RMD-115 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

無人航空機の認証に対応した証明手法の事例検討
115 サブ WG サイバーセキュリティ

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）」[(1)]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。

なお、解説対象とする文書は国土交通省航空局から 2022 年（令和 4 年）12 月 2 日発行時点の航空局ガイドラインとする。解説対象に関する詳細は本冊（RMD　Rev.01）1.2 を参照すること。

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（以降、「115 サブ WG」と呼ぶ）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）」[(2)]、「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）」[(3)]、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

基準の概要

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。

適合性証明方法(MoC):1、2

(a): セクション 115 セキュリティ適合性証明計画 (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)

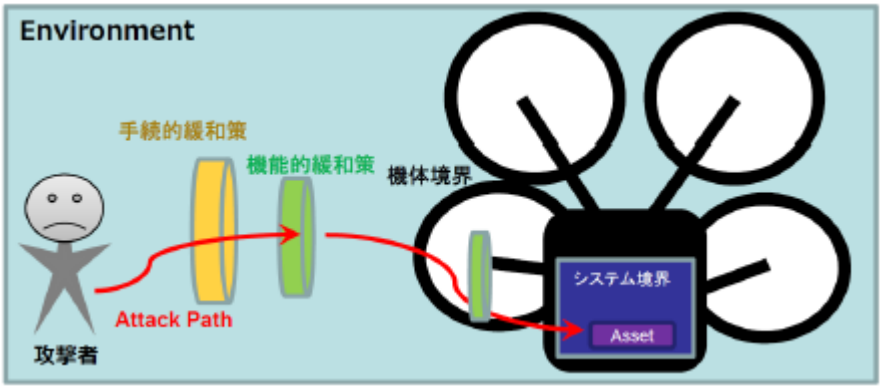
(a)項の結果を完了報告書としてまとめるとともに、ICA に定めるセキュリティ対策の維持手順および指示(セキュリティガイドライン)も完了報告書に記載します。

※「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

<u>その他参考となる情報</u>

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[(4)]に基づくサイバーセキュリティリスク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 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リスク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リスク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

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。

本項では、セキュリティ適合証明のための要求を、安全基準から解釈して 6 項目抽出した。6 項目の要求は以下の通りである。

- 要求 1: システム境界の明確な記述
- 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
- 要求 3: サイバーセキュリティリスクの特定
- 要求 4: 特定されたセキュリティリスクの評価
- 要求 5: 評価に基づく緩和策の実施と記述
- 要求 6: セクション 115 適合性証明計画書類の矛盾のない記述

また、以下の小項目では、各要求に紐づく活動も列挙する。

(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、対象とする無人航空機システムを含む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。この要求を満たすために、無人航空機システム全体の構成を具体的に記述するために推奨される活動として、3 つの活動が充てられる。

- 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」[(5)]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。この要求のために 3 つの活動が充てられる。

- 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が陥ってはならないセキュリティ上の脅威事象（Threat Condition）が示され、次に、無人航空機システム全体から、セキュリティ環境（Security Environment）を定義し、サイバーセキュリティで保護するべきセキュリティ境界（Security Perimeter）を設定し、その環境と境界との接点で脅威源（Threat Source）が提示されている必要がある。

セキュリティ環境は無人航空機システムの外側に位置するユーザーや攻撃者（Attacker）、または無人航空機システム外の電子的に接続する他のシステムのことである。

セキュリティ境界は無人航空機システム内の資産（Asset）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とは、これらセキュリティ環境、セキュリティ境界および無人航空機システムを含めたセキュリティに関連するもの全体をいう。

脅威源は攻撃者を含むすべてのアクター（Actor）である。

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。これらの安全性に関しては、RMD 本冊 2.2 章 安全基準の中で示されている事象が脅威事象である。

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］*

[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。

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。この要求のために 4 つの活動が充てられる。

- 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
- 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、発生した脅威事象の影響度（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。この要求のために 1 つの活動が充てられる。

- 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。この要求のために 4 つの活動が充てられる。

- 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 はユーザー側の整備に関する記述であるが、そのほかにメーカー側の整備などの記述として、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、バージョン管理も推奨される。

（6） セクション 115 適合性証明計画書類の矛盾のない記述

> *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］*

この要求は、適合性証明について、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、および、完了報告書が記述されるにあたって、計画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、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。この要求のために 4 つの活動が充てられる。

- 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
- 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。

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計画された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*
> *…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「セクション 001CONOPS(以降、「セクション 001」と呼ぶ)」でなされることが望ましい。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含まれる。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。

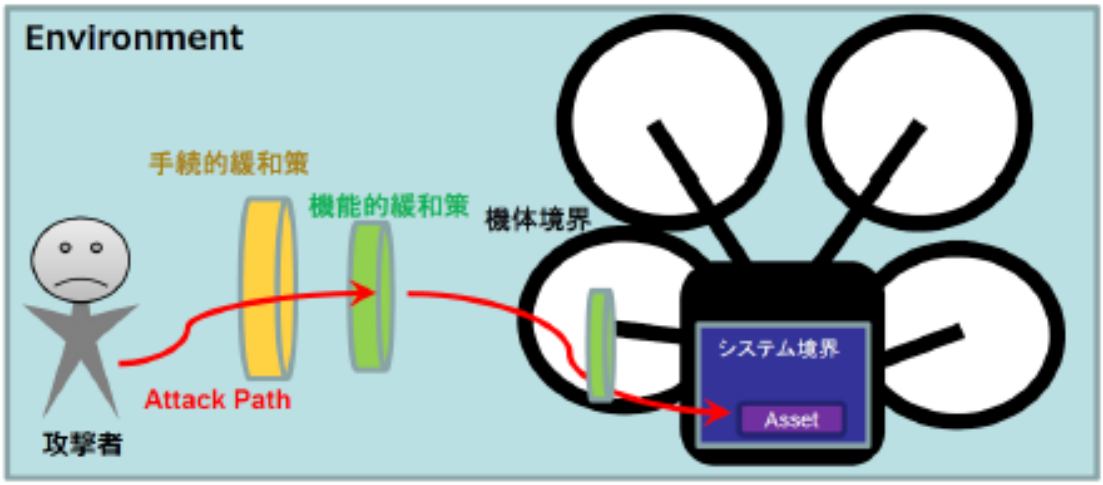


図 4.3-1 航空局ガイドライン セクション 115 内 機体境界、システム境界および資産の概念図
出所）航空局ガイドライン

「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。一方で、セクション 115 で記述するべき情報としては、図 4.3-1 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、セキュリティリスク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*
> *…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。*
> *［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*
> *…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。*
> *…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。*
> *…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*
> *…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(リスク重大度: Severity)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、脅威事象が発生しうる可能性を捉えた形で、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、このリスク重大度から、資産が奪われる場合の可能性を示す脅威レベル(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[6]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*
> *…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予想のことである。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を持つ可能性があると言える。

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。このため、勘案

すべき脅威レベルは、攻撃者のスキルによって、また、攻撃対象となるユースケースによって異なる。このような、攻撃者のスキルやユースケースなどの前提条件は、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*
> *…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。*
> *…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。

図 4.3-1 のセキュリティ環境、セキュリティ境界、攻撃者、攻撃経路、緩和策、機体境界およびシステム境界を示す図は、図 4.3-2 で示される RTCA DO-326A[(4)] Figure 3-6 に示される図の簡略化されたものである。保護すべき資産（Asset）は、図においてはシステム内部に含まれるが、必ずしも機体境界内やシステム境界内にあるとは限らない。特に、コマンドなどを扱う AE など、機体外部のシステムや、C2 リンク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。むしろ、セキュリティ境界は、図 4.3-3 のように、複数のセキュリティ境界が含まれるなど、セキュリティ環境全体に対して、柔軟に設定されるものである。そのため、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ことから、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。

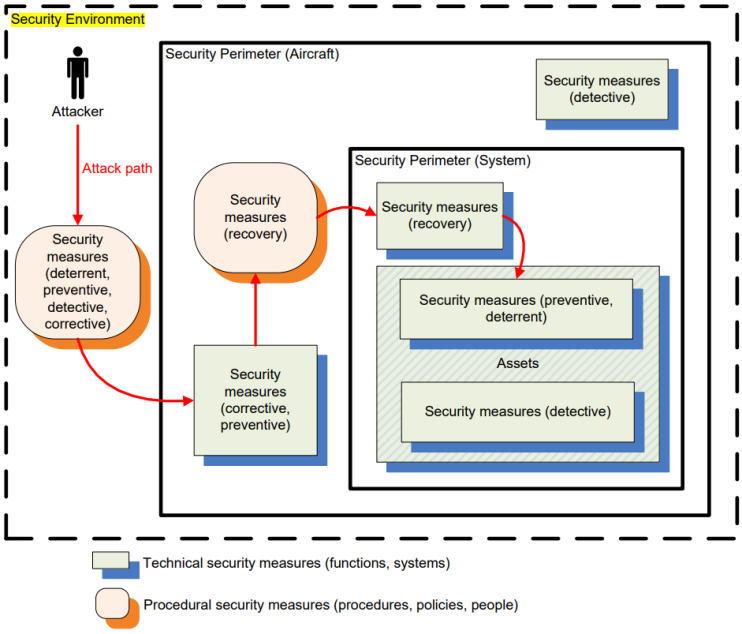


FIGURE 3-6: SIMPLIFIED EXAMPLE OF A SECURITY ARCHITECTURE WITH DIFFERENT TYPES OF TECHNICAL AND PROCEDURAL SECURITY MEASURES

図 4.3-2　セキュリティ環境、セキュリティ境界、機体と攻撃者の関係図

出所)RTCA DO-326A / EUROCAE ED-202A – Airworthiness Security Process Specification, https://my.rtca.org/productdetails?id=a1B36000001IcfuEAC、Figure 3-6

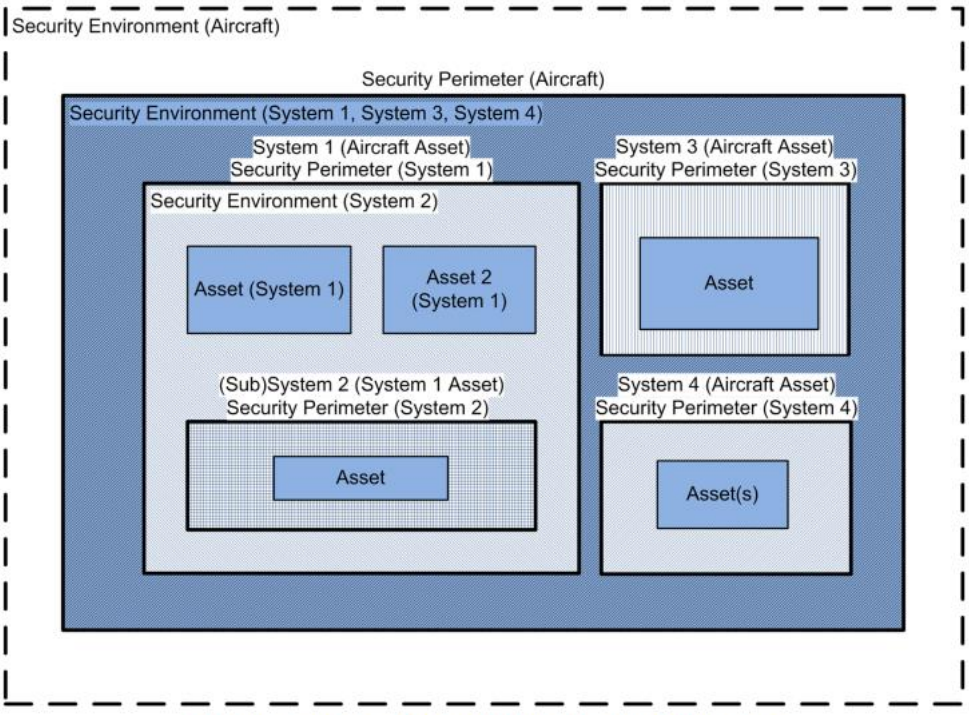


FIGURE 5-3: NESTED SECURITY ENVIRONMENTS

図 4.3-3　複数のセキュリティ境界が含まれる場合

出所)RTCA DO-356A / EUROCAE ED-203A – Airworthiness Security Methods and Considerations, https://my.rtca.org/productdetails?id=a1B36000006xdusEAA, Figure 5-3

（7） 資産とリスク重大度の定義

> *2: 解析・評価 / Calculation/Analysis*
> *…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[(4)]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、資産に対する重大度を脅威事象のリスク重大度として充当する。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頻度に基づく定量的な尺度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*
> *…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を提示しているが、より具体的に影響評価を行うために、脆弱性に脅威が及ぶことで資産が攻撃を受けるシナリオを用いることもできる。脅威分析のモデルとして STRIDE[7]が知られている。また、より詳細な脆弱性の評価の方法として、CVSS[8]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。

なお、脅威に対して、制御の情報などを外部から不正に取得すること、および不正に挿入することなどの無線通信による攻撃は具体的な脅威としてセクション 115 の考察の範囲内であるが、無線電波に対する干渉を与えてデータを取得できないようにする『ジャミング』に対しては、セクション 115 よりはセクション 100 の電波強度などの範囲で検証する必要がある。

(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*
> *…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。航空局ガイドラインには、既知の脆弱性について考慮するとされているが、緩和策を含んだ脆弱性とその影響に対する評価を行う必要があることを示している。また、この評価は、フライトフェーズ(保管時、離陸前後、飛行中)や、影響を受ける対象ごとに評価を行うことを推奨としている。

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: 脆弱性試験(ペネトレーションテスト)や、ファジング(ソフトウェア動作検証の一手法)[9]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。専門家によるチェックリストによる検査も推奨される。
- 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*
> *…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の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。このリスクの値には、緩和策に与えられる防御レベル(Level of Protection, LoP)や、脅威に対して与えられる脅威レベル(Level of Threat, LoT)が想定される。

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*
> *…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)
- 脅威事象とその重大度、およびその受け入れ可能な生起確率
- 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、および緩和策の有効性を勘案し、脅威事象の生起確率が、脅威事象のリスク重大度に見合った許容可能な範囲にまで、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*
> *…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]*

評価の結果、脅威シナリオの生起確率が許容可能な範囲にまで緩和されていない場合、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)[10]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[4]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、ソフトウェア機能として緩和策が実施される場合、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、運用にて緩和策が実現される場合は、「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、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。もしその時点で想定していない、未発見の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。そのため、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 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は、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[4], DO-356A[11]で記述されている活動や尺度、方法は、航空局ガイドラインでも参照されているとおり、非常に有用である。また、ASTM F3201-16[12]においても同様に、RTCA DO-326A[4]が積極的に利用されている。ASTM F3532-23[13]は有人航空機の IUEI に対するセキュリティリスクアセスメントの手法であるが、本質的には RTCA DO-326A[4]の手順を踏襲している。そのほか、ISO/SAE 21434(路上走行車両)[14], IEC 62443 (CSMS)[1], ISO 27005:2022 (ISMS)[10]などの記述、CC (ISO/IEC 15408)[16]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は、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[11]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は、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 能力及び機能(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[17]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、ISO/IEC 27005:2022[10]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 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[4], 356A[11], 355[18]および EUROCAE ED-202A[4], 203A[11], 204A[18]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 セキュリティ適合性証明計画書は CP と異なり、⑧設計書類等の提出の段階での提出となる。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。

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。以下に示す①～⑩のステップで構成される。

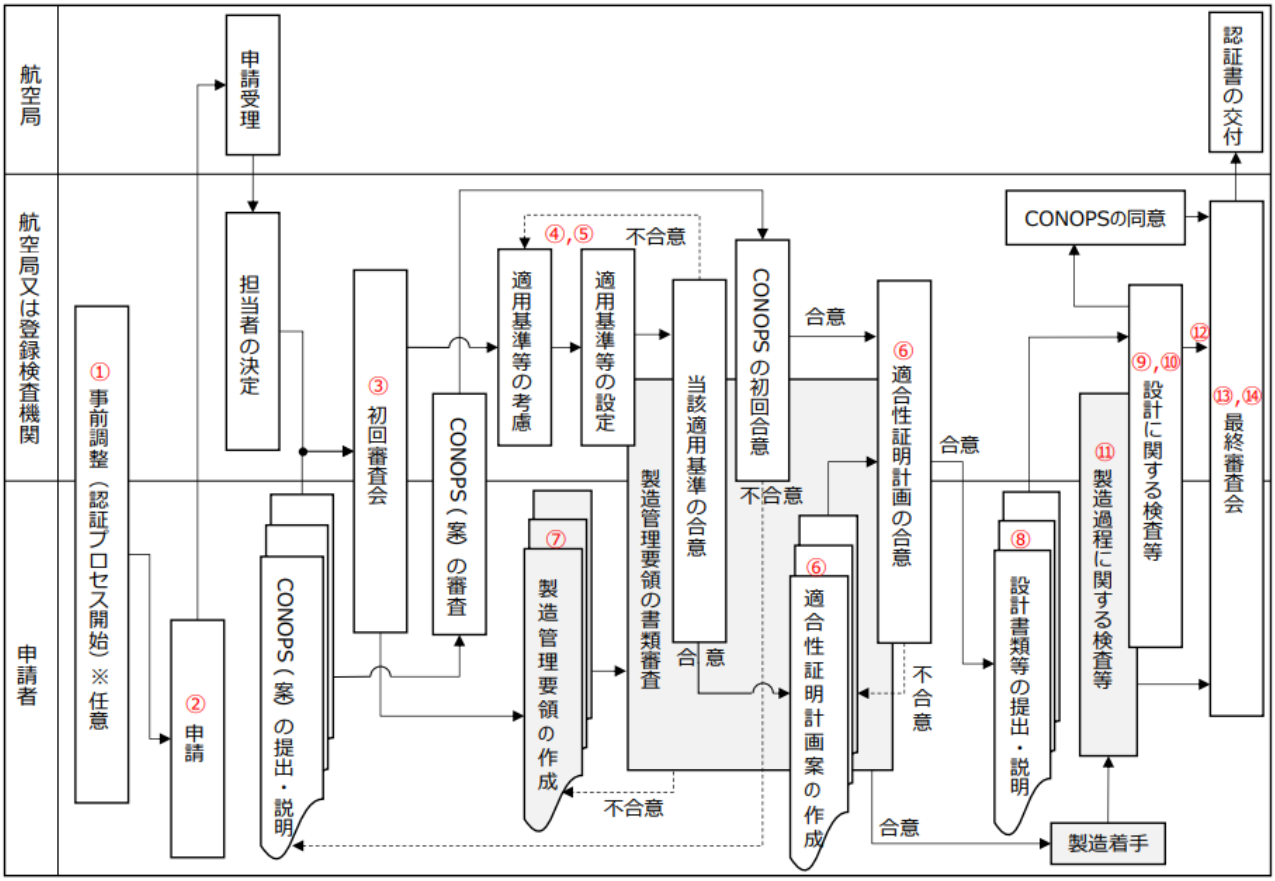


図 4.4-1 型式認証プロセスのフロー

出所）航空局ガイドライン

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

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・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 6～15 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。

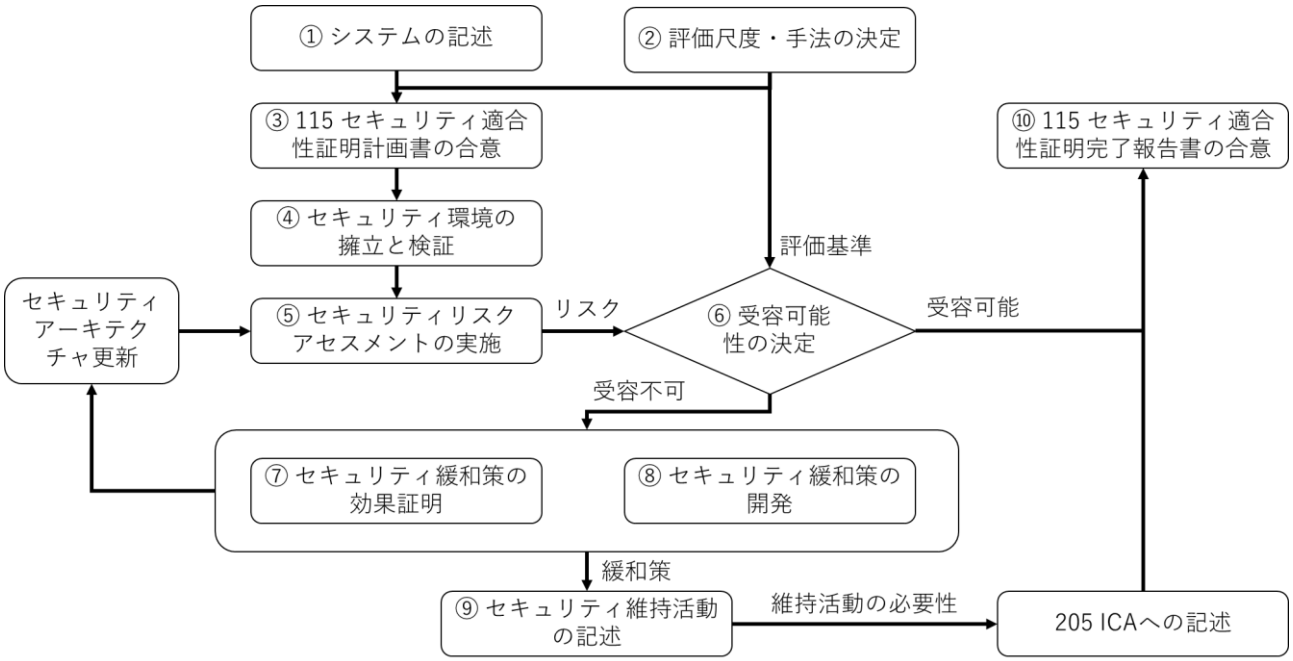


図 4.4-2 セクション 115 の認証活動プロセス

(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・実装したリスク緩和策が正しく、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。

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 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

プロセス	活動項目	M/R	手法および出力
要求 6: セクション 115 適合性証明計画書類の矛盾のない記述			
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	115 セキュリティリスクアセスメント適合性証明計画書
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	115 セキュリティリスクアセスメント適合性証明完了報告書

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、適合性証明計画書およびその中に含まれる適合性活動対照表として記述し、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[14], IEC 62443[1], ISO 27000 シリーズ[10][19]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[11] 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安全性に影響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。なお、無人航空機分野における一般的な情報システムにおけるサイバーセキュリティのガイドラインは経済産業省発行のドキュメント[20]に示されている。

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『計画外飛行（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』『計画外飛行』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。

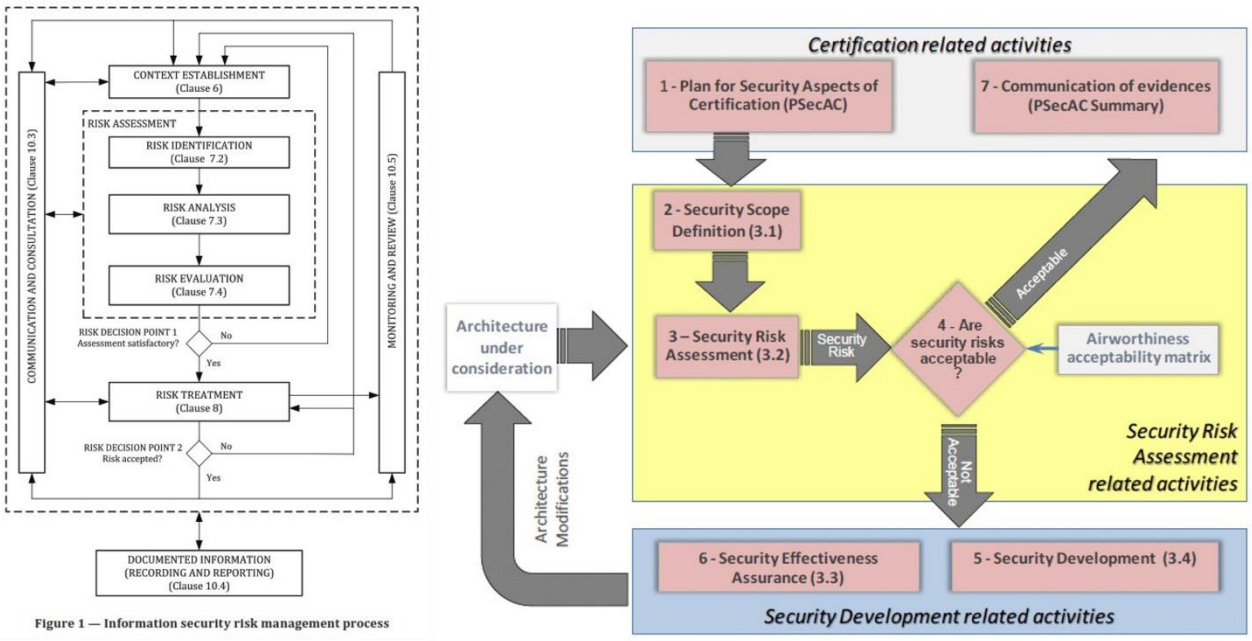


図 4.5-1 セキュリティリスクマネジメントモデル: ISO 27005(左) と DO-326A(右)

出所)ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks, https://www. iso.org/standard/80585.html
RTCA DO-326A / EUROCAE ED-202A – Airworthiness Security Process Specification, https://my.rtca.org/productdetails?id=a1B36000001IcfuEAC

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、セキュリティリスクアセスメントを行う方策を立てる。セキュリティリスクアセスメントの具体的な指針については、図 4.5-1 に、ISO27005 情報システムセキュリティリスクマネジメントモデル[10]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[4]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[4], DO-356A[11], 情報セキュリティのプロセスとしては ISO 27005:2022[10], IoT に関わる情報セキュリティの手法については NIST SP800-30[21], 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[1], 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[14](1)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。

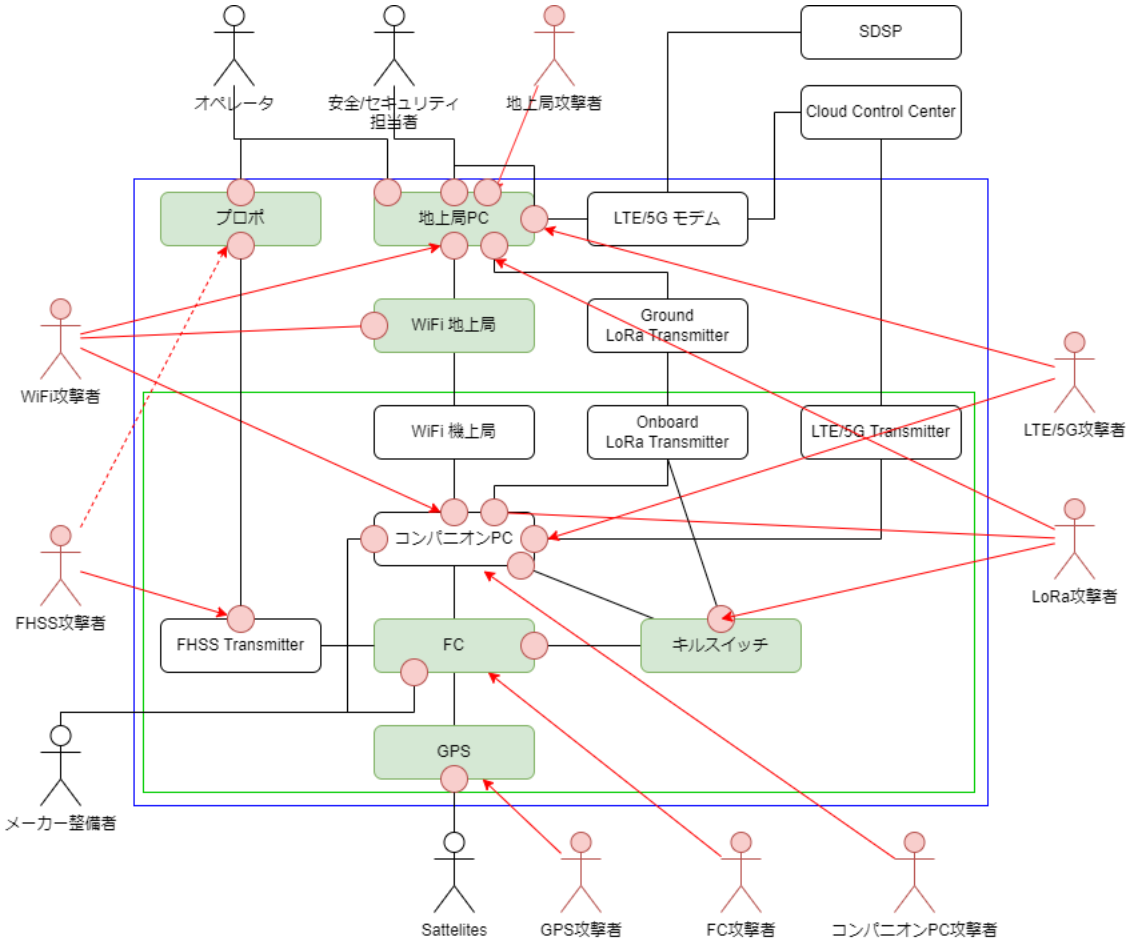


図 4.5-2 セキュリティ環境の模式図例

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)
  - Gate などがすべてコントロール下にある状態(内部者のみ)

攻撃者リストの例は表 4.5-1 のとおりとなる。

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

4) 資産リストの導出(活動 7)

図 4.5-2 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保護することを目論む。

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。

資産の ID の接頭語は[I.]とする。

資産リストの項目は以下のとおり。

- ID: 共通 ID［I.］＋［所在名］＋［資産名］
  - ［資産名］: 資産の素性・名称より
  - 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
- Description: 保護資産に対する記述
- 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

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: セキュリティ緩和策の存在(あればセキュリティ緩和策［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、セキュリティ緩和策によって、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。セキュリティ緩和策がない場合は『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[(7)]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(ISO/IEC 27001:2022[(19)]):

- 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[(7)])

- 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
- 緩和策: 脅威に対するセキュリティ対策の有無と具体的な緩和策 [O]の参照
- アクセスポリシー: 緩和策に対応するアクセスポリシー(ALLOWS/BLOCKS)
- 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	n/a	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	n/a	GCS サービス不能	n/a
AS.地上局 PC.USB	n/a	マルウェア混入	n/a	n/a	n/a	バックドア
AS.地上局 PC,SD カード	n/a	マルウェア混入	n/a	n/a	n/a	バックドア
AS.地上局 PC.Web	不正侵入	マルウェア混入	n/a	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	n/a	WiFi 設定情報漏洩	WiFi サービス不能攻撃	n/a
AS.地上局 PC.LoRa	n/a	テレメトリ情報改竄 キル情報不正送出	n/a	n/a	n/a	n/a
AS.地上局 PC.LTE	n/a	テレメトリ情報改竄	n/a	n/a	n/a	n/a
AS.プロポ.FHSS	FHSS 信号乗っ取り	FHSS 信号改竄	n/a	ホッピングパターン漏洩 ペアリング漏洩	n/a	n/a
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	n/a	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	n/a	ガイドソフト不能攻撃	n/a
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	n/a	n/a	n/a	n/a
AS.コンパニオン PC.SD カード	n/a	ファーム改竄 マルウェア混入	n/a	n/a	n/a	バックドア
AS.コンパニオン PC.USB	n/a	ファーム改竄 マルウェア混入	n/a	n/a	n/a	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	n/a	n/a	n/a	バックドア
AS.コンパニオン PC.LoRa	n/a	テレメトリ改竄	n/a	n/a	n/a	n/a
AS.コンパニオン PC.LTE	n/a	テレメトリ改竄	n/a	n/a	n/a	n/a
AS.FC.FHSS	n/a	FHSS 不正信号受信	n/a	n/a	n/a	n/a
AS.FC.SD カード	n/a	ファーム改竄 マルウェア混入	n/a	n/a	n/a	バックドア
AS.FC.USB	n/a	ファーム改竄 マルウェア混入	n/a	n/a	n/a	バックドア
AS.GPS	n/a	GPS 位置不正信号受信	n/a	n/a	n/a	n/a
AS.独立キルスイッチ	n/a	キル情報不正受信	キル否認	n/a	n/a	n/a

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］＋(［緩和策］or［脆弱性］)
  - ［緩和策］: 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))

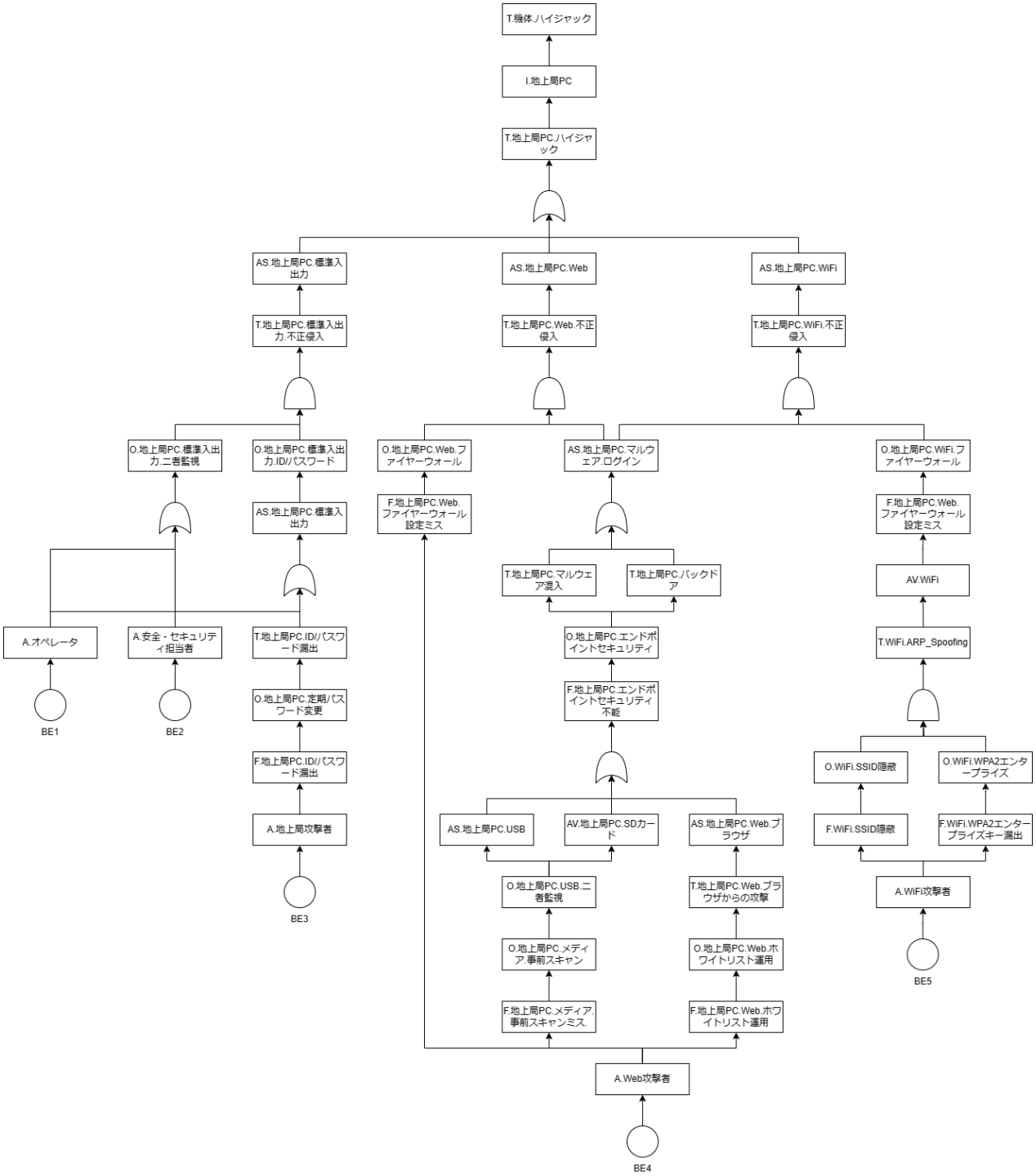


図 4.5-3　脅威木解析の一例: 地上局 PC へのハイジャックの脅威

- 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。

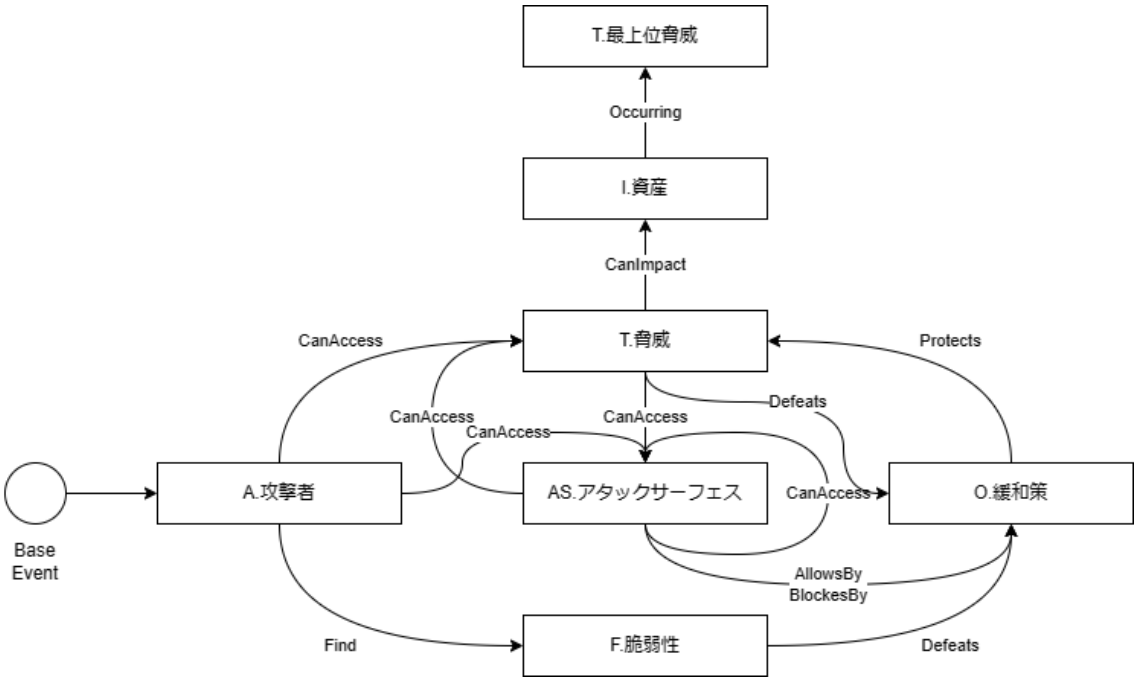


図 4.5-4 脅威木解析で扱われる各リストの結合の仕方

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(Base Event:BE) – 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(LoP Sum)
- 残存リスク重大度(RES = SEV-(LoP Sum+(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 カットセットリストの例

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	BE4	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	BE5	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

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。

未知の脆弱性を検出するには、ペネトレーションテストやファジングテスト、専門家によるチェックリストに基づくベースライン解析等がある。

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[(9)]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コストが掛かる。そのため、第二種型式認証では必須とすることは難しい。しかしながら、本テストは、リスクアセスメント全体に対するサイバーセキュリティの『D&R』であるとも考えられる。そのため、申請者が検査者との合意形成のために非常に有用であることから、推奨するものである。

(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[(18)]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リスク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 21384-3:2023[(22)]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。
    - フォレンジックは、証拠保全(発生状況時のログや挙動などのメモを取る)、データ解析(過去のログなどから復旧する)、調査(原因の特定および検証)および報告(再発防止のための調査結果の文書化)を行うことを含む。

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、完全性が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、他のソフトウェアとの間の整合性を検証する。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し、破損なくソフトウェアのロードが完了したことの確認を行う。
- 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セキュリティリスクアセスメント手法を検討する。

Appendix 1　115 セキュリティ適合性証明書類例

A.1.　型式認証対象とするモデルケース例

（1）　想定する機体・システムの例

※あくまで一事例であり、必ずしもこの通りに作成する必要はない

パーツ	型番	製造元	数量	備考
アンテナ	xxxx	A 社	1	
プロペラ	xxxx	B 社	4	サイズ：200mm
モーター	xxxx	自社	4	モーター対角：500mm
充電式バッテリー	xxxx	C 社	1	飛行時間：連続 xx 時間以上
GPS アンテナ	xxxx	D 社	1	
カメラ	xxxx	E 社	1	
スキッド	xxxx	G 社	1	

（2）　CONOPS 記載内容の例

※サイバーセキュリティに係る CONOPS のみ抜粋しているので詳細はセクション 001 を参照

（1）　気象及び電磁的外界条件：雷、雨、雪及び着氷状態、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は運用不可。電磁干渉（Electromagnetic Interference: EMI）及び高強度放射電界（High Intensity Radiated Field: HIRF）環境下においても運用不可。

（2）　運用時間：日中のみ

（3）　衝突回避：可視光／赤外線カメラ、ミリ波レーダ、LIDAR を搭載し、機体の外の様子（地上の人及び物件ならびに飛行経路周辺の他の航空機及び無人航空機）を監視。衝突回避装着は装備しておらず、手動操作にて衝突回避誘導する。

（4）　Pass/Fail Criteria（制御不能時*）：

- 操縦者の制御下での意図した非常着陸または墜落（想定飛行範囲内・計画内飛行*）。
- リカバリーゾーン*への管理された墜落（想定飛行範囲内・計画外飛行）
- 機体の不具合が生じ、操縦者が制御出来ない状態での意図した非常着陸または墜落（想定飛行範囲外・計画外飛行）。

（5）　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

（6）　最大通信距離：2km

（7）　ユースケース：橋梁下部構造などのドローンによる点検。

A.2. 115 セキュリティ適合性証明計画書

※ 本項は例示であり、記載内容や方法については検査者との合意が必要である。

Title	115 セキュリティ適合性証明計画書	
Ver.	Review Date	Contents
0.5	2023.10.1	
0.8	2023.11.1	
1.0	2023.12.1	

（1） 安全基準

安全基準はサーキュラーNo.8-001 115 サイバーセキュリティに準拠する。

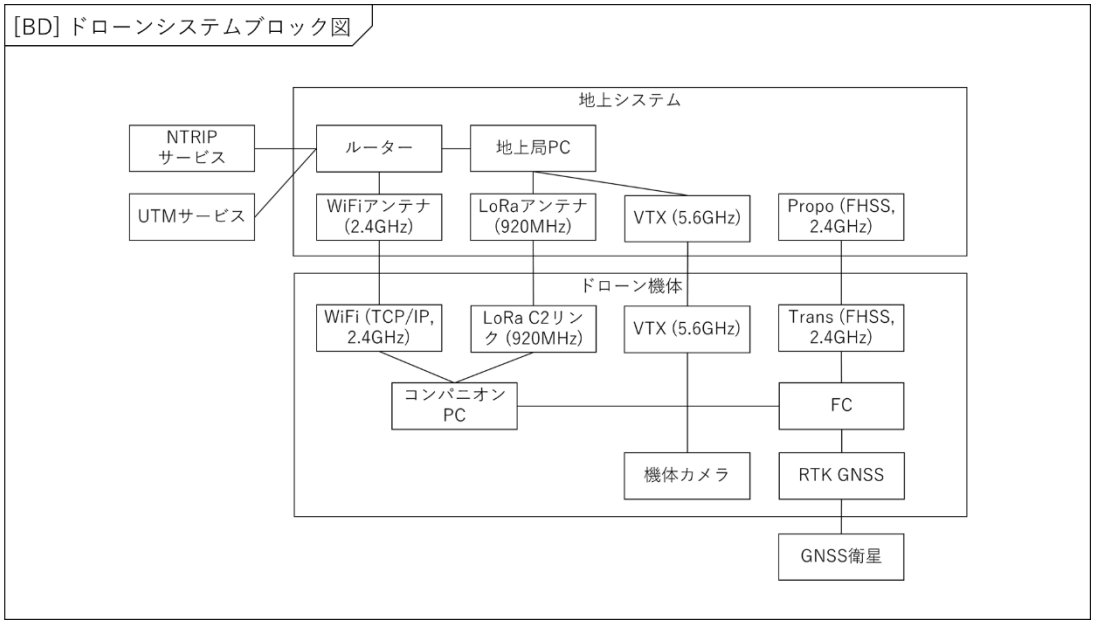
・115 サイバーセキュリティ

（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。

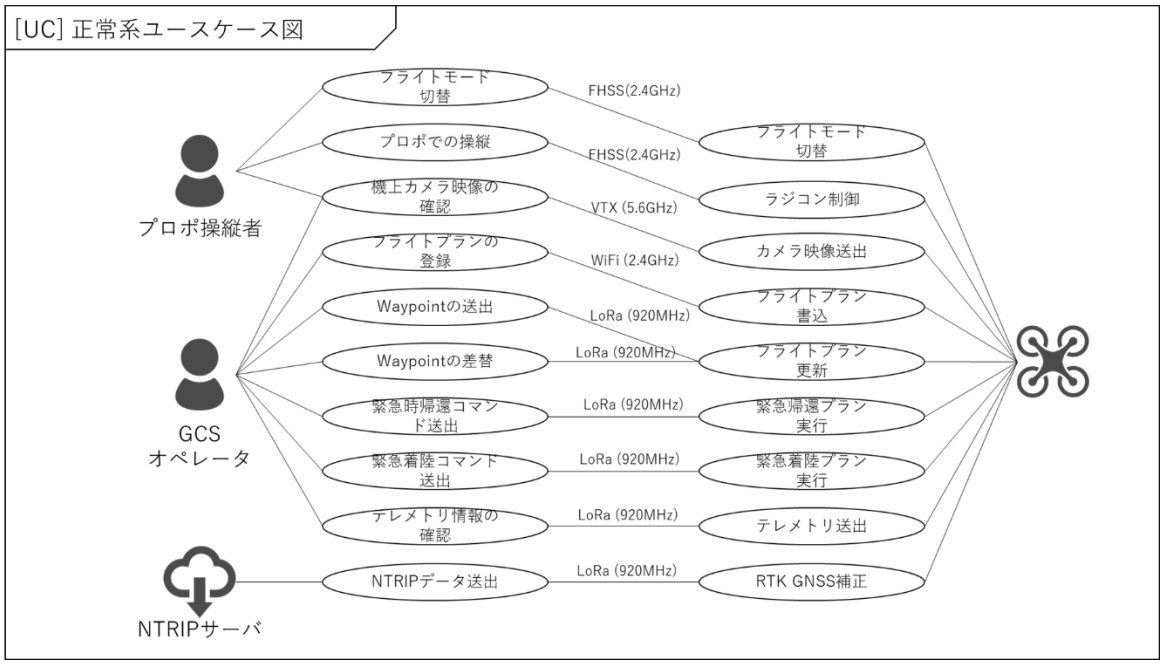
（b） 上記（a）項により必要とされる場合、セキュリティ対策が維持されるような手順および指示がICA に含まれなければならない。

（2） 機体及び運用の構成図

1） システム構成図



2） ユースケース図



（3） 適合方法(MoC)

適合方法については、航空局ガイドライン 第 3 部安全基準についてセクション 115 適合性証明方法(MoC)(a),(b)を基準として、4.4(3)に記されている表 4.4-2 に準拠する。

適合するための脅威事象は、4.5(2)2)に記載されている通り、

- 制御不能(Loss of Control)
- 計画外飛行(Loss of Flight) - 想定飛行範囲の逸脱
- ハイジャック(Hijack)

とする。

リスクアセスメントの評価尺度についても同様に、4.5(2)2)に記載されている通り、

リスク重大度(SEV): 0～5 までの 6 段階の尺度,上記脅威事象は、初期のリスク重大度が 5 となるように設定される。

- 各攻撃の脅威レベル(LoT): 1～5 までの 5 段階の尺度
- 各緩和策の防御レベル(LoP): 1～5 までの 5 段階の尺度
- 各資産 SEV: $SEV = LoT - LoP$

とし、脆弱性に対して攻撃者が攻撃する脅威によって、脅威事象が発生する可能性のある資産のリスク重大度が 0 以下となれば、リスクは受け入れ可能とする。

また、適合するための活動については適合性証明の活動計画で示される内容を行う。

（4） 適合性証明の活動計画

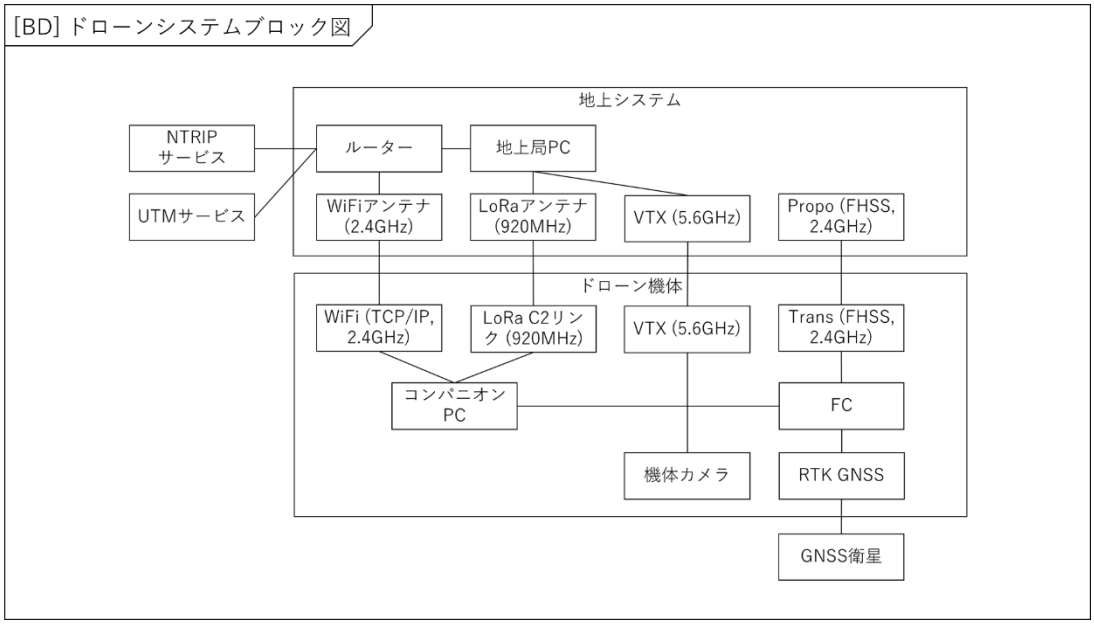
安全基準	活動項目(RMD-115 4.3 項の活動から抽出)	手法および出力
(a)	活動 1: システムの範囲の決定と記述	● システム構成図(本書(2)) ● ユースケース図(本書(2))
(a)	活動 3: 正常な運用におけるインターフェースとアクターの記述	
(a)	活動 4: 脅威事象と評価尺度の定義	● 脅威事象定義(本書(3)) ● リスク評価尺度定義(本書(3))
(a)	活動 5: 攻撃者と攻撃可能な干渉口の抽出	● 攻撃者を含むシステムブロック図 ● 攻撃者定義表 ● アタックサーフェスリスト
(a)	活動 6: セキュリティ環境におけるセキュリティ境界の定義	● セキュリティ環境・境界指示図
(a)	活動 7: 資産とリスク重大度の定義	● 資産-脅威リスト
(a)	活動 8: 具体的な脅威の抽出と脅威レベルの評価	● 脅威分析表
(a)	活動 9:既存の緩和策の抽出と防御レベルの評価	● 緩和策リスト ● 脆弱性クラスリスト
(a)	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	● 脅威木解析図
(a)	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分析表(カットセットリスト含む)
(b)	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	● セクション 205 への記述指示書 ● セクション 200 への記述指示書

A.3. 無人航空機システム・セキュリティリスクアセスメント報告書

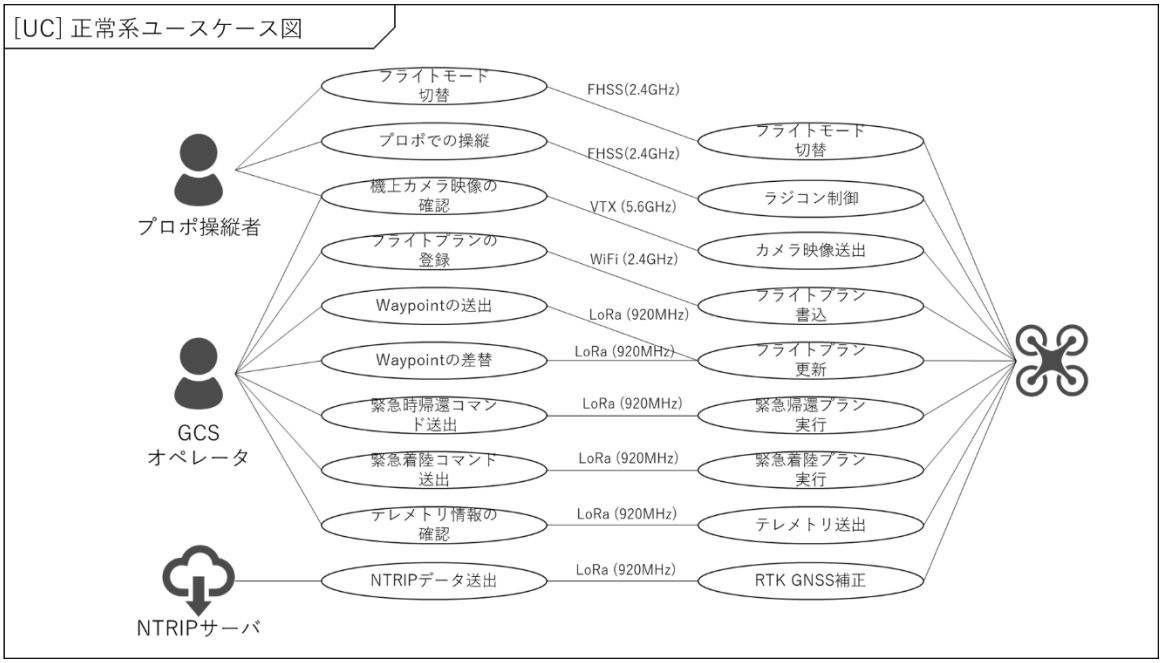
※ 本項は例示であり、記載内容や方法については検査者との合意が必要である。

Title	無人航空機システム・セキュリティリスクアセスメント報告書	
Ver.	Review Date	Contents
0.5	2023.10.1	
0.8	2023.11.1	
1.0	2023.12.1	

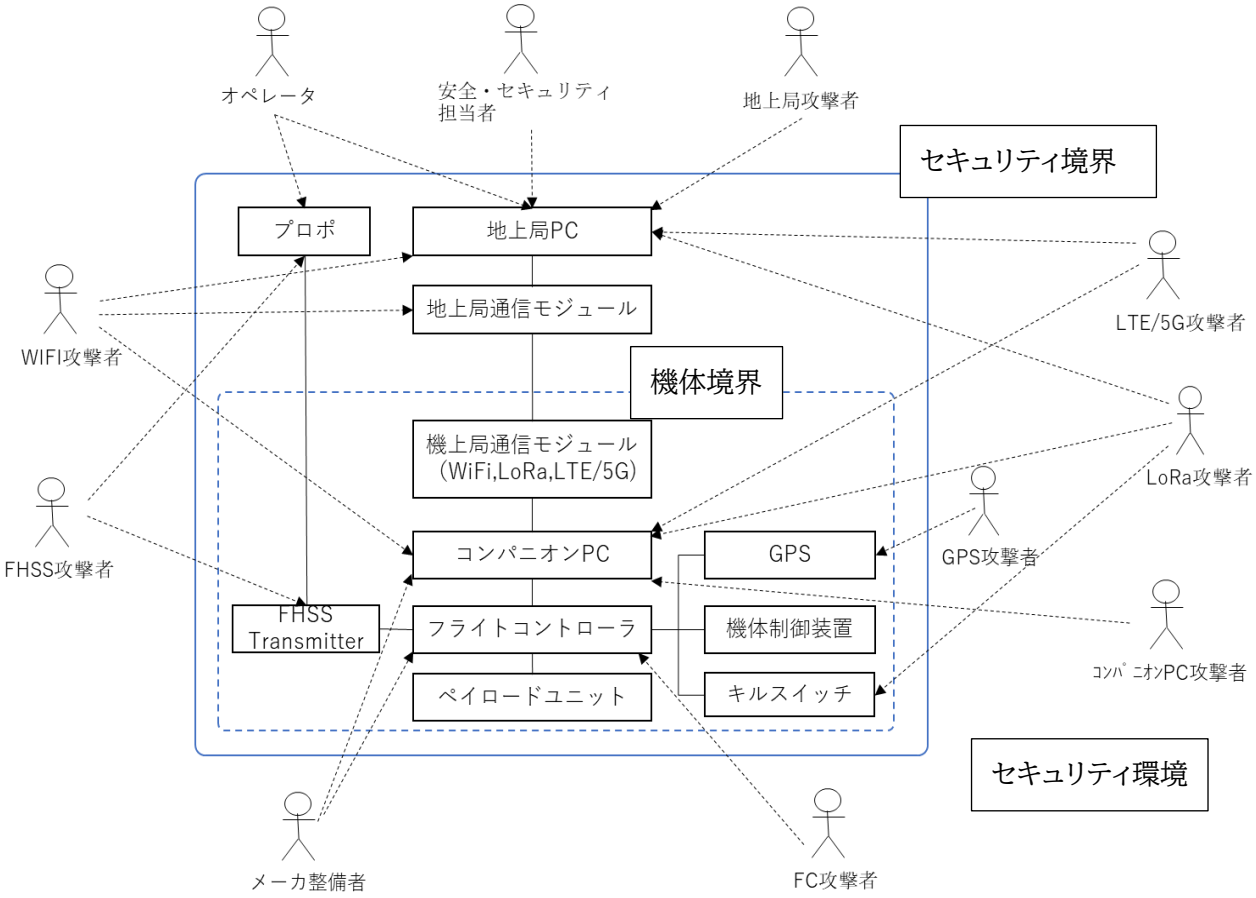
（1） システム構成図



（2） ユースケース図



（3） セキュリティ環境・境界指示図



（4） 攻撃者リスト

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

（5） 資産-脅威リスト

Asset	記述	SEV	Threat	Fatal Threat	資産の毀損観点		
					C 機密性	I 完全性	A 可用性
（例） 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		○	

（6） アタックサーフェスリスト

Access Point	記述	セキュリティ緩和策	アクセスコントロール	Access by:
(例)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
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	

（7） 脅威分析(STRIDE)

Access Point（AS:Attack Vector）	なりすまし	改竄	否認	漏洩	サービス拒否	権限昇格
(例)AS.地上局 PC.標準入出力	不正侵入	マルウェア混入	n/a	ID/パスワード漏洩	地上局 PC ハングアップ	バックドア

（8） 脅威リスト

脅威	記述	対処(緩和策)	ポリシー	Access By:
(例) 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 AV.地上局 PC.Web AV.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
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	
			ALLOWS	
			BLOCKS	

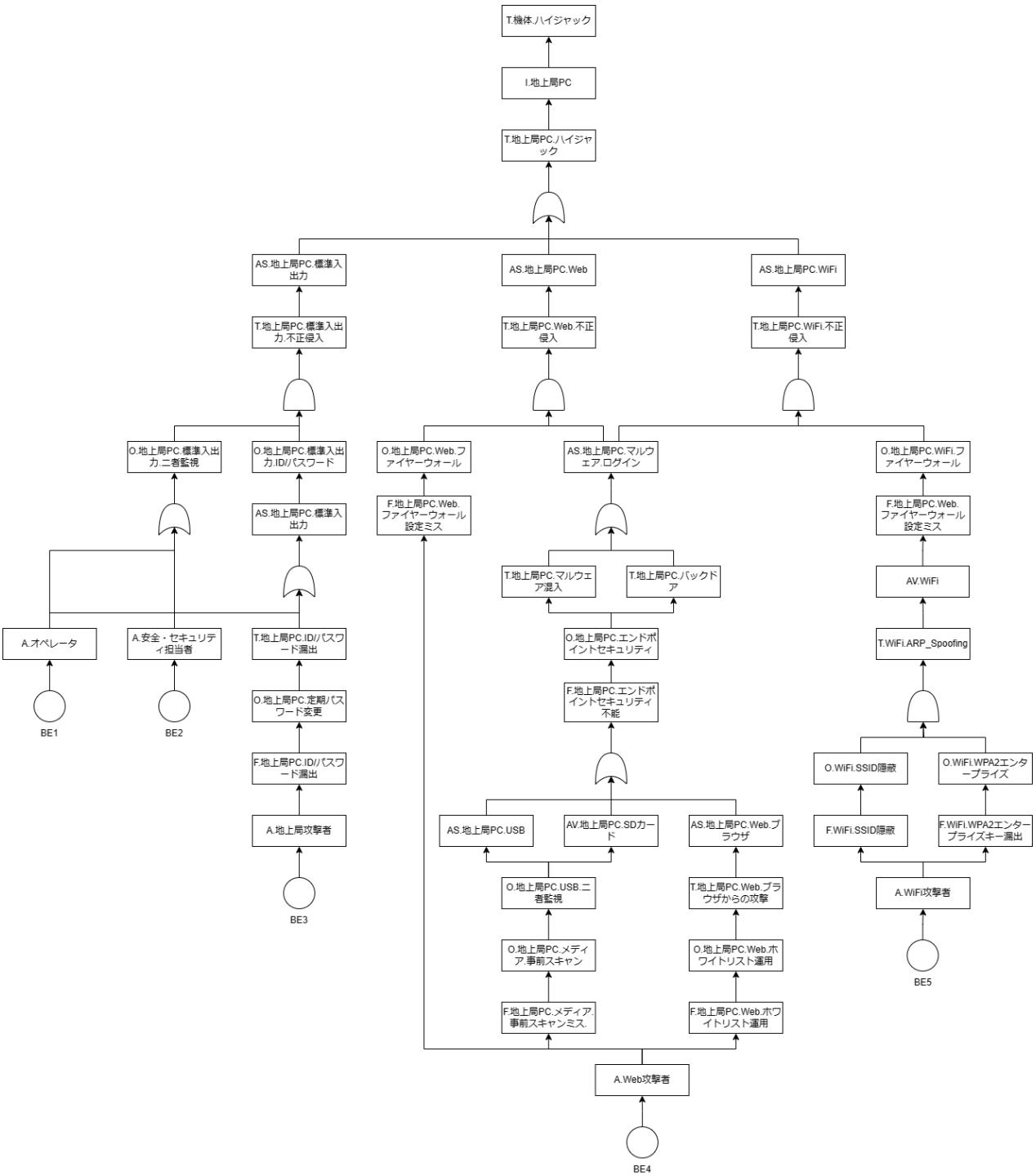
（9） 脆弱性クラスリスト

脆弱性クラス	記述	LoP	ICA	飛行規程	110
(例)F.地上局 PC.ID パスワード	弱いパスワード、ID の対	2	✓	✓	

（10） セキュリティ緩和策リスト

セキュリティ緩和策	記述	脆弱性クラスまたは脅威事象
(例)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

（11） 脅威木解析図


T.機体.ハイジャック
I.地上局PC
T.地上局PC.ハイジャック
AS.地上局PC.標準入出力
AS.地上局PC.Web
AS.地上局PC.WiFi
T.地上局PC.標準入出力.不正侵入
T.地上局PC.Web.不正侵入
T.地上局PC.WiFi.不正侵入
O.地上局PC.標準入出力.二者監視
O.地上局PC.標準入出力.ID/パスワード
O.地上局PC.Web.ファイヤーウォール
AS.地上局PC.マルウェア.ログイン
O.地上局PC.WiFi.ファイヤーウォール
AS.地上局PC.標準入出力
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.ファイヤーウォール設定ミス
T.地上局PC.マルウェア混入
T.地上局PC.バックドア
AV.WiFi
A.オペレータ
A.安全・セキュリティ担当者
T.地上局PC.ID/パスワード漏出
O.地上局PC.エンドポイントセキュリティ
T.WiFi.ARP_Spoofing
O.地上局PC.定期パスワード変更
F.地上局PC.エンドポイントセキュリティ不能
BE1
BE2
F.地上局PC.ID/パスワード漏出
O.WiFi.SSID隠蔽
O.WiFi.WPA2エンタープライズ
A.地上局攻撃者
AS.地上局PC.USB
AV.地上局PC.SDカード
AS.地上局PC.Web.ブラウザ
F.WiFi.SSID隠蔽
F.WiFi.WPA2エンタープライズキー漏出
BE3
O.地上局PC.USB.二者監視
T.地上局PC.Web.ブラウザからの攻撃
A.WiFi攻撃者
O.地上局PC.メディア.事前スキャン
O.地上局PC.Web.ホワイトリスト運用
BE5
F.地上局PC.メディア.事前スキャンミス.
F.地上局PC.Web.ホワイトリスト運用
A.Web攻撃者
BE4

（12） セキュリティリスク分析表

CU ID	Attacker	アタックサーフェス（AS）	Vulnerability(F)	Threat and Measure(O,T)	A. IoT	F. IoP	Asset SFV	LoP SLIM	Res. SFV
(例) 1	A.オペレーター	AS.地上局PC AS.プロポ	F.監視不備	O.監視 T.ハイジャック T.制御情報の改ざん	1	1	5	3	-2

（13） セクション 205 への記述指示

脆弱性	起こり得る脅威	記述内容
(例)F.地上局 PC.ID パスワード	T.地上局 PC.ハイジャック	パスワード設定の要求は、大文字、小文字、数字、記号をそれぞれ必ず 1 文字以上含む、特定のパターン(一般的に既知な単語など)に合致しない 8 文字以上の長さとする。

（14） セクション 200 への記述指示

脆弱性	起こり得る脅威	記述内容
F.WiFi.WPA2	T.機体.ハイジャック T.機体.制御不能	WiFi を接続する場合のルーター設定は、WPA2 を用いる必要がある。

A.4. 115 セキュリティ適合性証明完了報告書

※ 本項は例示であり、記載内容や方法については検査者との合意が必要である。

Title	115 セキュリティ適合性完了報告書	
Ver.	Review Date	Contents
0.5	2023.10.1	
0.8	2023.11.1	
1.0	2023.12.1	

以下の通り、115 セキュリティ適合性証明が完了したことを報告する。

(1) 活動計画実施対応表

安全基準	活動項目(RMD-115 4.3 項の活動から抽出)	手法および出力	確認日
(a)	活動 1: システムの範囲の決定と記述	● システム構成図(報告書(1)) ● ユースケース図(報告書(2))	2023.11.1
(a)	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		2023.11.1
(a)	活動 4: 脅威事象と評価尺度の定義	● 脅威事象定義(計画書(3)) ● リスク評価尺度定義(計画書(3))	2023.11.1
(a)	活動 5: 攻撃者と攻撃可能な干渉口の抽出	● 攻撃者を含むシステムブロック図(報告書(3)) ● 攻撃者定義表(報告書(4)) ● アタックサーフェスリスト(報告書(5))	2023.11.1
(a)	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	● セキュリティ環境・境界指示図(報告書(6))	2023.11.1
(a)	活動 7: 資産とリスク重大度の定義	● 資産-脅威リスト(報告書(7))	2023.11.1
(a)	活動 8: 具体的な脅威の抽出と脅威レベルの評価	● 脅威分析表(報告書(9))	2023.11.1
(a)	活動 9: 既存の緩和策の抽出と防御レベルの評価	● 緩和策リスト(報告書(10)) ● 脆弱性クラスリスト(報告書(11))	2023.11.1
(a)	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	● 脅威木解析図(報告書(12))	2023.11.1
(a)	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分析表(本書(2))	2023.11.1
(b)	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	● セクション 205 への記述指示書(本書(3)) ● セクション 200 への記述指示書(本書(4))	2023.11.1

（2） セキュリティリスク分析表

CU ID	Attacker	アタックサーフェス（AS）	Vulnerability(F)	Threat and Measure(O,T)	A. LoT	F. LoP	Asset SEV	LoP SUM	Res. SEV
(例) 1	A.オペレーター	AS.地上局PC AS.プロポ	F.監視不備	O.監視 T.ハイジャック T.制御情報の改ざん	1	1	5	3	-2

（3） セクション 205 への記述指示

脆弱性	起こり得る脅威	記述内容
(例)F.地上局 PC.ID パスワード	T.地上局 PC.ハイジャック	パスワード設定の要求は、大文字、小文字、数字、記号をそれぞれ必ず 1 文字以上含む、特定のパターン(一般的に既知な単語など)に合致しない 8 文字以上の長さとする。

（4） セクション 200 への記述指示

脆弱性	起こり得る脅威	記述内容
(例)F.WiFi.WPA2	T.機体.ハイジャック T.機体.制御不能	WiFi を接続する場合のルーター設定は、WPA2 を用いる必要がある。

Appendix 2 脅威分析モデル STRIDE

B.1. STRIDE モデルの解説

STRIDE モデル[7]は、コンピューターシステムに対する一般的な脅威を提示し、攻撃可能な部位や経路において、脅威がどのように影響を及ぼすかを算出できる。また、同時に、それに対応するための対策の基本概念も同時に適用可能である。一方で、STRIDE モデルは大きい括りとして纏められていることから、各モデルに紐づく詳細な脅威をあらかじめ想起しておく必要がある(SQL Injection など)。なお、詳細な脅威についての傾向脅威などは MITRE が公開している CAPEC[23]などが参照できる。

また、STRIDE モデルなどを用いて脅威分析を行うためには、データフローダイアグラム(DFD)などによってシステムが可視化・定義されている必要がある。脆弱性の分析よりも開発工程の上流で解析できることから、あらかじめどのような脅威が潜んでいるかを算出することが可能である。また、効率的に STRIDE による脅威分析を行うためには、DFD の要素すべてに対して STRIDE を適用して脅威を導き出す STRIDE-per-Element という手法と、DFD 内の Trust Boundary(信頼境界線)と交差するデータフローを取り出し、"Origin", "Destination", "Interaction"に着目して脅威を導出する STRIDE-per-Interaction という手法がある[24]。事前に綿密なデータフローが作成されており、攻撃経路の特定やセキュリティ境界が策定されていれば、STRIDE-per-Intersection を用いる方法が無駄は少ないが、網羅的に行う場合は STRIDE-per-Element を用いるのが好ましい。

- STRIDE による脅威事象のモデリングとその対応
  - 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)

B.2. STRIDE による無人航空機システムの解析例

STRIDE による解析の例として、図 B.2-1 で示される無人航空機システムに対して、STRIDE による脅威の解析を行った例を表 B.2-1 に示す。

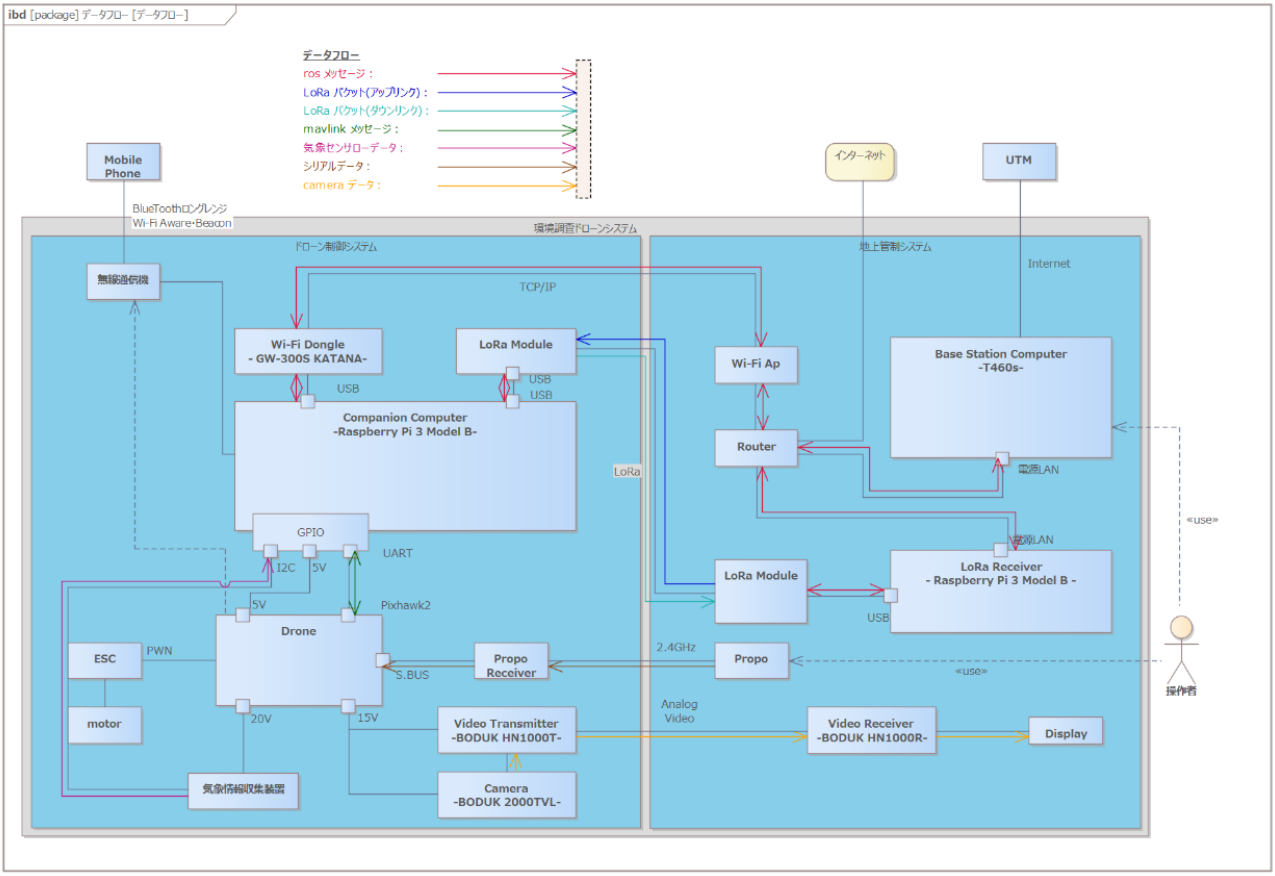


図 B.2-1 解析を行う無人航空機システム

表 B.2-1 STRIDE による脅威の解析例

アタックサーフェス	S(Spoofing:なりすまし)	T(Tampering:改ざん)	R(Repudiation:否認)
地上管制システム(直接操作／Web操作／マルウェア)	パスワードが流用し、不正に利用される ①不正な情報を送受信 ②不正なプログラムを実行 ③不正な応答	直接操作・マルウェアによる情報の改ざん。 ①システム設定の変更 ②ドローンから来る情報の書き換え ③送信情報の書き換え ④ログの削除	直接操作・マルウェアによる情報取得データの否認 ①ドローンからの正常な情報を異常とし、データを拒否させる
地上管制システムから飛行経路をドローンに送信するまでの通信経路	n/a	WiFi/LoRa に対する攻撃により、改ざんしている情報を送信 ①飛行経路の改ざん	n/a
ドローンから地上管制システムまでの情報受信経路	n/a	n/a	n/a
プロポからドローンまでの無線経路	n/	情報を改ざんしたデータを送信。 ①不正に改ざんしたプロポ情報を送信	n/a

アタックサーフェス	S(Spoofing:なりすまし)	T(Tampering:改ざん)	R(Repudiation:否認)
ドローン([地上]直接操作/マルウェア)	パスワードが流用し、不正に利用される ①FC/ラズパイデータの不正操作	直接操作・マルウェアによるドローン内部の改ざん ①設定ファイルの改ざん ②プログラムの改ざん ③送信情報の書き換え ④ログの削除	直接操作・マルウェアによる情報取得データの否認。 ①地上システムからの情報をすべて異常とし、データを拒否させる

アタックサーフェス	I(Information Disclosure:情報漏洩)	D(Denial of Service:サービス拒否)	E(Elevation of Privilege:特権の昇格)
地上管制システム(直接操作／Web操作／マルウェア)	不正操作による情報漏洩。 ①システム情報の漏洩 ②ログ情報の漏洩	地上システムの遅延・停止 ①プログラムの処理能力を低下	地上管制システムの権限を奪う ①不正な情報を送信 ②不正なプログラムを実行
地上管制システムから飛行経路をドローンに送信するまでの通信経路	WiFi/LoRa に対する攻撃により、情報を不正入手する。 ①飛行経路の取得により、ドローン経路を不正入手	WiFi/LoRa に対する攻撃により、送信に遅延をかける。 ①飛行経路送信に遅延をかける	n/a
ドローンから地上管制システムまでの情報受信経路	WiFi/LoRa に対する攻撃により、情報を不正入手する。 ①機体情報(機体映像・機体制御状態など)を不正入手	WiFi/LoRa に対する攻撃により、通信に遅延をかける。 ①機体情報受信に遅延をかける	n/a
プロポからドローンまでの無線経路	n/a	無線に対する攻撃により、遅延をかける。 ①プロポ情報送信に遅延をかける	n/a
ドローン([地上]直接操作／マルウェア)	不正操作による情報漏洩。 ①システム情報の漏洩 ②ログ情報の漏洩	ドローンシステムの遅延・停止。 ①プログラムの処理能力を低下	ペイロードユニットの特権を奪う。 ①正常な操作命令でも動作しない ②想定とは違う動作を行う

Appendix 3 各セクション特有の用語集

#	用語	解説	参考
1	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[25]
2	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[25]
3	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[26]
4	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[26]
5	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[27] FAA AC No.20-174[28]
6	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。	
7	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 [4]
8	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[25]
9	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。	
10	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 [4]
11	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 [4]
12	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 [4]
13	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 [4]

#	用語	解説	参考
14	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 [4]
15	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[29]
16	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[30]
17	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 [4]
18	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	
19	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[25]
20	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 [4]
21	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	
22	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。	
23	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[31]
24	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。	
25	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。	
26	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 [4]

#	用語	解説	参考
27	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[32]
28	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。	
29	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。	
30	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[33]
31	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[7]
32	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[25]
33	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	
34	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。	
35	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	
36	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[34]
37	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[31]
38	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 [35]
39	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 [35]
40	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[36]

#	用語	解説	参考
41	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。	
42	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[37]
43	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	TechTarget[38]
44	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[29]
45	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	
46	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 [4]
47	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 [4]
48	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。	
49	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 [35]
50	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[39]
51	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[39]
52	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 (29)

#	用語	解説	参考
53	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。	
54	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 [4]
55	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.2.9[40]
56	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	
57	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。	
58	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[29]
59	ミドルウェア （Middleware）	アプリケーション・ソフトウェアとそのインフラストラクチャーの複雑さを隠蔽したままの方法で、アプリケーション・ソフトウェアにサービスを提供する、アプリケーションに依存しないコンピューター・プログラム	IEC 60050 - International Electrotechnical Vocabulary [41] : 871-05-09
60	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 [4]
61	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 [4]
62	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。	
63	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[29]
64	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[21]
65	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[33]
66	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 (38)
67	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[33]
68	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	

#	用語	解説	参考
69	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。	
70	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[25]
71	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 explains blog[43]
72	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[21]
73	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[25]
74	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[44]
75	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。	
76	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[17]
77	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 blog[45]
78	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 [4]
79	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 [4]
80	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[29]

#	用語	解説	参考
81	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 [4]
82	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 [4]
83	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[25] RTCA DO-326A [4]
84	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。	
85	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 15288:2023[46] NIST SP 800-95[37]
86	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 [4]
87	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 [35]
88	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 15288:2023[46]
89	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 [35]
90	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。	
91	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。	
92	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[29]
93	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[29]
94	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 [35]

#	用語	解説	参考
95	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 [4]
96	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[29]
97	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 [4]
98	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 [4]
99	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。	
100	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	
101	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。	
102	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 [4]
103	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。	
104	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 [4]
105	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 [4]
106	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 [4]
107	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 [4]

Appendix 4 関連文書

(1) 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 12 月 2 日,
https://www1.mlit.go.jp/common/001574425.pdf

(2) 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。同年 12 月 2 日付け国空機第 645 号までの改正を含む。),
https://www.mlit.go.jp/koku/content/001520547.pdf

(3) 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

(4) RTCA DO-326A / EUROCAE ED-202A – Airworthiness Security Process Specification,
https://my.rtca.org/productdetails?id=a1B36000001IcfuEAC

(5) 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

(6) 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

(7) Microsoft Learn, The STRIDE Threat model,
https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

(8) 独立行政法人情報処理推進機構(IPA), 共通脆弱性評価システム CVSS v3 概説,
https://www.ipa.go.jp/security/vuln/scap/cvssv3.html

(9) IPA ファジング活用の手引き,
https://www.ipa.go.jp/security/vuln/fuzzing/ug65p9000001986g-att/000057652.pdf

(10) ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks,
https://www.iso.org/standard/80585.html

(11) RTCA DO-356A / EUROCAE ED-203A – Airworthiness Security Methods and Considerations,
https://my.rtca.org/productdetails?id=a1B36000006xdusEAA

(12) ASTM F3201-16 – Standard Practice for Ensuring Dependability of Software Used in Unmanned Aircraft Systems (UAS),
https://www.astm.org/f3201-16.html

(13) ASTM F3532-23 - Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions, https://www.astm.org/f3532-23.html
(14) ISO/SAE 21434:2021 – Road vehicles – Cybersecurity engineering, https://www.iso.org/standard/70918.html
(15) 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
(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) IEC 61508:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Parts 1 to 7, https://webstore.iec.ch/publication/22273
(18) RTCA DO-355A / EUROCAE ED-204A – Information Security Guidance for Continuing Airwhortiness, https://my.rtca.org/productdetails?id=a1B1R00000GshsyUAB
(19) ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements, https://www.iso.org/obp/ui/#!iso:std:82875:en
(20) 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.go.jp/policy/mono info service/mono/robot/pdf/drone cyber secirity guideline Ver1.0.pdf
(21) NIST SP800-30 Rev.1 – Guide for Conducting Risk Assessments, https://doi.org/10.6028/NIST.SP.800-30r1
(22) ISO 21384-3:2023 - Unmanned aircraft systems, - Part 3: Operational procedures, https://www.iso.org/standard/80124.html
(23) MITRE, Common Attack Pattern Enumeration and Classification (CAPEC™), https://capec.mitre.org/
(24) FFRI.inc, “STRIDE の変化形とセキュリティ要件で導き出す脅威分析手法,” https://www.ffri.jp/assets/files/monthly research/MR201610 STRIDE Variants and Security Requirements-based Threat Analysis JPN.pdf
(25) 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
(26) OMG Unified Modeling Language, https://www.omg.org/spec/UML/2.5/PDF

(27) SAE ARP4754A – Guidelines for Development of Civil Aircraft and Systems, https://www.sae.org/standards/content/arp4754a/
(28) FAA, Advisory Circular : 20-174, https://www.faa.gov/documentLibrary/media/Advisory Circular/AC 20-174.pdf
(29) NIST SP800-53 Rev.5 – Security and Privacy Controls for Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-53r5
(30) FEMA, Cybersecurity Glossary, https://www.fema.gov/about/glossary
(31) RTCA DO-178C / EUROCAE ED-12C – Software Considerations in Airborne Systems and Equipment Certification, https://my.rtca.org/productdetails?id=a1B36000001IcmqEAC
(32) ISO/IEC/IEEE 26512:2018 - Systems and software engineering - Requirements for acquirers and suppliers of information for users, https://www.iso.org/standard/72088.html
(33) NIST SP 800-12 Rev. 1 – An Introduction to Information Security, https://doi.org/10.6028/NIST.SP.800-12r1
(34) ISO/TR 12489:2013 - Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems, https://www.iso.org/standard/51456.html
(35) CNSSI 4009-2022 – Committee on National Security Systems (CNSS) Glossary, https://www.niap-ccevs.org/Ref/CNSSI_4009.pdf
(36) NIST IR 8323 Rev. 1 - Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services, https://csrc.nist.gov/pubs/ir/8323/r1/final
(37) NIST SP 800-95 – Guide to Secure Web Services, https://doi.org/10.6028/NIST.SP.800-95
(38) TechTarget, Security – Definition: Cyber Hijacking, https://www.techtarget.com/searchsecurity/definition/hijacking
(39) NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security, https://doi.org/10.6028/NIST.SP.800-82r3
(40) 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
(41) IEC 60050 – International Electrotechnical Vocabulary, https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=871-05-09

(42) ISO 9001:2015 – Quality management systems – Requirements, https://www.iso.org/standard/62085.html
(43) EXIDA, Explains Blog, Back to Basics 17 - PFH (Probability of Failure on Demand per Hour), https://www.exida.com/Blog/back-to-basics-17-pfh
(44) ISO/IEC Guide 51:2014 – Safety aspects – Guidelines for their inclusion in standards, https://www.iso.org/standard/53940.html
(45) Norton blog, What is a script kiddie? Definition + examples, https://us.norton.com/blog/emerging-threats/script-kiddie
(46) ISO/IEC/IEEE 15288:2023 – Systems and software engineering – System life cycle processes, https://www.iso.org/standard/81702.html

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 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、レビュワーの構成員名簿は本冊(RMD、Rev.01)Appendix4 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。