ドローンセキュリティガイド

- 第1版 -

2018年3月

一般社団法人セキュアドローン協議会

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

ドローンの活用がさまざまな業界で期待される中、墜落などの事件・事故の増大が危惧されている。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. ドローンのセキュリティ概要

産業用ドローンを安全に業務で利用するためには、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。これまでに、どのようなセキュリティにおけるリスクが発生し、事故や被害が起きたのか、その概要を解説する。

2.1. 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。

2.2. 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洩する。

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。

2.3. 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。

2.4. 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リスク分析
  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について解説
- ドローンの操縦者・管理者／機体の認証
  ドローンを安全に飛行させるための機体や操縦者、管理者などの認証について解説
- データセキュリティ
  ドローンで取り扱うデータに関するセキュリティ対策について解説
- 業務運用に関する注意点
  ドローンを業務で取り扱う上での各種の注意点について解説
- まとめ
  本セキュリティガイドについての総括

3. ドローンのセキュリティリスク分析

ドローンによるソリューションを提供する事業者（以下、事業者）は、フライトプランや撮影データといったドローンを活用することで得られる情報、ドローンとサービスを繋ぐ通信網やファームウェアといったインフラストラクチャーを保護することで、情報漏えいを始め、ハッキングによる墜落といった予期せぬ事態・事象を回避することができる。

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を達成することが困難になってしまうことも懸念される。

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。

3.1. ドローン固有の情報セキュリティリスク

3.1.1. 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」が公表[1]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

[1] http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

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。

3.1.2. 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。

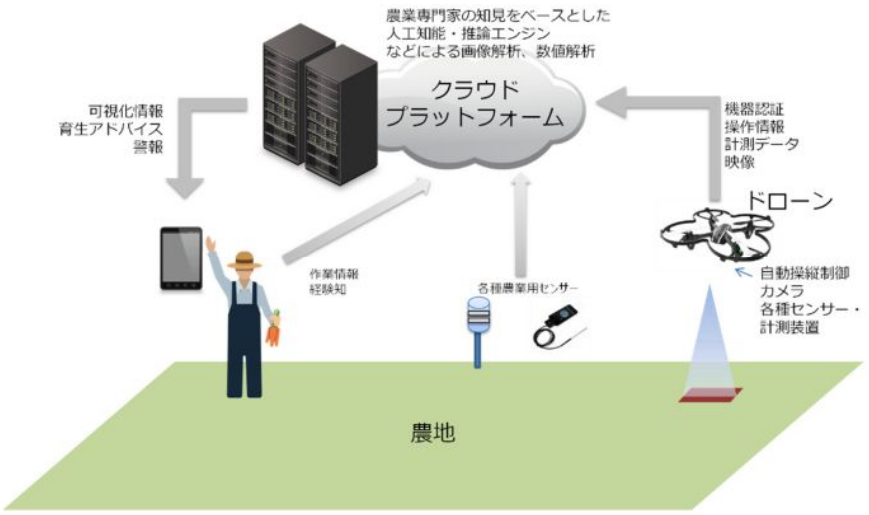


図 1：ドローンのユースケース

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) 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。

3.2. 資産のリストアップ

3.2.1. 事業上の作業フロー分析

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。

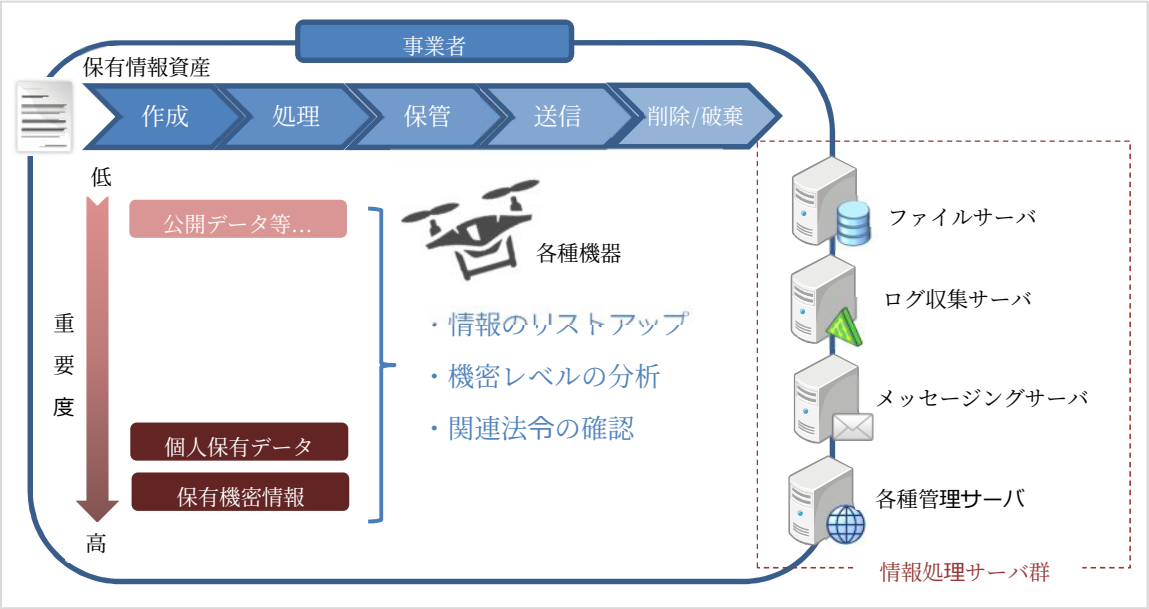


図 2：ドローンを活用する事業における保有情報資産と情報資産

3.2.2. 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。

3.2.3. 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。

3.2.4. 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) 情報の一時的又は恒久的な複製は、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。

3.2.5. 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「3.2.3 個人保有データのリストアップ」、「3.2.4 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又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。

3.2.6. 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又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、又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。

3.3. リスクの事前検証

3.3.1. 運用面におけるセキュリティホールの抽出

事業者は「3.2.1 事業上の作業フロー分析」に提示した、事業を実現するにあたり、利用中のドローン及びシステムの技術的脆弱性に関する情報を速やかに獲得しなければならない。これにより、脆弱性に組織が晒されている状況を常に評価し、それらと関連するリスクに対処

することができる。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) 技術的脆弱性の管理をサポートするために必要となる具体的な情報が管理され、ソフトウェアおよびハードウェアに対して、技術的責任のある組織内の担当者を設置する。
(2) 潜在していた技術的脆弱性を特定したときは、速やかに処置が行えるよう、技術的脆弱性に対する有効な管理プロセスを規定する。

3.3.2. ライフサイクルへの影響 分析／調査

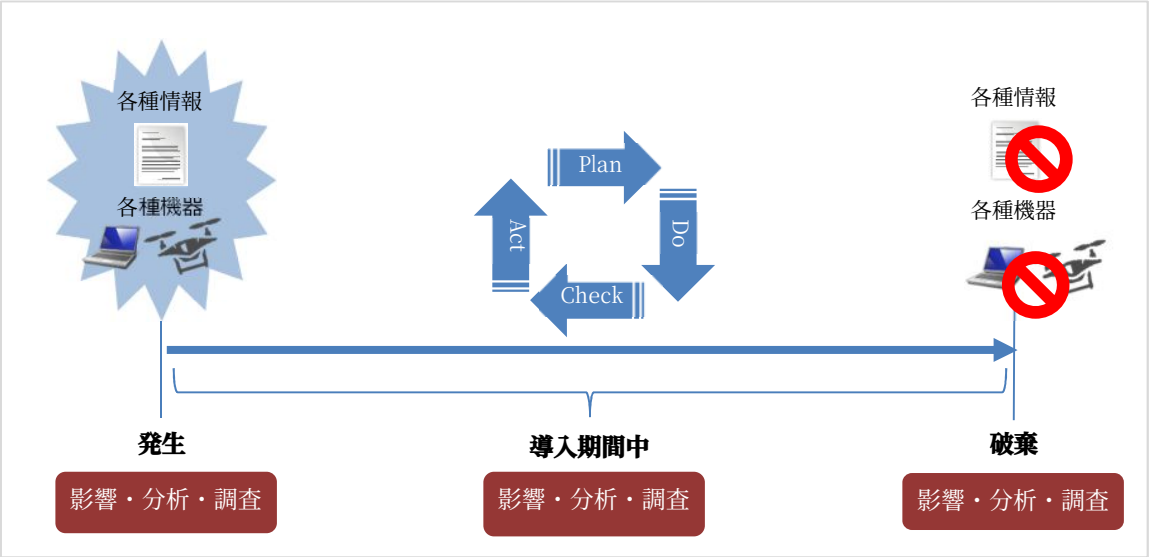


図 3：ライフサイクルの遷移

3.3.2.1. 発生時におけるライフサイクルへの影響 分析／調査

事業者は資産のライフサイクルを特定しなければならない。その重要度は文書化するものとし、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た、専用の目録又は既存の目録として維持していることが求められる。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) 資産目録は、正確で、最新に保たれ、一貫性があり、他の目録と整合させること。
(2) 情報資産について、管理責任者を割り当て、適切に分類すること。

3.3.2.2. 導入時におけるライフサイクルへの影響 分析／調査

事業者は、所有する資産に対して、法的要求事項、価値、重要性、及び許可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類を行うことを求められる。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) 情報の分類及び関連する保護管理策では、情報を共有又は制限する、事業の要求及び法的要求事項を考慮すること。
(2) 情報以外の資産も、その資産に保管される情報、処理される情報、又は他の形で取り扱われる若しくは保護される情報の分類に従って分類すること。

3.3.2.3. 廃棄時におけるライフサイクルへの影響 分析／調査

資産の管理責任者が資産を削除又は破壊する場合でも、情報資産は適切に扱われ、トレーサビリティが継続していなければならない。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) 許可されていない者に秘密情報が漏えいするリスクを最小化するために、媒体のセキュリティを保った処分のための正式な手順を定めること。
(2) 秘密情報を格納した媒体の、セキュリティを保った処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとすること。
(3) 処分のために媒体を集める場合、取扱いに慎重を要する情報ではない情報でも、その量が集まると、取扱いに慎重を要する情報に代わる場合があり、集積する影響に配慮する。
(4) 取扱に慎重を要するデータを含んだ装置が損傷した場合には、修理又は廃棄に出すよりも物理的に破棄するほうが望ましいか否かの決定プロセスを定めること。

3.4. リスク分析／評価

3.4.1. リスク分析

ここでは「3.3 リスクの」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) 「3.3 リスクの事前検証」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) 「3.3 リスクの」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。

3.4.2. 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 1：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 2：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。

3.4.3. 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。

3.4.4. 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 3：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 4：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 5：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。

3.4.5. 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 6：リスクレベル早見表例

	脅威								
	1			2			3		
	脆弱性								
脅威の価値	**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。

3.4.6. 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。

3.4.7. 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 7：リスク受容一覧の例

	脅威								
	1			2			3		
	脆弱性								
脅威の価値	**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。

3.4.8. 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。

3.5. ドローンのサイバー攻撃

2017 年 10 月 3 日に総務省から「IoT セキュリティ総合対策」が公表[2]され、その中で IoT デバイスに分類される機器においては脆弱性の検査を実施することが強く推奨されている。

既存の Web アプリケーションやプラットフォームだけではなく、IoT の普及により機器を繋ぐ通信経路が飛躍的に増加しており、また IoT の特性から該当の機器が物理的にオープンな環境に配置されることも想定される。機器を介した不正アクセスは依然として存在するため、セキュリティにおいて脆弱な機器を使用することはリスク要因となり得る。

ドローンにおいてもその条件は大きく違わず、本体、送信機(専用端末、スマートフォンアプリ)などにおいて脆弱性が存在する場合にはインシデントに直結することが想定される。そのような脆弱性の有無を診断(検査)することはインシデントに対するリスクを大幅に軽減するためには有効だと考えられる。本節ではドローンを中心とした脆弱性診断の概要を記載する。

3.5.1. 対象となる通信と機器の選定

ドローンを中心として構成されるサービスを「機器」、「通信」、「クラウド」に分類し、脆弱性診断の対象を選定する。

(1) 機器

ドローン本体を始めとし、スマートフォン(アプリを含む)や、プロポ（ドローンを操縦する際に欠かせない送信機やコントローラの意）などのコントローラを診断対象とする。

(2) 通信

機器間、またはクラウドとのデータ送受信を行うための経路が診断対象となる。

(3) クラウド

バックエンドサービス(データ収集、機器管理など)が存在する場合には、それを構成する Web アプリケーションやプラットフォームに対しても診断を行うことが望ましい。

[2] http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html

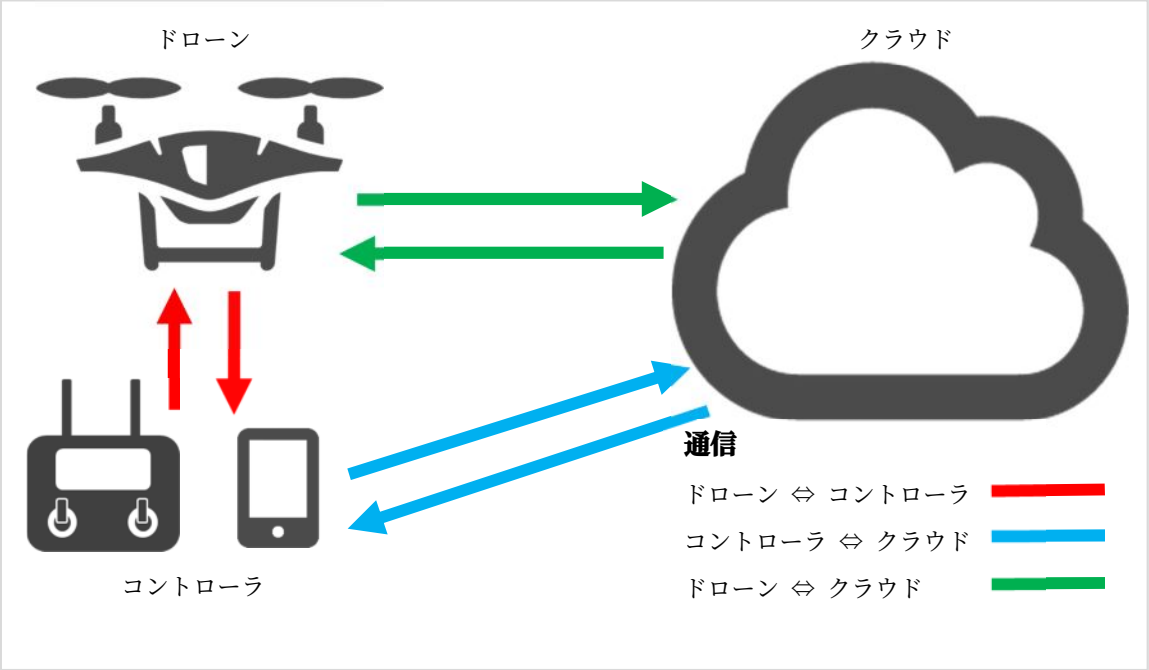


図 4：ドローンを利用したサービスの構築例

3.5.2. リスク分析

ドローンに限らず、IoT や M2M のような概念を持つサービスに対しては、汎用的な診断項目も存在するが、構成要素や対象製品におけるリスクは異なるため、攻撃シナリオを基にリスク分析を行う必要がある。

リスク分析によって脆弱性診断の目的を明確化し、危険度の高い脆弱性や影響範囲の広い脆弱性を早期に発見することが重要である。本項ではドローンにおけるリスクを 2 つのシナリオから分析する。

3.5.2.1. シナリオ 1：制御権限の奪取

本来、操縦をするための制御権限は、ドローン本体と認証を済ませた操縦機器(スマートフォンも含む)であるべきだが、その制御権限を奪取されてしまうという事象は既存の機器において確認されている。

所有者側からすると盗難という 1 つの面しか被害がないように見受けられるが、下記のようなシナリオも想定される。

- 飛行禁止エリアへの侵入
- 撮影禁止エリアでの撮影行為
- 運搬を目的としている場合、運搬中の「物」や「情報」ごと奪取される

このように「乗っ取り」と呼ばれるような行為が成立した場合には、複合的に被害が拡大していく可能性もあり、その規模が大きくなればなるほど重大なインシデントを招く可能性がある。

また、権限を奪取されなくとも「操作不能」とすることが目的であることも想定に含む必要がある。

3.5.2.2. シナリオ 2：データ改ざん

「自動操縦」や「データ収集」を目的としたサービスにおいてデータ改ざんは非常にリスクの高い脆弱性と考えられる。「自動操縦」においては制御権限の奪取と同様の被害が想定されるが、「データ収集」を目的としたサービスにおいてデータ改ざんが行われた場合には連動したシステムにおいても影響を及ぼすことが想定される。

例として、特定エリアにおいて気候や交通量などのデータをドローンが収集し、そのデータを基に各管理機器が各々の振る舞いを持つような仕組みが存在した場合に、そのデータ自体が不正なものであれば管理機器においても期待をした動作は行わないことが想定される。それに加え、重要インフラなどの領域において利用されている場合には、より深刻な被害をもたらす可能性も存在する。

3.5.3. 診断項目

構成される機器、通信に対して診断ツールなどを用いて網羅的に実施する。併せてリスク分析によって、より重要だと判断された対象については、手動診断などによる厳密な診断を実施する。下記に対象別の標準的な診断項目を示す。

(1) 機器

- 各種プロトコルに対してアクセスを試みて、適切なエラーハンドリングやアクセス制御の不備の有無を確認する
- 認証メカニズムやパスワードポリシーを調査
- ファームウェアに対する診断

(2) 通信

- 通信内容が暗号化の有無、またその強度を調査
- 中間者攻撃への耐性

(3) クラウド

バックエンドサービスが存在する場合には該当のシステム・環境に対して Web アプリケ

ーション診断やプラットフォーム(NW)診断などを実施することを推奨。その際に(1)、(2)で実施した機器側の診断結果を加味し、サービス全体を意識した診断を実施すること。

3.5.4. 診断結果と対策

診断によって発見された脆弱性においては改修を実施すること。特に、危険度が高い検出事項が存在した場合には速やかに改修を実施する。また危険が低い検出事項でもリスク受容が可能なレベルまでの保険的対策や、運用方針を定めること。

また、対策を講じた後には再度、診断ベンダーなどの手によって、改修が正しく実装され発見時のリスクが存在しないことを確認すること。

3.5.5. サイクル

新たな脆弱性が発見されることから、定期的(年１度程度)な診断実施をする。また、リスク分析において、過去の診断時とは違う観点での懸念が発生した場合にも同様に診断を実施することを推奨する。

大規模な機能追加／改修等を行う場合にも脆弱性が混入する可能性があり、そのような点における対策として、開発・運用スケジュールにおいても脆弱性診断を組み込むことでリリース時には診断がすでに完了しているといったケースも増加している。

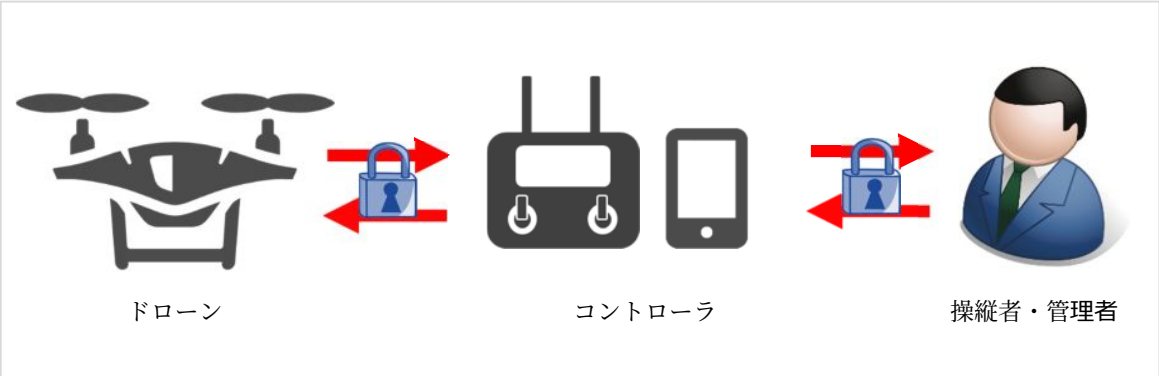
4. ドローンの操縦者・管理者／機体の認証

4.1. 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。

4.2. 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。

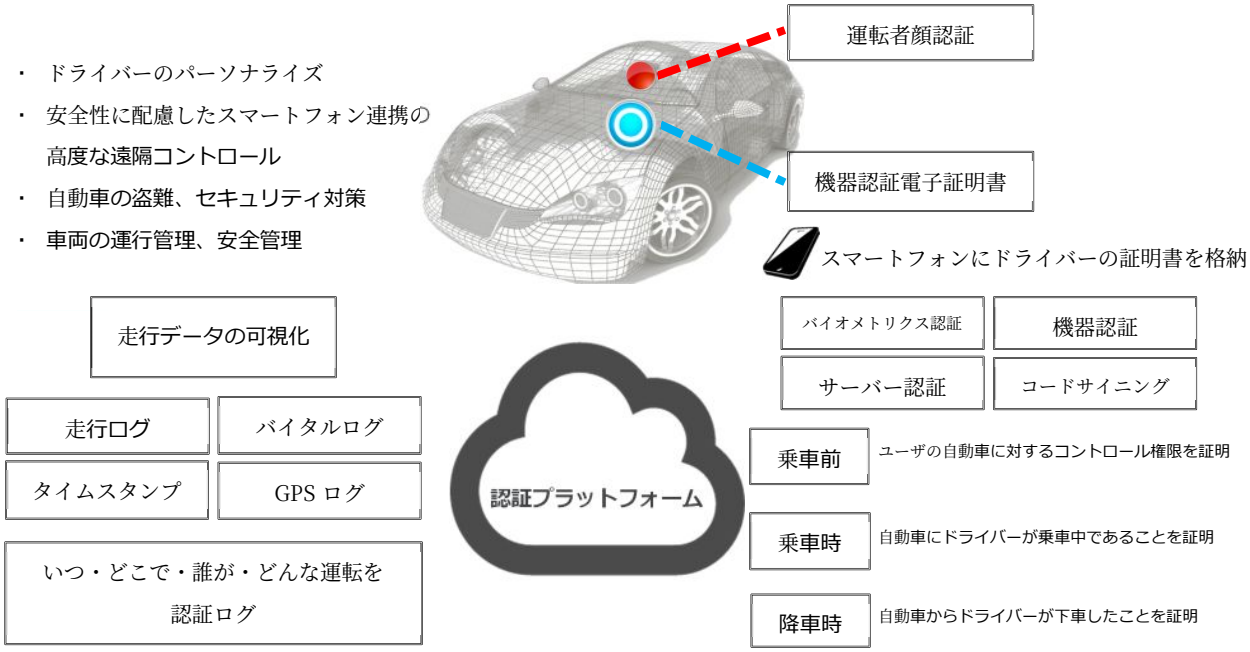


4.3. ドローン操縦者認証のシステム例

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、安全な運転走行やクルマと社会の抱え

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。



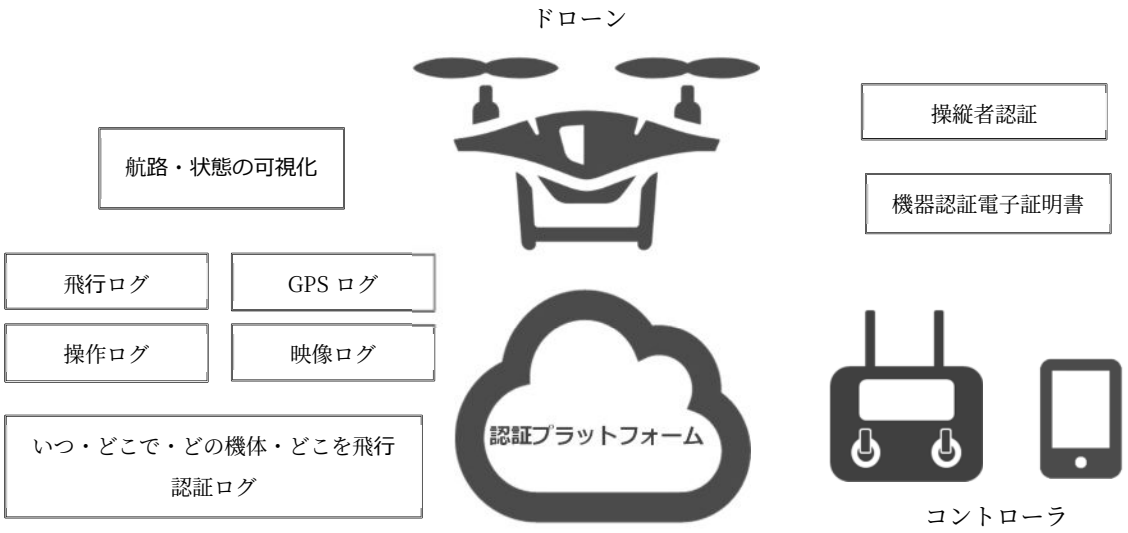
4.4. 生体認証によるドローンの飛行認証システム例

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。



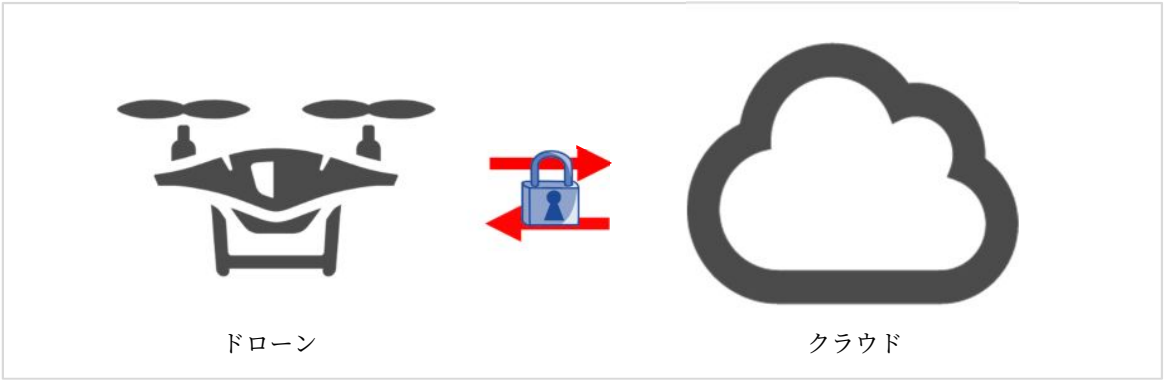
4.5. 自動航行におけるドローンの飛行認証システム例

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。現在は、まだ研究開発と実証実験の段階だが、2019 年を目標に開発が進んでいる。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。

5. データセキュリティ

5.1. 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。



5.2. 保護の対象となるデータ

データセキュリティの対象となる情報は、ドローンのカメラが撮影した画像や動画などのファイルに加え、ドローンの飛行に関連した位置情報や各種のセンサーが取得する環境情報などになる。また、将来的には飛行中のドローンから温度や湿度、風速などの気象条件や、他のドローンを検知するための信号なども交換されるようになる。さらに、ドローンの飛行管制システムからの指示やテレメトリー情報なども、保護するべきデータの対象となる。

5.2.1. 画像や動画ファイルのデータ保護

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洩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)[3]をデジタルカメラで利用する対策がある。

5.2.2. 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 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。

5.2.3. 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。

5.2.4. 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洩する危険性はない。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、

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

安全に保護していく取り組みが求められる。

6. 業務運用に関する注意点[4]

6.1. 無人航空機の点検・整備

6.1.1. 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。

- 各機器が確実に取り付けられている
- モーターに異音がない
- プロペラに傷や歪みがない
- バッテリーの充電量は十分ある

（2）飛行後の点検

- 機体にゴミ等の付着物
- ネジの緩み
- モーターやバッテリーに異常な発熱

（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

- 交換必要な部品の有無
- ネジの緩み
- プロペラに傷や歪みがない
- フレームに歪みがない

6.1.2. 点検・整備記録の作成

6.1.1 の（3）に定めた無人航空機の点検・検査を行った際には、「無人航空機の点検・整備記録」（様式１）により、点検・整備実施者がその実施記録を作成し、電子データまたは書面により管理する。

6.2. 無人航空機を飛行させる者の訓練および遵守事項

6.2.1. 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

[4] 国土交通省航空局標準マニュアル①（平成２９年６月２４日版）より抜粋

ものとする。訓練場所は許可等が不要な場所又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。

6.2.2. 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又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。

6.2.3. 操縦技量の維持

6.1.1，6.1.2 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

可等が不要な場所又は訓練のために許可等を受けた場所で行う。

6.2.4. 夜間における操縦練習

夜間においても、6.2.2 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 を受けた場所又は屋内にて練習を行う。

6.2.5. 目視外飛行における操縦練習

目視外飛行においても、２－２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又は屋内にて練習を行う。

6.2.6. 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又は屋内にて練習を行う。

6.2.7. 飛行記録の作成

無人航空機を飛行させた際には、「無人航空機の飛行記録」（様式２）により、その 飛行記録を作成し、電子的又は書面で記録を管理する。

6.2.8. 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を確認する。

（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） 衝突や後方乱気流による影響等を避けるため、航空機には接近しない。

（5） 酒精飲料等の影響により、無人航空機を正常に飛行させることができないおそれがある間は、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） 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。

（8） 物件のつり下げ又は曳航は行わない。

（9） 無人航空機の飛行の安全を確保するため、製造事業者が定める取扱説明書に従い、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。

（10）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）

（11）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又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又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。

- 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

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

6.3. 安全を確保するために必要な体制

6.3.1. 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。
- 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。
- 飛行場所付近の人又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、事前周知、物件管理者等との調整を行う。
- 公園、河川、港湾等で飛行させる場合には、管理者により飛行が禁止されている場所でないか、あらかじめ確認する。

※ 6.3.1 に加え、飛行の形態に応じ、6.3.2 から 6.3.7 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。

6.3.2. 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（空港管理事務所又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（又は空港出張所、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、別添又は申請書（様式１）その他参考となる事項に記載する。

6.3.3. 地表又は水面から 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、別添又は申請書（様式１）その他参考となる事項に記載する。

6.3.4. 人又は家屋の密集している地域の上空における飛行、地上又は水上の人又は物件との

間に 30mの距離を保てない飛行又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又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。
  - 催しの主催者等とあらかじめ調整を行い、次表に示す立入禁止区画を設定すること。

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
150m以上	飛行範囲の外周から落下距離（当該距離が70m未満の場合にあっては、70mとする。）以内の範囲

6.3.5. 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。

6.3.6. 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。

6.3.7. 危険物の輸送を行う際又は物件投下を行う際の体制

- 6.3.1 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。

6.3.8. 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、6.2.8（11）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安全部運航安全課、地方航空局保安部運用課又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。

  国土交通省航空局安全部運航安全課 03-5253-8111（内線：50157,50158）
  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
  最寄りの空港事務所 （執務時間外は次表に示した、飛行させた都道府県に対応する 24 時間対応の空港事務所へ連絡する。）

（様式１）無人航空機の点検・整備記録　　（参考様式）

（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	
		モーター	外観		
			異音の有無		
			回転の状態		
		プロペラ	外観		
			損傷		
			曲がり		
		フレーム	外観		
			損傷		
			ネジのゆるみ		
		電気系統	コネクタの状態		
			ケーブルの状態		
		送信機	外観		
			スティックの状態		
（特記事項）					

（様式２）無人航空機の飛行記録

（参考様式）

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	飛行場所	離陸時刻	着陸時刻	飛行時間	総飛行時間	夜間飛行、目視外飛行又は物件投下の該当の有無	飛行の安全に影響のあった事項

7. 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。

産業用途に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との連携が重要になる。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のガイドラインは、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。

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、ドローンの飛行技術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セキュリティ対策も、更に重要性を増していくことは間違いない。