）下の運用の可否
    可能な場合には運用可能な気象条件を記載

4.5 セクション 001(d) 使用者、無人航空機を飛行させる者及び関係者の責任

001 設計概念書（CONOPS）
(d)使用者、無人航空機を飛行させる者及び関係者の責任

FAA D&R.001 Concept of Operations（参考）
(d) Operators, pilots, and personnel responsibilities;
［引用:サーキュラーNo.8-001］

適合性証明方法(MoC):1（設計図面 / Design/Data Review）
以下の情報を含む CONOPS を作成します。
（d）運用者、操縦者及び当該無人航空機の運用に関係する者の責任
［引用:航空局ガイドライン］

【解説】

＜解釈＞

メーカー(設計者)から運航者に対して組織的に求める事項や推奨する運航体制などについて記載(個々の運航者の運航体制について、メーカーは義務付ける立場にない)。

本項目の記載はセクション 300 番台の飛行試験の体制などの構築のために参照される。

＜記載内容例＞

- 人航空機の形態管理(以下は参考例)
  - 許容される形態変更の範囲、管理方法について記載
- 無人航空機の点検・整備方法(以下は参考例)
  - 認証を受ける無人航空機の安全な運用に必要な点検・整備の考え方
  - 整備を実施するにあたり特別な整備体制や資格
  - 無人航空機システムの地上での輸送方法

(メーカーの推奨事項として以下の記載も有用)

- 運用方針(以下は参考例)
  - 実環境で制限された範囲内で運用を遂行できることを保証する、技術的または手続き上の指針
    想定されるすべての運用に適用される標準的な運用手順
    緊急手順、非常手順、事故および重大インシデント発生時の対処手順
- 運用体制(以下は参考例)
  - 安全な運用のための管理体制およびそれを維持するための手法(例:規約などの文書)

- 運用要員（以下は参考例）
  - 最低限必要な要員（運用責任者、操縦者、操縦補助者、監視者、安全管理者など）の任務および責任
- 運用要員の訓練（以下は参考例）
  - 運用要員に必要な能力を獲得または維持するための手順（例：初期訓練および資格付与の手順）

4.6 セクション 001(e) コントロールステーション、補助機器及びその他安全基準に適合するために必要な関連システム

001 設計概念書（CONOPS）
(e)コントロールステーション(Control Station: CS)、補助機器及びその他安全基準に適合するために必要な関連システム(Associated Elements : AE)

FAA D&R.001 Concept of Operations（参考）
(e) Control station, support equipment, and other associated elements (AE) necessary to meet the airworthiness criteria;

[引用:サーキュラーNo.8-001]

適合性証明方法(MoC):1（設計図面 / Design/Data Review）
以下の情報を含む CONOPS を作成します。
(e) コントロールステーション(CS)、補助機器及びその他安全基準に適合するために必要な関連システム(AE)

[引用:航空局ガイドライン]

【解説】

＜解釈＞

コントロールステーション(CS)、補助機器およびその他安全基準に適合するために必要な関連システム(AE)について、想定される運用から導かれる仕様(機能)について記載する。

本項目の記載はセクション 300 番台の飛行試験において実証することが求められる。

＜記載内容例＞

- コントロールステーション(CS)(以下は参考例)
  - コントロールステーション(プロポを含む。)の構成と構成要素の機能
    (システムブロック図を適宜使用するとわかりやすい)
  - 操縦者がコントロールステーションから把握できる姿勢、位置、高度の精度
  - 重大な結果に至る指令(例:「モーターを切る」指令)を誤って入力しないための安全対策
  - コントロールステーションの表示またはインターフェースのフリーズに対する対策
  - システムが操縦者に提供する警報(例:バッテリの残量不足、重要なシステムの故障)
  - コントロールステーションに電力を供給する手段。冗長性がある場合はその旨記載する。
- 補助機器およびその他安全基準に適合するために必要な関連システム
  (Associated Elements : AE)

(以下は参考例)

  - キネマチック用 GPS 地上局、発進・回収機材、電源装置などの地上支援機材で、安全な運用に直接影響し、かつ、運用者の責任において管理可能なもの
    (通常運用において使用するものと、バックアップまたは緊急時に使用するものを区別)

4.7 セクション 001(f) 無人航空機の運用のために使用される無線通信機能

001 設計概念書（CONOPS）
(f)無人航空機の運用のために使用される無線通信機能(コマンド、コントロール及びコミュニケーション)

FAA D&R.001 Concept of Operations（参考）
(f) Command, control, and communication functions;
[引用:サーキュラーNo.8-001]

適合性証明方法(MoC):1（設計図面 / Design/Data Review）
以下の情報を含む CONOPS を作成します。
(f) 無人航空機の運用のために使用される無線通信機能(コマンド、コントロール及びコミュニケーション)
[引用:航空局ガイドライン]

【解説】

＜解釈＞

無人航空機の運用のために使用される無線通信機能について、想定される運用から導かれる仕様(機能)について記載する。

本項目の記載はセクション 300 番台の飛行試験において実証することが求められる。

＜記載内容例＞

- C2(コマンド＆コントロール)リンクの仕様(以下は参考例)
  - C2 リンクの使用周波数および帯域幅
  - C2 リンクの構成(情報/データの流れ、サブシステムの性能および、可能であればデータ伝送速度とデータ遅延など)(システムアーキテクチャ図を適宜使用)
  - 無人航空機をコントロールステーションおよび、該当する場合、その他の地上システムまたは地上インフラに接続する C2 リンクに関する性能
    - 証明を受ける最大距離におけるリンクマージン(回線マージン)
    - 操縦者に対し、C2 リンクの信号強度および/または健全性を表示する機能がある場合、強度と健全性に係る表示の決定法値と危険なレベルの劣化と判断する閾値
    - 冗長および/または独立した C2 リンクを採用している場合、これらの設計の違いと、これらに共通した故障モード
- C2 リンク機能劣化に関する事項(以下は参考例)
  - C2 リンクの劣化を操縦者に注意喚起する機能および劣化時の対応
- C2 リンク機能喪失に関する事項(以下は参考例)
  - 以下に起因する C2 リンクの喪失を防止または低減する設計上の特徴

(13)無線周波数自体、または他からの干渉

（14）通信範囲外での飛行
（15）アンテナ遮蔽（旋回時および/または大きな姿勢角変化時）
（16）コントロールステーション機能の喪失
（17）機体機能の喪失（例：電源供給機能など）
（18）降水や霧を含む大気による減衰
＜上記以外に C2 リンク喪失に至る条件があれば記載する＞

■ C2 リンクを喪失した場合の対処手順
（喪失を判断する条件および対処手順に移行する条件を含む）

■ C2 リンクの喪失を操縦者に警告する機能

■ 領域/空域逸脱防止機能（運用領域/空域逸脱防止システム）および衝突回避機能（DAA システム）、ならびに地形認識機能（輻輳/衝突回避システム）がある場合、C2 リンク喪失に対処する自動帰還飛行

■ C2 リンクを短時間で再接続するための機能がある場合、その機能

4.8 セクション 001(g) 運用パラメータ

001 設計概念書（CONOPS）
(g)人口密度、運用(地理的)の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制(Air Traffic Control: ATC)との連絡、目視内飛行又は目視外飛行の種別(目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離)、航空機との間隔等の運用パラメータ

FAA D&R.001 Concept of Operations（参考）
(g) Operational parameters (such as population density, geographic operating boundaries, airspace classes, launch and recovery area, congestion of proposed operating area, communications with air traffic control, line of sight, and aircraft separation);

[引用:サーキュラーNo.8-001]

適合性証明方法(MoC):1（設計図面 / Design/Data Review）
以下の情報を含む CONOPS を作成します。
(g) 人口密度、運用(地理的)の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制(Air Traffic Control: ATC)との連絡、目視内飛行又は目視外飛行の種別(目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類及び最大通信距離)、航空機との間隔等の運用パラメータ

[引用:航空局ガイドライン]

【解説】

＜解釈＞

機体設計に影響を与えると想定される運用環境のうち、機体そのものの性能による制約を除くものを記載。人口密度などの地上(離着陸エリアを含む)の状況、目視内／外などの想定する運用状況、航空交通管制との通信などが想定される。本項目の記載がセクション 300 番台での実証における試験場所や試験方法の環境を決定する根拠となるとともに、証明される運用制限につながる。

＜記載内容例＞

- 運用環境(運用場所／運用方法)(以下は参考例)
  - 無人地帯／有人地帯(有人地帯の場合は人口密度や催し場所上空かどうかなどを含む)空域、飛行高度、運用エリアの混雑度
  - 必要離着陸エリアの広さや、最大運用可能な離着陸場の標高
  - 目視内／目視外、補助者の有無
  - 最大通信距離(目視内の場合)
  - 利用する無線システムの種類および最大通信距離(目視外の場合)
  - 夜間飛行の可否(運用時間)
- 管理制御手法(以下は参考例)
  - 操縦者が、以下からの指示や情報を受ける方法
    航空交通管制 / 監視者 / 運用責任者、安全責任者を含む他の運用要員
  - 二次監視レーダー(SSR)の質問信号に応答する際に送信する情報(位置、高度など)の精度

494 （トランスポンダーを装備する場合）

参考（航空機との間隔について）：
ASTM F3442（Standard Specification for Detect and Avoid System Performance Requirements）において、DAA 機能を用いて適切なアクションを取れば有人機との衝突を回避できる低リスクの領域（well-clear boundary 内）として、半径 2000ft、高低差 100ft（領域としては 200ft の高さ）の円柱状の領域が定義されており、この距離が有人機との間で保っておくべき距離の参考になると考えられる。

495

4.9 セクション 001(h) 衝突回避装置

【解説】

> *001 設計概念書（CONOPS）*
> *(h)認証に必要な場合、衝突回避装置*
>
> *FAA D&R.001 Concept of Operations（参考）*
> *(h) Collision avoidance equipment, whether onboard the UA or part of the AE, if requested.*
>
> *［引用：サーキュラーNo.8-001］*

> *適合性証明方法(MoC):1（設計図面 / Design/Data Review）*
> *以下の情報を含む CONOPS を作成します。*
> *（h）認証に必要な場合、衝突回避装置*
>
> *［引用:航空局ガイドライン］*

＜解釈＞

衝突回避システム／機能が認証に必要となる場合には、その概要（規格への適合性を含む）とともに関連するシステムとの連携、操縦者などの役割などについて記載する。本項目の記載は必要に応じてセクション 310 において実証することが求められる。なお航空局ガイドラインには衝突回避システムについて、性能基準や試験条件などの明確化のために適合性見解書が必要となる可能性があると記載されていることから、航空局との調整が必要となる。

＜記載内容例＞

- 衝突回避システムの仕様
  （機体／地上システムの関連機器に応じて記載する。以下は参考例）
  - 機能、性能、条件などの制約
  - システム／機器の概要、規格／標準への適合性 or 採用の指標
    協調して接近を回避するシステム／機器（例：ACAS）
    協調しない衝突回避システム（例：IR/EO 画像）
    障害物（地形、樹木など）への衝突回避機能
    運用が許容されない気象条件を回避するシステム
  - 操縦者や他の運用要員の役割
  - 飛行制御コンピューターとの連携
  - システムに適用される原理

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定) 項目は以下の通り。

5.1 解説書補足資料の作成

型式認証の申請者などの中には、航空分野の経験が少ないことなどに起因した航空法関係の知識やノウハウが不十分であることにより、本解説書の内容を理解することが難しい者が居ることも想定される。今後、他分野からの参入を含め型式認証の申請者の裾野が拡大していくであろうことを考慮すると、こうした者に対する最低限の知識のベースラインを構築することを目的とし、本解説書の補足資料を準備することが有用であると考えられる。補足資料の内容としては、前提となる基本的事項の解説や CONOPS の内容と各セクションでの証明との関連に関する解説といったことが考えられる。

Appendix 1 各セクション特有の用語集

DRAFT2 にて加筆予定

Appendix 2 関連文書

DRAFT2 にて加筆予定

Appendix 3 サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG における 001 サブ WG 設計概念書（CONOPS）の構成員名簿（サブ WG 主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD DRAFT Rev.01）Appendix3 を参照すること。

役割	氏名	所属
主査、ライター	宮川 毅也	一般財団法人日本海事協会
ライター	後藤 敬太	AeroVXR 合同会社

545

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

546

RMD-105 DARFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 105

無人航空機の安全な運用に必要な関連システム　解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

73

図 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」という）安全基準セクション「セクション 105 無人航空機の安全な運用に必要な関連システム（以降、「セクション 105」と呼ぶ）」に対する解説書である。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001 “無人航空機の型式認証 等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）の「セクション 105」を以下に引用する。

・105 無人航空機の安全な運用に必要な関連システム

無人航空機は、CONOPS に記載され、また型式認証データシート及び無人航空機飛行規程に無人航空機運用限界として含まれる、運用環境の制限下で運用された場合に耐久性と信頼性を持つように設計されなければならない。その耐久性及び信頼性はここに記載する要件に従い、飛行試験で実証しなければならない。試験は、計画外飛行、制御不能、想定飛行範囲からの逸脱又はリカバリーエリア外での非常着陸につながる不具合なく完了しなければならない。

（a） 申請者は、無人航空機の安全性に影響を与え、又は無人航空機が安全基準を満たすために必要な無人航空機システムのすべての関連システム（ AE ）及びインターフェース条件を特定し、検査者に提出しなければならない。この要件の一部として、以下のものが含まれる。

（1） 申請者は、特定の関連システム（ AE ）又は関連システム AE ）の最低限の仕様のいずれかを特定すること。

（i） 最低限の仕様が特定されている場合、性能、互換性、機能、信頼性、インターフェース、パイロットアラート、環境要件等、関連システム（ AE ）の重要な 項目を含める必要がある。

（2） 重要な項目とは、それが満足できない場合に、無人航空機を安全かつ円滑に運用する能力に影響を与えるものを指す。申請者は、無人航空機とのインターフェースとなる関連システム（ AE ）として明確に指定された旨が表示されたインターフェース管理図面、要求文書、その他文書を使用することができる。

（b） 申請者は、上記（ 項で特定された関連システム（ AE ）又は最低限の仕様が以下を満足することを示さなければならない。

（1） 関連システム（ AE ）は、関連システム以外の設計と組み合わせて無人航空機の安全性を保証するための機能、性能、信頼性及び情報を提供すること。

（2） 関連システム（ AE ）は、無人航空機の能力及びインターフェースと互換性があること。

(3) 関連システム(AE)は、安全な飛行と運用に必要なすべての情報(セクション 100 で特定されたものを含むが、これに限定されない。)を監視し、無人航空機を飛行させる者に送信する必要がある。

(4) 最低限の仕様が特定されている場合、それらは無人航空機の安全性を保証するために、正しく、完全で、一貫性が あり、検証可能であること。

(c) 航空局は、承認された関連システム(AE)又は関連システム AE)の最低限の仕様を運用限界として設定し、それらを無人航空機型式認証データシート及び申請者により作成される無人航空機飛行規程に含める。

(d) *申請者は、無人航空機の安全性に対する関連システム(AE)からの影響に対処するために必要な整備手順を作成しなければならない。これらの手順は、セクション 205 として要求される、無人航空機等に対する点検及び整備 を行うため の手順書(以下「 ICA 」という。)に含まれる。*

3 「航空局ガイドライン」(引用)

「航空局ガイドライン」 安全基準 「セクション 105」の「基準の概要」、「適合性証明方法(MoC)」、「その他参考となる情報」を以下に引用する。

・*105 無人航空機の安全な運用に必要な関連システム*

基準の概要

本基準は、無人航空機の安全性に影響を与えるすべての関連システム及びインターフェース条件が適切であることを示すために、それらの特定、適切性及び関連書類への反映を要求しています。

具体的には以下を行う必要があります:

- *関連システムとインターフェース条件の特定*
- *関連システムが無人航空機の安全な運用に適切なものとなっていることの検証*
- *関連システムの運用限界の設定*
- *関連システムの整備手順の設定*

適合性証明方法(MoC):1、6

(a),(b)(4): セクション 105 関連システム設計図面 (MoC 1)

当該設計図面には、上記基準(a)及び(b)(4)を満足する関連システムとインターフェース条件を示します。満足すべき上記基準(a)及び(b)(4)の詳細は以下の表のとおりです。

満足すべき基準(a)、(b)(4)の詳細

基準	*関連システム*	*インターフェース条件*
(a)	● *関連システムを特定することができる型式番号等で示すこと。または、関連システムを特定することができる最低限の仕様で示すこと。* ● *最低限の仕様で示す場合、性能、互換性、機能、信頼性、インターフェース、パイロットアラート、環境要件等の重要な項目を含むこと。(重要な項目とは、それが満足できない場合に、無人航空機の安全と効率的に運用する能力に影響を与えるものを指します。)*	● *無人航空機の安全な運用に影響を与えるインターフェース条件を示すに当たって、インターフェース管理図面、インターフェース要求文書又その他参考資料を使用すること。*
(b)(4)	● *最低限の仕様が特定されている場合、それらは無人航空機の安全性を保証するために、正しく、完全で、一貫性があり、検証可能であることを示すこと。*	*N/A*

(b)(1), (b)(2): セクション 300 飛行試験方案 (MoC 6)

無人航空機の信頼性を検証するセクション300 飛行試験をとおして、各関連システムが信頼性と安全性を保証するための情報を適切に提供していることを検証します。あわせて、関連システムが無人航空機の能力及びインターフェースと互換性があることを実証します。

(b)(1), (b)(2): セクション 300 飛行試験報告書 (MoC 6)

試験結果を報告書としてまとめます。

(b)(1), (b)(2): セクション 310 飛行試験方案 (MoC 6)

無人航空機の性能及び機能を検証するセクション 310 飛行試験をとおして、各関連システムが性能、機能及び安全性を保証するための情報を適切に提供していることを検証します。あわせて、関連システムが無人航空機の能力及びインターフェースと互換性があることを実証します。

(b)(1), (b)(2): セクション 310 飛行試験報告書 (MoC 6)

試験結果を報告書としてまとめます。

(b)(3): セクション 100 飛行試験方案 (MoC 6)

上記基準(a)、(b)(4)に対して特定された関連システムが安全な飛行と運用に必要なすべての情報(セクション 100 で特定されたものを含むが、これに限定されない。)を監視し、操縦者に送信することを検証するための飛行試験です。セクション 100 飛行試験方案に含めるか、またはセクション 105 飛行試験方案として別に設定するかは自由度があります。なお、運用エンベロープ及び運用制限内で各関連システムのクリティカルな運用環境を考慮して、飛行試験方案を作成する必要があります。

(b)(3): セクション 100 飛行試験報告書（MoC 6）

試験結果を報告書としてまとめます。

(c): 無人航空機飛行規程（MoC 1）

申請者は、承認された関連システムの型式番号等又は最低限の仕様を運用限界として設定し、その運用限界を無人航空機型式認証データシート(TCDS)及び無人航空機飛行規程に含めます。

なお、無人航空機飛行規程はセクション 200 に従い作成します。

(d): ICA (MoC 1)

無人航空機の安全性に影響を与える関連システムの整備手順を ICA に反映します。

その他参考となる情報

関連システムとは、無人航空機を運用するために必要となる無人航空機本体とは別の周辺機器などを指します。具体的にはプロポ、コントロールステーション、地上施設などが該当します。

英語では Assosiated Element といいますが、FAA において関連システムは Type Certification ではなく、Operational Approval で認められます(当該システムが安全性を有するかどうかについては、Type Certification の審査においても確認されます)。一方で、日本において関連システムは型式認証の対象となります。

例えば、プロポの場合、スマートフォンにインストールされるアプリとしてサービスが提供される形態も存在します。そういった場合、アプリが適切に機能するための動作環境の指定は型式認証の対象となりますが、動作環境そのものは対象外となります。例えば、アプリが適切に機能するためのスマートフォンと OS を指定する必要はありますが、スマートフォン及び OS そのものは型式認証の対象外となります。

89

4　解説書

4.1　安全基準セクション 105(a)について

(1)　定義(関連システムのタイプ)

サーキュラーNo.8-001 のセクション 105(a)の冒頭に「*申請者は、無人航空機の安全性に影響を与え、又は無人航空機が安全基準を満たすために必要な無人航空機システムのすべての関連システム(AE)及びインターフェース条件を特定し、検査者に提出しなければならない。*」とある。ここで「又は」とあるが、特定の過程においてはいずれも検討を行うこととなるため、以下の 2 つのタイプの特定を試みることになる、と読み解くことができる。

1)　無人航空機の安全性に影響を与える関連システム

“安全性”とは、セクション 005 定義(以降、「セクション005」と呼ぶ)を基本として“制御不能”と”想定飛行範囲からの逸脱”を引き起こさないことと定義でき、本書ではこれらの有無に影響を与える可能性があるものを「無人航空機の安全性に影響を与える関連システム」と解釈する。

なお、「セクション 135 重要な部品(フライトエッセンシャルパーツ)(以降、「セクション135」と呼ぶ)」に関し、重要な部品(エッセンシャルパーツ)を安全性解析により抽出する方法がガイドラインに記載があり、対象については機体のみならず関連システムも含むことが補足されている。セクション 135 の対象となる関連システムとは、単一故障またはエラーにより計画外飛行または回復できない制御不能につながる部品であるものという理解に対し、セクション 105 の対象となる「無人航空機の安全性に影響を与える関連システム」は、大部分でエッセンシャルパーツと一致する可能性もあるが、そうではない関連システムが含まれる可能性や逆にエッセンシャルパーツであるが機体の安全性に影響は与えない関連システムが存在する可能性があり、セクション 105 における安全性に影響を与える関連システムについては別途検討が必要と推測する。

本紙では、一連の安全性に影響しうるシステムについては、セクション 135 の安全性解析で機体と関連システムを合わせた無人航空機システム全体に対する評価結果を活用し、セクション 105 の観点で安全性解析結果に対し追加の評価や選定を実施することが必要であると解釈する。

2)　無人航空機が安全基準を満たすために必要な関連システム

”安全基準”とは、「セクション 001 設計概念書(CONOPS)(以降、「セクション001」と呼ぶ)」から 320 の各基準のことであり、特にここでは「セクション 100 無人航空機に係る信号の監視と送信(以降、「セクション100」と呼ぶ)」で示す直接的な要求と、セクション 100 を介する間接的な要求を満たすために必要となる関連システムを「無人航空機が安全基準を満たすために必要な関連システム」と解釈する。

> *・100 無人航空機に係る信号の監視と送信*
> *無人航空機は、安全な飛行と運用の継続に必要なすべての情報を監視し、関連システム（AE）に送信するように設計しなければならない。その情報には少なくとも以下を含むこと*
> *（a）すべてのエネルギー貯蔵系統のすべてのクリティカルパラメータの状態*
> *（b）すべての推進系統のすべてのクリティカルパラメータの状態*
> *（c）飛行及び航法の情報（例えば、対気速度、針路、高度、位置等）*
> *（d）緊急時の情報や状態を含む通信及び航法信号の強度並びに品質*
> *［引用: 航空局ガイドライン］*

セクション 100 を介する間接的な要求とは、その他の設計の証明や飛行試験による証明に用いられるものと、セクション 105(b)(3)で示される“*セクション 100 で特定されたものを含むが、これに限定されない*”が意味する機体とのインターフェース以外で監視（表示）が必要な情報などが該当する。機体とのインターフェース以外の例として、天候情報、電波状況、位置情報などが相当する。

これらには安全基準の証明行為だけに供される治工具類、計測装置、テスター、シミュレータなどは含まない。

（2） 関連システムの識別

サーキュラーNo.8-001 のセクション 105(a)では、の「関連システム（AE）およびインターフェース条件を特定し、検査者に提出しなければならない。」とあるが、その具体的な対象の識別方法については申請者に委ねられていることが推測される。4.1(1)1)に記載の通り、本紙ではセクション 135 の安全性解析を活用し、追加で必要な関連システムの選定評価を実施することに問題はないと解釈する。

関連システムの識別について、場合分けして以下に補足をまとめた。

1） 「無人航空機の安全性に影響を与える関連システム」の識別

本基準の対象/非対象の識別には、安全性解析手法を用いた安全性評価が有効である：

- 他セクション（例：「セクション 110 ソフトウェア（以降「セクション110」と呼ぶ）」、「セクション 115 サイバーセキュリティ（以降、「セクション115」と呼ぶ）」、セクション 135 、「セクション 305 起こり得る故障など（以降、「セクション305」と呼ぶ）」）においても同様な識別方法が有効であると読み解くことができる。
- セクション 135 では網羅的な識別が必要になるため、FMEA 手法を参考にした分析検討により部品表レベルでの識別を行うと推測する。セクション 105 においてはその結果を基に対象の関連システムに関する証明文書などの詳細検討をすればよいものと解釈する。
- セクション 135 での分析はソフトウェアを含む部品も含めハードウェアについて行うが、ソフトウェア単体についてはセクション 110 において、C2 リンクや GNSS などの関連システムを利用する部品は本セクションにおいて確実に検討を行うことが必要になると考える。

2） 「無人航空機が安全基準を満たすために必要な関連システム」の識別

本基準は、安全性に影響は与えないが「セクション 300 耐久性と信頼性（以降、「セクション300」と呼ぶ）」の飛行試験などを実行する上で必要となる関連システムが対象となる。具体的には GNSS 衛星や C2 リンクのアンテナなどのように、運用には必要だが「無人航空機の安全性に影響を与える関連システム」とは区別されるものが該当するものと読み解くことができる。

（3） 識別された無人航空機の安全な運用に必要な関連システムの特定

無人航空機の安全な運用に必要な関連システムは、関連システムの特定または関連システムの最低限の仕様の何れかにより提示することが要求されている。

サーキュラーNo.8-001 のセクション 105（a）（1）では、申請者が提出する関連システムの情報に関し、対象を「特定」する方法と「最低限の仕様」を示す方法の２パターンの申請方法が記載されている。これは関連システムに関し、申請者に選択の自由度を付加するための対応と推測する。

「特定」とは、部品リストに含まれる関連システムを文字通り型式や型番、必要に応じメーカ名や販売経路など無人航空機の使用者が迷うことなく選択できる対象品の情報を提供することを意味する。

一方「最低限の仕様」とは、部品リストに含まれる関連システムにはいくつかの選択肢が準備されており、使用者が型式認証で証明された範囲内の関連システムを調達し運用に用いることができるだけの必要十分条件の情報を提供することを意味する。この時証明された範囲を使用者が誤って解釈することがないようわかりやすく情報提供することが求められているものと解釈する。

「特定」の場合は、証明された関連システムを限定するため、証明活動は最低限の仕様の場合に比べシンプルで検査も容易となることが推測される。「最低限の仕様」の場合は、そもそも最低限の仕様が要求を満たすに十分条件であるかの判断が必要で、サーキュラーNo.8-001 でも最低限の仕様を使用する場合の追加要件があることから、証明活動が複雑になることが考えられる。

関連システムの特定方法について、場合分けして以下に解釈をまとめる。

1） 関連システムの特定

- 本条件で提示する場合、飛行試験に供する関連システムは特定された関連システムの型式や型番を使用し、飛行規程にもその特定するための情報を明記する
- 特定された関連システムの型式、型番の情報は、証明に用いられたものと同じ関連システムが確実に調達（購入）できるレベルである必要があると解釈する
- 飛行試験に供される関連システムが提示された特定の条件に一致するか否かはセクション 300 の飛行試験内で確認されるものと推測する

2） 関連システムの最低限の仕様

- 提示された最低限の仕様の場合も、その仕様に基づき、証明に用いられたものと同等以上の関連システムが確実に調達（購入）できるレベルで指示することが必要である。

- 最低限の仕様の場合、セクション105(b)(4)の“*正しく、完全で、一貫性があり、検証可能であること*”への対応が必要とされている。 証明活動に供される関連システムが、性能、互換性、機能、信頼性、機体と関連システム間のインターフェース、パイロットアラート、環境要件などの観点で指示された最低限の仕様と同等以上であることを示し、且つ飛行試験でそれを証明することが必要と読み解くことはできるが、その方法は申請者に任されているものと解釈される。
- 詳細な最低限の仕様が提示されれば、その仕様に基づき製造を発注し調達することは可能であるが、運用承認(operational approval)がない日本においては製造の均一性や証明を受ける無人航空機と組み合わせた機能、性能、特性を確認できる枠組みがないため、実現が難しいことが推測される。
- 関連システムに搭載されるソフトウェアの開発と更新時の対応については、本セクションだけでなくセクション 110 の基準にも当てはめて別途検討する必要があると考える。

4.2 安全基準セクション 105(b)について

(1) 関連システムの証明(b)(1)(2)

特定された関連システムまたはその最低限の仕様については、以下が要求されている。

- 無人航空機の安全性を保証する機能、性能、信頼性および情報の提供
  これらは、無人航空機システムの他の要素と組み合わせた使用において、これらの内容が機体の申請機能を満足するために問題なく提供できることが求められていることと解釈する。判定については、設計資料や社内試験の結果を用いて証明し、適合性証明飛行試験により確認するものと読み解くことができる。
- 無人航空機の能力および機体と関連システム間のインターフェースと互換性
  設計資料や社内試験の結果を用いて証明し、適合性証明飛行試験により確認する必要があると解釈する。

また関連システムの証明は、以下の他のセクションの内容と合わせて証明することで、無人航空機の安全性を保証するための機能、性能、信頼性および情報が提供されることを示すことが可能であると推測する。

1) セクション 300 飛行試験法案(MoC6)

- 航空局ガイドライン セクション 105(a)で特定された関連システムまたは関連システムの最低限の仕様に一致する代表部品を、無人航空機の信頼性を検証するセクション 300 の飛行試験に用い、飛行試験の合否をもって関連システム自体の提供する情報が信頼性と安全性を保証するに適切かを検証するものと考える。
- 試験法案では、最低限の仕様で指示される関連システムについては、申請者と検査者は、試験に供される実際の関連システムが申請者の提示する最低限の条件と整合するかを確認しなけ

ればならないものと推測する。

- 飛行試験報告書には、機体の試験結果と評価以外に関連システムの検証結果についてもまとめるものと考える。

2） セクション 310 能力および機能 飛行試験法案（MoC6）

- 航空局ガイドライン セクション 105(a)で特定された関連システムまたは関連システムの最低限の仕様に一致する代表部品を、無人航空機の性能および機能を検証する「セクション 310 能力及び機能（以降、「セクション310」と呼ぶ）」の飛行試験に用い、飛行試験の合否をもって関連システム自体の提供する情報が信頼性と安全性を保証するに適切かを検証するものと考える。
- 310 の飛行試験法案では、申請者と検査者は、機体の機能・性能のみならず関連システムが申請者の提示する無人航空機の能力および機体と関連システム間のインターフェースと互換性があることを実証するものと読み解く。
- 飛行試験報告書には、機体に関する機能・性能試験結果とその評価以外に関連システムとの互換性に関する検証結果もまとめるものと考える。

（2） セクション 100 の証明に係る関連システムとその証明(b)(3)

航空局ガイドライン セクション 105(b)(3)では、セクション 100 で特定されたものとそれ以外で、安全な飛行と運用に必要なすべての情報を監視し、操縦者に送信することが求められている。先ず、安全な飛行と運用に必要な情報を、設計と運用の観点からすべて特定することが必要であり、それらの情報が操縦者に適切に提供されていることを、適合性証明飛行試験により確認する必要あるものと推測する。 適合性証明飛行試験法案についての補足を以下にまとめた。

なお、航空局ガイドライン セクション 105(b)(3)の本文では、“*関連システム(AE)は、安全な飛行と運用に必要なすべての情報(セクション 100 で特定されたものを含むが、これに限定されない。)を監視し、無人航空機を飛行させる者に送信する必要がある。*” とあるが、特に「これに限定されない」の解釈について補足すると、セクション 100 は機体から関連システムに送信する情報については言及しているが、機体からではなくその他の情報元から直接関連システムに送信される情報については記載がない。ここでは、機体以外から直接関連システムに送信される情報で監視が必要なものを対象として証明活動をするものと推測する。

1） セクション 100 飛行試験法案（MoC6）

この試験法案では、セクション 100 で示す直接的な要求と、セクション 100 を介する間接的な要求についての証明をセクション 100 飛行試験案に基づき検証するものと解釈する。

- 航空局ガイドライン セクション 105 (a)で特定された関連システムまたは関連システムの最低限の仕様に一致する代表部品を、無人航空機に係る信号の監視と送信を証明するセクション 100 の飛行試験に用い、飛行試験の合否をもって関連システム自体の 100 に対する必要機

能を保証するに適切かを検証するものと推測する。

- ガイドラインには、本項に関し“*運用エンベロープ及び運用制限内で各関連システムのクリティカルな運用環境を考慮して、飛行試験方案を作成する必要があります。*”とある。これは監視と送信の実行条件が最も厳しい環境であってもその対策も含めて機体と関連システムを含む無人航空機システムが対応可能であることを確認する必要を示していると解釈する。例えば、機体の安全な飛行と運用を維持するために必要な情報送信の目的として、仮にセクション 305 の起こりうる故障の状況下（C2 リンク喪失時や GNSS 喪失時など）など特殊な環境下であったとしても監視と表示の機能により安全な飛行が阻害されるような影響があってはならないものと考える。言い換えると、監視と表示の機能不具合によりセクション 305 の試験法案を満足できないような場合は、その他の安全基準を満たせないだけではなく、安全性に影響を与えるシステムとして問題ありと判断される可能性があるという意味である。
- 飛行試験報告書には、機体に係る信号の監視と送信に対する試験結果とその評価以外に関連システム側の応答（表示）性能・機能についても実証結果をまとめるものと考える。

2） セクション 105 飛行試験法案（MoC6） オプション

- 航空局ガイドライン セクション 105（b）（3）の記載にある“*セクション 100 に限定されない*”の通り、セクション 105 飛行試験法案とすることも可。例えば、機体とのインターフェース以外で無人航空機の安全な飛行と運用に必要な情報があれば、セクション 100 またはセクション 105 試験法案にてそれらの情報が関連システムで操縦者が確認できることを実証する。機体とのインターフェース以外に関する詳細は 4.1（1）2）を参照。
- 105 飛行試験法案として 100 飛行試験法案と区別する場合でも、“*運用エンベロープ及び運用制限内で各関連システムのクリティカルな運用環境を考慮して、飛行試験方案を作成する必要があります。*”に対応する試験案を作成する。詳細は 1）を参照。
- 105 飛行試験報告書には、100 試験報告書が別途ある場合は関連システムに関する監視と受信、表示などの機能・性能確認結果をまとめるものと考える。

（3） 最低限の仕様の場合は、安全性を保証するために、正しく、完全で、一貫性があり、検証可能であることを示す（b）（4）

最低限の仕様で提示される場合、その仕様が、正確であり、抜けがなく、（仕様間などに）矛盾がなく、かつ、そのことが検証できるものでなければならないものと考える。具体的には、その仕様が、適合性証明飛行試験に用いる関連システムと同等以上であることを示し、かつ、その関連システムを用いて飛行試験を実施する必要があると解釈する。

1) セクション 105 関連システム設計図面(MoC1)

航空局ガイドラインには“*当該設計図面(MoC1)には、上記基準(a)及び(b)(4)を満足する関連システムとインターフェース条件を示します。満足すべき上記基準(a)及び(b)(4)の詳細は以下(下記表)のとおりです。*”とある。

基準	*関連システム*	*インターフェース条件*
(a)	● *関連システムを特定することができる型式番号等で示すこと。または、関連システムを特定することができる最低限の仕様で示すこと。* ● *最低限の仕様で示す場合、性能、互換性、機能、信頼性、インターフェース、パイロットアラート、環境要件等の重要な項目を含むこと。(重要な項目とは、それが満足できない場合に、無人航空機の安全と効率的に運用する能力に影響を与えるものを指します。)*	● *無人航空機の安全な運用に影響を与えるインターフェース条件を示すに当たって、インターフェース管理図面、インターフェース要求文書又はその他参考資料を使用すること。*
(b)(4)	● *最低限の仕様が特定されている場合、それらは無人航空機の安全性を保証するために、正しく、完全で、一貫性があり、検証可能であることを示すこと。*	*N/A*

[引用: 航空局ガイドライン]

- 4.1(3)2)に記載の通り、最低限の仕様で関連システムを指示する場合、その情報が正しく、完全で、一貫性があり、検証可能であることを示さなければならない。最低限の仕様については、設計図書や機体と関連システム間のインターフェース管理図面、インターフェース要求文書またはその他の参考資料に記載するとガイドラインにある。
- MoC1 とあるが、提供された最低限の仕様の情報が航空局ガイドライン セクション 105 (b)(4)の証明方法として困難な場合は、例えば最低限の仕様の代表部品と同等以上の別の部品を用いて飛行試験でその情報の検証を実施する代替案も考えられる。必ずしもガイドラインに示された証明手法に則る必要はなく、申請者が自由に計画することは可能である。
- 申請者と検査官によって、試験に供される実際の部品が最低限の仕様に対し、条件が合致しているか、またはより厳しい条件となっているかは、実施する飛行試験の中で確認される。

2） 飛行試験法案(MoC6） オプション

- 4.1(3)2)に記載の通り、最低限の仕様で関連システムを指示する場合、その情報が正しく、完全で、一貫性があり、検証可能であることを示す必要がある。もしMoC1での説明や証明が困難な可能性がある場合は 4.1(3)2)のとおり飛行試験(MoC6)とその合否を通して確認することも可能である。
- (b)(4)の証明は、飛行試験にて実証する場合、セクション 100 、セクション 300、セクション 305、セクション 310 の試験などの一環として証明する方法が考えられる。最低限の仕様のリスクを考慮するのであれば、最も厳しい試験条件を要するセクション 305 の飛行試験法案にて航空局ガイドライン セクション105 (b)(4)も併せて検証できるとよいかもしれない。

4.3 安全基準セクション105(c)について

(1) 無人航空機飛行規程(MoC 1)

申請者は、承認された関連システムの型式番号などまたは最低限の仕様を運用限界として設定し、その運用限界を無人航空機型式認証データシート(TCDS)および無人航空機飛行規程に含めなければならない。この時、無人航空機飛行規程は「セクション 200(無人航空機飛行規程)(以降、「セクション200」と呼ぶ)」に従い作成する。 参考までにセクション200の要求について補足すると、MoC1では申請者が飛行規程を案として定義しなければならず、証明後は航空局が全体を見て内容を精査したうえで最終化したものを定義するという流れになるものと解釈する。

> *・200 無人航空機飛行規程*
> *申請者は、無人航空機飛行規程を無人航空機一機毎に提供しなければならない。*
> *(a) 無人航空機飛行規程には、以下の情報を含むこと。*
> *(1) 無人航空機運用限界*
> *(2) 無人航空機の運用手順*
> *(3) 性能情報*
> *(4) 搭載情報*
> *(5) 設計、運用又は取扱いによる安全な運用に必要なその他の情報*
> *(b) 無人航空機飛行規程の上記(a)項(1)に関する箇所については、航空局の承認を受ける必要がある。*
>
> *[引用: 航空局ガイドライン]*

1） 承認された関連システムの型式番号などまたは最低限の仕様が運用限界

セクション 105(b)(1)(2)(3)(4)を飛行試験などにて証明した後、これらの関連システムは承認されたものとして、申請者はこれらの飛行試験に供した“関連システムと機体の組み合わせ”の無人航空

機システムの形態を飛行規程に明記し、運用限界を定義するものと推測する。

飛行規程に示す運用限界とは、実際に飛行試験で証明した形態（関連システムの特定または最低限の仕様）の能力を超えた状態を許可してはならないことを意味し、型式認証後に機体が想定外の運用で安全性に影響する飛行や使われ方がないよう飛行規程で仕様と利用範囲を明確にするものと解釈する。同様に TCDS にも記載する必要があると考える。

2） セクション 200 無人航空機飛行規程（MoC 1）（ご参考）

セクション 200 のガイドラインでは、参考資料（ASTM F2908-18）が引用されており、当該資料には飛行規程の構成や記載内容に関する仕様が標準化されている。航空局ガイドラインの参考資料のセクション番号は元の参考資料の更新により最新のものと異なる場合があるため留意が必要と推測する。

適合性証明は、セクション 200 の無人航空機飛行規程を参照し 105（c）の証明とするのがよいと考える。

注記：第二種の申請機体において、飛行規程は一般的に機体マニュアル（家電などの取扱い説明書）と同じような内容となる可能性がある。承認された関連システムと使用する機体の組み合わせが、証明範囲を逸脱しないよう使用者（操縦者や運航者）が理解しやすいよう記載することが必要である。

4.4 安全基準セクション 105（d）について

（1） 関連システムの整備手順（MoC 1）

申請者は、無人航空機の安全性に対する関連システムの影響（制御不能または想定飛行範囲からの逸脱に至る状態）に対処するために必要な整備手順を作成し、「セクション 205 ICA（以降、「セクション205」と呼ぶ）として要求される整備手順書（ICA）に含めなければならない。

また、セクション 135（b）には“*申請者はフライトエッセ ンシャルパーツの不具合を防ぐために必須となる整備手順若しくは制限寿命 またはその両方を設定し、定義しなければならない。*”とあり、そちらの要求とも併せて関連システムの整備手順は検討がされるものと解釈する。 ただし、エッセンシャルパーツとしての関連システムが、セクション 105（d）で求められている関連システムのすべてと合致するわけではないため、ここではセクション 135 の対象関連システムとその整備手順以外で必要な対象システムやその整備用件を検討し、整備手順に記載するものと解釈する。

1） 整備が必要な関連システム

申請者は、整備の必要性を以下の観点を含み検討するものと考える。セクション 135 の対象とその整備要件に追加で検討する場合も考慮し以下としている。

- フライトエッセンシャルパーツかどうか
- 機体の安全性に影響を与える関連システムかどうか
- その他の安全基準に影響を与える関連システムかどうか

上記に当該する関連システムが、時系的に変化する特性や機能を有する場合、それらの関連システムについて整備手順書を準備する必要があるものと解釈する。以下に整備手順が必要と推測される例をいくつか示すが、これに限定するものではない。

- 機械部品であれば劣化、疲労、摩耗するもの
- ソフトウェアであればバージョンアップが必要または OS など間接機能で実施されるもの
- コネクタなどの電気的接続の規格で規格が最新化されるもの、また最新化に伴い使用者によって簡単に接続方法などが交換・変更できるものなど

ICA に含める内容は、セクション 105(a)、セクション 105(b)への影響も考慮する必要があり、また必要な整備があればセクション 105(c)の無人航空機飛行規程にも明記することが必要であるものと考える。対象の関連システムがエッセンシャルパーツの場合は、セクション 135 と連携し参照することも可能であると解釈する。

2) セクション 205 ICA (MoC 1)（ご参考）

セクション 205 のガイドラインには、セクション 135 やセクション 115 などで要求される事項を記載とある。安全性に影響あり整備を必要とする関連システムは、セクション 135 として識別されるべき部品やソフトウェアであるため直接セクション 105 の記載はないが、ICA の対象であることはセクション 105(d)の通りであると読み解くことができる。

なお有人航空機における整備資格の有資格者制度とは異なり、無人航空機には有資格者という概念がないため、整備手順と言いつつもいわゆる点検程度の内容にすることとガイドラインには記載がある。ただし安全上必要な整備で特殊な治工具や技能を要する場合は、申請者が整備を行うために必要な訓練などを設定し、その訓練を受講し合格した者による整備を許容するなどを明記しなければならないものと推測する。

適合性証明は、セクション 205 を参照しセクション 105(d)の証明とするのがよい。

> *・205 ICA*
> *申請者は、検査者が受入れ可能な ICA を作成しなければならない。ここで言う ICA とは、使用者が無人航空機並びに装備品、部品及び落下傘等並びに関連システム(AE)に対して、適切に点検及び整備を行うための手順書であり、当該手順書の作成にあたり、耐空性審査要領第Ⅱ部 附録 A(耐空性を継続するための指示書)が参考となる。*
>
> *［引用: 航空局ガイドライン］*

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定) 項目は以下の通り。

5.1 安全性に影響を与える関連システムとその他の安全基準を満たすために必要な関連システムの違いと考え方、識別方法の明確化について

報告書本文 4.1(2)に関し、セクション 135 やセクション 110 などとは異なり、セクション 105 特有の証明が必要な関連システムの識別方法論について詳細が未議論。

5.2 関連システムの認証が必要な範囲とその管理要求について

報告書本文 3 章 「航空局ガイドライン」(引用)内におけるその他参考となる情報の“一方で、日本において関連システムは型式認証の対象となります。” の意味とその達成と維持に必要な管理に関する議論の深堀が未対応。特に下記の観点での解釈については重要課題との認識。

- 関連システムの形態管理
- 関連システムの品質管理

5.3 関連システムの特定または最低限の仕様の考え方について

報告書本文 4.1(3)に関し、特に最低限の仕様については対象の関連システムによって必要十分な条件やその示し方、詳細度が変わると推測するが、その導出方法や考え方などについては十分なディスカッションができていないため未対応。何をもって最低限とするかなどの確認方法や提供された情報の Validation 要否、証明方法などについては重要課題との認識。

5.4 関連システムの最低限の仕様が、「正しく、完全で、一貫性があり、検証可能である」について、それぞれの用語が意味することが誰でもわかるような補足説明の検討について

報告書本文 4.1(3)2)の「セクション 105(b)(4)の“*正しく、完全で、一貫性があり、検証可能であること*”への対応」について、各語彙の意味とセクション 105(b)(4)が求めることについての読み解き。

- 「正しく」の意味
- 「完全である」の意味
- 「一貫性がある」の意味
- 「検証可能である」の意味

以下は 5.4 に関する Appenndix 案であるが議論未対応のため参考のみの掲載とする。

日本語訳	英語標準用語	定義	参照元
正しく	Correctness	The degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
完全で	Completeness	Completeness is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c)
一貫性があり	Consistency	Consistency between requirements statements means the attributes are in agreement within the scope of the intended purposes. A design specification is consistent with the requirements if neither contradicts the other. A power budget summary is consistent with a design specification if a quantity in the budget that refers to the design specification is equal to the quantity implied by the design specification.	ED-202A/DO-326A
検証可能である	Verifiable	The requirements and specifications which are implementable, verification conductable and provable by verification to ascertain that each level of the implementation meets its specified requirements. The verification process ensures that the system implementation satisfies the validated requirements. Verification consists of inspections, reviews, analyses, tests, and service experience applied in accordance with a verification plan.	ED-79A / ARP4754A No definition, paragraph extract Section 5.4.2(c) and refering to Sectioin 5.5

源泉文書 抜粋	Reference	Correctness is the degree to which an individual requirement is unambiguous, verifiable, consistent with other requirements and necessary for the requirement set. Completeness is the degree to which a set of correct requirements, when met by a system, satisfy the interests of customers, users, maintainers, certification authorities as well as aircraft, system and item developers under all modes of operation and lifecycle phases for the defined operating environment. (Additional information on these checks is provided in 5.4.3 and 5.4.4).	Section 5.4.2(c)

図 5.4-1 「正しく、完全で、一貫性があり、検証可能である」に対する各用語の意味

具体例を含む解説補助情報：

<u>最低限の仕様が「正しい」の意味</u>

最低限の仕様が「正しい」とは、使用者が使える AE を決定するうえで、情報が“最低限”であり、提供情報が“正確である”ことを意味する。「最低限の仕様」情報が人によって解釈の幅があってはならないという意味である。

例えば、PC の Windows OS には、Windows 7 や 10 のようなバージョンがあるが、最低限の仕様が、“Windows 10” か “Windows 10 以上” かでは情報の正確性が異なる。“Windows 10” と記載したとき、申請者の意図は Windows 10 のみ検証済で使用可能ということかもしれない。一方で、読み手に最低限なのでそれ以上なら可と判断してしまうかもしれない。正確に伝えるには “Windows 10 のみ” などが適切かもしれない。他に精度に関連する記載情報として留意が必要なものに、表示桁数、公差の示し方、望小・望大・望目特性ごとの要求表記の仕方、官能で判定するものなどが考えられる。

<u>最低限の仕様が「完全である」の意味</u>

最低限の仕様が「完全である」とは、正しいかの観点と似ているが追加で補足するのであれば、提供された情報だけで申請機種に対し検査者や利用者が都合よくまたは悪く内容を解釈し、想定範囲外で AE を選択したり適用したりすることがないようにするための観点である。

例えば、PC の Windows OS には、Windows 7 や 10 のようなバージョン以外に、詳細レベルで

Home, Pro, Enterprise など々に加え、1507, 1607, 1809, 21H2, 22H2 などがある。細かいバージョンごとにサービス内容が異なる場合があるため、本来使用者が使用すべき OS が、Windows 10 だけ指示した場合では真に必要な最低限を満たさないリスクが生じる。申請者は、最低限の情報が正確で、必要十分であることを保証しなければならない。

最低限の仕様が「一貫性がある」の意味

最低限の仕様が「一貫性がある」とは、その他の仕様と相互作用がある場合などで特に注意が必要で、対象 AE を指示する内容が、その記載内容内外と矛盾が発生してはならないという意味である。ただし最低限の仕様はその特性から使用者に判断を委ねている自由度が、特定することに比べて高い分、矛盾リスクを完全に除外することが難しい。そのような場合やすべての矛盾を確認することが困難な場合は、矛盾した場合を想定し、どの情報を最優先すべきかを明記しておく方法もある。

極端な例でいえば、機体のマニュアルには雨天利用禁止とあるが、プロポの利用環境条件には、雨天使用可（防水仕様）とあった場合、当然ながら機体の要求が優先される。ただ機体が雨天利用禁止だからとプロポが防水仕様であってはならない理由はない。

その他、例えば GSC の最低限の仕様の一部が、OS は Windows 10 Enterprise 1809 以上であるのに対し、必ず使用する操作用ソフトウェアが OS は Windows 10 Home 22H2 以上、サイバーセキュリティ対策用のウィルス対策ソフトが OS は Windows 7 Pro 以上のような記載の場合、一貫性は確保できていなかったり不明瞭だったりする。申請者は利用者が必要なシステム全体を見据えて適切に最低限の仕様を指示する必要がある。

最低限の仕様が「検証可能である」の意味

最低限の仕様が「検証可能である」とは、下記二点を示すことを要求している。

- 飛行試験で使用する AE の最低限の仕様が“最低限”でありその指示が明確であること
- 最低限の仕様の代表システムにて“試験が成立し証明計画どおり検査可能”であること

具体的な落とし込み先としては、航空局ガイドラインにも記載あるとおり、MoC1 の 1 つとして(b)(4)に対し、『セクション 100 飛行試験方案に含めるか、またはセクション 105 飛行試験方案として別に設定するかは自由度があります。なお、運用エンベロープおよび運用制限内で各関連システムのクリティカルな運用環境を考慮して、飛行試験方案を作成する必要があります。』とあり、このことからも作業性や証明計画を効率的に遂行するため 105 飛行試験法案が必要と判断する場合は 100 と分けて試験法案を作成することも可能である。（※ (b)(4)のガイドラインでは試験法案含めて MoC1 といっている可能性あり）

Appendix 1　証明手順例など

DRAFT2 にて加筆検討中

Appendix 2 各セクション特有の用語集

DRAFT2 にて加筆検討中

Appendix 3 関連文書

DRAFT2 にて加筆検討中

Appendix 4　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 105 無人航空機の安全な運用に必要な関連システムの構成員名簿（サブ WG 主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD、Rev.01）Appendix3 を参照すること。

タイトル	氏名	所属
主査、ライター	山崎 まりか	株式会社電通総研（旧株式会社電通国際情報サービス）
ライター	中舘 正顯	一般財団法人日本海事協会
ライター	樋野 尊	株式会社電通総研（旧株式会社電通国際情報サービス）
ライター	二上 貴夫	株式会社 東陽テクニカ

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

477

RMD-110 DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 110 ソフトウェア　解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

表 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」という）安全基準セクション 110 ソフトウェアに対する解説書である。

2　対象の基準「サーキュラー」（引用）

サーキュラーNo.8-001“無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領“（以降、「サーキュラーNo.8-001」と呼ぶ）の「110 ソフトウェア」を以下に引用する。

> *・110 ソフトウェア*
>
> *残存するソフトウェアエラーを最小化するために、申請者は以下を行わなければならない。*
>
> *（a） 無人航空機の安全な運用に影響を与えるすべてのソフトウェアに対して試験による検証*
>
> *（b） ソフトウェアの全ライフサイクルを通した変更に対する追跡、管理及び保存を行うための形態管理システムの使用*
>
> *（c） ソフトウェアの修正及び欠陥を捕捉し記録するための PR（Problem Report）システムの導入及び活用*

3　「航空局ガイドライン」（引用）

「航空局ガイドライン」 安全基準 「110 ソフトウェア」の「基準の概要」、「適合性証明方法（MoC）」、「その他参考となる情報」を以下に引用する。

> *・110 ソフトウェア*
>
> *<u>基準の概要</u>*
>
> *本基準は、ソフトウェアエラーの残存を最小化するために必要となる活動を要求するものです。セクション 110 では、まずソフトウェアに対し試験（テスト）で要求が適切に実装されていることの確認を行います。なお、本テストはシステムレベルの要求に対して行います。続いてバージョン（Ver.）が刻々と変化する可能性の高いソフトウェアに対し、形態管理は重要であるため、どのようなソフトウェアが各型式に搭載されているのか（追跡）、適切なソフトウェアなのか（管理及び保存）について、ライフサイクルを通して維持・管理できることが要求されます。最後にソフトウェアのエラーを把握し記録、必要に応じた修正を行うための PR システムが必要となります。*
>
> *なお、有人航空機においてはソフトウェアに対し開発保証として多くの場合 RTCA DO-178 に基づいた活動が要求されます。適合性証明方法として DO-178（DAL D）を用いることもできます。*
>
> *<u>適合性証明方法（MoC）：1、2</u>*
>
> *（a），（b），（c）: セクション 110 ソフトウェア適合性証明計画/完了報告書（MoC 1, 2）*

セクション 110 への適合性を証明するための計画をまとめたセクション 110 ソフトウェア適合性証明計画を作成します。計画は、最終的には計画どおりに完了したことを記す完了報告書となります(計画と完了報告書の 2 文書が必要)。

無人航空機ソフトウェア適合性証明計画書には以下を記載します:

まず(a)項に対し、「安全な運用に影響を与えるソフトウェア」とは何か、無人航空機に使用される全ソフトウェアから抽出する必要があります。抽出の方法は、セクション 135 を準用してソフトウェアが誤った挙動をした場合の影響の程度を評価する方法、FHA (Functional Hazard Analysis)、SSA(System Safety Assessment)、FMEA(Failure Mode and Effect Analysis)等の安全性解析手法を用いるなど、いくつかあります。また、対象となるソフトウェアの抽出はせず、無人航空機に使用されるすべてのソフトウェアに対し試験を行う方法もあります。

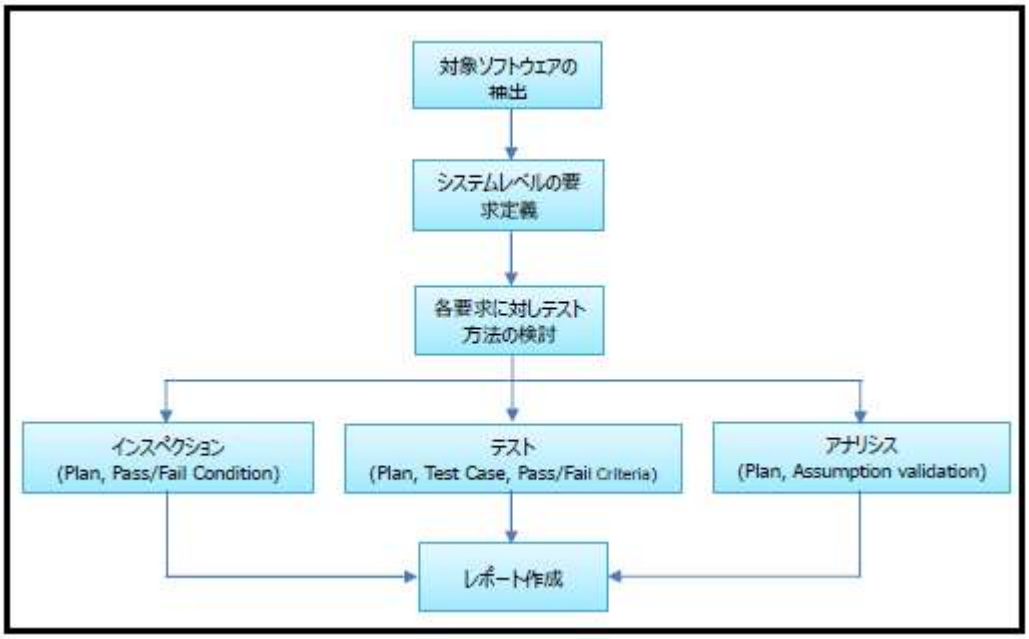
続いて、「安全な運用に影響を与えるソフトウェア」は「システムレベルのテスト」によりその動作を確認する必要があります。そのため、「システムレベルの要求」を定義する必要があります。システムは日本語では系統と訳せますが、無人航空機は様々なシステムから構成されています。例えば自機位置を把握する GNSS システム、飛行制御を行うフライトコントロールシステムなどがあります。システムレベルの要求は、それぞれのシステムが満たすべき一つひとつの要求です。例えば GNSS システムであれば位置情報を正しく出力することがひとつの要求となります。なお、ソフトウェアのテストには、ホワイトボックステスト、ブラックボックステスト、単体テスト、統合テスト、これ以外の分類も含め多種多様に存在しますが、要求ベースのテストとは、システムレベルの要求が正しくソフトウェアに実装されていることを確認するテストとなります。そのため、一般的にはブラックボックステストが該当し、試験装置によるテスト(ベンチテスト)及び機体レベルで行う地上試験が主体となります。このほか、セクション 300 で行う飛行試験及びベンチテスト、地上試験との組合せで確認できる要求もあります。

すべての要求は、基本テストにより確認される必要がある一方、テストでの確認が困難な要求に関しては解析(アナリシス)や検査(インスペクション)といった方法も許容されます。例えば、非機能要求(許容できるメモリ量、CPU 負荷など)は解析(アナリシス)により確認される要求となります。検査(インスペクション)は一般的に目視、聴覚や触覚などの感覚によって行う非破壊の評価となり、物理的な測定や操作などが該当します。

なお、要求からテストケース及び手順へはトレーサビリティを確保する必要があります。

システムレベルのテストについて、ASTM F3153-15 "Standard Specification for Verification of Avionics Systems"を参考にすることができます。

以上の活動を図示すると以下のようになります:



上記活動をもとに無人航空機ソフトウェア適合性証明計画書/完了報告書には以下を記載します(証明活動の結果は完了報告書のみに記載):

- *無人航空機のシステム概要(他の文書を引用可)*
- *ソフトウェア一覧(搭載、非搭載別)*
- *安全な運用に悪影響を与えるソフトウェアをどのように抽出するかの説明及びその結果*
- *システムレベル要求ベーステストをどのように実施するかの説明(計画)*
- *システムレベル要求ベーステストの結果概要*

また、完了報告書を補完する文書として以下が必要となります。

- *システムレベルの要求一覧*
- *システムレベル要求ベーステスト関連書類及び試験結果*

続いて(b)項に対し、ソフトウェアのライフサイクルを通した変更に対する追跡、管理及び保存を行うための形態管理システムが適用されることを提示します。

なお、対象となるソフトウェアは(a)項の対象と同じく安全な運用に影響を与えるソフトウェアです。

本項を満たすためには、形態管理がどのように行われるのか概要を説明するとともに、以下のアイテムについて形態管理されることの説明が必要になります。

i. 要求(Requirements)

ii.システム及びソフトウェアテスト環境の説明

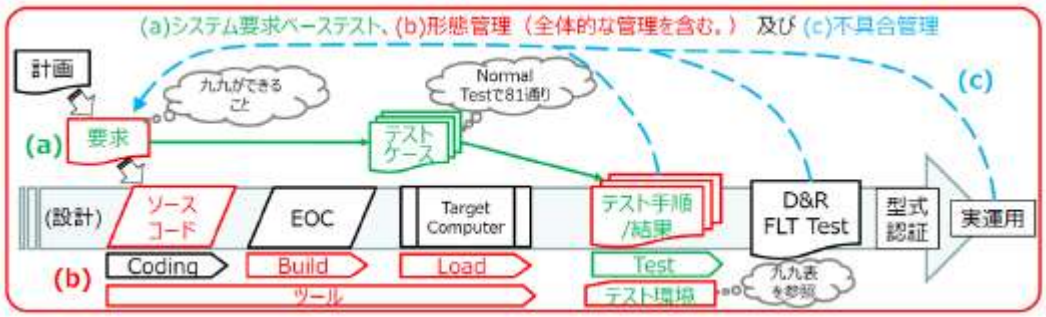
(System and software test environment descriptions)

iii.要求からテストケース及び手順へのトレーサビリティを含むテスト手順及び結果
(Test procedures, and results with requirements traceability to test cases and procedures)
iv.ソースコード及び開発環境/ツール
(Source code and development environment/tools)
v. 実行オブジェクトコードの複製のためのビルド/ロード手順
(Build and load procedures for replication of the executable object code)
形態管理は、ベースラインとして形態管理のスタート地点を定める必要がありますが、遅くとも(a)項のテストの開始前にはスタートする必要があります。

最後に(c)項に対し、ソフトウェアの修正及び欠陥を捕捉し記録するための PR(Problem Report)システムが適用されることを提示します。
なお、対象となるソフトウェアは(a)項の対象と同じく安全な運用に影響を与えるソフトウェアです。
本項を満たすためには、不具合管理がどのように行われるのかの説明が必要となります。

自己宣言について
「サーキュラー」の表 1 で求める自己宣言について以下に記します。
自己宣言とは、一部の認証区分において、航空局又は登録検査機関によるセクション 110 ソフトウェアに対する適合性の検査は受けないものの、申請者自身がセクション 110(a)、(b)及び(c)の各要件に対して適合していることを確認した上で、適合している旨を記載した宣言書を型式認証申請後に提出することが必要です。

その他参考となる情報
以下は(a)、(b)及び(c)項についての参考図です。
緑色が(a)項、赤色が(b)項、青色が(c)項に関するものとなります。



産業規格

- *RTCA DO-178C, Software Considerations in Airborne Systems and*

Equipment Certification

-
- *ASTM F3153-15, Standard Specification for Verification of Avionics Systems*

4　解説書

4.1 セクション 110 ソフトウェアの対象と範囲

> *(a) 無人航空機の安全な運用に影響を与えるすべてのソフトウェアに対して試験による検証*
> *[引用:サーキュラー No.8-001]*

サーキュラー No.8-001 によると、特にセクション 110(a)の範囲として、「*無人航空機の安全な運用に影響を与えるすべてのソフトウェアに対して*」、とある通り、セクション 110 ソフトウェア（以降「セクション 110」と呼ぶ）の活動対象は、無人航空機の安全な運用に影響を与える機体およびすべての関連システムなど含まれるソフトウェアに対して活動を行う。（フライトに関するソフトウェアにおいても、機体に搭載される場合や、機体に搭載されるかわりにクラウドなどに置かれ、そのクラウドに置かれたソフトウェアが運用の際に使用される場合もある。）

一方で、セクション 110 の対象には、FPGA や ASIC などのプログラマブルロジックデバイスは含まれないと考える。この根拠としては、FPGA や ASIC などのプログラマブルロジックデバイスはソフトェアよりはハードウェアの範疇であり、パーツ単位で管理されるものであると考えられるからである。

本解説書では、すべての第二種の無人航空機システムを対象としている。

4.2 セクション 110 ソフトウェアの活動

(1)　基準に対する活動要求とその理由

> *本基準は、ソフトウェアエラーの残存を最小化するために必要となる活動を要求するものです。”*
> *[引用: サーキュラー No.8-001]*

セクション 110 で行うべき認証としての活動はソフトウェアの品質を確保するために行われなければいけないソフトウェア開発プロセスの構築である。つまり、ソフトウェアの品質の確保を行うための「プロセス」を構築することがセクション 110 で認証される活動である。

無人航空機にとってソフトウェアは、電子的なプログラムで動く無人航空機にとって非常に重要な部位である。システム全体からの要求を充足する品質を持つソフトウェアを構築し、かつ適正にそれらが構成されていることを証明するものである。これらの要求や、品質の充足を管理するには、他のセク

ションから来る要求や他のセクションへの活動の委譲を理解して、型式認証全体の一活動であるとして対処されるべきである。一方で、機上のソフトウェアも、関連システムなどの機体外のソフトウェアも、完全なソフトウェアを目指して構築されるが、システム実装上の不具合が生じることが常である。このため、品質の充足のためには、システムズエンジニアリングに基づく開発プロセスの組織化が必要である。図 3.2 では、V&V と呼ばれるソフトウェア開発プロセスの中で、セクション 110 の認証活動の範囲を示している。セクション 110 で要求される 3 つの活動は以下のとおりである。

(a) システム要求ベーステスト

（a）無人航空機の安全な運用に影響を与えるすべてのソフトウェアに対して試験による検証

［引用:サーキュラー No.8-001］

(b) 形態管理

（b）ソフトウェアの全ライフサイクルを通した変更に対する追跡、管理及び保存を行うための形態管理システムの使用

［引用:サーキュラー No.8-001］

(c) 不具合管理

（c）ソフトウェアの修正及び欠陥を捕捉し記録するための PR(Problem Report）システムの導入及び活用

［引用:サーキュラー No.8-001］

（2） 他セクションとの関係性

セクション 110 は、ソフトウェア開発におけるプロセスと管理手法に対する「プロセス認証」が主である。一方で、実際のソフトウェア開発では、航空局ガイドライン セクション 110 その他参考となる情報における参考図で示される通り、計画を策定し、要求が導出し、その要求を充足するようにシステム、コンポーネント、コードへと要件を細分化して設計し、コードレベルから対応する単体テスト、結合テストを経て、システム全体のテスト、最終的な飛行テストまで行って型式の認証が成される。

このような無人航空機システム全体の計画と要求は他セクションからくる。航空局ガイドライン セクション 110 適合性証明方法(MoC):1, 2 における図は、システム開発における V&V プロセスに型式認証のプロセスを被せた形によるセクション 110 と他セクションとの関係を表した模式図になる。

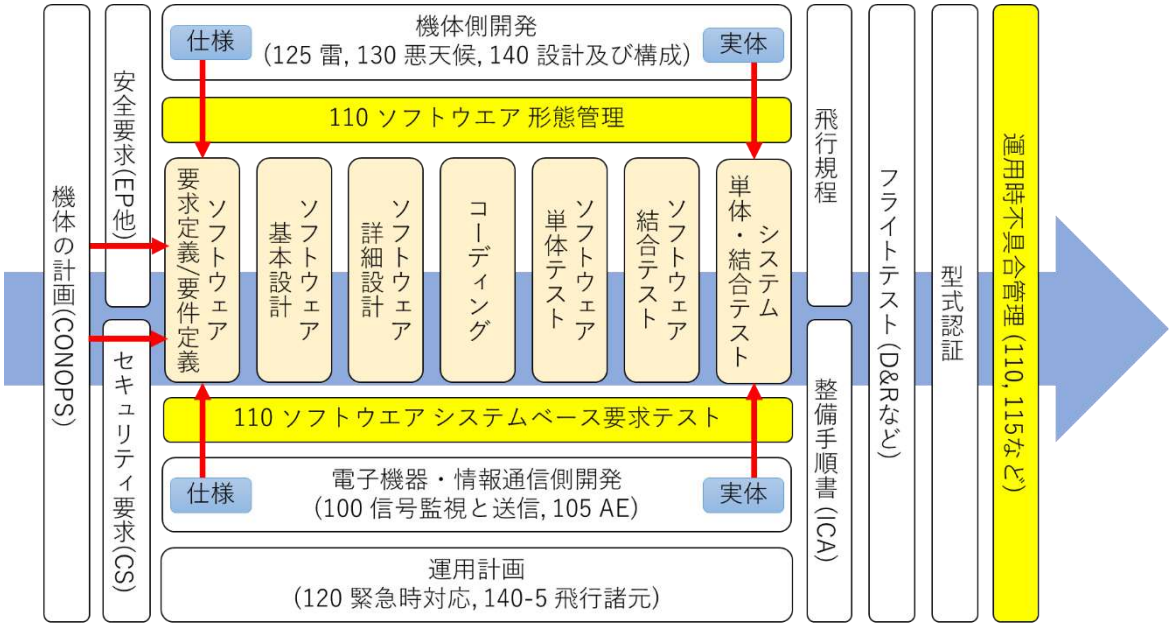


図 4.2-1 セクション 110 と他セクションとの関係

無人航空機システムに対するソフトウェアの開発は、機体の計画段階から始まり、必要な機能、やり取りされる情報などが CONOPS として定義される。この機体の計画に対して事前に安全性に対しておよびセキュリティに対してリスクアセスメントを行い、それぞれ必要な要求が導出されて計画が更新される。これらの情報から、機体側開発、ソフトウェア開発、電子機器・情報通信機器開発および運用計画にそれぞれ分解されて、各パートでシステム開発が行われる。一方で、ソフトウェア開発は、機体を動作させるようなものや、センサーなど電子機器情報を受け取り動作するもの、情報通信機器を介してコミュニケーションを取りながら動作するものなどがあるので、それらハードウェアに起因する仕様を受けてソフトウェア開発が始まり、システムベースの要求が充足するかをハードウェアの実体と併せて用いてテストを行うことが必要であることから、他セクションで定義されているハードウェアの仕様または実体と連携しながらソフトウェアが構築されるべきである。

セクション 110 において、形態管理は、そういった他セクションからの情報を受けて、いかに要求を充足するようにソフトウェアを開発するかについて追跡するものである。また、システムベース要求テストは、他セクションから発生する部分も含めた要求について考察され、それを充足するシステムの挙動が何かを定義し、開発されたソフトウェアとともにテストを行うものである。

不具合管理については、現実にはソフトウェア起因による不具合以外の不具合の可能性も存在する。ソフトウェア開発中においては、開発中に行われるソフトウェア単体・結合テストに対する不具合のレポーティングとして、供与後においては、ソフトウェア起因による不具合以外の不具合も含めてレポートとして受け取り、形態管理とともにソフトウェア起因による不具合であるかを解析するものとして用いることができる。

他セクションとの関連性についての詳細を以下の通りに記述する。

- セクション 001 概念設計書（CONOPS）(以降、「セクション 001」と呼ぶ)
  - セクション 110 への入力

- ■ ユースケースから機能要求の導出
- ■ シナリオから品質要求の導出
- ■ 初期的な安全性解析から安全要求の導出
- ■ 初期的なセキュリティ解析からセキュリティ要求の導出

- 安全性リスクアセスメント – セクション 135 重要な部品(フライトエッセンシャルパーツ)(以降、「セクション 135」と呼ぶ)、セクション 105 関連システム(以降、「セクション 105」と呼ぶ)

  - ■ セクション 110 への入力

    - 機能安全アセスメントによる安全要求の導出と追加要求の導出
    - エッセンシャルパーツにおけるシステムレベルでの単一故障における安全性解析
    - 機能ハザード解析や HAZOP ガイドワードによる解析結果

  - ■ セクション 110 とのギャップ

    - セクション 135 で提示される安全性要求は、当該するシステムが安全に関与するか、どのような故障モードが存在するかまでである。そのため、詳細なソフトウェアに対する安全性解析はソフトウェア要求の段階で行う必要がある。この部分はソフトウェア基本設計のフェーズで行うこと

- セキュリティリスクアセスメント – セクション 115 サイバーセキュリティ(以降、「セクション 115」と呼ぶ)

  - ■ セクション 110 への入力

    - セキュリティ要求に資するシステム開発項目の列挙
    - セキュリティ要求に資するシステムテスト項目の列挙

  - ■ セクション 110 からの出力

    - システムコンポーネント間におけるデータフローの記述およびインターフェース要件の列挙
    - セクション 110 で開発される各コンポーネントにおけるセキュリティ要素の列挙

  - ■ セクション 110 とのギャップ

    - 「悪意のある行動」に基づく安全性の侵害の考察はセクション 115 で行うことを前提とする。解析の結果導出された要求事項のうちソフトウェアに関するものはセクション 110 に関する追加要求として受理すること
    - 開発時における「悪意」もセクション 115 で解析され、ソフトウェア開発時の組織やコーディング規約などの必要な要求が導出される場合、その要求をソフトウェア開発要求に追加すること

- 機体以外のソフトウェア – セクション 105 関連システム

■ セクション 110 への入力

- 関連システムとされる他のシステムに対してのデータフロー、およびソフトウェア機能要求
- 関連システムと機体システムのインターフェース要件
- 関連システム内ソフトウェアのコンポーネント情報
- 安全性、品質の要求

■ セクション 110 からの出力

- 関連システムとされる他のシステムが 110 ソフトウェアのトレーサビリティの範疇外となる場合、その場合における保証の責任関係とインターフェース要件・データの流出入の要求を記述

● 機体側・電子機器側開発 – セクション 100 無人航空機に係る信号の監視と送信（以降、「セクション 100」と呼ぶ），セクション 105 無人航空機の安全な運用に必要な関連システム（以降、「セクション 105」と呼ぶ），セクション 125 雷（以降、「セクション 125」と呼ぶ），セクション 130 悪天候（以降、「セクション 130」と呼ぶ），セクション 140 その他必要となる設計及び構成（以降、「セクション 140」と呼ぶ）

■ セクション 110 への入力

- 機体側で定義される物理的なパラメータの定義（角度，回転数，制御パラメータ）
- 電子機器側で定義されるセンサー系・動力系パラメータの定義
- 機体側インターフェースの仕様（電気的特性含む）
- 自動運転などの構成を含む場合、自動運転のためのソフトウェア機能要求
- カメラなどの構成を含む場合、カメラなどのデータの受け渡し、およびソフトウェア機能要求
- 搭載されるセンサー、ハードウェアの値域の定義
- 機体本体のシステムテストへの供用

■ セクション 110 からの出力

- ソフトウェアで出力される物理コンポーネントへの制御パラメータの列挙
- 単体テスト項目として、物理コンポーネントへの入力データに対する特性をグラフなどで解析した結果

● 運用計画 – セクション 120 緊急時の対応計画（以降、「セクション 120」と呼ぶ），セクション 200 無人航空機飛行規程（以降、「セクション 200」と呼ぶ），セクション 205 ICA（以降、「セクション 205」と呼ぶ）

■ セクション 110 への入力

- 他セクションから導出される運用計画、飛行規程に関してセクション 110 の要求仕様が合致しているかの確認

- 整備のために必要な制御パラメータ入出力確認のための要求事項の追加
- 不具合管理に紐づく整備時点の異常の詳細な記述方法（ログ）

■ セクション 110 からの出力

- ソフトウェアから出力される物理コンポーネントや論理コンポーネントへのデータ変動と、インターフェースの関係に基づく飛行方法、制限の詳細な記述
- ソフトウェア開発における不具合修正アップデートの方法の提示
- ソフトウェアの管理方法についての教示

■ セクション 110 とのギャップ

- 200 飛行規程はソフトウェアの「使い方』であるので、基本的にオペレータ側ユーザーインターフェース要件は 200 飛行規程に入力すること
- また、機体側 API などの項目が存在する場合、200 飛行規程で、関連システムとの連携で利用される API などインターフェースの項目・値域と、値域の変動幅の許容量に対しての項目が記述されること
- 機体内部の OS や内部ツールなどに関して、一般的なフライトに資するものではなく、パラメータ調整など整備に関わる内容は 205 ICA に移譲
- 運用全体に対して、ユーザーインターフェースと管理方法についてソフトウェア開発者が言及すること

● フライトテスト – セクション 300 耐久性及び信頼性（以降、「セクション 300」と呼ぶ）セクション 305 起こりうる故障（以降、「セクション 305」と呼ぶ）

■ セクション 110 への入力

- セクション 300 におけるテストで不具合が発生した場合に対して、ソフトウェアに起因する不具合である場合のフィードバックと追加要求
- システムアーキテクチャが更新されない場合（ソフトウェア入出力の値域などの変更にとどまる場合）はゼロリセットではなく、更新による修正で対応
- システムアーキテクチャが更新される必要がある場合（ソフトウェアのみならずハードウェアの追加などが必要になり、結果的にソフトウェアコンポーネントの追加、更新も必要となる場合）はゼロリセットとなる可能性
- ソフトウェアで制限「されていない」、セクション 200 で「指定されていない」値域や値域の変動幅の許容量についてのリストを提示し、セクション 305 で「起こりうる故障」としてテストすべき値
- システムハングアップなど、データ流通がストップする場合においての制御フローの提示

■ セクション 110 からの出力

- ソフトウェア本体、セクション 200 などで扱われるユースケース
- セクション 110 で管理している関連システムソフトウェアなど

■ セクション 110 とのギャップ

- セクション 135，セクション 305 では機能に対する単一故障を見るが、ソフトウェア機能は場合によっては単一的に故障が発生したときに連鎖的に故障が発生するケースがみられる（メモリリークなど含む）。そのため、ソフトウェアシステム全体の連携の故障解析などは、あらかじめ結合テストなどで把握すること

4.3 セクション 110(a)に対する解説（ソフトウェアに対する試験による検証）

セクション 110(a)は、ソフトウェアに対するテストによる検証、しかもシステム要求ベーステストを求めている。各システムは連携して無人航空機システムを構築し、安全な運用のために相互作用するが、各システム（系統）は情報の流通（インターフェースを通したインプットとアウトプット）と内部の機能が機能要求や安全要求、セキュリティなどの他の要求によって定義されることから、これらの要求を満たす機能、入力に対する出力があることを、システム要求に応じてテストを行うことが規定される。この要求は網羅的に整理され、要求を満たす機能、出力が実現されていることを証明する必要がある。

ソフトウェアに対する検証の目的は、ソフトウェアエラーの発生に繋がる不具合が残存するのを最小化し、無人航空機を安全に運用するためである。ソフトウェア検証は、システムレベルの要求に対し、検証（テスト、アナリシスおよびインスペクション）により、各要求が適切に実装されていることの確認を行う。「航空局ガイドライン」では、 *ASTM F3153-15"Standard Specification for Verification of Avionics Systems"を参考にすることができる* としている。これらの活動を通じて、システムレベル要求ベーステストの結果を「無人航空機ソフトウェア適合性完了報告書」に記載し、完了報告書を補完する文書として、「システムレベルの要求一覧」および「システムレベル要求ベーステスト関連書類およびテスト結果」を作成する。「航空局ガイドライン」では、システムレベル要求の実装確認が対象であるが、本解説書では、ソフトウェア要求のインプットとアウトプットを確認する方法についても取り扱っている。

（1） 「無人航空機の安全な運用に影響を与えるすべてのソフトウェア」の特定

セクション 110(a)の対象は、無人航空機の「安全な運用に影響を与えるソフトウェア」が対象である。無人航空機開発時には多数のソフトウェアが使用されているため、それらを把握し、機能や関連性を理解することが非常に重要である。以下に手順を示す。

1） 「ソフトウェア一覧」の作成

無人航空機に使用される全ソフトウェアを次のインプットを参考に「ソフトウェア一覧」にリストアップする。ソフトウェアは、インストール単位で記載する。

＜インプット＞

- 機体図
- インターフェース管理図

- コンポーネント図
- 関連システム設計図など

次の記入要領を参考に「ソフトウェア名称」および「外部のシステムやユーザーとの相互作用の詳細」を「ソフトウェア一覧」に記載する。

表 4.3-1 記入要領

記載項目	記載事項
P/N および ID	ソフトウェアのインストール単位での Parts No.または ID を記載する
ソフトウェア名称	ソフトウェアの正確な名称や識別子を記載する
主な機能	ソフトウェアにより行われる主要な機能やタスクを記述する
搭載/非搭載	型式に搭載されるか、されないかを記述する
関連するハードウェア要素またはインターフェース	ソフトウェアがどのハードウェアコンポーネントやインターフェースと直接的に関連があるかを確認する
関連システムやユーザーとの相互作用	ソフトウェアが外部のシステムやオペレータとどのようにインタラクトするか特定する

2） ソフトウェアの影響評価

ソフトウェアのリストアップを通じて作成した「ソフトウェアの一覧」に対して、ソフトウェアが誤った挙動をした場合の運用の安全性に直接影響を及ぼす可能性のあるソフトウェアを抽出するための手順を以下に示す。

a. 安全性解析手法選択

「航空局ガイドライン」では、セクション 135 を準用してソフトウェアが誤った挙動をした場合の影響度を評価する方法として、FHA、SSA、FMEA などの安全性解析手法が紹介されており、これらの実施が困難な場合は簡易版 FMEA の実施が紹介されている。また、安全性解析を使用するための規格としては、航空機開発で利用されている安全性評価プロセス（SAE ARP4761）、およびシステム開発保証プロセス（SAE ARP4574A）などが参照可能である。

b. ソフトウェアの評価と抽出

選定した安全性解析手法を用いて、「ソフトウェア一覧」に対して評価を行う。評価の結果、ソフトウェアの動作不良などにより「S/W エラーで計画外飛行になるか①」が「No」の場合は「①が No の理由」を記載し、「セクション 110/135（b）適用 S/W」は「No」となる。一方、「S/W エラーで計画外飛行になるか①」が「Yes」の場合はセクション 110/135 適用 S/W に「○」を記入し、評価対象として抽出する。

なお、ソフトウェアの動作不良が発生した場合に、安全な運用に影響を与えないよう別のソフトウェアによってカバーすることができるならば、どちらか一方のソフトウェアのみをセクション 110 の対象とすることができる。（カバーするソフトウェアとカバーされるソフトウェアの両方をセクション 110 の対象としても良い）ソフトウェア以外の方法でカバーする。

ここまでのプロセスについて、「安全な運用に悪影響を与えるソフトウェアをどのように抽出するかの説明およびその結果」にまとめ、無人航空機の安全な運用に影響を与えるすべてのソフトウェアの特定プロセスが終結する。

表 4.3-2 フライトエッセンシャル S/W 特定解析書の記入例

No.	P/N	Nomen	Ver.	S/W エラーで計画外飛行になるか①	①が No の理由	セクション 110/135(b)適用 S/W
1	XXXXX-XXXXX	フライトモード制御ソフトウェア	A	Yes	-	○
2	XXXXX-XXXXX	帰還モード制御ソフトウェア	B	Yes	-	○
3	XXXXX-XXXXX	安全機能制御ソフトウェア	A	Yes	-	○
4	XXXXX-XXXXX	操作ソフトウェア	B	Yes	-	○
5	XXXXX-XXXXX	機器制御ソフトウェア	A	No	別の S/W がカバー	No

（2） システムレベル要求ベーステスト

1） システムレベル要求の導出

ソフトウェア開発の一般的な流れは、航空機では RTCA DO-178C および SAE ARP4754A がガイドラインとして規定され、V&V プロセスとして知られるプロセスが運用されている。

「ガイドライン」では、システムレベルのテストによりその動作を確認する必要がありそのため、「システムレベルの要求」を定義する必要がある。要求の定義は、ISO2382-20 および JISX0020 では、「要求とは、システムが満たさなければならない必須条件」とされている。なお、SAE ARP4754A では、要求の定義は「検証可能で、実装を検証できる機能仕様の特定可能な要素」とされている。具体的な機能要求の導出については、SysML の要求図などを用いて網羅的に導出する必要があるが、その中で、ソフトウェアに関わる要求であるかを考察すること、さらに、開発における非機能要求を含めてソフトウェアに対する要求を導出する必要がある。

図 4.3-1 は ISO 15271 ソフトウェアライフサイクルのガイドの中に掲載されている、組織におけるコンピュータシステムの位置づけと、それに基づく要求の種類である。実際のところ、CONOPS で記載される内容は組織全体の計画である。そのため、図 4.3-1 から紐解くと、4 つの要求が CONOPS の中に記載されていることとなる。

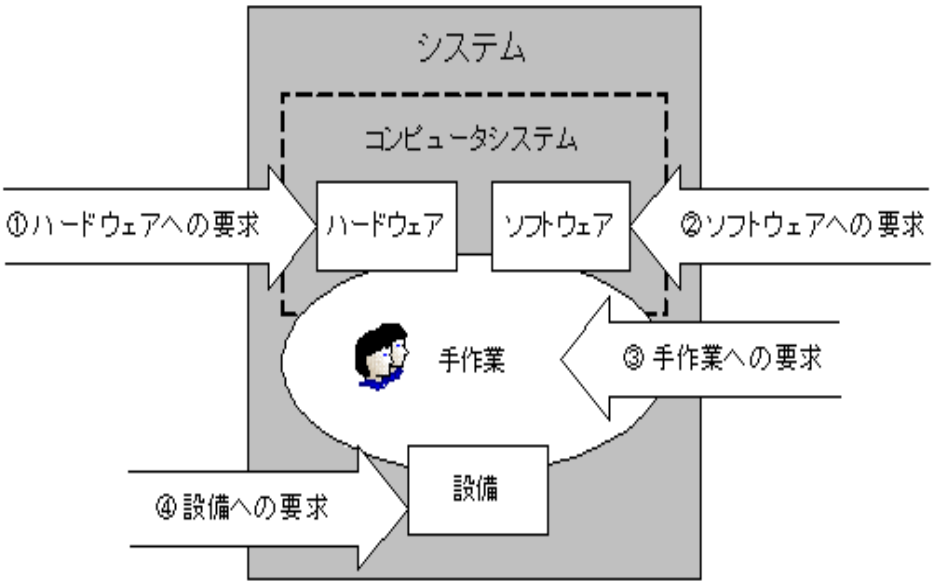


図 4.3-1　ISO15271 に記載されている組織におけるコンピュータシステムの位置づけに見る要求の分類

① 組織への要求
② ビジネスへの要求
③ システムへの要求
④ ビジネスプロセスへの要求

このうち、③のシステムへの要求がソフトウェアを含む箇所の要求である。

図 4.3-2 は、③のシステム要求をさらにブレイクダウンして、コンピュータシステムの中身として要求を列挙したものである。この中では 4 つの要求が含まれる。

① ハードウェアへの要求
② ソフトウェアへの要求
③ 手作業への要求
④ 設備への要求

セクション 110 で管理する部分は基本的に②の部分である。一方で、システムレベルの要求ベーステストを鑑みると、テストの設計段階では、これらシステム全体の構成を含めて設計する必要がある。

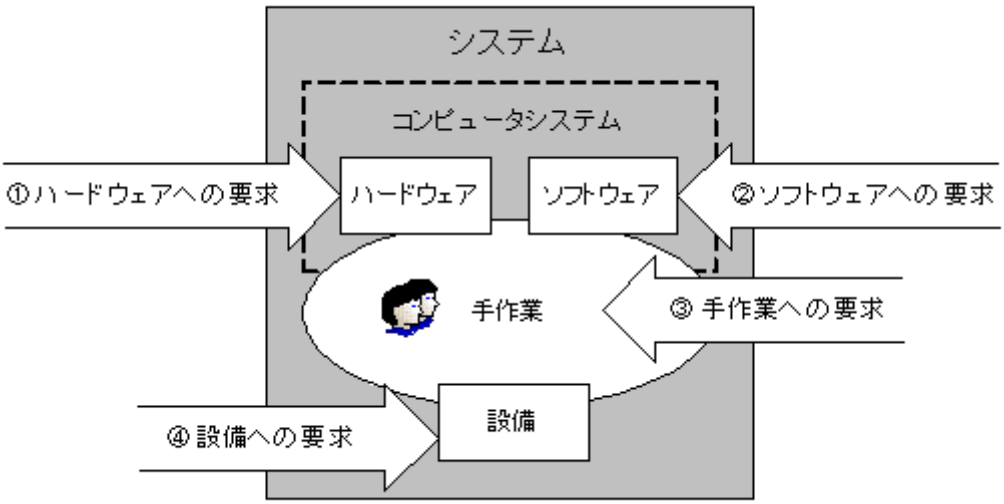


図 4.3-2 システム要求とソフトウェア要求

第二種型式認証で考えると、これらの「システム」とは、ハードウェアに起因する１つの系統として見ることができる。無人航空機システムは、大きく分解すれば、機体システムと地上システムに分解できるが、より細かく分解すると、通信システム、補助システムなどに分解でき、さらに、各サブシステム内には、一連のインストーラブルなソフトウェアのまとまりとして、「地上局ソフトウェア」や「フライトコントローラーソフトウェア」などとして解釈することができる。一方で、地上局ソフトウェアやフライトコントローラーソフトウェアは、ソフトウェア単体で動くものではなく、実機を伴うものであるため、この部分の形態管理を行う必要がある。

これらの、抽出された要求は、システムレベルでまとめられ、システムレベルテストの計画で利用することとなる。このため、システムレベルの要求は網羅的に抽出される必要があり、可能であれば、要求管理から無人航空機システム全体に対する形態管理を行うべきであると考えられる。また、この要求の抽出には、無人航空機システムの計画立案から、飛行テスト前まですべてのフェーズで開発者やステークホルダーを交えて検討されるべきである。なお、ソフトウェアの航空機安全性に対する要求に関しては、SAE ARP4754A や RTCA DO-178C などのドキュメントを参照されたい。

なお、DO-178C では、ソフトウェア要求フェーズにおいて、システムレベル要求をブレイクダウンして、HLR（ハイレベル要求）を作成するプロセスが定義されている。「航空局ガイドライン」では、ソフトウェアレベルの要求ベーステストについては規定されていないが、ソフトウェア単位でのテストが必要な場合は、システムレベル要求とソフトウェア要求の双方向のトレースを確保しておくことが重要である。

2） システムレベル要求ベーステストの計画

次に、「システムレベルの要求一覧」に記載された各要求に対してどのようにテストを行うかを検討する。「システムレベルの要求一覧」に定義した各システム要求を元にテストケースを作成する。テストケースは、各要求の確認を漏れなくダブりなく設計し、テストシナリオに落とし込む。テストケースは、下表の様な目次を含めることが推奨される。

表 4.3-3 テストケースの記入例

テストケースID	目的	前提条件（実行前の状態）	テスト手順	発生させるイベント	期待する結果(実行後の状態)	合否判定基準	テスト結果
GNSS_TC_001	GNSSシステムが、衛星から受け取った情報を適切に解釈し、正確な位置情報を生成できること	GNSSシステムが起動し、衛星からのシグナルを受信可能な状態であること	GNSSテスト手順書	衛星からの信号を手動で送信	GNSSシステムが正確な位置情報を表示	GNSSシステムが正確な位置情報を5秒以内に表示すればテストは合格（PASS）、それ以外の場合は不合格（FAIL）	
FC_TC_001	フライトコントローラがパイロットからの指示を適切に解釈し、これに基づいた無人航空機の運動を制御できること	無人航空機が離陸し、操縦可能な状態となっていること	フライトコントローラテスト手順書	パイロットが操縦桿を操作し、フライトコントローラに指示を送信	フライトコントローラが出力した指示に従って無人航空機が適切に飛行	無人航空機がフライトコントローラの指示に従い、予定した動きをすぐに実行すればテストは合格（PASS）、それ以外は不合格（FAIL）	

3） テスト手順書の作成

実際にテストを実行するためには、詳細なテスト手順が必要となる。そのため、各テストケースに対して詳細なテスト手順を作成し、それに基づいてテストを行う。手順は、実際にテストを行う担当者が理解できるレベルで明確に記載し、テスト手順書の目次例、および記載内容は下表を参照のこと。

409 表 4.3-4 テスト手順書の目次例

目次	目次タイトル	記載要領
1	はじめに	
1.1	目的	テストの全体的な目的と方針を明確に記載。テストが必要とする主な理由とその背景を説明する
1.2	適用範囲	テスト手順が適用する具体的なシステムの部分や設備を定義。特定のモジュールや機能に限定される場合がある
1.3	参照文書	使用される資料、システム要件仕様、デザイン文書など、テストケースを理解するために必要な参考文献をリストアップする
1.4	用語と略語	手順書内で使用する重要な専門用語や略語の説明を記載する
2	テストの概要	
2.1	テストするシステム、機器、装置などの概要	テストの対象である装置やシステムの基本機能や特性を記載する
2.2	テスト種類	システムテスト、統合テスト、単体テストなど、実施するテストの種類を記載する
2.3	テスト目標	テストを通じて実現したい具体的な目標を記載する
3	テストの前提条件	
3.1	環境条件	テストを行うために必要な環境、設定、またはその他の前提条件を記載する
3.2	機器セットアップ	システムが適切にセットアップされ、テストの準備が整った状態であることの確認方法を記載
3.3	テストデータ	テストの際に必要なデータの準備とその内容を記載する
3.4	テストツールと設備	テスト運用に必要なハードウェア、ソフトウェア、ツールをリスト化し、そのセットアップガイドを記載する
4	テスト手順	
4.1	テスト項目	テストする機能の詳細なリストを記載。各項目は明確に説明し、理解しやすいように構造化する
4.2	操作手順および確認項目	各テスト項目について具体的なテスト手順を記載し、テスト実施者がそれに従ってテストを正確に実行できるようにする
4.3	発生させるイベント	どのようなイベントを発生させ、その反応をテストするか具体的に記載する
5	合否判定基準	
5.1	期待する結果	各テスト項目に対する期待される出力または結果を記載する
5.2	合格(PASS)基準	テストパス(成功)の基準を明確に記述。これは、システムが期待通りに動作したことを確認するための基準である
5.3	不合格(FAIL)基準	テストが不合格になったときの基準を記述する。これは、システムが期待通りに動作しなかった条件を示す
6	テスト結果	
6.1	各テスト項目の実行結果	テスト項目ごとの結果と、その考察方法を記載する
6.2	問題発生時の対応	発生した問題と、その解決策を記載する
7	結論とアクションアイテム	
7.1	テストの結論	テスト全体の結果とその意義のまとめ方を記載する
7.2	アクションアイテム	追加テストや、見つかった問題に対する修正など、アクションアイテムの設定および管理を記載する
8	附録	
8.1	テストに使用したツールのリスト	テストで使用したすべてのツール、およびバージョン情報をリストアップする
8.2	参考資料	仕様書、デザイン資料、既存のテストケースなど、参考になる可能性のある他の資料を記載する

410

4） ソフトウェアレベルの要求ベーステスト

これまで、「システムレベルの要求」に対するテスト方法を解説したが、航空局ガイドラインでは、ソフトウェアに対するテストを否定しているわけではない。航空局ガイドラインでは、*「ソフトウェアのテストには、ホワイトボックステスト、ブラックボックステスト、単体テスト、統合テスト、これ以外の分類も含め多種多様に存在しますが」*と記載されているため、代表的なソフトウェア要求ベーステストの分類について解説する。

前述のとおり、無人航空機のソフトウェア開発は V&V プロセスで実施され、テストは、いくつかの工程に分かれており、解説書により表現の違いはあるが、JSTQB Foundation Level シラバスでは、下表の様に分類される。

表 4.3-5 テストレベルによる分類(JSTQB Foundation Level シラバス)

テストレベル	説明
単体テスト	個別にテスト可能なコンポーネントに焦点をあてるテスト
統合テスト	コンポーネントまたはシステム間の相互処理に焦点をあてるテスト
システムテスト	システムが実行するエンドツーエンドのタスクと、タスクの実行時にシステムが示す非機能的振る舞いといったシステムやプロダクト全体の振る舞いや能力に焦点をあてるテスト
受け入れテスト	システム全体の振る舞いや能力に焦点をあてるテスト システムが、ユーザーのニーズ、要件、ビジネスプロセスを満足するかをチェックするための公式なテスト

次に、各テストを「ソフトウェアの内部構造に着目する/しない」を基準に分類すると、大きく「ホワイトボックステスト」と「ブラックボックステスト」に大別される。

表 4.3-6 ソフトウェアの内部構造に着目する/しないによる分類

分類	説明
ホワイトボックステスト	コンポーネントやシステムの内部構造(コード、アーキテクチャ、ワークフロー、システム内のデータフローなど)やの分析に基づきテストケースを設計、選択する技法
ブラックボックステスト	コンポーネントやシステムの内部構造を参照することなく、機能仕様や非機能仕様の分析に基づきテストケースを設計、選択する技法

ホワイトボックステストは、ソフトウェアの最小単位であるモジュールの１つ１つを対象とした単体テストで用いられる。ホワイトボックステストには、命令文の処理順序を確認する「制御フローテスト」とデータの流れを確認する「デ―タフローテスト」がある。ホワイトボックステストを行うメリットは、モジュール内部の処理（命令文）単位で動作確認を行える点であり、検出された欠陥は、その原因箇所がモジュール内部に限定されるため、そのモジュールを調査・変更するだけで修正完了が可能である。

主にホワイトボックステストを用いた単体テストが終わると、続いて、ソフトウェアの内部構造を意識しないブラックボックステストを行う。ブラックボックステストは、主に機能テストとシステムテストにおいて実施する。

5） テスト計画、テストケース、テスト手順書およびテスト結果のトレーサビリティ

航空局ガイドラインでは、 *要求からテストケース及び手順へはトレーサビリティを確保する必要があ*

ります。 と記述されており、システム要求に対して、抜け・漏れなく「システムレベルのテストケース」が設定され、計画変更に追随した「テスト手順書」が設定され、「システムレベルのテストケース」および「テスト手順書」通りに実施した結果が「テスト結果」として完了していることが確認できる仕組みが必要である。また、各テストが要求を網羅しているか確認することもあり、ガイドでは求められていないが、適合性証明計画などで、計画することも有効であると考えられる。なお、ここでいう、トレーサビリティは、要求-テストが必ずしも「1:1」にはならず、「1:N」または「N:N」の関係も存在することに留意する必要がある。

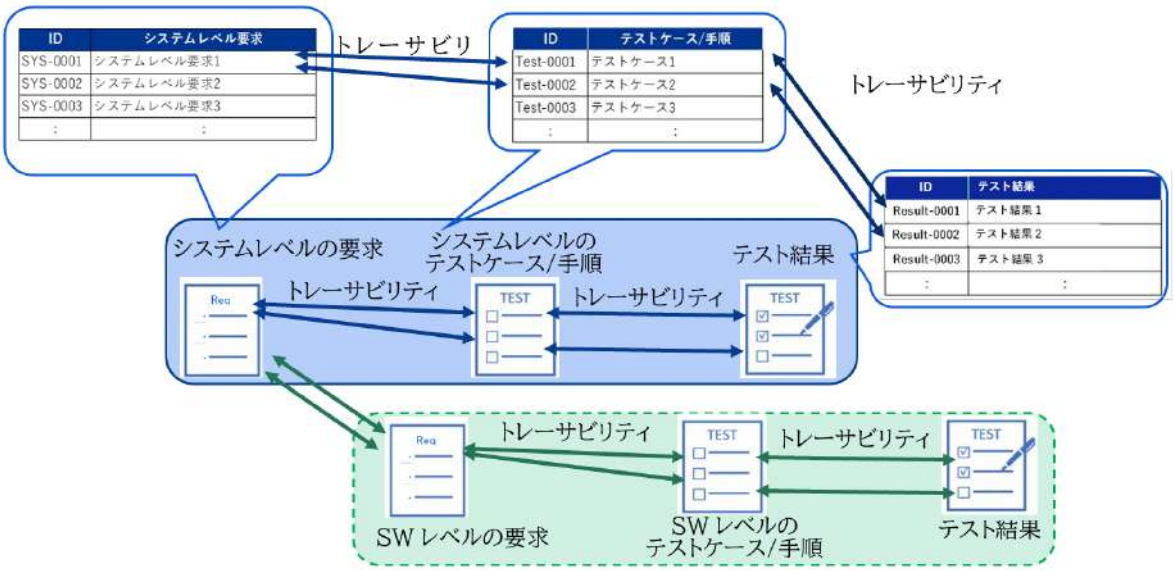


図 4.3-3 トレーサビリティのイメージ図

6） テストでの確認が困難な要求への対応方法

すべての要求は、基本的にはテストにより確認される必要がある一方、「航空局ガイドライン」では、「テストでの確認が困難な要求に関しては解析（アナリシス）や検査（インスペクション）といった方法も許容されます。」とあるため、システムレベルの要求は、テスト、解析またはアナリシスのどれを実施するかを決定し、計画する必要がある。テストでの確認が困難な要求に関してはこのステップでは、各要求に対しては確認方法がテストだけに限らない可能性があることに注意が必要である。例えば、非機能要求（許容できるメモリ量、CPU の負荷など）については、テストだけでなく、解析や検査なども確認方法として採用される。「システムレベル要求ベーステストをどのように実施するかの説明（計画）」に記載する。解析および検査について、ASTM F3153-22 の定義を引用し、事例を下表に例示した。

表 4.3-7 解析および検査の例示

要求	検査(インスペクション)	解析(アナリシス)
定義(**ASTM F3153-22**)	検査とは、1 つ以上の感覚(例えば、視覚、聴覚、触覚など)を用いたシステムの非破壊検査である。単純な物理的操作や測定を含むが、これに限定されない	解析とは、モデル、計算、テスト装置、またはそれらの組み合わせを用いてシステムを検証することである。分析により、既知のデータおよび仮定の外挿に基づき、期待されるシステム性能について予測的な言明を行うことができる
パフォーマンス	リソースの消費速度、CPU 負荷、メモリ使用量、バッテリ消耗などのパフォーマンス関連のデータを収集し、分析する	実際にシステムを観察し、温度上昇、異音、異臭などがないか確認する
耐久性	使用回数・時間、テストパターン(気温、湿度、振動、衝撃)に基づいて設計寿命を拡大推定する	長期使用後、システムに異常摩耗、損傷、変形が起きていないか、外観および振動・音を確認する
ロード	同時に多くの指示を与えるシミュレーションを通じて、フライトコントローラの制約や上限性能を理解する	高負荷環境下で稼働した後のコントローラを確認し、異音、異臭などがないか確認する
可用性	実際の稼働時間と全体の稼働可能時間をもとに、システムの可用性を統計分析する	長期にわたり連続稼働させたハードウェアを視察し、熱問題、劣化などを確認する
セキュリティ	暗号化、認証などのセキュリティ機能が正しく実装されているかを確認するために、コードレビューやセキュリティ解析ツールを使用する	物理的なセキュリティ特性(例えば、システムに物理的アクセスを遮断するケースなど)を視察上、損傷や変形を確認する

4.4 セクション 110(b)に対する解説(ソフトウェアの形態管理)

セクション 110(b)は、ソフトウェアエラーを減少させるため、形態管理システムの使用を求めている。

無人航空機のソフトウェア開発には、多くのステークホルダーが関わり、それぞれが異なる役割および責任を持つ。また、日々の作業では、それらステークホルダーにより、ソフトウェアが頻繁に変更される。このような状況において形態管理システムを使用すると、以下の利点が得られる:

- あるソフトウェアが変更されたときに、その変更内容(例えば、誰が変更を行ったのか、いつ変更が行われたのか、なぜ変更が行われたのか、どのデータのどの箇所が変更されたのかなど)について追跡できるようになる。その結果、ソフトウェアの変更から生じる現場の混乱が抑えられ、エラーがソフトウェアに入り込むリスクを低減させることができる。
- 開発に関わる人が、最新のバージョンのソフトウェアを容易に特定できるようになる。その結果、誤って古いバージョンのソフトウェアを使用するリスクを低減することができる。
- ソフトウェアの不適切な変更により新たなエラーが発生した場合、エラーが発生していない過去のバージョンを特定し、素早く戻ることができる。その結果、エラーの影響を最小限に抑えることが可能となる。
- 形態管理システムにより管理されているソフトウェアへのアクセス制御を行うことができる。これにより、特定の開発者のみがデータを変更することが保証され、不適切な変更が抑制され、ソフトウェアの整合性を保つことが可能になる。

なお、形態管理の目的は、ソフトウェアエラーの減少だけでなく、多岐にわたる。例えば、各型式に搭

載されているソフトウェアの追跡、適切なソフトウェアの管理および保存、ソフトウェア開発プロセスの効率化、セキュリティの向上、ソフトウェアの再利用性の向上、データ喪失からの復旧などである。

(1) 形態管理の対象

形態管理の対象は、無人航空機の安全な運用に影響を与えるソフトウェアの開発において作成するソフトウェアである。航空局ガイドラインには、以下のデータが形態管理の対象として明示されている。

> *i. 要求(Requirements)*
> *ii. システム及びソフトウェアテスト環境の説明*
> *(System and software test environment descriptions)*
> *iii. 要求からテストケース及び手順へのトレーサビリティを含むテスト手順及び結果*
> *(Test procedures, and results with requirements traceability to test cases and procedures)*
> *iv. ソースコード及び開発環境/ツール*
> *(Source code and development environment/tools)*
> *v. 実行オブジェクトコードの複製のためのビルド/ロード手順*
> *(Build and load procedures for replication of the executable object code)*
>
> *[引用:航空局ガイドライン]*

航空局ガイドラインは、型式認証が適切かつ円滑に行われるよう、安全基準に対する適合性証明方法をとりまとめたものであり、基本的には航空局ガイドラインに明示されているデータについての形態管理が必要となる。

しかし、明示されているデータの形態管理が難しい場合、その代替として他のデータの形態管理を行うことが適切な場合がある。例えば、

- COTS ソフトウェアを使用する場合、ソースコードは提供されず、オブジェクトコードまたは実行可能オブジェクトコードのみが提供されることがある。そのような場合、オブジェクトコードまたは実行可能オブジェクトコードを形態管理することが適切な場合がある。詳細については、本解説書の 4.7(1)を参照のこと。
- 特定のテストが実行できない場合、代わりにインスペクションまたはアナリシスを行うことがある。そのような場合、テストケース、テスト手順およびテスト結果の代わりにそれらのデータを形態管理することが適切である。
- ソフトウェアのテストを別のテスト(例えば、セクション 300 のテスト)と合わせて行うことがある。そのような場合、別のテストのデータも形態管理することが適切である。

また、パラメータデータアイテムを作成する場合、その形態管理を行うことが適切である。パラメータデータアイテムについては、本解説書の 4.7(2)を参照のこと。

また、プロジェクトの事情により、明示されているデータに加え、他のデータについても形態管理を行うことが適切な場合がある。例えば、以下に示すデータは、形態管理の対象とすることが適切な場合がある。

- ソフトウェア適合性証明計画書
- ソフトウェア設計
- 形態管理の記録(例えば、ベースラインの記録など)
- 不具合管理の記録(例えば、不具合の記録、不具合の分析結果など)
- ソフトウェア品質保証結果(注:航空局ガイドラインでは求められていないが、品質保証活動を実施する場合)
- ソフトウェア適合性完了報告書
- 宣言書
- 他のセクションの活動で生成されたデータ
- その他、社内資料やプロジェクト固有のニーズにより作成したデータ

(2) 形態管理の活動

プロジェクトにより、どのような形態管理が必要になるかは異なる。したがって、プロジェクトの特性(例えば、組織の規模/カルチャー/経験、ソフトウェアの規模/複雑性/開発プロセス、使用する形態管理ツール、その他のツールとの連携など)を考慮して、プロジェクトごとに形態管理の活動をテーラリングする必要がある。

参考として、表 4.4-1にRTCA DO-178Cのソフトウェア形態管理プロセス(Software Control Management Process)に要求されている活動の概要を示す。ただし、活動および用語の詳細はDO-178C を参照のこと。

528 表 4.4-1 DO-178C におけるソフトウェア形態管理プロセスの活動

活動	概要	DO-178C の参照	備考
形態識別（Configuration Identification）	形態アイテムを選定し、それぞれを一意に識別するための方法を確立する活動である	Section 7.2.1	航空局ガイドラインで明確に求められている活動ではないが、形態管理を行う上で必須の活動であり、実施する必要がある
ベースライン設定（Baseline）	成熟した形態アイテムをベースラインとしてソフトウェアライブラリ(注:リポジトリ)に保存する活動である。ベースラインとして設定した形態アイテムを変更する場合、変更の手続きが必要となる	Section 7.2.2	航空局ガイドラインで求められている活動である
不具合管理（Problem Reporting）	不具合を、識別し、分析し、解決するまで管理する活動である	Section 7.2.3	航空局ガイドラインでは、形態管理とは異なる活動として求められている。不具合管理については、本解説書の 4.5 を参照のこと
変更管理（Change Control）	ソフトウェア開発の過程で発生する変更を管理する活動である。変更は、不具合の解決、新機能の追加、性能の改善などのために行われる	Section 7.2.4	航空局ガイドラインで明確に求められている活動ではないが、不具合の解決などのために実施する必要がある
変更レビュー（Change review）	変更が適切に取り扱われていることを確認する活動である	Section 7.2.5	航空局ガイドラインで明確に求められている活動ではない。必要に応じて実施することが推奨される
形態状況報告（Configuration status accounting）	形態管理についての状況(例えば、形態アイテムの状況、ベースラインの状況、不具合管理の状況、変更履歴、リリースの状況など)について記録し、報告する活動である	Section 7.2.6	航空局ガイドラインで明確に求められている活動ではない。必要に応じて実施することが推奨される
保存、復元、リリース（Archive, Retrieval, and Release）	ソフトウェア製品に関連するデータ(形態アイテムを含む)を保存し、必要に応じて復元する活動である。「保存」はデータを長期間保存し、保護することを意味する。「復元」は保存したデータを取り出すことを意味する。「リリース」は形態アイテムを正式に利用可能にすることを意味し、認証のために利用する前や顧客または他のプロジェクトに提供する前に行われる	Section 7.2.7	航空局ガイドラインで明確に求められている活動ではない。必要に応じて実施することが推奨される
ソフトウェアロード管理（Software Load Control）	ソフトウェアをターゲットコンピュータにロードするためのロード手順を作成する活動である	Section 7.4	航空局ガイドラインで明確に求められている活動である
ソフトウェア環境の管理（Software Life Cycle Environment Control）	ソフトウェア環境(例えば、ツール、ツールを使用するコンピュータなど)を管理する活動である	Section 7.5	航空局ガイドラインで明確に求められている活動である

529

なお、形態管理の活動は、セクション 110(b)に記載されている通り、全ライフサイクルを通して実施される。全ライフサイクルとは、一般的には、プロジェクト立ち上げフェーズから始まり、開発フェーズ、テストフェーズ、運用および保守フェーズを経て、製品リタイアフェーズを指す。プロジェクト立ち上げフェーズでは、プロジェクトチームが発足され、形態管理システムの計画とセットアップが行われる。これには、形態管理ツールの選定、設定、トレーニングおよび適用が含まれる。また、製品リタイアフェーズにおいて、当該プロジェクトにおける形態管理システムが終了し、形態管理の対象が破棄または保存される。

注: 形態管理の活動のうち、ベースラインと不具合管理は、プロジェクトの立ち上げフェーズから実施する必要はない。ベースラインを開始するタイミングについては、本解説書の 4.4(3)を参照。不具合管理については、本解説書の 4.5 を参照。

(3) ベースラインを開始するタイミング

航空局ガイドラインでは、形態管理の活動の 1 つであるベースラインについて、「遅くともセクション 110(a)のテストの開始前にスタートする」ことを求めている。一般的には、プロジェクト立ち上げフェーズにおいて、形態管理の責任者がベースラインを開始するタイミングを決定する。

(4) 形態管理記録

形態管理が行われた結果として、以下の記録などを保持する。

- 形態管理対象のリスト
- ベースラインのリスト
- 文書の改訂履歴
- バージョン管理ツールに自動的に記録された変更履歴

4.5 セクション 110(c)に対する解説(PR システムの導入および活用)

サーキュラーNo.8-001 には、"*PR システムの導入と活用*"とあるが、PR システムを利用する目的は不具合管理であるため、不具合管理とそれを実現するための PR システムについての解説としている。

不具合管理の目的は、不具合の対応漏れを防ぎ、ソフトウェアエラーを最小化することである。そのために、発見された不具合を記録し、分析し、解決するまで確実に管理する必要がある。PR システムを導入、活用し、確実に不具合管理できるようにすることや、開発中においては開発者間、運用中においては開発者と運用者間のコミュニケーションに役立てるようにすることも重要である。

(1) 不具合管理の対象

セクション 110(a)の対象と同じく安全な運用に影響を与えるソフトウェアが対象である。

ソースコードの不具合のみでなく、システムレベルの要求、テストケースおよび手順、テスト環境の不具合も含まれる。テストのみでなく、解析（アナリシス）、検査（インスペクション）で発見された不具合も対象となる。

プロジェクト管理に関する問題や品質保証活動によるプロセスの問題はここでは扱わない。

（2） 不具合管理の対象テスト、フェーズ

以下のテスト、フェーズで発見されたソフトウェアに関する不具合が対象となる。ベースラインを設定し、テスト、実運用を開始する必要がある。

- セクション 110(a)のテストで発見されたソフトウェアに関する不具合
- 各種 D&R のテストで発見されたソフトウェアに関する不具合
- 型式認証後の実運用時に発見されたソフトウェアに関する不具合

発見される不具合には、ソフトウェアに関する不具合だけでなく、ハードウェアなど他の不具合の可能性もある。それらを同じ管理方法で管理しても構わない。セクション 110(c)での対象は、ソフトウェアに関する不具合のみとなる。

（3） 不具合管理活動

以下が、不具合発見後の不具合管理活動になる。(4)の記録する不具合情報も参照。

1） 不具合の記録

テスト、実運用時に、ソフトウェアの不具合が発見された場合、不具合が一意に識別できるよう ID などを付与し、不具合内容を記録する。

不具合の現象だけでなく、不具合を再現させるための情報も記録する。テスト時であれば、不具合が発生したテストケース、ベースラインなどの情報、実運用時であれば、運用者にヒアリングし収集した情報などの記録が考えられる。

2） 不具合の分析

不具合の原因、影響範囲、重大度などを分析し、修正対象と修正内容を決定する。分析には、テストケースとシステムレベルの要求間のトレース情報などが参考となる。

不具合から修正対象、修正内容までトレースを取り、不具合の修正を確実にする。

3） 不具合の修正

不具合を修正し、修正内容をテスト、レビューなどで確認する。

既存の機能が正常に動作するかを確認するための回帰テスト（リグレッションテスト）を実施する。

4） 再テスト

再設定されたベースラインを用いて、再度テストを実施する。

5） 不具合の解決の追跡

各不具合にステータス（オープン、クローズなど）を付与してステータスを管理し、解決まで追跡する。再テストに合格することで不具合のクローズとなる。

6） 未解決の不具合の正当化

今回の型式認証では解決しない“未解決の不具合”がある場合、その不具合を残存させても、“無人航空機の安全な運用”への影響が許容範囲であることを評価し、未解決でも良い理由を記録する。

すべての“未解決の不具合”とその正当化の情報を、ソフトウェア適合性完了報告書に記述する。

例えば、サプライヤが開発したソフトウェア、COTS ソフトウェア、オープンソースソフトウェア、関連システムの不具合が発見された場合、サプライヤ、COTS ソフトウェアの提供元、関連システムの開発元と調整し修正することや、オープンソースソフトウェアを修正することが望ましいが、修正できない場合があるかもしれない。

（4） 記録する不具合情報

不具合が一意に識別でき、再現できるようにするため、以下の項目などを記録する。

- 不具合 ID
- 不具合発見ベースライン
- 不具合発見テスト/フェーズ
- 不具合を発見したテストケース、手順
- 不具合内容
- ステータス（オープン、クローズなどの不具合のステータス）
- 重大度（安全な運用に影響を与えるかなど）
- 修正対象と修正内容
- 再テストケース、手順
- 再テスト結果
- 未解決の不具合の場合、正当化の情報など

（他にも日付、発見者、不具合タイトル、優先順位なども記録することがある）

（5） PR システム

上記の不具合管理を実施可能な PR システムを利用して、不具合管理を確実にする。不正なアクセスや不正な変更などのセキュリティの観点からも、アクセス権限の管理、変更ログが残る PR システムが良い。PR システムのデータの保護のため、バックアップも考慮する。

利用者が PR システムを正しく使用することができるよう、使用手順を定める。

4.6 ソフトウェア適合性証明計画、完了報告書、宣言書に対する解説

(1) ソフトウェア適合性証明計画書について

ソフトウェア適合性証明計画書は、申請者が開発されるソフトウェアに要求される厳密さに見合ったソフトウェアライフサイクルを提案しているかどうかを、検査者へ示すための計画をまとめたものである。

セクション 110 ではセクション 110(a)で「安全な運用に影響を与えるすべてのソフトウェア」の抽出とテストによる検証について、セクション 110(b)で形態管理の方策について、セクション 110(c)で PR システムの導入と活用について提示している。ソフトウェア適合性証明計画書は、申請者が セクション 110(a)にて抽出した「安全な運用に影響を与えるソフトウェア」についてセクション 110(a)～(c)それぞれの項目に対してどのように適合性証明を実施するかなどの計画を示した文書となる。以下に検証項目の例を示す。また、Appendix1～3 に記載例を示す。

表 4.6-1 セクション 110 各項におけるソフトウェア適合性証明計画における検証項目の例

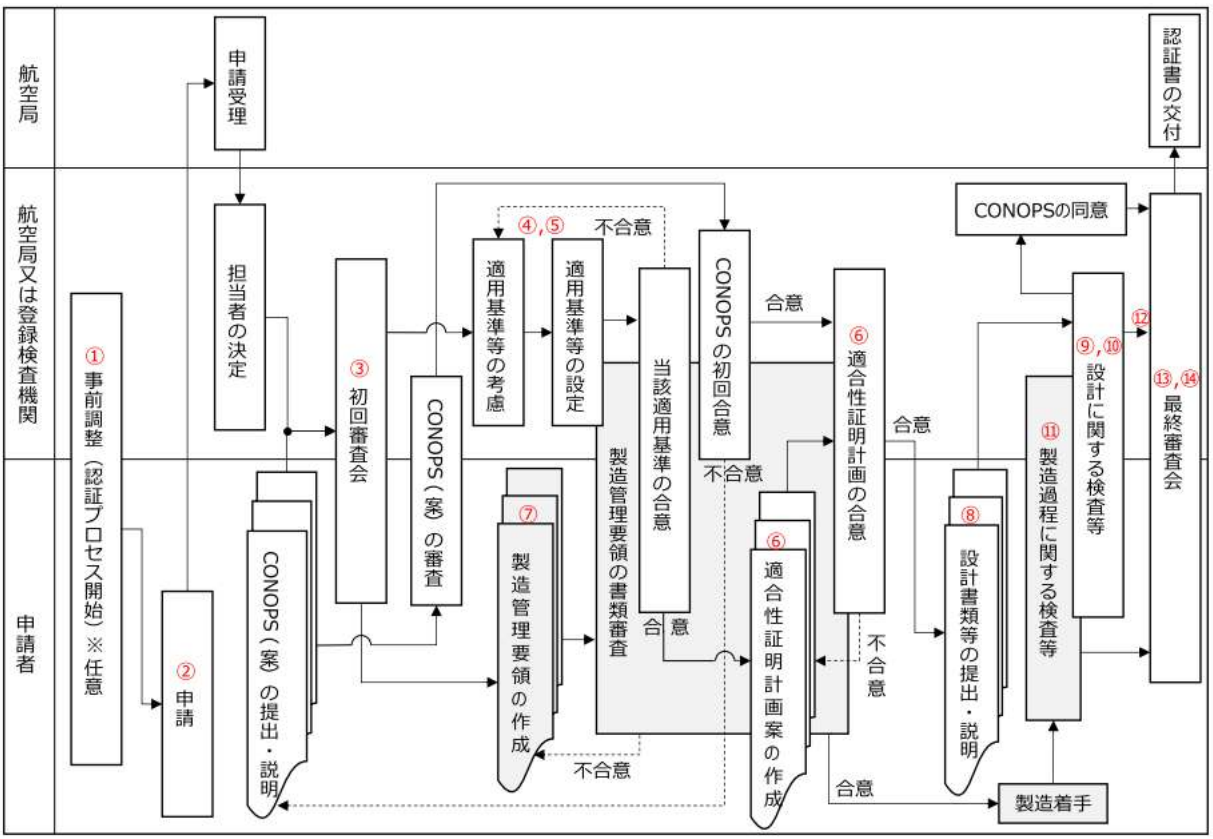
項	活動	記載項目
(a)	ベーステスト	● 無人航空機のシステム概要 ● ソフトウェア一覧(搭載、非搭載別) ● 「安全な運用に影響を与えるソフトウェア」をどの様に抽出するかの説明およびその結果 ● 「システムレベルの要求」定義(要求一覧)) ● システムレベル要求ベーステストをどのように実施するかの説明(計画) ● システムレベル要求ベーステスト関連書類要求×テストケース×手順マトリクス)テストツール、テスト環境 ● 各要求に対するテスト方法概要 ● テスト解析(アナリシス) ● 検査(インスペクション)
(b)	形態管理	● 形態管理対象、それらの識別方法 ● ベースラインを開始するタイミング、ベースラインの対象およびそれらの識別方法 ● 変更管理の方法 ● ビルド手順およびロード手順の作成方法 ● ソフトウェア環境(例えば、使用するツール、ツールを使用するコンピュータなど)の管理方法
(c)	不具合管理	● 不具合管理の対象 ● 不具合管理の対象テスト、フェーズ ● 不具合管理の活動内容(不具合の記録、分析、修正、再テスト、不具合解決の追跡、未解決不具合の扱いなど) ● 使用する PR システム

1) 申請の流れ

申請者はソフトウェア適合性証明計画(案)および必要書類を作成し、検査者から合意を得た後に、検査を開始する。ソフトウェア適合性証明計画は申請者の計画が示された文書となるので、以降の過程で計画の見直しが発生した場合、申請者は当該計画を変更し、再度検査者より合意を得る必要がある。

以下に型式認証取得までの全体フローを航空局ガイドラインより引用する。「*⑧設計書類等の提出・*

642 *説明*」までに完了させ全体フローに対して遅れのでないよう留意が必要となる。
643



644
645 図 4.6-1 型式認証取得までの全体フロー
646 出所）航空局ガイドライン
647
648

649
650 以下にソフトウェア適合性証明計画の完了までの流れの一例を示す。実際の設計/証明活動は並行
651 で進む場合や手戻りも発生するため一概に当てはまるものではない。
652

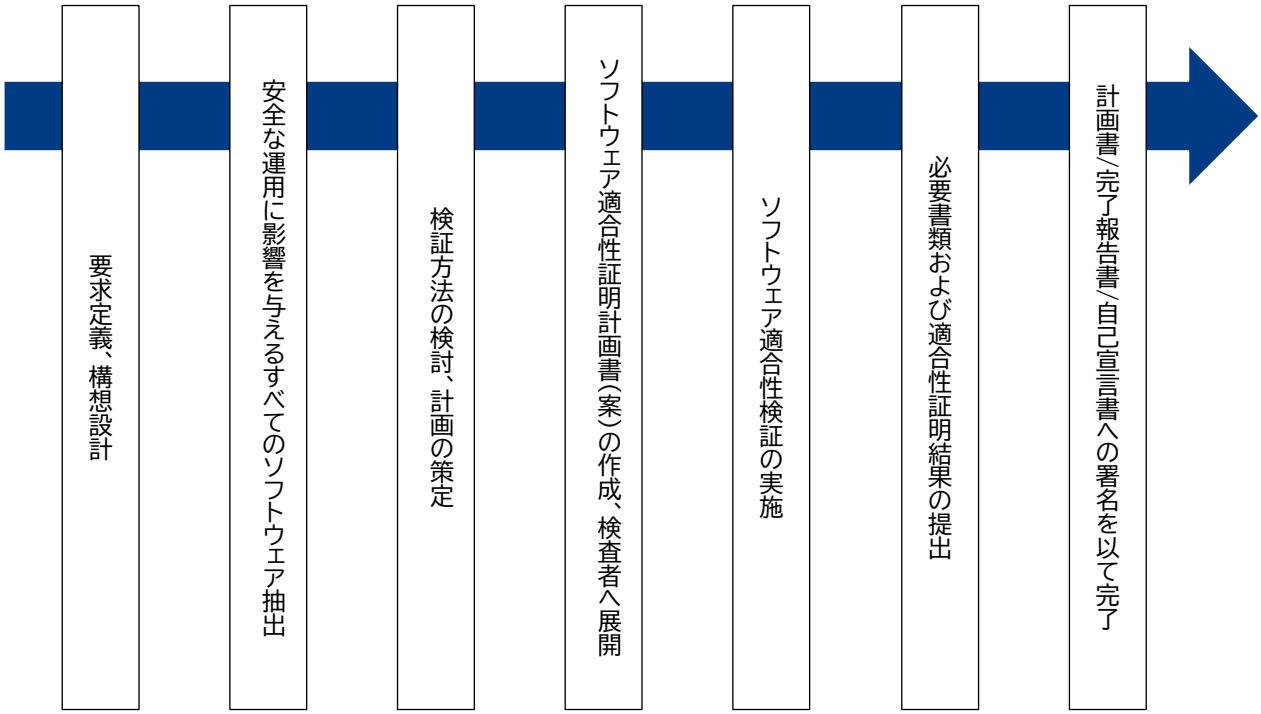


図 4.6-2 ソフトウェア適合性証明計画の流れ

653

2） 必要書類

下記 a～e をまとめた書類一式を適合性証明計画書とする。

a. システム概要

ソフトウェアに限らず、必要となる場合はハードウェア含めた機体仕様などシステムの概要を把握するための書類を作成する。

b. 安全に影響を与えるソフトウェア一覧

「安全に影響を与えるソフトウェア」の抽出基準およびその一覧を用意する。

c. 日程概略

申請者が希望する申請書の提出から証明活動完了までの日程の概略に係る情報を記載する。日程は四半期単位など大まかなものでも構わない。なお、ソフトウェア適合性証明計画の改訂の頻度などを勘案し、別途スケジュールの管理が可能な資料が存在する場合は当該資料を呼び出すことも可能とする。

d. ソフトウェア適合性証明計画表

Appendix 4 に記載例を示す。

ア） 適用基準などに関する事項

「安全な運用に影響を与えるソフトウェア」ついて、セクション 110(a)～(c)の適用基準、ソフトウェア適合性証明の必要性の有無、解析または実証の選択を含む適合を示す方法、実施時期などを記載する。

イ） 証明活動などに関連する人員に関する事項

本証明活動に関連する人員について、それぞれの責任および権限を明確にする。

e. その他必要となりうる書類

申請者が従来の無人航空機の設計にはないと考える新設計、新技術を採用する場合は、その概要ならびに検討事項およびその解決方法をまとめる。また、共同開発者がある場合は、共同開発者の名称、分担に関する情報を記載し、設計開発行為の一部を外部に委託する場合は、当該委託先（外注先）の名称、委託内容に関する情報を記載する。

3） 議事録

ソフトウェア適合性証明計画の説明および調整を行った際は、その説明内容、指摘およびその改善事項、調査事項、問題点などを明確にし、認識を共有する目的から、申請者において議事録を作成し、双方で記載の内容を確認する。

議事録には特に定まった様式はないが、「サーキュラーNo.8-002”無人航空機の型式認証等の手続き”（以降、「サーキュラーNo.8-002」と呼ぶ）」 の別添 3（JCAB FORM 8-002-3）の様式を使用することも可能である。

（2） ソフトウェア適合性証明完了報告書について

ソフトウェア適合性証明完了報告書は、申請者が適合性証明計画に沿って実施した結果を明記し、完了したことを証明するものである。完了を承認する検査者からのソフトウェア適合性証明計画書、完了報告書および自己宣言書への署名を以て該当する項目の証明活動完了となる。以下に記載項目の例を示す。また、Appendix5 に記載例を示す。

表 4.6-2 セクション 110 各項におけるソフトウェア適合性証明完了報告書の記載内容

項	活動	記載項目
(a)	ベーステスト	● システムレベル要求ベーステストの結果概要 ● システムレベル要求ベーステスト結果 ● 各要求に対するテスト方法結果概要 ● ソフトウェアテスト結果 ● ソフトウェア解析（アナリシス）結果 ● ソフトウェア検査（インスペクション）結果
(b)	形態管理	● 形態管理した対象、それらを識別した方法 ● ベースラインを開始したタイミング、ベースラインの対象としたデータおよびそれらを識別した方法 ● 変更管理した方法 ● ビルド手順およびロード手順を作成した方法 ● ソフトウェア環境（例えば、使用するツール、ツールを使用するコンピュータ）を管理した方法 ● ソフトウェア適合性証明計画書からの相違点
(c)	不具合管理	● 不具合管理の対象 ● 不具合管理の対象テスト、フェーズ ● 不具合管理の活動内容 ● 使用した PR システム ● ソフトウェア適合性証明計画書からの相違点 ● 未解決の不具合のリストとその正当化の情報

（3） 宣言書について

サーキュラーNo.8-001 にて記載される通り、機体認証および型式認証を受けようとする無人航空機のうち一部を除く第二種に分類される機体は、宣言書を以て検査の代替とする。

機体認証または型式認証申請者は、自身が当該要件の適合性を確認した上でその旨を宣言書に記載し検査者へ提出する。Appendix5 にその書き方の例を示す。

4.7 その他参考となる情報(議論中:現時点の内容)

(1) ソースコードを入手できない場合の扱い

航空局ガイドラインのセクション 110(b)においては、ソースコードの形態管理が求められている。一方で、申請者はフリーウェアや COTS ソフトウェアなどを入手することが可能である。一般的にこれらのソフトウェアについて、申請者がソースコードを入手することは難しいと考えられる。そこでこのような場合においても、申請者が型式認証を正しいプロセスで取得できるように解説を行う。はじめに申請者が入手可能なソフトウェアを一覧化し、ソースコードの入手可否を分類した上で、対応内容を記載する。

1) 申請者が入手可能なソフトウェア一覧

a. オープンソースソフトウェア(OSS)

特定のライセンスにしたがって、ソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称である。脆弱性調査を行った結果、問題がある場合はセクション 115 に則り対策を行う。

b. 自由ソフトウェア

ユーザーが自由に共有、研究、変更できるソフトウェアである。

c. 自社開発ソフトウェア

ア) 申請者がソフトウェアの情報を把握・入手できる場合

イ) 申請者がソフトウェアの情報を把握・入手できない場合(例:現在、組織存在しない人物が過去に作成した場合など)

この場合はテストを実施した結果、問題を抽出してもソースコードが無く、対応ができないため使用することは望ましくない。

d. COTS

ア) (COTS)システム

ハードウェア、ソフトウェアを組み合わせたシステムとして、販売されている場合を指す。

イ) (COTS)ソフトウェア

COTS ソフトウェアとして、ソフトウェア単品で、販売されている場合を指す。

e. フリーウェア

無料で利用することができるソフトウェアである。

f. 他社開発

申請者が所属する組織以外で開発されたソフトウェアを指す。ここでは特に、申請者が所属する組織が、ソフトウェア仕様書を作成して他社に開発を依頼する場合を指す。

2） ソースコードの入手可否

図 4.7-1 は、ソースコードの入手可否について一般的な考えに基づき、分類した図である。以降は図 4.7-1 で分類した例を基に解説を行う。

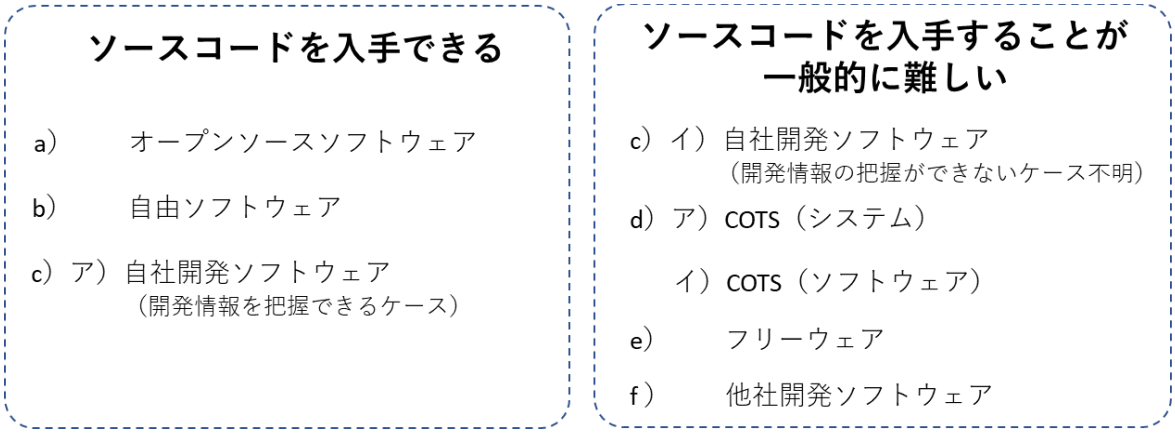


図 4.7-1 ソースコードの入手可否を一般的に整理したソフトウェアの分類

3） セクション 110(a)に対する解説(ソフトウェアに対する試験による検証)

a. ソースコードを入手できるソフトウェア

ソースコードの入手が可能なためセクション 110(a)に則り、テストを実施する。

b. ソースコードを入手することが一般的に難しいソフトウェア

ソースコードが入手できない場合、セクション 110(a)に則り、テストを実施する。ソースコードレベルのテストが必要な場合は、ソースコードを開発する組織に対応を依頼する。

4） セクション 110(b)に対する解説(ソフトウェアの形態管理)

a. ソースコードを入手できるソフトウェア

ソースコードの入手が可能なため、ソースコードレベルでセクション 110(b)に則った形態管理を実施

747 する。

748 b. ソースコードを入手することが一般的に難しいソフトウェア

749 一般的にソースコードの入手が困難なため、オブジェクトコードレベルでセクション 110(b)に則った
750 形態管理を行う。オブジェクトコードを入手できない場合は、実行可能オブジェクトコード(EOC)の形
751 態管理を実施する。EOC は不具合対応で更新される可能性があるため、最新の EOC のバージョン
752 情報を常に把握しておくことが必要である。さらに COTS においては形態管理と同時に、製品の販売
753 とサポートが終了するタイミングを把握しておくことが重要である。サポート終了後のソフトウェアを使
754 用して問題が発生した場合、対応ができないためである。
755 またソースコードの形態管理についてはサプライヤ管理の一環で、申請者はサプライヤにソースコー
756 ドの形態管理を行うことを求めることとする。

757 5) セクション 110(c)に対する解説(PR システムの導入および活用)

758 a. ソースコードを入手できるソフトウェア

759 ソースコードの入手が可能なため、 セクション 110(c)に則った不具合管理を実施する。

760 b. ソースコードを入手することが一般的に難しいソフトウェア

761 サプライヤがソフトウェアを開発している場合、サプライヤが実施している不具合管理がセクション
762 110 ソフトウェアのセクション 110(c)を満たすことを示すまでは不要と考える。申請者側でセクション
763 110 ソフトウェアのセクション 110(a)で求められているシステムレベルのテストを実施し、不具合が発
764 見された場合は、サプライヤによる不具合修正の後、申請者側で再テストによる確認を行うことで不具
765 合管理は可能である。申請者側の不具合管理活動を示すことで十分と考える。
766

767 (2) PDI File の扱い

768 PDI File とは パラメータを変更することによりターゲットコンピュータが直接利用できるデータであ
769 り、実行可能オブジェクトコード(EOC)の振る舞いを変えることができるファイルである。また PDI
770 File は、EOC から独立したファイルであり、EOC とは別に形態管理するデータである。

771 1) セクション 110(a)に対する仮説(ソフトウェアに対する試験による検証)

772 PDI File を使用する場合、システムレベルの要求において、データの値、範囲、フォーマットなどを定
773 義する。その上で、EOC と合わせてセクション 110(a)に則りテストを実施する。

774 2) セクション 110(b)に対する解説(ソフトウェアの形態管理)

775 PDI File に変更があった場合は、セクション 110(b)に則り形態管理を実施する。

3） セクション 110(c)に対する解説(PR システムの導入および活用)

PDI File に不具合があった場合は、セクション 110(c)に則り不具合管理を実施する。

(3） ソフトウェア変更時の対応

1） 開発中

ソフトウェアの不具合が発生した場合、対策後にセクション 110(a)～(c)の対応を行った上で、セクション 300 の飛行テスト時間を 0 時間にリセットするか否かについて申請者は検査者と協議すべきである。

2） 型式認証取得後

申請者の対応は以下の通りとなるが、図 4.7-2 に補足として対応フローを記述する。

型式認証等を既に取得した型式の無人航空機にあっては、型式認証書類の内容に変更が生じた 場合、当該型式の型式認証等保有者は速やかに変更の内容を航空局に連絡し、型式認証の変更に 係る承認申請を行うこと。 型式認証書類に変更が生じるような変更は、原則として型式認証の変更の承認対象となる。型 式認証の変更の区分及び内容は、次の表に定めるとおりとする。

変更の区分	*変更の内容*
その他の変更（大変更）	*下記に掲げる変更以外の変更*
軽微変更	*当該型式の無人航空機に係る塗装の変更その他これに類する 安全性及び均一性に影響しない設計又は製造過程の変更*

［引用:国土交通省 サーキュラー No.8-002］

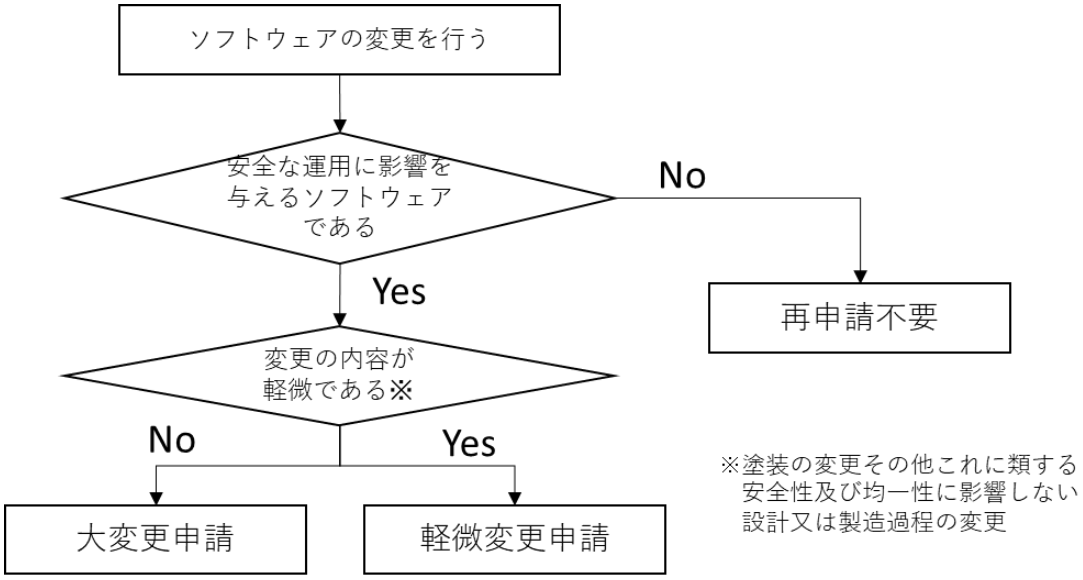


図 4.7-2 ソフトウェア変更時の対応フロー

3） セクション 110(a)に対する解説(ソフトウェアに対する試験による検証)

開発中および型式認証後に、ソフトウェアを変更する場合、まずは変更に伴う影響範囲を明らかする必要がある。確認の結果、必要なテストを検討して a)項に則りテストを実施する。

4） セクション 110(b)に対する解説(ソフトウェアの形態管理)

開発中および型式認証後に、ソフトウェアを変更する場合、セクション 110(b)に則り形態管理を実施する。

5） セクション 110(c)に対する解説(PR システムの導入および活用)

開発中および型式認証後に、ソフトウェアを変更する場合、(c) 項に則り不具合管理を実施する。

（4） 未認証の既存機体を型式認証取得する際の対応について

申請者が未認証の既存機体について、型式認証を取得することがあると想定して解説を行う。

1） セクション 110(a)に対する解説(ソフトウェアに対する試験による検証)

過去のテスト結果を引用できない場合は、セクション 110(a)に則り新たにテストを実施する。

2） セクション 110(b)に対する解説(ソフトウェアの形態管理)

未認証の機体においては、形態管理が実施されていないことがある。過去の再現が求められた場合は、セクション 110(b)に則った形態管理を開始した時点からの内容を提示する。

3） セクション 110(c)に対する解説(PR システムの導入および活用)

未認証の機体において、テスト記録は残っており、不具合が存在した記録があるが、その“不具合管理の記録”がない場合、再テストで不具合の修正が確認されていても、確実に修正されていることの確認が重要と考える。再テストなどを実施して不具合が修正されていることを確認し、レポート作成などで示せれば良いと考える。

5 今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定） 項目は以下の通り。

5.1 ソースコードを入手できない場合の扱いについて

4.7(1)において、現時点での記載を行ったが、ソースコードが入手できない場合の脆弱性対策、検証時に不具合が発生した際の対応などについて課題が残っている認識である。それ故、セクション 110(b)だけでなく、セクション 110(a)、(c)項における影響も併せて引き続き議論する必要がある。

さらに COTS(システム、ソフトウェア)、フリーウェアなどは市場実績も踏まえて、採用可否を検討する必要があると考えているが、深い議論まで行えていないため引き続き議論する必要がある。

5.2 PDI File の扱い

4.7(2)において、現時点での記載を行ったが、ライター間でも深い議論ができておらず、一般的なことは記載できている認識であるが、PDI 自体の詳細解説について図なども活用しながら解説を行う必要があると考えている。

5.3 110 ソフトウェアにおける PLD、FPGA および ASIC の扱いについて

PLD、FPGA および ASIC はロジックを持つハードウェアであるため、ソフトウェアと同様の性質を持つ。したがって、セクション 110 の範疇であるというレビュアーコメントも頂いているが、セクション 110 内で統一の見解を持てていない。 現状、本解説書では対象外と記載しており、引き続き議論が必要である。

Appendix 1 ソフトウェア適合性証明計画書 表紙記載例

ソフトウェア適合性証明計画書

〇〇年●●月〇〇日

〇〇〇〇株式会社
〇〇〇部〇〇〇課
担当:(申請者 氏名)

記

- 安全に影響を与えるソフトウェア一覧 1部
- 適合性証明計画日程概略 1部
- 適合性証明計画表 1部
- 自己宣言書 1部

改定来歴

Eddition No.	変更箇所	変更内容	発行日
1.00	-	初版	〇〇年●●月〇〇日

Appendix 2 安全に影響を与えるソフトウェア一覧 記載例

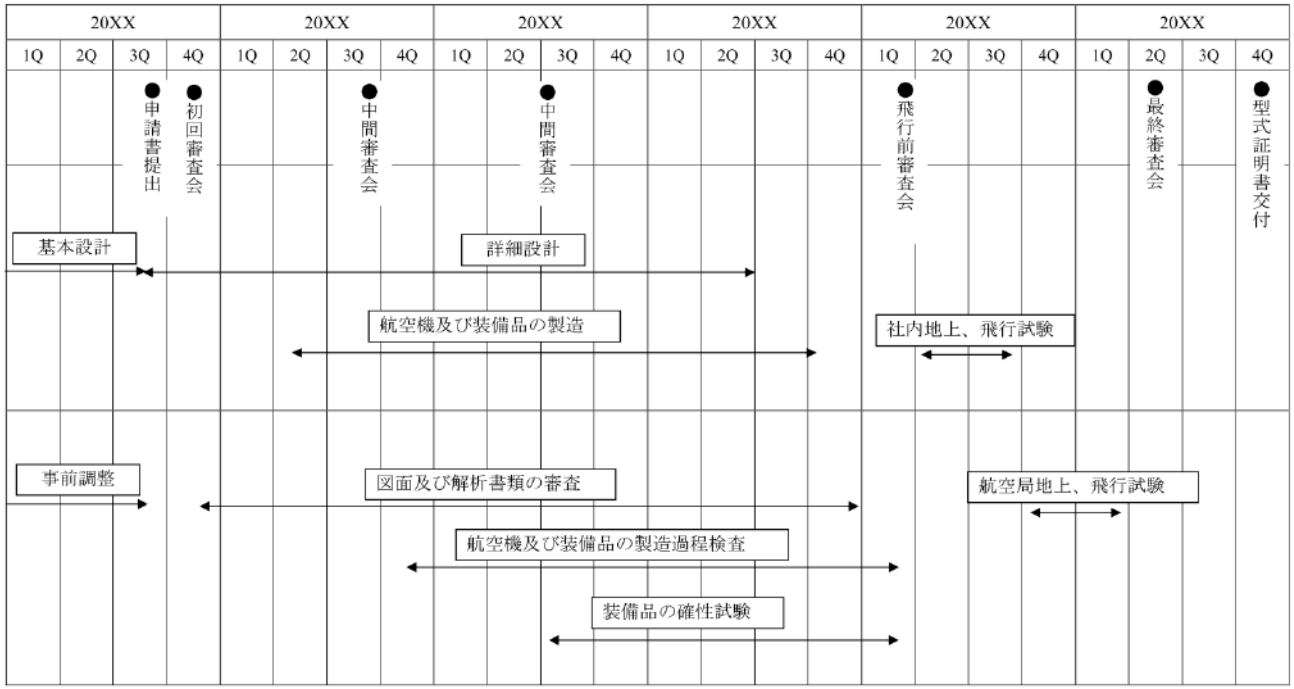
ソフトウェア名	バージョン	開発	搭載ハードウェア	適否	判断基準	備考
Aaaa	Ver1.000	○○システム株式会社	プロポ型番	適	○○○を○○すると、○○○となるため。	
Bbbb						
Cccc						
Xxxx						
Yyyy						
Zzzz						

Appendix 3　ソフトウェア適合性証明計画日程概略　記載例

○○ソフトウェア　適合性証明計画　日程概略

（設計及び製造に関する概略の日程の一例）　　別添 1

20XX 年 XX 月 XX 日　現在



1－307 (6)

Appendix 4 ソフトウェア適合性証明計画表 記載例

○○ソフトウェア 適合性証明計画表

YYYY 年 MM 月 DD 日 現在

基準項目	活動	適否	証明方法	適合性証明文書		関連文書		備考	進捗状況	担当
				管理番号	名称	管理番号	名称			
	②	③	④	⑤	⑥			⑦		⑧
(a)	ベーステスト	適	実技テスト	M001	xxx テスト仕様書	S001	xx システム仕様書			申請者
						S002	xx 要件定義書			申請者
(b)	形態管理	適								
(c)	不具合管理	否								

① :適用基準などに掲げられた項目番号を記載すること。

② :①の項目番号に対応した活動項目名を記載すること。

③ :今回の型式証明または型式設計変更にて証明する場合、以前に証明した内容が有効と判断する場合または同等性により証明する場合は「適」を記載し、未装備などの理由により証明が必要でない場合は「否」を記載すること。

④ :③にて「適」と判断した場合、図面、解析またはテストなどの証明方法を記載すること。

⑤ ,⑥:④にて提案した証明方法にしたがって作成した文書または図面番号およびそれらの名称を記載すること。 ただし、適合性証明計画には当該内容は未記入でよい。

⑦:③にて「適」と判断した場合はその証明概要を記入し、「否」と判断した場合はその理由を記載すること。

⑧:適合検査およびテスト立会を航空局と設計検査認定事業場で役割分担する場合、希望する分担を記載すること。

Appendix 5　宣言書記載例

自己宣言書

文書番号：No.001-0001
文書発行日：2023.09.01

【発行者の名称】　xxx 株式会社
【発行者の住所】　愛知県名古屋市 aaa　123-456　○○ビル 5F

【宣言の対象】
　　製品名：　　第二種　無人航空機 zzz
　　型式：　　AAA-01

上記の宣言の対象はサーキュラーNo.008 にて規定されるセクション 110　ソフトウェア要件へ適合している。

○○ソフトウェア　Ver.aaaa（開発元：xxx 株式会社）

△△ソフトウェア　Ver.bbbb（開発元：yyy 株式会社）

□□ソフトウェア　Ver.cccc （開発元：株式会社 zzz）

署名

【問い合わせ先】　xxx 株式会社 yyy 部
【代表者役職・氏名】　yyy 部部長　テスト受け太郎

Appendix 6 ソフトウェア適合性証明完了報告書 記載例

○○ソフトウェア 適合性証明完了報告書 TBD

YYYY 年 MM 月 DD 日 現在

基準項目	活動	適否	証明方法	適合性証明文書		備考	確認結果
				管理番号	名称		
①	②	③	④	⑤	⑥		
(a)	ベーステスト	適	実技テスト	M001	xxx テスト仕様書		
(b)	形態管理	適					
(c)	不具合管理	否					

署名

923

924 # Appendix 7 各セクション特有の用語集

925

用語	解説	出展
オブジェクトコード	コンピュータプログラムの低水準な表現形式のこと。通常はターゲットコンピュータが直接利用できる形式ではない。プロセッサへの命令情報に加えて、リロケーション情報も含まれている	DO-178C, ANNEX B, GLOSSARY
Commercial-Off-The-Shelf (COTS) software	ベンダーが公開カタログリストを通じて販売する市販のアプリケーションのこと。また、特定のアプリケーション向けに開発された契約交渉済のソフトウェアは COTS ソフトウェアではない	DO-178C, ANNEX B, GLOSSARY
サプライヤ	商品や部品、サービスなどの供給者のことであり、申請者によって特定の適合性証明活動の責任が移譲された、申請者とは独立した組織のこと	https://library.musubu.in/articles/35302
システム	定義された機能を成し遂げるために、相互に作用するハードウェアおよびソフトウェアを組み合わせたもの	INCOSE で定義された内容をアレンジ
ソースコード	アセンブリ言語や高水準言語などのソース言語で書かれたコードのこと。ソースコードは、アセンブラやコンパイラに入力するため、機械可読形式である	DO-178C, ANNEX B, GLOSSARY
ソフトウェア	無人航空機および関連システムにロードされる実行可能オブジェクトコードとパラメータファイルのこと。場合によっては、関連する文書とデータを含む	「DO-178C, ANNEX B, GLOSSARY」をベースに、本解説書向けにアレンジ
ソフトウェアテスト	ソフトウェアテスティングは、プログラムが、日常生まれる無限の実行ドメインから適切に選択されたテストケースの有限集合のうえで行われる、期待される振る舞いを提示するための動的検証から構成される	SWEBOK V3.0 テストの定義
ソフトウェアバグ	ソフトウェアプログラムに作り込まれた欠陥のこと	情報システム用語事典
テストケース	入力値、実行事前条件、期待結果、そして、実行事後条件のセットで、特定のプログラムパスを用いることや特定の要件が満たされていることを検証することのような、特定の目的またはテスト条件のために開発されたもの	Standard Glossary of Terms Used in Software Testing ISTQB
パラメータ データ アイテム ファイル(PDI ファイル)	Parameter Data Item File のこと。 ターゲット コンピュータの処理装置(processing unit)によって直接使用できて、パラメータ データ アイテムを有するファイルである	DO-178C, ANNEX B, GLOSSARY
パラメータ データ アイテム (PDI)	実行可能オブジェクト コードを変更せずにソフトウェアの動作に影響を与えることができるデータの集合体のこと	DO-178C, ANNEX B, GLOSSARY

ベースライン	ある時点における承認された 1 つ以上の形態アイテムのこと。ベースラインは、それ以降の開発の基準となる	DO-178C, ANNEX B, GLOSSARY -
形態アイテム(またはアイテム)	形態管理において 1 つの単位として扱われるソフトウェアの要素のこと。例えば、要求文書、ソースコード、テスト手順書などである	DO-178C, ANNEX B, GLOSSARY - Configuration item を参考に若干アレンジ
実行可能オブジェクトコード（EOC）	Executable Object Code のこと ターゲットコンピュータの処理装置が直接使用できる形式のコードである。それ故、ターゲットコンピュータのハードウェアにロードされるビルドされたバイナリイメージである。	DO-178C, ANNEX B, GLOSSARY

926

Appendix 8 関連文書

(1) サーキュラー No.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領、2022 年 9 月 7 日（国空機第 456 号）、https://www.mlit.go.jp/koku/content/001520547.pdf

(2) サーキュラーNo.8-002 無人航空機の型式認証等の手続き、2022 年 12 月 2 日（国空機第 645 号）、https://www.mlit.go.jp/koku/content/001574424.pdf

(3) 無人航空機の型式認証等の取得のためのガイドライン、2022 年 11 月 2 日、https://www.mlit.go.jp/common/001574425.pdf

(4) RTCA DO-178C / EUROCAE ED-12C – Software Considerations in Airborne Systems and Equipment Certification

(5) ASTM F3153-15, Standard Specification for Verification of Avionics Systems

(6) ASTM F3153-22, Standard Specification for Verification of Avionics Systems

Appendix 9 サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 110 ソフトウェアの構成員名簿(サブ WG 主査およびライター)を以下に示す。なお、レビュワーの講成員名簿は本冊(RMD、Rev.01)Appendix3 を参照すること。

タイトル	氏名	所属
主査	南 貴紘	株式会社電通総研(旧株式会社電通国際情報サービス)
ライター	金子 達哉	DNV ビジネスアシュアランスジャパン
ライター	榧野 尊	株式会社電通総研(旧株式会社電通国際情報サービス)
ライター	中川西 拓	株式会社 SClabAir
ライター	西岡 亮	株式会社ベリサーブ
ライター	矢口 勇一	公立大学法人会津大学

946

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

RMD-115 DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 115 サイバーセキュリティ 解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

表 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン（以降、「航空局ガイドライン」と呼ぶ）」内に記載されている「安全基準セクション 115 サイバーセキュリティ”（以降、「セクション 115」と呼ぶ）」に対する解説書である。

本解説書の目的は、安全基準に沿ったサイバーセキュリティの適合性証明計画書および適合性証明完了報告書作成に関して、「航空局ガイドライン」で示されている方法の解説および補足を行うものである。「航空局ガイドライン」で提示されている適合性証明案は一通りの活動を規定しているが、その活動を行うための要求の詳細や、活動に必要な前提条件や変数などは提示されていない。そのため、ReAMo PJ 無人航空機の認証に対応した証明手法の事例検討 WG 内 115 サブ WG サイバーセキュリティで議論された内容をもとに、安全基準に合致する適合性証明を実現するための「航空局ガイドライン」の解説と指針を提示することが目的である。

本解説書の構成は、国土交通省「サーキュラー No.8-001“無人航空機の型式認証等における安全基準および均一性基準に対する検査要領”（以降 「サーキュラー No.8-001」と呼ぶ）」、「サーキュラー No.8-002“無人航空機の型式認証の手続き”（以降 「サーキュラー No.8-002」と呼ぶ）」、および「航空局ガイドライン」の引用を行い、解説書として、安全基準に適合する要求リスト、活動リスト、プロセス、活動結果の出力としての文書リスト、適合のための手法、指針、および第二種型式認証に適用可能な手法例を提示することである。実際の適合性に対する認証行為は、型式認証や機体認証を申請する申請者が、対象とする運用に必要な機能安全の仮説を提示し、その仮説を証明するための指標と手法を決定し、それによって証明された内容を、検査者と確認していくという作業を行うものである。その仮説の与え方について指針を与えるものとして構成する。

2　対象の基準「サーキュラー」(引用)

「サーキュラー No.8-001」のセクション 115「サイバーセキュリティ」を以下に引用する。

> *・115 サイバーセキュリティ*
>
> *(a) 別のシステムと連携する無人航空機の機器、システムおよびネットワークは、無人航空機の安全性に悪影響を及ぼす意図的で許可されていない電子的な干渉から守られなくてはならない。セキュリティ対策は、セキュリティリスクが特定され、評価され、かつ、必要により緩和されていることを示すことによって確実になされなければならない。*
>
> *(b) 上記 (a) 項により必要とされる場合、セキュリティ対策が維持されるような手順および指示が ICA に含まれなければならない。*

3　「航空局ガイドライン」(引用)

「航空局ガイドライン」 安全基準　セクション 115「サイバーセキュリティ」の「基準の概要」、「適合性証明方法(MoC)」、「その他参考となる情報」を以下に引用する。

> *・115 サイバーセキュリティ*
>
> *<u>基準の概要</u>*
>
> *本基準は、無人航空機の安全性に悪影響を及ぼす意図的で許可されていない電子的な干渉から保護されることを要求するものです。*
>
> *<u>適合性証明方法(MoC):1、2</u>*
>
> *(a): <u>セクション 115 セキュリティ適合性証明計画</u> (MoC 1, 2)*
>
> *無人航空機が安全性に悪影響を及ぼす意図的で承認されていない電子的な干渉から保護されていることを示すため、リスクアセスメントを行い、セキュリティリスクを特定し、評価し、必要により緩和策を講じていることを提示します。*
>
> *本項を満たすためには、意図的で許可されていない電子的な干渉によって陥る、無人航空機の安全性に影響が及んだ事態(Threat Condition)をまず最初に定義します。例えば、「想定飛行範囲からの逸脱」が Threat Condition の一例として挙げられます。*
>
> *続いて、その Threat Condition の原因となる可能性のあるシステムを抽出します。システムはひとつだけとは限りません。例えば、想定飛行範囲からの逸脱であれば、一般に飛行管理システムと飛行制御システムのふたつが原因として考えられます。*
>
> *その次に、抽出したシステム内で Threat Condition を引き起こす可能性のある資産(Asset)を抽出します。例えば、前述の飛行管理システムと飛行制御システムであれば、その中の飛行計画データや飛行制御プログラムが改ざんされると Threat Condition を引き起こすと考えられる場合、飛行計画データと飛行制御プログラムが Asset になります。*

Asset の抽出と同時に、その Asset への入り口（Entry Point）となる境界(Perimeter)と、その外側の環境(Environment)がどういったものなのかを明らかにする必要があります。

続いて、セキュリティリスクアセスメントにより、どういったリスクがあるのかを特定し、その影響評価および必要に応じて緩和策を提示します。リスクアセスメントには様々な手法がありますが、一例として、抽出した Asset すべてに対し、その Asset ごとに Confidentiality(機密性)、Integrity(完全性)、Availability(可用性)の観点で悪影響を与えるシナリオ(Threat Scenario)を想定し、その影響評価を行うのも有効的です。また、シナリオには既知の脆弱性についても考慮する必要があります。なお、その評価の際はフライトフェーズ、影響を受ける対象(機体、操縦者、第三者など)ごとに評価を行うことを推奨します。例えば飛行計画データの完全性が改ざんで失われる場合、その Threat Scenario を考えると同時にそれの発生頻度(どの程度起こり得るか)を考えます。Threat Scenario の発生頻度と、Threat Condition の影響度を評価し、その結果、必要であれば緩和策(Security Measure)を考慮する必要があります。

最後にセキュリティレベルを維持するために運航者が順守すべき事項をセキュリティガイドラインにまとめます。

ここで、リスクアセスメントで考慮した Threat Scenario に対し、新たな脆弱性が発見され、シナリオに変更があった場合は、追加の評価が必要になります。

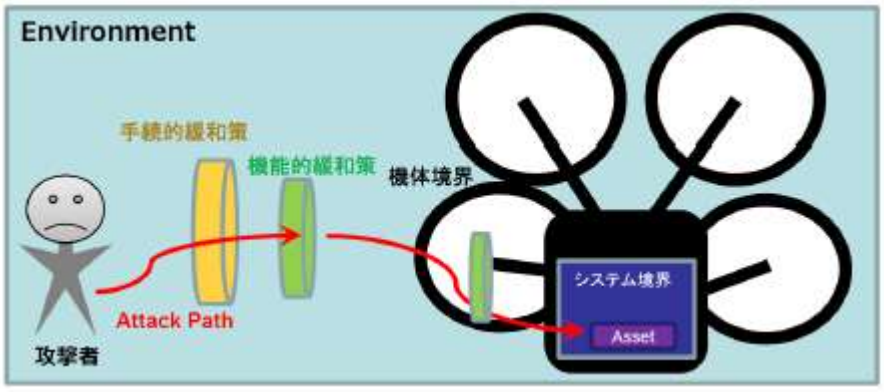
(a), (b): セクション 115 セキュリティ適合性証明完了報告書（MoC 1, 2）

(a)項の結果を完了報告書としてまとめるとともに、ICA に定めるセキュリティ対策の維持手順および指示(セキュリティガイドライン)も完了報告書に記載します。

その他参考となる情報

以下は Environment、Perimeter(機体境界およびシステム境界)および資産(Asset)の概念図です。

有人航空機におけるセキュリティリスク評価は、RTCA DO-326 に基づき行われるため、必要により参照することを推奨します。



4　解説書

4.1 本解説書について

(1)　本解説書の論理

本解説書では、以下の構成により解説を行う。

サイバーセキュリティ適合性証明を行うためには、「サーキュラー No.8-001」第Ⅱ部 安全基準の文章で言及している対象を明確化する必要がある。

そこで、4.2 章では、サイバーセキュリティ適合性証明を行うにあたり、適合性証明対象を明確化するために、「サーキュラー No.8-001」第 II 部 安全基準を読み解く。そこから読み解かれる要求と、型式認証に必要な要求である「サーキュラー No.8-002」に合致するための文書の要求を列挙し、それぞれに関連した活動項目を抽出する。

4.3 章では、「航空局ガイドライン」で提示されている活動を参照しながら、4.2 章で抽出した活動項目の概要を記述する。4.4 章では、「サーキュラー No.8-001」と「航空局ガイドライン」の内容の一般化に加えて、参照を推奨されている RTCA DO-326A に基づくサイバーセキュリティアセスメントの前提条件とプロセス、ならびに活動と出力文書の整理を行う。

最後に、4.5 章にて、各活動で実施されるべき個別の設定値の導出手法やアセスメント手法などを記述する。

(2)　本解説書の使用法

本解説書は、実際にサイバーセキュリティ適合性証明を行い、型式認証を受ける申請者の理解のために構成されている。そのため、教科書的な要求と活動の定義の部分と、実践的なプロセスと手法について、記述している章を分けている。具体的なプロセスの記述は 4.4(2)項および図 4.4-2 セクション 115 の認証活動プロセスに記載している。

- 教科書的な要求と活動の定義を理解し、他のサイバーセキュリティアセスメントの標準を用いてサイバーセキュリティ適合性証明を行う場合は 4.2 章、4.3 章および 4.4 章を用いて行う活動の確認を行うことができる。
- 実践的なプロセスと手法を参照してサイバーセキュリティアセスメントを行う場合は、4.4 章および 4.5(2)項を用いてサイバーセキュリティ適合性証明を行うことができる。

なお、本解説書で引用および参照されている文書は、基本的にその文書を購入せずとも本解説書で完結できるように記載しているが、詳細を知りたい場合は別途入手および購入を推奨する。

4.2 サイバーセキュリティ適合性証明のための要求

> *無人航空機が安全性に悪影響を及ぼす意図的で承認されていない電子的な干渉から保護されていることを示すため、リスクアセスメントを行い、セキュリティリスクを特定し、評価し、必要により緩和策を講じていることを提示します。*
>
> *［引用: 航空局ガイドライン］*

サイバーセキュリティ適合性証明を行うためには、「サーキュラー No.8-001」で記載されている安全基準に合致していることが必要である。また、セキュリティリスクアセスメントを行うための具体的な要求は安全基準から導出されるものである。加えて、適合性証明の手続きは「サーキュラー No.8-002」に記されている。

本項では、セキュリティ適合証明のための要求を、安全基準から 5 項目、「サーキュラー No.8-002」から 2 項目抽出し、計 7 項目を要求として抽出する。また、各要求に紐づく活動を列挙する。

(1) システム環境の明確な記述

> *別のシステムと連携する無人航空機の機器、システムおよびネットワークは～*
>
> *［引用: サーキュラー No.8-001］*

この要求で定義すべき項目は、対象とするシステム全体の構成およびネットワーク構成を記述によって定義し、全体像を明らかにすることである。

- 活動 1: システムの範囲の決定と記述
- 活動 2: ネットワークおよびデータフローの記述
- 活動 3: 正常な運用におけるインターフェースとアクターの記述

「セクション 115」の安全基準の中には、明示的にこの要求を示されていない。参考にしたと思われる「FAA D&R. 115 Cyber Security」を参照すると、

> (a) UA equipment, systems, and networks, addressed separately and in relation to other systems, ～
>
> *［引用: FAA D&R. 115 Cyber Security］*

との記述がある。このため、システム環境の明確な記述は、無人航空機システムの全体像を把握し、セキュリティリスクアセスメントのために必要な情報の掌握を行う重要な要求であるとわかる。

(2) サイバーセキュリティの範囲と脅威、攻撃者の定義

> *無人航空機の安全性に悪影響を及ぼす意図的で許可されていない電子的な干渉から守られなくてはならない。*
>
> *［引用: サーキュラー No.8-001］*

この要求は、無人航空機の安全性に悪影響を及ぼす意図的で許可されていない電子的な干渉（IUEI）から無人航空機システムを守るために、サイバーセキュリティの範囲と始点および終点の観点でセキュリティ要件[1]を定義し、セキュリティリスクアセスメントのための要素の列挙を行うことを求められている。

- 活動 4: 最上位の脅威事象と評価尺度の定義
- 活動 5: 攻撃者と攻撃可能なインターフェースの抽出
- 活動 6: セキュリティ環境とセキュリティ境界の設定

この要求を充足するためには、無人航空機システム全体から、サイバーセキュリティで保護するべきセキュリティ環境(Security Environment)を定義し、セキュリティ境界(Security Perimeter)を設定し、その環境の中で脅威源(Threat Source)と脅威事象(Threat Condition)が提示されている必要がある。

セキュリティ環境は資産(Assets)がその機能を実行するシステムの外側に位置するユーザーや攻撃者(Attacker)、外部との接続環境を含むセキュリティ状況のことである。セキュリティ境界は資産の内部のセキュリティ状況とセキュリティ環境との境目をいう。セキュリティの範囲はそれらの内部および外部のセキュリティ状況を含めた範囲をいう。

脅威源はすべての攻撃者を含むアクター(Actor)であり、脅威事象は無人航空機の安全性が失われている状態である。脅威事象については、「セクション 300 耐久性および信頼性(以降、「セクション 300」と呼ぶ)]や、「セクション 305 起こり得る故障(以降、「セクション 305」と呼ぶ)」などで実証されるべき『安全性』が失われないようにするべきである。加えて、セキュリティに関する脅威の特性である、機密性、完全性、可用性（CIA）について考慮されたセキュリティリスクの評価尺度について定義される必要がある。このために、脅威事象が起こりうるセキュリティリスクについて、定量的または定性的に数値化し、評価尺度を構成する必要がある。

（3） サイバーセキュリティリスクの特定

> *セキュリティ対策は、セキュリティリスクが特定され、*
>
> *[引用: サーキュラー No.8-001]*

この要求では、サイバーセキュリティの範囲、すなわちセキュリティ環境、セキュリティ境界、脅威源と脅威事象が特定されているところから、セキュリティリスクとなる個別の資産やリスク重大度(Severity)が特定され、リスクアセスメントの実施のためのすべての脅威シナリオ(Threat Scenario)が特定されることを要求している。

- 活動 7: 資産とリスク重大度の定義
- 活動 8: 具体的な脅威の抽出と脅威レベルの評価
- 活動 9: 既存の緩和策の抽出と防御レベルの評価

[1] Security Requirements は漠然とした『要求』ではなく、機能などを実現するために必要な『要件』と捉えられるので、『セキュリティ要件』としている。

- 活動 10: *脅威源から脅威事象が引き起こされる脅威シナリオの同定*

サイバーセキュリティリスクは、*脅威源*が脆弱性(Vulnerability)を発見してシステムに侵入し、*脅威事象*を引き起こす資産に到達できることで発生する。また、発生したセキュリティリスクの影響度(Impact)によって、そのセキュリティリスクが深刻なものであるかを特定することができる。サイバーセキュリティリスクは、最終的に*脅威源*から*脅威事象*までどのように到達するかを示すため、すべての*脅威シナリオ*が特定されている必要がある。また、ここでいう活動 8 や活動 9 の評価は、個別の*脅威*、緩和策に対する評価(スコアリング)を意味する。

(4) 特定されたセキュリティリスクの評価

> *セキュリティ対策は、～ 評価され、*
>
> *[引用: サーキュラー No.8-001]*

この要求では、特定され、導出された*脅威シナリオ*に対して、セキュリティリスクアセスメントを実施し、リスクの起きる確率または頻度について評価を行う。すべての*脅威シナリオ*について、セキュリティリスクアセスメントを実施した結果、そのリスクが受容可能かどうかの判断が行われることを要求している。

- 活動 11: *脅威シナリオ*中に含まれる既存の緩和策を含めたリスクの評価

セキュリティリスクを正しく評価するために、要求 2 で定義されたセキュリティリスクアセスメントの手法と評価尺度を用いて全体の評価を行い、各*脅威シナリオ*がリスク受容可能かを評価する。セキュリティリスクアセスメントの観点の中には、*脅威事象*の起きる生起確率や、攻撃者のスキルレベルに基づく到達可能性などが考えられる。そのほか、定性的・定量的表現によって資産のセキュリティ重大度、*脅威*レベル、セキュリティ保護レベル、脆弱性レベルなどが定義されて、個別の*脅威シナリオ*や緩和策に対して適切に評価される必要がある。この個別の評価を用いて、*脅威シナリオ*全体に対する評価を行う。個別の評価のために、追加で脆弱性の発見難易度や攻撃の再現性、既存の緩和策の効果などの、その他の指標が必要となる場合がある。

(5) 評価に基づく緩和策の実施と記述

> *セキュリティ対策は、～ かつ、必要により緩和されていることを示すことによって…*
> *上記（a）項により必要とされる場合、セキュリティ対策が維持されるような手順および指示が ICA に含まれなければならない。*
>
> *[引用: サーキュラー No.8-001]*
>
> *2.2.1 項（l）その他参考事項を記載した書類(提出時期:現状についての検査実施前）その他参考事項を記載した書類とは、次の書類をいう。 a. 安全性を確保するための管理の計画*
>
> *[引用: サーキュラー No.8-002]*

この要求は、セキュリティリスクアセスメントの結果で得られた各*脅威*イベントのセキュリティリスクの評価に基づいて、受容不可能なリスクを持つイベント(不許可イベント)が発生する場合には適切に緩

和策が提示され、その緩和策を追加要求として機体やシステムの設計にフィードバックし、再度セキュリティリスクアセスメントを実施することで、正しく緩和されていることを示すことを求めている。

- 活動 12: 評価されたリスクに対する緩和策の追加
- 活動 13: 残存する脆弱性とセキュリティリスクの評価
- 活動 14: 点検・整備・運用などで行われる緩和策についての記述
- 活動 15: セキュリティリスクアセスメントのバージョン管理

特定の脅威イベントが受容不可能なリスクを持つ場合、受容可能となるまで必要な緩和策を提示し、すべての脅威イベントのリスクが受容可能となることが証明されるべきである。また、実際に緩和策が講じられた場合に、その緩和策が十分機能していることを証明する必要がある。この緩和策は、技術的要求のみならず、運用的な観点で緩和策が講じられることがあり、セキュリティ対策を維持するための手順や指示があるならば、ICA に記述することが要求される。

加えて、どのようにセキュリティリスクアセスメントを行い、適合するように機能や指示が追加されたかを管理するために、セキュリティリスクアセスメントについてのバージョン管理も求められる。最終的に、残存する脆弱性を検査し、セキュリティリスクがすべて受容可能であることを示す必要がある。

なお、ICA にはその他事項として、安全性を確保するための管理の計画が必要である。このために、継続的なセキュリティ品質の維持計画について、セキュリティリスクアセスメントが供用後に継続的に実施可能なように、バージョン管理も必要である。

（6） セクション 115 適合性証明計画書の矛盾のない記述

> *セキュリティ対策は、 ～ 確実になされなければならない。*
>
> *［引用: サーキュラー No.8-001］*
>
> *2-1-3 項 ⑥ 適用基準および適合性証明計画の原案*
>
> *［引用: サーキュラー No.8-002］*

この要求は、適合性証明計画書について、要求 1～5 までの活動についての計画が正しく設計され、安全基準に適合するための活動が、他のセクションに記載される情報との間で矛盾なく記述されていることをチェックすることである。なお、この要求は、「サーキュラー No.8-002」に記載されているとおり、原案は事前調整の段階から必要である。

- 活動 16: リスクアセスメントで利用する証明手法・手順についての記述

セクション 115 適合性証明計画書は、安全基準に合致するためにどのような評価基準、手法、活動を用いて安全基準に適合するかの計画を示すものである。評価基準や手法、活動を定義するには、システムの記述とセキュリティ環境、脅威源や脅威事象などが適切に列挙されており、その上で評価基準と手法、活動が選定されていることが望ましい。

（7） セクション 115 適合性証明完了報告書の矛盾のない記述

セキュリティ対策は、 ～ 確実になされなければならない。

［引用: サーキュラー No.8-001］

6-1 項 型式認証書類: 証明の管理に必要な書類等(以下「型式認証書類」という。)について、適合性証明で確認された設計データが的確に反映できるよう必要な管理がなされなければならない。

［引用: サーキュラー No.8-002］

この要求は、適合性証明計画書に基づいて、適合性証明が行われ、完了報告書が記述されるにあたって、適合性証明計画書で記載されている解析手法や個別に行われるセキュリティ緩和策へのテスト方法と、実際に行われた解析結果、テスト結果に矛盾がないかを確認し、記述し、すべての緩和策について対処されていることを記述することである。

- 活動 17: すべての脅威シナリオについてのリストの作成
- 活動 18: すべてのセキュリティリスク緩和策についてのリストの作成
- 活動 19: すべてのセキュリティリスク緩和策についての適合性評価の結果の記述

セクション 115 適合性証明完了報告書は、セクション 115 適合性証明計画書で示されたコンプライアンスマトリクスで提示されている活動がすべて完了し、適切に処理されていることを報告する。そのために、安全基準に合致する活動として、脅威シナリオが受容可能かについてのリスト、セキュリティリスク緩和策が十分機能しているかの証明を表すリストと、セキュリティリスクアセスメントプロセスを正しく実行し、完了したことを示す証拠を添えて、報告されるべきである。

4.3 サイバーセキュリティ適合性証明のための活動

サイバーセキュリティの適合性証明方法については、「航空局ガイドライン」には以下のとおりに記載されている。

適合性証明方法(MoC):1、2
1: 設計図面 / Design/Data Review
2: 解析・評価 / Calculation/Analysis

［引用: 航空局ガイドライン］

サイバーセキュリティ適合性証明は基本的に設計図面と解析・評価を行って証明するものである。これを前提として、各サイバーセキュリティ適合性証明を行うための活動を定義する。なお、活動は 19 項目掲載してあるが、この活動における順序性について、特に強制されないものとする。

(1) システムの範囲の決定と記述

1: 設計図面 / Design/Data Review
(ウ) 続いて、その Threat Condition の原因となる可能性のあるシステムを抽出します。システムはひとつだけとは限りません。

［引用: 航空局ガイドライン］

型式の対象となるシステムの記述は本来「セクション 001 CONOPS(以降、「セクション 001」と呼ぶ)」で記述されるべきである。このシステムの記述には、システム全体の物理的・論理的構成、機器接続構成図などが示されている必要がある。機体の物理的な構成および構造に関しては各セクションに分散して記述されるため、それぞれのセクションで何が記述されるかを意識しなければならない。以下にセクションと記述される内容の概略を列挙する。

- 「セクション 100 無人航空機に係る信号の監視と送信(以降、「セクション 100」と呼ぶ)」に通信機器などの情報が含まれる。
- 「セクション 105 無人航空機の安全な運用に必要な関連システム(以降、「セクション 105」と呼ぶ)」では安全な運用に必要な、機体以外のシステムについての情報が含まれる。
- 機体システムおよび関連システムにおけるソフトウェア機能などの構成は「セクション 110 ソフトウェア(以降、「セクション 110」と呼ぶ)」にてソフトウェアの形態管理がなされている。
- 機体システムおよび関連システムに関して機体の安全に資するシステムコンポーネントおよび機能の特定については「セクション 135 重要な部品 (フライトエッセンシャルパーツ) (以降、「セクション 135」と呼ぶ)」で行われる解析を参照することができる。
- その他、灯火、表示、自動操縦系統やカメラ、飛行諸元の記録など、情報技術が含まれるもので安全に直接寄与する機体側のシステムは「セクション 140 その他必要となる設計および構成(以降、「セクション 140」と呼ぶ)]に記述される。

「航空局ガイドライン」で指定されるシステムの範囲は無人航空機の安全な運用に係る部分である。ここでいう安全な運用とは、「航空局ガイドライン」に示される『制御不能』や『計画外飛行』という脅威事象が発生した際に、地上の管理外の対象物件に対して危害が及ばない運用である。これらの運用に関するシステムの範囲の記述は「セクション 105」で記述されるべきである。一方で、「セクション 115」で記述するべき情報としては、航空局ガイドラインセクション 115 における Environment、Perimeter(機体境界及びシステム境界)及び資産(Asset)の概念図に示されるとおり、運用を行う環境の中で、どのように攻撃を受けるかであることから、まずは「セクション 001」で記述されているシステムの全体像を捉えておくのが望ましい。

「セクション 115」で直接的に参照が必要なシステムの物理的な記述として、システムブロック図、内部ブロック図などである。また、振る舞いの記述として、ユースケース図によるシステムとステークホルダーとの関係性の記述、アクティビティ図およびフロー図による業務プロセスの記述は、セキュリティアセスメント時に非常に有益である。

第二種型式認証において、システム構成図の粒度は、物理コンポーネントレベルのシステム構成図であっても、インターフェースの明確化およびインターフェースでやり取りされる電子情報の種類・定義域・値域が指定されていれば過不足ない。また、機能ブロックレベルのシステム構成図があれば、より精密に脅威事象につながる経路を導出することができる。

（2） ネットワークおよびデータフローの記述

> *1: 設計図面 / Design/Data Review*
> *（イ）本項を満たすためには、意図的で許可されていない電子的な干渉によって陥る、無人航空機の安全性に影響が及んだ事態(Threat Condition)をまず最初に定義します。*
> *[引用: 航空局ガイドライン]*

システムの利用方法、および構成図が記載されていれば、それに基づいてネットワークの記述やデータの流れを、ネットワーク図やデータフロー図などを用いて記述する。第二種型式認証においては、物理的なコンポーネントレベルもしくは機能ブロックレベルで記述されているのが望ましい。なお、ネットワーク図やデータフロー図は設計段階で示され、無人航空機の安全な運用のための安全解析に用いられる可能性が高く、「セクション 001」や「セクション 105」、「セクション 135」の成果物を利用可能である。

ネットワーク図およびデータフロー図で記述される内容についての注意点は、サブシステムごとのインターフェースと、そこで取り扱われるデータの特性、値域、頻度などである。特に、フライト時のみならず、地上待機時や保管時などで取り扱われるインターフェースやデータにも注意する必要がある。

（3） 正常な運用におけるインターフェースとアクターの記述

> *1: 設計図面 / Design/Data Review*
> *（イ）本項を満たすためには、意図的で許可されていない電子的な干渉によって陥る、無人航空機の安全性に影響が及んだ事態(Threat Condition)をまず最初に定義します。*
> *（オ）Asset の抽出と同時に、その Asset への入り口 (Entry Point) となる境界 (Perimeter) と、その外側の環境(Environment)がどういったものなのかを明らかにする必要があります。*
> *（カ）…なお、その評価の際はフライトフェーズ、影響を受ける対象(機体、操縦者、第三者など)ごとに評価を行うことを推奨します。*
> *[引用: 航空局ガイドライン]*

型式認証において、すべてのインターフェースが指定され、記述されている必要がある。これに関して、どのタイミングでアクセス可能か(保管時、地上待機時、フライト中)について記述される必要がある。加えて、各インターフェースでどのような情報がやり取りされるかについて記述されていることが望ましい。

また、すべてのインターフェースに対して、どのようなアクターが存在するかを考慮する必要がある。これについて、正規にインターフェースにアクセスすることの可能なアクターについての記述を行う。なお、アクターが正規にインターフェースにアクセスする場合に必要な情報(ログイン情報や資格情報など)にも記述されていることが望ましい。

加えて、これらの正常な運用は、フライトフェーズによってユースケースが異なる可能性があることから、保管時、運用前、運用中、運用後などのフライトフェーズに分けて記載することが望ましい。

活動 3 における記述はあくまで正常に動作している場合の記述までである。悪意の記述は活動 6 で行う。

（4） 最上位の脅威事象と評価尺度の定義

> *2: 解析・評価 / Calculation/Analysis*
> *（イ）本項を満たすためには、意図的で許可されていない電子的な干渉によって陥る、無人航空機の安全性に影響が及んだ事態（Threat Condition）をまず最初に定義します。例えば、「想定飛行範囲からの逸脱」が Threat Condition の一例として挙げられます。*
> *［引用: 航空局ガイドライン］*

脅威事象（Threat Condition）とは、機体に対する安全性が失われ、リスクのある運用が行われる可能性のある事象である。機体に対する安全性の評価は、「セクション 135」などで行われるが、これに加えて、セキュリティでは『攻撃者による正常系を用いた操作（ハイジャック）』などが考慮されるべきである。

脅威事象の把握に関しては、想定するフライトのユースケースから機能安全解析を用いて行うのが推奨される。第二種型式認証においては、地上レベルで立ち入り管理を施された空域を用いての運用であり、脅威事象としては『制御不能』または『想定飛行範囲からの逸脱』であるといえる。脅威事象を引き起こすリスクの代表的なものは以下のとおりである。

- 制御のハイジャック
- 攻撃により引き起こされる、管理空域からの逸脱を引き起こすセンサ系・制御系の不具合
- 攻撃により引き起こされる、第 3 者物件の墜落を引き起こす制御系、プログラムの不具合
- 攻撃により引き起こされる、通信の不具合および通信経路への不正な侵入
- 電子機器への不正侵入
- 電子機器本体の過負荷による攻撃

加えて、脅威事象に対して、リスクアセスメントのための活動目標となる評価尺度の定義をここで行う。脅威事象に対して、その脅威事象がどの程度リスクが重大であるかについての評価尺度を定義する必要がある。評価尺度については、脅威事象が発生することを故障として捉えた形で、単位時間におけるオンデマンド故障確率（Probability Failure on Demand per Hour, PFH）を用いることも可能であるが、定性表現として、3 段階、5 段階の指標を定義することも可能である。また、このリスク重大度（Severity）から、資産が奪われる場合の脅威レベル（Level of Threat）などの定義を行う必要があるため、このような評価尺度の設計もこの活動で必要となる。なお、具体的に脅威分析を行う場合は、脅威のモデリング手法としていくつかの手法が挙げられることから、既存のモデリング手法を適切に用いて脅威分析を行うべきである。

（5） 攻撃者と攻撃可能なインターフェースの抽出

> *2: 解析・評価 / Calculation/Analysis*
> *（オ）Asset の抽出と同時に、その Asset への入り口 （Entry Point）となる境界（Perimeter）と、その外側の環境(Environment)がどういったものなのかを明らかにする必要があります。*
>
> *[引用: 航空局ガイドライン]*

活動 3 にて、正常な運用が行われる場合に対するインターフェースやアクターの記述を行ったが、活動 5 ではその記述に重ねて攻撃者と攻撃可能なインターフェース、つまりアタックサーフェス(Attack Surface)を抽出する。

セキュリティリスクとは、攻撃者が脆弱性を含む脅威としての干渉口を発見し、そこから資産まで到達可能である場合に引き起こされる損害の程度のことである。そのため、セキュリティリスクアセスメントでは、攻撃者の性質の特定と、攻撃可能な脆弱性を含む脅威を列挙する必要がある。この攻撃可能な脆弱性を含む脅威源は、すべてアクセス可能なインターフェースに付随するため、セキュリティ境界と交差するインターフェースはすべて脆弱性であると言える。

インターフェースが守るべき資産に紐づく場合は脅威であると認められる。資産は先ほどの脅威事象に紐づくものであり、サイバーセキュリティに関しては流通するデータや機体管理を行うパスワード、および制御を行うソフトウェア本体などが資産である。

これらの情報が攻撃者と結びつく場合、リスクが発生するが、型式認証では、実際のユースケースから、どれほどの敵意を持っている攻撃者が存在するかについて想定するべきである。攻撃者はスキルレベルによって脅威レベルは異なる。また、攻撃対象となるユースケースによっても脅威レベルは異なる。こうした、対策されるべき『敵意のレベル』によってアクセス頻度が設定される必要がある。想定する敵意のレベルについては、型式認証を受ける申請者が、検査者と議論しながら適正に決められる必要がある。

（6） セキュリティ環境とセキュリティ境界の定義

> *1: 設計図面 / Design/Data Review*
> *（ウ）続いて、その Threat Condition の原因となる可能性のあるシステムを抽出します。システムはひとつだけとは限りません。例えば、想定飛行範囲からの逸脱であれば、一般に飛行管理システムと飛行制御システムのふたつが原因として考えられます。*
> *（オ）Asset の抽出と同時に、その Asset への入り口 （Entry Point）となる境界（Perimeter）と、その外側の環境(Environment)がどういったものなのかを明らかにする必要があります。*
>
> *[引用: 航空局ガイドライン]*

システム全体の記述に対して、機体の安全に資するシステムの範囲のうち、セキュリティで守られるべき境界を定義して、開発するシステムで担保するべきセキュリティの範囲を最初に定義することで、

『何をどこから防御するのか』を明確化する必要がある。

「航空局ガイドライン」では、セキュリティ境界の設定は、脅威事象の定義の後で、その脅威事象に関連するサブシステムレベルで考察することが示されている。一方で、これらセキュリティ環境とセキュリティ境界の定義については、設計図面上での定義であることから、脅威事象の定義よりも先に対象とするセキュリティ境界を定義できる。

「航空局ガイドライン」で示されている環境と攻撃者、攻撃経路と緩和策、機体境界、システム境界および資産(Asset)は、システム境界が機体側に限定されている図であるが、これの意味するところは、資産は機体システムの中に限定されている。一方で、資産が必ずしもシステム境界内にあるとは限らず、重要関連機器とされる機体外部のシステムや通信が乗っ取られることで、結果的に正規のパスを通って乗っ取りが発生する可能性も存在する。セキュリティ境界は、攻撃者から見た場合における攻撃平面の顕在化を行うものであるため、型式として認証すべきシステム全体から、守るべき境界を適切に設定するべきである。

(7) 資産とリスク重大度の定義

> *2: 解析・評価 / Calculation/Analysis*
> *(エ) その次に、抽出したシステム内で Threat Condition を引き起こす可能性のある資産(Asset)を抽出します。例えば、前述の飛行管理システムと飛行制御システムであれば、その中の飛行計画データや飛行制御プログラムが改ざんされると Threat Condition を引き起こすと考えられる場合、飛行計画データと飛行制御プログラムが Asset になります。*
>
> *[引用: 航空局ガイドライン]*

資産については、RTCA DO-326A に記述されているとおり、無人航空機の安全性に資する論理的および物理的なリソースであり、その中には機能、システム、データ、インターフェース、プロセスおよびそれらを扱う情報が含まれる。この中で、システムは論理的および物理的なコンポーネントとして提示される。機能は論理的にはプログラム、物理的にはコンポーネントおよびパーツに付随する。データはインターフェースに付随する。インターフェースには通信経路の末端、および伝送路を含む。また、プログラムを動作させる OS のログイン情報など、安全やセキュリティに資する運用情報を資産として定義する必要がある。これらに対して、侵害があった場合のリスク重大度の評価を事前に行う必要がある。

それぞれ資産が攻撃を受けた場合に、脅威事象が起きうるかについて評価し、資産に対するリスク重大度を決定する。リスク重大度のモデリング手法は様々あり、観点によって異なるが、それらのモデリング手法を適切に用いて、評価尺度を決定する必要がある。なお、リスク重大度の最大値は脅威事象に対して導出される PFH や定性的な評価尺度を用いて表現し、各資産に対してのリスク重大度は、資産が攻撃を受けて顕在化する脅威事象の点数が割り当てられる。

（8） 具体的な脅威の抽出と脅威レベルの評価

> *2: 解析・評価 / Calculation/Analysis*
> *（カ）続いて、セキュリティリスクアセスメントにより、どういったリスクがあるのかを特定し、その影響評価および必要に応じて緩和策を提示します。リスクアセスメントには様々な手法がありますが、一例として、抽出した Asset すべてに対し、その Asset ごとに Confidentiality（機密性）、Integrity（完全性）、Availability（可用性）の観点で悪影響を与えるシナリオ（Threat Scenario）を想定し、その影響評価を行うのも有効的です。*
> *［引用: 航空局ガイドライン］*

セキュリティリスクアセスメントの目的は、システムが電子的な攻撃を受けた際に発生するリスクを明確化することである。リスクが顕在化するためには、脅威源である攻撃者が、システムの脆弱性と結びつく必要がある。脆弱性は攻撃者の発見しうる最初の攻撃の入り口であり、脆弱性が攻撃と結びつくことで実際の脅威となる。

脆弱性の発見については、すでに活動 5 で記述されているとおり、干渉口が脆弱性となる。この脆弱性が攻撃者と結びついて、どのような脅威に晒されるかの評価として、攻撃方法の特定（Attack Vector）と難易度の評価を行う。

「航空局ガイドライン」では、到達可能な資産ごとに Confidentiality（機密性）、Integrity（完全性）、Availability（可用性）（CIA）の 3 つの観点について影響評価を行うことで、脆弱性に対する脅威の評価を行うとされている。また、脅威のモデルとして、CIA を拡張した形となる STRIDE も存在する。より詳細な脆弱性の評価の方法として、CVSS が知られている。なお、脆弱性の評価には、少なくとも攻撃方法が特定されていること、もしくは攻撃可能なインターフェースが網羅的に示されていること、仮想的な攻撃者の特徴が指定されており、その攻撃者について検査者と合意がなされていることが必要である。その上で、当該の脆弱性がどの程度脅威に結び付きやすいのかを、形式的または非形式的な形で検証することである。

（9） 既存の緩和策の抽出と防御レベルの評価

> *2: 解析・評価 / Calculation/Analysis*
> *（カ）～ また、シナリオには既知の脆弱性についても考慮する必要があります。なお、その評価の際はフライトフェーズ、影響を受ける対象（機体、操縦者、第三者など）ごとに評価を行うことを推奨します。*
> *［引用: 航空局ガイドライン］*

脅威源から脅威事象までのシナリオ（脅威シナリオ）を記述するにあたって、既存の緩和策がどのように対応されているのかと共に、その緩和策がどの程度緩和できているのか（もしくはどのくらい破られやすいのか）について抽出され、評価されている必要がある。

一般的に、既存の緩和策の防御レベルに準ずる評価や、追加の緩和策に対する目標値の設定のために、緩和策を正当に評価する評価方法が必要である。評価方法としては以下の手法が挙げられる

- 形式手法: 数理的な証明を用いて検証される方法。暗号化や鍵などの緩和策に対して、計算論的もしくは計算量的に健全であることを証明する。なお、計算量で示される場合、計算量と攻撃頻度を用いて攻撃の生起確率を算出可能である。
- 実証的手法: ファジングなどを用いて、実装されている緩和策に対して攻撃を仕掛け、その攻撃の生起確率や攻撃者特徴を加味して検証して証明する。形式手法で証明が難しい場合や、モジュール化されて論理的な検証が行えないなどの場合に用いる。
- 定量的計算: システムに対する実装以外の非機能的な緩和策を設定する場合、インターフェースにアクセスする時間の割合や、監視者などが居る時間、物理的な鍵による保管の実施など、生起確率やアクセスの容易度などを定量的に計算してそれを証拠として用いる。なお、そうした管理の前提がある場合、ICA に前提条件を記述し、免責事項とするべきである。

（10） 脅威源から脅威事象が引き起こされる脅威シナリオの同定

> *2: 解析・評価 / Calculation/Analysis*
> *（カ） ～ 一例として、抽出した Asset すべてに対し、その Asset ごとに Confidentiality（機密性）、Integrity（完全性）、Availability（可用性）の観点で悪影響を与えるシナリオ（Threat Scenario）を想定し、その影響評価を行うのも有効的です。また、シナリオには既知の脆弱性についても考慮する必要があります。なお、その評価の際はフライトフェーズ、影響を受ける対象（機体、操縦者、第三者など）ごとに評価を行うことを推奨します。*
> *［引用: 航空局ガイドライン］*

攻撃者は脅威の源であり、攻撃者が脆弱性であるインターフェースに紐づく場合、その箇所をすべて脅威源であるとみなすことができる。この脅威源から脅威事象が引き起こされると、リスクとしてみなすことができるが、このリスクが成立する頻度や生起確率、定性表現によるリスク値の計算を行うことで、実際にその脅威源からの経路（脅威シナリオ）が、対策が必要な脅威であるかを判定することが可能である。

脅威シナリオの同定について、複数の資産または脅威事象が存在し、かつ複数の脅威源（攻撃者とインターフェース）が存在すること、かつその経路は複数存在する可能性があることから、これらを解析する必要がある。具体的には、脅威木解析（Threat Tree Analysis）などを用いるべきである。詳細な脅威シナリオの同定には、さらに脅威源である攻撃者が脆弱性に結び付く場合に引き起こされる事象を資産まで辿る『カットセット』を抽出する。

（11） 脅威シナリオ中に含まれる既存の緩和策を含めたリスクの評価

> *2: 解析・評価 / Calculation/Analysis*
> *(カ)～悪影響を与えるシナリオ(Threat Scenario)を想定し、その影響評価を行うのも有効的です。また、シナリオには既知の脆弱性についても考慮する必要があります。なお、その評価の際はフライトフェーズ、影響を受ける対象(機体、操縦者、第三者など)ごとに評価を行うことを推奨します。例えば飛行計画データの完全性が改ざんで失われる場合、その Threat Scenario を考えると同時にそれの発生頻度(どの程度起こり得るか)を考えます。Threat Scenario の発生頻度と、Threat Condition の影響度を評価し、～*
>
> *[引用: 航空局ガイドライン]*

脅威シナリオが特定され、記述されているときに含まれる情報は、以下のとおりである

- 脅威源の状態 – インターフェースの属性（攻撃者特徴もしくは脆弱性の重大度）
- 脅威事象または資産、およびその重大度または生起確率の目標値
- 中間にある緩和策の保護レベル

これらの情報を用いて、脅威源に付与される攻撃確率および重大度から中間にある緩和策を経て、資産や脅威事象の生起確率および目標値まで、緩和されているかを評価する。

脅威源を中心にしてセキュリティに関する数値化を行う場合、以下の項目が考慮されるべきである

- 攻撃者特徴、攻撃者の技術レベル
- 脆弱性の発見のしやすさ、インターフェースの可視性
- 攻撃に利用される可能性、アクセスのしやすさ

資産や脅威事象の重大度を中心にしてセキュリティに関する数値化を行う場合、以下の項目が考慮されるべきである。

- 想定される損害の重大度
- 攻撃が成功する再現可能性
- 影響を受けるユーザーの規模

また、中間にある緩和策については、機器の保管状況やメンテナンスの方法、ファームウェアアップデートなどに関する手続きなどを含め、どの程度セキュリティリスクを緩和させるかについて、記述する必要がある。

（12） 評価されたリスクに対する緩和策の追加

> *2: 解析・評価 / Calculation/Analysis*
> *（カ） ～ Threat Scenario の発生頻度と、Threat Condition の影響度を評価し、その結果、必要であれば緩和策(Security Measure)を考慮する必要があります。*
> *［引用: 航空局ガイドライン］*

評価されたリスクに対して、必要により緩和することを求められる場合、そのようなイベントを不許可イベントと呼び、不許可イベントに対してどのように対処をするかを決定する必要がある。この活動では、不許可イベントに対してどのようにリスクを緩和するかを決定し、緩和策の追加を行う。

一般的なリスクの緩和策の方針(ISO 27005:2022)については以下の4つの方法が定義されている。

- Reduce(低減) – ゴール達成のためのサイバーセキュリティ要件を定義する
- Accept/Retain (受容/保有) – 受容可能の理由・根拠を定義する
- Avoid (回避) – アーキテクチャ・仕様変更を行う
- Share (移転/共有) – 保険や上位システムの構築方法への活動の決定と、活動の正当性事由を定義する

不許可イベントについて、Accept/Retain という方策をとることは非常に難しく、安全や品質の低下を許容することと同義であることから、避けるべきである。

また、RTCA DO-326A に記載されている、不許可イベントについての対策の分類は以下のとおり。

- Deterrent(抑止)– 不許可イベントを発生させないような対策
- Preventive(予防)– 不許可イベント発生を防止する対策
- Detective(検知)– 不許可イベント発生を検知・報告する対策
- Corrective(是正)– 不許可イベント発生に応答することを意図した対策
- Restorative(回復)– 不許可イベント発生後の正常状態への復帰

対策を決定し、その構成を導入する場合は、対策をとると決定された構成をシステムに記述し、再度セキュリティリスクアセスメントを実施する。

なお、これらの追加のための緩和策に対する目標値の設定については、特に実証的手法や定量的計算を用いる場合について、「セクション 110」への追加要求として提示するほか、「セクション 300」「セクション 305」における検査項目としてのフィードバックを行うこと、また、管理の前提がともなう場合は「セクション 205 ICA(以降、「セクション 205」と呼ぶ)］への記述を行う必要がある。

（13） 残存する脆弱性とセキュリティリスクの評価

> *2: 解析・評価 / Calculation/Analysis*
> *無人航空機が安全性に悪影響を及ぼす意図的で承認されていない電子的な干渉から保護されていることを示すため、リスクアセスメントを行い、セキュリティリスクを特定し、評価し、必要により緩和策を講じていることを提示します。*
>
> *［引用: 航空局ガイドライン］*

セキュリティリスクアセスメントで証明すべきことは、アセスメントで対象となるセキュリティリスクが許容範囲内となることである。そのため、想定していない、残存している脆弱性がある場合は、想定しているリスクの範囲を逸脱した脅威やリスクが存在する可能性があることから、常にシステムに対して残存する脆弱性の有無を調査する必要がある。

残存する脆弱性を調査するには、ファジング・テストやペネトレーション・テストなどが有効である。ファジング・テストは各システムに対してランダムデータなどを用いて反応応答を調査する手法である。また、ペネトレーション・テストは専門家による、専門性の高いツールを用いて、システム全体に対して攻撃を仕掛ける手法である。

（14） 点検・整備・運用などで行われる緩和策についての記述

> *1: 設計図面 / Design/Data Review*
> *最後にセキュリティレベルを維持するために運航者が順守すべき事項をセキュリティガイドラインにまとめます。*
> *～ ICA に定めるセキュリティ対策の維持手順および指示（セキュリティガイドライン）も完了報告書に記載します。*
>
> *［引用: 航空局ガイドライン］*

セキュリティリスク緩和策で点検・整備や運用に対して移転が行われ、それが正しくセキュリティ機能を得ていると証明されれば、移転された緩和策に対してどのように点検・整備を行うか、また、運用を行うかについての他のセクションへの記述指示が行われ、正しく記述されていることの証拠を得るべきである。また、他のセキュリティ緩和策の維持のために点検・整備や運用に対して必要な要求が存在する場合にも、同様に点検・整備および運用のための要求を整理して、記述する必要がある。

なお、点検・整備に関しては、「セクション 205」への記述を行うこと、運用に関しては「セクション 200 無人航空機飛行規程（以降、「セクション 200」と呼ぶ）」への記述を行うことが求められる。

（15）セキュリティリスクアセスメントのバージョン管理

> *1: 設計図面 / Design/Data Review*
> *ここで、リスクアセスメントで考慮した Threat Scenario に対し、新たな脆弱性が発見され、シナリオに変更があった場合は、追加の評価が必要になります。*
> *［引用: 航空局ガイドライン］*
> *2.2.1 項（1）その他参考事項を記載した書類(提出時期:現状についての検査実施前）その他参考事項を記載した書類とは、次の書類をいう。 a. 安全性を確保するための管理の計画*
> *［引用: サーキュラー No.8-002］*

セキュリティリスクアセスメントは、供用されるシステムのセキュリティリスクが許容範囲内であることを保証する活動として、PDCA サイクルを回す中で実施される。これらは、セキュリティリスクを中心にとらえた、システムに対する要求管理プロセスであるため、追加要求が発生するたびにシステムの構成が変更される。この活動によって得られるセキュリティの設計はセキュリティアーキテクチャ(Security Architecture)として型式で認証されるべき固有のアウトプットとなるべきである。システムの構成が変更された場合、更新された部分を追記してセキュリティリスクアセスメントを再度実施する必要があることから、以前行ったセキュリティリスクアセスメントの構成管理を行うことで、他のセクションの文書との間で矛盾なく、かつ二度手間を防いで効率よくセキュリティリスクアセスメントを行うことを求められる。

そのため、セキュリティリスクアセスメントにおいても、既存のバージョン管理システムなどを用いてセキュリティアーキテクチャに対するバージョン管理を行い、セキュリティリスクアセスメントのログの記述と変更点のトレーサビリティを確保する必要がある。また、追加要求などで出現した他のセクションへの要求は、他のセクションで行ったテストの結果などを、セキュリティリスクアセスメントのバージョン管理に適切にフィードバックされ、トレーサビリティを確保する必要がある。

（16）リスクアセスメントで利用する証明方法・手順についての記述

> *1: 設計図面 / Design/Data Review*
> *無人航空機が安全性に悪影響を及ぼす意図的で承認されていない電子的な干渉から保護されていることを示すため、リスクアセスメントを行い、セキュリティリスクを特定し、評価し、必要により緩和策を講じていることを提示します。*
> *［引用: 航空局ガイドライン］*

セキュリティ適合性証明計画を行う際に適用するセキュリティリスクアセスメント手法およびその評価尺度を定義し、検査者と合意が取れている必要がある。この時、セキュリティ適合証明計画書の中では、適合方法(MoC)として手法が記述されている必要がある。

各手法や評価尺度などは、他の標準を充てて用いることができる。特に、RTCA DO-326A, DO-356A で記述されている活動や尺度、方法は、航空局 MoC でも参照されているとおり、非常に有用である。また、ASTM 3201-16 においても同様に、RTCA DO-326A が積極的に利用されて

いる。そのほか、ISO/SAE 21434 (路上走行車両), IEC 62443 (CSMS), ISO 27005:2022 (ISMS)などの記述、CC (ISO/IEC 15408)などの指標を用いることが出来、どの部分にどの標準を適用しているかなどを明記する必要がある。

(17) すべての脅威シナリオについてのリストの作成

> *1: 設計図面 / Design/Data Review*
> *2: 解析・評価 / Calculation/Analysis*
> *一例として、抽出した Asset すべてに対し、その Asset ごとに Confidentiality(機密性)、Integrity(完全性)、Availability(可用性)の観点で悪影響を与えるシナリオ(Threat Scenario)を想定し、その影響評価を行うのも有効的です。*
> *[引用: 航空局ガイドライン]*

適合性評価の証拠のために、行ったセキュリティリスクアセスメントが正しく網羅的に行われたかについて、脅威シナリオの表を添付することが望ましい。

脅威シナリオとは、攻撃者が攻撃可能な侵入口となるシステムの脆弱性を発見した場合に、そこから辿って攻撃可能な資産が現れる場合に表現される。これら一連の脅威シナリオを、「航空局ガイドライン」では資産ごとにリスト化し、影響評価を行うことも可能であるが、一方で、攻撃者と攻撃可能な侵入口を起点にして影響評価を行うことも可能である。

RTCA DO-356A には一連の脅威シナリオのリスト作成の詳細な手法が記載されている。

(18) すべてのセキュリティリスク緩和策についてのリストの作成

> *1: 設計図面 / Design/Data Review*
> *2: 解析・評価 / Calculation/Analysis*
> *その結果、必要であれば緩和策(Security Measure)を考慮する必要があります。*
> *[引用: 航空局ガイドライン]*

適合性評価の証拠のために、行ったセキュリティリスクアセスメントが正しく網羅的に行われたかについて、対策されたすべてのセキュリティリスク緩和策の表を添付することが望ましい。

セキュリティリスク緩和策は、技術的な緩和策、運用的な緩和策を含めて記述されているべきである。また、ソフトウェア的な緩和策については、その要求が安全性に資するものであれば、「セクション 110」によって管理され、正に実装されていることを示す。ハードウェア的な緩和策については、機体設計などに実装されていることを示す。運用的な緩和策において、運用中に対応する緩和策であれば、「セクション 200」、整備中に対応する緩和策であれば、「セクション 205」に記載される必要があるため、そのための指示も記述しておく必要がある。

（19）すべてのセキュリティリスク緩和策についての適合性評価の結果の記述

> *1: 設計図面 / Design/Data Review*
> *2: 解析・評価 / Calculation/Analysis*
> *ここで、リスクアセスメントで考慮した Threat Scenario に対し、新たな脆弱性が発見され、シナリオに変更があった場合は、追加の評価が必要になります。*
> *(a)項の結果を完了報告書としてまとめるとともに、ICA に定めるセキュリティ対策の維持手順および指示(セキュリティガイドライン)も完了報告書に記載します。*
> *[引用: 航空局ガイドライン]*

セクション 115 適合性証明完了報告書のために、適合性評価が適正に行われ、かつ適合性証明計画書に記された活動が適正に終了したことを矛盾なく示すための記述が必要である。

セクション 115 適合性証明完了報告書には、活動のすべてを記載する必要はない。適合性証明計画書に記された内容が適正に行われたことを示す補助資料として、最終的な出力結果が示されていればよいが、一方で、セキュリティリスクアセスメントの過程および評価の変遷について申請者が保持しており、検査の段階で検査者が開示を要求する場合に適正に提示できるように準備する必要がある。そのために、矛盾のない記述、矛盾のない資料の準備が必要である。

加えて、「セクション 115」で解析された内容から波及して記述がなされる「セクション 205」についても、正しく記載が完了されていることを報告する必要がある。

4.4 サイバーセキュリティ適合性証明プロセス

(1) セクション 115 の適用範囲と目標

「サーキュラー No.8-001」で示される安全基準では、用語として『安全性』という語が定義されており、『*無人航空機のリスクレベルが許容できる範囲に収まっている状態のこと*』を指す。このリスクレベルとは、「セクション 300」における正常運用時の耐久性および信頼性を阻害するようなリスクであり、かつ「セクション 305」や「セクション 310 能力および機能(以降、「セクション310」と呼ぶ)」などで触れられる不具合時運用における安全機能を阻害するリスクの程度である。

機能安全規格 IEC 61508 では、安全性の目標として、安全度水準 (SIL)が定義されており、リアルタイムシステムである無人航空機システムでは、高頻度モードにおける安全度水準を基準にして、安全機能の危険側失敗の平均頻度 (PFH)として定義され、リスクを許容する頻度の程度を示している。

セクション 115 適合性証明は、この『安全性』に対する適合性証明である。つまり、「セクション 115」で取り扱うセキュリティリスクアセスメントの目標は『無人航空機の安全性』の担保である。そのため、一般的なサイバーセキュリティで扱われるプライバシーや業務用で取得される情報についての漏洩リスクなどは扱わない。一方で、そういった一般的なサイバーセキュリティで扱われる情報資産に対してのセキュリティリスクアセスメントについては、関連文書(6)を参照されたい。

また、一般的に機能安全とは、『機能や機械が外界に対して危害を与えないことの保証』に用いられるのに対して、セキュリティとは、『外部からの攻撃に対して内部の資産が毀損されない保証』として用いられる。このことから、セクション 115 適合性証明で扱われる定義を 5W1H で定義すると、以下のとおりとなる。

- What: 航空機上に無人である航空機システムが (Unmanned Aircraft System)
- When: 開発段階から運用・破棄に至るまで (in Lifetime)
- Where: 電子情報および電子通信における経路上で (on Cyberspace)
- Who: 第 3 者または外部から (from Third Person or Outside)
- Why: 意図的または随意的な (by Intentional or Voluntary)
- How: 攻撃を受けた場合に (to Attack)
- Effect: (機能的な)安全性を失うことを防ぐ (正常な運航ができなくなる) (lost Airworthiness)

また、表 4.4-1 本解説書の範囲の定義表で示されるとおり、本解説書の範囲はセキュリティにおいての電子的な側面に対する機能安全についてであり、加えて、運用時の継続的なセキュリティ活動の定義を含む。これらに対する海外の対応規格は、RTCA DO-326A, 356A, 355 および EUROCAE ED-202A, 203A, 204A である。

表 4.4-1 本解説書の範囲の定義表

セキュリティ	機能安全面	運用面	商用面
物理的側面	200 飛行規程 205 ICA	空港・Vertiport等 格納庫等セキュリティ Counter UAS等	
電子的側面	115 サイバーセキュリティ RTCA DO-326A/ EUROCAE ED-202A RTCA DO-356A/ EUROCAE ED-203A	205 ICA / 115 CS, 継続的なセキュリティ EUROCAE ED-204A ATM-UTMセキュリティ EUROCAE ED-205A Air Transport EUROCAE ED-201A	経済産業省 無人航空機分野サイバーセキュリティガイドライン NIST SP-800-53A NIST SP-800-82 rev.2

（2） セクション 115 適合性証明プロセス

セクション 115 適合性証明プロセスは、システムが脆弱性に対するセキュリティ要件を満たすことを検証し、文書化する手続きである。型式認証に関しては、図 4.4-1 のように「航空局ガイドライン」中にプロセスが記載されている。

この基準からすると、適合性証明計画まで①事前調整からはじまり、②初回審査会を経て、④,⑤適用基準などの考慮・設定が検査者より提示されて当該適用基準が合意されたのち、⑥適合性証明計画案の作成および合意を行うこととなる。本来であれば、適合性証明計画が合意されたのち、設計などを行い、設計検査および適合検査/試験立会（Request for Conformity/Test Witnessing, RFC/W）が実施され、供試体適合検査、試験セットアップ適合検査を経て、試験立会、TWR（Test Witness Record）が作成、発行されたのち、試験結果に問題がないならば、試験報告書が作成され、適合性判定が行われたうえで、CONOPS 最終版と総合判定案、型式認証データシート（TCDS: Type Certification Data Sheet）案を、飛行規程および ICA などの最終確認を経て、⑬,⑭最終審査会を行い、認証書が交付されることとなる。

セクション 115 適合性証明活動は、設計検査および解析・評価による検査であり、RFC/W は不要であるが、一方で、最終審査会において確認される ICA の構築に深く関わることおよび継続的なセキュリティの担保のための活動を含むことから、記述されるセキュリティアーキテクチャに関わる開発および変更などがある度に、再度、検査・解析・評価が行われるべきである。なお、セクション 115 適合性証明計画書の初版は事前調整時に提示されることが望ましいとの記載が「サーキュラー No.8-002」2－1－3 章⑥項にあるが、ある程度の合意は図 4.4-1⑥のタイミングで取れているものとする。また、セクション 115 適合性証明完了報告書に関しては、図 4.4-1⑨設計に関する検査など、特に RFC/W 前に行われる設計検査の段階でほぼ出来上がっており、「セクション 200」や「セクション 205」へフィードバックが行われていることが望ましい。

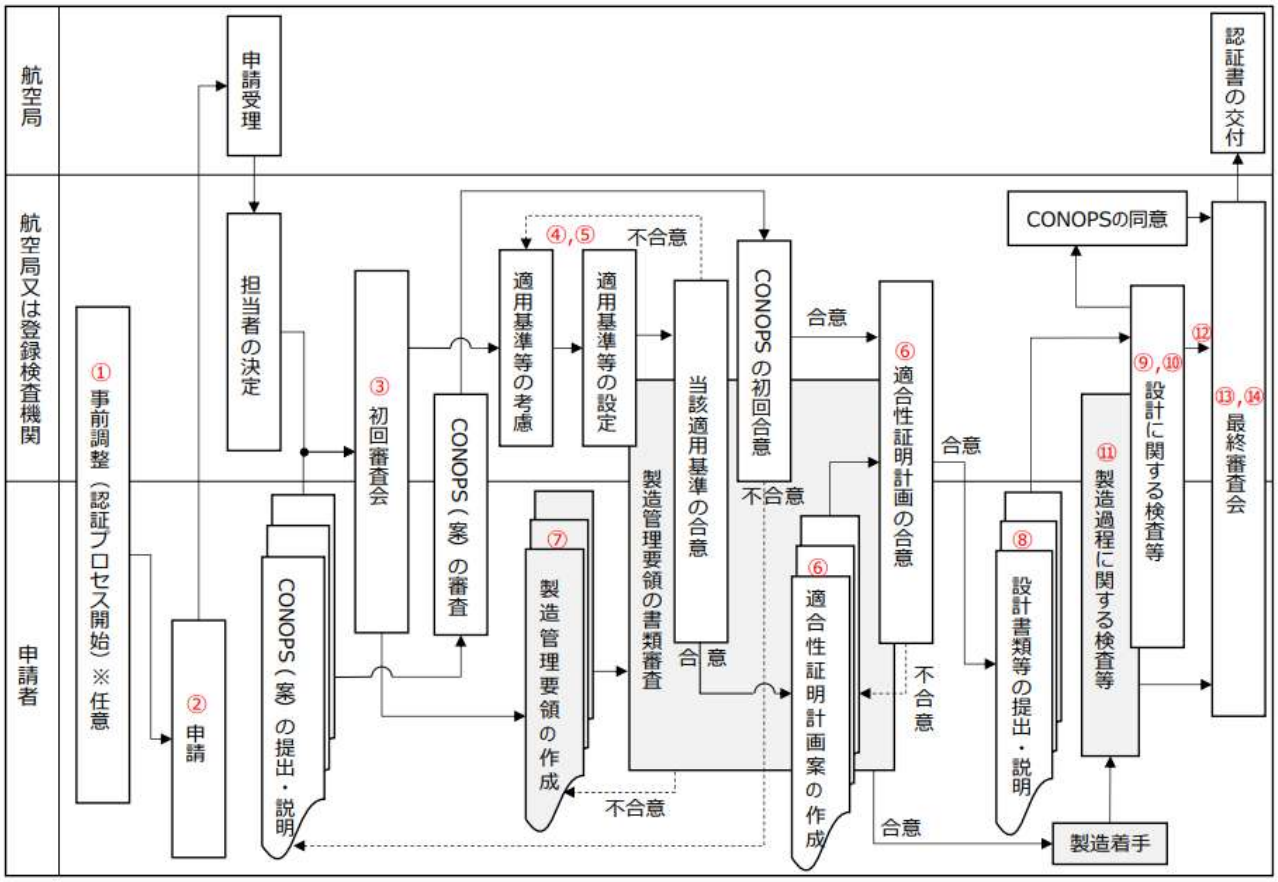


図 4.4-1 型式認証プロセスのフロー

出所）航空局ガイドライン

662 セクション 115 適合性証明活動をプロセスとしてフローにまとめたものを図 4.4-2 に示す。以下に
663 示す①～⑩のステップで構成される。

664 ① システムの記述［要求 1］
665 ② 評価尺度・手法の決定［要求 3］
666 ③ 115 セキュリティ適合性証明計画書の合意［要求 6］
667 ④ セキュリティ環境の擁立と検証［要求 2］
668 ⑤ セキュリティアセスメントの実施［要求 3，要求 4］
669 ⑥ 受容可能性の決定［要求 4］
670 ⑦ セキュリティ緩和策の効果証明［要求 5］
671 ⑧ セキュリティ緩和策の開発［要求 5］
672 ⑨ セキュリティ維持活動の記述［要求 5］
673 ⑩ 115 セキュリティ適合性証明完了報告書の合意［要求 7］

674 この活動において、4.3 章における活動を充てるとする場合、活動 1～5、および活動 10,11 の指針・
675 手法について、活動 16 と併せてセキュリティ適合証明計画書の中で記述される必要がある。活動 6～
676 15 までの具体的な実施は、活動 17～19 の出力という形でセキュリティ適合性証明完了報告書に記
677 述される。なお、本活動は、「セクション 205」や「セクション 200」、セキュリティ維持活動の記述に関

連して、「サーキュラー No.8-002」2.2.1 章(i),(j),(l)項で示されるとおり、『現状についての検査実施前』までに確定され、実施されていなければいけない。

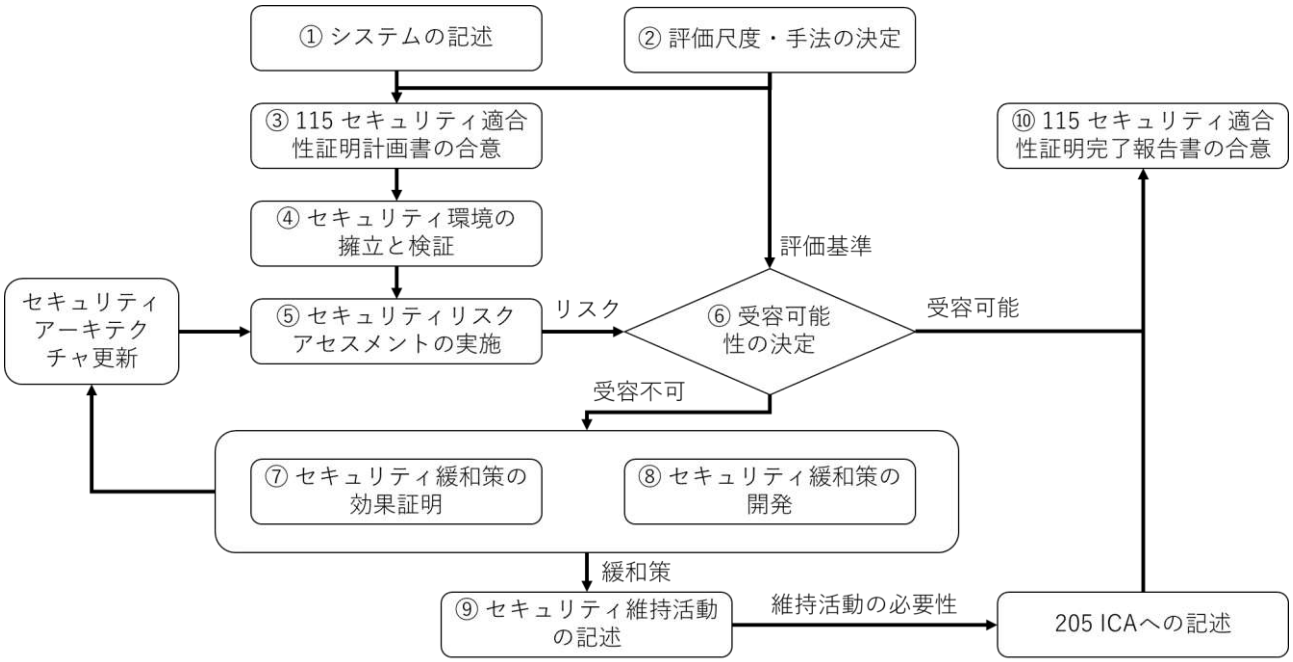


図 4.4-2 セクション 115 の認証活動プロセス

(3) セクション 115 適合性証明活動とプロセスの対応

セクション115適合性証明活動の活動目標は『無人航空機の安全性を侵害する攻撃からのサイバーセキュリティリスクの緩和』である。実際の活動の項目は、「リスクアセスメント」、「緩和策の設計と実装」および「検証と文書化」の 3 つで実施される。

「リスクアセスメント」では、はじめに無人航空機システムの運航環境や目的に応じた脅威と脆弱性を特定し、評価するための環境、評価手法、評価尺度を定義する。次に、実際に無人航空機のCONOPSから起算される脅威源となる攻撃者の仮説を立て、脅威事象を引き起こす資産を導出し、システムの脆弱性、脅威、起こり得るリスクを導出する。続いて、攻撃者が脆弱性に結び付き、対象とする資産を攻撃する脅威シナリオを抽出し、その中に含まれるリスクの重大度、脅威レベル、緩和策の防御レベルを加味して各脅威シナリオに掛かる残存リスク重大度を算出し、それが受容可能かを評価する。

次に、リスク緩和策の設計と実装である。この活動は、リスクアセスメントで明らかになった脅威・脆弱性を考慮し、それらに対する最適なリスク緩和策を設計・実装する。

最後に、検証と文書化を行う。この活動では、設計・実装したリスク軽減策が正しく、効果的に適用されていることを検証し、その結果を文書化する。これによって、証明可能なセキュリティを保証し、持続的なマネジメントを可能にする。

4.3 章で定義された活動項目についてそれぞれ具体的な検証と文書化についての項目を表 4.4-2 に列挙する。必須要件とは、その活動が適合性証明活動に必須と思われる活動、推奨活動とは、その活動が適合性証明活動に有用であり、推奨される活動である。なお、必須要件は M、推奨要件を R と

700 する。また、M/R の判定方法については、第二種型式認証では一通りのセキュリティリスクアセスメン
701 ト活動を一回以上行うことに加えて、4.5(2)項に示される具体的な作業を行っている活動を M とした。
702
703 表 4.4-2 セクション 115 活動項目と手法・出力の対応表

プロセス	活動項目	M/R	手法および出力
要求 1: システム環境の明確な記述			
①	活動 1: システムの範囲の決定と記述	M	システムブロック図
①	活動 2: ネットワークおよびデータフローの記述	R	ネットワーク図 データフロー図
①	活動 3: 正常な運用におけるインターフェースとアクターの記述	M	ユースケース図 ステークホルダー表
要求 2: サイバーセキュリティの範囲と脅威、攻撃者の定義			
②	活動 4: 脅威事象と評価尺度の定義	M	脅威事象定義表 リスク評価尺度定義書
②④	活動 5: 攻撃者と攻撃可能な干渉口の抽出	M	ミスユースケース図 攻撃者を含むシステムブロック図 攻撃者定義表 アタックサーフェスリスト
④	活動 6: セキュリティ環境におけるセキュリティ境界の定義	M	セキュリティ環境・境界指示図
要求 3: サイバーセキュリティリスクの特定			
④	活動 7: 資産とリスク重大度の定義	M	資産-脅威リスト
⑤	活動 8: 具体的な脅威の抽出と脅威レベルの評価	M	脅威分析表 脅威-対処リスト
⑤	活動 9: 既存の緩和策の抽出と防御レベルの評価	M	緩和策リスト 脆弱性クラスリスト
⑤	活動 10: 脅威源から脅威事象が引き起こされる脅威シナリオの同定	M	脅威木の構築 カットセットリスト
要求 4: 特定されたセキュリティリスクの評価			
⑤⑥	活動 11: 脅威シナリオ中に含まれる既存の緩和策を含めたリスクの評価	M	セキュリティリスク分析表
要求 5: 評価に基づく緩和策の実施と記述			
⑦⑧	活動 12: 評価されたリスクに対する緩和策の追加	R	追加要求の設計 開発者ガイドライン(追加要求)
⑦	活動 13: 残存する脆弱性とセキュリティリスクの評価	R	ファジング・テスト結果報告書 ペネトレーション・テスト結果報告書
⑨	活動 14: 点検・整備・運用などで行われる緩和策についての記述	M	セクション 205 への記述 セクション 200 飛行規程への記述

⑨	活動 15: セキュリティリスクアセスメントのバージョン管理	R	バージョン管理ツールの利用 要求管理ツールの利用
要求 6: セクション 115 適合性証明計画書の矛盾のない記述			
③	活動 16: リスクアセスメントで利用する証明方法についての記述	M	コンプライアンスマトリクス
要求 7: セクション 115 適合性証明完了報告書の矛盾のない記述			
⑩	活動 17: すべての脅威シナリオについてのリストの作成	R	脅威シナリオ解析書
⑩	活動 18: すべてのセキュリティリスク緩和策についてのリストの作成	R	セキュリティ緩和策妥当性解析書
⑩	活動 19: すべてのセキュリティリスク緩和策についての適合性評価の結果の記述	M	コンプライアンスマトリクスへの追記

この表において、特に活動 2 は、4.5(2)項の作業には寄与していないため、R としたが、実際には活動 2 はシステム設計においても非常に重要な活動である。また、活動 17,18 は、すでに活動 10,11 で行われており、それらは M であることから、フォーマットを変更し提出できるようにすれば十分対応できるものであるが、第二種型式認証における証拠として求められるものがセクション 115 適合性証明計画書およびセクション 115 適合性証明完了報告書であることから、セクション 115 適合性証明のために各解析書を添付する旨が適合性証明計画で含まれないまま合意されているとすれば、必要ないと判断して、R としている。この部分については、審査者が検査者との合意で決定することであるため、R の活動であっても検査者が要求する可能性がある。

4.5 サイバーセキュリティ適合性証明のための指針と手法

サイバーセキュリティ適合性証明のための手法については、本来は申請者が定義し、コンプライアンスマトリクスとして記述し、検査者と合意を得て進める項目であるため、個別の指針や手法については既存の様々なセキュリティリスクアセスメントの標準（ISO/SAE 21434，IEC 62443，ISO 27000 シリーズなど）を用いて進めることが可能である。

ここでは、脅威分析についての指針、一例として、第二種型式認証で用いることが可能と思われる手法を、RTCA DO356-A Appendix F の方法を簡素化した手法を指針として掲示する。

（1） 脅威事象の定義と手法、評価尺度についての指針

サイバーセキュリティ適合性証明計画において最も重要なことは、『何の脅威』に対して、『どのような評価尺度』を用いて、『どの程度』守るべきなのかという目標設定を、申請者側から提案することである。そのため、何が脅威事象として含まれるのか、また、どのような手法、尺度を用いるかについての指針を示す。

1） セキュリティリスクアセスメントの目的: 無人航空機の安全の確保

無人航空機の型式認証は総じて無人航空機システムを運用する際に発生するリスク、特に地上リスクと呼ばれる地上にいる人や第三者物件など対しての被害を低減・緩和し、受容可能であるようにするために行われる。そのため、「セクション 115」の目標は、このような安全に対するリスク緩和策やシステムに対して外部から電子的な攻撃を受けて毀損しないことが目標となる。つまり、「セクション 115」で行う活動は、この目標に沿って行われるべきであり、所謂一般的な情報システムにおけるプライバシーなどの保護については、無人航空機の安全に関与していない場合はこのセクションの活動の範囲外である。

2） 脅威事象の特定: 安全基準に適合

「航空局ガイドライン」では、無人航空機の安全に関する適合基準について示されている。この中の最たるものとして、『操縦不能（Loss of Control）』と『目的外飛行（Loss of Flight）』が挙げられている。また、「航空局ガイドライン」における「セクション 115」では、『想定飛行範囲の逸脱』が例として挙げられている。

安全基準に適合する最終的な判定基準は、その無人航空機システムの完全性を保証する「セクション 300」と、異常系を加味した上で安全性を担保する「セクション 305」との間でギャップが存在するが、「セクション 115」では、基本的に「セクション 300」においても「セクション 305」においても想定している『安全リスクの緩和策』が侵害された結果、『操縦不能』『目的外飛行』もしくは『想定飛行範囲の逸脱』が発生しないようにするべきである。

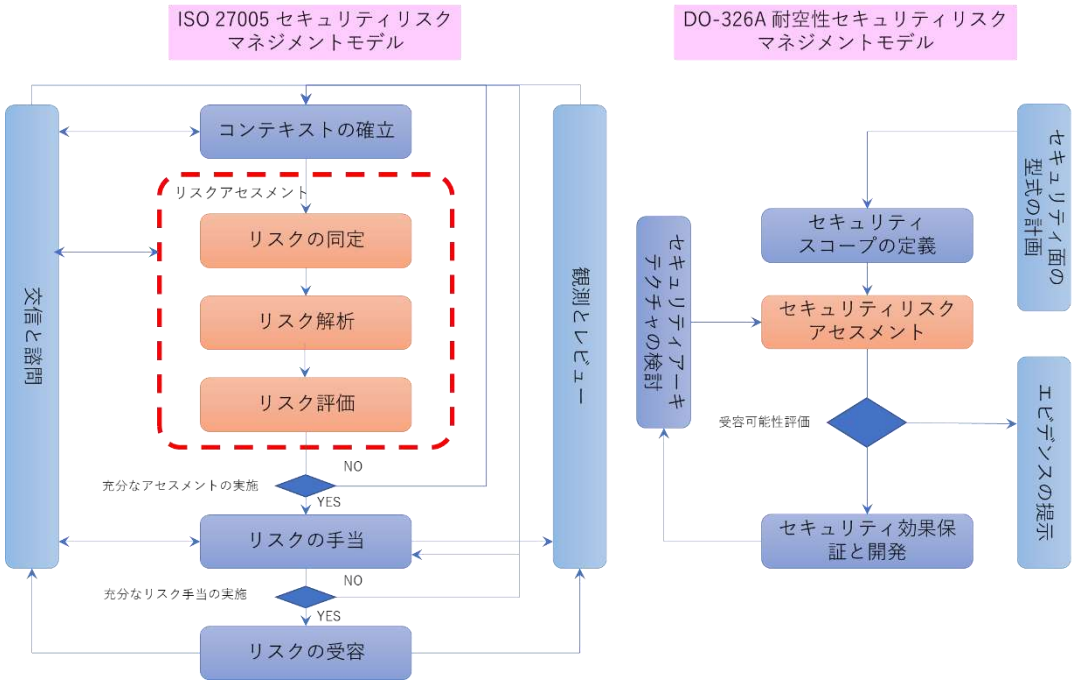


図 4.5-1 セキュリティリスクマネジメントモデル: ISO 27005 と DO-326A の比較

加えて、それらの事象が発生する可能性のあるサイバーセキュリティにおける脅威のモデルとの突合せが必要である。どのような安全リスクの緩和策が行われていても、電子機器に対する『ハイジャック』が発生すれば、すべての安全リスク緩和策が破綻する可能性がある。電子機器に対するセキュリティの 3 要素は『機密性(Confidentiality)』『完全性(Integrity)』『可用性(Availability)』であるが、それらに対応して、機密性の侵害である『システムアクセスに関する情報の漏洩』、完全性の侵害である『マルウェアなどの混入』、可用性の侵害である『サービス停止攻撃』などの状況が、安全リスクの緩和策を侵害し、脅威事象に至る原因となり得る。

これらのことを踏まえて最上位の脅威事象を定義し、それらに対するリスクの程度を決定する。

3) 手法と評価尺度の決定: バランスと証明のための対応の明確化

脅威事象を決めると、その脅威事象に至らないように、セキュリティアセスメントを行う方策を立てる。セキュリティアセスメントの具体的な指針については、図 4.5-1 に、ISO27005 セキュリティリスクマネジメントモデルおよび DO-326A 耐空性セキュリティリスクマネジメントモデルとして示す。ここで必要なことは、どのような手法を用いて、どのような評価尺度でリスクを同定し、解析し、評価するかである。

リスクの同定については、どのように脅威源である攻撃者からリスクに紐づくかを定義するモデリングが有効である。それは、凡そ次のようにして行われる: 脅威源となる攻撃者がシステムの脆弱性を発見し、そこに対して攻撃を行うと資産を侵害される脅威が発生する。発生した脅威が何らかの影響を安全に与える場合、影響を受けた度合いによりリスクが発生する。リスクを緩和するために、攻撃される経路の途中にセキュリティの緩和策を置く

このモデルを基に、必要な評価尺度を考慮すると以下のとおりである。

- 攻撃者レベル
- 脆弱性レベル
- 資産が侵害される時の重大度
- 攻撃の脅威レベル
- 緩和策の保護レベル

これらの項目について、評価尺度を用いて矛盾なく、最上位となる脅威事象が起きうるかについての評価がなされるべきである。なお、このような手法を定義している国際標準が多々存在し、航空機分野では RTCA DO-326A，DO-356A，情報セキュリティのプロセスとしては ISO 27005:2022，IoT に関わる情報セキュリティの手法については NIST SP800-30，産業オートメーションについての情報セキュリティとしては IEC 62443，自動車に関するサイバーセキュリティの規格として ISO/SAE 21434:2021 が挙げられているが、どの規格においても、第二種型式認証に資する丁度良い評価手法・尺度とするには多少の考察と更新が必要である。

4） セキュリティリスクアセスメント活動の目的: 継続的なセキュリティの担保

実のところ、セキュリティリスクアセスメントは型式認証においては設計の段階の活動であり、一度「セクション 115」に対して適合可能な設計が仕上がれば、型式認証段階において他のセクションの大きな更新点がない限り（キルスイッチやパラシュートなどのコンポーネントの追加が起こらない限り）そこまで大きな活動の更新はない。しかしながら、セキュリティリスクアセスメントの一番の目的は製造され、運用に供されてからである。運用に供されてから、ハードウェアは徐々に劣化し、交換を余儀なくされるのと同様に、セキュリティは運用に供されてから、もしくは場合によっては開発段階から常にセキュリティリスクは上昇していく。システムが人目にさらされれば、それだけ攻撃者の関心を呼び、残置されたソフトウェアやハードウェアの脆弱性のみならず、新しく発見された攻撃手法が出現して、ときには搭載されているコンピューターシステム全体が即時に乗っ取り可能（ゼロデイアタック）となる可能性も存在するからである。

セキュリティリスクアセスメントを用いて、継続的なセキュリティの担保を行う活動をする場合は、セキュリティリスクアセスメントで用いた文書を適切に保管し、リスクの再評価を行う体制を立てることである。定期的な、内部レビューを行うことも重要であり、また、ホワイトハッカーなどに依頼してペネトレーション・テストを実施し、脆弱性の発見を行うことも重要である。何より、システムに対しての Problem Report や、世の中のセキュリティ報告などに目を通し、関連するシステムやソフトウェアのセキュリティホールなどの発生について常に監視が必要である。このような活動についても文書化し、体制を整える必要がある。

（2） 第二種型式認証に資するリスクアセスメント手法例

1） システム記述の粒度と範囲（活動 1～3,6）

第二種型式認証においては、他のセクションと同様に、システムレベルによる記述であることを前提に記述をする。無人航空機システムを構築するシステムの記述の例は図 4.5-2 のとおりとなる。

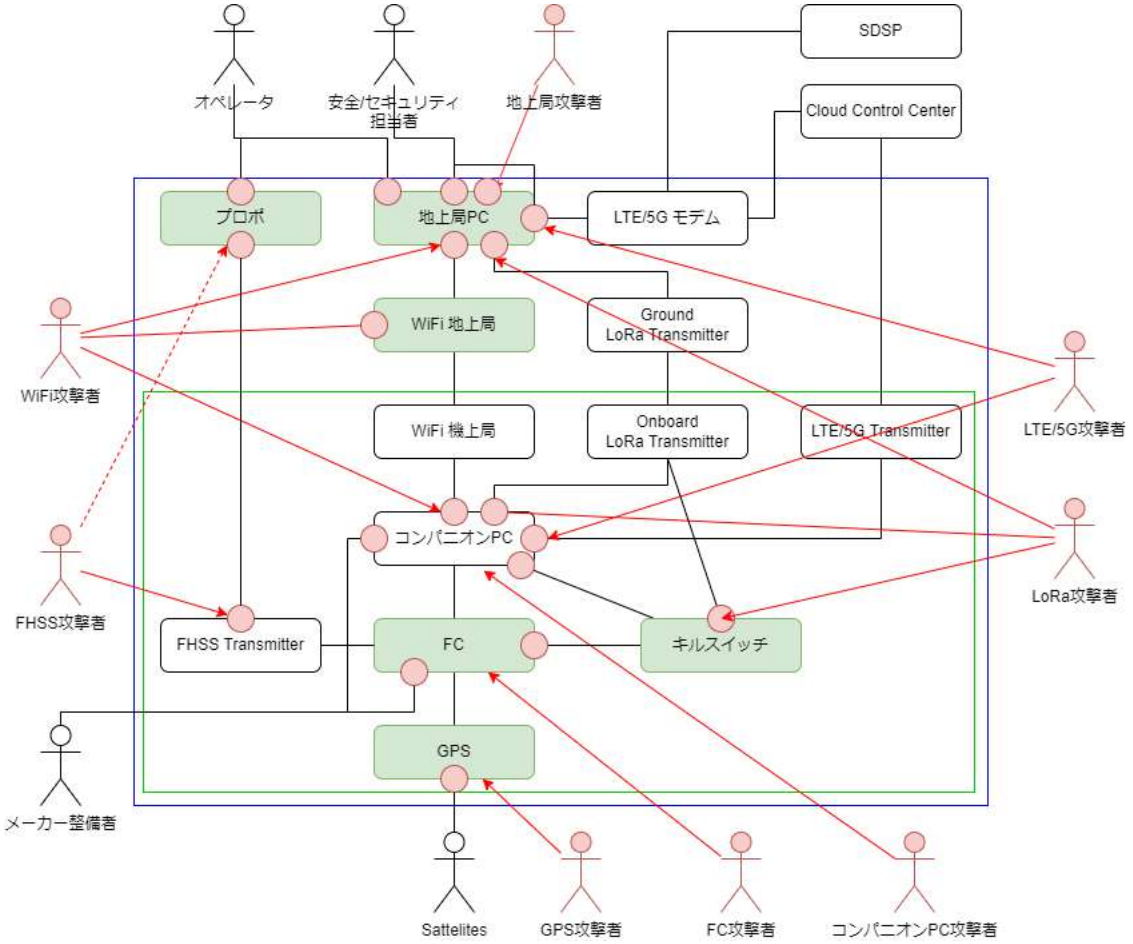


図 4.5-2 セキュリティ環境の模式図例

セキュリティ環境とは、無人航空機システムの外部に関連する部分であり、実際のユーザー、攻撃者を含めた全ステークホルダーまたは連携する外部システムが登場する部分である。図 4.5-2 の青枠の外は、とある無人航空機のセキュリティ環境を表す図である。

セキュリティ境界は、図 4.5-2 において青枠で示される。この部分は、メーカーが指定するシステムの内部であり、セキュリティで守られるべき範囲として記述される。また、図 4.5-2 の緑枠は、無人航空機の機体に対する境界(機体境界)である。

2) 脅威事象と評価尺度（活動 4）

第二種型式認証の安全性に基づく脅威事象とは、

- 制御不能(Loss of Control)
- 計画外飛行(Loss of Flight)（想定飛行範囲の逸脱）

である。これらの事象を引き起こすようなセキュリティとしての脅威が存在する場合、最上位の脅威レベルを付与するべきである。また、セキュリティの問題として、これらの 2 つの脅威事象に紐づく可能性のある脅威の最上位の脅威事象は

- ハイジャック（Hijack）

であると仮定する。

評価尺度に対しては、被害に対する重大度(Severity – SEV)を充てる。本解説書では、最大の SEV を 5 として、0 から 5 までの 6 段階で SEV を定義する。また、SEV に対して、脅威レベル(Level of Threat – LoT)を、脅威を緩和する保護レベル(Level of Protection – LoP)をそれぞれ定義し、以下の関係式で脅威シナリオ中に含まれる各コンポーネントにおける SEV の値を以下の関係式で計算することとする。

$$SEV = LoT - LoP$$

なお、最上位の脅威事象の 3 つは、SEV =5 であるとする。

3) 攻撃者リストの導出（活動 5）

図 4.5-2 で示されたセキュリティ環境の図を用いて、攻撃者リストを導出する。

以下、リストとして構築する場合、それぞれの要素は一意となる ID を付与する。

攻撃者である ID の接頭語は[A.]である。

- ID: 共通 ID [A.] + [名称]
  - [名称]：オペレーター、地上局 PC 攻撃者、WiFi 攻撃者 など
- Description: 攻撃者の特徴の説明
- LoT: 攻撃者の脅威レベル

攻撃者の想定脅威レベルを考慮すると、

- LoT = 5 (LoP = 0)
  - 悪意のある専門的な人間による攻撃/頻度高
- LoT = 4 (LoP = 1)
  - 悪意のある専門的な人間による攻撃/頻度中
  - 悪意のない専門的な人間による攻撃/頻度高（愉快犯，スクリプトキディなど）
- LoT = 3 (LoP = 2)
  - 悪意のある一般人による攻撃（侵入意図が明確，DOS など含む）
  - 悪意のある専門的な人間による『間接的な』攻撃（ファーム汚染など）
  - 悪意のある専門的な人間による攻撃/頻度低
- LoT = 2 (LoP = 3)
  - 悪意のない一般人による攻撃（誤侵入など）
  - 悪意のない専門的な人間による攻撃/頻度低
- LoT = 1 (LoP = 4)

849 ■ Gate などがすべてコントロール下にある状態（内部者のみ）

850 攻撃者リストの例は表 4.5-1 のとおりとなる。
851

表 4.5-1 攻撃者リストの例

Attacker	記述	LoT
A.オペレーター	標準オペレーター、内部者	1
A.安全・セキュリティ担当者	内部者、ユーザ側安全、セキュリティ担当	1
A.メーカー整備者	メーカー整備者、内部者	1
A.GPS 衛星	GPS 衛星、標準	1
A.地上局攻撃者	地上局への攻撃、内部者中心	2
A.WiFi 攻撃者	外部からの WiFi 侵入	3
A.FHSS 攻撃者	外部からの FHSS 信号侵入	3
A.LTE/5G 攻撃者	外部からの LTE/5G 侵入	4
A.LoRa 攻撃者	外部からの LoRa 侵入	3
A.コンパニオン PC 攻撃者	コンパニオン PC への攻撃、内部者、外部侵入者	3
A.GPS 攻撃者	GPS 信号への攻撃	3
A.FC 攻撃者	FC への攻撃、内部者、外部侵入者	3

852

853 4） 資産リストの導出（活動 7）

854 図 4.5-2 セキュリティ環境の模式図例のとおり、第二種型式認証ではシステムレベルによる記述
855 であるため、資産もシステムレベルで解析される。資産はシステムおよび通信であるが、通信路上の
856 データを保護しようとするには限界があるため、通信とシステムの接点であるインターフェース部分で
857 保護することを目論む。
858 また、システムレベルの中でサブシステムとなるインストールされたソフトウェアが存在する場合、これ
859 らもひとつのシステムとして計上することを推奨する。例えば、地上局 PC 内に GCS ソフトウェアをイ
860 ンストールする場合、GCS ソフトウェアも資産として登録するべきである。また、これらの資産としての
861 情報は、「セクション 135」や「セクション 110」と連携して定義される必要がある。
862 資産の ID の接頭語は[I.]とする。
863 資産リストの項目は以下のとおり。

864 ● ID: 共通 ID［I.］＋［所在名］＋［資産名］

865 ■ ［資産名］: 資産の素性・名称より
866 ■ ネット接続、サービス、コマンド、状態情報、データ、コード、設定データ、ID、パスワード など

867 ● Description: 保護資産に対する記述
868 ● Severity: 保護資産の持つリスク重大度［SEV］

- Threat Condition: 保護資産が侵害されるときの脅威事象（脅威事象モデルからの引用）
  → 脅威リストに対応
- Fatal Threat: 最上位の脅威事象に結びつく場合に何に該当するかの記述

なお、資産を判断する場合に、Fatal Threat に直接的に接続される可能性のある資産は、SEV＝5 を付与する。また、侵害されると直接的にではなくても安全に関与する他のシステムやデータに触れることが可能である場合、SEV のレベルを勘案して付与する。

安全に資する資産の候補として挙げられるものの候補は以下のとおりである。

- コマンド＆コントロール（C2）
- 運航テレメトリ信号
- 制御ソフトウェア
- 制御に必要な映像信号
- 機上システムの OS および関与するドライバ
- ファームウェア
- GPS など位置情報信号
- 各システムの認証情報(ログイン情報、暗号情報など)
- 各システムのシステムアプリケーションソフトウェア(OS，ミドルウェアなど)

資産リストの例は表 4.5-2 のとおり。

表 4.5-2 資産リストの例

Asset	記述	SEV	Threat	Fatal Threat
I.地上局 PC	地上局 PC の乗っ取り/サービス不能	5	T.地上局 PC.ID/パスワード漏出 T.地上局 PC.ハイジャック T.地上局 PC.バックドア侵入	T.機体.ハイジャック
			T.地上局 PC.マルウェア混入 T.地上局 PC.パラメータデータ書換 T.地上局 PC.GCS パラメータデータ書換	T.機体.制御不能 T.機体.計画外飛行
I.地上局 PC.GCS	地上局 PC の GCS 機能の不能/不正	5	T.地上局 PC.マルウェア混入 T.地上局 PC.GCS パラメータデータ書換 T.地上局 PC.DOS	T.機体.制御不能 T.機体.計画外飛行
I.地上局 PC.WiFi	地上局 PC の WiFi 通信不能	5	T.地上局 PC.WiFi.サービス拒否 T.地上局 PC.WiFi.ネットワークパラメータデータ書換	T.機体.制御不能 T.機体.計画外飛行 T.機体.ハイジャック
I.地上局 PC.LoRa	地上局 PC の LoRa 通信不能	5	T.地上局 PC.LoRa.改竄 T.地上局 PC.LoRa.サービス拒否	T.機体.制御不能 T.機体.計画外飛行
I.地上局 PC.LTE	地上局 PC の LTE 通信不能	5	T.地上局 PC.LoRa.改竄 T.地上局 PC.LoRa.サービス拒否	T.機体.制御不能 T.機体.計画外飛行
I.プロポ	プロポ不能/不正	5	T.プロポ.ファームウェア不正更新 T.プロポ.ホッピングパターン漏出	T.機体.制御不能 T.機体.計画外飛行
I.プロポ.FHSS	プロポ通信不能	5	T.プロポ.FHSS.電波干渉 T.プロポ.FHSS.不正電波混入	T.機体.制御不能 T.機体.計画外飛行
I.WiFi	WiFi ルータ、ネットワーク	5	T.WiFi.ARP Spoofing T.WiFi.ルーターハイジャック T.WiFi.WPA 鍵漏出	T.機体.ハイジャック
I.LTE	LTE 回線上での侵入	5	T.LTE.なりすまし T.LTE.改竄 T.LTE.サービス拒否	T.機体.ハイジャック
I.コンパニオン PC	コンパニオンPCの不能/不正	5	T.コンパニオン PC.不正ファーム T.コンパニオン PC.バックドア侵入 T.コンパニオン PC.ハイジャック T.コンパニオン PC.ID パスワード漏出	T.機体.ハイジャック
			T.コンパニオン PC.マルウェア混入 T.コンパニオン PC.不正コード混入 T.コンパニオン PC.パラメータデータ書換 T.コンパニオン PC.サービス拒否	T.機体.制御不能 T.機体.計画外飛行
I.コンパニオン PC.ガイドソフト	コンパニオン PC 内ガイドソフトの指示系統	5	T.コンパニオン PC.ガイドソフト.パラメータデータ書換 T.コンパニオン PC.ガイドソフト.不正コード混入 T.コンパニオン PC.ガイドソフト.サービス拒否	T.機体.ハイジャック
I.コンパニオン PC.キルスイッチ	コンパニオンPC経由のキルの指示系統	5	T.コンパニオン PC.キルスイッチ.不正キル信号受信 T.コンパニオン PC.キルスイッチ.プロセスロック T.コンパニオン PC.キルスイッチ.サービス拒否	T.機体.ハイジャック
I.コンパニオン PC.RTK	コンパニオンPC経由のRTK 情報の授受	5	T.コンパニオン PC.RTK.不正 RTK 信号受信	T.機体.計画外飛行
I.コンパニオン PC.WiFi	地上局 PC の WiFi 通信不能	5	T.コンパニオン PC.WiFi.不正コマンド受信 T.コンパニオン PC.WiFi.ネットワーク侵入 T.コンパニオン PC.WiFi.サービス拒否攻撃	T.機体.制御不能 T.機体.計画外飛行 T.機体.ハイジャック
I.コンパニオン PC.LoRa	地上局 PC の LoRa 通信不能	5	T.コンパニオン PC.LoRa.不正コマンド受信 T.コンパニオン PC.LoRa.サービス拒否攻撃	T.機体.制御不能 T.機体.計画外飛行
I.コンパニオン PC.LTE	地上局 PC の LTE 通信不能	5	T.コンパニオン PC.LTE.不正コマンド受信 T.コンパニオン PC.LTE.サービス拒否攻撃	T.機体.制御不能 T.機体.計画外飛行
I.FC	FC の不能/不正	5	T.FC.ファームウェア不正更新 T.FC.マルウェア混入	T.機体.制御不能 T.機体.計画外飛行
I.FC.RTK	FC 内RTK 情報の授受	5	T.FC.RTK.不正 RTK 信号受信	T.機体.計画外飛行
I.FC.FHSS	FC 側プロポ電波の不能	5	T.FC.FHSS.不正 RC コマンド受信 T.FC.FHSS.妨害電波	T.機体.制御不能 T.機体.計画外飛行
I.GPS	GPS の不正	5	T.GPS.不正 GPS 信号の受信	T.機体.制御不能 T.機体.計画外飛行
I.独立キルスイッチ	キルスイッチの不正	5	T.独立キルスイッチ.不正キル信号の受信 T.独立キルスイッチ.サービス拒否攻撃	T.機体.制御不能
I.独立キルスイッチ.LoRa	キルスイッチ電波の不正	5	T.独立キルスイッチ.LoRa.サービス拒否攻撃 T.独立キルスイッチ.LoRa.不正コマンド受信	T.機体.制御不能

886

5） 攻撃者の侵入口(アタックサーフェス)の導出（活動 5, 6）

図 4.5-2 において、赤丸に色を塗った部分のように、攻撃者からセキュリティ境界を踏み越えた先にある資産やインターフェースの接点が侵入口（アタックサーフェス)である。アタックサーフェスは侵入の可能性が少しでもある場合、網羅的に示される必要がある。

アタックサーフェスの ID の接頭語は［AS.]とする。

アタックサーフェスリストの項目は以下のとおり。

- ID: 共通 ID［AS.］＋［所在名］＋［AS 箇所名］
  - ［AS 箇所名]: アタックサーフェスの記述（USB, SD カード, WiFi, LoRa, FHSS, GPS, Net など）
- Security Measure: セキュリティ対策の存在（あればセキュリティ対策［O]を引用）
- Access Control Policy: アクセスコントロールポリシー
  - ALLOWS（許可）/ BLOCKS（拒否）
  - Security Measure によって確実にブロックされる場合は BLOCKS、攻撃者へのアクセス許可が出る場合は ALLOWS
- Access By: アタックサーフェスにアクセスする可能性のある攻撃者［A]，アタックサーフェス［AS]，脅威［T］などを記述
  - アタックサーフェスには攻撃者のみならず、他のインターフェースや脅威が接続される可能性がある。

アタックサーフェスを抽出するにあたって注意すべき点は、『誰がアクセスする可能性があるのか』をきちんと調べることである。また、アクセスする可能性がある場合に、セキュリティ対策によって、アクセス可能なのか、不可とするべきなのかを切り分けて記述する必要がある。セキュリティ対策がない場合は『n/a』と記述し、すべて許可される。

アタックサーフェスリストの例は表 4.5-3 のとおりである。

表 4.5-3 アタックサーフェスリストの例

Access Point	記述	セキュリティ対策	アクセスコントロール	Access by:
AS.地上局 PC.標準入出力	地上局 PC.標準入出力	O.地上局 PC.ID パスワード	ALLOWS	A.オペレーター A.安全・セキュリティ担当者
		O.地上局 PC.ID パスワード	BLOCKS	A.地上局攻撃者
AS.地上局 PC.GCS	GCS アプリケーション	n/a	ALLOWS	T.地上局 PC.マルウェア混入 T.地上局 PC.GCS.マルウェア混入 AS.地上局 PC.標準入出力
AS.地上局 PC.USB	地上局 PCUSB ポート	O.地上局 PC.2 者監視	ALLOWS	A.安全・セキュリティ担当者
		O.地上局 PC.2 者監視	BLOCKS	A.オペレーター A.地上局攻撃者
AS.地上局 PC,SD カード	地上局 PCSD カード	O.地上局 PC.2 者監視	ALLOWS	A.安全・セキュリティ担当者
		O.地上局 PC.2 者監視	BLOCKS	A.オペレーター A.地上局攻撃者
AS.地上局 PC.Web	地上局 PC の Web 接続(地図情報等)	O.地上局 PC.ファイヤーウォール	ALLOWS	A.SDSP(80 番 In)
		O.地上局 PC.ファイヤーウォール	BLOCKS	A.地上局攻撃者
AS.地上局 PC.WiFi	地上局 PC の WiFi 接続経由	O.WiFi.WPA2	ALLOWS	AS.コンパニオン PC.WiFi
		O.WiFi.WPA2	BLOCKS	A.WiFi 攻撃者
AS.地上局 PC.LoRa	地上局 PC の LoRa 接続経由（USB）	n/a	ALLOWS	AS.コンパニオン PC.LoRa A.LoRa 攻撃者
AS.地上局 PC.LTE	地上局 PC の LTE 接続経由（Web と同義かも）	O.LTE.SSL 通信	ALLOWS	AS.コンパニオン PC.LTE
		O.LTE.SSL 通信	BLOCKS	A.LTE/5G 攻撃者
AS.プロポ.FHSS	プロポの FHSS 経由	O.FHSS.ホッピング	ALLOWS	A.オペレーター
		O.FHSS.ホッピング	BLOCKS	A.FHSS 攻撃者
AS.コンパニオン PC	コンパニオン PC ログイン	O.コンパニオン PC.USB キー制限	ALLOWS	A.メーカー整備車
		O.コンパニオン PC.USB キー制限	BLOCKS	A.安全・セキュリティ担当者 A.オペレーター A.コンパニオン PC 攻撃者
AS.コンパニオン PC.ガイドソフト	コンパニオン PC 搭載のガイドソフト	n/a	ALLOWS	T.コンパニオン PC.マルウェア混入
AS.コンパニオン PC.キルスイッチ	コンパニオン PC 搭載のキルスイッチ	n/a	ALLOWS	T.コンパニオン PC.マルウェア混入
AS.コンパニオン PC.SD カード	コンパニオン PC の SD カード	O.コンパニオン PC.2 者監視	ALLOWS	A.安全・セキュリティ担当者 A.メーカー整備者
		O.コンパニオン PC.2 者監視	BLOCKS	A.オペレーター A.コンパニオン PC 攻撃者
AS.コンパニオン PC.USB	コンパニオン PC の USB ポート	O.コンパニオン PC.2 者監視	ALLOWS	A.安全・セキュリティ担当者 A.メーカー整備者
		O.コンパニオン PC.2 者監視	BLOCKS	A.オペレーター A.コンパニオン PC 攻撃者
AS.コンパニオン PC.WiFi	コンパニオン PC の WiFi 接続経由	O.WiFi.WPA2	ALLOWS	AS.地上局 PC.WiFi
		O.WiFi.WPA2	BLOCKS	A.WiFi 攻撃者
AS.コンパニオン PC.LoRa	コンパニオン PC の LoRa 接続経由	O.LoRa.軽量暗号	ALLOWS	AS.地上局 PC.LoRa
		O.LoRa.軽量暗号	BLOCKS	A.LoRa 攻撃者
AS.コンパニオン PC.LTE	コンパニオン PC の LTE 接続経由	O.コンパニオン PC.LTE.入力制限	BLOCKS	AS.地上局 PC.LTE A.LTE/5G 攻撃者
AS.FC.FHSS	FC の FHSS 経由	O.FHSS.ペアリング	ALLOWS	A.オペレーター
		O.FHSS.ペアリング	BLOCKS	A.FHSS 攻撃者
AS.FC.SD カード	FC の SD カード	O.FC.CC 経由 SD カードロック	ALLOWS	AS.コンパニオン PC
		O.FC.メンテナンス経由 SD カードロック	ALLOWS	A.メーカー整備者
		O.FC.CC 経由 SD カードロック	BLOCKS	A.オペレーター A.安全・セキュリティ担当者 A.FC 攻撃者
AS.FC.USB	FC の USB	O.FC.CC 経由 USB ロック	ALLOWS	AS.コンパニオン PC
		O.FC.メンテナンス経由 USB ロック	ALLOWS	A.メーカー整備者
		O.FC.CC 経由 USB ロック	BLOCKS	A.オペレーター A.安全・セキュリティ担当者 A.FC 攻撃者
AS.GPS	GPS 信号への攻撃	n/a	ALLOWS	A.GPS 攻撃者
AS.独立キルスイッチ	独立キルスイッチへのアクセス	n/a	ALLOWS	A. 安全・セキュリティ担当者 A. LoRa 攻撃者

6） 脅威-対応リストの導出（活動 8）

脅威リストは、資産リスト、既存のセキュリティ緩和策リストから導出する。脅威を導出する際に、「航空局ガイドライン」で参照されている CIA や、セキュリティの脅威モデルである STRIDE を利用して、資産や既存の緩和策に対してどのような攻撃が可能かを調査することが可能である。

CIA によるモデル（JIS Q 27000:2014）:

- Confidentiality（機密性）: 認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性。
- Integrity（完全性）: 正確さ、および完全さの特性。
- Availability（可用性）:認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性。

STRIDE によるモデル（Microsoft）

- なりすまし（Spoofing）- 認証/真正性（Authentication/ Authenticity）
- 改竄（Tampering）- 完全性（Integrity）
- 否認（Repudiation）- 否認防止/責任追跡性（Non-repudiability/Accountability）
- 情報開示（Information disclosure）- 機密性（Confidentiality）
- サービス妨害(Denial of Service）- 可用性（Availability）
- 権限昇格（Elevation of Privilege）- 認可（Authorization）

脅威が脆弱性と結びつくと、攻撃可能性があるということで脅威事象が行われるリスクがあると定義できる。このため、発見されている脆弱性に、これらの脅威モデルを充てて、実際に最上位の脅威が引き起こされる可能性があるのかを調べることで、脅威を抽出することが可能である。

一方で、STRIDE を用いるのみでは具体性に欠けるため、STRIDE で解析される攻撃が引き起こされる具体例を考察する必要がある。例えば、なりすましであれば、機器の ID やパスワードが漏出し、それを利用されることなどである。これらの項目を具体的に用いて、脅威リストを作成する。表 4.5-4 はアタックサーフェスと STRIDE の相関表の例であり、相関表で示される内容を用いて脅威リストの名称として定義するとよい。

脅威リストの ID の接頭語は[T.]とする。

脅威リストの項目は以下のとおりである。

- ID: 共通 ID［T.］＋［システム名］＋［脅威事象名］
  - ［脅威事象名］: 具体的な脅威事象
- 対策: 脅威に対するセキュリティ対策の有無と具体的な対策［O］の参照
- アクセスポリシー: 対策に対応するアクセスポリシー（ALLOWS/BLOCKES）
- Access By: 脅威に直結するアタックサーフェス［AS］および攻撃者［A］の参照

最上位の脅威の値が SEV=5 で定義されているので、この脅威リストで占める大半の脅威は中間的な脅威として示される。各脅威の点に対する SEV は計算で示される。

表 4.5-4 アタックサーフェスと STRIDE の相関表

Access Point	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
AS.地上局 PC.標準入出力	不正侵入	マルウェア混入		ID/パスワード漏洩	地上局 PC ハングアップ	バックドア
AS. 地上局 PC.GCS	不正侵入	フライトデータ改竄 パラメータデータ書換	タスク完了否定		GCS サービス不能	
AS. 地上局 PC.USB		マルウェア混入				バックドア
AS.地上局PC,SD カード		マルウェア混入				バックドア
AS. 地上局 PC.Web	不正侵入	マルウェア混入		ID/パスワード漏洩	サービス不能攻撃	バックドア
AS. 地上局 PC.WiFi	ARP Spoofing	テレメトリ情報改竄 コマンド改竄		WiFi 設定情報漏洩	WiFi サービス不能攻撃	
AS. 地上局 PC.LoRa		テレメトリ情報改竄 キル情報不正送出				
AS. 地上局 PC.LTE		テレメトリ情報改竄				
AS.プロポ.FHSS	FHSS 信号乗っ取り	FHSS 信号改竄		ホッピングパターン漏洩 ペアリング漏洩		
AS.コンパニオン PC	不正侵入 FC への DoS 攻撃 UART/SPI/CAN 乗っ取り	マルウェア混入		ID/パスワード漏洩	コンパニオン PC ハングアップ	バックドア
AS.コンパニオン PC.ガイドソフト	不正侵入	ガイダンスコマンド改竄 キル情報不正送出	緊急コマンド受付否定		ガイドソフト不能攻撃	
AS.コンパニオン PC.キルスイッチ	キルスイッチ乗っ取り	キル情報不正受信				
AS.コンパニオン PC.SD カード		ファーム改竄 マルウェア混入				バックドア
AS.コンパニオン PC.USB		ファーム改竄 マルウェア混入				バックドア
AS.コンパニオン PC.WiFi	地上局信号乗っ取り	コマンド改竄 テレメトリ改竄				バックドア
AS.コンパニオン PC.LoRa		テレメトリ改竄				
AS.コンパニオン PC.LTE		テレメトリ改竄				
AS.FC.FHSS		FHSS 不正信号受信				
AS.FC.SD カード		ファーム改竄 マルウェア混入				バックドア
AS.FC.USB		ファーム改竄 マルウェア混入				バックドア
AS.GPS		GPS 位置不正信号受信				
AS.独立キルスイッチ		キル情報不正受信	キル否認			

脅威リストの例は表 4.5-5 のとおりである。

表 4.5-5 脅威リストの例

脅威点	記述	対処	ポリシー	Access By:
T.地上局 PC.ハイジャック	地上局 PC がハイジャックされ、地上局 PC の権限を奪われる	n/a	ALLOWS	A.オペレーター A.安全・セキュリティ管理者 A.整備担当者 AS.地上局 PC.Web AS.地上局 PC.WiFi
	地上局 PC の ID/ログイン情報が漏洩することで、不正侵入される	O.地上局 PC.定期パスワード更新	BLOCKS	A.地上局 PC 攻撃者
T.地上局 PC.ID/パスワード漏出	地上局 PC の ID/pass が漏出し、外部から侵入可能となる	O.地上局 PC.定期パスワード更新	ALLOWS	A.オペレーター A.安全・セキュリティ担当者
			BLOCKS	A.地上局 PC 攻撃者
T.地上局 PC.マルウェア混入	地上局 PC にマルウェアが混入され、地上局 PC に対して DoS やサービスに対する攻撃が可能となる	O.地上局 PC.エンドポイントセキュリティ	ALLOWS/ BLOCKS	AS.地上局 PC.USB AS.地上局 PC.SD カード AS.地上局 PC.Web
T.地上局 PC.ハングアップ攻撃	地上局 PC に対して高負荷を掛けてハングアップさせるなどの DoS 攻撃を仕掛ける	O.地上局 PC.エンドポイントセキュリティ	BLOCKS	AS.地上局 PC.USB AS.地上局 PC.SD カード AS.地上局 PC.Web
T.地上局 PC.バックドア	地上局 PC に対してバックドアを仕掛ける	O.地上局 PC.エンドポイントセキュリティ	BLOCKS	AS.地上局 PC.USB AS.地上局 PC.SD カード AS.地上局 PC.Web
T.地上局 PC.標準入出力.不正侵入	ID/ログイン情報の漏洩などによって不正に侵入される	O.地上局 PC.二者監視	ALLOWS	A.オペレーター A.安全・セキュリティ管理者 A.整備担当者
			BLOCKS	A.地上局 PC 攻撃者
T.地上局 PC.GCS.不正侵入	GCS に対して不正侵入を行う	n/a	ALLOWS	AS.地上局 PC.標準入出力
T.地上局 PC.GCS.マルウェア混入	GCS にマルウェアが混入され、GCS に不備をきたす	O.地上局 PC.マルウェアチェック	BLOCKS	AS.地上局 PC.USB AS.地上局 PC.SD カード AS.地上局 PC.Web
T.地上局 PC.GCS.パラメータデータ書換	GCS 利用パラメータが故意に書き換えられて不備をきたす	n/a	ALLOWS	AS.地上局 PC.標準入出力 A.地上局 PC 攻撃者
T.地上局 PC.GCS.タスク完了否定	機体システムからのタスク完了信号の否定によってタスク移行が行われない	n/a	ALLOWS	A.地上局 PC.WiFi A.地上局 PC.LoRa A.地上局 PC.LTE
T.地上局 PC.GCS.GCS サービス不能	GCS に DOS 攻撃がしかけられ不能をきたす	n/a	ALLOWS	AS.地上局 PC.Web AS.地上局 PC.WiFi AS.地上局 PC.LoRa AS.地上局 PC.LTE
T.地上局 PC.マルウェア混入	地上局 PC にマルウェアが混入され、地上局 PC が不能となる	O.地上局 PC.マルウェアチェック	BLOCKS	AS.地上局 PC.USB AS.地上局 PC.SD カード AS.地上局 PC.Web
T.地上局 PC.WiFi.DOS	地上局 PC の WiFi 部ネットワークが不能にされる	O.地上局 PC.WiFi.MAC 接続制限	BLOCKS	AS.地上局 PC.WiFi
T.地上局 PC.WiFi.ネットワークパラメータデータ書換	地上局 PC の WiFi 部パラメータが毀損されて QoS が悪くなる	n/a	ALLOWS	AS.地上局 PC.Web AS.地上局 PC.WiFi

…

7） 既存のセキュリティ緩和策リストの導出（活動 9）

既存のセキュリティ緩和策リストは、アタックサーフェスリストおよび脅威リストとともに導出される。アタックサーフェスに対して対策が施されている場合、脅威に対して対策が施されている場合に ID が付与され、それらをリストとしてまとめるのがこの部分である。

既存のセキュリティ緩和策リストの ID の接頭語は[O.]とする。

既存のセキュリティ緩和策リストの項目は以下のとおりである。

- ID: 共通 ID [O.] + [所在名]+ [緩和策]
  - [緩和策]: セキュリティ対策の内容（検査、照合、パスワード、フィルタ、暗号化、期限設定、データ最小化、堅牢化）

- 記述: セキュリティ対策の記述
- 脆弱性クラスおよび脅威: セキュリティ対策を通過する可能性のある脆弱性［F］および脅威事象［T］の参照（セキュリティに対する迂回路は記述しない）

既存のセキュリティ緩和策リストでは、セキュリティを突破される場合についての保護レベルについて記述はしない。この部分は脆弱性クラスリストで示す。また、セキュリティ緩和策を講じている場合においても、そこから発生する脅威があることも考慮に入れる必要がある。

既存のセキュリティ緩和策リストの例は表 4.5-6 のとおりである。

表 4.5-6 セキュリティ緩和策リストの例

セキュリティ緩和策	記述	脆弱性クラスまたは脅威事象
O.地上局 PC.ID パスワード	ID とパスワードによる地上局 PC のアクセス制限	T.地上局 PC.ID パスワード漏出 F.地上局 PC.ID パスワード
O.地上局 PC.2 者監視	地上局 PC の利用で、2 者監視で相互監視を行う	F.地上局 PC.2 者監視
O.地上局 PC.ファイヤーウォール	ファイヤーウォール設定による外部からの PC アクセスの遮断	F.地上局 PC.ファイヤーウォール
O.WiFi.WPA2	WPA2 設定による WiFi ネットワークの堅牢化	F.WiFi.WPA2
O.LTE.SSL 通信	SSL 通信によるデータの暗号化	F.LTE.SSL 通信
O.FHSS.ホッピング	ホッピングパターンによる RC 信号の隠蔽	T.FHSS.ホッピングパターン漏出
O.コンパニオン PC.USB キー制限	USB キー制限を付けることによるコンパニオン PC アクセス制限	T.USB キー盗難
O.コンパニオン PC.2 者監視	コンパニオン PC の更新で、2 者監視で相互監視を行う	F.コンパニオン PC.2 者監視
O.コンパニオン PC.LTE.入力制限	コンパニオン PC に対する LTE からの入力制限（出力のみにする）	F.コンパニオン PC.LTE.入力制限
O.FHSS.ペアリング	FHSS ペアリングによる機器接続制限	F.FHSS.ペアリング
O.FC.CC 経由 SD カードロック	CC 経由での SD カードのロック機構	F.FC.カードロック
O.FC.メンテナンス経由 SD カードロック	メンテナンスポート経由での SD カードのロック機構	F.FC.カードロック
O.FC.CC 経由 USB ロック	CC 経由での USB のロック機構	F.FC.USB ロック
O.FC.メンテナンス経由 USB ロック	メンテナンスポート経由での USB のロック機構	F.FC.USB ロック
O.地上局 PC.マルウェアチェック	地上局 PC でのマルウェアチェック	F.地上局 PC.マルウェアチェック
O.地上局 PC.定期パスワード更新	ID パスワード漏出対策としてのパスワード更新	F.地上局 PC.定期パスワード更新
O.地上局 PC.WiFi.MAC 接続制限	MAC 接続制限による WiFi アクセス制限	F.地上局 PC.WiFI.MAC 接続制限

8） 脆弱性クラスリストの導出（活動 9）

セキュリティ緩和策に紐づく脆弱性クラスとは、緩和策が完全でないことを示し、かつ緩和策の限界を正しく記述するものである。脆弱性クラスの導出には、既存のセキュリティ緩和策について評価が必要である。ここでは、第二種型式認証のために、簡易的な基準を設けて防御レベル(LoP)を定義する。

脆弱性クラスリストの ID の接頭語は[F.]とする。

脆弱性クラスリストの項目は以下のとおり。

- ID: 共通 ID［F.］＋［所在名］＋（［対策］or［脆弱性］）
  - ［対策］: セキュリティ対策の内容(対応する[O.]と同様のサブ ID)

- [脆弱性]: その他セキュリティ対策に対する脆弱性表記 （一般脆弱性を含む（Common））

- 記述: 脆弱性の内容の記述
- 防御レベル（LoP): 現在の保護状況の防御レベル
  - 暗号化，システム的なセキュリティ対策: LoP = 3
  - パスワード、ID などによるセキュリティ対策: LoP = 2
  - 人為的なスクリーニングなどによるセキュリティ対策 : LoP = 1
- 他セクションへの関係性の記述
  - ICA:「セクション 205」で適正に扱われるべき対策
  - 飛行規程:「セクション 200」で適正に扱われるべき対策
  - 110:「セクション 110」へ要求として送られる対策

防御レベルについては簡易的な指標として掲示している。暗号化など、性能が保証されている保護については LoP＝3 を付与する。また、パスワードや ID 管理によるアクセス制限など、標準的な機械による保護は LoP＝2 を付与する。人為的な制限・制約による保護は LoP＝1 を付与するとした。

脆弱性クラスリストの例は表 4.5-7 のとおり。

表 4.5-7 脆弱性クラスリストの例

脆弱性クラス	記述	LoP	ICA	飛行規程	110
F.地上局 PC.ID パスワード	弱いパスワード、ID の対	2	✓	✓	
F.地上局 PC.2 者監視	二者監視を怠った	1	✓		
F.地上局 PC.ファイヤーウォール	ファイヤーウォールの設定ミス	2	✓		
F.WiFi.WPA2	WPA2 の設定の脆弱性	3		✓	
F.LTE.SSL 通信	SSL 通信設定の脆弱性	3		✓	
F.コンパニオン PC.2 者監視	2 者監視を怠った	1	✓		
F.コンパニオン PC.LTE.入力制限	入力制限設定ミス	2			
F.FHSS.ペアリング	ペアリングの重複	3		✓	
F.FC.カードロック	カードロックが機能していない・設定ミス	3			
F.FC.USB ロック	USB ロックが機能していない・設定ミス	3			
F.地上局 PC.マルウェアチェック	マルウェアチェックを怠る/すり抜け	2	✓		
F.地上局 PC.定期パスワード更新	パスワード更新を怠る	1	✓		
F.地上局 PC.WiFI.MAC 接続制限	MAC 接続制限を怠る	2		✓	

9） 脅威木の導出（活動 10）

(1)から(8)までの情報を踏まえて、脅威木解析を行う。脅威木解析で用いる情報は、以下のリストである。

- 攻撃者リスト［A.］
- 資産リスト［I.］
- アタックサーフェスリスト［AS.］
- 脅威リスト［T.］

- セキュリティ緩和策リスト［O.］
- 脆弱性クラスリスト［F.］

なお、それぞれの接続関係は以下のとおりで整理される。

- CanAccess: アクセス可能（（A｜AS）→ T，（A｜AS｜T）→ AS））
- Find: 脆弱性の発見（A → F）
- AllowedBy: 許可される（(A｜AS）→ O）
- BlockedBy; 拒否される（(A｜AS）→ O）
- Defeats: 破られる（(F｜T）→ O）
- CanImpact: 衝撃を与える/危害を加える（T → I）
- Protects: 保護する（O →（AS｜T））

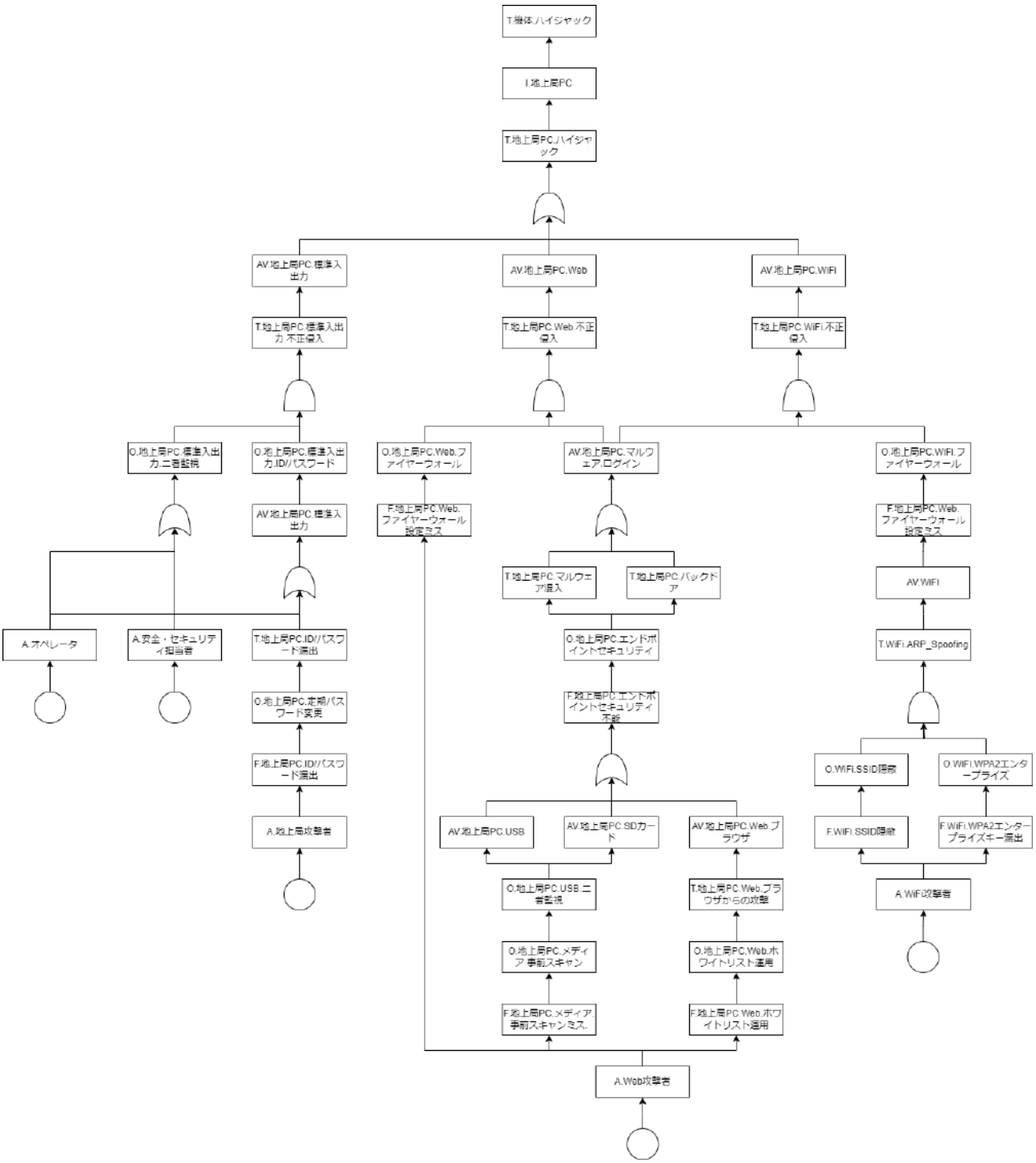


図 4.5-3 脅威木解析の一例: 地上局 PC へのハイジャックの脅威

- Occurring: 最上位の脅威事象が発生する（I → T）

この接続関係を、最上位の脅威事象から木構造にまとめていく。

脅威木解析の例を図 4.5-3 に示す。また、脅威木で扱われる結合のパターンを図 4.5-4 に示す。

なお、脅威木解析にでは、(1)から(8)までの情報を用いながら解析を行うが、実態と整合が合わない、もしくは修正が必要である考察が脅威木解析中に得られる場合がある。その場合、脅威木解析で

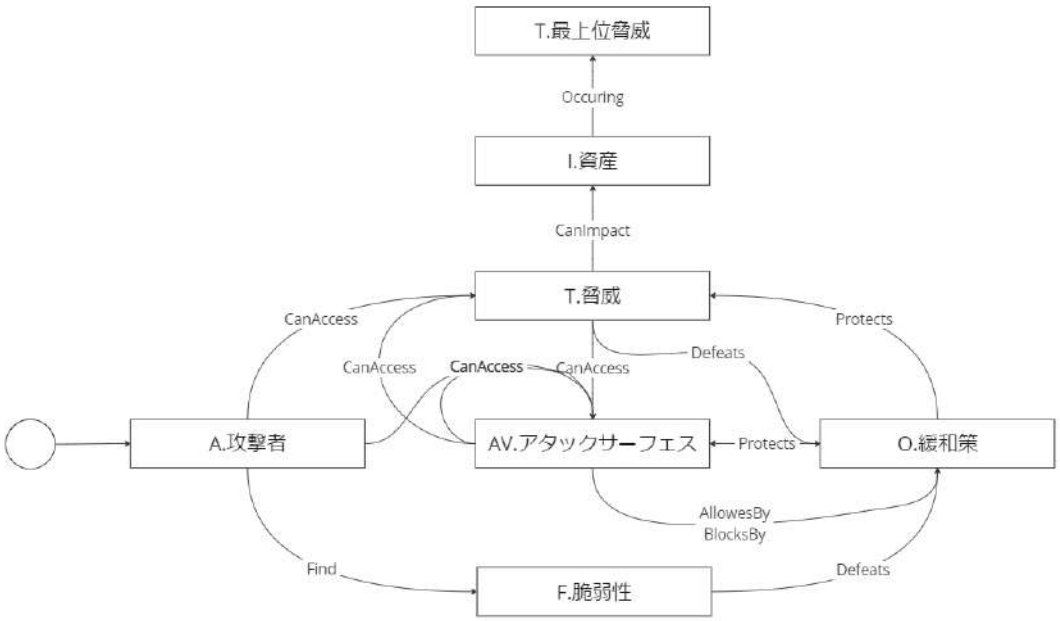


図 4.5-4 脅威木解析で扱われる各リストの結合の仕方

提案される他の表の項目が追加もしくは削除される場合の項目が発生し、(1)から(8)までの情報にフィードバックされることになる。そのため、(1)から(8)の活動と、脅威木解析はリスクアセスメントにおける両輪となるような形の活動となる。

10) カットセットリストの導出（活動 11）

カットセットとは、各脅威シナリオにおける木構造で示されたグラフの部分集合である。カットセットの抽出に関しては、『攻撃者』が『脆弱性』ないし『アタックサーフェス』を発見した際にイベントが発生するとして考察する。

カットセットリストの項目は以下のとおり

- カットセット ID
- 攻撃者 – 攻撃者 ID
- 顕在化する脆弱性 – 脆弱性リスト ID もしくは none.
  - カットセットは攻撃者と顕在する脆弱性の 2 項目の積として表現されて一意であるべきである
- 侵害される資産と緩和策 – 資産に至る経路に存在するすべてのアタックサーフェス、緩和策、脅威
- 基本イベント – 脅威木解析における葉の固有 ID
- 攻撃者に与えられている脅威レベル（A.LoT）
- 顕在化する脆弱性に与えられている直接の保護レベル（F.LoP）
- 出発地点に存在する脅威レベル（DS=A.LoT-F.LoP）

- 資産に存在する重大度（SEV）
- 資産までの中間に与えられている緩和策の保護レベルの和（T.LoP）
- 残存リスク重大度（RES = SEV-(T.LoP+(5-DS)))

このカットセットリストを用いることで、残存リスク重大度を計算し、それが 0 以下になることを目標に、緩和策を追加する。カットセットリストのすべての残存リスク重大度が 0 以下になれば、セキュリティリスクは許容可能である。

カットセットリストの例は表 4.5-8 のとおりである。

表 4.5-8 カットセット表例

CU ID	Attaker	Vulnerability	Threat and Measure	BE ID	[A] LoT	[F] LoP	Assets SEV	LoP sum	Res. SEV
CU1	A.オペレーター	n/a	O.地上局 PC.標準入出力.ID/パスワード O.地上局 PC.標準入出力.二者監視 T.地上局 PC.標準入出力.不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE1	1	0	5	3	-2
CU2	A.安全・セキュリティ担当者	n/a	O.地上局 PC.標準入出力.ID/パスワード O.地上局 PC.標準入出力.二者監視 T.地上局 PC.標準入出力.不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE2	1	0	5	3	-2
CU3	A.地上局攻撃者	F. 地上局 PC.ID/パスワード漏出	O.地上局 PC.定期パスワード変更 T.地上局 PC.ID/パスワード漏出 O.地上局 PC.標準入出力.ID/パスワード O.地上局 PC.標準入出力.二者監視 T.地上局 PC.標準入出力.不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE3	2	1	5	3	-2
CU4	A.Web 攻撃者	F. 地上局 PC.Web. ファイヤーウォール設定ミス F.地上局PC.メディア事前スキャンミス	O.地上局 PC.メディア事前スキャン O.地上局 PC.メディア.二者監視 T.地上局 PC.メディア.挿入時マルウェア感染 O.地上局 PC.エンドポイントセキュリティ T.地上局 PC.マルウェア混入 O.地上局 PC.Web.ファイヤーウォール T.地上局 PC.Web.不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE4	4	2,2	5	2	-2
CU5	A.Web 攻撃者	F. 地上局 PC.Web. ファイヤーウォール設定ミス F. 地上局 PC.Web. ホワイトリスト運用	。.地上局 PC.ホワイトリスト運用 T.地上局 FC.Web.ブラウザからの攻撃 O.地上局 PC.エンドポイントセキュリティ T.地上局 PC.マルウェア混入 O.地上局 PC.Web.ファイヤーウォール T.地上局 PC.Web.不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE5	4	2,1	5	2	-1
CU6	A.WiFi 攻撃者	F.WiFi.SSID 隠蔽ミス F.WiFI.WPA2 エンタープライズキー漏出 AS, 地上局 PC.マルウェアログイン	O.WiFI.SSID 隠蔽 O.WiFi.WPA2 エンタープライズ T.WiFi.ARP_Spoofing O.地上局 PC.WiFi ファイヤーウォール T.地上局 PC.バックドア T.地上局 PC.マルウェア混入 T.地上局 PC.WiFi 不正侵入 T.地上局 PC.ハイジャック T.機体.ハイジャック	BE6	3	2,2,2	5	2	-5

（3） 緩和策の適合性検査

1） 緩和策の実施

特定されたリスクに対処するために、適切な緩和策を実施する。これには、セキュリティ機能の導入や既存の機能の強化、ネットワーク設定の変更などが含まれる。

表 4.5-9 に、サイバーセキュリティリスクと緩和策を例示する。

表 4.5-9 サイバーセキュリティリスクと緩和策例

No.	サイバーセキュリティリスク例	緩和策事例
1	制御システムへの不正アクセス	・強力な認証手段や二要素認証を実装 ・暗号化技術を使用して通信を保護
2	不正なデータ送信および偽装信号	・強固な暗号化を使用 ・デジタル署名による信頼性向上 ・信号認証を確認するセキュリティプロトコルを実装
3	ファームウェアやソフトウェアに存在する脆弱性の悪用	・定期的かつ自動的なセキュリティアップデート実施 ・最新のセキュリティパッチ適用 ・セキュリティテストを通じた脆弱性の発見

2） 検証とテスト

導入された緩和策が期待どおりに機能するかを確認するために、適切な検証とテストを実施する。これは、セキュリティ要件の満たし、機能の適正な動作を確認することを含む。

3） 文書化

実施されたすべての適合性検査の結果やプロセスは、適切に文書化する。これには、導入された緩和策の詳細な説明やテストの結果が含まれる。

4） 監視と継続的改善

サイバーセキュリティリスクは常に進化するため、定期的な監視と継続的な改善が不可欠である。新たな脅威に対応するために、システムのセキュリティポリシーと手順を適宜更新する。

（4） 未知の脆弱性に対する反駁解析

反駁解析（Refutation Analysis）とは、実施されている緩和策やシステムの堅牢性について反証を与え、その中で正しくリスクが緩和されているかについて検査するものである。

既知の脆弱性についてはもちろん、未知の脆弱性について、個別のシステムおよびシステム全体に対して解析を行い、脆弱性を発見していくことが反駁解析の目的である。

1)　ファジング・テスト

ファジング・テスト（ファジング）は、無効、不正、または予期しない入力をシステムに挿入してソフトウェアの欠陥や脆弱性を明らかにする自動化されたソフトウェア・テスト手法である。

ファジング・ツールは、システムにこれらの入力を挿入し、クラッシュや情報漏洩などの例外を監視します。つまり、ファジングはシステムに予期しない入力を与え、セキュリティ、パフォーマンス、品質のギャップや問題を示す入力がシステムに悪影響を与えるかどうかを監視する。

IPA より「ファジング活用のてびき」という資料が示されているほか、ファジングのためのツールがオープンソースなどで提供されている。

第二種型式認証においては、システムレベルの記述によるリスクアセスメントを行うために、システムのインターフェースに対するテストが有効である。このため、第二種型式認証では、ファジングは推奨される。

2)　ペネトレーション・テスト

ペネトレーション・テスト（ペンテスト）とは、日本語で「侵入テスト」を意味し、システム全体の観点でサイバー攻撃耐性がどのくらいあるかを試す為に、悪意のある攻撃者が実行するような方法に基づいて実践的にホワイトハットハッカーがシステムに侵入するテストを指す。

いわゆる「模擬ハッキング」を行うため、技術レベルの高い攻撃手法を行うことのできるセキュリティの専門家により、あらゆるハッキング技術やツールを使って脆弱な箇所に攻撃を行う。これを通して、セキュリティ機能の回避または無効化を試みながらシステム内部へ侵攻できるかについてテストをする。

ペンテストの際には、システム設計の構成図があれば、より深化した攻撃を行うことができる。一方で、多岐にわたるセキュリティの専門知識と機材が必要であるため、第二種型式認証においては特に推奨することはない。

（5）　継続的なセキュリティ保証のための活動指針

継続的なセキュリティ保証のためには、型式認証の申請者のみならず、使用者との間で取り決められたセキュリティ保証活動の計画に基づいて、活動する必要がある。基準となる証拠は型式認証において作成されたドキュメントであり、特にカットセットリストはセキュリティインシデントが発生した際に、影響するイベントと対応する残存リスクの数値の変化を評価するのに重要な情報となりうるため、申請者はバージョン管理などを行って慎重に管理すべきである。

有人航空機の継続的なセキュリティ保証活動の指針については RTCA DO-355A/EUROCAE ED-204A に記載されている。一方で、無人航空機において、有人航空機のように整備担当者や運用者、メーカーなどの責任関係が正しく分割されているわけではなく、また、ICA や飛行規程などの記載と実際の運用についての乖離がある場合、セキュリティインシデント発生時の型式に対する改善点などの評価は難しい。

そのため、この活動指針ではごくごく一般的な視点を検討する。

1)　継続的なサイバーセキュリティ保証のための一般的な考え方

継続的なサイバーセキュリティ保障のためには、電子的かどうかに関わらず、サイバーセキュリティの 3 つの一般的な領域（予防、検出、対応）に対処する必要がある。これらについて、どのように定義し、対策するかを検討することが、継続的なサイバーセキュリティ保障にとって重要である。また、この項目は、セクション 205 に記載されるほか、実際の飛行のときに必要な場合はセクション 200 に記載されるように指示が必要となる。

a. 予防:

予防は問題の発生を未然に防ぐことをいう。技術的、人的および組織的にそれぞれ予防策を講じることが重要である。サイバーセキュリティの目標は、セキュリティインシデントや侵害を防ぐことであり、予防は最も費用対効果の高い戦術であるが、詳細な行動計画が必要である。対策としては、技術的、人的、組織的という 3 つの視点がある。

技術的な予防として、サイバーセキュリティ要件をあらかじめシステムに組み込む。例えば、暗号化プロトコルの設定など、無人航空機のシステムの構築段階で適切な策を講じる。適切な策とは、サイバーセキュリティアセスメントプロセスにて評価されたカットセットに対して十分な技術的な対策を挿入することで、強化が可能である。

人的な予防として、組織でサイバーセキュリティ意識の文化を構築し、無人航空機システムのサイバーセキュリティリスクを理解するようにトレーニングを行う必要がある。また、ISO 21384-3 に記載されているセキュリティ担当者を決めて、正しく運用におけるサイバーセキュリティの管理を行うようにする必要がある。

組織的な予防として、問題発生時に報告すべき関係者を事前に洗い出し、即時対応できるよう手順書を準備する。また、専門の第三者に依頼し、セキュリティについてのアドバイスと監督を受けることで、より高度なセキュリティ予防策を講じることが可能となる。

b. 検出:

検出は、将来の攻撃から防御するために、ネットワークを監視し、それらの試みをできるだけ早く見つけることである。ほとんどのセキュリティインシデントは、システムログとネットワークログに表示されるイベントから始まる。セキュリティと運用に脅威をもたらす技術的なソースとレポートからイベントを特定できるならば、セキュリティ侵害を完全に防ぐために何を行うべきかを判断できる。

ネットワーク、ログ、レポートの監視と評価は、定期的かつ継続的なタスクである必要がある。また、組織内のすべてのユーザーを含む検出の技術的戦略を実装する必要がある。技術的な検出方法としては、侵入検知システム（IDS）や侵入防止システム（IPS）の導入が挙げられる。また、人的、組織的な方法として、システムやネットワークログの定期的なレビュー、またシステムの異常動作やパフォーマンスの低下のサインを迅速に捉えられるようにトレーニングするなどの方法が挙げられる。

c. 対応:

対応とは、実際にセキュリティインシデントが起こった場合にどのように対処するかを決定することで

ある。つまり、問題の発生時にどのように行動するかを具体化し、リスクに応じて実行可能な対応計画を事前に策定する。これにはサイバーセキュリティイベントの発生時に即座に対応する手順書を準備すること、運用者やメーカーなどの適切な関係者に情報を迅速に報告することを定義し、攻撃の影響を最小限に抑える行動を取ることなどが挙げられる。なお、このような関係者の定義については、運用中に対しての整備計画として事前に記述する必要がある。

対応のための計画では、次のことについて考慮する必要がある。

- 何が「インシデント」と見なされるかを定義する。これは企業ごとに異なる。
- サイバーセキュリティとセキュリティインシデント対応に関する明確なポリシーを確立する。
- セキュリティインシデントが特定されたときに警告する主要な担当者（インシデント対応チーム）を決定する。
- セキュリティインシデントが発生した場合の参照用にすべてを記録して監視する。
- 組織内およびその他の関係者とインシデントを報告、通知、および伝達するためのプロトコルを作成する。
- フォレンジック（鑑識調査および法的証拠）要素を含めた計画を立てる。法的義務に対する行動を擁護し、ビジネスを安全に運営するための防御可能なプロセスを文書化できる。

なお、対応で必須となる項目は、運用者やメーカーなどの適切な関係者に情報を迅速に報告することである。報告を受けた者は、事前に準備した手順書にしたがって行動することで、攻撃の影響を最小限に抑える。

2） 継続的なセキュリティ保証のために対策すべき項目

a. 機体搭載ソフトウェア

機体に搭載するソフトウェアは基本的に運用者がメンテナンスする部分はなく、ファームウェアアップデートなどの操作についても基本的にはメーカーもしくは整備者が行うものである。そのため、機体ソフトウェアの更新などはICAに記載されている手順により行われるものとする。一方で、機体内に保持されているデータの取り回しに関しては運用者も行う場合があることから、飛行規程や ICA、その他マニュアルなどに記載されるべきである。

機体ソフトウェアに関わるセキュリティインシデントは安全性に関わる部分が非常に大きいこと、またエンドポイントのセキュリティ対策が難しいため、ファームウェアアップデートには十分に気を付けてデータの取り回しを行うべきである。

ソフトウェアの配布についての一般的なセキュリティ手法は以下のとおり

- メディアベース配布の場合は、的確な資格情報を持つ、物理的に安全な環境に居る信頼できる人に、物理メディアを準備、ラベル付け、パッケージ化し、対象の受信者に送信させることによって実装される。
- 電子的なソフトウェア配布の場合、公開／秘密鍵暗号方式を使用してファイルに 1 つ以上の暗号署名を添付する手段を使用し、完全性と信頼性を実装すべきである。ソフトウェアパッケージ

を送信する前に、デジタル署名を関連付けることも可能である。

運用に対するセキュリティ緩和策は以下のとおり

- ソフトウェアの受け取り: 信頼性と完全性の確認。デジタル署名、密封された封筒などによって配布時における攻撃を防ぐ。
- 作成・変更:「セクション 110」に準拠している方法で構築されたソフトウェアであることを確認する。
- 保管: 無人航空機の機体ソフトウェアを地上で保管する場合は、ソフトウェアの完全性と機密性を保護するために、不正アクセスを防止・検出するのに暗号化、鍵のかかった部屋、パスワードなどの十分なセキュリティ対策を実装する。
- メディア: メディア本体にマルウェアなどの悪意のあるコードが含まれていないことを確認する。また、メディア本体のライフサイクル全体にわたって悪意のあるコードから保護され、検証できることを確認する。バージョンなどの管理のために、適切なラベルがつけられていることを確認する。
- ソフトウェアツール:ソフトウェアツールの実行に使用される機器を安全に保ち、不正なコードが含まれないようにし、この機器の構成を制御するべきである。つまり、この機器にインストールされているソフトウェアツールの完全性と信頼性を検証する。
- ソフトウェアの配布: 機体ソフトウェアの転送は、ソフトウェアのアクセス、管理、および保存を運用者によって許可された担当者のみが実行するべきである。
- データのロード: ソフトウェアを無人航空機にロードする前に、機体ソフトウェアの信頼性と整合性を検証する。ICA にしたがって、機体搭載ソフトウェアがロードされていることを確認する。
- 機密保持: 必要に応じて、情報が無許可の団体に利用可能になったり、開示されたりしないようにすることを目的とした機密性が、無人航空機搭載ソフトウェアのライフサイクル全体(廃止を含む)にわたって維持されるようにするべきである。
- 事故管理: 情報セキュリティインシデントを報告および調査して、安全への影響を適切に把握し、将来のセキュリティを向上できるようにするべきである。

b. ネットワークアクセスポイント

無人航空機および地上におけるネットワークのアクセスポイントについて、適正に機器間の接続許可設定を行う必要がある。機器間の接続許可設定には、主として無線電波であり、周波数の管理とプロトコルの管理、およびそれらのエンドポイントに搭載されるセキュリティ対策を考慮する必要がある。

- C2 リンク（プロポ、WiFi、LTE、5G など）
- 運行管理情報（テレメトリ、UTM などに接続するための回線）
- 安全に関する機器を接続する特別な無線（パラシュート、キルスイッチなど）
- 映像など受送信機

アクセス制御手段は物理的に保護することが難しいため、物理的に制限されていないエリアにあるネットワークアクセスポイントには、より高度な電子制御が必要である。そのため、無人航空機のアクセ

スポイントを安全に管理するために、運用上のセキュリティ対策が必要な場合がある。

- ネットワークアクセスポイントの明示と制限エリアの識別、表示
- ネットワークアクセスポイントと制限エリアの監視、保護、安全確保

c. 地上局における情報システム

地上局の情報システムには、無人航空機の操縦や制御点などを与えるようなグラウンドコントロールステーションなども含まれる。これらのソフトウェアからセキュリティが侵害される恐れがあることから、無人航空機システムにデジタル接続する機器・ソフトウェアに対して、セキュリティを担保する必要がある。

地上局における情報システムに対するセキュリティ緩和策は以下のとおり。

- 機器のセキュリティと運用管理:
  - 地上局における情報システムに対するエンドポイントセキュリティを確立し、様々なセキュリティ攻撃に対して対応可能とすること。
  - 機器へのアクセスは許可された担当者のみに制限すること。
  - 不要なソフトウェアの追加を避け、ソフトウェアやハードウェア構成を管理すること。
  - 内部の特権の原則を使用して、アクセスを必要最小限に制限すること。
  - 常に効果的な技術的脆弱性管理を実行して、機器上の脆弱性を特定、評価し、対応する。（OS のセキュリティアップデートのインストールなどを通じて）
- アクセスコントロール:
  - 管理者と整備車のタスクに関する機器・ソフトウェアのアクセス権を定義する。
  - 機器・ソフトウェアへのすべてのリモートアクセスを制限および保護する。
  - ユーザーのライフサイクルを管理するための ID およびアクセス管理プロセスを確立する。
  - ユーザーおよびアカウントの一元管理を検討する。
  - 場合によっては二要素認証などを用いてアクセス制限を厳密化する。
- 使用法:
  - 地上局における情報システムの使用者は、組織によって認可された担当者のみが使用すること。
  - 地上局における情報システムのメンテナンス作業は、この目的のために認可された整備者のみ実行すること。
  - 紛失、破損、盗難された場合、または安全ではない場所に放置された場合は社内に報告すること。
- 保管:
  - 保守組織の安全な場所を定義して、適切な管理お酔い物理的な管理が施された場所に保

管すること。

- 保管場所から取り出す際の機器の移動について記録すること。
- 事故管理: 情報セキュリティインシデントを報告および調査して、安全への影響を適切に把握し、将来のセキュリティを向上できるようにすること。

- ライフサイクル管理: 地上局における情報システムは、そのライフサイクル中に管理する必要があるため、ツールまたはオペレーティングプラットフォームで脆弱性が特定された場合は、ツールプロバイダーと連携して適切な緩和策を決定すべきである。
- 廃止措置: 適切なサイバーセキュリティプロセスを使用して、廃止された情報システムからデータを復元できないようにする。

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定) 項目は以下の通り。

5.1 115 サイバーセキュリティ適合性証明書例

サブ WG 内で適合性証明関連書類(適合性証明計画書、適合性証明完了報告書)を作成し、その適合性証明書類に対して模擬的に適合性の一連の確認を行うことを予定していたが、未議論となっている。

5.2 運用の状態によるユースケース毎の考察

運用の時系列的に複数ユースケースが存在する。特に、正常な運用は、フライトフェーズによってユースケースが異なる可能性があることから、保管時、運用前、運用中、運用後などのフライトフェーズに分けて記載することが望ましい。一方で、本解説書では運用の状態についての詳細なセキュリティ環境の変化については未検討である。詳細なセキュリティ環境の変化については、次稿以降の調査とする。

5.3 より簡便なセキュリティリスクアセスメントの手法の検討

本解説書で記載した内容としては、リスクアセスメントとして充足する方法を提示し、その中で簡単化するために、5段階の定性表現を用いた手法とすること、システムレベルでの検討とすることとして扱った。一方で、セキュリティリスクアセスメント自体が、非常に難易度が高いものであることから、より簡便な手法を検討する必要がある。なお、以下の点について考慮する必要がある。

- セキュリティリスクアセスメントの中には、2つの評価が存在する
  - セキュリティアセスメント (セキュリティ評価)
    - セキュリティ評価および分析は、『セキュリティ制御または制御ファミリに関連する要件を評価』する。
    - CIA(機密性、完全性、可用性)を保護するために使用。
    - セキュリティ制御のソリューションが実装されると要件は満たされる。
  - リスクアセスメント (リスク評価)
    - 脅威の特定、脆弱性の判断、システムの影響の評価を通して、(凡そ)定量化されたレベルによるリスクの見積もりを行う。
    - L(尤度) x I (影響度) = R(リスク)

これらのことを踏まえて、今後第第二種型式認証で利用できるリスクアセスメント手法を検討する。

Appendix 1　証明手順例など

A.1. 型式認証対象とするモデルケース例

DRAFT2 にて追記予定

（1）　想定する機体・システムの例

（2）　CONOPS 記載内容の例

A.2. セキュリティ適合性証明計画書例

DRAFT2 にて追記予定

1286 Appendix 2 各セクション特有の用語集

用語	解説	出典
アクセス （Access）	システム資源を使用するためにシステムに対して通信またはその他の対話を行う能力および手段	IEC/TS 62443-1-1:2009
アクセスコントロール （Access Control）	認可されていないアクセスからのシステム資源の保護	IEC/TS 62443-1-1:2009
アクティビティ図 （Activity Diagram）	高水準業務プロセスを図式化。システム内のデータフロー、複合ロジックのロジックを模型化する。	OMG UML
アクター （Actor）	ユーザーやその他のシステムが、被写体と相互作用する際に演じる役割を指す。	OMG UML
航空機レベル （Aircraft Level）	航空機全体の運用環境と機能を考慮に入れた開発プロセス	SAE ARP4754A FAA AC No.20-174
機体境界 （Aircraft Boundary）	航空機のシステムや構成品の開発プロセスにおいて、そのシステムや構成品がどの程度までの範囲や機能を持つべきかを定義するための境界を示す。	
安全性(耐空性) （Airworthiness）	航空機、航空機システム、または部品が、その本来の機能を安全に遂行できる状態	RTCA DO-326A EUROCAE ED-202A
耐空性セキュリティ （Airworthiness Security, AWS）	意図で認証されていない電子的な相互作用から無人航空機の安全性を保護すること:人間の行動(意図的または非意図的)による被害、アクセス、使用開示、データおよび/またはデータインターフェースの混乱、改変、または破壊を使用する。これには、マルウェアと偽造データの結果、および他のシステムが無人航空機システムにアクセスすることも含まれる。	RTCA DO-326A EUROCAE ED-202A
アプリケーション （Application）	ユーザコマンドまたはプロセス事象によって開始された特定の機能を実行し、またシステム制御、監視または管理特権へのアクセスがなくても実行可能であるソフトウェアプログラム	IEC/TS 62443-1-1:2009
評価尺度 （Assessment Scale）	システムや構成品がその機能を喪失した場合、または誤った振る舞いをした場合に航空機がどの程度の危険な状態に陥るかを評価するための尺度。	
評価 （Assessment）	技術的判断に基づく評価	RTCA DO-326A EUROCAE ED-202A
資産 （Asset）	機能、システム、アイテム、データ、インターフェース、プロセス、情報など、無人航空機の安全性に寄与する無人航空機の論理的・物理的資源。	RTCA DO-326A EUROCAE ED-202A
仮説 （Assumptions）	証拠なしに提供される声明、原則、および/または前提。	RTCA DO-326A EUROCAE ED-202A
保証 （Assurance）	製品またはプロセスが所定の要件を満たしているという十分な確信を得るために必要な、計画的かつ体系的な行動。	RTCA DO-326A EUROCAE ED-202A
攻撃 （Attack）	システムのセキュリティポリシーを侵害しようとする行為に起因するシステムに対する攻撃。 これには、意図的な行為と非意図的な行為が含まれる。	RTCA DO-326A EUROCAE ED-202A

攻撃経路 （Attack Path）	攻撃者が攻撃を実行する経路、インターフェース、行動。	RTCA DO-326A EUROCAE ED-202A
攻撃平面 （Attack Surface）	攻撃者がそのシステム、システム要素、または環境に侵入したり、そのシステム、システム要素、または環境に影響を与えたり、その環境からデータを取り出したりしようとすることができる、システム、システム要素、または環境の境界上の点の集合。 （RTCA DO-326A などでは Attack Vector と表現されているが、本解説書では Attack Surface とする）	NIST SP 800-53 Rev. 5
攻撃ベクタ （Aattack Vector）	サイバー攻撃者がペイロードや悪意のある結果を提供するために、コンピューターやネットワーク・サーバーにアクセスする経路や手段。攻撃ベクトルにより、攻撃者は人的要素を含むシステムの脆弱性を悪用することができる。	FEMA Cybersecurity Glossary
攻撃者 （Attacker）	攻撃を開始し、指示する主体。これには、インテリジェントな攻撃者だけでなく、ボットやワームなどの攻撃コードの自動的な動作や、そのようなコードの作者も含まれる。	RTCA DO-326A EUROCAE ED-202A
攻撃者特徴 （Attacker Characteristics）	攻撃者の能力（技術的なスキルやリソース）、動機、目標などを考慮に入れた評価尺度	
監査 （Audit）	システム管理策の適切さのアセスメントの実施、確立されたポリシーおよび運用手順への確実な準拠、および管理策、ポリシーまたは手順における必要な変更の推奨を行うための、記録および活動に対する独立したレビューおよび調査	IEC/TS 62443-1-1:2009
可用性 （Availability）	許可されたユーザーが、必要なときに情報や関連資産にアクセスできるようにする。	RTCA DO-326A EUROCAE ED-202A
境界 （Boundary）	システムまたはシステムの一部に対するアクセスを制限する、ソフトウェア、ハードウェアまたはその他の物理的障壁	IEC/TS 62443-1-1:2009
CIA （Confidentiality, Integrity, Availability）	情報セキュリティの 3 つの主要な目標である機密性、完全性、可用性の頭文字をとったもの。	
コード （Code）	特定のデータまたは特定のコンピュータ・プログラムを、ソース・コード、オブジェクト・コード、マシン・コードなどの記号形式で実装すること。	RTCA DO-178C
コマンド （Command）	特定の操作を実行するためにシステムや構成品に送信される指示。ソフトウェアやハードウェアが受け取る入力信号やデータ、またはそれらが生成して外部に送信する出力信号やデータに含まれる。	
コンポーネント （Component）	システムの明確な機能を果たす、自己完結型の部品、部品の組み合わせ、サブアセンブリ、またはユニット。	RTCA DO-178C
計算量 （Computational Complexity）	計算の複雑さを表す概念で、アルゴリズムが問題を解決するために必要なリソース（時間や空間）を定量的に評価する。	
機密性 （Confidentiality）	アクセスを許可された者のみが情報にアクセスできるようにすること。	RTCA DO-326A EUROCAE ED-202A

構成管理 （Configuration Management）	技術的および管理的な指示と監視を適用する規律: - 構成項目の機能的および物理的特性を特定し、文書化すること - これらの特性に対する変更を管理すること - 変更処理と実施状況の記録と報告 - 指定された要件への準拠を検証すること	ISO/IEC/IEEE 26512:2018
カットセット （Cutset）	脅威（または脅威木上のイベント）のリストであり、それらが一緒に発生した場合に、最上位イベントにつながるもの。	Wilde（改稿）
データ （Data）	情報は特定の表現で、通常は意味を持つ記号列として表現される。	IETF RFC 4949 Ver 2
データフロー図 （Dataflow Diagram）	システムを流れるデータの流れをグラフィカルに表現したものである。データのソース、データストア、データフロー、データ変換がシステム内でどのように発生するかを示している。	
サービス拒否（DOS） （Denial of Service）	リソースへの許可されたアクセスを阻止したり、タイムクリティカルな操作を遅らせたりすること。	NIST SP 800-12 Rev. 1
特権昇格 （Elevation of Privilege）	最初に与えられた権限を超える権限を攻撃者に与えることに起因する。例えば、”読み取り専用 ”の権限セットを持つ攻撃者が、何らかの方法で ”読み取りと書き込み ”を含む権限セットに昇格させる。	Microsoft Learn
暗号化 （Encryption）	データの元の意味を隠して、それらが知られたり仕様されたりするのを防止する、暗号文への平文の暗号変換。	IEC/TS 62443-1-1:2009
イベント （Event）	システムまたはその環境の状態の変化であり、セキュリティへの影響がある場合もない場合もある	
証拠 （Evidence）	主張や結論を裏付けるために使用できる物理的なオブジェクト。セキュリティ要件が満たされていることを実証したり、セキュリティリスクが軽減されていることを実証したりするために使用できる。	
既存の緩和策 （Existing Security Measure）	すでに導入されているまたは導入が計画されているセキュリティ緩和策	
故障 （Failure）	システムまたはシステムコンポーネントが、指定された範囲内で必要な機能を果たすことができないこと。障害が発生すると、故障が生じることがある。	RTCA DO-178C EUROCAE ED-12C
故障状態 （Failure Condition）	直接的または結果的に、航空機および／またはその乗員に影響を及ぼす状態であって、飛行段階および関連する運航上または環境上の不利な条件、または外部事象を考慮した上で、1 つまたは複数の故障またはエラーが原因または一因となっているもの。	RTCA DO-326A EUROCAE ED-202A
オンデマンド故障 （Failure on Demand）	「要求が発生したときに観察される可能性の高い故障」を意味する。これには、要求前に発生した故障と、要求そのものによって発生した故障の両方が含まれる	ISO/TR 12489:2013
不具合 （Fault）	ソフトウェアのエラーの現れ。不具合が発生すると故障の原因となる。	RTCA DO-178C

ファームウェア （Firmware）	実行中に動的に書き込まれたり変更されたりする可能性のあるコンピュータ・プログラムおよび関連データ。	NIST SP 800-53 Rev. 5
フォレンジック （Forensics）	データの完全性を維持する方法で、捜査目的でコンピューター関連データを収集、保持、分析すること。	CNSSI 4009-2015
形式手法 （Formal Method）	厳密な数学に基づいた記法と言語を用いて、ソフトウェアの仕様化、開発、検証を行うソフトウェア工学の手法。	CNSSI 4009-2015
頻度 （Frequency）	繰り返し事象の発生率。繰り返し事象の周期を T とすると、周波数 f はその逆数である 1/T となる。	NIST IR 8323r1
機能 （Function）	実装に関係なく、定義された一連の要件に基づく製品の意図された動作。	RTCA DO-178C EUROCAE ED-12C
機能レベル （Functional Level）	システムのコンポーネントの機能の要求を定義し、コンポーネントの機能的要件を満たすために必要な設計と開発を行うプロセスのレベル。	
ファジング （Fuzzing, Fuzz Test）	フォールト・インジェクションに似ているが、無効なデータが環境を経由してアプリケーションに入力されたり、あるプロセスから別のプロセスに入力されたりする。	NIST SP 800-95
ハイジャック （Hijacking, Cyber Hijack）	輸送中の陸上車両、航空機、その他の輸送手段を不法に押収すること。また、攻撃者がコンピューターシステム、ソフトウェアプログラム、および/またはネットワーク通信を制御するネットワークセキュリティ攻撃の一種	Britannica, TechTarget
影響度 （Impact）	情報またはシステムの機密性、完全性、または可用性の喪失が、組織運営、組織資産、個人、他の組織、または国家（米国の国家安全保障上の利益を含む）に及ぼす影響。	NIST SP 800-53 Rev. 5
情報漏洩 （Information Disclosure）	許可されていない第三者に情報を不正に開示すること。具体的には以下のとおり: パスワードの漏洩、データの誤送信、ハードウェアの紛失、ソフトウェアの脆弱性による情報の漏洩	
完全性 （Integrity）	システムまたは品目の質的または量的な属性で、それが正しく機能することを信頼できることを示す。正しく動作する基準を満たさない確率で表現されることもある。	RTCA DO-326A EUROCAE ED-202A
意図的で認証されていない電子的な相互作用 （IUEI）	不正なアクセス、使用、開示、拒否、妨害、変更、または情報および/または無人航空機システムインターフェースの破壊による人為的な行為により、無人航空機に影響を与える可能性のある状況または事象。これには、マルウェアや外部システムが無人航空機システムに与える影響が含まれますが、物理的な攻撃者や電磁波ジャミングは含まれない。	RTCA DO-326A EUROCAE ED-202A
インターフェース （Interface）	相互作用が行われる独立したシステムまたはモジュール間の共通の境界。	NIST SP 800-53 Rev. 5
内部ブロック図 （Internal Block Diagram）	ブロックの内部構造をグラフィカルに表現したものである。ブロックの構成要素、それらの接続、およびそれらの相互関係を示している。	

侵入 （Intrusion/Penetration）	セキュリティインシデントを構成するセキュリティイベント、または複数のセキュリティイベントの組み合わせで、侵入者が権限を持たずにシステムまたはシステムリソースへのアクセスを獲得する、または獲得しようとするもの。	CNSSI 4009-2015
侵入検知システム （Intrusion Detection System, IDS）	不正な方法でシステムリソースにアクセスしようとする試みを発見し、リアルタイムまたはほぼリアルタイムの警告を提供する目的で、ネットワークまたはシステムイベントを監視・分析するセキュリティサービス。	NIST SP 800-82 Rev. 2
侵入防止システム （Intrusion Prevention System, IPS）	侵入活動を検知し、理想的にはその活動が目標に到達する前に、その活動を停止させることができるシステム。	NIST SP 800-82 Rev. 2
鍵 （Key）	暗号アルゴリズムとともに使用され、その動作を決定するパラメータ。	NIST SP 800-12 Rev. 1
防御レベル （Level of Protection, LoP）	セキュリティ緩和策が脅威のリスクを低減する効果を測定するもの。	
脅威レベル （Level of Threat, LoT）	脅威事象が発生する可能性の定量的評価	RTCA DO-326A EUROCAE ED-202A
論理アーキテクチャ （Logical Architecture）	システムの論理アーキテクチャは、システムの論理的な動作をサポートする、関連する技術的な概念と原則の集合で構成される。これには、機能アーキテクチャ、動作アーキテクチャ、時間アーキテクチャが含まれる。	SEBoK v.2.8
ログイン情報 （Login Information）	ユーザーがシステムにログインするために必要な情報	
悪意 / 敵意 （Malicious）	他人に危害を加えようとすること、またはそれを示すこと。	Merriam-Webster
マルウェア （Malware）	システムの機密性、完全性、可用性に悪影響を及ぼす不正な処理を実行することを意図したソフトウェアまたはファームウェア。ウイルス、ワーム、トロイの木馬など、ホストに感染するコードベースのエンティティ。スパイウェアやある種のアドウェアも悪意のあるコードの一例である。	NIST SP 800-53 Rev. 5
ミドルウェア （Middleware）	オペレーティング・システムが提供する以上のサービスをソフトウェア・アプリケーションに提供するコンピュータ・ソフトウェアの一種。	Middleware.org
ミスユース （Misuse）	人またはシステムがシステム、インターフェース、またはデータと相互作用する際に行われる、（設計意図に従った）意図しない行為。	RTCA DO-326A EUROCAE ED-202A
緩和 （Mitigation）	重大性の軽減または発生件数の減少によるリスクの軽減。	RTCA DO-326A EUROCAE ED-202A
ネットワーク図 （Network Diagram）	ユーティリティ・ネットワークまたはトレース・ネットワークに参加するネットワーク機能またはネットワーク・オブジェクトの表現。	ArcGIS Pro
否認防止 （Non-Repudiation）	ある行為を行ったと偽って否定する個人からの保護と、情報の作成、メッセージの送信、情報の承認、メッセージの受信など、個人がある行為を行ったかどうかを判断する機能を提供する。	NIST SP 800-53 Rev. 5

生起確率 （Probability of Occurrence）	ある脅威がある脆弱性または一連の脆弱性を悪用できる確率を主観的に分析し、重み付けしたもの。	NIST SP 800-30 Rev. 1
パスワード （Password）	ID の認証またはアクセス認可の検証に使用される文字列（文字、数字、その他の記号）。	NIST SP 800-12 Rev.1
PDCA サイクル （Plan,Do,Check,Action Cycle）	プロセスとシステムの管理に使用できるツール。PDCA は、継続的な改善のサイクルとして機能し、各段階でリスクに基づいた思考が行われる。	ISO 9001:2015
ペネトレーション・テスト （Penetration Test）	通常、特定の制約のもとで作業する評価者が、システムのセキュリティ機能を回避したり、打ち破ったりすることを試みるテスト手法。	NIST SP 800-12 Rev.1
物理コンポーネント （Physical Component）	システムの機能またはサービスを提供する物理的な部品	
実証的手法 （Practical Method）	具体的な問題解決や実装に焦点を当てた手法を指します。形式手法ほど厳密ではないが、現実的な制約（時間、リソースなど）の下で効率的に問題を解決するために用いられる。	
特権 （Privilage）	特にコンピュータオペレーていんぐシステムの文脈において、特定の機能を実行するための認可または一連の認可	IEC/TS 62443-1-1:2009
単位時間当たりの故障確率 （Probability of Failure Demands per Hour, PFH）	システムが危険な故障を起こし、必要なときに安全機能を果たせなくなる確率。PFH は、1 時間の期間における確率または最大確率として決定することができる。	EXIDA
再現性 （Reproducibility）	異なる専門家が同じデータから同じ結果を出す能力。	NIST SP 800-30 Rev. 1
残存リスク （Residual Risk）	セキュリティ緩和策が適用された後に残っているリスク。	IEC/TS 62443-1-1:2009
リスク （Risk）	危害の発生確率とその深刻さの組み合わせ。	ISO/IEC Guide 51:1999
リスク受容可能 （Risk Acceptable）	ユーザーにとって許容できるリスクレベル。このリスクレベルは、組織のリスク許容度と、リスクがシステムに与える潜在的な影響を考慮して、ユーザーによって決定される。	
安全度水準 （Safety Integrity Level）	E/E/PE 安全関連システムに割り当てられる安全機能の安全完全性要件を規定するための個別レベル（4 つのうちの 1 つ）。安全完全性レベル 4 が最も高い安全完全性レベルであり、安全完全性レベル 1 が最も低い安全完全性レベルである。	IEC 61508-4:1998
スクリプトキディ （Script Kiddie）	既存のスクリプトやソフトウェアを使ってサイバー攻撃を行う初心者のハッカーを指す。	Norton
セキュリティアーキテクチャ （Security Architecture）	セキュリティ要件を満たすための条件や基本的な方法に関係するアーキテクチャの側面。セキュリティアーキテクチャは、セキュリティ対策を実装し、サポートするアーキテクチャ要素を、その役割、責任、相互関係とともに定義する。要素には、ハードウェア、ソフトウェア、アルゴリズム、手順、ポリシーが含まれる。	RTCA DO-326A EUROCAE ED-202A

セキュリティ環境 （Security Environment）	セキュリティ環境とは、資産がその機能を実行する外部セキュリティ状況のことである。航空機、または航空機のシステムの場合、航空機／システムのセキュリティ環境は、航空機／システムの安全性評価において使用される、航空機／システム開発者の管理外の一連のセキュリティ想定によって特徴付けられる。	RTCA DO-326A EUROCAE ED-202A
セキュリティインシデント （Security Incident）	合法的な権限なしに、情報または情報システムの機密性、完全性、または可用性を実際にまたは差し迫った形で危険にさらす、あるいは法律、セキュリティポリシー、セキュリティ手順、または許容される使用ポリシーに対する違反または違反の差し迫った脅威を構成する出来事。	NIST SP 800-53 Rev. 5
セキュリティ緩和策 （Security Measure）	脅威の状態を緩和または制御するために使用される。セキュリティ緩和策には、機体内外の機能、手順がある。セキュリティ緩和策には、技術的、運用的、管理的なものがある。	RTCA DO-326A EUROCAE ED-202A
セキュリティ境界 （Secuirty Perimeter）	資産の内部セキュリティ状況とセキュリティ環境との境界である。	RTCA DO-326A EUROCAE ED-202A
セキュリティリスク （Security Risk）	特定の脅威が特定の脆弱性を利用し、特定の結果が生じる確率として表現される損失の予想。ある出来事のリスクは、有害な出来事の重大性とその出来事の脅威のレベルの関数である。	IEC/TS 62443-1-1:2009, RTCA DO-326A EUROCAE ED-202A
セキュリティリスクアセスメント （Security Risk Assessment）	情報システムまたはネットワークに対するセキュリティリスクを特定、分析、評価するプロセス。	
サービス （Service）	活動、仕事、職務の遂行。 サービス指向アーキテクチャに参加するソフトウェアコンポーネントで、機能を提供したり、1 つ以上の機能の実現に参加したりする。	ISO/IEC/IEEE 15288:2015, NIST SP 800-95
リスク重大度 （Severity, SEV）	脅威事象の悪影響の大きさを定性的に示すもの。	RTCA DO-326A EUROCAE ED-202A
なりすまし （Spoofing）	送信アドレスを偽り、安全なシステムに不正に侵入すること。	CNSSI 4009-2015
ステークホルダー （Stakeholder）	あるシステム、またはそのシステムが持つニーズや期待に応える特性に対して、権利、共有、請求、または利益を有する個人または組織。	ISO/IEC/IEEE 15288:2015
システム境界 （System Boundary）	情報システムのすべての構成要素のうち、権限を有する職員によって運用が許可されるもので、情報システムが接続される別途許可されたシステムを除く。	CNSSI 4009-2015
システム図 （System Diagram）	システムのアーキテクチャとコンポーネントをグラフィカルに表現したものである。コンポーネントが相互にどのように関連しているか、そしてそれらがどのように相互作用してシステムを形成しているかを示している。	
システムレベル （System Level）	システムの要求を定義し、システムの安全性と信頼性を保証するために必要な設計と開発を行うプロセスのレベル。	

改竄 （Tampering）	システム、システムの構成要素、意図された動作、またはデータの改変をもたらす、意図的ではあるが不正な行為。	NIST SP 800-53 Rev. 5
脅威 （Threat）	不正アクセス、情報の破壊、開示、変更、および/またはサービス拒否により、システムを通じて組織の運営、組織の資産、個人、他の組織、または国家に悪影響を及ぼす可能性のある状況または事象。	NIST SP 800-53 Rev. 5
脅威分析 （Threat Analysis）	情報システムまたは企業に対する脅威の程度を正式に評価し、脅威の性質を説明するプロセス。	CNSSI 4009-2015
脅威事象 （Threat Condition）	直接的または結果的に、航空機および／またはその乗員に影響を及ぼす状態。これは、飛行段階および関連する運航上または環境上の悪条件を考慮した上で、サイバー脅威を含む、意図的な不正電子的相互作用の１つまたは複数の行為によって引き起こされた、またはその一因となったものである。	RTCA DO-326A EUROCAE ED-202A
脅威モデル （Threat Modeling）	リスク評価の一形態で、データ、アプリケーション、ホスト、システム、環境などの論理的実体の攻撃側と防御側の側面をモデル化する。	NIST SP 800-53 Rev. 5
脅威シナリオ （Threat Scenario）	意図的な無許可の電子的相互作用を特定するもので、寄与する脅威源（攻撃者および攻撃ベクタ）、脆弱性、運用状況、結果として生じる脅威状況、および標的が攻撃された事象から構成される。	RTCA DO-326A EUROCAE ED-202A
脅威源 （Threat Source）	(1)意図的に脆弱性を悪用することを狙った意図や方法、または(2)誤って脆弱性を誘発する可能性のある状況や方法。脅威の発生源は意図と方法であり、攻撃者と攻撃ベクタである。	RTCA DO-326A EUROCAE ED-202A
脅威木解析 （Threat Tree Analysis）	脅威が発生した場合にどのような影響があるかを分析し、脅威に対処するための戦略を策定する手法。	
不許可イベント （Unauthorized Event）	システムのセキュリティポリシーで許可されていないイベント	
ユースケース図 （Usecase Diagram）	ユースケース図とは、システムとそのユーザーまたはその他のシステムとの間の相互作用をグラフィカルに表現したものである。システムの機能要件とそれらの相互関係を示す。	
妥当性(確認) （Validation）	製品の要求事項が正しく、完全であるという判断。	RTCA DO-326A EUROCAE ED-202A
検証 （Verification）	要件が満たされているかどうかを判断するために、要件の実装を評価すること。	RTCA DO-326A EUROCAE ED-202A
随意的 （Voluntary）	自分の自由意志で行われる、与えられた、または行動すること。	
脆弱性 （Vulnerability）	システム・セキュリティの手順、設計、実施、内部統制における欠陥や弱点で、行使される可能性があり（意図せずに誘発されたり、意図的に悪用されたり）、セキュリティ侵害やシステムのセキュリティポリシー違反につながるもの。	RTCA DO-326A EUROCAE ED-202A

脆弱性評価 （Vulnerability Assessment）	脅威源によって爆発する可能性のある航空機／システム／品目の開発および予想される運用を評価する際に使用される、脆弱性分析または脆弱性テストの 2 つの既存の方法を包含する総称。	RTCA DO-326A EUROCAE ED-202A
脆弱性テスト （Vulnerability Testing）	未知の機能や堅牢性をテストする方法。探索的テスト手法を用いて、実装に存在しうる脆弱性や、セキュリティ対策を破ったり回避したりしようとする試みを検出し、証明する。	RTCA DO-326A EUROCAE ED-202A
既知の脆弱性 （Well-known Vulnerability）	システムのある部分の以前の使用中に文書化された脆弱性で、その文書が既知であり、開発者が入手可能なもの。	RTCA DO-326A EUROCAE ED-202A

1287

Appendix 3 関連文書

(1) サーキュラー No.8-001 無人航空機の型式認証等における安全基準および均一性基準に対する検査要領, 2022 年 9 月 7 日(国空機第 456 号), https://www.mlit.go.jp/koku/content/001520547.pdf

(2) サーキュラー No.8-002 無人航空機の型式認証等の手続き, 2022 年 12 月 2 日(国空機第 645 号), https:// www.mlit.go.jp/koku/content/001574424.pdf

(3) 無人航空機の型式認証等の取得のためのガイドライン, 2022 年 11 月 2 日, https://www1.mlit.go.jp/common/001574425.pdf

(4) ASTM F3201-16 – Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS), https://www.astm.org/f3201-16.html

(5) CNSSI 4009-2022 – Committee on National Security Systems (CNSS) Glossary, https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf

(6) Airworthiness Criteria: Special Class Airworthiness Criteria for the 3DRobotics Government Services 3DR-GS H520-G, https://www.govinfo.gov/content/pkg/ FR-2020-11-24/pdf/2020-25661.pdf

(7) FAA AC 20-174 - Development of Civil Aircraft and Systems, https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1019527

(8) IEC TS 62443-1-1:2009 – Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, https://webstore.iec.ch/publication/7029

(9) IEC TR 62443 Security for Industrial Automation and Control Systems – Part 4-1: Secure product development lifecycle requirements, https://webstore.iec.ch/publication/33615&preview

(10) IETF RFC 4949: Internet Security Glossary, Version 2 - RFC Editor,

(11) IPA　ファジング活用の手引き, https://www.ipa.go.jp/security/vuln/fuzzing/ug65p9000001986g-att/000057652.pdf

(12) ISA/IEC 62443 Industrial Communication Networks – Network and system security – Part 3-3: System security rerquirements and security levels, https://webstore.iec.ch/publication/7033&preview=1

(13) ISO/IEC Guide 51:2014 – Safety aspects – Guidelines for their inclusion in standards, https://www.iso.org/standard/53940.html

(14) ISO 9001:2015 – Quality management systems – Requirements, https://www.iso.org/standard/62085.html

(15) ISO/IEC/IEEE 15288:2023 – Systems and software engineering – System life cycle processes, https://www.iso.org/standard/81702.html

(16) ISO/IEC 15408-1:2022 – Information security, cybersecurity and privacy protection – Evaluation criteria for IT security, https://www.iso.org/standard/72891.html
(17) ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks, https://www.iso.org/standard/80585.html
(18) ISO/SAE 21434:2021 – Road vehicles – Cybersecurity engineering, https://www.iso.org/standard/70918.html
(19) MITRE, HSSEDI 18-1174 - Cyber Threat Modeling: Survey, Assessment, and Representative Framework, https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf
(20) NIST SP 800-12 Rev. 1 – An Introduction to Information Security, https://doi.org/10.6028/NIST.SP.800-12r1
(21) NIST SP800-30 Rev.1 – Guide for Conducting Risk Assessments, https://doi.org/10.6028/NIST.SP.800-30r1
(22) NIST SP800-53 Rev.5 – Security and Privacy Controls for Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-53r5
(23) NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security, https://doi.org/10.6028/NIST.SP.800-82r3
(24) NIST SP 800-95 – Guide to Secure Web Services, https://doi.org/10.6028/NIST.SP.800-95
(25) OMG Unified Modeling Language, https://www.omg.org/spec/UML/2.5/PDF
(26) RTCA DO-178C / EUROCAE ED-12C – Software Considerations in Airborne Systems and Equipment Certification, https://my.rtca.org/productdetails?id=a1B36000001IcmqEAC
(27) RTCA DO-326A / EUROCAE ED-202A – Airworthiness Security Process Specification, https://my.rtca.org/productdetails?id=a1B36000001IcfuEAC
(28) RTCA DO-356A / EUROCAE ED-203A – Airworthiness Security Methods and Considerations, https://my.rtca.org/productdetails?id=a1B36000006xdusEAA
(29) RTCA DO-355A / EUROCAE ED-204A – Information Security Guidance for Continuing Airwhortiness, https://my.rtca.org/productdetails?id=a1B1R00000GshsyUAB
(30) SAE ARP4754A – Guidelines for Development of Civil Aircraft and Systems, https://www.sae.org/standards/content/arp4754a/
(31) SEBoK – Guide to the Systems Engineering Body of Knowledge (SEBoK) v.2.9, https://sebokwiki.org/w/images/sebokwiki-farm!w/8/83/Guide_to_the_Systems_Engineering_Body_of_Knowledge_v2.9.pdf
(32) 経済産業省 無人航空機分野 サイバーセキュリティガイドライン Ver 1.0, https://www.meti.

1363 go.jp/policy/mono_info_service/mono/robot/pdf/drone_cybersecirity_guideline_
1364 Ver1.0.pdf
1365

Appendix 4　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 115 サイバーセキュリティの構成員名簿（サブ WG 主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD、Rev.01）Appendix3 を参照すること。

役割	氏名	所属
主査、ライター	矢口 勇一	公立大学法人 会津大学
ライター	西岡 亮	株式会社ベリサーブ
ライター	市原 和雄	株式会社プロドローン

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

1372

RMD-135 DARFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン
安全基準セクション 135 重要な部品（フライトエッセンシャルパーツ） 解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

68

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」という）安全基準セクション「セクション 135 重要な部品（フライトエッセンシャルパーツ）（以降、「セクション 135」と呼ぶ）」 に対する解説書である。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）」の「135 重要な部品（フライトエッセンシャルパーツ） 」を以下に引用する。

> *・135 重要な部品（フライトエッセンシャルパーツ）*
>
> *（a） フライトエッセンシャルパーツとは、その不具合により計画外飛行又は回復できない制御不能につながる部品である。*
>
> *（b） もし型式設計がフライトエッセンシャルパーツを含む場合、申請者はフライトエッセンシャルパーツリストを作成しなければならない。申請者はフライトエッセンシャルパーツの不具合を防ぐために必須となる整備手順若しくは制限寿命又はその両方を設定し、定義しなければならない。その必須となる処置は、 ICA の無人航空機等の安全性を確保するために必須となる点検及び整備の章に記載しなければならない。*

3　「航空局ガイドライン」（引用）

「航空局ガイドライン」 安全基準 「セクション 135」の「基準の概要」、「適合性証明方法（MoC）」、「その他参考となる情報」を以下に引用する。

> *・135 重要な部品（フライトエッセンシャルパーツ）*
>
> *<u>基準の概要</u>*
>
> *本基準は、無人航空機における設計の弱点を洗い出し、それらに対し整備処置の設定を要求するものです。なお、ここで「その不具合」とは複合故障ではなく、単一故障又はエラーを指します。フライトエッセンシャルパーツには、電気・電子部品、構造部品、ソフトウェアを含む機器、装備品など無人航空機を構成する部品及び関連システムのすべての部品が含まれます。*
>
> *<u>適合性証明方法（MoC）：0、1、3</u>*
>
> *（a）: <u>セクション 135 フライトエッセンシャルパーツ特定解析書 （MoC 3）</u>*
>
> *フライトエッセンシャルパーツの特定には安全性解析として FHA（Functional Hazard Analysis）、FTA（Fault Tree Analysis）、FMEA（Failure Mode and Effect Analysis）*

などが有効です。FHA、FTA、FMEA の実施が困難な場合は、簡易版 FMEA として、すべての部品に対し、その部品が喪失または誤作動を起す要因として考えられる故障モードの列挙、その影響評価を行い、計画外飛行又は回復できない制御不能を引き起こす部品を抽出する方法があります。簡易版 FMEA にて評価する場合の参考として、以下にフライトエッセンシャルパーツ特定解析書(イメージ)を示します。

フライトエッセンシャルパーツ特定解析書(イメージ)

No.	P/N	Nomen	計画外飛行①	① が No の理由		制御不能②	② が No の理由		フライトエッセンシャルパーツ
				故障モード	対策		故障モード	対策	
1	012-xxxx	カウル(ケース)	No	破断	見栄えのための部品であり性能要求がないため。Ref. Doc xxx	No	破断	見栄えのための部品であり性能要求がないため。Ref. Doc xxx	NA
2	012-xxxx	BBB	Yes	-	-	Yes	-	-	○
3									
4									

フライトエッセンシャル S/W 特定解析書(イメージ)

No.	P/N	Nomen	Ver.	S/W エラーで計画外飛行になるか①	① が No の理由	セクション 110/135(b)適用 S/W
1	980-XXX	ZZZ	A	No	別の S/W がカバー	No
2	980-XXX	YYY	B	Yes	-	○
3						

(b): フライトエッセンシャルパーツリスト (MoC 0, 1)

(a)項で抽出した結果をフライトエッセンシャルパーツリストにまとめるとともに、フライトエッセンシャルパーツに対し、整備手順若しくは制限寿命又はその両方を設定します。制限寿命については、例えばバッテリーなど部品単体の寿命が決まっていればその寿命を記載します。構造部品については、セクション 315 疲労試験で証明された時間を設定します。寿命がない部品については、使用前点検、定期点検などの整備手順について検討します。

該当する部品の寿命が無人航空機の使用寿命よりはるかに長いものは、寿命の設定は不要ですが、使用前点検、定期点検の要否について検討する必要があります。寿命がなく整備手順も不

要のフライトエッセンシャルパーツについてはその理由の説明が必要となります。

最後に設定した整備手順若しくは制限寿命又はその両方を ICA の無人航空機等の安全性を確保するために必須となる点検及び整備の章に記載します。ICA は、セクション 205 に従って適合性を証明します。

その他参考となる情報

なし。

4 解説書

4.1 サーキュラーNo.8-001 本文に対する解説

・135 重要な部品(フライトエッセンシャルパーツ)

(a) フライトエッセンシャルパーツとは、その不具合により計画外飛行又は回復できない制御不能につながる部品である。

(b) もし型式設計がフライトエッセンシャルパーツを含む場合、申請者はフライトエッセンシャルパーツリストを作成しなければならない。申請者はフライトエッセンシャルパーツの不具合を防ぐために必須となる整備手順若しくは制限寿命又はその両方を設定し、定義しなければならない。その必須となる処置は、 ICA の無人航空機等の安全性を確保するために必須となる点検及び整備の章に記載しなければならない。

[引用:サーキュラーNo.8-001]

(1) フライトエッセンシャルパーツの条件

*「**計画外飛行**」の解説(ガイドライン 005 定義より)*

「(b) 計画外飛行:計画外飛行とは、無人航空機が当初計画された着陸地点まで、計画どおりに飛行を完了できないことを意味する。

これには、無人航空機の制御下における地表面、障害物等への衝突又は深刻若しくは回復不可能な高度の喪失が含まれる。

計画外飛行には、パラシュート等の回収系統の展開による運用者が指定したリカバリーゾーン外の計画外の着陸も含まれる。」

*「**回復できない制御不能**」の解説（ガイドライン 005 定義より）*

「(a) 制御不能：制御不能とは、無人航空機の制御された飛行状態からの意図しない逸脱を意味する。これには、逆効き又は縦、横若しくは方向の安定性及び操縦性の過度な喪失が含まれる。また、地表面への制御不可能な衝突の可能性が高い計画外又は命令外の姿勢への変化が含まれる。

制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。」

（2） セクション 135 の作業の流れ

安全性評価で「フライトエッセンシャルパーツ特定解析書」を作製

※MoC3

↓

上記の安全性評価の結果から「フライトエッセンシャルパーツリスト」を作製

※MoC0,1

↓

フライトエッセンシャルパーツと特定された部品に対し、整備手順若しくは制限寿命またはその両方を設定

☆設定するのは「整備手順」と「制限寿命」のどちらかでも良く、両方でも良い

（3） 「制限寿命」の考え方」（特定された部品をフライトエッセンシャルパーツに設定する場合）

部品の制限寿命がデータ不足で定義できない場合や、部品メーカーから提示されない場合もある。その場合は申請者側の設計根拠として、例えば「相当の負荷で 200 時間使用の確認を行ったので、制限時間をその 1/2 の 100 時間と定義する」のような説明（証明）方法もある。

4.2 「航空局ガイドライン」：適合性証明方法（MoC）に対する解説

（1） 「設計の弱点を洗い出す」方法の例

第二種型式認証の場合は「簡易 FMEA」を用いての安全性解析方法を別項で解説する。

※別項：Appendix 1 簡易 FMEA の記載例

（2） 「単一故障又はエラー」の解説

フライトエッセンシャルパーツと判断する考え方を整理する。セクション 135 の目的は「使用者が無人航空機ならびに装備品、部品および落下傘等ならびに関連システム（AE）に対して、適切に点検および整備を行う」際に必要な ICA 作成情報の一部を特定することにある。

航空局ガイドラインでは*「複合故障ではなく、単一故障又はエラーを指す」*とあり「簡易 FMEA」で、それを考慮した解析を行う。ただし、下記の様なケースで単一故障ではそのフライトの「計画外飛行または回復できない制御不能」につながらないケースがあるが、着陸後の点検や次回の飛行前点検では「不具合」と判断され交換、修理となる部品はフライトエッセンシャルパーツとして特定することも、申請者の判断で可能である。

例1） マルチコプターのモータ・ESC・プロペラ破損
例2） 並列接続バッテリパックの電力供給機能喪失

上記の例では機体側のフェールセーフ機能によりそのフライトでは「計画外飛行または回復できない制御不能」には陥らないが、次回のフライトでは点検や整備で不具合対応がされる為、フライトエッセンシャルパーツと選定されるべきと考える。セクション 135 のフライトエッセンシャルパーツとして特定されなかったとしても、申請者が「セクション 205 ICA（以降、「セクション 205」と呼ぶ）」の ICA に記載することに問題はない。しかしサーキュラーNo.8-001 のセクション 135 には「その不具合」に対して「複合故障ではなく、単一故障またはエラーを指す」とは記載されておらず、サーキュラーNo.8-001 の記述に対しては不整合のない特定方法と考えられる。

申請者側の判断で「単一故障またはエラー」では「計画外飛行または回復できない制御不能につながる部品」でないとしても「特定」する範囲を広めに解釈してフライトエッセンシャルパーツとする方が適切な場合もある。申請者はユーザーが安全な運行や整備を行う為の検討を行い、ICA に記載するパーツを特定する必要がある。

（3） 検討する対象の粒度（セクション 135 でのソフトウェアの扱い）

部品のレベル（粒度）は、製品のパーツリストに記載される単位とすることは適切である。ただし、機体の要件から申請者の判断で、パーツリストに記載される単位より粒度の細かなレベルとすることも可能であり、申請者の判断を優先する。交換できる部品単位で検討し、それ以下の部品での検討は一般的には不要（申請者が必要と判断すれば、それを優先する）とも考えられる。それに伴いセクション 135 では「ソフトウェア」は部品とせず、「ソフトウェアを含む機器」の単位で検討することも可能である。

4.3 「航空局ガイドライン」：適合性証明方法（MoC）に対する解説

（1） 「フライトエッセンシャルパーツ特定解析書（MoC 3）」の解説

航空局ガイドラインでは FHA、FTA、FMEA などが紹介されているが、第二種型式認証の場合は「簡易版 FMEA」で特定解析を行う方法を解説する。第二種であっても申請者が FHA や FTA を必要と判断した場合は、機体の特長に対して適切な方法での特定解析を推奨する。

※「簡易 FMEA」での特定解析は、別項の「Appendix 1 簡易 FMEA の記載例」で解説する。

（2） 「特定解析作業」の流れ

- 製品の部品表の粒度で解析用のリストを作成
- 部品の機能を定義
- 故障モードとして「故障状態（現象）」と「推定故障原因」を抽出
- 影響を「下段システム」と「上段システム」で検討
- 検知方法を検討
- 対策を検討
- 「計画外飛行」「制御不能」「飛行範囲逸脱」の可能性を判断
- 対象/非対称の判断

※セクション 135 以外の「セクション 105 無人航空機の安全な運用に必要な関連システム（以降、「セクション 105」と呼ぶ）」/「セクション 110 ソフトウェア（以降、「セクション 110」と呼ぶ）」/「セクション 115 サイバーセキュリティ（以降、「セクション 115」と呼ぶ）」/「セクション 305 起こり得る故障（以降、「セクション 305」と呼ぶ）」の対象/非対象の判断も行える解析を行う

（3） 「フライトエッセンシャル S/W 特定解析書（MoC 3）」の解説

航空局ガイドラインにはソフトウェアの特定解析の例も掲載されているが、第二種型式認証においては「ソフトウェアを含む機器」の単位での特定解析を行い、ソフトウェアのみの解析は不要として証明を進めることも可能と考える。ただし、申請者が機体の特長に応じてソフトウェアのみでの特定解析が必要と判断すれば、適切な方法での特定解析を推奨する。またセクション 110 を含めて、安全基準の証明を進める。

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定) 項目は DARFT2 にて追記予定。

Appendix 1　簡易 FMEA の記載例

簡易 FMEA は下記の手順で行うこともできる。

- 製品の部品表の粒度で解析用のリストを作成
- 部品の機能を定義
- 故障モードとして「故障状態（現象）」と「推定故障原因」を抽出
- 影響を「下段システム」と「上段システム」で検討
- 検知方法を検討
- 対策を検討
- 「計画外飛行」「制御不能」「飛行範囲逸脱」の可能性を判断
- 対象/非対称の判断

※セクション 135 以外のセクション 105/セクション 110/セクション 115/セクション 305 の対象/非対象の判断も行える解析を行う。

サンプルは別添する。
セクション 135_FMEA を参考にしたセクションの対象非対象分析検討表（例）.xlsx

Appendix 2 関連資料(JIS W 0711)の説明

下記の資料では航空法に定める無人航空機を含む産業用無人航空機システムについて，本質的安全設計方策，安全防護および付加保護方策ならびに使用上の情報に対する要求事項について規定されている。

日本産業規格 JIS W 0711:2021
無人航空機システム設計管理基準
Unmanned aircraft system design management requirements

上記資料には無人航空機の安全性評価に関係する情報が記載されている。
当該解説書は第二種型式認証を対象としており、安全性評価を行う範囲や手法は申請者（設計者）が判断することになるが、無人航空機のブロック図、FT 図、危険源、FMEA 結果などが例示されており参考となる。

Appendix 3 各セクション特有の用語集

DARFT2 にて追記予定

Appendix 4 関連文書

(1) 関連文書 日本産業規格 JIS W 0711:2021 無人航空機システム設計管理基準 Unmammed aircraft system design management requirements

Appendix 5　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 135 重要な部品（フライトエッセンシャルパーツ）の構成員名簿（サブ　WG　主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD、Rev.01）Appendix3 を参照すること。

役割	氏名	所属
主査、ライター	兵頭 淳	株式会社 東京アールアンドデー
ライター	上の 香	合同会社山猿
ライター	中舘 正顯	一般財団法人日本海事協会

無人航空機の型式認証等の取得のためのガイドライン解説書

2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

226

RMD-300 DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 300 耐久性及び信頼性

解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

表 目次

1 目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」と呼ぶ）安全基準「セクション 300 耐久性及び信頼性（以降、「セクション300」と呼ぶ）」に対する解説書である。

2 対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）」の「300 耐久性及び信頼性」を以下に引用する。

・300 耐久性及び信頼性

無人航空機は、CONOPS に記載され、また型式認証データシート及び無人航空機飛行規程に無人航空機運用限界として含まれる、運用環境の制限下で運用された場合に耐久性と信頼性を持つように設計されなければならない。その耐久性及び信頼性はここに記載する要件に従い、飛行試験で実証しなければならない。試験は、計画外飛行、制御不能、想定飛行範囲からの逸脱又はリカバリーエリア外での非常着陸につながる不具合なく完了しなければならない。

（a） このセクションへの適合を証明するために試験を開始した後は、その機体の全ての飛行を飛行試験報告書に含むこと。

（b） 試験には運用のすべてのフェーズにおけるすべての飛行エンベロープの評価を含まなければならない。さらに、少なくとも以下を考慮すること。

（1） 飛行距離
（2） 飛行時間
（3） ルートの複雑性
（4） 重量
（5） 重心
（6） 密度高度
（7） 外気温度
（8） 対気速度又は対地速度
（9） 風速
（10） 天候
（11） 夜間運用（夜間運用を行う場合
（12） エネルギー貯蔵系統の容量
（13） 操縦者に対する機体の数（1 対 1，1 対複数等）

（c） 試験には上記（ 項のうち最も厳しい条件の組合せ及び形 態を含まなければならない。

（d） 試験では CONOPS で指定される運用タイプに応じた別々の飛行プロファイル及びルートの分布を示さなければならない。

(e)　試験は、 CONOPS で指定される想定環境下で行わなければならない。これには、電磁干渉(EMI)と高強度放射電界(HIRF)環境を含む。

(f)　試験においては、特別な操縦者のスキルや注意力を要求してはならない。

(g)　試験に使用する無人航空機は、運用中に想定される地上での機体取扱時(貨物の積み込みを含む。)及び輸送時における取扱いによる負荷の最悪値を 考慮したものでなければならない。

(h)　試験に使用する無人航空機は、セクション 105 で特定された最低限の仕様を満足するが、それを超えない関連システム(AE)を使用しなければならない。 複数の関連システム(AE)が特定された場合、申請者は各形態を実証しなければならない。

(i)　試験に使用する無人航空機は、 ICA 及び無人航空機飛行規程に基づいた運用及び維持がされなければならない。このセクションへの適合性を示すに当たり、 ICA に設定された整備間隔よりも短い間隔で整備を行うことは許容されない。

(j)　機体の内部に搭載し、又は外部に固定すること等によって貨物を輸送する運用を行う場合、重量・重心の組合せが最も厳しい貨物の搭載状態における飛行エンベロープに対して以下の試験を行わなければならない。

(1)　機体が安全に制御・操縦できること。

(2)　機体の内部に搭載し、又は外部に固定すること等によって貨物を輸送できること。

79　3「航空局ガイドライン」(引用)

80　「航空局ガイドライン」 安全基準 「300 耐久性及び信頼性」の「基準の概要」、「適合性証明方法
81　(MoC)」、「その他参考となる情報」を以下に引用する。
82

・300 耐久性及び信頼性

<u>基準の概要</u>

本基準は、D&R の要となる設計基準と試験実証となります。セクション 300 では、意図した運用ができるような耐久性と信頼性を持つよう設計し、それを実証することが要求されます。適切な設計であることを確認するために設計基準チェックリストを活用することを推奨します。また、実証は飛行試験で行います。セクション 300 の一番の目的は、機体レベルで無人航空機全体の信頼性を実証することです。加えて、無人航空機飛行規程及び ICA もセクション 300 の試験において評価されます。そのほかに飛行実証において、機体の構造が十分な強度を持ち、耐久性があることも併せて評価されます。設計基準評価書により、機体の安全な制限寿命の算出に必要なデータが蓄積されます。セクション 300 の飛行時間を蓄積し、それを制限寿命の算出に活用することで証明活動がスムーズに進む可能性があります。

なお、本試験は可能な限り実際に運用する環境で行うことが望ましいものの、その実施が合理的でない場合は代替の手段が認められます。例えば、夏場における最低温度環境など実環境での飛行試験実施が合理的でない場合、恒温室等の使用などによる模擬環境での飛行試験が許

容されます。模擬環境の妥当性等については、事前に検査者とよく相談することを推奨します。

適合性証明方法(MoC):6

(a)～(j): セクション 300 飛行試験方案 (MoC 6)

無人航空機の耐久性及び信頼性を実証するため、運用エンベロープ及び運用制限における全範囲に渡って、飛行フェーズ(離陸、巡航、着陸など)も考慮した上で、制御不能、計画外飛行などの事象がなく、必要な時間の試験を完了させることが求められます:

(1) 複数の代表的な運用の仕方(ミッション)及び飛行ルートをできるだけ満遍なく飛行させること。この際、最大の飛行距離及び時間並びに複雑性も考慮すること。もし C2 リンクの送信機と受信機の距離がクリティカルなファクターである場合、考えられる最大距離での実証も行うこと。

全範囲に渡って実証が必要となるパラメータは以下のとおり:

① 重量(最大及び最小)
② 重心(最も厳しい重心における最も厳しい縦横方向)
③ 密度高度(最高及び最低)
④ 温度(最高及び最低)
⑤ 速度(フライトフェーズごとの値)
⑥ 風速(最大、最も厳しい方向、最も厳しいフライトフェーズ及びモード並びに突風)
⑦ 気象状態(運用を想定するすべて)
⑧ 昼夜
⑨ バッテリー容量(最高及び最低気温における最も厳しい SOC(state of charge)、SOH(state of health)、放電状態(depth of discharge))
⑩ 操縦者と機体の比率(1操縦者が同時に操縦する無人航空機の最大の数)
⑪ バージョン又は機体の能力が運用に応じて変化する場合、各々のフライトモード、機体のセッティング及び自動・自律状態
⑫ 地形、場所、環境、障害物、電波反射、ノイズ及び交通状態(例えば、高層物件の谷間や都市環境は、電波のマルチパス及び乱反射並びに局所的な風及び天候変化などから、証明活動がより困難になることが想定されます。)
⑬ 以下の組合せ状態における操縦性及び運用評価
   a. 最小重量、最も厳しい重心、最大風速(最大の突風及び横風状態を含む)
   b. 最大重量、最も厳しい重心、最高温度及び密度高度、最大の飛行距離・時間
   c. 最大重量、最も厳しい重心、最高温度及び密度高度、最大のエネルギー消費率(運用で考えられる空中待機または上昇など)
   d. 最高温度及び飛行前の最大地上運用

(2) 貨物輸送を行う場合

運用エンベロープにおける貨物を考慮した最も厳しい重量重心で、無人航空機及び貨物が安全に制御、操作、輸送及び格納できることを実証する(もし想定されるのであれば側方変

化及び急激な停止も考慮する）こと。貨物の回転、よじれ又は飛行中におけるその他の反応について無人航空機が耐えうることを実証すること。クリティカルな負荷及び速度のすべての組合せを考慮すること。さらにカーゴの横ずれなどの影響評価を行うこと。

(a)～(j): セクション 300 飛行試験報告書（MoC 6）

試験結果を報告書としてまとめます。

その他参考となる情報

- 第一種型式認証の実証飛行試験の時間について

人口密度		運用場所の目安（米国の例）	基本形態(FLT HR)	危害軽減を行う場合（FLT HR）
1 マイル四方 あたりの数	1 キロ四方 あたりの数			
258 以下	390 以下	田舎	375	150
3,000	1,159	郊外	1,100	540
7,000	2,703	米国の 95%	2,500	1,300
10,000	3,863	ワシントン DC	3,600	1,800
14,000	5,408	ボストン	5,000	2,500
20,000	7,725	ニューヨーク以外の都市	7,200	3,600

上記を参考に、実際に飛行する経路、想定飛行範囲、昼夜の別等を考慮しプロジェクトごとに必要となる実証飛行試験の時間を計算します。

基本式:

安全目標値(5E-7) ＝ 致命傷発生率(1) × 外出率(9%) × ｸﾗｯｼｭｴﾘｱ(1.72m2) × (人口密度 人/km2 ÷ 1,000,000) ÷ 必要となる飛行時間(HR) × 3(統計処理)

※:人口密度については、統計データとして公表されている最新の国勢調査による市町村単位のデータを基本的に使用することとしますが、関係する自治体等から更に詳細な区分のデータの提供を受けている場合等は、当該データを使用することも可能です。

なお、一番右の欄に記載される危害軽減とは、一例として、ASTM F3322-18 に適合したパラシュートの搭載により危害軽減を行ったもの等が該当しますが、具体的な取扱いについては、第一種型式認証の審査において航空局と調整いただくこととなります。

- 第二種型式認証の実証飛行試験の時間について
  - 最大離陸重量が 25kg 以上の型式は、150 時間の実証飛行試験が必要となります。
  - 最大離陸重量が 25kg 未満の型式は、 50 時間の実証飛行試験が必要となります。

- *試験方案の記載事項について*

試験方案には、試験実施に必要なすべての情報、条件、仕様等を記載するとともに、後から見返した時にどのような試験が行われたか明確に分かるように、必要であれば将来同じ試験をそのまま再現できるような精度で情報を記入する必要があります。

以下は試験方案に最低限記載すべき事項です:

- *試験供試体の説明*
- *試験を行うのに必要な計測器等のリスト*
- *必要な計測器類の校正内容*
- *校正状況の確認方法*
- *試験前に確認すべき事項(供試体及びセットアップ)*
- *証明する基準のリスト(セクション 300(b)項(1)等)及びそれをどのように証明するのかの説明*
- *ステップバイステップで記載する試験手順及び各々の試験の Pass/Fail Criteria*

上記の他、日付、試験場所、試験開始時間、試験終了時間、試験時間、離陸時間、着陸時間、飛行時間、試験管理番号、供試体の型式、部品番号(Part Number:P/N)、製造番号(Serial Number: S/N)、天候、視程、気温、湿度、高度、速度、風向き、風速、距離、試験実施者、試験管理者、試験責任者等の設定又は記録に関する事項が含まれること。

- *試験の条件*

試験を開始するには、無人航空機の形態(ソフトウェア、ハードウェア、構造及び推進系統などを含む)が型式認証を取得する最終形態と同等といえるまで十分に成熟した上で、形態を確定、さらに供試体、セットアップの適合性について報告される必要があります。試験開始後の形態変更は、セクション 300 の飛行試験時間を 0 時間にリセットし、すべての試験の再実施が要求される場合があります。無人航空機は、実運用で行われる点検、整備及び交換作業のみを行い、運用維持される必要があります。無人航空機飛行規程又は ICA に設定されていない、点検、整備及び交換作業はいかなる場合も許容されません。

また、運用中に想定される地上での機体取扱時(貨物の積み込みを含む。)及び輸送時における取扱いによる負荷の最悪値を考慮し、それを無人航空機に課さなければなりません。さらに、試験を行う操縦者及び整備者は、運用において要求される最低限の訓練を受けた者であり、熟練者であってはなりません。

セクション 300 試験の意図は、妥当なサンプル量により初期故障及び摩耗故障の発見に寄与させることも考慮しています。そのため、膨大な数の機体を一斉に飛行させる実証、余りに少ない(例えば一機)機体での実証は行うべきではありません。セクション 300 の実証を行うのに必要な最少機体数は原則三機です。

- *不具合発生時の扱い*

セクション 300 試験中に計画外飛行、制御不能、想定飛行範囲からの逸脱又はリカバリーゾーン外への非常着陸が発生した場合は根本原因解析(Root cause analysis)を行い、再発を防止するために、必要に応じて、設計変更又は運用手順の変更が必要になります。その上で追加のセクション 300 の飛行試験が必要になります。追加の飛行時間量は、不具合の種類及び影響度並びに根本原因解析とその是正処置の精度及び網羅性に依存します。そのほか、是正処置の範囲、厳密さ、変更を評価するための試験又は解析の深度、変更がその他の事項に悪影響がないことの裏付けされた確証度合いが影響します。もし根本原因が明確に分からなかった場合又は最悪のケースでは、セクション 300 の飛行時間を 0 時間にリセットし、すべての試験の再実施が必要になります。一方で、試験及び解析が完遂しており、変更による悪影響が防止され、不具合自体が無害、封じ込めが十分、原因が明確、是正処置が包括的である場合には、再試験の飛行時間が少なくなる場合があります。不具合が発生した場合、再試験について申請者は検査者と十分に協議する必要があります。

- *セクション 300 設計基準評価書*

セクション 300 の基準における「設計されなければならない」に対し、設計基準評価書の活用を推奨します。この設計基準は、無人航空機が適切な設計であり、最低限の安全が確保されていることを確認するのに有益です。無人航空機の設計が適切であることを設計基準評価書に照らし合せて確認し、その結果を適合性証明計画書(Certification Plan)とともに検査者へ提示します。

この設計基準評価書は、無人航空機に関連する安全性基準から、無人航空機の運用リスクを考慮した上で抽出されたもので、セクション 300 以外の基準も含まれますが、いずれもセクション 300 の試験を開始する上で必要な要件となります。本チェックリストが満たせない場合は、安全基準を満足していない可能性があるため、もし満たせない基準がある場合は、設計の見直しや同等の安全性が確保できる代替策を検討する必要があります。設計の見直しや代替策の検討が必要となる場合は、検査者と協議することを推奨します。

設計基準評価書			
型式認証の手続			
型式設計データ、試験結果及び解析結果は、無人航空機が適用基準に適合していることを示すために必要となります。型式設計データとは、形態及び設計の特徴を定義する図面及び仕様書であり、寸法、材料、構造強度のための工作法、ICA の制限事項及びその他必要となるデータが含まれます。			*□*
安全基準に係る事項			
	ハザード	*期待される軽減策*	*✓*
1	*適切な設計特性又は運用制限がされず、厳しい環状態又は降雨状態が計画外飛行を引き起こす。*	*無人航空機飛行規程に要求される制限事項及び適切な手順が設定されること。※1*	*□*

2	振動及び繰り返し荷重が疲労破壊の原因となる。	ICA どおりに厳密に維持管理され、実運用又は最も厳しい環境及び状態を模擬した飛行結果に基づき構造の制限寿命を設定すること。※2	□
3	無人航空機が非想定又は非安全なエリアに入るかもしれない。飛行中断機能が意図せず働くかもしれない。	無人航空機が飛行中断、非常着陸又は非常帰還機能を有すること。もし飛行中断機能を有する場合、それが意図せず機能しないこと。	□
4	もし操縦者が無人航空機の位置及び進路が分らない場合、無人航空機が非想定又は非安全なエリアに入るかもしれない。	無人航空機の速度、進路、方位、方向、高度及び位置情報が操縦者に提供されること。	□
5	もし操縦者に必要な情報が提供されない場合、無人航空機が非安全なエリアに入るか若しくは制御不能になるかもしれない。	CS は安全な飛行の継続及び制限内での運用に必要なすべての情報を操縦者へ提供すること。すべての必須電源系統又はバッテリー管理系統における残飛行時間、SOC(State Of Charge)、残量又は必要な同様の情報を含む数量が操縦者に提供されること。飛行中のモニタリング及び/又はバッテリー及びモーターの不具合センシングを導入する。	□
6	ソフトウェアのエラーが計画外飛行を引き起こす。	ソフトウェアがテストされ又は許容可能な信頼水準となっていることが実証されること(セクション 110)	□
7	無人航空機が予期しない又は好ましくない性能/振る舞いにより、事故が発生するかもしれない。通信の喪失が状況認識を失わせる不安全な状態を引き起こす可能性がある。問題の根本原因が不明となるかもしれない。その結果、型式認証等保有者による安全基準への適合を維持させることができない可能性がある。	型式認証等保有者の安全基準への適合における報告要件を満たすために必要な場合、無人航空機/CS はログファイルとして回収可能な機体のテレメトリデータを保存する能力を持つべきである。データログファイルは、システムの性能及び不具合/異常事態の根本原因を解析するために必要十分なパラメータを含むべきである。	□
8	もし C2 リンクの通信品質が低下しそれが操縦者に知らされなかった場合、無人航空機が不安全な状態になるかもしれない。	無人航空機が操縦者に対し C2 リンクの通信強度、品質又は状態を知らせる手段を提供すること。	□
9	もし C2 リンクが喪失するか、コマンド&コントロールができなくなり、それが操縦者に知らされなかった場合、無人航空機が不安全な状態になるかもしれない。	コマンド&コントロール機能が完全に喪失した場合又は C2 リンクの性能低下により無人航空機の即時の遠隔操作が保証できなくなる場合、操縦者に対しアラートを提供すること。	□
10	予想されるリンク切れのための緊急時の対応計画がない場合、リンク切れが不安全又は予期しない無人航空機の挙動を引き起こすかもしれない。	無人航空機には予想されるリンク切れのための緊急時の対応計画が設定されており、リンクの再構築、指定エリア/パターンでのロイター飛行、ベース地点へのリターン及び着陸、代替着陸地点への着陸又は安全な方法による飛行の中断がある。	□
11	無人航空機が非想定又は非安全なエリアを避けるための呼び戻し又はルートの変更能力なしに出発及び運用されるかもしれない。	無人航空機飛行規程には C2 リンクの使用状況又はサービス品質における最低要件を含み、使用状況又はサービス品質が計画する運用に十分かどうか判断するための手順を設定すること。無人航空機飛行規程の規定又は無人航空機の設計により、C2 リンクが使用不可の際に離陸/発射を許可しないこと。	□

12	無人航空機が EMI/HIRF によりシステム及び機器の故障につながる意図しない影響を受けるかもしれない。	無人航空機飛行規程には、無人航空機が評価(実証)を行った EMI/HIRF の環境を説明すること。もし無人航空機が EMI/HIRF 要件への適合を評価していない場合、無人航空機飛行規程には以下の事項を記載し、注意喚起を行うこと: この無人航空機は無線周波数における感受性について、すべての環境適合性を得るための十分な試験を行っていない。そのため、この無人航空機が無線周波数にさらされた場合、確実に機能しない可能性がある。 "This UAS has not undergone sufficient testing to obtain full environmental qualification for RF susceptibility, and the UAS may not operate reliably when exposed to RF power."	☐
13	無人航空機が雷撃により喪失するかもしれない。	無人航空機飛行規程には、雷雲を避けるための適切な制限を設けること。もし無人航空機が耐雷性能を持たない場合、無人航空機飛行規程には以下の制限を行うこと: 雷活動のエリアへ無人航空機が入る運用は禁止。雷撃により無人航空機が喪失する可能性がある。 "Operation of the aircraft into areas of lightning activity is prohibited. A lightning strike could cause loss of aircraft."	☐
14	無人航空機が文書化された手順なしに運航された場合、計画外飛行につながる誤った運用がされるかもしれない。	セクション 200 に従った無人航空機飛行規程を作成すること。無人航空機飛行規程は可能な限り最大限に検証/確認がされること。	☐
15	無人航空機が文書化された手順なしに整備された場合、計画外飛行につながる誤った維持がされるかもしれない。	セクション 205 に従った ICA を作成すること。そして ICA に無人航空機並びに装備品、部品及び落下傘等並びに関連システム(AE)に対して、適切に点検及び整備を行うための手順として、必要十分な情報が含まれていることを保証すること。	☐
16	無線機器が有害な妨害につながる、法令に抵触する又は人体にばく露される電波の許容値を超える電波を放射するかもしれない。	放射電波のスペクトラムが許容される範囲内であること。	☐
17	電子的なサイバー攻撃が安全な飛行に影響を与えるかもしれない。	電子的なサイバー攻撃が安全な飛行に影響を与える 可能性について考慮され、可能な限り最大限防護さること。コントロールステーション、航法システム(GNSS)及び C2 リンクは許可されないアクセス、侵入、データ抽出又はその他の攻撃に耐性があること。	☐

18	*セキュアでない IT システムが電子サイバー攻撃に対し脆弱性を生ずる。*	*無人航空機及びその関連システムに対し、最低でもスタンダードに従った、セキュリティ対策を行うこと。例えば、分離されたネットワークの使用、ファイヤーウォール、ウィルス対策ソフトウェア、OS の維持管理及び最新化、プラットフォームに応じた適切なセッティング又はフィーチャの選択。*	*□*
19	*セキュアでない IT システムが電子サイバー攻撃に対し脆弱性を生ずる。*	*無人航空機の運用に専用のプラットフォーム/機器を使用する。無人航空機の運用に使用するスマートフォン、タブレット又はコンピュータ等はほかの関係ない一般的な事務等の目的に使用しないこと(第一種型式認証の場合)。*	*□*
20	*暗号化されないデータ及び C2 リンクは搾取される傾向がある。*	*C2 リンク、保存又は送信データなど、実現可能なものは暗号化する。*	*□*

※1 無人航空機に記載すべき事項は以下のとおり:

無人航空機のローター及びプロペラを含むあらゆる表面におけるいかなる霜、雪又は着氷がある状態での離陸は禁止する。
以下の場合における離陸及び着陸を含む運用は禁止:
・ あらゆる降水状態(霧雨、雨、雪、凍雨を含む)
・ 潜在的な着氷状態(+5℃以下の外気温における雲、降雨、もや、霧を含むあらゆる湿気)

Takeoff is prohibited with any frost, snow, or ice on any surface of the UAS, including rotors and propellers.
Operations, including takeoff and landing, are prohibited in:
・ Any precipitation (including drizzle, rain, snow, ice pellets); and
・ Potential icing conditions (any moisture including clouds, precipitation, mist, fog, below an ambient temperature of +5°C)

※2 構造の制限寿命の設定方法は以下のとおり:

構造の制限寿命は、一機又は複数の長時間を飛行した機体で実証された最大サイクル及び時間に基づく。申請者は、典型的なミッションを飛行した典型的な無人航空機で実証した値以下で制限寿命を設定すべきである。長時間を飛行する機体は、ICA に基づく整備だけを受け、典型的又は最悪な環境及び状態において行った典型的なミッションの時間を蓄積すべきである。

4　解説書

本解説書の適用範囲

「航空局ガイドライン：安全基準について【適用】の再掲」

ここで解説する安全基準および適合性証明方法の一例は、「サーキュラーNo.8-001」の第2章に規定しているものを対象としている。

D&R（Durability & Reliability）を土台とするこの安全基準は、具体的には以下の仕様およびCONOPS に該当する無人航空機に適用される。以下に該当しない無人航空機に対しては、特別要件などの要否について、航空局または登録検査機関（以降、「検査者」と呼ぶ）と追加の調整が必要となる。

- 無人航空機が C2 リンクを有し、操縦者が緊急時の対応を取ることができるもの
- 着氷気象状態での運用を行わないもの
- 操縦者と無人航空機の数の比率が 1:20 以下のもの
- 電動推進の無人航空機であること（内燃機関または燃料電池を除く）

本解説書は上記に加え下記「サーキュラーNo.8-001 安全基準 第一章 1－1」に定める区分のうち、第二種/最大離陸重量4kg以上25kg未満に当てはまる機体を主に対象としている。

表 4.1-1 区分に応じて適用される規定

（凡例）✓：適用されるもの、✓✓：該当する特定飛行※1に応じて適用されるもの、N/A：適用されないもの

区分	第二種				第一種
	機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機				機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機
			最大離陸重量25kg以上のもの		
	最大離陸重量4kg未満のもの	最大離陸重量4kg以上25kg未満のもの	法第132条の85第１項各号に掲げる空域以外の空域を飛行し、かつ、法第132条の86第２項第１号から第４号までのいずれにも該当する方法により飛行するもの※2	その他のもの※3	特定空域を含まない空域を飛行するもの
001 設計概念書（CONOPS）	✓	✓	✓	✓	✓
005 定義	✓	✓	✓	✓	✓
100 無人航空機に係る信号の監視と送信	✓※4	✓	✓	✓	✓
105 無人航空機の安全な運用に必要な関連システム	✓	✓	✓	✓	✓
110 ソフトウェア	✓※5	✓※5	✓※5	✓	✓
115 サイバーセキュリティ	✓	✓	✓	✓	✓
120 緊急時の対応計画	✓✓※6	✓	✓	✓	✓
125 雷	✓	✓	✓	✓	✓
130 悪天候	✓	✓	✓	✓	✓
135 重要な部品（フライトエッセンシャルパーツ）	✓	✓	✓	✓	✓
140 その他必要となる設計及び構成	✓※7	✓※7	✓※7	✓※7	✓※7
200 無人航空機飛行規程	✓	✓	✓	✓	✓
205 ICA	✓	✓	✓	✓	✓
300 耐久性及び信頼性	✓	✓	✓	✓	✓
305 起こり得る故障	✓✓※8	✓✓※8	✓	✓	✓
310 能力及び機能	✓※9	✓	✓	✓	✓
315 疲労試験	N/A	N/A	✓	✓	✓
320 制限の検証	N/A	N/A	✓	✓	✓

出所）サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領

4.1 「セクション 300」の目的

「航空局ガイドライン 冒頭」

> *無人航空機は、CONOPS に記載され、また型式認証データシート及び無人航空機飛行規程に無人航空機運用限界として含まれる、運用環境の制限下で運用された場合に耐久性と信頼性を持つように設計されなければならない。その耐久性及び信頼性はここに記載する要件に従い、飛行試験で実証しなければならない。試験は、計画外飛行、制御不能、想定飛行範囲からの逸脱又はリカバリーエリア外での非常着陸につながる不具合なく完了しなければならない。*
>
> *［引用：航空局ガイドライン］*

【解説】

- 試験は無人航空機飛行規程および ICA に則とった飛行試験方案にしたがって行われる。メーカーは自信をもってユーザーに使ってもらえる機体を提供するために、この試験飛行にて耐久性と信頼性を証明する。

- 設計に関しては、ガイドラインに記載されている「設計基準評価書」を参考にすることが可能である。
- 試験は、計画外飛行、制御不能、想定飛行範囲からの逸脱またはリカバリーエリア外での非常着陸につながる不具合なく完了しなければならならない。
  各用語については「セクション 005 定義（以降、「セクション 005」と呼ぶ）の用語の説明を参照。
  ※「セクション 005」の用語は、「セクション 300」の飛行試験 MoC6 の試験 Pass 要件とは異なる点に注意が必要です。
  Pass/Fail 要件は、試験方案ごとにそれぞれ設定され、記入される必要がある。
- 「セクション 300」の Pass 要件は、試験計画に指定された飛行を完結することが求められる。
  飛行試験途中での緊急着陸エリアへの着陸などは Fail となる。
  飛行中断が発生したときは、その原因の解析と次試験飛可否の別途判断が必要である。

4.2 「セクション 300」基準の概要

「航空局ガイドライン 基準の概要」

> *・300 耐久性及び信頼性*
>
> *<u>基準の概要</u>*
>
> *本基準は、D&R の要となる設計基準と試験実証となります。セクション 300 では、意図した運用ができるような耐久性と信頼性を持つよう設計し、それを実証することが要求されます。適切な設計であることを確認するために設計基準チェックリストを活用することを推奨します。また、実証は飛行試験で行います。セクション 300 の一番の目的は、機体レベルで無人航空機全体の信頼性を実証することです。加えて、無人航空機飛行規程及び ICA もセクション 300 の試験において評価されます。そのほかに飛行実証において、機体の構造が十分な強度を持ち、耐久性があることも併せて評価されます。設計基準評価書により、機体の安全な制限寿命の算出に必要なデータが蓄積されます。セクション 300 の飛行時間を蓄積し、それを制限寿命の算出に活用することで証明活動がスムーズに進む可能性があります。*
>
> *なお、本試験は可能な限り実際に運用する環境で行うことが望ましいものの、その実施が合理的でない場合は代替の手段が認められます。例えば、夏場における最低温度環境など実環境での飛行試験実施が合理的でない場合、恒温室等の使用などによる模擬環境での飛行試験が許容されます。模擬環境の妥当性等については、事前に検査者とよく相談することを推奨します。*
>
> *［引用：航空局ガイドライン］*

【解説】

- 無人航空機飛行規程、ICA（整備手順書）も同時に評価されることに注意
  飛行エンベロープの規定が正確にされているかを確認することが大事である。
  次項以下の飛行条件の導出の基準となる。

● 環境条件について

① 夏～冬にわたって、実環境での飛行試験を実施することが望ましい。

② 例えば環境模擬試験として、夏場の低温試験、冬場の高温試験など実環境での飛行試験実施が合理的でない場合、恒温室などの模擬試験環境での飛行試験が許容され得る。ただし、模擬環境の妥当性や証明すべき項目を試験方案において明確にし、事前に検査者とよく相談することを推奨する。

③ 環境模擬飛行が不可能な機体については、特殊ケースとして扱い、検査者と相談が必要である。

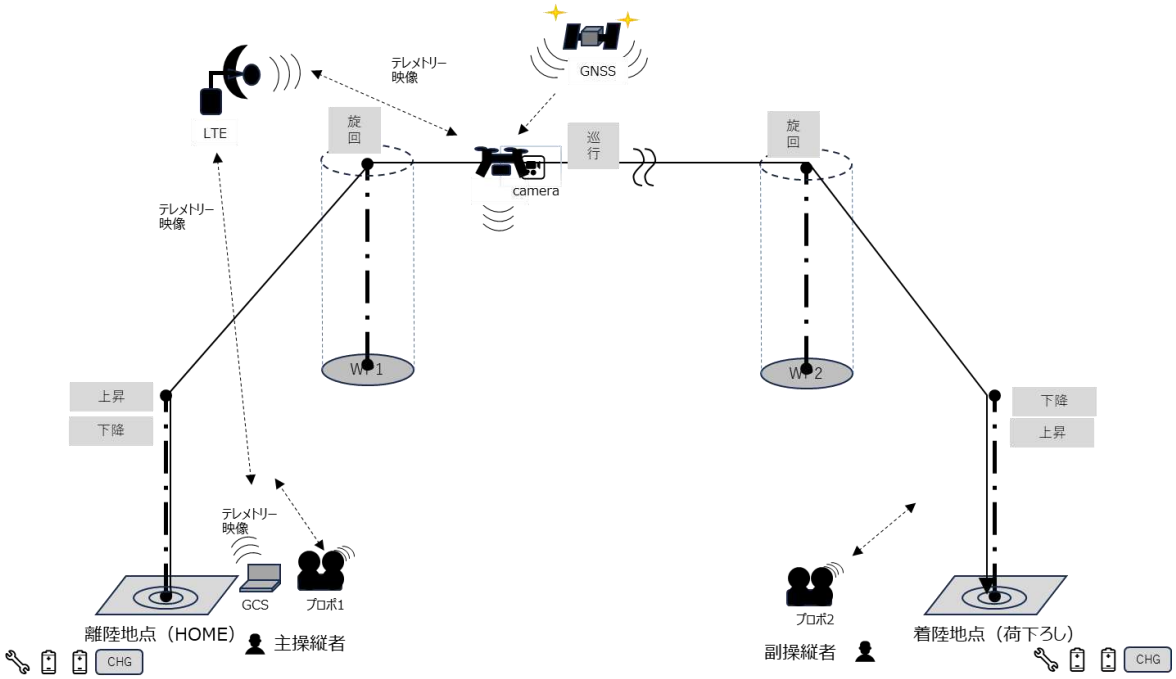


図 4.2-1 CONOPS から得られる代表的な飛行パターンの一例

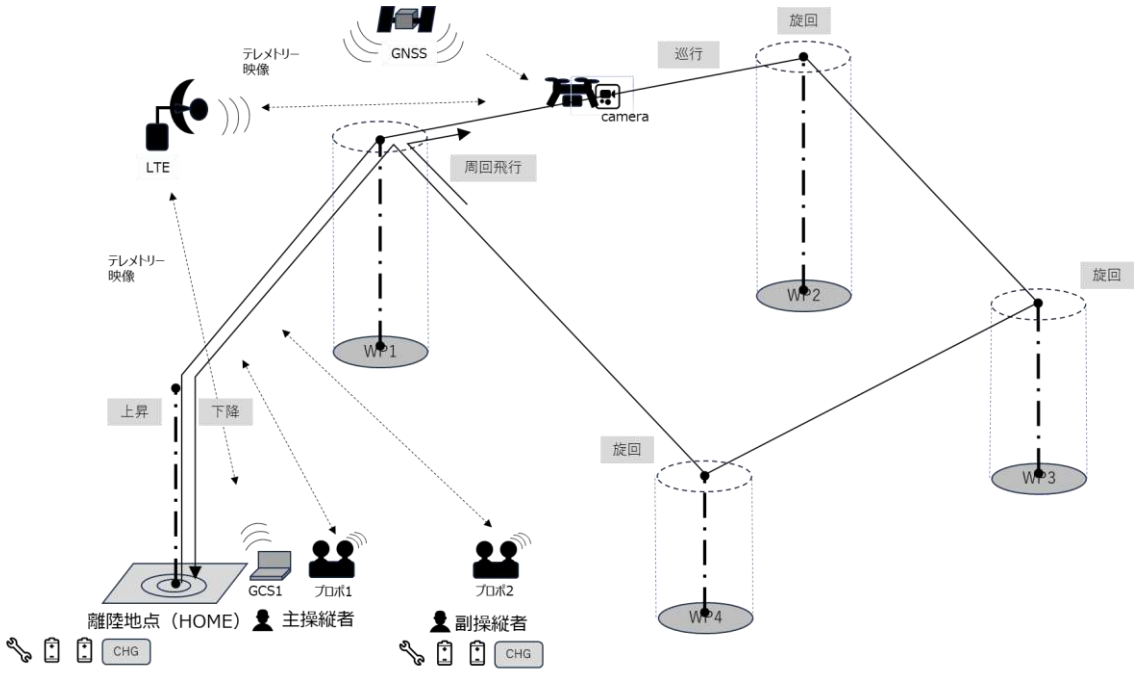


図 4.2-2 代表的な飛行パターンを「セクション 300」飛行試験パターンに置き換えた一例

4.3 飛行試験における飛行エンベロープについて

「サーキュラーNo8-001 セクション 300(b)」

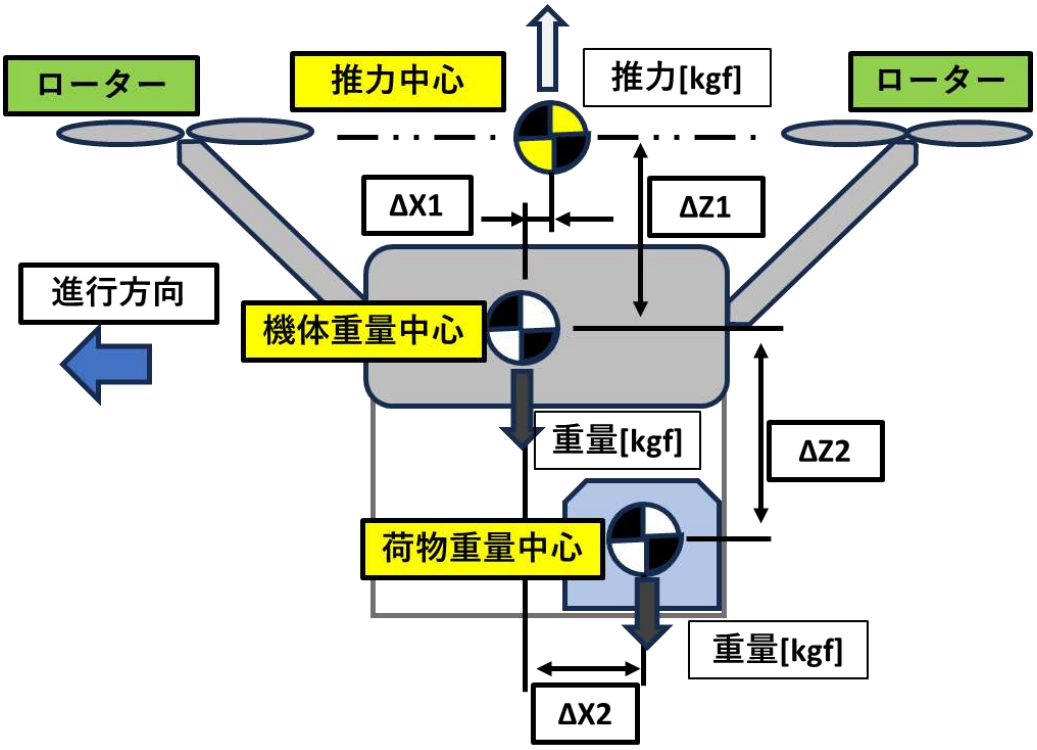
> *(b) 試験には運用のすべてのフェーズにおけるすべての飛行エンベロープの評価を含まなければならない。さらに、少なくとも以下を考慮すること。*
>
> *(1) 飛行距離*
> *(2) 飛行時間*
> *(3) ルートの複雑性*
> *(4) 重量*
> *(5) 重心*
> *(6) 密度高度*
> *(7) 外気温度*
> *(8) 対気速度又は対地速度*
> *(9) 風速*
> *(10) 天候*
> *(11) 夜間運用(夜間運用を行う場合*
> *(12) エネルギー貯蔵系統の容量*
> *(13) 操縦者に対する機体の数（1 対 1, 1 対複数等）*
>
> *[引用:サーキュラーNo.8-001]*

【解説】

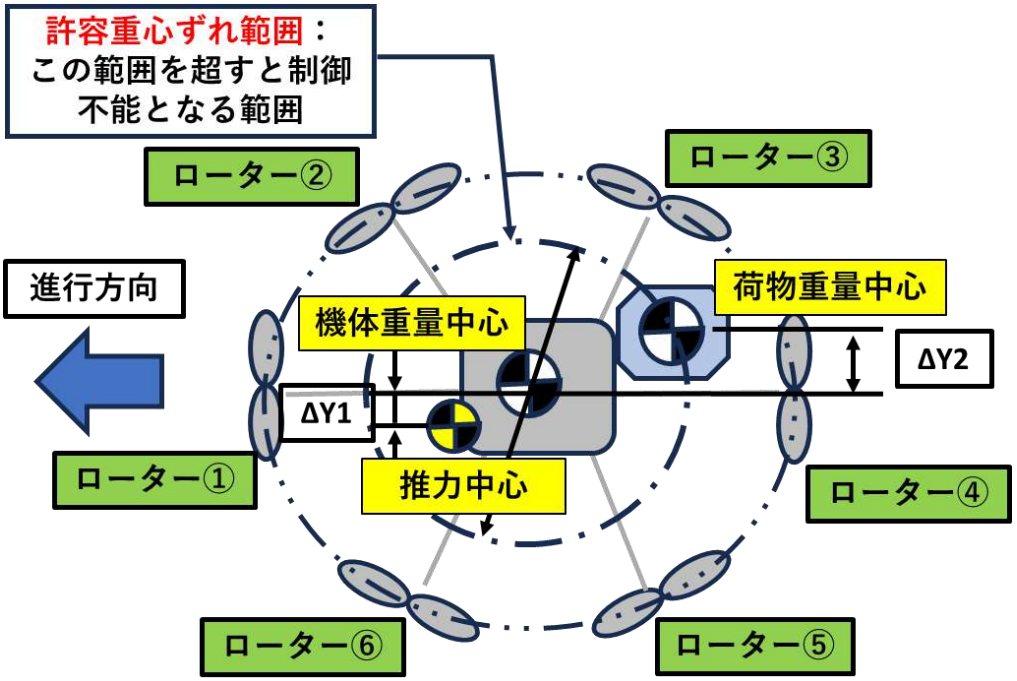
- 飛行試験は、(b)-(1)～(13)を組み合わせることで、合理的な飛行試験を計画することができる。
  飛行試験の条件の組み合わせには本解説書の Appendix 1 に示すような、飛行試験ケースマトリックスを参考にしてもよい。
  本解説書で例示している飛行試験マトリックスは、飛行試験条件を以下の2条件に大きく分類し、それぞれを組み合わせてマトリックスを整理している。

  ① 環境依存条件：意図的に設定不可能なもの
  （外的環境に合わせて計画が必要なもの）
  ② 機体形態：意図的に設定可能なもの

- (b)(1)飛行距離：CONOPS に示されている運用上の飛行距離
- (b)(2)飛行時間：CONOPS に示されている運用上の飛行時間
- (b)(3)ルートの複雑性：
  本解説書**項に例示するような、CONOPS に示されている運用フライトの飛行要素をすべて網羅した飛行試験パターンを作成する。
- (b)(4)重量、(5)重心：本解説書図 4.3-1
- (b)(6)密度高度：意味：PHAK Chapter 4 (mlit.go.jp)(4)
  CONOPS で示される最高高度での試験飛行による証明が必要。
- (b)(7)外気温度:最高/最低　基準の概要を参照
- (b)(8)対気速度または対地速度：
  マルチローターは一般的に対気速度の測定が難しい。風速と対地速度から推定が可能。



(a)垂直方向の重心のずれ範囲



(b) 平面方向の重心のずれ範囲

図 4.3-1 機体の重心位置(参考例)

- (b)(9)風速：自然環境での試験を基本とする。
  風速や気象状況は試験当日の状況に依存する。したがって試験当日の気象環境に中で、突風を定義して試験をすることが大変難しいと考えられる。突風の定義は、有人の航空機に関しては明確に定義されているものの、無人航空機に対して今まで突風を定義したものは存在しない。また、たとえ突風が定義されても無人航空がどのような反応をすれば良しとするかはこれまた定義が難しい。このため、試験においては校正された風速計などを用いて試験期間における風速を計測し、後処理として統計的な処理を行いどの程度の風速の変化があったかを検討することが望ましい。このような情報をもとに当該無人航空機の突風応答ついて、機体が耐えうる風速の範囲を機体メーカーサイドの見解として提示することが可能である。この情報に関しては機体メーカーの考え方によって異なるため、検査者とよく相談することを推奨する。
  突風応答に対する機体の安全性は、突然の突風が機体に作用したとしても計画外飛行、制御不能、想定飛行範囲からの逸脱またはリカバリーエリア外での非常着陸につながる不具合なく飛行が可能であることである。
- 風速の計測
  飛行試験エリアの複数場所に校正済みの風速計を地上高さ1．5mに設置し、風速を計測することを推奨する。この風速の時系列は試験後の風速の解析に使われるので、時間や試験ケースなど必要な記録をしっかりつけることが推奨される
  ドップラーレーダーなどの計測機器も存在するが、一般的に使用することは難しい。

- 風洞の利用
  風洞では基本的に乱れの少ない気流を発生させ、その中で機体の空力性能などを計測するために用いられる。このため通常は模型などを風洞内に固定し定常風を当てながら空力的な特性を計測するのが通常である。他方気流に上下左右の速度変動を畳重させた突風風洞も存在する（例えば JAXA 所有の突風風洞）。無人航空機のサイズによってはこのような突風風洞を用いることが可能であるがあくまで機体を拘束させて空気力を測定することが基本である。他方JAXAの大型低速風洞（縦6．5m、横5.5m）では過去において機体を固定せずにフリーフライトをさせた例もあります。このような、風洞を目的に応じて利用することも１つの考え方です。風洞施設内での限界飛行試験、フライトフェーズごとの試験は、実現性と墜落などのトラブルに対する十分な配慮と、試験の有意性の説明が必要である。
  ※JAXA の風洞については民間の方も利用可能である。

CFD やそのほかの数値解析手法は、マルチローターの運動を解析するのに有効である。運動解析には各ローターの計算精度を向上させることが重要である。しかしながら、今までこの種の解析手法は確立されておらず、また飛行試験との比較検証も十分なされていないというのが現状である。今後この種の解析手法が発展することで、飛行試験に代わりうる手段として確立する可能性がある。

- (b)(10)天候　未議論
- (b)(11)夜間運用　未議論
- (b)(12)エネルギー貯蔵系統の要領　未議論
- (b)(13)操縦者に対する機体の数：今回の検討対象外
- (c)試験ケースとして採用済み
- (d)別々の飛行プロファイルおよびルート　未議論
- (e)EMI、HIRF　未議論
- (f)二などライセンスパイロットのイメージ
- 複数人の技量の異なるパイロットによる操縦も可
- (g)例えば、トラックでの輸送時の振動や衝撃、アームの先端を持ってのハンドリングなど、運用時に考えられる機体への入力を考慮することが求められている。また、運用現場での炎天下放置、保管条件なども考慮する必要がある。
- (j)試験飛行ケースに取り込み。重量、重心の変動に含める

4.4 飛行試験時間、機数

> *その他参考となる情報　第二種型式認証の実証飛行試験の時間について*
>
> *最大離陸重量が 25kg 未満の型式は、 50 時間の実証飛行試験が必要となる。*
>
> *［引用：航空局ガイドライン］*

> *試験の条件*
>
> *セクション 300 試験の意図は、妥当なサンプル量により初期故障及び摩耗故障の発見に寄与させることも考慮している。そのため、膨大な数の機体を一斉に飛行させる実証や、余りに少ない機体数（例えば一機）での実証は行うべきではない。セクション 300 の実証を行うのに必要な最少機体数は原則三機である。。*
>
> *［引用：航空局ガイドライン］*

【解説】

「セクション 300」では 25kg 未満の機体は、飛行時間は 50 時間、機数は最小三機（次項）と規定されている。この時間設定と機数設定は、初期故障と摩耗故障の発見のためとされている。（次項およびバスタブカーブの例を参照）。

一方、二種 25kg 未満の機体には「セクション 315 疲労試験（以降、「セクション 315」と呼ぶ）」による耐久寿命の証明と寿命の ICA への記載を求められていない。

二種 25kg 未満の機体については、運用する機体の寿命に関して機体メーカーが ICA および無人航空機飛行規程に記載し運用者に周知することを推奨する。

上記の点から、「セクション 300」の飛行試験の目的を初期故障の発見と位置づけ、飛行時間と機数については 50h÷3 機=16.7hを三機で飛ばすことが可能である。

市場寿命については機体メーカーの判断によります。また、ICAに適切な部品交換時期を指定する

ことにより、16.7h 時間以上の運用をすることができる。

※構造寿命については「航空局ガイドライン」「セクション 315」を参照（二種 25kg 未満は適用なし）

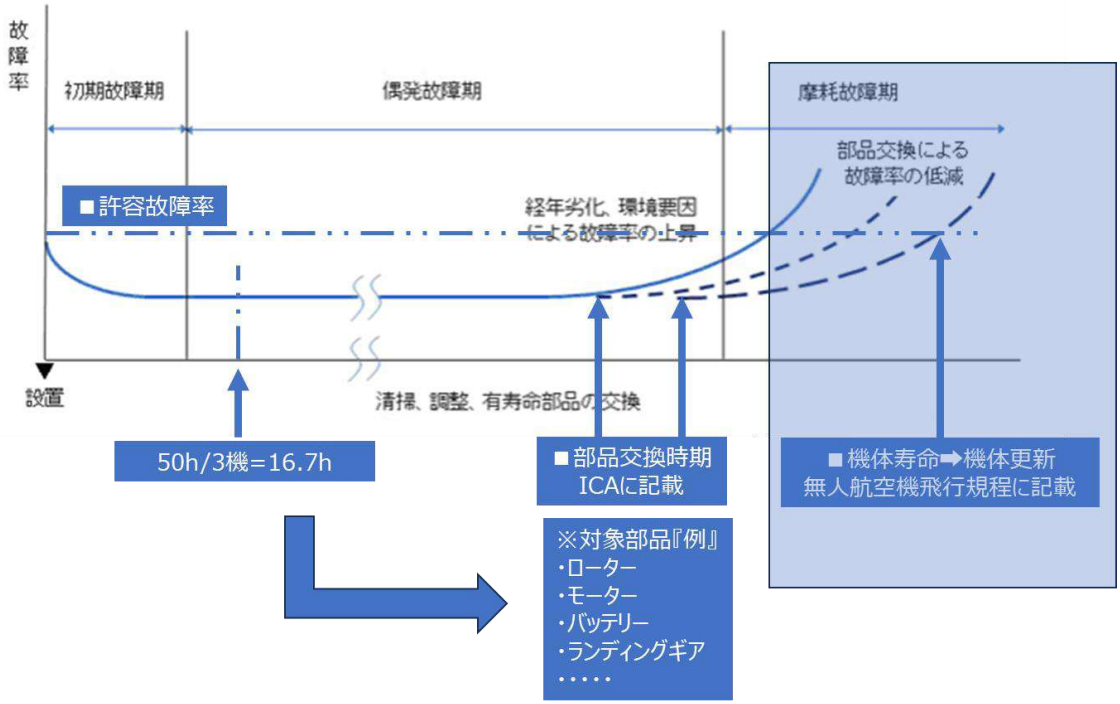


図 4.4-1 機器の故障率の一般的な解説

5 今後の課題（未議論項目）

WG 活動で議論があったが未対応（今後対応予定） 項目は以下の通り。

5.1 飛行エンベロープ

- (b)(10)天候　未議論
- (b)(11)夜間運用　未議論
- (b)(12)エネルギー貯蔵系統の要領　未議論
- (d)別々の飛行プロファイルおよびルート　未議論
- (e)EMI、HIRF　未議論

5.2 試験方案の記載事項について　および飛行準備段階から飛行試験広告までの流れ

- 「セクション CP」をベースに必要に応じ「セクション 300」向けに修正

5.3 不具合発生時の扱い

DRAFT2 にて追記予定

Appendix 1 証明手順例など

D&R.300 試験ケース検討表

- 試験ケースは、試験地域/場所および/または試験季節/時間などに依存する条件ごと、など、機体形態に依存する条件ごとに設定する。
  (b) (13)機体対操縦者比、など、(e)電磁干渉 EMI および/または高強度放射電界 HIRF は当面対象外とする。
- 試験地域/場所および/または試験季節/時間などに依存する条件:
  - 条件を組み合わせた証明は最小限とすることでよいか?
  - (b)-(6)密度高度
  - (b)-(7)外気温度
  - (b)-(9)風速
  - (b)-(10)天候
  - (b)-(11)夜間運用(ConOps に指定される場合)
- 機体形態に依存する条件:
  - (b)-(4)重量
  - (b)-(5)重心
  - (b)-(12)エネルギー貯蔵システムの容量(劣化バッテリー搭載)
  - (j)貨物搭載
  - (b)-(1)飛行距離、(b)-(2)飛行時間、(b)-(3)ルートの複雑性:
- 高負荷形態のみで実施することでよいか?
- 試験条件の刻み:
- 重量、重心および風速は、最小、中間、最大の 3 形態を基本とすることでよいか?
- (b)-(8)速度および飛行フェーズ(離陸、上昇、水平飛行、旋回、降下、着陸)など、ケース中で変化させることができる条件は、飛行試験方案/飛行試験手順書作成時に設定する。(試験すべき速度は表 5.3-2 に示す。)

293
294 表 5.3-1「セクション 300」飛行試験ケース案(ConOps で指定がない場合 40 ケース)

D&R.300 番号	変化させる条件	条件(整数値は実施する飛行回数=ケース数)							特記事項
		重量 / 密度高度	+0%(最小)	+25%	+50%(中間)	+75%	+100%(最大)	備 考	
(b)-(6)	密度高度(3 ケース)	最大	1	-	-	-	2		最大密度高度においては高負荷(最大重量、最後方重心) 最小高度、地上高度における試験で証明
		中間	-	-	-	-	-	密度が中間	
		最小	-	-	-	-	-		
		重量 / 外気温度	+0%(最小)	+25%	+50%(中間)	+75%	+100%(最大)	備 考	
(b)-(7)	外気温度(5 ケース)	最高	-	-	-	-	2		最高温度では高負荷(推力係数大)、最低温度では低負荷(推力係数小)を重点実施。
		中間	-	-	-	-	-		
		最低	2	-	-	-	1		
		重心 / 重量	-50%(最前方)	-25%	0%(中間)	+25%	+50%(最後方)	備 考	設計者/製造者が指定する方向、または、操縦者が前進操舵時に飛行する方向を前方とする。
(b)-(4) (b)-(5)	重量・重心の組み合わせ (15 ケース)	+100%(最大)	1	-	1	-	1		特記の他、重心は左右中央。 左右の対称性から、左方または右方重心を中心に実施し、逆側は最小限のみ実施する。 重心の上下の変化(荷物やペイロードカメラの機体下部搭載などによる)は、(i)において試験する。 前後重心、左右重心とも、試験条件には、重量・重心エンベロープが形成する多角形の全頂点を含むことを基本とする。 許容誤差: 重量 設定値の-1%から+5% 重心 中間から±7%
		同上	1	-	1	-	1	最左方	
		同上	-	-	1	-	-	最右方	
		75%	-	-	-	-	-		
		同上	-	-	-	-	-	最左方	
		+50%(中間)	-		1		-		
		同上	-		-		-	最左方	
		+25%	-	-	-	-	-		
		同上	-	-	-	-	-	最左方	
		+0%(最小)	1	-	1	-	1		
		同上	1	-	1	-	1	最左方	
		同上	-	-	1	-	-	最右方	
		重心 / 重量	-50%(最前/左)	-25%	0%(中間)	+25%	+50%(最後/右)	備 考	
(b)-(9)	風速(6 ケース)	+100%(最大)	-	-	-	-	-	前方風最大*(向風)	風の影響を受けやすい最小重量で実施。 重心は、風向の最逆側(前方風の場合は最後方、後方風は最前方、右/左横風は最左/右方(対称性から片側のみ実施)。 許容誤差: 2 m/s *定常風の値
		+0%(最小)	2	-	-	-	-		
		+100%(最大)	-	-	-	-	-	後方風最大*(背風)	
		+0%(最小)	-	-	-	-	2		
		+100%(最大)	-	-	-	-	-	(右)横風最大*	
		+0%(最小)	2	-	-	-	-		
		重心 / 重量			適宜			備 考	
(b)-(10)	天候(6 ケース)	適宜	-	-	3	-	-	降雨(XX mm/h)	ConOps で指定される天候
			-	-	3	-	-	他 (TBD)	
		重心 / 重量			適宜			備 考	
(b)-(11)	夜間運用(5 ケース)	適宜	-	-	5	-	-		ConOps で指定される場合。
		重心 / 外気温度			適宜			備 考	
(b)-(12)	エネルギー貯蔵システムの容量 (5 ケース)	最高	-	-	2	-	-		劣化した電池が部分充電された状態で実施する。
		最低	-	-	3	-	-		
		重心 / 重量	-50%(最前方)	-25%	0%(中間)	+25%	+50%(最後方)	備 考	
(j)	機外下部に荷物格納箱、カメラなどを搭載する運用(10 ケース)	最大重量	1***	-	1***	-	2+1***	最大速度まで実施	**搭載状態で実現できる最小重量。 ***スリング搭載場合。
		最小重量**	1***	-	1***	-	2+1***	最大速度まで実施	
		重量**** / 密度高度	+0%(最小)	+25%	+50%(中間)	+75%	+100%(最大)	備 考	****重心は最後方を基本とする。
(b)-(1)	航続距離、航続時間、ルートの複雑さ(6 ケース)	適宜	-	-	-	-	2	最大航続距離	最大航続距離速度で実施。
(b)-(2)			-	-	-	-	2	最大航続時間	最大航続時間速度で実施。
(b)-(3)			-	-	-	-	2	ルートの複雑さ	

295

296

表 5.3-2 試験条件案

		速度* / 飛行フェーズ*	最小	1/4	中間**	3/4	最大	備 考	*各許容飛行ﾌｪｰｽﾞおける許容速度。 **ノミナル速度（最小パワー速度近傍）
	密度高度、外気温度、重量・重心の各ケースで実施すべき飛行条件（飛行フェーズおよび速度） ***当該条件において 2 倍または 3 倍の時間飛行することでよいか?	**離陸**	-	-	1	-	2***		離陸上昇を含む。
		ホバリング	-	-	2***	-	-		地面効果外。
		上昇	1	-	2***	-	2***		
		巡航	1	-	1	-	3***		
		旋回	1	-	1	-	2***		
		降下	1	-	1	-	2***		
		着陸	-	-	1	-	2***		着陸アプローチを含む。

297

298

299

Appendix 2 各セクション特有の用語集

DRAFT2 にて加筆予定

Appendix 3 関連文書

(1) サーキュラー No.8-001 無人航空機の型式認証等における安全基準および均一性基準に対する検査要領、2022 年 9 月 7 日(国空機第 456 号)、https://www.mlit.go.jp/koku/content/001520547.pdf

(2) 無人航空機の型式認証等の取得のためのガイドライン、2022 年 11 月 2 日、https://www1.mlit.go.jp/common/001574425.pdf

Appendix 4　サブ WG の構成員名簿

　無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 300 耐久性と信頼性の構成員名簿（サブ　WG　主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD、Rev.01）Appendix3を参照すること。

役割	氏名	所属
主査	森下　尚久	イームズ・ロボティクス株式会社
ライター	三輪　昌史	国立大学法人　徳島大学
ライター	齊藤　茂	一般財団法人日本海事協会

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

322

RMD-305 DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

安全基準セクション 305 起こり得る故障 解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

65

図 目次

表 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」と呼ぶ）安全基準「セクション 305　起こり得る故障（以降、「セクション 305」と呼ぶ）」に対する解説書である。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”（以降、「サーキュラーNo.8-001」と呼ぶ）」の「305　起こり得る故障」を以下に引用する。

・305 起こり得る故障

無人航空機は、単一の起こり得る故障によって機体の制御不能又は想定飛行範囲からの逸脱を生じないように設計されなければならない。これは、試験により実証されなければならない。

（a）　起こり得る故障については、少なくとも以下の機器に関係するものを考慮しなければならない。

（1）　推進系統

（2）　C2 リンク

（3）　全球測位衛星システム（GNSS）

（4）　単一障害点がある操縦系統の機器

（5）　コントロールステーション

（6）　申請者によって指定されるその他の関連システム（AE）

（b）　試験に使用する無人航空機は、無人航空機飛行規程に従って運用されること。

（c）　個々の試験は、飛行におけるクリティカルフェーズ及びモードに対し、最も厳しい操縦者と無人航空機数の比率で 実施しなければならない。

3　「航空局ガイドライン」（引用）

「航空局ガイドライン」 安全基準 「305　起こり得る故障」の「基準の概要」、「適合性証明方法（MoC）」、「その他参考となる情報」を以下に引用する。

・305 起こり得る故障

<u>基準の概要</u>

本基準では、起こり得る故障に対し試験を行うものです。これはセクション 300 の試験に追加で行うもので、セクション 300 とは別の観点で無人航空機を評価する必要性から行うものです。具体的には、単一の起こり得る故障（a probable failure）が発生した場合における無人航空機の機能・性能が低下した状態を評価するものです。

セクション 300 とは Pass/Fail Criteria が異なり、起こり得る故障に起因する機体の制御不能又は想定飛行範囲からの逸脱のみが許容されません。

想定飛行範囲からの逸脱については、無人航空機が飛行する空間と時間の観点から、明らかな飛行経路又は運用エリアからの逸脱を考慮します。本基準では、原則として着陸場所以外でのパラシュートや制御下にある非常着陸は許容され、着陸場所以外での墜落は制御不能とみなされますが、第一種型式認証と第二種型式認証との違い、またCONOPS によってPass/Fail Criteria の調整が必要になるため、検査者とよく話し合う必要があります。

なお、本試験は可能な限り飛行試験で行うことが望ましいものの、その場合、故障模擬を行うための専用ソフトウェア又はハードウェアが必要になるケースが考えられます。一方で、飛行試験が合理的でない場合又は安全への影響が考えられる場合、地上試験、ラボ試験又は解析も許容されます。

また、(a)項(1)～(6)に限らず、無人航空機の設計に応じてその他のフェイラーモードが考えられる場合、それが制御不能又は想定飛行範囲からの逸脱に繋がらないことを実証する必要があります。

この試験はエースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者によって評価される必要があります。なお、最低限の要件を満たした操縦者とは、型式認証の種類(第一種型式認証又は第二種型式認証)に応じた操縦者資格又は当該資格に相当する能力及び当該機における最低限の操縦要件を満たす者となります。

適合性証明方法(MoC):6

(a),(b),(c): セクション 305 飛行試験方案 (MoC 6)

以下の故障状態を意図的に発生させて、無人航空機が制御不能又は想定飛行範囲からの逸脱を起さないことを評価します。試験ケースとして以下を考慮し、試験方案を作成します:

- *(1) 少なくともひとつの推進システム(例えばモーター)又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う*
- *(2) C2 リンクの品質低下(可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続及び遅延など)を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(3) C2 リンクが完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(4) GNSS の品質低下を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(5) GNSS が完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う*
- *(6) フライトコントロール機構における単一障害点(喪失)を実証する。例えば、シングルストリングサーボがある無人航空機では、ハードオーバーを実証すべきである*
- *(7) コントロールステーションの電源、表示ディスプレイ及び/又は運航者の制御用インターフェースの喪失を実証する*
- *(8) 関連機器に応じた故障状態を実証する*

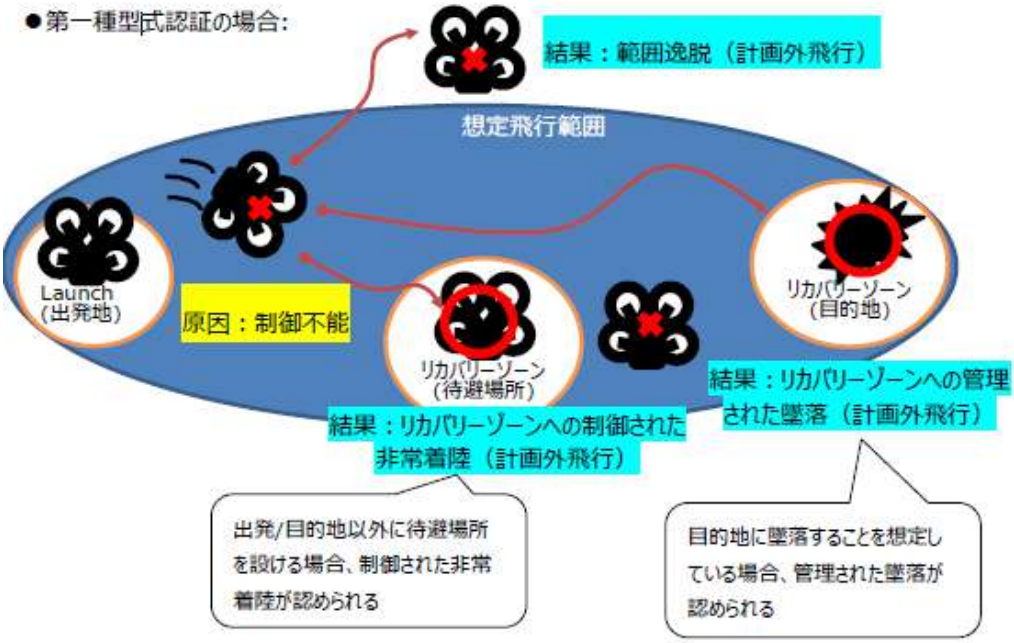
（9） 複数の機体を一人の操縦者で制御する場合、同時に発生し得る最大機数の故障模擬において、その管理能力を実証する

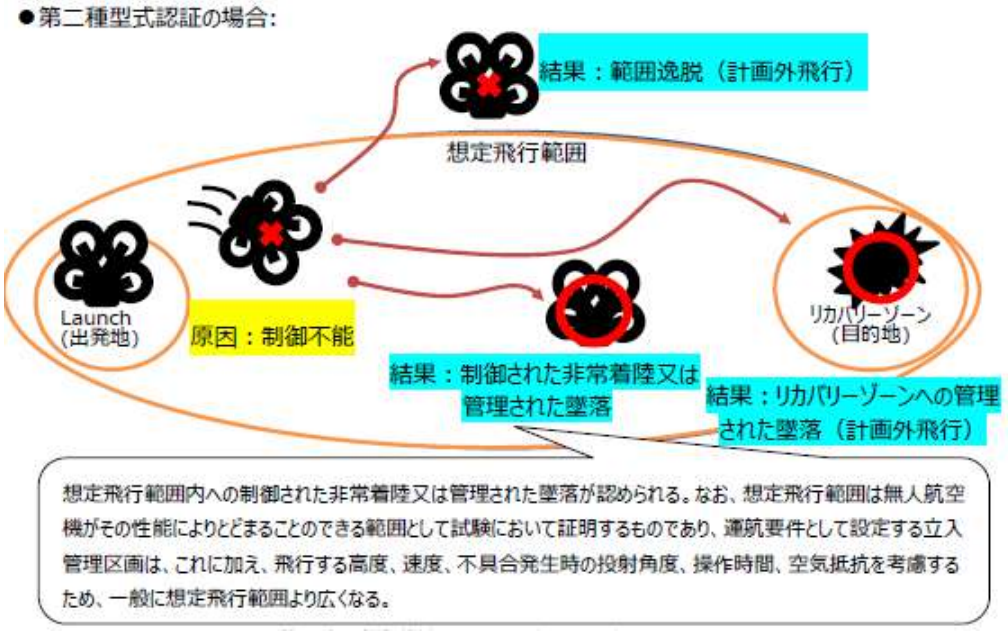
(a),(b),(c): <u>セクション 305 飛行試験報告書</u>（MoC 6）

試験結果を報告書としてまとめます。

<u>その他参考となる情報</u>

セクション 305 の Pass/Fail Criteria を図示したものが以下となります:





4　解説書

4.1 はじめに

本基準では、起こり得る故障に対し試験を行う。これは「セクション 300 耐久性と信頼性（以降、「セクション 300」と呼ぶ）」の試験に追加で行うものであり、「セクション 300」とは別の観点で無人航空機を評価する必要性から行うものである。具体的には、単一の起こり得る故障（a probable failure）が発生した場合における無人航空機の機能・性能が低下した状態を評価し、それに起因する「制御不能又は想定飛行範囲からの逸脱」が発生しないことを原則として試験により検証するものである。

本基準の第一の趣旨は任意の一故障時に地上の第三者などに被害を与えないことであり、第三者を排除した立入監視区域上空で運用をおこなう第二種認証対象の機体においては、飛行中断などを含め何らかの手段により、任意の一故障時に想定飛行範囲から逸脱しないことが重要である。一方で「サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領の安全基準（以降、「安全基準」と呼ぶ）」の要求にはそれと並んで「制御不能」を生じないことが挙げられており、この意義も含めて検査者と申請者の調整により試験方案、pass/fail criteria を確立した上で立証を行うことが課題となる。

4.2 適用対象などについて

（1） 基準の適用範囲

2 章で示したサーキュラー基準本文の適用範囲について示す。

同じく「サーキュラーNo.8-001」 第Ⅱ部第 1 章の表 1 に示される。以下表 4.2-1 に該当箇所（枠内）を示す。最大離陸重量が 25kg 未満の機体（表中二重枠で表示）で、目視外飛行を実施しないものについては、「セクション 305」自体が適用されない。一方同じ 25kg 未満の機体で目視外飛行を実施するものについては、※8 が適用され、「セクション 305 a）項（2）、（3）、（6）」のみ適用される

（2）C2 リンク
（3）全球測位衛星システム（GNSS）
（6）申請者によって指定されるその他の関連システム（AE）

「セクション 305」はすべての機器を対象としたうえで、、「セクション 305 a）項」指定のものを最低限とする規定であるが、限定の趣旨を考えると、ここでは（2）、（3）、（6）についてのみ立証を行えば良いものと解釈される。

その他機体区分（表中点線枠で表示）については、すべて適用となる。

なお、この解説書内では、すべて適用となる場合（最大離陸重量が 25kg 以上の機体）を想定して記載する。

表 4.2-1 区分に応じて適用される規定

（凡例）✓：適用されるもの、✓✓：該当する特定飛行※1に応じて適用されるもの、N/A：適用されないもの

区分	第二種				第一種
	機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機				機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機
	最大離陸重量4kg未満のもの	最大離陸重量4kg以上25kg未満のもの	最大離陸重量25kg以上のもの		人口密度の低い地域その他の無人航空機の飛行により航空機の航行の安全並びに地上及び水上の人及び物件の安全を損なうおそれが少ないと認められる地域を飛行するもの
			特定飛行を行うもののうち、無人航空機の飛行により航空機の航行の安全並びに地上及び水上の人及び物件の安全を損なうおそれが少ないと認められるもの※2	その他のもの※3	
001 設計概念書（CONOPS）	✓	✓	✓	✓	✓
005 定義	✓	✓	✓	✓	✓
100 無人航空機に係る信号の監視と送信	✓※4	✓	✓	✓	✓
105 無人航空機の安全な運用に必要な関連システム	✓	✓	✓	✓	✓
110 ソフトウェア	✓※5	✓※5	✓※5	✓	✓
115 サイバーセキュリティ	✓	✓	✓	✓	✓
120 緊急時の対応計画	✓✓※6	✓	✓	✓	✓
125 雷	✓	✓	✓	✓	✓
130 悪天候	✓	✓	✓	✓	✓
135 重要な部品（フライトエッセンシャルパーツ）	✓	✓	✓	✓	✓
140 その他必要となる設計及び構成	✓※7	✓※7	✓※7	✓※7	✓※7
200 無人航空機飛行規程	✓	✓	✓	✓	✓
205 ICA	✓	✓	✓	✓	✓
300 耐久性及び信頼性	✓	✓	✓	✓	✓
305 起こり得る故障	✓✓※8	✓✓※8	✓	✓	✓
310 能力及び機能	✓※9	✓	✓	✓	✓
315 疲労試験	N/A	N/A	✓	✓	✓
320 制限の検証	N/A	N/A	✓	✓	✓

※8：目視外飛行の場合は305(a)項(2)、(3)及び(6)がそれぞれ適用。それ以外の飛行の場合は非適用

出所）サーキュラーNo.008-1 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領

（2）「起こり得る故障」とは

「起こり得る故障：probable failure」を設計検討の際に、極端に故障の発生確率が低い機器に対し過剰な試験を行うことは合理的ではない。設計情報として故障の発生確率を示すことができれば「起こり得る故障」に該当しないと考えられる。ただし、その場合でも最低限実施しなければならない対象を識別したのが、「セクション 305 a）項」の規定であると考えられる。

では、どの程度の確率を目標とすることが合理的か、いくつかの数値例を紹介する。ただし、ここで紹介する数値には大きな差があり、どの場面において、どの数値が妥当かについては十分な検討の上、検査者との合意形成が必要である。

【参考 1】航空機に関する情報：

- FAA AC23.1309[1]（軽飛行機向け）probable failure
  → 1.0×10^{-3}
- FAA AC25.1309[2]
  → 1.0×10^{-5}
- より大規模なハザード（領域外の他の航空機を巻き込む事故事例などを想定した場合）と考え

る場合(参考 JARUS　AMC RPAS 1309-01[3]、EUROCAE ER-110[4]など)

→ 1.0×10^{-7}

【参考 2】機能安全に関する情報:

IEC61508-1(JIS C0508-1) [5]高頻度作動・連続モード時 失敗尺度

SIL4　10^{-9} 以上 10^{-8} 未満

SIL3　10^{-8} 以上 10^{-7} 未満

SIL2　10^{-7} 以上 10^{-6} 未満

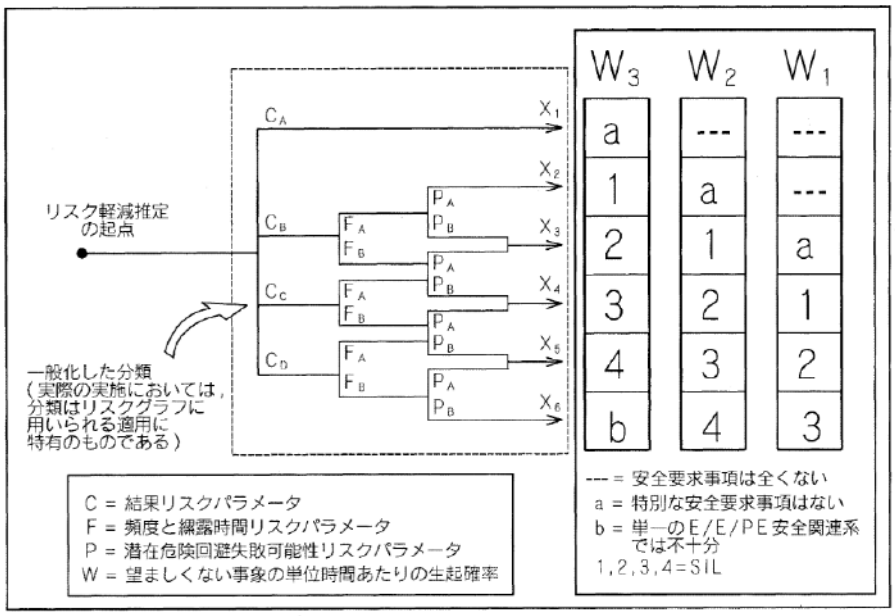
SIL1　10^{-6} 以上 10^{-5} 未満

SIL はリスク(被害のひどさ、頻度、回避可能性などの組み合わせ)によって変化する。一般的には確率が低くても複数人の死亡がある場合などは SIL4 といわれる。詳しくは、IEC61508-5 AnnexD で紹介されるリスクグラフなどが参考となる。

【参考】
「数値を明確に示してほしい」は設計者が持つ当たり前の要求である。故障の発生確率の数値が 10^{-3} か 10^{-7} で異なると、例えばハードウェアは、単一部品か、もしくは、信頼性向上のために冗長設計が求められる等の違いがあり、設計や製品コンセプトに多大な影響を与える。
当解説書作成のワーキンググループでも、専門家により故障の発生確率についての議論が行われたが、主張する数値に大きな乖離が出て結論には至っていない。これには、以下 2 つの理由が考えられる。

1. 数値を定められるほどの実績が市場に存在していない
2. 既存で用いられる数値の妥当性を社会合意できる情報が存在しない(例えば壊滅的を防ぐために10^{-x}で十分かを説明されることはない。規格策定では、実績を元にした技術限界／社会情勢を鑑み、妥協も含む合意形成で決めている)

これら 2 つの理由が示すのは、数値を定めるためには、経験的に得られる実績を元に社会的な合意形成(各種の規格書策定の議論も該当)が必要である。市場に製品を普及させる製造者が、より良い製品づくりのために、規格策定活動に参加する意義が見いだせる事例とも捉えられる。



附属書D図1　リスクグラフ：一般的スキーム

図 4.2-1 安全に関するリスクグラフ

出所)JIS C0508-5:1999[5] 附属書 D(参考)「定性的方法による SIL の決定:リスクグラフ)」

（3） 対象となる機器・フェイラーモードの識別

「航空局ガイドライン」には、基準の概要にて

> *(a)項(1)～(6)に限らず、無人航空機の設計に応じてその他のフェイラーモードが考えられる場合、それが制御不能又は想定飛行範囲からの逸脱に繋がらないことを実証する必要があります。*
>
> *［引用:航空局ガイドライン／セクション 305　基準の概要］*

と記述されている。そのため基本的にはすべての機器が対象になると考えられる。またフェイラーモードについても、単なる機能喪失にとどまらず、その他にも、暴走、劣化、遅延、固着など、期待した通りに動作しないすべてのフェイラーモードを考慮する必要がある。とはいえ、実行上すべての機器のすべてのフェイラーモードについて立証することは現実的でないため、安全性解析などの手法により、「機体の制御不能又は想定飛行範囲からの逸脱」が起こる可能性のあるものに限定して、試験などによる立証を行うこととなる。安全性解析の結果は、検査者と製造者の間で、部品別のフェイラーモードとその至る結果を共有しやすい文書となる。そのため、すべてをただ網羅的に確認するよりも効率的に試験を行うべき箇所を抽出できるものとなる。ただし、これはすべてのフェイラーモードを網羅的に試験してはいけない、ということではない。部品点数がそれほど多くなく、すべてを試すことが合理的である場合には、1 つの方法として総当たりでの試験も実施可能である。

安全性解析については FTA、FMEA、FHA、STAMP/STPA、リスクアセスメントなどの手法があるが、特に「セクション 135 重要な部品（フライトエッセンシャルパーツ）（以降、「セクション 135」と呼ぶ）」について解説する関連文書(6)において、フライトエッセンシャルパーツ識別の手段として簡易 FMEA によるケースが解説されているため、そちらを参照されたい。ただし、同文書で識別されるフライトエッセンシャルパーツは「セクション305」の対象の識別とはクライテリアが異なるため、フライトエッセンシャルパーツが必ずしも「セクション 305」の対象となる、またはその逆となるわけではないことには注意しなければならない。解析の結果から得られる機体システムへの最終的な影響を勘案し、4.3 項で述べる「セクション 305」としての pass/fail criteria に基づいて対象となる機器、フェイラーモードを識別することが必要になる。

注意点として、「対策」として冗長設計などにより「制御不能又は想定飛行範囲からの逸脱」を防ぐ構造となっている場合についても冗長設計の正しさを証明する観点から「セクション 305」の対象になると考えられる。換言すれば「機体の制御不能又は想定飛行範囲からの逸脱」いわば頂上事象として FTA を実施した際に、原因として識別される機器・フェイラーモードが「セクション 305」の対象になると考えれば良い。

解析の粒度についても、申請時に提出する書類に含まれる(e)部品表との一致が望ましいが、試験方法や設計活動の結果、部品表よりも要素単位が「統合する」「分割する」は、発生しても直接的な問題はない。必要なことはそれぞれ文書間、設計情報の間に発生するトレーサビリティが取れることとなる。

安全性解析で行う簡易 FMEA ともトレーサビリティが必要となるため、部品表、簡易 FMEA などで設計粒度をあわせ、「セクション 305」試験の対象となる機器の切り分けを行うことで、トレーサビリティのための煩雑な作業を避けることができる。

また、“故障”が対象であることから、構造部材などの構造破壊については対象とならないものと考えるが、機器のいわゆる“故障”が内部の物理的・機械的な損傷に起因するようなケースについては考慮が必要と考える。

サンプル事例：（これらがすべてではない点に留意が必要）

- モーター・ステータ折れ → 一般的には故障と見做される。
- ボルトの破損 → 複数本で止めているようなもの（1 本の破損が「機体の制御不能又は想定飛行範囲からの逸脱」に至らない場合）は、含まれない。

（4） ソフトウェアエラーの扱い

ソフトウェアエラーによる「機体の制御不能又は想定飛行範囲からの逸脱」が発生することが想定される場合には対象として扱う。

ただし、ソフトウェアエラーは、一般的にはシステマチック故障として扱われる（バスタブ曲線による発生ではなく、バグとして潜在的にある故障モード）ため、開発プロセスの品質によって担保する以外の技術的解決策は存在しない。

「セクション 110 ソフトウェア（以降、「セクション 110」と呼ぶ）」で規定された、テスト、構成管理、不具合管理が行われることは前提となるが、動作確認のための評価時間についても十分にソフトウェア品質に貢献していると考えられる。これら手法を活用し、ソフトウェアエラーを最小化する必要がある。

（5） ヒューマンファクターの取り扱い

「航空局ガイドライン」では基準の概要において

> *この試験はエースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者によって評価される必要があります。*
>
> *［引用：航空局ガイドライン／セクション 305 基準の概要］*

のように記述されている。

「セクション 305」の対象となる機器の故障にヒューマンエラーは含まなくてよい。ただし、試験時の操縦者の規定については検討を行う必要がある。「エースパイロットのような熟練の操縦者ではなく、最低限の要件を満たした操縦者」は、飛行規程に添った操作を確実に実施できる一方で、それ以上の咄嗟の判断やより適切な操作などまでは実施できない操縦者と解釈できる。

また、操縦者へ与えるワークロードも考える必要があるが、有人航空機で用いられている handling quality 評価の Cooper-Harper Rating（CHR）Scale などが参考になると考えられる。以下は不可となると考えられる項目を抽出した。

- 継続的に過度な作業負荷が求められる
- 過度な繰り返し作業が求められる
- 誤操作が致命的な影響となる操作が不用意に実施できる
- 操縦者が知るべき機器の状態が明確に伝達されていない

- 情報取得に手間取るユーザインタフェース
- 多様な解釈が可能となる警告表示
- 自律制御から人制御の切り替えが明確でない
- 自律制御から人制御への切り替えと同時に急な制御が求められる
- その他

一部項目については、「セクション 310 能力及び機能（以降、「セクション 310」と呼ぶ）」でも規定されており、相関を取りながら設計検討する必要がある。

4.3 前提となる安全管理手法

（1） 立証のポイント

「安全基準」にある通り、「制御不能又は想定飛行範囲からの逸脱」が発生しないことがポイントとなる。

第二種においては、飛行領域（落下時の飛散領域も含む）に第三者がいない前提となるため、「想定飛行範囲からの逸脱」が発生しないことが重視されると考えられる。ただし、要求に「制御不能」が追加されている趣旨を考慮すると、その場合においても、飛行領域における立入管理措置の実効性や第三者の資産（含むライフラインなどのインフラなど）への重大な危害、運用関係者の死傷なども考慮されている可能性があり、単純に「想定飛行範囲からの逸脱」さえしなければ良いとも言いかねる点に留意する必要がある。

（2） 飛行中断に関する“制御不能”の考え方

第二種認証を想定する機体は概ね立入管理区域の上空を飛行するものと想定され、故障などが生じて制御された飛行を継続することができない場合に、地上からの操作やフライトコントローラの指示により飛行を中断することで想定飛行範囲からの逸脱を防止し、第三者への危害を防止するものが多くある。また、特定の故障（例えばフライトコントローラからの信号喪失、動力の喪失など）に際しては、結果的に速やかに自由落下状態に至り、発生地点付近に落着することで、立入管理区域からの逸脱、ひいては第三者への危害防止を担保するような機体も存在する。このような機体についても飛行範囲や安全措置の条件などを飛行規程に適切に規定し、それにしたがって運用することにより「セクション 305」の条件のうち「想定飛行範囲からの逸脱」を防止することができる一方、飛行中断措置実施後、ないし故障発生後の自由落下状態、パラシュート降下状態などでは制御された飛行状態を維持しているわけではないことから、もう一つの条件である「制御不能」を防止できておらず、「セクション 305」の pass/fail criteria をクリアできていないのではないかとの指摘が考えられる。

制御不能については、「安全基準」にて

> *制御不能とは、無人航空機の制御された飛行状態からの意図しない逸脱を意味する。（中略）制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。*
>
> *［引用：サーキュラー No. 8-001／セクション 005］*

のように定義されている。例えばパラシュート降下については 2 つの視点が必要である。

1. （制御可能）操縦者が意図的、もしくは設計者が意図した条件下で自動的に開く場合には、「意図」された環境と考える
2. （制御不能）パラシュートで吊られた状態（風によって流される可能性がある）については、制御された飛行状態と言えない

1 と 2 の関係は、1 によって対策された後に 2 の追加リスクが発生した状態であり、安全措置に対する責任も複数のステークホルダが有する。このような複雑なリスク構造を図解説明できる SafeML（SysML を拡張した安全設計用の言語[1]）にて解説を行う。

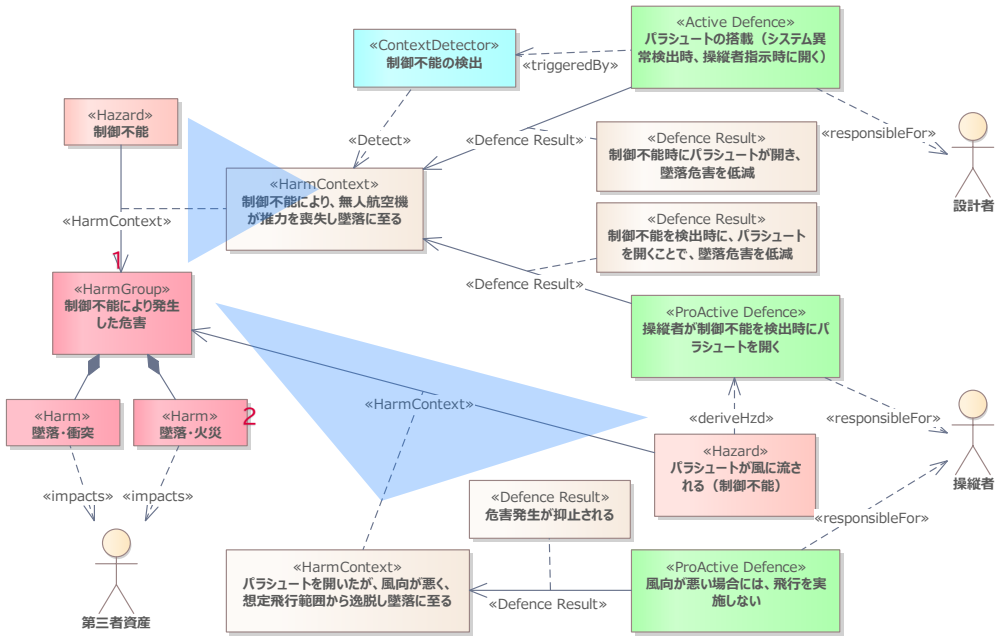


図 4.3-1 SafeML を用いた飛行中断時のリスク構造分析

推力喪失を意図的に行った場合にも、以下 2 つの視点で考えることができる。

1. （制御可能）墜落の意思決定は操縦者が行うため、制御可能である
2. （制御不能）墜落に至る制御不能状態である

一方で、関連文書[7]では「制御不能」の解釈について

> *制御不能とは、きりもみ、制御権限の喪失、空力安定性の喪失、飛行特性の発散又は同様な事象を意味し、一般的に墜落につながる状態である。 ただし、運用者によって管理されている飛行中断は制御不能の範疇に入らない。*
>
> *運用者によって管理されている飛行中断とは、結果としても死傷者（死者及び又は重傷者）が生じないための管理がされた飛行空域及び地上範囲に運用者によって意図的に飛行を完了させること*
>
> *［引用：安全 SubWG 解説書（後日正式名称と置き換え）］*

[1] RRI, WG3/SafeML メタモデル仕様書 Ver.2.1　公開, https://www.jmfrri.gr.jp/document/library/4662.html

とする見解を示している。上記の「死傷者が生じないための管理」は必ずしも第三者に限定されるものではないため、「想定飛行範囲からの逸脱」を防止しさえすれば良いというものではないが、それらが担保される限りにおいては制御された飛行状態を維持することまでは必須ではないと考えられる。また実際、「航空局ガイドライン」においても、その他参考となる情報に pass/fail criteria が図示されており、その吹き出しの中で

> *想定飛行範囲内への制御された非常着陸又は管理された墜落が認められる*
> *［引用：航空局ガイドライン／セクション 305　その他参考となる情報］*

との記述があるため、一時的に制御された飛行状態を維持できなくなることについて、最終的に「管理された墜落」に至ることを条件として、原則としては許容されていると見ることができる。

（3） 管理された墜落の考え方

「管理された墜落」は、「航空局ガイドライン」（共通 3.2 用語/略語）にて

> *想無人航空機そのものに加え、墜落後の部品の飛散範囲を考慮するなど予め設計上で想定された墜落のこと。無人航空機飛行規程で操縦者（運航体制）へ別途具体的な指示を行うことを前提とした墜落が該当。*
> *（例）部品の飛散が立入管理区画を超えないように墜落させること　等*
> *［引用：航空局ガイドライン／共通 3.2 用語/略語］*

と規定されているため、飛行中断などについても墜落後の部品の飛散範囲の考慮など、設計時点で想定されたものであれば「管理された墜落」に該当すると考えられる。追記の「飛行規程で操縦者へ別途具体的な指示を行うことを前提とした墜落が該当。」については、落下分散や上記部品の飛散も含めて想定飛行範囲領域から出ないように、そのような飛行計画の立案方法、風速制限、運用条件（高度、速度、重量など）に応じた落下分散や部品の飛散範囲の導出方法とかが飛行規程に明記されているということを言っていると考えられる。

フライトコントローラの機能喪失や電源の喪失などの単一故障により、操縦者のその時の意図・操作に関係なく墜落に至るような機体も考えられが、このような挙動についても設計上で想定されており、墜落時の飛散範囲などを示すなど、想定飛行範囲からの逸脱を防止し、安全を確保するための手段が飛行規程に明示されていることで「管理された墜落」と見做すことが可能となる。

ただし、一時的にも制御された飛行状態からの逸脱が発生することから、安全についての実効性を示す必要がある。これらも CONOPS との相関がある事象のため、個別のケースに対応して、検査者と申請者の相談により認証プロセスの早い段階から合意した方針が示せることが望ましい。

4.4 実際の立証方法

本項では、実際の立証法について、各対象に共通する基本的な考え方を記述する。実際の試験方案

については Appendix 1 にそれぞれのケースに対応してまとめた。

(1) 飛行試験の必要性

「セクション 305」の記述では「試験により」となっており、立証のための試験は必ずしも飛行試験である必要はないと考えられるが、一方で「航空局ガイドライン」の MoC では

> *以下の故障状態を意図的に発生させて、無人航空機が制御不能又は想定飛行範囲からの逸脱を起さないことを評価します。*
>
> *［引用：航空局ガイドライン／セクション 305　MoC］*

となっており、単純に故障状態から制御不能又は想定飛行範囲からの逸脱を起こさないことを立証する以上、想定する飛行状況での試験が暗に前提となっているようにも読める。ただ、一方で同じ「航空局ガイドライン」でも

> *なお、本試験は可能な限り飛行試験で行うことが望ましいものの、その場合、故障模擬を行うための専用ソフトウェア又はハードウェアが必要になるケースが考えられます。一方で、飛行試験が合理的でない場合又は安全への影響が考えられる場合、地上試験、ラボ試験又は解析も許容されます。*
>
> *［引用：航空局ガイドライン／セクション 305　基準の概要］*

との記述もあり、やはり飛行試験が必須とまでは要求していないと考えられる。総合すると

- 本来の要求としては解析ではなく「試験」である必要がある（は除外）
- 「飛行試験が合理的でない場合 or 安全への影響が考えられる場合」に限定して、地上試験、ラボ試験、さらには解析へと緩和することが許容される

と言える。ただし、「航空局ガイドライン」の MoC に記述されているような飛行状態からの立証によらない場合、単純に試行して「制御不能又は想定飛行範囲からの逸脱」が起きなかったという形では立証できないため、どのような形で pass/fail criteria を設定するかが問題になると考えられる。例えば不具合に対して安全機能を activate できることを地上試験などで立証した上で、安全機能が activate できれば「制御不能又は想定飛行範囲からの逸脱」が起きないことを別の試験や解析で立証するような方法、環境条件の影響に関係ない部分を飛行実験で実証した上で、環境条件の影響は解析で補完するような方法、解析で立証した上で、解析の妥当性を飛行実験で実証したりするようなこともあり得ると考える。そのうえで重要なことは、地上試験にせよ解析にせよ、

- 飛行試験では合理性や安全性に問題があること
- その手法で要求される故障許容性が（飛行試験よりも合理的に）立証できること

を申請者が検査者に筋道立てて説明した上で、合意された試験方案および pass/fail criteria を得ることであると考える。

（2）「厳しい飛行フェーズ」とは

例えば「航空局ガイドライン」では、適合性証明方法（MoC）の(1)で

> *この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う*
> *［引用：航空局ガイドライン／セクション 305　MoC］*

のように記述されている。最も不利な重量重心位置については「セクション 300」と同様に考えられる。

厳しい飛行フェーズについては故障ケースに依存すると考えられるが、例えば、典型的なパターンとして、機体の暴走に対応して地上からの指令で強制降下するような状況を想定すると

- 想定飛行範囲から導出される飛行可能な空域の外縁に一番近いところで
- 外縁のほうに向かって最大（対地）速度で飛行しており
- 外部風も真後ろから運用可能な最大風速で吹いていて
- 不具合の検出や操縦者の判断に要する時間が最大（といっても判断ミスや不必要な逡巡などはないとして）である

ような状況が考えられる。この場合でも、例えば巡航だけではなく上昇・降下を考えた場合

- 上昇中は、水平速度が低いことから巡航中に比べると落下分散が少なくなる傾向がある一方、出力が大きいので暴走（例えば推力指令値の固着など）の時により速度が上がりやすく、高度が上がることで落下分散が拡大する傾向がある。
- 降下中も、水平速度は比較的小さいが、出力を絞っていることで制御余裕が少なくなり、安定性が低くなるような傾向もある。

など、どのフェーズが最も厳しいか単純には決められない場合もある。上記のような状況を総合的に検討して「厳しい飛行フェーズ」を選定する、場合によっては複数フェーズを「厳しい飛行フェーズ」として識別したりするといった可能性もある。

ただし、落下分散については、実際に飛行領域の外縁で試験を実施しなくても、安全なところで故障を模擬して発生地点から最終的な落下地点までの距離を計測し、飛行規程で要求されているクリアランスの範囲内であることを確認するような方法もあると考えられる。また外部風の影響についても、解析で加算するような方法も考えられる。外部風の落下分散への影響を解析的に評価する方法については、JIS W 0711[8]の解説書が参考になる。

（3） 試験回数について

「セクション 300」には使用する機数についての要求があるが、「セクション 305」については「航空局ガイドライン」他には試験の回数に対する具体的な要求はなく、クリティカルな状況を押さえられれば 1 回の試験で良いと考えられる。一方で、確率事象や気象条件、ヒューマンファクターなんかの影響のために 1 回でクリティカルな状況を押さえられるか分からない場合は、複数回試験を実施するケースも出てくると考える。一方で、品質のばらつきやソフトウェアエラーは「セクション 300」や「セクション 110」で押さえている筈であり、その再現のために複数回の試験を実施する必要はないと考えられる。最終

346 的には所定の回数の試験でクリティカルな状況を押さえられることを検査者に説明し、合意された試
347 験方案および pass/fail criteria を得られれば良いと考える。

348 （4） 故障模擬の方法

349 故障模擬の方法については、故障を想定する機器や想定するフェイラーモードに依存するが、飛行
350 中に実際に故障を発生させるために、ハードなりソフトなりの改修は許容されると考えられる。
351 例えば、喪失の模擬としては、実際に配線を抜く、伝送経路に継電器などを挿入して実際に伝送経路
352 を切断するなどの方法が考えられるが、これを飛行中に実施するのは困難であったり危険であったり
353 するため、ソフトウェア的に模擬することも許容されると考えられる。ただし、喪失の結果が「不定」にな
354 る場合など、ソフトウェアでの模擬が妥当か、検討が必要な場合もあると思われる。
355 結局のところ、想定する故障の結果としてどのような効果が生じて、実際に模擬する手段でそれが包
356 含できているということを、検査者に説明して、合意された試験方案および pass/fail criteria を得
357 る必要がある。故障の結果がどのようになるかについては、安全性解析の分析結果も利用することが
358 できる。
359 模擬のための改修は機体コンフィギュレーションの変更になるが、それなしで故障を模擬することが
360 困難である以上、許容されると考えられる。これについても変更の内容、それが立証したい機能の部
361 分に影響がないことの説明などを通じて、検査者と合意する必要がある。また、コンフィギュレーション
362 を変えたために、試験そのものが危険にならないように注意する必要がある。例えば 1 fail safe 設計
363 になっている機体でも、最初から 1fail した状態だと一故障で危険な状況が発生しうることに注意し、
364 安全が確保できない場合は、地上試験や屋内試験などにより、安全を確保することも考える必要があ
365 る。

366 （5） 複数同時喪失の考え方

367 「航空局ガイドライン」では MOC(1)の中で、推進系の故障について

> *又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。*
>
> *[引用:航空局ガイドライン／セクション 305 MoC]*

368
369 のように記述されていることから、「セクション 305」においては、「単一の起こり得る故障」を対象とす
370 るが、「複数同時喪失」が存在する場合を想定することが望まれていると考えられる。
371 例えば、2 つの推進システムを 1 つのモーターコントローラ(ESC)で制御している場合において、
372 ESC が故障(すなわち単一の起こり得る故障)した場合の対策を求める記述である。この場合の試験
373 においては、2 つの推進システムが同時に停止した場合に、想定した対策が取れることを証明する必
374 要がある。
375
376
377
378

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定) 項目はなく、必要に応じて DARAFT2 にて加筆予定

Appendix 1　証明手順例など

本付録においては、4.4 項で述べた実際の立証方法について、特に「航空局ガイドライン」の MoC の項で特記された個別の対象について、マルチコプターを例にして実際の試験方法事例を示すものである。

> *(1)　少なくともひとつの推進システム（例えばモーター）又は複数同時喪失があり得る場合は複数の推進システムの喪失を実証する。この試験は厳しい飛行フェーズ、モード、最も不利な重量重心位置で行う。*
>
> *［引用：航空局ガイドライン／セクション 305　MoC］*

＜機体条件＞

第二種認証をおこなう機体で、最大離陸重量 25kg 以上を想定する（25kg 未満は立証の必要なし）。

飛行規程で示される故障発生後の対処について、以下の 2 ケースを想定する。

a）自動制御による飛行を継続し、地上からの指令により制御された非常着陸を実施する場合（1 推進器を喪失した状態で飛行を継続できる機体でも、劣化した飛行性能でそのままミッションを継続することは考えにくいことから、本ケースを想定した。）

b）地上からの指令により飛行中断をおこない、落着させる場合

＜実証方法＞

ケース a）

飛行中に推進器の一故障を発生させ、制御可能な飛行が継続できることを実証する。墜落を伴わないため、飛行試験により実施する。劣化した飛行性能でミッションを継続することはリスクがある（という機体を想定する）ことから、故障の検知と非常着陸指示、実際の着陸までのシークエンスを実証する。機体が極端な異常姿勢を取ることは考えにくいため、故障検知は各モーターへの指令値の変動や ESC からのステイタス情報により行われることを想定する。

試験が必要なクリティカルフェーズ（危険な状態）は 4.4（2）項を参照のこと。原則としては以下の 4 フェーズに包含されると考えられる。申請者はこの全ケースを実施する必要はないが、実施しないフェーズについては、実施するいずれかのフェーズと比較して危険度がより低いことを説明し、検査者と合意する必要がある。

①ホバリング時
②上昇時
③下降時
④最大速度前進時

具体的な工程は以下の通り

	目 的	方 法
1	推進器停止機能の装着	飛行中に 1 つの推進システムを停止できるシステムを追加。実証方法の具体的な案を以下に挙げる。 フライトコントローラからの回転指令信号線を継電器などにより遮断 モーターに供給される電源を遮断 フライトコントローラのソフトウェアにより、1 つの推進器への信号を 0(またはその他停止を意図する値)に設定する その他 いずれのケースについても推進器停止機能は地上からの指令により動作するもの、時限的に動作するものが考えられる。地上からの指令による場合、既存の C2 通信に相乗りするもの、新規に通信機器を装備するものが考えられる。
2	推進器停止機能の動作確認	プロペラを外したモーターのみでアイドリングさせ、推進器停止機能が正常にコントロールできることを地上試験で確認する。
3	正常状態確認 (1 分間の離着陸・ホバリング)	推進器停止機能を付けた状態で、離陸後安全な高度でホバリング、水平移動などを実施し、正常飛行が可能であることを確認する。安全な試験のためにも正常に飛行できることを実証することは重要。
4	故障模擬	機体離陸後、クリティカルフェーズで、推進器停止機能を発動させて 1 つの推進器を停止させ、機体が制御された飛行状態を維持できること、故障が検知され、地上局の表示などにより操縦者に認識されることを確認する。停止させる推進器の選定に当たり、推進器によって停止の影響が異なる可能性を考慮する必要がある。
5	着陸指示	地上局からの指令により、機体が非常着陸に移行できること、操縦者が着陸点などを指定する仕様の場合、地上局より正常に指定できることなどを確認する。フライトコントローラにより自動的に非常着陸に移行する仕様の場合は、前項にて検知に伴って発動することを確認する。
6	着陸	機体が自動制御により、想定飛行範囲内に着陸することを確認する。

ケース b)

飛行試験で実証しようとすると墜落による機体の喪失や、試験要員の危険を伴うことから、地上試験により、故障が検知できること、強制停止やパラシュート動作の発動が実施できることなどを実証する。故障の検知方法については、機体の傾き角や、各モーターの異常な指令値のばらつきなど、各機体の設計に依存するため、それらの故障検知方法が合理的であることの説明が必要である。また、操縦者が飛行中断を発動させる場合には、故障状態の伝達方法についても実証が必要である。一方、それらの検知方法が通常運用で誤動作しないことは「セクション 300」で立証されるため、ここでは実証の必要はない。

試験が必要なクリティカルフェーズ(危険な状態)は 4.4(2)項を参照のこと。ただし、地上試験の為実測により落下分散を実証するわけではないこと、制御された飛行状態を維持できなくても良いことなどから限定された状況でのみ試験をおこなえば良い可能性がある。

具体的な工程は以下の通り

	目 的	方 法
1	推進器停止機能の装着	必要に応じ、飛行中に 1 つの推進システムを停止できるシステムを追加する。実証方法の具体的な例はケース a)と同様であるが、地上試験が前提となるため、直接スイッチ操作などにより動作するものも考慮される。
2	故障検知の実証	設定した故障検知方法により故障検知できるかを実証する。地上からの指示により飛行中断措置をおこなう場合は、地上局の表示により操縦者が故障を認識できることも併せて実証する。 例 1:機体の傾きにより検知する場合 地上で機体の傾きを再現し、所定の閾値で故障が検知されることを確認する。また、推進器の一故障に対して生じるケースを閾値の設定が包含していること、ないし閾値を超えない範囲では危険な状況が起こり得ないことを説明し、必要に応じてシミュレーションなどで立証する。 例 2:モーター回転数の変動により検知する場合 地上で実施する場合は、機体が姿勢制御を自律でき、ホバリング状態を継続できる装置上で、1 つの推進システムを停止させ、モーター回転数がアンバランスな状態を作り出し、故障検知動作を確認する。 モーター回転数のアンバランス状態はソフトウェア的に作り出すことも可能であるが、実際の飛行状態と同等であることを説明する必要がある。 例 3:ESC からのステイタス情報などにより検知する場合 地上で飛行を模擬して推進器を運転し、推進器停止機能を用いて 1 つの推進器を停止させて、故障が検知されることを確認する。
3	飛行中断措置の実証	地上からの指示により飛行中断措置をおこなう場合は、地上局の指示により操縦者が飛行中断措置を実施できたこと(全推進器の停止、パラシュートの放出など)を実証する。 フライトコントローラが自動的に飛行中断措置をおこなう場合は、前項の検知の実証と同時に同様の実証をおこなう。
4	墜落範囲の検証	故障検知後、飛行中断措置を実施した場合の落下分散、部品などの飛散範囲を解析により算出し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを確認する。

＜結果判定＞

Pass/fail criteria については 4.3 項で解説した通りであるが、原則としてはいずれのケースにおいても「制御された非常着陸又は管理された墜落」に至ると考えられることから最終的に想定飛行範囲内に着陸／落着することを示せば良いと考えられる。ただし、ケース b)のように実際に落下させて落下分散を実証するわけではない場合は、別途実験、または解析により落下分散、部品などの飛散範囲を示し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを示す必要がある。落下分散の解析に当たっては一般的な高度と初速度から計算すればよいが、空気抵抗の影響は考慮する必要がある。機体の抵抗係数などを正確に導出することが困難である場合は、無視ないし概算値を取ることも想定されるが、結果が安全側(基本的には落下分散が拡大する側)となるように仮定を置くよう注意すること。

ケース a)のように飛行状態での実証を行う場合も、飛行エリア外縁でちょうど故障を起こすことが難しいこと、気象条件についても最も厳しい条件を再現することが困難であることなどを考えると、実際に飛行エリア外縁で故障を模擬して想定飛行範囲から逸脱しないことを示すという形ではなく、故障

発生個所から着陸点までの偏差を実測し、外部風の影響などを解析的に補足することで、最大の偏差を推定し、飛行規程に記載されたマージンなどを設定することで想定飛行範囲からの逸脱が発生しないことを示すことが現実的であると考えられる。

「セクション 305」の pass/fail criteria にあっては 4.3 項で述べたように操縦者の意図や、設計上考慮されていることなどが重要であるため、CONOPS や飛行規程で説明されている通りに安全性が確保されている必要があり、例えば自動着陸により安全を確保する筈がそのまま墜落してしまい、しかし結果的に想定飛行範囲からは逸脱しなかったという結果が出た場合に、それが「安全基準」を満たしていると見做されることは難しい。申請者は事前に検査者とよく協議し、CONOPS や飛行規程との整合も含めて合意された pass/fail criteria を確立しておく必要がある。

＜注意すべき事項＞

- 推進器停止機能の実装にあたって、フライトコントローラのソフトウェアにより、1 つの推進器への信号を 0（またはその他停止を意図する値）に設定する場合、原則としてはソフトウェアの出力端で値を変更することにより、値が 0 であることがソフトウェア内で認識・利用されないように、また値がソフトウェア内のリミッタなどにより変更されたり、フィルタなどにより変更過程が平滑化されたりしないよう注意するとともに、検査者から求められた場合はそれを立証する必要がある。
- また、フライトコントローラから ESC への信号線を遮断する場合も、ESC で前値保持などの設定により回転数が 0 にならない可能性があり、必要に応じて設定変更するなどの対応が必要になることに注意すべきである。
- 飛行試験で実施する場合の飛行高度についてはクリティカルな状況を包含できるように注意する必要がある。例えば単純な落下分散であれば高度が高くなるほど広くなるが、制御された着陸をおこなう場合、故障発生時に一度水平面の位置が変動した後で降下しながら修正するような動きをする場合もあり、発生高度が低いほうがクリティカルになるようなケースもありえる。
- マルチコプターは一般に軸対象に推進器を配置しているが、巡航中などは推進器によって出力が異なるため停止した場合の影響も異なる。また、外部風の風向、重心位置（最も不利な重心位置を設定する場合、推力中心から水平面内で推力中心から偏差した場所に重心が設定される可能性は高い）などによっても、推進器によって停止した場合の影響は異なると考えられる。特に飛行中に 1 推進器を停止させる場合、これらの要素を総合的に勘案し、最も悪影響の大きい推進器を停止させる必要がある。
- 固定翼型（ないし VTOL 型の固定翼モード）においては、滑空する能力を有することから推進システムが故障しても直ちに墜落しない可能性が高く、結果的に想定範囲外に容易に逸脱することが想定される。そのため、マルチコプター以上に、機体の故障状態の伝達、飛行中断の確実性などについて、十分な検討が必要である。

(2)　C2 リンクの品質低下(可用性の低下、サービス品質の悪化、信号雑音比(Signal-Noise Ratio: S/N)の低下、断続接続及び遅延など)を実証する。この試験は厳しい飛行フェーズ、モードで行う。

(3)　C2 リンクが完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う。

[引用:航空局ガイドライン／セクション 305 MoC]

DRAFT2 にて追記予定

(4)　GNSS の品質低下を実証する。この試験は厳しい飛行フェーズ、モードで行う。

(5)　GNSS が完全に喪失し、復旧しない状態を実証する。この試験は厳しい飛行フェーズ、モードで行う。

[引用:航空局ガイドライン／セクション 305 MoC]

DRAFT2 にて追記予定

(8)　連機器に応じた故障状態を実証する。

[引用:航空局ガイドライン／セクション 305 MoC]

DRAFT2 にて追記予定

Appendix 2 各セクション特有の用語集

用 語	意 味	備 考
ESC		
GNSS		
制御された飛行状態		
飛行中断		
非常着陸		
フェイラーモード		
フライトコントローラ		

DRAFT2 にて加筆予定

Appendix 3 関連文書

(1) FAA Advisory Circular No.23 .1309-lE: SYSTEM SAFETY ANALYSIS AND ASSESSMENT FOR PART 23 AIRPLANES
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_23_1309-1E.pdf

(2) FAA Advisory Circular No.25 .1309-lA: SYSTEM DESIGN AND ANALYSIS
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_25.1309-1A.pdf

(3) JARUS AMC RPAS 1309-01
http://jarus-rpas.org/wp-content/uploads/2023/07/jar_04_doc_amc_rpas_1309_issue_2_2.pdf

(4) EAUROCAE ER-010 - UAS / RPAS Airworthiness Certification - "1309" System Safety Objectives and Assessment Criteria

(5) IEC61508-1 (JIS C0508-1) - Functional safety of electrical / electronic / programmable electronic safety-related systems

(6) 無人航空機の型式認証等の取得のためのガイドライン安全基準セクション 135 重要な部品(フライトエッセンシャルパーツ) 解説書(RMD-135、Rev.01)

(7) 無人航空機の型式認証等の取得のためのガイドライン解説書(RMD、Rev.01)2.2.1 安全基準の各セクションにおける「安全」等の用語の解釈

(8) JIS W 0711 無人航空機システム設計管理基準

Appendix 4　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG セクション 305 起こり得る故障の構成員名簿（サブ WG 主査およびライター）を以下に示す。なお、レビュワーの講成員名簿は本冊（RMD、Rev.01）Appendix3 を参照すること。

役割	氏名	所属
主査	河野　敬	国立研究開発法人 宇宙航空研究開発機構
ライター	下地広泰	大分県産業科学技術センター
ライター	三輪 昌史	国立大学法人徳島大学
ライター	三好 崇生	サイバネット MBSE 株式会社
ライター	幸 嘉平太	大分県産業科学技術センター

無人航空機の型式認証等の取得のためのガイドライン解説書

2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

518

RMD-CP DRAFT Rev.01

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

型式認証プロセス 適合性証明計画（CP） 解説書

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

表 目次

1　目的

本解説書は「無人航空機の型式認証等の取得のためのガイドライン」（以降、「航空局ガイドライン」と呼ぶ）型式認証プロセス　適合性証明計画（CP）に対する解説書である。

2　対象の基準「サーキュラー」（引用）

「サーキュラーNo.8-002”無人航空機の型式認証等の手続き”（以降、「サーキュラーNo.8-002」と呼ぶ）」の「適合性証明計画」、「適合性検査表」を以下に引用する。

> *1）適合性証明計画*
>
> *型式認証等に係る申請者は、全ての適用基準の項目について設計図面、解析・評価、飛行試験等の選択を含む適合を示す方法（一例として、サーキュラーNo.8-001 の検査要領における 110 ソフトウェアは“解析・評価”により、200 無人航空機飛行規程は“設計図面”により、300 耐久性及び信頼性は“飛行試験”により、それぞれ適合性証明を行う等）、実施時期等を記載する適合性証明計画を作成し、検査者の合意を得ること。検査者は、原則として当該計画に合意した後、検査を開始するものとする。また、当該計画はプロジェクトの進行に伴い変更されることがあるため、一旦、合意を得た計画を変更する場合にあっても、検査者の合意を得ること。*
>
> *2）適合性検査表*
>
> *適合性検査表は、適用基準の項目ごとに証明状況を示すものである。*
>
> *検査者は、申請者が作成した適合性証明計画に基づく適用基準への適合性の状況を本適合性検査表により管理する。*

3　「航空局ガイドライン」（引用）

「航空局ガイドライン」 型式認証プロセス　適合性証明計画を以下に引用する。

> *6.　適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *適合性証明計画は、申請者により検査要領に記載される全ての適用基準等（安全基準や均一性基準　及び　特別要件の設定や同等の安全性、適用除外を設定した場合はその内容も含む。）の項目について、試験で証明を行うか、解析で証明を行うか等の計画を示した文書となります。申請者は適合性証明計画（案）及び必要書類を作成し、検査者から合意を得た後に、検査を開始します。適合性証明計画は、申請者の計画が示された文書となりますので、以降の設計の検査の過程で計画の見直しが発生する可能性もあります。計画の見直しが発生した場合、申請者は当該計画を変更し、再度検査者より合意を得る必要があります。以下に申請者が作成する資料を記載しますが、提出書類はこれに限るものではございません。*

【適合性証明計画(案)】

① 適用基準等に関する事項(特別要件等に関する事項を含む。)

適用を想定する適用基準等及びそれらに規定された全ての要件について、適合性証明の必要性の有無、解析又は実証の選択を含む適合を示す方法、実施時期等を記載します。

本ガイドライン第 3 部の証明文書一覧及び第 4 部の均一性基準に、6-4 項に記載の適合性検査表と紐付けてまとめると理解が深まります。なお、適用基準に特別要件等がある場合は、当該内容についても 6-4 項に含めること。

② 型式認証等に関連する人員に関する事項

型式認証等に関連する人員について、それぞれの責任及び権限を明確にします。

【必要書類】

③ 基本設計又は型式認証の変更の概要に関する事項

機体仕様又は型式認証の変更の概要について把握できる書類を作成します。この時点で確定している CONOPS を提出することも可能です。

④ 設計及び製造に関する日程の概略

申請者が希望する申請書の提出から型式認証の取得までの日程の概略に係る情報を記載します。日程は下記に示す添付 1 のとおり、四半期単位など大まかなもので構いません。なお、適合性証明計画の改訂の頻度等を勘案し、別途スケジュールの管理が可能な資料が存在する場合は当該資料を呼び出すことも可能です。

⑤ その他必要となり得る書類

申請者が従来の無人航空機の設計にはないと考える新設計、新技術、新素材及び新しい製造方法を採用する場合は、その概要並びに検討事項及びその解決方法をまとめてください。また、共同製造者がある場合は、共同製造者の名称、製造分担及び所在地に関する情報を記載し、設計又は製造の一部を外部に委託する場合は、当該委託先(外注先)の名称、委託内容及び所在地に関する情報を記載してください。

上記①～⑤に係る事項は 1 つの文書にまとめて検査者から承認を得ることが望ましいです。

なお、第二種型式認証を受けようとする型式の無人航空機であって最大離陸重量が 25kg 未満のものについては、①～⑤のうち全てではなく、最低限①適用基準等に関する事項(特別要件等に関する事項を含む。)及び④設計及び製造に関する日程の概略を把握してください。

6-2. 議事録

適合性証明計画の説明及び調整を行った際は、その説明内容、指摘及びその改善事項、調査事項、問題点等を明確にし、認識を共有する目的から、申請者において議事録を作成し、双方で記載の内容を確認します。議事録には特に定まった様式ありませんが、サーキュラーNo.8-002 の別添 3(JCAB FORM 8-002-3)の様式を使用することも可能です。

6-3. 参考資料

6-1 項及び 6-2 項に対する参考資料は以下のとおりです。

サーキュラーNo.1-307「適合性証明計画の作成について」

6-4. 適合性検査表について

適合性検査表には、少なくとも以下を含み、適用基準等の項目ごとに証明状況を示すためにも重要となります。

① :適用基準等に掲げられた全要件に対し、最小単位毎に項目番号を記載すること。

ただし、②以降の内容が同じであればその上位の単位を記入することにより集約しても構いません。

② :①の項目番号に対応した項目名を記載すること。

③ :証明が必要な場合は「適」と記載し、未装備等の理由で証明が不要な場合は「否」と記載すること。

④ :③にて「適」と判断した場合、図面、解析又は試験等の証明方法を記載すること。
(本ガイドライン第 3 部で記載される MOC 番号を記載することも可能です)

⑤ 、⑥:④にて提案した証明方法に従って作成した文書又は図面番号及びそれらの名称を記載すること。

⑦ :⑤、⑥の文書の訂符番号を記載すること。

⑧ :③にて「適」と判断した場合はその証明概要を記入し、「否」と判断した場合はその理由を記載すること。

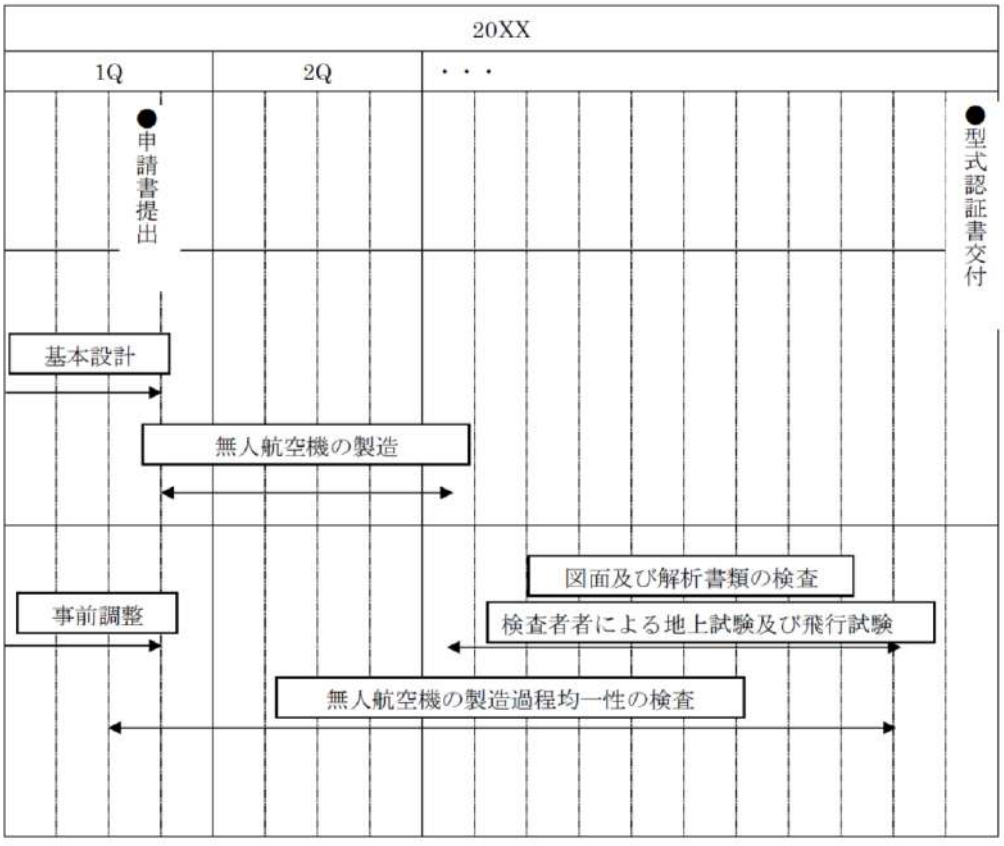
⑨ :検査者が立ち会うのか、申請者検査のみとするのかをここで明確にします。検査者は特に重要な試験項目に立ち会うことを想定していますので、全ての試験に立ち会う必要はございません。どの試験に立ち会うべきか判断に迷った場合は、本ガイドライン第 3 部の各セクションに記載のある検査者の関与度(LOI)等を参考に立ち会う試験を決めることができます。

また、第 4 部の均一性基準に係る事項についても同様に適合性の計画を示してください。

適用基準	項目名	適否	MOC	適合性証明文書			備考	立会担当
			方法	文書番号	文書名称	訂符		
①	②	③	④	⑤	⑥	⑦	⑧	⑨
<記載例>								
～(前略)～								
140-3	自動操縦系統、カメラ等	適	1,7	ABC123	自動操縦・カメラ等の設計概要書	NC	自動操縦システムを装備し、機体装備カメラ等により機外を監視できるこ	-
			6	DEF123	自動操縦・カメラ	A		申請者

					等実証飛行試験方案		とを図面及び実物で確認する。また、自動操縦システムやカメラが適切に動作することを飛行試験で確認する。	検査
			6	DEF456	自動操縦・カメラ等実証飛行試験報告書	A		-
140-4	危険物輸送	否	-	-	-	-	危険物輸送を実施しないため、本項は非該当。	-
～(中略)～								
均一性基準	製造管理要領	適	-	XYX123	○○型無人航空機製造管理要領	B	当該型式の均一性が確保されることを証する書類として、製造管理要領を作成する。	検査者による確認

添付 1



83
84

4　解説書

4.1 項以降では、2 項「サーキュラーNo.8-002」および 3 項「航空局ガイドライン」の内容について解説を加える。各項にて解説を加える「サーキュラーNo.8-002」および「航空局ガイドライン」の引用箇所に関して、太字下線で示すものとする。

4.1 適合性証明計画の目的

> *1)　適合性証明計画*
> *型式認証等に係る申請者は、全ての適用基準の項目について設計図面、解析・評価、飛行試験等の選択を含む適合を示す方法(後略)*
> *[引用:サーキュラーNo.8-002]*

> *6.　適合性証明計画*
> *6-1. 適合性証明計画について*
> *適合性証明計画は、申請者により検査要領に記載される全ての適用基準等(安全基準や均一性基準 及び(後略)*
> *[引用:航空局ガイドライン]*

本項では、適合性証明計画の目的、型式認証プロセスにおける位置づけなどについて解説する。

「航空局ガイドライン」の第 2 部図 1 に示されている型式認証取得までの全体的なフローを図 4.1-1 に引用する。適合性証明計画は設計および製造過程に関する検査などに着手するにあたり、適合性の判定基準となる適用基準や基準に対する証明計画を示すものであり、その内容について検査者と合意すること(適合性証明計画の合意)は型式認証プロセスを進める際の重要なマイルストーンとなる。

適合性証明計画の目的に関する理解を深めるために、「航空局ガイドライン」第 2 部の図 2「初回審査会～適合性証明計画の合意まで」および図 3「適合性証明計画の合意～RFC/W の発行まで」を参考に、適合性証明計画作成および適合性証明計画審査の前後の活動や各活動のインプット・アウトプットとなる文書を記載したフローを図 4.1-2 に示す。

適合性証明計画の作成においては、はじめに適用基準を明確にする必要がある。適用基準に関する詳細な説明は 4.2 項で述べるが、CONOPS を前提として「適用基準」「特別要件」「適用除外」「同等の安全性」に関する考え方を整理して適合性証明計画を作成することになる。最終的には「当該適用基準の合意」をもって適合性証明計画が作成されることになるが、その内容が今後の型式認証プロセスに大きな影響を与えることから、CONOPS の作成と同様に型式認証プロセスの初期段階から適合性証明計画の作成に着手し、事前調整などの場を活用して検査者との意見交換を実施しておくことを推奨する。なお、「航空局ガイドライン」(図 4.1-1 に引用)において、「適用基準等の考慮」「適用基準等の設定」が検査者(航空局または登録検査機関)の区分に記載されているが、あくまでもこれらの議論の土台となる部分(適用基準の案など)は申請者側が検討し準備するものである。

作成した適合性証明計画は、適合性証明計画審査の場で検査者によって審査され、その議事録をもって適合性証明計画の合意に至る。適合性証明計画の合意が得られた後は、申請者は適合性証明計画に基づいて設計データ（図面や解析書など）や試験方案などを作成し、検査者による適合検査を受ける流れとなる。一方で、検査者側も適合性証明計画に基づいて適合検査の実施計画を立てるものと考えられるため、検査者が検査の計画を立てるために必要な情報を適合性証明計画に盛り込んでおくことが重要である。

以上から、適合性証明計画の目的は以下のとおり整理できる。

- 「サーキュラーNo.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領の安全基準（以降、「安全基準」と呼ぶ）」などへの適合性を判定するための審査に先立って、適用するすべての適用基準、証明方法および実施時期などを計画する
- これによって、申請者における型式設計ならびに検査者における一連の審査および検査業務の円滑かつ効率的な実施を可能とする

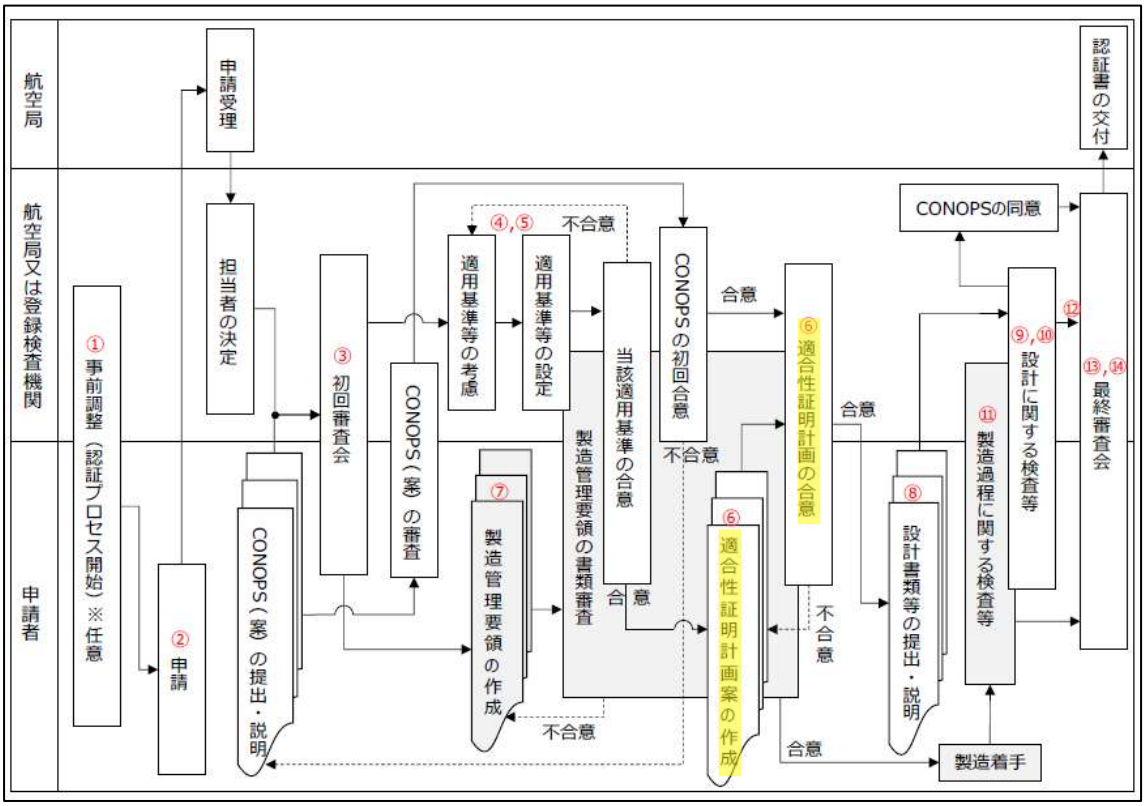
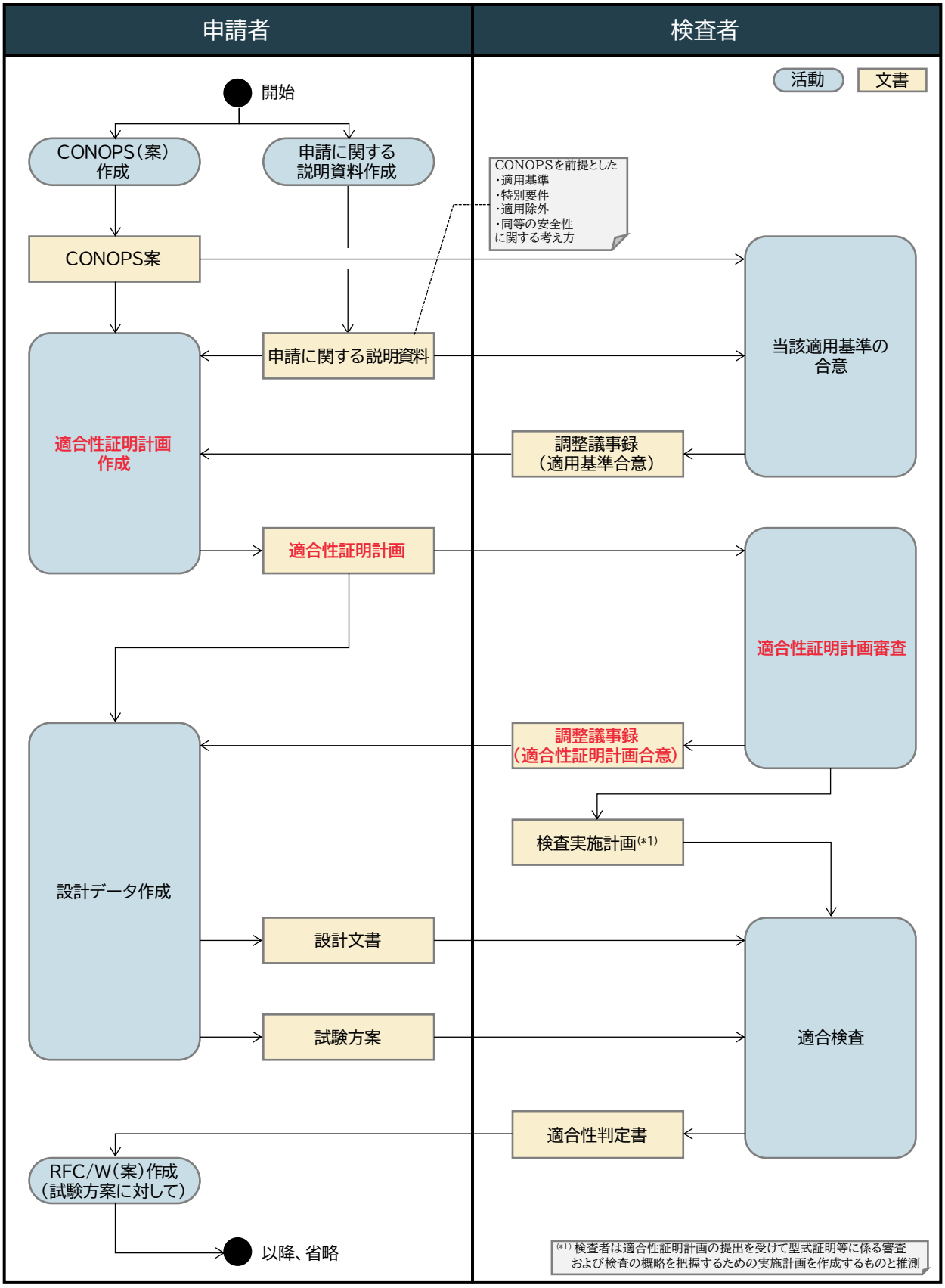


図 4.1-1 型式認証取得までの全体的なフロー

出所）航空局ガイドライン

127



128 図 4.1-2 適合性証明計画に着目したフロー

129

4.2 適用基準等について

> *1)　適合性証明計画*
> *型式認証等に係る申請者は、全ての適用基準の項目について設計図面、解析・評価、飛行試験等の選択を含む適合を示す方法(後略)*
> *[引用:サーキュラーNo.8-002]*

> *6.　適合性証明計画*
> *6-1. 適合性証明計画について*
> *適合性証明計画は、申請者により検査要領に記載される全ての適用基準等(安全基準や均一性基準 及び特別要件の設定や同等の安全性、適用除外を設定した場合はその内容も含む。)の項目について、試験で証明を行うか(後略)*
> *[引用:航空局ガイドライン]*

本項では、適用基準について解説する。

(1) 適用基準に関係する法令の概要

航空法に限らず、法令は上位の規定を下位の規定に再掲しない。下位の規定はあくまでも上位の規定の詳細化、具体化をするものである。

型式認証に関係する法令は、上位側から航空法、航空法施行規則、サーキュラー、通達である。(航空法施行令もあるが、無人航空機に関連する規定は本解説書の執筆時点ではない)

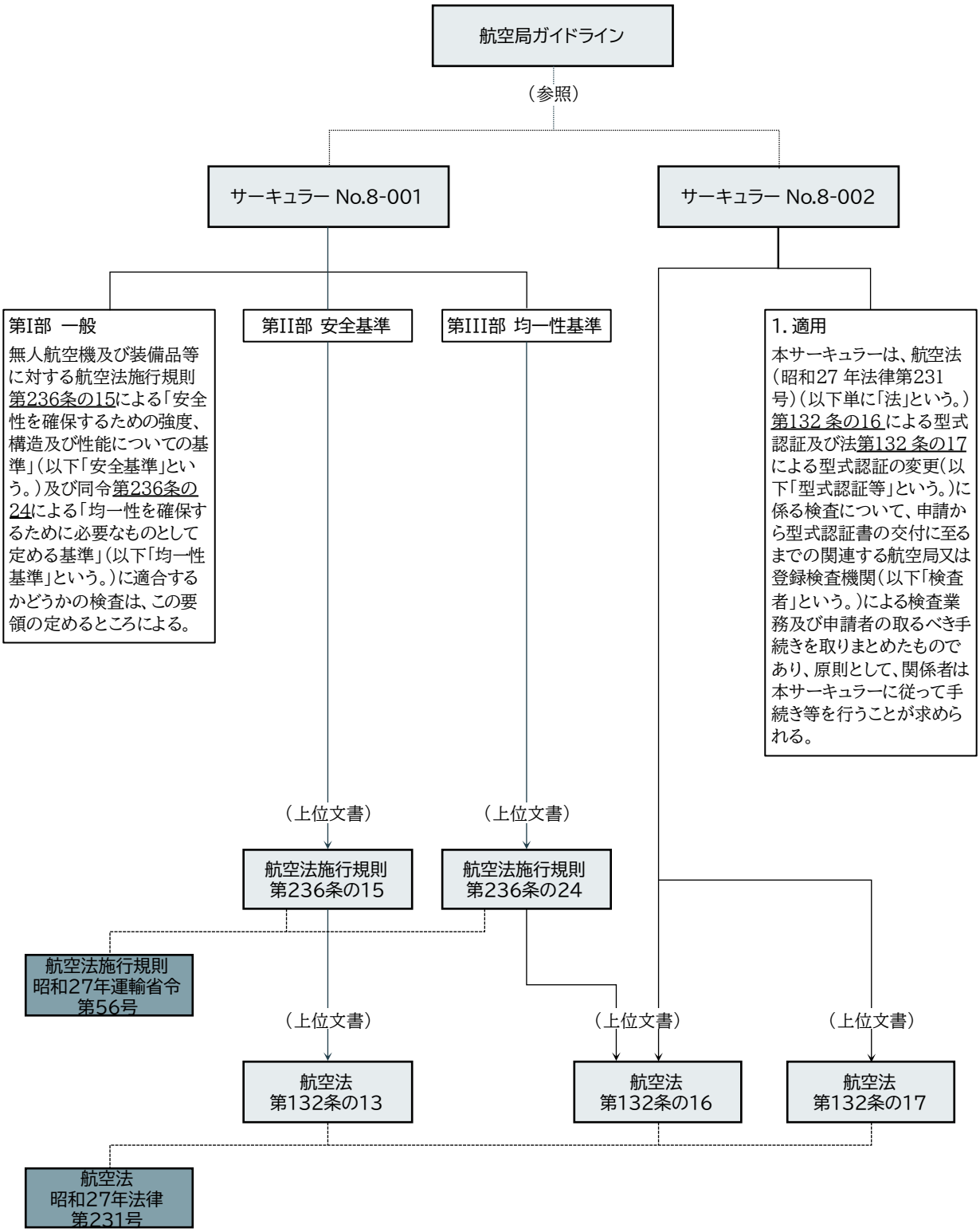
なお、「安全基準」や均一性基準を定めているサーキュラーは通達の内で航空機、装備品などの「安全基準」、環境基準およびこれらに関係すると認められるものについて取り纏められたものである。

「航空局ガイドライン」は法令ではないため、あくまでも解説である。あくまでも参考とするものであり、現時点で法令として確定させにくい解釈などについても意図やイメージを伝えやすいツールとしての位置づけである。

そのため、「航空局ガイドライン」は読みやすく使いやすいが、正しい情報はサーキュラー以上の法令であり、正式な根拠として使用することができないことに注意する必要がある。

次に、無人航空機の適用基準の全体像を確認する。ここで、適用基準の検討を行う際には、航空法を出発点として航空法施行規則、サーキュラーと下位を確認していくべきだが、法令に馴染みがない方にとってはイメージがつきにくい。具体的に基準を解説している文書から始めた方が、イメージがつかみやすく、本解説の対象である「航空局ガイドライン」を出発点として、「安全基準」と均一性基準、型式認証プロセスから航空法までの関係性を図 4.2-1 に示す。

153



154 図 4.2-1 適用基準を定める航空法および航空法施行規則

155

（2） 適用基準検討で留意するべきこと

適用基準は申請対象となる型式の機体および運用に対して漏れなく、妥当な内容を設定する必要がある。上記の法令の構造上、適用基準を検討する場合に 2 点、確認することを推奨する。

第一に、「安全基準」や均一性基準のような具体的な基準だけでなく、その根拠となっている航空法に遡り適用の妥当性を確認することである。上記の通り下位であるサーキュラーには記載されていない文言が航空法および航空法施行規則には記載されており、申請対象に関係しないことも含めて検査者に説明が必要である。

第二に各種通達の確認を行うことで、規定で用いられている各種概念（例えば「第三者」、「立入管理措置」など）を確認することである。法令の用語は慣用的に用いられている用語と意味が異なる場合があり、特に通達などで定義されている用語については定義された意味で用いる必要があるからである。

通達などで定義されていない用語については、事前調整もしくは検査時に検査者に質問することも可能であるが、プロジェクト毎に総合的に判断して運用されるようなものであれば、申請対象となる型式の機体および運用に則して申請者側から定義について提案することが議論を円滑に進めるために有効であろう。

（3） 適用基準に関係する用語

図 4.1-1 のフローで適用基準に関して「適用基準等」「当該適用基準」という言葉が使われている。法令用語の読み方として、「等」の有無は意図的であるため、「適用基準等」というのは「適用基準」に何らかそれ以外のものが意識されている。

適用基準は原則として、「サーキュラーNo.8-001」に規定されている「安全基準」および均一性基準に対して、特別要件、適用除外、同等の安全性を考慮して設定することになる。これらは適合性見解書（以降、「見解書」と呼ぶ）にて明確にされる。そのため「安全基準」および均一性基準と各種内容に関する見解書により、適用基準が設定される。見解書は適用基準に対して特別要件、適用除外、同等の安全性の設定に関するものの他、その他必要と認められる場合についても発行される。

以上の適用基準の構造を考えると、「適用基準等」が示すものは、「安全基準」および均一性基準に見解書を加えたもの、その結果として明確になった適用基準が「当該適用基準」と解釈することができる。これらの各用語の関係性を整理したイメージ図を図 4.2-2 に示す。

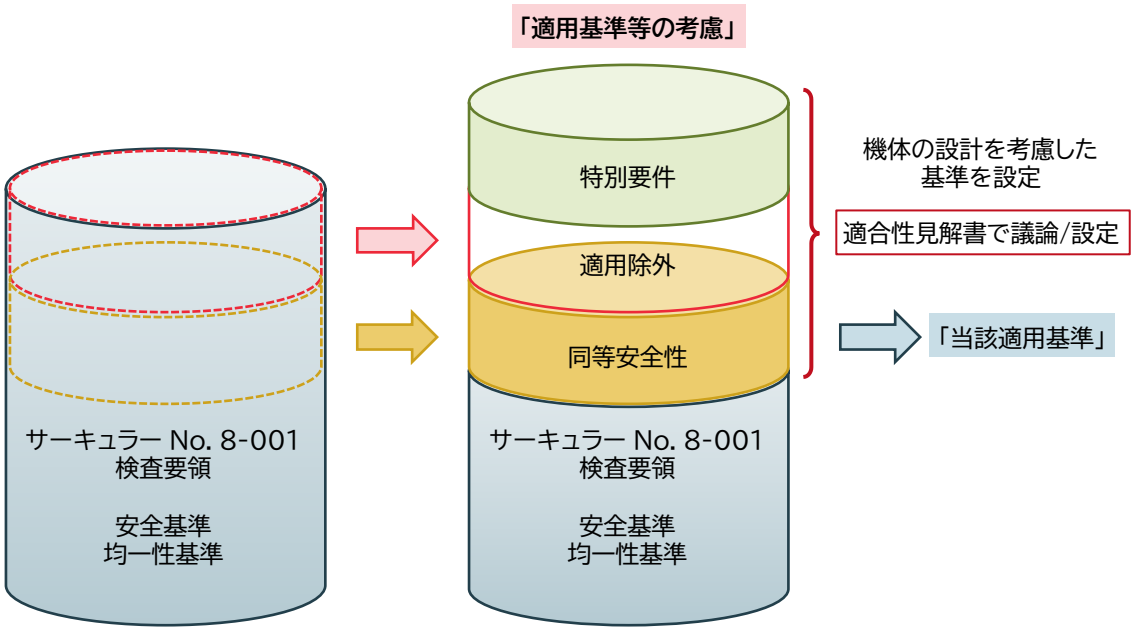


図 4.2-2 適用基準に関連する用語・関係性の整理

出所）AeroVXR 合同会社 HP（https://aerovxr.co.jp/tech.library/698/）を引用し加筆

（4） 当該適用基準の設定に際に考慮する事項のまとめ

「航空局ガイドライン」 第 3 部 「安全基準」（3/71）および（4/71）に、以下の 4 項目に該当しない項目がある場合は、特別要件などの要否について検査者と追加の調整が必要になるとある。

- 無人航空機が C2 リンクを有し、操縦者が緊急時の対応を取ることができるもの
- 着氷気象状態での運用を行わないもの
- 操縦者と無人航空機の数の比率が 1:20 以下のもの
- 電動推進の無人航空機であること（内燃機関または燃料電池を除く）

また、同じく「航空局ガイドライン」 第 3 部 「安全基準」（3/71）および（4/71）に適合性見解書が必要となる可能性のある技術要素リストが示されている。

当該適用基準を設定する際には、表 4.2-1 に示すとおり、図 4.2-2 に示す適用基準などに上記を加えた内容を考慮することで全体を整理することができる。

適用基準の記載には、その引用基準、適用の可否、否の場合の理由についてそれぞれ記載が必要である。その表示一例を Appendix 1 適合性証明計画のサンプルに示す。

表 4.2-1 当該適用基準の設定に際し考慮する事項

No.	区分	内容	備考
1	適用基準 （サーキュラーNo. 8-001 検査要領）	申請する機体および運用に対して適用される基準	
2	特別要件などの要否について追加の調整が必要となる仕様	「航空局ガイドライン」第 3 部「安全基準」について（3/71）に示されている仕様への該当/非該当の整理	
3	適合性見解書が必要となる可能性のある技術要素リスト	「航空局ガイドライン」第 3 部「安全基準」について（3/71）に示されている適合性見解書候補リストへの該当/非該当の整理	
4	新技術	No.3 の技術要素リストに含まれず、適合性見解書を要する可能性のある技術要素を整理	
5	適用外となる項目	No.1 の適用基準に対して、適用外となる項目の整理	
6	特別要件	特別要件を必要とする項目を整理	
7	同等の安全性	同等の安全性を適用する項目を整理	
8	適用除外	適用除外とする項目を整理	

4.3 適合性証明方法について

> *1)　適合性証明計画*
>
> *型式認証等に係る申請者は、全ての適用基準の項目について設計図面、解析・評価、飛行試験等の選択を含む適合を示す方法（一例として、サーキュラーNo.8-001 の検査要領における 110 ソフトウェアは“解析・評価”により、200 無人航空機飛行規程は“設計図面”により、300 耐久性及び信頼性は“飛行試験”により、それぞれ適合性証明を行う等）、実施時期等を記載する適合性証明計画を作成し、（後略）*
>
> *［引用：サーキュラーNo.8-002］*

> *6.　適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *適合性証明計画は、申請者により検査要領に記載される全ての適用基準等（安全基準や均一性基準 及び 特別要件の設定や同等の安全性、適用除外を設定した場合はその内容も含む。）の項目について、試験で証明を行うか、解析で証明を行うか等の計画を示した文書となります。（後略）*
>
> *［引用：航空局ガイドライン］*

本項では、適合性証明手法について解説する。

(1) 用語

適合性証明方法は英語で Means of Compliance という表現され、“MoC”もしくは“MOC”という略語がよく用いられる。「航空局ガイドライン」で以下のとおり例示されているように、MOC に ID を振り、例えば、安全基準に対して解析で適合していることを示したい場合には、“MOC は解析”“MOC は 2”などというコミュニケーションをすることが多い。

0: 他の適合性証明結果を活用 / Compliance Statement
1: 設計図面 / Design/Data Review
2: 解析・評価 / Calculation/Analysis
3: 安全性評価 / Safety Assessment
4: 実験室試験 / Laboratory Test（※MoC 5、6 および 9 に該当しない試験）
5: 試験機による地上試験 / Ground Test on UA
6: 飛行試験 / Flight Test
7: 実物検査 / Physical Inspection
8: シミュレーション試験 / Simulation
9: 装備品の検証 / Equipment Qualification

「航空局ガイドライン」に例示されている ID は何かに規定されたものではなく、申請者として設定することは自由である。しかし、検査者も同様に「航空局ガイドライン」を参照することが多いと考えられるこ

とから、申請者はIDの意味することの誤解を与えないように「航空局ガイドライン」に例示されたIDを準用することを推奨する。

（2） 適合性証明方法の検討で留意すること

適合性証明は、その言葉が示す通り「安全基準」および均一性基準の各基準への適合性を明確に示すことを意味している。ここで、申請者にとって第三者の立場で検査者が明確に判断できることが重要である一方で、基準が一定程度の機体や運用の多様性の中で運用されることを想定しているために抽象度が高い。また、妥当な証明方法であることが重要であるのに対して、高度な技術であるほど証明には有効だ、というような誤解が生じやすいため注意が必要である。

そのため、適合性証明方法を検討する際には、まず適合性証明の対象となる要求の具体化を行い、基準の意味を機体や運用の文脈に沿って詳細化をする。ここで機体や運用で何かしら特殊な条件を有する場合ほど、基準が意図している背景や前提（想定している場面やリスク）を検査者とよく議論をすることが重要である。基準はそのクライテリアを明示するべきものであるが、現状の基準は必ずしもすべてを明確に記載していない。そのため、特にプロジェクトに大きな影響を与えるもの（機体の大規模な設計変更、試験期間の大幅な変更などに繋がる内容）は事前調整などの段階で明確にしておくことが必要である。

次に、その具体化／詳細化された要求に対して妥当な証明方法を検討する。ここで、数点注意が必要である。

① 所謂エンジニアリングジャッジが入らないように注意する

一般的に機体開発プロジェクトでは、限られた期間と人的リソースで活動を推進する必要があり、経験則に基づく技術的な判断（“エンジニアリングジャッジ“と呼ぶ）が多く用いられる。エンジニアリングジャッジは端的に結論を出すという特徴から、開発の現場で良い意味で捉えられることがあるが、適合性証明においては、逆に網羅性や客観性が乏しく検査者にとって受入れられないことが多いことに注意する。過去の実績を使うのであれば定性、定量的な実績についての分析、公知となっている研究成果などを使うのであれば引用と適用の妥当性、特定のケースに絞って示すのであれば全体としてどういうケースがあり得、当該ケースで他の多くのケースが含有し得るなど、丁寧に説明する必要がある。

② 高度な解析は必ずしも適合性証明に適さない

しばしば起こる誤解として、必要以上に高精度な解析によって適合性を示そうという考えであり、高精度な解析ほどそこで扱う多くの情報や精度に対しての説明、技術的な背景や過去の実績、解析手法の妥当な運用などについての説明が必要となる。例えば、構造に関する証明を行う際に高精度の非線形応力解析をFEMで実施しようとする場合に、各種物性値やメッシュサイズ、モデリングの考え方、数値解析誤差についての考え方など多くの説明が必要になる場合がある。それよりも、支持条件が単純である場合には初歩的な材料力学を用いた計算方法で示した方が、合理的になる場合がある。特に研究で使われているような手法を適用する場合は、慣例的、または実際の現象と合わせるために調整されるパラメーターがある場合もあり、注意を要する。

③ 安全仮定

上記の通り、高精度で複雑な証明方法よりも、明らかに安全側であり、単純な証明方法のほう

が合理的である場合が多く、安全仮定を多く採用することを推奨する。

④　目的は基準への適合性

「安全基準」や均一性基準自体が一定水準の安全性を確保するための基準であるためにしばしば誤解を生みやすいが、それぞれの適用基準に対して適合性を示した結果として、基準が意図している安全性を確保することに繋がる。逆に、個別のトピックに対して安全性を示すことは基準への適合性を示すことに必ずしも直結しない。そのため、繰り返しになるが、各基準への適合性を示せることが重要であり、安全であるということだけを主張することは、安全性の確保という点では間違いではないが、適合性証明という点では必ずしも正しくないことに注意が必要である。

（3） ソフトウェア・サイバーセキュリティの適合性証明計画

「航空局ガイドライン」によれば、「セクション 110 ソフトウェア（以降、「セクション 110」と呼ぶ）」および「セクション 115 サイバーセキュリティ（以降、「セクション 115」と呼ぶ）」に関する基準への適合性証明方法（MoC）として、「ソフトウェア適合性証明計画」および「セキュリティ適合性証明計画」の作成が例示されている。これは、本解説で対象としている適合性証明計画と、「航空局ガイドライン」で想定されているソフトウェアおよびサイバーセキュリティに関する適合性証明計画の位置付けが異なる点に注意が必要である。

前者は、すべての適用基準の項目について設計図面、解析・評価、飛行試験などの選択を含む適合を示す方法、実施時期などを検査者と合意を得るために作成する文書であり、後者は、ソフトウェアおよびサイバーセキュリティの「安全基準」に対する適合性だけではなく、適合性証明活動（安全な運用に悪影響を与えるソフトウェアの抽出、システムレベル要求の確認方法、形態管理および PR システムの管理体制、セキュリティリスクの特定および評価、緩和策の提示など）のプロセスの妥当性に重きが置かれており、結果を実施報告書で示す点である。これは、想定されるリスクが試験や解析などのみだけでは証明が難しい「安全基準」に対して、「なぜ」あるいは「どのように」その対象を抽出したのかといった前提条件およびプロセスを明確にすることで、申請者が管理対象外としたリスクファクターに関する説明の妥当性を主張する上で重要である。

以上は「航空局ガイドライン」で想定されている「セクション 110」および「セクション 115」に関する適合性証明計画を解説したものであるが、他の「安全基準」についても、適合性証明方法を決定するためのプロセスが重要であることは変わらない。機体や運用の特徴、また証明方法によっては、適合性証明計画中に適合性証明方法（MoC）の決定プロセスについて、詳述が必要になる。「航空局ガイドライン」の例示もこれら「セクション 110」および「セクション 115」に関する適合性証明計画の内容を全体の適合性証明計画を作成する時点で明確にし、合意対象とすることを否定しているわけではない。そのため、申請者はいつ、何を合意対象とし、証明方法とするのがプロジェクト全体にとって効率的か、総合的に判断するのが良いだろう。

（4） それぞれの適合性証明方法

各適合性証明方法の共通する考え方を示すことで、第二種型式認証であれば適合性検査表に記載する概略程度の記述でほとんどの説明は可能であると考える。以下に限らないが、例として記載をす

る。

0: 他の適合性証明結果を活用 / Compliance Statement

文字通り、他の項目に対して作成した適合性証明文書の内容に含有される場合に適用する。適合性検査表には該当する文書と使用する部分について記載する。

1: 設計図面 / Design/Data Review

設計図面の技術指示内容により基準への適合性を示す場合には、設計図面とする。適合性検査表には、設計図面により確認するキーポイントを記載する。

2: 解析・評価 / Calculation/Analysis

実績のある解析手法や適切な安全側の仮定を元に単純化して設定した手法により解析評価を行い適合性を示す場合には、解析・評価とする。適合性検査表には、具体的に用いるツールや手法(例えば構造解析では手計算や Nastran など)、ツールの場合には実績について補足する。準拠/参照する規格がある場合には、その規格名を記載する。(ASTM Fxxxx など)

3: 安全性評価 / Safety Assessment

安全性解析などによって適合性を示す場合には、安全性評価とする。具体的な手法名(FHA, FTA, FMEA など)と共に、準拠/参照する規格があれば規格名を適合性検査表に記載する。

4: 実験室試験 / Laboratory Test(※MoC 5、6 および 9 に該当しない試験)

システム単体試験のような要素技術試験などで適合性を示す場合は、実験室試験とする。準拠/参照する規格があれば、それも適合性検査表に記載する。

5: 試験機による地上試験 / Ground Test on UA

試験機を用いて構造試験、環境影響試験や故障模擬試験で適合性を示す場合には、試験機による地上試験とする。準拠/参照する規格があれば、それも適合性検査表に記載する。

6: 飛行試験 / Flight Test

実機の飛行試験で適合性を示す場合には、飛行試験とする。準拠/参照する規格があれば、それも適合性検査表に記載する。

7: 実物検査 / Physical Inspection

解析や試験ではなく、実物の検査により適合性を示す場合は、実物検査とする。検査で主に確認するべきポイントとともに、準拠/参照する規格があれば、それも適合性検査表に記載する。

8: シミュレーション試験 / Simulation

解析に類似するが、CAE などを援用して示す場合を特に区別したい場合には、シミュレーショ

ン試験とする。解析と同様に、適合性検査表には、具体的に用いるツールや手法（例えば構造解析では手計算やNastranなど）、ツールの場合には実績について補足する。準拠／参照する規格がある場合には、その規格名を記載する。（ASTM Fxxxx など）

9: 装備品の検証 / Equipment Qualification

実験室試験に類似するが、装備品の機能性や信頼性などを個別に検証する場合を区別する場合には、装備品の検証とする。準拠／参照する規格があれば、それも適合性検査表に記載する。

4.4 適合性証明計画(案)および必要書類の作成

> *1)　適合性証明計画*
>
> *型式認証等に係る申請者は、全ての適用基準の項目について設計図面、解析・評価、飛行試験等の選択を含む適合を示す方法(中略)、実施時期等を記載する適合性証明計画を作成し、検査者の合意を得ること。*
>
> *[引用:サーキュラーNo.8-002]*

> *6.　適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *(中略)申請者は適合性証明計画(案)及び必要書類を作成し、検査者から合意を得た後に、検査を開始します。(中略)以下に申請者が作成する資料を記載しますが、提出書類はこれに限るものではございません。*
>
> *【適合性証明計画(案)】*
>
> *①　適用基準等に関する事項(特別要件等に関する事項を含む。)*
> *(中略)*
>
> *②　型式認証等に関連する人員に関する事項*
> *(中略)*
>
> *【必要書類】*
>
> *③　基本設計又は型式認証の変更の概要に関する事項*
> *(中略)*
>
> *④　設計及び製造に関する日程の概略*
> *(中略)*
>
> *⑤　その他必要となり得る書類*
> *(中略)*
>
> *上記①～⑤に係る事項は 1 つの文書にまとめて検査者から承認を得ることが望ましいです。*
>
> *[引用:航空局ガイドライン]*

本項では、適合性証明計画(案)および必要書類に関する解説として、具体的な適合性証明計画の目次案について検討し例示する。なお、本項に示す目次案はあくまでも一例であり、すべての項目が必須というものではなくプロジェクトごとの判断によるものであることに注意する。

適合性証明計画に記載すべき内容として、適合性証明手法(4.3 項参照)とスケジュールが必須となる。適合性証明手法を明確にするためには、その前に適用基準など(4.2 項参照)を明確にする必要がある。また、適用基準などを明確にするためには、機体の概要や CONOPS 相当の情報を整理しておくとよい。スケジュールについては、適合性証明方法に基づき適合性証明文書を整理することで具体

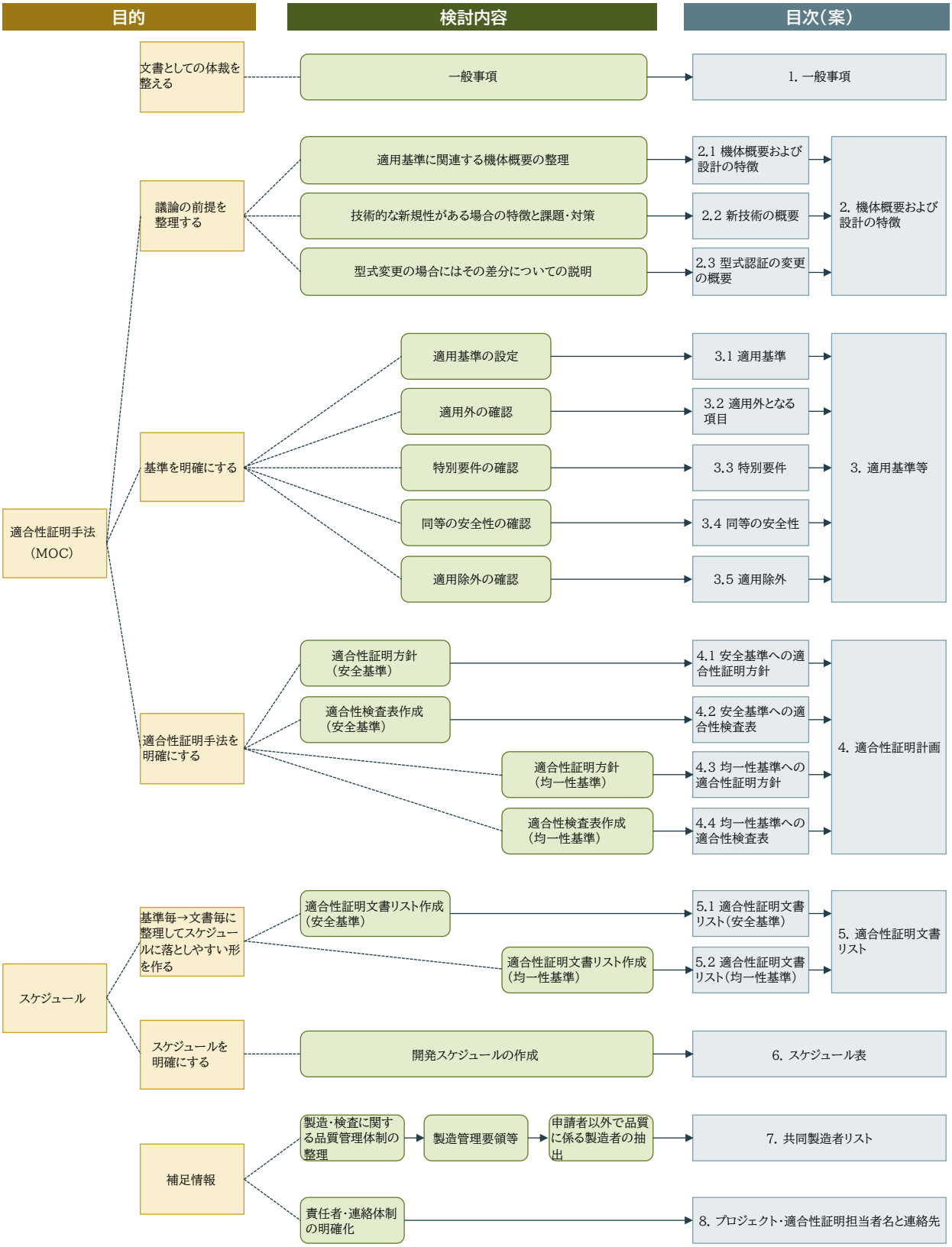
化を図りやすくなる。

「航空局ガイドライン」の【適合性証明計画(案)】【必要書類】で説明されている上記以外の内容もまとめて 1 つの文書として構成した場合の目次案を表 4.4-1 に、目次案を設定した根拠などの背景情報を図に整理する。

表 4.4-1 適合性証明計画 目次(案)

項番および項目	備考
1. 一般事項	
2. 機体概要および設計の特徴	
2.1 機体概要および設計の特徴	
2.2 新技術の概要	
2.3 型式認証の変更の概要	
3. 適用基準など	
3.1 適用基準	
3.2 適用外となる項目	
3.3 特別要件	
3.4 同等の安全性	
3.5 適用除外	
4. 適合性証明計画	
4.1 「安全基準」への適合性証明方針	
4.2 「安全基準」への適合性検査表	必要に応じて別添とする
4.3 均一性基準への適合性証明方針	
4.4 均一性基準への適合性検査表	必要に応じて別添とする
5. 適合性証明文書リスト	
5.1 適合性証明文書リスト(「安全基準」)	
5.2 適合性証明文書リスト(均一性基準)	
6. スケジュール表	
7. 共同製造者リスト	必要に応じて別添とする
8. プロジェクト・適合性証明担当者と連絡先	

371



372

373 図 4.4-1 適合性証明計画 目次(案)の導出

374

(1)　型式認証等に関連する人員に関する事項について

> *6.　適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *（中略）*
>
> *【適合性証明計画(案)】*
>
> *①　適用基準等に関する事項(特別要件等に関する事項を含む。)*
> *（中略）*
>
> *②　型式認証等に関連する人員に関する事項*
> *型式認証等に関連する人員について、それぞれの責任及び権限を明確にします。*
>
> *［引用:航空局ガイドライン］*

本項では、型式認証などに関連する人員に関する事項について解説する。

適用基準は、型式認証において適合性を証明するべき対象になるものであるが、その基準を定める根拠となる「航空局ガイドライン」のもとになる「サーキュラーNo.8-002」では記載の要件となる要件が記載されていないことから有人機のサーキュラーNo.1-307「適合性証明計画について」4.2.1 適合性証明計画(案)③型式証明または型式設計変更に関連する人員に関する事項を参考に解説する。

(i)　全体の責任者の氏名およびその権限
(ii)　設計、製造などに関連するすべての部門の名称、権限および責任者の氏名
(iii)　航空局との主な調整窓口である部門の名称、担当者名および連絡先

“(ⅰ)全体の責任者”は、当該型式認証における全体の責任者であり、プロジェクト組織ならばPMO(Project Management Office: 組織内における個々のプロジェクトマネジメントの支援を横断的に行う部門や構造システム)、機能別組織なら当該事業を統括する責任者などが該当すると考えらえるが、無人航空機の型式認証に係る組織の範囲で適切な職制を選定し、その権限について記述する。

“(ⅱ)設計、製造などに関連するすべての部門の名称、権限および責任者の氏名”は、当該型式の「安全基準」、および均一性基準の適合に係る部門のすべてが対象であるが、組織が細分化されていない場合は、責任の範囲は「適合性検査表」の担当部門欄、および「品質管理体制」を網羅するよう記述することが推奨される。

“(ⅲ)航空局の主な調整窓口である部門の名称、担当者名および連絡先”は、上記(ⅱ)で示した部門の中から型式認証などの窓口になる部門を選定する必要がある。また、ここでは責任者名ではなく、担当者名および連絡先が求められているので、実務を担当する者の氏名とメールアドレス、電話番号などを記載することが必要である。

（2） その他必要となり得る書類：新技術などについて

> *6. 適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *（中略）*
>
> *【必要書類】*
>
> *（中略）*
>
> *⑤ その他必要となり得る書類*
>
> *申請者が従来の無人航空機の設計にはないと考える新設計、新技術、新素材及び新しい製造方法を採用する場合は、その概要並びに検討事項及びその解決方法をまとめてください。（後略）*
>
> *［引用：航空局ガイドライン］*

本項では、「新設計、新技術、新素材および新しい製造方法」（以降、「新技術など」と呼ぶ）について解説する。

「その他必要となり得る書類」として、新技術などに関してまとめる必要がある理由は、特別要件の設定要否について検査者と協議するためである。新技術などに関する協議が必要になるケースとして、

① 申請者が自ら判断して提案する場合
② 検査者が適用基準の検査中に指摘して申請者が追加する場合
③ 審査を進める段階で問題（試験中の不適合など）が発生し対応する場合

が考えられるが、最も望ましいのは①のケースである。

申請者が気を付けなければならないのは、ここで新技術などを挙げたとしてもすぐに特別要件として設定されるわけではないという点である。その特徴やリスクに加えて実績についても検査者と共有し、妥当な適用基準や適合性見解書の要否を申請者と検査者で議論することで、早期に技術面・事業面の不確実性を解消し、プロジェクトリスクを減らすことができる。したがって、申請者が新技術などに該当するかどうかの判断に悩む場合は、①のケースとして検査者と協議することを推奨する。

4.5 適合性証明計画の合意

> *2)　適合性証明計画*
>
> *型式認証等に係る申請者は、(中略)実施時期等を記載する適合性証明計画を作成し、検査者の合意を得ること。検査者は、原則として当該計画に合意した後、検査を開始するものとする。(中略)また、当該計画はプロジェクトの進行に伴い変更されることがあるため、一旦、合意を得た計画を変更する場合にあっても、検査者の合意を得ること。*
>
> *[引用:サーキュラーNo.8-002]*

> *6.　適合性証明計画*
>
> *6-1. 適合性証明計画について*
>
> *(中略)申請者は適合性証明計画(案)及び必要書類を作成し、検査者から合意を得た後に、検査を開始します。(中略)計画の見直しが発生した場合、申請者は当該計画を変更し、再度検査者より合意を得る必要があります。(中略)*
>
> *6-2. 議事録*
>
> *適合性証明計画の説明及び調整を行った際は、その説明内容、指摘及びその改善事項、調査事項、問題点等を明確にし、認識を共有する目的から、申請者において議事録を作成し、双方で記載の内容を確認します。議事録には特に定まった様式ありませんが、サーキュラーNo.8-002の別添 3(JCAB FORM 8-002-3)の様式を使用することも可能です。*
>
> *[引用:航空局ガイドライン]*

本項では、適合性証明計画の合意について解説する。

図 4.1-2 に示すとおり、適合性証明計画は適合性証明計画の審査において検査者から合意を得る。また、審査のアウトプットとして申請者は合意の内容を議事録に記録する。議事録に記録すべき内容については、「航空局ガイドライン」の 6-2. 議事録を参照のこと。

適合性証明計画作成の前提となった各種の情報は、開発の進捗に伴い更新される。更新の内容によっては、当初の計画では証明が出来なくなる、もしくはより合理的な証明方法が可能となるなど、適合性証明計画の内容を更新する必要が生じる。それ以外にも、適合検査(「安全基準」などへの適合性に関する技術的な判定)において不適合となり適合性証明計画の内容を更新する必要が生じる場合もある。このような場合に再度検査者により合意を得るプロセスとして明確な定めはサーキュラーなどに記載されていないものの、基本的には適合性証明計画を改訂し、改訂版について検査者と調整したうえでその結果を議事録に残すことで合意を得るプロセスが想定される。適合性証明計画を変更する場合のフローの例を

図 4.5-1 に示す。

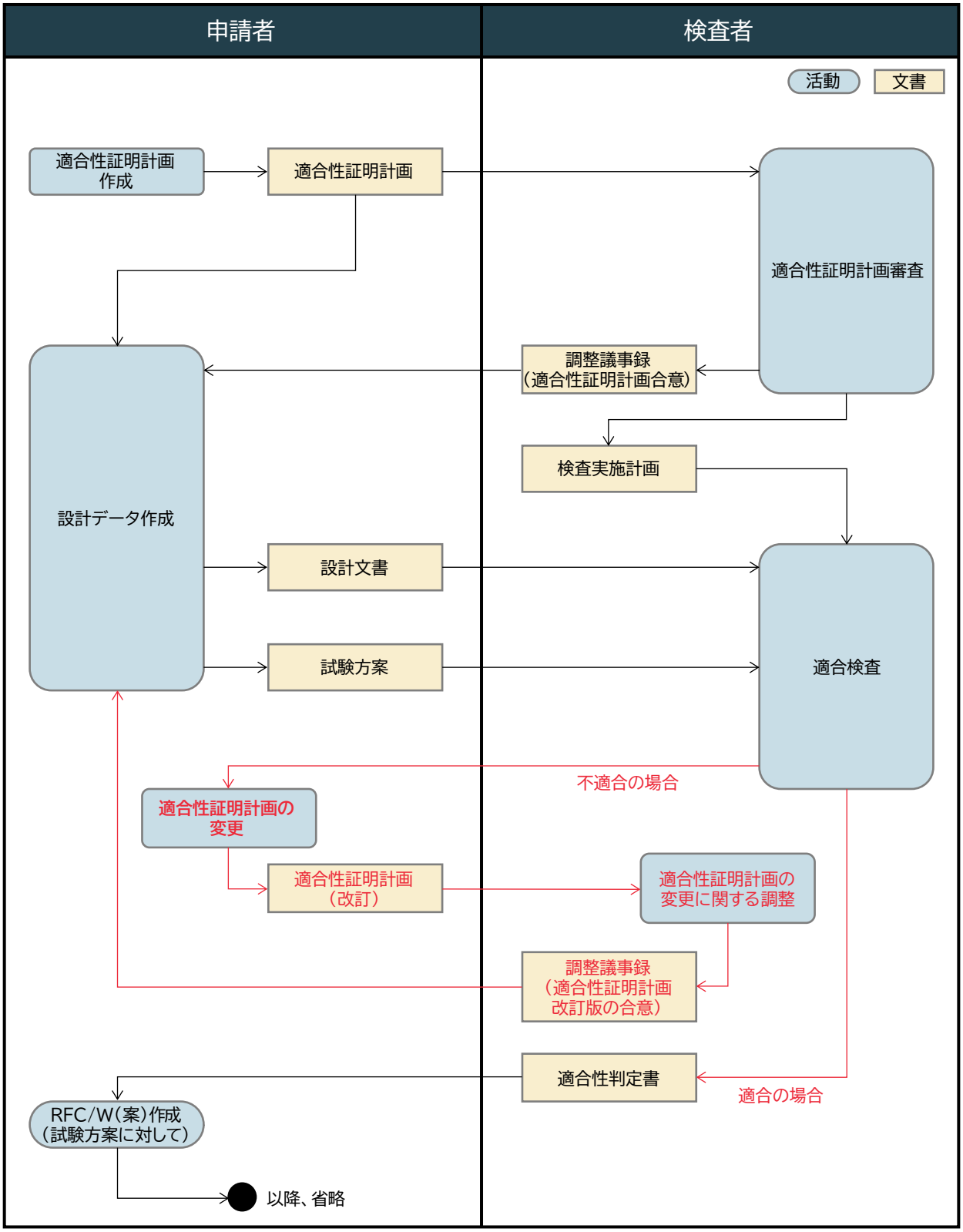


図 4.5-1 適合性証明計画を変更する場合のフローの例(適合検査で不適合となった場合)

4.6 適合性検査表について

> *2） 適合性検査表*
> *適合性検査表は、適用基準の項目ごとに証明状況を示すものである。*
> *検査者は、申請者が作成した適合性証明計画に基づく適用基準への適合性の状況を本適合性検査表により管理する。*
> *［引用：サーキュラーNo.8-002］*

> *6-4. 適合性検査表について*
> *適合性検査表には、少なくとも以下を含み、適用基準等の項目ごとに証明状況を示すためにも重要となります。*
> *（中略）*
> *また、第 4 部の均一性基準に係る事項についても同様に適合性の計画を示してください。*
> *［引用：航空局ガイドライン］*

本項では、適合性検査表について解説する。「適合性検査表」は「適合性証明計画」作成の重要な部分であり、提出書類の中心をなすものである。型式認証プロセスでは、無人航空機が製造される段階から様々な評価が行われ、適切な証明が求められる。この「適合性検査表」は製造管理要領、無人航空機飛行規程、無人航空機整備手順書など、型式認証申請に必要な文書群の多くの項目と共に審査され、製造者が適切な設計、製造、品質管理を守るための重要なツールとなる。

型式認証を申請する機体が航空法のすべての基準を満たしているかを確認するためには、「適合性検査表」の作成が必要不可欠であり、この表を活用することで、綿密に調査・確認を行い、不適切または不整合が見出された場合には、その箇所を特定し、適切な解決策を見つけることが可能となる。この表は、製品が規定の基準をクリアしているかどうかを明示し、安全要件の準拠に関する情報を保存するために使われる。

「適合性検査表」の作成に必要となる文書や情報は多岐にわたる。無人航空機の型式、モーターや ESC などのコンポーネントの詳細、製造者の情報、検査手順への準拠状況、最大離陸重量や重心位置などの重量情報、限界速度、風速、高度などの運用限界、出力や推力、回転翼の回転速度、気温などの諸元、装備品や部品の情報などを仕様書、規程、手順書などに詳細に記述する必要がある。これらの情報は無人航空機の性能や安全性を客観的に評価し、適合性を判定するために以下のステップで作成する。

(1) ステップ 1：適用基準の理解

「適合性検査表」作成の第 1 ステップは、「航空局ガイドライン」の「安全基準」および「均一性基準」の理解である。「サーキュラーNo. 8-001」 および「サーキュラーNo. 8-002」がこれに相当する。「安全基準」は機体の性能や機能が安全性を確保する要件に適合しているかを評価する基準であり、「均一性基準」は製品が一貫した品質で製造され、各製品が同一の安全性を保証していることを確認する基準である。これらの基準の理解は「適合性検査表」作成の土台である。サーキュラーの内容を細読し、理解を深めることは必須である。

（2） ステップ 2：設計データおよび製造管理要領などの参照

次のステップは、製造予定の無人航空機の設計データの参照である。この設計データは、「適合性検査表」への情報の供給源となる。設計データに基づく「安全基準」の評価は、「適合性検査表」の充実に寄与する。図面、スペックシート、試験データなどの設計データは、製品の安全性や品質を保証するための根拠となる。設計者からの詳細な解説も求められ、これにより、より深い理解と適切な評価が可能となる。なお、「安全基準」と同様に、「均一性基準」についても製造管理要領および品質管理体制などに基づき、詳細な文書を参照する。

（3） ステップ 3：適合性検査表（案）の作成

基準の理解と設計データの参照後は、「適合性検査表（案）」の作成を行う。この段階では進捗管理が重要である。作業は個々の要素ごとに進められ、検査者と合意したスケジュールに基づき「適合性検査表（案）」を完成に向けて記入する。各項目は設計データに基づいて慎重に評価し、「適合性検査表（案）」を作成する。基準を満たさない場合や疑義が生じた場合は、その箇所は明確に記録し、解決策を検討する。

（4） ステップ 4：適合性検査表（案）の説明

記入完了した「適合性検査表（案）」は、「適合性証明計画（案）」と一緒に検査者への説明前に社内で関連部門とレビューし、整理する。「安全基準」、「均一性基準」の各要求に対して、具体的な設計や製造過程と合わせた適合性の説明がされているかを確認し、立証するためのドキュメントが揃っていることを第三者的な観点で確認し、過去の調整結果の議事録、および見解書（案）で合意した内容と整合せしているかも確認する。

5　今後の課題(未議論項目)

WG 活動で議論があったが未対応(今後対応予定)の項目は以下の通り。

5.1 均一性基準に関する適合性検査表など

現時点では適合性検査表などの細部の議論は「安全基準」を主な対象としており、均一性基準に関する議論は今後深掘りし、解説書に追記する予定としている。

5.2 適合性証明計画のサンプル(Appendix 1)

表 4.4-1 に示す適合性証明計画の目次に沿って具体的な内容を記述したサンプルを Appendix 1 適合性証明計画のサンプル に添付する予定であるが、現時点では TBD を含んでいる。今後、TBD の項目についても DARFT2 にて追記する予定としている。

Appendix 1 適合性証明計画のサンプル

表 4.4-1 に示す適合性証明計画の目次に沿って具体的な内容を記述したサンプルを Appendix1 として別紙にまとめる。

Appendix 2 各セクション特有の用語集

DARFT2 にて追記予定

Appendix 3 関連文書

(1) サーキュラー No.8-001 無人航空機の型式認証等における安全基準および均一性基準に対する検査要領、2022 年 9 月 7 日(国空機第 456 号)、
https://www.mlit.go.jp/koku/content/001520547.pdf

(2) サーキュラー No.8-002 無人航空機の型式認証等の手続き、2022 年 12 月 2 日(国空機第 645 号)https:// www.mlit.go.jp/koku/content/001574424.pdf

(3) サーキュラー No.1-307 適合性証明計画について、2005年 9 月 30 日 制定(国空機第 5029 号)、https://www.mlit.go.jp/notice/noticedata/pdf/20190403/1-307.pdf

Appendix 4　サブ WG の構成員名簿

無人航空機の第二種認証に対応した証明手法の事例検討 WG におけるサブ WG 型式認証プロセス　適合性証明計画(CP)の構成員名簿(サブ WG 主査およびライター)を以下に示す。なお、レビュワーの講成員名簿は本冊(RMD、Rev.01)Appendix3 を参照すること。

役割	氏名	所属
主査	橋本　寛之	株式会社プロドローン
ライター	松橋　雅彦	株式会社スカイワード・オブ・モビリティーズ
ライター	西岡　亮	株式会社ベリサーブ

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日 2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

524

RMD-CP DARFT Rev.01 Appendix 1

国立研究開発法人新エネルギー・産業技術総合開発機構
（NEDO）
次世代空モビリティの社会実装に向けた実現プロジェクト
（ReAMo プロジェクト）

無人航空機の型式認証等の取得のためのガイドライン

型式認証プロセス 適合性証明計画（CP） 解説書

Appendix 1 適合性証明計画サンプル

2024 年 3 月

国立大学法人東京大学
一般財団法人日本海事協会
公立大学法人会津大学
株式会社電通総研（旧株式会社電通情報サービス）

目次

図 目次

表 目次

本書の目的

本書は、「無人航空機の型式認証などの取得のためのガイドライン（以降、「航空局ガイドライン」と呼ぶ）」に関する適合性証明計画（CP）の解説書の Appendix として、適合性証明計画のサンプルをまとめるものである。解説書の内容に関して具体的なイメージをつかむための参考文書であり、本書のとおりに適合性証明計画を作成したとしても、実際の認証プロセスにおいて十分なものになっているとは限らないことを注意する。

1　一般事項

1.1　目的

本書は、1.2 項に示す型式の第二種型式認証における適合性証明計画（案）をまとめるものである。

☝　解説
申請者が適合性証明計画を作成した段階ではあくまでも（案）であり、適合性証明計画の審査により合意が得られたのちに（案）ではなくなるため、適合性証明計画（案）と記載している。

1.2　対象とする型式

AAA 式 BBB 型

1.3　申請区分

- 第二種型式認証
- 最大離陸重量 4kg 以上 25kg 未満のもの

1.4　関連文書

関連文書[1]　サーキュラーNo. 8-001”無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領”

関連文書[2]　サーキュラーNo. 8-002”無人航空機の型式認証等の手続き”

関連文書[3]　無人航空機の型式認証等の取得のためのガイドライン

関連文書[4]　設計概念書（CONOPS）

1.5　略語/用語書

DARFT2 にて追記予定

2　機体概要および設計の特徴

2.1　機体概要および設計の特徴

(1)　機体概要および主要諸元

申請する型式の機体(以降「対象機体」という)の概要を図 2.1-1 に、主要諸元を表 2.1-1 に示す。

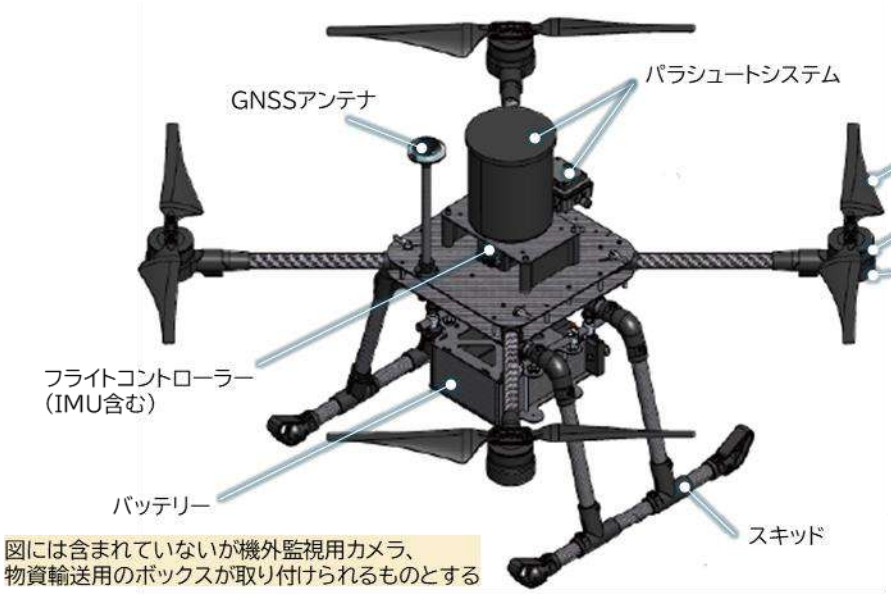


図 2.1-1 機体概要

表 2.1-1 主要諸元

仕様			備考
分類		マルチローター	電動推進
主要寸法	機体全長	700 mm	
	機体全幅	700 mm	
	全高	560 mm	
	プロペラ直径	17 inch(432mm)	
主要重量	最大離陸重量	11.0 kg	
	機体重量	9.0 kg	バッテリー含む
	最大ペイロード	2.0 kg	
最大飛行時間		15 分	

（2） 想定する運用

想定する運用環境を関連文書[4]から抜粋して表 2.1-2 に示す。対象機体の用途は物資輸送であり、代表的な運用イメージを図 2.1-2 に示す。

表 2.1-2 CONOPS に関する設定

CONOPS の項目			申請型式における設定
（a）意図する運用のタイプ	航空法第 132 条の 85 第 1 項(飛行の禁止空域)および同第 132 条の 86 第 2 項(飛行の方法)における適否	空港などの周辺の空域、緊急用務空域または 150m 以上の上空	非適用
		人または家屋の密集している地域(DID)の上空	非適用
		夜間飛行	非適用
		目視外飛行	適用
		人または物件から 30m 以上の距離が確保できない飛行	適用
		催し場所上空の飛行	非適用
		危険物の輸送	非適用
		物件投下	非適用
（b）無人航空機の仕様	性能特性	飛行フェーズごとの自動・自律状態	離陸～ウェイポイント飛行～着陸のフェーズにおいて、すべて自動飛行
（c）気象状態	雷、雨、雪および着氷状態など運用できる気象条件		雨天 10mm/h まで可。 雷・雪・着氷気象状態は不可。 耐風速：10m/s
（d）使用者、無人航空機を飛行させる者および関係者の責任			TBD

CONOPS の項目	申請型式における設定
(e) コントロールステーション(CS)、補助機器およびその他安全基準に適合するために必要な関連システム(AE)	主操縦装置(GCS): PC にインストールしたソフトウェア 副操縦装置: プロポによる緊急介入
(f) 無人航空機の運用のために使用される無線通信機能(コマンド、コントロールおよびコミュニケーション)	機体～GCS 間: LTE 通信 機体～プロポ間: 2.4GHz
(g) 人口密度、運用(地理的)の境界、空域、離着陸エリア、運用エリアの混雑度、航空交通管制(Air Traffic Control: ATC)との連絡、目視内飛行または目視外飛行の種別(目視内の場合は最大通信距離、目視外の場合は利用する無線システムの種類および最大通信距離)、航空機との間隔などの運用パラメータ	TBD
(h) 認証に必要な場合、衝突回避装置	なし

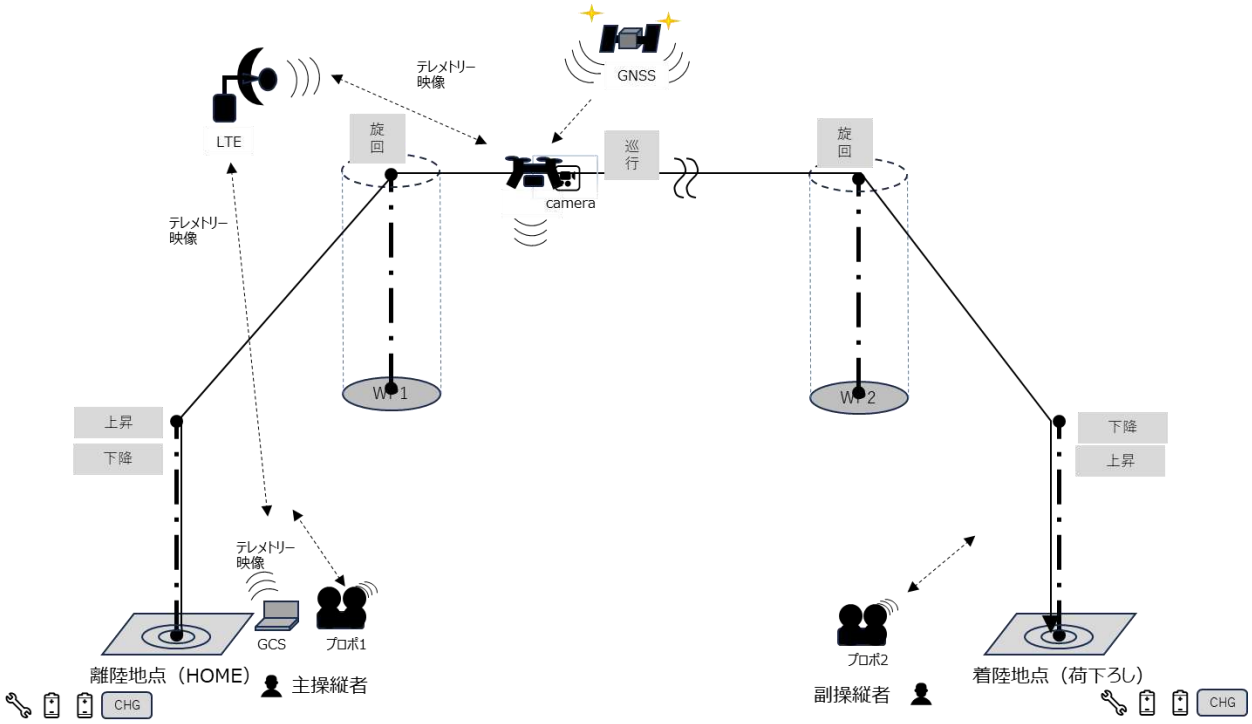


図 2.1-2 運用イメージ

解説
本項に示す内容は、関連文書[3]第 2 部 型式認証プロセス(31/72)【必要書類】③に相当するものであり、CONOPS を提出することで対応することも可能と考えられる。

（3） 非該当の場合に特別要件などの調整が必要となる機体および運用の仕様

対象機体および運用について、関連文書[3]第 3 部 安全基準(3/71)に示されている仕様に対する非該当の有無を表 2.1-3 に示す。

表 2.1-3 非該当の場合に特別要件などの調整が必要となる仕様

機体および運用の仕様 （非該当の場合に特別要件などの調整が必要）	該当/ 非該当	根拠など
無人航空機が C2 リンクを有し、操縦者が緊急時の対応を取ることができるもの	該当	表 2.1-2(e)項および(f)項
着氷気象状態での運用を行わないもの	該当	表 2.1-2(c)項
操縦者と無人航空機の数の比率が 1:20 以下のもの	該当	図 2.1-2 に示すとおり操縦者 1 名または 2 名に対して 1 機の運用とする(操縦者と無人航空機の数の比率が 1:20 以下)
電動推進の無人航空機であること(内燃機関または燃料電池を除く)	該当	表 2.1-1

（4） 該当の場合に適合性見解書の調整が必要となる技術要素

適合性見解書が必要となる可能性のある技術要素リスト(関連文書[3]第 3 部 安全基準(3/71)参照)への該当の有無および該当する場合には、特別要件、適用除外、同等の安全性のいずれに関する適合性見解書であるかを表 2.1-4 に示す。

表 2.1-4 該当の場合に適合性見解書が必要となる可能性のある技術要素リスト

技術要素リスト	説明	該当	適合性見解書(案)
自律飛行	D&R は操縦者の介入を前提とする基準のため、飛行中に遭遇するあらゆる状況に対し、地上からの指示によらず、安全を確保した自動動作を継続し得る自律飛行であれば各基準に対し同等の安全性の証明が必要になる可能性があります。	非該当	N/A

技術要素リスト	説明	該当	適合性見解書(案)
内燃機関	実証飛行試験に必要な飛行時間の算出に使用するパラメータの 1 つであるクラッシュエリアが電動推進の無人航空機と異なる可能性があるため、飛行時間が追加される可能性があります。また、内燃機関そのものや内燃機関に付帯する燃料系統／給排気系統などに特有の安全性への影響に対し、追加の基準が必要になる可能性があります。 なお、内燃機関には推進用途のものだけでなく、発電用途のものも含みます。	非該当	N/A
燃料電池	同上	非該当	N/A
着氷気象状態での運用	着氷気象状態での運用が安全性に影響を与えないことを設計で証明する場合、証明に必要な試験条件などの明確化が必要になる可能性があります。	非該当	N/A
耐雷特性	雷環境での運用が安全性に影響を与えないことを設計で証明する場合、証明に必要な試験条件などの明確化が必要になる可能性があります。	非該当	N/A
電磁干渉(EMI)と高強度放射電界(HIRF)耐性	EMI と HIRF 環境での運用が安全性に影響を与えないことを設計で証明する場合、証明に必要な試験条件などの明確化が必要になる可能性があります。	非該当	N/A
人工知能(AI)	AI が安全性に影響を与えないことの証明が必要になる可能性があります。なお、ここでいう AI には自律飛行のほか、画像認識や異常検知など限られた範囲で使用する場合も含まれます。	非該当	N/A
Detect and Avoid (DAA) システム	DAA(協調型および非協調型)の性能基準および証明に必要な試験条件などの明確化が必要になる可能性があります。	非該当	N/A
危害軽減機能など	プロペラガード、 衝突した際の衝撃を緩和する素材の使用またはパラシュートなどの危害軽減機能などについて追加の基準が必要になる可能性があります。	パラシュートシステム	同等の安全性(※1)
危害防止機能など	エアバッグなどの危害防止機能などについて追加の基準が必要になる可能性があります。	非該当	N/A
キルスイッチ	第二種型式認証で不具合発生時に立入管理区画内にあえて墜落させ安全を確保する方法(いわゆるキルスイッチ)について、その妥当性について追加の基準が必要になる可能性があります。	キルスイッチ	不要(※2)

159
160

※1 パラシュートシステムについての同等の安全性

性能確認試験で使用する機体は本型式に類するが、カメラなどの試験データに影響のない搭載品を省略するため、同等の安全性について適合性見解書を必要とする。

※2 キルスイッチの適合性見解書

特別要件を設定する可能性があるが、機体の安全基準の各規定で妥当性について確認ができるものと考える。

解説
※1 や※2 は解説書の内容を広く記載するための一例であり、実際の申請に際しては申請者と検査者で協議し、プロジェクト毎の判断で設定される。

2.2 新技術の概要

2.1(4)項にはなく、適合性見解書を要する可能性のある技術要素を新技術として設定する。表2.2-1に示すとおり、対象機体においては新技術に該当する技術要素はない。

表 2.2-1 新技術リスト

技術要素リスト	説明	該当	適合性見解書(案)
(なし)	N/A	N/A	N/A

2.3 型式認証の変更の概要

型式認証の変更ではないため該当しない。

3　適用基準など

3.1 適用基準

2 項の機体概要および運用を前提とした適用基準を表 3.1-1 に、機体の安全基準の区分に応じて適用される規定の該当区分を表 3.1-2 に示す。

表 3.1-1 適用基準

基準	適用可否
航空法(昭和 27 年法律第 231 号)第 132 条の 13 ならびに同第 132 条の 16 に定める安全基準並びに均一性基準	■適用 □非適用
航空法施行規則(昭和 27 年運輸省令第 56 号)第 236 条の 15 ならびに同第 236 条の 24	■適用 □非適用
サーキュラーNo.8-001「無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領」(令和 4 年 9 月 7 日制定(国空機第 456 号))	■適用 □非適用

表 3.1-2 区分に応じて適用される規定

（凡例）✓：適用されるもの、✓✓：該当する特定飛行※1に応じて適用されるもの、N/A：適用されないもの

区分	第二種				第一種
	機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機				機体認証を受けようとする無人航空機／型式認証を受けようとする型式の無人航空機
	最大離陸重量4kg未満のもの	最大離陸重量4kg以上25kg未満のもの	最大離陸重量25kg以上のもの		特定空域を含まない空域を飛行するもの
			法第132条の85第1項各号に掲げる空域以外の空域を飛行し、かつ、法第132条の86第2項第1号から第4号までのいずれにも該当する方法により飛行するもの※2	その他のもの※3	
001 設計概念書（CONOPS）	✓	✓	✓	✓	✓
005 定義	✓	✓	✓	✓	✓
100 無人航空機に係る信号の監視と送信	✓※4	✓	✓	✓	✓
105 無人航空機の安全な運用に必要な関連システム	✓	✓	✓	✓	✓
110 ソフトウェア	✓※5	✓※5	✓※5	✓	✓
115 サイバーセキュリティ	✓	✓	✓	✓	✓
120 緊急時の対応計画	✓✓※6	✓	✓	✓	✓
125 雷	✓	✓	✓	✓	✓
130 悪天候	✓	✓	✓	✓	✓
135 重要な部品（フライトエッセンシャルパーツ）	✓	✓	✓	✓	✓
140 その他必要となる設計及び構成	✓※7	✓※7	✓※7	✓※7	✓※7
200 無人航空機飛行規程	✓	✓	✓	✓	✓
205 ICA	✓	✓	✓	✓	✓
300 耐久性及び信頼性	✓	✓	✓	✓	✓
305 起こり得る故障	✓✓※8	✓✓※8	✓	✓	✓
310 能力及び機能	✓※9	✓	✓	✓	✓
315 疲労試験	N/A	N/A	✓	✓	✓
320 制限の検証	N/A	N/A	✓	✓	✓

出所）サーキュラー No.8-001 無人航空機の型式認証等における安全基準及び均一性基準に対する検査要領

3.2 適用外となる項目

安全基準の区分に応じて適用となる規定の内、適用外となる項目を表 3.2-1 に示す。

表 3.2-1 適用外となる項目

適用外となる項目		理由
安全基準	001(h)	衝突回避装置を具備しない。
	125(a)	落雷の可能性がある天候での運用を禁止するものとし、無人航空機は雷撃による計画外飛行または制御不能がないような設計特性を有さない。(125 (b) を適用する)。
	130(c)(2)	無人航空機の運用が認められていない悪天候について、悪天候への不意の飛行を防ぐための運用限界を設定する。(130 (c) (1) を適用する)
	140-1(c)	最大離陸重量が 25kg に満たない。
	140-2(c)	夜間飛行を実施しない。
	140-4	危険物の輸送を行わない。
	140-5	最大離陸重量が 25kg に満たない。

3.3 特別要件

表 2.1-3 および 表 2.1-4 から、表 3.3-1 に示すとおり特別要件を必要とする項目はない。

表 3.3-1 特別要件を必要とする項目

特別要件を必要とする項目	理由
(なし)	N/A

3.4 同等の安全性

表 2.1-4 から、同等の安全性を適用する項目を表 3.4-1 に示す。

表 3.4-1 同等の安全性を適用する項目

適用外となる項目		理由
安全基準	140-1(d)	危害軽減のためのパラシュートシステムに関する性能確認試験について、対象機体の型式に類し、試験目的と実施内容から試験データへの影響がない機体を試験に用いる可能性がある。

3.5 適用除外

表 2.1-4 から、表 3.5-1 に示すとおり適用除外とする項目はない。

表 3.5-1 適用除外とする項目

適用除外とする項目	理由
(なし)	N/A

4　適合性証明計画

4.1 安全基準への適合性証明方針

DARFT2 にて追記予定

4.2 安全基準への適合性検査表

DARFT2 にて追記予定

4.3 均一性基準への適合性証明方針

DARFT2 にて追記予定

4.4 均一性基準への適合性検査表

DARFT2 にて追記予定

5　適合性証明文書リスト

5.1 適合性証明文書リスト(安全基準)

DARFT2 にて追記予定

5.2 適合性証明文書リスト(均一性基準)

DARFT2 にて追記予定

6　スケジュール表

DARFT2 にて追記予定

7　共同製造者リスト

DARFT2 にて追記予定

8　プロジェクト・適合性証明担当者と連絡先

DARFT2 にて追記予定

無人航空機の型式認証等の取得のためのガイドライン解説書

発行日：2024 年 3 月

この成果は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務（JPNP22002）の結果得られたものです。

257