

ドローンのための飛行データ保持機構の提案

坂元建斗¹ 田中優弥² 八槇博史²

概要: 近年ドローンは産業界をはじめ、様々な目的で利活用されている。2020年には、有人地帯での目視外飛行を目指し、制度の制定、設備の整備が進められている。一方でドローンの普及に伴う事故・事件の増大が懸念されている。飛行前後のメンテナンスを行い、トラブルを未然に防ぐ取り組みは為されているものの、事故・事件が日々起きている。本稿では、事故・事件は起きるものとして、原因究明を行える技術を探求する。海外で報告されている事例と論文、日本のドローン産業動向を基に、ドローンの事故が起きた際の分析とその対応の中で行われるフォレンジック作業で何が必要となるか考察した。考察したうえで我々は、ドローンにおけるブラックボックスを提案し、ドローン・フォレンジックを検討した。

A Proposal of Flight Record Mechanism for Drones

KENTO SAKAMOTO¹ YUYA TANAKA² HIROFUMI YAMAKI²

1. はじめに

ドローンを利活用することへの普及が高まっている^[1]。山の状態を確認する空撮や農業で使用される農薬散布、トンネルの設備点検など利用目的は様々である。2020年には有人地帯での目視外飛行を目指し、制度の制定、設備の整備が進められている^[2]。

一方、ドローンの普及に伴う事故・事件の増大が懸念されている。事故・事件が起きた際、回収した第三者によりデータが漏洩・改竄される恐れがある。また、ドローンには機微情報が含まれていることがあり、簡単にデータが見られるような状態は適当であるのかを検討する必要がある。

本稿では、日本のドローン産業動向を基に、事故・事件が起きた際の分析とその対応の中で必要となるフォレンジック作業で何が必要となるか考察した。考察を踏まえたうえで、本稿では、ドローン用のブラックボックスを提案し、それに基づいたフォレンジック手法、すなわちドローン・フォレンジックを検討した。

2. ドローンによる事故・事件

2.1 ドローンのトラブル事例

2015年4月には首相官邸の屋上でドローンが落下する事件が起きた^[3]。この事件を機に法整備が進められた。国がドローンの事故・事件への連絡を求めるようになった2015年12月以降、2017年10月までに国土交通省に報告のあった事故だけでも計約100件に上る。ドローン墜落による人身事故が日本で初めて報告されたのは2017年2月である。

神奈川県藤沢市で工事関係事業者が建築現場を撮影するために飛行させたところ、電波障害により操縦不能となり、クレーンに衝突し落下した。その結果、下にいた男性作業員が顔に大けがを負った^[4]。国内での死亡事故は報告されていないが、ドローンの事故・事件は後を絶たない。また、海外ではドローンに乗っ取るなどの事件も多く存在する。

2018年12月19日から20日にかけて、イギリスのロンドン南部にあるガトウィック国際空港で上空をドローンが飛行することにより、便の運航ができなくなる事件が発生した。1台だけでなく、複数台が敷地のフェンスを越え、滑走路にまで侵入した^[5]。3日間の閉鎖を経て、21日の夜に犯人の男女2人を逮捕し、ドローンを捕獲した。逮捕には軍用グレードのアンチドローン装置が使用されていた。この逮捕経緯は国民の不安を煽った。このようにドローンに関する事件はいままでにない新たな脅威であることがあり、本件のような逮捕方法は賛否をもたらした^[6]。

日本でもドローンの普及が高まれば、機体内に保存されている情報や荷物運搬の荷物を狙い、第三者が悪事をはたらくことは十分に考えられる。これから日本でドローンを運用していくうえで、トラブルへの対応を考えていかなければならない。事故・事件後は原因究明を速やかに行う必要があり、フォレンジック技術がドローンの普及に欠かせない要素となっている。

2.2 ドローンの飛行レベルと展望

現時点の日本におけるドローン飛行は、目視内で飛行を行うもの(レベル1~2)と目視外で離島や山間部への荷物配送、被災状況調査をするもの(レベル3)が実験飛行段階としてある。今後、環境整備と技術開発を行いながら2020年を目途にレベル4へと発展するようなロードマップ

1 東京電機大学 情報環境学研究所 足立区
2 東京電機大学 情報環境学部 足立区

を経済産業省は発表している（表 1）¹²。飛行実験によって計画通り飛行が可能でも、ドローンへのセキュリティ対策と法整備が並行的に行われないと、運用実現は厳しいものとなる。よって、レベル 3、レベル 4 での活用を可能にするためには起こりうる事故・事件を考え、レベルに応じたリスク評価とセキュリティ実装が必要となる。

表 1. 飛行レベル

レベル 1	目視内での操縦飛行
レベル 2	目視内での自動・自律飛行
レベル 3	無人地帯での目視外飛行
レベル 4	有人地帯（第三者上空）での目視外飛行

また飛行レベルが上がるにつれて、操縦者の特定が難しくなることが挙げられる。目視内では操縦者がドローンの近くで操作しているため、何等かで操作が不可能になっても墜落場所の把握やどの方角へ飛んで行ってしまったかある程度把握できる。目視外については、どこへ飛び、どこに墜落したかを把握することが困難である。GPS で位置を確認できるとの見方もあるが、機体の不具合や墜落の衝撃により、電源が突如遮断されることも十分考えられる。そのため、行方不明になったり、墜落したりする際にドローンを回収する仕組みと操縦者を特定できる仕組みが必要となる。これらは、レベル 1~2 でも起こり得ることであり、公園で飛ばしていたら見失った、見失ったドローンを探したが見つからなかった、墜落した場所は分かったが立ち入ることが難しく諦めた等、トイドローンををはじめ産業用ドローンにおいても考えられる事象である。ドローン特有の回収のしにくさが一種の課題となる。回収しようとしたが第三者によって既に回収されていた等も考えられる。ドローンは機体ごと捕獲されるため、ハードウェアに直接アクセスが可能である。データが暗号化されていないことも多く、アクセスが容易であり、いとも簡単にデータを改竄できてしまうという問題を抱えている。

2.3 レベル 4 活用でのドローンの事故

レベル 4 への活用が可能となっても、以下のようなトラブルが起きる可能性がある。

- 墜落したドローンが人や物に接触
- 道路、鉄道の線路上に落ちる
- 墜落の衝撃でバッテリーが発火

これらのどれもが国民の生活を不安にさせるものである。人に接触すれば、傷害事件へつながる。道路や鉄道の線路上などへ墜落すれば、交通妨害や交通事故へとつながる。また、墜落の衝撃によってはバッテリーから発火し、

火災を招くこともあり得るだろう。これらはドローンへの法整備が進められるなかで、考慮すべき点でもある。また、事故が起きたのは、どこなのか、何時なのか、なぜ起きたのかまで分析できるようにならなければ、レベル 4 への活用まで進むことは難しい。

2.4 ドローンの事故・事件ケース分け

前項で述べたようにドローンは、新たな脅威が発生している。英ガトウィック空港で起きた事件は、まさにドローンが身近に存在する脅威であるという認識が低かったうえ、確立した逮捕方法、ドローンの捕獲方法がなかったことを体現していた。また、このような大きな事件になっていなくてもドローンの事故・事件は後を絶たない。操縦者の誤操作によるものやドローン自体の不具合も数多い。そこで我々はこのような事故・事件の原因究明の仕組みを考えるべく、ケース分けを行った。ドローンにも種類が存在するが、ここでは、トイドローンや産業用ドローンなどの空中を飛行するドローンを想定している。本稿では、操縦者とドローンを回収する者の 2 つの立場からそれぞれの悪意の有無に着目し、以下 4 つのケース分けを行った（表 2）。

表 2. 事故・事件のケース分け

		回収する者の悪意	
		有	無
操縦者の悪意	有	1	3
	無	2	4

証拠の確保が難しい順位として 1~4 まで示してある。それぞれのケースの例を下記に示す。

(1) 悪意のある操縦者が飛行させ、悪意のある者の手に渡る

- 例1. 操縦者はドローンを使用して意図的に危害を加えようと企んでいる。ドローンが悪事を企む第三者の手に渡り、警察の捜査を困難にさせる。
- 例2. 操縦者はドローンを使用して意図的に危害を加えようと企んでいる。ドローンを自ら回収し、機体内にあるデータを改竄し、警察の捜査を困難にさせる。

(2) 悪意のない操縦者が飛行させ、悪意のある者の手に渡る

- 例1. 操縦者は悪意なく、許可された場所で飛ばしていた。第三者のハッカーによってサイバー攻撃を受け、乗っ取り被害にあう。
- 例2. 操縦者の思わぬ誤操作、機体の不具合によってドローンを見失う。そこで悪意のある第三者が

回収し、個人情報等が抜き取られる、データが改竄、破壊される。

(3) 悪意のある操縦者が飛行させ、悪意のない者の手に渡る

- 例1. 操縦者は悪意を持って飛行させている。ドローンを使用して意図的に危害を加えようと企んでいる。ドローンが捕獲される時、警察、航空局の手に渡る。
- 例2. 操縦者は飛行禁止エリアで飛行させている。ドローンが捕獲される時、警察、航空局の手に渡る。

(4) 悪意のない操縦者が飛行させ、悪意のない者の手に渡る

- 例1. 操縦者の思わぬ誤操作、機体の不具合によってドローンを見失う。GPS 情報やログをたどり、操縦者が回収する。または、事故が起きた際、警察、航空局の手に渡り調査が行われる。
- 例2. 操縦者の思わぬ誤操作、機体の不具合によってドローンを見失う。発見した者が警察や航空局に速やかに連絡する。

(1) と (3) は悪意のある操縦者を法律で取り締まり、警察、航空局等で事故・事件の原因究明を行う。(2) と (4) は操縦者の誤操作や機体の不具合などによって起きる。その後警察や航空局等によって、事故・事件の原因究明を行えることが理想である。

悪意のない者の手に渡れば、証拠が残されている可能性が高いため、原因究明が速やかに行える。2 項で述べた空港での事例は、空港内に飛ばそうという悪意があり、結果警察に逮捕、捕獲されたため「悪意のある操縦者が飛行させ、悪意のない者の手に渡る」例となる。ただし、悪意のない者の手に渡るまでの経緯が壮大であり、賛否両論の逮捕、捕獲方法であった。

しかし、これが悪意のある者の手（そのドローンを使い新たに悪さをする、データの改竄を行う等）に渡ると、さらに捜査が困難になることが窺える。データの改竄を防ぐための暗号技術が必要であり、ドローン本体を回収し、そのドローンから、操縦者の特定と事故・事件原因を分析できることが望ましい。分析を行うためには証拠が必要となり、この証拠をどう残すかが重要となる。悪意のある者の手に渡ることを考慮して、フォレンジック技術が確立されなければならない。

3. ドローンセキュリティ

事故・事件を防ぐにはセキュリティ対策が欠かせない。

対策を講じるためには、ドローンが持つリスクを把握することが重要である。Hartman ら^[7]は、ドローンが持つリスクを秘匿性、完全性、可用性についてそれぞれスコア化し、リスク評価を行う手法を提案している。

日本でもドローンのセキュリティについて議論され、様々な検討がされている。その考えをまとめたものとして、2018 年 5 月末に一般社団法人セキュアドローン協議会^[8]にて「ドローンセキュリティガイド」^[9]が策定された。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ようセキュリティガイドは策定された。策定時には、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 関連技術を生かしたものが盛り込まれた。内容はドローンにおけるセキュリティリスク分析をはじめとする、操縦者、管理者と機体の認証、データセキュリティ、業務運用に関する注意点などがまとめられている。非常時の対応は警察や航空局等の機関へ報告するよう促している。

これらの検討は、事故の防止に主眼を置いているが、事故後の対応についても検討していくべきだと我々は考える。ドローンのセキュリティ対策を万全に行ったとしても、事故を完全に防ぐことはできない。セキュリティ対策を施したり、各ドローン提供社の配布するファームウェアをアップデートしていたり、メンテナンスを行っていても事故・事件は発生している。事故を起こした際の対応とその後原因究明を速やかに行える技術、環境を含め現状でも考える必要がある。

4. ドローン用ブラックボックスの提案

4.1 航空機の場合

ドローンの場合、証拠の確保が課題となるが、これと同様の問題をもつ航空機には、FDR（フライトデータレコーダー）と CVR（コックピットボイスレコーダー）から構成されるブラックボックスの搭載が義務づけられ、長く運用されている。本研究でもそれらの設計・運用を参考にドローンの運行情報保持を考える。

FDR には、機体の操作、姿勢、状態、実際の動きなどが記録される。CVR には、過去 2 時間に操縦室で交わされた乗務員同士の会話、航空交通管制との交信の内容が記録される。これらのデータを基に事故・事件発生時の機体操作や動きをコンピュータで再現し、機体に何が起こったのかを突き止めることができる。また、完全性を保つために、RAID による冗長化が行われ、情報が失われないような構造になっている。事故による衝撃が大きくなることを予想して、頑丈なチタンなどの金属で守られている。事故が発生すると自動的に探索用の電波信号、音波信号を発信する機構になっている。また、データは誰が発見しても分析できるよう、暗号化が行われていないこともある^[10]。



図1. ブラックボックス

4.2 ドローンの場合

ドローンは様々な情報を載せ飛行している。空撮した画像データや操縦者情報、飛行記録など様々である。これらの情報はその重要度によって、データの保存方法を考えなければならない。データは以下の条件が重要となる。

- 揮発性の有無
- データの暗号化

揮発性のあるメモリに保存する場合、可用性が低くなるため、情報資産の重要度を見極めて、保存方法を考えなければならない。データの暗号化は様々な視点から考える必要がある。暗号化方法はデータを保存する場所によって異なる。例として、クラウドへの保存やSDカードへの保存などが挙げられる。クラウドへ保存する際には、ドローンとクラウド間の通信を暗号化しなければならない。またSDカードへ保存する際にはデータに対して、暗号化しなければならない。ドローンには、操縦者情報やその他個人情報などの機微情報が含まれていることもある。暗号化せずにデータを保存した際は、悪意のある者によって、それらの情報が漏洩する恐れがある。PCとは違い、ドローンは様々な種類の情報があるため、これらの情報はその重要度によって、データの保存先、保存方法を決めなければならない。ドローンは機体ごと悪意ある第三者の手に渡ること、すなわちハードウェアに直接アクセスされることが前提である。これらの特性と航空機のブラックボックスを踏まえたうえで、図2に示すようなドローン用のブラックボックスを提案する。

- 記録媒体

ICチップを利用することで耐タンパ性を高める。

- データの暗号化

第三者の手に渡ることを考慮し、公開鍵暗号を使用する。機体内に秘密鍵を保持し、公開鍵を操縦者自身が管理し保持する。こうすることで、データの秘匿性を高め、データの改竄を防ぐことを可能とする。また、ICチップを利用し耐タンパ性を高めるため、暗号鍵の抜き取りを防ぐことができる。

- 記録事項

操縦者情報、通信ログ（制御コマンド情報等）、GPS（緯度・経度・高度情報）、映像データ、ドローンの接続元情報（IPアドレス、MACアドレス等）

- ビーコン搭載

ドローンを見失うことが考えられるため、ビーコンを搭載し、探索を可能とする。

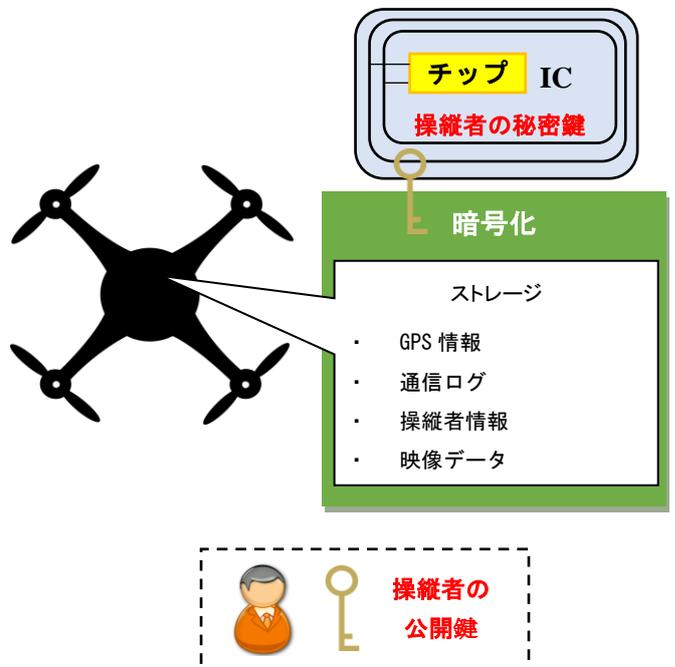
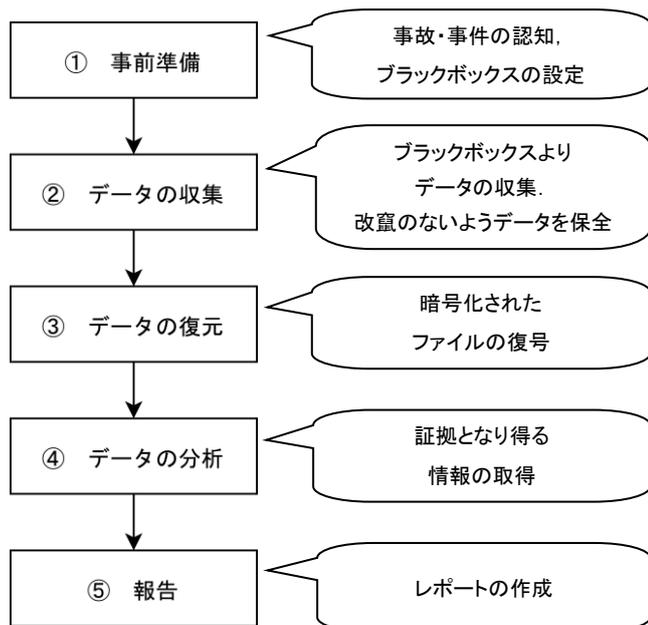


図2. ストレージ暗号方法

5. ドローン・フォレンジック

4項で述べたブラックボックスを基にデジタル・フォレンジック手法の検討を行った。今回は、警察や航空局が事故・事件の原因究明を行うものとして、検討を行う。デジタル・フォレンジックの一連の手順を図3に示す。図3の手順に従い、ドローン・フォレンジックの手法①～⑤を示す^[4]。



佐々木良一編「デジタル・フォレンジックの基礎と実践」p6の図1.5を参考に作成

図3. デジタル・フォレンジックの手順

- ① **事前準備**：事故・事件に備え普段からログを収集しておくとともに、対象となる事故・事件を認知し、対応方針、対応体制を決定し、準備作業を行う。ブラックボックスでログの収集を行う。このブラックボックスを使用して、事故・事件の原因究明を行う。
- ② **データの収集**：事故・事件が発生した場合に、ブラックボックスより調査に必要なデータを収集し、不正に改竄されないようデータを保全する。
悪意ある第三者の手に渡ることを考慮し、耐タンパ性を高める必要がある、ICチップを利用することで耐タンパ性を高めている。
- ③ **データの復元**：収集したデータから暗号化されたデータを復号したり消去されたデータを復元したりする。解析用ファイル形式に変換された証拠データを解析用ソフトウェアで認識する。ブラックボックスより、操縦者情報、GPSデータ(緯度・経度・高度)など暗号化されたファイルの復号を試みる。
- ④ **データの分析**：復号したデータに対し、法的に正当とみられる手法を使用して分析を実施し、証拠となり得る情報を得る。事故・事件原因をブラックボックスより分析する。操縦者情報より操縦者の特定を行う。映像データ、GPS情報などから、事故・事件が起きた場所を特定する。

- ⑤ **報告**：調査結果を依頼主に報告する。
法廷において最重要視されるレポートの作成を行う。報告書の内容は公平であること、客観的であること、真実であること、理解可能であることなどが求められる。

6. おわりに

今回、4つの事故・事件のケースに分け、ドローンにおけるブラックボックスを提案し、それに基づいたデジタル・フォレンジック手法、すなわちドローン・フォレンジックを検討した。ブラックボックスより、操縦者の特定、ドローンの捕獲、なぜ事故は起きたのか、その事故によって何が起きたのかを分析できる仕組みが一連のプロセスとして表すことができた。現状でも事故・事件後の対応とその原因究明を行える仕組みを確立したい。このブラックボックスはICチップを用いてドローンのデータを暗号化し、安全に保持する一例であり、この他にTPMを用いた暗号化方法も考えられる。今後はこの機構を設計したうえで、ドローンへ実装し、デモとして検証していく予定である。

参考文献

- [1] 野波健蔵, ドローンの最先端技術とビジネス最前線及び近未来展望, 飛躍するドローン マルチ回転翼型無人航空機の開発と応用研究, 海外動向, リスク対策まで, pp4-7, 2016年1月15日
- [2] 経済産業省「小型無人機の利活用と技術開発のロードマップ」<https://www.meti.go.jp/policy/mono_info_service/mono/robot/drone.html>, 本体, 補助資料(参照2019/5/10)
- [3] 日本経済新聞「首相官邸にドローン落下 けが人はなし」<https://www.nikkei.com/article/DGXLASDG22H5G_S5A420C1CC000/>(参照2019/5/10)
- [4] 日本経済新聞「ドローン事故, 各地で相次ぐ けが人はまれ」<<https://www.nikkei.com/article/DGXMZ023118340U7A101C1CC1000/>>(参照2019/5/10)
- [5] BBC.com「英ガトウィック空港, ドローン侵入で閉鎖続く 警察は「ドローンを撃ち落とす」可能性も」<<https://www.bbc.com/japanese/46643482>>(参照2019/5/10)
- [6] THEVERGE「London's Heathrow and Gatwick airports have purchased their own anti-drone systems」<<https://www.theverge.com/2019/1/5/18169215/london-heathrow-gatwick-airports-anti-drone-defense-systems>>(参照2019/5/10)
- [7] The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment, 2013 5th International Conference on Cyber Conflict, 1-23(2013)
- [8] 一般社団法人セキュアドローン協議会「ドローンのICT業務活用をセキュアに」<<https://www.secure-drone.org/>>(参照2019/5/10)
- [9] 一般社団法人セキュアドローン協議会「ドローンセキュリティガイド」<https://www.secure-drone.org/wp-content/uploads/drone_security_guide_201803.pdf>(参照2019/5/10)
- [10] カスペルスキー公式ブログ「ブラックボックスが伝えるもの: フライトレコーダーの秘密」<<https://blog.kaspersky.co.jp/flight-recorders/9507/>>(参照2019/5/10)
- [11] 佐々木良一編, デジタル・フォレンジックの基礎と実践, pp6-7, 2017年3月10日