

IoT Authorization Technology for Appropriate Drone Usage

Service Innovation Department Kohsuke Yamasaki Kazuhiko Ishii

Use of drones has expanded in recent years, and legal regulations for drone flight in Japan are being created. However, in enterprises using drones, there has not been sufficient study of mechanisms for managing drone use according to regulation on worksites, which are generally at a different location than the department managing the drones. As such NTT DOCOMO has developed a system to support drone use according to regulations, using digital keys and IoT authorization technology. With the system, enterprises using drones can manage drones on the worksite using digital keys, drone use in the enterprise can be tracked from the key-use log, and unauthorized use can be prevented. This article describes the proposed technology.

1. Introduction

The term “Internet of Things” (IoT) is coming into general use in recent years, with all kinds of devices being connected to the internet. The Information and Communications White Paper from the Ministry of Internal Affairs and Communications (MIC) estimates that in 2022, approximately

35 billion devices around the world will be connected to the internet [1]. The IoT devices proliferating in this way are taking many forms, from sensor devices to automobiles, small unmanned aircraft (hereinafter refer to as “drones”) and other mobile devices. As these IoT devices increase in performance, we expect that they will begin to operate more autonomously, coordinating with each

©2022 NTT DOCOMO, INC.

Copies of articles may be reproduced only for personal, noncommercial use, provided that the name NTT DOCOMO Technical Journal, the name(s) of the author(s), the title and date of the article appear in the copies.

All company names or names of products, software, and services appearing in this journal are trademarks or registered trademarks of their respective owners.

other. In such a world, with IoT devices communicating and controlling each other, the authorization mechanism, which determines what is allowed, will be an important element. NTT DOCOMO has been studying various concepts for such a world, and as an IoT use case, we have applied authorization technologies to drones, which is a rapidly expanding market. This article describes some issues with enterprise use of drones, along with features of a system that we have developed.

2. Drone-use Conditions in Japan and Issues with Enterprises Using Drones

2.1 Drone Flight Rules within Japan

As of August, 2021, any flights in Japan by drones weighing 200 g or more are required to comply with rules set by the Ministry of Land, Infrastructure, Transport and Tourism (MLIT) [2]. For any flight not complying with these MLIT rules, prior application must be made and approval received from the Minister of Land, Infrastructure, Transport and Tourism, or from the regional civil aviation bureau chief. The relevant conditions are given below.

- 1) **Airspace Requiring Permission from the Minister of Land, Infrastructure, Transport and Tourism**
 - (1) Airspace above and surrounding airports
 - (2) Airspace at or above 150 m
 - (3) Airspace above densely populated areas
- 2) **Flights Requiring Approval from the Regional Civil Aviation Bureau Chief**
 - (1) Night-time flights
 - (2) Flights beyond visual range
 - (3) Flights within 30 m of people (3rd party) or property (3rd-party buildings, vehicles, etc.)

- (4) Flights above events
- (5) Transport of dangerous materials
- (6) Dropping of any object

A person wishing to perform a flight under any of these conditions must apply through the Drone/UAS Information Platform System (DIPS) [3], which manages such applications, and receive permission or approval. For the application, information must be submitted regarding the flight plan (date/time, location, route, etc.), the pilot (flight experience, license, etc.), the drone aircraft (design documentation giving specifications, functionality and performance of aircraft and control equipment, etc.), and a flight-safety manual. After the flight, a flight report must also be submitted through DIPS, summarizing the flight date and time, pilot, drone device, and location.

In addition to the above, regardless of aircraft weight, for flights in the vicinity of important national facilities such as the National Diet Buildings, the Prime Minister's residence, the Supreme Court, the Imperial Palace, designated official foreign residences, and nuclear power generating stations, the prefectural public safety commission must also be notified through the police station in the region where the flight will be conducted [4].

2.2 Issues with Enterprises Using Drones

As the use of drones has increased around the world, flights that violate the rules described above are becoming a problem in society [5]. Flights violating these rules can result in serious accidents, so enterprises using drones are also required to operate drones according to the rules. Conducting a flight without following the application procedure

is also illegal, which is a risk in itself. However, enterprise departments managing drones generally do not have a system able to confirm that this application process has been completed when the drone flight is conducted at the worksite. This is one issue for appropriate on-site operation of drones by enterprises.

3. Summary of System Requirements

We now describe the usual configuration for use of drones and roles for drone operation within enterprises.

To create system requirements, we conducted hearings with several enterprises that use drones and summarized the results.

3.1 General Configuration When Using Drones

Except for hobby devices and some industrial devices that are highly customizable, most drones are used in the configuration shown in **Figure 1** (based on a survey of products from the top three manufacturers with the largest global market share: DJI, Parrot, and 3D Robotics [6]).

Normally, the pilot flies the drone using a transmitter, which is called the controller, connected by a cable to a mobile terminal such as a smartphone or tablet. The transmitter is equipped with a controller stick, which the pilot uses to control the drone. A dedicated radio signal is used for communication between the transmitter and the drone. A drone flight application is installed on the mobile terminal, which provides functions to control the drone, and also to display video and other sensor data obtained by the drone.

3.2 Division of Roles for Drone Operation within Enterprises

Within an enterprise, drone operation is divided into the following three roles (**Table 1**).

- Drone management
- Project leader
- Pilot

The drone management department handles all drone aircraft and manages all drone use within the enterprise. The project leader is responsible for work involving a drone (such as agriculture, public works, construction, logistics, inspections, or

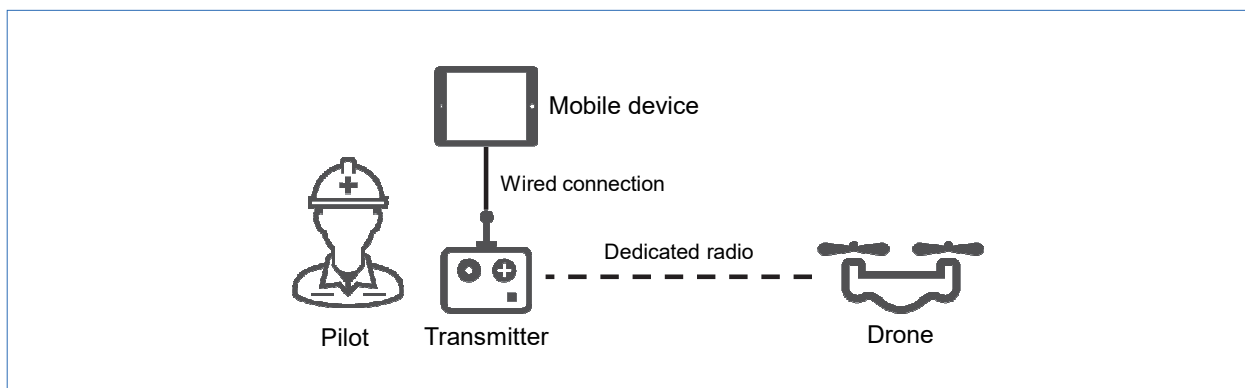


Figure 1 General configuration for drone use

measurement), studying flight plans with consideration of the work plan, and preparing applications to administrative agencies as necessary. Finally, the pilot is assigned by the project leader and performs the actual operation of the drone at the worksite. Note that the work of drone management, project leader and pilot is expected to

be done at different locations.

3.3 System Requirements

We held hearings with enterprises using drones and summarized requirements for a system. These requirements are summarized in **Table 2**.

Requirements (1) to (4) are regarding flights

Table 1 Division of roles for drone operation







Staff	Location	Role
 Drone management department	 Head office	Handles drone hardware and usage within the company
 Project leader	 Office	Studies work plans and flight plans, making applications to administrative agencies as necessary
 Pilot	 Worksite	Operates drones at worksites

Table 2 System requirements for drone operation

Requirement (1)	Use of the drone must only be permitted if the operating pilot is the same as the pilot specified in the request. No other pilot is permitted.
Requirement (2)	Only the drone specified in the request can be used for a flight. No other drone is permitted.
Requirement (3)	Use of the drone is only permitted if the start of flight operation is within the time period specified in the request. Start of operation is not permitted at any other time. The time of completion must also be recorded, in a manner that is not easily overwritten.
Requirement (4)	Drone flight is only permitted at the location specified in the request. Flight at any other location is not permitted.
Requirement (5)	Results of the flight must be provided such that they can be checked by the drone management department and project leader.
Requirement (6)	Worksites where flight work is done must consider that connection to the internet may not be possible.
Requirement (7)	General configurations for drone use must be supported.

based on application to administrative authorities as described above. However, for requirement (3), terminating operation of a drone during flight at the planned end-of-flight time would result in safety issues, so only the flight start time is checked and end-of-flight time is recorded in the log. For requirement (5), we envision a mechanism whereby the drone management department is able to check that all company flights are conducted according to the corresponding application. For requirement (6), we learned from our hearings that in many cases, connection to the internet is not possible in the environments where drones are used. As such, it was necessary to implement a mechanism able to check that flights are conducted according to the application, even when a connection to the

internet is not available. Finally, requirement (7) was included for drones already in use by enterprises, which are general-purpose drones on the market and not highly-customizable, specialized drones.

4. Prototype System Overview

Our prototype system uses a mechanism that issues a digital key with embedded conditions based on the application made to the administrative authority, and this key permits operation of the drone only under conditions consistent with the requirements, by the pilot holding the key. The system architecture is shown in **Figure 2**.

The functions of each entity^{*1} are described

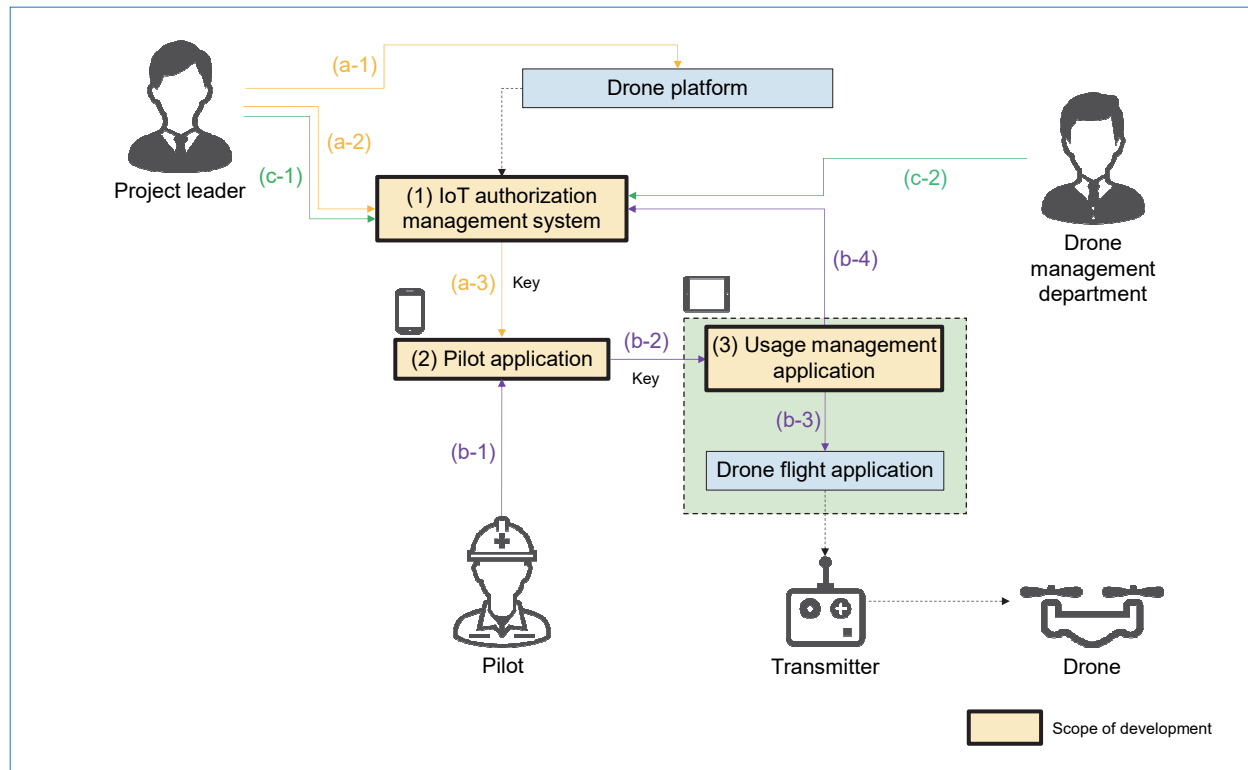


Figure 2 Prototype system configuration

^{*1} Entity: A constituent element providing a function in logical architecture.

below.

4.1 Functions of Each Entity

The entities we developed are described in Fig. 2 as (1) the IoT authorization management system, (2) a pilot application, and (3) a usage management application. In addition to these, an existing system with functions to support making flight plans and submitting applications to the administrative agency (hereinafter referred to as a “drone platform”) is also used, and in this case we used NTT DOCOMO’s docomo sky [7] application. Existing applications associated with the drone are also used for the drone flight application, and we used the DJI GO 4 application [8] from DJI with our prototype. For the drone, we used the MAVIC2Pro [9] from DJI.

(1) IoT authorization management system

The IoT authorization management system is a server application. The system is able to retrieve flight-plan data created with the drone platform through an Application Programming Interface (API)^{*2}. It also has functions to issue, modify and add-to digital keys based on the flight plan created on the drone platform. The digital key is a document that specifies pilot, drone and time conditions and is signed with the digital signature^{*3} of the IoT authorization management system, to detect any falsification. When a key is issued, the IoT authorization management system transmits the key to the pilot application on the smartphone of the specified pilot. There is also a function that collects a usage log after completion of each drone flight and has a flight-list screen that highlights any flights that have exceeded the

planned flight time. The system is designed to prevent unplanned flight activity using a mechanism that detects such activity. The system can also provide signed documents verifying flight logs.

(2) Pilot application

The pilot application is installed in the pilot’s smartphone. The current NTT DOCOMO prototype was developed for Android 8.0. The pilot application receives a key from the IoT authorization management system, and has a function to provide the key to the mobile device connected to the transmitter. We used Near Field Communication (NFC)^{*4} for communication between the smartphone and the mobile device. We also use biometric authentication to verify the identity of the pilot.

(3) Usage management application

The usage management application is installed on the mobile device connected to the transmitter. The current NTT DOCOMO prototype was developed as an Android 8.0 tablet application on the same mobile device as the drone flight application. The application verifies the key received from the pilot application and checks whether the conditions are met. If a key has not been received, if the key verification fails, or if the conditions are not met, operation of the drone will be restricted, even if the drone flight application is launched. When the drone flight application is enabled, the times it is launched and terminated are recorded in the background, and this usage log is sent to the IoT authorization management system.

^{*2} API: An interface specification for different software to mutually connect.

^{*3} Digital signatures: A mechanism used to prevent forgery or falsification of digital data.

^{*4} NFC: A short-range wireless communication technology used by FeliCa and other systems.

4.2 Procedures for Usage

The steps shown in Fig. 2 are categorized into three phases: Pre-flight (a-1 to a-3), In-flight (b-1 to b-4), and Post-flight (c-1 to c-2). The procedures in each of these phases are described below.

1) Pre-flight (a-1 to a-3)

- a-1 The project leader studies the work plan and creates a flight plan using the drone platform. The leader then applies to the administrative agency and receives approval or authorization.
- a-2 The project leader logs in to the IoT authorization management system through a browser, selects the flight plan created on the drone platform, and issues a key.
- a-3 The IoT authorization management system extracts the pilot, drone and flight time from the flight plan, creates a key, and sends the key to the pilot application on the pilot's smartphone.

2) In-flight (b-1 to b-4)

- b-1 The pilot launches the pilot application and performs biometric authentication.
- b-2 The pilot selects the relevant key and sends it by NFC to the usage management application.
- b-3 The usage management application verifies the key it has received, checks the conditions, and if there are no problems, it enables the drone flight application.
- b-4 The usage management application records the times when the drone flight application was launched and terminated, and sends a log containing that information to the IoT authorization management system.

3) Post-flight (c-1 to c-2)

- c-1 The project leader obtains the data for the flight report and creates the flight report.
- c-2 Staff at the drone management department check flight status on the company flight list screen, and if a flight exceeds the permitted flight time, they can issue warnings, conduct a hearing or consider other measures to prevent recurrence.

4.3 Authentication and Key Verification between Devices

The authors' authorization concept for use of IoT is shown in **Figure 3**. A digital certificate^{*5} is assigned to each IoT related device, which devices use to authenticate each other. This creates an environment where permissions information can be exchanged, and a way to enforce detailed permissions requirements. In the current drone-service application, the IoT devices include smartphones, mobile devices and drones, and permissions information refers to the keys, which incorporate the permission conditions.

We now describe the implementation of our system, assuming the concepts just described (**Figure 4**). In our system, the smartphone and mobile device perform one-way authentication. The smartphone sends a key together with smartphone authentication information to the mobile device, within 60 seconds of creating the data. The usage management application on the mobile terminal then verifies the smartphone authentication information to perform the one-way authentication.

The usage management application then verifies the key by verifying the digital signature attached

^{*5} Digital certificate: A mechanism for preventing impersonation, issued by a trusted certificate authority.

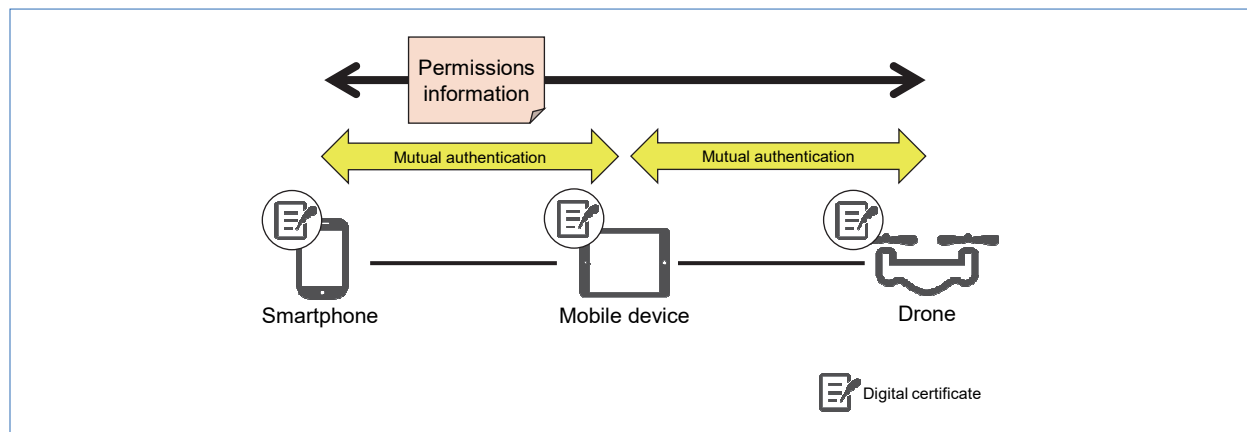


Figure 3 Authorization concept for IoT use

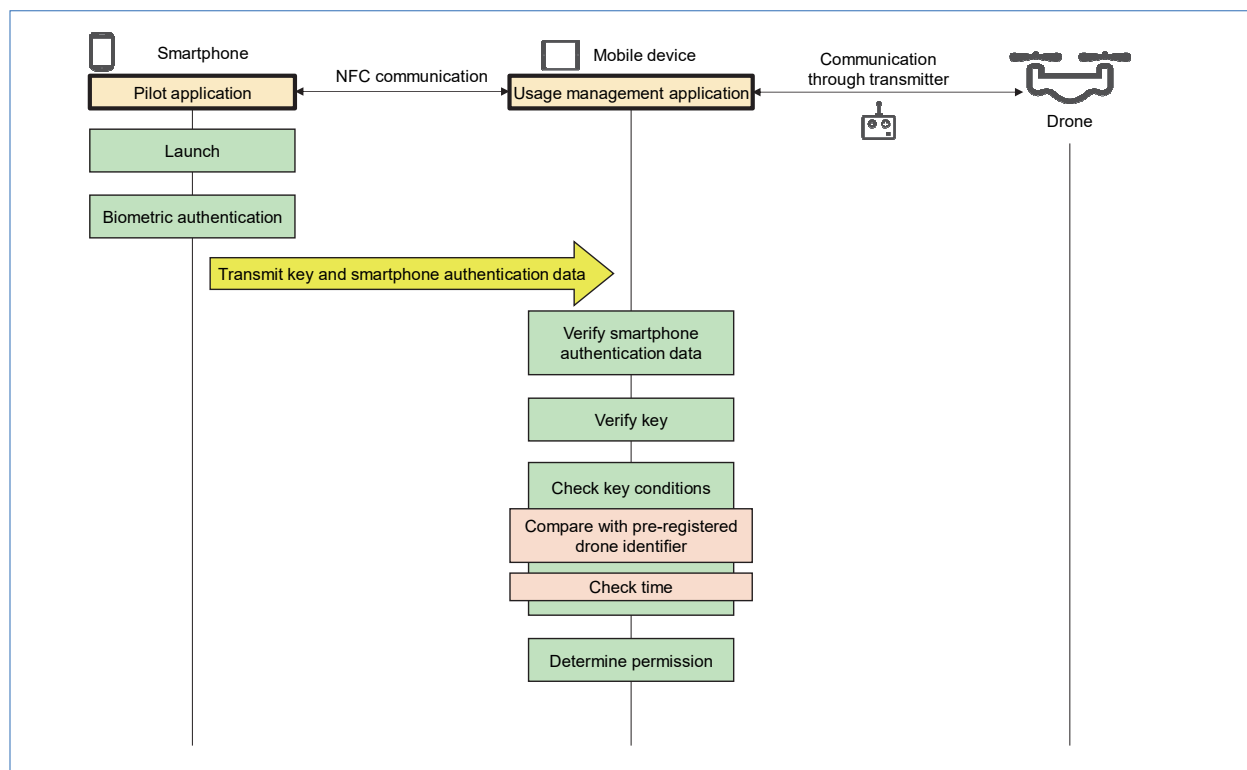


Figure 4 Authentication between devices and key verification

to it when the IoT authorization management system issued the key. To check the conditions in the key, a drone identifier that was previously registered in the usage management application is used,

rather than obtaining authentication information from the drone itself. It also compares the current time in the mobile device with that stipulated in the conditions to decide whether authorization is

granted. It is important to check that the pilot stipulated in the key conditions is the same as the pilot accessing the system. To ensure this, the IoT authorization management system manages pre-registered information associating the pilot, smartphone and pilot application, and sends the key to the smartphone of the pilot stipulated in the key conditions. When pilots launch the pilot application, their identity is verified biometrically before presenting the received key to the usage management application, so as a result, only the pilot stipulated in the key conditions can use the key in the usage management application. For this reason, there is no need to check the pilot identity within the usage management application.

4.4 Implementation of System Requirements in the System

We now describe how the above system requirements are implemented in the system. Requirements (1) to (3) are embedded in the key issued in a-3, and the usage management application checks the conditions in the key it receives in b-2, giving authorization based on the result, which enforces these requirements. For requirement (3), the flight-end time is recorded in the usage log, which the pilot cannot edit. The pilot application maintains this log and sends it to the IoT authorization management system. Requirement (4) was not implemented in the current prototype. Requirement (5) is implemented with the usage log obtained in b-4, and by showing the drone usage state on a management screen, where it can be checked. Requirement (6) is implemented by enabling the pilot to complete operation steps b-1 to b-3 at worksites, even when an internet connection is

not available. To implement requirement (7), the usage management application monitors the drone flight application in the background, and is able to limit use of this application. The drone flight application is not fixed, and the system can be used with various drone flight applications.

5. Discussion

We discuss several issues arising in development of the system below.

1) Drone Aircraft Authentication

With the current prototype, it is not possible to authenticate the drone aircraft itself. This is because current general-purpose drones do not have an authentication function. The MAVIC2 PRO [9] from DJI, which we used, has a Mobile Software Development Kit (SDK)^{*6} [10] that enables a serial number to be retrieved from the drone as an identifier. However, we were unable to run an application using the Mobile SDK on the mobile device where the drone flight application was installed. Thus, for the prototype, we implemented a function to record the drone identifier on the mobile device beforehand. Authentication and exchange of permissions information is done between the smartphone and the mobile device and is not done with the drone. Ultimately, it would be better to authenticate the drone itself, and compare against the conditions in the key.

2) Authentication between Smartphone and Mobile Device

For our prototype, we implemented one-way authentication from the mobile device to the smartphone using NFC communication. Two-way authentication would be preferable, but due to development-time

^{*6} Mobile SDK: Software required for developing applications on mobile devices such as smartphones.

constraints, only one-way authentication was implemented in our prototype. This leaves open the possibility of attack, stealing a key by impersonating the mobile device. To prevent this, we added a time limit on the data sent by NFC from the smartphone, separate from the time limit of the conditions described in the key, so that the authorization cannot be enacted if the data sent by NFC is leaked. More specifically, if a person obtaining the leaked data attempts to use it, the usage management application will verify the time limit on the transmitted data and prevent authorization. To achieve this, the time limit on the transmitted data is shorter than the limit stipulated in the key conditions.

3) Preventing Over-use

The prototype system is not able to prevent flights from exceeding the authorized time. As such, to discourage operation beyond the authorized time, we highlight flights that exceed the planned time on the flight-list screen, so that the drone management department will be alerted. It will still be necessary to verify whether this mechanism works to reduce use outside of the authorized time in actual operation.

4) Internal Unauthorized Use

With the prototype system, it is still possible to use a completely new mobile device to fly a drone without receiving authorization, but even in such a case, an inconsistency would be created in the usage logs, making it possible to detect the unauthorized use. However, if a legitimate pilot enables the drone flight application and then gives it to another unauthorized pilot, that pilot will be able to operate the drone. The current prototype system is not able to prevent such unauthorized use.

One possible way to counter this would be to use the user-facing camera on the mobile device to photograph the pilot during operation, so the pilot could be verified afterward. In the future we will investigate how strictly to enforce restrictions in relation to cost, among other issues, as we continue to conduct tests with enterprises that are actually using drones.

6. Conclusion

This article describes a system created to support operation of drones according to authorized flight conditions. The system was designed based on requirements compiled from hearings held with enterprises that are actually using drones. The system embeds conditions in a digital key, based on an application made to the applicable administrative agency. It then only permits a pilot with the key to use the drone, at the worksite and according to the approved flight plan. We studied the prototype system further, clarifying how well we can maintain security in current usage environments, and what further functionality is needed to create a more ideal system. As a next step in the future, we will conduct further tests with enterprises using drones, evaluate the utility of the system, and examine what functionality is needed in real environments. The rules regarding drones are also being updated each year, so the system design will need to enable the new rules to be followed.

In the future, we also want to apply the IoT authorization management system to use cases other than drones, to implement a mechanism by which IoT devices can collaborate autonomously,

while reliably enforcing authorization with each other.

REFERENCES

- [1] Ministry of Internal Affairs and Communications: "2020 Information and Communications White Paper," (Accessed May 19, 2021) (In Japanese).
<https://www.soumu.go.jp/johotsusintokei/whitepaper/r02.html>
- [2] Ministry of Land, Infrastructure, Transport and Tourism: "Flight rules for unmanned aircraft (drones, radio-controlled, etc.)," (Accessed May 19, 2021) (In Japanese).
https://www.mlit.go.jp/koku/koku_tk10_000003.html#a
- [3] Ministry of Land, Infrastructure, Transport and Tourism: "Drone information platform system," (Accessed May 19, 2021) (In Japanese).
<https://www.dips.mlit.go.jp/portal/>
- [4] National Police Agency: "Regarding prohibition of small unmanned aircraft flights," (Accessed May 19, 2021) (In Japanese).
<https://www.npa.go.jp/bureau/security/kogatamujinki/index.html>
- [5] Nippon Keizai Shinbun: "Exposing illegal drone flights: A record 111 in 2019," Mar. 2020 (In Japanese).
<https://www.nikkei.com/article/DGXMZO57242650W0A320C2MM0000/>
- [6] Japan Patent Office: "FY2018 Survey Report on Technology Trends in Patent Applications: Drones," Feb. 2019 (In Japanese).
https://www.jpo.go.jp/resources/report/gidouuhoukoku/tokkyo/document/index/30_05.pdf
- [7] NTT DOCOMO Co. Ltd.: "The docomo sky Drone Platform," (In Japanese).
<https://www.docomosky.jp/>
- [8] DJI: "DJI GO 4," (In Japanese).
<https://www.dji.com/jp/downloads/djiapp/dji-go-4>
- [9] DJI: "MAVIC 2," (In Japanese).
<https://www.dji.com/jp/mavic-2?site=brandsite&from=nav>
- [10] DJI: "DJI DEVELOPER," (In Japanese).
<https://developer.dji.com/>