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

非耐空性の領域における情報セキュリティの対応指針

2022 年 3 月

国立研究開発法人新エネルギー・産業技術総合開発機構

本ガイドラインは、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「ロボット・ドローンが活躍する省エネルギー社会の実現プロジェクト」（JPNP17004）の結果得られたものです。

目次

1 背景と目的

1.1 背景～ドローン分野におけるセキュリティの現状と課題

1）無人航空機分野における社会的、政策的背景

近年、無人航空機分野は市場規模としても著しい成長を示しており、2020 年度には前年度比37%増の 1932 億円に拡大し、2025 年度には 6427 億円（2019 年度の約 4.6 倍）に達すると見込まれている[1]。産業分野としても、物流、防犯、農業、点検、建設など、幅広い分野へ利用領域が拡大しており、無人航空機による業務の効率化や、省エネルギー化が期待されている。こうした状況を踏まえ、小型無人機に係る環境整備に向けた官民協議会は 2020 年 4 月に「空の産業革命に向けたロードマップ 2019」を公開し、2021 年度までに無人地帯における目視外飛行（レベル３）、2022 年度以降に有人地帯での目視外飛行（レベル４）の実現に向けた計画が示されている。NEDO 事業においても、レベル４の実現に向けて、小項目「６）第三者上空での飛行に向けた無人航空機の性能評価基準の研究開発」が 2018 年度～2019 年度で実施された。

2）無人航空機におけるセキュリティの現状

一方で無人航空機におけるセキュリティという面では、既に多くの ICT(情報通信)技術が組み込まれ、IoT 機器と同様の高度化、自動化が進行している。我が国における IoT（Internet of Things）領域の政策としては、平成 28 年 1 月 22 日に閣議決定された「第５期科学技術基本計画」において、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」を提唱している。「Society5.0」及び、様々なつながりによって新たな付加価値を創出する「Connected Industries」では、IoT によって製品やサービスに対する新たな価値の創出が期待される一方、企業やサプライチェーンについては、より複雑化したサイバーセキュリティ上の脅威に対応していく必要がある。また国際的なセキュリティカンファレンスである「Blackhat」や「DEFCON」においても、アーキテクチャ上の脆弱性の指摘や、ハッキング事例が示されており、無人航空機分野においても、こうした状況への対応が急務である。

具体的なセキュリティ対策の指針としては、本書に先行して 2021 年 4 月には「ドローンセキュリティガイド 第 2 版」[2]が、また類似領域としてはロボットを対象とした「サービスロボット・セキュリティガイドライン」[3]が 2019 年 5 月に公開されている。また、広く IoT 分野を対象としたセキュリティ基準としては、一般社団法人重要生活機器連携セキュリティ協議会（以下、CCDS）が、2019 年 10 月に IoT 機器を対象としたセキュリティ基準のガイドライン「IoT 分野共通セキュリティ要件ガイドライン 2019 年版」を公開すると共に、民間主導による認証制度「サーティフィケーションプログラム」[4]を開始している。

---

[1] インプレス総合研究所 「ドローンビジネス調査報告書 2020」

[2] 一般社団法人セキュアドローン協議会 「ドローンセキュリティガイド 第２版」

[3] 公立大学法人会津大学、TIS 株式会社、ネットワンシステムズ株式会社「サービスロボット・セキュリティガイドライン 第１版」

[4] 一般社団法人 重要生活機器連携セキュリティ協議会
https://www.ccds.or.jp/certification/index.html

1.2 本書の目的

本書は、無人航空機を中心に、その制御に関わる関連機器や、サービス用のクラウド（サーバ）を対象とし、その開発、生産、販売、サービス運用におけるセキュリティ対策の指針となる事項を示すものである。

1.3 本書の対象範囲

本書の対象範囲は、無人航空機システムの下記構成要素を対象とし、非耐空性のセキュリティ（Non-Airworthiness Security）に関するリスク分析の方法論や指針をフレームワークとして提示し、対象領域において必要とされるセキュリティ対策事項を示すことで、無人航空機分野の対象事業者が提供するそれぞれの製品やサービスにおけるセキュリティの検討に資するものである。

本書で対象とする構成要素

- 無人航空機本体（以降ドローン本体とする）
- 地上制御局に相当するプロポやトランスミッター、グランドコントロール・ステーション（以降 GCS とする）
- 無人航空機システムメーカが運用するクラウドシステム（メンテナンス機能）及び、無人航空機のデータを活用するサービス事業者が運用するクラウドシステム

※ドローン本体、地上制御局は産業利用を想定した量産品を対象とし、特殊用途の機体（開発中の機体や実験に使用するために試験的に飛行が必要なもの等）は対象に含まれない。

※無人航空機運航管理システム（以降 UTM とする）については、2018 年 DRESS プロジェクト[5]において研究開発が実施されており、本書の対象外とする。

本書で対象とするセキュリティ領域の定義

- 無人航空機システムの製品ライフサイクルとして、次の各段階を対象とする。
- 「企画」、「設計・製造※1」、「評価」、「運用」、「廃棄※2」における、セキュリティ管理上のリスク及びその対策

  ※1）「設計・製造フェーズ」におけるサプライチェーン上のセキュリティリスク及びその対策を含む

  ※2）廃棄あるいは墜落などに起因する情報窃取に対する無人航空機システムのセキュリティリスク及びその対策を含む
- なお、本書は構成要素（表 2-1）において取り扱われる「情報※３」のセキュリティリスクを対象としており、無人航空機の安全性（耐空性）に影響を与えるリスクについては取り扱わないものとする。

  参考とした航空機分野において定義された耐空性の対象範囲を図 1-1 に示す。

  ※３）構成要素間の伝送データ、各構成要素内データなど。

[5] 2018 年 DRESS プロジェクト「無人航空機の運航管理システム及び衝突回避技術の開発」

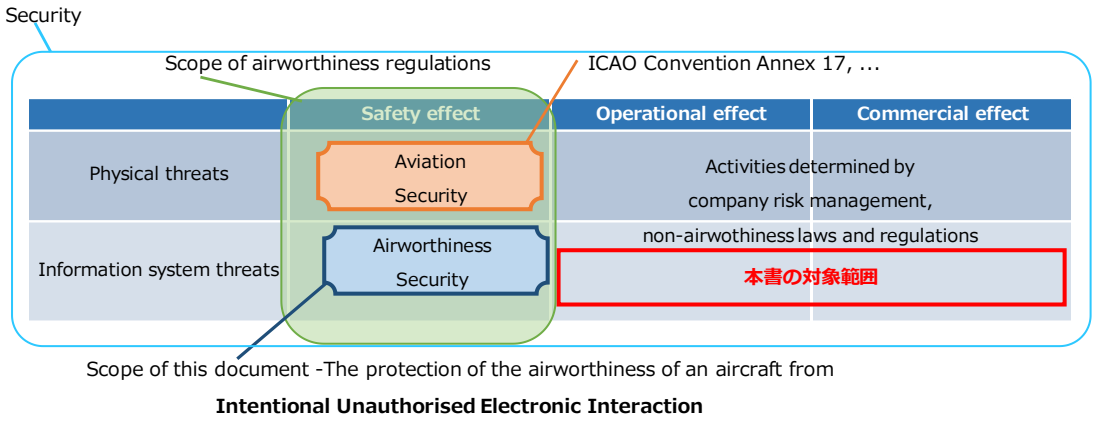


図 1-1 DO-356A が定義する耐空性に関するセキュリティの範囲[6]と、本書の対象スコープ

■本書が対象とする非耐空性のセキュリティ（Non-Airworthiness Security）の定義

本書において対象範囲とする、無人航空機の耐空性に影響しないセキュリティ領域を非耐空性のセキュリティ（Non-Airworthiness Security）と定義する。

- What：無人航空機システムにおいて実装されるソフトウェアや、取り扱われるデータが
- When：「企画」、「設計・製造」、「評価」、「運用」、「廃棄」に至るまで
- Where：電子情報及び、電子通信における経路上において
- Who：第三者や外部、あるいは内部から
- Why：意図的または随意的な
- How：攻撃を受けた場合や過失により
- Event：経済的損失、社会的信用の失墜、法制度への抵触、プライバシ侵害、セキュリティ機能の低下につながる

1.4 本書の対象者

本書は、上記の対象範囲において開発、生産、販売を行う無人航空機システムメーカ（以降メーカと呼称）、部材（ハードウェア及びソフトウェア部品）の提供を行うサプライヤ、無人航空機システムのデータを活用したサービス事業者（サービスプロバイダ）を対象とする。また、副次的な対象者として、セキュリティの検証を行う検証サービス事業者を対象とする。無人航空機分野におけるステークホルダーマップについては、第２章の図 2-4 に示す。

1.5 本書の構成

第１章においては、本書の背景や目的、対象範囲、対象者、用語定義を示す。

---

[6] RTCA DO-356A "Airworthiness Security Methods and Considerations"
https://my.rtca.org/NC__Product?id=a1B36000006xdusEAA

第２章においては、無人航空機のシステムモデルイメージを定義し、システムモデル上のデータフローから取り扱われるデータを明確化する。また、無人航空機分野におけるステークホルダーとユースケースを定義し、取り扱われるデータを明確化する。（取り扱われるデータは本書の第 4.2 節において守るべき資産の検討へつながる）

第３章では、無人航空機分野に関連する法令や、ハッキング・脆弱性事例、将来的な技術動向、航空機分野における情報セキュリティ対策事項、個人情報保護やプライバシ保護上の対策事項の調査結果を示し、無人航空機分野として考慮すべきセキュリティ対策事項を導出する。

第４章では、第２章の無人航空機のシステムモデルに対するリスク分析プロセスや、実施例を示す。

第５章では、第３章の調査結果及び、第４章のリスク分析結果を踏まえ、無人航空機システムの構成要素別（無人航空機、地上制御局、クラウドなどの機器）にセキュリティ要件を示す。また、第３章の調査結果及び、製品ライフサイクルに対するリスク分析結果を踏まえ、ステークホルダー別（メーカ、サプライヤ、サービス事業者）別に、組織の活動に関するセキュリティ要件を示す。

Appendix_A では、第５章のセキュリティ要件について、国内外の主要なガイドラインとの対応関係を示す。

Appendix_B では、第４章のリスク分析プロセスの参考として、リスクレベルの検討例を示す。

Appendix_C では、本書で使用した用語に関する用語集を示す。

Appendix_D では、本書において参考、参照した規格、ガイドライン文書を示す。

本書の構成及び、各章の関係性を、図 1-2 に示す。

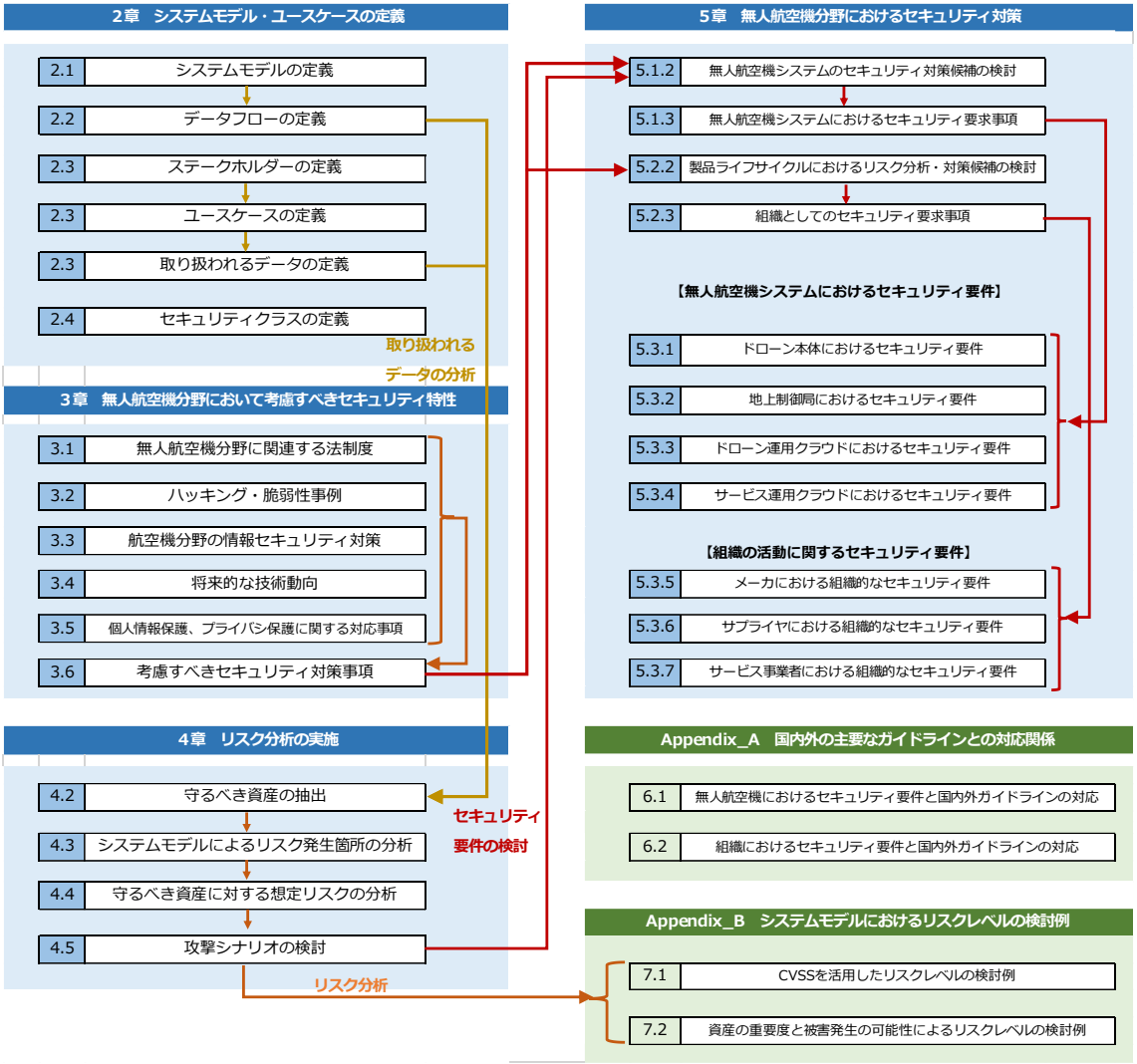


図 1-2 本書の構成と、各章の関係性の整理

1.6 本書における用語の定義

本書において使用される用語の定義一覧を表 1-1 に示す。

表 1-1 本書における用語定義の一覧

用語	本書における定義
非耐空性のセキュリティ	本書においては、無人航空機の耐空性に影響しないセキュリティ領域を非耐空性のセキュリティと定義する。 ・What：無人航空機システムにおいて実装されるソフトウェアや、取り扱われるデータが ・When：「企画」、「設計・製造」、「評価」、「運用」、「廃棄」に至るまで ・Where：電子情報及び、電子通信における経路上において

	・Who：第三者や外部、あるいは内部から ・Why：意図的または随意的な ・How：攻撃を受けた場合や過失により ・Event：経済的損失、社会的信用の失墜、法制度への抵触、プライバシ侵害、セキュリティ機能の低下につながる
システム	対象機器やその周辺機器に限らず、本書の対象範囲である無人航空機を活用したサービスや運航管理に利用されるサブシステムを含め、本書ではシステムとして定義する。
構成要素	システムを構成する機器及び、サービス提供に利用されるクラウドなどのサブシステムを含めて、本書では構成要素として定義する。
利用目的（ミッション）	様々な業態において、無人航空機を利活用する目的は異なる。各業態における無人航空機の利用目的を、本書では利用目的（ミッション）として定義している。
セキュリティクラス	本書では無人航空機分野における利用目的（ミッション）を業態別に分類し、４つのクラスに整理する。それぞれのクラスでは、目的の達成が阻害された場合に生じる影響や必要なセキュリティ対策が異なる。このセキュリティに関するクラス分類を本書においては、セキュリティクラスと定義している。
テレメトリデータ	無人航空機に実装された遠隔計測装置による測定結果のデータ。
リスク	ある脅威が脆弱性を利用して損害を与える可能性を示す。 ※JISQ27000:2019 では「目的に対する不確かさの影響」と定義される。
守るべき資産	企業や組織が保有している価値のある情報や保有する情報資産のうち、保護すべき対象に該当するものを本書では守るべき資産と定義する。
インシデント	製品またはシステムにおいて、情報セキュリティの機密性、完全性、可用性の脅威が発生した事象を示す。 ※JISQ27000:2019 では「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」と定義される。
脅威	システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。
脆弱性	脅威によって影響を受ける内在する弱さ。
リスク	損害や影響を発生させる可能性。 ※JISQ27000:2019 では「目的に対する不確かさの影響」と定義される。
リスク分析	リスクアセスメントを構成するプロセスの一つであり、リスクの特質を理解し、リスクレベルを決定するプロセスを示す。
リスクレベル	結果とその起こりやすさの組合せとして表現される、リスクの大きさ。（JISQ27000:2019 における定義）
リスク基準	リスクの重大性を評価するための目安とする条件。
リスク評価	リスク及び／又はその大きさが受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。

セキュリティ対策事項	対象として構成要素（機器やサブシステム）において求められるセキュリティ対策及び、対象ステークホルダーの組織活動において求められるセキュリティ対策を、本書ではセキュリティ対策事項と定義する。セキュリティ対策事項は、セキュリティ要求事項やセキュリティ要件を含む広義の用語として定義する。
セキュリティ要求事項	調査結果やリスク分析によって導出された、機器やシステムに求められるセキュリティ機能や脆弱性対策へのニーズ又は期待を本書ではセキュリティ要求事項として定義する。
セキュリティ要件	セキュリティ要求事項をもとに、対策として実施すべき具体的内容を加えて整理した実施対策項目の一覧を、本書ではセキュリティ要件として定義する。
脆弱性スキャン	対象の属性（OS、アプリケーション、ネットワークサービスポート等）を識別し、脆弱性を検出することを示す。古いソフトウェアやパッチの未適用、設定ミス、セキュリティポリシーへの適合検証等にも有効な場合がある。
ソフトウェアの真正性	ソフトウェアが開発メーカやサービス事業者から提供されていることを検証、信頼できることを示す。
ソフトウェアの完全性	不正な改ざんや消去からソフトウェアを保護することを示す。
ペネトレーションテスト	セキュリティ対策を回避する方法が存在しないか確認するために行うセキュリティテスト手法を示す。
物理的セキュリティ	開発や運用を行う建物や部屋へのセキュリティ対策を示す。物理的セキュリティには、入退室管理や盗難防止策等が含まれる。
環境的セキュリティ	自然災害や人為的ミスにより発生する物理的な損害に対するセキュリティを示す。環境的セキュリティには、停電対策や水害対策等が含まれる。
デザインレビュー	セキュリティに関する設計レビューを示す。セキュリティ要件に対する対策漏れや既知の脆弱性パターンの確認等が含まれる。
コードレビュー	セキュリティに関するソースコードレビューを示す。ソースコードを元に、脆弱性やその兆候について読み取り確認する。
ライフサイクル管理	製品や情報の設計・開発から廃棄・サポート終了までを管理することを示す。
インシデント管理	インシデントの検出から対応、報告、サポート等のプロセスを通してインシデントのライフサイクル管理を行うことを示す。 ※JISQ27000:2019 では「（情報セキュリティ）インシデントを検出し、報告し、評価し、応対し、対処し，更にそこから学習するための一連のプロセス」と定義される。
インシデントレスポンス	インシデントへの緩和策やサポート対応の実施を示す。

2 システムモデル・ユースケースの定義

2.1 無人航空機分野における汎用的なシステムモデルの定義

無人航空機は一般消費者や産業分野、自治体などが主体となり、非常に広範な領域において活用が進められており、実際のシステムモデルは使用される利用シーンによって異なる。本書では、なるべく広範なユースケースに対応するため、汎用的なシステムモデルを図 2-1 として定義した。本システムモデルは、サイバーセキュリティのリスク分析に用いるため、構成要素間におけるデータ通信のフローを明確化することを目的としており、構成要素内部の処理や信号の伝送については記載しない。

以下にシステムモデルの概略を示す。

[ドローン本体]

まずドローン本体は、姿勢、飛行制御（自動操縦を含む）を行うフライトコントローラが中心となり、制御に必要な情報を収集するための GNSS（GPS）や IMU、各種センサ、そして機体制御装置である UBEC、ECU、モータ、バッテリが主要な構成となる。加えて地上制御局や、クラウドシステムと通信を行うための通信モジュール、フライトログ記録用の記録装置が実装される。またドローンが様々なユースシーンで動作を行うためには、他にもカメラや、散布機、DAA システム[7]などペイロードやアプリケーション用のユニットが実装され、オンボードコンピュータにより制御される。リモート ID モジュールについては航空法の改正により、無人航空機の機体情報と所有者の登録を義務化する法案（100g 以下の無人航空機を除く）が可決し、2022 年 6 月に登録制度が開始された。登録制度の開始により、ドローン本体の識別を行うためのリモート ID を電波発信し、管理していく方針が示されている。本書では国土交通省 航空局 次世代航空モビリティ企画室発行の「リモート ID 技術規格書（案） 」[8]を参考としてシステムモデルに記載している。

[地上制御局]

ドローン本体を操作するための地上制御局は、GCS やプロポなどが該当し、ドローン本体やクラウドと通信を行うための通信モジュールを実装している。また、地上制御局のアプリケーションを補完する目的で、スマートフォンとの通信連携が行われる場合も想定されるが本書では対象から除外している。

[ドローン本体・地上制御局の通信モジュール]

ドローン本体及び、地上制御局の通信モジュールについて、本書では制御信号通信用のモジュールと、データ通信用のモジュールに分離しているが、既に運用されている無人航空機システムでは、同一のモジュールを利用するケースや、同一のモジュールの中で周波数を分けているケースなど多くの形態が想定され

[7] DAA（Detect and Avoid）：危険回避機能

[8] 国土交通省 航空局 次世代航空モビリティ企画室 「リモート ID 技術規格書（案） 」
https://www.kantei.go.jp/jp/singi/kogatamujinki/kanminkyougi_dai16/betten1.pdf

る。なお、制御信号通信モジュール及び GNSS については、耐空性に影響する領域であり、本書では対象外とする。

[クラウドシステム]

本書においてクラウドシステムは、メーカが運用し、ドローン本体や地上制御局の更新ソフトウェアを管理するドローン運用クラウドと、サービスプロバイダーが映像やデータを利活用したサービスを展開するための、サービス運用クラウドに分類している。ドローン運用クラウドでは、ドローン本体の更新用ソフトウェアを配信する目的でメーカが管理、運用することを想定している。サービス運用クラウドは、撮影した映像・画像や収集データの処理、解析等の具体的なサービス提供及び、受発注情報や顧客情報の管理など、サービス事業者が管理、運用するクラウドを想定している。

[UTM]

UTM[9]は、ドローン運用事業者が運用し、無人航空機のサービスに応じて、個別に運航管理を行う UASSP と、各 UASSP と連携し、フライト情報・飛行計画、空域情報、運航状況の一元的な管理を行う FIMS で構成されるが、本書はメーカを主たる対象とするため、詳細は除外する。

[リモート ID キャプチャ機器]

リモート ID キャプチャ機器は、航空局や重要施設管理者、警察官などが、飛行中の無人航空機を識別、照会する目的で、無人航空機から発信されたリモート ID の受信機器を示す。

[各構成要素間の通信]

各構成要素間の通信は、ドローン本体と地上制御局の間では、姿勢・飛行制御の信号と、映像やテレメトリデータなどのデータの通信が行われる。この通信には、2.4GHz 帯など無人移動体画像伝送システムが用いられるシステムと LTE などのモバイル通信が用いられるシステムが存在する。

[9] UTM（Unmanned Air System Transport Management）：ドローン運航管理システム

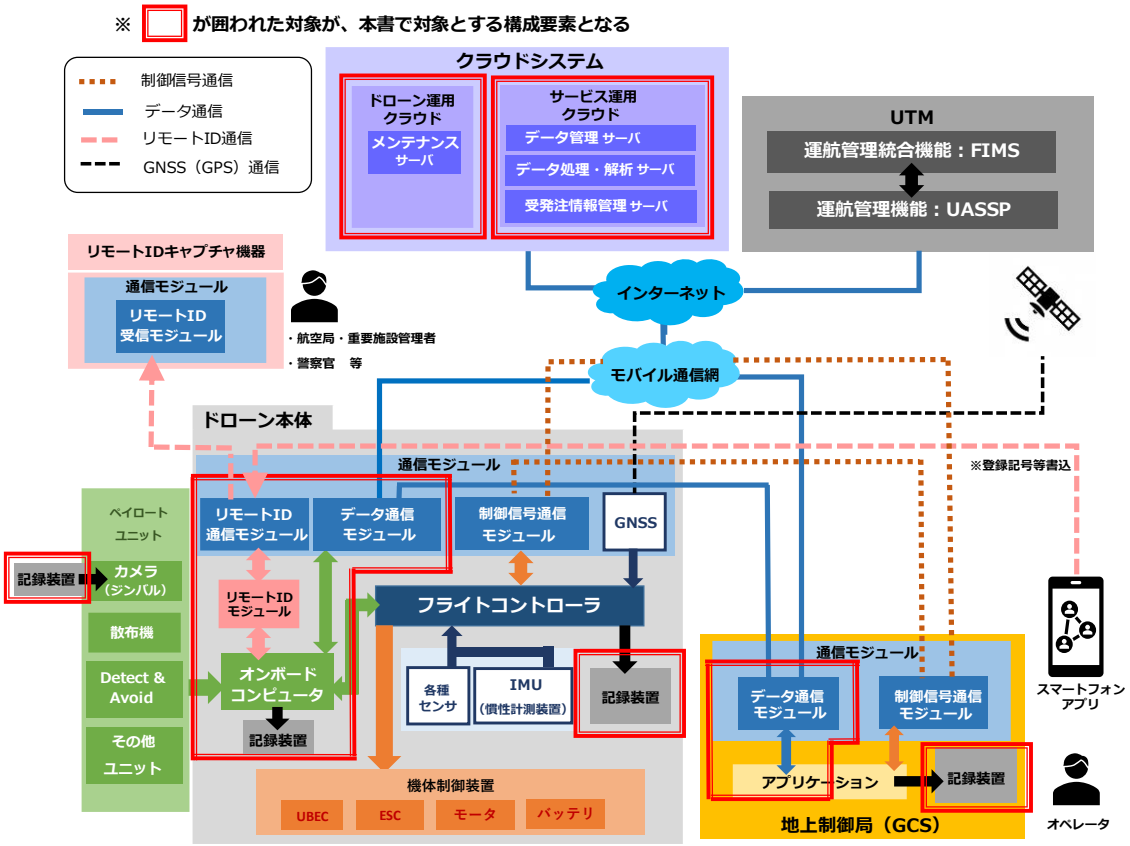


図 2-1 無人航空機の汎用的なシステムモデル

無人航空機のシステムモデルにおける構成要素の説明を表 2-1 に示す。

表 2-1 システムモデルにおける構成要素

名称	説明
■ドローン本体	
フライトコントローラ	位置情報や各種センサの情報を演算処理し、ドローン本体の姿勢制御や自律飛行の制御を行う。
オンボードコンピュータ	映像の撮影やセンサによるデータの収集、ペイロードユニットの管制御などを行うマイクロコンピュータを示す。
ペイロードユニット	カメラや散布機、危険回避機能など、無人航空機のアプリケーション機能を実現するユニット。
リモート ID モジュール	無人航空機を識別するためのリモート ID の管理を行う。
機体制御装置	ESC[10]、UBEC[11]、モータ、バッテリ等で構成され、ドローン本体の動作制御を行う。

[10] ESC（Electronic Speed Controlle）：モータの回転速度制御を行うモジュール

[11] UBEC（universal Battery Elimination Circuit）：電圧の降圧制御を行うモジュール

名称	説明
記録装置	フライトログなどを蓄積する記録装置。
GNSS	（Global Navigation Satellite System：全地球的航法衛星システム） 航空機から３つの航法衛星（GNSS 用周回衛星）を捕捉することで各衛星からの距離を得るとともに、４つ目の航法衛星からの信号で時刻合わせを行い、航空機の３次元での飛行位置を得ることができる航法システム。
各種センサ	姿勢制御用センサ：ジャイロセンサ、加速度センサなど 高度制御用センサ：気圧センサ、超音波センサなど その他：磁気方位センサ、障害物検知センサなど
IMU（慣性計測装置）	加速度センサ、角速度(ジャイロ)センサにより、3 次元の慣性運動（直行３軸方向の並進運動および回転運動）を検出する。
通信モジュール	無人航空機の制御（コマンド送信）や、データ送受信、リモート ID の送信に使用される通信モジュール。国内の無人航空機では、制御（コマンド送信）・監視（テレメトリ受信）、映像信号の伝送に 2.4GHz 帯の無線通信を利用することが主流であるが、産業用としては 73MHz 帯のほか、特定小電力無線局である 920 MHz 帯も一部利用されている。また、モバイル通信用の LTE の実装も進んでおり、将来的には 5G の利用も想定される
■地上制御局	
アプリケーション	ドローンを制御するためのアプリケーション。ドローン本体へ、オペレータの操作を制御信号として伝送する他、自律飛行のミッション情報や各種フライトモードの送信、受信したフライトログによりバッテリ残量などの機体状態を測定する機能などを有する。
記録装置	フライトログなどを蓄積する記録装置。
通信モジュール	無人航空機の制御（コマンド送信）や、データ送受信、リモート ID の送信に使用される通信モジュール。国内の無人航空機では、制御（コマンド送信）・監視（テレメトリ受信）、映像信号の伝送に 2.4GHz 帯の無線通信を利用することが主流であるが、産業用としては 73MHz 帯のほか、特定小電力無線局である 920 MHz 帯も一部利用されている。また、モバイル通信用の LTE の実装も進んでおり、将来的には 5G の利用も想定される。
■クラウドシステム	
A)ドローン運用クラウド	
メンテナンスサーバ	ドローン本体や地上制御局の更新ソフトウェアの配信を行う。

名称	説明
B)サービス運用クラウド	
データ管理サーバ	ドローン本体から送信されたデータの蓄積、管理を行う。
データ処理・解析サーバ	サービス提供のためのデータ処理、解析を行う。
受発注情報管理サーバ	顧客情報、受発注情報の管理を行う。
■UTM	
UASSP（運航管理サブシステム）	・UASSP 自身が管理する複数のオペレータを安全に飛行させるための以下のサービスを提供することに責任を持つ。 ・UASO に対する運航管理サービス：飛行計画作成/申請、飛行経路の最適化、飛行監視、機材・操縦者管理／飛行中の Conflict 情報等安全運航に関する情報提供
FIMS（運航管理統合サブシステム）	・無人航空機に関する情報を一元管理し、飛行承認に責任を持つ。 ・各運航者（UASSP、オペレータ）に飛行計画、運航状況等の無人航空機の運航状況の情報共有/提供を行う。

2.2 システムモデルにおけるデータフローの定義

第 2.1 節で定義したシステムモデルをもとに、第 3 章の守るべき資産の検討に向けて、データフローの定義を行う。本書では、「レベル 1 ～ 2 飛行におけるデータフロー」と、「レベル 3 [12]～レベル 4 [13]飛行におけるデータフロー」をそれぞれ定義する。本書のデータフローでは、無人航空機の飛行開始から飛行終了までの流れを分かりやすく整理するため、セキュリティ対策の検討対象から除外している UTM や制御信号についても記載を行っている。

2.2.1 レベル 1 ～レベル 2 飛行におけるデータフロー

レベル 1 ～レベル 2 飛行におけるデータフローを図 2-2 に示す。レベル 1 ～レベル 2 飛行では、地上制御局より、制御信号をドローン本体へ送信し、オペレータが直接操作を行う。便宜上、データフローでは 1 ～ 5 の連番を記載しているが、実際には、1 ～ 5 はほぼ並行して通信や処理が行われる。具体的な内容については、表 2-2 を参照とする。

[12] レベル 3 ：無人地帯（離島や山間部等）における補助者なし目視外飛行

[13] レベル 4 ：有人地帯（都市を含む地域）における目視外飛行

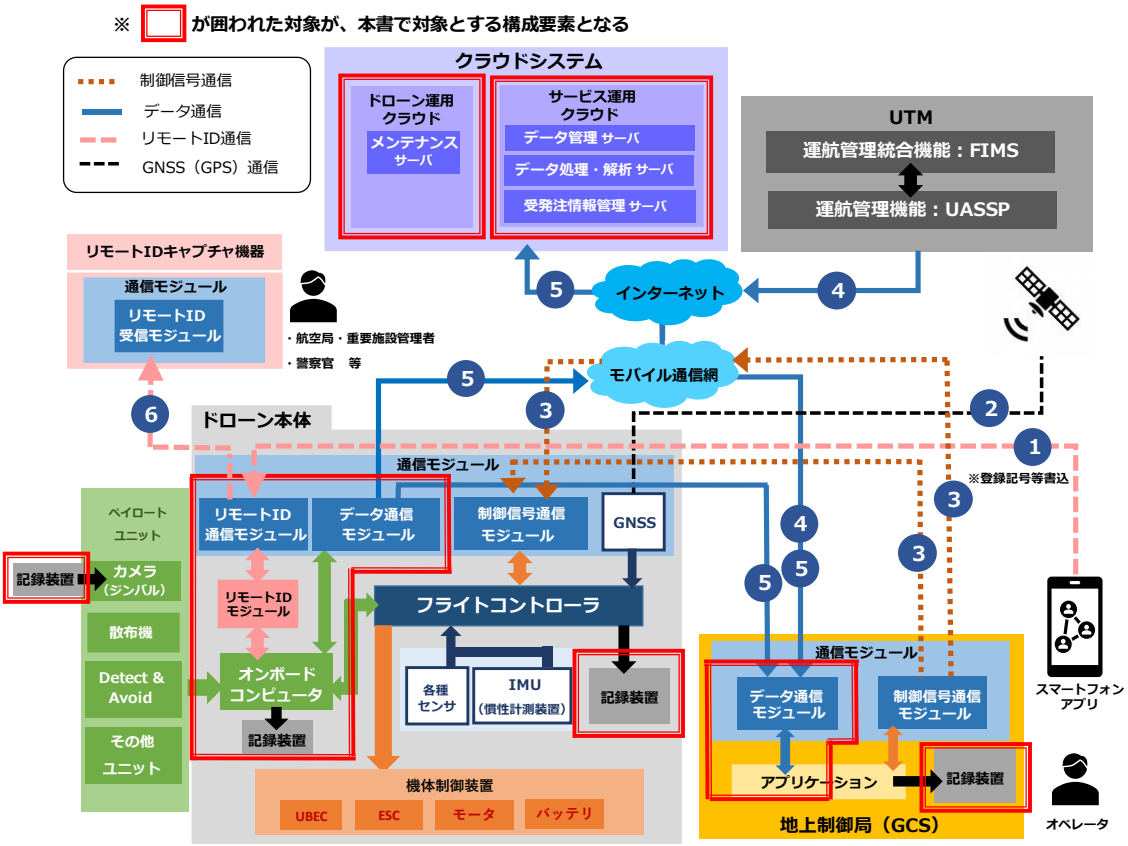


図 2-2 データフローの例（レベル１、レベル２）

表 2-2 データフローの説明（レベル１、レベル２）

図番号	アクション	説明	取り扱われるデータ
1	登録記号等の書込	スマートフォンアプリからドローン本体へリモートＩＤの登録記号が送信、書込まれる。	・リモート ID
2	位置情報受信	GPS を使用し、衛星から位置情報を受信する。	・位置情報
3	地上制御局による操作	地上制御局から、ドローン本体へ機体操作のコマンドを送信する。 ※将来的には LTE や 5G 通信への対応が想定される。	・制御信号
4	UTM からの通知	UTM から地上政局に対し、近傍機体情報、警報情報などの通知を送信する。	・空域情報 ・警報情報
5	テレメトリ情報の送受信	ドローン本体から、地上制御局及びドローン運用クラウドへ映像や、	・記録映像 ・テレメトリデータ

図番号	アクション	説明	取り扱われるデータ
		テレメトリデータを送信する。※製品によって 2.4GHz 帯などの無線通信に加えて、LTE などのモバイル通信に対応するものもある。	・フライトログ ・その他センサ取得情報（測量データなど飛行制御に関係しない情報）
6	リモート ID の送受信	ドローン本体より送信されたリモートＩＤを、航空局、重要視施設管理者、警察官等が、キャプチャ機器受信し、飛行ドローンの識別、照会を行う。	・リモート ID

2.2.2 レベル 3 ～レベル 4 飛行におけるデータフロー

レベル 3 ～レベル 4 飛行におけるデータフローを図 2-3 に示す。

レベル 3 飛行については、全国的にまだ事例は少なく、物流分野や農業、森林資源調査といった領域で実証実験が行われている。レベル 4 飛行については、2022 年度の解禁が政府によって、閣議決定された。本書では、現状想定可能な範囲のデータフローを記述している。

レベル 3 ～レベル 4 飛行では、地上制御局より、自律飛行のミッション情報がドローン本体へ送信され、プログラムにもとづく飛行が行われる。具体的な内容については、図 2-3 を参照とする。

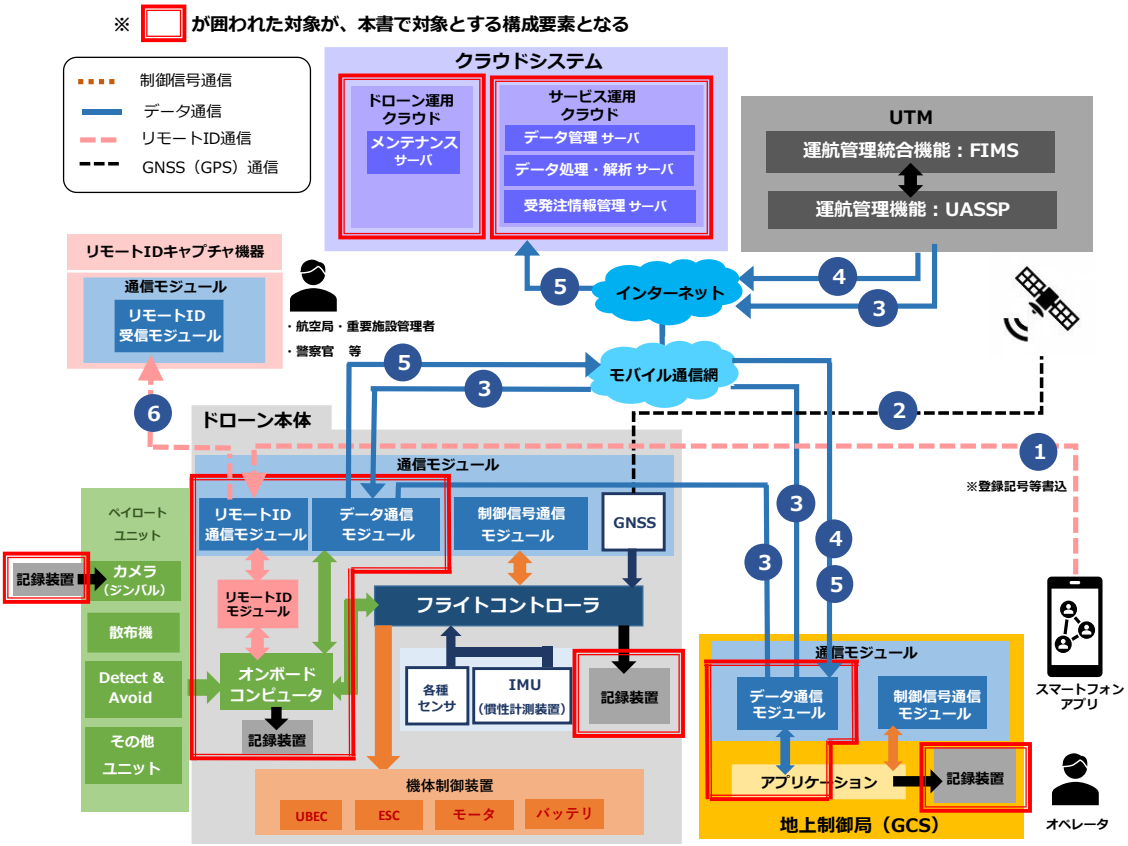


図 2-3 データフローの例（レベル３、レベル４）

表 2-3 データフローの説明（レベル３、レベル４）

図番号	アクション	説明	取り扱われるデータ
1	登録記号等の書込	スマートフォンアプリからドローン本体へリモートＩＤの登録記号が送信、書込まれる、	・リモートID
2	位置情報受信	GPS を使用し、衛星から位置情報を受信する。	・位置情報
3	自律飛行用のミッション情報にもとづく飛行	地上制御局（あるいは UASSP）からドローン本体へ、自律飛行用のミッション情報を送信する。プログラムはオンボードコンピュータを経由し、フライトコントローラへ伝達される。※地上制御局からの通信は、製品によって 2.4GHz 帯などの無線通信に加えて、LTE などのモバイル通信に対応するものもある。	・ミッション情報（自律飛行用ウェイポイント・イベント等）

図番号	アクション	説明	取り扱われるデータ
4	UTM からの通知	UTM から地上政局に対し、近傍機体情報、警報情報などの通知を送信する。	・空域情報 ・警報情報
5	テレメトリ情報の送受信	ドローン本体から、地上制御局及びクラウドへ映像や、テレメトリデータを送信する。※製品によって 2.4GHz 帯などの無線通信に加えて、LTE などのモバイル通信に対応するものもある。	・記録映像 ・テレメトリデータ ・フライトログ ・その他センサ取得情報（測量データなど飛行制御に関係しない情報）
6	リモート ID の送受信	ドローン本体より送信されたリモート ID を、航空局、重要視施設管理者、警察官等が、キャプチャ機器受信し、飛行ドローンの識別、照会を行う。	・リモート ID

2.3 ユースケースの定義

本節では、無人航空機分野におけるステークホルダー及び、ユースケースを整理し、無人航空機のサービス利用においてデータを取り扱う主体や取り扱われるデータの検討を行う。ユースケースについては、特定の産業分野に依存しない汎用ユースケースモデルと、産業分野別のユースケースとして 6 例のサンプル（測量分野、物流分野、設備点検分野、警備分野、災害対応分野）を示している。

また、ユースケースに図については、統一モデリング言語（Unified Modeling Language, UML）の記載ルール従い記述し、表 2-4 に使用する記号の説明を示す。

表 2-4 ユースケース図で使用する記号の説明

名称	記号	説明
アクター	 アクターの名称	システムを利用する、またはシステムに働きかけるユーザを示す。
ユースケース		システムがどのように利用されるのか、アクターによるシステムへの具体的な働きかけや命令の内容を示す。
関連		アクターとユースケースの関係を示す。アクターとユースケースが実線でつながれている場合、アクターが対象のユースケースを利用（実行）することを示す。
先行	<<precedes>> A- - - - - - - ▶B	ユースケースとユースケースの関係を示し、B のユース―スに先行して A のユースケースが利用（実行）されることを示す。

名称	記号	説明
拡張	<<extend>> A－－－－－－－▶B	ユースケースとユースケースの関係を示し、A のユースケースを利用すると B のユースケースが追加されることを示す。

2.3.1 無人航空機分野におけるステークホルダーの定義

無人航空機分野のユースケースを定義するにあたり、まずはステークホルダーの整理を行う。図 2-4 に各ステークホルダーと担当する役務を相関図として示す。

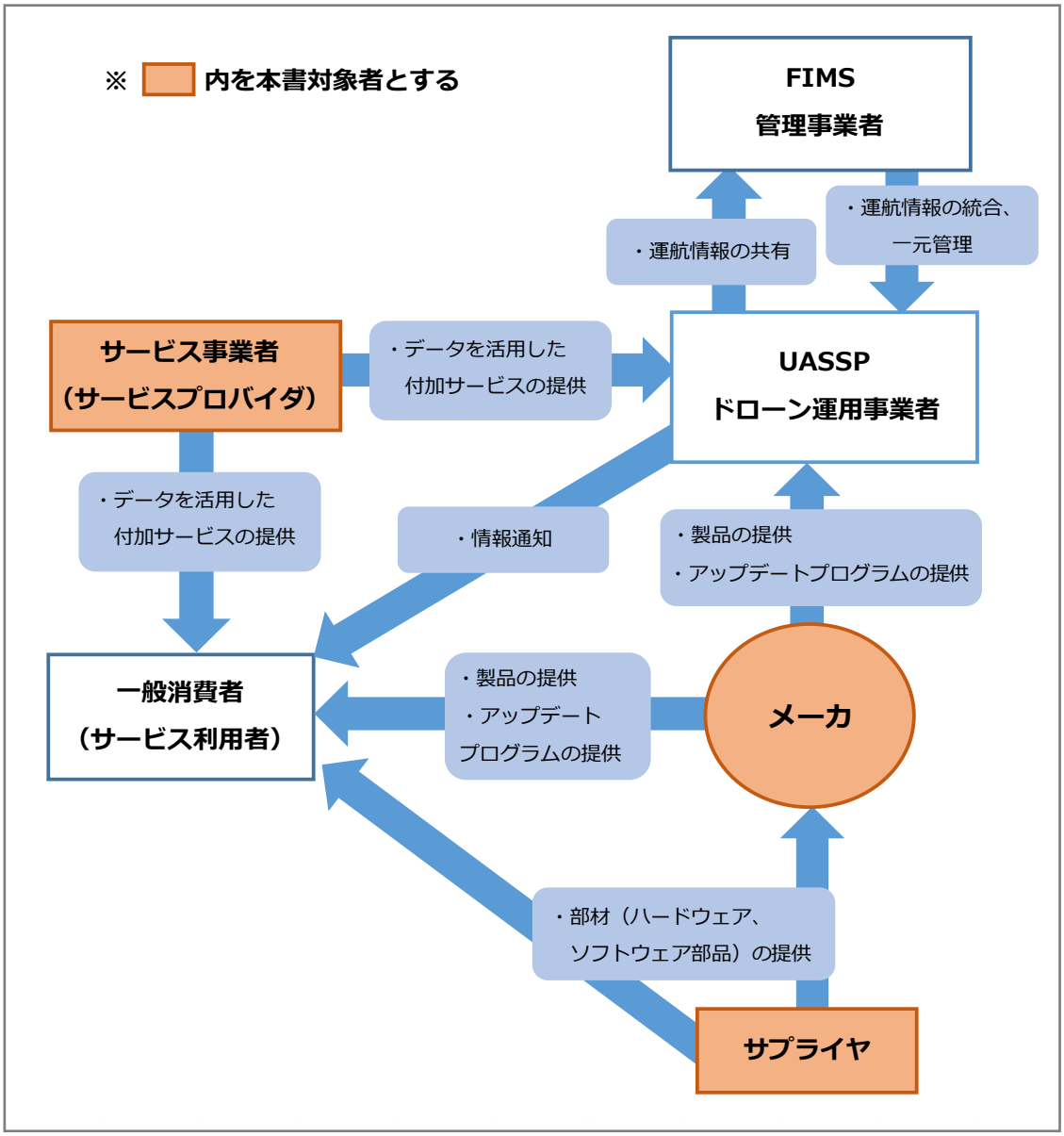


図 2-4 無人航空機分野におけるステークホルダーマップ

2.3.2 汎用的なユースケースの定義

ユースケースの整理にあたり、まず特定の産業分野に依存しない汎用的なユースケースを定義し、ユースケース図とデータ一覧を、それぞれ図 2-5 及び表 2-5 に示す。取り扱われるデータについては、ユースケース図の（）に番号を記載し、表 2-5 において番号別に具体的なデータの例を示している。

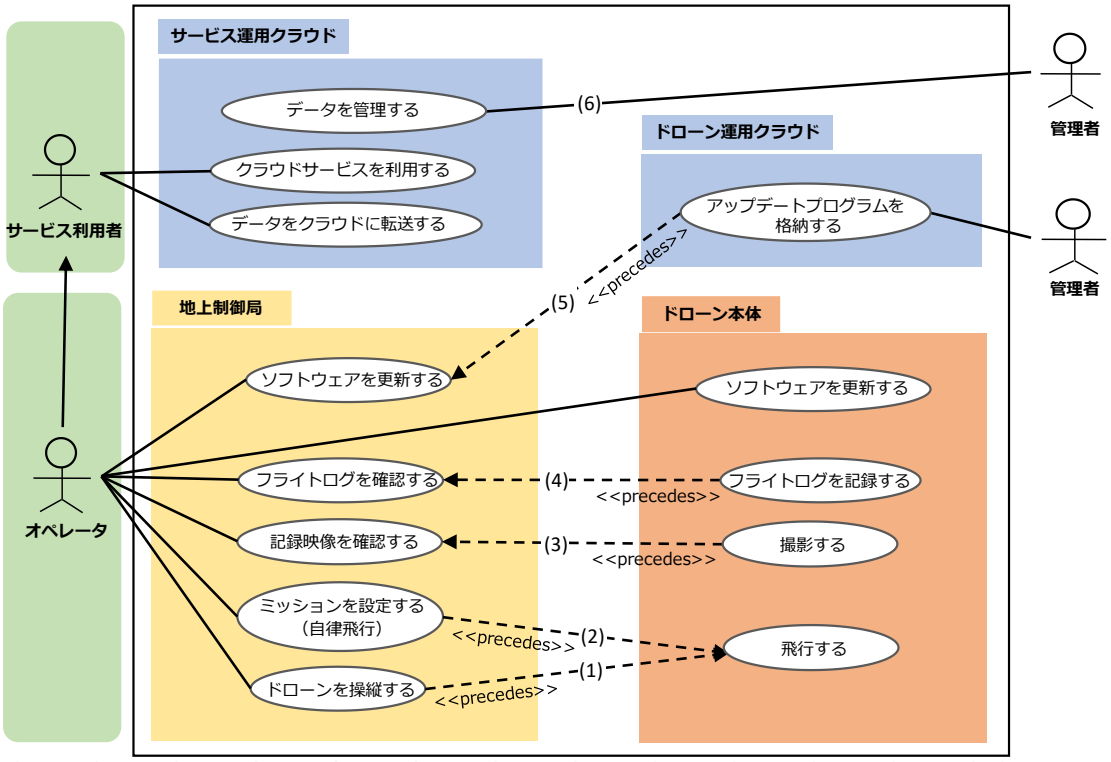


図 2-5 無人航空機の運用における汎用ユースケース図

表 2-5 汎用ユースケース図において取り扱われるデータ一覧

※（）内のデータはユースケース図の番号に対応

番号	取り扱われるデータ
(1)	制御信号、設定情報（フライトモード等）
(2)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(3)	記録映像
(4)	テレメトリデータ、フライトログ、センサ取得情報
(5)	アップデート用のプログラムコード
(6)	記録映像、テレメトリデータ ※クラウド上で管理されるデータ

2.3.3 産業分野別のサンプルユースケース

次に産業分野別のサンプルユースケースと取り扱われるデータを示す。本書に示す産業別のサンプルユースケースは、実際に事業を展開している事業者及び、事業化に向けて実証実験を実施している事業者にヒアリングを行い作成している。また各事業者にとって、競争領域に関わる機微な情報は極力排除し、公開可能な範囲で作成している。

A. 測量分野におけるサンプルユースケース

測量分野におけるサンプルユースケースを以下に示す。またユースケース図を図 2-6 に、ユースケースから導出されたデータ一覧を表 2-6 に示す。

[サンプルユースケース]

①ドローンによる測量対象地域の飛行：オペレータ（サービス利用者）

※飛行は自律飛行の場合を含む

②記録映像を PC へ移動：オペレータ（サービス利用者）

③オルソ画像の作成等、アップロード用のデータ作成：サービス利用者

④サービス運用クラウドへのログイン：サービス利用者

⑤映像処理、解析サービスの利用：サービス利用者

※提供サービスはオルソ化、3D 化、点群化や業種別の画像解析など、サービスによって異なる

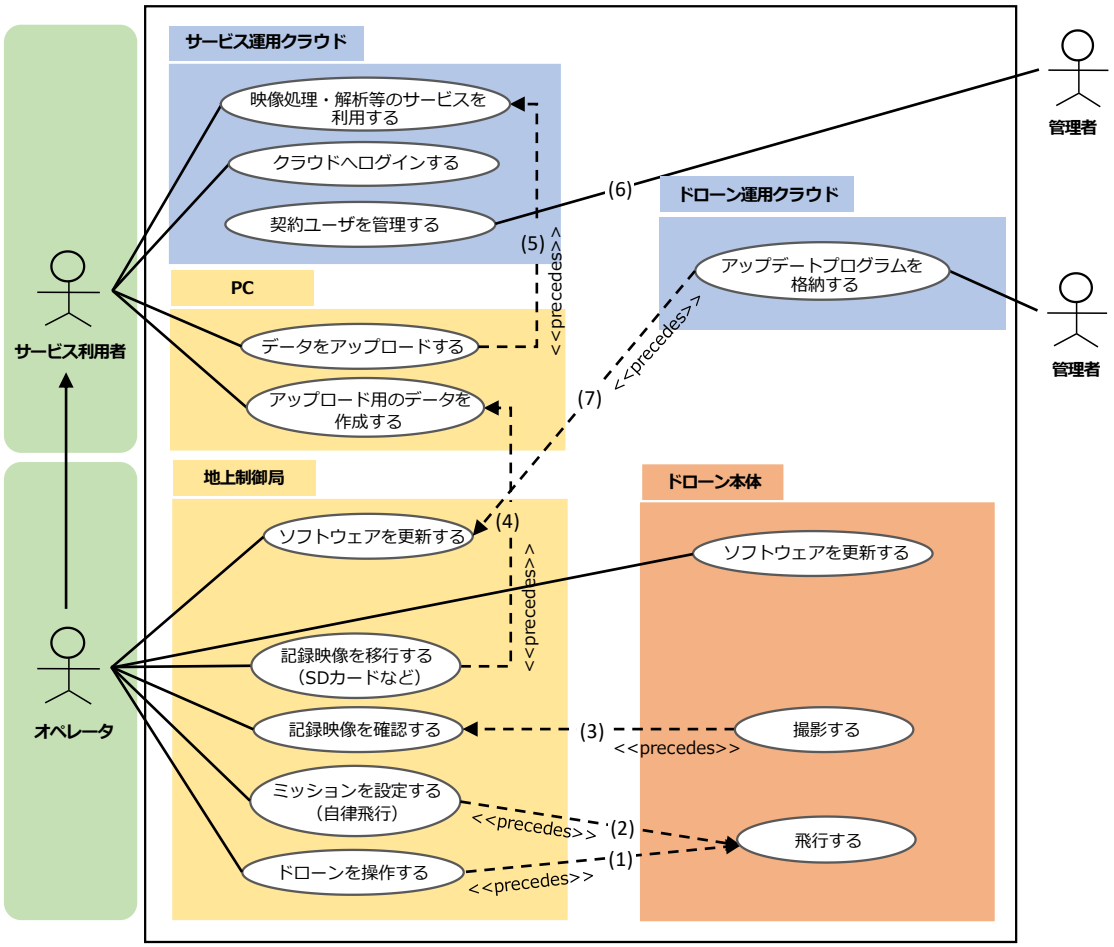


図 2-6 測量分野におけるサンプルユースケース図

表 2-6 測量分野において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	制御信号、設定情報（フライトモード等）
(2)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(3)	記録映像
(4)	SD カード内の記録映像
(5)	記録映像　※テレメトリデータを解析にするケースもある
(6)	顧客情報
(7)	アップデート用のプログラムコード

B. 物流分野におけるサンプルユースケース

物流分野におけるサンプルユースケースを以下に示す。またユースケース図を図 2-7 に、ユースケースから導出されたデータ一覧を表 2-7 に示す。

[サンプルユースケース]

①商品の発注：サービス利用者

②商品の受発注確認及び、発送指示：サービス事業者

③飛行ルート、目的地等の設定：サービス事業者

④商品受領用の鍵情報の受領：サービス利用者

※医薬品は、厳格な本人確認が求められるため、本人認証用の鍵情報が別途送信される

⑤商品の受け取り：サービス利用者

※最寄りのドローンポート等の配送先より商品を受領

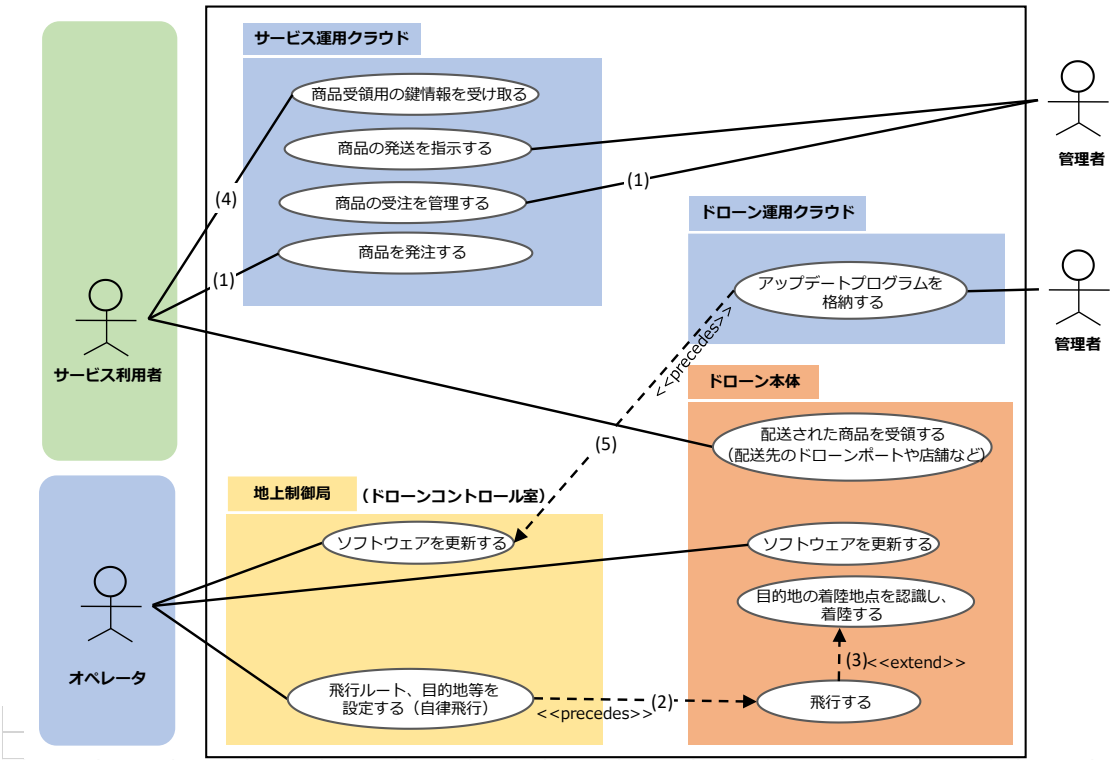


図 2-7 物流分野におけるサンプルユースケース図

表 2-7 物流分野において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	顧客情報（顧客の個人情報、サービスの受発注情報など）
(2)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(3)	ミッション情報（自律飛行用ウェイポイント・イベント等）、記録映像
(4)	商品受領用の鍵情報（宅配 BOX の開錠鍵など） ※医薬品は、本人認証のための鍵情報が別途送信される
(5)	アップデート用のプログラムコード

C. 設備点検分野におけるサンプルユースケース

設備点検分野では、サービス事業者によりサービスの提供範囲が異なる。本ユースケースでは、サービス事業者が無人航空機と連携した設備点検システムの提供及び導入支援を行うものとし、設備点検業務は、サービス事業者もしくは、対象設備の管理責任を有するサービス利用者のいずれかが担当する前提としている。

設備点検分野におけるサンプルユースケースを以下に示す。またユースケース図を図 2-8 に、ユースケースから導出されたデータ一覧を表 2-8 に示す。

[サンプルユースケース]

①点検時の飛行ルート設定：オペレータ（サービス事業者/サービス利用者）

②飛行及び設備の点検：オペレータ（サービス事業者/サービス利用者）

※設定ルート、センサ取得情報を利用した自律飛行

③ドローンの飛行状況の確認：オペレータ（サービス事業者/サービス利用者）

※レベル 3 飛行時には、地上制御局側のモニターで飛行状況をリアルタイムで確認

※レベル 4 飛行時には、遠隔地の拠点（例.ドローンコントロール室）からモニターで飛行状況をリアルタイムで確認

④気象情報や接近機体等を監視し、適宜オペレータへ通知：運航管理者（サービス事業者）

※サービル運用クラウドが UTM の一部機能を有する場合

⑤点検～飛行終了後、記録映像から設備、機器の状態を確認：サービス事業者/サービス利用者

※サービスによっては AI による解析技術を活用

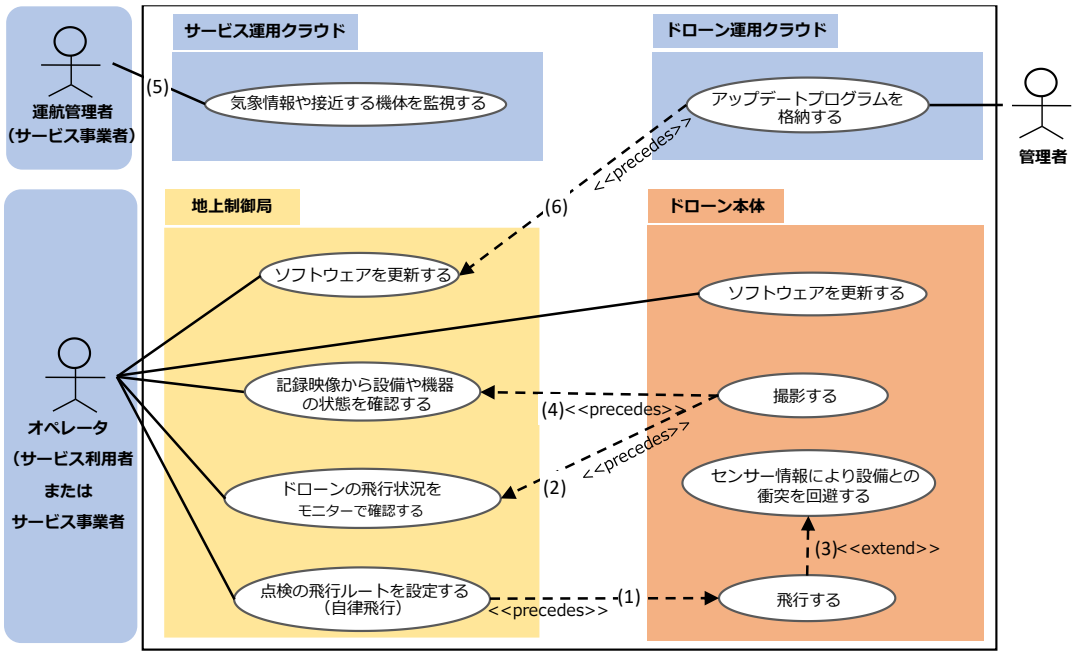


図 2-8 設備点検分野におけるサンプルユースケース図

表 2-8 設備点検分野において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(2)	記録映像（リアルタイムで送信される簡易映像）
(3)	センサ取得情報（対象設備との測位距離など）
(4)	記録映像、テレメトリデータ、フライトログ
(5)	空域情報、警報情報　※サービス運用クラウドが UTM の一部機能を有する場合
(6)	アップデート用のプログラムコード

D. 警備分野におけるサンプルユースケース

警備分野では、サービス事業者にヒアリングを実施した結果から、巡回監視サービス、侵入監視サービスの 2 種類を典型的なサービスとして記載している。また本ユースケースでは、サービス事業者は無人航空機と連携した監視システムの提供や導入支援を行うものとし、施設の警備業務はサービスを利用する側が担当することを前提としている。

以下にそれぞれのサンプルユースケースを示す。

D-1）巡回監視サービス

巡回監視サービスにおけるサンプルユースケースを以下に示す。またユースケース図を図 2-9 に、ユースケースから導出されたデータ一覧を表 2-9 に示す。

[サンプルユースケース]

①ドローンの巡回ルート設定：サービス事業者による設定

②発進指示：サービス利用者

※もしくはスケジュールで設定された時刻に自動で発進

③記録映像の確認：サービス利用者

※監視室モニターでリアルタイムの映像を確認

④過去の記録映像の確認：サービス利用者

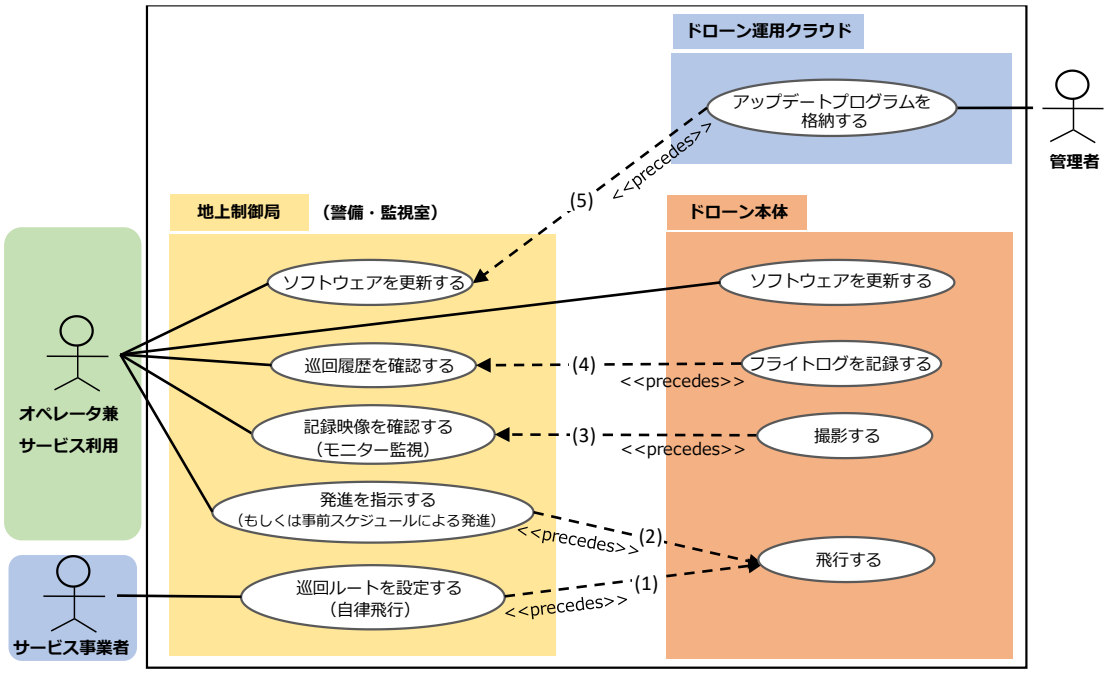


図 2-9 警備分野（巡回監視サービス）におけるサンプルユースケース図

表 2-9 警備分野（巡回監視サービス）において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(2)	制御信号
(3)	記録映像
(4)	記録映像、テレメトリデータ、フライトログ
(5)	アップデート用のプログラムコード

D-２）侵入監視サービス

侵入監視サービスにおけるサンプルユースケースを以下に示す。またユースケース図を図 2-10 に、ユースケースから導出されたデータ一覧を表 2-10 に示す。

[サンプルユースケース]

①施設内への侵入を検知

②ドローンが自動で発進

※不審者、不審車両を識別し、自動追記を行う

③記録映像の確認：サービス利用者

※監視室モニターでリアルタイムの映像を確認

※ドローンによる追跡は補助的な対応であり、平行して警備員が現地へ駆け付ける

④過去の記録映像の確認：サービス利用者

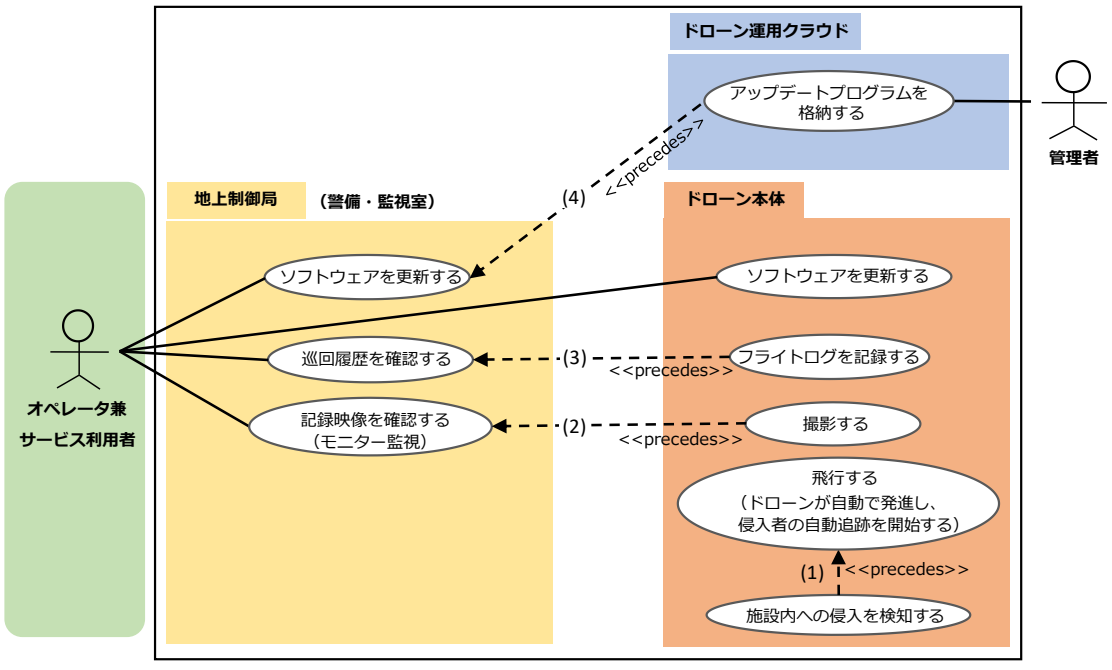


図 2-10 警備分野（侵入監視サービス）におけるサンプルユースケース図

表 2-10 警備分野（巡回監視サービス）において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	センサ取得情報（レーザセンサなど、侵入者の追跡に利用する情報）
(2)	記録映像
(3)	記録映像、テレメトリデータ、フライトログ
(4)	アップデート用のプログラムコード

E. 災害対応分野におけるサンプルユースケース

災害対応分野におけるサンプルユースケースを以下に示す。またユースケース図を図 2-11 に、ユースケースから導出されたデータ一覧を表 2-11 に示す。

[サンプルユースケース]

①ドローンによる飛行：オペレータ（サービス利用者）

※自律飛行を含む

②記録映像、データによる被災状況の確認：オペレータ（サービス利用者）

※要救助者の情報を含む

③記録映像の送信：オペレータ（サービス利用者）

※国や自治体の各対策拠点へ

④記録映像を PC へ移動：サービス利用者

⑤記録映像などのデータのアップロード：サービス利用者

⑥映像処理、解析等を利用し、詳細な被災状況や、要救助者の情報を確認：サービス利用者

※平時のドローン運用で蓄積されたデータを利用し、災害発生時との比較や解析に活用することも想定される

※地方自治体と民間サービス事業者との協力協定により、非常時には民間サービス事業者の無人航空機（システム）による運用協力も想定される

※災害時の被害認定など、課税分野への応用も想定される

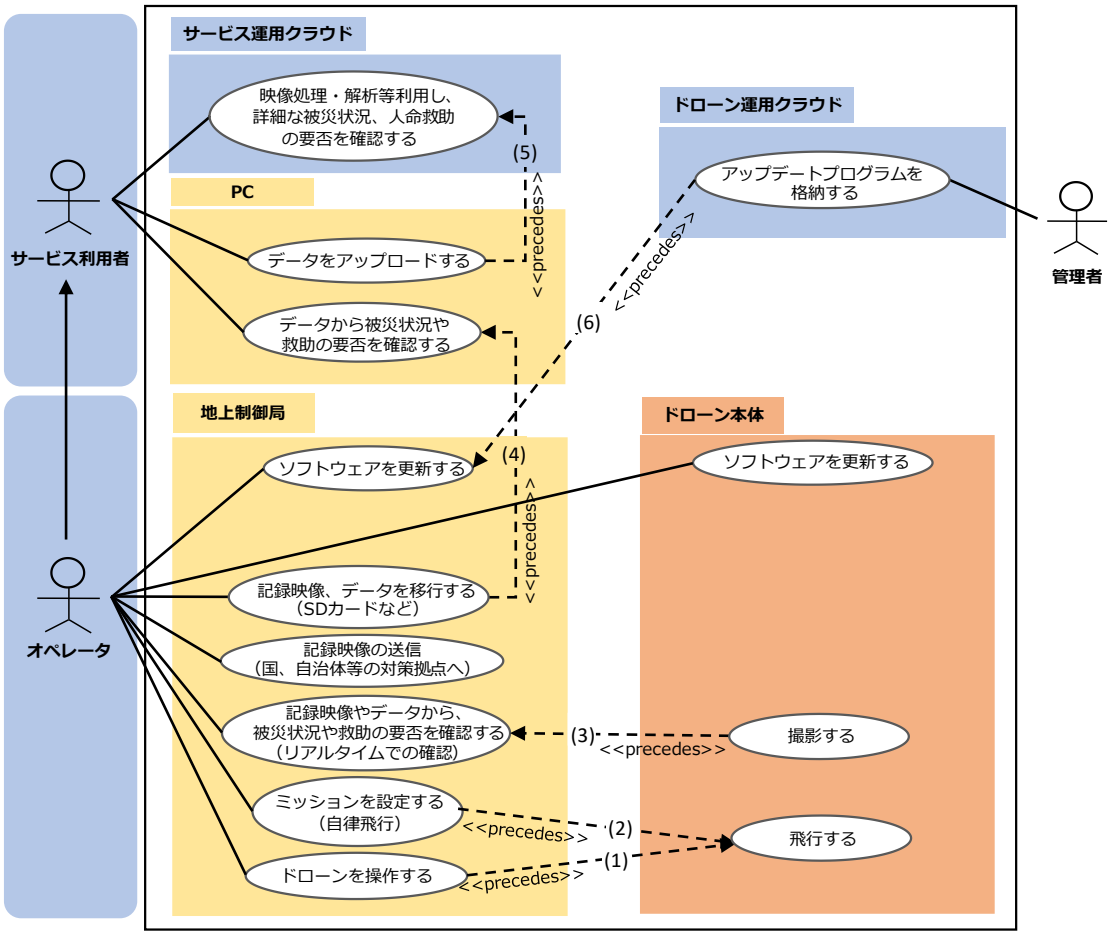


図 2-11 災害対応分野におけるサンプルユースケース図

表 2-11 災害対応分野において取り扱われるデータ一覧

※（）内の番号はユースケース図の番号に対応

番号	取り扱われるデータ
(1)	制御信号、設定情報（フライトモード等）
(2)	ミッション情報（自律飛行用ウェイポイント・イベント等）、設定情報（フライトモード等）
(3)	記録映像 センサ取得情報（赤外線センサなど、被災状況や人命救助に利用する情報）
(4)	記録映像（SD カードなどのストレージメディアに記録された情報）
(5)	記録映像 センサ取得情報（赤外線センサなど、被災状況や人命救助に利用する情報）
(6)	アップデート用のプログラムコード

2.4 業態別の利用目的に応じたセキュリティ対策のクラス分類（セキュリティクラスの定義）

本節では業態別の利用目的を整理し、それぞれの目的に応じたセキュリティ対策の検討を行うため、クラス分類を行う（以下、分類したクラスをセキュリティクラスと呼ぶ）。本書第 5 章では、本節のセキュリティクラス別に、セキュリティ対策の検討を行う。

2.4.1 無人航空機の利活用が想定される業態、利用目的の定義

本書では無人航空機の利活用が想定される業態や利用目的（ミッション）を調査し、全１６のケースに分類した。

各業態における利用目的（ミッション）の分類結果を表 2-12 に示す。

表 2-12 無人航空機の活用が想定される業態[14]、利用目的

分類	利用される業態	No.	利用目的（ミッション）
一般利用	一般消費者	①	・撮影、娯楽
産業利用 公共利用	娯楽業	②	・スポーツ、ショーなどの企画、開催
	物品賃貸業	③	・無人航空機のレンタル
	農業水産業	④	・調査、点検（撮影） ・農薬、肥料等の散布
	設備工事業	⑤	・調査、点検（撮影） ・運搬（工事補助）
	総合工事業	⑥	・調査、点検（撮影） ・測量（出来形管理） ・施工補助（塗装・洗浄など）
	道路貨物運送業	⑦	・配送
	情報通信業	⑧	・映像配信など
	専門技術サービス業	⑨	・広告宣伝 ・映像、画像、データの営業利用等 ・調査（非破壊検査業）
	教育・学習支援業	⑩	・無人航空機の技能教授業
	設備工事業（公共的インフラ設備）	⑪	・調査、点検（撮影）
	警備業	⑫	・巡回（撮影）、緊急通報など
	情報通信業	⑬	・通信中継（移動型の通信基地局）
	公務、道路貨物運送業	⑭	・医療（緊急）物資や機器の輸送

[14] 日本年金機構「事業所業態分類票」に基づき整理

	公務	⑮	・災害状況調査（撮影）、救助
その他	公務（軍事・国防）	⑯	・哨戒、防衛任務など

2.4.2 セキュリティクラスの分類基準の定義

次に表 2-12 で定義した業態別の利用目的に対して、セキュリティ対策事項の基準となるセキュリティクラスの定義を行う。

セキュリティクラスは、経済産業省が 2020 年 11 月に公開した『IoT セキュリティ・セーフティ・フレームワーク』[15]を参考に、無人航空機システムが遂行すべきミッションに着目し、ミッション失敗時における影響度を「社会的、経済的影響」、「安全や人命に対する影響（回復困難性）」という 2 つの軸にて分類を行った。

また影響がもたらす重要度の算定基準については、IPA が発行した「制御システムのセキュリティリスク分析ガイド 第 2 版[16]」の事業被害レベルの判断基準を参考に策定を行った（表 2-13）。ミッション失敗時における重要度を「深刻」、「重大」、「軽微」、「なし」の 4 段階に分類し、「社会的、経済的影響」×「安全や人命に対する影響（回復困難性）」の算出結果に対して、重要度の評価値： 1 をセキュリティクラス 1、重要度の評価値： 2 以上～4 以下をセキュリティクラス 2、重要度の評価値： 6 以上をセキュリティクラス 3 として、定量的に分類している。

クラス 1 は、ミッションの達成が阻害されたとしても、「社会的、経済的な影響」、「安全や人命に対する影響（回復困難性）」共に被害が想定されない領域である（主にホビー利用が想定される領域）。クラス 2 はミッションの達成が阻害された場合に「社会的、経済的な影響」において被害が想定される領域となる。クラス 3 はミッション達成が阻害された場合に「社会的、経済的な影響」に加えて、「安全や人命に対する影響（回復困難性）」において被害が想定される領域となる。各クラスに応じて求められるセキュリティ対策のレベルは異なり、レベルが上がるにつれて、より厳格な対策が求められる。後述する第 5 章では、本セキュリティクラスに対応したクラス 2、クラス 3 のセキュリティ対策事項を示す。なお、クラス 4 の「軍事や国防を想定した領域」については、本書のスコープからは外れるため、対象外する。

上記にて分類した業態、利用目的に対するセキュリティクラス及び重要度の区分を表 2-14 に示す。

表 2-13 業態別のセキュリティクラスの定量分類基準

重要度		社会的・経済的影響	安全・人命の影響（回復困難性）
深刻	4	ミッションの失敗により、広範な社会的被害、経済的被害が発生する	ミッションの失敗により安全・人命への直接的な被害が発生する

[15] 経済産業省 『IoT セキュリティ・セーフティ・フレームワーク』
https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

[16] IPA 『制御システムのセキュリティリスク分析ガイド 第 2 版』
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

重要度		社会的・経済的影響	安全・人命の影響（回復困難性）
		例）電力設備、橋梁、道路、情報通信網、上下水道など公共的なインフラ設備が利用不可	例）災害時の救助活動
重大	3	ミッションの失敗により、企業単位での社会的被害、経済的被害が発生する 例）個別企業への深刻な経済的被害の発生等	ミッションの失敗により安全・人命への間接的な被害が発生する 例）緊急物資、医療物資の搬送
軽微	2	ミッションの失敗により、一部利用者への社会的被害、経済的被害が発生する	ミッションの失敗により安全・人命への間接的な被害が発生する可能性がある 例）施設警備等
なし	1	被害想定なし	被害想定なし

表 2-14 業態、利用目的に対するセキュリティクラス及び重要度の区分

計算式：「社会的・経済的影響」 × 「安全・人命への影響」＝
1 ＝セキュリティクラス 1
2 以上～ 4 以下 ＝セキュリティクラス 2
6 以上 ＝セキュリティクラス 3

分類	利用される業態	No.	利用目的 （ミッション）	社会的・経済的影響	安全・人命への影響 （回復困難性）	重要度	セキュリティクラス
一般利用	一般消費者	①	撮影、娯楽	1	1	1	クラス 1 ： ホビー利用を想定した領域
産業利用	娯楽業	②	スポーツ、ショーなどの企画、開催	3	1	3	クラス 2 ： ビジネス利用を想定した領域
	物品賃貸業	③	無人航空機のレンタル	2	1	2	
	農業水産業	④	・調査（撮影） ・農薬、肥料等の散布	3	1	3	
	設備工事業	⑤	・調査（撮影） ・運搬（工事補助）	3	1	3	
	総合工事業	⑥	・調査（撮影） ・測量（出来形管理） ・施工補助（塗装・洗浄など）	3	1	3	
	道路貨物運送業	⑦	・配送	2	1	3	
	情報通信業	⑧	・映像配信など	3	1	3	

分類	利用される業態	No.	利用目的 （ミッション）	社会的・経済的影響	安全・人命への影響 （回復困難性）	重要度	セキュリティクラス
	専門技術サービス業	⑨	・広告宣伝 ・映像、画像、データの営業利用等 ・調査（非破壊検査業）	3	1	3	
	教育・学習支援業	⑩	・無人航空機の技能教授業	2	1	2	
	設備工事業 （公共的インフラ）	⑪	・公共的インフラの調査（撮影）	4	1	4	
産業/公共利用	警備業	⑫	・巡回（撮影）、緊急通報など	3	2	6	クラス３： 人命や安全にかかわる領域
	情報通信業	⑬	・通信中継（移動型の通信基地局）	3	2	8	
	公務、道路貨物運送業	⑭	医療（緊急）物資や機器の輸送	3	4	12	
	公務	⑮	災害状況調査（撮影）、救助	4	3	12	
その他	公務（軍事・国防）	⑯	哨戒、防衛任務など				クラス４：軍事や国防を想定した領域※本書対外

3 無人航空機分野において考慮すべきセキュリティ特性

本章では、無人航空機分野において特有のセキュリティ特性について検討を行う。

調査領域としては、１）関連する法制度、２）ハッキング及び脆弱性の事例、３）将来的な技術動向の３領域について調査を行い、必要となるセキュリティ対策の考察を示す。

3.1 無人航空機分野に関連する法制度への対応

3.1.1 セキュリティ対策に影響する法制度

無人航空機分野において関連する法制度については、表 3-1 に示す制度を対象に調査を行った。対象の法制度の中で、セキュリティ対策への影響が想定される制度は、「航空法」と「電気通信事業法」が該当し、それぞれの概要と必要とされるセキュリティ対策の考察を示す。

表 3-1 無人航空機分野に関連する法制度

法制度	法令番号	セキュリティ対策への影響
航空法	昭和 27 年 7 月 15 日法律第 231 号	有り
重要施設の周辺地域の上空における小型無人機等の飛行の禁止に関する法律	平成 28 年法律第 9 号	無し
道路交通法	昭和 35 年法律第 105 号	無し
電波法	昭和 25 年法律第 131 号	無し
電気通信事業法	昭和 59 年 12 月 25 日法律第 86 号	有り

3.1.2 航空法において関連するセキュリティ対策

まず航空法については、無人航空機の所有者の登録を義務付ける航空法の改正案が、2020 年 6 月に参議院本会議で可決され、2022 年 6 月 20 日より登録制度の施行が開始される（2021 年 12 月 20 日より、事前登録受付開始。2022 年 6 月 20 日より登録義務化）。規制対象となる無人航空機は 2020 年 12 月に 100ｇ以上の機体が対象となる方針が示されており、一部のホビー利用の機体を除き、殆どの機体が対象となる。今後の方向性としては機体の識別を行うためのリモート ID を電波発信し、管理していく方針が示されており、具体的な実装の方法については、小型無人機に係る環境整備に向けた官民協議会にて検討が行われている。リモート ID を含む発信情報については、認証情報を付加することが求められており、鍵情報は暗号化による保護が必要となる。

3.1.3 電気通信事業法に関連するセキュリティ対策

次に電気通信事業法については、無線免許が不要な周波数帯（2.4GHz 帯 ※送信出力が 10mW/MHz のもの）を使用する無人航空機については、電気通信事業法に基づき、技術基準適合

認定を受ける必要がある。技術基準適合認定は、近年セキュリティに関する規則が追加され、2020 年 4 月に施行となり、無人航空機において対応が必要となる。表 3-2 に技術基準適合認定において求められるセキュリティ対応事項を示す。

表 3-2 技術基準適合認定におけるセキュリティ対応事項[17]

No.	認定要件	対象となる規則
1	規則第 34 条の 10 第 1 号関係 **アクセス制御機能**	当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。
2	同 2 号関係 **アクセス制御機能に係る識別符号の初期状態変更を促す機能**	前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であって、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること、若しくはこれに準ずる措置が講じられていること。
3	同第 3 号関係 **ソフトウェアの更新の機能**	当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること
4	同第 4 号関係 **電力供給停止時のアクセス制御機能、ソフトウェア維持の機能**	当該専用通信回線設備等端末への電力の供給が停止した場合であっても、第一号のアクセス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

3.1.4 法制度に関連し、求められるセキュリティ対策事項の整理

法制度に関連し、求められるセキュリティ対策事項は以下のように整理される。

- LR-01：リモートＩＤ発信時の暗号化対応：航空法※2022 年 6 月 20 日より登録義務化
- LR-02：電気通信機能に係る設定変更については、アクセス制御機能を有する：電気通信

[17] 総務省、「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」
https://www.soumu.go.jp/main_content/000615696.pdf

事業法

- LR-03：アクセス制御機能については、識別符号の初期値の変更を促す機能を有する：電気通信事業法
- LR-04：ソフトウェアの更新機能を有する：電気通信事業法
- LR-05：電力供給停止時も、アクセス制御機能の設定、更新ソフトウェアを維持する：電気通信事業法

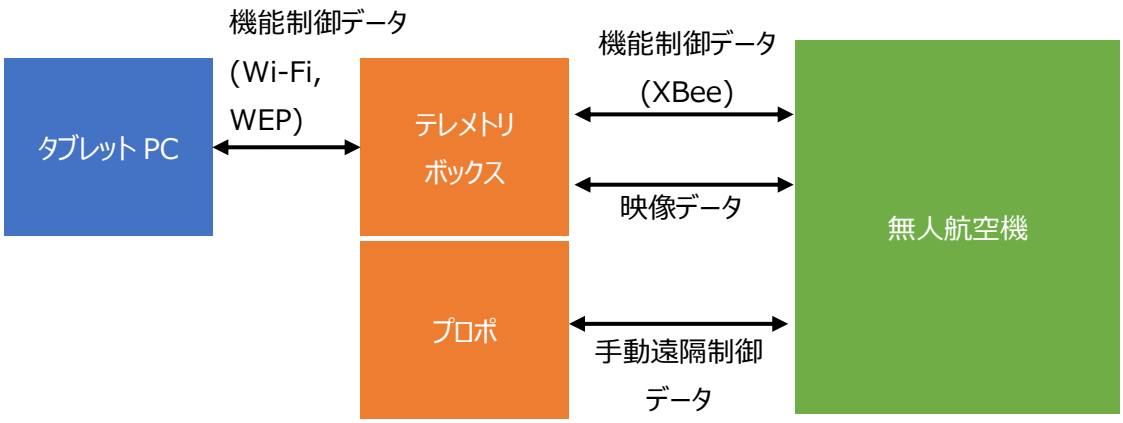
3.2 無人航空機分野におけるハッキングや脆弱性事例

国際的なセキュリティ会議や学会等において、ホビー用途だけでなくハイエンドな無人航空機についても十分なセキュリティ対策がされておらず脆弱なシステムとなっている事例が報告されている。本節では、無人航空機分野におけるサイバーセキュリティ上の脅威事例として発表されたハッキングや脆弱性について紹介する。

3.2.1 暗号通信、非暗号通信の脆弱性を利用した不正操作

セキュリティ会議「Black Hat Asia 2016」において、警察や農業分野で利用されるハイエンドな無人航空機に対し、地上制御局との無線通信をなりすました攻撃を行い、不正に制御可能な事例が発表された。対象の無人航空機のシステム構造を図 3-1 に示す。同無人航空機は、手動の遠隔制御用のプロポと通信チャンネルがあり、機能制御用のテレメトリボックスに XBee プロトコルの通信チャンネルがある。また、テレメトリボックスはタブレット PC とも WEP 暗号方式を利用した Wi-Fi の通信チャンネルでつながっており、タブレット PC からも機能制御が可能となっている。この機能制御では、無人航空機のエンジンの起動や停止、自律飛行や飛行地点の設定が可能であり、これらの制御を不正に行われる恐れがあった。不正操作が可能となる主要な原因として、XBee プロトコルの通信が暗号化されていなかったことが挙げられる。また、WEP は脆弱なプロトコルであり、暗号鍵が容易に解析されてしまうことも指摘されていた。

以上のように、通信が暗号化されていない、または、脆弱な暗号方式を利用している場合には、なりすましやデータ改ざん等のリスクが高くなるため、これらのリスクの軽減には通信の適切な暗号化が必要となる。第三者の解析によるセキュリティリスクを軽減するためには、リバースエンジニアリングやハードウェアハッキング等への対策が有効である。また、脆弱性診断を実施することで、これらの対策が効果的かどうかを評価可能である。



※テレメトリボックスとプロポは独立したシステム

図 3-1 事例として発表された無人航空機システムの構成
（発表資料を参考に構成図を作成）

3.2.2 サービス不能（DoS）攻撃による無人航空機の停止

米国ジョンズ・ホプキンス大学ラニエ・ワトキンス教授の研究発表において、ホビー用途の無人航空機システムの脆弱性を利用して同システムをサービス不能状態にする攻撃手法の実証結果が報告された。本研究発表では、次の 3 つの攻撃実験の事例が紹介されている。

- 無人航空機に対して約 1,000 回の無線接続要求パケットを送信
  →無人航空機の CPU が過負荷になり、サービス不能になった
- 制御用アプリケーションになりすまし、無人航空機のソフトウェアのバッファ容量を超えるデータパケットを送信
  →無人航空機のシステムがクラッシュし、サービス不能になった
- 無人航空機のコントローラになりすましのデータパケットを繰り返し送信し、無人航空機とコントローラの接続を遮断
  →コントローラとの接続が切断されたため、無人航空機が緊急着陸モードで着陸後、停止

上記の事例は、本ガイドラインのセキュリティクラスの定義ではクラス 1 のホビー用途の無人航空機であり、サービス不能攻撃による影響は少ないが、無人航空機の停止後に機体本体が回収され、記録した映像データやフライトログ等が盗まれる恐れがある。また、クラス 3 などサービス不能によって人命や安全に関わるシステムでは、インシデント発生による影響が大きい。このため、機密性の高い収集データの暗号化や安全な格納、ネットワーク通信における一定の負荷試験の実施等のサービス不能対策が求められる。

3.2.3 不正なファームウェアへの書き換え

米国 InGuardians 社のセキュリティアナリストによる発表では、ビジネスでも利用されている市販の無人航空機のファームウェア更新機能に脆弱性があり、非正規なファームウェアへ書き換え可能なことが実証された。また、同氏は該当する製品のファームウェアを実際に書き換える手順をツール化して公開してい

る。本脆弱性は、レースコンディション脆弱性に分類されるものであり、ファームウェアの更新時にファームウェアの正当性を検証する機能に対して予期せぬタイミングや同時アクセスにより、非正規ファームウェアに書き換えられる脆弱性となっている。

本脆弱性により脆弱性のあるファームウェアへのダウングレードやマルウェア等に書き換えられる恐れもあるため、ファームウェア更新機能の実装に合わせたセキュアな実装や、更新機能に脆弱性が報告された場合には同機能自体の修正が求められる。

3.2.4 ハッキング、脆弱性事例において求められるセキュリティ対策事項の整理

本項で紹介した脅威事例に関連するセキュリティ対策を以下に整理する。

- VR-01：通信の暗号化、および、セキュアな暗号方式の採用
- VR-02：機密性の高い収集データの暗号化
- VR-03：ネットワーク通信における一定の負荷試験の実施
- VR-04：ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装
- VR-05：リバースエンジニアリング対策
- VR-06：ハードウェアハッキング対策
- VR-07：脆弱性診断の実施

無人航空機分野のセキュリティにおいては、無線を中心とする通信の機密性や完全性に関連するセキュリティリスクが特徴となっており、通信の暗号化等の対策が必要となる、また、可用性に係るインシデントから、機体本体内のデータの窃取等も考えられるため、特に機密性の高いデータについては暗号化や安全な領域への格納、改ざん防止等の保護が求められる。

3.3 航空機分野における情報セキュリティ対策

3.3.1 航空機分野における情報セキュリティ関連文書

無人航空機分野に先行して対応が進む航空機分野の情報セキュリティ対策について、米国、欧州における関連基準やガイドラインの調査を実施した。図 3-2 に、米国、航空分野の情報セキュリティに関連する文書の相関を示す。

米国の連邦航空局及び、航空交通管制システムについては、2002 年に制定された連邦情報セキュイリティマネジメント法（Federal Information Security Management Act：FISMA）に準拠し、取り扱われる情報や情報システムの保護が必要となる。航空機及び、その運用やサービスについては、連邦規則集 タイトル 14 の規則を遵守した対応が求められる。また連邦航空局（Federal Aviation Administration 以降 FAA）では、AC-119-1 にて、航空機の運航許可を取得するためのプロセスや条件を定義しており、一部、情報セキュリティに関連する内容も含まれる。また同じく FAA では、PS-AIR-21.16-02 において耐空性に影響する特別要件（Special Condition）の適用範囲や適用のタイミングについて定義をしている。情報セキュリティに関連するガイドラインとしては、欧州の RTCA[18]SC-

[18] Radio Technical Commission for Aeronautics
https://www.rtca.org/

216/EUROCAE[19]WG-72 が情報セキュリティを含むリスクアセスメントプロセスを記載したガイドラインとして ED-202A/DO-326A を、情報セキュリティに関する詳細については ED-204A/DO-355A をそれぞれ発行し、これらの文書は FAA の文書によっても参照されている。

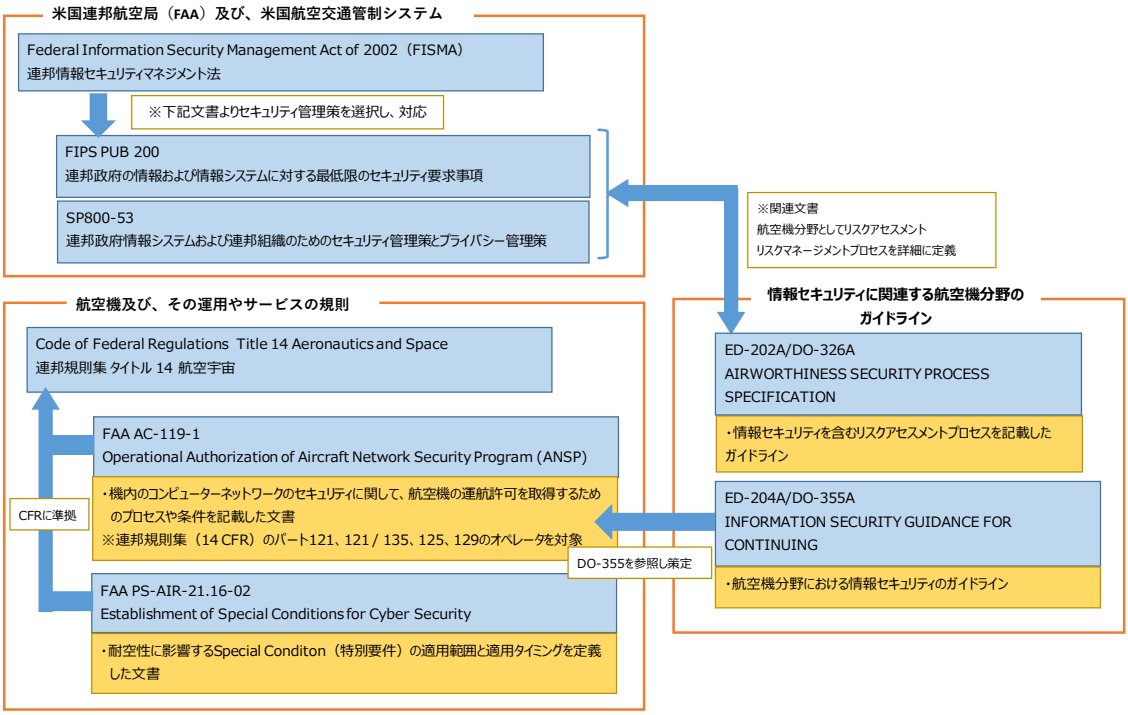


図 3-2 米国、航空分野における情報セキュリティ関連文書の相関

本節では、以下の文書を対象に無人航空機の情報セキュリティにおいても対応が必要な事項について整理を行う。

“FAA AC-119-1
Operational Authorization of Aircraft Network Security Program (ANSP) ”
”FAA PS-AIR-21.16-02
Establishment of Special Conditions for Cyber Security”
“ED-202A/DO-326A AIRWORTHINESS SECURITY PROCESS SPECIFICATION”
”ED-204A/DO-355A INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS”

[19] European Organisation for Civil Aviation Equipment
https://www.eurocae.net/

3.3.2 無人航空機においても対応が必要な事項（FAA AC-119-1/ FAA PS-AIR-21.16-02）

表 3-3 に FAA AC-119-1 において定義された情報セキュリティに関する主要な要件を示す。なお、情報セキュリティに関連する内容のみを抜粋して記載している。

表 3-3 情報セキュリティに関する主要な対応事項（FAA AC-119-1）

Chapter	セキュリティ活動	
7.1	ANSP の監視	・ Data Security Manager をポジション毎に設定し、オペレータによる ANSP プロセス全体の管理を行う。 ・ANSP の最終的な責任は、オペレータが有する。
7.2	ANSP のスコープ	オペレータは、以下を達成するために、範囲と詳細が十分に包括的である ANSP を開発および維持する必要がある。 1)データセキュリティ保護が、許可されていないデバイスまたは航空機の外部の人員によるアクセスを防ぐのに十分であることを確認する。 2)証明書保有者（certificate holder's ）の業務に固有のセキュリティ脅威が特定および評価されていること、および航空機の継続的な耐空性を確保するためにリスク軽減戦略が実装されていることを確認する。 3)メンテナンス活動によって引き起こされた可能性のあるものを含め、航空機ネットワークへの不注意または悪意のある変更を防止する。 4)機内のソースからの不正アクセスを防止する。
9.2	マニュアル	包括的なマニュアルには、次の ANSP コンポーネントの計画と手順を含める必要がある。 1)権限と責任を持つ人を含む役割と責任; 2)トレーニング/資格 3)メンテナンスラップトップ/地上支援装置（GSE）のアクセスと使用の制御 4)空港の有線および無線サービスネットワークへのアクセスの制御 5)Loadable Software Airplane Part（LSAP）librarianresource へのアクセスを制御する 6)安全な部品署名プロセスを作成し、秘密鍵へのアクセス制御する 7)Type design（型式設計）への航空機の適合性の管理 8)部品プーリングおよび部品借入の規定。 9)自社フリート内での部品交換の手順。 10)イベントの認識と応答 11)プログラムの改善を考慮したイベント評価プロセス 12)セキュリティ環境の説明
11	ANSP の特別な機器要件	ANSP タスクに関連する機器の仕様は、DAH によって確立される。 意図された目的施行のため、この機器には厳密な物理的および構成制御を実

Chapter	セキュリティ活動	
		装する必要がある。紛失した機器または説明されていない可能性のある機器を報告する手順は、ANSP に記載する必要がある。さらに、ANSP は、ANSP に関連する航空機またはシステム向けのデータを転送するための個人データストレージデバイスの使用を禁止する必要がある。安全な伝送を確保するために、オペレータが承認したストレージデバイスのみを使用する。
12	ANSP のメンテナンスプログラムへの影響	予め定義されたスケジュールにて、データの整合性やソフトウェアの適合性チェックから、航空機に割り当てられたメンテナンスラップトップや GSE の復元に至るまでのアクティビティを、メンテナンスプログラムに追加する必要がある。
13	Special Condition が必要とする可能性のあるセキュリティログファイルの処理	セキュリティログが生成される場合、オペレータは航空機のコアネットワークから抽出されたセキュリティログを保持する必要がある。 一部のログには、SC または DAH のマニュアルで義務付けられている転送方法、保持時間、分析ツールが指定されている場合がある。 オペレータは、これらのログの継続的またはスケジュールされた分析を実行して、通常のシステム動作をよりよく理解し、運用/脅威プロファイルと一致する範囲でセキュリティリスクを特定することが期待される。 ANSP は、ログの頻度、保存方法、取得方法、および分析方法を指定する必要がある。 これらのファイルは、安全な方法で送信する必要がある。
14	セキュリティイベントに対するオペレータの対応	オペレータは、ANSP の監視を実施して、プログラムへの準拠を確認し、システム全体に対する脅威を特定する必要がある。この監視の不可欠な部分は、脅威を分析し、IT セキュリティポリシーと一致する形式と方法でそれらを報告することである。 これらのポリシーには、関連する脅威情報を DAH および国土安全保障省（DHS）に転送する方法を含める必要がある。レポートインフラストラクチャを作成する代わりに、航空情報共有分析センター（A-ISAC）に参加することも可能である。 この監視の文書は、技術的な問題についてはオペレータの継続分析および監視システム（CASS）プログラムで、脅威情報についてはオペレータの年次セキュリティ評価で利用できる必要がある。

定義された対策のうち、無人航空機分野においても対応が必要と想定される事項を抽出し、無人航空機分野に置き換えて整理した内容を、表 3-4 に示す。

表 3-4 情報セキュリティに関する主要な対応事項（FAA AC-119-1）

Chapter	セキュリティ活動		表 3-3 との対応
AMFR-01	情報セキュリティプロセスの管理	・情報セキュリティ管理者を専任し、情報セキュリティプロセス全体の管理を行う。	7.1 ANSP の監視
AMFR-02	情報セキュリティプロセスのスコープ	情報セキュリティプロセスには、以下が含まれることを確認し、運用する。 1)データセキュリティ保護が、許可されていないデバイスまたは外部の人員によるアクセスを防ぐのに十分であることを確認する。 2)証明書保有者（certificate holder's ）の業務に固有のセキュリティ脅威が特定および評価されていること、および情報セキュリティを確保するためにリスク軽減戦略が実装されていることを確認する。 3)メンテナンス活動によって引き起こされた可能性のあるものを含め、無人航空機ネットワークへの不注意または悪意のある変更を防止する。	7.2 ANSP のスコープ
AMFR-03	マニュアル	情報管理マニュアルには、次の計画と手順を含める必要がある。 1)権限と責任を持つ人を含む役割と責任; 2)トレーニング/資格 3)機器やサービスに使用するシステムへのアクセスと使用の制御 5)無人航空機の更新ソフトウェアへのアクセスを制御する 6)秘密鍵へのアクセス制御する 8)ソフトウェアコンポーネントの管理や管理手順の規定。 9)情報セキュリティイベントの認識と応答 10)情報セキュリティプログラムの改善を考慮したイベント評価プロセス 11)セキュリティ環境の説明	9 .2 マニュアル
AMFR-04	情報セキュリティの特別な機器要件	無人航空機のデータを転送するための個人データストレージデバイスの使用を禁止する。安全な伝送を確保するために、オペレータが承認したストレージデバイスのみを使用する。	11 ANSP の特別な機器要件
AMFR-05	メンテナンスプログラムへの影響	データの整合性やソフトウェアの適合性チェックから、ソフトウェアの更新実行に至るまでのアクティビティを、メンテナンスプログラムとして定義する。	12 ANSP のメンテナンスプログラムへの影響
AMFR-06	セキュリティログファイルの処理	セキュリティログが生成される場合、オペレータはセキュリティログを安全に保持する必要がある。 オペレータは、これらのログの継続的またはスケジュールされた分析を実	13 Special Condition が

Chapter	セキュリティ活動		表 3-3 との対応
		行して、通常のシステム動作をよりよく理解し、運用/脅威プロファイルと一致する範囲でセキュリティリスクを特定することが期待される。 これらのファイルは、安全な方法で送信する必要がある。	必要とする可能性のあるセキュリティログファイルの処理
AMFR-07	セキュリティイベントに対するオペレータの対応	オペレータは、情報セキュリティプログラムの監視を実施して、プログラムへの準拠を確認し、システム全体に対する脅威を特定する必要がある。この監視の不可欠な部分は、脅威を分析し、IT セキュリティポリシーと一致する形式と方法でそれらを報告することである。 これらのポリシーには、関連する脅威情報を連携する外部機関へ報告するプロセスを含める必要がある。	14 セキュリティイベントに対するオペレータの対応

表 3-5 に、PS-AIR-21.16-02 において定義された主要な内容を示す。なお、FAA PS-AIR-21.16-02 は耐空性の証明に関する内容が定義されており、直接情報セキュリティに関連する内容は記載されていない。

表 3-5 主要な対応事項 FAA PS-AIR-21.16-02

Chapter	セキュリティ活動	
5	ポリシー	連邦航空局（FAA）は、次の条件下で外部サービスおよびネットワークに直接接続する航空機システムの初期型式証明書（TC）、補足型式証明書（STC）、修正 TC、または修正 STC アプリケーションに対して特別要件（SC=Special Condition）を発行する。 1.外部サービスまたはネットワークは非政府組織となる 2.航空機システムは、非政府サービスまたはネットワークから情報を受け取る 3.航空機システムの「メジャー以上」の故障影響分類において適用される
		航空機システムを受信（読み取り専用）し、送信しない非政府サービスは、特別な条件の発行を必要としない。 以下は、航空機システムに接続する非政府サービスの例 ・空港ゲートリンクネットワーク（例：Gatelink） ・パブリックネットワーク（インターネットなど） ・ワイヤレス航空機センサおよびセンサネットワーク ・セルラーネットワーク ・航空機システムに送信するポータブル電子デバイス（PED）および/またはポータブル電子フライトバッグ（EFB）
7	実装	このステートメントは、最終ポリシーステートメントの発効日以降の申請日を持つプログラ

Chapter	セキュリティ活動	
		ムに適用される。

3.3.3 無人航空機においても対応が必要な事項（ED202A/DO-326A）

表 3-6 に ED-202A/DO-326A において定義された情報セキュリティに関する主要な内容を示す。

表 3-6 情報セキュリティに関する主要な対応事項（ED-202A/DO-326A）

Chapter	セキュリティ活動	
3.1	セキュリティスコープの確立	
3.1.1	セキュリティ境界	航空機システムにおける守るべき資産へのエントリポイントを特定する。
3.1.2	セキュリティ環境	法令や契約等の、航空機システム以外の情報セキュリティに影響するコンテキストを特定する。
3.2	セキュリティリスクアセスメント	
3.2.1	脅威状態の特定と評価	脅威に関連する脆弱性や脅威が実行される環境についての状況を確認する。
3.2.2	脅威シナリオの特定	航空機システムに対する脅威が実行されうるシナリオを想定し、攻撃の経路や脅威への対策について検討する。
3.2.3	セキュリティ対策の特徴	セキュリティ対策を「予防、抑止、回復」等に分類し、脆弱性への対策の有効性を評価する。
3.2.4	脅威評価のレベル	脅威状態、脅威シナリオ、セキュリティ対策から、脅威の重大レベルを定性的に評価する。
3.3	セキュリティ有効性	
3.3.2.1	セキュリティ有効性の判断	航空機システムが脅威から守られている状態の目標を判断する。
3.3.2.2	セキュリティ有効性の要件	セキュリティ有効性の目標が満たされているかどうかを確認するための要件を導出する。
3.3.2.3	セキュリティ保証	脅威の発生時の保証のための活動内容について検討する。
3.4	セキュリティ開発活動	
3.4.1	セキュリティアーキテクチャ	航空機システムが満たすべきセキュリティの環境と要件を整理する。
3.4.2	セキュリティ対策	セキュリティリスクを軽減するための手法を検討する。
3.4.3	セキュリティガイダンス	航空機システムのセキュアな運用・保守のための要件を定義する。
3.4.4	セキュリティ検証	航空機のシステムやハードウェア、ソフトウェアがセキュリティ要件を満たすかどうか検証、評価する。

ED202A/DO-326A で定義された対策のうち、無人航空機分野においても対応が必要と想定される事項を抽出し、表 3-7 に示す。

表 3-7 無人航空機分野においても対応が必要なセキュリティ対策事項（ED-202A/DO-326A）

ID	セキュリティ対策事項	表 3-6 との対応
AMR-01	セキュリティスコープの確立 ・セキュリティ境界、セキュリティ環境等の明確化	3.11 セキュリティ境界 3.1.2 セキュリティ環境
AMR-02	セキュリティアセスメントの実施 ・脅威状態の特定と評価 ・脅威シナリオの特定 ・セキュリティ対策の特徴、有効性の評価 ・脅威評価レベルの定性的評価	3.2.1 脅威状態の特定と評価 3.2.2 脅威シナリオの特定 3.2.3 セキュリティ対策の特徴 3.2.4 脅威評価のレベル
AMR-03	セキュリティ有効性の判断基準、要件を導出し、有効性を保証するための活動を検討する。	3.3.2.1 セキュリティ有効性の判断 3.3.2.2 セキュリティ有効性の要件 3.3.2.3 セキュリティ保証
AMR-04	セキュリティ開発活動の実施 ・セキュリティアーキテクチャ（満たすべきセキュリティ環境と要件）を整理する ・セキュリティリスク対策の検討する ・セキュアな保守、運用のための要件を定義する ・セキュリティ検証の実施	3.4.1 セキュリティアーキテクチャ 3.4.2 セキュリティ対策 3.4.3 セキュリティガイダンス 3.4.4 セキュリティ検証

3.3.4 無人航空機においても対応が必要な事項（ED204A/DO-355A）

表 3-8 に ED-204A において定義された情報セキュリティに関する主要な内容を示す。

表 3-8　情報セキュリティに関する主要な対応事項（ED-204A/DO-355A）

Chapter	セキュリティ対策	
2	**航空用ソフトウェア**	
2.2.1	受信	受信時にソフトウェアの信頼性（真正性）と整合性（完全性）を確認する
2.2.2	ユーザの作成と変更	・ED-202A / DO-326A および ED-203A / DO-356A で定義されている安全なプロセスを適用する
2.2.3	データの保存 （ストレージ）	不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
		ストレージ内のデジタル証明書の有効期限を管理する
		管理責任者が必要とみなした場合は、アクセス制御に加えて暗号化を使用する
2.2.4	航空ソフトウェアが保存されているメディア	メディアに悪意のあるコードがないことを確認する
		メディアが悪意のあるコードから保護され、検証できることを確認する
		航空ソフトウェアがその整合性を維持し、検証できることを確認する
		利用可能な様々なタイプのメディアに関連する使用制限とライフサイクル、および市販のソフトウェア製品の可能性を検討する
		適切なラベルが付けられていることを確認する（部品番号、バージョン、日付など）
		リムーバブルメディアが物理的に制御されていることを確認する
		ポータブル/モバイルメンテナンスデバイスと同じようにリムーバブルメディアを扱う
		廃止措置を含めメディア内のコンテンツがライフサイクル中に開示されないように保護する
2.2.5	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、不正なコードが無いよう、機器の構成を制御する。 ・機器にインストールする場合は、ソフトウェアツールの整合性と信頼性を確認する
		ソフトウェアツールが、管理責任者またはソフトウェアサプライヤによって指定された以外の目的で使用されていないことを確認する
2.2.6	ソフトウェアの配布	航空ソフトウェアの転送の際は、ソフトウェアへのアクセス、管理、および保存をオペレータから許可された担当者のみが実施する
		エンティティ（飛行操作、エンジニアリング、航空機、空港、店舗など）間の転送（物理的および論理的）中に、航空機搭載ソフトウェアの整合性、信頼性、および機密性を確保する
2.2.8	機密性	航空ソフトウェアのライフサイクル全体（廃止措置を含む）を通じて、情報が許可されていないエンティティに提供または開示されないよう管理を行う

Chapter	セキュリティ対策	
		ソフトウェアの開示によるリバースエンジニアリングを防ぐため、インターネットなどのオープンネットワーク上で配布される場合は、https などの暗号化技術を使用する
2.2.9	インシデント管理	情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる
3	**航空機のコンポーネント**	
3.2.1	データの保存 （ストレージ）	航空機コンポーネントの安全な保管により、不正アクセスを防止する
3.2.2	伝送	航空機のコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
		航空機コンポーネントが信頼できる施設に入るときの保護手段を確認する
		航空機のコンポーネントを輸送する際に、一連の管理を行う（記録管理）。
3.2.3	修復	コンポーネントを修復するための安全な環境を整備する（人員、ツール、およびインフラストラクチャ）。
		潜在的に悪意のあるシステムやストレージメディアからの隔離を行う。
3.2.4	ツール	・管理責任者または同等のツールによって承認/推奨されているツールのみを使用する ・ツールの使用を意図された目的のみに制限する ・ツールを良好な動作状態に保つ
3.2.5	廃棄	アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ
		コンポーネントのメンテナンスマニュアルまたは該当する民間航空規制に従って、航空機部品の廃棄手順を遵守する
3.2.6	インシデント管理	情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる
4	**航空機のネットワークアクセスポイント**	
4.2	運用上のセキュリティ対策	航空機のドキュメントにおいて、ネットワークアクセスポイントと制限区域の識別と表示を行う
4.2	運用上のセキュリティ対策	ネットワークアクセスポイントと制限区域の監視、保護を行う
4.2	運用上のセキュリティ対策	情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる
5	**GROUND SUPPORT EQUIPMENT（GSE）：航空機地上支援機材 ※無人航空機分野としては該当する機器がないため割愛**	
6	**GROUND SUPPORT INFORMATION SYSTEMS（GSIS）：地上支援情報システム ※無人航空機分野としては該当する機器がないため割愛**	
7	**デジタル証明書**	
7.2		許可された認証局を定義する

Chapter	セキュリティ対策	
	オペレーション上のセキュリティ対策	デジタル証明書で使用できる許可されたツールを定義する
		・以下の管理を行うための役割、責任、およびプロセスを定義する -デジタル証明書の有効期限 -デジタル証明書のアクセシビリティ、処理、および制御 -トラストアンカー、ホワイトリスト、証明書ブラックリスト、証明書失効リスト、またはオンライン証明書ステータスプロトコル（OCSP） -デジタル証明書で使用されるツールへのアクセス -証明書の失効（例：秘密鍵の侵害、従業員の解雇、または非活動の場合） -秘密鍵へのアクセスの制限
		・タイムリーかつ効果的な方法で証明書の失効を行う
		情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる
8	**航空機情報セキュリティインシデント管理**	
8.2	オペレーション上のセキュリティ対策	「情報セキュリティイベント管理に関するガイダンス」に沿ってセキュリティ対策を行う
9	**航空オペレータの情報セキュリティプログラム**	
9.2	オペレーション上のセキュリティ対策	航空機の情報セキュリティ管理プログラムを ISMS27001 と調和させ、プロセス要素の重複を回避する
10	**オペレータの組織に関するリスクアセスメント**	
10.2	オペレーション上のセキュリティ対策	・フライトに関連するビジネスプロセスと、使用されるすべての物理資産および情報資産を特定する ・機密性、完全性、可用性の側面に関する耐空性と安全性への影響を特定する ・脅威、脆弱性を特定する ・脅威の決定のレベルを定義する ・リスクを決定する ・セキュリティ対策の推奨事項を決定する ・リスクレポートとリスクの受容を行う。
11	**オペレータの役割と責任**	
11.2.1	オペレータ情報セキュリティ管理に必要なスキル	航空機の情報ネットワークのスキルに加えて、航空機情報セキュリティスペシャリストは、ソフトウェアの動作、アルゴリズム、暗号化などを理解する必要がある
12	**オペレータ要員の訓練**	
12.2.1	トレーニング、意識、および能力	・情報セキュリティ管理に関連する業務を行う担当者の必要な能力を決定する ・情報セキュリティ管理に関連する特定のタスクごとにトレーニングとドキュメントを提供する

Chapter	セキュリティ対策	
		・行動の有効性を評価する ・教育、トレーニング、スキル、経験、資格の記録を維持する

ED204A/DO-355A で定義された対策のうち、無人航空機分野においても対応が必要と想定される事項を抽出し、適用した一覧を表 3-9 に示す。

表 3-9 無人航空機分野においても対応が必要なセキュリティ対策事項（ED-204A/DO-355A）

ID	セキュリティ対策事項	表 3-8 との対応
AR-01	無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する	2.2.1 受信
AR-02	無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する	2.2.2 ユーザの作成と変更
AR-03	無人航空機システムのソフトウェアを配布、転送する際は、ソフトウェアへのアクセス、管理、および保存をオペレータから許可された担当者のみが実施する	2.2.3 データの保存
AR-04	無人航空機システムのソフトウェアの機密性の管理 ・ライフサイクル全体（廃止措置を含む）を通じて、情報が許可されていないエンティティに提供または開示されないよう管理を行う。 ・ソフトウェアの開示によるリバースエンジニアリングを防ぐため、インターネットなどのオープンネットワーク上で配布される場合は、https などの暗号化技術を使用する	2.2.8 機密性
AR-05	無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する	3.2.1 データの保存
AR-06	無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する	3.2.2 伝送
AR-07	無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ	3.2.5 廃棄
AR-08	デジタル証明書の以下の管理を行うための役割、責任、およびプロセスを定義する ・デジタル証明書の有効期限 ・デジタル証明書のアクセシビリティ、処理、および制御 ・トラストアンカー、ホワイトリスト、証明書ブラックリスト、証明書失効リスト、	7 デジタル証明書

ID	セキュリティ対策事項	表 3-8 との対応
	またはオンライン証明書ステータスプロトコル（OCSP） ・デジタル証明書で使用されるツールへのアクセス ・証明書の失効（例：秘密鍵の侵害、従業員の解雇、または非活動の場合） ・秘密鍵へのアクセスの制限 ・タイムリーかつ効果的な方法で証明書の失効を行う	
AR-09	情報セキュリティ管理プログラムを ISMS27001 と調和させ、プロセス要素の重複を回避する	8 航空機情報セキュリティインシデント管理 9 航空オペレータの情報セキュリティプログラム
AR-10	無人航空機に関連するビジネスプロセスと、使用されるすべての物理資産および情報資産を特定する ・機密性、完全性、可用性の側面に関する耐空性と安全性への影響を特定する ・脅威、脆弱性を特定する ・脅威の決定のレベルを定義する ・リスクを決定する ・セキュリティ対策の推奨事項を決定する ・リスクレポートとリスクの受容を行う	10 オペレータの組織に関するリスクアセスメン
AR-11	オペレータの教育訓練 ・情報セキュリティ管理に関連する業務を行う担当者の必要な能力を決定する ・情報セキュリティ管理に関連する特定のタスクごとにトレーニングとドキュメントを提供する ・行動の有効性を評価し、教育、トレーニング、スキル、経験、資格の記録を維持する	11 オペレータの役割と責任 12 オペレータ要員の訓練
AR-12	情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる（インシデント管理）	2 航空用ソフトウェア 2.2.9 インシデント管理 3 航空機のコンポーネント 3.2.6 インシデント管理

3.4 無人航空機分野における将来的な技術動向

「空の産業革命に向けたロードマップ」では技術開発項目として、運航管理システムや衝突回避等の技術が挙げられている。本節では、これらの技術の動向や社会実装における事例を紹介する。

3.4.1 自律制御・目視外飛行の事例

2017 年に行われた新エネルギー・産業技術総合開発機構「インフラ維持管理・更新等の社会課題対応システム開発プロジェクト」の「完全自律制御の無人航空機による長距離荷物配送の実証実験」を皮切りに、国内では物流や警備分野など将来的な無人・有人地帯での目視外飛行を見据えた実証実験が幅広く行われている。また、2019 年頃より、モバイル通信キャリアを中心として、自律制御や目視外飛行システムを実際のビジネスソリューションとして提供するサービスも展開され、無人航空機システムの社会における実用化が進んでいる。

福島県にあるロボットテストフィールドで行われている「無人航空機の運航管理システムの開発プロジェクト」では、同一空域における複数事業者の無人航空機の安全飛行のため、統合管理された運航管理システムと複数事業者の無人航空機の相互接続試験が行われている。同システムは、運航管理統合機能として、無人航空機の飛行計画やリアルタイムの飛行状況等の情報をその他の無人航空機と共有するサービスを提供する。安全な運航管理のためには、飛行計画や飛行状況の正しい情報が必要であり、正しく認証・識別された相手との通信や経路上のデータ改ざん等への対策が必要となる。

3.4.2 モバイル通信ネットワークを利用したデータ通信の事例

2016 年より開始されている総務省の「無人航空機における携帯電話等の利用の試験的導入」の取り組み以降、無人航空機分野においてもモバイル通信ネットワークを利用したデータ通信の活用が進んでいる。国際的にはモバイル通信に関する国際標準化機関 3GPP によって「携帯電話の上空利用時の送信電力制御機能（パワーコントロール）に関する国際標準（3GPP Release 15）」が制定され、同標準に準拠した製品が国内でも発表されている。国内で行われている無人航空機の実証実験におけるモバイル通信ネットワークの利用事例では、運航管理情報の伝送による遠隔操作、映像データやテレメトリデータの伝送のための通信手段に利用されている。

一方、サイバーセキュリティの観点では、これまで無人航空機と地上制御局との通信のみが行われていたシステムに、無人航空機とクラウドシステム等へのデータ伝送の経路が増えるため、モバイル通信ネットワークを介したデータ伝送に起因するセキュリティリスクの分析や対策が必要となる。

3.4.3 技術動向事例において求められるセキュリティ対策事項の整理

本節で紹介した技術動向の事例に関連するセキュリティ対策を以下に整理する。

- TR-01：通信相手の適切な認証、識別
- TR-02：通信の暗号化、および、セキュアな暗号方式の採用
- TR-03：新たなデータ伝送方式、経路を考慮したリスクアセスメントの実施

「空の産業革命に向けたロードマップ」の構想では、無人航空機は機体本体や地上制御局だけでなく、

他の機体やクラウドシステム等との連携が進められており、なりすましやデータ改ざん等のセキュリティリスクが発生する。各セキュリティリスクに起因するインシデントによって無人航空機のミッション達成への影響が懸念されるため、セキュリティリスクへの適切な対策や軽減策が求められる。

3.5 個人情報保護、プライバシ保護に関する対応事項

無人航空機を利用した映像等の撮影には、一般の被撮影者の写りこみが想定される場合、個人情報保護法に配慮した対応を行う必要がある。また無人航空機分野におけるサービスでは、例えば測量分野などにおいて、地理空間情報を活用した情報の処理、解析によるサービス提供が行われるケースもある。

本節では撮影、記録された映像及び地理空間情報に関して、個人情報やプライバシ、肖像権を保護する上で必要な対応事項を、公開されている文書の調査結果から整理を行う。

3.5.1 撮影、記録された映像の取り扱い

無人航空機分野において、撮影、記録された映像を活用したサービス提供を行う場合には、個人情報保護に留意した対応が必要となる。

本書では「ドローンによる撮影映像等のインターネット上での取扱いに係るガイドライン[20]」及び、「カメラ画像利活用ガイドブック_ver2.0[21]」を対象として調査を行った。

１）個人情報保護に関する基本的な考え方

・無人航空機による撮影行為により、プライバシや肖像権といった権利を侵害する可能性がある。

・撮影行為の違法性は、一般的には、①撮影の必要性（目的）、②撮影方法・手段の相当性、③撮影対象（情報の性質）等を基に、総合的かつ個別的に判断される。

・撮影行為が違法とされる場合には、当該映像等をインターネット上で閲覧可能とした場合、原則として閲覧可能とした行為自体も違法となる。

・個人情報保護については、サービス事業者が対応の主体となり、サービス提供における組織的あるいは、運用上の対応を行う必要がある。

想定される対応事項）

- 取得・処理・保存・利活用の各過程におけるデータのライフサイクルを定義すること。
- データが記録・保存される機器やサーバ群、及びネットワーク上の各所における責任主体を定め、リスク分析を適切に実施すること。

---

[20] 総務省 「ドローンによる撮影映像等のインターネット上での取扱いに係るガイドライン」
https://www.soumu.go.jp/main_content/000376723.pdf

[21] IoT 推進コンソーシアム 「カメラ画像利活用ガイドブック_ver2.0」
https://www.soumu.go.jp/main_content/000542668.pdf

- データの取得と利活用にあたっては、運用実施主体を明確に定め、相談や質問・苦情等を受け付けることのできる一元的な連絡先を設置すること。
- パブリック空間を撮影する場合、設置場所の自治体で定められる条例を遵守すること。
- 個人情報が含まれる情報を利活用する場合には、利活用に対する方針を被撮影者へ事前告知し、同意を得る。

２）プライバシ及び肖像権との関係

・プライバシについては、公開する利益と公開により生じる不利益との比較衡量により侵害の有無が判断される。

※一般に、個人の住所とともに当該個人の住居の外観の写真が公表される場合には、 プライバシとして法的保護の対象になり得る。

※屋内の様子、車両のナンバープレート及び洗濯物その他生活状況を推測できるような私物が写り込んでいる場合もプライバシとして法的保護の対象となり得る。

・肖像権については、公共の場での情景を機械的に撮影しているうちに人の容貌が入り込んでしまった場合は、容貌が判別できないようにぼかしを入れたり解像度を落として公開したりしている限り、社会的な受忍限度内として肖像権の侵害は否定されると考えられる。

※公共の場でない場所における撮影はこの限りではない。

・プライバシ及び肖像権についてはサービス事業者が主体となって対応を行う必要があるが、無人航空機システムを開発、販売するメーカについても撮影態様への配慮等を、利用者（ユーザ）へ注意喚起することが望ましい。

想定される対応事項）

- 住宅地にカメラを向けないようにするなど撮影態様に配慮すること（無人航空機利用者への注意喚起を含む）。
- 撮影映像や測量成果等をインターネット上で公開する場合、削除依頼への対応を適切に行うこと。
- 削除依頼の担当者、担当窓口等を明確化し、インターネットでの相談窓口に加え、必要に応じて電話対応もできるようにすること。

3.5.2 地理空間情報、測量成果の取り扱い

無人航空機分野において、地理空間情報を活用したサービス提供を行う場合には、地理空間情報の個人情報保護にも留意した対応が必要となる。

本書では「地理空間情報の活用における個人情報の取扱いに関するガイドライン[22]」及び、「地理空間情報の活用における個人情報の取扱いに関するガイドライン（測量成果等編）[23]」を対象として調査を行った。

１）個人情報保護に関する基本的な考え方

・無人航空機のカメラによって撮影された映像、画像が特定の個人を識別可能な場合、個人情報として取り扱うこと。

・地理空間情報や、測量成果には、地番又は住居番号、所有者名等の情報が含まれる場合があることに注意すること。

・地番、住居番号が含まれる場合、不動産登記情報（全部事項証明書、所有者証明書等）や市販の住宅地図と照合することで、個人情報に該当する可能性があるので注意すること。

・上記に該当する情報をデータ処理、描画表示し、活用する場合、個人保護法の遵守と対策が必要となる。

想定される対応事項）

- インターネットによるサービス提供において地理空間情報や測量成果が取り扱われ、かつ地番又は住居番号、所有者名等の情報が含まれる場合は、削除要求対応の仕組み整備し、削除依頼への対応を適切に行うこと。

同ガイドライン文書で提示されている地理空間情報における個人情報の該当性を表 3-10 に、測量成果における個人情報保護の該当性を表 3-11 に示す。

表 3-10 地理空間情報の種類と個人情報への該当性

分類	対象となる地理空間情報	個人情報の該当性	備考・特記事項
地図	都市計画図及び都市計画基本図（「公共測量標準図式」に準拠）	該当せず	地方公共団体において、拡張して取得する事項が個人情報に該当する場合がある
	ハザードマップ	該当せず	ただし地番又は住居番号がハザードマップに明示されている場合は個人情報に該当する可能性がある

[22] 地理空間情報活用推進会議 「地理空間情報の活用における個人情報の取扱いに関するガイドライン」
https://www.gsi.go.jp/common/000055897.pdf

[23] 測量行政懇談会 「地理空間情報の活用における個人情報の取扱いに関するガイドライン（測量成果等編）」
https://www.gsi.go.jp/common/000063604.pdf

分類	対象となる地理空間情報	個人情報の該当性	備考・特記事項
	森林計画図	該当せず	ただし森林計画図に含まれる林班番号及び小班番号と森林簿を照合する事や、森林計画図に地番が明示されている場合があり、この場合は不動産登記簿の情報と照合することで個人情報に該当する可能性がある
台帳情報	固定資産課税台帳及び地番現況図	該当	何人も写しの交付を請求することができる不動産登記簿及び地図（市販の住宅地図を含む）と照合が可能
	住居表示台帳・住居表示旧新対照表	該当せず	ただし住居表示台帳における特定の建物に係る住居番号、新旧対照表における新住所表示欄の記載及び旧住所表示欄の記載は、個人情報に該当する可能性がある
	道路台帳	該当せず	ただし道路管理者の裁量により、法定記載事項に付加した情報として、民有地に係る地番や建物所有者名等が含まれる場合がある
	災害時要援護者情報	該当	一般に当事者の住所、氏名、身体の状況、家族構成、介護者の状況、緊急連絡先、家屋内における本人の居室の場所等から構成される
統計情報	国勢調査	該当せず	
	住民基本台帳に基づく人口・人口動態及び世帯数	該当せず	例外的に、市町村が独自に公表している集計結果のうち、集計後の合計数が極めて少数になる場合がある
空中写真・衛星画像	空中写真	該当せず	撮影対象・撮影縮尺によっては、プライバシや防犯への配慮ついて十分な検討が必要となる場合がある
	衛星画像	該当せず	現在の技術水準で撮影される衛星画像は特定の個人を識別するには至らない

（出典：地理空間情報活用推進会議発行 「地理空間情報の活用における個人情報の取扱いに関するガイドライン」より、一部記載を編集し、掲載）

表 3-11 測量成果の情報の種類と個人情報への該当性

分類	対象となる測量成果の情報	個人情報の該当性	備考・特記事項
地図	都市計画図及び都市計画基本図（「公共測量標準図式」に準拠）	該当せず	表 3-10 と同様
	ハザードマップ	該当せず	表 3-10 と同様
	森林計画図	該当せず	表 3-10 と同様
	地番現況図	該当	行政機関等における内部利用及び行政機関等相互間の提供については一般に問題ないと考えられる
	公共下水道事業平面図	該当せず	ただし公共下水道事業平面図の建築物の個人名が記載されているもの、地番や住居番号が記載されているケースがあり、これらは個人情報に該当する可能性がある
空中写真・衛星画像・地上写真	空中写真	該当せず	撮影対象・撮影縮尺によっては、プライバシや防犯への配慮ついて十分な検討が必要となる場合がある
	衛星画像	該当せず	現在の技術水準で撮影される衛星画像は特定の個人を識別するには至らない
	地上写真	該当	地上写真は、人の顔や家屋の表札、自動車のナンバー等が写り込んでおり、それらが特定個人の識別を可能とするものであった場合、個人情報に該当する可能性が高いと考えられる

（出典：測量行政懇談会発行 「地理空間情報の活用における個人情報の取扱いに関するガイドライン（測量成果等編）」より一部記載を編集し、掲載）

3.5.3 無人航空機分野における個人情報保護、プライバシ保護上の対応事項

本節において調査結果から導出された個人情報保護、プライバシ保護に関する対応事項を、表 3-12 に示す。また対応を行う主体について、ステークホルダー別に整理した結果を表 3-13 に示す。

表 3-12 無人航空機分野における個人情報保護、プライバシ保護上の対応事項

ID	対応事項
PR-01	個人情報保護の観点から、収集する個人情報やデータに関する管理方針を利用者へ周知する。
PR-02	取得する情報（映像、画像）が、特定の個人を識別可能な場合には、個人情報として取り扱う必要があることから、ウェブページ等により、利用目的を事前告知することが望ましい。また、無人航空機による情報（映像、画像）がサービスに提供に利用される場合には、生活者の特定を目的したものではない点を、提供サービスのウェブページ等により明示すること。
PR-03	取得する情報（撮影映像や測量成果等）に個人情報が含まれる場合、インターネット上で公開するサービス事業者は、本人関与や削除要求対応の仕組み整備し、削除依頼への対応を適切に行うこと。担当者、担当窓口等を明確化し、インターネットでの相談窓口に加え、必要に応じて電話対応もできるようにすること。

表 3-13 ステークホルダー別の対応一覧表

ステークホルダー	個人情報	プライバシ	肖像権	備考
メーカ	△	△	△	セキュリティ対策の実施は不要だが、撮影態様への配慮については利用者への注意喚起が望ましい
サプライヤ	×	×	×	実施対象外
サービス事業者	○	○	○	表 3-12 に示す対応が必要 ※具体的なセキュリティ要件については、本書 5.3.7 項の「ORG-C2M-P04 個人情報やテレメトリデータの収集に関するポリシーの公開」を参照

3.6 無人航空機分野の特性として考慮すべきセキュリティ対策事項

本章において検討を行った無人航空機分野の特性として考慮すべきセキュリティ対策事項を、表 3-14 に整理する。後述の第 5 章においては、本内容も含めてセキュリティ要求事項の検討を行う。

表 3-14 無人航空機分野の特性として考慮すべきセキュリティ対策事項

ID	セキュリティ対策事項	本書関連箇所
LR-01	リモートＩＤ発信時の暗号化対応	3.1 無人航空機分野に関連する法制度への対応
LR-02	電気通信機能に係る設定変更については、アクセス制御機能を有する	
LR-03	アクセス制御機能については、識別符号の初期値の変更を促す機能を有する	
LR-04	ソフトウェアの更新機能を有する	
LR-05	電力供給停止時も、アクセス制御機能の設定、更新ソフトウェアを維持する	
VR-01	通信の暗号化、および、セキュアな暗号方式の採用	3.2 無人航空機分野におけるハッキングや脆弱性事例
VR-02	機密性の高い収集データの暗号化	
VR-03	ネットワーク通信における一定の負荷試験の実施	
VR-04	ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装	
VR-05	リバースエンジニアリング対策	
VR-06	ハードウェアハッキング対策	
VR-07	脆弱性診断の実施	
AMFR-01	情報セキュリティプロセスの管理	3.3 航空機分野における情報セキュリティ対策
AMFR-02	情報セキュリティプロセスのスコープ	
AMFR-03	マニュアル	
AMFR-04	情報セキュリティの特別な機器要件	
AMFR-05	メンテナンスプログラムへの影響	
AMFR-06	セキュリティログファイルの処理	
AMFR-07	セキュリティイベントに対するオペレータの対応	
AMR-01	セキュリティスコープの確立 ・セキュリティ境界、セキュリティ環境等の明確化	
AMR-02	セキュリティアセスメントの実施 ・脅威状態の特定と評価 ・脅威シナリオの特定 ・セキュリティ対策の特徴、有効性の評価	

ID	セキュリティ対策事項	本書関連箇所
	・脅威評価レベルの定性的評価	
AMR-03	セキュリティ有効性の判断基準、要件を導出し、有効性を保証するための活動を検討する。	
AMR-04	セキュリティ開発活動の実施 ・セキュリティアーキテクチャ（満たすべきセキュリティ環境と要件）を整理する ・セキュリティリスク対策の検討する ・セキュアな保守、運用のための要件を定義する ・セキュリティ検証の実施	
AR-01	無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する	
AR-02	無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する	
AR-03	無人航空機システムのソフトウェアを配布、転送する際は、ソフトウェアへのアクセス、管理、および保存をオペレータから許可された担当者のみが実施する	
AR-04	無人航空機システムのソフトウェアの機密性の管理 ・ライフサイクル全体（廃止措置を含む）を通じて、情報が許可されていないエンティティに提供または開示されないよう管理を行う。 ・ソフトウェアの開示によるリバースエンジニアリングを防ぐため、インターネットなどのオープンネットワーク上で配布される場合は、https などの暗号化技術を使用する	
AR-05	無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する	
AR-06	無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する	
AR-07	無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ	
AR-08	デジタル証明書の以下の管理を行うための役割、責任、およびプロセスを定義する ・デジタル証明書の有効期限 ・デジタル証明書のアクセシビリティ、処理、および制御 ・トラストアンカー、ホワイトリスト、証明書ブラックリスト、証明書失効リスト、またはオンライン証明書ステータスプロトコル（OCSP）	

ID	セキュリティ対策事項	本書関連箇所
	・デジタル証明書で使用されるツールへのアクセス ・証明書の失効（例：秘密鍵の侵害、従業員の解雇、または非活動の場合） ・秘密鍵へのアクセスの制限 ・タイムリーかつ効果的な方法で証明書の失効を行う	
AR-09	情報セキュリティ管理プログラムを ISMS27001 と調和させ、プロセス要素の重複を回避する	
AR-10	無人航空機に関連するビジネスプロセスと、使用されるすべての物理資産および情報資産を特定する ・機密性、完全性、可用性の側面に関する耐空性と安全性への影響を特定する ・脅威、脆弱性を特定する ・脅威の決定のレベルを定義する ・リスクを決定する ・セキュリティ対策の推奨事項を決定する ・リスクレポートとリスクの受容を行う	
AR-11	オペレータの教育訓練 ・情報セキュリティ管理に関連する業務を行う担当者の必要な能力を決定する ・情報セキュリティ管理に関連する特定のタスクごとにトレーニングとドキュメントを提供する ・行動の有効性を評価し、教育、トレーニング、スキル、経験、資格の記録を維持する	
AR-12	情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる（インシデント管理）	
TR-01	通信相手の適切な認証、識別	3.4 無人航空機分野における将来的な技術動向
TR-02	通信の暗号化、および、セキュアな暗号方式の採用	
TR-03	新たなデータ伝送方式、経路を考慮したリスクアセスメントの実施	
PR-01	個人情報保護の観点から、収集する個人情報やデータに関する管理方針を利用者へ周知する	3.5 個人情報保護、プライバシ保護上の対応事項
PR-02	取得する情報（映像、画像）が、特定の個人を識別可能な場合には、個人情報として取り扱う必要があることから、ウェブページ等により、利用目的を事前告知することが望ましい。 また、無人航空機による情報（映像、画像）がサービスに提供に	

ID	セキュリティ対策事項	本書関連箇所
	利用される場合には、生活者の特定を目的したものではない点を、提供サービスのウェブページ等により明示すること	
PR-03	取得する情報（撮影映像や測量成果等）に個人情報が含まれる場合、インターネット上で公開するサービス事業者は、本人関与や削除要求対応の仕組み整備し、削除依頼への対応を適切に行うこと。担当者、担当窓口等を明確化し、インターネットでの相談窓口に加え、必要に応じて電話対応もできるようにすること	

4 リスク分析の実施

4.1 リスク分析の実施プロセス

無人航空機システムの開発メーカにとって、必要なセキュリティ対策の検討を行うにあたり、リスク分析を実施し、検討の指針とすることが必要となる。リスク分析には、様々なアプローチが存在するが、本書では、IPA「IoT 開発におけるセキュリティ設計の手引き[24]」を参考としたプロセスを示すものとする。

リスク分析のプロセスは図 4-1 に沿って、「ステップ 1 守るべき資産の分析」から、「ステップ 5　リスクレベルの検討」までを順を追って実施する。※ステップ 5 のリスクレベルの検討については、本書の Appendix_B にて実施例を記載する。

リスク分析実施後、リスク分析結果が受容可能かを決定するリスク評価を行うが、リスク評価については、各事業者において組織の目的、外部状況及び内部状況に基づき、決定される。

またリスク分析実施後、リスクに対するセキュリティ対策の検討を行うが、本書では第 5 章にてセキュリティ要求事項及び対応すべきセキュリティ要件を示す。

また本書に示すリスク分析は、システムモデルを対象に実施した一例であり、実際のリスクは無人航空機の業種や運用形態によって異なる可能性がある。本書の例を参考として、対象事業者により、それぞれの製品やサービスを対象にリスク分析を実施することを前提としている。

[24] IPA 「IoT 開発におけるセキュリティ設計の手引き」
https://www.ipa.go.jp/security/iot/iotguide.html

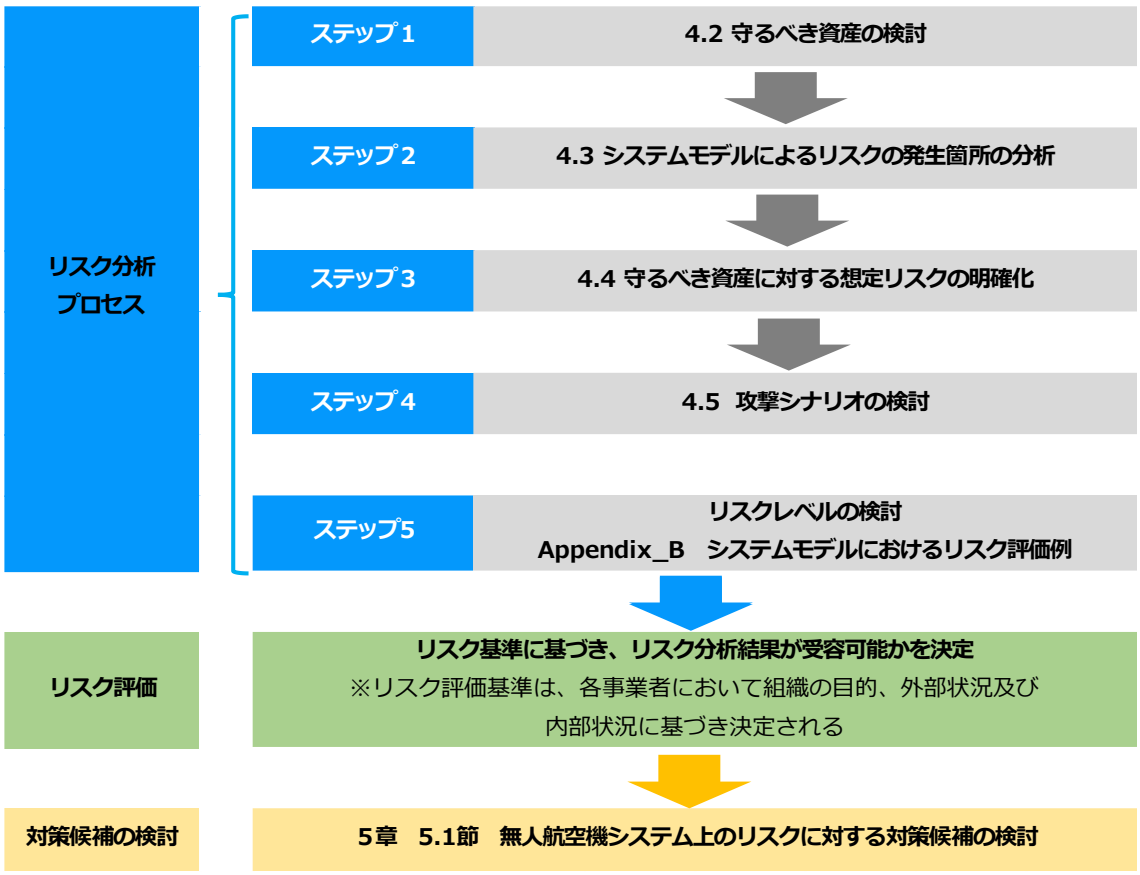


図 4-1 リスク分析の実施プロセス

4.2 守るべき資産の抽出

リスク分析の最初のステップとして、守るべき資産を抽出する。

守るべき資産の選定については、表 2-2、表 2-3、表 2-5 にて定義した取り扱われるデータを対象とし、インシデント発生時に製品提供や企業活動に与える影響（＝重要度）の検討を行う。

以下に具体的な影響の例を示す。

- **経済的な損失につながる**
- **業務活動やサービス提供が阻害される**
- **法制度に抵触する（航空法、個人情報保護法など）**
- **評判、ブランドの毀損につながる**
- **改ざんやなりすましによって飛行の安全に影響が生じる**
- **守るべき資産を保護するためのセキュリティ機能に影響する（機能が無効化される）**

無人航空機の分野では、機密性の高い資産だけでなく、完全性、可用性についての考慮や、情報が漏洩した結果、解析によってなりすましなどに悪用される可能性がある資産についても考慮する必要がある。ただし、具体的に何を守るべき資産として取り扱うかについては、メーカ側で実際の利用シーンや上記例の影響を踏まえて、個別に検討を行う必要がある。本書では、無人航空機のメーカや、無人航空機を

活用したサービスを提供しているサービス事業者にヒアリングを行い、重要度を決定している。

表 4-3 に無人航空機において想定される守るべき情報の抽出例を示す。情報資産の重要度については、IPA の「中小企業の情報セキュリティ対策ガイドライン 第 3 版[25]」の重要度判断基準（表 4-1、表 4-2）に準拠し、C：機密性、I：完全性、A：完全性に基づく整理を行った。

表 4-1 情報資産の重要度判断基準

判断基準	重要度
機密性・完全性・可用性評価値のいずれかまたはすべてが「２」の情報資産	2
機密性・完全性・可用性評価値のうち最大値が「１」の情報資産	1
機密性・完全性・可用性評価値すべてが「０」の情報資産	0

（出典：IPA「中小企業の情報セキュリティ対策ガイドライン 第 3 版」）

表 4-2 情報資産の機密性・完全性・可用性に基づく重要度の定義

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	**2**	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている。	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データ１として指定されている。 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため）漏洩すると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	1	漏洩すると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	0	漏洩しても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	**2**	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている。	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報

[25] IPA「中小企業の情報セキュリティ対策ガイドライン 第 3 版」
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

評価値		評価基準	該当する情報の例
			●顧客から製造を委託された設計図
	1	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	**2**	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供している EC サイト ●顧客に提供しているクラウドサービス
	1	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ （インターネット向け事業の場合）
	0	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログデータ

（出典：IPA「中小企業の情報セキュリティ対策ガイドライン 第 3 版」）

表 4-3 無人航空機システム（システムモデル）における情報の例

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
ドローン本体	一次資産[26]	フライトログ A) ※クラス２：通常の産業利用に影響するもの	1	1	1	**1**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、プライバシ侵害とみなされる可能性がある。 ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		フライトログ B) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	1	1	**2**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、侵入や攻撃の経路を解析される可能性がある。 ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		記録映像 A) ※個人情報、肖像権や個人のプライバシ、業務機密に影響しないもの、並びに災害救助、警備業務などの安全に影響しないもの	0	0	0	**0**	
		記録映像 B) ※個人情報あるいは個人情報に類する情報、肖像権や個人のプライバシ、業務機密に影響するもの 例）特定の個人を識別可能な映像、画像、プライ	2	1	1	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。 ・完全性：改ざんによって、ドローンの利用目的が達成できない可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある

[26] 保護すべき資産そのものを一次資産と定義

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		バシや業務機密が写りこんだ映像、画像）					
		記録映像 C) ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い　※地方自治体等のルールに準じた対応が必要 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		記録映像 D) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	2	2	**2**	・機密性：記録映像の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備や施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		リモート ID	0	1	1	**1**	・機密性：リモート ID 自体の機密性は低い ※リモート ID 発信時の暗号鍵については、機密情報として取り扱う必要がある ・完全性：改ざんによって、リモート ID の通知義務を満たせない可能性がある。 ・可用性：リモート ID にアクセスできなくなることによって、通知義務を満たせない可能性がある。
		オンボードコンピュータのプログラムコード	2	2	2	**2**	・機密性：主力製品のプログラムであり、流出すると他社との差別化ができなくなり、売上が減少する。 ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品が使用できなくなり、製品の信頼性を失う可能性があり、売上が減少す

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							る
		フライトコントローラのプログラムコード	2	2	2	**2**	・機密性：主力製品のプログラムであり、流出すると他社との差別化ができなくなり、売上が減少する ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品が使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する
		センサ取得情報 A) 測量データなど飛行制御に関係しない情報	0	0	0	**0**	
		センサ取得情報 B) 対象設備との測位距離など、飛行制御に影響する情報 ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの	1	1	1	**1**	・機密性：センサ取得情報の漏えいにより、設備の場所等が解析され、設備への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、周辺設備との衝突など、周辺被害やドローンの利用目的の達成に支障が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		センサ取得情報 C) レーザセンサ、赤外線センサなど、警備や被災状況の把握、人命救助に利用される情報 ※クラス３：　警備業務、災害救助業務など、人命や安全に影響するもの	0	2	2	**2**	・機密性：センサ取得情報自体の機密性は低い ・完全性：改ざんによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる ・可用性：データにアクセスできなくなることによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる
		機能・サービス	0	2	2	**2**	・機密性：提供される機能やサービスは開示されており、漏洩による影響はない ・完全性：データによっては改ざんによって、提供機能やサービスが損なわれ、製品の信頼

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							性を失う可能性があり、売上が減少する ・可用性：製品の機能やサービスが使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する
		機器本体（ハードウェア）	1	2	0	**2**	・機密性：ハードウェアから、差別化要素となる機器の仕様や攻撃に利用可能な情報が漏えいし、売上の低下や製品の信頼性の失墜につながる可能性がある。 ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：ハードウェアの改ざんによって、提供機能やサービスが損なわれ、製品の信頼性を失う可能性があり、売上が減少する ・可用性：ハードウェアについては、一般的に攻撃後の可用性担保までは対応困難であり、影響は少ない ※可用性については、メーカによる保証などのビジネスコンディションによって判断される。
	二次資産[27]	認証情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある
		復号鍵（秘密鍵）、検証鍵（公開鍵、ハッシュ）	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある
		デジタル証明書	0	1	1	**1**	・機密性：公開情報であり、機密性はない ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある

[27] 一次資産を保護するために必要な暗号化対策や、認証に関する副次的な資産を二次資産と定義

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある
地上制御局	一次資産	フライトログ A) ※クラス２：通常の産業利用に影響するもの	1	1	1	**1**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、プライバシ侵害とみなされる可能性がある。※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		フライトログ B) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	1	1	**2**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、侵入や攻撃の経路を解析される可能性がある。※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		記録映像 A) ※個人情報、肖像権や個人のプライバシ、業務機密に影響しないもの、並びに災害救助、警備業務などの安全に影響しないもの	0	0	0	**0**	
		記録映像 B) ※個人情報あるいは個人情報に類する情報、肖像権や個人のプライバシ、業務機密に影響するもの 例）特定の個人を識別可能な映像、画像、プライバシや業務機密が写りこんだ映像、画像）	2	1	1	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。 ・完全性：改ざんによって、ドローンの利用目的が達成できない可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		記録映像 C) ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い　※地方自治体等のルールに準じた対応が必要 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		記録映像 D) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	2	2	**2**	・機密性：記録映像の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備や施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		設定情報（フライトモード等）	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		ミッション情報 A) 自律飛行用ウェイポイント・イベント等 ※クラス２：通常の産業利用に影響するもの	0	2	1	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		ミッション情報 B) 自律飛行用ウェイポイント・イベント等 ※クラス２：公共性の高い設備、機器の点検業務	2	2	2	**2**	・機密性：ミッション情報の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備、施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、公共性の高い設備へ

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの					の重大な影響、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、公共性の高い設備への重大な影響、人命や安全上の影響が生じる
		ミッション情報 C) 自律飛行用ウェイポイント・イベント等 ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		テレメトリデータ A) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス２：通常の産業利用に影響するもの	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		テレメトリデータ B) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス３：災害救助、警備業務など、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		地上制御局のプログラムコード	2	2	2	**2**	・機密性：主力製品のプログラムであり、流出すると他社との差別化ができなくなり、売上が減少する ※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品が使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		センサ取得情報 A) 測量データなど飛行制御に関係しない情報	0	0	0	**0**	
		センサ取得情報 B) 対象設備との測位距離など、飛行制御に影響する情報 ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの	1	1	1	**1**	・機密性：センサ取得情報の漏えいにより、設備の場所等が解析され、設備への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、周辺設備との衝突など、周辺被害やドローンの利用目的の達成に支障が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		センサ取得情報 C) レーザセンサ、赤外線センサなど、警備や被災状況の把握、人命救助に利用される情報 ※クラス３：　警備業務、災害救助業務など、人命や安全に影響するもの	0	2	2	**2**	・機密性：センサ取得情報自体の機密性は低い ・完全性：改ざんによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる ・可用性：データにアクセスできなくなることによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる
		機能・サービス	0	2	2	**2**	・機密性：提供される機能やサービスは開示されており、漏洩による影響はない ・完全性：データによっては改ざんによって、提供機能やサービスが損なわれ、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品の機能やサービスが使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する
		機器本体（ハードウェア）	1	2	0	**2**	・機密性：ハードウェアから、差別化要素となる機器の仕様や攻撃に利用可能な情報が漏えいし、売上の低下や製品の信頼性の失墜につながる可能性がある。※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：ハードウェアの改ざんによって、提供機能やサービスが損なわれ、製品の信頼性を失う可能性があり、売上が減少する

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							・可用性：ハードウェアについては、一般的に攻撃後の可用性担保までは対応困難であり、影響は少ない。※可用性については、メーカによる保証などのビジネスコンディションによって判断される。
	二次資産	認証情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		復号鍵（秘密鍵）、検証鍵（公開鍵、ハッシュ）	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		デジタル証明書	0	1	1	**1**	・機密性：公開情報であり、機密性はない ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
ドローン運用クラウド	一次資産	アップデート用プログラムコード	0	2	2	**2**	・機密性：アップデートプログラムは公開された URL よりダウンロード可能であり、機密性は低い ・完全性：改ざんによって、製品の信頼性を失う可能性があり、売上が減少する ・可用性：データにアクセスできなくなることによって、その間アップデートが利用できなくなる可能性がある。（製品の信頼性を失う可能性があり、売上が減少）
		セキュリティ上の設定情報	1	2	2	**2**	・機密性：設定値の漏えいによって、攻撃方法の解析に利用される可能性がある ・完全性：設定値の改ざんによって、クラウドのセキュリティ機能が、重大な影響が生じる

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							・可用性：データにアクセスできなくなることによって、セキュリティ機能の設定変更が行えなくなる可能性や、機能が無効化される可能性がある
		アクセスログ等の監査情報	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんにより、セキュリティ監査や運用監視上の証跡としての信頼性を失う ・可用性：データにアクセスできなくなることによって、セキュリティ監査や運用監視上の証跡が失われる
		機能・サービス	0	2	2	**2**	・機密性：提供される機能やサービスは開示されており、漏洩による影響はない ・完全性：データによっては改ざんによって、提供機能やサービスが損なわれ、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品の機能やサービスが使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する
	二次資産	認証情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		復号鍵（秘密鍵）、検証鍵（公開鍵、ハッシュ）	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		デジタル証明書	0	1	1	**1**	・機密性：公開情報であり、機密性はない ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							がある。
サービス運用クラウド	一次資産	記録映像 A) ※個人情報、肖像権や個人のプライバシ、業務機密に影響しないもの、並びに災害救助、警備業務などの安全に影響しないもの	0	0	0	**0**	
		記録映像 B) ※個人情報あるいは個人情報に類する情報、肖像権や個人のプライバシ、業務機密に影響するもの 例）特定の個人を識別可能な映像、画像、プライバシや業務機密が写りこんだ映像、画像）	2	1	1	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。 ・完全性：改ざんによって、ドローンの利用目的が達成できない可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		記録映像 C) ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い　※地方自治体等のルールに準じた対応が必要 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		記録映像 D) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	2	2	**2**	・機密性：記録映像の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備や施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		テレメトリデータA) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス２：通常の産業利用に影響するもの	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		テレメトリデータB) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス３：災害救助、警備業務など、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		セキュリティ上の設定情報	1	2	2	**2**	・機密性：設定値の漏えいによって、攻撃方法の解析に利用される可能性がある ・完全性：設定値の改ざんによって、クラウドのセキュリティ機能が、重大な影響が生じる ・可用性：データにアクセスできなくなることによって、セキュリティ機能の設定変更が行えなくなる可能性や、機能が無効化される可能性がある
		アクセスログ等の監査情報	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんにより、セキュリティ監査や運用監視上の証跡としての信頼性を失う ・可用性：データにアクセスできなくなることによって、セキュリティ監査や運用監視上の証跡が失われる
		地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果	2	1	1	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。 ・完全性：改ざんによって、ドローンの利用目的が達成できない可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		顧客情報	2	2	2	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。また漏えいによ

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		顧客の個人情報、サービスの受発注情報など ※医療物資搬送の業務では、医薬品名等も要配慮個人情報に類するものとして管理が必要となる。					って、対象顧客にも重大な影響が生じる。 ・完全性：改ざんによって、サービスの利用目的の達成に重大な支障が生じる可能性がある ・可用性：データにアクセスできなくなることによって、サービスの利用目的の達成に重大な支障が生じる可能性がある
		機能・サービス	0	2	2	**2**	・機密性：提供される機能やサービスは開示されており、漏洩による影響はない ・完全性：データによっては改ざんによって、提供機能やサービスが損なわれ、製品の信頼性を失う可能性があり、売上が減少する ・可用性：製品の機能やサービスが使用できなくなり、製品の信頼性を失う可能性があり、売上が減少する
	二次資産	認証情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		復号鍵（秘密鍵）、検証鍵（公開鍵、ハッシュ）、商品受領用の鍵情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		デジタル証明書	0	1	1	**1**	・機密性：公開情報であり、機密性はない ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
各構成要素間の通信経路	一次資産	記録映像 A) ※個人情報、肖像権や個人のプライバシ、業務機密に影響しないもの、並びに災害救助、警備業務などの安全に影響しないもの	0	0	0	**0**	
		記録映像 B) ※個人情報あるいは個人情報に類する情報、肖像権や個人のプライバシ、業務機密に影響するもの 例）特定の個人を識別可能な映像、画像、プライバシや業務機密が写りこんだ映像、画像）	2	1	1	**2**	・機密性：漏洩によって、個人情報保護法による管理義務に抵触する。 ・完全性：改ざんによって、ドローンの利用目的が達成できない可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		記録映像 C) ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い　※地方自治体等のルールに準じた対応が必要 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		記録映像 D) ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	2	2	**2**	・機密性：記録映像の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備や施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる
		センサ取得情報 A) 測量データなど飛行制御に関係しない情報	0	0	0	**0**	

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		センサ取得情報 B) 対象設備との測位距離など、飛行制御に影響する情報 ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの	1	1	1	**1**	・機密性：センサ取得情報の漏えいにより、設備の場所等が解析され、設備への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、周辺設備との衝突など、周辺被害やドローンの利用目的の達成に支障が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的が達成できない可能性がある
		センサ取得情報 C) レーザセンサ、赤外線センサなど、警備や被災状況の把握、人命救助に利用される情報 ※クラス３：　警備業務、災害救助業務など、人命や安全に影響するもの	0	2	2	**2**	・機密性：センサ取得情報自体の機密性は低い ・完全性：改ざんによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる ・可用性：データにアクセスできなくなることによって、警備業務や被害状況の把握、人命救助等、ドローンの利用目的の達成に重大な支障が生じる
		位置情報	1	1	1	**1**	・機密性：位置情報の漏洩により、プライバシ侵害とみなされる可能性がある。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		フライトログ A) ※クラス２：通常の産業利用に影響するもの	1	1	1	**1**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、プライバシ侵害とみなされる可能性がある。※機密性については、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		フライトログ B) ※クラス２：公共性の高い設備、機器の点検業務	2	1	1	**2**	・機密性：ログからドローンの挙動に関する仕様の解析が行われる可能性がある。位置情報の漏洩により、侵入や攻撃の経路を解析される可能性がある。※機密性について

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの					は、メーカのビジネスコンディションによって判断される。 ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		ミッション情報 A) 自律飛行用ウェイポイント・イベント等 ※クラス２：通常の産業利用に影響するもの	0	2	1	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある。 ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある
		ミッション情報 B) 自律飛行用ウェイポイント・イベント等 ※クラス２：公共性の高い設備、機器の点検業務において、社会的な影響が大きいもの ※クラス３：警備、監視業務などにおいて、対象の人命や安全に影響するもの	2	2	2	**2**	・機密性：ミッション情報の漏えいにより、設備の場所や警備、監視地点、飛行ルート等が解析され、設備、施設への攻撃（侵入）に利用される恐れがある。 ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、公共性の高い設備への重大な影響、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、公共性の高い設備への重大な影響、人命や安全上の影響が生じる
		ミッション情報 C) 自律飛行用ウェイポイント・イベント等 ※クラス３：災害救助業務において、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		テレメトリデータ A) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス２：通常の産業利用に影響するもの	0	1	1	**1**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの運用に支障が生じる可能性がある ・可用性：データにアクセスできなくなることによって、ドローンの運用に支障が生じる可能性がある

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
		テレメトリデータ B) 機首の方向、水平距離、高度、バッテリ残量等 ※クラス３：災害救助、警備業務など、対象の人命や安全に影響するもの	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		空域情報、警報情報	0	2	2	**2**	・機密性：漏洩による直接の影響は低い ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
		アップデート用のプログラムコード	0	2	2	**2**	・機密性：アップデートプログラムは公開された URL よりダウンロード可能であり、機密性は低い ・完全性：改ざんによって、製品の信頼性を失う可能性があり、売上が減少する ・可用性：データにアクセスできなくなることによって、その間アップデートが利用できなくなる可能性がある。（製品の信頼性を失う可能性があり、売上が減少）
		制御信号 ※制御信号の通信については本書対象外	2	2	2	**2**	・機密性：機密情報であるドローンの制御に関する仕様が解析される可能性がある ・完全性：改ざんによって、ドローンの利用目的に支障が発生し、人命や安全上の影響が生じる ・可用性：データにアクセスできなくなることによって、ドローンの利用目的達成に支障が発生し、人命や安全上の影響が生じる
	二次資産	認証情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性

構成要素	資産種別	情報	評価値			総合評価値	重要度判断の例
			C 機密性	I 完全性	A 可用性		
							がある。
		復号鍵（秘密鍵）、検証鍵（公開鍵、ハッシュ）、商品受領用の鍵情報	2	1	1	**2**	・機密性：漏洩によって、重要な機能や他のデータ流出につながる可能性がある ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。
		デジタル証明書	0	1	1	**1**	・機密性：公開情報であり、機密性はない ・完全性：改ざんによって、認証機能に利用できなくなる可能性がある。 ・可用性：データにアクセスできなくなることによって、認証機能に利用できなくなる可能性がある。

4.3 システムモデルによるリスク発生箇所の分析

守るべき資産の検討後、システムモデルをもとにリスクの発生箇所の分析を行う。システムモデルは、対象機器やその周辺機器に限らず、サービス提供に利用されるクラウドなどのサブシステムを含めたシステム全体を俯瞰し、検討対象とする。

無人航空機システムにおいてリスクが発生する箇所は下記が想定されるが、本内容では参考文献[28]をもとに本書独自で考察を行った内容となる。

- **対象機器における入出力インタフェース：**機器に対する入出力インタフェースを介した攻撃・侵入の入り口となる可能性
  例：Ethernet、無線 LAN（Wi-Fi）、Bluetooth、IrDA、USB、SD カード、JTAG など
- **対象機器の基板、回路上に存在する伝送経路：**機器の電子基板上の伝送経路に対する攻撃・侵入の入り口となる可能性
  例：CPU Bus、Memory Bus など
- **システム構成上の通信経路**：中間者攻撃など、経路上での情報漏洩、改ざんの可能性

無人航空機システムの各構成要素において、想定されるリスク発生箇所の例を図 4-2、図 4-3、図 4-4 に示す。また各構成要素間の通信経路において想定されるリスク発生箇所の例を図 4-5 に示す。なお、制御信号通信モジュール及び GNSS については、耐空性に影響する領域であり、本書では対象範囲外とし、通信経路を含めてリスク発生箇所の分析から除外している。

[28] Michael Howard, Jon Pincus, Jeannette M. Wing "Measuring Relative Attack Surface"
https://www.researchgate.net/publication/227020448_Measuring_Relative_Attack_Surfaces

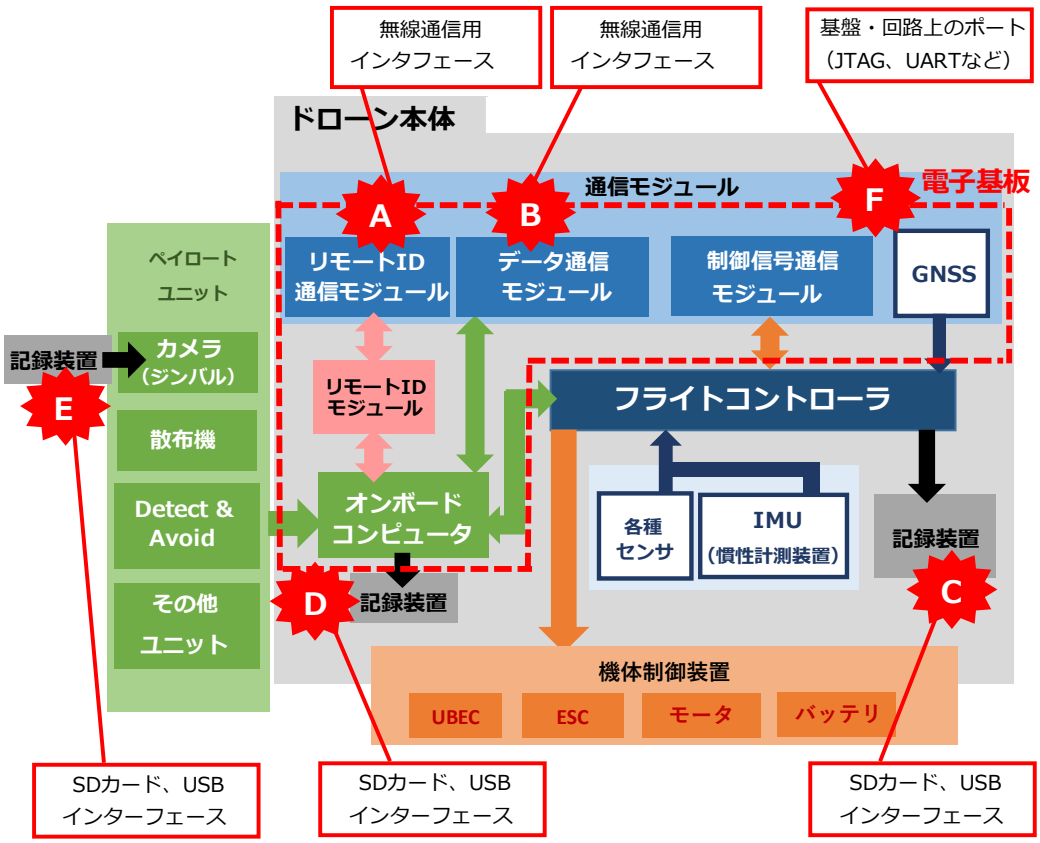


図 4-2 ドローン本体、地上制御局における攻撃ポイント例

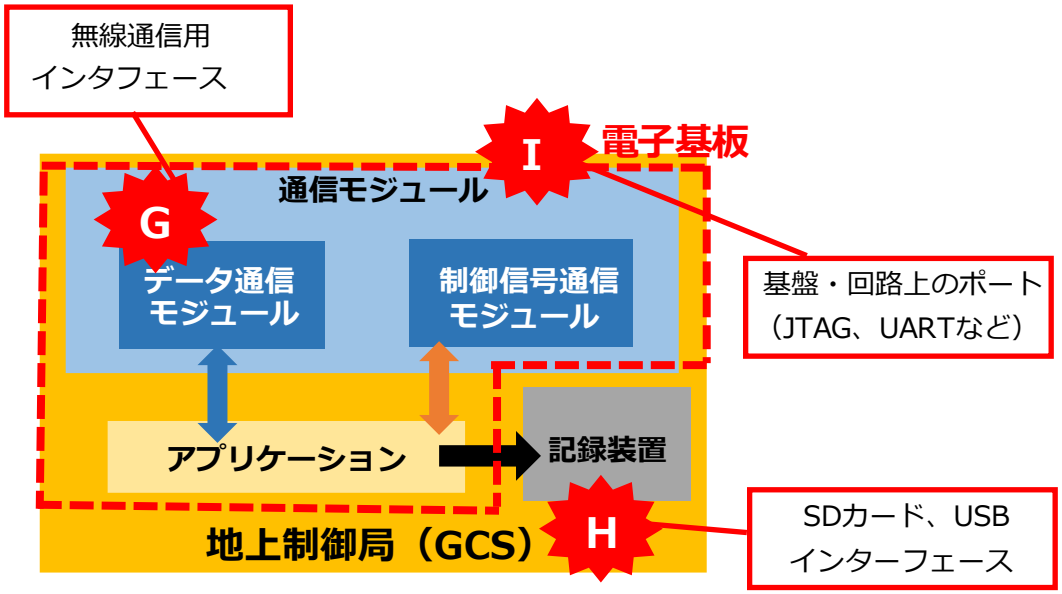


図 4-3 地上制御局における攻撃ポイントの例

図 4-4 クラウドシステムにおける攻撃ポイントの例

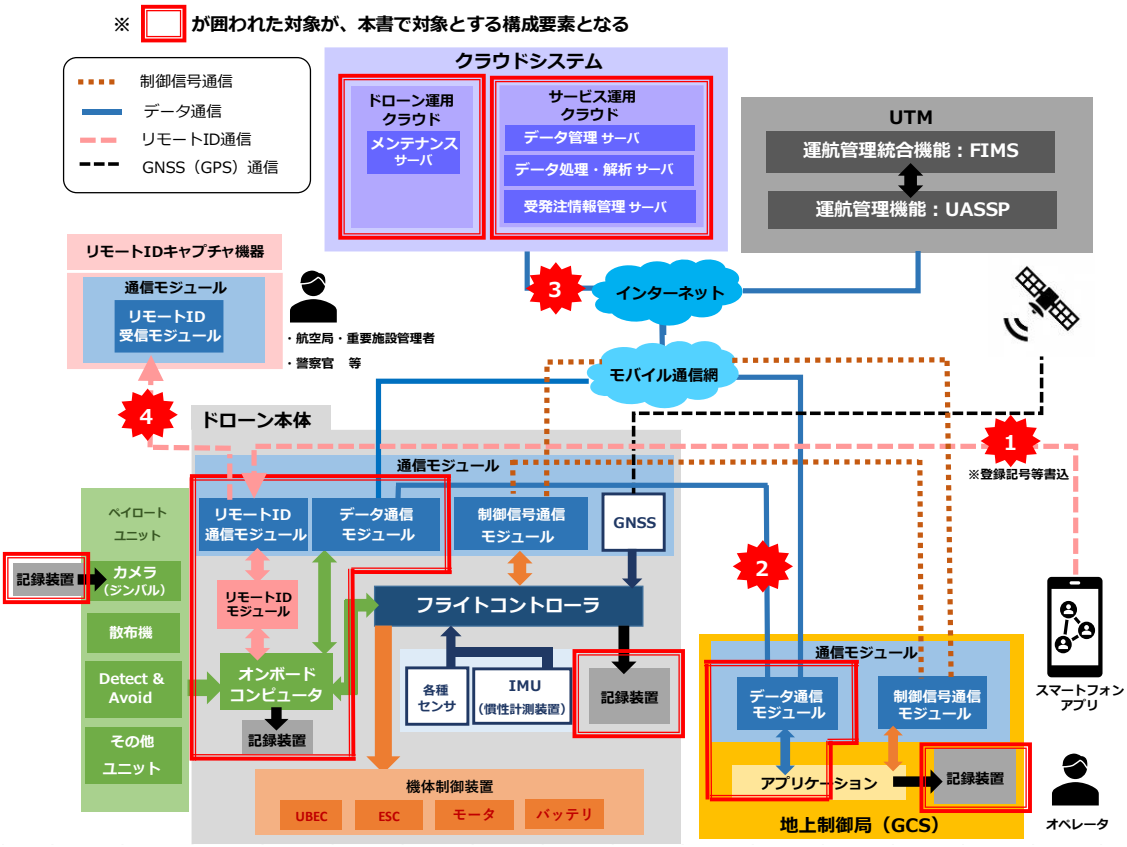


図 4-5 無人航空機システムの通信経路における攻撃ポイント例

補足事項）モバイル通信網による通信は、国内通信キャリアよってセキュリティ強度の高い認証

（RADIUS[29]など）及び、通信経路の暗号化（排他的論理和によるストリーム暗号方式）によって対策されているため、攻撃ポイント除外している。また、UTM とインターネット間の通信経路は本書対象外として、検討範囲から除外している。

4.4 守るべき資産に対する想定リスクの分析

本節では発生箇所において想定されるリスクの分析を行う。想定リスクの分析については、マイクロソフトが考案した脅威分類モデル「STRIDE モデル」[30]を参考とし、カスタマイズしたモデルを用いて分析の指標とする。実施手順としては、第 4.3 節で抽出した各発生箇所において、脅威分類モデルをガイドワードとして順にあてはめていき、該当する脅威の抽出を行っていく。

以下に脅威分類の検討方法については、考慮すべきポイントを示す。

- **無人航空機や関連 IoT 分野の事例から、各発生箇所において、それぞれの脅威が該当する可能性はあるか**
- **一つの脅威に起因し、複数の脅威が該当する場合には、それぞれを漏れなく抽出できているか**

一つの脅威に起因し、複数の脅威の可能性がある場合であっても、それぞれの脅威に応じて異なるセキュリティ機能の実装や対策が必要となる可能性があるため、該当するものを漏れなく抽出することが必要となる。

表 4-4 脅威分類モデル（STRIDE モデルをもとにしたカスタマイズモデル）

脅威名称	英語表記	説明
なりすまし	**S**poofing	コンピュータに対し、他のユーザを装うこと
データの改ざん	**T**ampering with Data	権限なしでデータを改ざんし、データの完全性を失わせること
否認	**R**epudiation	ユーザがあるアクションを行ったことを否認し、相手はこのアクションを証明する方法がないこと
情報の暴露(漏洩)	**I**nformal Disclosure	アクセス権限を持たない個人に情報が公開されること
サービス不能	**D**enial of Service	正規のユーザがサーバやサービスにアクセスできないこと
権限の昇格	**E**levation of Privilege	権限のないユーザがアクセス権限を得ること
不正アクセス	Unauthorized access	アクセス権限を持たない者にアクセスされること
マルウェア感染	Malware infection	他の機器への汚染源になる。ランサムウェアなど

[29] RADIUS：RFC 2865 等で規定されたユーザ認証の認証プロトコル
https://tools.ietf.org/html/rfc2865

[30] STRIDE：マイクロソフト提唱による脅威分類モデル
https://docs.microsoft.com/ja-jp/security-updates/planningandimplementationguide/19871865

脅威名称	英語表記	説明
		により業務妨害を受けること
踏み台	Stepping stone attack	他の機器へ不正アクセス等を行う際の中継地点として使用されること
不正改造 (HW/SW)	Tampering with device	不正（違法）なハード、ソフトウェアの改造により、内部データを抜き取りや、脆弱性の要因を組み込まれること

4.5 攻撃シナリオの検討

次のステップとして、脅威分類に対する攻撃シナリオを検討する。攻撃シナリオの検討手順としては、まず回避しなければならない被害を列挙し、その被害を発生させる複数の攻撃シナリオの抽出を行う。

以下に攻撃シナリオの検討にあたり、考慮すべきポイントを示す。

- **無人航空機や関連 IoT 分野において過去の脆弱性報告事例を参照し、どのような攻撃が想定されるのか。**
- **攻撃方法に対して、影響を受ける対象は構成要素のみに留まるのか、それとも機器に接続された他の要素やシステムにも影響が発生しうるのか。**
- **具体的に攻撃の影響を受ける資産は、どのような資産が想定されるのか。**

表 4-5 から表 4-9 に脅威分類モデルを用いて、システムモデルを対象にリスク分析を行った例を示す。本書の攻撃シナリオは、検討の一例として全体の網羅性を確保できる粒度で記載を行っているが、攻撃シナリオを更に複数の攻撃手順に分解（攻撃ツリー）し、AND 条件や OR 条件で細分化を行う場合もある。また本書の攻撃シナリオについては無人航空機分野や IoT 分野において、実際に報告があった内容（研究報告を含む）を記載している。なお、本書では非耐空性のセキュリティ領域を対象とし、システムモデルにおいて分析の対象を明確に区分しているが、想定されるリスク（表 4-2）が、結果として耐空性にも影響する可能性がある項目については、「耐空性への影響」の欄に「影響有り」としている。

表 4-5 ドローン本体における攻撃シナリオの検討例

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
A	無線通信用インタフェース（リモート ID 通信）	不正アクセス	リモート ID 通知に関する機能・サービス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域へ不正にアクセスされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領域へ不正にアクセスされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域へ不正にアクセスされる。	–
		情報の暴露	鍵情報（リモート ID）	ドローン本体のメモリ領域から、リモート ID の鍵情報が窃取される。	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域から秘匿すべき情報が窃取される。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領域上の秘匿すべき情報が窃取される。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域上の秘匿すべき情報が窃取される。	–
		データ改ざん	リモート ID	ドローン本体のメモリ領域から、リモート ID の値を改ざんされる。	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域から情報が改ざんされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領	–

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
					域上の情報が改ざんされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域上の情報が改ざんされる。	
		サービス不能	リモート ID の通知に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、リモート ID 通知に関する機能に影響が生じる。	・無線 LAN リクエストを繰り返し送信し、CPU へ負荷を与える DoS 攻撃が行われる。 ・ Wi-Fi の DeAuthentication（認証解除）フレームを繰り返し送信し、DoS 攻撃が行われる。 ・アプリケーションからバッファ容量を超えるサイズのパケットを送信する DoS 攻撃が行われる。	－
		マルウェア感染	リモート ID の通知に関する機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	・Android 等の汎用的な OS を使用している場合に、無線通信用インタフェースを経由し、マルウェアに感染する可能性がある。 ・接続機器がドローン本体の OS と同じものを利用している場合に二次感染につながる。	影響有り
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者へ	・Android 等の汎用的な OS を利用している場合に、「Sockbot」等のボットネットに感染し、攻撃の踏み台に利用される。	－

発生箇所		脅威分類	影響を受ける 守るべき資産	想定される被害	攻撃シナリオ例	耐空性への 影響
No.	対象					
				の攻撃行為、不正な情報送信による漏洩など。		
B	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域へ不正にアクセスされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領域へ不正にアクセスされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域へ不正にアクセスされる。	－
		情報の暴露	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、プログラムコード上の機密情報漏洩など	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域から秘匿すべき情報が窃取される。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領域上の秘匿すべき情報が窃取される。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域上の秘匿すべき情報が窃取される。	－
		データ改ざん	・フライトログ ・記録映像、	ドローン本体のメモリ領域から、フライトログや記録映像、	・認証や暗号化機能が未実装な機器に対して、ドローン本体のメモリ領域から情報が改ざんされる。	－

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	オンボードコンピュータのプログラムコードなどを改ざんされる。 ※プログラムコードの改ざんによる著作権の侵害など	・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、ドローン本体のメモリ領域上の情報が改ざんされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリ領域上の情報が改ざんされる。	
		なりすまし	オンボードコンピュータのプログラムコード	攻撃者が地上制御局になりすましオンボードコンピュータに対する不正な指示が行われる。	・ソフトウェア無線のプロトコルが解析され、なりすまされた地上制御局からオンボードコンピュータに対する不正な指示が行われる。	–
		サービス不能	機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体の機能に影響が生じる。	・無線 LAN リクエストを繰り返し送信し、CPU へ負荷を与える DoS 攻撃が行われる。 ・ Wi-Fi の DeAuthentication（認証解除）フレームを繰り返し送信し、DoS 攻撃が行われる。 ・アプリケーションからバッファ容量を超えるサイズのパケットを送信する DoS 攻撃が行われる。	–
		権限の昇格	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード	オンボードコンピュータの OS に対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソ	・Android 等の汎用的な OS を使用している場合に、既知の脆弱性を組み合わせた攻撃により、権限昇格やバックドアの設置等の攻撃が行われる。	–

発生箇所		脅威分類	影響を受ける 守るべき資産	想定される被害	攻撃シナリオ例	耐空性への 影響
No.	対象					
			・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ースの OS を使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。		
		マルウェア感染	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	・Android 等の汎用的な OS を使用している場合に、無線通信用インタフェースを経由し、マルウェアに感染する可能性がある。 ・接続機器がドローン本体の OS と同じものを利用している場合に二次感染につながる。	影響有り
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	・Android 等の汎用的な OS を利用している場合に、「Sockbot」等のボットネットに感染し、攻撃の踏み台に利用される。	–
C	SD/USB インタフェース	情報の暴露	フライトログ	落下したドローン本体の SD/USB メディアが回収さ	・落下したドローン本体の SD/USB メディアが回収され、フライトログが窃取される。	–

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
	（フライトコントローラの記録装置）			れ、フライトログ等の漏洩につながる可能性がある。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。		
		マルウェア感染	・フライトログ ・機能・サービス	マルウェアが組み込まれたSD/USB メディアとの接続により、ドローン本体のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	・システム更新上の脆弱性（レースコンディション）を突き、USB 経由でドローン本体のファームウェアの書き換えが行われる。 ・Android 等、汎用的な OS を使用している場合に、USB 経由でマルウェアの感染につながる。	影響有り
D	SD/USB インタフェース（オンボードコンピュータの記録装置）	情報の暴露	オンボードコンピュータのプログラムコード	落下したドローン本体のSD/USB メディアが回収され、オンボードコンピュータのプログラムコードの漏洩につながる可能性がある。	・落下したドローン本体の SD/USB メディアが回収され、オンボードコンピュータのプログラムコードが窃取される。	–
		マルウェア感染	・オンボードコンピュータのプログラムコード	マルウェアが組み込まれたSD/USB メディアとの接続に	・システム更新上の脆弱性（レースコンディション）を突き、USB 経由でオンボードコンピュータのソフト	影響有り

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			・機能・サービス	より、オンボードコンピュータのマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	ウェア、ファームウェアの書き換えが行われる。 ・Android 等、汎用的な OS を使用している場合に、USB 経由でマルウェアの感染につながる。	
E	SD/USB インタフェース（カメラの記録装置）	情報の暴露	・記録映像	落下したドローン本体の SD/USB メディアが回収され、記録映像の漏洩につながる可能性がある※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	・落下したドローン本体の SD/USB メディアが回収され、記録映像が窃取される。	–
		マルウェア感染	・記録映像 ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、ドローン本体のマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常	・Android 等、汎用的な OS を使用している場合に、USB 経由でマルウェアの感染につながる。	影響有り

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
				動作や、不正な情報送信による漏洩など。		
F	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	・デバッグポートからシリアルコンソールに出力されるログ情報を解析され、フラッシュメモリ上のデータのダンプやメモリ上にロードしたファームフェアの抽出等の攻撃が行われる。	影響有り

表 4-6 地上制御局における攻撃シナリオの検討例

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
G	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・データ通信に関する機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	・認証や暗号化機能が未実装な機器に対して、地上制御局のメモリやファイル領域へ不正にアクセスされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、地上制御局のメモリやファイル領域へ不正にアクセスされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリやファイル領域へ不正にアクセスされる。	–
		情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード	地上制御局のメモリやファイル領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、機密情報やプログラムコードの漏洩による	・認証や暗号化機能が未実装な機器に対して、地上制御局のメモリやファイル領域から秘匿すべき情報が窃取される。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、地上制御局のメモリやファイル領域上の秘匿すべき情報が窃取される。 ・既知の脆弱性を突くことで認証や暗号機能を迂	–

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	著作権侵害など。	回し、メモリやファイル領域上の秘匿すべき情報が窃取される。	
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域から、フライトログや記録映像、プログラムコードなどを改ざんされる。※フライトログや設定情報、ミッション情報の改ざんによる飛行の妨害や、プログラムコードの漏洩による著作権侵害など。	・認証や暗号化機能が未実装な機器に対して、地上制御局のメモリやファイル領域から情報が改ざんされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、地上制御局のメモリやファイル領域上の情報が改ざんされる。 ・既知の脆弱性を突くことで認証や暗号機能を迂回し、メモリやファイル領域上の情報が改ざんされる。	影響有り
		なりすまし	データ通信に関する機能・サービス	攻撃者がドローン本体になりすまし、不正な情報が伝達される。 ※間接的には誤った情報（テレメトリなど）による、飛行操作や判断ミスなど。	・ソフトウェア無線のプロトコルが解析され、なりすまされたドローンから地上制御局へ不正な情報が伝達される。	－ 間接的には操作に影響

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
		サービス不能	データ通信に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体とのデータ通信が阻害される。	・無線 LAN リクエストを繰り返し送信し、CPU へ負荷を与える DoS 攻撃が行われる。 ・ Wi-Fi の DeAuthentication（認証解除）フレームを繰り返し送信し、DoS 攻撃が行われる。 ・アプリケーションからバッファ容量を超えるサイズのパケットを送信する DoS 攻撃が行われる。	－
		権限の昇格	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局の OS に対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースの OS を使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	・Android 等の汎用的な OS を使用している場合に、既知の脆弱性を組み合わせた攻撃により、権限昇格やバックドアの設置等の攻撃が行われる。	影響有り
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素	・Android 等の汎用的な OS を使用している場合に、無線通信用インタフェースを経由し、マルウェアに感染する可能性がある。	影響有り

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス	への二次感染の可能性がある。※地上制御局の異常動作や、不正な情報送信による漏洩など。	・接続機器が地上制御局の OS と同じものを利用している場合に二次感染につながる。	
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素に対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	・Android 等の汎用的な OS を利用している場合に、「Sockbot」等のボットネットに感染し、攻撃の踏み台に利用される。	–
H	SD/USB インタフェース（記録装置）	情報の暴露	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	SD/USB の盗難、紛失によって、保存された情報の漏洩につながる。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	・SD/USB メディアの盗難、紛失によって、フライトログや記録映像などが窃取される。	–
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等）	マルウェアが組み込まれた SD/USB メディアとの接続により、地上制御局のマルウェア感染につながるまたドローン	・システム更新上の脆弱性（レースコンディション）を突き、USB 経由でドローン本体のファームウェアの書き換えが行われる。 ・Android 等、汎用的な OS を使用している場合	影響有り

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			・ミッション情報 ・センサ取得情報 ・機能・サービス	本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	に、USB 経由でマルウェアの感染につながる。	
I	基盤・回路上のポート（ JTAG 、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	・デバッグポートからシリアルコンソールに出力されるログ情報を解析され、フラッシュメモリ上のデータのダンプやメモリ上にロードしたファームフェアの抽出等の攻撃が行われる。	影響有り

表 4-7 ドローン運用クラウドにおける攻撃シナリオの検討例

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
J	インターネット通信用インタフェース	不正アクセス	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域へ不正にアクセスされる。 ・既知の脆弱性を突くことで認証やアクセス制御を迂回し、サーバのファイル領域へ不正アクセスされる。 ・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバへの不正アクセスが行われる。	－
		情報の暴露	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバのファイル領域から、アップロード用のプログラムなどの秘匿すべき情報が窃取される。	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域から秘匿すべき情報が窃取される。 ・既知の脆弱性を突くことで認証やアクセス制御を迂回し、サーバのファイル領域から秘匿すべき情報が窃取される。 ・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバのファイル領域から秘匿すべき情報が窃取される。	－
		データの改ざん	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	サーバのファイル領域からアップロード用のプログラムなどを改ざんされる。※アップロード	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域の情報が改ざんされる。 ・既知の脆弱性を突くことで認証やアクセス制御を	影響有り

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
				用プログラムコードの改ざんによる著作権侵害に加えて、不正なプログラムが無人航空機にインストールされるなど。	迂回し、サーバのファイル領域の情報が改ざんされる。 ・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバのファイル領域の情報が改ざんされる。	
		サービス不能	機能・サービス	DoS 攻撃により、ドローン運用クラウドの運用が阻害される。※クラウドの機能障害による、アップデートの実行不可など。	・大量のパケットを送信することで、ネットワークやサーバ、DNS 等に負荷を与え、サービスの運用を阻害される。	–
		権限の昇格	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	・既知の脆弱性を組み合わせた攻撃により、権限昇格やバックドアの設置等の攻撃が行われる。	–
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサ	・インターネット通信用インタフェースを経由し、マルウェアに感染する可能性がある。	–

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
				ーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	・サーバに接続機器する構成機器や無線航空機システムに対する二次感染が発生する。	
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	・サーバがボットネットに感染し、攻撃の踏み台に利用される。	－

表 4-8 サービス運用クラウドにおける攻撃シナリオの検討例

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
K	インターネット通信用インタフェース	不正アクセス	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サービス運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある。	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域へ不正にアクセスされる。 ・既知の脆弱性を突くことで認証やアクセス制御を迂回し、サーバのファイル領域へ不正アクセスされる。 ・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバへの不正アクセスが行われる。	－
		情報の暴露	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名	サーバのファイル領域から、秘匿すべき記録映像や、データが窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、業務機密であるテレメトリデー	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域から秘匿すべき情報が窃取される。 ・既知の脆弱性を突くことで認証やアクセス制御を迂回し、サーバのファイル領域から秘匿すべき情報が窃取される。	－

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
			等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス、認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）、デジタル証明書	タの漏洩による信用失墜など。	・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバのファイル領域から秘匿すべき情報が窃取される。	
		データの改ざん	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など）	サーバのファイル領域から、記録映像や、データが削除あるいは改ざんされる。 ※記録映像や、業務機密であるテレメトリデータの改ざん、削除による信用失墜など。	・認証やアクセス制御が未実装なシステムにおいて、サーバのファイル領域の情報が改ざんされる。 ・既知の脆弱性を突くことで認証やアクセス制御を迂回し、サーバのファイル領域の情報が改ざんされる。 ・ブルートフォース攻撃や辞書攻撃などにより、認証情報が解析され、サーバのファイル領域の情報が改ざんされる。	–
		サービス不能	機能・サービス	DoS 攻撃により、サービスの提供が阻害される。※クラウドの機能障害によりサ	・大量のパケットを送信することで、ネットワークやサーバ、DNS 等に負荷を与え、サービスの運用を阻害される。	–

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
				ービス提供が阻害され、経済的損失につながるなど。		
		権限の昇格	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	・既知の脆弱性を組み合わせた攻撃により、権限昇格やバックドアの設置等の攻撃が行われる。	－
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機シス	・インターネット通信用インタフェースを経由し、マルウェアに感染する可能性がある。 ・サーバに接続機器する構成機器や無線航空機システムに対する二次感染が発生する。	－

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
				テムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。		
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	・サーバがボットネットに感染し、攻撃の踏み台に利用される。	–

表 4-9 無人航空機システムの通信経路における攻撃シナリオの検討例

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	攻撃シナリオ例	耐空性への影響
No.	対象					
1	ドローン本体とスマートフォン（タブレット）間の通信	データ改ざん	・リモート ID	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情報が改ざんされる。	–
2	ドローン本体と地上制御局間の通信経路（データ通信）	情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃により、通信経路上の秘匿すべき情報が窃取される。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、通信経路の中間者攻撃により、通信経路上の秘匿すべき情報が窃取される。	–
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	無線信号の傍受やインジェクション攻撃などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情報が改ざんされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情	–

			・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		報が改ざんされる。	
3	クラウドシステムとインターネット間の通信経路（データ通信）	情報の暴露	・アップデート用のプログラムコード ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃により、通信経路上の秘匿すべき情報が窃取される。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、通信経路の中間者攻撃により、通信経路上の秘匿すべき情報が窃取される。	－
		データ改ざん	・アップデート用のプログラムコード ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など）	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情報が改ざんされる。 ・WEP 等の脆弱な暗号方式を使用している場合に、暗号機能を迂回され、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情報が改ざんされる。	影響有り

			・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			
4	ドローン本体とリモート ID キャプチャ機器間の通信	情報の暴露	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃により、通信経路上の秘匿すべき情報が窃取される。	－
		データ改ざん	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	・認証や暗号化機能が未実装である場合に、通信経路の中間者攻撃やインジェクション攻撃により、通信経路上の情報が改ざんされる。	－

5 無人航空機分野におけるセキュリティ対策

第５章では、本書の第４章までに実施したリスク分析結果に対し、無人航空機システムの構成要素において必要とされるセキュリティ対策事項の検討結果を示す。また、対象ステークホルダーの組織的の活動において必要とされるセキュリティ対策事項について、リスク分析プロセスを含む検討結果を示す。

5.1 無人航空機システム上のリスクに対するセキュリティ対策の検討

本節では、これまでに実施したリスク分析結果をもとに、実装すべきセキュリティ機能や脆弱性への対策など、対象の無人航空機システムに求められる対策候補の検討を行う。

5.1.1 対策候補の選定における参考文献

表 5-1 に対策候補の検討にあたり、参考とした文献を示す。対策候補の導出手順としては、第 4.5 節までに検討を行ったリスク分析結果に対して、IoT 関連、航空機関連のセキュリティガイドラインを中心に、それぞれのリスクに対抗するため対策候補を抽出し、無人航空機分野へと適用している。なお、参照文書と対策候補の対応については、Appendix_A の第 6.1 節にセキュリティ要件の対応表として記載する。

表 5-1 対策候補の検討における参考文献

分野	対象文書	発行機関	発行日
IoT 関連	NISTIR 8259 “Foundational Cybersecurity Activities for IoT Device Manufactures “	米国商務省、米国国立標準技術研究（以下、NIST）	2020 年 5 月
IoT 関連	NISTIR 8259A “IoT Device Cybersecurity Capability Core Baseline”	NIST	2020 年 5 月
IoT 関連	”Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”	NIST	2022 年 2 月
IoT 関連	ETSI EN 303 645 ”Cyber Security for Consumer Internet of Things: Baseline Requirements”（V2.1.1）	欧州電気通信標準化機構（以下、ETSI）	2020 年 6 月
IoT 関連	IoT 分野共通セキュリティ要件ガイドライン 2021 年版	CCDS	2020 年 11 月

IoT 関連	IoT 機器セキュリティ実装ガイドライン(ソフトウェア更新機能)_1.0 版	CCDS	2020 年 12 月
航空機関連	AC-119-1 Operational Authorization of Aircraft Network Security Program (ANSP)	FAA	2015 年 9 月
航空機関連	ED-202A/ DO-326A AIRWORTHINESS SECURITY PROCESS SPECIFICATION	EUROCASE/RTCA	2014 年 6 月
航空機関連	ED-204A/ DO-355A INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS	EUROCASE/RTCA	2020 年 9 月

5.1.2 無人航空機システムのリスクに対する対策候補の検討

第 4.5 節で分析したリスクに対して、表 5-1 の文献を参考に、対策候補を適用した例を表 5-2 から表 5-6 に示す。

表 5-2 ドローン本体における想定リスクの対策候補例

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
A	無線通信用インタフェース（リモートID通信）	不正アクセス	リモートID通知に関する機能・サービス	－	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		情報の暴露	リモートIDの鍵情報	－	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		データ改ざん	リモートID	－	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用 UAV-R07-B：データ保護（本体）

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
					※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		サービス不能	リモートIDの通知に関する機能・サービス	－	UAV-R08：DoS 対策 UAV-R09：ログ記録 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		マルウェア感染	リモートIDの通知に関する機能・サービス	影響有り	UAV-R10：脆弱性診断 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		踏み台	※他の構成要素への影響	－	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
					※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
B	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	UAV-R11：アクセス制御 UAV-R12：機器認証 UAV-R13：セキュリティ設定の変更及び安全な初期設定への復元機能 UAV-R14：不要な TCP/UDP ポートの無効化 UAV-R15：不要な機能の無効化 UAV-R03：最新の Wi-Fi 認証方式を利用 UAV-R02：Bluetooth のセキュリティ対策 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		情報の暴露	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラム	－	UAV-R07-B：データ保護（本体） UAV-R16-B：データ消去機能（本体）

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
			コード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		データ改ざん	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	UAV-R07-B：データ保護（本体） UAV-R17：セキュアブート ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		なりすまし	オンボードコンピュータのプログラムコード	－	UAV-R13：機器認証 UAV-R14：セキュリティ設定の変更及び安全な初期設定への復元機能 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
		サービス不能	機能・サービス	−	UAV-R09：DoS 対策 UAV-R10：ログ記録 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		権限の昇格	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	−	UAV-R10：ログ記録 UAV-R11：脆弱性診断 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		マルウェア感染	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス	影響有り	UAV-R15：不要な機能の無効化 UAV-R17：セキュアブート ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
					UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
		踏み台	※他の構成要素への影響	－	UAV-R10：ログ記録 UAV-R11：アクセス制御 UAV-R12：機器認証 UAV-R13：セキュリティ設定の変更及び安全な初期設定への復元機能 ※問題発生後の事後対策として有効なもの UAV-R04：ソフトウェア更新機能 UAV-R05：ソフトウェアの真正性と完全性の検証 UAV-R06：電源停止や障害発生時の対応
C	SD/USB インタフェース（フライトコントローラの記録装置）	情報の暴露	フライトログ	－	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）
		マルウェア感染	フライトログ、機能・サービス	影響有り	UAV-R18：USB デバイスの不要機能の無効化
D	SD/USB インタフェース	情報の暴露	オンボードコンピュータのプログラムコード	－	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）
		マルウェア感染	・オンボードコンピュータのプログラムコード	－	UAV-R18：USB デバイスの不要機能の無効化

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
	（オンボードコンピュータの記録装置）		・機能・サービス		
E	SD/USB インタフェース（カメラの記録装置）	情報の暴露	記録映像	−	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）
		マルウェア感染	・記録映像 ・機能・サービス	影響有り	UAV-R18：USB デバイスの不要機能の無効化
F	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	影響有り	UAV-R16-B：データ消去機能（本体） UAV-R19：ハードウェアハッキング対策 UAV-R20：リバースエンジニアリング対策

表 5-3 地上制御局における想定リスクの対策候補例

攻撃ポイント		脅威分類	影響を受ける守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
G	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・データ通信に関する機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	GCS-R01：アクセス制御 GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定の変更及び安全な初期設定への復元機能 GCS-R05：不要な TCP/UDP ポートの無効化 GCS-R06：不要な機能の無効化 GCS-R07：最新の Wi-Fi 認証方式を利用 GCS-R08：Bluetooth のセキュリティ対策 ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
		情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード	－	GCS-R12-B：データ保護（本体） GCS-R13-B：データ消去機能（本体） ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
			・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	影響有り	GCS-R12-B：データ保護（本体） GCS-R14：セキュアブート ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
		なりすまし	データ通信に関する機能・サービス	－ 間接的には操作に影響	GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定の変更及び安全な初期設定への復元機能 ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
					GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
		サービス不能	データ通信に関する機能・サービス	－	GCS-R15：DoS 対策 GCS-R16：ログ記録 ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
		権限の昇格	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）	影響有り	GCS-R16：ログ記録 GCS-R17：脆弱性診断 ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
			・デジタル証明書		
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス	影響有り	GCS-R06：不要な機能の無効化 GCS-R14：セキュアブート ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能 GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
		踏み台	※他の構成要素への影響	－	GCS-R01：アクセス制御 GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定の変更及び安全な初期設定への復元機能 GCS-R16：ログ記録 ※問題発生後の事後対策として有効なもの GCS-R09：ソフトウェア更新機能

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
					GCS-R10：ソフトウェアの真正性と完全性の検証 GCS-R11：電源停止や障害発生時の対応
H	SD/USB インタフェース	情報の暴露	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	－	GCS-R12-S：データ保護（外部ストレージ） GCS-R13-S：データ消去機能（外部ストレージ）
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・機能・サービス	影響有り	GCS-R18：USB デバイスの不要機能の無効化
I	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	影響有り	GCS-R13-B：データ消去機能（本体） GCS-R19：ハードウェアハッキング対策 GCS-R20：リバースエンジニアリング対策

表 5-4 ドローン運用クラウドにおける想定リスクの対策候補例

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
J	インターネット通信用インタフェース	不正アクセス	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	DPF-R01：アクセス制御 DPF-R02：機器認証 DPF-R03：ユーザ認証 DPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 DPF-R05：不要なネットワーク接続、論理インタフェースの無効化 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		情報の暴露	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	DPF-R08：データ暗号化 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		データの改ざん	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	影響有り	DPF-R08：データ暗号化 ※問題発生後の事後対策として有効なもの

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
					DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		サービス不能	機能・サービス	−	DPF-R09：DoS 対策 DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		権限の昇格	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	−	DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録 DPF-R12：脆弱性診断 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		マルウェア感染	機能・サービス	−	

攻撃ポイント		脅威分類	影響を受ける	耐空性への影響	リスクへの対策候補
No.	対象		守るべき資産		
					DPF-R13：アンチマルウェア DPF-R14：不要なソフトウェアの無効化 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証
		踏み台	※他の構成要素への影響	－	DPF-R01：アクセス制御 DPF-R02：機器認証 DPF-R03：ユーザ認証 DPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録 ※問題発生後の事後対策として有効なもの DPF-R06：ソフトウェア更新機能 DPF-R07：ソフトウェアの真正性と完全性の検証

表 5-5 サービス運用クラウドにおける想定リスクの対策候補例

攻撃ポイント		脅威分類	影響を受ける守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
K	インターネット通信用インタフェース	不正アクセス	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	SPF-R01：アクセス制御 SPF-R02：機器認証 SPF-R03：ユーザ認証 SPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 SPF-R05：不要なネットワーク接続、論理インタフェースの無効化 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証
		情報の暴露	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名	－	SPF-R08：データ暗号化 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証

攻撃ポイント		脅威分類	影響を受ける守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
			等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス、認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）、デジタル証明書		
		データの改ざん	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など）	－	SPF-R08：データ暗号化 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証
		サービス不能	機能・サービス	－	SPF-R09：DoS 対策 SPF-R10：IDS/IPS（不正アクセス監視、遮断機能）

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
					SPF-R11：ログ記録 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証
		権限の昇格	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	SPF-R10：IDS/IPS（不正アクセス監視、遮断機能） SPF-R11：ログ記録 SPF-R12：脆弱性診断 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
		マルウェア感染	機能・サービス	−	SPF-R13：アンチマルウェア SPF-R14：不要なソフトウェアの無効化 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証
		踏み台	※他の構成要素への影響	−	SPF-R01：アクセス制御 SPF-R02：機器認証 SPF-R03：ユーザ認証 SPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 SPF-R10：IDS/IPS（不正アクセス監視、遮断機能） SPF-R11：ログ記録 ※問題発生後の事後対策として有効なもの SPF-R06：ソフトウェア更新機能 SPF-R07：ソフトウェアの真正性と完全性の検証

表 5-6 通信経路における想定リスクの対策候補例

攻撃ポイント		脅威分類	影響を受ける守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
1	ドローン本体とスマートフォン（タブレット）間の通信	データ改ざん	・リモート ID	–	UAV-R02：Bluetooth のセキュリティ対策
2	ドローン本体と地上制御局間の通信経路（データ通信）	情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	–	TP-R01：通信経路暗号化
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報	–	TP-R01：通信経路暗号化

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
			・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		
3	クラウドシステムとインターネット間の通信経路（データ通信）	情報の暴露	・アップデート用のプログラムコード ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	－	TP-R01：通信経路暗号化
		データ改ざん	・アップデート用のプログラムコード ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報	影響有り	TP-R01：通信経路暗号化

攻撃ポイント		脅威分類	影響を受ける 守るべき資産	耐空性への影響	リスクへの対策候補
No.	対象				
			・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		
4	ドローン本体とリモート ID キャプチャ機器間の通信	情報の暴露	リモート ID の鍵情報	–	UAV-R01：リモートＩＤ発信時の暗号化対応
		データ改ざん	リモート ID の鍵情報	–	UAV-R01：リモートＩＤ発信時の暗号化対応

5.1.3 無人航航空機システムにおけるセキュリティ要求事項の整理

第 5.1.2 項ではリスク分析結果をもとに対抗する対策候補を検討した（表 5-2 から表 5-6）。本項では、この対策候補を第 3 章で調査を行った無人航空機分野の特性から導出したセキュリティ対策と統合し、セキュリティ要求事項として整理を行った（表 5-7 から、表 5-10）。

表 5-7 ドローン本体に対するセキュリティ要求事項一覧

ID	対象インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応（表 3-14）
UAV-R01	無線通信用インタフェース（リモート ID 通信）	リモートＩＤ発信時の暗号化対応	LR-01：リモートＩＤ発信時の暗号化対応
UAV-R02	無線通信用インタフェース（データ通信）	Bluetooth のセキュリティ対策	TR-01 ：通信相手の適切な認証、識別
UAV-R03	無線通信用インタフェース（データ通信）	最新の Wi-Fi 認証方式を利用	VR-01：通信の暗号化、および、セキュアな暗号方式の採用
UAV-R04	無線通信用インタフェース（データ通信）	ソフトウェア更新機能	LR-04：ソフトウェアの更新機能を有する
UAV-R05	無線通信用インタフェース（データ通信）	ソフトウェアの真正性と完全性の検証	AR-01 ：無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する VR-04：ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装
UAV-R06	無線通信用インタフェース（データ通信）	電源停止や障害発生時の対応	LR-05：電力供給停止時も、アクセス制御機能の設定、更新ソフトウェアを維持する
UAV-R07-B	無線通信用インタフェース（データ通信）	データ保護（本体）	AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフ

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との 対応（表 3-14）
			ェースを物理的な改ざんから保護する VR-02：機密性の高い収集データの暗号化
AV-R07-S	SD/USB インタフェース	データ保護（外部ストレージ）	AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
UAV-R08	無線通信用 インタフェース （データ通信）	DoS 対策	VR-03：ネットワーク通信における一定の負荷試験の実施
UAV-R09	無線通信用 インタフェース （データ通信）	ログ記録	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
UAV-R10	無線通信用 インタフェース （データ通信）	脆弱性診断	VR-07：脆弱性診断の実施
UAV-R11	無線通信用 インタフェース （データ通信）	アクセス制御	LR-02：電気通信機能に係る設定変更については、アクセス制御機能を有する AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
UAV-R12	無線通信用 インタフェース （データ通信）	機器認証	TR-01：通信相手の適切な認証、識別 AR-02：無人航空機システムの

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との 対応（表 3-14）
			ソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
UAV-R13	無線通信用 インタフェース （データ通信）	セキュリティ設定の変更及び安全な初期設定への復元機能	LR-03：アクセス制御機能については、識別符号の初期値の変更を促す機能を有する
UAV-R14	無線通信用 インタフェース （データ通信）	不要な TCP/UDP ポートの無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
UAV-R15	無線通信用 インタフェース （データ通信）	不要な機能の無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
UAV-R16-B	無線通信用 インタフェース （データ通信）	データ消去機能（本体）	AR-07：無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ
UAV-R16-S	SD/USB インタフェース	データ消去機能（外部ストレージ）	AR-07：無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ
UAV-R17	無線通信用 インタフェース （データ通信）	セキュアブート	
UAV-R18	SD/USB インタフェース	USB デバイスの不要機能の無効化	

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との 対応（表 3-14）
UAV-R19	基盤・回路上のポート	ハードウェアハッキング対策	VR-06：ハードウェアハッキング対策
UAV-R20	基盤・回路上のポート	リバースエンジニアリング対策	VR-05：リバースエンジニアリング対策
UAV-R21 （TR-R01）	通信経路	通信経路暗号化	VR-01・TR-02：通信の暗号化、および、セキュアな暗号方式の採用 AR-04：無人航空機システムのソフトウェアの機密性の管理

表 5-8 地上制御局に対するセキュリティ要求事項一覧

ID	対象インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応(表 3-14)
GCS-R01	無線通信用インタフェース（データ通信）	アクセス制御	LR-02：電気通信機能に係る設定変更については、アクセス制御機能を有する AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
GCS-R02（TP-R02）	無線通信用インタフェース（データ通信）	機器認証	TR-01：通信相手の適切な認証、識別 AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
GCS-R03	無線通信用インタフェース（データ通信）	ユーザ認証	TR-01：通信相手の適切な認証、識別 AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
GCS-R04	無線通信用インタフェース（データ通信）	セキュリティ設定の変更及び安全な初期設定への復元機能	LR-03：アクセス制御機能については、識別符号の初期値の変更を促す機能を有する
GCS-R05	無線通信用インタフェース（データ通信）	不要な TCP/UDP ポートの無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
GCS-R06	無線通信用インタフェース（データ通信）	不要な機能の無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するの

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との 対応(表 3-14)
			に十分なセキュリティ対策を実装する
GCS-R07	無線通信用 インタフェース （データ通信）	最新の Wi-Fi 認証方式を利用	VR-01：通信の暗号化、および、セキュアな暗号方式の採用
GCS-R08	無線通信用 インタフェース （データ通信）	Bluetooth のセキュリティ対策	TR-01：通信相手の適切な認証、識別
GCS-R09	無線通信用 インタフェース （データ通信）	ソフトウェア更新機能	LR-04：ソフトウェアの更新機能を有する
GCS-R10	無線通信用 インタフェース （データ通信）	ソフトウェアの真正性と完全性の検証	R-01：無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する VR-04：ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装
GCS-R11	無線通信用 インタフェース （データ通信）	電源停止や障害発生時の対応	VR-02：機密性の高い収集データの暗号化 AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
GCS-R12-B	無線通信用 インタフェース （データ通信）	データ保護（本体）	AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との 対応(表 3-14)
			する VR-02：機密性の高い収集データの暗号化
GCS-R12-S	SD/USB インタフェース	データ保護（外部ストレージ）	AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
GCS-R13-B	無線通信用インタフェース（データ通信）	データ消去機能（本体）	AR-07：無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ
GCS-R13-S	SD/USB インタフェース	データ消去機能（外部ストレージ）	AR-07：無人航空機システムのコンポーネントの廃棄時に、アクセスキーコードやパスワードなどの機密データが、許可されていない担当者によって航空機のコンポーネントから解析されることを防ぐ
GCS-R13	無線通信用インタフェース（データ通信）	DoS 対策	VR-03：ネットワーク通信における一定の負荷試験の実施
GCS-R14	無線通信用インタフェース（データ通信）	セキュアブート	
GCS-R15	無線通信用インタフェース（データ通信）	DoS 対策	VR-03：ネットワーク通信における一定の負荷試験の実施
GCS-R16	無線通信用インタフェース	ログ記録	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応(表 3-14)
	（データ通信）		正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
GCS-R17	無線通信用インタフェース（データ通信）	脆弱性診断	VR-07：脆弱性診断の実施
GCS-R18	SD/USB インタフェース	USB デバイスの不要機能の無効化	
GCS-R19	基盤・回路上のポート	ハードウェアハッキング対策	VR-06：ハードウェアハッキング対策
GCS-R20	基盤・回路上のポート	リバースエンジニアリング対策	VR-05：リバースエンジニアリング対策
GCS-R21（TR-R01）	通信経路	通信経路暗号化	VR-01・TR-02：通信の暗号化、および、セキュアな暗号方式の採用 AR-04：無人航空機システムのソフトウェアの機密性の管理

表 5-9 ドローン運用クラウドに対するセキュリティ要求事項一覧

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応(表 3-14)
DPF-R01	インターネット通信用インタフェース	アクセス制御	LR-02：電気通信機能に係る設定変更については、アクセス制御機能を有する AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R02	インターネット通信用インタフェース	機器認証	TR-01：通信相手の適切な認証、識別 AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するの

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応 (表 3-14)
			に十分なセキュリティ対策を実装する
DPF-R03	インターネット通信用インタフェース	ユーザ認証	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R04	インターネット通信用インタフェース	アクセス制御機能の認証情報について、初期値の変更機能	LR-03：アクセス制御機能については、識別符号の初期値の変更を促す機能を有する
DPF-R05	インターネット通信用インタフェース	不要なネットワーク接続、論理インタフェースの無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R06	インターネット通信用インタフェース	ソフトウェア更新機能	LR-04：ソフトウェアの更新機能を有する
DPF-R07	インターネット通信用インタフェース	ソフトウェアの真正性と完全性の検証	AR-01：無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する VR-04：ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装
DPF-R08	インターネット通信用インタフェース	データ暗号化	VR-02：機密性の高い収集データの暗号化 AR-05: 無人航空機システムのコンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
DPF-R09	インターネット通信	DoS 対策	VR-03：ネットワーク通信における

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応 (表 3-14)
	用インタフェース		一定の負荷試験の実施
DPF-R10	インターネット通信 用インタフェース	IDS/IPS（不正アクセス監視、遮断機能）	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R11	インターネット通信 用インタフェース	ログ記録	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R12	インターネット通信 用インタフェース	脆弱性診断	VR-07：脆弱性診断の実施
DPF-R13	インターネット通信 用インタフェース	アンチマルウェア	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
DPF-R14	インターネット通信 用インタフェース	不要なソフトウェアの無効化	
DPF-R15 （TR-R01）	通信経路	通信経路暗号化	VR-01・TR-02：通信の暗号化、および、セキュアな暗号方式の採用 AR-04：無人航空機システムのソフトウェアの機密性の管理

表 5-10 サービス運用クラウドの対するセキュリティ要求事項一覧

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応 (表 3-14)
SPF-R01	インターネット通信 用インタフェース	アクセス制御	LR-02：電気通信機能に係る設定変更については、アクセス制御機能を有する AR-02：無人航空機システムのソフトウェアをデータ保存する際、不

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応 (表 3-14)
			正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R02	インターネット通信用インタフェース	機器認証	TR-01：通信相手の適切な認証、識別 AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R03	インターネット通信用インタフェース	ユーザ認証	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R04	インターネット通信用インタフェース	アクセス制御機能の認証情報について、初期値の変更機能	LR-03：アクセス制御機能については、識別符号の初期値の変更を促す機能を有する
SPF-R05	インターネット通信用インタフェース	不要なネットワーク接続、論理インタフェースの無効化	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R06	インターネット通信用インタフェース	ソフトウェア更新機能	LR-04：ソフトウェアの更新機能を有する
SPF-R07	インターネット通信用インタフェース	ソフトウェアの真正性と完全性の検証	AR-01：無人航空機システムのソフトウェア受信時にソフトウェアの真正性と完全性を確認する VR-04：ソフトウェア（ファームウェア）更新におけるセキュアな更新機能の実装
SPF-R08	インターネット通信用インタフェース	データ暗号化	VR-02：機密性の高い収集データの暗号化 AR-05: 無人航空機システムのコ

ID	対象 インタフェース	セキュリティ要求事項	第 3 章の要求事項との対応 (表 3-14)
			ンポーネントのデータ保存の際、安全な保管により、不正アクセスを防止する AR-06：無人航空機システムのコンポーネントとコンポーネントインタフェースを物理的な改ざんから保護する
SPF-R09	インターネット通信用インタフェース	DoS 対策	VR-03：ネットワーク通信における一定の負荷試験の実施
SPF-R10	インターネット通信用インタフェース	IDS/IPS（不正アクセス監視、遮断機能）	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R11	インターネット通信用インタフェース	ログ記録	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R12	インターネット通信用インタフェース	脆弱性診断	VR-07：脆弱性診断の実施
SPF-R13	インターネット通信用インタフェース	アンチマルウェア	AR-02：無人航空機システムのソフトウェアをデータ保存する際、不正アクセスを防止および検出するのに十分なセキュリティ対策を実装する
SPF-R14	インターネット通信用インタフェース	不要なソフトウェアの無効化	
SPF-R15 （TR-R01）	通信経路	通信経路暗号化	VR-01・TR-02：通信の暗号化、および、セキュアな暗号方式の採用 AR-04：無人航空機システムのソフトウェアの機密性の管理

5.2 組織の活動に関するセキュリティ対策の検討

無人航空機の製品ライフサイクルにおいて、一定水準のセキュリティ品質を確保するためには、製品本体やクラウドシステムについて、情報セキュリティ管理や製造プロセス管理、そして運用から廃棄にいたるサイクル全般での活動が求められる。本章では、無人航空機のメーカやサプライヤ、サービス事業者を対象とした製品開発のライフライクルごとのセキュリティ要求事項を定義する。本セキュリティ要求事項は以下の流れで定義する。

1. 無人航空機の製品ライフサイクルにおけるフェーズを定義する（5.2.1 項）
2. 4.2 節で抽出した守るべき資産に対し、各フェーズでのセキュリティ上の脅威とセキュリティ要求事項を導出する（5.2.2 項及び 5.2.3 項）

なお、セキュリティ活動指針のフェーズごとの分類については、経済産業省「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」を参考に、製品ライフサイクルにおけるフェーズに分けて要求事項を整理している。IoT セキュリティ・セーフティ・フレームワークでは、「発生したインシデントの影響の回復困難性の度合い」と「発生したインシデントの経済的影響の度合い」を元にシステムや機器の重要度をカテゴライズし、セキュリティ・セーフティ要求を複数の観点から分類している（図 5-1）。本書ではこれらの観点に対し、製品ライフサイクルのフェーズにセキュリティ要求事項を割り当てて分類している。

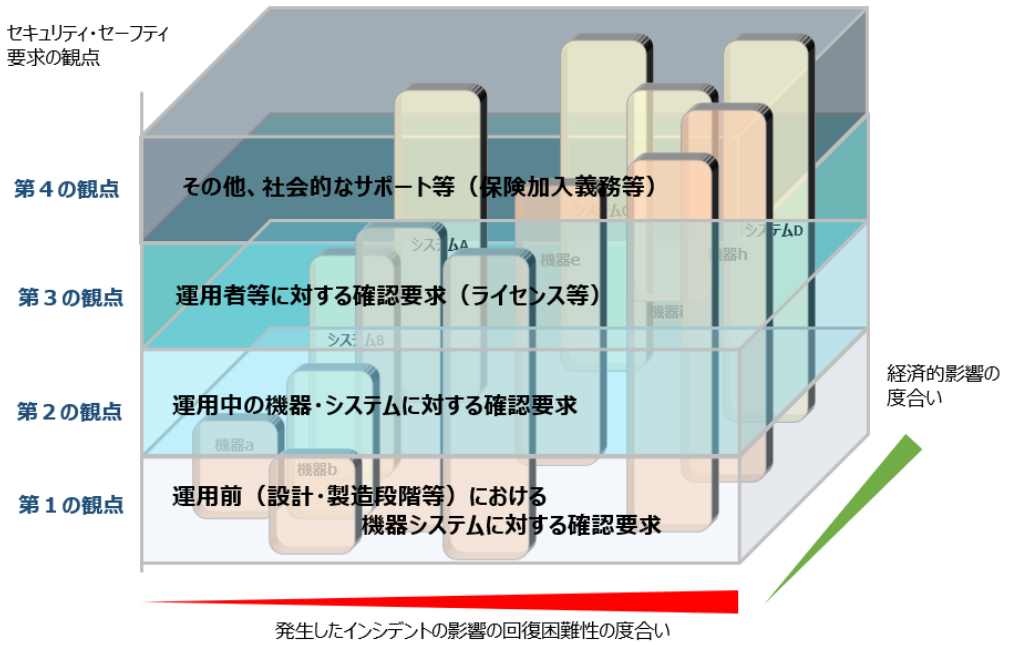


図 5-1 カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ

（出典：経済産業省「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）Ver1.0」[31]）

[31] 経済産業省「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）Ver1.0」
https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf

5.2.1 製品ライフライクルにおけるフェーズの定義

本項では、無人航空機の製品ライフライクルにおけるフェーズを定義する。定義した各フェーズを図 5-2、表 5-11 に示す。無人航空機の製品開発ライフサイクルは、大きく「製品企画」、「設計・製造」、「評価」、「運用・保守」、「廃棄」の 5 フェーズに分類される。製品や関連サービスにおいて十分なセキュリティを確保するためには、各フェーズにおいて企業としての方針・計画策定や、法令遵守すべき要件、運用体制等の幅広い範囲において対策を施し、製品のセキュリティ品質を確実なものとすべきである。

図 5-2 無人航空機の製品ライフサイクルにおけるフェーズ定義

表 5-11 無人航空機の製品ライフサイクルにおける各フェーズ説明

フェーズ	説明
製品企画	製品のコンセプト、要件定義、ユースケース定義、想定システムモデルにもとづくリスクアセスメント等を行う。
設計・製造	製品企画フェーズの内容をもとに、製品やクラウドシステムの設計、実装、製造を行う（あるいは外部委託する）。
評価	製品やクラウドシステム提供においてインシデントが発生しないよう、セキュリティ要件に対する適合性の確認や脆弱性診断等を行う。
運用・保守	利用者へのサポート業務やサービス提供における運用・保守、インシデントへの対応等を行う。
廃棄	製品の廃棄における注意点の周知をする。また、製品のサポート期間や関連サービスが終了する場合に、利用者に必要な事項を周知する。

5.2.2 製品ライフサイクルにおけるリスク分析と対策候補の検討

本項では、4.2 節で抽出した守るべき資産に対する製品ライフサイクル上のリスクを分析する。表 5-13 において、NIST SP 800-30 [32]Appendix.E「脅威事象（Threat Events）」を参考に、製品ライフサイクルの各フェーズにおけるリスクを抽出した例を示す。またリスクに対応するセキュリティ対策候補を、表 5-12 に示す文献を参考に導出し、あわせて表 5-13 に示す。

表 5-12 対策候補の検討おける参考文献

文書名	発行機関	発行月
ISO/IEC 27001:2013	ISO/IEC[33]	2013 年 8 月
ISO/IEC 27017:2015	ISO/IEC	2015 年 12 月
NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers	NIST[34]	2020 年 5 月
” Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”	NIST	2022 年 2 月
政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）	NISC[35]	2018 年 7 月
外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書	NISC	2016 年 10 月

[32] NIST SP 800-30 Guide for Conducting Risk Assessments

[33] International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

[34] National Institute of Standards and Technology

[35] 内閣サイバーセキュリティセンター

表 5-13 製品ライフサイクルにおけるフェーズごとのリスクとセキュリティ要求事項の分析結果

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
製品企画	ドローン本体	・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	情報セキュリティの管理方針や管理体制構築の不備により、製品やクラウドシステムに関する機密情報が漏えいする。 ※漏えいにより経済的損失につながる恐れがある	ORG-PR01	情報セキュリティの管理方針の策定
					ORG-PR02	情報セキュリティの管理体制の構築
					ORG-PR03	製品やサービスのシステムモデル、ユースケースの定義
					ORG-PR04	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。
					ORG-PR05	情報セキュリティや関連法令に関する教育および訓練
	地上制御局	・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	情報セキュリティの管理方針や管理体制構築の不備により、製品やクラウドシステムに関する機密情報が漏えいする。 ※漏えいにより経済的損失につながる恐れがある	ORG-PR01	情報セキュリティの管理方針の策定
					ORG-PR02	情報セキュリティの管理体制の構築
					ORG-PR03	製品やサービスのシステムモデル、ユースケースの定義
					ORG-PR04	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。
					ORG-PR05	情報セキュリティや関連法令に関する教育および訓練
	ドローン運用クラウド	・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	情報セキュリティの管理方針や管理体制構築の不備により、製品やクラウドシステムに関する機密情報が漏えいする。 ※漏えいにより経済的損失につながる恐れがある	ORG-PR01	情報セキュリティの管理方針の策定
					ORG-PR02	情報セキュリティの管理体制の構築
					ORG-PR03	製品やサービスのシステムモデル、ユースケースの定義
					ORG-PR04	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。
					ORG-PR05	情報セキュリティや関連法令に関する教育および訓練
	サービス運用クラウド	・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	情報セキュリティの管理方針や管理体制構築の不備により、製品やクラウドシステムに関する機密情報が漏えいする。 ※漏えいにより経済的損失につながる恐れがある	ORG-PR01	情報セキュリティの管理方針の策定
					ORG-PR02	情報セキュリティの管理体制の構築
					ORG-PR03	製品やサービスのシステムモデル、ユースケースの定義
					ORG-PR04	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。
					ORG-PR05	情報セキュリティや関連法令に関する教育および訓練
設計・製造	ドローン本体	・プログラムコード ・認証情報	情報の暴露		ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		開発者、製造者への標的型攻撃や内部犯行等によって、リモート ID 情報やプログラムコードが漏えいする。	ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
		・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	開発者、製造者、サプライヤへの標的型攻撃や内部犯行等によって、不正な情報を追加されたり、守るべき資産を改ざんされる。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
		・機能・サービス	サービス不能	開発者、製造者への標的型攻撃や過失によって、必要なセキュリティ対策機能を停止される。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
	地上制御局	・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	開発者、製造者への標的型攻撃や内部犯行等が原因となり、守るべき資産が漏えいする。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
		・プログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	開発者、製造者、サプライヤへの標的型攻撃や内部犯行等によって、不正な情報を追加されたり、守るべき資産を改ざんされる。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
		・機能・サービス	サービス不能	開発者、製造者への標的型攻撃や過失によって、必要なセキュリティ対策機能を停止される。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
					ORG-MR05	デザインレビューやコードレビュー
	ドローン運用クラウド	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	開発者への標的型攻撃や内部犯行等によって、アップデート用プログラムコードや設定情報が漏えいする。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
		・アップデート用プログラムコード ・セキュリティ上の設定情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	開発者への標的型攻撃や内部犯行等によって、不正な情報を追加されたり、守るべき資産を改ざんされる。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
		・機能・サービス	サービス不能	開発者への標的型攻撃や内部犯行等によって、必要なセキュリティ対策機能を停止される。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
	サービス運用クラウド	・セキュリティ上の設定情報 ・認証情報（デジタル証明書） ・暗号鍵	情報の暴露	開発者への標的型攻撃や内部犯行等によって、設定情報が漏えいする。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
		・セキュリティ上の設定情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	開発者への標的型攻撃や内部犯行等によって、不正な設定情報を追加・改ざんされる。	ORG-MR01	開発・製造環境のセキュリティ対策
					ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
		・機能・サービス	サービス不能		ORG-MR01	開発・製造環境のセキュリティ対策

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
				開発者への標的型攻撃や内部犯行等によって、必要なセキュリティ対策機能を停止される。	ORG-MR02	サプライチェーンリスクの管理
					ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求
					ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理
					ORG-MR05	デザインレビューやコードレビュー
評価	ドローン本体	・プログラムコード ・セキュリティ上の設定値 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サプライチェーンを含む情報セキュリティ管理が適切に行われない結果、製品やクラウドシステムに関する機密情報が漏えいする。	ORG-ER01	情報セキュリティ管理方針や体制のレビュー
					ORG-ER02	製品に対する品質保証体制の確立と実行
	地上制御局	・プログラムコード ・セキュリティ上の設定値 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サプライチェーンを含む情報セキュリティ管理が適切に行われない結果、製品やクラウドシステムに関する機密情報が漏えいする。	ORG-ER01	情報セキュリティ管理方針や体制のレビュー
					ORG-ER02	製品に対する品質保証体制の確立と実行
	ドローン運用クラウド	・プログラムコード ・セキュリティ上の設定値 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サプライチェーンを含む情報セキュリティ管理が適切に行われない結果、製品やクラウドシステムに関する機密情報が漏えいする。	ORG-ER01	情報セキュリティ管理方針や体制のレビュー
					ORG-ER02	製品に対する品質保証体制の確立と実行
	サービス運用クラウド	・プログラムコード ・セキュリティ上の設定値 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サプライチェーンを含む情報セキュリティ管理が適切に行われない結果、製品やクラウドシステムに関する機密情報が漏えいする。	ORG-ER01	情報セキュリティ管理方針や体制のレビュー
					ORG-ER02	製品に対する品質保証体制の確立と実行
運用	ドローン本体	・フライトログ	情報の暴露		ORG-OR01	個人情報やテレメトリデータの収集に関するポリシーの公開

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		ドローン本体のソフトウェアの脆弱性が悪用され、フライトログや記録映像等が漏えいする。	ORG-OR02	製品のセキュリティサポートに関する利用者への周知
					ORG-OR03	脆弱性やセキュリティに関する連絡窓口の設置
					ORG-OR04	更新ソフトウェアの提供
		・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	ドローン本体のソフトウェアに脆弱性が悪用され、フライトログや記録映像等が改ざんされる。	ORG-OR01	個人情報やテレメトリデータの収集に関するポリシーの公開
					ORG-OR02	製品のセキュリティサポートに関する利用者への周知
					ORG-OR03	脆弱性やセキュリティに関する連絡窓口の設置
					ORG-OR04	更新ソフトウェアの提供
	地上制御局	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	地上制御局のソフトウェアの脆弱性が悪用され、フライトログや記録映像等が漏えいする。	ORG-OR01	個人情報やテレメトリデータの収集に関するポリシーの公開
					ORG-OR02	製品のセキュリティサポートに関する利用者への周知
					ORG-OR03	脆弱性やセキュリティに関する連絡窓口の設置
					ORG-OR04	更新ソフトウェアの提供
		・フライトログ ・記録映像	データ改ざん		ORG-OR01	個人情報やテレメトリデータの収集に関するポリシーの公開
					ORG-OR02	製品のセキュリティサポートに関する利用者への周知

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		地上制御局のソフトウェアの脆弱性が悪用され、フライトログや記録映像等が改ざんされる。	ORG-OR03	脆弱性やセキュリティに関する連絡窓口の設置
					ORG-OR04	更新ソフトウェアの提供
	ドローン運用クラウド	・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	ドローン運用クラウドのソフトウェアの脆弱性が悪用され、テレメトリデータやプログラムコード等が漏えいする。	ORG-OR05	運用上のオペレーション手順や管理手順の明確化、遵守
					ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	オペレータへの標的型攻撃や内部犯行等によって、テレメトリデータやプログラムコード等が漏えいする。	ORG-OR05	運用上のオペレーション手順や管理手順の明確化、遵守
					ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報	データ改ざん	ドローン運用クラウドのソフトウェアの脆弱性が悪用され、テレメトリデータやプログラムコード等が改ざんされる。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	オペレータへの標的型攻撃や内部犯行等によって、テレメトリデータやプログラムコード等が改ざんされる。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・機能・サービス	サービス不能	ドローン運用クラウドのソフトウェアの脆弱性が悪用され、機能・サービスが停止する。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・機能・サービス	サービス不能	オペレータへの標的型攻撃や過失等によって、機能・サービスが停止する。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
	サービス運用クラウド	・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果	情報の暴露	サービス運用クラウドのソフトウェアの脆弱性が悪用され、記録映像やテレメトリデータ等が漏えいする。	ORG-OR05	運用上のオペレーション手順や管理手順の明確化、遵守
					ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書				
		・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	オペレータへの標的型攻撃や内部犯行等によって、記録映像やテレメトリデータ等が漏えいする。	ORG-OR05	運用上のオペレーション手順や管理手順の明確化、遵守
					ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	データ改ざん	サービス運用クラウドのソフトウェアの脆弱性が悪用され、記録映像やテレメトリデータ等が改ざんされる。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
		・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書				
		・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	データ改ざん	オペレータへの標的型攻撃や内部犯行等によって、記録映像やテレメトリデータ等が改ざんされる。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR07	守るべき資産のバックアップ
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・機能・サービス	サービス不能	ドローン運用クラウドのソフトウェアの脆弱性が悪用され、機能・サービスが停止する。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
		・機能・サービス	サービス不能	オペレータへの標的型攻撃や内部犯行等によって、機能・サービスが停止する。	ORG-OR06	運用環境のセキュリティ対策
					ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理
					ORG-OR09	ログの取得、監視、分析
					ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応
廃棄	ドローン本体	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	ユーザが廃棄したドローン本体を回収、解析され、保存されたフライトログや記録映像等が漏えいする。	ORG-DR01	個人情報や収集データの消去方法の利用者への周知
	地上制御局	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	ユーザが廃棄した地上制御局を回収、解析され、保存されたフライトログや記録映像等が漏えいする。	ORG-DR01	個人情報や収集データの消去方法の利用者への周知

フェーズ	構成要素	守るべき資産	脅威分類	想定されるリスク	対策候補 ID	対策候補
	ドローン運用クラウド	・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サービス終了したドローン運用クラウドにテレメトリデータやプログラムコード等が適切に消去されず、漏えいする。	ORG-DR02	収集した個人情報やテレメトリデータの消去
	サービス運用クラウド	・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	情報の暴露	サービス終了したドローン運用クラウドにテレメトリデータやプログラムコード等が適切に消去されず、漏えいする。	ORG-DR02	収集した個人情報やテレメトリデータの消去

5.2.3 組織としてのセキュリティ要求事項の整理

第 5.2.2 項において導出した製品ライフサイクル対策候補をセキュリティ要求事項として整理し、表 5-14 に示す。なお、フェーズごとのセキュリティ要求事項の ID については、以下のルールで接頭辞を付与している。

- ORG-PR：製品企画フェーズのセキュリティ要求事項
- ORG-MR：設計・製造フェーズのセキュリティ要求事項
- ORG-ER：評価フェーズのセキュリティ要求事項
- ORG-OR：運用フェーズのセキュリティ要求事項
- ORG-DR：廃棄フェーズのセキュリティ要求事項

表 5-14 企業組織や製品ライフサイクルに対するセキュリティ要求事項

ID	セキュリティ要求事項	フェーズ	構成要素	対象	第 3 章の要求事項との対応 (表 3-7)
ORG-PR01	情報セキュリティの管理方針の策定	製品企画	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMFR-02：情報セキュリティプロセスのスコープ AR-09：情報セキュリティ管理プログラムを ISMS27001 と調和させ、プロセス要素の重複を回避する AR-10：無人航空機に関連するビジネスプロセスと、使用されるすべての物理資産および情報資産を特定する
ORG-PR02	情報セキュリティの管理体制の構築	製品企画	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMFR-01：情報セキュリティプロセスの管理

ID	セキュリティ要求事項	フェーズ	構成要素	対象	第 3 章の要求事項との対応 (表 3-7)
ORG-PR03	製品やサービスのシステムモデル、ユースケースの定義	製品企画	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-PR04	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	製品企画	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMR-01：セキュリティスコープの確立 AMR-02：セキュリティアセスメントの実施 AMR-03：セキュリティ有効性の判断基準、要件を導出し、有効性を保証するための活動を検討する。 AMR-04：セキュリティ開発活動の実施
ORG-PR05	情報セキュリティや関連法令に関する教育および訓練	製品企画	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AR-11：オペレータの教育訓練
ORG-MR01	開発・製造環境のセキュリティ対策	設計・製造	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMFR-04：情報セキュリティの特別な機器要件 AR-04：無人航空機システムのソフトウェアの機密性の管理
ORG-MR02	サプライチェーンリスクの管理	設計・製造	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AR-04：無人航空機システムのソフトウェアの機密性の管理

ID	セキュリティ要求事項	フェーズ	構成要素	対象	第 3 章の要求事項との対応 (表 3-7)
ORG-MR03	開発委託先や部材調達先に対するセキュリティ管理の要求	設計・製造	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-MR04	ソフトウェア、ハードウェアコンポーネントの管理	設計・製造	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-MR05	デザインレビューやコードレビュー	設計・製造	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-ER01	情報セキュリティ管理方針や体制のレビュー	評価	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMFR-07：セキュリティイベントに対するオペレータの対応
ORG-ER02	製品に対する品質保証体制の確立と実行	評価	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-OR01	個人情報やテレメトリデータの収集に関するポリシーの公開	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サービス事業者	

ID	セキュリティ要求事項	フェーズ	構成要素	対象	第 3 章の要求事項との対応 (表 3-7)
ORG-OR02	製品のセキュリティサポートに関する利用者への周知	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-OR03	脆弱性やセキュリティに関する連絡窓口の設置	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	
ORG-OR04	更新ソフトウェアの提供	運用	・ドローン本体 ・地上制御局	・メーカ ・サプライヤ ・サービス事業者	AMFR-05：メンテナンスプログラムへの影響
ORG-OR05	運用上のオペレーション手順や管理手順の明確化、遵守	運用	・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	AMFR-03：マニュアル AR-03：無人航空機システムのソフトウェアを配布、転送する際は、ソフトウェアへのアクセス、管理、および保存をオペレータから許可された担当者のみが実施する AR-04：無人航空機システムのソフトウェアの機密性の管理
ORG-OR06	運用環境のセキュリティ対策	運用	・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	AMFR-04：情報セキュリティの特別な機器要件
ORG-OR07	守るべき資産のバックアップ	運用	・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	

ID	セキュリティ要求事項	フェーズ	構成要素	対象	第 3 章の要求事項との対応 (表 3-7)
ORG-OR08	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	AMFR-02：情報セキュリティプロセスのスコープ AR-08：デジタル証明書の管理を行うための役割、責任、およびプロセスを定義する
ORG-OR09	ログの取得、監視、分析	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	AMFR-06：セキュリティログファイルの処理 AR-12：情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる（インシデント管理）
ORG-OR10	情報セキュリティのインシデント管理およびインシデントレスポンス対応	運用	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・メーカ ・サプライヤ ・サービス事業者	AMFR-07：セキュリティイベントに対するオペレータの対応 AR-12：情報セキュリティの状況を報告および調査し、安全性への影響を適切に理解し、将来的にセキュリティを向上させる（インシデント管理）
ORG-DR01	個人情報や収集データの消去方法の利用者への周知	廃棄	・ドローン本体 ・地上制御局	・メーカ ・サービス事業者	
ORG-DR02	収集した個人情報やテレメトリデータの消去	廃棄	・ドローン本体 ・地上制御局 ・ドローン運用クラウド ・サービス運用クラウド	・サービス事業者	

5.3 無人航空機分野におけるセキュリティ要件

本節では、これまでに検討したリスク分析結果やセキュリティ要求事項の内容を踏まえて、無人航空機システムのセキュリティ要件を示す。無人航空機分野において、情報セキュリティの観点からセキュリティ要件を定義したガイドラインや標準文書は存在しないため、NIST IR 8259 及び"Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products"、ETSI 303 645 を始めとする国内外の IoT 機器向けのセキュリティガイドラインを参考として導出している。

各セキュリティ要件は、5.1 節および 5.2 節で提示したセキュリティ要求事項を元に構成要素別（ドローン本体や地上制御局、クラウド等の機器別）、ステークホルダー別（メーカ、サプライヤ、サービス事業者）に示している。

各セキュリティ要件は、2.4 節で定義したセキュリティクラスを踏まえ、図 5-3 に示す区分に従い、対応優先度を「Mandatory（必須要件）」と「Optional（より強固なセキュリティ対策を求める場合の追加要件）」に区分している。セキュリティクラス 2 に該当する業種では、セキュリティクラス 2 の Mandatory 要件を満たすことを必須とし、Optional 要件については対象のユースケースに応じて各ステークホルダーで対応可否の検討を行う。セキュリティクラス 3 に該当する業種では、セキュリティクラス 2 の Mandatory＋Optional 要件及びセキュリティクラス 3 の Mandatory 要件を満たすことを必須とし、Optional 要件については対象のユースケースに応じて各ステークホルダーで対応可否の検討を行う。

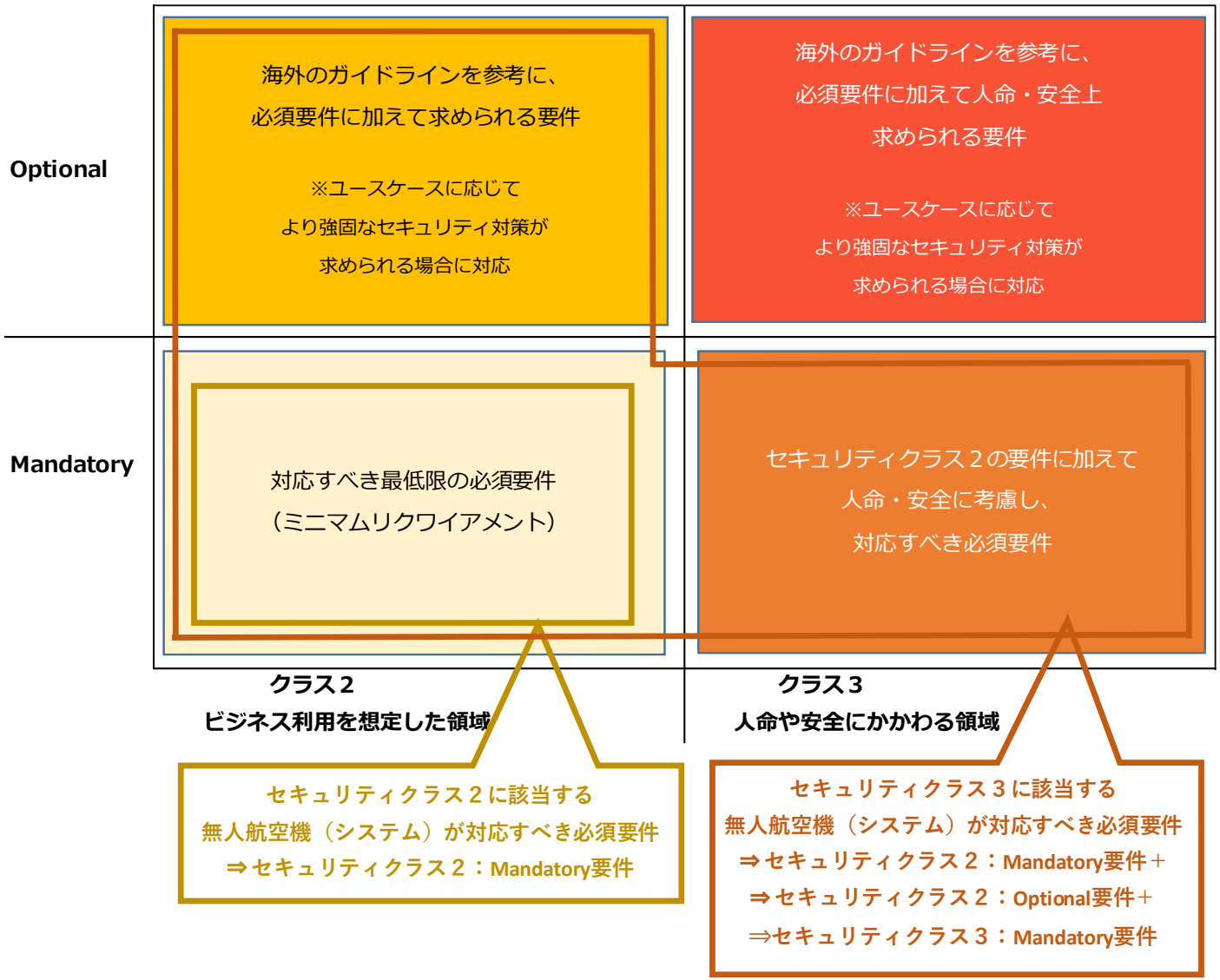


図 5-3 セキュリティ要件に対するクラス区分

5.3.1 ドローン本体におけるセキュリティ要件

ドローン本体におけるセキュリティ要件を表 5-15 に示す。

無線通信用のインターフェイス（データ通信）については、地上制御局と直接無線通信を行う場合と、LTE 等のモバイル通信網を経由して通信を行う場合のどちらも対象とする。

- クラス 2　Mandatory 要件：13 要件
- クラス 2　Optional 要件：10 要件
- クラス 3　Mandatory 要件：5 要件
- クラス 3　Optional 要件：2 要件

表 5-15 ドローン本体におけるセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
UAV-C2M-101	クラス 2	Mandatory	1)機能要件 データの保護	データ消去機能（本体）	①無人航空機本体に蓄積されている、利用者が設定した情報、および機器が利用中に取得した情報の中で、守るべき資産に該当する情報については、容易に消去できる機能を有すること。 ※メーカによるセーフティ上のエラー解析に必要なログ情報については、消去対象から除外とする。	フライトログ ・記録映像 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・基盤・回路上のポート（JTAG、UART など）	[情報漏洩] ・本体ストレージ領域のデータ消去機能がない、もしくは、消去対象に不備があり、機器を廃棄した際に、データが漏えいする。	UAV-R16-B
UAV-C2M-102	クラス 2	Mandatory	1)機能要件 データの保護	データ消去機能（外部ストレージ）	①外部ストレージ（SD カード等）に蓄積されている、利用者が設定した情報、および機器が利用中に取得した情報の中で、守るべき資産に該当する情報については、容易に消去できる機能を有すること。 ※PC 等の外部機器を経由したデータの消去による対応も可能とする。	・フライトログ ・記録映像	・SD/USB インタフェース（記録装置） ・SD/USB インタフェース（カメラ）	[情報漏洩] ・外部ストレージの遺失や盗難、もしくは消去対象に不備があり、データが漏えいする。	UAV-R16-S
UAV-	クラス 2	Mandatory	1)機能要件	リモート ID 発	①リモート ID 信号のメッセージ認証コードを生成する暗号	リモート ID の鍵情報	・無線通信用イン	[情報漏洩]	UAV-R01

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
C2M-103			データの保護	信時の暗号化対応	鍵情報は、暗号化して格納する等、窃取、改ざんその他の第三者による攻撃が容易にできないための対策を講じた上で対象機器に保持すること。		タフェース（リモート ID 通信）	・リモート ID の暗号鍵の漏えい	
UAV-C2M-104	クラス 2	Mandatory	1)機能要件 データの保護	通信経路暗号化	①インターネットで通信を行う区間は、暗号化による保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ※LTE 等を使用し通信を行う場合は、通信キャリア側で適切な暗号化対策が行われているサービスを選定すること。 ②通信経路の暗号化に用いる鍵や証明書の管理を適切に行うこと。（鍵情報は機器ごとに一意の値を使用し、変更可能とすること） ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討 －調査報告書－」	・フライトログ ・記録映像 ・プログラムコード ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[情報漏えい、データの改ざん] ・クラウドシステムや地上制御局との通信におけるデータが傍受、改ざんされる。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	UAV-R21
UAV-C2M-105	クラス 2	Mandatory	1)機能要件 インタフェースへの論理的	アクセス制御	①各ネットワーク・インターフェースへのアクセスを、権限を有するユーザ、または機器のみに論理的に制限できること。 ※本項目と関連項目「UAV-C2M-107 機器認証」につ	・フライトログ ・記録映像 ・プログラムコード	・無線通信用インタフェース（データ通信	[不正アクセス、データ改ざん] 不正アクセスによる不正なコマンド発行や保護すべきデータに	UAV-R11

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
			アクセス		いては、機器の実装や運用を踏まえ、いずれか対応可能な項目を選択するものとする。	・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		対する書き込みが行われる。	
UAV-C2M-106	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	セキュリティ設定の変更及び安全な初期設定への復元機能	①アクセス制御や認証情報の設定値については、利用者あるいはメーカの保守員による設定変更を可能とすること。 ※関連要件 ID：「UAV-C2M-105　アクセス制御」、「UAV-C2M-107　機器認証」 ②工場出荷後の初回起動時には、一意であるパスワードでない場合には強制的にパスワードを変更する機能を実装すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・初期設定時のパスワードが容易に解析可能な値である場合に、値を解析され、不正アクセスや地上制御局のなりすましに利用される。	UAV-R13
UAV-C2M-107	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①対象機器が一意の ID を有すること。 ②接続している機器の的 ID を読み取り可能とすること。また最新の状態に更新可能であること。 ③通信先として正当な地上制御局を識別し、許可された地上制御局あるいはクラウドとのみ接続を行うこと。 TCP/UDP による通信を行う場合には、機器毎にユニークな ID とパスワードによる認証を行うこと。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハ	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・無線通信インタフェースへの論理的アクセスにおいて偽装を識別できず、不正アクセスや地上制御局のなりすましに利用される。 ・総当り攻撃によってアカウント	UAV-R12

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					※上記基準以上の実装を行っている場合にも、要件を満たすものとする ④連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権的ユーザへのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ⑤機器のセキュリティ関連機能を含め、重要な構成変更を行う機能については特権的ユーザを適切に識別、認証し、特権的ユーザ以外による機能の実行を制限すること。	ッシュ） ・デジタル証明書		を乗っ取られ、不正に利用される。	
UAV-C2M-108	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	不要な TCP/UDP ポートの無効化	①システム運用上、利用が必要な TCP/UDP 通信を対象とし、システム運用上、開放が不要な TCP/UDP ポートは停止しておくこと。 ②システム運用上、開放が必要なポートについては、セキュリティ要件「UAV-C3M-201」に従い、脆弱性診断を実施すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス] ・無線通信用インタフェースにおいて、管理されていない不要なサービスポートが動作しており、不正アクセスが行われる。	UAV-R14
UAV-C2M-109	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	USB デバイスのアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。	・記録映像 ・フライトログ ・機能・サービス	・SD/USB インタフェース（記録装置） ・SD/USB インタフェース（カメラ）	不正アクセス、マルウェア感染] ・ドローン本体と地上制御区間のデータ移行に USB 通信を利用している場合、通信デバイスクラス（CDC）等の不	UAV-R18

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
								要な USB デバイスクラスを本体が認識し、不正アクセスにつながる。または USB 経由によるマルウェア感染につながる。	
UAV-C2M-110	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	Bluetooth のアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。 ※Bluetooth SIG 推奨の適切なペアリング方式が装備されていること Bluetooth4.X で定義された Low Energy の通信モードに対応し、LE Secure Connections（Just Works）に基づくペアリング方式を実装	・記録映像 ・フライトログ ・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ※Bluetooth を利用する場合 ・無線通信用インタフェース（リモート ID 通信）	[不正アクセス、マルウェア感染] ・Bluetooth のペアリングにおいて、脆弱な方式を利用している場合、適切な認証が行われず不正アクセスにつながる。また、Blueborne の脆弱性により、対象機器を外部から不正に操作あるいはマルウェアを組み込まれる可能性がある。	UAV-R02
UAV-C2M-111	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	Wi-Fi のアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。 ※Wi-Fi Alliance ®（ワイファイ アライアンス）推奨の適切な認証方式が装備されていること。 認証方式「WPA2（Wi-Fi Protected Access 2）」以上に対応すること。 －「WPA2 Personal」（パーソナルモード/WPA2-PSK）あるいは、「WPA2 Enterprise」（エンタープライズモー	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[不正アクセス、その他の複合的な脅威] ・Wi-Fi を実装している対象機器において、脆弱な認証方式を利用している場合、中間者攻撃による解析により、不正アクセスにつながる。	UAV-R03

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					ド）のいずれかに対応する。 －暗号化プロトコル：CCMP －暗号化アルゴリズム：AES（128 ビット以上） ②SSID は機体ごとにユニークな値であり、パスフレーズは機器ごとにユニークな値、もしくは容易に解析可能な値を使用しないこと。				
UAV-C2M-112	クラス 2	Mandatory	1)機能要件 ソフトウェアの更新	ソフトウェア更新機能	①ローカルまたはネットワーク経由による機器のソフトウェアを更新できること。 ②機器の管理者が更新ファイルのインストール結果の成否やバージョンを確認する手段を有すること。 ※ローカル経由でのソフトウェア更新については、メーカの保守員（あるいは利用者）による手動での対応及び、ネットワークに接続した地上制御局経由の更新による対応のどちらも可能とする。	・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信） ・SD/USB インタフェース（記録装置）	[セキュリティ、可用性への脅威] ・ソフトウェアの脆弱性への対策や機能修正を実施できず、対象機器のセキュリティや可用性を維持できない。 ・ソフトウェア更新によってクリティカルな業務に悪影響が出た場合に復旧できない。	UAV-R04
UAV-C2M-113	クラス 2	Mandatory	1)機能要件 製品のセキュリティ	電源停止や障害発生時の対応	①アクセス制御や認証情報の設定値および、更新されたソフトウェアについては、電源停止後も設定値、ソフトウェアバージョンを維持できること。 ※関連要件 ID：「UAV-C2M-101　アクセス制御」、「UAV-C2M-102　機器認証」、「UAV-C2M-112　ソフトウェア更新機能」 ②ネットワークの停止後、他機器との接続において、アクセス制御や認証のプロセスを経由し、安全な状態での接続を再	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[不正アクセス、その他の複合的な脅威] ・電源停止後に変更された認証上の設定値や更新されたソフトウェアのバージョンが初期化され、セキュリティ機能が動作せず不正アクセス等の要因となる。	UAV-R06

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					確立できること。				
UAV-C2O-101	クラス 2	Optional	1)機能要件 製品の構成	不要な機能の無効化	①ソフトウェアの設定変更において、不要な機能を無効化できること	機能・サービス	・無線通信用インタフェース（データ通信）	[不正アクセス、情報漏洩] ・オープンソースや第三者が開発している OS やソフトウェアを利用している場合に、想定外の機能や通信インタフェースが実装され、予期しない脆弱性の原因となる。	UAV-R15
UAV-C2O-102	クラス 2	Optional	1)機能要件 データの保護	データ保護（本体）	①機器本体のメモリ領域へ保存される守るべき資産を、不正なアクセスや変更から保護することができること。 ※具体的な実装方法については、暗号化による対応、あるいは安全な領域（「TrustZone」やセキュアエレメント等）にデータを格納するなど、運用される業態や状況に応じて選択可能とする。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[情報漏洩、データの改ざん] ・本体メモリ領域への、不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・データ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	UAV-R07-B
UAV-C2O-103	クラス 2	Optional	1)機能要件 データの保護	データ保護（外部ストレージ）	①SD カード等の外部ストレージへ保存される守るべき資産を、不正なアクセスや変更から保護することができること。	・記録映像 ・フライトログ	・SD/USB インタフェース（記録装置）	[情報漏洩、データの改ざん] ・外部ストレージの遺失や盗難、不正アクセスが行われた	UAV-R07-S

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
							・SD/USB インタフェース（カメラ）	場合に、守るべき資産が窃取され、データが漏えいする。 ・外部ストレージのデータ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	
UAV-C2O-104	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	セキュリティ設定の変更及び安全な初期設定への復元機能	①認証情報の設定変更機能は、メーカあるいは特権的ユーザ以外による機能の実行を制限すること。 ※工場出荷後の初回起動時におけるパスワード変更も、同様とする。 ②機器のセキュリティを初期設定において安全な状態とすること。 ③権限を有するユーザや機器が、初期設定へ復元可能な機能を実装すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・初期設定時のパスワードが容易に解析可能な値である場合に、値を解析され、不正アクセスに利用される。	UAV-R13
UAV-C2O-105	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	機器認証	①認証情報は情報の漏えいに配慮し、保護されたオフラインの領域で管理すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス	・無線通信用インタフェース（データ通信）	不正アクセス、その他の複合的な脅威] ・不正アクセスが発生した場合に、窃取された認証情報が攻	UAV-R12

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
						・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		撃に悪用され、対象機器のセキュリティや可用性が阻害される。	
UAV-C2O-106	クラス 2	Optional	1)機能要件 インタフェースへの論理的アクセス	不要な TCP/UDP ポートの無効化	①開放している TCP/UDP ポートを識別可能であり、開放/停止を変更できる機能を実装すること。 ②TCP/UDP ポートの開放/停止を変更する機能については、特権的ユーザ以外による実行を制限すること。 ③インタフェースを通して受け取った入力が、フォーマットとコンテンツの指定された定義に一致するかどうかを検証する機能を有すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス] ・無線通信用インタフェースにおいて、管理されていない不要なサービスポートが動作しており、不正アクセスが行われる。	UAV-R14
UAV-C2O-107	クラス 2	Optional	1)機能要件 インタフェースへの論理的アクセス	USB デバイスの不要機能の無効化	①サービス上、不要な USB 接続端子については、実装を行わないこと。 ②USB 接続端子（ポート）は、運用担当者以外が使用しにくい状態とするよう対策を行うこと。	・記録映像 ・フライトログ ・機能・サービス	・SD/USB インタフェース（記録装置） ・SD/USB インタフェース（カメラ）	[不正アクセス、マルウェア感染] ・通信デバイスクラス（CDC）等の不要な USB デバイスクラスを本体が認識し、不正アクセスにつながる。または USB 経由によるマルウェア感染につながる。	UAV-R18
UAV-	クラス 2	Optional	1)機能要件	ソフトウェア更新	①アップデート用ソフトウェアは、通信経路の暗号化、あるい	機能・サービス	・無線通信用イン	[セキュリティ、可用性への脅	UAV-R04

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
C2O-108			ソフトウェアの更新	機能	は送信時にデータの暗号化を行うこと。 ②ソフトウェア更新機能を無効化する機能を実装する場合は、特権ユーザ以外による実行を制限すること。 ③アップデートに関する通知を有効または、無効に変更することが可能であること。 ④暗号化に使用する鍵や証明書の管理を適切に行うこと。（鍵や証明書は機器ごとに一意の値を使用し、変更可能とすること） ※暗号化による対応は、以下の参考ガイドラインに準拠した実装とすること。 A)暗号化ガイドライン 「電子政府における調達のために参照すべき暗号のリスト」、もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 B）鍵管理に関するガイドライン 「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」		タフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	威] ・不正な更新ファイルをインストールすることにより、対象機器の可用性とセキュリティが損なわれる	
UAV-C2O-109	クラス 2	Optional	1)機能要件 ソフトウェアの更新	ソフトウェアの真正性と完全性の検証	①更新ソフトウェアが改ざんされていないこと、あるいは正規の管理者によってリリースされたソフトウェアであることを保証すること。	・プログラムコード ・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ	[セキュリティ、可用性への脅威] ・不正な更新ファイルをインストールすることにより、対象機器の可用性とセキュリティが損な	UAV-R05

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
							通信）	われる。 ・管理者の意図しないソフトウェア更新が実施され、対象機器の可用性とセキュリティが損なわれる。	
UAV-C2O-301	クラス 2	Optional	3)監査要件サイバーセキュリティの状態認識	ログの記録	①サイバーセキュリティ関連の状態情報（ソフトウェアアップデートのインストール、ログイン試行の失敗、設定変更など）を監査証跡としてログに記録できること。 ※監査証跡の蓄積機能は、機器またはサーバ側のいずれかが有するものとする。 ②特権的ユーザによる監査証跡（ログ）の読み出しを可能とすること。 ③監査証跡の保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行うこと。 ※監査証跡（ログ）を保存する期間については、対象製品やサービスごとに必要な期間を検討し、定義するものとする。	・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・インシデント分析に必要なログ情報の不足によってインシデントへの対応の遅れや、再発防止策の検討が困難となる。	UAV-R09
UAV-C3M-101	クラス 3	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①クラウドシステム、地上制御局との相互認証を行う仕組みを有すること。 ②相互認証に必要な情報の管理（相互認証に必要な情報が漏えいしないような仕組み）を実装すること。 ※暗号化による相互情報の管理を行う場合は、以下の参考ガイドラインに準拠した実装とすること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報	・無線通信用インタフェース（データ通信）	不正アクセス、なりすまし] ・無線通信インタフェースへのアクセス時に適切な認証が行われず、不正アクセスや地上制御局のなりすましに不正操作が行われる。	UAV-R12

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討 －調査報告書－」	・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			
UAV-C3M-102	クラス 3	Mandatory	1)機能要件 ソフトウェアの更新	ソフトウェア更新機能	①使用している OS、boot プログラム、アプリケーションに脆弱性が報告された場合には、テストを実施した上で、速やかに更新用ソフトウェアの提供を行うこと。	機能・サービス	・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・ソフトウェアの脆弱性への対策や機能修正を実施できず、対象機器のセキュリティや可用性を維持できない。	UAV-R04
UAV-C3M-201	クラス 3	Mandatory	2)運用要件 脆弱性の診断	脆弱性診断	①機器が外部からの脆弱性スキャンに対応できる能力を有すること。 ②製品の開発完了時、および、更新ソフトウェアの提供前に、脆弱性スキャンツールによる TCP/UDP サービスポートをネットワークスキャンし、脆弱性の有無をチェックすること。 ※Bluetooth については、Blueborne の脆弱性についても診断及び対策を行うこと。 ③製品の開発完了時、および、更新ソフトウェアの提供前に、実装しているプラットフォームに影響を与える既知のマルウェアの有無を検査すること。 ④脆弱性やマルウェアが検出された場合には、問題の影響度、重要度を踏まえ、セキュリティ対策の必要可否を検討の上、対応すること。	・フライトログ ・記録映像 ・プログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[情報漏洩、データの改ざん、その他複合的な脅威] ・ソフトウェアに潜在する既知の脆弱性を利用し、機器内のデータの窃取や改ざん、あるいは可用性がそこなわれる。	UAV-R10

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					⑤バッファオーバーフローに類する問題が検出された場合には、実装しているプラットフォームに応じたバッファオーバーフロー対策（攻撃に対する手がかりの最小化等）を行うこと。 ⑥製品販売後に問題が確認された場合には、「ORG-C2M-M04」で定義する脆弱性情報の開示ポリシーに応じた対応を行うこと。 ※上記①は、機器自体に脆弱性検知の仕組みの実装を求めるものではない。				
UAV-C3O-101	クラス 3	Optional	1)機能要件 製品のセキュリティ	DoS 対策	①可用性に配慮し、冗長性を持たせた設計とすること。 例）対象機器のリソースに過剰な負荷を掛けたり、脆弱性を突くことによる(D)DoS 攻撃を想定し、負荷試験の実施及び一定レベルの負荷に耐える設計とすること。	機能・サービス ※対象機器の可用性	・無線通信用インタフェース（リモート ID 通信） ・無線通信用インタフェース（データ通信）	[サービス不能] ・無線通信用インタフェースに DoS 攻撃された結果、本体の機能やサービスが停止し、必要なデータにアクセスできなくなる。	UAV-R08
UAV-C3O-102	クラス 3	Optional	1)機能要件 製品のセキュリティ	セキュアブート	①対象機器起動時の安全性を確保するため、セキュアブートを有すること。	プログラムコード	・無線通信用インタフェース（データ通信）	[改ざん、マルウェア感染] ブートローダや OS などが外部の攻撃者やマルウェアによって不正に改ざん、偽装されることで、対象機器のセキュリティや可用性が損なわれる。	UAV-R17
UAV-C3O-103	クラス 3	Optional	1)機能要件 製品のセキュリティ	ハードウェアハッキング対策	①対象機器の信頼性を保証するための RoT（Root of Trust）を有すること。 ②ハードウェアのデバッグインタフェースを無効化すること。	・プログラムコード ・機器本体（ハードウェア）	・基板・回路上のポート（JTAG、UART など）	[情報漏洩、その他の複合的な脅威] ・本体からソフトウェアを抽出さ	UAV-R19

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
						・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		れ、ハードコートされたパスワードや脆弱性等の解析により、攻撃に利用される。	
UAV-C3O-104	クラス 3	Optional	1)機能要件製品のセキュリティ	リバースエンジニアリング対策	①対象機器の不正な複製デバイスの作成を防止するため、リバースエンジニアリング対策を行うこと。 ※リバースエンジニアリング対策の例 ・プログラムデータの難読化、動的ライブラリの暗号化 ・セキュア OS の利用による、アクセス制御や特権の最小化 ・コードは、サービス/デバイスが動作するために必要な機能に最小化 ・ハッシュツリーによる、保存・処理・転送されるデータの検証（改ざん防止）…など	・プログラムコード	・基板・回路上のポート（JTAG、UART など）	[なりすまし、情報漏洩] ・不正に作成された複製デバイスにより、企業のブランドや信用力の低下につながる可能性がある。	UAV-R20

5.3.2 地上制御局におけるセキュリティ要件

地上制御局におけるセキュリティ要件を表 5-16 に示す。

無線通信用のインターフェイス（データ通信）については、ドローン本体と直接無線通信を行う場合と、LTE 等のモバイル通信網を経由して通信を行う場合のどちらも対象とする。

- クラス 2　Mandatory 要件：13 要件
- クラス 2　Optional 要件：11 要件
- クラス 3　Mandatory 要件：5 要件
- クラス 3　Optional 要件：2 要件

表 5-16 地上制御局におけるセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
GCS-C2M-101	クラス 2	Mandatory	1)機能要件 データの保護	データ消去機能（本体）	①地上制御局本体に蓄積されている、利用者が設定した情報、および機器が利用中に取得した情報の中で、守るべき資産に該当する情報については、容易に消去できる機能を有すること。 ※メーカによるセーフティ上のエラー解析に必要なログ情報については、消去対象から除外とする。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）	・基盤・回路上のポート（JTAG、UART など）	[情報漏洩] ・本体ストレージ領域のデータ消去機能がない、もしくは、消去対象に不備があり、機器を廃棄した際に、データが漏えいする。	GCS-R13-B

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
						・デジタル証明書			
GCS-C2M-102	クラス 2	Mandatory	1)機能要件 データの保護	データ消去機能（外部ストレージ）	①外部ストレージ（SD カード等）に蓄積されている、利用者が設定した情報、および機器が利用中に取得した情報の中で、守るべき資産に該当する情報については、容易に消去できる機能を有すること。 ※PC 等の外部機器を経由したデータの消去による対応も可能とする。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	・SD/USB インタフェース（記録装置）	[情報漏洩] ・外部ストレージの遺失や盗難、もしくは消去対象に不備があり、データが漏えいする。	GCS-R13-S
GCS-C2M-103	クラス 2	Mandatory	1)機能要件 データの保護	通信経路暗号化	①インターネットで通信を行う区間は、暗号化による保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ※LTE 等を使用し通信を行う場合は、通信キャリア側で適切な暗号化対策が行われているサービスを選定すること。 ②通信経路の暗号化に用いる鍵や証明書の管理を適切に行うこと。（鍵情報は機器ごとに一意の値を使用し、変更可能とすること） ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイド	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）	・無線通信用インタフェース（データ通信）	[情報漏えい、データの改ざん] ・クラウドシステムやドローン本体との通信におけるデータが傍受、改ざんされる。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	GCS-R21

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					ライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・デジタル証明書			
GCS-C2M-104	クラス 2	Mandatory	1)機能要件 インタフェースへの論理的アクセス	アクセス制御	①各ネットワーク・インターフェースへのアクセスを、権限を有するユーザ、または機器のみに論理的に制限できること。 ※本項目と関連項目「GCS-C2M-106　機器認証」については、機器の実装や運用を踏まえ、いずれか対応可能な項目を選択するものとする。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信	[不正アクセス、データ改ざん] 不正アクセスによる不正なコマンド発行や保護すべきデータに対する書き込みが行われる。	GCS-R01
GCS-C2M-105	クラス 2	Mandatory	1)機能要件 製品の構成	セキュリティ設定の変更及び安全な初期設定への復元機能	①アクセス制御や認証情報の設定値については、利用者あるいはメーカの保守員による設定変更を可能とすること。 ※関連要件 ID：「GCS-C2M-104　アクセス制御」、「GCS-C2M-106　機器認証」 ②工場出荷後の初回起動時には、一意であるパスワードでない場合には強制的にパスワードを変更する機能を実装す	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・初期設定時のパスワードが容易に解析可能な値である場合に、値を解析され、不正アクセスや地上	GCS-R04

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					ること。	・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		制御局のなりすましに利用される。	
GCS-C2M-106	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①対象機器が一意の ID を有すること。 ②接続している機器の的 ID を読み取り可能とすること。また最新の状態に更新可能であること。 ③通信先として正当なドローン本体を識別し、許可されたドローン本体あるいはクラウドとのみ接続を行うこと TCP/UDP による通信を行う場合には、機器毎にユニークな ID とパスワードによる認証を行うこと。 ※上記基準以上の実装を行っている場合にも、要件を満たすものとする。 ④連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権的ユーザへのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ⑤機器のセキュリティ関連機能を含め、重要な構成変更を	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・無線通信インタフェースへの論理的アクセスにおいて偽装を識別できず、不正アクセスやドローン本体のなりすましに利用される。 ・総当り攻撃によってアカウントを乗っ取られ、不正に利用される。	GCS-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					行う機能については特権的ユーザを適切に識別、認証し、特権的ユーザ以外による機能の実行を制限すること。	・デジタル証明書			
GCS-C2M-107	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	ユーザ認証	①TCP/IP を対象とし、利用ユーザごとにユニークな ID とパスワードによる認証を行うこと。 ②システム運用上、開放が必要なポートについては、セキュリティ要件「GCS-C3M-201」に従い、脆弱性診断を実施すること。 ③連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権的ユーザへのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ④機器のセキュリティ関連機能を含め、重要な構成変更を行う機能については特権的ユーザを適切に識別、認証し、特権的ユーザ以外による機能の実行を制限すること。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信	[不正アクセス、なりすまし] ・無線通信インタフェースへの論理的アクセスにおいて偽装を識別できず、不正アクセスやユーザのなりすましに利用される。 ・総当り攻撃によってアカウントを乗っ取られ、不正に利用される	GCS-R03
GCS-C2M-108	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	不要な TCP/UDP ポートの無効化	①システム運用上、利用が必要な TCP/UDP 通信を対象とし、システム運用上、開放が不要な TCP/UDP ポートは停止しておくこと。 ②システム運用上、開放が必要なポートについては、セキュリティ要件「UAV-C3M-201」に従い、脆弱性診断を実施すること。 ※地上制御局として、利用者の PC にソフトウェアをインスト	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	・無線通信用インタフェース（データ通信）	[不正アクセス] ・無線通信用インタフェースにおいて、管理されていない不要なサービスポートが動作しており、不正アクセスが行われる。	GCS-R05

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					ールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場合のセキュリティリスクについては、提供事業者側で対応を行うこと。 例）セキュリティ設定の変更の抑止や利用者への注意喚起など。	・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			
UAV-C2M-109	クラス 2	Mandatory	1)機能要件 インタフェースへの論理的アクセス	USB デバイスのアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。 ※地上制御局として、利用者の PC にソフトウェアをインストールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場合のセキュリティリスクについては、提供事業者側で対応を行うこと。	・記録映像 ・フライトログ ・機能・サービス	・SD/USB インタフェース（記録装置）	不正アクセス、マルウェア感染] ・ドローン本体と地上制御区間のデータ移行に USB 通信を利用している場合、通信デバイスクラス（CDC）等の不要な USB デバイスクラスを本体が認識し、不正アクセスにつながる。または USB 経由によるマルウェア感染につながる。	GCS-R06

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					例）セキュリティ設定の変更の抑止や利用者への注意喚起など。				
GCS-C2M-110	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	Bluetooth のアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。 ※Bluetooth SIG 推奨の適切なペアリング方式が装備されていること ※地上制御局として、利用者の PC にソフトウェアをインストールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場合のセキュリティリスクについては、提供事業者側で対応を行うこと。 例）セキュリティ設定の変更の抑止や利用者への注意喚起など。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス	・無線通信用インタフェース（リモート ID 通信） ※Bluetooth を利用する場合	[不正アクセス、マルウェア感染] ・Bluetooth のペアリングにおいて、脆弱な方式を利用している場合、適切な認証が行われず不正アクセスにつながる。また、Blueborne の脆弱性により、対象機器を外部から不正に操作あるいはマルウェアを組み込まれる可能性がある。	GCS-R08
GCS-C2M-111	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	Wi-Fi のアクセス制御	①適切なアクセス制御及び、アクセス権限の制限を行うこと。 ※Wi-Fi Alliance ®（ワイファイ アライアンス）推奨の適切な認証方式が装備されていること。 認証方式「WPA2（Wi-Fi Protected Access 2）」以	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等）	・・無線通信用インタフェース（リモート ID 通信）	[不正アクセス、その他の複合的な脅威] ・Wi-Fi を実装している対象機器において、脆弱な な認証方式を利用してい	GCS-R07

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					上に対応すること。 －「WPA2 Personal」（パーソナルモード/WPA2-PSK）あるいは、「WPA2 Enterprise」（エンタープライズモード）のいずれかに対応する。 －暗号化プロトコル：CCMP －暗号化アルゴリズム：AES（128 ビット以上） ②SSID は機体ごとにユニークな値であり、パスフレーズは機器ごとにユニークな値、もしくは容易に解析可能な値を使用しないこと。②SSID は機体ごとにユニークな値であり、パスフレーズは機器ごとにユニークな値、もしくは容易に解析可能な値を使用しないこと。 ※地上制御局として、利用者の PC にソフトウェアをインストールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場合のセキュリティリスクについては、提供事業者側で対応を行うこと。 例）セキュリティ設定の変更の抑止や利用者への注意喚起など。	・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス	・無線通信用インタフェース（データ通信）	る場合、中間者攻撃による解析により、不正アクセスにつながる。	

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
UAV-C2M-112	クラス 2	Mandatory	1)機能要件 ソフトウェアの更新	ソフトウェア更新機能	①ローカルまたはネットワーク経由による機器のソフトウェアを更新できること。 ②機器の管理者が更新ファイルのインストール結果の成否やバージョンを確認する手段を有すること。 ※ローカル経由でのソフトウェア更新については、メーカの保守員（あるいは利用者）による手動での対応及び、ネットワークに接続した地上制御局経由の更新による対応のどちらも可能とする	・機能・サービス	・無線通信用インタフェース（データ通信） ・SD/USB インタフェース（記録装置）	[セキュリティ、可用性への脅威] ・ソフトウェアの脆弱性への対策や機能修正を実施できず、対象機器のセキュリティや可用性を維持できない。 ・ソフトウェア更新によってクリティカルな業務に悪影響が出た場合に復旧できない。	GCS-R09
GCS-C2M-113	クラス 2	Mandatory	1)機能要件 製品のセキュリティ	電源停止や障害発生時の対応	①アクセス制御や認証情報の設定値および、更新されたソフトウェアについては、電源停止後も設定値、ソフトウェアバージョンを維持できること。 ※関連要件 ID：「UAV-C2M-101　アクセス制御」、「UAV-C2M-102　機器認証」、「UAV-C2M-112　ソフトウェア更新機能」 ②ネットワークの停止後、他機器との接続において、アクセス制御や認証のプロセスを経由し、安全な状態での接続を再確立できること。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス	・無線通信用インタフェース（データ通信）	[不正アクセス、その他の複合的な脅威] ・電源停止後に変更された認証上の設定値や更新されたソフトウェアのバージョンが初期化され、セキュリティ機能が動作せず不正アクセス等の要因となる。	GCS-R11
GCS-C2O-101	クラス 2	Optional	1)機能要件 製品の構成	不要な機能の無効化	①ソフトウェアの設定変更において、不要な機能を無効化できること	機能・サービス	・無線通信用インタフェース（デ	[不正アクセス、情報漏洩]	GCS-R06

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
							ータ通信）	・オープンソースや第三者が開発している OS やソフトウェアを利用している場合に、想定外の機能や通信インタフェースが実装され、予期しない脆弱性の原因となる。	
GCS-C2O-102	クラス 2	Optional	1)機能要件 データの保護	データ保護（本体）	①機器本体のメモリ領域へ保存される守るべき資産を、不正なアクセスや変更から保護することができること。 ※具体的な実装方法については、暗号化による対応、あるいは安全な領域（「TrustZone」やセキュアエレメント等）にデータを格納するなど、運用される業態や状況に応じて選択可能とする。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[情報漏洩、データの改ざん] ・地上制御局のメモリ領域への不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・データ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	GCS-R12-B

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
GCS-C2O-103	クラス 2	Optional	1)機能要件 データの保護	データ保護（外部ストレージ）	①SD カード等の外部ストレージへ保存される守るべき資産を、不正なアクセスや変更から保護することができること。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・機能・サービス	・SD/USB インタフェース（記録装置）	[情報漏洩、データの改ざん] ・外部ストレージの遺失や盗難、不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・外部ストレージのデータ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	GCS-R12-S
GCS-C2O-104	クラス 2	Optional	1)機能要件 インタフェースへの論理的アクセス	セキュリティ設定の変更及び安全な初期設定への復元機能	①認証情報の設定変更機能は、メーカあるいは特権的ユーザ以外による機能の実行を制限すること。 ※工場出荷後の初回起動時におけるパスワード変更も、同様とする。 ②機器のセキュリティを初期設定において安全な状態とすること。 ③権限を有するユーザや機器が、初期設定へ復元可能な	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・初期設定時のパスワードが容易に解析可能な値である場合に、値を解析され、不正アクセスに利用される。	GCS-R04

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					機能を実装すること。	・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			
GCS-C2O-105	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	機器認証	①認証情報は情報の漏えいに配慮し、保護されたオフラインの領域で管理すること。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス、その他の複合的な脅威] ・不正アクセスが発生した場合に、窃取された認証情報が攻撃に悪用され、対象機器のセキュリティや可用性が阻害される。	GCS-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
GCS-C2O-106	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	ユーザ認証	①二段階認証、多要素認証等を使用した高度な認証方式を実装していること。 ①認証情報は情報の漏えいに配慮し、保護されたオフラインの領域で管理すること。	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・無線通信用インタフェース（データ通信）	[不正アクセス、なりすまし] ・無線通信インタフェースへの論理的アクセスにおいて偽装を識別できず、不正アクセスやユーザのなりすましに利用される。 ・総当り攻撃によってアカウントを乗っ取られ、不正に利用される	GCS-R03
GCS-C2O-107	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	不要な TCP/UDP ポートの無効化	①開放している TCP/UDP ポートを識別可能であり、開放/停止を変更できる機能を実装すること。 ②TCP/UDP ポートの開放/停止を変更する機能については、特権的ユーザ以外による実行を制限すること。 ③インタフェースを通して受け取った入力が、フォーマットとコンテンツの指定された定義に一致するかどうかを検証する機能を有すること。 ※地上制御局として、利用者の PC にソフトウェアをインスト	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御	・無線通信用インタフェース（データ通信）	[不正アクセス] ・無線通信用インタフェースにおいて、管理されていない不要なサービスポートが動作しており、不正アクセスが行われる。	GCS-R05

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					ールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場合のセキュリティリスクについては、提供事業者側で対応を行うこと。 例）セキュリティ設定の変更の抑止や利用者への注意喚起など。	局) ・機能・サービス			
GCS-C2O-108	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	USB デバイスの不要機能の無効化	①サービス上、不要な USB 接続端子については、実装を行わないこと。 ②USB 接続端子（ポート）は、運用担当者以外が使用しにくい状態とするよう対策を行うこと。 ※地上制御局として、利用者の PC にソフトウェアをインストールしたものを利用する場合には、本項目の対応は利用者側の設定に依存する。この場合、本項目は対象外とするが、使用する PC のセキュリティ対策については、利用者側へ注意喚起を行うこと。 ※市販の PC にソフトウェアをインストールし、製品として提供する場合には、本項目の対応が必要となる。この場合、本項目に関連するセキュリティ設定をユーザ側で変更する場	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス	・SD/USB インタフェース（記録装置）	[不正アクセス、マルウェア感染] ・通信デバイスクラス（CDC）等の不要な USB デバイスクラスを本体が認識し、不正アクセスにつながる。または USB 経由によるマルウェア感染につながる。	GCS-R18

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					合のセキュリティリスクについては、提供事業者側で対応を行うこと。 例）セキュリティ設定の変更の抑止や利用者への注意喚起など。				
GCS-C2O-109	クラス 2	Optional	1)機能要件 ソフトウェアの更新	ソフトウェア更新機能	①アップデート用ソフトウェアは、通信経路の暗号化、あるいは送信時にデータの暗号化を行うこと。 ②ソフトウェア更新機能を無効化する機能を実装する場合は、特権ユーザ以外による実行を制限すること。 ③アップデートに関する通知を有効または、無効に変更することが可能であること。 ④暗号化に使用する鍵や証明書の管理を適切に行うこと。 （鍵や証明書は機器ごとに一意の値を使用し、変更可能とすること） ※暗号化による対応は、以下の参考ガイドラインに準拠した実装とすること。 A)暗号化ガイドライン 「電子政府における調達のために参照すべき暗号のリスト」、もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 B）鍵管理に関するガイドライン 「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	機能・サービス	・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・不正な更新ファイルをインストールすることにより、対象機器の可用性とセキュリティが損なわれる	GCS-R09

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
GCS-C2O-110	クラス 2	Optional	1)機能要件 ソフトウェアの更新	ソフトウェアの真正性と完全性の検証	①更新ソフトウェアが改ざんされていないこと、あるいは正規の管理者によってリリースされたソフトウェアであることを保証すること。	・プログラムコード ・機能・サービス	・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・不正な更新ファイルをインストールすることにより、対象機器の可用性とセキュリティが損なわれる。 ・管理者の意図しないソフトウェア更新が実施され、対象機器の可用性とセキュリティが損なわれる。	GCS-R10
GCS-C2O-301	クラス 2	Optional	3)監査要件 サイバーセキュリティの状態認識	ログの記録	①サイバーセキュリティ関連の状態情報（ソフトウェアアップデートのインストール、ログイン試行の失敗、設定変更など）を監査証跡としてログに記録できること。 ※監査証跡の蓄積機能は、機器またはサーバ側のいずれかが有するものとする。 ②特権的ユーザによる監査証跡（ログ）の読み出しを可能とすること。 ③監査証跡の保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行うこと。 ※監査証跡（ログ）を保存する期間については、対象製品やサービスごとに必要な期間を検討し、定義するものとする。	・機能・サービス	・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・インシデント分析に必要なログ情報の不足によってインシデントへの対応の遅れや、再発防止策の検討が困難となる。	GCS-R16
GCS-	クラス 3	Mandatory	1)機能要件	機器認証	①クラウドシステム、地上制御局との相互認証を行う仕組み	・フライトログ	・無線通信用イ	不正アクセス、なりすまし]	GCS-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
C3M-101			インタフェースへの論理的アクセス		を有すること。 ②相互認証に必要な情報の管理（相互認証に必要な情報が漏えいしないような仕組み）を実装すること。 ※暗号化による相互情報の管理を行う場合は、以下の参考ガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」、「NIST SP（Special Publications） 800-57」、「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ンタフェース（データ通信）	・無線通信インタフェースへのアクセス時に適切な認証が行われず、不正アクセスや地上制御局のなりすましに不正操作が行われる。	
GCS-C3M-102	クラス 3	Mandatory	1)機能要件ソフトウェアの更新	ソフトウェア更新機能	①使用している OS、boot プログラム、アプリケーションに脆弱性が報告された場合には、テストを実施した上で、速やかに更新用ソフトウェアの提供を行うこと。	機能・サービス	・無線通信用インタフェース（データ通信）	[セキュリティ、可用性への脅威] ・ソフトウェアの脆弱性への対策や機能修正を実施できず、対象機器のセキュリティや可用性を維持できない。	GCS-R09
GCS-C3M-201	クラス 3	Mandatory	2)運用要件脆弱性の診	脆弱性診断	①機器が外部からの脆弱性スキャンに対応できる能力を有すること。	・フライトログ ・記録映像	・無線通信用インタフェース（デ	[情報漏洩、データの改ざん、その他複合的な脅	GCS-R17

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
			断		②製品の開発完了時、および、更新ソフトウェアの提供前に、脆弱性スキャンツールによる TCP/UDP サービスポートをネットワークスキャンし、脆弱性の有無をチェックすること。 ※Bluetooth については、Blueborne の脆弱性についても診断及び対策を行うこと。 ③製品の開発完了時、および、更新ソフトウェアの提供前に、実装しているプラットフォームに影響を与える既知のマルウェアの有無を検査すること。 ④脆弱性やマルウェアが検出された場合には、問題の影響度、重要度を踏まえ、セキュリティ対策の必要可否を検討の上、対応すること。 ⑤バッファオーバーフローに類する問題が検出された場合には、実装しているプラットフォームに応じたバッファオーバーフロー対策（攻撃に対する手がかりの最小化等）を行うこと。 ⑥製品販売後に問題が確認された場合には、「ORG-C2M-M04」で定義する脆弱性情報の開示ポリシーに応じた対応を行うこと。 ※上記①は、機器自体に脆弱性検知の仕組みの実装を求めるものではない。	・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・プログラムコード(地上制御局) ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ータ通信）	威] ・ソフトウェアに潜在する既知の脆弱性を利用し、機器内のデータの窃取や改ざん、あるいは可用性がそこなわれる。	
GCS-C3O-101	クラス 3	Optional	1)機能要件製品のセキュリティ	DoS 対策	①可用性に配慮し、冗長性を持たせた設計とすること。 例）対象機器のリソースに過剰な負荷を掛けたり、脆弱性を突くことによる(D)DoS 攻撃を想定し、負荷試験の実施及び一定レベルの負荷に耐える設計とすること。	機能・サービス ※対象機器の可用性	・無線通信用インタフェース（データ通信）	[サービス不能] ・無線通信用インタフェースに DoS 攻撃された結果、本体の機能やサービ	GCS-R15

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
								スが停止し、必要なデータにアクセスできなくなる。	
GCS-C3O-102	クラス 3	Optional	1)機能要件 製品のセキュリティ	セキュアブート	①対象機器起動時の安全性を確保するため、セキュアブートを有すること。	/ プログラムコード(地上制御局)	・無線通信用インタフェース（データ通信）	[改ざん、マルウェア感染] ブートローダや OS などが外部の攻撃者やマルウェアによって不正に改ざん、偽装されることで、対象機器のセキュリティや可用性が損なわれる。	GCS-R14
GCS-C3O-103	クラス 3	Optional	1)機能要件 製品のセキュリティ	ハードウェアハッキング対策	①対象機器の信頼性を保証するための RoT（Root of Trust）を有すること。 ②ハードウェアのデバッグインタフェースを無効化すること。	・プログラムコード(地上制御局) ・機器本体（ハードウェア） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	・基板・回路上のポート（JTAG、UART など）	[情報漏洩、その他の複合的な脅威] ・本体からソフトウェアを抽出され、ハードコートされたパスワードや脆弱性等の解析により、攻撃に利用される。	GCS-R19
GCS-C3O-104	クラス 3	Optional	1)機能要件 製品のセキュリティ	リバースエンジニアリング対策	①対象機器の不正な複製デバイスの作成を防止するため、リバースエンジニアリング対策を行うこと。 ※リバースエンジニアリング対策の例 ・プログラムデータの難読化、動的ライブラリの暗号化 ・セキュア OS の利用による、アクセス制御や特権の最小化 ・コードは、サービス/デバイスが動作するために必要な機能に	・プログラムコード	・基板・回路上のポート（JTAG、UART など）	[なりすまし、情報漏洩] ・不正に作成された複製デバイスにより、企業のブランドや信用力の低下につながる可能性がある。	GCS-R20

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					最小化 ・ハッシュツリーによる、保存・処理・転送されるデータの検証（改ざん防止）…など				

5.3.3 ドローン運用クラウドにおけるセキュリティ要件

クラウドの要件については、既に総務省、経済産業省よりガイドライン[36]がリリースされており、本書では、以下に該当する要件に絞り、記載している。

・守るべき資産のデータ保護を行う上で、本質的な対策要件

・「ドローン本体」や「地上制御局」との連携において必要な対策要件

ドローン運用クラウドにおけるセキュリティ要件を表 5-17 に示す。

- クラス 2　Mandatory 要件：2 要件
- クラス 2　Optional 要件：3 要件
- クラス 3　Mandatory 要件：1 要件
- クラス 3　Optional 要件：要件記載なし

表 5-17 ドローン運用クラウドにおけるセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
DPF-C2M-101	クラス 2	Mandatory	1)機能要件 データの保護	通信経路暗号化	①インターネットで通信を行う区間は、暗号化による保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ②通信経路の暗号化に用いる鍵や証明書の管理を適切に	・アップデート用プログラムコード ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	インターネット通信用インタフェース	[情報漏えい、データの改ざん] ・ドローン本体や地上制御局との通信におけるデータが傍受、改ざんされる。 ・鍵情報の漏洩によって、	DPF-R15

[36] 総務省 『クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）』 2021 年 9 月
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html
経済産業省 『クラウドサービス利用のための情報セキュリティマネジメントガイドライン』 2014 年 3 月
https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000146.html

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」 「NIST SP（Special Publications） 800-57」 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」			守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	
DPF-C2M-102	クラス 2	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①対象機器が一意の論理的 ID または物理的な ID を有すること。 ②接続している機器の論理的 ID（または物理的 ID）を読み取り可能とすること。また最新の状態に更新可能であること。 ③ドローン本体、地上制御局、クラウドサーバ間で行われる TCP/UDP 通信については、通信相手を識別・認証する仕組みを有すること。 ④連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権的ユーザへのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ⑤機器のセキュリティ関連機能を含め、重要な構成変更を行う機能については特権的ユーザを適切に識別、認証し、特権的ユーザ以外による機能の実行を制限すること。	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス	インターネット通信用インタフェース	[不正アクセス・なりすまし] ・インターネット通信インタフェースへのアクセス時に認証が行われず、無人航空機や地上制御局になりすまされる。 ・ソフトウェアの脆弱性を突かれ、クラウドシステム上の認証情報が改ざんされる。	DPF-R02
DPF-C2O-	クラス 2	Optional	1)機能要件	データ暗号化	①クラウドシステムに記録される守るべき資産については、暗	・アップデート用プログラムコード	インターネッ	[情報漏洩、データの改ざ	DPF-R08

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
101			データの保護		号化によるデータの保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ②データの暗号化に用いる鍵の管理を適切に行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」 「NIST SP（Special Publications） 800-57」 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ト通信用インタフェース	ん] ・クラウドシステムへの、不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・データ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	
DPF-C2O-102	クラス 2	Optional	1)機能要件インタフェースへの論理的アクセス	機器認証	①認証に必要な情報について、適切な暗号化をすること ※暗号化については、以下を参考にガイドラインに準拠した実装とすること 「TLS 暗号設定ガイドライン」 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	インターネット通信用インタフェース	[不正アクセス、その他の複合的な脅威] ・不正アクセスが発生した場合に、窃取された認証情報が攻撃に悪用され、対象機器のセキュリティや可用性が阻害される。	DPF-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
DPF-C2O-301	クラス 2	Optional	3)監査要件サイバーセキュリティの状態認識	ログの記録	①サイバーセキュリティ関連の状態情報（ソフトウェアアップデートのインストール、ログイン試行の失敗、設定変更など）を監査証跡としてログに記録できること。 ※監査証跡の蓄積機能は、機器またはサーバ側のいずれかが有するものとする。 ②特権的ユーザによる監査証跡（ログ）の読み出しを可能とすること。 ③監査証跡の保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行うこと。 ※監査証跡（ログ）を保存する期間については、対象製品やサービスごとに必要な期間を検討し、定義するものとする	・機能・サービス	インターネット通信用インタフェース	[セキュリティ、可用性への脅威] ・インシデント分析に必要なログ情報の不足によってインシデントへの対応の遅れや、再発防止策の検討が困難となる。	DPF-R11
DPF-C3M-101	クラス 3	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①ドローン本体、地上制御局との相互認証を行う仕組みを有すること。 ②相互認証に必要な情報の管理（相互認証に必要な情報が漏えいしないような仕組み）を実装すること。 ※暗号化による相互情報の管理を行う場合は、以下の参考ガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」 「NIST SP（Special Publications） 800-57」 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	インターネット通信用インタフェース	[情報漏洩、データの改ざん] ・クラウドシステムへの、不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・データ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。	DPF-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
								・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	

5.3.4 サービス運用クラウドにおけるセキュリティ要件

クラウドの要件については、既に総務省、経済産業省よりガイドラインがリリースされており、本書では、以下に該当する要件に絞り、記載している。

（総務省、経済産業省のガイドラインについては、本書 5.3.3 項の脚注を参照）

・守るべき資産のデータ保護を行う上で、本質的な対策要件

・「ドローン本体」や「地上制御局」との連携において必要な対策要件

サービス運用クラウドにおけるセキュリティ要件を表 5-18 に示す。

- クラス 2　Mandatory 要件：2 要件
- クラス 2　Optional 要件：3 要件
- クラス 3　Mandatory 要件：1 要件
- クラス 3　Optional 要件：要件記載なし

表 5-18 サービス運用クラウドにおけるセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
SPF-C2M-101	クラス 2	Mandatory	1)機能要件 データの保護	通信経路暗号化	①インターネットで通信を行う区間は、暗号化による保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ②通信経路の暗号化に用いる鍵や証明書の管理を適切に行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」	・記録映像 ・テレメトリデータ ・センサ取得情報 ・アクセスログ等の監視情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	インターネット通信用インタフェース	[情報漏えい、データの改ざん] ・ドローン本体や地上制御局との通信におけるデータが傍受、改ざんされる。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	SPF-R15

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					「NIST SP（Special Publications） 800-57」 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」				
SPF-C2M-102	クラス 2	Mandatory	1)機能要件 インタフェースへの論理的アクセス	機器認証	①対象機器が一意の論理的 ID または物理的な ID を有すること。 ②接続している機器の論理的 ID（または物理的 ID）を読み取り可能とすること。また最新の状態に更新可能であること。 ③ドローン本体、地上制御局、クラウドサーバ間で行われる TCP/UDP 通信については、通信相手を識別・認証する仕組みを有すること。 ④連続したログイン試行による攻撃への対処として、一定回数を越えるログイン試行に対して特権的ユーザへのアラート通知、あるいは対象アカウントを一定時間無効化する等の対策を行うこと。 ⑤機器のセキュリティ関連機能を含め、重要な構成変更を行う機能については特権的ユーザを適切に識別、認証し、特権的ユーザ以外による機能の実行を制限すること。	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス	インターネット通信用インタフェース	[不正アクセス・なりすまし] ・インターネット通信インタフェースへのアクセス時に認証が行われず、無人航空機や地上制御局になりすまされる。 ・ソフトウェアの脆弱性を突かれ、クラウドシステム上の認証情報が改ざんされる。	SPF-R02
SPF-C2O-101	クラス 2	Optional	1)機能要件 データの保護	データ暗号化	①クラウドシステムに記録される守るべき資産については、暗号化によるデータの保護を行うこと。 ※暗号化については、以下を参考にガイドラインに準拠した実装とすること。 「電子政府における調達のために参照すべき暗号のリスト」	・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	インターネット通信用インタフェース	[情報漏洩、データの改ざん] ・クラウドシステムへの、不正アクセスが行われた場合に、守るべき資産が窃	SPF-R08

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」 ②データの暗号化に用いる鍵の管理を適切に行うこと。 ※鍵管理の方法については、以下を参考にガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」 「NIST SP（Special Publications） 800-57」 「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		取され、データが漏えいする。 ・データ暗号用の鍵が改ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	
SPF-C2O-102	クラス 2	Optional	1)機能要件 インタフェースへの論理的アクセス	機器認証	①認証に必要な情報について、適切な暗号化をすること ※暗号化については、以下を参考にガイドラインに準拠した実装とすること 「TLS 暗号設定ガイドライン」 「電子政府における調達のために参照すべき暗号のリスト」 もしくは「CRYPTREC 暗号技術ガイドライン(軽量暗号)」	・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報	インターネット通信用インタフェース	[不正アクセス、その他の複合的な脅威] ・不正アクセスが発生した場合に、窃取された認証情報が攻撃に悪用され、対象機器のセキュリティや可用性が阻害される。	SPF-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
						・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書			
SPF-C2O-301	クラス 2	Optional	3)監査要件サイバーセキュリティの状態認識	ログの記録	①サイバーセキュリティ関連の状態情報（ソフトウェアアップデートのインストール、ログイン試行の失敗、設定変更など）を監査証跡としてログに記録できること。 ※監査証跡の蓄積機能は、機器またはサーバ側のいずれかが有するものとする。 ②特権的ユーザによる監査証跡（ログ）の読み出しを可能とすること。 ③監査証跡の保存容量を超過した場合には、古い記録から順次上書きするなど、管理上の対策を行うこと。 ※監査証跡（ログ）を保存する期間については、対象製品やサービスごとに必要な期間を検討し、定義するものとする	・機能・サービス	インターネット通信用インタフェース	[セキュリティ、可用性への脅威] ・インシデント分析に必要なログ情報の不足によってインシデントへの対応の遅れや、再発防止策の検討が困難となる。	SPF-R11
SPF-C3M-101	クラス 3	Mandatory	1)機能要件インタフェースへの論理的アクセス	機器認証	①ドローン本体、地上制御局との相互認証を行う仕組みを有すること。 ②相互認証に必要な情報の管理（相互認証に必要な情報が漏えいしないような仕組み）を実装すること。 ※暗号化による相互情報の管理を行う場合は、以下の参考ガイドラインに準拠した実装とすること。 「TLS 暗号設定ガイドライン」 「NIST SP（Special Publications） 800-57」	・記録映像 ・テレメトリデータ センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果	インターネット通信用インタフェース	[情報漏洩、データの改ざん] ・クラウドシステムへの、不正アクセスが行われた場合に、守るべき資産が窃取され、データが漏えいする。 ・データ暗号用の鍵が改	SPF-R02

要件 ID	セキュリティクラス	対応優先度	セキュリティ対策			守るべき資産	対象インタフェース	対策すべき脅威	要求事項 ID
			大分類/中分類	小分類	内容				
					「SSL/TLS 暗号設定ガイドライン改定及び鍵管理ガイドライン作成のための調査・検討－調査報告書－」	・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書		ざん・漏えいされ、暗号化されたデータを解析される。 ・鍵情報の漏洩によって、守るべき資産が窃取、改ざんされ、対象機器のセキュリティや可用性が損なわれる。	

5.3.5 メーカにおける組織としてのセキュリティ要件

メーカにおける組織の活動に関するセキュリティ要件を表 5-19 に示す。

- クラス 2　Mandatory 要件：8 要件
- クラス 2　Optional 要件：7 要件
- クラス 3　Mandatory 要件：4 要件
- クラス 3　Optional 要件：要件記載なし

表 5-19 メーカにおける組織としてのセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
ORG-C2M-M01	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理方針の策定	①企業組織としての情報セキュリティに対するリスクマネジメントの方針やルールなど、情報セキュリティの管理方針を策定する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR01
ORG-C2M-M02	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理体制の構築	①組織内の情報セキュリティの役割及び責任を明確にし、情報セキュリティの管理体制を構築する。	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR02
ORG-C2M-M03	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスのシステムモデル、ユースケースの定義	①製品の要件を踏まえ、システムモデルやユースケースの定義を行う。システムモデルにおいては、サービス事業者と外部委託先等、提携する企業との責任分解点を明確化する。 ②システムモデルにおいてはソフトウェア構成及び、ハードウェア構成を明確にすると共に、各機能を明示すること。 ③ユースケースにおいては、物理的な使用環境（設置場所等）や	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR03

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					関係するアクター（ステークホルダー）についても明示しておくこと。			
ORG-C2M-M04	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	脆弱性やセキュリティに関する連絡窓口の設置	①製品やサービスにおいて、脆弱性やセキュリティへの影響が懸念される問題の連絡窓口を設置する。 ②脆弱性関連情報の取扱いや情報開示についてのポリシーを策定、公表していること。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR03
ORG-C2M-M05	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	更新ソフトウェアの提供	①使用しているソフトウェアに脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行う。	運用	・ドローン本体 ・地上制御局	ORG-OR04
ORG-C2M-M06	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	①リスクアセスメントを行い、想定される脅威およびリスクの評価、対策を行う。 ②リスクアセスメントの過程で、個人情報や機密データなどの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、製品の重要度を定義する。 ③製品やサービスが関連する、情報セキュリティ関連法令や要求事項を確認し、遵守する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR04
ORG-C2M-M07	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品のセキュリティサポートに関する利用者への周知	①初期設定の方法など、利用上、情報セキュリティ面に影響が生じる設定や使用方法については、安全に利用できる手順を利用者に明示する。 ②製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを利用者へ周知する。 ③想定される事故や障害に対して、免責事項を利用者へ周知する。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR02

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					④対象製品やサービスのサポート期限やサポート終了時の方針を利用者に通知する。 ⑤保守、メンテナンス業務の要件や手順及び、サイバーセキュリティ上の考慮事項を定義し、文書化する。また、外部委託を行う場合は、委託先の選定要件を定義する。 ※ISO27001 を取得している場合は、免除			
ORG-C2M-M08	クラス 2	Mandatory	3)サプライチェーン対策	ソフトウェア、ハードウェアコンポーネントの管理	①製品やクラウドシステムで利用される各コンポーネントに対して、名称やバージョンなどをソフトウェア・ハードウェアの構成表として管理し、更新を適用した場合には構成表の更新を行う。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR04
ORG-C2O-M01	クラス 2	Optional	2) 必要な情報セキュリティ管理体制	情報セキュリティや関連法令に関する教育および訓練	①情報セキュリティ管理の方針や手順、事業に関連する法令等について、教育および訓練を実施する。 ②情報セキュリティのインシデントから得られた情報について、再発防止のための教育および訓練を実施する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR05
ORG-C2O-M02	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	個人情報や収集データの消去方法の利用者への周知	①機器内にデータが残留したまま廃棄することで想定される脅威、リスクを取扱説明書等で明示し、利用者へ注意喚起を促す。 ②廃棄時には機器の設定やメモリ内のデータを初期化（工場出荷状態)することを取扱説明書等で推奨し、実施手順を明示する。	廃棄	・ドローン本体 ・地上制御局	ORG-DR01
ORG-C2O-M03	クラス 2	Optional	1) 脆弱性の評価及び適切	情報セキュリティ管理方針や体制のレビュー	①情報セキュリティ管理の方針や手順に沿って管理やリスクアセスメントが実施されているかどうか評価する。	評価	・ドローン本体 ・地上制御局	ORG-ER01

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
			な対策		※ISO27001 を取得している場合は、免除		・クラウド運用プラットフォーム ・サービス運用クラウド	
ORG-C2O-M04	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	個人情報やテレメトリデータの収集に関するポリシーの公開	①個人情報保護の観点から、収集する個人情報やデータに関する管理方針を利用者へ周知する。 ※ISO27001 を取得している場合は、免除	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR01
ORG-C2O-M05	クラス 2	Optional	3)サプライチェーン対策	サプライチェーンリスクの管理	①サプライチェーンを通じて組み合わされたソフトウェア、ハードウェア製品及び部品要素等が、要求仕様通りに開発、製造され、意図していない変更が加えられていないことを確認する。 ②サプライチェーンリスクを増大させる要因となる脆弱性を可能な限り軽減させるための対策として、製造プロセスや情報セキュリティ管理体制が透明化、可視化され、機器に不正が見つかったときの追跡力（トレーサビリティ）を確保する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR02
ORG-C2O-M06	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	製品に対する品質保証体制の確立と実行	①製品やサービスに対する品質保証体制を確立し、情報セキュリティを含めた検証を実施する。 ②サプライチェーンのリスク管理として、委託先やサプライヤに対して情報セキュリティを含めた検証を義務付ける。	評価	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-ER02
ORG-C2O-M07	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	情報セキュリティのインシデント管理およびインシデントレスポンス対応	①製品やサービスにおいてインシデントが発生した場合には、 担当部門が対処し、再発防止対策も行う。 ②発生したインシデントについて、外部組織と連携し、適切な対応を行う。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム	ORG-OR10

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					※ISO27001 を取得している場合は、免除		・サービス運用クラウド	
ORG-C3M-M01	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	開発・製造環境のセキュリティ対策	①PC 等には、マルウェア対策ソフトを導入し、マルウェアに関するリスクを軽減する。 ②入退室管理や装置の物理的な保護等、物理的及び環境的セキュリティを考慮した保護を行う。 ③ネットワークのアクセス制御や通信ログの取得、監視等を実施する。 ※ISO27001 を取得している場合は、免除	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR01
ORG-C3M-M02	クラス 3	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティや関連法令に関する教育および訓練	①サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置していること	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR05
ORG-C3M-M03	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	デザインレビューやコードレビュー	①セキュア設計・開発プロセスの一環として、情報セキュリティに関するデザインレビューやコードレビューを実施する。 ②レビュワーについては、対象製品や情報セキュリティに関する技術面でのスキル、知識、実績を踏まえて、人材を選出する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR05
ORG-C3M-M04	クラス 3	Mandatory	3)サプライチェーン対策	開発委託先や部材調達先に対するセキュリティ管理の要求	①製品やクラウドシステムの開発委託を行う場合は、委託先の情報セキュリティ管理体制が自社と同程度の水準をポリシーとして満たすことを要求する。 ②新たな機器の開発やソリューションが必要となった場合、製品のセ	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム	ORG-MR03

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					キュリティ要求事項を委託先へ提示し、準拠することを必須とする。 ※ISO27001 を取得している場合は、免除		・サービス運用クラウド	

5.3.6 サプライヤにおける組織としてのセキュリティ要件

サプライヤにおける組織の活動に関するセキュリティ要件を表 5-20 に示す。

- クラス 2　Mandatory 要件：8 要件
- クラス 2　Optional 要件：5 要件
- クラス 3　Mandatory 要件：3 要件
- クラス 3　Optional 要件：要件記載なし

表 5-20 サプライヤにおける組織としてのセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
ORG-C2M-S01	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理方針の策定	①企業組織としての情報セキュリティに対するリスクマネジメントの方針やルールなど、情報セキュリティの管理方針を策定する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR01
ORG-C2M-S02	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理体制の構築	①組織内の情報セキュリティの役割及び責任を明確にし、情報セキュリティの管理体制を構築する。	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR02
ORG-C2M-S03	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスのシステムモデル、ユースケースの定義	①製品の要件を踏まえ、システムモデルやユースケースの定義を行う。システムモデルにおいては、サービス事業者と外部委託先等、提携する企業との責任分解点を明確化する。 ②システムモデルにおいてはソフトウェア構成及び、ハードウェア構成を明確にすると共に、各機能を明示すること。 ③ユースケースにおいては、物理的な使用環境（設置場所等）や	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR03

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					関係するアクター（ステークホルダー）についても明示しておくこと。			
ORG-C2M-S04	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	脆弱性やセキュリティに関する連絡窓口の設置	①製品やサービスにおいて、脆弱性やセキュリティへの影響が懸念される問題の連絡窓口を設置する。 ②脆弱性関連情報の取扱いや情報開示についてのポリシーを策定、公表していること。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR03
ORG-C2M-S05	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	更新ソフトウェアの提供	①使用しているソフトウェアに脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行う。	運用	・ドローン本体 ・地上制御局	ORG-OR04
ORG-C2M-S06	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	①リスクアセスメントを行い、想定される脅威およびリスクの評価、対策を行う。 ②リスクアセスメントの過程で、個人情報や機密データなどの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、製品の重要度を定義する。 ③製品やサービスが関連する、情報セキュリティ関連法令や要求事項を確認し、遵守する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR04
ORG-C2M-S07	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品のセキュリティサポートに関する利用者への周知	①初期設定の方法など、利用上、情報セキュリティ面に影響が生じる設定や使用方法については、安全に利用できる手順を利用者に明示する。 ②製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを利用者へ周知する。 ③想定される事故や障害に対して、免責事項を利用者へ周知する。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR02

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					④対象製品やサービスのサポート期限やサポート終了時の方針を利用者に通知する。 ⑤保守、メンテナンス業務の要件や手順及び、サイバーセキュリティ上の考慮事項を定義し、文書化する。また、外部委託を行う場合は、委託先の選定要件を定義する。 ※ISO27001 を取得している場合は、免除			
ORG-C2M-S08	クラス 2	Mandatory	3)サプライチェーン対策	ソフトウェア、ハードウェアコンポーネントの管理	①製品やクラウドシステムで利用される各コンポーネントに対して、名称やバージョンなどをソフトウェア・ハードウェアの構成表として管理し、更新を適用した場合には構成表の更新を行う。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR04
ORG-C2O-S01	クラス 2	Optional	2) 必要な情報セキュリティ管理体制	情報セキュリティや関連法令に関する教育および訓練	①情報セキュリティ管理の方針や手順、事業に関連する法令等について、教育および訓練を実施する。 ②情報セキュリティのインシデントから得られた情報について、再発防止のための教育および訓練を実施する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR05
ORG-C2O-S02	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	情報セキュリティ管理方針や体制のレビュー	①情報セキュリティ管理の方針や手順に沿って管理やリスクアセスメントが実施されているかどうか評価する。 ※ISO27001 を取得している場合は、免除	評価	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-ER01
ORG-	クラス 2	Optional	3)サプライチェ	サプライチェーンリスクの	①サプライチェーンを通じて組み合わされたソフトウェア、ハードウェア製	設計・製造	・ドローン本体	ORG-

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
C2O-S03			ーン対策	管理	品及び部品要素等が、要求仕様通りに開発、製造され、意図していない変更が加えられていないことを確認する。 ②サプライチェーンリスクを増大させる要因となる脆弱性を可能な限り軽減させるための対策として、製造プロセスや情報セキュリティ管理体制が透明化、可視化され、機器に不正が見つかったときの追跡力（トレーサビリティ）を確保する。		・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	MR02
ORG-C2O-S04	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	製品に対する品質保証体制の確立と実行	①製品やサービスに対する品質保証体制を確立し、情報セキュリティを含めた検証を実施する。 ②サプライチェーンのリスク管理として、委託先やサプライヤに対して情報セキュリティを含めた検証を義務付ける。	評価	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-ER02
ORG-C2O-S05	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	情報セキュリティのインシデント管理およびインシデントレスポンス対応	①製品やサービスにおいてインシデントが発生した場合には、 担当部門が対処し、再発防止対策も行う。 ②発生したインシデントについて、外部組織と連携し、適切な対応を行う。 ※ISO27001 を取得している場合は、免除	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR10
ORG-C3M-S01	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	開発・製造環境のセキュリティ対策	①PC 等には、マルウェア対策ソフトを導入し、マルウェアに関するリスクを軽減する。 ②入退室管理や装置の物理的な保護等、物理的及び環境的セキュリティを考慮した保護を行う。 ③ネットワークのアクセス制御や通信ログの取得、監視等を実施する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR01

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					※ISO27001 を取得している場合は、免除			
ORG-C3M-S02	クラス 3	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティや関連法令に関する教育および訓練	①サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置していること	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR05
ORG-C3M-S03	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	デザインレビューやコードレビュー	①セキュア設計・開発プロセスの一環として、情報セキュリティに関するデザインレビューやコードレビューを実施する。 ②レビュワーについては、対象製品や情報セキュリティに関する技術面でのスキル、知識、実績を踏まえて、人材を選出する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR05
ORG-C3M-M04	クラス 3	Mandatory	3)サプライチェーン対策	開発委託先や部材調達先に対するセキュリティ管理の要求	①製品やクラウドシステムの開発委託を行う場合は、委託先の情報セキュリティ管理体制が自社と同程度の水準をポリシーとして満たすことを要求する。 ②新たな機器の開発やソリューションが必要となった場合、製品のセキュリティ要求事項を委託先へ提示し、準拠することを必須とする。 ※ISO27001 を取得している場合は、免除	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR03

5.3.7 サービス事業者における組織としてのセキュリティ要件

クラウドシステムのサービス事業者における組織の活動に関するセキュリティ要件を表 5-21 に示す。

- クラス 2　Mandatory 要件：13 要件
- クラス 2　Optional 要件：5 要件
- クラス 3　Mandatory 要件：3 要件
- クラス 3　Optional 要件：要件記載なし

表 5-21 サービス事業者における組織としてのセキュリティ要件

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
ORG-C2M-P01	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理方針の策定	①企業組織としての情報セキュリティに対するリスクマネジメントの方針やルールなど、情報セキュリティの管理方針を策定する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR01
ORG-C2M-P02	クラス 2	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理体制の構築	①組織内の情報セキュリティの役割及び責任を明確にし、情報セキュリティの管理体制を構築する。	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR02
ORG-C2M-P03	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスのシステムモデル、ユースケースの定義	①製品の要件を踏まえ、システムモデルやユースケースの定義を行う。システムモデルにおいては、サービス事業者と外部委託先等、提携する企業との責任分解点を明確化する。 ②システムモデルにおいてはソフトウェア構成及び、ハードウェア構成を明確にすると共に、各機能を明示すること。 ③ユースケースにおいては、物理的な使用環境（設置場所等）や	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR03

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					関係するアクター（ステークホルダー）についても明示しておくこと。			
ORG-C2M-P04	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	個人情報やテレメトリデータの収集に関するポリシーの公開	①個人情報保護の観点から、収集する個人情報やデータに関する管理方針を利用者へ周知する。 ②取得する情報（映像、画像）が、特定の個人を識別可能な場合には、個人情報として取り扱う必要があることから、ウェブページ等により、利用目的を事前告知することが望ましい。また、無人航空機による情報（映像、画像）がサービスに提供に利用される場合には、生活者の特定を目的したものではない点を、提供サービスのウェブページ等により明示すること。 ③取得する情報（撮影映像や測量成果等）に個人情報が含まれる場合、インターネット上で公開するサービス事業者は、本人関与や削除要求対応の仕組み整備し、削除依頼への対応を適切に行うこと。担当者、担当窓口等を明確化し、インターネットでの相談窓口に加え、必要に応じて電話対応もできるようにすること。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR01
ORG-C2M-P05	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	脆弱性やセキュリティに関する連絡窓口の設置	①製品やサービスにおいて、脆弱性やセキュリティへの影響が懸念される問題の連絡窓口を設置する。 ②脆弱性関連情報の取扱いや情報開示についてのポリシーを策定、公表していること。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR03
ORG-C2M-P06	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	更新ソフトウェアの提供	①使用しているソフトウェアに脆弱性が報告された場合には、速やかに更新用ソフトウェアの提供を行う。 ※運用しているクラウド環境及び機器については更新対応を行う。	運用	・ドローン本体 ・地上制御局	ORG-OR04
ORG-C2M-P07	クラス 2	Mandatory	1) 脆弱性の評価及び適切	個人情報や収集データの消去方法の利用	①機器内にデータが残留したまま廃棄することで想定される脅威、リスクを取扱説明書等で明示し、利用者へ注意喚起を促す。	廃棄	・ドローン本体 ・地上制御局	ORG-OR02

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
			な対策	者への周知	②廃棄時には機器の設定やメモリ内のデータを初期化（工場出荷状態)することを取扱説明書等で推奨し、実施手順を明示する。			
ORG-C2M-P08	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	収集した個人情報やテレメトリデータの消去	①製品やサービスのサポートの終了時には個人情報の管理ポリシーに沿って、収集した個人情報やテレメトリデータを消去する。 ②廃棄を行う事業者に依頼する場合、データの初期化を求める。 ※上記①は原則であり、利用ユーザとの契約期間が満了し、サポートが終了した場合に、収集した個人情報及び、テレメトリデータを消去するかは、サービス事業者と利用ユーザ間での契約（約款）に従うものとする。	廃棄	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-DR02
ORG-C2M-P09	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	①リスクアセスメントを行い、想定される脅威およびリスクの評価、対策を行う。 ②リスクアセスメントの過程で、個人情報や機密データなどの重要なデータの取り扱いの有無、および生命・財産への影響の有無を検討して、製品の重要度を定義する。 ③製品やサービスが関連する、情報セキュリティ関連法令や要求事項を確認し、遵守する。 ※ISO27001 を取得している場合は、免除	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR04
ORG-C2M-P10	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	製品のセキュリティサポートに関する利用者への周知	①初期設定の方法など、利用上、情報セキュリティ面に影響が生じる設定や使用方法については、安全に利用できる手順を利用者に明示する。 ②製品のソフトウェア更新の内容や必要性、更新を行わない場合の影響などを利用者へ周知する。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR02

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
					③想定される事故や障害に対して、免責事項を利用者へ周知する。 ④対象製品やサービスのサポート期限やサポート終了時の方針を利用者に通知する。 ⑤保守、メンテナンス業務の要件や手順及び、サイバーセキュリティ上の考慮事項を定義し、文書化する。また、外部委託を行う場合は、委託先の選定要件を定義する。 ※ISO27001 を取得している場合は、免除			
ORG-C2M-P11	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	運用上のオペレーション手順や管理手順の明確化、遵守	①過失等による情報の漏えいや紛失を防ぐため、システムの操作手順書（取扱説明書）や管理手順書を整備する。 ※ISO27001 を取得している場合は、免除	運用	・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR05
ORG-C2M-P12	クラス 2	Mandatory	1) 脆弱性の評価及び適切な対策	守るべき資産のバックアップ	①バックアップ対象の情報資産や保管場所に関するポリシーに沿ったバックアップを実施する。 ②・データをリカバリ可能かどうかを含め、バックアップが確実に行われているか確認する。 ※ISO27001 を取得している場合は、免除	運用	・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR07
ORG-C2O-P13	クラス 2	Mandatory	3)サプライチェーン対策	ソフトウェア、ハードウェアコンポーネントの管理	①製品やクラウドシステムで利用される各コンポーネントに対して、名称やバージョンなどをソフトウェア・ハードウェアの構成表として管理し、更新を適用した場合には構成表の更新を行う。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR04
ORG-	クラス 2	Optional	2) 必要な情	情報セキュリティや関	①情報セキュリティ管理の方針や手順、事業に関連する法令等につ	製品企画	・ドローン本体	ORG-

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
C2O-P01			報セキュリティ管理体制	連法令に関する教育および訓練	いて、教育および訓練を実施する。 ②情報セキュリティのインシデントから得られた情報について、再発防止のための教育および訓練を実施する。 ※ISO27001 を取得している場合は、免除		・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	PR05
ORG-C2O-P02	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	情報セキュリティ管理方針や体制のレビュー	①情報セキュリティ管理の方針や手順に沿って管理やリスクアセスメントが実施されているかどうか評価する。 ※ISO27001 を取得している場合は、免除	評価	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-ER01
ORG-C2O-P03	クラス 2	Optional	3)サプライチェーン対策	サプライチェーンリスクの管理	①サプライチェーンを通じて組み合わされたソフトウェア、ハードウェア製品及び部品要素等が、要求仕様通りに開発、製造され、意図していない変更が加えられていないことを確認する。 ②サプライチェーンリスクを増大させる要因となる脆弱性を可能な限り軽減させるための対策として、製造プロセスや情報セキュリティ管理体制が透明化、可視化され、機器に不正が見つかったときの追跡力（トレーサビリティ）を確保する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR02
ORG-C2O-P04	クラス 2	Optional	1) 脆弱性の評価及び適切な対策	製品に対する品質保証体制の確立と実行	①製品やサービスに対する品質保証体制を確立し、情報セキュリティを含めた検証を実施する。 ②サプライチェーンのリスク管理として、委託先やサプライヤに対して情報セキュリティを含めた検証を義務付ける。	評価	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-ER02
ORG-C2O-M07	クラス 2	Optional	1) 脆弱性の評価及び適切	情報セキュリティのインシデント管理およびイン	①製品やサービスにおいてインシデントが発生した場合には、 担当部門が対処し、再発防止対策も行う。	運用	・ドローン本体 ・地上制御局	ORG-OR10

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
			な対策	シデントレスポンス対応	②発生したインシデントについて、外部組織と連携し、適切な対応を行う。 ※ISO27001 を取得している場合は、免除		・クラウド運用プラットフォーム ・サービス運用クラウド	
ORG-C3M-P01	クラス 3	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティの管理体制の構築	①サイバーセキュリティの確保のための管理体制について、第三者認証（ISO 27001）を取得し、維持していること	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR02
ORG-C3M-P02	クラス 3	Mandatory	2) 必要な情報セキュリティ管理体制	情報セキュリティや関連法令に関する教育および訓練	①サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士又はこれと同等以上の知識及び技能を有すると認められる者を配置していること	製品企画	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-PR05
ORG-C3M-P03	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	デザインレビューやコードレビュー	①セキュア設計・開発プロセスの一環として、情報セキュリティに関するデザインレビューやコードレビューを実施する。 ②レビュワーについては、対象製品や情報セキュリティに関する技術面でのスキル、知識、実績を踏まえて、人材を選出する。	設計・製造	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-MR05

サービス事業者のセキュリティ要件では、セキュリティクラス３の「ORG-C3M-P03　情報セキュリティの管理体制の構築」において、ISO27001 の取得を求めている。本書 5.2 節の要求事項で提示した項目の中には、ISO27001 の管理基準に包含されるため、セキュリティ要件から除外した項目が存在する。表 5-22 に参考情報として、該当する要件を示す。

表 5-22　別表 ISO27001 に含まれるセキュリティ要件（参考情報）

要件 ID	セキュリティクラス	対応優先度	セキュリティクラス			フェーズ	構成要素	要求事項 ID
			大分類	小分類	内容			
ORG-C3M-P04	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	運用環境のセキュリティ対策	①PC 等には、マルウェア対策ソフトを導入し、マルウェアに関するリスクを軽減する。 ②入退室管理や装置の物理的な保護等、物理的及び環境的セキュリティを考慮した保護を行う。 ③ネットワークのアクセス制御や通信ログの取得、監視等を実施する。	運用	・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR06
ORG-C3M-P05	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理	①認証情報の漏えいや紛失等を防ぐため、認証情報のライフサイクル管理を行う。 ②暗号に関する安全性を高めるため、暗号鍵のライフサイクル管理を行う。 ③デジタル証明書の有効期限や失効等の管理を行うため、デジタル証明書のライフサイクル管理を行う。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR08
ORG-C3M-P06	クラス 3	Mandatory	1) 脆弱性の評価及び適切な対策	ログの取得、監視、分析	①情報セキュリティインシデント管理の一環として、製品やクラウドシステムのアクセスログ等を取得および監視する。 ②インシデント発生時のエビデンスとして、収集したログデータの分析を行う。	運用	・ドローン本体 ・地上制御局 ・クラウド運用プラットフォーム ・サービス運用クラウド	ORG-OR09

6 Appendix_A 国内外の主要なガイドラインとの対応関係について

6.1 無人航空機におけるセキュリティ要件と国内外のガイドラインとの対応関係について

本書の無人航空機におけるセキュリティ要件（表 5-15、表 5-16、表 5-17、表 5-18）と国内外における主要なガイドラインとの対応関係を表 6-1 に示す。

表 6-1 セキュリティ要件と関連ガイドラインの対応関係

構成要素	ID	要件	ETSI 303 645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
ドローン本体	UAV-C2M-101	データ消去機能（本体）	○	○	–	–	–	–
ドローン本体	UAV-C2M-102	データ消去機能（外部ストレージ）	○	○	–	–	–	–
ドローン本体	UAV-C2M-103	リモートＩＤ発信時の暗号化対応	○	–	○	○	○	–
ドローン本体	UAV-C2M-104	通信経路暗号化	○	○	○	○	○	○
ドローン本体	UAV-C2M-105	アクセス制御	○	○	○	○	○	○

[37] NIST “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”

[38] 内閣サイバーセキュリティセンター（NISC）「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」

[39] 内閣サイバーセキュリティセンター（NISC）「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
ドローン本体	UAV-C2M-106	セキュリティ設定の変更及び安全な初期設定への復元機能	○	○	○	–	○	–
ドローン本体	UAV-C2M-107	機器認証	○	○	○	○	○	○
ドローン本体	UAV-C2M-108	不要な TCP/UDP ポートの無効化	○	○	○	–	–	○
ドローン本体	UAV-C2M-109	USB デバイスのアクセス制御	○	–	○	–	○	–
ドローン本体	UAV-C2M-110	Bluetooth のアクセス制御	–	–	–	–	–	–
ドローン本体	UAV-C2M-111	Wi-Fi のアクセス制御	–	–	–	–	–	–
ドローン本体	UAV-C2M-112	ソフトウェア更新機能	○	○	○	○	○	–
ドローン本体	UAV-C2M-113	電源停止や障害発生時の対応	–	○	–	–	–	–
ドローン本体	UAV-C2O-101	不要な機能の無効化	○	○	–	–	–	–
ドローン本体	UAV-C2O-102	データ保護（本体）	○	○	○	○	○	○

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
ドローン本体	UAV-C2O-103	データ保護（外部ストレージ）	○	○	○	○	○	○
ドローン本体	UAV-C2O-104	セキュリティ設定の変更及び安全な初期設定への復元機能	○	○	○	–	○	–
ドローン本体	UAV-C2O-105	機器認証	○	–	○	○	○	○
ドローン本体	UAV-C2O-106	不要な TCP/UDP ポートの無効化	○	○	○	–	–	○
ドローン本体	UAV-C2O-107	USB デバイスの不要機能の無効化	○	–	○	–	○	–
ドローン本体	UAV-C2O-108	ソフトウェア更新機能	○	○	○	○	○	–
ドローン本体	UAV-C2O-109	ソフトウェアの真正性と完全性の検証	○	○	○	–	○	○
ドローン本体	UAV-C2O-301	ログの記録	○	○	○	○	○	○
ドローン本体	UAV-C3M-101	機器認証	○	–	○	○	○	○
ドローン本体	UAV-C3M-102	ソフトウェア更新機能	○	–	○	○	○	–

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
ドローン本体	UAV-C3M-201	脆弱性診断	○	–	–	○	○	○
ドローン本体	UAV-C3O-101	DoS 対策	○	–	–	○	○	–
ドローン本体	UAV-C3O-102	セキュアブート	–	–	–	–	–	–
ドローン本体	UAV-C3O-103	ハードウェアハッキング対策	○	–	○	–	–	○
ドローン本体	UAV-C3O-104	リバースエンジニアリング対策	–	–	–	–	○	○
地上制御局	GCS-C2M-101	データ消去機能（本体）	○	○	–	–	–	–
地上制御局	GCS-C2M-102	データ消去機能（外部ストレージ）	○	○	–	–	–	–
地上制御局	GCS-C2M-103	通信経路暗号化	○	○	○	○	○	○
地上制御局	GCS-C2M-104	アクセス制御	○	○	○	○	○	○
地上制御局	GCS-C2M-105	セキュリティ設定の変更及び安全な初期設定への復元機能	○	○	○	–	○	–

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
地上制御局	GCS-C2M-106	機器認証	○	○	○	○	○	○
地上制御局	GCS-C2M-107	ユーザ認証	○	○	○	○	○	○
地上制御局	GCS-C2M-108	不要な TCP/UDP ポートの無効化	○	○	○	–	–	○
地上制御局	GCS-C2M-109	USB デバイスの不要機能の無効化	○	–	○	–	○	–
地上制御局	GCS-C2M-110	Bluetooth のセキュリティ対策	–	–	–	–	–	–
地上制御局	GCS-C2M-111	最新の Wi-Fi 認証方式を利用	–	–	–	–	–	–
地上制御局	GCS-C2M-112	ソフトウェア更新機能	○	○	○	○	○	–
地上制御局	GCS-C2M-113	電源停止や障害発生時の対応	–	○	–	–	–	–
地上制御局	GCS-C2O-101	不要な機能の無効化	○	○	–	–	–	–
地上制御局	GCS-C2O-102	データ保護（本体）	○	○	○	○	○	○

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
地上制御局	GCS-C2O-103	データ保護（外部ストレージ）	○	○	○	○	○	○
地上制御局	GCS-C2O-104	セキュリティ設定の変更及び安全な初期設定への復元機能	○	○	○	–	○	–
地上制御局	GCS-C2O-105	機器認証	○	–	○	○	○	○
地上制御局	GCS-C2O-106	ユーザ認証	○	–	○	○	○	○
地上制御局	GCS-C2O-107	不要な TCP/UDP ポートの無効化	○	○	○	–	–	○
地上制御局	GCS-C2O-108	USB デバイスの不要機能の無効化	○	–	○	–	○	–
地上制御局	GCS-C2O-109	ソフトウェア更新機能	○	○	○	○	○	–
地上制御局	GCS-C2O-110	ソフトウェアの真正性と完全性の検証	○	○	○	–	○	○
地上制御局	GCS-C2O-301	ログの記録	○	○	○	○	○	○
地上制御局	GCS-C3M-101	機器認証	○	–	○	○	○	○

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
地上制御局	GCS-C3M-102	ソフトウェア更新機能	○	–	○	○	○	–
地上制御局	GCS-C3M-201	脆弱性診断	○	–	–	○	○	○
地上制御局	GCS-C3O-101	DoS 対策	○	–	–	○	○	–
地上制御局	GCS-C3O-102	セキュアブート	–	–	–	–	–	–
地上制御局	GCS-C3O-103	ハードウェアハッキング対策	○	–	○	–	–	○
地上制御局	GCS-C3O-104	リバースエンジニアリング対策	–	–	–	–	○	○
ドローン運用クラウド	DPF-C2M-101	通信経路暗号化	○	○	○	○	○	○
ドローン運用クラウド	DPF-C2M-102	機器認証	○	○	○	○	○	○
ドローン運用クラウド	DPF-C2O-101	データ暗号化	○	○	○	○	○	○
ドローン運用クラウド	DPF-C2O-102	機器認証	○	–	○	○	○	○

構成要素	ID	要件	ETSI 303　645	NIST Recommended Criteria for Cybersecurity Labeling[37]	NIST IR 8259A	NISC 要件策定マニュアル[38]	NISC 対策基準策定ガイド[39]	EUROCAE ED-204A
ドローン運用クラウド	DPF-C2O-301	ログの記録	○	○	○	○	○	○
ドローン運用クラウド	DPF-C3M-101	機器認証	○	–	○	○	○	○
サービス運用クラウド	SPF-C2M-101	通信経路暗号化	○	○	○	○	○	○
サービス運用クラウド	SPF-C2M-102	機器認証	○	○	○	○	○	○
サービス運用クラウド	SPF-C2O-101	データ暗号化	○	○	○	○	○	○
サービス運用クラウド	SPF-C2O-102	機器認証	○	–	○	○	○	○
サービス運用クラウド	SPF-C2O-301	ログの記録	○	○	○	○	○	○
サービス運用クラウド	SPF-C3M-101	機器認証	○	–	○	○	○	○

6.2 組織におけるセキュリティ要件と国内外のガイドラインとの対応関係について

本書の組織におけるセキュリティ要件（表 5-19、表 5-20、表 5-21）と国内外における主要なガイドラインとの対応関係を表 6-2 に示す。

表 6-2 セキュリティ活動指針と関連ガイドラインの対応関係

ID	要件	ISO/IEC 27001, 27017	EUROCAE ED-202A	EUROCAE ED-204A	NIST Recommended Criteria for Cybersecurity Labeling[40]	NIST IR 8259	NISC 対策基準策定ガイド[41]	NISC サプライチェーンリスク手引書[42]
ORG-C2M-M01	情報セキュリティの管理方針の策定	○	–	○	–	–	○	–
ORG-C2M-M02	情報セキュリティの管理体制の構築	○	–	–	–	–	○	–
ORG-C2M-M03	製品やサービスのシステムモデル、ユースケースの定義	–	○	–	○	○	–	–
ORG-C2M-M04	脆弱性やセキュリティに関する連絡窓口の設置	–	–	○	○	○	○	–
ORG-C2M-M05	更新ソフトウェアの提供	–	–	–	○	○	–	–
ORG-C2M-M06	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	○	○	–	○	○	–	–
ORG-C2M-M07	製品のセキュリティサポートに関する利用者への周知	○	–	–	○	○	○	–
ORG-C2M-M08	ソフトウェア、ハードウェアコンポーネントの管理	–	–	–	○	–	○	–
ORG-C2O-M01	情報セキュリティや関連法令に関する教育および訓練	○	–	○	–	–	○	–
ORG-C2O-M02	個人情報や収集データの消去方法の利用者への周知	–	–	–	○	○	–	–
ORG-C2O-M03	情報セキュリティ管理方針や体制のレビュー	○	–	–	–	–	○	○

[40] NIST “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”

[41] 内閣サイバーセキュリティセンター（NISC）「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）」

[42] 内閣サイバーセキュリティセンター（NISC）「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」

ID	要件	ISO/IEC 27001, 27017	EUROCAE ED-202A	EUROCAE ED-204A	NIST Recommended Criteria for Cybersecurity Labeling[40]	NIST IR 8259	NISC 対策基準策定ガイド[41]	NISC サプライチェーンリスク手引書[42]
ORG-C2O-M04	個人情報やテレメトリデータの収集に関するポリシーの公開	○	–	–	–	–	○	–
ORG-C2O-M05	サプライチェーンリスクの管理	○	–	–	○	–	○	○
ORG-C2O-M06	製品に対する品質保証体制の確立と実行	○	–	–	○	–	○	○
ORG-C2O-M07	情報セキュリティのインシデント管理およびインシデントレスポンス対応	○	–	○	○	–	○	–
ORG-C3M-M01	開発・製造環境のセキュリティ対策	○	–	–	–	–	○	–
ORG-C3M-M02	情報セキュリティや関連法令に関する教育および訓練	–	–	–	–	–	–	–
ORG-C3M-M03	デザインレビューやコードレビュー	–	–	–	–	–	–	–
ORG-C3M-M04	開発委託先や部材調達先に対するセキュリティ管理の要求	○	–	–	–	–	○	○
ORG-C2M-S01	情報セキュリティの管理方針の策定	○	–	○	–	–	○	–
ORG-C2M-S02	情報セキュリティの管理体制の構築	○	–	–	–	–	○	–
ORG-C2M-S03	製品やサービスのシステムモデル、ユースケースの定義	–	○	–	○	○	–	–
ORG-C2M-S04	脆弱性やセキュリティに関する連絡窓口の設置	–	–	○	○	○	○	–
ORG-C2M-S05	更新ソフトウェアの提供	–	–	–	○	○	–	–
ORG-C2M-S06	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	○	○	–	○	○	–	–
ORG-C2M-S07	製品のセキュリティサポートに関する利用者への周知	○	–	–	○	○	○	–
ORG-C2M-S08	ソフトウェア、ハードウェアコンポーネントの管理	–	–	–	○	–	○	–

ID	要件	ISO/IEC 27001, 27017	EUROCAE ED-202A	EUROCAE ED-204A	NIST Recommended Criteria for Cybersecurity Labeling[40]	NIST IR 8259	NISC 対策基準策定ガイド[41]	NISC サプライチェーンリスク手引書[42]
ORG-C2O-S01	情報セキュリティや関連法令に関する教育および訓練	○	–	○	–	–	○	–
ORG-C2O-S02	情報セキュリティ管理方針や体制のレビュー	○	–	–	–	–	○	○
ORG-C2O-S03	サプライチェーンリスクの管理	○	–	–	○	–	○	○
ORG-C2O-S04	製品に対する品質保証体制の確立と実行	○	–	–	○	–	○	○
ORG-C2O-S05	情報セキュリティのインシデント管理およびインシデントレスポンス対応	○	–	○	○	–	○	–
ORG-C3M-S01	開発・製造環境のセキュリティ対策	○	–	–	–	–	○	–
ORG-C3M-S02	情報セキュリティや関連法令に関する教育および訓練	–	–	–	–	–	–	–
ORG-C3M-S03	デザインレビューやコードレビュー	–	–	–	–	–	–	–
ORG-C3M-S04	開発委託先や部材調達先に対するセキュリティ管理の要求	○	–	–	–	–	○	○
ORG-C2M-P01	情報セキュリティの管理方針の策定	○	–	○		–	○	–
ORG-C2M-P02	情報セキュリティの管理体制の構築	○	–	–		–	○	–
ORG-C2M-P03	製品やサービスのシステムモデル、ユースケースの定義	–	○	–	○	○	–	–
ORG-C2M-P04	個人情報やテレメトリデータの収集に関するポリシーの公開	○	–	–		–	○	–
ORG-C2M-P05	脆弱性やセキュリティに関する連絡窓口の設置	–	–	○	○	○	○	–
ORG-C2M-P06	更新ソフトウェアの提供	–	–	–	○	○	–	–
ORG-C2M-P07	個人情報や収集データの消去方法の利用者への周知	–	–	–	○	○	–	–
ORG-C2M-P08	収集した個人情報やテレメトリデータの消去	○	–	–		–	○	–

ID	要件	ISO/IEC 27001, 27017	EUROCAE ED-202A	EUROCAE ED-204A	NIST Recommended Criteria for Cybersecurity Labeling[40]	NIST IR 8259	NISC 対策基準策定ガイド[41]	NISC サプライチェーンリスク手引書[42]
ORG-C2M-P09	製品やサービスに対するリスクアセスメントの実施 ※関連法令に対するリスク対応を含む。	○	○	–	○	○	–	–
ORG-C2M-P10	製品のセキュリティサポートに関する利用者への周知	○	–	–		○	○	–
ORG-C2M-P11	運用上のオペレーション手順や管理手順の明確化、遵守	○	–	–	○	–	○	–
ORG-C2M-P12	守るべき資産のバックアップ	○	–	–		–	○	–
ORG-C2M-P13	ソフトウェア、ハードウェアコンポーネントの管理	–	–	–	○	–	○	–
ORG-C2O-P01	情報セキュリティや関連法令に関する教育および訓練	○	–	○		–	○	–
ORG-C2O-P02	情報セキュリティ管理方針や体制のレビュー	○	–	–	–	–	○	○
ORG-C2O-P03	サプライチェーンリスクの管理	○	–	–	○	–	○	○
ORG-C2O-P04	製品に対する品質保証体制の確立と実行	○	–	–	○	–	○	○
ORG-C2O-P05	情報セキュリティのインシデント管理およびインシデントレスポンス対応	○	–	○	○	–	○	–
ORG-C3M-P01	情報セキュリティの管理方針の策定	–	–	–	–	–	○	○
ORG-C3M-P02	情報セキュリティや関連法令に関する教育および訓練	–	–	–	–	–	–	–
ORG-C3M-P03	デザインレビューやコードレビュー	–	–	–	–	–	–	–
ORG-C3M-P04	運用環境のセキュリティ対策	○	–	–	–	–	○	–
ORG-C3M-P05	クレデンシャル（認証情報、暗号鍵、デジタル証明書）のライフサイクル管理	○	–	○	–	–	○	–

ID	要件	ISO/IEC 27001, 27017	EUROCAE ED-202A	EUROCAE ED-204A	NIST Recommended Criteria for Cybersecurity Labeling[40]	NIST IR 8259	NISC 対策基準策定ガイド[41]	NISC サプライチェーンリスク手引書[42]
ORG-C3M-P06	ログの取得、監視、分析	○	–	○	–	–	○	–

7 Appendix_B システムモデルにおけるリスクレベルの検討例

Appendix_B では、第４章に記載したリスク分析プロセスにおけるリスクレベルの検討例を示す。リスクの深刻度や重要度を算定するリスクレベルの算定基準は、多くの手法、基準が定義されているが、本書では脆弱性の報告において標準的に使用されている CVSS を用いた検討例と、IPA が策定した守るべき資産の重要度と被害発生可能性に基づく検討例の２種類を示す。

7.1 CVSS を活用したリスクレベルの検討例

CVSS は脆弱性を報告する際に標準的に使用されているリスクレベルの算定手法であり、脆弱性の深刻度・対応緊急度を定量的に判断することができる（表 7-1）。CVSS は本来、脆弱性の深刻度の算出を目的した指標となるが、本書では想定脅威の深刻度の算出に応用している。

表 7-1 CVSSv3 における深刻度のスコア表

深刻度	CVSS スコア
緊急（Critical）	9.0～10.0
重要（High）	7.0～8.9
警告（Medium）	4.0～6.9
注意（Low）	0.1～3.9
なし	0

CVSS の評価値は「基本評価値」、「現状評価値」、「環境評価値」の３つの評価値から構成される。基本評価値は、脆弱性そのものの特性を示す値であり、主にセキュリティ課題を検出した検証技術者が評価を行う。現状評価値は、攻撃コードや対策情報の公開有無などの補足情報を加えて、補正した値となり、主に開発者が評価を行う。環境評価値は対象機器の実際の利用環境や、セキュリティ対策状況を踏まえて、再計算する値であり、主に運用関係者が評価を行う。このように CVSSv3 は脆弱性そのものの深刻度に対して、異なる視点から補正や再計算を行い、より現実に即した値を算出することが可能であり、課題対策の優先度を決定する上で、有用な指標となる。CVSSv3 の具体的な計算式については、IPA の公開情報[43]

[43] IPA 共通脆弱性評価システム CVSS 概説
https://www.ipa.go.jp/security/vuln/CVSS.html

等を参照されたい。

以下に前節までに分析を行った結果に対するリスクレベル（＝リスク値）の算出例を示す（表 7-2、表 7-3、表 7-4、表 7-5、表 7-6、表 7-7、表 7-8）。評価値についてはリスクが想定であり、実在する脆弱性の情報が該当しないものもあるため、基本評価値のみを記載している。また、ドローン本体と地上制御間のデータ通信については、2.4GHz 帯等による無線通信を行う場合と、LTE 等のモバイル通信を行う場合が想定されるため、それぞれのケースにおける算出例を示している。

補足事項）リスクレベル検討の前提について

・ドローンと地上制御局間の通信において、2.4GHz 等の無線通信が使用される場合、S.BUS などの独自プロトコルが利用されているケースが多く、セキュリティ上も傍受や解析が困難となる（攻撃の複雑さ「高」）。ただし、DSMx のように SDR（ソフトウェア無線）の普及に伴い、解析や攻撃に成功した研究事例も報告されている。

・リモート ID の通信には、Wi-Fi や Bluetooth が想定されているが、使用される暗号化アルゴリズムやプロトコルによっては、既知の脆弱性を突いた攻撃が可能であり、セキュリティ対策が実施されていない状態ではよりリスクが高いと判断される。

表 7-2 ドローン本体のリスクレベルの検討例（データ通信に 2.4GHZ 等の無線を利用） ※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
A	無線通信用インタフェース（リモートID通信）	不正アクセス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	−	隣接	低	不要	不要	変更なし	高	高	高	8.8	重要
		情報の暴露	ドローン本体のメモリ領域から、リモートIDの鍵情報が窃取される。	−	隣接	低	不要	不要	変更なし	高	なし	なし	6.5	警告
		データ改ざん	ドローン本体のメモリ領域から、リモートIDの値を改ざんされる。	−	隣接	低	不要	不要	変更なし	高	高	なし	8.1	重要
		サービス不能	既知の脆弱性を突いたDoS攻撃により、リモートID通知に関する機能に影響が生じる。	−	隣接	低	不要	不要	変更なし	なし	なし	高	6.5	警告
		マルウェア感染	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	隣接	低	不要	不要	変更なし	高	高	高	8.8	重要
		踏み台	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	−	隣接	高	不要	不要	変更なし	なし	高	なし	5.3	警告
B	無線通信用インタフェース（データ通信） ※2.4GH z 等の無線通信を利用	不正アクセス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	−	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		情報の暴露	ドローン本体のメモリ領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、プログラムコード上の機密情報漏洩など	−	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
B	無線通信用インタフェース（データ通信） ※2.4GHｚ等の無線通信を利用	データ改ざん	ドローン本体のメモリ領域から、フライトログや記録映像、オンボードコンピュータのプログラムコードなどを改ざんされる。※プログラムコードの改ざんによる著作権の侵害など	－	隣接	高	不要	不要	変更なし	高	高	なし	6.8	警告
		なりすまし	攻撃者が地上制御局になりすましオンボードコンピュータに対する不正な指示が行われる。	－	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		サービス不能	既知の脆弱性を突いたDoS攻撃により、ドローン本体の機能に影響が生じる。	－	隣接	高	不要	不要	変更なし	なし	なし	高	5.3	警告
		権限の昇格	オンボードコンピュータのOSに対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースのOSを使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	－	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		マルウェア感染	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		踏み台	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	－	隣接	高	不要	不要	変更なし	なし	高	なし	5.3	警告

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
C	SD/USBインタフェース（フライトコントローラの記録装置）	情報の暴露	落下したドローン本体のSD/USBメディアが回収され、フライトログ等の漏洩につながる可能性がある。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	−	物理	低	不要	要	変更なし	高	なし	なし	4.3	警告
		マルウェア感染	マルウェアが組み込まれたSD/USBメディアとの接続により、ドローン本体のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	物理	低	不要	要	変更なし	高	高	高	6.6	警告
D	SD/USBインタフェース（オンボードコンピュータの記録装置）	情報の暴露	マルウェアが組み込まれたSD/USBメディアとの接続により、オンボードコンピュータのマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	−	物理	低	不要	要	変更なし	高	なし	なし	4.3	警告
		マルウェア感染	落下したドローン本体のSD/USBメディアが回収され、記録映像の漏洩につながる可能性がある※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	影響有り	物理	低	不要	要	変更なし	高	高	高	6.6	警告

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
E	SD/USBインタフェース（記録装置）	情報の暴露	落下したドローン本体のSD/USBメディアが回収され、記録映像の漏洩につながる可能性がある※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	–	物理	低	不要	要	変更なし	高	なし	なし	4.3	警告
		マルウェア感染	マルウェアが組み込まれたSD/USBメディアとの接続により、ドローン本体のマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	物理	低	不要	要	変更なし	高	高	高	6.6	警告
F	基盤・回路上のポート（JTAG、UARTなど）	不正改造（HW/SW	基盤上のデバッグポート（JTAG端子、UART端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	影響有り	物理	高	不要	不要	変更なし	高	高	高	6.4	警告

表 7-3 ドローン本体のリスクレベルの検討例（データ通信に LTE 等のモバイル通信を利用） ※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
B	無線通信用インタフェース（データ通信） ※LTE等のモバイル通信を利用	不正アクセス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	－	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		情報の暴露	ドローン本体のメモリ領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、プログラムコード上の機密情報漏洩など	－	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データ改ざん	ドローン本体のメモリ領域から、フライトログや記録映像、オンボードコンピュータのプログラムコードなどを改ざんされる。※プログラムコードの改ざんによる著作権の侵害など	－	ネットワーク	高	不要	不要	変更なし	高	高	なし	7.4	重要
		なりすまし	攻撃者が地上制御局になりすましオンボードコンピュータに対する不正な指示が行われる。	－	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		サービス不能	既知の脆弱性を突いたDoS攻撃により、ドローン本体の機能に影響が生じる。	－	ネットワーク	高	不要	不要	変更なし	なし	なし	高	5.9	警告
		権限の昇格	オンボードコンピュータのOSに対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースのOSを使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	－	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
B	無線通信用インタフェース（データ通信） ※LTE等のモバイル通信を利用	マルウェア感染	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		踏み台	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	－	ネットワーク	高	不要	不要	変更なし	なし	高	なし	5.9	警告

表 7-4 地上制御局のリスクレベルの検討例（データ通信に 2.4GHZ 等の無線を利用） ※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
G	無線通信用インタフェース（データ通信） ※2.4GH z 等の無線通信を利用	不正アクセス	地上制御局のメモリやファイル領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	–	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		情報の暴露	地上制御局のメモリやファイル領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、機密情報やプログラムコードの漏洩による著作権侵害など。	–	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告
		データ改ざん	地上制御局のメモリやファイル領域から、フライトログや記録映像、プログラムコードなどを改ざんされる。※フライトログや設定情報、ミッション情報の改ざんによる飛行の妨害や、プログラムコードの漏洩による著作権侵害など。	影響有り	隣接	高	不要	不要	変更なし	高	高	なし	6.8	警告
		なりすまし	攻撃者がドローン本体になりすまし、不正な情報が伝達される。 ※間接的には誤った情報（テレメトリなど）による、飛行操作や判断ミスなど。	– 間接的には操作に影響	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		サービス不能	既知の脆弱性を突いたDoS攻撃により、ドローン本体とのデータ通信が阻害される。	–	隣接	高	不要	不要	変更なし	なし	なし	高	5.3	警告
		権限の昇格	地上制御局のOSに対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースのOSを使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	影響有り	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
G	無線通信用インタフェース（データ通信） ※2.4GHｚ等の無線通信を利用	マルウェア感染	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※地上制御局の異常動作や、不正な情報送信による漏洩など。	影響有り	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
		踏み台	ボットネットの感染などによって、他の構成要素に対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	–	隣接	高	不要	不要	変更なし	なし	高	なし	5.3	警告
H	SD/USBインタフェース（記録装置）	情報の暴露	SD/USBの盗難、紛失によって、保存された情報の漏洩につながる。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	–	物理	低	不要	要	変更なし	高	なし	なし	4.3	警告
		マルウェア感染	マルウェアが組み込まれたSD/USBメディアとの接続により、地上制御局のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	影響有り	物理	低	不要	要	変更なし	高	高	高	6.6	警告
I	基盤・回路上のポート（JTAG、UARTなど）	不正改造（HW/SW	基盤上のデバッグポート（JTAG端子、UART端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	影響有り	物理	高	不要	不要	変更なし	高	高	高	6.4	警告

表 7-5 地上制御局のリスクレベルの検討例（データ通信に LTE 等のモバイル通信を利用） ※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
G	無線通信用インタフェース（データ通信） ※LTE等のモバイル通信を利用	不正アクセス	地上制御局のメモリやファイル領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	–	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		情報の暴露	地上制御局のメモリやファイル領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、機密情報やプログラムコードの漏洩による著作権侵害など。	–	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データ改ざん	地上制御局のメモリやファイル領域から、フライトログや記録映像、プログラムコードなどを改ざんされる。※フライトログや設定情報、ミッション情報の改ざんによる飛行の妨害や、プログラムコードの漏洩による著作権侵害など。	影響有り	ネットワーク	高	不要	不要	変更なし	高	高	なし	7.4	重要
		なりすまし	攻撃者がドローン本体になりすまし、不正な情報が伝達される。 ※間接的には誤った情報（テレメトリなど）による、飛行操作や判断ミスなど。	– 間接的には操作に影響	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		サービス不能	既知の脆弱性を突いたDoS攻撃により、ドローン本体とのデータ通信が阻害される。	–	ネットワーク	高	不要	不要	変更なし	なし	なし	高	5.9	警告
		権限の昇格	地上制御局のOSに対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースのOSを使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	影響有り	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
G	無線通信用インタフェース（データ通信） ※LTE等のモバイル通信を利用	マルウェア感染	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※地上制御局の異常動作や、不正な情報送信による漏洩など。	影響有り	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
		踏み台	ボットネットの感染などによって、他の構成要素に対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	－	ネットワーク	高	不要	不要	変更なし	なし	高	なし	5.9	警告

表 7-6 ドローン運用クラウドのリスクレベルの検討例　※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
J	インターネット通信用インタフェース	不正アクセス	ドローン運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある。	−	ネットワーク	高	不要	不要	変更なし	高	高	低	7.7	重要
		情報の暴露	サーバのファイル領域から、設定情報やアップロード用のプログラムなどの秘匿すべき情報が窃取される	−	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データの改ざん	サーバのファイル領域から、設定情報やアップロード用のプログラムなどを改ざんされる。※アップロード用プログラムコードの改ざんによる著作権侵害に加えて、不正なプログラムが無人航空機にインストールされるなど。	影響有り	ネットワーク	高	不要	不要	変更なし	高	高	なし	7.4	重要
		サービス不能	DoS攻撃により、ドローン運用クラウドの運用が阻害される。※クラウドの機能障害による、アップデートの実行不可など。	−	ネットワーク	低	不要	不要	変更なし	なし	なし	高	7.5	重要
		権限の昇格	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	−	ネットワーク	高	不要	不要	変更なし	高	高	低	7.7	重要
		マルウェア感染	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	−	ネットワーク	低	不要	不要	変更なし	高	高	高	9.8	緊急
		踏み台	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	−	ネットワーク	低	不要	不要	変更なし	なし	高	なし	7.5	重要

表 7-7 サービス運用クラウドのリスクレベルの検討例　※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
K	インターネット通信用インタフェース	不正アクセス	サービス運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある。	–	ネットワーク	高	不要	不要	変更なし	高	高	低	7.7	重要
		情報の暴露	サーバのファイル領域から、秘匿すべき記録映像や、データが窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、業務機密であるテレメトリデータの漏洩による信用失墜など。	–	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データの改ざん	サーバのファイル領域から、記録映像や、データが削除あるいは改ざんされる。※記録映像や、業務機密であるテレメトリデータの改ざん、削除による信用失墜など。	–	ネットワーク	高	不要	不要	変更なし	高	高	なし	7.4	重要
		サービス不能	DoS攻撃により、サービスの提供が阻害される。※クラウドの機能障害によりサービス提供が阻害され、経済的損失につながるなど。	–	ネットワーク	低	不要	不要	変更なし	なし	なし	高	7.5	重要
		権限の昇格	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	–	ネットワーク	高	不要	不要	変更なし	高	高	低	7.7	重要
		マルウェア感染	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	–	ネットワーク	低	不要	不要	変更なし	高	高	高	9.8	緊急
		踏み台	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	–	ネットワーク	低	不要	不要	変更なし	なし	高	なし	7.5	重要

表 7-8 通信経路におけるリスクレベルの検討例　※CVSSv3 によるリスクレベル

攻撃ポイント		脅威分類	想定される脅威例	耐空性への影響	基本値									
No.	対象				攻撃元区分	攻撃条件の複雑さ	攻撃に必要な特権レベル	利用者の関与	影響の想定範囲（スコープ）	機密性への影響	完全性への影響	可用性への影響	リスク値	リスク値ランク
1	ドローン本体とスマートフォン（タブレット）間の通信	データ改ざん	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	－	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告
2	ドローン本体と地上制御局間の通信経路（データ通信） ※2.4GHｚ等の無線通信を利用	情報の暴露	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	－	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告
		データ改ざん	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	－	隣接	高	不要	不要	変更なし	高	高	高	7.5	重要
2	ドローン本体と地上制御局間の通信経路（データ通信） ※LTE等のモバイル通信を利用	情報の暴露	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	－	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データ改ざん	無線信号の傍受やインジェクション攻撃などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	－	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
3	クラウドシステムとインターネット間の通信経路（データ通信）	情報の暴露	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	－	ネットワーク	高	不要	不要	変更なし	高	なし	なし	5.9	警告
		データ改ざん	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	影響あり	ネットワーク	高	不要	不要	変更なし	高	高	高	8.1	重要
4	ドローン本体とリモートIDキャプチャ機器間の通信	情報の暴露	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	－	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告
		データ改ざん	無線信号の傍受やインジェクション攻撃などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	－	隣接	高	不要	不要	変更なし	高	なし	なし	5.3	警告

7.2 資産の重要度と被害発生の可能性によるリスクレベルの検討例

もう一つの例として、IPA「中小企業の情報セキュリティ対策ガイドライン[44]」で定義されている守るべき資産（情報資産）の重要度と、被害発生の可能性に基づくリスクレベルの検討例をサンプルドキュメントとして掲載する。IPA が提示する手法は、図 7-1 に示す通り、守るべき資産の価値や事故の影響の大きさを重要度として設定し、これに被害発生の可能性を掛け算することでリスクレベル（リスク値）を算定する基準となる。本書では重要度を、本書 4.2 で整理した守るべき資産の重要度の値を参照し、リスクレベルを選定した。

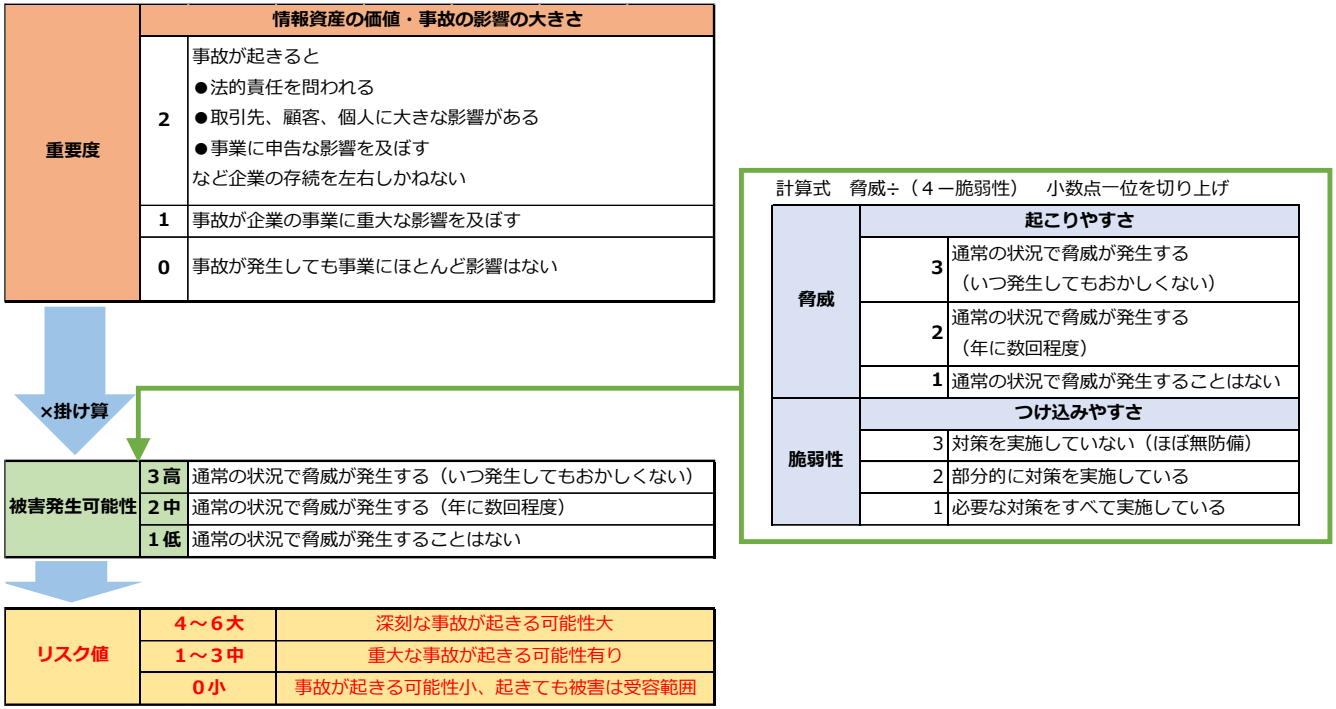


図 7-1 資産の重要度と被害発生の可能性によるリスクレベルの算定基準

（出典：IPA 「中小企業の情報セキュリティ対策ガイドライン」）

本書の第４章で実施した脅威分析結果に対するリスクレベルの検討例を、構成要素別に表 7-11 から表 7-18 に示す。表 7-11 から表 7-13 までは、セキュリティ対策が未実施の場合のリスク値であり、表 7-14 から表 7-18 までが、本書のセキュリティ対策を実施した場合のリスク値となる。

[44] IPA「中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

表 7-9 ドローン本体のリスクレベルの検討例（セキュリティ対策実施前） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a x b	リスク値
No.	対象					脅威	脆弱性（未対策）			
A	無線通信用インタフェース（リモート ID 通信）	不正アクセス	リモート ID 通知に関する機能・サービス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	2	2	3	2	4	リスク大
		情報の暴露	鍵情報（リモート ID）	ドローン本体のメモリ領域から、リモート ID の鍵情報が窃取される。	2	2	3	2	4	リスク大
		データ改ざん	リモート ID	ドローン本体のメモリ領域から、リモート ID の値を改ざんされる。	1	2	3	3	2	リスク中
		サービス不能	リモート ID の通知に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、リモート ID 通知に関する機能に影響が生じる。	2	3	3	3	6	リスク大
		マルウェア感染	リモート ID の通知に関する機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大
B	無線通信用インタフェース	不正アクセス	・フライトログ ・記録映像、	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	2	2	3	2	4	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a x b	
	（データ通信）		・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書							
		情報の暴露	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、プログラムコード上の機密情報漏洩など	2	2	3	2	4	リスク大
		データ改ざん	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵）	ドローン本体のメモリ領域から、フライトログや記録映像、オンボードコンピュータのプログラムコードなどを改ざんされる。※プログラムコードの改ざんによる著作権の侵害など	2	2	3	2	4	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a x b	リスク値
No.	対象					脅威	脆弱性（未対策）			
			・検証鍵（公開鍵、ハッシュ） ・デジタル証明書							
		なりすまし	オンボードコンピュータのプログラムコード	攻撃者が地上制御局になりすましオンボードコンピュータに対する不正な指示が行われる。	2	2	3	2	4	リスク大
		サービス不能	機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体の機能に影響が生じる。	2	3	3	3	6	リスク大
		権限の昇格	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	オンボードコンピュータの OS に対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースのOSを使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	2	1	3	1	2	リスク中
		マルウェア感染	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a x b	リスク値
No.	対象					脅威	脆弱性（未対策）			
		踏み台	–	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大
C	SD/USB インタフェース（フライトコントローラの記録装置）	情報の暴露	フライトログ A	落下したドローン本体の SD/USB メディアが回収され、フライトログ等の漏洩につながる可能性がある。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	1	2	3	2	2	リスク中
		情報の暴露	フライトログ B	※同上	2	2	3	2	4	リスク大
		マルウェア感染	・フライトログ ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、ドローン本体のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大
D	SD/USB インタフェース（オンボードコンピュータの記録装置）	情報の暴露	オンボードコンピュータのプログラムコード	落下したドローン本体の SD/USB メディアが回収され、オンボードコンピュータのプログラムコードの漏洩につながる可能性がある。	2	2	3	2	4	リスク大
		マルウェア感染	・オンボードコンピュータのプログラムコード	マルウェアが組み込まれた SD/USB メディアとの接続により、オンボードコンピュータのマル	2	3	3	3	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a x b	
			・機能・サービス	ウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。						
E	SD/USB インタフェース（カメラの記録装置）	情報の暴露	記録映像 A	落下したドローン本体の SD/USB メディアが回収され、記録映像の漏洩につながる可能性がある※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	0	2	3	2	0	リスク小
		情報の暴露	記録映像 B～D	※同上	2	2	3	2	4	リスク大
		マルウェア感染	・記録映像 ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、ドローン本体のマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	2	3	3	3	6	リスク大
F	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	2	1	3	1	2	リスク中

表 7-10 地上制御局のリスクレベルの検討例（セキュリティ対策実施前） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の需要度（最大値）：a			被害発生可能性:b	a × b	リスク値
No.	対象					脅威	脆弱性（未対策）			
G	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・データ通信に関する機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	2	2	3	2	4	リスク大
		情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵）	地上制御局のメモリやファイル領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、機密情報やプログラムコードの漏洩による著作権侵害など。	2	2	3	2	4	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の需要度（最大値）：a			被害発生可能性:b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
			・検証鍵（公開鍵、ハッシュ） ・デジタル証明書							
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域から、フライトログや記録映像、プログラムコードなどを改ざんされる。※フライトログや設定情報、ミッション情報の改ざんによる飛行の妨害や、プログラムコードの漏洩による著作権侵害など。	2	2	3	2	4	リスク大
		なりすまし	データ通信に関する機能・サービス	攻撃者がドローン本体になりすまし、不正な情報が伝達される。 ※間接的には誤った情報（テレメトリなど）による、飛行操作や判断ミスなど。	2	2	3	2	4	リスク大
		サービス不能	データ通信に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体とのデータ通信が阻害される。	2	3	3	2	6	リスク大
		権限の昇格	・フライトログ ・記録映像	地上制御局の OS に対するアクセス権限の不正変更により、攻撃者に管	2	1	2	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の需要度（最大値）：a			被害発生可能性:b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
			・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	理者権限を付与する。特にオープンソースの OS を使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。						
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※地上制御局の異常動作や、不正な情報送信による漏洩など。	2	3	3	2	6	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素に対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	2	3	3	2	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の需要度（最大値）：a			被害発生可能性:b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
H	SD/USB インタフェース（記録装置）	情報の暴露	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	SD/USB の盗難、紛失によって、保存された情報の漏洩につながる。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	2	2	3	2	4	リスク大
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、地上制御局のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	2	3	3	2	6	リスク大
I	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	2	1	3	1	2	リスク中

表 7-11 ドローン運用クラウドのリスクレベルの検討例（セキュリティ対策実施前） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a × b	リスク値
No.	対象					脅威	脆弱性（未対策）			
J	インターネット通信用インタフェース	不正アクセス	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある	2	3	3	2	6	リスク大
		情報の暴露	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバのファイル領域から、アップロード用のプログラムなどの秘匿すべき情報が窃取される。	2	3	3	2	6	リスク大
		データの改ざん	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	サーバのファイル領域からアップロード用のプログラムなどを改ざんされる。※アップロード用プログラムコードの改ざんによる著作権侵害に加えて、不正なプログラムが無人航空機にインストールされるなど。	2	3	3	2	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
		サービス不能	機能・サービス	DoS 攻撃により、ドローン運用クラウドの運用が阻害される。※クラウドの機能障害による、アップデートの実行不可など。	2	3	3	2	6	リスク大
		権限の昇格	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	2	1	3	1	2	リスク中
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	2	3	3	2	6	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに	2	3	3	2	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
				対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。						

表 7-12 サービス運用クラウドのリスクレベルの検討例（セキュリティ対策実施前） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a × b	リスク値
No.	対象					脅威	脆弱性（未対策）			
K	インターネット通信用インタフェース	不正アクセス	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サービス運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある。	2	3	3	2	6	リスク大
		情報の暴露	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果	サーバのファイル領域から、秘匿すべき記録映像や、データが窃取される。 ※記録映像の漏洩によるプライバシや肖像権の侵害、業務機密であるテレメトリデータの漏洩による信用失墜など。	2	3	3	2	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
			・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス、認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）、デジタル証明書							
		データの改ざん	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など）	サーバのファイル領域から、記録映像や、データが削除あるいは改ざんされる。※記録映像や、業務機密であるテレメトリデータの改ざん、削除による信用失墜など。	2	3	3	2	6	リスク大
		サービス不能	機能・サービス	DoS 攻撃により、サービスの提供が阻害される。※クラウドの機能障害によりサービス提供が阻害され、経済的損失につながるなど。	2	3	3	2	6	リスク大
		権限の昇格	・記録映像 ・テレメトリデータ ・センサ取得情報	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回に	2	1	3	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
			・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	よる他の脅威への派生など。						
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	2	3	3	2	6	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※	2	3	3	2	6	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象					脅威	脆弱性（未対策）		a × b	
				意図しない第三者への攻撃行為、不正な情報送信による漏洩など。						

表 7-13 通信経路におけるリスクレベルの検討例（セキュリティ対策実施前） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	資産の重要度（最大値）：a			被害発生可能性：b	a × b	リスク値
No.	対象					脅威	脆弱性（未対策）			
1	ドローン本体とスマートフォン（タブレット）間の通信	データ改ざん	・リモート ID	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	1	2	3	2	2	リスク中
2	ドローン本体と地上制御局間の通信経路（データ通信）	情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	2	2	3	2	4	リスク大
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵）	無線信号の傍受やインジェクション攻撃などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	2	2	3	2	4	リスク大

			・検証鍵（公開鍵、ハッシュ） ・デジタル証明書							
3	クラウドシステムとインターネット間の通信経路（データ通信）	情報の暴露	・アップデート用のプログラムコード ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	2	3	3	3	6	リスク大
		データ改ざん	・アップデート用のプログラムコード ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	2	3	3	3	6	リスク大

4	ドローン本体とリモート ID キャプチャ機器間の通信	情報の暴露	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	2	2	3	2	4	リスク大
		データ改ざん	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	2	2	3	2	4	リスク大

表 7-14 ドローン本体のリスクレベルの検討例（セキュリティ対策実施後） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b	a x b	リスク値
No.	対象						脅威	脆弱性			
A	無線通信用インタフェース（リモート ID 通信）	不正アクセス	リモート ID 通知に関する機能・サービス	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用	2	2	1	1	2	リスク中
		情報の暴露	鍵情報（リモート ID）	ドローン本体のメモリ領域から、リモート ID の鍵情報が窃取される。	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用	2	2	1	1	2	リスク中
		データ改ざん	リモート ID	ドローン本体のメモリ領域から、リモート ID の値を改ざんされる。	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用 UAV-R07-B：データ保護（本体）	1	2	1	1	1	リスク中
		サービス不能	リモート ID の通知に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、リモート ID 通知に関する機能に影響が生じる。	UAV-R08：DoS 対策 UAV-R09：ログ記録	2	3	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象						脅威	脆弱性		a x b	
		マルウェア感染	リモートIDの通知に関する機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	UAV-R10：脆弱性診断	2	3	2	2	4	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	UAV-R01：リモートＩＤ発信時の暗号化対応 UAV-R02：Bluetooth のセキュリティ対策 UAV-R03：最新の Wi-Fi 認証方式を利用	2	3	1	1	2	リスク中
B	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	UAV-R11：アクセス制御 UAV-R12：機器認証 UAV-R13：セキュリティ設定の変更及び安全な初期設定への復元機能 UAV-R14：不要な TCP/UDP ポートの無効化 UAV-R15：不要な機能の無効化 UAV-R03：最新の Wi-Fi 認証方式を利用 UAV-R02：Bluetooth の	2	2	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b	ａｘｂ	リスク値
No.	対象						脅威	脆弱性			
					セキュリティ対策						
		情報の暴露	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、プログラムコード上の機密情報漏洩など	UAV-R07-B：データ保護（本体） UAV-R16-B：データ消去機能（本体）	2	2	1	1	2	リスク中
		データ改ざん	・フライトログ ・記録映像、 ・オンボードコンピュータのプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン本体のメモリ領域から、フライトログや記録映像、オンボードコンピュータのプログラムコードなどを改ざんされる。※プログラムコードの改ざんによる著作権の侵害など	UAV-R07-B：データ保護（本体） UAV-R17：セキュアブート	2	2	1	1	2	リスク中
		なりすまし	オンボードコンピュータのプログラムコード	攻撃者が地上制御局になりすましオンボードコンピュータに対する不正な指示が行われる。	UAV-R13：機器認証 UAV-R14：セキュリティ設定の変更及び安全な初期設定への復元機能	2	2	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象						脅威	脆弱性		a x b	
		サービス不能	機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体の機能に影響が生じる。	UAV-R09：DoS 対策 UAV-R10：ログ記録	2	3	1	1	2	リスク中
		権限の昇格	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	オンボードコンピュータの OS に対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースの OS を使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	UAV-R10：ログ記録 UAV-R11：脆弱性診断	2	1	1	1	2	リスク中
		マルウェア感染	・フライトログ ・記録映像 ・オンボードコンピュータのプログラムコード ・機能・サービス	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素や無人航空機への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	UAV-R15：不要な機能の無効化 UAV-R17：セキュアブート	2	3	2	2	4	リスク大
		踏み台	－	ボットネットの感染などによって、他の構成要素やドローンに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	UAV-R10：ログ記録 UAV-R11：アクセス制御 UAV-R12：機器認証 UAV-R13：セキュリティ設定の変更及び安全な初期設定	2	3	1	1	2	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b	a x b	リスク値
No.	対象						脅威	脆弱性			
					への復元機能						
C	SD/USB インタフェース（フライトコントローラの記録装置）	情報の暴露	フライトログ A	落下したドローン本体の SD/USB メディアが回収され、フライトログ等の漏洩につながる可能性がある。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）	1	2	1	1	1	リスク中
		情報の暴露	フライトログ B	※同上	※同上	2	2	1	1	2	リスク中
		マルウェア感染	・フライトログ ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、ドローン本体のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	UAV-R18：USB デバイスの不要機能の無効化	2	3	2	2	4	リスク大
D	SD/USB インタフェース（オンボードコンピュータの記録装置）	情報の暴露	オンボードコンピュータのプログラムコード	落下したドローン本体の SD/USB メディアが回収され、オンボードコンピュータのプログラムコードの漏洩につながる可能性がある。	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）	2	2	1	1	2	リスク中
		マルウェア感染	・オンボードコンピュータのプログラムコード ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、オンボードコンピュータのマルウェア感染につながる。	UAV-R18：USB デバイスの不要機能の無効化	2	3	2	2	4	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象						脅威	脆弱性		a x b	
				またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。							
E	SD/USB インタフェース（カメラの記録装置）	情報の暴露	記録映像 A	落下したドローン本体の SD/USB メディアが回収され、記録映像の漏洩につながる可能性がある※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	UAV-R07-S：データ保護（外部ストレージ） UAV-R16-S：データ消去機能（外部ストレージ）	0	2	1	1	0	リスク小
		情報の暴露	記録映像 B～D	※同上	※同上	2	2	1	1	2	リスク中
		マルウェア感染	・記録映像 ・機能・サービス	マルウェアが組み込まれた SD/USB メディアとの接続により、ドローン本体のマルウェア感染につながる。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。	UAV-R18：USB デバイスの不要機能の無効化	2	3	2	2	4	リスク大
F	基盤・回路上のポート（JTAG、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏	UAV-R16-B：データ消去機能（本体） UAV-R19：ハードウェアハッキング対策 UAV-R20：リバースエンジニ	2	1	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a x b	
				洩など。	アリング対策						

表 7-15 地上制御局のリスクレベルの検討例（セキュリティ対策実施後） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の需要度（最大値）：a			被害発生可能性:b	a × b	リスク値
No.	対象						脅威	脆弱性			
G	無線通信用インタフェース（データ通信）	不正アクセス	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・データ通信に関する機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域にアクセスされ、他の複数の脅威の要因となる恐れがある。	GCS-R01：アクセス制御 GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定の変更及び安全な初期設定への復元機能 GCS-R05：不要なTCP/UDP ポートの無効化 GCS-R06：不要な機能の無効化 GCS-R07：最新の Wi-Fi 認証方式を利用 GCS-R08：Bluetooth のセキュリティ対策	2	2	1	1	2	リスク中
		情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	地上制御局のメモリやファイル領域から、フライトログや記録映像などの秘匿すべき情報が窃取される。※記録映像の漏洩によるプライバシや肖像権の侵害、機密情報やプログラムコードの漏洩による著作権侵害など。	GCS-R12-B：データ保護（本体） GCS-R13-B：データ消去機能（本体	2	2	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の需要度（最大値）：a			被害発生可能性:b	a × b	リスク値
No.	対象						脅威	脆弱性			
			・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書								
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局のメモリやファイル領域から、フライトログや記録映像、プログラムコードなどを改ざんされる。※フライトログや設定情報、ミッション情報の改ざんによる飛行の妨害や、プログラムコードの漏洩による著作権侵害など。	GCS-R12-B：データ保護（本体） GCS-R14：セキュアブート	2	2	1	1	2	リスク中
		なりすまし	データ通信に関する機能・サービス	攻撃者がドローン本体になりすまし、不正な情報が伝達される。 ※間接的には誤った情報（テレメトリ	GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定	2	2	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の需要度（最大値）：a			被害発生可能性:b	a × b	リスク値
No.	対象						脅威	脆弱性			
				など）による、飛行操作や判断ミスなど。	の変更及び安全な初期設定への復元機能						
		サービス不能	データ通信に関する機能・サービス	既知の脆弱性を突いた DoS 攻撃により、ドローン本体とのデータ通信が阻害される。	GCS-R15：DoS 対策 GCS-R16：ログ記録	2	3	1	1	2	リスク中
		権限の昇格	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	地上制御局の OS に対するアクセス権限の不正変更により、攻撃者に管理者権限を付与する。特にオープンソースの OS を使用している場合に、既知の脆弱性を突いた攻撃が行われる可能性がある。※バックドアや認証の迂回による他の脅威への派生など。	GCS-R16：ログ記録 GCS-R17：脆弱性診断	2	1	1	1	2	リスク中
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモ	マルウェアの送信による感染の恐れがある。またドローン本体を経由し、他の構成要素への二次感染の可能性がある。※地上制御局の異常動作	GCS-R06：不要な機能の無効化 GCS-R14：セキュアブート	2	3	2	2	4	リスク大

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の需要度（最大値）：a			被害発生可能性:b	a × b	リスク値
No.	対象						脅威	脆弱性			
			ード等） ・ミッション情報 ・センサ取得情報 ・地上制御局のプログラムコード ・機能・サービス	や、不正な情報送信による漏洩など。							
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素に対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	GCS-R01：アクセス制御 GCS-R02：機器認証 GCS-R03：ユーザ認証 GCS-R04：セキュリティ設定の変更及び安全な初期設定への復元機能 GCS-R16：ログ記録	2	3	1	1	2	リスク中
H	SD/USB インタフェース（記録装置）	情報の暴露	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報	SD/USB の盗難、紛失によって、保存された情報の漏洩につながる。※記録映像の流出によるプライバシや肖像権の侵害、フライトログ上の機密情報の漏洩など。	GCS-R12-S：データ保護（外部ストレージ） GCS-R13-S：データ消去機能（外部ストレージ）	2	2	1	1	2	リスク中
		マルウェア感染	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモ	マルウェアが組み込まれた SD/USB メディアとの接続により、地上制御局のマルウェア感染につながるまたドローン本体を経由し、他の構成要素への	GCS-R18：USB デバイスの不要機能の無効化	2	3	2	2	4	リスク大

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の需要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性:b	a × b	
			ード等） ・ミッション情報 ・センサ取得情報 ・機能・サービス	二次感染の可能性がある。※ドローン本体の異常動作や、不正な情報送信による漏洩など。							
I	基盤・回路上のポート（ JTAG 、UART など）	不正改造（HW/SW）	・プログラムコード ・機器本体（ハードウェア）	基盤上のデバッグポート（JTAG 端子、UART 端子）を使用し、ソフトウェアの抽出や、解析、不正改造につながる。※不正なソフトウェア改造による著作権の侵害、機密情報の漏洩など。	GCS-R13-B：データ消去機能（本体） GCS-R19：ハードウェアハッキング対策 GCS-R20：リバースエンジニアリング対策	2	1	1	1	2	リスク中

表 7-16 ドローン運用クラウドのリスクレベルの検討例（セキュリティ対策実施後） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
J	インターネット通信用インタフェース	不正アクセス	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	ドローン運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある	DPF-R01：アクセス制御 DPF-R02：機器認証 DPF-R03：ユーザ認証 DPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 DPF-R05：不要なネットワーク接続、論理インタフェースの無効化	2	3	1	1	2	リスク中
		情報の暴露	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）	サーバのファイル領域から、アップロード用のプログラムなどの秘匿すべき情報が窃取される。	DPF-R08：データ暗号化	2	3	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b	a × b	リスク値
No.	対象						脅威	脆弱性			
			・デジタル証明書								
		データの改ざん	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	サーバのファイル領域からアップロード用のプログラムなどを改ざんされる。※アップロード用プログラムコードの改ざんによる著作権侵害に加えて、不正なプログラムが無人航空機にインストールされるなど。	DPF-R08：データ暗号化	2	3	1	1	2	リスク中
		サービス不能	機能・サービス	DoS 攻撃により、ドローン運用クラウドの運用が阻害される。※クラウドの機能障害による、アップデートの実行不可など。	DPF-R09：DoS 対策 DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録	2	3	1	1	2	リスク中
		権限の昇格	・アップデート用プログラムコード ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録 DPF-R12：脆弱性診断	2	1	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b		リスク値
No.	対象						脅威	脆弱性		a × b	
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	DPF-R13：アンチマルウェア DPF-R14：不要なソフトウェアの無効化	2	3	2	2	4	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	DPF-R01：アクセス制御 DPF-R02：機器認証 DPF-R03：ユーザ認証 DPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 DPF-R10：IDS/IPS（不正アクセス監視、遮断機能） DPF-R11：ログ記録	2	3	1	1	2	リスク中

表 7-17 サービス運用クラウドのリスクレベルの検討例（セキュリティ対策実施後） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
K	インターネット通信用インタフェース	不正アクセス	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス ・認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	サービス運用クラウドのファイル領域にアクセスされ、他の様々な脅威の要因となる恐れがある。	SPF-R01：アクセス制御 SPF-R02：機器認証 SPF-R03：ユーザ認証 SPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 SPF-R05：不要なネットワーク接続、論理インタフェースの無効化	2	3	1	1	2	リスク中
		情報の暴露	・記録映像 ・テレメトリデータ ・センサ取得情報	サーバのファイル領域から、秘匿すべき記録映像や、データが窃取される。 ※記録映像の漏洩によるプライバシ	SPF-R08：データ暗号化	2	3	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
			・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・機能・サービス、認証情報、復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ）、デジタル証明書	や肖像権の侵害、業務機密であるテレメトリデータの漏洩による信用失墜など。							
		データの改ざん	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報	サーバのファイル領域から、記録映像や、データが削除あるいは改ざんされる。※記録映像や、業務機密であるテレメトリデータの改ざん、削除による信用失墜など。	SPF-R08：データ暗号化	2	3	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
			・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの受発注情報など）								
		サービス不能	機能・サービス	DoS 攻撃により、サービスの提供が阻害される。※クラウドの機能障害によりサービス提供が阻害され、経済的損失につながるなど。	SPF-R09：DoS 対策 SPF-R10：IDS/IPS（不正アクセス監視、遮断機能） SPF-R11：ログ記録	2	3	1	1	2	リスク中
		権限の昇格	・記録映像 ・テレメトリデータ ・センサ取得情報 ・セキュリティ上の設定情報 ・アクセスログ等の監視情報 ・地番又は住居番号、所有者名等の情報が含まれる地理空間情報、測量成果 ・顧客情報（顧客の個人情報、サービスの	サーバ側のアクセス権限の不正な変更により、攻撃者に管理者権限を付与する。※バックドアや認証の迂回による他の脅威への派生など。	SPF-R10：IDS/IPS（不正アクセス監視、遮断機能） SPF-R11：ログ記録 SPF-R12：脆弱性診断	2	1	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
			受発注情報など） ・機能・サービス ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書								
		マルウェア感染	機能・サービス	サーバへのマルウェア送信により感染の恐れがある。またサーバを経由し、他の構成要素や無人航空機システムへの二次感染の可能性がある。※アップデートの障害に加え、不正な情報送信による漏洩、クラウドを経由で無人航空機に感染した場合、飛行への支障が発生する可能性など。	SPF-R13：アンチマルウェア SPF-R14：不要なソフトウェアの無効化	2	3	2	2	4	リスク大
		踏み台	※他の構成要素への影響	ボットネットの感染などによって、他の構成要素や無人航空機システムに対する攻撃の踏み台につながる。※意図しない第三者への攻撃行為、不正な情報送信による漏洩など。	SPF-R01：アクセス制御 SPF-R02：機器認証 SPF-R03：ユーザ認証 SPF-R04：アクセス制御機能の認証情報について、初期値の変更機能 SPF-R10：IDS/IPS（不正アクセス監視、遮断機能） SPF-R11：ログ記録	2	3	1	1	2	リスク中

表 7-18 通信経路におけるリスクレベルの検討例（セキュリティ対策実施後） ※資産の重要度と被害発生の可能性によるリスクレベル

発生箇所		脅威分類	影響を受ける守るべき資産	想定される被害	セキュリティ対策	資産の重要度（最大値）：a			被害発生可能性：b	a × b	リスク値
No.	対象						脅威	脆弱性			
1	ドローン本体とスマートフォン（タブレット）間の通信	データ改ざん	・リモート ID	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	UAV-R02：Bluetooth のセキュリティ対策	1	2	1	1	1	リスク中
2	ドローン本体と地上制御局間の通信経路（データ通信）	情報の暴露	・フライトログ ・記録映像、 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	TP-R01：通信経路暗号化	2	2	1	1	2	リスク中
		データ改ざん	・フライトログ ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報	無線信号の傍受やインジェクション攻撃などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	TP-R01：通信経路暗号化	2	2	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
			・センサ取得情報 ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書								
3	クラウドシステムとインターネット間の通信経路（データ通信）	情報の暴露	・アップデート用のプログラムコード ・記録映像 ・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が窃取される	TP-R01：通信経路暗号化	2	3	1	1	2	リスク中
		データ改ざん	・アップデート用のプログラムコード	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が	TP-R01：通信経路暗号化	2	3	1	1	2	リスク中

発生箇所		脅威分類	影響を受ける	想定される被害	セキュリティ対策	資産の重要度			被害発生		リスク値
No.	対象		守るべき資産			（最大値）：a	脅威	脆弱性	可能性：b	a × b	
			・テレメトリデータ ・設定情報（フライトモード等） ・ミッション情報 ・センサ取得情報 ・顧客情報（顧客の個人情報、サービスの受発注情報など） ・認証情報 ・復号鍵（秘密鍵） ・検証鍵（公開鍵、ハッシュ） ・デジタル証明書	改ざんされる							
4	ドローン本体とリモート ID キャプチャ機器間の通信	情報の暴露	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、フライトログや記録映像などが窃取される	UAV-R01：リモートＩＤ発信時の暗号化対応	2	2	1	1	2	リスク中
		データ改ざん	リモート ID の鍵情報	無線信号の傍受などの中間者攻撃によって、通信経路間の伝送情報が改ざんされる	UAV-R01：リモートＩＤ発信時の暗号化対応	2	2	1	1	2	リスク中

8 Appendix_C 用語集

- **ASLR（Address Space Layout Randomization）**
  標準ライブラリなどのメモリアドレス空間の配置をランダム化するバッファオーバーフロー対策機能。

- **CVSS（Common Vulnerability Scoring System）**
  脆弱性の深刻度を同一の基準の下で定量的に比較できる評価方法であり、0～10.0 の間でスコアが定まる。FIRST (Forum of Incident Response and Security Teams) が管理。

- **CWE（Common Weakness Enumeration）**
  Common Weakness Enumeration の略。ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準。米国非営利団体 MITRE を中心として仕様策定。

- **DEP（Data Execution Protection）**
  メモリ上のプログラム領域以外のデータに関する領域でのプログラム実行を禁止するバッファオーバーフロー対策機能。

- **IoT（Internet of Things）**
  既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノをネットワーク接続した、高度なサービスを実現するグローバルインフラ。[IoT セキュリティガイドライン ver 1.0]

- **ISMS（Information Security Management System）**
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。国際規格 ISO/IEC 27001 に要求事項が定められている。

- **JVN (Japan Vulnerability Notes)**
  日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に役立てることを目的とした脆弱性対策情報ポータルサイト。JPCERT/CC と情報処理推進機構（IPA）が共同で管理。

- **NVD (NATIONAL VULNERABILITY DATABASE)**
  NIST が管理する脆弱性情報 DB で他の DB 機関へのリンクに留まらず、関連する外部サイト情報も提供する。

- **エントロピー解析**
  データの情報量（エントロピー）を解析して定量化する手法。圧縮や暗号化されたデータの場合は高い値を示す。

- **脅威（Threat）**

システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。[JIS Q 27000:2014]

- **脅威情報（Threat Intelligence）**
  脅威からの保護、攻撃者の活動検知、脅威への対応等に役立つ可能性のある情報。[NIST SP 800-150]

- **サイバー攻撃（Cyber attack）**
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセスもしくは使用の試み。[JIS Q 27000:2014]

- **サイバーセキュリティ（Cybersecurity）**
  電子データの漏洩・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

- **サプライチェーン（Supply Chain）**
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れ。[ISO 28001:2007, NIST SP 800-53 Rev.4]

- **シグネチャ（Signature）**
  通信パケットに含まれる、攻撃に関係する認識可能で特徴的なパターン。マルウェア中のバイナリ文字列や、システムへの不正アクセスを得るために使用する特定のキーストロークなど。[NIST SP 800-61 Rev.1]

- **シルク**
  部品やピンの配置をわかりやすくするためにプリント基板に印字したテキストや記号。

- **脆弱性（Vulnerability）**
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2014]

- **脆弱性検証（Vulnerability Validation）**
  脆弱性の存在を確認するアクティブなセキュリティ検証手法。[NIST SP 800-115]
  脆弱性を洗い出すことを目的とする。

- **セキュリティ検証（Security Validation）**
  機器、システム、組織における脅威に対するセキュリティ対策の妥当性や脆弱性の有無を確認する手法。本手引きでは、特に機器に対するセキュリティ検証について記載している。

- **セキュリティ・バイ・デザイン**

情報セキュリティを企画・設計段階から確保するための方策。[内閣サイバーセキュリティセンター]
IoT 機器等においても、製品の企画・設計のフェーズからセキュリティ対策を組み込み、サイバーセキュリティ対策を確保しておく概念として、適用することができる。

- **耐タンパ性**
  モジュールの外部からのデータの読み取りや改ざんを困難にした機能

- **テイント解析**
  バイナリコードにデータを入力した際に当該データに関連するデータフローを解析する手法。

- **認証（Authentication）**
  エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

- **バックドア（Backdoor）**
  機器に設けられた、正規のログイン方法ではない非公表のアクセス方法。潜在的なセキュリティリスクとなりうる。[NIST SP 800-82 Rev.2]

- **プロトコル（Protocol）**
  複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

- **ペネトレーションテスト（Penetration Test）**
  組織が有するすべてのシステムや、指定されたシステム全体を対象とし、明確な意図を持った攻撃者によって、その目的が達成されうるかを確認するセキュリティ検証手法。

- **マルウェア（Malware）**
  許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェア。[NIST SP 800-53 Rev.4]
  セキュリティ上の被害を及ぼすマルウェア、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

- **リスク（Risk）**
  目的に対する不確かさの影響。[JIS Q 27000:2014]

9 Appendix_D 参考文書

- **サイバー・フィジカル・セキュリティ対策フレームワーク（経済産業省）**
  https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
- **IoT 開発におけるセキュリティ設計の手引き （IPA）**
  https://www.ipa.go.jp/files/000052459.pdf
- **ドローンセキュリティガイド 第２版（一般社団法人セキュアドローン協議会）**

  https://www.secure-drone.org/drone-security-guide/
- **リモート ID 技術規格書（案）（国土交通省 航空局 次世代航空モビリティ企画室）**

  https://www.kantei.go.jp/jp/singi/kogatamujinki/kanminkyougi_dai16/betten1.pdf
- **AC-119-1 Operational Authorization of Aircraft Network Security Program（FAA）**

  https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1028288
- **PS-AIR-21.16-02 Establishment of Special Conditions for Cyber Security（FAA）**

  https://www.icao.int/cybersecurity/SiteAssets/FAA/PS-AIR-21.16-02.pdf
- **ED-202A/DO-326 AIRWORTHINESS SECURITY PROCESS SPECIFICATION**

  https://eshop.eurocae.net/eurocae-documents-and-reports/ed-202a/
- **D-204A /DO-355A INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS（EUROCASE）**

  https://www.eurocae.net/news/posts/2019/december/eurocae-open-consultation-ed-204a/
- **サービスロボット・セキュリティガイドライン 第１版（公立大学法人会津大学、TIS 株式会社、ネットワンシステムズ株式会社）**

  https://rtc-fukushima.jp/wp/wp-content/uploads/2019/05/e8d215d9e3f39a8c5e09f6a126b5f34f.pdf

- **電気通信事業法に基づく端末機器の基準認証に関するガイドライン（総務省）**

  https://www.soumu.go.jp/main_content/000615696.pdf

- **IoT セキュリティ・セーフティ・フレームワーク（経済産業省）**
  https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

- **経済産業省　情報セキュリティ管理基準　平成 28 年改正版（経済産業省）**

  https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

- **ドローンによる撮影映像等のインターネット上での取扱いに係るガイドライン（総務省）**

  https://www.soumu.go.jp/main_content/000376723.pdf

- **カメラ画像利活用ガイドブック_ver2.0（IoT 推進コンソーシアム、総務省、経済産業省）**

  https://www.soumu.go.jp/main_content/000542668.pdf

- **地理空間情報の活用における個人情報の取扱いに関するガイドライン（地理空間情報活用推進会議）**

  https://www.gsi.go.jp/common/000055897.pdf

- **地理空間情報の活用における個人情報の取扱いに関するガイドライン（測量成果等編）（測量行政懇談会）**

  https://www.gsi.go.jp/common/000063604.pdf

- **ISO/IEC27017　JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範（ISO）**

  https://www.iso.org/standard/43757.html

- **NISTIR 8259 “Foundational Cybersecurity Activities for IoT Device Manufactures”（NIST）**
  https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

- **NISTIR 8259A “IoT Device Cybersecurity Capability Core Baseline”（NIST）**
  https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf

- **"Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products"（NIST）**

  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

- **ETSI EN 303 645 ”Cyber Security for Consumer Internet of Things: Baseline Requirements”（ETSI）**
  https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

- **IoT 分野共通セキュリティ要件ガイドライン 2021 年版_ver1.0（CCDS）**
  https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTCommonReq_2021_v1.0_jpn.pdf

- **IoT 機器セキュリティ実装ガイドライン(ソフトウェア更新機能)_1.0 版（CCDS）**
  https://www.ccds.or.jp/public_document/index.html#20201202_report1

- **政府機関等の対策基準策定のためのガイドライン 平成 30 年度版（NISC）**
  https://www.nisc.go.jp/active/general/pdf/guide30.pdf

- **外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（NISC）**
  https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf

- **情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（NISC）**
  https://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf

- **CRYPTREC 暗号技術ガイドライン （軽量暗号）（CRYPTREC）**
  https://www.cryptrec.go.jp/tech_guidelines.html

- **TLS 暗号設定ガイドライン Ver.3.0.1（IPA）**
  https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

- **TLS 暗号設定ガイドライン_チェックリスト（IPA）**
  https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

- **中小企業の情報セキュリティ対策ガイドライン（IPA）**
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- **制御システムのセキュリティリスク分析ガイド 第 2 版（IPA）**
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/

無人航空機のセキュリティ WG（令和 3 年度）　構成員

委員長	荻野　司	一般社団法人　重要生活機器連携セキュリティ協議会　代表理事 情報セキュリティ大学院大学　客員教授
委　員	吉岡　克成	横浜国立大学　大学院環境情報研究院/先端科学高等研究院　准教授
委　員	森　達哉	早稲田大学　理工学術院　基幹理工学部　教授
委　員	矢口　勇一	会津大学　情報システム学部門　准教授
委　員	菊池　浩明	明治大学　総合数理学部　専任教授
委　員	角家　弘志	角家・江木法律事務所　弁護士
委　員	秋本　修	日本無人機運航管理コンソーシアム　事務局長
委　員	中島　一彰	日本産業用無人航空機工業会 ISO 委員会　副委員長(セキュリティ担当)
委　員	西林　卓也	ソニーグループ株式会社　AI ロボティクスビジネスグループ ソフトウェア設計部　統括部長
委　員	坂牧　隆夫	株式会社 ACSL　事業推進ユニット　生産品質保証
委　員	田中　将弘	セコム株式会社　技術開発本部　開発センター サービスロボット開発 1G　チーフエンジニア
関係省庁		経済産業省　製造産業局　産業機械課　次世代空モビリティ政策室
関係省庁		経済産業省　商務情報政策局　サイバーセキュリティ課
オブザーバ		国立研究開発法人新エネルギー・産業技術総合開発機構
事務局		国立研究開発法人産業技術総合研究所
事務局		株式会社マストトップ
事務局		株式会社三菱総合研究所