Vol.2020-DPS-182 No.15
Vol.2020-CSEC-88 No.15
2020/3/12

民生用ドローンに対するセキュリティと安全性の調査と対策の提案

池睦樹[1]　大久保隆夫[1]

概要：2020 年現在，ドローン発展を遂げている．空撮や農薬散布に活用されており，今後は宅配などの活躍が期待されている．本研究では，個人または企業が入手可能である民生用ドローンのセキュリティ脅威について着目した．ドローンの構成やセキュリティ脅威について調査を行い，対策の提案をした．

キーワード：ドローン

1. はじめに

多種多様なドローンであるが，無線通信を使い操縦者と制御命令やドローンの状態などの情報をやり取りしていることや Internet of Things(IoT)機器同様，組み込み系の OS を使っていることからドローンはコンピュータやネットワークに大きく依存していると言える．そのため，攻撃者によってハッキングされ，意図的に墜落や制御を乗っ取るといったセキュリティのリスクが考えられる．乗っ取りによって機体の損失だけではなく，墜落によって人身事故や社会インフラストラクチャに影響を及ぼす危険性がある．

しかし，ドローンのセキュリティ対策は現状不十分である．法整備によってドローンの操縦に関する規制があるが，機体そのものに対する整備は日本国内では無線通信法のみしかなく，ドローンの国際標準化も決まっていない現状である．

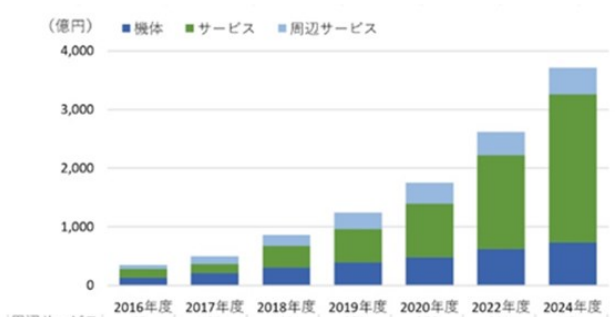
そこで本研究は，個人または企業が入手可能である民生用ドローンのセキュリティ脅威について着目した．ドローンの構成や法整備，ドローンが引き起こす事故について調べ，まとめた．また，市販されている民生用ドローン 4 台に対し，スペックや脆弱性を調査し，ドローンに対し適切であるセキュリティ対策の提案，攻撃者がドローンを狙う目的，ドローンのセキュリティ対策の問題点などを述べた．

2. ドローンについて

ドローンとは無人で遠隔操縦や自動制御によって飛行できる航空機の総長である．ドローンの定義は幅広いため，本論文では自立飛行できるマルチコプターをドローンとし説明していく．

2.1 ドローンの市場規模

2020 年現在，日本国内のドローン市場規模は急激に拡大している．図 1 は国内のドローンビジネス市場規模の予測を示したグラフである．2018 年度の日本国内のドローンビジネス市場規模は 931 億円と推測され，2017 年度の 503 億円から 428 億円増加している．2019 年度には前年比 56%増の 1450 億円に拡大し，2024 年度には 5073 億円（2018 年度の約 5.4 倍）に達すると見込まれる．[1]



	2016年度	2017年度	2018年度	2019年度	2020年度	2022年度	2024年度
周辺サービス	65	138	189	279	355	398	451
サービス	154	155	363	567	917	1,599	2,530
機体	134	210	308	394	481	624	730
合計	353	503	860	1,240	1,753	2,621	3,711

図 1 国内のドローンビジネス市場規模の予測[1]

2.2 ドローンのアーキテクチャ

ドローンのアーキテクチャについて説明する．図 2 はドローンの構成を図にしたものである．以下で各要素について説明する．

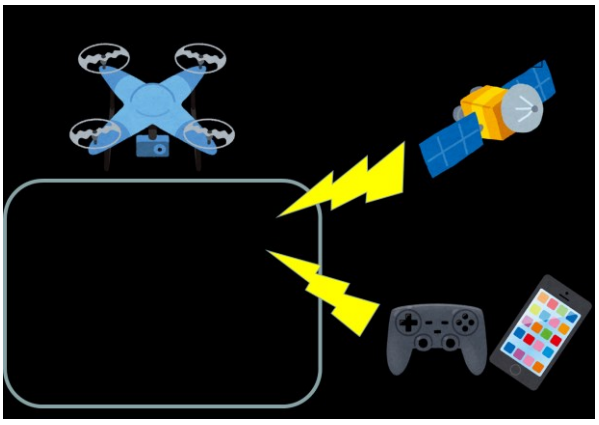


図 2 ドローンの構成図

1 情報セキュリティ大学院大学
Institute of information security

・フライトコントローラ

フライトコントローラとはドローンの中核部分である．フライトコントローラはマイクロコンピュータと Inertial Measurement Unit(IMU)が搭載されている．IMU はドローンが外部の情報を取得するために必要なセンサー類を指す．マイクロコンピュータは送受信機から命令を受け，モーターを動かしドローンの制御を行う．また，IMU から得た情報をもとに処理を行い，自動飛行制御やドローンの高度や現在地などの情報を送受信機に送信する．主にフライトコントローラは ARM プロセッサを用いられ，OS は Linux を使用している[2].

・GPS

GPS(Global Positioning System)とは，衛星からの発射した時刻信号の到達時間などから，地球上の電波受信者の位置を 3 次元測位するものである．

ドローンの現在地を操縦者が把握するためや操縦者への元へ戻るために GPS を搭載している．GPS 搭載ドローンでは，自律飛行が可能で設定したルート通りに位置を把握しながら飛行することができる．室内で飛ばすホビードローンには搭載されていないケースが多い．

・送信機

送信機はドローンの操縦機器であり，ドローンに制御命令を送ることやドローンの現在地や高度などの情報と確認することができる．送信機はメーカーや機種によって様々であり，スマートフォンまたはタブレット PC にアプリを入れ，送信機にするものと，ゲーム機のコントローラーのような形の送信機がある．

スマートフォンまたはタブレット PC を使用する際は，メーカーからアプリが配信されており，アプリストアにてインストールをする．アプリを起動することでドローンの送信機となり，操縦を行うことができる．カメラ付きドローンであれば，画面にカメラ映像が映し出される．

・通信

ドローンと送信機の間は主に 2.4Ghz 帯，5Ghz 帯の無線通信を使用している．ホビー用は許可や資格が必要のない 2.4Ghz を，商用やレースで使うドローンは免許や資格が必要な 5.7Ghz が使われていることが多い[3].

3. 法律・条令

ドローンに関する法律・条令について紹介していく．航空法や操縦規制，ドローンの登録義務について説明する．

3.1 航空法

2015 年 4 月 22 日に首相官邸にドローンが落下した事件[4]が起こったため，2015 年 8 月に航空法の一部が改訂され，ドローンやラジコン機などの飛行ルールが新たに導入された. 対象となる無人航空機は,「飛行機, 回転翼航空機, 滑空機，飛行船であって構造上人が乗ることができないもののうち，遠隔操作又は自動操縦により飛行させることができるもの（200 g 未満の重量（機体本体の重量とバッテリーの重量の合計）のものを除く）」[5]．これにより 200g 以上ドローンは当てはまることとなる．

以下では，国土交通省の「無人航空機（ドローン，ラジコン機等）の安全な飛行のためのガイドライン」[6]から定められている規定を紹介する．

3.1.1 飛行の禁止区画

有人の飛行機に衝突するおそれや，落下した場合に地上の人などに危害を及ぼすおそれがある空域で無人航空機を飛行させることは原則禁止されている．これらの空域で飛行させようとする場合には，国土交通大臣の許可を受ける必要である．飛行禁止の区間は以下の 3 つになる．以下 3 つに該当しない空域・地域であれば航空法対象のドローンを飛ばすことができる．

・地表または水面から 150m 以上の高さの空域
・空港やヘリポート周辺の空域
・人口集中地区の上空

3.2 小型無人機等飛行禁止法

小型無人機等飛行禁止法とは国会議事堂. 内閣総理大臣官邸その他の国の重要な施設等，外国公館及び原子力事業所の周辺地域の上空における小型無人機の飛行の禁止に関する法律である[7]．対象になるのは重要施設の周囲 300m である．200g 以上のドローンのみに適応させる改正航空機に対し，小型無人機等飛行禁止法は 200g 以上・未満すべてのドローンに適応される．和文ならびに英文の表題を罫線内に記述する．

3.3 電波法

ドローンの操縦には電波を使用するため，混線等を防ぐため「特定無線設備の技術基準適合証明(技適)」[8]の取得が義務付けられている．大手メーカーの正規販売代理店が販売するものではない場合，技適が通過していない可能性がある．また，5.8Hz 帯のドローンは国内では許可なく使用できないため注意する必要である．

3.4 登録義務

国土交通省は 2021 年度に，小型無人機ドローンの所有者に期待情報の登録を義務付ける方針を明らかにした．氏名や型式を届けた上で，国が付与する番号を表示する仕組みを想定している．事故やトラブル時に所有者を特定しやすくなる．全機体の登録組お選択肢に入れており，ホビー用の小型ドローンも対象に含まれる可能性がある．[9, 10]

Vol.2020-DPS-182 No.15
Vol.2020-CSEC-88 No.15
2020/3/12

4. 墜落

ドローンが墜落するリスクについて紹介する．ドローンが墜落または紛失する要因や墜落の危険性と墜落事故の事例について説明する．

4.1 要因

ドローンが墜落・紛失する要因として，天候・通信障害・操縦ミス・ソフトウェアの異常などがあげられる．こういった要因からドローンが操縦不能に障害物にぶつかることで墜落してしまう．

4.2 墜落の危険性

ドローンが墜落した際に事故を引き起こす危険性について紹介する．墜落事故の事例や考えられる危険性について説明する．

2019 年度の日本国内ドローンに係る事故トラブルは国土交通省に報告があったもので 70 件確認されている[11]．墜落の要因は，強風や衝突，制御不能などである．

日本国内では，2017 年 11 月にイベント会場にて，ドローンが墜落し，子供 4 人を含む 6 人が顔や背中に軽い傷をした事故が[12]，2017 年 2 月には工事現場にて空撮するために飛行していたドローンが墜落し，顔を数針縫う怪我を負った事故が起こっている[13]．海外でもドローン墜落による事故は起こっており，2016 年にスイスでは屋外イベント中にドローンが落下し，女性の頭に衝突し大けがをした事故[14]や 2019 年に国政郵便会社が利用していた輸送ドローンが子供の近くに墜落したため業務を中断した事例[15]もある．後者の事故では，安全装置であるパラシュートを装着していたが，パラシュートの紐が切れ，墜落している．

人身事故だけではなく，道路や鉄道線路，飛行場などの公共交通機関に墜落した場合，大きな影響を及ぼす可能性がある．事故の規模によっては通行止めや運休などが起こりえる．原則．鉄道線路や飛行場などの付近ではドローンを飛ばすことは禁止されているが，飛行場にドローンが近付いたことにより離着陸が断続的に停止になる事態[16]も起きている．

5. セキュリティ脅威

本章ではドローンに対するセキュリティ脅威について紹介する．ドローンはマイクロコンピュータを内蔵していることや 2.4Ghz, 5Ghz 帯の無線通信を使用しているため，他の IT 製品を同じくバグや脆弱性を悪用され，ハッキングされる危険性がある．ハッキングされると制御を乗っ取られ，ドローンが墜落または盗まれてしまう．

5.1 マルウェア

ドローンのフライトコントローラは，マイクロコンピュータを使用しているため，マルウェアに感染する危険性がある．感染方法としては，ドローンのアクセスポイントに不正にアクセスし，空いているポートなどを悪用しマルウェアを仕込む．また，送信機に不正なドローンアプリをインストールさせ，制御を奪う，または，送信機からドローンにマルウェアを仕込む．2020 年 1 月現在，攻撃者によって作成されたドローンに対するマルウェアは発見されていない．

しかし，研究者によって Parrot 社製ドローン「AR.Drone 2.0」(図 3)[17]に対してマルウェアを作成しており，ドローンに感染させ制御を奪う攻撃が多数発表されている．AR.Drone2.0 には脆弱性があり，Wi-Fi 接続時のパスワードが設定されていないことや telnet と ftp が空いており，認証無しでアクセスでき，管理者権限を最初から持っていること．また，パケットが暗号化されておらず，中身が確認できてしまう問題点がある．

CODE BULE 2014 にて DONGCHEOL HONG が発表した攻撃[18]では，ネットワーク経由または送信機の偽造アプリから AR.Drone2.0 に対し，FTP 使いマルウェアを感染させる．その後 telnet を使い，マルウェアを実行させることで制御を奪う．また，感染させた AR Drone2.0 から他の AR Drone2.0 に対しマルウェアを感染させることも可能となっている．

Rahuk Sasi がドローン用バックドアマルウェアをハッカーフォーラムにて公開[19]，nullcon 2015 にて発表している[41]．このマルウェアは「Maldrone」と呼称されている．Maldrone は ARDrone2.0 の各種センサーとシリアルポートを使用して通信し，ドローンを制御しているプログラム悪用する．各種センサーへのシリアルポートを改ざんし，Maldrone を介して通信が行われるように設定する．これによりバックドアが作成され，プログラムに対し偽の命令を送ることで制御を奪うことが可能となっている．

以上の攻撃例から，脆弱性があるドローンに対してマルウェア感染させることは可能ということが確認されている．

図 3 AR.Drone2.0

5.2 電波の成りすまし

ドローンは送信機からの制御命令や人工衛星からの GPS 信号を受信している．そのため，ドローンと送信機の間で行われる通信を解析され，偽の通信を受信することによってドローンの制御が奪われることや偽の GPS 信号を受信

してドローンの現在地を偽造される可能性が考えられる．

Ethical Hacking Conference 2016 にて Mark Szabo-Simon が，AR Drone2.0 に対し，偽造パケットを流すことによって制御を奪う攻撃を発表している[20]．この攻撃は AR Drone2.0 と送信機の間のパケットの詳細を確認できることや UDP を使っているため，電話の IP を簡単に偽造できるために，偽造パケットでドローンを乗っ取ることが可能となっている．偽造パケットを送信するソースコードは公開しており，誰でも実行可能となっている．また，「SkyJack」と呼ばれる攻撃が Samy Kamkar によって公開されている[21]．SkyJack は AR Drone2.0 と Raspberry Pi を組み合わせたドローンを使い，他の Parrot 社製ドローンに対し，切断パケットを送信することで所有者との無線通信を強制的に遮断させる．その後，所有者のふりをし，ドローンにアクセスすることで制御を奪うものとなっている．これもソースコードや必要なソフトウェアとハードウェアが紹介されており，知識さえあれば実行することができる．

オハイオ州立大学にて，DJI 社製ドローンに GPS スプーフィングをし，ヘリポートなどの飛行禁止区間にいるように偽造する実験が行われている[22]．これにより，DJI 社製ドローンは飛行禁止区間では離陸できないため，飛行していた場合は強制着陸し，離陸不可能な状態となる．

5.3 DoS 攻撃

Gabriel Vasconcelos らの研究[23]は，Wi-Fi を使用している商用ドローン(AR Drone2.0 と 3DR SOLO)に対する DoS 攻撃を評価している．結果として，DoS 攻撃によって送信機に映るドローンのリアルタイムのカメラ映像のフレームレートが低下した．また，AR Drone2.0 に比べ，3DR SOLO はハードウェアとソフトウェアの構成が改善されているのにも関わらず，DoS 攻撃中のパフォーマンスに違いがないことを示している．

6. 調査

民生用ドローン対して安全性や脆弱性の調査した結果とドローンのソフトウェアアップデート方式について説明する．

6.1 機体調査

民生用のドローンに対し，基本スペックや操縦方法，脆弱性の調査を行った．本研究にて，調査したドローンは「AR Drone 2.0」，「SPARK」，「HS100]，「Tello」の 4 台である(図 4)．

AR Drone2.0 は脆弱性があることや攻撃対象になることが多いため，残り 3 台はメーカー別であることや amazon にて人気があるものを選出した．4 台のドローンの基本情報について図 5 にて示す．

各ドローンに対し，ポートスキャンやパスワードとファームウェア更新の有無などの調査結果を以下にて説明する．

図 4 調査ドローン(左上「AR Drone 2.0」，右上「SPARK」，左下「HS100」，右下「Tello」)

	AR Drone 2.0	SPARK	HS100	Tello
メーカー	Parrot	DJI	Holy stone	Ryze Tech
発売日	2012年7月	2017年6月	2017年11月	2018年1月
重量 (バッテリー込み)	420g	300g	700g	80g
価格	32,500円	65,800円	23,820円	12,693円
サイズ	52 x 52 cm	143 x 143 mm	50 x 50 cm	98 x 92.5 mm
送信機	スマートフォン	スマートフォン または コントローラ	コントローラ	スマートフォン
スマートフォン アプリケーション	AR.FreeFlight	DJI GO 4	HS GPS V1	tello
GPS	×	○	○	×

図 5 ドローン 4 台のスペック

調査した結果を図 6 に示す．機種によってパスワードとポートに違いがある．また，HS100 のセキュリティが他機種に比べ，低いことが確認できる．

初期パスワードが設定されているのは，SPARK のみであり，ユーザーがパスワード設定・変更を行えるのは SPARK と Tello の 2 台だけである．ポートに関しては，機体ごとに開放されているポートが違う結果となった．しかし，Tello 以外は，21 番の ftp か 23 番の telnet が空いている．ftp はドローンが撮影した映像をスマートフォンに転送するためか，ファームウェア更新用に空いていると考えられるが，telnet に関しては，不明である．AR.Drone の telnet と ftp，Spark の ftp は認証無しでアクセスできることが確認することができた．

HS100 は，初期パスワードなし，パスワード・SSID 変更不可，ファームウェア更新機能なし，21 番ポート開放という結果となっており，セキュリティが非常に低いことがわかる．HS100 に関しては他機種とは違い，アプリケーションから操縦することができなく，ペアリング接続したコントローラーからしか操縦することができない．そのため，不正アクセスされたとしても，制御を奪われる危険性は他機種と比べると少ない．しかし，ドローンの映像を盗み見られることは可能であり，制御を奪われる危険性も

Vol.2020-DPS-182 No.15
Vol.2020-CSEC-88 No.15
2020/3/12

ないわけではない．

また，AR.Drone2.0 と Tello は UDP を使っていることが判明しているが，SPARK と HS100 はわかっていない．そのため，Nmap を使い，UDP スキャンを行ったところ，UDP スキャンの性質上，時間が大幅にかかり，ドローンのバッテリーが切れてしまう問題が発覚した．ドローンに対する UDP スキャンはバッテリーの問題やフライトコントローラのスペック不足等の問題があり，現実的ではないことが確認できた．

	AR Drone 2.0	SPARK	HS100	Tello
初期パスワード	なし	あり	なし	なし
パスワード変更・設定	×	○	×	○
初期SSID (xは可変)	ARDrone2_xxxx	Spark-xxxxxx	holystoneFPV-xxxxx	TELLO-XXXXXX
SSID変更	○	○	×	○
ファームウェアアップデート	○	○	×	○
TCP ポートスキャン	21、23、5555	21	23、8888	9999

図 6 機体調査結果

6.2 ファームウェアアップデート

ドローンのファームウェアアップデートの仕組みについて調査した結果を紹介する．

ファームウェアの更新は，図 7 のように行われる．アプリケーション起動時，または，アプリケーション内のファームウェアの更新ボタンを押すことで，メーカーのサーバーへバージョンの確認をする．更新がある場合は，ファームウェア更新のパッケージファイルをサーバーからアプリケーションを起動している端末へダウンロードする．ダウンロード後，Wi-Fi またはケーブルで端末とドローンを接続し，ドローンへアップデートファイルを転送させ，インストールすることでファームウェアの更新を行う．

本調査にて，ドローン本体のバージョンを確認し，ファームウェアの更新を行うのではなく，アプリケーション内のバージョンを参照し，更新することが確認できた．

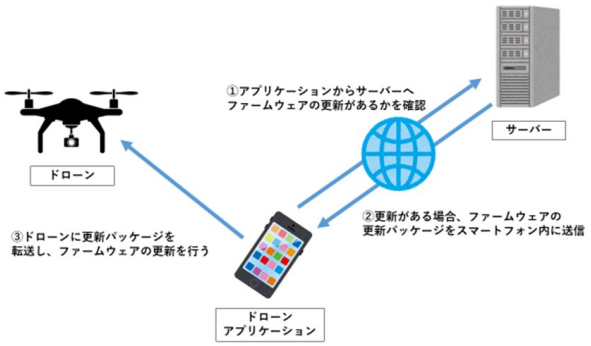


図 7 ドローンファームウェア更新の手順

7. ドローンを狙う攻撃者について

本章では，ドローンを狙った攻撃者について考察したことを紹介する．本研究にて調査した結果から，攻撃者がどのような目的としてドローンを攻撃するか．また，攻撃する上での問題点について述べる．

7.1 攻撃者の目的

ドローンに対する攻撃によって引き起こされるものは，機体の盗難・墜落・データの盗難があげられる．

盗難は，機種によっては高価なものもあり，商用利用される大型のドローンは 1 台, 100 万円を超えるものが多く，価値が高い．また，宅配ドローンは宅配物を盗む目的で狙われる可能性は高い．そのため，金銭目的の攻撃が考えられる．

墜落に関しては，墜落によって攻撃者が得られるものは少なく, 愉快犯もしくはテロ目的で行われると考えられる．墜落によってドローンが破損してしまうだけではなく，イベント会場など大人数がいる場所でドローンを墜落させられると大きな被害が出てしまう．

データの盗難には，ドローンが撮影した映像や現在地などの操縦者の個人情報や宅配ドローンから航行ルートや宅配物の情報，届け先の住所などの情報を盗む目的から電波の盗聴または機体の盗難などの攻撃をすると考えられる．

7.2 攻撃する上での問題点

ドローンを攻撃する上での問題が多数存在している．民生用ドローンは基本的に，送信機とドローンと接続しており，送信機であるスマートフォンなどのデバイスを介してインターネットに接続している．また，常にドローンはデバイスと接続されているわけではなく，使用時のみ電源をいれ接続するものとなっている．そのような仕組みからインターネットからドローンに対しての直接ハッキングやマルウェア感染は原則不可能となっている．そのため，スマートフォンなどのデバイスから攻撃を行うか，ドローンの電波が届く範囲にて攻撃をしなければならない．

デバイスから攻撃をする場合には，スマートフォンにマルウェアを感染させ，遠隔操作するか偽のドローンアプリケーションを仕込まなければならない．問題点として，スマートフォンにマルウェアや偽アプリケーションを入れさせるのは非常に困難である．攻撃が成功した場合もスマートフォンから情報を抜き取ればよく，そこから攻撃者がドローンを狙うとは考えづらい．また，この方法では特定したドローンに攻撃するのは難しく，窃盗は現実的ではない．そのため，ドローンの電波が届く範囲にて攻撃を行うのが現実的である．しかし，攻撃者が物理的にドローンに近づく必要があり，攻撃した際に発見される可能性もないとは言えない．制御を奪った場合も攻撃者は電波の届く範囲ま

でしか制御はできないため，場所によっては窃盗できないことも可能性もある．他にも，攻撃対象のドローンが飛んでいるかはその場に行き，確認しなければいけない問題点もある．

以上の理由から，民生用ドローンに対しては，攻撃が成功した際に得られるものと攻撃する上でのリスクが見合ってないと思われる．しかし，今後宅配などの完全自動制御などの用途別で狙われる危険がある．

8. 対策の提案

本章では，ドローンのセキュリティと安全性の向上のため，ドローンの法整備や規制の提案と機体に対する対策の提案を述べる．現在の法整備やドローンについての安全性とセキュリティの観点での問題点を述べ，改善法を提案する．

本研究にて，ドローンによって引き起こされる脅威やセキュリティ上の問題点について紹介した．法整備や機体のセキュリティ対策が不十分だと考えられる．ドローンを使用する際に安全に使えるよう，法整備の改善とドローンのセキュリティを向上する必要がある．

8.1 法・規制の提案

本文 3 章にてドローンに対する法律や規制について述べたが，日本国内では操縦に関するものが大半であり，機体に関する法や規制は「電波通信法特定無線設備の技術基準適合証明」[8]しかない．米国連邦航空局（FAA）では米国内におけるドローンの遠隔識別に関する規則案を発表し，機体にナンバープレートを提供するものを決めており，機体に対する法整備も進まれている．

そのため，ドローンの機体に関する規制が必要あり，安全性やセキュリティ上の問題点があるドローンを屋外にて使用することを制限すべきだと考える．ドローンには，IoT 機器の技術基準適合認定(IoT 技適)[24]のような技術基準適合認定が必要である．IoT 技適とは，IoT がマルウェアによるボット化を防ぐもので，認証機能や初期パスワードの設定，ソフトウェアの更新が義務化されるものである．ドローンもハッキングの脅威や不具合による墜落を防ぐため，同様の技術適応認定が必要であるべきだと考える．

また，2018 年 11 月国際標準化機構によるドローンの国際規格の草案が公表されている[25]．飛行に関するルール，技術仕様，製造品質，飛行管理などが決められる予定である．国際規格に，満たないドローンに関しては飛行の制限または禁止などを制定すべきである．しかし，2019 年内には採択される見通しの予定だが，2020 年 1 月現在，草案の公表から音沙汰がなく，採択される見通しが立っていない．

日本国内だけではなく，世界全体としてドローンのルールを決めておく必要がある．国ごとに法や規制が違うため，外国人観光客のドローン違法飛行が問題となっている．パンフレットや張り紙にてドローンの違法飛行を伝えているが，根本的な解決にはなっていない．2020 年の東京オリンピックや 2025 年の大阪万博にて，観光客が急増することが想定される中で，より良い対策を検討していく必要があるだろう．

8.2 機体の対策

ドローンの対策としては，基礎的なセキュリティ対策が必要である．パスワードが設定されていないのは非常に危険で，誰でも接続ができてしまうのは問題である．そのため，パスワードは初期状態から設定しておくべきである．初期パスワードがドローンの機種で統一されているのはセキュリティに問題があり，初期起動時にユーザーに変更させるべきである．SSID に関しては，初期では機体名が書かれていることが多く，SSID から近くにどの機種のドローンが稼働しているかがわかってしまう．セキュリティの向上には機体名は SSID に書かないことが好ましいが，操縦者がわからなくなってしまう可能性がある．また，ドローンに接続する端末は限られており，Wi-Fi にアクセスするのは原則一台である．そのため，複数台接続できないようにすることで正規の接続以外はアクセスできず，不正なアクセスを防ぐことができる．他にも，ファームウェアの更新機能は実装する必要がある．機能の更新だけではなく，バグや不具合を即座に修正できるように更新機能が必要である．また，ファームウェアの更新がある場合はユーザーに通知するか，自動更新するように設定しておくのが好ましい．

本調査にて，telnet や ftp のポートが空いているドローンがあることが確認できている．不要なポートは閉じておく必要がある．特に telnet や ftp は 5 章で紹介した攻撃に利用される危険性があり，使用する際は注意する必要がある．また，GPS スプーフィングは明確な対策方法はなく，研究・実験段階である．アプリケーション側で対策できることとして，急激にドローンの位置が変わった際に操縦者へ警告するなどが考えられる．

利便性だけを考えるのであれば，パスワードは設定せず，初期起動時でパスワードの設定を強制させないほうがいい．特に，屋内で飛ばすことを想定した小型のホビードローン等は設定すると，子供やデバイスに疎い人が使いづらくなってしまう．セキュリティを高めてしまうと利便性が損なわれる問題があり，検討しなければいけないことである．原則，屋外で飛ばすドローンに関しては最低限のセキュリティ対策はするべきだろう．

9. 対策の問題点

本章では，ドローンのセキュリティ対策における問題点を述べる．ドローン特有の問題や不正ドローンに対する防

衛手法との利害衝突について説明する．

ドローンは空を飛ぶ関係で，なるべく軽量化する必要がある．重量が増すとその分モーターやプロペラを大きくしなければいけない．また，操縦に影響がないようにリアルタイム性を維持しなければいけない．このような問題から高性能な暗号やアクセス制御などのセキュリティ対策の実装は難しくなっている．実装することによる処理の遅延の問題や遅延に対するフライトコントローラのスペック向上をすることによる重量増加によって機体サイズが大きくなり，コストが増大する．特に，非商用ドローンはコストの増加による販売価格の上昇は売上に関わってくるため問題である．200g 以下のホビードローンから商用の大型ドローンがある中で，高度なセキュリティ対策をどのドローンまで適応させる必要があるかは検討すべきである．

また，不正ドローンに対する防衛手法と利害衝突する問題点もある．飛行禁止区域を無許可で飛ぶドローンに対して，妨害電波装置を使い，強制的に着陸させる防衛手法がある．日本国内でも，警視庁が不正ドローンに対する妨害電波装置の導入を進めている[26]．この手法は攻撃者も使用することが想定でき，攻撃者が出す妨害電波によってドローンは着陸してしまう危険性がある．また，攻撃者だけではなく高圧電線などにより電波障害が起こってしまう可能性もある．安全を考えるとドローンは他の電波からの障害を受けないよう対策し，意図せず着陸してしまうことを防ぐ必要がある．しかし，妨害電波に強いドローンが出ると，不正ドローンに対する防御手法も防いでしまう可能性が悪用される危険がある．このような利害衝突が起きてしまう問題があり，一概に安全性を高めるだけではなく，不正ドローンに対する防御手法を考慮して検討していく必要があるだろう．

10. まとめ

本研究では，民生用ドローンに着目し，ドローン対し脅威や脆弱性と安全性の調査を行い，攻撃者目線のリスクを明確化し，法整備と機体の対策を提案した．民生用ドローンは基礎的なセキュリティが抜けており，他の IT 製品同様の対策が必要なことが確認できた．

ドローンは他の IT 製品を違い，空を飛んでいる独自性があり，墜落する危険性がある．墜落するによって人や物に大きな影響を与える可能性があり，安全性の向上は必要不可欠である．また，マイクロコンピュータを搭載していることや無線通信にて制御命令を送っているため，ハッキングといったセキュリティの脅威が存在している．ドローンが墜落することで起こる脅威やハッキングの危険性はあまり認知されていない．本研究にて危険性やセキュリティ脅威を明確化することで，ドローンのセキュリティ意識を向上が期待できる．

新たな法整備や機体のセキュリティ対策を提案することによって制御を乗っ取られることや意図的に墜落させられるリスクを少なくし，墜落による被害が減ることが期待できる．

11. 今後の課題

今後検討すべき課題として，いくつか提案する．

(1)重量別の調査

本研究では，ドローンの重量に関らず調査を行った．しかし，重量によって性能や航空法の適応がされるかなどの違いがあった．そのため，同じ重さのドローンまたは航空法が適応されるかで分けた調査・比較などの実験を行う．

(2)ドローンへの既存セキュリティ対策の導入

既存のドローンに対して，既存のセキュリティ対策が導入できるかを実験し，攻撃が防げるのを検証する．既存のドローンだけではなく，自作でドローン作成し，既知のセキュリティ対策が実装可能か，実装した際の影響などについて調査・検討する．

(3)自立制御型ドローンのセキュリティ脅威の検討

宅配や警備ドローンなどは，インターネットからドローンに対し直接制御命令を送ると考えられる．インターネットに繋がっているため，遠隔での攻撃が想定される．自立型ドローンのセキュリティ脅威の調査や対策方法の提案などを今後検討する．

謝辞 本研究を進めるにあたり，研究への取り組み方や研究の方向性についてご指導してくださった，情報セキュリティ大学院大学大久保隆夫教授．また，ゼミ発表などにおいてコメントやアドバイスを頂きました大久保研究室の皆さまに心から感謝いたします．

参考文献

[1] 株式会社インプレス-ドローンビジネス調査報告書 2019 https://research.impress.co.jp/report/list/drone/500602 <参照 2019/08/20>

[2] Renju Liu and Mani Srivastav “PROTC: PROTeCting Drone’s Peripherals through ARM TrustZone” DroNet '17 Proceedings of the 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications Pages 1-6

[3] 総務省 電波利用ホームページ - ドローン等に用いられる無線設備について https://www.tele.soumu.go.jp/j/sys/others/drone/ <参照 2019/12/28>

[4]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_S5A420C1CC0000/<参照 2020/1/23>

[5] 国土交通省-飛行ルールの対象となる機体
http://www.mlit.go.jp/koku/koku_fr10_000040.html
<参照 2019/05/20>
[6] 国土交通省 航空局 - 無人航空機(ドローン，ラジコン機等)の安全な飛行なためのガイドライン
https://www.mlit.go.jp/common/001202589.pdf
<参照 2020/12/20>
[7] 警察庁 - 小型無人機等飛行禁止法について
https://www.keishicho.metro.tokyo.jp/kurashi/heion/drone.html
<参照 2020/1/9>
[8] 総務省 電波利用 - 特定無線設備の技術適合証明等に関する規則
https://www.tele.soumu.go.jp/horei/reiki_honbun/a723430001.html<参照 2020/1/8>
[9] 東京新聞 TOKYO web - ドローン，登録義務化へ 国交省 時期未定，罰則も検討
https://www.tokyo-np.co.jp/article/politics/list/201912/CK2019120302000135.html
<参照 2020/1/10>
[10] 東京経済新聞 - ドローン登録義務化 21 年度中に
https://www.nikkei.com/article/DGKKZO53383730V11C19A2PE8000/<参照 2020/1/10>
[11] 国土交通省 - 平成 31 年度 無人航空機に係る事故トラブル等の一覧
https://www.mlit.go.jp/common/001292055.pdf
<参照 2020/1/11>
[12] 日本経済新聞 - ドローン落下，6 人軽傷 岐阜・大垣公園
https://www.nikkei.com/article/DGXMZO23115890U7A101C1CN8000/<参照 2020/1/11>
[13] 日本経済新聞 - ドローン墜落で初のけが人 神奈川の建築現場
https://www.nikkei.com/article/DGXLASDG28H2L_Y7A220C1000000/<参照 2020/1/11>
[14] rumble - Rogue drone crashes into public event
https://rumble.com/v30xil-recreational-drone-operator-crashes-in-public-event.html<参照 2020/1/11>
[15] cnet japan - スイス国営郵便の配達ドローン，墜落事故でサービス中断--幼稚園児から 50m の地点に
https://japan.cnet.com/article/35140755/<参照 2020/1/11>
[16] 日本経済新聞 - 関空周辺でドローンか 離着陸，断続的に停止
https://www.nikkei.com/article/DGXMZO51936270X01C19A1000000/<参照 2020/1/11>
[17] Parrot - Parrot AR. Drone 2.0 Elite Edition
https://www.parrot.com/jp/doron/parrot-ardrone-20-elite-edition
<参照 2020/1/11>
[18] slideshare - CODE BLUE 2014 : [ドローンへの攻撃] マルウェア感染とネットワーク経由の攻撃 by ドンチョル・ホン DONGCHEOL HONG
https://www.slideshare.net/codeblue_jp/cb14-dongcheol-hongja
<参照 2020/1/11>
[19] garage4hackers - Maldrone the First Backdoor for drones.]
http://garage4hackers.com/entry.php?b=3105<2020/1/12>
[20] GitHub – markszabo/drone-hacking
https://github.com/markszabo/drone-hacking
<参照 2020/1/12>
[21] samy kamkar – SkyJack:autonomous drone hacking
http://samy.pl/skyjack/
<参照 2020/1/12>
[22] ResearchGate Vishal Dey - GPS Spoofing Google Maps and DJI Phantom 4 Pro
https://www.researchgate.net/profile/Vishal_Dey3/project/Establishing-secure-reliable-communication-between-drones-and-mobile-devices/attachment/59e62673b53d2fe117b6ba77/AS:550476978835456@1508255347382/download/gps_spoofing.pdf?context=ProjectUpdatesLog<参照 2020/1/11>
[23] Vasconcelos, Gabriel & Miani, Rodrigo & Guizilini, Vitor & Souza, Jefferson. (2019). Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. International Journal of Computer Network and Information Security. 11. 212.
[24] 総務省 - IoT 機器のセキュリティ対策に関する技術基準の改正
https://www.soumu.go.jp/main_content/000620788.pdf
<参照 2020/1/17>
[25] engadget 日本版 - ISO，ドローン関連の標準規格草案を発表
https://japanese.engadget.com/2018/11/27/iso/
<参照 2020/1/17>
[26] 無許可ドローンに妨害電波を発信 警察庁，装置導入へ
https://www.asahi.com/articles/ASM4D3D0CM4DUTIL00B.html<参照 2020/1/17>