Technology Reports

認証認可技術　セキュリティ　ドローン

適正なドローン利用を実現するIoT認可技術

サービスイノベーション部　山﨑 公輔（やまさき こうすけ）†　石井 一彦（いしい かずひこ）†

近年，ドローンの利用が拡大しており，国内ではドローンの飛行に関する法整備をはじめとするルールの整備が行われている．しかし，ドローンの企業利用において，社内のドローンを管理する部門とは別のロケーションである現場にてルールどおりの利用を管理する仕組みは，十分に検討されていない．そこでドコモは，IoT認可技術を活用することで，電子的な鍵を用いてルールどおりのドローン利用を支援するシステムを開発した．これにより，ドローンを利用する企業は，現場におけるドローンを電子的な鍵で管理し，その鍵の利用ログから社内のドローン利用状況の把握を行い，不正な利用が防止できるようになった．本稿ではその提案技術を解説する．

1. まえがき

近年，さまざまな機器がインターネットに接続され，IoT（Internet of Things）という言葉が一般化しつつある．総務省の情報通信白書によれば，2022年には世界中で約350億台の機器がインターネットに接続されると予測している［1］．このように増加の一途をたどるIoT機器は，センサ機器から，自動車や小型無人航空機（以下，ドローン）のような移動する機器まで，さまざまな形態が存在する．これらIoT機器の高性能化の先には，各IoT機器が相互に自律協調して動作する世界が実現されると考える．そのような世界で，IoT機器が互いに通信や制御などを実行する際に，その可否を判断する認可の仕組みは，重要な要素の1つといえる．ドコモは前述した世界をコンセプトに検討を進めてきており，今回は，IoTのユースケースとして，市場規模が急速に拡大しているドローンに認可技術を適用した．本稿では企業におけるドローン利用の課題，開発したシステムの特徴について解説する．

† 現在，クロステック開発部

2. 国内におけるドローンの現状とドローンを利用する企業の課題

2.1 国内におけるドローンの飛行ルール

2021年8月現在，国内で機体の総重量が200g以上のドローンを飛行させる場合，国土交通省の定めたルール［2］に基づき飛行することが決められている．また，国土交通省のルールに基づかない飛行の場合は，事前に申請を行い，国土交通大臣の許可もしくは地方航空局長の承認を必要とする．該当する条件を以下に示す．

⑴国土交通大臣の許可が必要となる空域
- ①空港などの周辺の上空の空域
- ②150m以上の高さの空域
- ③人口集中地区の上空

⑵地方航空局長の承認が必要となる飛行の方法
- ①夜間飛行
- ②目視外飛行
- ③人（第三者）または物件（第三者の建物，自動車など）との間が30m未満の飛行
- ④イベント上空飛行
- ⑤危険物輸送
- ⑥物の投下

これらの条件に該当する場合，飛行を実施したい者が，申請を管理するシステム「ドローン情報基盤システム（DIPS：Drone/UAS Information Platform System）［3］」を経由して申請を行い，許可もしくは承認を得る必要がある．申請時には飛行計画情報（日時，場所，経路など），パイロットに関する情報（飛行経歴，ライセンス情報など），飛行させるドローンに関する情報（機体および操縦装置の機能や性能，仕様のわかる設計書など），安全に関する飛行マニュアルを提出しなければならない．また，飛行実施後に飛行日時，パイロット，飛行させたドローン，場所をまとめた飛行実績報告書をDIPS経由で提出することが定められている．

上記に加えて，機体重量に関係なく，国会議事堂，内閣総理大臣官邸，最高裁判所，皇居，対象と指定される在日本（駐日）外国公館や原子力発電所などの国の重要施設周辺での飛行は，対象施設周辺地域を管轄する警察署を経由して都道府県公安委員会に通報する必要がある［4］．

2.2 ドローンを利用する企業の課題

世の中でドローンの利用が増加する一方で，上記ルールを守らない違反飛行が社会問題化している［5］．違反飛行の先には重大な事故の恐れもあり，ドローンを利用する企業においても，ルールに則ったドローンの運用が求められている．申請漏れによる未申請状態での飛行は違法になるため，それがリスクとなり得る．しかしながら，企業のドローンを管理する部門が，実際の現場でドローンを飛行させる際に申請どおりか否かを確認する体制は確立されていない．従って，企業として現場のドローンの適正な運用は課題の1つといえる．

3. システム要件の整理

ドローン使用の一般的な構成と企業内でのドローン運用における役割について解説する．

システム要件は，複数のドローンを利用する企業にヒアリングを実施し，整理を行った．

3.1 ドローン使用の一般的な構成

ドローンは，ホビー向けと，一部のカスタマイズ性が高い産業向けを除けば，**図1**の利用構成が多い（世界シェア上位3社であるDJI，Parrot，3D Robotics［6］の製品を調査）．

パイロットは通常，ドローンを操縦する際に，送信機と呼ばれるコントローラにスマートフォンやタブレットといったモバイル端末を有線ケーブルで接

続して利用する．送信機には操縦スティックが搭載されており，パイロットはそれを用いてドローンの操縦を行う．送信機とドローン間の通信は専用無線を用いる．モバイル端末にはドローン操縦アプリがインストールされており，ドローンの操縦機能だけでなく，ドローンが取得するセンサ情報や動画データを表示する役割ももつ．

3.2 企業内でのドローン運用における役割分担

企業内でのドローン運用における役割分担として，以下3つが存在する（**表1**）．

・ドローン管理部門
・プロジェクトリーダー
・パイロット

ドローン管理部門は，社内のすべてのドローンの機体・利用管理を取りまとめる役割を担う．次にプロジェクトリーダーは，ドローンを用いた作業（例えば，農業・土木・建築・物流・点検・測量など）の責任者であり，作業計画を考え，飛行計画を検討

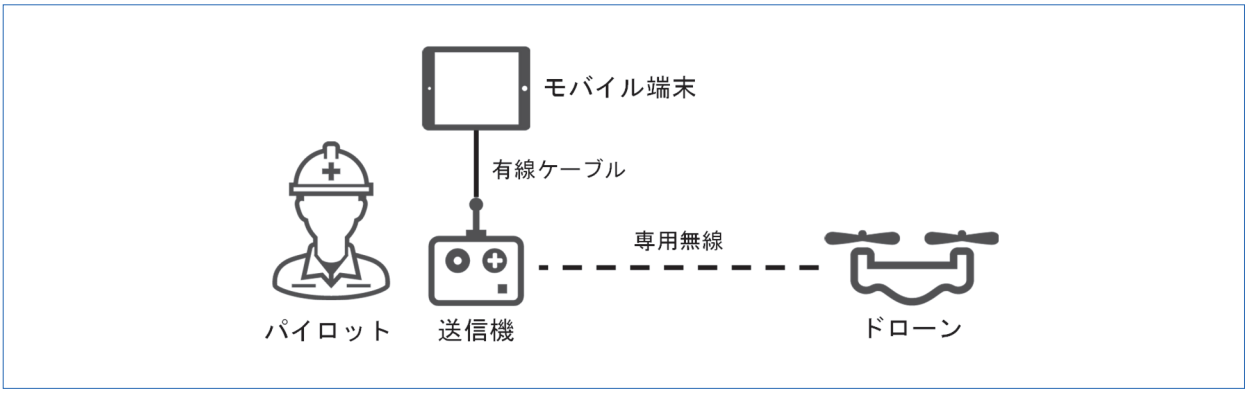

図1　ドローン使用の一般的な構成

表1　ドローン運用における役割分担

担　当	ロケーション	分担内容
ドローン管理部門	本　社	社内におけるドローンの機体，利用管理を取りまとめる．
プロジェクトリーダー	事務所	作業計画を考え，飛行計画を検討し，必要に応じて行政機関への申請を行う．
パイロット	作業現場	作業現場でドローンを操縦して作業を行う．

し，必要な場合は行政機関への申請を行う．最後にパイロットは，プロジェクトリーダーよりアサインを受け，実際の作業現場でドローンを操縦する．なお，ドローン管理部門とプロジェクトリーダー，パイロットはそれぞれ別のロケーションで業務を行っている想定である．

3.3 システム要件

ドローン利用企業のヒアリングを通して，企業が利用する際のシステム要件を整理した．システム要件を**表2**にまとめる．

要件①～④は，前述した行政機関への申請に基づいた飛行に関することである．ただし，要件③では，飛行中に終了予定時刻になり，ドローンを操作不能状態にすることは安全上問題があると判断し，開始時刻のみの確認を行い，終了時刻はログとして記録することとした．要件⑤については，ドローン管理部門が，社内の全フライトに対し，申請どおりに行われているか確認する仕組みを想定している．要件⑥に関しては，ドローンの利用にあたってインターネットに接続できない環境が多々あることが，ヒアリングにより分かった．このため，インターネットに接続できない環境でも，申請どおりの条件のみ飛行可能にするための仕組みを実現する必要がある．最後に要件⑦については，企業がすでに利用しているドローンがカスタマイズ性の高い専用ドローンではなく，汎用的な市販ドローンであるため要件として列挙した．

4. 試作システム概要

本試作システムは，行政機関への申請に基づいた条件を埋め込んだ電子的な鍵を発行し，その鍵を所有するパイロットに対し，条件に一致した場合のみドローンの制御を許可する仕組みである．システム構成を**図2**に示す．

各エンティティ[*1]の機能について以下に解説する．

4.1 各エンティティの機能

今回開発したエンティティは，図2に記載される①IoT認可管理システム，②パイロットアプリ，③利用管理アプリの3つである．それらとは別に飛行計画の作成と行政機関への申請を支援する機能をもつ既存のシステム（以下，ドローンプラットフォーム）があり，今回はドコモのdocomo sky［7］を利用した．ドローン操縦アプリもドローンに付属する

表2　ドローン運用におけるシステム要件

要件①	操縦するパイロットが申請内容と同一のパイロットの場合にのみ，ドローンの利用を許可しなければならない．前述以外のパイロットを許可してはならない．
要件②	飛行するドローンが申請内容と同一のドローンの場合にのみ，ドローンの利用を許可しなければならない．前述以外のドローンを許可してはならない．
要件③	飛行作業を開始する時刻が申請内容の期間内の場合にのみ，ドローンの利用を許可しなければならない．それ以外の作業開始時刻を許可してはならない．また終了時刻を記録し，容易に書替えができないようにしなければならない．
要件④	飛行する場所が申請内容と同一の場所の場合にのみ，ドローンの利用を許可しなければならない．それ以外の場所を許可してはならない．
要件⑤	飛行実施結果を，ドローン管理部門とプロジェクトリーダーが確認できるようにしなければならない．
要件⑥	飛行作業を実施する作業現場において，インターネットに接続できない環境を想定しなければならない．
要件⑦	一般的な構成で利用されるドローンに対応しなければならない．

＊1　エンティティ：論理アーキテクチャにおいて，機能を提供する構成要素．

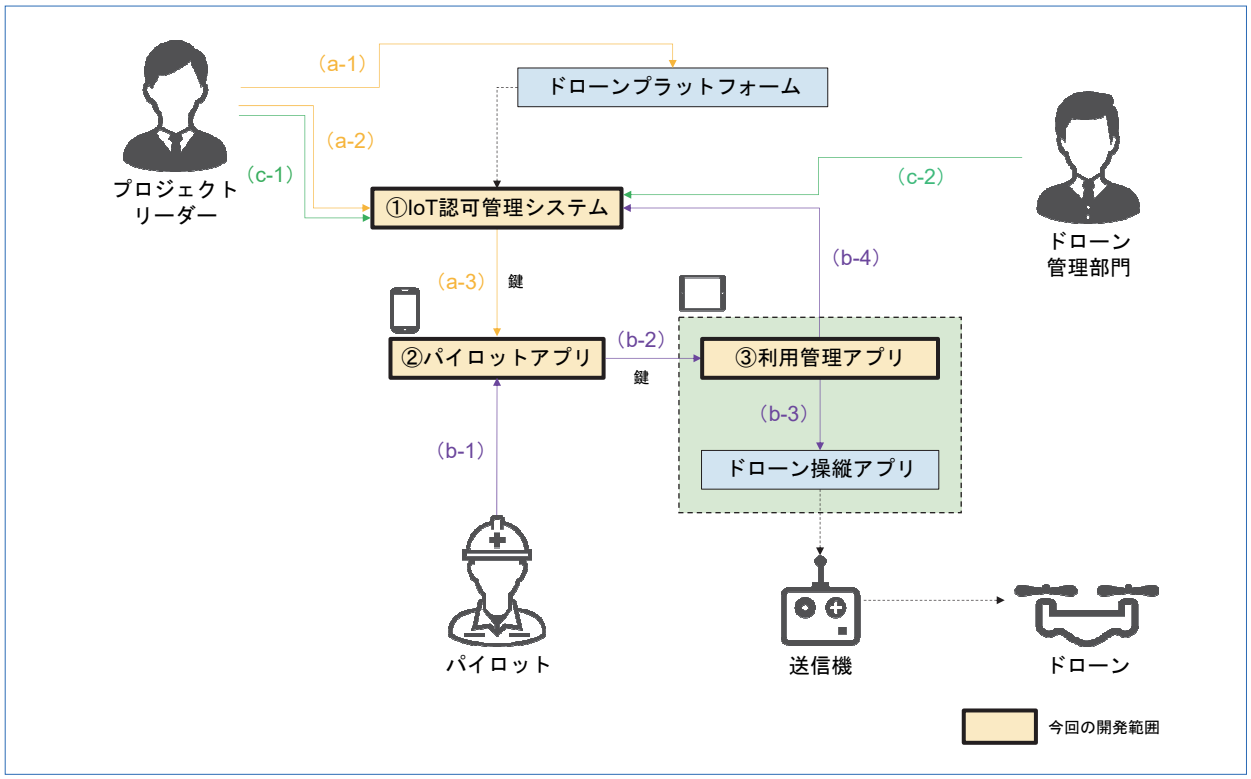

図2　試作システムの構成

既存のアプリケーションであり，今回の試作ではDJI製のDJI GO 4アプリ［8］を利用した．さらにドローンはDJI製のMAVIC2 PRO［9］を利用している．

①IoT認可管理システム

IoT認可管理システムは，サーバアプリケーションである．本システムは，ドローンプラットフォームで作成した飛行計画情報をAPI（Application Programming Interface）*2経由で取得することができる．また，ドローンプラットフォームで作成された飛行計画に基づき，電子的な鍵を発行，変更，追加する機能をもつ．電子的な鍵は，パイロット，ドローン，時間を条件として指定し，改ざん検知のためIoT認可管理システムの電子署名*3が付与されたドキュメントである．この鍵が発行されるとIoT認可管理システムは，指定パイロットのスマートフォン（パイロットアプリ）へ鍵を送信する．また，ドローンの飛行実施後に利用ログを収集し，飛行一覧画面で予定時間を超過した飛行のハイライトを行う機能をもつ．計画外の飛行が検知できるこのような仕組みを運用の中で活用することによって，計画外飛行に対する抑止を図る．さらに利用ログは飛行実績証明書用のデータとして取得することも可能である．

②パイロットアプリ

パイロットアプリは，パイロットが所有するスマートフォンにインストールされるアプリケーションである．今回ドコモはAndroid 8.0対応のものを開発した．パイロットアプリは，IoT認可管理システムから鍵を受信し，送信機に接続されたモバイル端末に鍵を提示する機能

＊2　API：ソフトウェアを互いに接続するのに使用するインタフェースの仕様．
＊3　電子署名：電子的なデータの偽造や改ざんを防止するために用いられる仕組み．

をもつ．今回はスマートフォン，モバイル端末間の通信としてNFC（Near Field Communication）[*4]を使用した．さらにパイロットの本人性の確認には生体認証を用いる．

③利用管理アプリ

利用管理アプリは，送信機に接続されたモバイル端末にインストールされるアプリケーションである．今回ドコモが開発した利用管理アプリは，ドローン操縦アプリと同一モバイル端末内に存在するAndroid 8.0対応のタブレットアプリケーションである．本アプリはパイロットアプリから受信した鍵を検証し，条件の一致確認を行う．鍵の未受信もしくは鍵の検証失敗，条件の不一致の際は，ドローン操縦アプリを起動しても操作できないように制限をかける機能をもつ．さらに，ドローン操縦アプリの利用可能状態において，ドローン操縦アプリの起動時刻と終了時刻の記録をバックグラウンドで行っており，これを利用ログとしてIoT認可管理システムへ送信する．

4.2 利用フローについて

図2に記載されているa-1～3，b-1～4，c-1～2は飛行実施前，ドローン利用時，飛行実施後で分類されている．各分類での利用フローを解説する．

⑴飛行実施前（a-1～3）

・a-1 プロジェクトリーダーは，作業計画を検討し，ドローンプラットフォームで飛行計画を作成する．その後，行政機関へ申請を行い許可もしくは承認を受ける．

・a-2 プロジェクトリーダーは，ブラウザ経由でIoT認可管理システムにログインし，ドローンプラットフォームで作成した飛行計画を選択して鍵を発行する．

・a-3 IoT認可管理システムは，飛行計画に記載されているパイロット，ドローン，時間帯を抽出し，鍵を作成して，対象のパイロットに紐づいたパイロットアプリに鍵を送付する．

⑵ドローン利用時（b-1～4）

・b-1 パイロットは，パイロットアプリを起動し，生体認証を行う．

・b-2 パイロットは，対象の鍵を選択し，利用管理アプリに鍵をNFC経由で送信する．

・b-3 利用管理アプリは，受信した鍵を検証し，条件確認で問題がない場合，ドローンの操縦アプリを利用可能とする．

・b-4 利用管理アプリは，ドローンの操縦アプリの起動時刻と終了時刻を記録し，それを利用ログとしてIoT認可管理システムに送信する．

⑶飛行実施後（c-1～2）

・c-1 プロジェクトリーダーは，飛行実績報告書用データを取得し，報告書を作成する．

・c-2 ドローン管理部門担当者は，社内の飛行一覧画面でフライト状況を確認し，時間超過した飛行を実施したフライトがある場合のみ，注意喚起やヒアリングを行い，再発防止策の検討を行う．

4.3 機器間の認証と鍵の検証

筆者らのIoTの使用における認可のコンセプトは**図3**に記載したとおり，各IoT関連機器に電子証明書[*5]を配備し，機器間で相互認証を行うことであり，そのような環境下で，認可情報のやり取りを行い，きめ細やかな認可を執行する方法の具体化である．今回のドローンサービスへの適用で言えば，各IoT機器がスマートフォン，モバイル端末，ドローンであり，認可情報が条件を埋め込んだ鍵となる．

上記のコンセプトを前提に今回のシステムの実装について解説する（**図4**）．今回のシステムでは，スマートフォンとモバイル端末間は片方向認証としている．スマートフォンはモバイル端末に，鍵とともにスマートフォンの認証情報を送信データとして，

＊4 NFC：近距離無線通信技術であり，FeliCaなどを含む．

＊5 電子証明書：なりすましを防止する仕組みであり，信頼できる認証局から発行される．

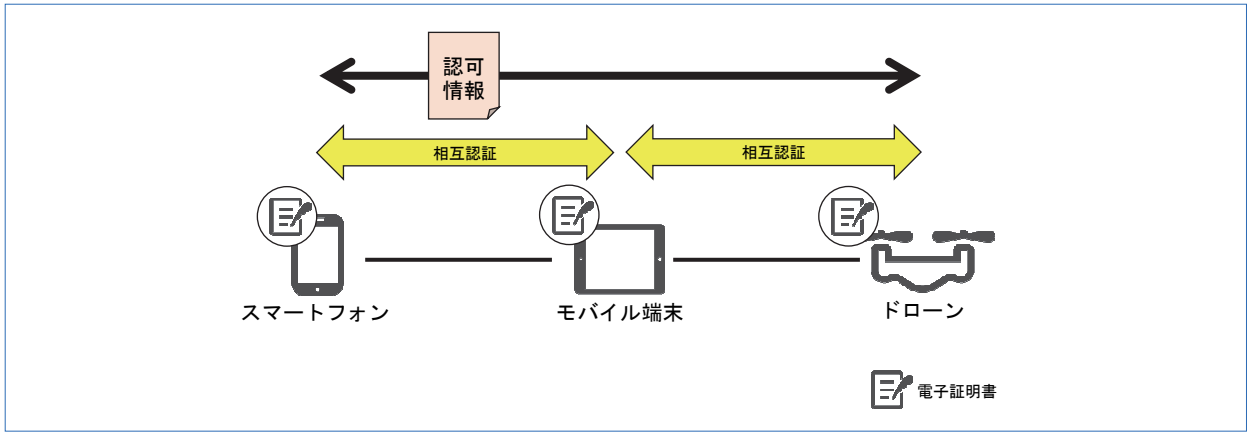

図3　IoTの使用における認可のコンセプト

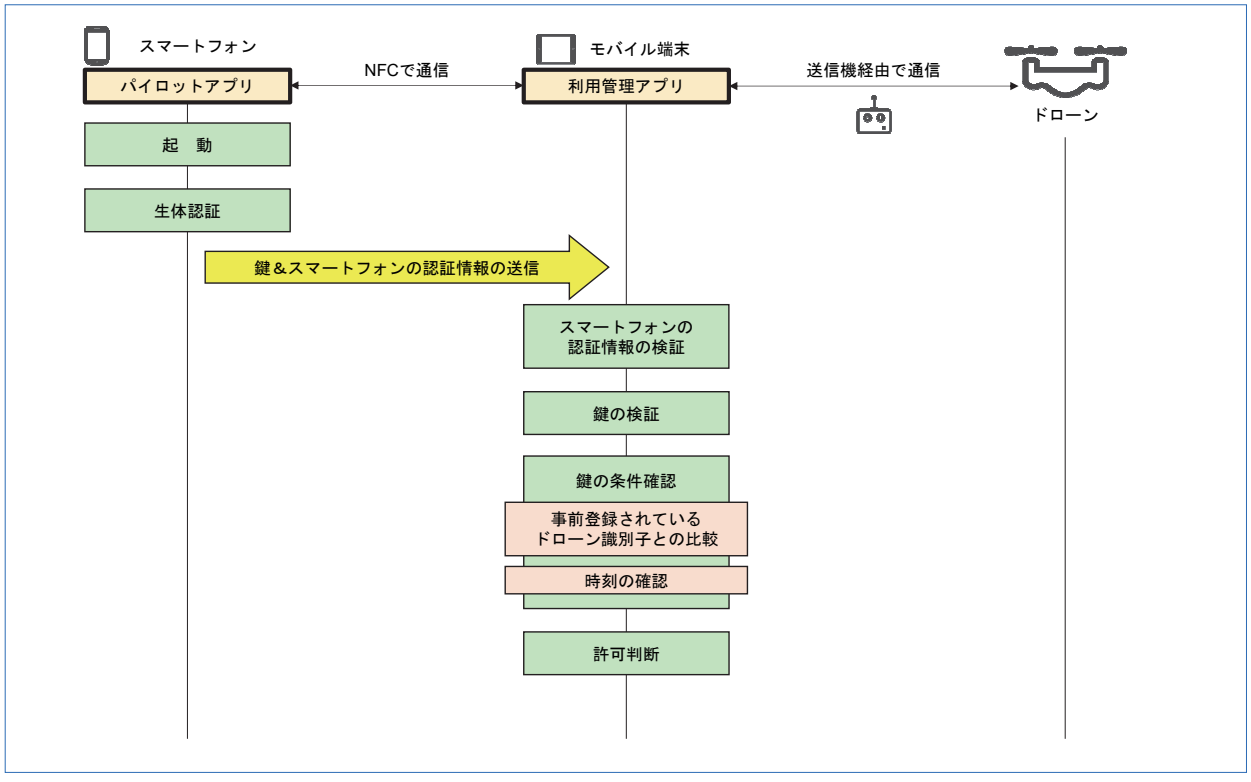

図4　今回の機器間の認証と鍵の検証

データ作成時点から60秒以内に送信する．そして，モバイル端末上の利用管理アプリ内でスマートフォンの認証情報を検証することで片方向認証を実現している．

次に利用管理アプリで実施される鍵の検証では，IoT認可管理システムが鍵を発行する際に付与した電子署名の検証を行っている．鍵の条件確認では，ドローン本体から認証情報を取得するのではなく，

利用管理アプリに事前に登録したドローン識別子を用いて実施する実装とした．そして，モバイル端末のもつ時刻と条件に記載されている時刻の比較を行い，許可の判断をしている．パイロットの確認については，鍵の条件に記載されているパイロットとアクセスしたパイロットが同一であるかが重要である．そのため，IoT認可管理システムは，あらかじめパイロットとスマートフォン，パイロットアプリの紐づけ情報を管理し，鍵の条件に記載されているパイロットのスマートフォンに鍵を送信する．パイロットはパイロットアプリ起動時に生体認証を用いて本人性確認を行い，受信した鍵を利用管理アプリに提示するため，結果，利用管理アプリに鍵を提示できるパイロットは，鍵の条件に記載されているパイロットだけである．そのため，利用管理アプリ内ではパイロットの確認は行っていない．

4.4 本システムにおけるシステム要件の実現方法

前述したシステム要件を本システムでどのように実現したか述べる．要件①～③については，a-3で発行される鍵にそれらを条件として埋め込み，利用管理アプリがb-2で受信した鍵の条件確認結果を基に許可判断をすることで実現した．また要件③では，終了時刻を利用ログとして記録し，この利用ログはパイロットが編集をできないようにパイロットアプリ内で管理し，IoT認可管理システムに送信する仕様とした．要件④については，今回の開発では対応しないこととした．要件⑤では，b-4で取得した利用ログを活用し，ドローンの利用状況を管理画面で確認できるようにすることで実現している．要件⑥については，パイロットが作業現場でインターネットに接続できない環境でも，b-1～3のフローを利用できる仕様とした．要件⑦の実現方法については，バックグラウンドで利用管理アプリがドローン操縦アプリの監視を行い，ドローン操縦アプリの利用制限を行うことで実現している．ドローン操縦アプリに指定はなく，さまざまなドローン操縦アプリに適用可能である．

5. 考　察

今回，開発した本システムを通しての考察を以下にまとめる．

⑴ドローン機体の認証

まず，今回の開発ではドローン機体自身の認証は実現できていない．理由として，現在の汎用ドローンは認証機能をもっていないためである．今回利用したDJI製のMAVIC2 PRO［9］では，DJIが用意しているMobile SDK（Software Development Kit）*6［10］を用いることで，識別子としてシリアルナンバーをドローン本体から取得することは可能である．しかし，ドローン操縦アプリがインストールされている状態では，同じモバイル端末内でMobile SDKを用いたアプリケーションを動作させることができなかった．そのため，今回はモバイル端末内にドローンの識別子をあらかじめ記憶しておく機能を実装した．ドローンとの間で相互認証や認可情報のやり取りは行っておらず，スマートフォンとモバイル端末間のやり取りが行われる．本来であれば，ドローン自体の認証を行い，鍵のもつ条件と比較すべきであると考える．

⑵スマートフォンとモバイル端末間の認証

今回，スマートフォンとモバイル端末間のNFC通信では，モバイル端末がスマートフォンを認証する片方向認証で実装を行った．本来は双方向認証が望ましいが，開発期間の関係によりモバイル端末がスマートフォンを認証する片方向認証しか実装していない．そのため，モバイル端末側が偽のモバイル端末で鍵を盗む攻撃が想定される．それに対する対策として，スマートフォンがNFCで送信するデータ自身に，鍵の条件に記載されている有効期間とは

*6　Mobile SDK：スマートフォンなどのモバイル端末上で動作するアプリケーションを開発するために必要なプログラム．

別の有効期限をもたせることで，NFCでの送信データが漏洩しても認可を執行できない仕様とした．具体的には，送信データを盗んだ者が，これを流用しようとしても利用管理アプリが送信データ自身の有効期間を確認し，認可執行を防ぐ．そのため，送信データ自身の有効期間は，鍵の条件に記載されている期間と比べ短期間としている．

⑶超過利用の防止

今回の試作システムでは，終了時刻を超過する飛行を防ぐことができない．そこで，運用上で超過利用に対する抑止となるよう，予定時間を超過した飛行を飛行一覧画面でハイライトすることでドローン管理部門が把握できるようにした．今回の仕組みによって，実際の運用の中で超過利用に対する抑止となるか，実証実験で検証する必要がある．

⑷内部不正

今回の試作システムでは，全く新規のモバイル端末を用意することで認可を受けずにドローンを飛行させる可能性がある．その場合でも，利用ログの不整合が発生するため，全体の運用の中で不正利用を検知することが可能である．しかし，正規のパイロットがドローン操縦アプリを利用可能状態にして，別の非正規のパイロットに渡し，そのパイロットが操縦することは可能である．このような共謀に対する不正を今回の試作システムでは防ぐことはできない．対策としては，操縦中にモバイル端末のインカメラを利用してパイロットを撮影することで，事後検出ができるようにすることが考えられる．今後，どこまで厳しく制限し，コストをかけるかの精査は，実際のドローン利用企業と実証実験を進めながら検討していくべき項目であると考える．

6. あとがき

本稿では，申請どおりのドローン運用を支援するシステムについて解説した．実際のドローン利用企業へのヒアリングを通してシステム要件を整理し，設計を行った．構築したシステムは，行政機関への申請を基に，電子的な鍵に条件を埋め込み，鍵を所有するパイロットのみがドローンを利用できる仕組みであり，ドローン利用現場での計画どおりの運用を可能とした．さらに試作システムの考察を行い，現状の利用環境でどこまでセキュリティを担保できるか，理想に近づくために不足している機能を整理し明らかにした．今後は次のステップとして，ドローン利用企業と実証実験を行い，有用性の評価および実環境での運用に必要な機能を精査していく．また，ドローンに関するルールは年々更新されており，それらに追随できるシステム設計が必要である．

さらに，今後はIoT認可管理システムをドローン以外のユースケースに適用させていくことで，IoT機器が自律協調する世界で機器同士が確実な認可を執行できる仕組みを実現したいと考える．

文　献

[1] 総務省：“令和2年版　情報通信白書，”（参照 2021年5月19日）．
https://www.soumu.go.jp/johotsusintokei/whitepaper/r02.html

[2] 国土交通省：“無人航空機（ドローン・ラジコン機等）の飛行ルール，”（参照 2021年5月19日）．
https://www.mlit.go.jp/koku/koku_tk10_000003.html#a

[3] 国土交通省：“ドローン情報基盤システム，”（参照 2021年5月19日）．
https://www.dips.mlit.go.jp/portal/

[4] 警察庁：“小型無人機等飛行禁止法関係，”（参照 2021年5月19日）．
https://www.npa.go.jp/bureau/security/kogatamujinki/index.html

[5] 日本経済新聞：“ドローンの違法飛行摘発，19年は過去最多111件，”Mar. 2020.
https://www.nikkei.com/article/DGXMZO57242650W0A320C2MM0000/

[6] 特許庁：“平成30年度　特許出願技術動向調査報告書　ドローン，”Feb. 2019.
https://www.jpo.go.jp/resources/report/gidou-

houkoku/tokkyo/document/index/30_05.pdf
［7］ 株式会社NTTドコモ “ドローンプラットフォーム docomo sky.”
https://www.docomosky.jp/
［8］ DJI：“DJI GO 4.”
https://www.dji.com/jp/downloads/djiapp/dji-go-4
［9］ DJI：“MAVIC 2.”
https://www.dji.com/jp/mavic-2?site=brandsite&from=nav
［10］ DJI：“DJI DEVELOPER.”
https://developer.dji.com/