ドローンセキュリティガイド

<Drone Security Guide>

- 第 5 版 -

2024 年 6 月

一般社団法人セキュアドローン協議会

改訂履歴

版数	発行日	改訂履歴
第 1 版	2018 年 3 月 18 日	初版発行
第 2 版	2021 年 4 月 1 日	以下の章の追記ならびに修正。 3. ドローンにおけるセキュリティ対策の要件 4. ドローンのセキュリティリスク分析 4.1. ドローンのリスク管理 4.2. ドローンのリスクの侵入モデルと被害 4.3. ドローンのセキュリティ対策 4.4. 悪意あるドローンに対する対策 7. 業務運用に関する注意点
第 3 版	2022 年 6 月 14 日	以下の章の追記ならびに修正。 5.3. クラウドを使用したドローンの認証例 7. リモート ID について 8. ドローン関連サービス、プロトタイプ開発事例 9. 業務運用に関する注意点
第 4 版	2023 年 6 月 20 日	以下の章の追記ならびに修正。 2. セキュリティ仮想事例 3.3. 機体認証 3.4. 各ガイドラインとの関係性 4. ドローンセキュリティ対策の進め方 5.1. ユースケースの定義 5.4. セキュリティ要求の定義 8. ドローンにおけるセーフティ
第 5 版	2024 年 5 月 23 日	以下の章の追記ならびに修正。 ドローンのステークホルダ毎のサイバーセキュリティ作業内容 4.6. ソフトウェアサプライチェーン 4.7. ドローンに関連するサイバーセキュリティ国際規格 6.2.4. 位置情報の保護 8.2.3. 国内統計事例（改正航空法施行後） 8.3.4. 墜落

目次

1. はじめに

1.1. ドローンセキュリティガイドの策定趣旨

2020 年 9 月に内閣官房より「ドローンに関するセキュリティリスクへの対応について」という資料が提出された。これまで政府がドローンの利活用を推進してきており、Level 4（人口集中地区での目視外飛行）の実現や「ドローンの利活用推進に向けたガイドライン策定への取組」[1]という政府のガイドライン（インフラ点検、プラント点検、警備、パブリックセーフティ、災害時など）が整備されてきたこともあり、本格的な社会実装が間近である。

2022 年 3 月には経済産業省より「無人航空機分野 サイバーセキュリティガイドライン」[2]が公開された。これは、測量や物流、設備点検、警備、災害時の被災状況調査など無人航空機システムの活用分野が広がる中、活用される用途とそれぞれで扱われる情報などの特性を踏まえ、リスク分析を実施した上で情報セキュリティ上の対策がまとめられており、機体メーカーやサービス事業者からユースケースごとの情報資産やセキュリティ要件などの内容も反映されている。セキュリティリスク分析に用いるため、無人航空機システムの汎用的なシステムモデルについても定義されている。

[1] ドローンの利活用推進に向けたガイドライン策定への取組
https://www.kantei.go.jp/jp/singi/kogatamujinki/kanminkyougi_dai14/siryou8.pdf

[2] 無人航空機分野 サイバーセキュリティガイドライン
https://www.meti.go.jp/policy/mono_info_service/mono/robot/drone_cybersecurity.html

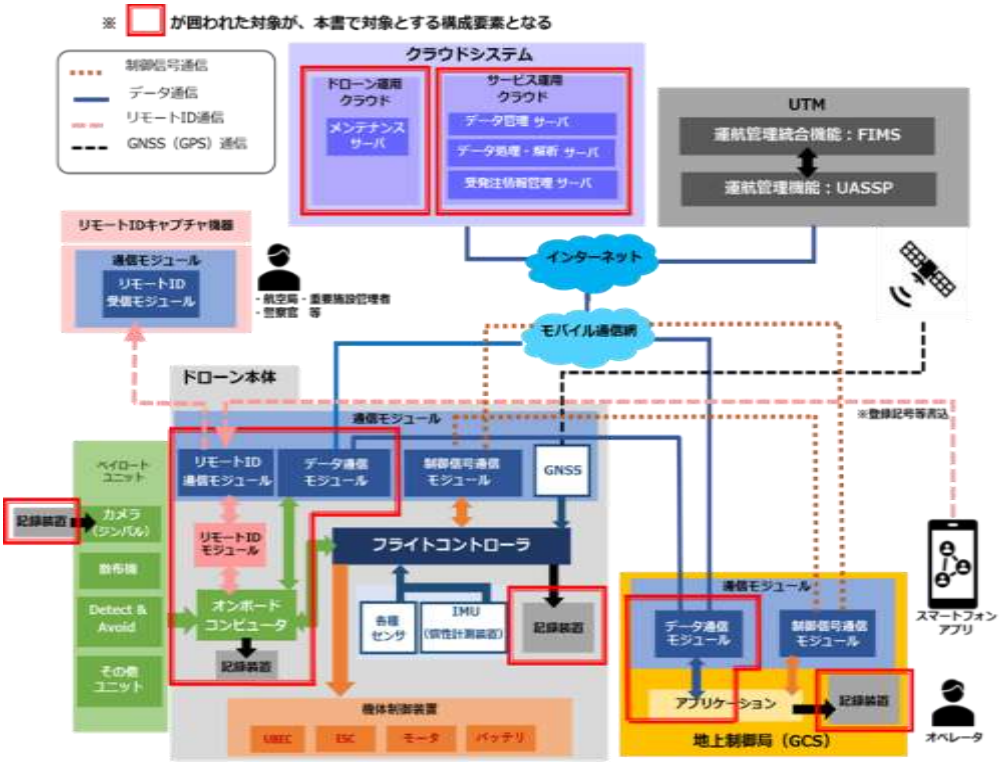


図 1 ：無人航空機の汎用的なシステムモデル（出典：経済産業省）

2022 年 6 月からは無人航空機の登録が義務化され、3 年ごとに更新登録を行う必要があり、登録しなければ飛行することができない。機体への表示が義務化され、登録記号を機体に直接記載もしくは貼付する必要があり、機体メーカーはリモート ID 機器およびアプリケーション[3]を備えることが義務付けされる。

本格的な社会実装を迎えるにあたり、現状のドローンにおけるセキュリティの脆弱性はさまざまな混乱を引き起こす可能性があり、それにより進んできた利活用の推進がストップしてしまう懸念がある。その点からいえば、ドローンのセキュリティ対策は推進に対し前向きなもので、この壁を乗り越えれば、ドローンの利活用が進んでいくということになる。このセキュリティ対策にむけて、ベースとなる政府の組織は「内閣サイバーセキュリティセンター（NISC）」[4]におけるサイバーセキュリティ戦略本部である。

[3] リモート ID 機器等及びアプリケーションが備えるべき要件
https://www.mlit.go.jp/koku/content/001444589.pdf

[4] 内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/index.html

このサイバーセキュリティ戦略本部で「サイバーセキュリティ 2020」[5]が公開され、日本全体のサイバーセキュリティ戦略が提示されている。この中で IoT や自動運転自動車システムなどのセキュリティも検討されているが、それらと同様にドローンソリューションも俎上に載せていかなければならないということで、その中でドローン（将来的には空だけでなく、陸上、水上、水中なども含んでいくだろう）には自律機体制御や機体管理といった移動体特有のセキュリティリスクもあり、今後定義付けし対策を講じていくことになる。

現在、ドローンは航空法などによる規制もあるため、コンシューマ向け（個人の趣味や娯楽）といった用途よりも、企業や団体による産業用途での活用がメインであるところは、ドローン関連者の多くが認識していることである。ドローンはそのものが目的ではなく、企業や団体にとって、何らかの目的を実現するための手段であるということで、ドローンがその目的に対して価値創造を行っており、その価値に対して、企業や団体は投資しドローンを活用していると言える。

2017 年ごろから、点検や測量といった分野で徐々に実証実験を越えて、社会実装がされてきたこともあり、まずはドローンのセキュリティの考え方というものを整理するために「ドローンセキュリティガイド」の策定を行い、2018 年 3 月に本ガイドの第 1 版を公開した。

セキュリティリスクを考える前に民間企業においては、現在のドローンソリューションがどのような価値創造を行っているかを再検討することが必要であり、その価値創造がベースとなり、セキュリティ対策の優先順位が決まる。セキュリティ対策を行うことで、それまで築き上げてきた価値創造を著しく劣化させるようなことを起こさないという観点が重要となる。

すでに社会実装されているものや実証実験が最終段階を迎えているドローンのソリューションにとって、ドローンシステムのセキュリティ対策はほぼ行われておらず、システムとして脆弱である。それは現状までは、実証実験などを通じて、ドローンの利活用といったところに視点が置かれてきており、セキュリティ対策は考慮されていなかったためである。現在もまだドローンのシステム全体を考えると、ユーザビリティなども考えた場合には解消しなければならない課題も多いが、それでも実装が近づくにつれ、悪意ある第三者による攻撃などのセキュリティ対策を行い、企業は関連する法令への順守、事故や事件発生時のブランドイメージへの影響、機密データの漏えいによ

[5] サイバーセキュリティ 2020
https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf

る悪用などのリスクへの対応が必要となる。

ドローンの本格的な社会実装にあたり、サイバーセキュリティにおける事件・事故の増大が危惧される。一般社団法人セキュアドローン協議会において、参加各社の先端ドローン技術、セキュリティ技術、IoT 関連技術、エネルギー管理システムといった ICT 関連技術を生かし、ドローンの安心・安全な操作環境とデータ送信環境を確立していくための指標となる本セキュリティガイドの策定を行う。

2. セキュリティ仮想事例

こういったガイドラインを作成する際に、事例や事案の章が必ずあるが、セキュリティに関しては現状、表立った事案はほとんどない。それは表に出にくいということもあり、また、セキュリティといった内容だからということもあるだろう。

このガイドラインの別項でも説明されているが、セーフティとセキュリティの明確な違いは、セーフティは安全面全般の事項に対して、セキュリティはあくまで「悪意ある第三者が起こす事案」ということとなるだろう。

そして、ドローン（自律航空機）に関してのセキュリティに関しては、大きく二つにその内容が区分される。一つが他のＩＴ機器と同様に、情報セキュリティといったデータ関連のセキュリティだ。その中でも大きく二つに分かれるが、1）機体情報（航行データや機体状態データなど）2）ペイロード（カメラやセンサなど）の情報となる。これに関しては、政府もドローンのセキュリティガイドラインを出して注意喚起を行っている。しかし、ドローンにとっては、よりリスクが高い内容となるのは、もう一つのセキュリティである耐空性のセキュリティである。これは所謂乗っ取りや墜落などを引き起こすものとなり、企業や関係者にとっては、一般的にはより被害が大きいものとなる。

こういったセキュリティ事案をこれまであまり見聞してきていないのは、現在までのドローン使用状況において実証実験が多く、実用化しているケースが少なかったことにも因るだろう。

それは「悪意ある第三者」の動機が関係している。「悪意ある第三者」の動機は、一般の犯罪と同様で、大きく３つ、もしくはその混合にある。１）愉快犯的な要素、２）その企業や人に対する怨恨的な要素、３）金銭的な要素。いわば、今後、ドローンの実用化が進んでいった場合には、こういった「悪意ある第三者」にとって、犯罪を誘発する動機が増えていく可能性があるし、また、ドローンに関しては、まだ、そのセキュリティ対策が施されていないケースも多い。

ここに示した事案はあくまでフィクションであり、実際起こった事案ではなく、そこに登場する企業や団体もまったく実際の企業や団体とは関係がない。また、ここに書かれた行為自体は当然何らかの犯罪となる行為である。しかし、この事案を読んでいただき、各企業や関連者にとっても、「いま、そこにある危機」だと自分事として捉えていただければ幸いだ。

2.1. プロポの略奪

Ａ社は、鉄塔などの構造物の点検にマルチコプター型のドローンを採用して、点検業務を日常的に行っている。毎日、機体点検を行い安全対策に余念はない。

いつもの通りに現場に向かい、２人１組にて、ドローンにて鉄塔点検の業務を開始していた。対象の鉄塔に関する自動航行による点検モードにて、飛行を開始した。１人は鉄塔近くで、状況を確認し、１人は離れたところで、操作を行っていた。その操作者はドローンが異常を示した際の時のた

めに、プロポをいつでも持ち、マニュアルモードへの切替えが出来るようにしていた。

その操作者のもとに、1 人の人間がおもむろに近づき、その操作者に暴行を加え、プロポを略奪した。そのプロポによって、ドローンをマニュアル操縦にて操作し、他の共犯者近くまで飛行させ、それによって、ドローンが盗まれてしまった。

操作者は幸いにも軽傷で済んだが、ドローンの盗難被害と、また、別の現場で取得していた点検データも盗まれてしまった。

点検データは企業機密情報であり、機密情報漏洩の事案ともなり、新聞やメディアにも大きく取り上げられてしまい、今後の対応が迫られることになった。

対策：

自動航行の運用であっても、何かの時に備えて、プロポでのマニュアル操作で操縦するような運用を行っているケースがほとんどだ。

こういった事案の対策としては、メインプロポが奪われた際にメインプロポを使用停止にし、サブプロポもしくは GCS（Ground Control Station）にて対応する仕組みの導入が必要だろう。また、ドローンで取得するデータが会社の機密情報にあたる場合には、パソコンなどで導入しているような取得したデータの暗号化対策なども重要となる。

2.2. ハッキング

B 社は工場やプラントなどにおける監視業務をドローンで行っている。

この警備用のドローンは LTE が搭載されており、中央センタから完全目視外でインターネットを介して遠隔操作を実施するという進んだ形での遠隔監視システムとなっている。

この日もいつも通りに定期運用の中でドローンによる上空監視を実施していた。

その日の数回目かの監視飛行にあたるときに、急にドローンが墜落し、その墜落により工場設備を破壊してしまい、依頼先企業に大きな被害を与えてしまっただけでなく、その混乱に乗じて、その工場で使う重要な部品の盗難にもつながってしまった。大きな事件として、新聞やメディアにも大きく取り上げられ、早急な対応が迫られることになった。

対策：

こういった遠隔監視は、日本ではまだ実用段階に入っているところは多くはないが、レベル 3 やレベル 4 のルールが定まる中で、こういった監視や警備業務でドローンを使用するケースは増えてくるだろう。

今回のケースに関しては、クラウドハッキング対策は勿論だが、基本的には定期航行による監視ということで、その業務以外を実施する際（コース逸脱やキルスィッチの使用など）には二重のアクション対策といったものも施すことも必要となってくるだろう。また、墜落した場合に被害が甚大になるケースにおいてはパラシュートの搭載も有効な手段となってくるだろう。

2.3. 通信妨害

C 社はドローン物流を実用化している。特に、この会社は薬販売のチェーン会社と組んで、処方箋薬搬送業務をメインで行っている。特に山間部などの過疎地向けにリモート診療と連動する形でサービスを提供し、話題となっている。

この日もいつもと同様で、配送センタから 10ｋｍ程度離れた山向こうのＸ地区の 5 件のお客さんから配送依頼が入った。（Ｘ地区では集会所でのドローンポートによる集中受け取りを行っている）その日の気象条件に合わせ、ルート選択がなされ、危険を回避する形で配送センタからドローンが飛び立った。片道 20 分程度となる。

12 分程度航行した山あいで、急に、プロポ、テレメトリー、FPV の通信すべてが繋がらなくなった。その後、ずっと通信が回復しないまま、20 分以上の時間が経過した。

（このドローンの飛行限界時間は 30 分程度）

最後にテレメトリーに示された GPS 地点に捜索したが、結局、山林が深いこともあって、ドローンを見つけることが出来なかった。

話題となっていたサービスでもあり、その機体の喪失は新聞やメディアで大きく扱われることになった。

対策：

現在、こういったサービスが実運用にむけて、実証実験が多く行われている。

その中でも遠距離の通信は安全性の面からも、様々な対策が必要な分野でもある。

まずは、通信の多重化はベースにして対策を行う必要があるが、残念ながら通信妨害する可能性のある機器（合法・非合法を問わず）は多く存在しており、ドローンのセキュリティにとっても通信妨害対策は非常に重要である。

多重化といったことだけでなく、通信が取れなくなったときのフェールセーフの対策の充実となる。通常、通信途絶のフェールセーフは、しばらく上空でホバリングを行い、一定時間を超えると、ホームポイントに帰ってくるというものが多いが、こういった山間部の場合は直線で戻ることが出来ないケースもあり、スマート帰還といった航行した航路を戻る方式や、緊急着陸用ポイントを設定しておき、一番近いポイントに戻るという方式なども機体によっては設定できるようになっている。

こういった目視外で数ｋｍ飛行する機体に関しては、こういったフェールセーフを活用することも重要であろう。

また、ドローン搭載の GPS はドローンのバッテリーが切れた後には発信しなくなってしまうため、ドローンが墜落した際のドローン発見用のタグを別途装着しておく対策も重要であろう。

2.4. GPS 妨害

Ｄ社は昨今ＣＯ２排出権取引でも話題になっている山林調査をドローンで行っている会社だ。現在、国や各自治体で所有の山林状況の調査を多く受注している。

この日もＹ地区という山林の調査をドローンで調査するため、ドローンの準備をしている。対象の山林を数ｋｍにわたって、自動航行で往復しながら、調査をする手法となっている。

数ｋｍ先は山影に入る部分もあって、レベル３の申請も行い、飛行を行っている。

今回も自動航行で飛行を実施していたが、その山影に入ってしばらくしたら、GPS のエラーが発生した。今までそういったエラーは発生したことがなく、完全に目視外での手動操作となり、ホバリングも出来ず、ＦＰＶの映像やテレメトリーの情報も安定しないこともあり、ドローンの手動制御不能となり、どこかで墜落させてしまった。

山での墜落となり、墜落したドローンも発見できず、その損害を回収できないだけでなく、幸いに山火事には至らなかったが、自治体の信頼を失い、その後の受注を失う形となった。

対策：

この GPS ロストは、最近はあまり聞かなくなかったが、2015-16 年あたりは時々こういった事象に遭遇し、急に手動で操縦しなくてはならなくなり、大変な思いをしたものだ。

最近、GPS 関連のデバイスの性能向上などもあるのかもしれないがこういった事象を聞くケースは少なくなったが、現在でも、大きな建物のそばや山影ではこういったケースもあるので注意が必要だ。

今回はこういったセーフティ関連のケースでなく、セキュリティのケースとして記載しているのは、GPS ジャマーといった GPS 妨害をする機器が市販されているからである。

これは今後、多くの自律ロボットが普及していく際にも自律制御上で大きな問題となっていく事案かと思うが、現在の目視外運用のドローンにおいても、対策が必要な事案となっている。

現在、機体によっては、GPS が繋がらなくなっても、非 GPS の制御機能や IMU／コンパスと連動してある程度、自動で安全な飛行が出来るような機能が開発され始めている。こういった新しい機能で対策していくことも重要であるし、また、場合によっては、キルスイッチ（墜落スイッチ）とパラシュートの連動でなるべく安全に墜落させる機能も検討する必要があるだろう。また、通信妨害の際にも記載したが、ドローン墜落した際のドローン発見用のタグを別途装着することも重要であろう。

今回、フィクションとして、この４つのケースを記したが、これ以外、もしくは、ここに挙げたケースの混合型のリスクも様々に内在している。

「いま、ここにある危機」として、各活用企業は優先順位を定めて、対策を進めていくことが必要だろう。

3. ドローンのセキュリティ概要

産業用ドローンを安全に利用するためには、取得したデータの保護や安全な通信手段の確立など、各種のセキュリティ対策が必要となる。本章では、今までにどのようなセキュリティ上のリスクが発生し、事故や被害が起きたのか、また、今後どのようなセキュリティ上の対策が必要であるのか解説する。

3.1. これまでに発生したドローンに係る事故およびセキュリティ上のリスク

ドローンの操縦の乗っ取り

2017 年にラスベガスで開催された DEF CON(ハッキング会議)では、ポケットサイズのマイクロコンピュータを使用して、ワイヤレスキーボードからドローンの制御を乗っ取った事例が紹介されている。このハッキング事例では、ARM ベースの組み込みシステムによって Bluetooth 経由でワイヤレスキーボードからの信号を盗聴し、ユーザ ID やパスワードなどの情報を入手する技術を応用して、マイクロコンピュータをドローンのコントローラに接続して、フライトコントローラを乗っ取った。このような事例だけではなく、コントローラとドローンの機体間で利用している Wi-Fi などの通信方式をハッキングすることで、操縦者になりすましてドローンを悪用する危険性もある。

データの盗み出し

RGB カメラやマルチスペクトルカメラなどで空から撮影した画像データは、貴重な情報資産。そのデータを守る対策も重要だ。ドローンによる空撮や地上のスキャニングデータは、機体内部の不揮発性メモリや Micro SD カードに保存される。その段階で、ドローン本体を何者かに盗まれてしまうと、暗号化されていないデータは容易に漏えいする。

また、ドローンから Wi-Fi などの無線通信でデータを転送する場合にも、第三者に通信を傍受される危険性がある。そして、MicroSD カードから PC などを利用してデータをクラウドサービスにアップロードする場合にも、インターネット経由での安全なデータ転送に配慮しなければ、データをハッキングされる心配がある。

今後も拡大するドローンのセキュリティ被害

ここで説明した事例の他にも、産業用ドローンが測量や点検に、精密農業やインフラ監視など、様々な業務に利用されるようになれば、一度のフライトから得られる画像データやスキャニングイメージは、貴重な情報資産となる。その情報資産を安全に守るためには、ドローンのセキュリティ対策が重要になる。本書では、空撮により取得するデータの保護から、運行などに関連する機体の認証など、IoT 機器としてのドローンに関するセキュリティ対策についてのガイドラインを提

唱する。

3.2. ドローンセキュリティガイドの概要

本書では、以下の内容について解説する。

- ドローンのセキュリティ概要
  レベル３，４運行に必要となる機体認証制度、および他業界含む各種ガイドラインと本ガイドラインの位置づけ等について説明
- ドローンセキュリティ対策の進め方
  ドローン事業を推進するために必要なセキュリティ対策を開発工程ごとに説明
- リスクアセスメント
  ドローンを安全に運用するために必要なセキュリティ要求を定義するための脅威分析、リスク評価方法の説明
- セキュリティ要素技術
  セキュリティ要求をドローンおよび周辺システムに適用するための実装技術について説明
- 運用手順および運用時の注意事項
  ドローン運用において安全な飛行を維持するために遵守すべき事項を説明
  セーフティ
  ドローン運用時に起こりうる事故の原因および対策方法、セーフティとセキュリティの関係性について説明
- まとめ
  本セキュリティガイドについての総括
- Appendix. ドローン関連サービス、プロトタイプ開発事例
  本協議会加入企業が取り扱うドローン関連サービスおよびプロトタイプ開発事例の紹介

3.3. 機体認証

政府はレベル 4（有人地帯の目視外飛行）での飛行に向けて機体認証制度を開始した。ドローンサービス提供事業者はリスクの高い一部ユースケースに応じて、機体認証をクリアしたドローンの使用が求められる。機体認証にはリスクに応じて第一種と第二種がある。

区分	説明
第一種	レベル 4 飛行相当となり、その中でも人口密度の高いエリアでの飛行と人口密度の低いエリアでの飛行に分かれている。
第二種	レベル 4 以外の飛行となり、機体の重量によって、以下のように区分されている。 ● 100g 以上 4kg 未満 ● 4kg 以上 25kg 未満 ● 25kg 以上 ● 25kg 以上＋リスク高

3.3.1. 機体認証の手続き

機体認証は、以下[6]の流れで進行する。認証に関する大枠としては、設計（開発時に実機で検証）、製造過程（製品の均一性を審査）、現状機体検査に分かれており、型式認証は設計・製造過程の認証となる。機体認証に関しては、この設計・製造過程に加えて、現状機体検査が付加される。

型式認証取得済の量産機を用いる場合には、機体認証時に設計・製造過程の認証は省略できる。一方、自作機を用いた場合の機体認証は、機体ごとに設計・製造過程の認証が必要となる。

図 2：ドローンの機体認証型式認証の流れ

[6]参考サイト：Drone.jp 春原久徳のドローントレンドウォッチング
https://www.drone.jp/column/20221208165405600 72.html

3.3.2. 型式認証

型式認証ではドローンのユースケースに応じてセーフティ、セキュリティの両面からリスクを特定し、リスク評価結果に応じた要求をドローンおよび周辺システム（機体制御）が実装していることを、設計書およびテスト結果として、当局に提出する必要がある。

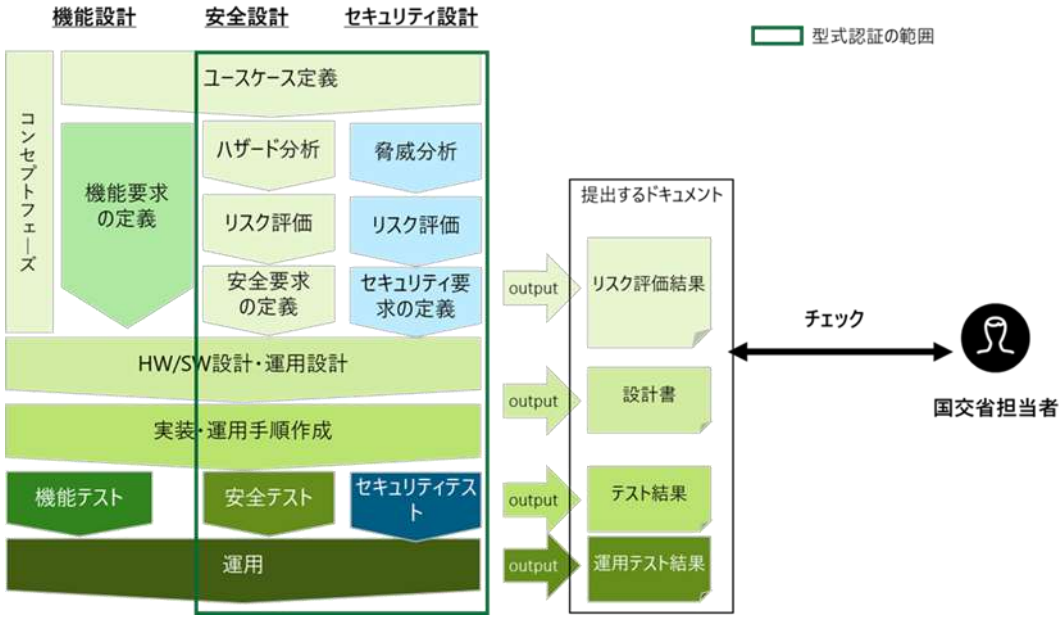


図 3 ：ドローンの開発プロセスと型式認証の流れ

日本の型式認証[7]は米国 FAA の認証制度（D&R プロセス）を踏襲しており、セーフティに関する要件が大半であるが、セキュリティについても検討する必要がある。

[7] 参考サイト：国土交通省：無人航空機の型式認証等の取得のためのガイドライン
https://www.mlit.go.jp/common/001574425.pdf

項目	タイトル
001	運用コンセプト
005	定義
100	無人航空機に係る信号の監視と送信
105	無人航空機の安全な運用に必要な関連システム
110	ソフトウェア
115	サイバーセキュリティ
120	緊急時の対応計画
125	雷
130	悪天候
135	重要な部品
140	その他必要となる設計及び構成
200	無人航空機飛行規程
205	ICA
300	耐久性と信頼性
305	起こりうる故障
310	能力及び機能
315	疲労試験
320	制限の保証

115 サイバーセキュリティ

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

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

115Cybersecurity

a. UA equipment, systems, and networks, addressed separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in an adverse effect on the security or airworthiness of the UA.Protection must be ensured by showing that the security risks have been identified, assessed, and mitigated as necessary.

b. When required by paragraph (a) of this section, procedures and instructions to ensure security protections are maintained must be included in the ICA.

図 4 ：型式認証制度におけるセキュリティ項目と内容

型式認証におけるセキュリティの記載は簡潔であるが、開発プロジェクト全般において多岐にわたる対策が必要であることを示している。下図は開発プロジェクトにおける各プロセスと本ガイドライン該当項目を当てはめたものである。製品出荷後であってもセキュリティ対策が維持されているか継続的に確認する必要がある。

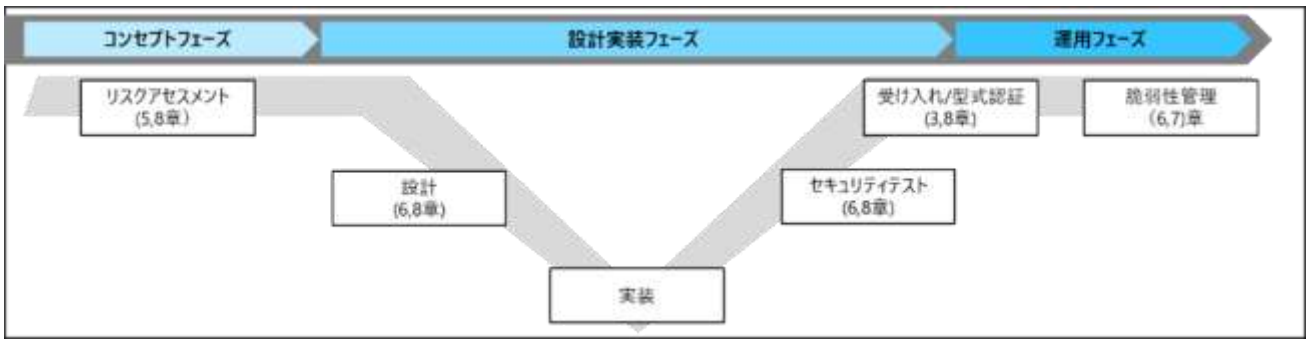


図 5 ：開発プロジェクトと本ガイドライン項目の整理

3.4. 各ガイドラインとの関係性

以図は本ガイドラインと他業界のガイドラインを比較したものである。

観点として、以下で分類したものである。

① システムの利用ポリシー、開発プロセスをまとめた「組織」

② システムのセキュリティ要求の定義方法をまとめた「システム」

③ システムのセキュリティ要求を実装する際に参考する「個別技術」

ドローンとの関係性を見てみると、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）が作成した無人航空機分野 サイバーセキュリティガイドラインはシステムに焦点を当てているのに対し、本ガイドラインはシステムに加え、個別技術まで記載している。これは本ガイドラインの趣旨が、ドローン事業者に対し、より具体的な支援を行うことを目的としているためである。

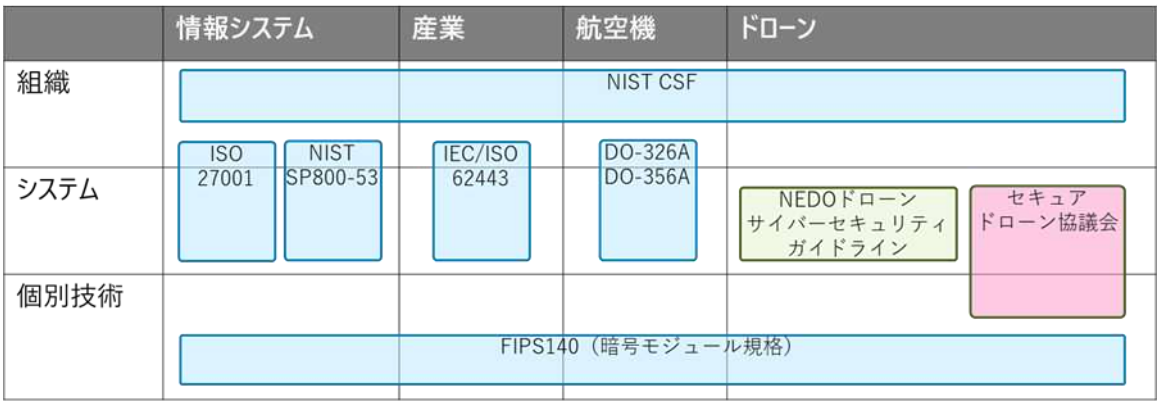


図 6 ：本ガイドラインと他業界ガイドラインとの関係性

4. ドローンセキュリティ対策の進め方

ドローンのセキュリティ対策を考える上で、ドローンのライフサイクルに当てはめ各フェーズでのセキュリティ対策を考える必要がある。各フェーズで必要となるセキュリティ対策を解説する。

4.1. ドローンのライフサイクルに対するセキュリティ対策の全体的な流れについて

一般的なドローンの開発から運用、廃棄までのライフサイクルに対して必要となるセキュリティ対策を下図に示す。ドローンでは、ステークホルダによって対策を実施するフェーズも異なるため、ステークホルダ毎に必要となるセキュリティ対策を表にまとめる。各ステークホルダの説明は 5.1.1 章を参照。

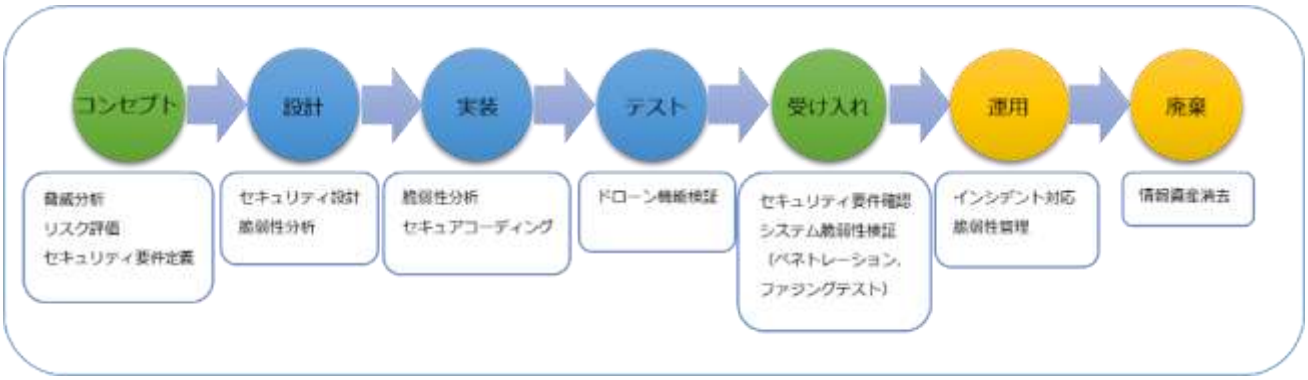


図 7 ：セキュリティ対策の全体的な流れ

表 1：ステークホルダ毎のサイバーセキュリティ作業内容

フェーズ	サイバーセキュリティ作業内容	個人ユーザ	企業	サービス業者	機体メーカ
			例：運送会社	例：データセンター	ドローンメーカー
コンセプト	脅威分析		○		
	リスク評価		○		
	セキュリティ要件定義		○		
設計	セキュリティ設計			○	○
	脆弱性分析			○	○
実装	脆弱性分析				○
	セキュアコーディング				○
	静的解析				○
テスト	セキュリティ機能検証			○	○
	ドローン脆弱性検証			○	○
受け入れ	セキュリティ要件確認（個人ユーザの場合は＊1参照）	○	○		
	システム脆弱性検証（ペネトレーション、ファジングテスト）		○		
運用	インシデント対応（個人ユーザの場合は＊2参照）	○	○	○	○
	脆弱性管理		○	○	○
廃棄	情報資産消去		○	○	○
全体フェーズ	ソフトウェアサプライチェーンの管理	△（利用）	○	○	○

※ユーザまたは、サービス業者が部品を購入して組み立てた場合は、各部品の脆弱性判断が必要

※1　個人ユーザの場合は購入したドローンメーカーのサイトのセキュリティ情報やホワイトペーパーを確認（セキュリティ対策を把握）

※2　個人ユーザの場合は購入したドローンメーカーのサイトのセキュリティ情報、アップデート情報を定期的に確認し対策する（脆弱性対応を確認）

※3　ソフトウェアサプライチェーンに関しては 4.6 を参照

4.2. コンセプトフェーズ

ドローンの使用用途、環境、保持資産から脅威分析を行い、脅威を抽出する。

抽出された脅威に対してリスク評価を行い、セキュリティ対策を定義する。

このセキュリティ対策に関しては 6 章にて解説する。

4.3. 開発フェーズ

開発の設計、実装、テストの各フェーズにおける対策は下記のようになる。

設計　　セキュリティ要件の設計、およびセキュリティ設計に対する脆弱性分析

実装　　ソースコードに対する、脆弱性分析、セキュアコーディング、静的解析

テスト　　セキュリティ機能の検証、脆弱性検証

4.4. 受け入れ・運用フェーズ

脆弱性管理、脆弱性診断、セキュリティインシデント対応などのセキュリティ対策が必要。

6.2.6 章で解説する。

4.5. 個人ユーザの場合の対応

表 1 の注意事項に記載したように、最低限ドローンが踏み台など不正に利用されないために、ドローンメーカーのサイトのセキュリティ情報を確認し積極的にセキュリティ対策が講じられているかを確認が必要となる。

また、定期的に脆弱性対策のファームウェア更新がされていないか確認し、適時ファームウェア更新を行うこと。

4.6. ソフトウェアサプライチェーン

近年ソフトウェアサプライチェーンが複雑化し、オープンソースソフトウェア（OSS）の利用が一般化する中で、ソフトウェアに対するセキュリティ脅威が急激に増大している。ドローンにおいてもソフトウェアの規模が増大し、OSS および、市販モジュールを組み込むことが多くなっており、ソフトウェアサプライチェーンのセキュリティ脅威も考慮していく必要がある。

ソフトウェアサプライチェーンとは、ソフトウェア開発ライフサイクルに関わる要素と、その相互依存関係の総称であり、具体的には、オープンソースソフトウェア（OSS）を始め、コードや設定ファイル、ライブラリ、プラグイン、コンパイラなども含まれる。

このソフトウェアサプライチェーンが肥大化し、複雑化する中で、ソフトウェアのセキュリティを確保するための管理手法の一つとして、SBOM（Software Bill of Materials）が着目されている。

4.6.1. SBOM の概要

SBOM とは、ソフトウェア管理の一手法であり「ソフトウェア部品表」とも呼ばれる。ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストを作成することで、ソフトウェアサプライチェーンの透明性を高めることが期待されており、コンポーネントの脆弱性管理の課題に対する一つの解決策として期待されている。OSS を利用する可能性が高いドローンにおいても、SBOM を作成し、使用する OSS の管理を徹底することは、脆弱性対策として必要となる。SBOM については、経済産業省 商務情報政策局サイバーセキュリティ課にて「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」が策定されている[8]。

[8] 経済産業省：「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」
https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-2.pdf

4.6.2. ドローンのソフトウェアサプライチェーン

ここで、ドローンでのソフトウェアサプライチェーンを考える。SBOM を導入するメリットとしては、脆弱性管理のメリット、ライセンス管理のメリット、開発生産性向上のメリットの 3 つが挙げられる。

4.1 で示したように、ドローンでは、ステークホルダによって取り扱うソフトウェアが異なり、セキュリティ対策を実施するフェーズも異なる為ステークホルダによって対応が異なる。特にドローンの場合は、フライトコントローラ等の部品で提供する場合もあり、5.1.3 で示す、ドローンの保護の主体の観点で、ソフトウェアサプライチェーンで管理することが必要となる。今後、ドローンメーカーは SBOM などを利用し、ソフトの脆弱性を管理し、必要があれば利用ユーザへセキュリティ情報を提供、または脆弱性対策されたファームウェアを提供することが必要となってくる。

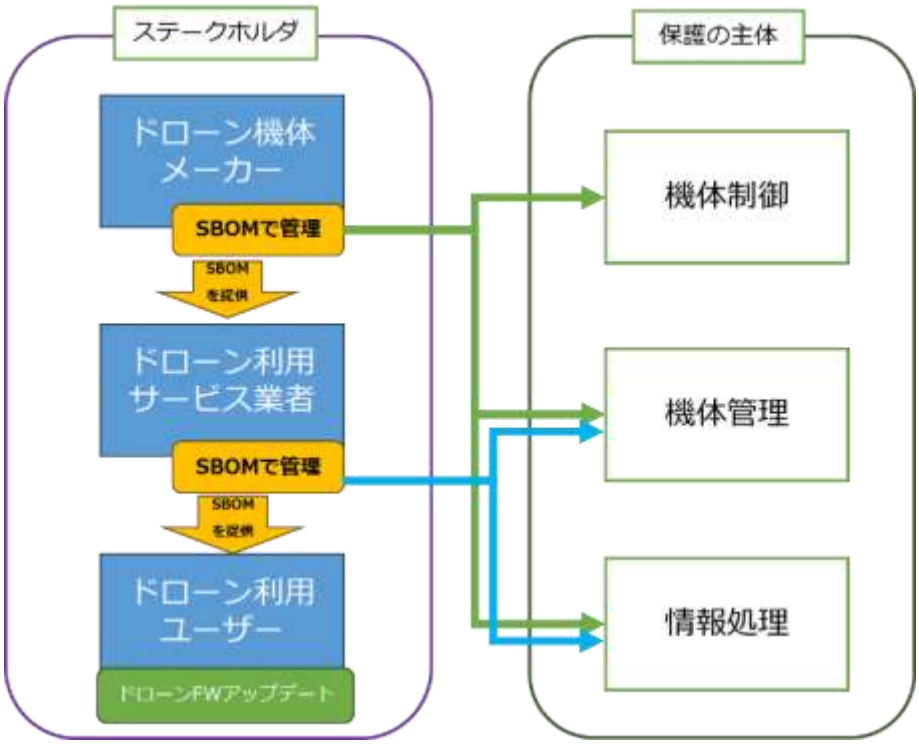


図 8：ドローンのソフトウェアサプライチェーン

4.7. ドローンに関連するサイバーセキュリティ国際規格

ドローンに関連する可能性のあるサイバーセキュリティ国際規格を以下に説明する。近年、IoT 機器などインターネットに接続する機器を中心にサイバーセキュリティ関連の法整備が加速してきている。（図 6、図 9 参照）特に EU においては法令が整備されつつ有り、EU へ輸出する可能性のあるドローンは考慮する必要がある。

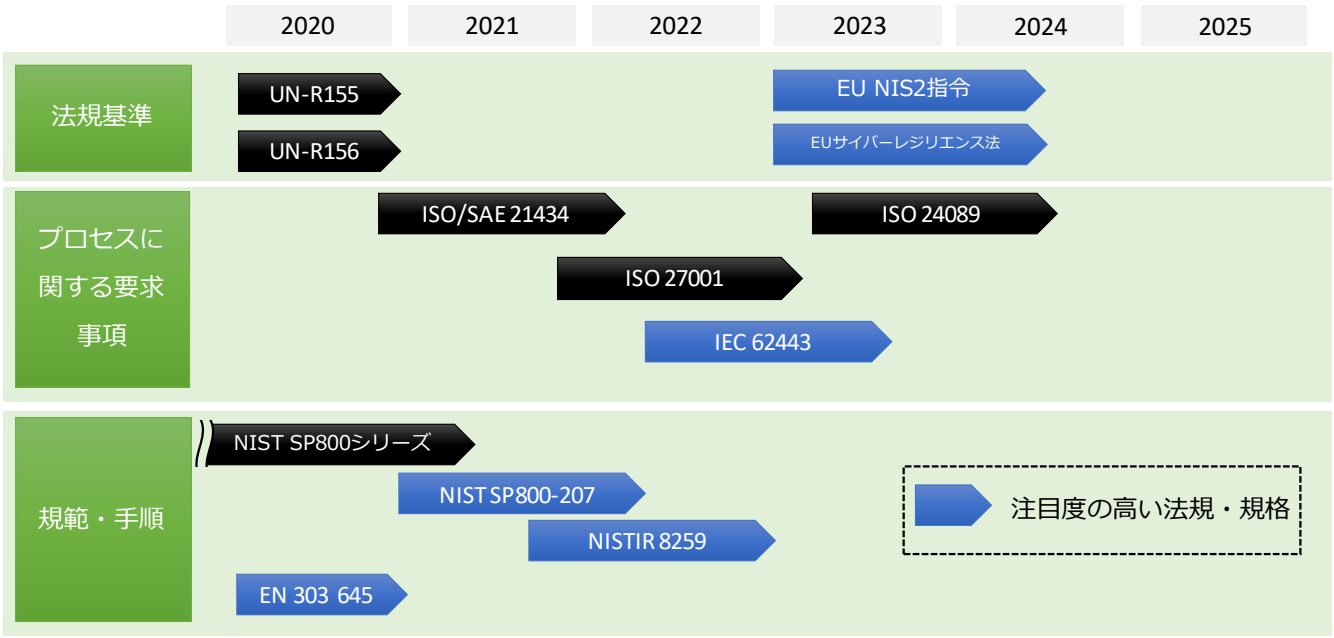


図 9：法規・標準仕様からみるサイバーセキュリティ規格動向

4.7.1. EU 無線機器指令（RED）

RED は、直接または間接的にインターネットに接続する無線製品が対象となっており、ドローンも対象となる。

機器のサイバーセキュリティ、個人情報、プライバシー保護が義務付けられている。

4.7.2. EU サイバーレジリエンス法(CRA)

サイバーレジリエンス法は、デジタル要素を備えた全ての製品が対象となり、ドローンも対象となる可能性が高い。

サイバーセキュリティを確保するよう設計・開発・生産されていること、速やかな脆弱性情報の公開、修正が求められる。

4.7.3. その他の国際規格

その他、各国のドローンに関連する可能性のあるサイバーセキュリティの規格や対応状況を下記に示す。

米国：

「IoT Cybersecurity Improvement Act of 2020」[9]

「NISTIR8259」

英国：

「Product Security and Telecommunications Infrastructure Act（PSTI 法)」[10]

日本：

IoT セキュリティガイドラインを複数発表（経済産業省、IPA）

その他：

ドイツ、シンガポール、フィンランドでは IoT 製品に対するセキュリティラベリング制度運用開始

[9] IoT Cybersecurity Improvement Act of 2020

https://www.congress.gov/bill/116th-congress/house-bill/1668

[10] Product Security and Telecommunications Infrastructure Act（PSTI 法）

https://bills.parliament.uk/bills/3069

5. リスクアセスメント

リスクアセスメントではドローンのユースケースに応じたセキュリティ要求を定義することが目的となる。

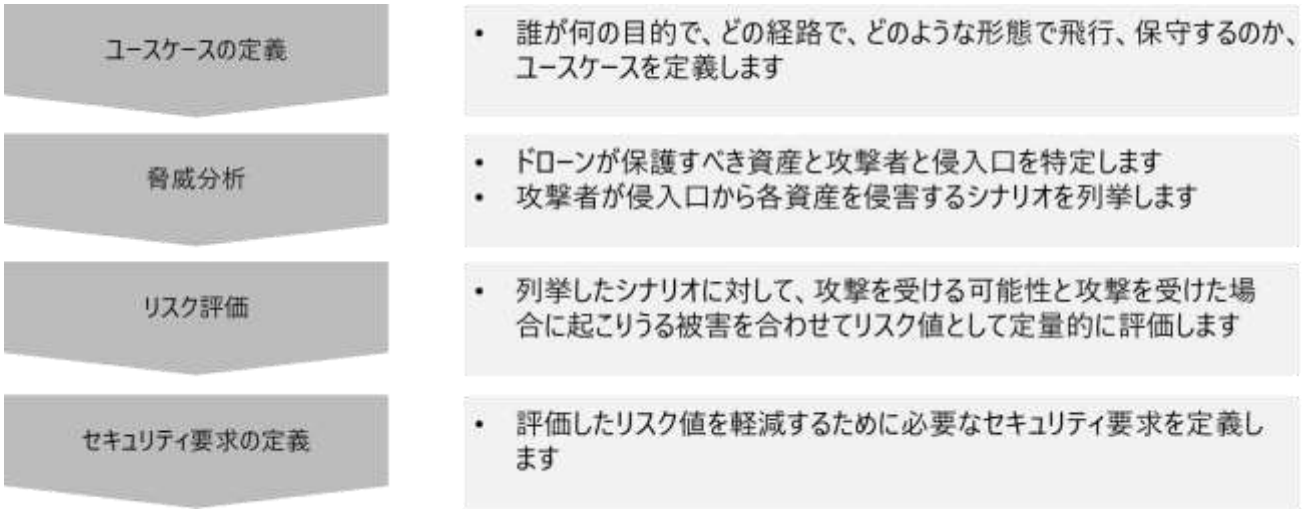


図 10：セキュリティ要求定義のステップ

5.1. ユースケースの定義

ドローンを誰が何の目的で、どのような方式で飛行するのか、ユースケースを定義する。次ステップの脅威分析のために、ステークホルダ、サービスのライフサイクル、保護の主体を明確にしておく。

5.1.1. ステークホルダ

ドローン開発に当たり複数のステークホルダが想定される。主なステークホルダを以下に示す。

（1） ドローン機体メーカー

ドローン機体を製造するメーカーを示す。

（2） ドローンサービス提供事業者

ドローン機体、通信キャリア、クラウドサービス等を統合して、ドローンを活用したサービスを提供するインテグレータを示す。

（3） ドローン活用ユーザ

ドローン機体を購入して使用する。あるいは、ドローンサービス提供事業者のサービスを利用するエンドユーザを示す。

具体的にはドローンを用いた農薬散布を行う農業従事者や鉄塔、橋梁等の点検を行うインフラ事業者等が該当する。

5.1.2. サービスのライフサイクル

ドローン事業のリスクは特に運用時が中心となるが、ドローン製造時、運用終了後のリスクも検討しておく。ステークホルダによって検討するライフサイクルは異なる。

ライフサイクル	製造時	運用終了後
リスク	ドローンとサーバー間の通信で利用する暗号、署名用の鍵が開発時に漏洩することで、将来ドローンが飛行中になりすまし攻撃を受ける可能性がある	売却、オーナーチェンジの際、前オーナーの情報や暗号鍵が漏洩する可能性がある
主な対策	工場側に HSM、ドローン側にセキュアマイコンを用いた鍵配送を行い、第 3 者への鍵の漏洩を防ぐ	リセット機能を搭載し、全てのストレージ上のデータを削除する

5.1.3. 保護の主体

ドローンのリスクアセスメントを行うにあたり、ドローンのどの構成部位に対してセキュリティ対策を実施すべきか、明確にするため、保護の主体を定義しておく。

（1） 機体制御

ドローン機体本体が該当する。主にドローンに搭載された機器（フライトコントローラー、センサーなど）のセキュリティ、通信のセキュリティ、機体制御のコードや高度な自律処理（衝突回避や SLAM など）のアプリケーションなどが含まれる。セキュリティ対策は基本的にドローン機体本体を製造するメーカーが担うことになる。

ドローン機体メーカーは、ドローン本体のハードウェアだけではなく、ソフトウェアにおけるセキュリティ機能における実装内容を記したホワイトペーパー（技術文書）を提供する必要がある。

ドローン機体メーカーは、本ガイドラインに記載する 6 セキュリティ要素技術を参考にセキュリティ機能を実装し、その対策内容をホワイトペーパー（技術文書）として機体を活用するユーザに提供もしくはウェブなどに公開することを推奨する。

（2） 機体管理

ドローン機体本体の外部機器が該当する。主にプロポの操縦者・機体間の認証などのセキュリティ、地上側のグランドコントロールステーションなどからのコマンド送信のセキュリティ、機体の状態や位置情報などのセキュリティ、目視外飛行におけるグランドコントロールなどのアプリケーションのセキュリティなどが含まれる。セキュリティ対策は基本的にドローン機体本体を製造するメーカーが担うことになるが、カスタマイズや専用用途化といったことについては、ドローンサービス提供事業者やドローン活用ユ

ーザが行う必要がある。

本ガイドラインに記載する Appendix 1 ドローン関連サービス、プロトタイプ開発事例を参考にセキュリティ機能を実装することを推奨する。

（3） 情報処理

ドローンに搭載された、映像・画像や各種センサーで取得したデータが該当する。これは、PC やスマートフォンなど今まで対策を講じてきた内容を応用できるケースが多い。例えば、カメラや各種センサーに搭載された SD カード内のデータの暗号化である。ドローン本体が紛失・盗難となった場合でも、データの不正利用を防ぐことができる。また、SIM の上空利用の制限が緩和されることで、データを扱うプロセスが変わってくる。これまでドローン自身がインターネットオフライン（常時インターネット非接続）であり、データをクラウドに送信する場合は SD カードに保存されたデータを PC やスマートフォンで行っていた。SIM の上空利用が可能となることで直接クラウドに各種データを送信することができるため、ドローンで取得する各種データのセキュリティ対策が必要となる。

セキュリティ対策は、ドローンサービス提供事業者やドローン活用ユーザが行う必要がある。本ガイドラインに記載する 6 セキュリティ要素技術を参考に実装することを推奨する。

5.2. 脅威分析

脅威分析ではドローン事業においてどのような資産が侵害を受けたら、どのような被害を受けるか、明確にしておく必要がある。最初のステップとして識別すべきリスクと、リスクを引き起こす資産を特定する。

5.2.1. ドローンのリスク管理

ドローンのリスク管理は、以下の要素に分類される。本ガイドラインが取り上げるリスクは主にセキュリティとセーフティとなるが、それ以外にも様々なリスクが存在する。

（1）法令順守（コンプライアンス）

関連する法令（航空法、道路交通法、民法などの関連法だけでなく、各業種業態に関連する法律）、また直接の法令ではないが、飛行地域の住民説明などが含まれる。

（2）トラブルに対するセーフティの確保

無線障害、GPS エラー、バッテリーエラーなど、ドローンを運用する際にはさまざまな

トラブルが想定されるが、その際のセーフティ確保の方法、優先順位などの策定が必要である。

（3）管理者・操縦者/機体の認証

人と機体の認証で、正しい人が正しい機体に紐づけられて使用しているかということだ。例えば、現状ではプロポ（ドローン操縦用のコントローラー）が盗まれた場合などには、その盗んだプロポでドローンが操縦できてしまう。対策としては、スマートフォンなどで使われているような指紋認証のような仕組みをプロポに搭載することなどが必要である。

（4）データ保護

前述のように、取得したデータや機体のデータなどの保護が必要となる。これは PC やスマートフォンで培われてきた技術やその管理の応用となり、その技術をドローンにも適用することが必要である。

（5）悪意ある第三者による攻撃

これはドローンを始めとするヴィークル型ロボット（自動走行車なども含む）に新たに生じている脅威である。特にマルチコプターの場合は空を飛行するということもあり、墜落を生じさせることによる機体の損害だけでなく、対人・対物への損害を及ぼすリスクがある。

（6）運用

リスクを最小化するための準備、確認事項、緊急時の対応など、リスク管理のためには運用も非常に重要な要素となるため、運用におけるルール策定が必要である。

（7）再発防止

トラブルが起こってしまった場合に、再発防止のためのステップが明確に規定されていることが重要だ。特に各種ログデータを初めとして、トラブルが起こった原因を検証することは必須である。

上記にあるようなドローンリスク管理体制を構築していくことが、事業者やユーザにとって重要になるが、一方で、完璧な対策を目指そうとするほど、コスト増となってしまい、ドローンを利用して解決したかった課題に対し、費用対効果が見合わなくなる。

よって、事業者はリスクベースド・アプローチを取り、リスクアセスメントを実施し、根拠を持った指標による管理策を実施することが望まれる。本書では ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 をベースラインとし、資産のリストアップ、リスクの事前検証、リスク分析／評価を実施することを推奨する。

5.2.2. 情報資産のリストアップ

事業者は、情報のライフサイクルに関連した資産を特定し、その重要度を文書化する。情報のライフサイクルには、作成、処理、保管、送信、削除及び破棄を含め。これらの文書を専用の目録、若しくは既存の目録に含める。

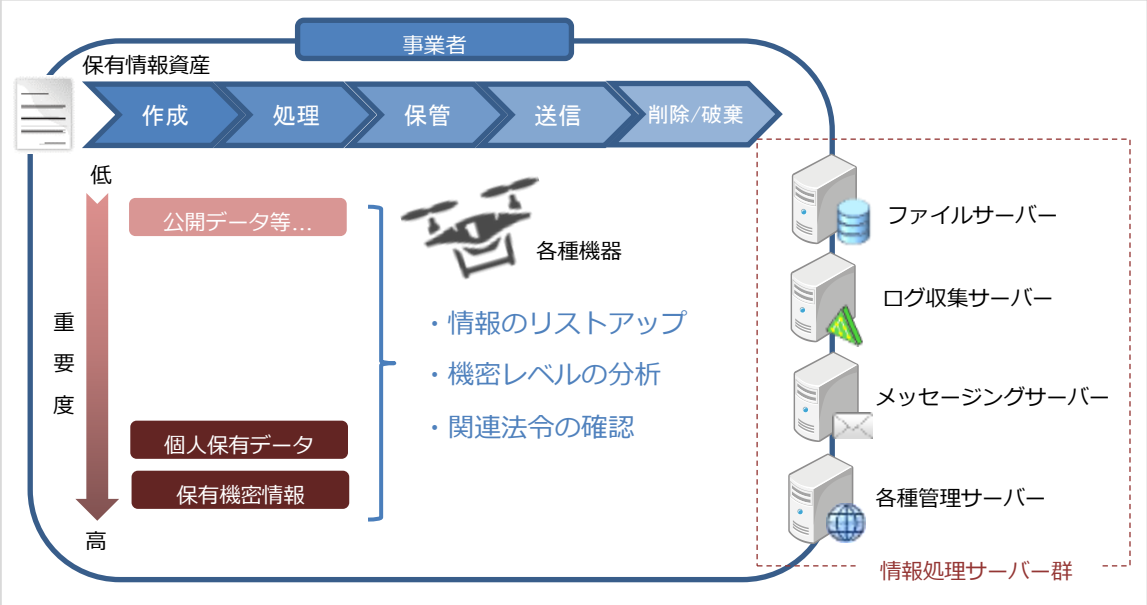


図 11：ドローンを活用する事業における保有情報資産と情報資産

A) 情報分類

事業者は飛行記録を始めとする各種情報を法的要求事項、価値、重要性、許可されていない開示・変更に対して取扱いに慎重を要する度合いに応じて分類を行う。これらの要求を実現するため、以下の要件を盛り込むこと。

（1） 情報分類は、事業上の要求及び法的要求事項を考慮すること。
（2） 情報分類における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価すること。
（3） 情報分類体系における、それぞれのレベルには、その分類体系を呼称するための、意味

をなすような名称を付けることが望ましい。

（４） 情報分類の結果は、ライフサイクルを通じた、情報の価値、取扱いに慎重を要する度合い及び重要性の変化に応じて、更新すること。

（５） 分類体系には、分類の規則及びその分類を時間が経ってからレビューするための基準を含めること。

（６） 情報資産の管理責任者は、その情報の分類に対して責任を負うこと。

B) 個人保有データのリストアップ

事業者はプライバシー及び個人を特定できる情報（PII）の保護は、関連する法令及び規則が適用される場合には、その要求に従って確実にしなければならない。これらの要求を実現するため、以下の要件を盛り込むこと。

（１） 資産目録に対して、保有する個人データの事項が必要範囲で限定（選定）され、正確、最新に保たれ、一貫性があり、他の目録と整合しているか。

（２） プライバシー及び PII の保護に関する事業者の方針を確立すること。

（３） 管理責任を明確にするため、プライバシー担当役員のような責任者を一名以上任命すること。

（４） 責任者は、管理者、利用者及びサービス提供者に対して、それぞれの責任及び従うことが望ましい特定の手順について、手引を提供すること。

（５） PII の取扱い、及びプライバシーの原則の認識を確実にすることについての責任は、関連する法令及び規則の準備状況を定めること。

（６） PII を保護するための適切な技術的及び組織的対策を実施すること。

C) 保有機密情報のリストアップ

情報資産の取扱いに関する手順は、事業者が採用した情報分類体系に従って策定し、実施しなければならない。情報分類に従って取り扱い、処理し、保管し、伝達するための手段を作成する。

また、関連子会社といった外部組織との情報共有を含む合意には、その情報の情報分類を特定し、その組織における情報分類を解釈するための手順を含める。これらの要求を実現するため、以下の要件を盛り込むこと。

（１） 各レベルの分類に応じた保護の要求事項に対応するアクセスを制限する。

（２） 契約者より情報資産が授与された場合、正式な記録を維持する。

（3） 情報の一時的または恒久的な複製は、情報の原本と同等のレベルで保護する。
（4） 情報資産が保存されるハードディスクドライブ等の情報記憶媒体は、製造業者の仕様に従って保管する。
（5） 情報をメディアにバックアップ等をした場合、複製であることを明確に示すため印をつけること。

D) 保有情報資産のリストアップ

情報のラベル付けに関する適切な一連の手順は、事業者が採用した情報分類体系に従って策定し実施する。本項は「B) 個人保有データのリストアップ」、「C) 保有機密情報のリストアップ」を実施する基本指針であり、個人情報および機密情報を含めた、関連する全ての情報資産のリストアップを目的としている。これらの要求を実現するため、以下の要件を盛り込むこと。

（1） 情報のラベル付けに関する手順は、物理的形式および電子的形式の情報及び関連する資産に適用すること。
（2） 媒体の種類に応じて、情報がどのようにアクセスされるかまたは資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を作成すること。
（3） 作業負荷を減らすために、ラベル付けを省略する場合（例えば、秘密でない情報のラベル付け）を定めること。

E) 資産の管理責任

情報資産台帳の中で維持される資産は、管理されなければならない。管理責任者はその資産の所有権をもっている必要はないが、資産のライフサイクル全体を管理する責任を与えられた個人またはエンティティである管理責任者を設置する必要がある。

(1) 資産の管理責任は時機を失せずに割り当てることを確実にするためのプロセスを、実施すること。
(2) 資産が生成された時点、または資産が事業者に移転された時点で、管理責任を割り当てられるプロセスとすること。
(3) 資産の管理責任者が、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負うことを定めること。

5.2.3. HW 資産のリストアップ

機能の完全性、可用性が喪失すると運行不能に支障を起こす HW 資産をリストアップする。下図はオープンソースのフライトコントローラを利用した場合におけるコンポーネント図であり、ドローンは様々なマイコンにより構成されていることがわかる。機体に応じて構成は異なるものの、黄色で表示された箇所はドローンを運航する上で重要なマイコンであり保護すべき資産である。

(1) プロポ、GCS からの制御命令により機体全体の制御を行うフライトコントローラ
(2) サーバーからの制御命令を処理するコンパニオンコンピュータ
(3) ハートビート信号等を定期的に送り機器の異常を検知する安全マイコン
(4) プロポや GCS からの命令を受信するレシーバー
(5) 通信の認証、暗号化を行う暗号鍵を格納するセキュアマイコン

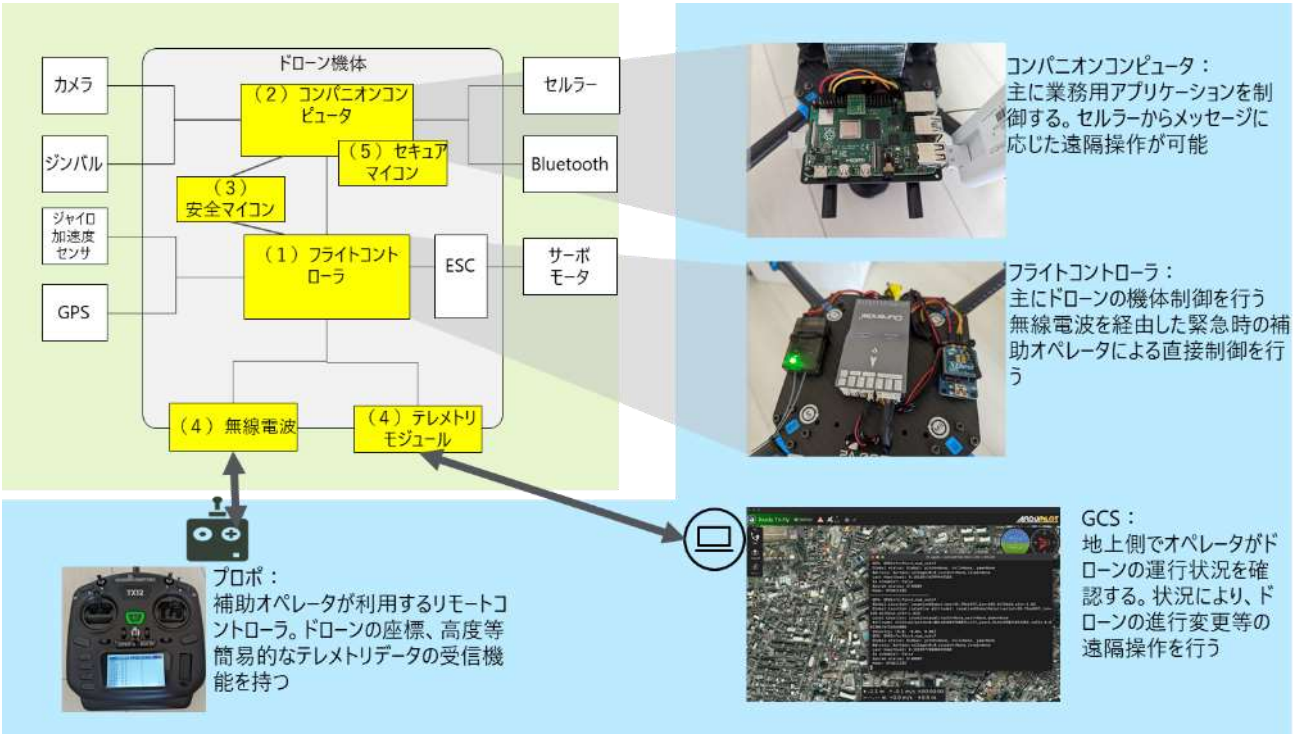


図 12：オープンソースドローンを構成するコンポーネント

5.2.4. 主な侵入口と攻撃主体

A) ドローンの一般的な接続形態

ドローンのリスクに関して、まずは接続手法の把握が重要である。

これまでは以下のようなドローンからプロポへの通信を通じて、テレメトリーなどの機体状態や取得データの情報がタブレットやスマートフォン、PC に入り、そこからクラウドに接続する手法（接続手法１）か、ドローンからプロポへの通信とドローンとタブレットやスマー

トフォン、PC への通信に分かれ、そのタブレットやスマートフォン、PC からテレメトリーなどの機体状態や取得データの情報がクラウドに接続する手法（接続手法２）が中心であった。

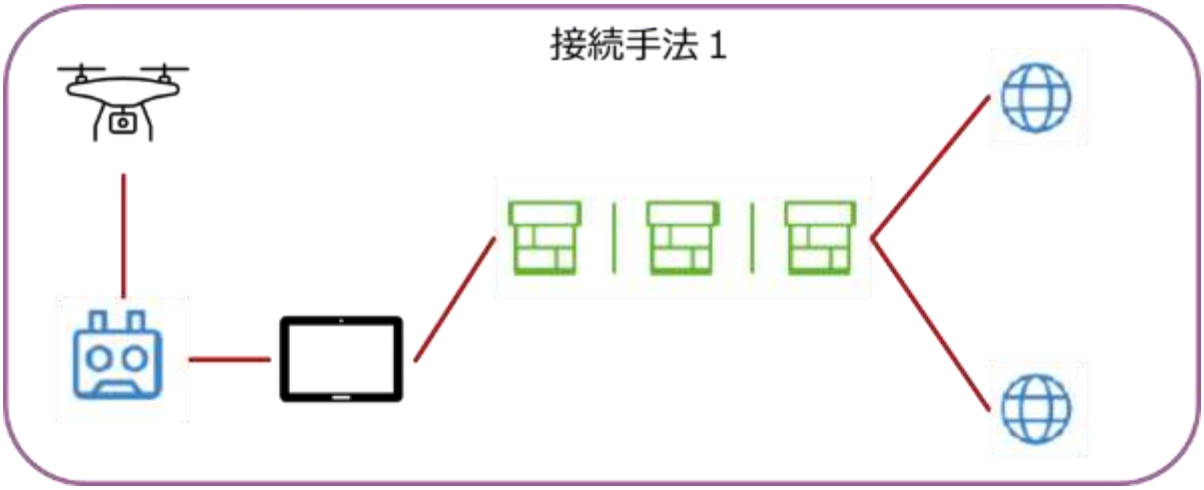


図 13：ドローンの接続手法 1

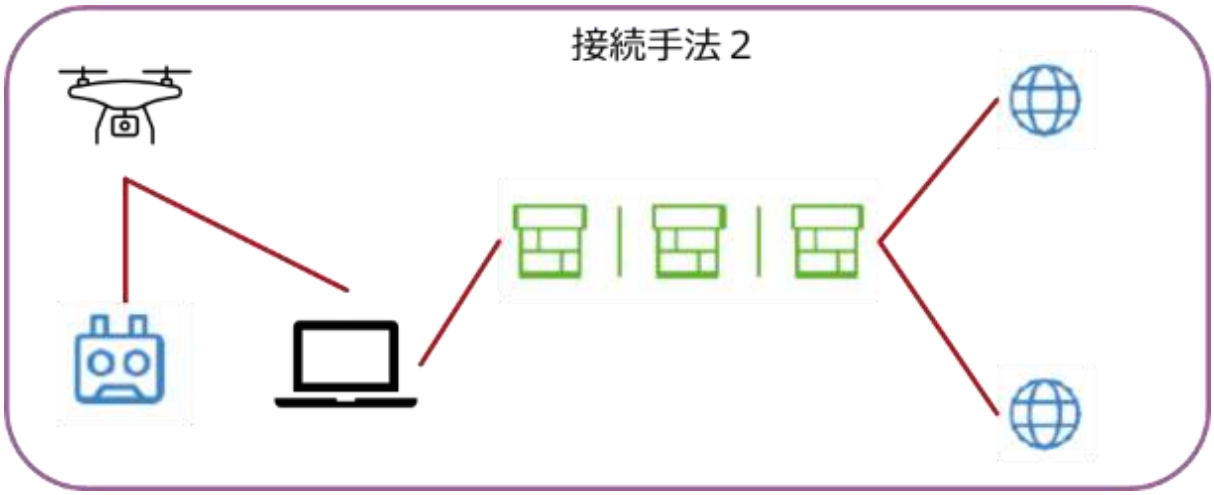


図 14：ドローンの接続手法 2

しかし、SIM などのモバイルネットワークをドローンに搭載可能な流れに応じて、接続手法１、２に加えて、直接ドローンからクラウドにテレメトリーなどの機体状態や取得データの情報を送るだけでなく、機体制御のコマンドをクラウドから直接ドローンに送る手法（接続手法３、接続手法４）が可能になった。

これはドローンの活用にとって、より幅を広げるかたちにはなっているが、ドローンがインターネットオンラインになるということで、そのリスクは高まっている。

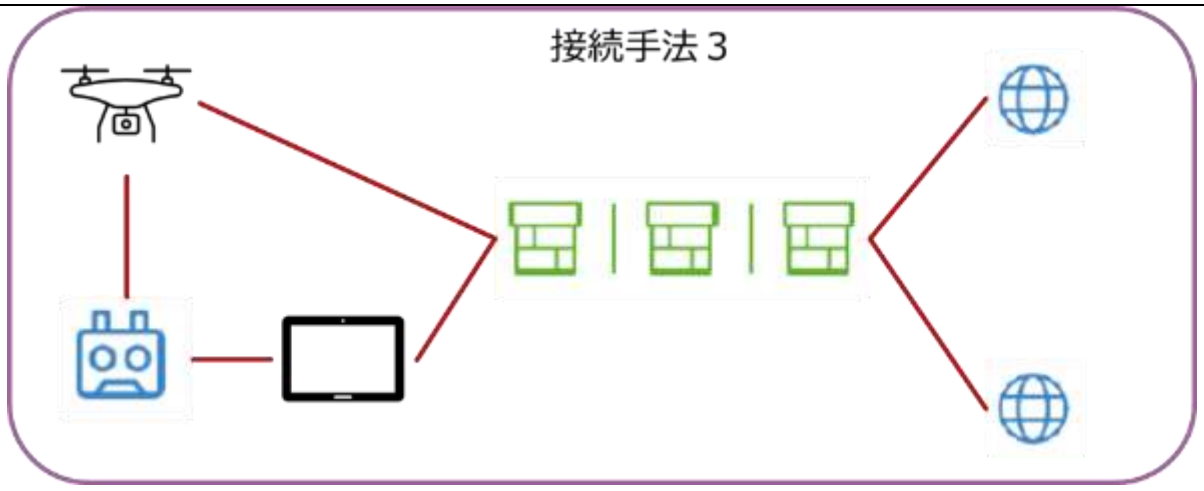


図 15：ドローンの接続手法 3

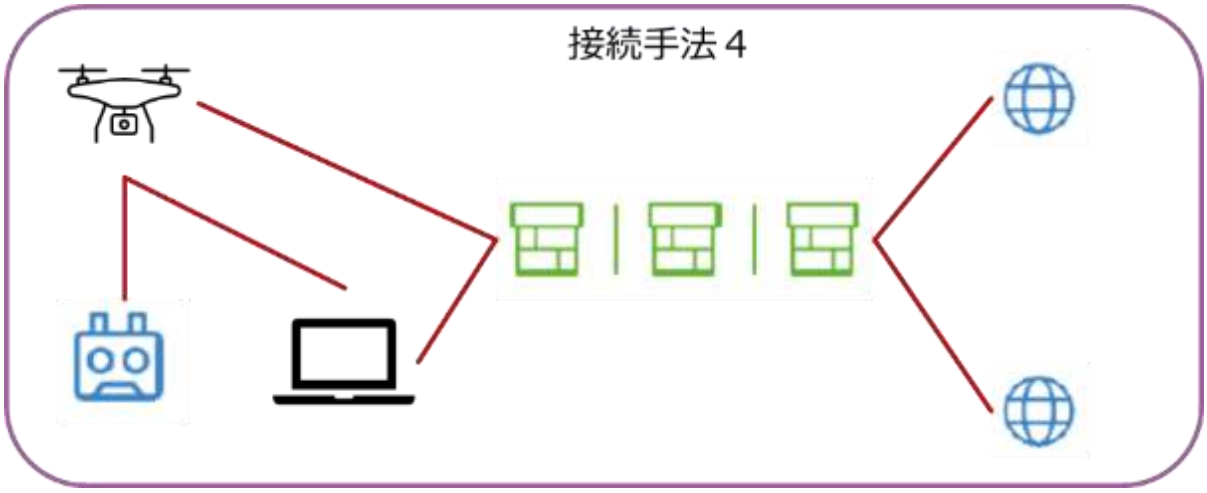


図 16：ドローンの接続手法 4

B) ドローンのリスクの侵入モデルと直接被害

ドローンのリスクを考えるにおいて、攻撃主体、侵入口、攻撃対象、それに伴う直接被害の把握が重要である。

攻撃主体としては、悪意ある第三者（現場）、悪意ある第三者（遠隔）、悪意ある内部者、不注意な内部者がある。

侵入口としては、無線、プロポ、Ground Control Station（GCS）制御端末、インターネット、USB メモリ、クラウド・サーバー、正規ログインがある。

攻撃対象としては、Flight Controller（FC）、コンパニオンコンピュータ、プロポ、PC、スマートフォン・タブレット、サーバーがある。

それにより、墜落、航路逸脱、業務中断、情報盗難、搬送物盗難、故障といった直接被害が

生じてくる。

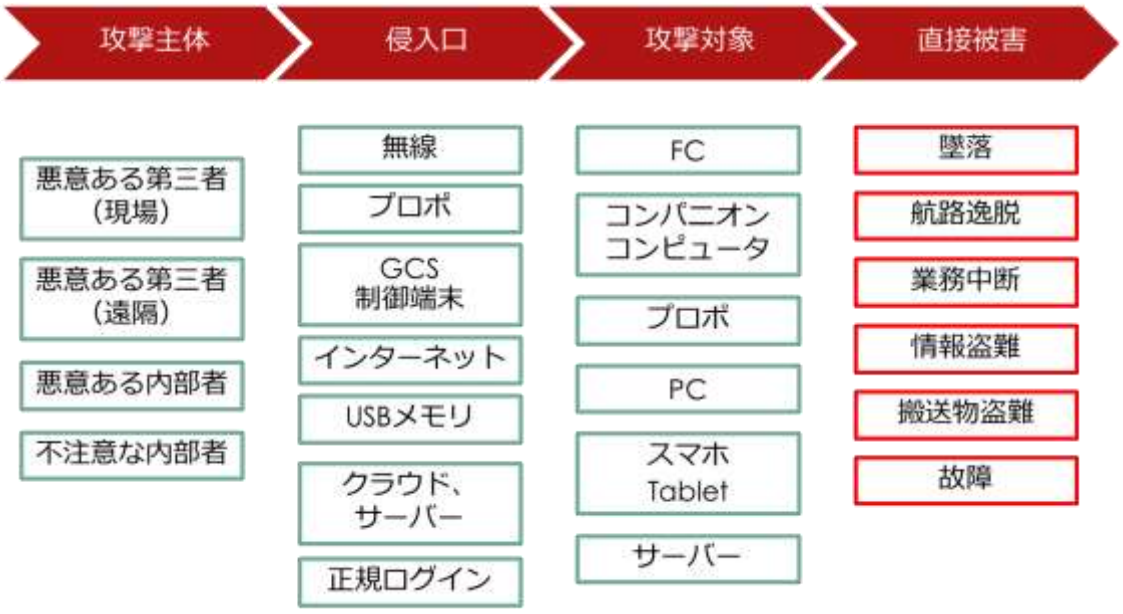


図 17：ドローンのリスクの侵入モデルと直接被害

(1) 攻撃主体

悪意ある第三者には、現場でのものと遠隔でのものがあり、その攻撃対象を具体的に決めているケースと大雑把に妨害を与えるケースがある。

悪意ある内部者には、正規ログイン、不正ログインのケースがある。また、故意のオペレーターのケースもある。

不注意な内部者が引き起こす内容は、ID 盗用、セキュリティ設定ミス、フェールセーフ設定ミス、外部・内部ガイドライン違反などがある。

(2) 侵入口

無線（プロポ－機体間）は現場で発生し、無線ハッキングや無線妨害がある。

プロポは現場で発生し、略奪や接続 ID の略奪がある。

Ground Control Station、機体制御・管理端末は現場でも遠隔で発生し、略奪やウィルスソフトウェア混入・マルウェア混入、遠隔ハッキングがある。

インターネットは現場でも遠隔でも発生し、ドローン本体（FC、コンパニオンコンピュータ、情報取得デバイス）、PC・スマホ・タブレット、サーバー・クラウドでの侵入可能性がある。

USB メモリは現場でも社内などの環境で発生し、ドローン本体、PC・スマホ・タブレット、サーバーでの侵入可能性がある。
クラウド、サーバーは社内などの環境や遠隔で発生し、機体管理、遠隔操作、データ盗難がある。
正規ログインでの侵入は、ID 盗難などに加えて、悪意ある内部者のケースもある。

(3) 攻撃方法

攻撃方法としては、略奪（プロポ、PC やタブレット・スマホ、機体（ドローン本体・SD カード）、ID／PW など）やセンサー妨害（IMU、コンパス、気圧計など）、電波妨害（機体－プロポ、機体－テレメトリー端末、機体－クラウド、テレメトリー端末－クラウドなど）、ハッキング（機体（FC、コンパニオンコンピュータ、ペイロード）、PC やタブレット・スマホ、サーバー、クラウドなど）、ウィルス・マルウェア混入（機体（FC、コンパニオンコンピュータ）、PC やタブレット・スマホ、サーバーなど）なりすまし（PC やタブレット・スマホ、サーバー、クラウドなど）がある。

上記に示した直接被害も勿論ではあるが、それに伴う企業や団体のリスクとしては、以下関連する法令の法令順守（コンプライアンス）、ブランドイメージ、機密データの漏えいなどの間接被害も甚大なものになる。

＊関連する法令（航空法、道路交通法、電波法、民法などの関連法だけでなく、各業種業態に関連する法律など）

5.3. リスク評価

侵入口と保護対象資産を列挙した後、各シナリオの起こりやすさと、起きた場合の損害をもとにリスク値として評価する。リスク値の大きさによって、リスクを回避（ユースケース自体を再考する等）するか、後述のセキュリティ要件で示す対策でリスクを軽減するか、あるいは許容するかの対策を行う。

5.3.1. 情報セキュリティリスク特性

2016 年 7 月 5 日に IoT 推進コンソーシアム　IoT セキュリティワーキンググループから「IoT セキュリティガイド」[11]が公表された。国民が安全で安心して暮らせる社会を実現するために必要

[11] IoT セキュリティガイド https://www.soumu.go.jp/main_content/000428393.pdf

な取組の検討が目的であり、本書にはドローンセキュリティにも共通する IoT 機器特有の性質を述べている。本項ではそれに倣いドローンにおいて対処すべき情報セキュリティリスクの特性とは何かを定める。

(1) 脅威の影響範囲・影響度合いが大きい

インターネットを介して接続される IoT 機器であればサービス全体へ脅威が波及する可能性が高くなる。ドローンについても移動通信システムや Wi-Fi によりインターネットへの接続が可能であり、データ漏えいも想定される。

(2) ライフサイクルが長い

構築・接続時には適用したセキュリティ対策であっても、時間経過によりセキュリティ対策は危殆化する。長期使用による物理的破損等は修復されていても、ファームウェア等がアップデートされない状態でネットワークに接続され続けることが想定される。

(3) 監視が行き届きにくい

自動航行する場合等は多くが人目による監視が行き届きにくく、利用者自身が問題を発見できない場合もある。管理されていないドローンが意図せずネットワークに接続し、マルウェアに感染することも想定される。

(4) 環境や特性の相互理解が不十分

ドローン本体とネットワーク、双方が有する業態の環境や特性が相互間で理解されていない状態でドローン本体がネットワークに接続することによって、所要の安全や性能を満たさない可能性も想定される。

(5) 機能・性能が限られている

センサー等のリソースが限られたドローンでは、暗号等のセキュリティ対策を適用できない場合も想定される。一般にインターネットを経由する接続であれば通信間の暗号強度を維持することが求められる。

(6) 開発者が想定していなかった接続が行われる可能性がある

例えば、これまで外部につながっていなかったシステムとドローンが連携するような場合、設計時には想定されていない負荷や脅威が顕著化することも想定される。

5.3.2. 情報セキュリティリスクの特定

ドローンは多目的に使用される機器であり、農業、配達、空撮と多彩である。それらのユースケースに応じてプラットフォームやネットワーク構成は変化し、潜在的な情報セキュリティリスクも変化すると考える。これらの潜在的な情報セキュリティリスクはユースケースを想定しながら、下記の要点に応じた情報資産のリストアップとリスクの想定を行う必要がある。

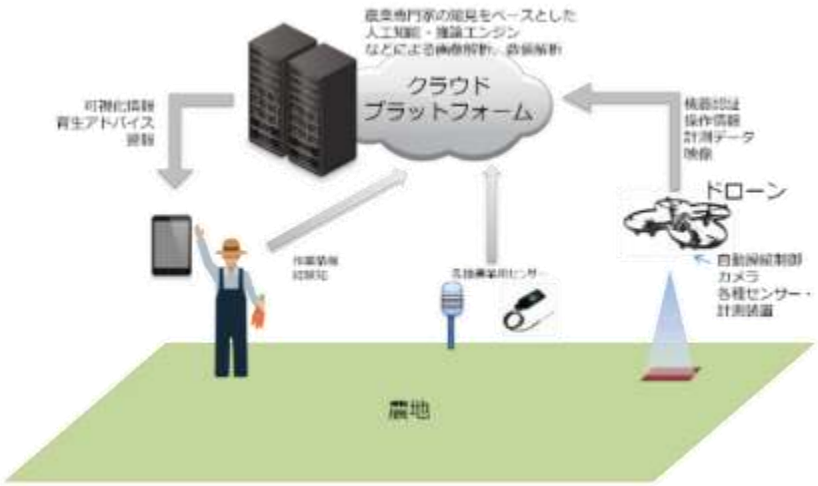


図 18：ドローンのユースケース

（8）守るべきものを特定する

- 外部からの攻撃や誤動作の影響を第三者に波及させないよう、ドローン及び周辺機器の守るべき機能、画像・動画等のデータ、機器認証情報等を特定する。

（9）つながることによるリスクを想定する

- クローズド・ネットワークがターゲットであっても、インターネットに接続される前提でリスクを想定する。
- 保守作業自体や保守用ツールの悪用によるリスクを想定する。

（１０）つながりで波及するリスクを想定する

- セキュリティ上の脅威や機器の故障の影響が、他の機器とつながることにより波及するリスクを想定する。
- 特に、対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。

（１１）物理的なリスクを認識する

- 盗難や紛失した機器の不正操作、管理者のいない場所での物理的な攻撃に対するリスクを想定する。
- 廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。

（１２）過去の事例に学ぶ

- パソコン等の ICT の過去事例から攻撃事例や対策事例を学ぶ。
- IoT の先行事例から攻撃事例や対策事例を学ぶ。

5.3.3. リスク分析

ここでは「5.3.2 情報セキュリティリスクの特定」により特定された情報セキュリティリスクを分析する。分析方法は一般的には最初に定性的な分析を採用し、リスクレベルの一般的兆候を得て重要リスクをリストアップする。重大リスクについては、より具体的な分析、定量的（根拠ある）分析を実施しなければならない。

（1） 「5.3.2 情報セキュリティリスクの特定」で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行うこと。

（2） 「5.3.2 情報セキュリティリスクの特定」で特定されたリスクの現実的な起こりやすさについてリスクアセスメントを行うこと。リスクアセスメントは情報資産にとって「発生しては困る事象（脅威）」と「固有の弱点（脆弱性）」を特定することから始める。

（3） 「資産価値」、「脅威」、「脆弱性」によりリスクレベルを決定すること。

5.3.4. 事業上起こり得る結果のアセスメント

資産目録に基づき、事業上の脅威、機密性（C）完全性（I）可用性（A）が損なわれた場合の事業継続影響度（損害）を評価する。主要な事業上の脅威・損害の評価は、保有する情報資産（顧客データやサービス提供の詳細）と組織をよく理解している情報の管理責任者によって行われなければならない。また、事業上の損害を判定する際に組織独自の判断基準を CIA それぞれの観点において明確にしなければならない。

この評価作業は、外部の専門家に支援を依頼し実施した方が客観性や効率性の確保の面から良い場合がある。下表に影響度の判断基準の例を示す。

表 2：機密性の評価基準例

資産価値	クラス	説明
1	公開	内容が漏えいした場合でも、ビジネスへの影響はほとんど無い
2	社外秘	内容が漏えいした場合、ビジネスへの影響は少ない
3	秘密	内容が漏えいした場合、ビジネスへの影響は大きい
4	極秘	内容が漏えいした場合、ビジネスへの影響は深刻かつ重大である

表 3：影響度の評価基準例

価値評価	影響度	金銭・機会損失（短期）	金銭・機会損失（中長期）	信用・ブランド損失
1	非常に小さい	当期経営にはほとんど影響はない	中長期的な経営には影響はない	ほとんど影響がない
2	小さい	当期経営に軽微な影響（当期利益の 1%以下を及ぼす）	中長期的な経営には影響はない	限定された人に対して悪い風評が及ぶ
3	中程度	当期経営に影響（当期利益の 3%以下）を及ぼす	中長期的な経営にはほとんど影響はない	多くの人に対して悪い風評が及ぶ
4	大きい	当期経営に重大な影響（当期利益の 10%未満）を及ぼす	2 年程度の経営に影響が及ぶ	限定された人に長期的に悪いイメージが残る
5	非常に大きい	当期経営に極めて重大な影響（当期利益の 10%以上）を及ぼす	3 年以上の経営に影響が及ぶ	多くの人に対し長期的に悪いイメージが残る

※ 例示では、評価レベルを 5 段階とし、3 つの視点から総合的に評価することを想定し、利益と信用を価値評価の中心としている。評価の視点は組織の重要な利害関係者（ステークホルダ）の利益に関連する視点にあわせるとよい。

5.3.5. 事業上の起こりやすさのアセスメント

保有する情報資産に対し事業上起こり得るセキュリティ障害等、現実的に発生する可能性を評価するために、認識されている脅威および脆弱性を評価する。脅威と脆弱性の評価は個別に行っても組み合わせて評価しても構わない。その際に資産に影響を及ぼす脅威や連動して起こりうる脅威などを事前に検証し、現在実施されている管理策から脆弱性を考慮する必要がある。

5.3.6. 脅威と脆弱性の評価 （数値化）

■ 脅威の評価

脅威の評価は、脅威の識別と同様にドローンを活用した事業と関連する他部門と協力して整理を行う。作成した脅威一覧に基づき、事業上の経験や過去に収集した統計的なデータに基づいて検討する。評価にどの程度の正確性を要求するか検討が必要となるが、一般的なインターネットを活用する事業を想定した、分類基準を下記に例示する。

表 4：脅威の分類基準例（1）

資産価値	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回である。

表 5：脅威の分類基準例（2）

レベル	意図的（計画的）脅威	偶発的脅威	環境的脅威
1	実施による利益はない	通常では発生しない	3 年以内に一度も発生しない
2	実施による利益はあまりない	特定の状況下での発生が考えられる	3 年に一度程度発生する
3	実施による利益は多少ある	専門能力のあるものの不注意で発生する	1 年に一度程度発生する
4	実施による利益がある	一般者の不注意で発生する	1 ヶ月に一度程度発生する
5	発生が具体的に予想される	通常の状態で発生する	1 ヶ月に一度以上発生する

■ 脆弱性の評価

脆弱性の評価は、該当資産の現在の実施対策を考慮したうえで、弱点を評価する。十分な管理策が実施されている場合は脆弱性が少なくなるが、管理策を実施してなく弱点が顕わである場合の脆弱性は高いと判断される。一般的なインターネットを活用する事業を想定した、分類基準を下記に例示する。

表 6：脆弱性の分類基準例

レベル	意図的（計画的）脅威に対する脆弱性	偶発的脅威に対する脆弱性	環境的脅威に対する脆弱性
1	最高程度の対策を実施済み	最高程度の対策を実施済み	最高程度の対策を実施済み
2	高度な専門知識や設備を持つ者によって可能な状況	通常の利用状況ではほとんどリスクが顕著化する恐れがない状況	通常の利用環境ではほとんどリスクが顕在化する恐れがない状況
3	専門能力を持つものによって可能な状況	専門能力がある者の不注意によりリスクが顕著化する恐れがある状況	専門能力がある者の不注意によりリスクが顕在化する恐れがある状況
4	一般者が調査を実施すれば可能な状況	一般者の不注意によりリスクが顕在化する恐れがある状況	一般者の不注意によりリスクが顕在化する恐れがある状況

5	一般者が普通に実施可能な状況	特段の対策を実施しておらず、いつリスクが顕著化してもおかしくない状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況

自らの組織において、もっとも適切な評価方法を確立することが重要である。評価方法の確立、評価実施にあたっては、外部支援の協力が有効となる場合がある。

5.3.7. リスクレベルの決定 （数値化）

リスクレベルは、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「脆弱性の度合い」を用いて、簡易的に次の様な計算式で算出する。

リスクレベル ＝ 「資産の価値」 × 「脅威」 × 「脆弱性」

表 7：リスクレベル早見表例

	脅威								
	1			2			3		
	脆弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	13	12	16	24	12	24	36

資産単位のリスクレベルについて、資産目録に合わせた算出・管理を行うことが迅速な判断ができて、効率的である。算出方法において外部専門家による第三者評価を受けることが有効といえる。

5.3.8. リスク評価

次によって情報セキュリティリスクを評価する。

（1） リスク分析の結果とリスク基準とを比較すること。

（2） リスク対応のために、分析したリスクの優先順位付けを行うこと。

5.3.9. 分析結果とリスク基準との比較

前項で分析し決定したリスクレベルについて、リスク基準と比較して評価する。リスク基準は経営陣が受容可能なリスクの水準として採取的に承認することになるものである。例えばリスク基準で受容可能レベルを「9」未満と決めた場合、リスク対応が必要となる情報資産と脆弱性の観点から以下の通りになる。

表 8：リスク受容一覧の例

	脅威								
	1			2			3		
	脆弱性								
資産の価値	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
1	1	2	3	2	4	6	3	6	A	9
2	2	4	6	4	8	12	6	12	I	18
3	3	6	9	6	12	18	9	18		27
4	4	8	13	12	16	24	12	24	C	36

このリスク受容一覧はあくまでリスク評価実施時のリスク環境を表すものであって、残留リスクについては管理検討が必要となる。資産の価値や脅威、脆弱性などの環境に変化が生じた場合は、適宜リスクレベルの見直しを実施し、リスク対応（受容、低減、共有、回避）判断を行い、管理策を決定しなければならない。

5.3.10. リスク対応の優先順位

リスクについては、リスク対応のための優先順位付けを行う。順位については一般にはリスクレベルの高いものから検討を行うが、対象とする情報資産を保有する組織およびリスク所有者の判断で行うものとする。また契約、法令および規制の要求事項が決定されたリスクに加えて考慮すべき要素となる。

5.4. セキュリティ要求の定義

5.4.1. セキュリティ要求の整理

セキュリティ要求を考える際、リスクの大きさと、技術と運用、セキュリティとセーフティとのバランスをとる必要がある。下図はドローンに対するセキュリティ要求を各 NIST CSF に当てはめた場合、本ガイドラインの該当項目をまとめた表である。

図 19：ドローンのセキュリティ要求

セキュリティ要求を整理する観点として以下の 3 つがある。

（1） 技術でカバーするのか運用手順でカバーするのか、自社のリソースに応じて適切に使い分ける

例えば、通信暗号化のない市販ドローンを市街地で利用する場合、なりすましによる不正操作される可能性があるため、不正操作に備え同地域にオペレーターを常時配備する等、運用でカバーできるか検討する。

（2） セキュリティ要求を CSF に分類し、偏りがないか確認する

技術的要求のみ注目するのではなく、攻撃が成立した場合に備え、インシデント対応策を用意するなど、攻守のバランスよく用意しておくことが重要である。検討したセキュリティ要求を NIST CSF（識別、検知、防御、対応、復旧）に整理することで偏りがないか確認することが有効である。

（3） セーフティ側のリスク低減策がサイバー攻撃をカバーしているか確認する

セーフティ対策はサイバー攻撃のリスク軽減策にもなりうる。

例えば、フライトコントローラ機能が喪失した場合、自動的に安全マイコンが検知し、パラシュートが開くというセーフティ対策を行ったとする。

この対策はフライトコントローラが DOS 攻撃を受けた場合は有効であるが、ドローンが不正操作を受けた場合はパラシュートが開かないため、全てのサイバー攻撃に対してリスクが軽減されるわけではない。

セーフティ対策とセキュリティ対策の漏れを防ぐためには、セーフティ機能が有効に

働くシナリオを想定し、それをサイバー攻撃によって起こすことができるか確認する作業が必要となる。

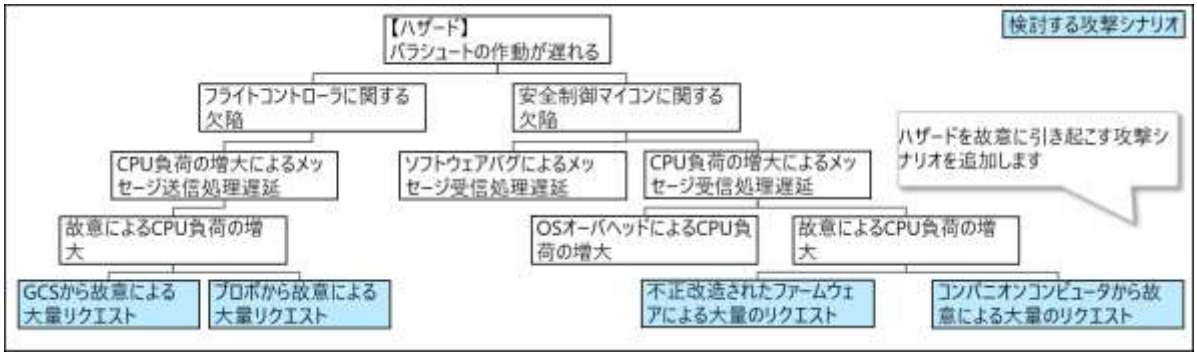


図 20：パラシュートが開かなくなる故障を起こすための確認方法の例

6. セキュリティ要素技術

ドローン本体のセキュリティ対策としては、セキュリティソリューション全体計画、フェールセーフ、運用管理・多重監視がある。

6.1. セキュリティソリューション全体計画

セキュリティソリューション全体計画は、ドローン機器（本体・プロポ）、アプリケーション、クラウドに分かれ、以下のような項目がある。

図 21：ドローンのセキュリティソリューション全体計画

6.1.1. ドローン機器のセキュリティ

- チップおよびハードウェアのセキュリティ
  - 搭載 CPU などのチップのセキュリティ技術の実装
    - ✓ ドローンのキー、証明書、 ID 等の機密情報を格納など。
  - セキュアエンジンおよびキー管理
    - ✓ ドローンのセキュア環境で動作し 、OTP（ワンタイムプログラマブル）領域のキーへのアクセスおよび使用が可能
  - 機体独自のシリアルナンバー
  - デバッグチャンネルの無効化

※ハードウェアのセキュリティ支援がない場合でも PKCS#12 などで鍵や証明書を暗号化、暗号化ファイルシステムを使用するなどでソフト的に対策することも可能。

- ファームウェアのセキュリティ
  - セキュアブート
    - ✓ ファームウェアの暗号化と電子署名を実施
    - ✓ ブートローダー、カーネル、セキュアオペレーティングシステム、飛行制御ファームウェア等で構成
  - パーティションの整合性の保護
    - ✓ ハッシュツリー構造によってシステムパーティション全体のデータをマッピング
  - セキュア OS の採用
    - ✓ システムのアクセス制御ポリシーが侵害されないようにプロセスやオペレーション、ファイル等のあらゆるリソースへのアクセスを制御
  - セキュアアップデート
    - ✓ マルウェアのドローンへのインストールとその実行を効果的に防止
- 機器のデータセキュリティ
  - システムログの暗号化
    - ✓ ドローンに保存されたシステムログにはシステムの実行情報が記録されるため、エクスポートされたシステムログを暗号化することにより、攻撃者がシステムを理解するのが困難になり、セキュリティが向上
  - 機体のパスワード保護
    - ✓ ドローンのメディアデータと機体を、パスワードや認証で保護
    - ✓ パスワードや証明書の流出に備えて、変更もできること

＊データの種類と詳細

フライトログ（データフラッシュログ）

説明：飛行中のセンサーのデータ情報、飛行操作ログなど

保存場所：機体内部のストレージ

ライブフライトステータス（テレメトリーログ）

説明：機在の高度、緯度および経度、電圧等の飛行中のドローンの環境情報およびリアルタイム情報

保存場所：GCS 内のストレージ（GCS 接続時）

システムログ

説明：システムのバグを発見し、解決するため、ドローンの操作中にシステムログが生成

保存場所：機体内部のストレージ

メディアデータ（オンボード）

説明：ユーザが撮影した写真または動画

保存場所：機体内部のストレージ

メディアデータ（SD カードまたは SSD）

説明：ユーザが撮影した写真または動画

保存場所：SD または SSD

アップデートパッケージ

説明：ドローンシステムのファームウェア

保存場所：機体内部のストレージ

6.1.2. 通信のセキュリティ

- 伝送システムのセキュリティ
  - セキュリティ機能を搭載したプロトコルの採用
    （例）AES アルゴリズムによって制御リンクが暗号化され、ドローンの電源を入れるたびに真性乱数生成器で暗号用のセッションキーが生成され、毎回独自の暗号化キーを使用
  - セキュアキーのネゴシエーションバインド方式や通信暗号化といった技術により、通信ハイジャックや中間者攻撃、リプレイ攻撃、通信傍受からユーザを効果的に保護
- Wi-Fi 通信のセキュリティ
  - 世界標準の無線 LAN プロトコルが用いられ、これは WPA2 PSK や WPA3 暗号化方式に対応
    （例）カスタム Wi-Fi プロトコルで、暗号化に物理層保護が追加

6.1.3. PC、タブレット端末、スマートフォンのセキュリティ

- PC、タブレット・スマホのセキュリティの対応
  - 認証
  - パスワード
  - PIN
  - バイオメトリクス認証
  - 二段階認証／多要素認証
- セキュリティ更新
- アンチウィルスソフト、マルウェア対策ソフト

6.1.4. アプリケーションのセキュリティ

- アプリケーションのセキュア設計・開発
- アプリケーションの脆弱性診断
- アプリケーションの堅牢性

1） Android アプリの堅牢性

- 逆コンパイル対策
  - ✓ コードを難読化し、圧縮することにより、攻撃者はコードを逆コンパイルしてデータの処理手順を理解することができなくなる（通信ロジック、暗号化ロジック、機体操作ロジック）

- 動的ライブラリの暗号化保護
  - ✓ アセンブリコードの圧縮および暗号化保護、動的ライブラリの実行可能ファイル（ ELF ）情報保護、動的ライブラリの暗号化、解読後の動的なコードのクリアランス
  - ✓ 動的ランタイムの保護
  - ✓ ローカルリソースの保護
  - ✓ 整合性の保護
- 仮想マシン保護
  - ✓ 仮想マシン保護技術を使いアプリケーションを保護し、リバースエンジニアリングを困難にする

2） iOS アプリの堅牢性

- コードロジックの難読化
  - ✓ アプリ開発プロセスにおいて、冗長なデータ処理手順等を追加
- リバース解析の実行の困難化
  - ✓ グローバルポイントを経由して機密データを取得、またはクリティカルメソッドをコール
- 機密コマンド保護
  - ✓ 機体と通信する基幹モジュールに対する保護
- ホワイトボックス暗号の適用
  - ✓ アプリ（ユーザーセンター、飛行制限、飛行記録等）で使用されるキーおよびログイン認証情報に対する暗号

6.1.5. クラウドのセキュリティ

- ユーザアカウントのセキュリティ
  - アカウントセンターのリスク管理システム
    - ✓ 異常なログイン、衝突攻撃、悪意ある登録等、悪意のある行為を検出
  - トラフィックの制限
    - ✓ 大量の悪意あるリクエストを防止するため、ユーザーセンターではトラフィックの制限を行い、悪意ある IP をブラックリストに登録
  - ユーザ情報の暗号化
    - ✓ データベース上の重要なユーザ情報を暗号化し、ネットワークトラフィックを HTTPS で暗号化
- サーバーのセキュリティ
  - ホストのセキュリティ
  - インターネットアプリケーションのセキュリティ
    - ✓ 定期的に徹底的なペネトレーションテストと静的コード脆弱性解析を実施
    - ✓ ドローンに関連するアプリケーションのコードについては、セキュリティ専門家が厳格な監査を実施
  - オペレーションのセキュリティ
    - ✓ クラウドサービスによって推奨されているリソース管理および認証管理のベストプラクティスを実施
    - ✓ サーバーエンドにおけるオペレーションは、厳格な標準作業手順書（SOP）によって制限
- クラウドサービスとデータセキュリティ
  - 個人情報の暗号化
    - ✓ 氏名や電子メール、位置情報、飛行記録といった個人情報は、AES 256 CBC などを使用して暗号化
  - 手法
    - ✓ ブラウザとサーバーのデータ通信には TLS1.2／1.3 プロトコルを使用
    - ✓ モバイルアプリとサーバーのデータ通信には TLS1.2／1.3 を使用
    - ✓ クラウドの多層セキュリティ保護（一般的なクラウドサービスで実装）

6.2. 技術対策

6.2.1. 認証

A） 操縦者・管理者の認証（人の認証）

ドローン本体の飛行・操縦にあたっては、プロポなどを使用するが、操縦者・管理者（人）を認証するための仕組みが存在しない。所有者や認証された人のみが使用できる仕組みを実装することにより、操縦者・管理者のなりすまし防止などの対策を行うことができる。さらに、ドローンの業務活用にあたっては、操縦者・管理者を認証する仕組みとして、スマートフォンや PC で実装されている ID/パスワードでの認証技術の実装に加え、より強度の高い、生体認証や電子証明書などを利用したセキュアな認証技術の実装が必要である。

B） 機体とプロポの認証

ドローン本体とプロポ間の通信は、基本的に Wi-Fi で通信されており、SSID とパスワードのみで接続されている。ドローン利用にあたっては、工場出荷時の SSID、パスワードが利用されているケースが多く見受けられる。これは、Wi-Fi ルータや Web カメラ、監視カメラで課題となっているケースと同様で、デフォルトの設定で利用することは、セキュリティリスクが高いと言えるため、最低限、設定を変更して使用することが望ましい。また、ドローン本体とプロポもしくは PC、スマートフォン間の通信には暗号強度の低い技術が使用されているため、セッションハイジャック（乗っ取り）の危険性がある。操縦者・管理者（人）の認証同様、ドローン本体とプロポ間の認証には、生体認証や電子証明書などを利用したセキュアな認証技術の実装が必要である。

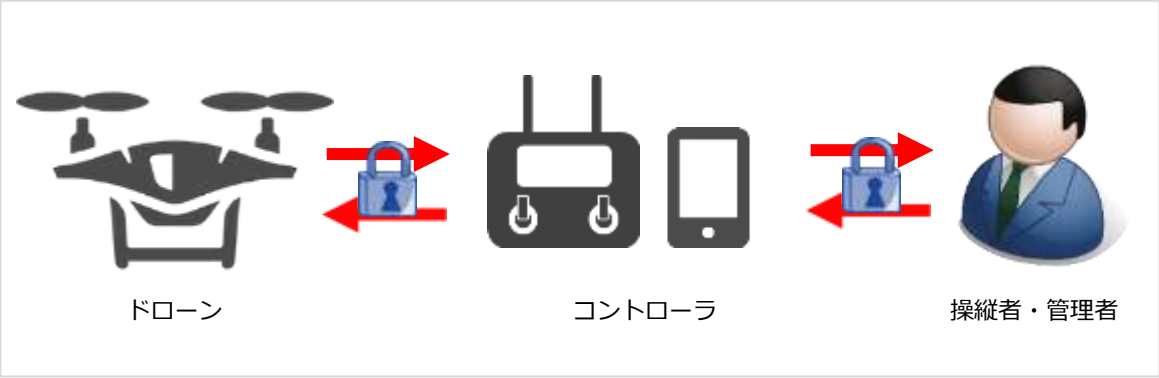


図 22：機体とプロポの認証

C） クラウドを使用したドローンの認証

ドローンの管理を AWS などのクラウドサービスを用いて管理する場合、ユーザ-クラウド間、クラウド-ドローン間の認証を考える必要がある。クラウドで管理をする場合、不特定多数のユーザやドローンを管理しているクラウドに対してアクセス対象となるため、セキュリティリスクとし

ては下記が考えられる。

- 悪意ある第三者にドローンの制御権を与えてしまう乗っ取り
- 意図しないドローンに機密情報を与えてしまう
- クラウド内に格納している機密データを盗まれる

上記のようなリスクを防ぐためには、アクセス要求者が意図したユーザであるか、通信を行うドローンが適切かどうかを認証する必要がある。

この認証方法の 1 つとして、クライアント証明書など証明書を用いた認証方式がある。この方式を採用した際には証明書を含めたドローンの管理や、証明書とペアの秘密鍵が盗まれてしまった場合の対策(証明書の失効、失効後の再発行)も考慮する必要がある。

D） ドローン操縦者認証のシステム例

ドローン操縦者の個人認証と飛行情報を可視化する認証システムの一例として、自動車を運転するドライバーズ認証の応用がある。ドライバーズ認証では、ドライバー本人を特定したうえで、自動車の車載コンピューター（ECU）から得られる運転中の情報をログとして記録する。そしてドライバーの運転傾向を時系列で正確に可視化することで、安全な運転走行や車と社会の抱える多様な課題解決に役立てる。同認証システムでは、ドライバー個人の生体認証を行った後に、乗車した車のエンジンがかけられる。ドローンの場合には、操縦者を生体認証することで、プロポから信号を送信できるようにする、といった対応が考えられる。

また、ドライバーズ認証では、目的地までそのドライバーがハンドルを握っていたことを証明する。あわせてドライバーの運転傾向もリアルタイムにクラウドへアップする。記録されたログは、ビッグデータとして集積され、安全運転の支援や危険運転防止、盗難予防、カーシェアリングの効率的運用など、さまざまな用途に役立てられる。同様の仕組みをドローンの飛行ログに応用することにより、リアルタイムにフライト経路の記録ができる。

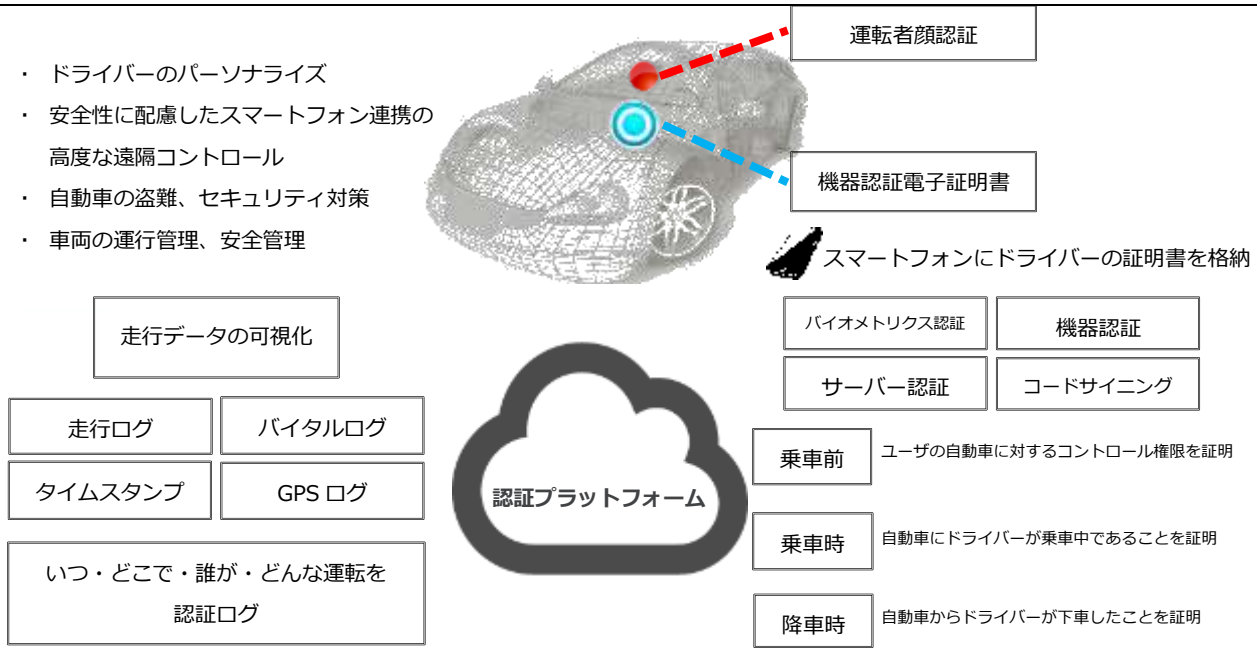


図 23：ドライバーズ認証のシステム例

E） 生体認証によるドローンの飛行認証システム例

ドライバーズ認証の例をドローンに応用すると、次のような飛行認証システムが実現できる。まず、プロポで「指紋認証」を行い、操縦者が登録されているオーナーであるかを認証し、承認されるとドローンが始動できる。さらに、顔認証を組み合わせることで、操縦中のオーナーの操作権限とドローンの端末識別用の電子証明書で認証され、「誰が」「どのドローンを操作しているか」を証明した後に、飛行を開始できる。

そして飛行時には、常時顔認証が行われ、操縦者が本人であることを認証する。「いつ」「どこからどこまで」「何時から何時まで」「どこを」「どのように」飛行したのかを、GPS の位置情報やプロポの操作ログ、時刻情報などで記録する。さらに要件によっては、操縦者の健康状態をモニタリングするモジュール、Healthcare のバイタルセンサを組み合わせて、飛行操作中の体調の変化なども記録できる。

収集されたデータは SSL により暗号化された状態でリアルタイムにクラウド上のサーバーへアップし、個々の操縦者の飛行傾向や事故リスクなどの分析に役立てる。操縦者の個人情報は、端末認証サービスや公開鍵基盤（PKI）に SSL サーバー証明書などを組み合わせて、最高レベルのセキュリティ技術で強固に保護できる。

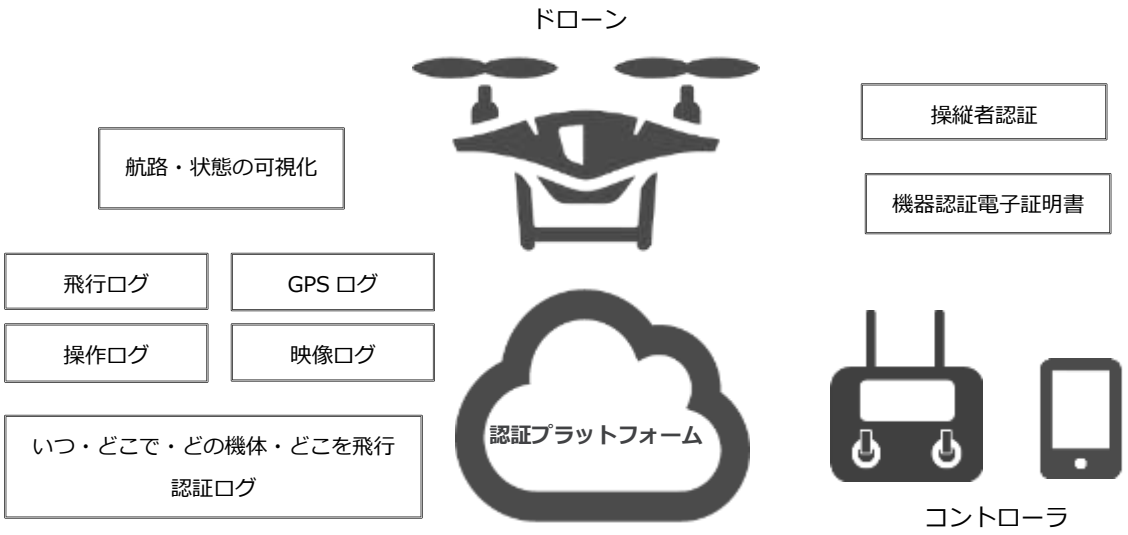


図 24：生体認証によるドローンの飛行認証システム例

F） 自動航行におけるドローンの飛行認証システム例

将来的に、産業用ドローンの飛行は人手による操縦ではなく、運航システムと連動した自動航行が中心になる。ドローンが制御信号で自律飛行をするようになると、個々のドローンの機体認証や制御信号の安全な通信が必要になる。目視外を超えて、ソフトウェアの制御によりドローンが自動航行するようになると、新たなセキュリティのリスクも発生する。この課題を解決するための取り組みとして、スマートフォンなどで利用されている通信用の SIM を使用して、4G 通信回線によるリアルタイムでのドローン追跡技術の研究開発も進んでいる。無線測位システム(RPS)と呼ばれる SIM 追尾システムは、レーダーなどで追跡できないドローンでも、最大 50 メートルの精度で機体をリアルタイムでトレースできる。RPS のようなドローン間の追尾システムと SIM や個々のドローンに埋め込まれた証明書などを活用して、自動航行における機体の認証システムも、近い将来は必要になる。

6.2.2. データの保護

A） データの管理・保管

ドローン本体に搭載したカメラのデータは、SD カード等のメディアに保存される。この保存されたデータのメディアの管理・保管については注意を払う必要がある。特に測量、橋梁・構造物・太陽光パネル検査、リモートセンシングなど業務活用にあたっては、データや保存メディアの管理・保管については注意が必要である。また、クラウドサービスの利用

にあたって保存、利用する際は、ID/パスワード以外のセキュアな認証技術を利用し、不正アクセス等の対策が必要である。

また、今後 LTE や 5G を利用し、直接クラウドサービスにデータを転送することも考えられる。クラウドサービス側でドローン本体を認証するための、仕組みが確立されておらず、認証にあたっては、電子証明書などを使用したセキュアな認証技術の実装が必要である。

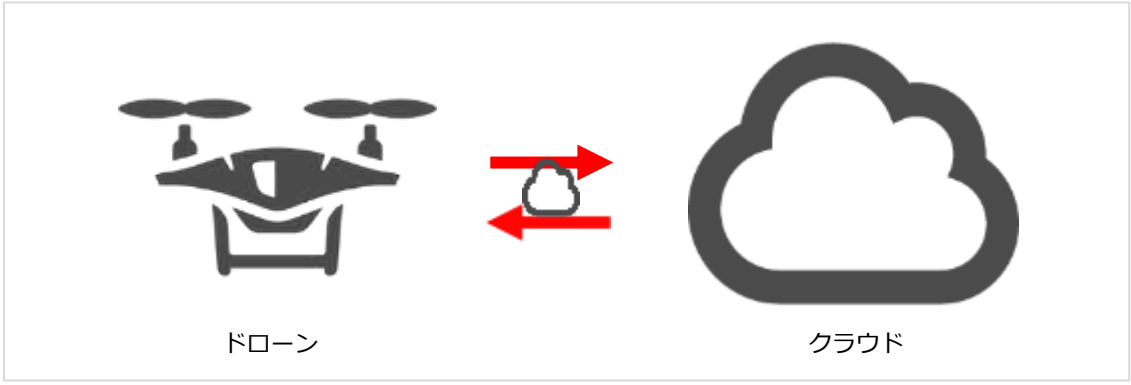


図 25：ドローンのデータの管理例

B） 保護の対象となるデータ

- ドローンに保存するデータ

  ドローンのカメラやセンサーで撮影された画像や動画ファイルは、基本的には PC などで読み書きできるデータ形式となっている。そのため、ドローンやカメラ側で何らかのセキュリティ対策が施されていない場合には、SD カードなどに記録されたデータは、誰でも容易に読み取ることができる。ドローンやカメラにファイルの暗号化機能が備えられていない場合には、機体やカメラの盗難はデータの漏えいに直結する危険がある。こうしたリスクを未然に防ぐ方法として、暗号化機能を備えた SD カード(例、東芝の Mamolica など)[12]をデジタルカメラで利用する対策がある。

- PC にコピーしたデータの保護

  ドローン本体や SD カードから各種のファイルを PC に転送する場合には、PC 側に何らかのデータ保護対策を施しておく必要がある。例えば、Windows には BitLocker という記憶デバイスの暗号化機能がある。BitLocker を利用すると、ディスク全体や特定の領域を暗号化して、そこにコピーされたデータはパスワードを入力しなければ利用できなくなる。Windows や BitLocker が利用できない PC では、利用している OS

[12] 参考サイト:Mamolica http://special.nikkeibp.co.jp/atclh/TEC/17/toshiba0828/

に対応したファイルの暗号化ツールなどを利用して、コピーしたデータを安全に保護する必要がある。例えば、Mac OS X では、FileVault というセキュリティ機能を使って、フォルダまたはディスク全体を暗号化できる。また、ZIP などのファイル圧縮ツールでも、パスワードを付けて保存できるので、第三者にファイルを受け渡しする場合には、データの保護に活用できる。

- クラウドにアップロードするデータの保護

  PC に保存されたデータをクラウドにアップロードする場合には、セキュアな通信プロトコルを利用する必要がある。インターネットでホームページを閲覧する代表的なプロトコルとして、URL が http://からはじまる Hyper Text Transfer Protocol と、https://からはじまる Hypertext Transfer Protocol Secure がある。現在は、多くのサイトが通信内容を暗号化してやり取りする HTTPS を利用している。しかし、中には HTTP のままでファイルのアップロードに対応するサイトもある。こうした HTTP のままのサイトの利用は、アップロード時にデータをハッキングされる危険性が高まる。また、HTTPS に対応しているサイトであっても、正規の運用サイトであるかどうか、認証が正しいかどうかを確認して、フィッシング詐欺などに騙されないようにする運用面での配慮も必要になる

- テレメトリーデータの保護

  将来的に、飛行中のドローンから各種のデータを収集して通信回線を使いリアルタイムでデータを交換するようになると、通信データを保護する仕組みも必要になる。現在のスマートフォンなどで利用されている LTE ネットワークは、無線区間は強固な暗号化により、鍵が盗まれなければデータが漏えいする危険性はない。しかし、基地局の背後の有線ネットワークなどに脆弱性があれば、データが流出する懸念もある。そのため、通信回線の信頼性だけにデータの保護を委ねること無く、将来的にはドローンから発信されるテレメトリーデータも認証システムと暗号化を用いて、安全に保護していく取り組みが求められる。

- ドローンの保護データの考え方

  今後ドローンを使用したサービスを展開するにあたって、具体的にどのようなデータが保護対象となるか、また保護データに該当するかを判断する分析方法についても考慮していく必要がある。

  - 保護データ分析具体例(TARA)[13]

    自動車の脅威分析で使用される分析方法として TARA を使用した分析方法があ

[13] ISO/SAE 21434 Road vehicles-Cybersecurity engineering

る。これは洗い出した情報資産を「安全性」、「金銭的」、「運用」、「プライバシー」の損害に対する評価を 4 段階で実施し、システム構成なども踏まえて各情報資産に対して保護対策が必要かを判断する分析方法である。

表 9：「安全性」に関する評価例

評価	評価基準
深刻	S3：生命を脅かす侵害(生存不確実)
重大	S2：重度及び生命を脅かす侵害(生存可能性あり)
中程度	S1：軽度及び中程度の侵害
無視できる	S0：侵害なし

レベル４（人口集中地域、目視外飛行）の解禁に伴い、ドローンでもより自動車の脅威分析のような精度の高い分析を実施することが求められる。

- 具体的なデータ保護対策(運送業利用時の顧客住所)

  運送業において、ドローンを用いた配送を行う際のデータ保護対策について、この時ドローンは配送先の位置情報を持っているため、この情報が洩れると顧客(配送先住所)のプライバシーが侵害されてしまう。これを防ぐ対策として顧客住所の暗号化などがある。
- 具体的なデータ保護対策(農業利用時の作物の画像データ)

  農業において、ドローンを用いた作物の成長確認を行う際のデータ保護対策について、この時ドローンは作物の画像データを持っているため、この情報が洩れることによって、収穫時期を迎えた作物の盗難が考えられる。ここではドローン内の作物の画像データの保護だけではなく、ドローンからクラウドなどに画像データを送る際の通信経路の保護(HTTPS 通信といった暗号化など)も必要となる。

6.2.3. 発行元証明

ドローン機器、またはドローンが扱うデータの発行証明の仕組みとして、電子署名やｅシールなどの仕組みがある。電子署名、ｅシール共にデータの起源と完全性を保証する為に電子データに付与されるか、又は論理的に関係している電子形式のデータをいう。電子署名との違いは、電子署名は個人に紐づくが、ｅシールは組織に紐づくものであり、ドローンのファームウェアの発行元証明や、ドローンがクラウドへ送るデータ、取得するデータの証明に使用することが可能となる。ｅシールに関してはデジタルトラスト協議会が公開している「ｅシール解説

～実用化に向けて～」[14]を参照。

6.2.4. 位置情報の保護

A） Spoofing 対策

自動運転やドローンなど先端モビリティ領域においては、GNSS（測位衛星システムの総称、GPS は米国版 GNSS の名称）に代表される位置情報に対する依存度は非常に高い。一方で、偽装、改ざんに関するセキュリティの課題も存在する。偽の GPS 信号を自由に生成・配信することができるため、位置情報を改ざんする「GPS Spoofing、(以下、Spoofing)」と呼ばれる攻撃のリスクが高まっているからだ。Spoofing は検出が困難なため、自動運転車やドローンの開発／実装が進む中、Spoofing（スプーフィング）による事故発生の脅威や、それらの普及を妨げる要因になることが懸念されている。

① 実際の Spoofing 事例

Spoofing は、現在世界各地で確認されている 。 安全保障や組織犯罪関連の事案が多く、 ドローン、船舶などのモビリティが対象となりやすい。

図 26：世界各地の特徴的な Spoofing 事例

Forbes の記事[15]によると、GPS に関する妨害は、ウクライナ紛争が長期化する中、

[14] デジタルトラスト協議会 「ｅシール解説～実用化に向けて～」
https://jdtf.or.jp/report/whitepaper/

[15] https://www.forbes.com/sites/davidhambling/2023/04/21/ukraine-is-spoofing-russian-drones-out-of-the-sky/?sh=1cdcf6c6100c

至るところで見られるようになった。よく知られているのはジャミングで、GPS 周波数で妨害電波を飛ばし、ドローンの位置情報の取得そのものを妨げる行為だ。それに加えて、Spoofing も多く確認されている。例えば、飛んできた敵国ドローンの位置情報を、空港などの飛行禁止エリアにいると勘違いさせて機能停止させるなど、ドローン損失率の増加について報告されている。

② Spoofing 手法

Spoofing とは、GPS 信号に対する干渉の一種で、受信機を騙して誤った位置を算出させる。Spoofing 攻撃では、ターゲット受信機に偽の GPS 信号を送信することで、偽の現在地を表示させるなど、簡単に位置の改ざんを実行することが可能となっている（図 27 参照）。この行為は、数万円程度の安価なデバイス（SDR（Software Defined Radio）機器、等）と公開コードを利用し、専門家でなくても簡単に実現可能であると指摘されている。

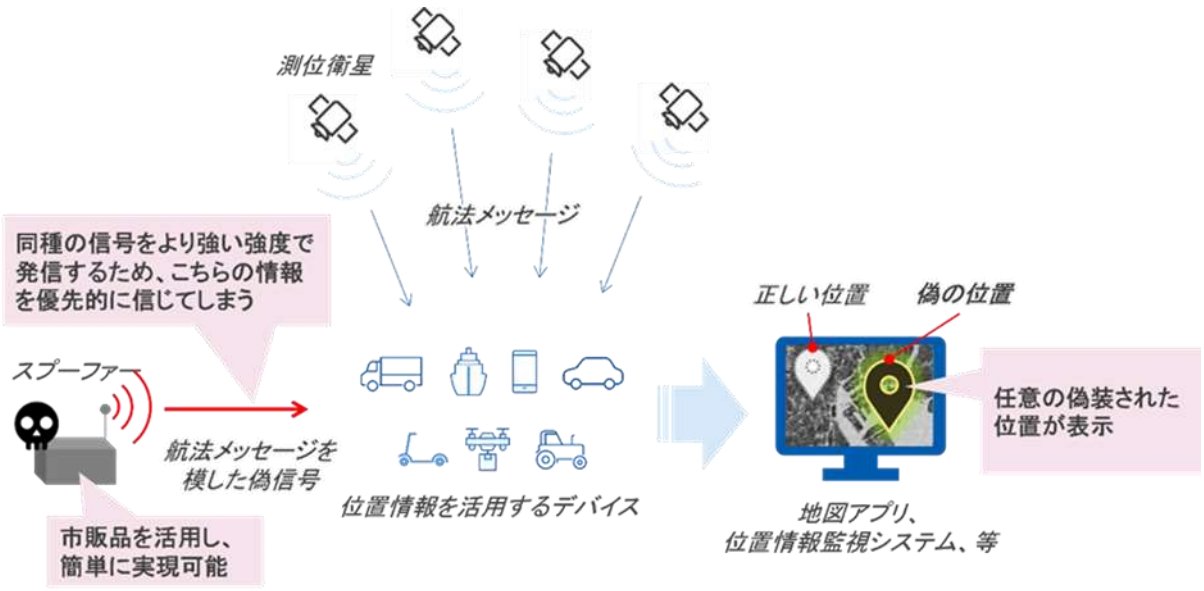


図 27：Spoofing の概念図

③ Spoofing 対策

- Spoofing に対する GNSS 受信機の保護

日本版 GPS とも言われる準天頂衛星「みちびき」の信号認証サービスは、電子署名を使った認証技術を活用することで、測位信号の真正性を検証することができる。衛星の位置情報を伝える航法メッセージの認証を可能にすることで、信号を受け取る側

（受信機）においては、受信している信号が本当に測位衛星から来ているものかを確認できるため、第三者からの Spoofing による位置情報の改ざんを防止できるようになる。自動運転車・ドローン配送・スマートフォンアプリケーションなど幅広い領域で、位置情報利用に安全かつ高信頼性を付与できる。航法メッセージのセキュリティは、この情報が改ざんされると誤った測位計算につながるため、多くの社会インフラにとって安全性や信頼性担保のために重要である。

- みちびき信号認証対応受信機による認証

みちびきの信号認証対応受信機内の高度なアルゴリズムにより、予め入手した公開鍵、受信した電子署名、及び航法メッセージを用いて、航法メッセージそのものの改ざんの有無を検証する（図 28 参照）。

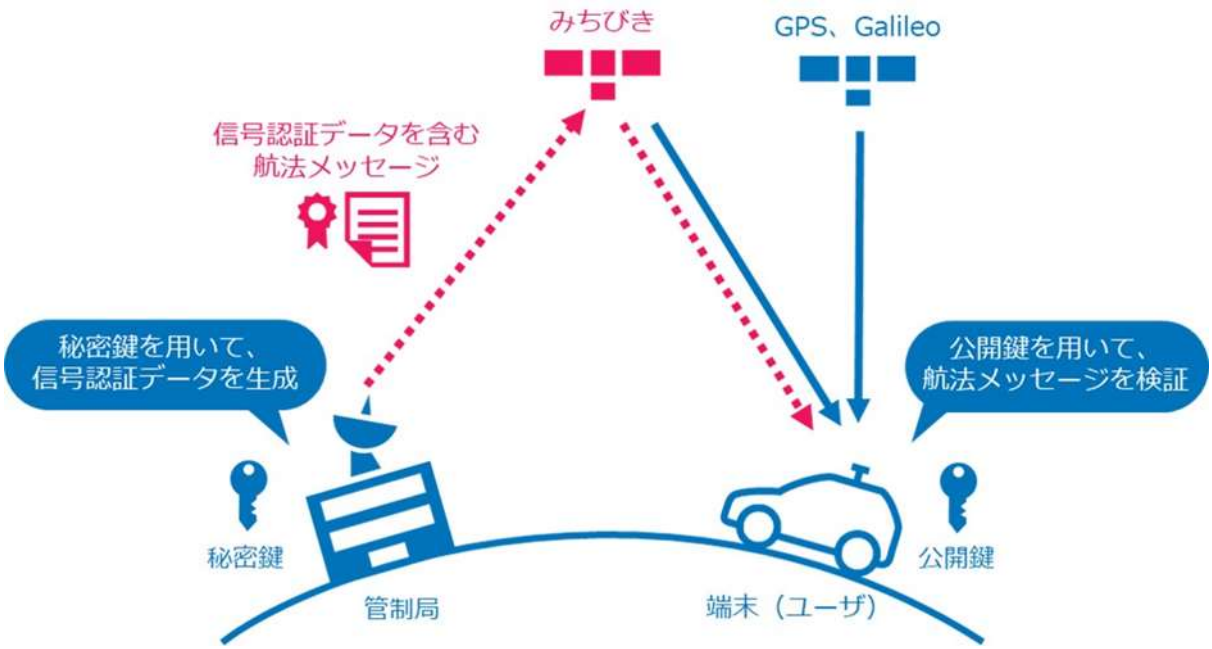


図 28：みちびきの信号認証（内閣府より引用）

これにより、端末側においては、測位衛星から送信された測位信号を用いた、真正な位置情報の計測が可能となる。またこの方式は、受信機のハードウェアへの影響は限定的で、原則ソフトウェア/ファームウェアの変更のみで容易に実装可能である。

- 海外動向

欧州においては、Galileo の OSNMA （Open Service Navigation Message Authentication）対応受信機として、Septentrio 社の受信機に既に実装されている。

mosaic-T GNSS モジュールは、ミッションクリティカルなインフラに耐障害性のあるソリューションを提供しており、Airbus 社を含むグローバル企業が、Septentrio 社の GNSS 受信機で Galileo 信号の OSNMA 認証の実証を行っている。

アメリカの GPS システムも、Chimera と呼ばれる独自の認証メカニズムを開発中である。将来の GNSS 受信機は、OSNMA、Chimera、みちびきの信号認証などの GNSS 付加価値サービスが一般に利用可能になり次第、ユーザがそれをいち早く活用できるように市場投入されることが期待されている。高精度ソリューションに安全性・信頼性の高い受信機を統合することで、ユーザ企業は最新の PNT レジリエンスを提供する製品やサービスを社会実装することが可能となる。

④ まとめ｜展望

- Spoofing に対する GNSS 受信機の保護

日本においては、Spoofing による大きな障害の報告例は現時点で多くないが、インシデント発生時のインパクトを考慮すると、事前に GNSS セキュリティ対策を講じることが重要と言える。近年では、国内外の GNSS 機器メーカーや、ソリューションプロバイダなどが、対策技術の導入に関心を寄せている。また、ゲートレスの道路課金システムなど、GNSS を利活用した新しいソリューションへの展開も期待されている。

GNSS セキュリティは、これまであまり注目されてこなかった。しかしながら高度に DX 化された社会基盤においては、位置情報の重要性／依存性はますます増加し、精度だけでなくセキュリティの面にも注目していかなければならないフェーズに来ている。

今後の普及に向けた課題として、安全かつ信頼性の高い位置情報を担保するための認証の仕組みづくりや、それに伴う対策技術やソリューションに関する市場形成が望まれる。

B） 位置時刻認証

位置時刻認証とは、「あるエンティティがいつどこにいたのか」もしくは「ある事象がいつどこで起こったのか」について一定の基準をもって確からしいと認定するものある。位置時刻認証を行うためにはこの「一定の基準」を定めなければならない。

位置時刻の算出は位置時刻を算出するための「適切な測位情報源」を使用して「適切な位置時刻計算」を行わなければならない。この 2 つのどちらかに問題があれば正しい位置時刻は得られない。従って位置時刻認証を行うためには少なくともこの 2 つについて基準を決めなければならない。

【適切な情報と計算】

① 適切な測位情報源

位置時刻を算出するための情報源として改ざん防止などの措置が取られている情報源に準天頂衛星みちびきの信号認証システムがある。みちびきの信号認証システムの改ざん防止措置は日本全体で有効である。空が開けている場所においては準天頂衛星みちびきの使用が安全である。

② 適切な位置時刻計算

適切な位置時刻計算とは、正確な位置時刻を計算することも大事ですが、ここでは位置時刻計算を意図した通りにできることを指しています。第三者によって計算ロジック自体や計算結果を改ざんされたりすることがない状態だ。

【適切な情報と計算を行うための仕組み】

適切な情報として GPS・QZSS をあげたが、2024 年 4 月現在、この情報には電子署名が付与されている。このため測位情報は改ざんができない。安全な測位情報を使用して安全に位置時刻を計算し、その結果に電子署名をつけることで位置時刻情報を安全に出力できる。

ここで問題となるのは、位置時刻計算の部分を改ざんされたり結果を改ざんされたりしないようになっていなければ安全は担保されない。また、その結果に電子署名を行う部分も同様である。この部分の安全は物理的に耐タンパ化することで実現が可能である。以下の図のように測位情報源から位置時刻情報までの処理の流れがすべて安全に守られている必要がある。

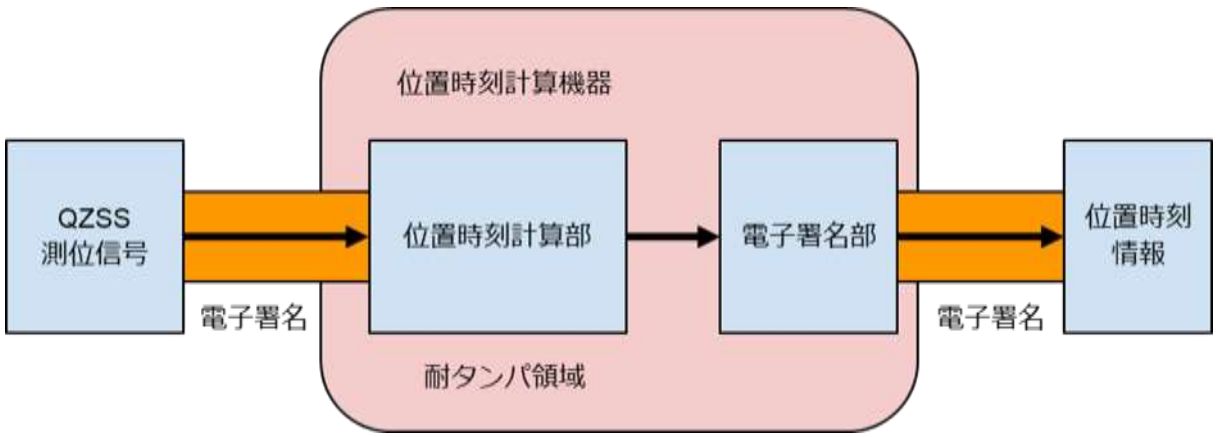


図 29：適切な情報と計算を行うための仕組み

【適切な情報と計算を行うための基準】

「適切な情報と計算を行うための仕組み」のような安全な処理の流れの基準がなければ安全性は担保されない。この基準を決めるために少なくとも以下の２つを決めなければならない。

- コンプライアンス・ルール（遵守規定）
- ロバストネス・ルール（強靭性に関する規定）

① コンプライアンス・ルール

コンプライアンス・ルール（遵守規定）には以下のようなものがある。

- 信号認証システムの電子署名検証方法の規定
- 認証された信号情報を使用した測位計算法の規定
- 信号認証システムで配布される公開鍵の取り扱い規定
- 測位計算結果への電子署名方法の規定
- 測位計算結果への電子署名に使用されるデジタル証明書と秘密鍵の取り扱い規定
- 出力する電子署名付き位置時刻情報のフォーマットの規定

② ロバストネス・ルール

ロバストネス・ルール（強靭性に関する規定）には以下のようなものがある。

- 信号認証システムの署名検証計算部、測位計算部及び測位計算結果への電子署名計算部分など計算部分の耐タンパ化に関する規定
- 信号認証システムの署名検証に使用される公開鍵及び測位計算結果への電子署名に使用されるデジタル証明書と秘密鍵等の秘密情報の保管と管理に関する規定

【基準をとりまとめるオーソリティ】

これらの基準を管理し、基準を満たした機器等に対して認証を行うオーソリティが必要である。このオーソリティは認証の証として機器に対してデジタル証明書を発行する。機器はこのデジタル証明書を使用して算出した位置時刻情報に電子署名を行う。

位置時刻認証を行うためにはこのオーソリティを設立し、基準を定め、基準を遵守している機器等の認証を行える体制を整える必要がある。

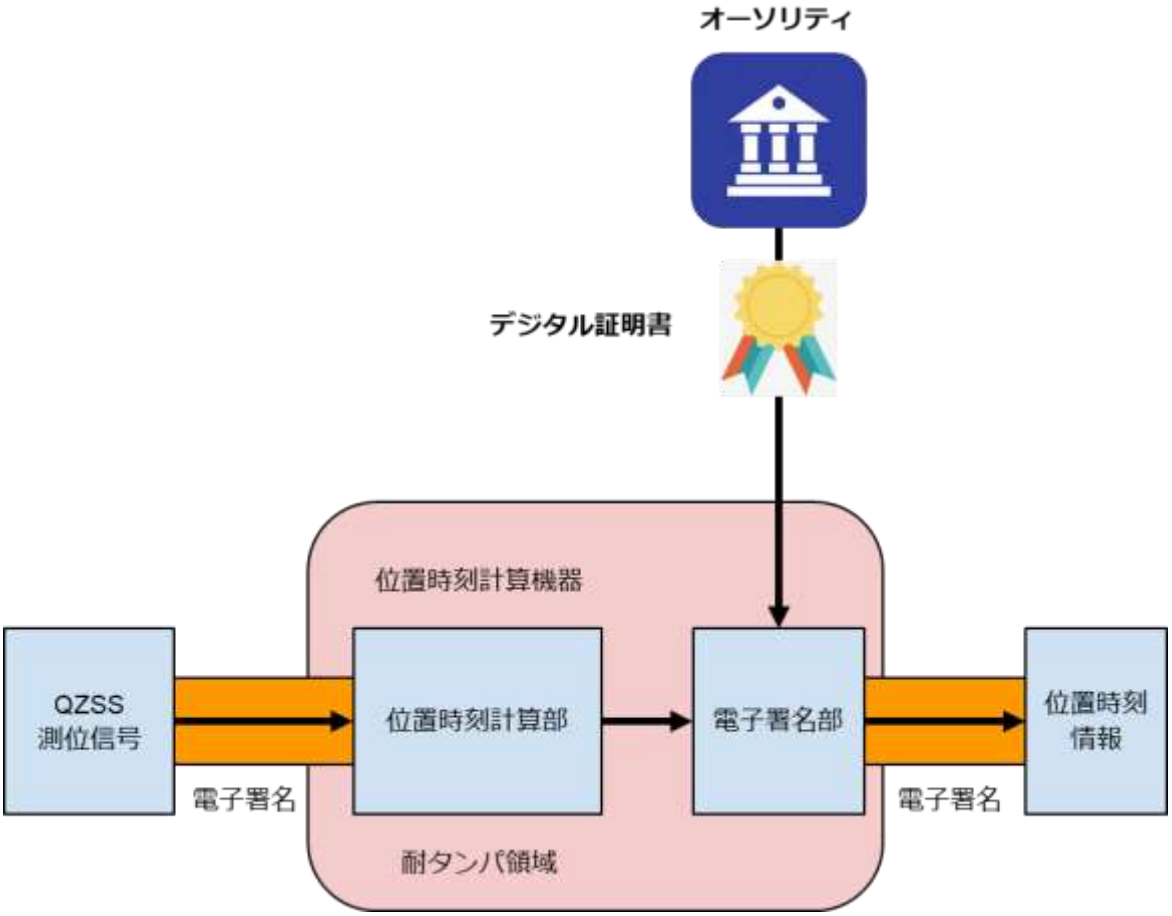


図 30：基準をとりまとめるオーソリティ

6.2.5. 障害検知

A） 障害検知方法

これまでドローンに対するセキュリティ対策として、機体との認証やデータの暗号化といった技術的対策を紹介してきたが、ドローン本体に対してのみのセキュリティ対策では限界がある。そこで、ドローン本体のみではなく、システムや人間監視などを含めた多重的な監視体制の構築が必要となる。

主な多重監視体制として、ドローンの飛行を別システムで監視し、意図しない飛行ルートへの進行などの障害が発生した場合、管理者に報告してドローンを安全に着陸させるなどが考えられる。ドローンの位置情報監視についてはリモート ID や GPS などを使用した手法がいくつか考えられる。この手法で重要になってくるのが、ドローンの安全着陸は特権機能になるため実行可能者を制限する必要がある。また、特権を持った者かを正しく認証する機能を安全着陸機能に搭載する必要があり、その認証情報の管理方法についても考

慮が求められる。

B） 悪意あるドローンに対する対策（アンチドローン、カウンタードローン）

悪意ある第三者による不正ドローンでの攻撃は、事業者側だけで対策ができず、アンチドローンやカウンタードローン（不正ドローンに対して妨害を行うシステムのこと）といった不正ドローンへの対策が必要である。

攻撃的な悪意のあるドローンへのアプローチは主に 3 つある。

1. 検出・警報

空域を監視し、侵入してくるドローンの大きさの目安を読み取り、その対応の警戒レベルを発報する。特に小型で機敏なドローンに対してはその認識が難しく課題としては高く、それが可能になるかがポイントである。

2. 識別・分類

ドローンを鳥などの飛行物と区別できること。ドローンが検出されると、そのモデル名までも認識でき、オペレーターの位置も確認できる技術がある。

3. 追跡・無力化

ドローンがそれ以上近づくと危険な場合、無力化の技術でドローンの接近を停止させるか物理的にドローンを妨害する、あるいはソフトウェアに干渉することで方向転換もしくは着陸させることができる。ただし、この無力化はアクティブな電波装置を使用するために GPS などの電波に干渉するために特別な許可が必要になるケースが多い。

上記をすべて提供していない対策システムでは、個々の対策装置を一貫した計画の中で統合する必要が生じる。現在のほとんどの対策装置はこれらの一部のみを提供している場合が多く、うまく配置・計画する必要がある。

アンチドローンの運用に関しては、攻撃から保護する区域の環境や性質、また、攻撃してくる可能性がある潜在的脅威の標的の状況に応じて、24 時間 365 日の対策が必要になる場合もある。また、アンチドローンに関してルールや法律の整備が必要である。

6.2.6. インシデントレスポンス

A） 脆弱性情報監視

運用中では、使用しているソフト部品、ハード部品のベンダー発行の脆弱性情報の監視が必要になってくる。また、脆弱性データベースである CVE、NVD、JVN などの公開脆弱性情報の監視も有効となってくる。

B） インシデント発生時の対応の定義

セキュリティリスクが顕在化すると顧客に損害を与える可能性がある。また、企業イメージの低下という問題に発展する可能性もある。この為、セキュリティ事故や、脆弱性情報など情報受診時に的確に対応できるように、事前に対応できる十分な能力と体制を整えておく。

参考に IT セキュリティの教育研究機関 SANS Institute で提唱されている 6 ステップを下記に示す。

図 31：インシデント対応

C） 残留脆弱性管理

脆弱性を保有するとした場合に、定期的に管理する必要がある。保有する脆弱性を持つソフトモジュール、部品、管理する期間などを定め、定期的に追加の脆弱性や、対策など情報が更新されていないか確認を行う。

7. 運用手順および運用時の注意事項

7.1. リモート ID について

A） 米国の Remote ID

米国連邦航空局（FAA）は、2020 年 12 月に米国でドローンの操縦者に 2 つの規則[16]を発表した。1 つ目は、Remote ID で無人航空機のデジタルナンバープレートのような機能として、機体本体の位置情報を含む識別情報を送信する。2 つ目は、人の頭上と夜間の運用に関するものであり、有人地帯の上空や夜間の飛行についての規則である。この規則は、重量 250g 以下のドローンで対象は何段階かに分かれている。

Remote ID の運用要件に準拠するには、次の 3 つの方法があります。

1. ドローンとコントロールステーションの識別情報と位置情報をブロードキャストする標準の Remote ID ドローンを運用する。
2. Remote ID をブロードキャストするモジュールを使用して運用する。
3. FAA の認識領域で Remote ID なしでドローンを運用する。

B） 日本国内の機体登録制度とリモート ID

2020 年 6 月に公布された改正航空法に基づき、無人航空機の機体の登録制度[17]が創設された。これは、所有者の把握、危険性を有する機体を排除するなど無人航空機の飛行の安全性の向上を図るためのものである。2021 年 11 月に公布された政省令などにより、2022 年 6 月 20 日から無人航空機の登録が義務化となる。本制度の手続きなどの詳細が規定され、2021 年 12 月から事前登録が開始された。リモート ID 機器を搭載できない機体については、2022 年 6 月 19 日までに登録すれば、3 年後まではリモート ID 機器を搭載せず飛行することが可能で、未登録の場合は飛行することが出来なくなり、飛行した場合は 1 年以下の懲役または 50 万円以下の罰金が科せられる。

[16] U.S. Department of Transportation Issues Two Much-Anticipated Drone Rules to Advance Safety and Innovation in the United States
https://www.faa.gov/news/press_releases/news_story.cfm?newsId=25541

[17] 無人航空機の登録制度
https://www.mlit.go.jp/koku/koku_ua_registration.html

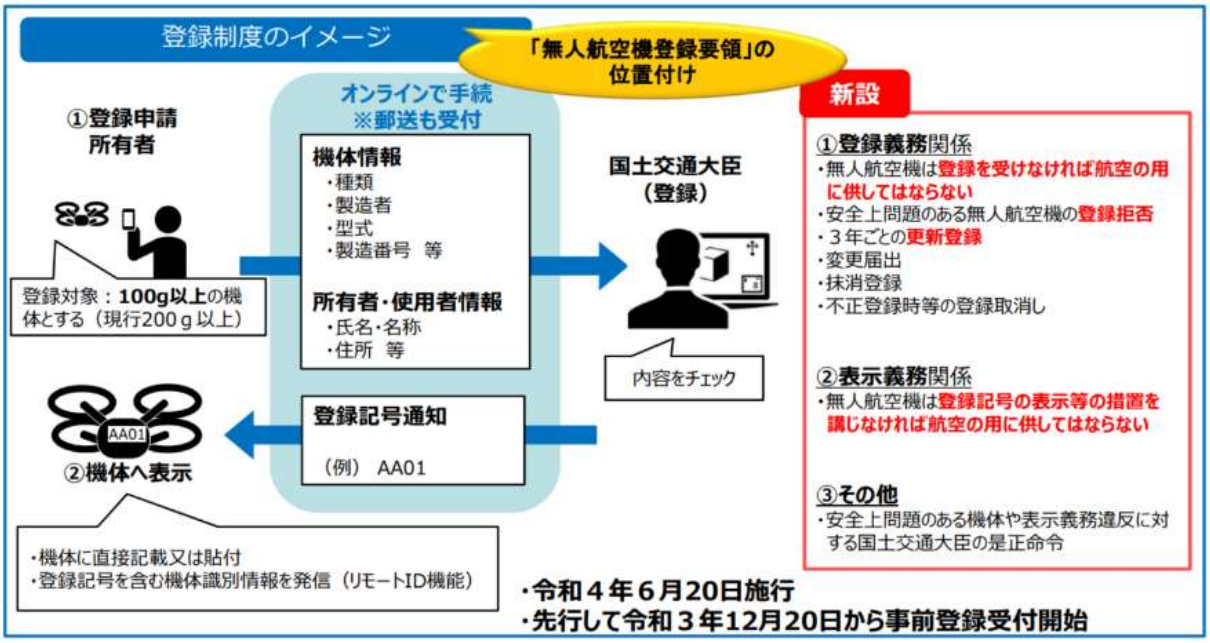


図 32：無人航空機登録制度の概要（出典：国土交通省）

改正航空法により、登録を受けた無人航空機には、無人航空機の登録記号を遠隔から識別するための機能であるリモート ID を備え、作動させなければ飛行してはならないことを義務付けている。

本要件は、航空法規則第 236 条の６第２号に基づき、登録記号の表示のためのリモート ID 機能の無人航空機への搭載について義務付けしており、無人航空機が搭載するリモート ID 機能または外付けのリモート ID 機器および登録記号その他の必要な情報を入力するためのアプリケーションを開発・製造にあたり製造者が従うべき具体的な要件を定めている。

リモート ID 機器等およびアプリケーションが備えるべき要件[18]を満たすためには、国土交通省が公開する仕様書などを参照してほしい。

- リモート ID 技術規格書
- リモート ID 機器等インターフェース仕様書
- メーカーアプリ アプリケーション・インターフェース仕様書
- 自己検証結果・型式情報等届出書
- リモート ID 公開鍵・アプリ認証コード通知申請書

[18] リモート ID 機器等およびアプリケーションが備えるべき要件
https://www.mlit.go.jp/koku/content/001444589.pdf

7.2. 無人航空機の点検・整備

A） 機体の点検・整備の方法

（1）飛行前の点検

飛行前には、以下の点について機体の点検を実施する。

- 各機器は確実に取り付けられているか（ネジ等の脱落やゆるみ等）
- 発動機やモーターに異音はないか
- 機体（プロペラ、フレーム等）に損傷やゆがみはないか
- 燃料の搭載量またはバッテリーの充電量は十分か
- 通信系統、推進系統、電源系統及び自動制御系統は正常に作動するか

（2）飛行後の点検

- 機体にゴミ等の付着はないか
- 各機器は確実に取り付けられているか（ネジ等の脱落やゆるみ等）
- 機体（プロペラ、フレーム等）に損傷やゆがみはないか
- 各機器の異常な発熱はないか

（3）20 時間の飛行毎に、以下の事項について無人航空機の点検を実施

- 交換の必要な部品はあるか
- 各機器は確実に取り付けられているか（ネジ等の脱落やゆるみ等）
- 機体（プロペラ、フレーム等）に損傷やゆがみはないか
- 通信系統、推進系統、電源系統及び自動制御系統は正常に作動するか

B） 点検・整備記録の作成

7.2 の（3）に定める飛行の前後及び 20 時間の飛行毎に無人航空機の点検・検査を行った際には、「無人航空機の飛行日誌の取扱要領」に従い、点検・整備記録を作成し管理する。

7.3 無人航空機を飛行させる者の訓練および遵守事項[19]

A） 基本的な操縦技量の習得

プロポの操作に慣れるため、以下の内容の操作が容易にできるようになるまで 10 時間以上の操縦練習を実施する。なお、操縦練習の際には、十分な経験を有する者の監督の下に行うものとする。訓練場所は許可等が不要な場所または訓練のために許可等を受けた場所で行う。

項目	内容
離着陸	操縦者から３m離れた位置で、３mの高さまで離陸し、指定の範囲内に着陸すること。 この飛行を５回連続して安定して行うことができること。
ホバリング	飛行させる者の目線の高さにおいて、一定時間の間、ホバリングにより指定された範囲内（半径１mの範囲内）にとどまることができること。
左右方向の移動	指定された離陸地点から、左右方向に２０m離れた着陸地点に移動し、着陸することができること。 この飛行を５回連続して安定して行うことができること。
前後方向の移動	指定された離陸地点から、前後方向に２０m離れた着陸地点に移動し、着陸することができること。 この飛行を５回連続して安定して行うことができること。
水平面内での飛行	一定の高さを維持したまま、指定された地点を順番に移動することができること。 この飛行を５回連続して安定して行うことができること。

B） 業務を実施するために必要な操縦技量の習得

基礎的な操縦技量を習得した上で、以下の内容の操作が可能となるよう操縦練習を実施する。訓練場所は許可等が不要な場所または訓練のために許可等を受けた場所で行う。

項目	内容
対面飛行	対面飛行により、左右方向の移動、前後方向の移動、水平面内での飛行を円滑に実施できるようにすること。
飛行の組合	操縦者から１０m離れた地点で、水平飛行と上昇・下降を組み合わせて飛行を５回連続して安定して行うことができること。
８の字飛行	８の字飛行を５回連続して安定して行うことができること。

[19] 航空局標準マニュアルより引用　https://www.mlit.go.jp/common/001521378.pdf

C） 操縦技量の維持

A），B）で定めた操縦技量を維持するため、定期的に操縦練習を行う。訓練場所は許可等が不要な場所または訓練のために許可等を受けた場所で行う。

D） 夜間における操縦練習

夜間においても、B）に掲げる操作が安定して行えるよう、訓練のために許可等を受けた場所または屋内にて練習を行う。

E） 目視外飛行における操縦練習

目視外飛行においても、B）に掲げる操作が安定して行えるよう、訓練のために許可等を受けた場所または屋内にて練習を行う。

F） 物件投下のための操縦練習

物件投下の前後で安定した機体の姿勢制御が行えるよう、また、5 回以上の物件投下の実績を積むため、訓練のために許可等を受けた場所または屋内にて練習を行う。

G） 飛行記録の作成

無人航空機を飛行させた際には、「無人航空機の飛行日誌の取扱要領」に従い、飛行記録を作成し管理する。

H） 無人航空機を飛行させる者が遵守しなければならない事項

（1） 第三者に対する危害を防止するため、第三者の上空で無人航空機を飛行させない。

（2） 飛行前に、気象、機体の状況及び飛行経路について、安全に飛行できる状態であること、飛行させる場所が緊急用務空域に指定されていないことを確認する。また、他の無人航空機の飛行予定の情報（飛行日時、飛行経路、飛行高度）を飛行情報共有システム（https://www.fiss.mlit.go.jp/）で確認するとともに、当該システムに飛行予定の情報を入力する。ただし、飛行情報共有システムが停電等で利用できない場合は、国土交通省航空局安全部安全企画課に無人航空機の飛行予定の情報を報告するとともに、自らの飛行予定の情報が当該システムに表示されないことを鑑み、特段の注意をもって飛行経路周辺における他の無人航空機及び航空機の有無等を確認し、安全確保に努める。

（3） 5ｍ／ｓ以上の突風が発生するなど、無人航空機を安全に飛行させることができなくなるような不測の事態が発生した場合には即時に飛行を中止する。

（4） 多数の者が集合する場所の上空を飛行することが判明した場合には即時に飛行を中止する（承認を受けて催し場所の上空を飛行する場合を除く）。

（5） アルコールまたは薬物の影響により、無人航空機を正常に飛行させることができない恐れがある間は、飛行させない。

（6） 飛行の危険を生じるおそれがある区域の上空での飛行は行わない。

（7） 飛行前に、航行中の航空機を確認した場合には、飛行させない。

（8） 飛行前に、飛行中の他の無人航空機を確認した場合には、飛行日時、飛行経路、飛行高度等について、他の無人航空機を飛行させる者と調整を行う。

（9） 飛行中に、航行中の航空機を確認した場合には、着陸させるなど接近または衝突を回避させる。

（10） 飛行中に、飛行中の他の無人航空機を確認した場合には、当該無人航空機との間に安全な間隔を確保して飛行させる。その他衝突のおそれがあると認められる場合は、着陸させるなど接近または衝突を回避させ、飛行日時、飛行経路、飛行高度等について、他の無人航空機を飛行させる者と調整を行う。

（11） 不必要な低空飛行、高調音を発する飛行、急降下など、他人に迷惑を及ぼすような飛行を行わない。

（12） 物件のつり下げまたは曳航は行わない。

（13） 十分な視程が確保できない雲や霧の中では飛行させない。

（14） 「無人航空機の飛行日誌の取扱要領」に従い、定期的に機体の点検・整備を行うとともに、点検・整備記録を作成する。

（15） 無人航空機を飛行させる際は、次に掲げる飛行に関する事項を記録する。

- 飛行年月日
- 無人航空機を飛行させる者の氏名
- 無人航空機の名称
- 飛行の概要（飛行目的及び内容）
- 離陸場所及び離陸時刻
- 着陸場所及び着陸時刻
- 飛行時間
- 無人航空機の飛行の安全に影響のあった事項（ヒヤリ・ハット等）

（16） 無人航空機の飛行による人の死傷、第三者の物件の損傷、飛行時における機体の紛失または航空機との衝突若しくは接近事案が発生した場合には、次に掲げる事項を速やかに、許可等を行った国土交通省航空局安全部運航安全課、地方航空局保安部運用課また

は空港事務所まで報告する。なお、夜間等の執務時間外における報告については、24時間運用されている航空領域を管轄する空港事務所に電話で連絡を行う。

- 無人航空機の飛行に係る許可等の年月日及び番号
- 無人航空機を飛行させた者の氏名
- 事故等の発生した日時及び場所
- 無人航空機の名称
- 無人航空機の事故等の概要
- その他参考となる事項

（17）飛行の際には、無人航空機を飛行させる者は許可書または承認書の原本または写しを携行する。

7.4 安全を確保するために必要な体制

A） 無人航空機を飛行させる際の基本的な体制

- 場所の確保・周辺状況を十分に確認し、第三者の上空では飛行させない。
- 風速５ｍ／ｓ以上の状態では飛行させない。
- 雨の場合や雨になりそうな場合は飛行させない。
- 十分な視程が確保できない雲や霧の中では飛行させない。
- 飛行させる際には、安全を確保するために必要な人数の補助者を配置し、相互に安全確認を行う体制をとる。
- 補助者は、飛行範囲に第三者が立ち入らないよう注意喚起を行う。
- 補助者は、飛行経路全体を見渡せる位置において、無人航空機の飛行状況及び周囲の気象状況の変化等を常に監視し、操縦者が安全に飛行させることができるよう必要な助言を行う。
- 飛行場所付近の人または物件への影響をあらかじめ現地で確認・評価し、補助員の増員等を行う。

  ※ A）に加え、飛行の形態に応じ、B）から I）の各項目に記載される必要な体制を適切に実行すること。

B） 進入表面等の上空の空域における飛行を行う際の体制

- 無人航空機を飛行させる際には、空港設置管理者等（空港管理事務所またはヘリポート管理事務所（及び管制機関が配置されている場合は、空港事務所（または空港出張所、基地）管制機関））と常に連絡がとれる体制を確保する。なお、予め調整した空港設置管

理者等からの条件についても申請書（様式 1）その他参考となる事項に、調整結果として記載する。

- 予め空港事務所と調整した方法により、飛行を予定する日時、飛行高度（上限、下限）、機体数及び機体諸元などを空港事務所の求めに応じ連絡する。なお、必要に応じ、調整した連絡方法について、別添または申請書（様式 1）その他参考となる事項に記載する。
- 無人航空機の飛行について、補助者が周囲に周知を行う。

C） 進入表面及び転移表面の下の空域並びに敷地上空の空域における飛行を行う際の体制

- 無人航空機を飛行させる際には、空港設置管理者（空港事務所または空港管理事務所）と常に連絡がとれる体制を確保する。なお、予め調整した空港設置管理者からの条件についても申請書（様式 1）その他参考となる事項に、調整結果として記載する。
- 無人航空機の飛行について、補助者が周囲に周知を行う。
- 飛行場所が人口集中地区にあっては、飛行させる無人航空機について、プロペラガードを装備して飛行させる。装備できない場合は、第三者が飛行経路下に入らないように監視及び注意喚起をする補助者を必ず配置し、万が一第三者が飛行経路下に接近または進入した場合は操縦者に適切に助言を行い、飛行を中止する等適切な安全措置をとる。

D） 地表または水面から 150m以上の高さの空域における飛行を行う際の体制

- 無人航空機を飛行させる際には、関係機関（空港事務所・航空交通管制部）と常に連絡がとれる体制を確保する。なお、予め調整した空港設置管理者等からの条件についても申請書（様式 1）その他参考となる事項に、調整結果として記載する。
- 予め空港事務所と調整した方法により、飛行を予定する日時、飛行高度（上限、下限）、機体数及び機体諸元などを空港事務所の求めに応じ連絡する。なお、必要に応じ、調整した連絡方法について、別添または申請書（様式 1）その他参考となる事項に記載する。
- 無人航空機の飛行について、補助者が周囲に周知を行う。

E） 人または家屋の密集している地域の上空における飛行、地上または水上の人または物件との間に 30mの距離を保てない飛行または催し場所の上空における飛行を行う際の体制

- 飛行させる無人航空機について、プロペラガードを装備して飛行させる。装備できない場合は、第三者が飛行経路下に入らないように監視及び注意喚起をする補助者を必ず配

置し、万が一第三者が飛行経路下に接近または進入した場合は操縦者に適切に助言を行い、飛行を中止する等適切な安全措置をとる。

・ 無人航空機の飛行について、補助者が周囲に周知を行う。

F） 催し場所の上空における飛行を行う際の体制

・ 飛行させる無人航空機について、プロペラガードを装備して飛行させる。

・ 地表等から１５０m未満で飛行させる。

・ 飛行速度と風速の和が７m／s以上の状態では飛行させない。

・ 無人航空機の飛行について、補助者が周囲に周知を行う。

・ 催しの主催者等とあらかじめ調整を行い、以下に示す立入禁止区画を設定し、第三者が当該区画に立ち入らないよう措置する。 なお、予め調整した催しの主催者等からの条件についても申請書（様式１）その他参考となる事項に、調整結果として記載する。

飛行の高度	立入禁止区画
２０m未満	飛行範囲の外周から３０m以内の範囲
２０m以上５０m未満	飛行範囲の外周から４０m以内の範囲
５０m以上１００m未満	飛行範囲の外周から６０m以内の範囲
１００m以上１５０m未満	飛行範囲の外周から７０m以内の範囲

G） 夜間飛行を行う際の体制

・ 夜間飛行においては、目視外飛行は実施せず、機体の向きを視認できる灯火が装備された機体を使用し、機体の灯火が容易に認識できる範囲内での飛行に限定する。

・ 飛行高度と同じ距離の半径の範囲内に第三者が存在しない状況でのみ飛行を実施する。

・ 操縦者は、夜間飛行の訓練を修了した者に限る。

・ 補助者についても、飛行させている無人航空機の特性を十分理解させておくこと。

・ 夜間の離発着場所において車のヘッドライトや撮影用照明機材等で機体離発着場所に十分な照明を確保する。

H） 目視外飛行を行う際の体制

・ 飛行の前には、飛行ルート下に第三者がいないことを確認し、双眼鏡等を有する補助者のもと、目視外飛行を実施する。

・ 操縦者は、目視外飛行の訓練を修了した者に限る。

・ 補助者についても、飛行させている無人航空機の特性を十分理解させておくこと。

I） 危険物の輸送を行う際または物件投下を行う際の体制

- A）に基づき補助者を適切に配置し飛行させる。
- 危険物の輸送の場合、危険物の取扱いは、関連法令等に基づき安全に行う。
- 物件投下の場合、操縦者は、物件投下の訓練を修了した者に限る。

J） 非常時の連絡体制

- あらかじめ、飛行の場所を管轄する警察署、消防署等の連絡先を調べ、7.3 章 H）（16）に掲げる事態が発生した際には、必要に応じて直ちに警察署、消防署、その他必要な機関等へ連絡するとともに、以下のとおり許可等を行った国土交通省航空局次世代モビリティ企画室、地方航空局保安部運用課または空港事務所まで報告する。なお、夜間等の執務時間外における報告については、24 時間運用されている最寄りの空港事務所に電話で連絡を行う。

国土交通省航空局次世代航空モビリティ企画室	
	03-5253-8111（内線：48675,48687）
東京航空局保安部運用課	03-6685-8005
大阪航空局保安部運用課	06-6949-6609
東京空港事務所	050-3198-2865（24 時間）
大阪空港事務所	072-455-1330（執務時間内）
	050-3198-2870（執務時間外）

（様式１）無人航空機の点検・整備記録

（点検機体名：　　）

点検日	点検者	点検内容			交換部品等
		点検項目		点検結果	
		機体全般	機器の取付け状態（ネジ、コネクタ、ケーブル等）		
		プロペラ	外観		
			損傷		
			ゆがみ		
		フレーム	外観		
			損傷		
			ゆがみ		
		通信系統	機体と操縦装置の通信品質の健全性		
		推進系統	モーター又は発動機の健全性		
		電源系統	機体及び操縦装置の電源の健全性		
		自動制御系統	飛行制御装置の健全性		
		操縦装置	外観		
			スティックの健全性		
			スイッチの健全性		
（特記事項）					

（様式２）無人航空機の飛行記録

年月日	飛行させる者の氏名	飛行概要	飛行させた無人航空機	離陸場所	離陸時刻	着陸場所	着陸時刻	飛行時間	総飛行時間	飛行の安全に影響のあった事項

8. ドローンにおけるセーフティ

8.1. ドローンにおけるセーフティの考え方

ドローン活用・運用において、セキュリティの要件が今後ますます重要度を増してくる一方で安全にドローンを活用・運用するためのセーフティの概念も欠かすことのできない要素である。本章では、セーフティの観点でどのような配慮が必要かを記載していく。

8.1.1. セーフティとセキュリティ

以下の図はドローンのユースケースと落下リスクの関係性をまとめた図である。手動より自動のほうが落下の可能性が高く、無人地帯より有人地帯を飛行するほうが被害は大きい。

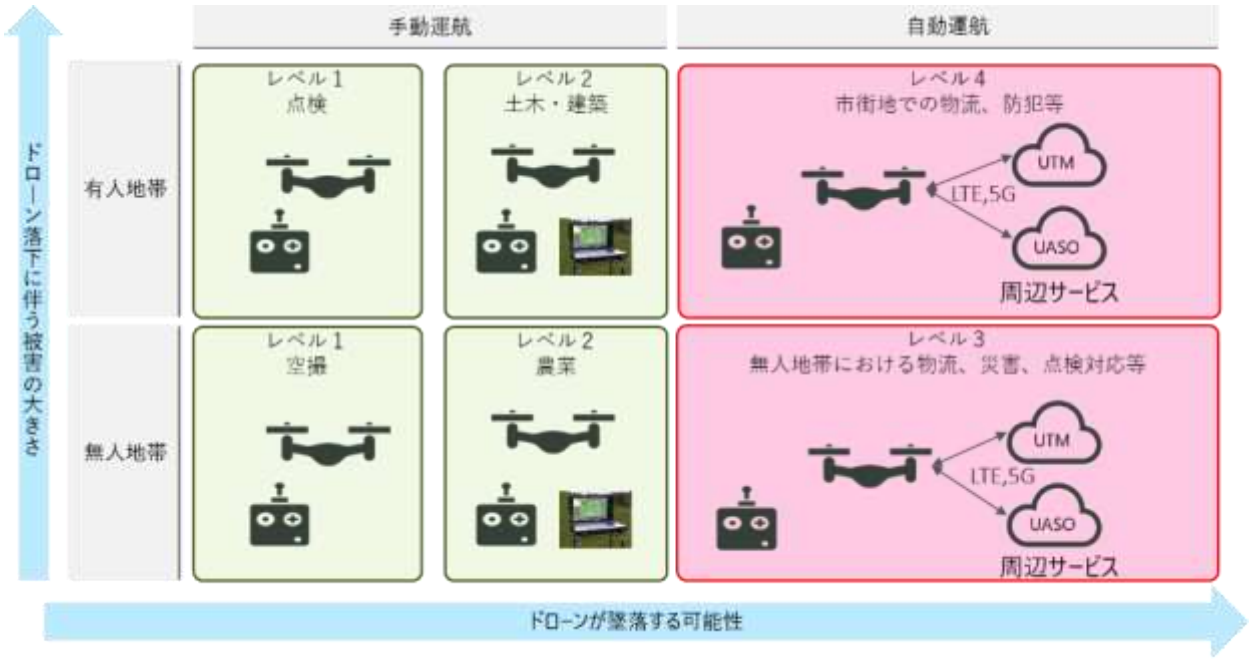


図 33：運航レベル、飛行区域、飛行方法と落下リスクの関係

ドローンにおけるセーフティとセキュリティは不可分な領域もあり、明確な区分は困難であるが、墜落、衝突、紛失など、物理的な損害が発生しうる事故に対する備えを「セーフティ」に関わる事項と捉える。事故要因は自然災害や部品破損等、偶発的要因と第三者の悪意による意図的要因が考えられるが、前者がセーフティ、後者がセキュリティで取り扱う範囲と言える。

8.1.2. セーフティの分類[20]

安全工学上の分類	概略	ドローンに適用した場合の考え方
フェールセーフ	製品が故障した時に、安全側の状態となるようにする設計の考え方。多くの製品で「安全側の状態≒機能停止」を意味する。	ドローンの場合、運用中は空中に存在することになるため、プロペラやバッテリーなど、重要部品の故障の場合、墜落という事態に発展する。ドローンのセーフティを考える上ではこのフェールセーフの備えを行うことが最も肝要となる。 またフェールセーフを実現するためには「故障」自体を検知するための仕組みが必要となる。バッテリー状態を監視しローバッテリー状態でフェールセーフの挙動を取る、などが一般的であるが、いかに多種の「故障」を検知できるかもフェールセーフを実現するために必要な要素である。 故障発生時にその事実を捉え、安全な状態、つまり地上に復帰するための技術要素には複数のものがある。 【着陸飛行可能な故障の場合】 ・ロイター飛行 ・Return to home ・緊急着陸 【継続飛行不可な故障の場合】 ・パラシュート ・エアバッグ ・ウォーターフロート ・プロペラ停止 ・分解 最も検討すべき事象であり、本補足ではこのセーフティの要素としてこのフェールセーフに属する内容が多いものとなる。また、故障ではないものの操縦者との通信途絶、GNSS 電波喪失など、ドローンならではの障害に対してもフェールセーフを備えていくことが重要となる。

[20] 安全設計手法
https://seihin-sekkei.com/framework/saftydesign/

安全工学上の分類	概略	ドローンに適用した場合の考え方
フールプルーフ	使用者が誤った使い方（誤使用）をしても、安全性や信頼性を確保する設計の考え方。	ドローンの場合、限られた飛行範囲を守るためのジオフェンス機構や最高高度、速度設定などが当てはまる。また ADS-B 受信機の搭載により航空機付近を飛行しないよう制御する、など使用者が意図しないケースの安全性確保の観点もある。また各種センサーによる地表や障害物検知、回避機能なども含まれる。また衝突が発生しても飛行に影響を及ぼさないよう、プロペラガードを装備する、プロペラ自体を機体内側に配置するなどもフールプルーフの考えに基づく対処である。
フォールトトレランス	構成要素の一部が故障しても、製品の機能や安全性を維持する設計の考え方。一般に、製品構成やシステムを冗長化することによって目的を達成する。	ドローンの場合、古くから行われている対策としてプロペラを 5 枚以上備えるドローンがあげられる。一般的にドローンは 4 枚のプロペラが稼働していれば飛行継続可能だが 5 枚以上のプロペラが存在すれば 1 枚プロペラが破損しても飛行や帰還が可能になる。一般的には飛行バランスの観点で偶数枚である 6 枚を備えることが普通である。 また昨今ではプロペラに限らず、バッテリー、フライトコントローラ、IMU といった重要パーツを冗長化し、フォールトトレランスを高めたドローンも登場しつつある。 またフェールセーフと同様に、故障ではないが通信機能の冗長化もドローンに組み入れるべきフォールトトレランス要素となる。2.4GHz 帯のみに依存すると通信混雑時、混線なども発生する可能性があるため、別バンドの通信(920Mhz、LTE 等)を並列して備え、緊急時の操縦を可能にしておくことも重要である。

安全工学上の分類	概略	ドローンに適用した場合の考え方
フォールトアボイダンス	構成要素の信頼性を向上させる（故障しにくくする）ことにより、製品が故障しないようにする設計の考え方。	ドローンは絶えず飛行しているため、風雨の影響や振動の影響を受けることで各種パーツの劣化は激しい。フレームにカーボンのような対候性の高い素材を活用する、コネクタ類に車載規格用パーツを利用するなど、振動に強い仕組みが導入されつつある。一方で技術進歩の早いドローンでは 1 つの機体を長く利用するより、買い替えによる最新機体を導入する方が安全面でも優位性があるケースが多く、長期運用を視野に含められているケースは少ない。また対候性に対する指標として IP 指標などによる防水性能などを謳われたドローンも登場してきている。
セーフライフ（安全寿命設計）	製品寿命内で壊れないようにする設計の考え方。構造、要求コストなどの理由でフェールセーフやフォールトトレランスなどが適用できない製品で採用される。航空・宇宙機器から身の回りの製品に至るまで、あらゆる製品で採用されている。	航空機の降着装置など、フェールセーフの概念の導入が難しい機構で採用される概念だが、フォールトアボイダンスと同様、まだドローンではあまり根付いていない検討要素である。

安全工学上の分類	概略	ドローンに適用した場合の考え方
フェールソフト	構成要素に故障が発生しても、機能の一部でも維持し被害を最小限に抑える設計の考え方。	ランフラットタイヤのように損耗(パンク)が発生しても一定距離を走れる概念が当てはまるが、ドローンの場合、運用時には空中に存在するためプロペラ機では難しい。 ヘリコプターのようなシングルローター機であれば、オートローテーションのようなエンジン故障時も不時着できる機構が存在するが、マルチローター機では一般的ではなく、パラシュートやエアバッグに頼っているのが現状である。 また VTOL 機のような固定翼も備える機体であれば、故障、即墜落とはならないため、固定翼を活かした不時着方法などを検討していくことが今後の課題である。
ダメージトレランス （損傷許容設計）	構成要素の一部が損傷（疲労、摩耗、亀裂など）しても製品の安全性や機能を維持し、その上で適切な期間でメンテナンスを行う設計の考え方。	ドローンの場合、プロペラやバッテリーは使用を繰り返すことでダメージが蓄積していく部品になり定期的な交換が必要になる。他のフレームやフライトコントローラ等はフォールトアボイダンスと同様、長く使うよりは機体そのものを入れ替えることが一般的でメンテナンス観点ではまだ十分なノウハウが蓄積されているとは言えない状況である。

8.2. ドローンの事故発生状況

8.2.1. 著名な事故

首相官邸でのドローン落下事件[21]はドローンを直接規制する法律が事実上存在しないことを露呈させたが、一般の人にドローンの存在を広く知らせることになり、その後のドローンの産業活用が広がるきっかけにもなった。この件も含め、著名なドローン事故について振り返る。

	事故	時期	場所	事故内容
1	首相官邸にドローンが落下	2015 年 4 月	首相官邸	首相官邸の屋上で、小型の無人航空機（ドローン）が落下しているのが見つかり、警視庁が機体を調べた結果、微量の放射性セシウムを検出した。
2	姫路城にドローンが衝突[22]	2015 年 9 月	兵庫県姫路市	巡回中の警備担当者が、南から北に飛行するドローンを発見し、ドローンが大天守に衝突するのを目撃した。ドローンはそのまま大天守の 5 階の屋根上に落下しており、漆喰壁や屋根瓦などに被害はなかったが、窓枠の一つにある「水切り銅板」に傷が見つかった。
3	ドローンで国内初の人身事故[23]	2017 年 2 月	神奈川県藤沢市	建築現場を空撮するために飛行していたドローンが、高さ約 70 メートルの場所でクレーンに接触して墜落し、30 代の男性作業員に衝突した。作業員は顔に大けがを負った。国土交通省に報告があったドローンの事故では、初めての人身事故とされている。

[21] 首相官邸でのドローン落下事件
https://www.nikkei.com/article/DGXLASDG22H82_S5A420C1EA2000/

[22] 姫路城にドローンが衝突
https://www.huffingtonpost.jp/2015/09/19/himeji-castle-drone_n_8162222.html

[23] ドローンで国内初の人身事故
https://www.nikkei.com/article/DGXLASDG28H2L_Y7A220C1000000/

4	イベントの上空からドローンが落下[24]	2017 年 11 月	岐阜県大垣市	上空から来場者に菓子をまいていたドローンが約 10 メートルの高さから落下し、5～48 歳の男女 6 人が額や肩を擦りむくなどの軽傷を負った。ドローンは菓子約 100 個を入れたかごを取り付けていた。午前 11 時半ごろにも 5～10 分間の飛行を 4 回繰り返して菓子をまいたが異常はなかったという。ドローンによる菓子まきは 5 日も実施予定だったが、中止となった。
5	ドローンの飛行により空港の滑走路を封鎖[25]	2019 年 10 月～11 月	大阪府泉佐野市	関西空港の第 2 ターミナルで 11 月 9 日朝 8 時ごろ、複数の地上作業員がドローンのようなものを目撃した。約 10 分後、2 本ある滑走路は閉鎖された。空港を運営する関西エアポートや警察、海上保安庁が機体を捜したが見つからず、約 1 時間 10 分後に離着陸が再開された。国内線の 2 便が欠航し、国内・国際線の 17 便が目的地変更するなど、計 44 便に影響が出た。関空ではこの他にも、10 月 19 日夜に約 40 分間、11 月 7 日夜にも 2 回にわたって計約 2 時間、滑走路が閉鎖された。

[24] イベントの上空からドローンが落下
https://www.nikkei.com/article/DGXMZO23115890U7A101C1CN8000/

[25] ドローンの飛行により空港の滑走路を封鎖
https://www.asahi.com/articles/ASMD14QRGMD1PTIL006.html

6	大分のドローン重傷事故で調査官を初指名[26]	2023 年 7 月	大分県九重町	大分県九重町で訓練飛行中のドローンが、近くの電柱に接触、操縦者が右手の骨を折る重傷を負った。国交省は無人航空機の事故に認定。運輸安全委員会は航空事故調査官 2 人を指名した。ドローン事故で調査官が指名されるのは初めて。 国交省によると、令和 4 年 12 月施行の改正航空法でドローンの事故は国交相への報告義務が課されている。これまで負傷して重大インシデントになったケースはあったが、重傷を負って事故と認定されたのは初。
7	列車にドローン衝突、緊急停止　けが人なし　操縦者が回収[27]	2023 年 7 月	福島県猪苗代町	猪苗代町西舘の JR 磐越西線の踏切付近で会津若松行きの快速列車がドローンと衝突し、緊急停止した。列車は 2 両編成で、車内には乗客がいたが、乗客と乗員にけがは無し。車両の点検を行ったところ、車両の破損もないため、停止して 15 分後に運転を再開した。 ドローンの飛行目的は不明であるが、その後、近くにいた操縦者により回収された。

[26] 大分のドローン重傷事故で調査官を初指名
https://www.sankei.com/article/20230719-PLAE5HPNAVOXLHKZKR6UIGFGKI/

[27] 列車にドローン衝突、緊急停止　けが人なし　操縦者が回収
https://newsdig.tbs.co.jp/articles/-/628374?display=1

8.2.2. 国内統計事例（改正航空法施行前）

2019 年度から 2021 年度までの「無人航空機に係る事故等の一覧（国土交通省）」[28]をもとに、NEC ソリューションイノベータにて分類・分析を実施した。

事故状況を、「墜落」、「紛失（墜落）」、「木・建物等への衝突」、「その他」で分類すると、墜落と衝突は同程度の比率で二分されるが、2021 年度においては墜落後紛失に至るケースが激増している。

また、事故原因を、「操縦ミス」、「バッテリー切れ」、「整備不良」、「機体制御不能」、「機体等の故障」、「通信途絶/GPS ロス」、「強風・突風」、「鳥攻撃」、「その他」で分類し、「人為的ミス（操縦ミス、バッテリー切れ、整備不良）」、「機体異常（機体制御不能、機体等の故障）」、「通信異常（通信途絶/GPS ロス）」、「自然現象・鳥（強風・突風、鳥攻撃）」の比率を見ると、人為的ミスが 50%以上を占めるが、機体異常、通信異常の比率が増加傾向にある。

[28] 無人航空機に係る事故等の一覧(国土交通省)
改正航空法により無人航空機の事故等の報告が義務化される前に国土交通省に報告されていた情報。改正航空法の施行に伴い、現在は令和 4 年 12 月 5 日以降に報告のあった事案が公開されている（令和 4 年 12 月 4 日以前の情報は含まれていない）。

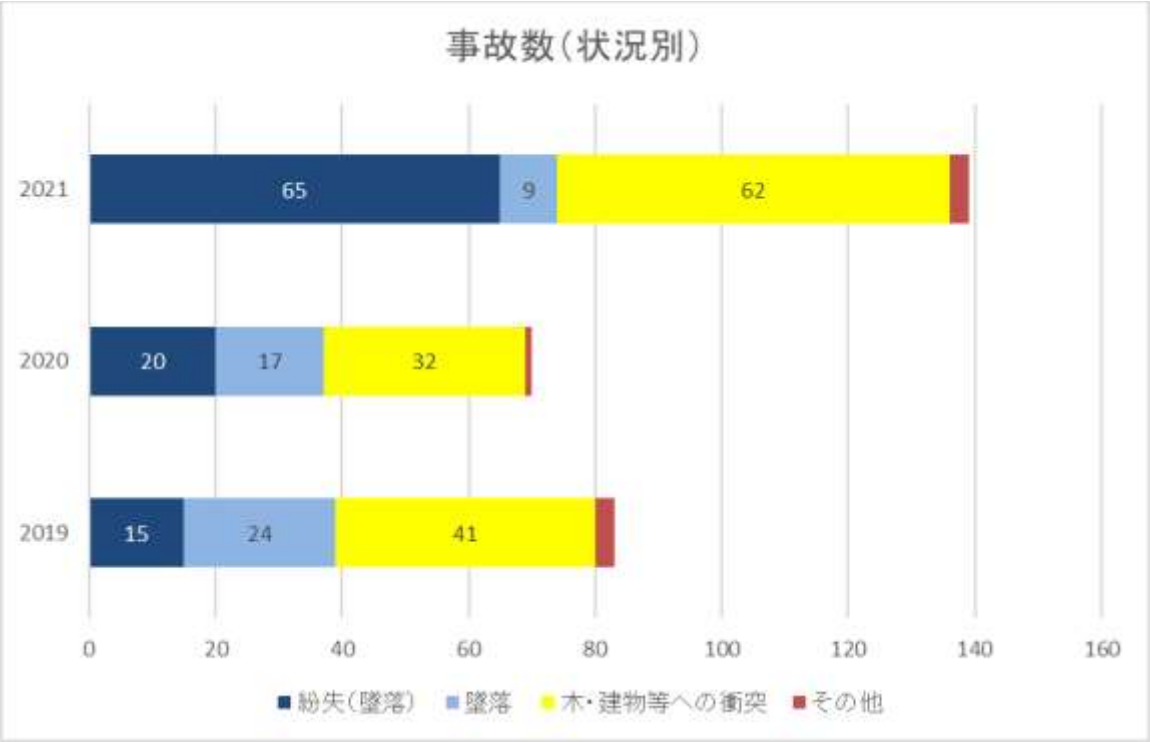


図 34：年度別の無人航空機事故数（状況別）

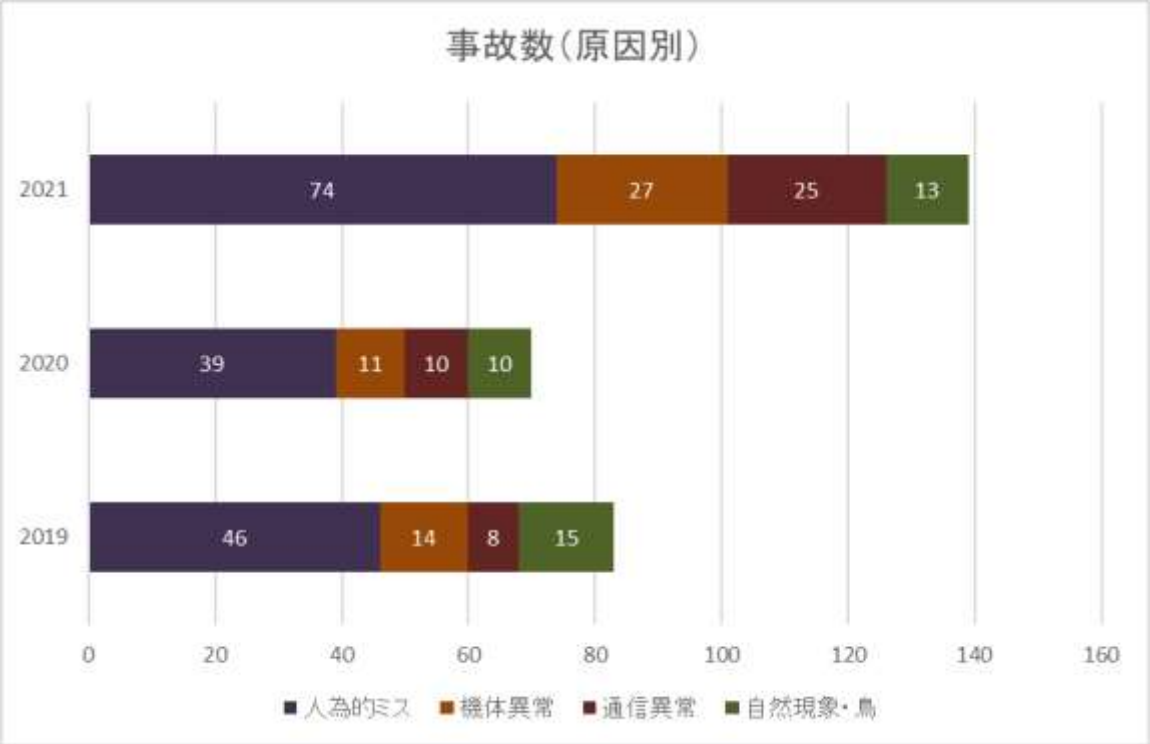


図 35：年度別の無人航空機事故数（原因別）

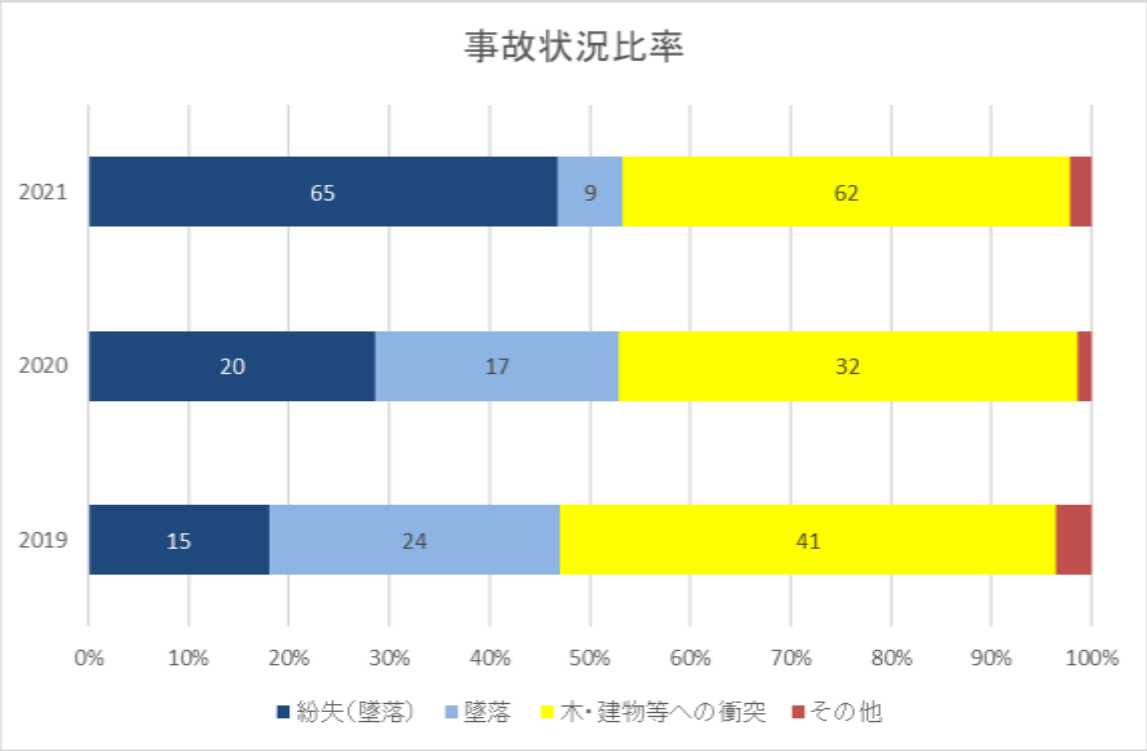


図 36：年度別の無人航空機事故状況比率

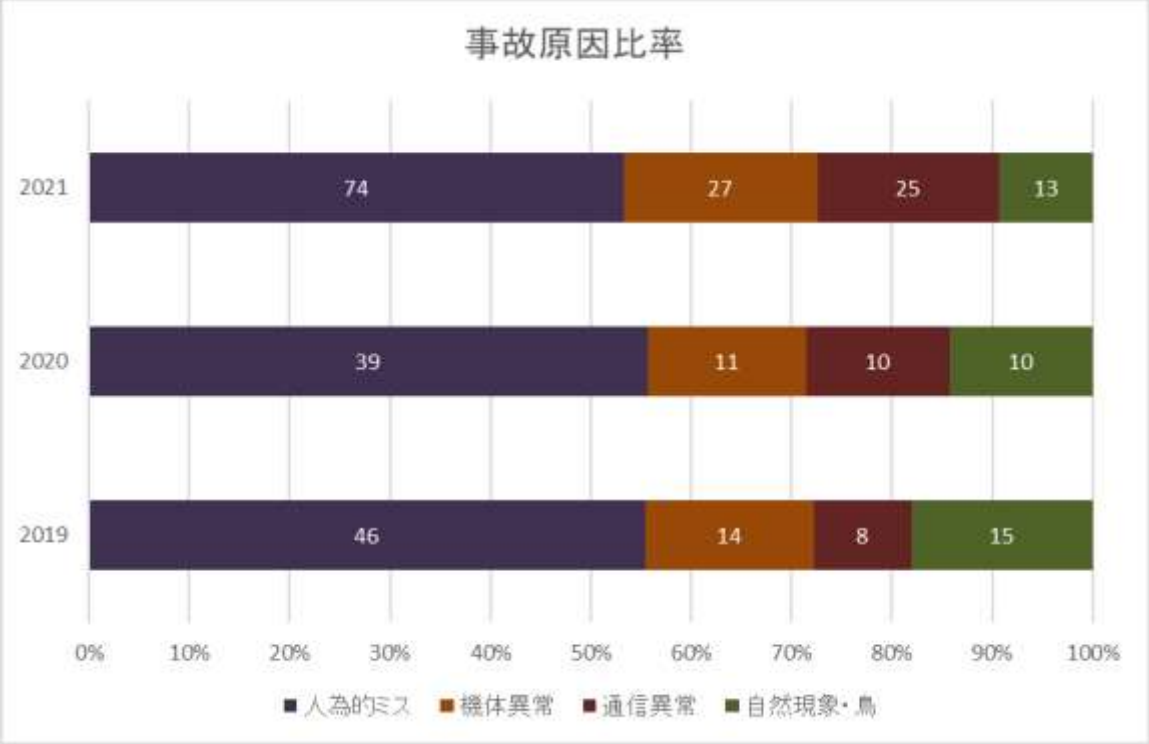


図 37：年度別の無人航空機事故原因比率

A） 事故原因

国土交通省の公開している事故情報より、事故の傾向が確認できるが、原因追及までいたっていないものも多い。ここでは、一般的に取り上げられている事故原因について紹介する。

①機体の障害

制御不能となる事故のうち利用者側では究明困難な原因としてドローン本体の異常が考えられる。

・フライトコントローラの物理的故障
・ソフトウェアの誤動作
・プロペラの破損
・モーターの停止（配線類の断線等）
・ESC の故障
・バッテリーの突然死

②通信の異常

ドローンにおける通信にはコントロールライン、テレメトリー通信、FPV(映像)配信の 3 種類がある。通信異常の発生は各通信に影響を与え、事故の発生につながる。

コントロールラインでの通信が確保できない場合、ドローン操縦の制御が困難になる。テレメトリー通信が遮断されると、ドローンの飛行状態（高度、スピード、バッテリー残量等）が確認できず、構造物への衝突や墜落につながる。FPV(映像)配信が途絶すると、特に目視外飛行を行っている場合にカメラ映像による位置確認ができず、墜落に至った場合、機体の紛失につながる。

通信途絶が生じやすいケースとして、ドローンと操縦者の間に遮蔽物がある場合や強い電波を発する鉄塔の周辺を飛行する場合が考えられる。また、通常、GPS 信号によって自己位置を把握しながら飛行するため、深い渓谷や山間部などで GPS 信号をうまくキャッチできない場合に操縦が困難になることがある。

・電波干渉等による電波障害
・GPS エラー

③自然現象や鳥の影響

突発的に発生する自然現象や鳥の行動は予測することが難しく、咄嗟の事態に素早く対応できない場合に事故につながる可能性がある。

・突発的な強風
・急な雨

・鳥の襲撃や鳥との衝突

操縦者のスキルにも関連するが、海上での低空飛行時に波にさらわれる可能性もある。

④メンテナンス不足

飛行前に機体の整備・点検を実施しなったことにより機体の異常に気付くことができず、飛行中の事故につながる可能性がある。

・高度不足やスピードの出しすぎ

・飛行中のバッテリー消耗確認漏れ

・飛行中周囲の確認不足

・RTH 動作の理解不足

・自律飛行時の航路設定不備

B） 事故による損害

国土交通省の公開している事故情報より、事故に伴いどのような損害・傷害が発生しているか拾い上げてみた。

●機体の紛失・破損

●電線／電話線の切断・損傷

●民家の家屋／屋根／外壁／アンテナ／ソーラーパネルの損傷

●園芸ハウスの窓ガラス損傷

●車両の損傷

●墓石の損傷

●火災発生による竹藪延焼

●操縦者／補助者のけが

2019 年度～2021 年度の事故の被害・損害状況を見てみると、約 8 割は第三者への影響がなかったものの、約 2 割は第三者に被害・損害を与えている。第三者への被害・損害の種類を「物損事故（建物、電線、車両）」、「人身事故」、「火災」に分類すると、物損事故が約 8 割を占めるものの、ケガや火災に至るケースも発生している。

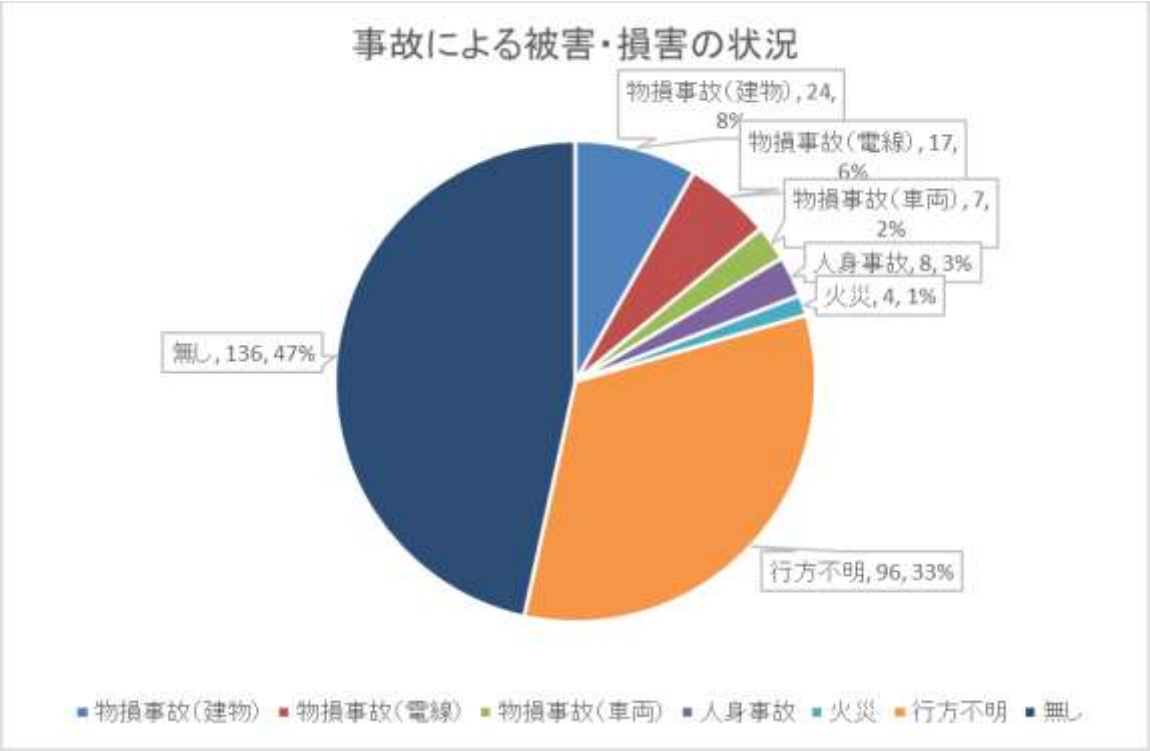


図 38：事故による損害・被害の状況

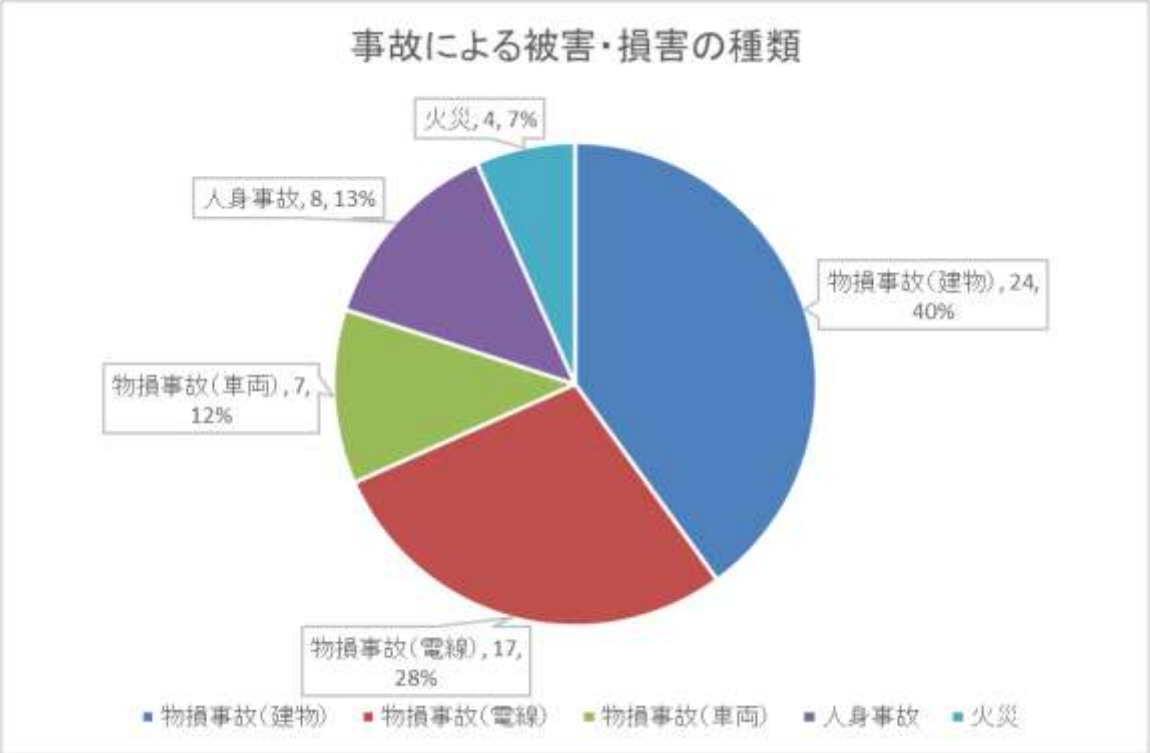


図 39：事故による損害・被害の種類

8.2.3. 国内統計事例（改正航空法施行後）

2022 年 12 月 5 日に改正航空法が施行され、無人航空機に関する事故等の報告が義務化された。改正航空法施行後に報告のあった事案については無人航空機に係る事故等報告一覧[29]にて公開されている。なお、報告内容は「事故」と「重大インシデント」に分類される。

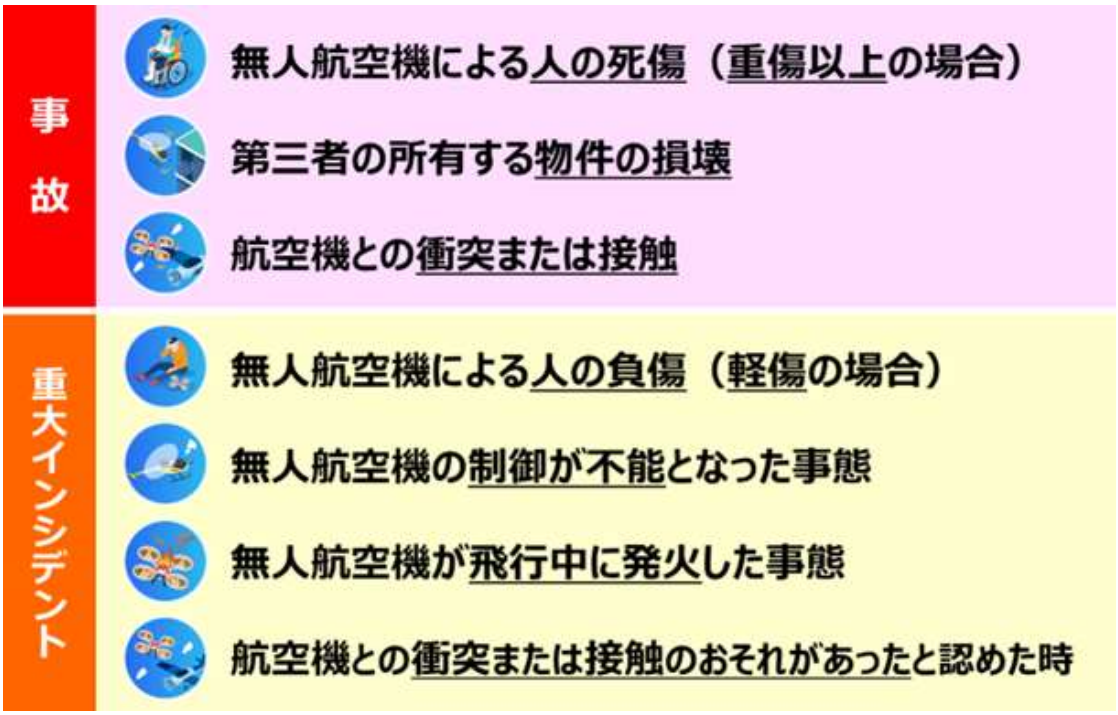


図 40：無人航空機　事故報告内容の分類

重大インシデントとして報告された事案のうち、非該当となるケースが多数あることから、国土交通省では「無人航空機の制御が不能になった事態」に該当しなかった事例を、よくある非該当事例として紹介している。

・単純な操作誤り（飛行経路の設定ミス、目測誤り等）によって墜落した事案

・自動帰還機能が作動し、帰還中に樹木に衝突する事案のうち、帰還経路や高度設定を飛行前に確認することで回避可能だったと思われる事案

・飛行前点検が不十分だったことが明確である事案

非該当事例の扱いに伴い、国交省に報告のあった事案の多くが「無人航空機に係る事故報告一覧」に掲載されないため、事故の傾向が改正航空法施行前とは異なった見え方となる。

[29] 無人航空機に係る事故等報告一覧
https://www.mlit.go.jp/common/001585162.pdf

改正航空法施行前（2021 年度分）と比較すると墜落するケースが大幅に減少しているが、何らかの対策により墜落事故が減ったということではなく、非該当事例として扱われたことにより隠れてしまったと考えられる。また、事故原因についても、機体制御不能、通信途絶、強風・突風が大幅に減少しているが、非該当事例の事案に多い原因であると考えられる。

なお、重大インシデントとして扱われる「無人航空機の制御が不能となった事態」については、原因不明が 19 件中 3 件のみであり、改正航空法施行前より原因が特定された状態で情報が公開されている。残り 16 件の内訳は以下の通りである。

	原因	件数
ソフトウェア関連	飛行制御の不具合	1
	位置制御の不具合	1
	姿勢制御の不具合	1
	速度検知の不具合	1
ハードウェア関連	モーター故障	5
	バッテリー故障	3
	ESC 故障	2
	アンテナ故障	1
	アーム破断	1

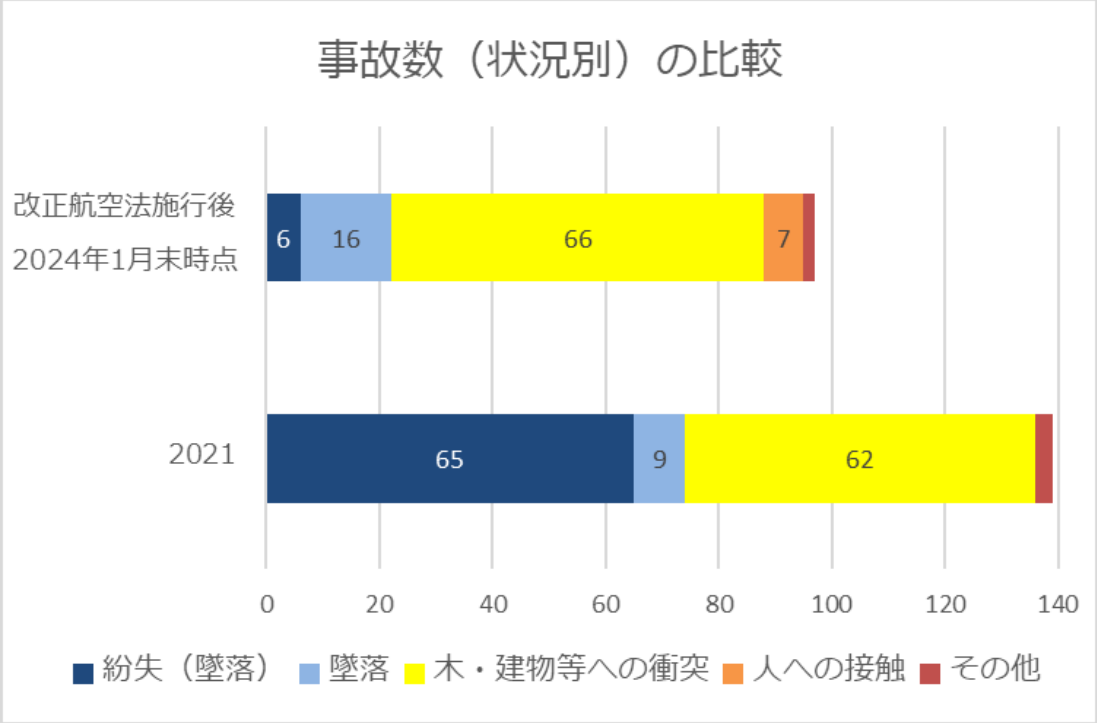


図 41：事故数（状況別）の比較

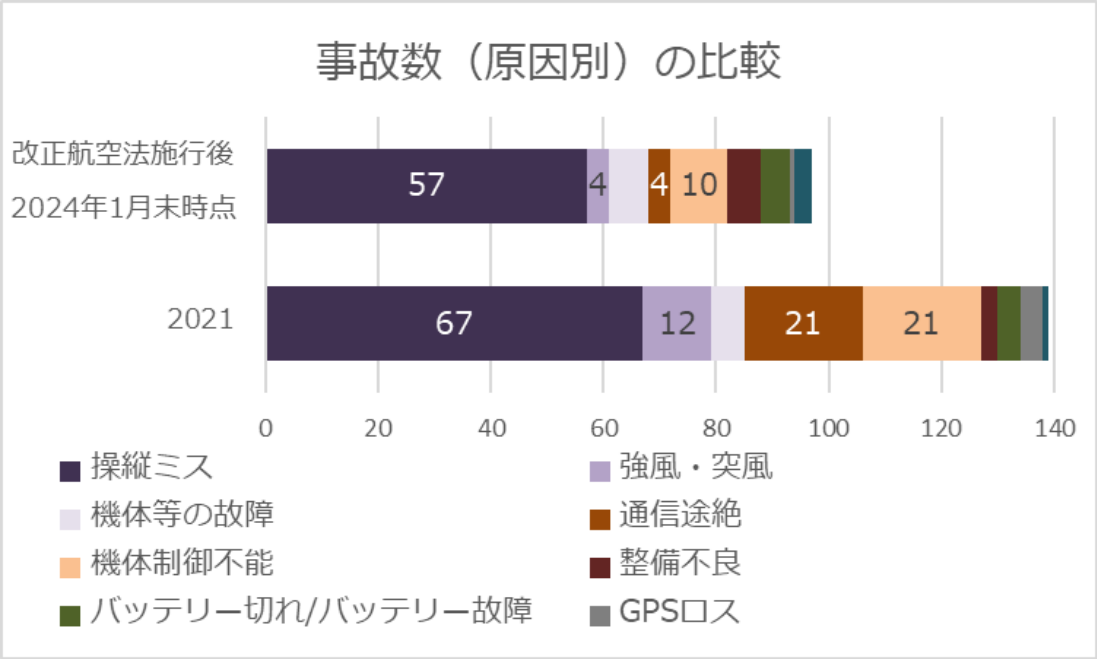


図 42：事故数（原因別）の比較

8.3. 事故のパターン

8.3.1. 電波の喪失

電波を喪失するとドローンを操作することができなくなる。特に遠隔地から目視外で操作している場合、状況の確認もできなくなるため、対策の重要性が高くなる。ドローンの操縦用としてよく使用される 2.4Ghz 帯は、Wi-Fi 通信など多くの機器でも使用されており、とくに市街地では電波干渉にも注意する必要がある。対策としては、通信経路を複数用意する多重化や電波喪失時の動作としてホームポイントへの帰還などを行う設定をしておくことが考えられる。

8.3.2. 電源の喪失

電源を喪失するとドローンは墜落する。バッテリーは劣化や真冬の低温環境などにより、電圧が急激に低下することがあり、事故につながることがある。事前の点検や低温環境での飛行時はバッテリーを飛行前に温めておくなどの対策が必要である。飛行計画はバッテリー容量を考慮した経路、緊急時の退避場所、方法を策定しておき、飛行中はバッテリーの状態（残量、低下速度）には十分注意をしておくことが必要である。

8.3.3. 衝突

A） 建造物

操縦位置からドローンが離れると距離感が掴みにくくなるため、建造物が見えていても衝突することがある。また、ドローン用モニタにてドローンのカメラ映像に集中してしまうと、飛行中ドローンの周囲の環境への配慮が不足し、ドローンの飛行方向を変える際に、建造物に衝突することがある。また、手動または自動で RTH 機能を作動させる場合、飛行位置から飛行開始位置まで一直線に帰還するため、途中に構造物があると衝突する。

B） 電線

農薬散布機による事故報告のほとんどが電線への接触、電線の切断である。電線との距離を見誤ったり、背景と電線が同化し視認できなかったり、操縦者と離れた位置で指示を行う補助者との連携がとれなかったり、人為的な原因が多くを占めている。

C） 鳥、航空機

カラスやトンビは巣の周囲に近づいた物体を敵と見なして攻撃する習性があると言われており、繁殖期での卵や雛を守るための攻撃や好奇心による接近が見られる。カラスの群れによる襲撃や翼開長が 150cm にもなるトンビの衝突により、プロペラが破損して墜落にいたる。衝突に至らないまでもドローンとヘリコプターや航空機との接近事例はある。人命救助でヘ

リコプターが降りてくることがあり、また、空港近辺は飛行禁止区域であるが、許可申請を受けて飛行させる場合も離陸着陸時は低い高度のため、注意が必要である。

8.3.4. 墜落

ドローン落下による周辺住民への危害が懸念される。手動より自動、無人より有人のほうが被害は大きくなる。機体を墜落させてしまった場合、機体を回収する必要があるが、回収しない場合あるいは回収できない場合、以下のような問題が生じる可能性がある。

・情報漏洩のリスク（飛行情報や撮影データの記録された SD カードの盗難）
・廃棄物処理法違反の可能性（紛失時に適切な処理を行わない場合）
・海洋汚染や火災の原因
・機体保険の補償対象外（機体破損のエビデンス無し）

墜落させないことが一番であるが、墜落状態に陥った場合の被害軽減策としてドローン用パラシュート／エアバッグの搭載が考えられる。また、墜落位置を詳細に特定するために、事故発生直前までの飛行経路を確認する手段を確立しておくこと、通信途絶を回避するための通信の冗長化対策を行うこと、位置情報を発信するビーコン装置を搭載することなどが考えられる。

落下要因は自然災害や部品破損等、偶発的要因と第三者による意図的要因がある。前者が機能安全、後者がセキュリティに起因している。

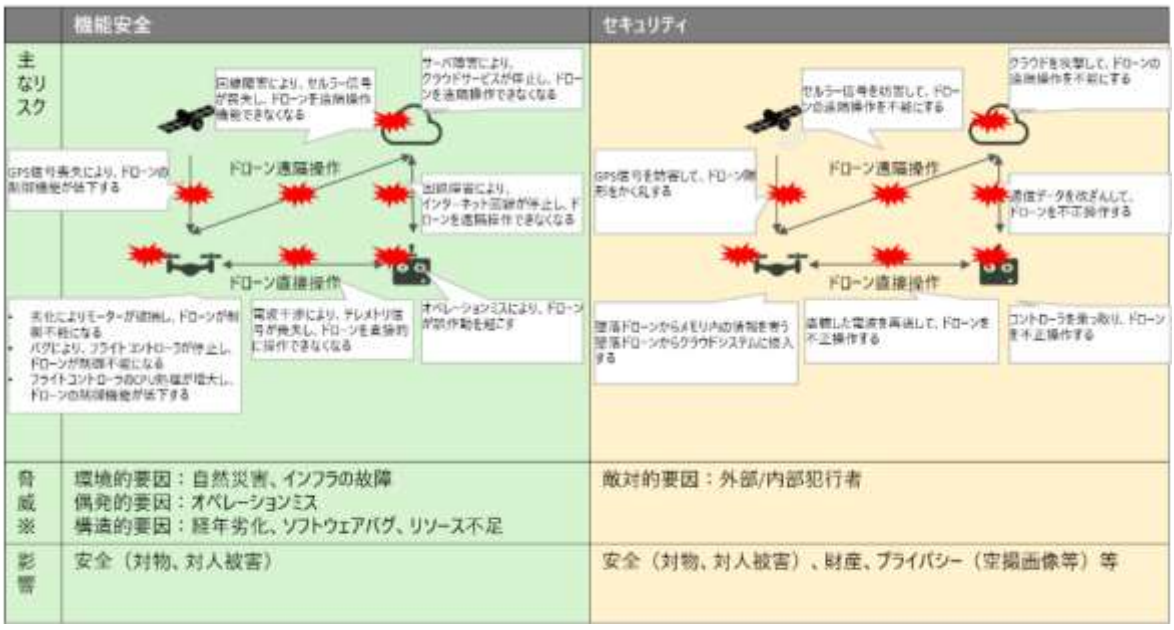


図 43：レベル 3,4 を想定したドローン運行時におけるリスク、脅威、要因の違い

「8.2.2. A）事故原因」に起因して発生する墜落事故以外に、飛行目的や飛行環境に特有のパタ

ーンがある。

A） 地面

地面すれすれでドローン撮影を行う場合に土地の起伏への配慮不足があったり、ドローンを着陸させる場合にプロポの操作ミスによる急降下が生じたりして、地面に激突する可能性がある。また、ドローンなどの回転翼機が垂直に降下するとき、吹き下ろした空気が再び吸い込まれ、回転翼の上下に循環する空気の渦が生じ、急激に揚力を失って失速する状態（ボルテックスリングステート）が発生し、墜落につながる可能性がある。

B） 山中

山中は、樹木や送電塔、鳥など平野部とは違った障害物が多い。特に樹木に関して、標高図で地面の高さがわかっていても木々の高さはわからないため、木々へ衝突して、墜落する可能性がある。また、山中という立地の影響から電波障害が生じる可能性が高く、操縦不能による墜落のリスクもある。墜落した場合、機体の捜索にコストが掛かるだけでなく、バッテリーの発火から山火事を起こす恐れもあり、墜落時のリスクも高い。

C） 水没

川や海において水面近くを飛行させる場合、水面かどうかの判断が目視では視認が難しく、またカメラでは遠近の距離感がつかみにくく、水中に突入してしまうリスクがある。また、海において水没してしまうと捜索が困難となる可能性が高くなる。

8.3.5. 故障

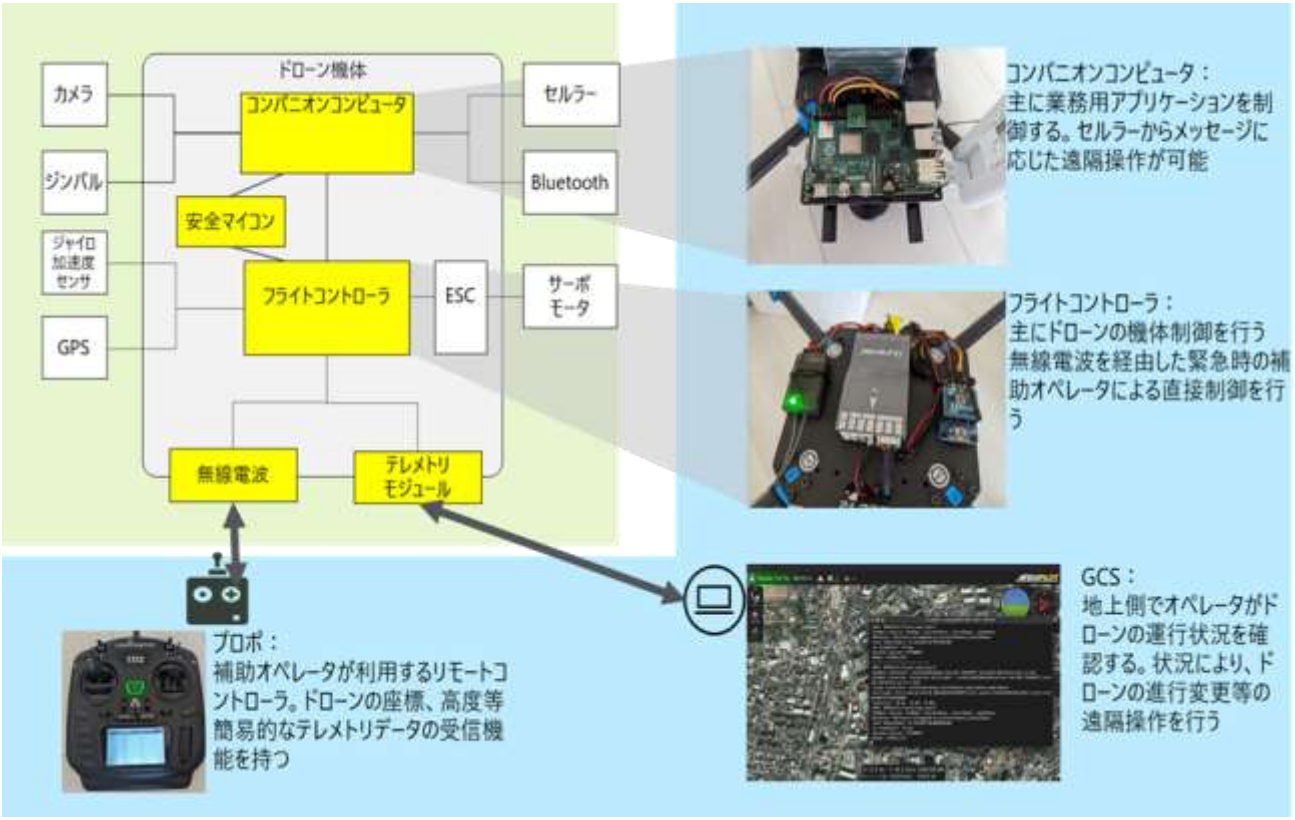


図 44：ドローン機体と周辺機器の構成

A） フライトコントローラ

フライトコントローラは機体の制御を行う心臓部であるため、故障が発生すると致命的である。フライトコントローラの障害としては、ソフトウェア、ハードウェアの障害の両方を考慮する必要がある。搭載センサーを二重化しているものもある。しかしながらすべてのハードウェアの障害やソフトウェアの障害に対応することは難しいため、追加の安全対策が必要となっている。

(1) GNSS

GNSS に異常が発生すると、GNSS による自己位置推定ができなくなるため、自動飛行や飛行制御に影響が出る。受信機の故障以外にもビルや山などにより十分な数の衛星からの電波を受信できない状態やマルチパスによる測位誤差が問題となることがある。

(2) ジャイロ・加速度センサー

ジャイロ・加速度センサーに異常が発生すると自己位置推定ができなくなるため、自動飛行や飛行制御に影響が出る。フライトコントローラの機種によっては、障害への対策と

して機体制御に必要な IMU などのセンサーを二重化しているものもある。

B） 無線電波・プロポ

手動操縦用の無線電波・プロポが故障すると手動操縦が不可能となる。対策として二重化構成や通信途絶時のフェールセーフ動作を設定しておくことが考えられる。

C） テレメトリーモジュール・GCS

テレメトリーモジュール・GCS が故障すると自動飛行の制御や機体の状態が不明となる。対策として二重化構成やフェールセーフの設定、可能であれば手動操縦での緊急避難を行うことが考えられる。

D） ESC・サーボモーター

ESC・モーターに異常が発生すると機体制御が難しくなるため、対策として双方向 ESC によるモーターの状態を監視できるようにし、6 発機など、一台が故障しても飛行を継続できる構成とすることが考えられる。故障としては過負荷による焼損などのモーター自体の故障、振動や衝撃による断線、モーターを制御する ESC の故障が考えられる。

E） コンパニオンコンピュータ

コンパニオンコンピュータの障害としては、ソフトウェア、ハードウェアの障害の両方を考慮する必要がある。コンパニオンコンピュータに担わせている機能が不能となるため、機能によっては二重化や安全対策を行う必要がある。

(1) LTE

LTE 通信に障害が起こると、遠隔地からの操縦や機体状態の監視が不能となる。特に目視外での活用をしている場合、危険性が大きくなる。

(2) 救難ビーコン

遺失時捜索用の救難ビーコンなどを搭載していた場合、その故障が発生すると万一の遺失時の捜索手段が失われる。飛行中に随時、救難ビーコン用電源の確認や電波が発せられているかの確認手段が必要である。

(3) パラシュート

パラシュートの開傘をコンパニオンコンピュータから制御している場合、コンパニオンコンピュータの故障により万一の際の開傘が行えない可能性が生じる。パラシュート

自体の定期点検のほか、コンパニオンコンピュータとの結線状況の確認が電子的に行えるようになっていることが望ましい。

(4) 画像解析装置

近年では電線点検用に電線をコンパニオンコンピュータで認識しつつ飛行を行うような仕組みも実装されつつある。こういったドローン誘導の仕組みをコンパニオンコンピュータで担っている場合、その機構が失われた場合の挙動についてもフェールセーフを意識しておく必要ある。本用途では電線近傍を飛行している状態が想定されるため、安易な RTH や着陸は危険なケースも想定される。

F）バッテリー

経年劣化による動作異常、取り付け・接触不良に起因する機体振動等による機体電源の断絶、内部基板の偶発故障等が実際に発生しており、いずれも電源喪失に陥り、プロペラ停止・墜落に至っている。バッテリー異常は機体の墜落に直結するため、定期的なバッテリー交換、入念な取り付け・接続確認、飛行前のバッテリー点検等、安全への十分な配慮が必要である。

8.4. 事故による損害

ドローンの事故に対しては法律上の責任が伴う。その責任には 3 つの観点がある。[30]

①民事責任

民事責任とは、事故により第三者の建物を傷つけたり、物を破壊したり、人体を傷つけた場合に、それを補償する責任である。

②刑事責任

刑事責任とは、刑事法により禁止された行為を行う事で、罰金や懲罰などの刑罰を受ける事を言う。ドローンによって故意に人を傷つけると「暴行罪」「傷害罪」に問われる。

③行政上の責任

行政上の責任は、自動車と違ってまだ、ドローンを飛行させる免許は入らないが、運用上必要となる無線免許等の許認可取り消しになる等の、不利益処分を言う。

[30] 法律上の責任
https://amatatu-i.hateblo.jp/entry/lesson25

8.4.1. 物損事故

国土交通省の公開している事故情報では、多くの物損事故が報告されている（「8.2.2. B） 事故による損害」参照）。

ニュース報道されたものとしては、2015 年 9 月に発生した姫路城への衝突事故[31]がある。

- 2015 年 9 月 19 日、兵庫県姫路市にある世界遺産・姫路城の大天守最上層の南面にドローンが衝突し、そのまま大天守の 5 階の屋根上に落下。漆喰壁や屋根瓦に被害は確認されていないが窓枠の一つにある「水切り銅板」に傷が見つかった。

8.4.2. 人身事故

ニュース報道された代表的な事故として、2017 年 2 月に神奈川県藤沢市の工事現場で発生した初の人身事故[32]、2017 年 11 月に岐阜県大垣市のイベントで発生した墜落事故[33]がある。

- 2017 年 2 月 18 日、神奈川県藤沢市の建設工事現場を空撮するために飛行していたドローンが墜落し、男性作業員に衝突した。作業員はヘルメットを着用していたが、顔を数針縫うけがを負った。

- 2017 年 11 月 4 日、岐阜県大垣市で開催されたイベント「ロボフェスおおがき 2017」で、上空から来場者に菓子をまいていたドローンが 10m の高さから落下し、5～48 歳の男女 6 人が額や肩を擦りむくなどの軽傷を負った。

8.4.3. 火災

ドローンで使用されるリチウムイオンポリマーバッテリーが落下の衝撃で損傷し、発火したと推測される事故が発生している。

---

[31] 姫路城への衝突事故
https://www.huffingtonpost.jp/2015/09/19/himeji-castle-drone_n_8162222.html

[32] 神奈川県藤沢市の工場現場で発生した初の人身事故
https://droneagent.jp/flights/2017dronenews

[33] 岐阜県大垣市のイベントで発生した墜落事故
https://www.nikkei.com/article/DGXMZO23115890U7A101C1CN8000/

- 2017 年 11 月 21 日、埼玉県秩父市にある東京大学大学院農学部生命科学研究所の演習林で、ドローンの落下に伴う森林火災が発生した。秩父消防本部によると、少なくとも約４ヘクタールの演習林の下草などが燃えた模様。近くに住宅などはなく、負傷者や家屋への被害はなかった。[34]

8.4.4. 行方不明

国土交通省の公開している事故情報では、ドローンが行方不明になる事故が多数報告されている。ドローンを紛失した場合、その捜索がどれだけ大変なことであるかを示す事故がニュース報道されている。

- 2020 年 11 月 14 日、大分県の日出生台演習場で夜間訓練を行なっていた陸上自衛隊がドローン 1 機を紛失した。捜索の結果、演習場外の北側およそ 300m 付近にある木の枝に引っかかった状態でドローンが見つかっているが、1000 人態勢で捜索が行われていた。[35]

8.5. ドローンにおけるセーフティ対策要件

ドローン活用シーンでのセーフティは機体の機能だけで実現するのではなく、その管理、運用まで含めて検討することが肝要である。ここでは、機体制御、機体管理、情報処理の 3 点に分解して説明する。

8.5.1. ドローンにおけるセーフティ対策の要件

A） 機体制御

機体制御におけるセーフティ実現のために必要な要素として、まずセーフティを脅かす要因を検知する必要がある。その上で検知結果に基づいて自律的な回避動作を行うことが機体制御に求められるポイントとなる。

[34] ドローンの落下に伴う森林火災
https://drone-school-navi.com/news/wa201712191/

[35] 陸上自衛隊のドローン紛失と捜索
https://droneowners.jp/dronesdf/

セーフティを脅かす要因	検知方法	回避方法
障害物に接しそうになった	・障害物検知用可視カメラ ・赤外線カメラ ・超音波センサー ・ADS-B などの受信による航空機回避	操作者の操作とは別に自律的に回避行動をとる
ローバッテリー	・バッテリー電圧やインテリジェントバッテリーによる残量検知 ・飛行時間による飛行可能時間割り出し	帰還可能な範囲である場合は Return To Home。 帰還困難な場合は緊急着陸。
プロペラ破損	・双方向 ESC によるモーター推力の異常検知 ・IMU による機体の傾き検知	残ったプロペラに適切に推力を割り当て、平衡飛行を継続
通信途絶	・GCS やプロポとの通信状態を RSSI 等によりアルタイムに把握する	・一つでも通信路が失われた場合の警告 ・Return To Home や緊急着陸
機器異常	・GPS や IMU など、リアルタイムに更新されるべき情報の非更新を感知 ・機器の電気的な異常を検知	・飛行継続可能な場合は緊急着陸 ・飛行継続不可の場合、パラシュートやエアバックを展開しての着陸
飛行範囲逸脱	・バーチャルフェンスによる飛行範囲逸脱検知	・飛行可能範囲へ自律的に復帰 ・緊急着陸

B） 機体管理

ドローンは複数の機器が集合した移動体であり、自動車と同じように定期的なメンテナンスが必要となる。バッテリーやプロペラなど、使用に伴い損耗が進んでくるデバイスの定期チェックはもちろん、稼働ログなどから他の構成要素の稼働状況をチェックするなどの検査も必要である。また、そういった地上での管理の他に、飛行中の稼働状況をチェックすることも肝要である。これはドローン同士の衝突を回避するための空域の分離などの概念も含まれる。現在は地上側コントロール端末(GCS)や、事前の空域登録(DIPS 2.0)で運用者が個別に管理

している実情であるが、リモート ID からの発信情報を元に UTM で統合的に管理するなどが今後検討されていく領域になる。

C） 情報処理

一般的にドローンはカメラを備え、空撮映像を自己に保存していることが多い。そのため万一の墜落・紛失時には同時に情報セキュリティ事故となりうる可能性があり、この点に留意が必要である。運用者視点では以前の撮影情報をドローンに入れたままにしない、などの対処を行っておく必要がある。また、墜落と判断したら自動的に映像を消去する、あるいは暗号化された状態で保持されるようにし、紛失時に情報セキュリティ観点での事故にならないような配慮が必要となる。情報セキュリティ観点の留意事項は本書本編に詳しく記載している。

8.5.2. ドローンのセーフティ対策のステップ

A） ドローン機体メーカー

現在でも障害物の回避動作を行うための機体用赤外線や可視カメラの装備などは機体メーカー側で行われている。今後も機体メーカー主導でセーフティ要件を満たす検知機構、回避機能は実装されていく流れではあるが、まだ完全な自律制御には至っておらず、今後、一部の機能においてはオプショナルな機構がサードパーティから販売されていくことも検討されている。現状はバッテリーや障害物に対する備えが中心であるが、フライトコントローラ、モーター、IMU、GPS、プロペラ、通信機構など多くの構成要素からドローンは成立しており、それぞれの機構の故障にも備えることが必要とされてきている。

特に通信機構や GPS は電波を受信することで機能を発揮する機構であるため、故障ではなくとも電波を喪失することは通常運用においても発生しうる。通常の 2.4Ghz 帯だけではなく、機体機能として多様な通信経路で冗長化しておくことが電波喪失の備えにつながる。

B） ドローンサービス提供事業者

機体管理の項目を着実に実施していくことが肝要となる。特に複数ドローンを運用している場合、それぞれの損耗判断や飛行状況のリアルタイムな把握が欠かせない義務となってくる。そのための情報収集手段を整備し、情報を整理、保存しておくことで万一の事故発生時の分析にも活用できる。

C） ドローン活用ユーザ

衝突回避機能やジオフェンス機能、RTH の適切な運用など、現在実装されている機能を有効に利用していくことが重要である。RTH の高度なども利用状況によって変更の必要がある

が、一度設定されたものをそのまま運用し続ける状況も散見される。飛行プラン毎に見直していく運用が肝要である。また補助者の適切な配置、万一の事故発生時の連絡先一覧の準備、保険の用意など、活用ユーザ側で検討しておくべき項目を飛行毎にもれなく運用していく体制構築が必要である。

8.6. 活用シーン別のセーフティ

8.6.1. 空撮

撮影場所、目的によっては、第三者の立ち入りに十分気を付ける必要がある。

また、他の用途と比べるとより高い高度で飛行させるケースが多いと考えられる。高度が上がるほど風の影響を受けやすく、また電波が届かない事態にいたる可能性も高まる。飛行姿勢をくずす、また通信途絶が発生すること等により墜落に至る場合、操縦者からかなり離れた位置となる可能性が高く、紛失する可能性も高まる。突風等の影響により飛行バランスが崩れた場合の対策として、飛行姿勢の監視や姿勢異常時のアクション設定（RTH、設定ポイントへの着陸等）、通信途絶への対策として通信経路の多重化が考えられる。

8.6.2. 物流

山間部や離島での物流シーンでは、遠隔制御での目視外飛行となる。この場合、電波障害による機体状況の把握ができなくなるケースが考えられる。また、離島や山間部での飛行においては、天候の変化や異常発生時の避難場所を確保することが困難である。事故発生時の人的被害のリスクは低いが、山間部では山火事の発生リスクや海上では海洋汚染のリスクがある。また墜落位置が海上の場合はフロートなどを搭載していない場合に、地上でも険しい山間部の場合、回収が非常に困難となる。

8.6.3. 点検

室内などの狭所や橋の下などはGNSSを受信できないため、安定した飛行を行うためにはSLAMなどの別の手段で自己位置推定を行う必要がある。また構造物に接近する必要がある場合は、衝突回避の対策としてカメラや音波などで障害物を検知する手段が考えられる。

8.6.4. 農業

農薬散布で使用する場合、農薬飛散による健康被害を防止するため、事前周知による立ち入り制限などの対策が必要である。

「無人航空機に係る事故等の一覧（国土交通省）」より、農薬散布作業中に電線への接触・切断事故が多発していることから、作業者が電線への注意を払うことが基本と考えるが、人為的ミスの

抑制方法としてジオフェンス機能の活用が考えられる。

また、農薬散布中の風の影響により農薬散布対象外の圃場へ農薬が流されることにより「農薬ドリフト（基準外の農薬が作物へ付着する現象）」が発生し、作物が出荷できない事態を招く可能性があるため、風の強い日や農薬散布対象外の圃場の際での農薬散布を避ける必要があるが、こちらについても人為的ミスの抑制方法としてジオフェンス機能が有効と考えられる。

8.6.5. 警備

自動飛行による巡回を行う場合、巡回経路や監視体制を考慮する必要がある。イベントなどの人出が多い場所での利用では特に注意が必要となる。

人出のある場所での警備においてドローンの墜落は大事故につながる可能性があるため、墜落回避の対策が重要である。思わぬ通信途絶への対策として通信経路の多重化、突風等の影響によりバランスが崩れた場合の対策として、飛行姿勢の監視や姿勢異常時のアクション設定（RTH、設定ポイントへの着陸等）、緊急事態発生時の対策としてパラシュート連動などが考えられる。

安全側で講じた対策はセキュリティ側でも有効である場合が多い。例えばパラシュートの装備は安全、セキュリティどちらの要因で落下しても有効な対策である。安全を考えるエンジニアとセキュリティを考えるエンジニアが協調してリスクを捉える必要がある。

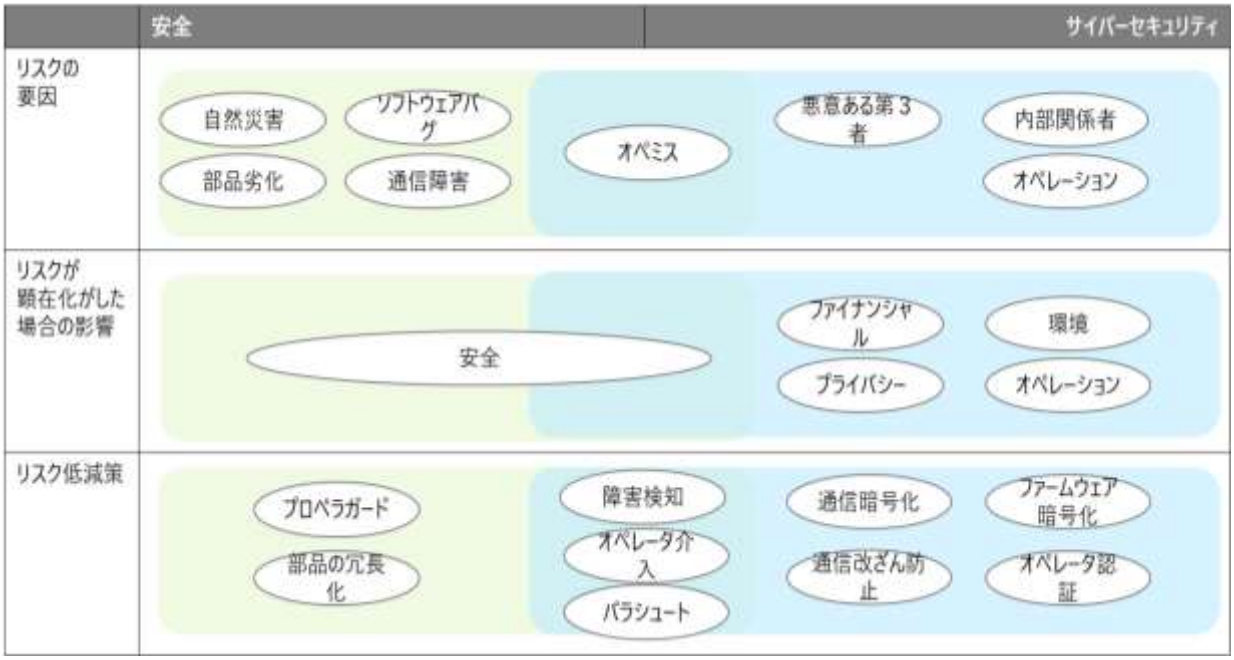


図 45：安全とセキュリティのリスクの捉え方の違い

8.7. 事故の原因と対策例

① 製鉄所の煙突点検をドローンで行っていたところ、目測を誤って煙突に衝突し墜落した。

原因　機体の操縦操作を誤った。

対策　・対象物と接近する用途の場合はプロペラガードを必ず装着する。

・障害物センサーを装備する。

・ジオフェンスで建造物をガードする。

高い構造物の周囲では、地上よりも大きな風が発生していることもあり、対象物に近づきすぎないためにズームカメラなどを活用して対象物と距離を置くことも必要である。

② 林業従事者が伐採状況の確認のためドローンを飛行させていたところ、機体との通信が途絶え林内に墜落し、紛失した。

原因　機体が伐採前の樹木との影に入ったことで機体と送信機との通信が途絶えて機体の制御が不能となった。2.4Ghz 帯の電波は水分で減衰しやすく、距離が近くても突然電波が途絶えることもある。

対策　・複数の通信経路を確保しておく（2.4GHz 帯の通信以外に LTE や LPWA など）。

・デュアル送信機モードが可能な送信機を活用する（例えば、山の場合、稜線の手前と向こう側で切り替えて使用するなど）。

・紛失するケースの対策としてドローン発見用のタグを装着しておく。

・通信途絶時のアクション(RTH か自動航行継続か)は飛行場所・高度に応じて判断する。

※想定外の位置からの RTH による帰還中に障害物に衝突する可能性があるため。

③ 物流会社が過疎地域でドローンによる物資輸送を行っていたところ、バッテリー残量が急激に低下し、墜落した。

原因　バッテリーの経年劣化による（バッテリー個体の問題）、または外気温の低下や強風等の影響により急速にバッテリーが消耗した（気象状況に起因）。

対策　・バッテリーの使用回数の上限を設定し、上限に達したら使用不可、長距離・長時間での使用不可等の運用制限を設ける。

・インテリジェントバッテリーを使用し、適切にバッテリー管理を行う。

・高級機ではバッテリーを温める機能があるため、外気温が低い場合は利用する。

・緊急着陸ポイントを設定し、バッテリー残量低下により帰還できない場合は近くのポイントに着陸させる。

④ 研究機関が研究のため無人航空機を飛行させていたところ、突如制御不能となり、墜落した。

原因　モーター停止、プロペラ破損、フライトコントローラ停止など、機械的な要因による。
また、炎天下におけるフライトコントローラ暴走など、気象状況に起因する場合もある。
※通信途絶やバッテリー切れでは突如制御不能にはならない。

対策　・日常的に機体整備、点検を徹底する。特に特にプロペラやバッテリーは消耗品との意識を持ち、利用回数など記録しておく。
・ドローン用パラシュートを装備する。
・将来的には、機体異常時にその場に留まる機能(ホバリングのみ)が備えられることを期待する。

⑤ 建設業者が高架橋建設の進捗把握のためドローンを自律飛行させていたところ、高架橋と 5m 以上の距離を取る経路に設定にしていたにも関わらず衝突した。

原因　・高架橋により GNSS 電波の反射が発生し、マルチパス現象が発生。測位位置に大きなずれを生じ、予定航路から外れてしまったため。
・GNSS 電波は建造物などによって反射波が発生し、精度が大きくずれてしまうことや、測位に十分な衛星が足りなく可能性がある。また天空からの電波であるため、上空に積乱雲その受信状況は天候などにも左右されるがその認識が不足していた。

対策　・街中や山中など、構造物や起伏が大きい場所での自律飛行は控え、手動操作を行う。
・受信衛星数を随時チェックし、一定数を下回る場合には自律飛行を控えるなどのルールを設けておく。
・GPS のみでなく、GLONASS、Galileo、QZSS など複数種の測位衛星が利用可能な GNSS システムを用いる。
・RTK などの相対測位を利用することで測位精度を高める
・雲の過多など GNSS 電波に影響のある気象現象を把握し、受信状況の悪化に備える。

9. まとめ

一般社団法人セキュアドローン協議会は、本セキュリティガイドの策定を通して、信頼できるドローンの安心安全な操作環境とデータ送信環境を確立していくための指標を提言する。

産業用途でドローンが普及していくためには、情報処理においてこれまで配慮されてきた情報セキュリティ対策や、最新の IoT 関連のセキュリティ技術が重要になる。本セキュリティガイドが提唱しているドローンを取り巻くセキュリティは、今後も新たな脅威や危険性が発見されるたびに、更新され考慮しなければならない項目や対策を追加していく予定である。

今後もドローンの飛行性能が向上し、取得できる画像や各種のセンシングデータの精度が向上すればするほど、セキュリティの脅威も増してくる。安全で信頼できる空の産業革命を推進していくためには、ドローンの飛行に対する技術革新に加えて、セキュアにドローンを飛行、運用しデータを活用するためにはセキュリティ対策も、更に重要性を増すことは間違いない。

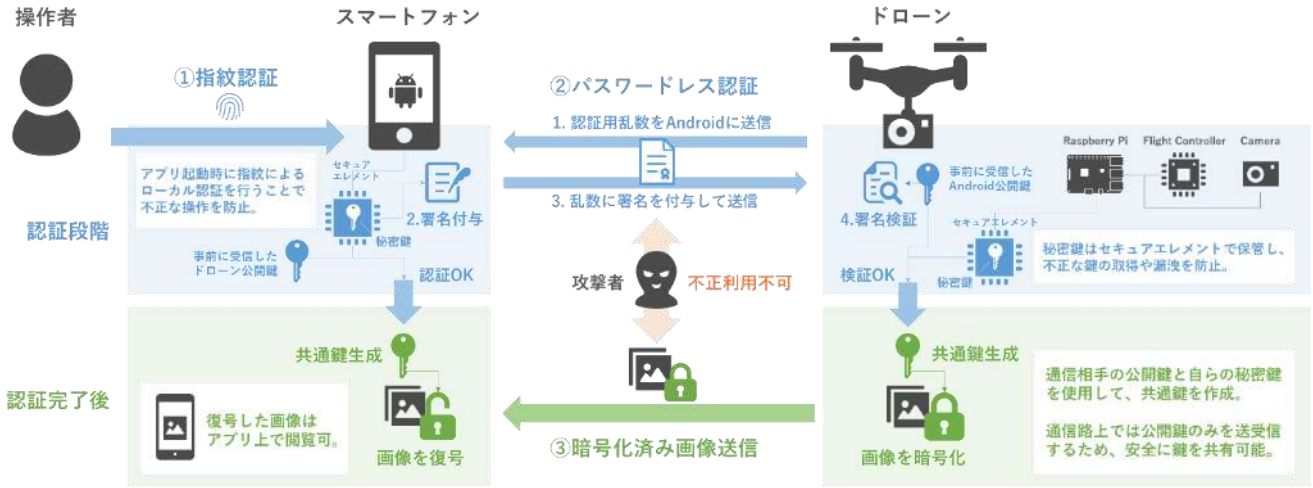
Appendix 1. ドローン関連サービス、プロトタイプ開発事例

1.1. ドローンプロトタイプ開発事例

概要

本ガイドラインの「6.2.1 認証」、「6.2.2 データの保護」を実現する開発事例としてプロトタイプ開発を実施した。このプロトタイプは、下図のような構成のシステムとなっており、スマートフォン(以下では端末と記載)とドローン間でのセキュアな通信を実現するために、以下の機能を実装している。

- 操作者と端末間・機体と端末の認証
- データセキュリティ



通信路上では、お互いの秘密情報をやりとりせず、認証・データ保護機能を実現

操作者と端末間・機体と端末の認証

本システムではドローンの操作を行う端末と操作者間で「オペレーター認証」として「指紋認証」を行い、操作者が登録されているユーザかを検証し、承認されると端末の使用が可能になる。

そして、「端末認証」として端末とドローン間での通信リクエストにおいて、認証用乱数による「署名検証」を行い、認証が通ればドローンとの通信が可能となる。

今回のこれらの認証機能は 6.2.1 で説明した技術対策の認証に紐づいている。

データセキュリティ

ドローン側で保持しているデータ(画像データ)は暗号化して保存し、データのやり取りでは暗号化済みデータを操作者側に送り、操作者側で復号を行う。この暗復号の処理を行うことで、ドローン内のデータの漏えいを防いでいる。

また、暗復号で使用する鍵については、通信相手の公開鍵と自らの秘密鍵を使用した鍵交換を行う

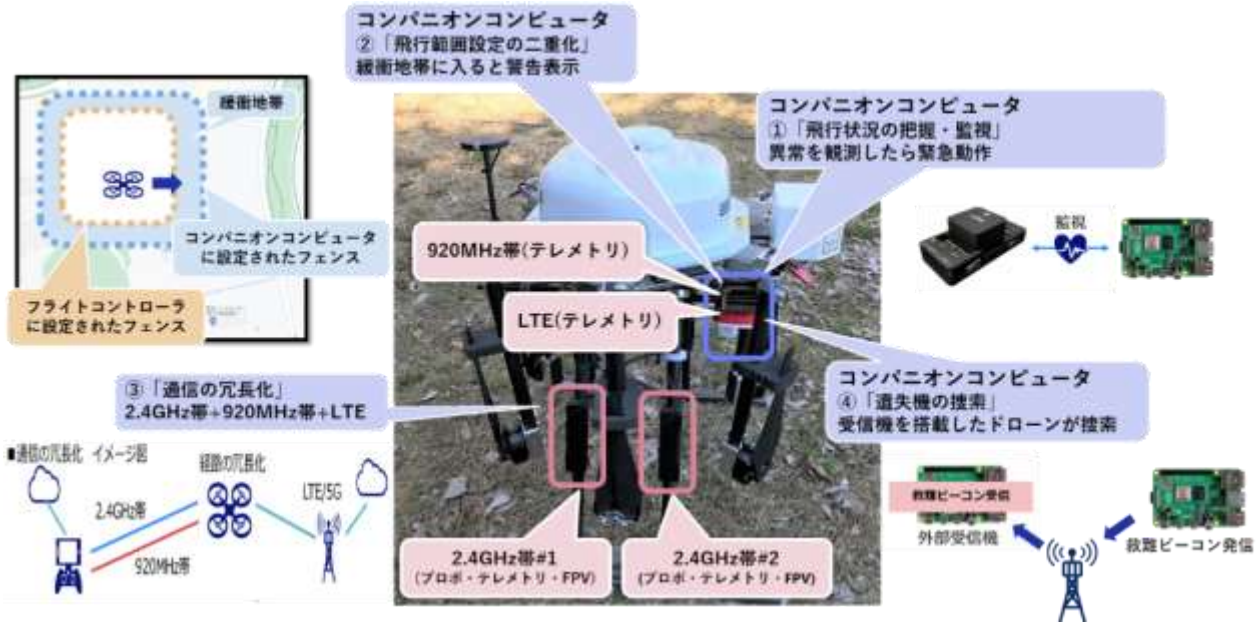
ことで、共通鍵を生成する ECDH(楕円曲線ディフィー・ヘルマン鍵共有)を使用してドローン側と端末側とで暗復号で使用する共通鍵を生成する。また、プロトタイプ開発では秘密鍵をセキュアエレメントに格納することにより、不正な鍵の取得や漏えいを防止している。

今回のこれらの鍵交換、暗復号の機能は 6.2.2 で説明した技術対策のデータの保護に紐づいている。

1.2. 高可用性ドローン基盤開発事例

概要

レベル 4 解禁の下でドローンの社会実装が進む中、「安全安心」に対する重要性はさらに増している。NEC ソリューションイノベータ社では、ArduPilot をプラットフォームとする国産ドローンを対象に高可用性ドローン基盤の技術研究に取り組んでいる。「安全安心」における”セーフティ”に着目した「①飛行状況の把握・監視」、「②飛行範囲設定の二重化」、「③通信の冗長化」、「④遺失機の捜索」等をテーマとしている（下図参照）。



今後の取組み

ドローンの安全性を高めるために、高可用性ドローン基盤では以下の強化を想定している。

■コンパニオンコンピュータの独立性強化

・　電源・GPS の独立等、フライトコントローラに依存しない構成を確保

■監視項目・対応アクションのバリエーション強化

・　バッテリー残量管理（帰還可能状況の把握）

・ 緊急着陸地点の設定

■飛行範囲設定の高機能化

・ 形状（多角形、フリーフォーム）

・ 高度設定

・ 自動設定（自動飛行経路の周囲）

・ 空間 ID との連動

■上空での自律制御

・ パラシュートの自律開傘（緊急事態の自律判断）

・ 自律的な人物検知&着陸制御（物流における戸配時の危険回避）

物流分野での活用を始め、地域住民の生活圏上空をドローンが飛行するという運用形態に関して、社会実装を加速させるためにはドローンに対する社会受容性の高まりが必要である。そのためにはドローンの安全性を強化し、地域住民の理解を得ることが重要である。

1.3. モビリティの安全な運行管理基盤サービスの実現

概要

ドローンをはじめ多くのモビリティサービスにおいて、不正アクセスからのデバイス防御は重要課題です。2022 年度から本格化するドローンのレベル 4 運用(有人地域での目視外飛行)では、ドローンがネット接続することから企業における IT 環境に近いセキュリティが求められます。

これらのモビリティデバイスの運行管理において、操作元と操作対象の位置関係、距離関係を元にしたアクセス制御の実現により、ドローン等デバイスを対象としたモビリティサービスの安全な運行機能提供を目指す。

モビリティの安全な運行管理基盤サービス

本サービス（実用化検証中）は、①クラウドサービス、②API サービス提供を想定し、現在実証実験に向けた準備を進めている。位置情報を元にしたアクセス制御の知財（特許第 6267818 号（特開 2018-164222)）を基に、①操作対象の規模を問わないクラウドサービスに加え、②既に利用中のドローン運行管理クラウドサービスへの API 連携による付加価値提供を視野に入れている。

本サービスを利用することで、例えばドローンの運行管理を行うアクセス元を限定し、更に対象となるドローンの飛行範囲も限定することができる。万が一、操作対象に組み込まれたソフトウェアに許容していない外部への通信機能があった場合でも、指定した地理的な範囲外からの操作は制御することが可能となり、例えば国外からの不正アクセスを防止することができる。

本サービスは、ラック社の「town/SmartX 事業」にも取込み、多くのデバイスにアクセス制御の

機能提供を行う予定です。本サービスの実証実験に参加いただける製品メーカー様も広く募集している。

1.4. セキュアなエッジ AI コンピューティング環境の構築に最適なプラットフォーム

概要

ドローンの社会実装が進み、様々なデータが取得されるようになっていく。今後、5G の実用化によるスマートシティの実現など、新たなサービス展開とともにデータ処理の過負荷、リアルタイム処理の制限、ハードウェアアーキテクチャやファームウェアの複雑化、電力制限など、さまざまな課題が発生する。また、長期利用の IoT 機器やミッションクリティカルな自動航行などにおいては、日々進歩するサイバー攻撃に対して、長期間に渡る安全性の確保が必須要件となる。

エッジ AI コンピューティングのメリット

エッジ AI コンピューティングの実現には、データ処理のためのエッジ向け推論エンジンの開発や最適化と、エッジ環境開発の導入・保守・更新が求める。推論エンジンの開発や、パフォーマンスと精度を向上するための最適化においては、データサイエンスと実装技術に跨るマルチスキルエンジニアの確保が必要だ。また、法制度や IEC62443 などの国際標準規格によってデバイス認証やモニタリングが義務化される中、実使用状態での推論精度を監視モニタリングし継続的に推論エンジンを更新することが必要となる。サイバートラスト社は、quadric 社とともにこれらの課題を解決するためのセキュアエッジ AI ソリューションを提供している。

■セキュリティ強化

- 機密情報やプライバシーに関わるデータ処理はエッジ側で行い通信時のデータ漏えいを防止
- プライバシー保護規制、個人データ越境移転規制への動きにも対応可能

■通信コスト削減

- データの送受信量が大幅に減少するためネットワーク負荷を低減し、通信コストを削減

■リアルタイム性向上

- AI での推論やデータ処理をエッジ側で行うため通信の遅延を抑え処理を高速化

1.5. ドローンセキュリティコンサルティングサービス

概要

レベル 4（人口集中地域、目視外飛行）の解禁、上空における LTE サービスの開始といった飛行

環境の変化やドローンを使ったソリューションが実証実験から社会実装のフェーズに移るなか、ドローンに関するセキュリティ対策が必要となってきている。

ドローン・ジャパンでは、この「ドローンセキュリティガイド」や経済産業省が示す「無人航空機分野 サイバーセキュリティガイドライン」をベースにし、ドローン機体メーカー、ドローンサービス提供者、ドローン活用企業向けに対するドローンセキュリティコンサルティングのサービスを行っている。

サービス提供内容

ドローン・ジャパンが提供する「ドローンセキュリティコンサルティングサービス」では、以下の項目について、業態や業務に応じたコンサルティングを提供している。

■ドローンのセキュリティに関する社内トレーニング
■セキュリティリスクの洗い出し
■セキュリティ対策手法の提示
■セキュリティ対策の優先順位
■セキュリティ対策の実施

1.6. Secure IoT Platform （SIOTP）

概要

ドローンのクラウド連携ソリューション

ドローンのライフサイクルマネージメントを管理し、クラウドサービスへドローン情報の登録（プロビジョニング）と 証明書認証ベースでの安全なテレメトリーデータの送信、OTA によりドローンの FW アップデートなどが可能になります。

サービス詳細

ドローンの認証には、予め機器を認証するための鍵をセキュアエレメントで管理することにより、厳密な機器認証が可能となります。

クラウドとの接続においてライフサイクルに応じた証明書の更新や無効化は重要な要素です。クラウドとの通信で利用する証明書と証明書発行の際に機器を認証する鍵を分けることで柔軟で安全なクラウド認証を実現します。

テレメトリーデータやログなどのドローンの機密データは TLS 通信により安全にクラウドにアップロードできます。

ドローンに限らず長期的に利用される IoT デバイスにおいては、脆弱性が見つかった場合対応や新機能を実装するなど、継続的にアップデートが必要となります。

SIOTP サービスでは、コード署名を行ったファームウェアを OTA 経由で アップデートが可能となるため、長期にわたって運用するドローンを安心してご利用いただけます。

1.7. SIOTP Client Manager

概要

SIOTP Client Manager は証明書や鍵を安全に格納・運用する機能を提供します。格納している暗号鍵を使い、ドローン内のデータを暗号化してデータの盗み出しに対処します。暗号鍵をファイルシステム上に展開せずに利用するため、鍵情報の盗聴を防止できます。

また、コード署名などのセキュリティ機能も有しているので、ドローン内のアプリケーションに対しての改ざんを確認・抑止します。

サービス詳細

■証明書・鍵格納機能

証明書や鍵などの重要な情報を SecureModule※に格納することで、盗聴や改ざんなどから保護します。また、暗号鍵を安全に生成・格納する機能も備えており、暗号鍵を一度もファイルシステム上に置かずに SecureModule 上のみで鍵生成を行い格納することで鍵情報の漏洩を防止します。

この機能は 6.1.1 で説明したドローン機器のセキュリティ要件に対応します。

・ドローンのキー、証明書、ID 等の機密情報を格納

・機体独自のシリアルナンバーの保護

※SecureModule：サンプル実装として SoftHSM に対応。HSM にもカスタムで対応します。

■データ暗号化機能

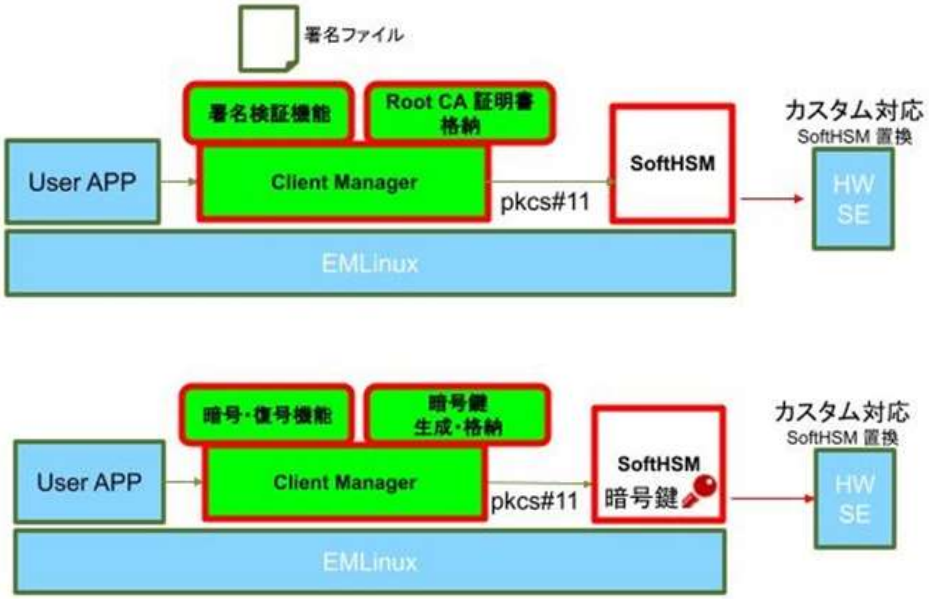
証明書・鍵格納機能で生成・格納した暗号鍵を使って、ドローンのセンシティブデータ・ログを保護する機能です。

この機能は 6.1.1 で説明したドローン機器のセキュリティ要件に対応します。

・データ、ログの暗号化

■署名検証機能

署名検証は改ざん確認に加え、RootCA までの各証明書の検証を行うことで、より安全な検証機能を提供します。検証の際に利用する RootCA は証明書・鍵格納機能によって安全に保護されます。データファイルだけでなく、アプリケーションのコードやコンテナも署名対象と想定しています。



1.8. ドローンコンサルティング／開発支援

概要

パナソニック システムデザインは、「ドローン向けクラウドセキュリティシステム」・「パラシュート×遠隔制御システム」の他にも「災害対応・監視ソリューション」・「農業向け自律飛行ソリューション」などのドローンソリューションを技術サプライヤーとして提供し、パートナー様と一緒にドローンの社会実装課題の解決に取り組んでいる。ドローンを活用した DX への取り組み、システム開発、セキュリティ、

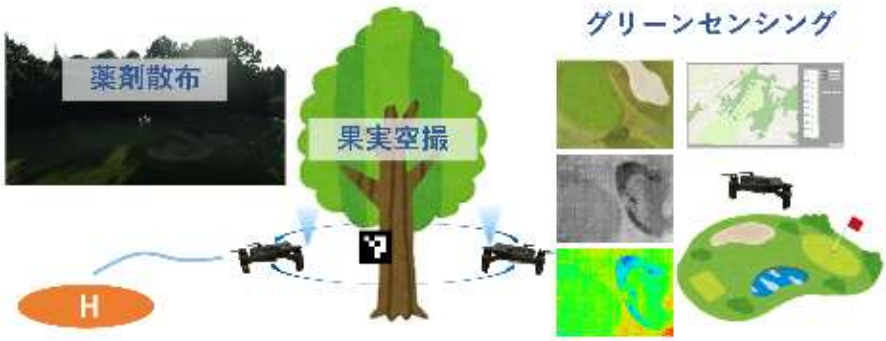
安全対策など幅広くコンサルティングサービスを提供している。

サービス詳細

事例① 災害対応・監視ソリューション

人が駆け付けることが困難な被災地を遠隔地からドローンの映像で監視を可能とし、遭難者を探索するためにココヘリ(*）サービスの仕組みを利用した自律探索のシステムによる災害対応のソリューション。平常時のドローン活用としては、河川等の巡視を行うパトロールドローンのシステムを構築し実証実験を支援している。

事例② 農業向け自律飛行ソリューション



農家やゴルフ場キーパーの作業効率化のため自律飛行ドローンによるピンポイントでの薬剤散布、ドローンが農園やゴルフ場を自律飛行し空撮を行うことで、果実の成熟度分析やグリーンの温度管理を実施するソリューションに対応している。

1.9. ドローン向けクラウドセキュリティシステム構築支援

概要

SIM の上空利用の制限緩和に伴い、ドローンのデータの扱いもクラウドへの直接リアルタイム送信が可能となる。しかし、クラウド活用ではパスワードなどの認証情報の漏えいという課題がある。

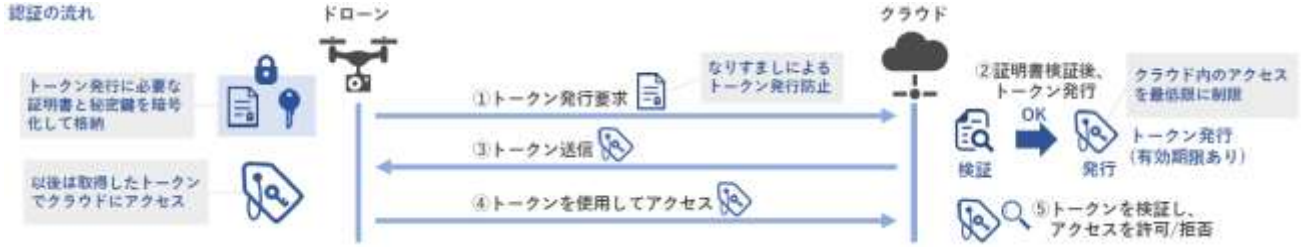
パナソニック システムデザインではドローンのクラウドアクセス時の認証の課題に対して、クライアント認証、有効期限付きのトークンによる認証システムなどドローンのクラウドセキュリティシステムの

構築を支援している。将来的にはクラウドによるドローンの機体管理のセキュリティシステムについても構築支援を実施する予定である。

サービス詳細

事例：ドローンクラウド間の認証システム

この認証システムではドローンにあらかじめクライアント証明書と秘密鍵を暗号化して格納する。ドローンがクラウドに対してアクセスする際に、まず有効期限付きのトークンを発行する。この際の認証はクライアント証明書を用いて実施する。ドローンの飛行時には、発行されたトークンを用いて再度認証を実施し、認証が通ればクラウド環境にアクセスが可能となる。



この認証システムを使用することで、パスワードなどの情報がインターネット上を流れることは無くなり、ドローン飛行中も処理の重いクライアント認証の代わりにトークンによる認証を行うことで比較的性能の高くないドローンのコンピュータでも認証が可能となる。

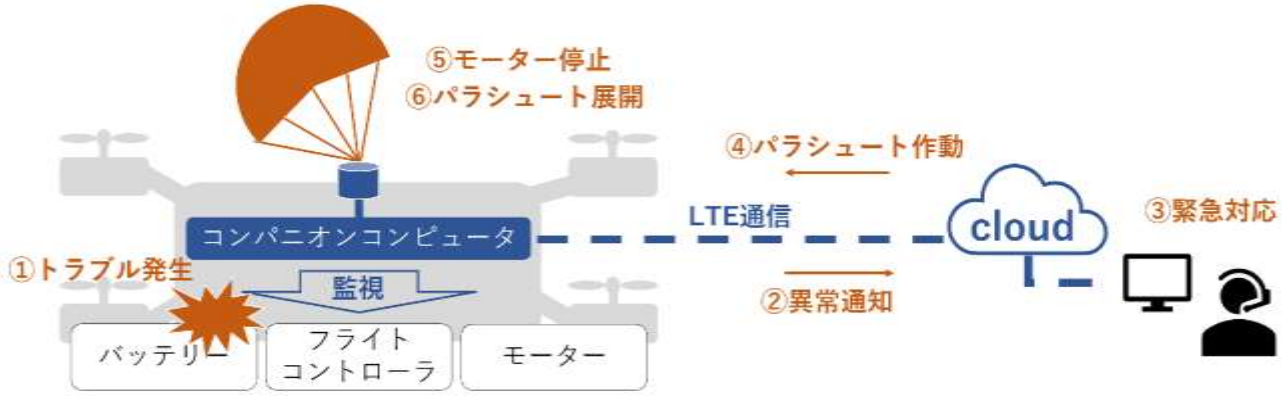
1.10. パラシュート×遠隔制御システム構築支援

概要

ドローン社会実装レベル 4 の実現に向け、今後目視外飛行での安全性の確保が重要となる。しかし、自律飛行で想定される、駆動停止・暴走など様々な安全上の問題に対し、目視外から対策を行うことは非常に難しい。パナソニック システムデザインでは一例として、遠隔地からドローンの監視を行い、異常発生時に日本化薬製パラシュートによる緊急着陸を行うことで課題を解決した。

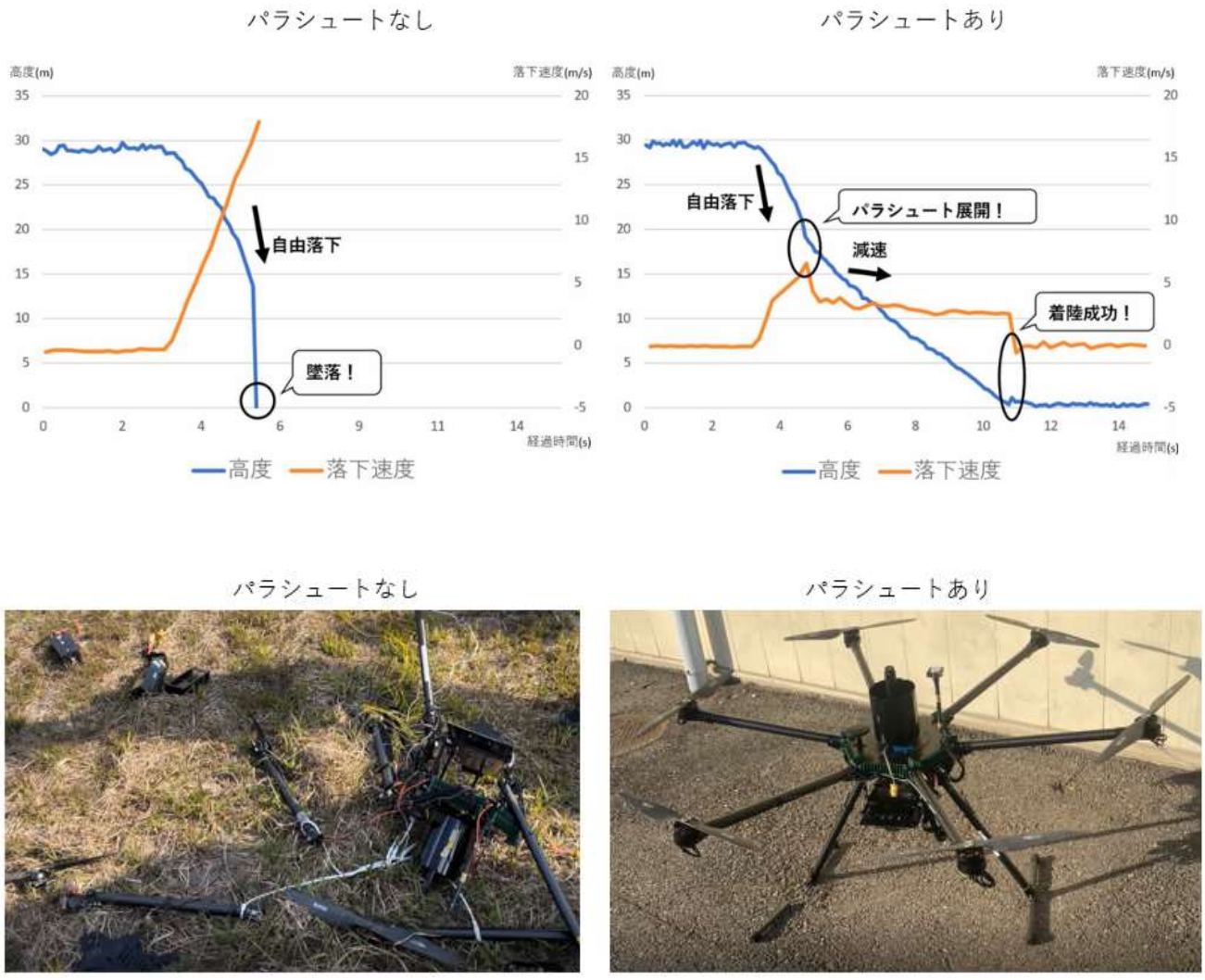
今後もドローンの安全をソフトウェアで支援していく。

サービス詳細



本システムは、ドローンに「①トラブル発生」すると、コンパニオンコンピュータが LTE 通信を介して遠隔地のオペレーターに「②異常通知」を行う。通知を受け、オペレーターが「③緊急対応」として「④パラシュート作動」を実施すると、ドローンはまず「⑤モーター停止」し、その後「⑥パラシュート展開」を行い緊急着陸する。オペレーターがパラシュートを作動させる際、ドローン搭載カメラにより着陸予想地点のガイドを表示する。これによりオペレーターは目視飛行同様に安全を確保した上で着陸を行うことができる。

本システムの実証実験での検証内容を下図に示す。本システムによりドローンの落下速度を大幅に減速し、着陸時の損害を最小限に抑えることができている。



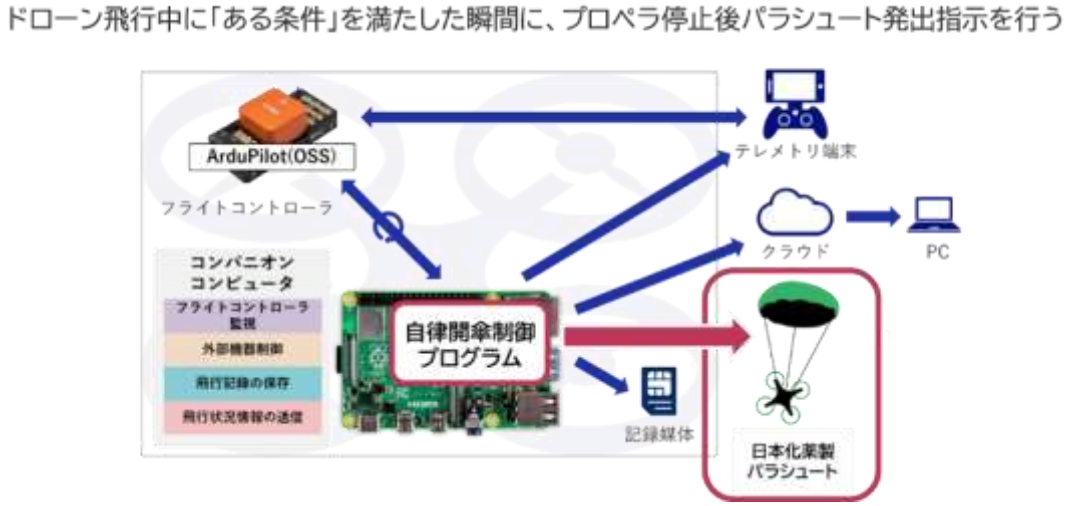
1.11. パラシュート自律開傘 PoC 開発事例

概要

ドローンの安全性を確保する手段の１つとしてドローン用パラシュートの適用があり、一般的な活用方法として、目視外飛行をリモート監視しているオペレーターがドローンの緊急事態を認識し、パラシュート作動の指示を行うという運用が考えられる。しかし、一瞬の見逃しや判断の遅れが生じ、パラシュート作動のタイミングが遅れると、その間にもドローンは落下しているため、パラシュートの効果を得るために必要な高度が確保できず、地上での被害につながる可能性がある。ドローンが自律的に緊急事態を把握し、パラシュートを自律開傘する仕組みをドローンに整備することにより、そのようなリスクを軽減させることができる。

ドローンが自律開傘することの検証を行うために、飛行中に「ある条件」を満たした瞬間に、プロペラ停止後パラシュート発出指示を行う仕組みを実装した。本 PoC 開発では、「ある条件」として、「進入禁止エリアへの進入検知」を適用した。

システム構成



実証実験イメージ

1.12. 人物検知&飛行制御 PoC 開発事例

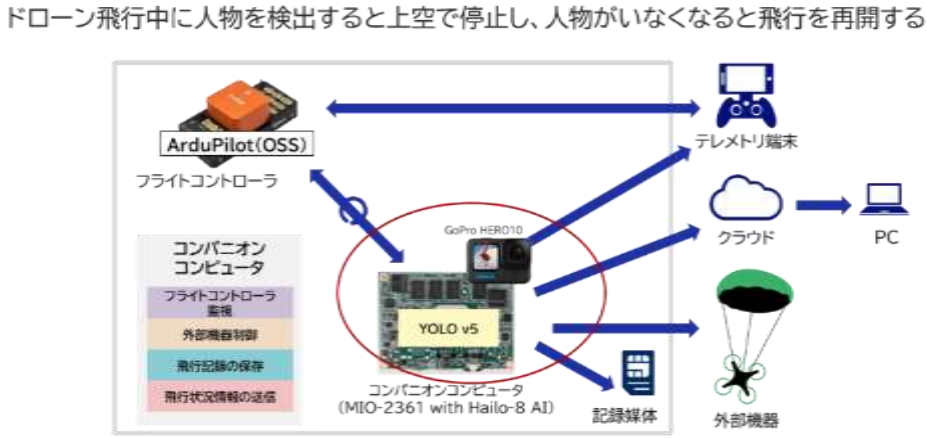
概要

ドローン物流の実証実験が国内の中山間地域や離島間で数多く進められており、物流分野でのドローンの活用が期待されている。実証実験から実運用に移行していくためには運用シーンを想定した安全対策が必要であり、特に荷物配達先でのドローンの着陸時に注意を払う必要がある。ドローンと人の接触を生じさせないことが重要であり、上空から人を検知する仕組み、かつ人を検知したら着陸せずに上空に留まる仕組みを備えることが考えられる。また、2023 年 12 月に新設された「レベル 3.5 飛行」の制度では、「機体に搭載されたカメラによって、飛行経路下に歩行者等がいない無人地帯であることを確認して飛行する」ことが飛行承認する要件の 1 つとなっており、上空での人物検知＆着陸制御はこの要件を満たす仕組みとなる。

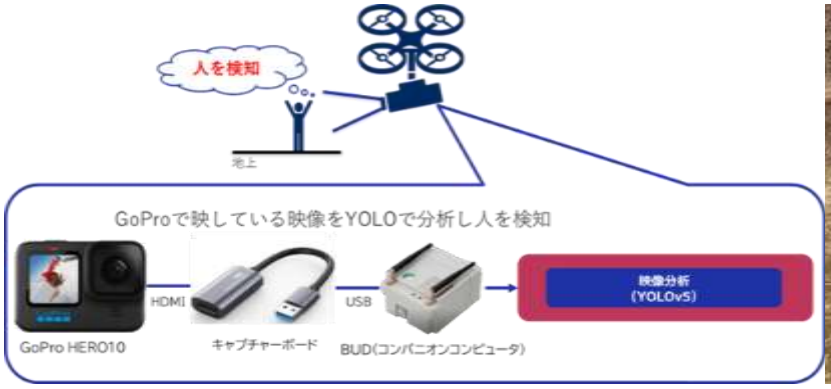
人物検知＆着陸制御の検証を行うために、ドローン機体に搭載されたカメラ（実験では GoPro

HERO10 を使用）が上空から捉えた映像をコンパニオンコンピュータ上の人物検知プログラム（実験では YOLOv5 を使用）が解析し、人物を検出した場合にホバリング、人物不検出の状態になったら自律飛行を再開する仕組みを実装した。

システム構成



実証実験イメージ



ドローン関連サービス、プロトタイプ開発事例 問い合わせ先

【セキュリティ機能のプロトタイプ開発事例】

【ドローンコンサルティング／開発支援】

【ドローン向けクラウドセキュリティシステム構築支援】

【パラシュート×遠隔制御システム構築支援】

お問い合わせ先	パナソニック システムデザイン株式会社　システム技術部
	psd_drone@ml.jp.panasonic.com

【高可用性ドローン基盤開発事例】

【パラシュート自律開傘 PoC 開発事例】

【人物検知&飛行制御 PoC 開発事例】

お問い合わせ先	NEC ソリューションイノベータ株式会社　ファウンデーションサポート事業部
	nes-drone@nes.jp.nec.com

【モビリティの安全な運行管理基盤サービスの実現】

お問い合わせ先	株式会社ラック　新規事業開発部
	nbd-support@lac.co.jp

【セキュアなエッジ AI コンピューティング環境の構築に最適なプラットフォーム】

【Secure IoT Platform （SIOTP)】

【SIOTP Client Manager】

お問い合わせ先	サイバートラスト株式会社　フィールドマーケティング部
	iot-contact@cybertrust.co.jp

【ドローンセキュリティコンサルティング】

お問い合わせ先	ドローン・ジャパン株式会社
	info@drone-j.com

ドローンセキュリティガイド第 5 版 執筆者

セキュリティガイド WG　リーダー：広野 徹（パナソニック システムデザイン株式会社）

WG メンバー

下問 勝司（NEC ソリューションイノベータ株式会社）

一二三 淳志（NEC ソリューションイノベータ株式会社）

佐野 勝大（サイバートラスト株式会社）

船引 裕司（株式会社ラック）

瀬瀬 考平（一般社団法人セキュア IoT プラットフォーム協議会）

藤田 智明（一般社団法人セキュア IoT プラットフォーム協議会 位置情報部会）

久留 吉伸（一般社団法人セキュア IoT プラットフォーム協議会 位置情報部会）

春原 久徳（一般社団法人セキュアドローン協議会 代表理事・会長）

田上 利博（一般社団法人セキュアドローン協議会 事務局長）