SONY

Airpeak Security

White Paper

June 2022 (Ver.1.0)

Issue Date

June 21, 2022 (Ver.1.0)

Scope Covered in This White Paper

This white paper covers main unit hardware for Sony's professional drone Airpeak, the cloud services and communication environments supporting Airpeak, software such as applications operating on smart devices provided by Sony, and infrastructure security systems.

Listed Content

The content contained in this white paper is intended for use in the United States. We do not guarantee the completeness of the product and service specifications described in this white paper. Product and service specifications are subject to change without notice. The Sony Group and its affiliated companies are not obligated to provide compensation in the event of any damage caused by the use of products or services based on the content contained in this white paper.

Publisher

If you have any inquiries, suggestions, etc., regarding the contents contained in this white paper, please contact us at the following information.

Sony Group Corporation
1-7-1 Konan, Minato-ku, Tokyo 108-0075 Japan
https://www.sony.com/electronics/support

Trademarks

Prohibition of Reproduction, Modification, or Redistribution

Table of Contents

1. Security Lifecycle 4

2. Provisioning 6

Overview of Security Server 6

Secure Flash 7

3. Development 9

Secure Boot 9

System Security 11

Application Security 13

4. Operation 18

Network Security 18

5. Maintenance 19

6. Disposal, Retirement, and Transfer 20

1. Security Lifecycle

Importance of ensuring integrated security

Generally speaking, operational (in-flight) security tends to be an important focus for drones (unmanned aerial vehicles). For example, is the content transmitted during operation being eavesdropped? Could control of the aircraft be hijacked? However, in order to ensure operational security, it is not enough to simply encrypt the wireless communication channel. It is also important to prevent malicious software from being installed on the aircraft and to prevent the communication content from being decrypted by a third party. Therefore, it is essential to prevent malicious individuals from extracting, decrypting, rewriting, or tampering with internal software. It is also essential to prevent access to the inside of hardware, which would constitute a breach of security. Consequently, in addition to encryption, there must also be mechanisms which only allow writing with guaranteed integrity for the keys and programs used as the basis of encryption. Safe storage and execution in safe environments is also required for those items.

If malicious individuals are unable to hijack communications, they will attempt to directly read, decrypt, or rewrite the internal software. If unable to do so, they will attempt a lower level of cracking closer to the hardware; for example, physically accessing the flash memory in which programs are stored. Therefore, in order to achieve products with complete security, it is extremely important to eliminate all opportunities for third parties to access internal software or data. Security measures must span from the silicon level of semiconductors used in hardware to all processes related to the product, including manufacturing, maintenance, and customer service.

Accumulation of security technology over many years

The Sony Group has long been involved in network-connected products such as "Xperia" smartphones which are always connected to the Internet and a huge number of smartphones exist on the market, so they are ideal targets for malicious actors. In the past, there were problems with cloned smartphones in the early 2010s. As far back as the 1980s, there were problems with car phones using disguised telephone numbers. Over a long period of time, Sony has cultivated advanced security technology by working on such products which were among the first to be targeted for security vulnerabilities. We now utilize and have enhanced this cumulative technology in Airpeak.

Figure 1 shows the security life cycle of Airpeak. We ensure complete security from the stage of selecting the SoC (system-on-chip = semiconductor that integrates the CPU and peripheral circuits) that controls the aircraft to the disposal or discontinuation of the product. In the following sections, we will explain the specific mechanism for ensuring security at each of these stages.

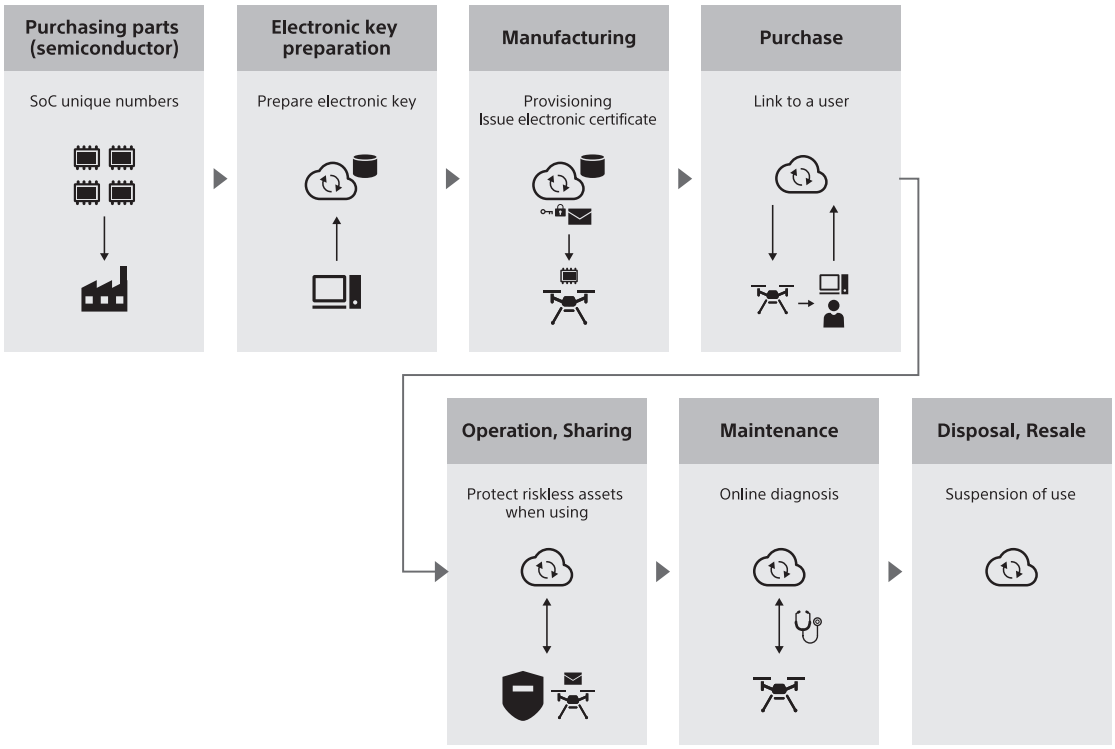

Figure 1

2. Provisioning

Overview of Security Server

Security server

A security server is a server for signing software written to a product, generating and managing keys used for encryption, and managing access to the product.

Electronic key

The security server manages the electronic signatures, electronic certificates, and electronic keys required to prove the authenticity of the software.

All employees involved in development can voluntarily issue electronic signatures, electronic certificates, and electronic keys for development at any time. On the other hand, authentication is required for the issuance operation of electronic signatures, electronic certificates, and electronic keys that can be used in actual products on the market. Only a very small number of authorized employees are capable of and authorized for issuance operation.

Secure Flash

Security on manufacturing lines

The firmware written to the product at the time of manufacturing is signed electronically. Even if the manufacturing equipment is infected with a virus and the Airpeak firmware is modified as a result, writing of that firmware to Airpeak is prevented by Airpeak's electronic signature verification using the secure area TrustZone in the SoC (described later in this document).

Communication between the security server and Airpeak is encrypted. It is not possible to check the electronic key ring or electronic certificates used by Airpeak for the encryption/decryption processing of various software and communications on the manufacturing line. The electronic certificates and electronic keys written to the product are linked to different unique keys for each product, and verification is performed in the same way using TrustZone. Therefore, even if reading is performed through a physical method (for example, removing the flash memory soldered to the printed circuit board), the raw binary data of the software cannot be diverted to another unauthorized device (creating a clone device, etc.).

Some SoCs that use ARM architecture can use an eFuse* to control security functions. The SoC used in Airpeak also supports security function control using an eFuse. Airpeak uses electronic signatures in a method similar to firmware in order to prevent the creation of unauthorized SoC settings. There is a security risk regarding the interface (debug interface) for connecting the SoC to an external computer for development, and performing internal rewriting and information retrieval during debugging at the development stage. Therefore, an eFuse is set to eliminate this risk in products which are actually distributed on the market.

Airpeak has multiple processors (including a vision processor) in addition to the main SoC. For these peripheral processors, the main SoC becomes the parent, verifies the passed image, and then conducts distribution to the peripheral processors. These processors also use their own security features to verify the received image and then write to their own flash memory. Figure 2 summarizes the overall flow.

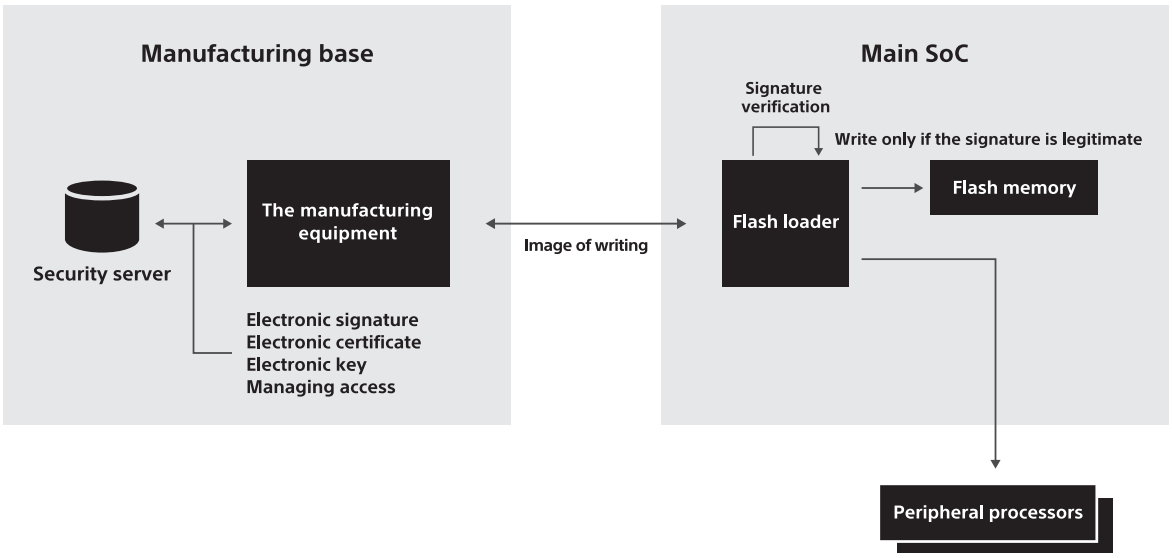

Figure 2

**eFuse: A collection of fine fuses that are prepared on the SoC and can be electrically operated. A "fuse" means wiring that cannot be restored once it is blown. Similarly, once an eFuse is blown (cut), it is physically impossible to restore the eFuse. Practically, an eFuse is treated like "memory that can only be written once and never disappears" (one-time ROM). In actuality, similar to a fuse, a bit that has not been blown can be blown again, so a bit is prepared to instruct the prohibition of blowing again. When this "instructor bit" is blown, it becomes impossible to make any modifications. Since the prohibition of subsequent blowing is implemented as a hardware function of the semiconductor, the chip written with prohibition of subsequent blowing by the eFuse cannot be modified, even by the semiconductor manufacturer itself. Setting information for the various peripheral functions of the SoC is written in this eFuse. Individual information related to security is also written to the eFuse.*

3. Development

Secure Boot

Figure 3 shows a conceptual diagram of a “secure boot” in which specific steps are used to boot the system while ensuring that the software has not been modified.

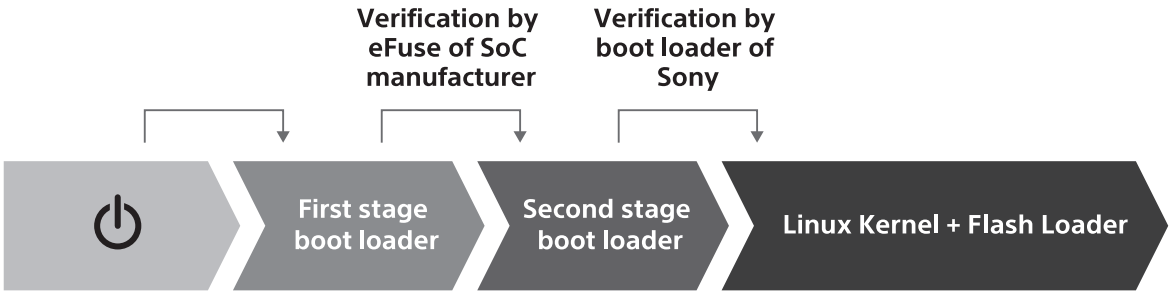

Figure 3

First stage boot loader

The main SoC installed in Airpeak goes through a multi-step booting (software startup) process. First, when the power of the SoC is turned on, the first stage boot loader (first stage startup program) starts. This program is written in the SoC from the time the semiconductor is shipped. It is a fixed program (mask ROM) formed from the semiconductor manufacturing stage (exposure, etching, etc.) as a physical wiring pattern of the silicon inner layer. Therefore, after semiconductor manufacturing, the program cannot be modified by the chip vendor (SoC manufacturer).

This first stage boot loader is an extremely small program that performs initialization for accessing flash memory and RAM. Also, if the second stage boot loader which should be started next is not written in the flash memory, the first stage boot loader performs the minimum processing required to write the second stage boot loader to flash memory from an external source.

The first stage boot loader verifies the signature of the second stage boot loader based on the Root of Trust in the eFuse when secure boot is enabled. The signature must match in order for the second stage boot loader to start.

For example, there are cases in which SoC writing tools (software) provided by chip vendors are leaked to the internet. Even if a malicious individual uses a leaked tool to write an unauthorized second-stage boot loader, there is a verification process for the second-stage boot loader that will prevent actual booting.

Second stage boot loader

After processing by the first stage boot loader is finished, the second stage boot loader is started. The second stage boot loader was developed by Sony and contains the minimum program to pass startup to the OS written in flash memory; for example, initialization of the main memory (RAM). After processing by the second stage boot loader is finished, the electronic signature of the OS (Linux kernel) is verified, and the Linux kernel is started only when the signatures match.

Double check when writing and starting software

There are two types of electronic signatures in software handled by Airpeak. These two signatures can be broadly divided into 1) signatures that are verified at the time of writing and 2) signatures that are verified at the time of startup. The signature used at the time of writing is for verifying the authenticity of the flash image and the eFuse layout sent to Airpeak, and the signature itself is not written to the flash memory or eFuse. On the other hand, the signature used at the time of startup is for verifying the authenticity of the software written in the flash memory, and is verified each time the software is loaded and started. In other words, Airpeak uses different digital signatures when writing and reading software to double check the authenticity of software.

The electronic signature used here cannot be freely generated even by employees involved in the development of Airpeak. In other words, even employees involved in the development of Airpeak

cannot freely create firmware that can be written and executed on products distributed in the market. This means that the products are safe.

System Security

Authenticity verification for Linux systems

After starting the Linux kernel, additional measures are also required to ensure a robust system. Since the adoption of Linux for embedded devices in the late 1990s, the system area of the file system has been made read-only in order to mitigate attacks during startup. However, these measures are powerless against an attack method which uses software vulnerabilities to rewrite the system area.

Airpeak adopts the function “dm-verity,” which detects modification of the block device (file system area on the memory) of the Linux OS. dm-verity is also able to detect modification of the system area itself. By integrating dm-verity with the secure boot discussed above, the OS itself can be executed securely. Even if vulnerabilities exist in the Linux OS, rewriting of the system area is detected immediately and execution is stopped.

On the other hand, if all areas are made read-only, it will not be possible to write or save any of the data that is necessary for product operation. Therefore, Airpeak has reserved some areas where data can be written. For these areas, the “not executable” (noexec) attribute is added together with the read/write attribute. Therefore, even if an executable file is written in these areas, it cannot be started from these areas. Since these attribute settings are managed by a program that is protected by secure boot and dm-verity, Airpeak is able to prevent rewriting by a malicious attacker.

dm-verity

In dm-verity, hashes of the memory space expanded by the file system are taken in blocks of 4kB (4,096 bytes), and a hash tree is generated in the form of hashes expanding further from those multiple hashes. All of these hashes are saved in separate areas which can only be accessed from the kernel. Furthermore, a signature is used for the root hash (the top-level hash of the hash tree). This signature is performed on the security server.

Even if the file in the target partition were to be rewritten without updating the hash, the operation would stop when dm-verity detects tampering. Even if the hash could be rewritten with a higher degree of sophistication, performing another signature would require generation by a security server. In this case as well, dm-verity would detect a signature mismatch and prohibit operation.

Security of executable files

For executable files, Airpeak enables basic security supported by compilers, linkers, Linux OS, and ARM architecture processors. Examples include ASLR (Address Space Layout Randomization), which makes it difficult to guess the address where a specific area is located by randomly positioning offsets from the base for areas such as the library heap stack, PIE (Position-Independent Executable), which randomizes the positioning of the text area, SSP (Stack Smashing Protection) which detects attacks such as stack buffer overflow attacks by positioning a variable known as a “canary” (in reference to the bird used by miners to detect trace amounts of toxic gases) at the address between the base pointer and the local variable in the stack frame, and XN bits (eXecute Never bits), which similarly prevent the execution of unauthorized code through attacks such as buffer overrun attacks by marking memory areas other than the executable file as non-executable areas.

Additionally, the executable file itself will not start if it has been modified because it is only started after verification by signature.

Application Security

TrustZone

Airpeak uses various technologies to support high security, from authentication and signatures to encryption and decryption processing. The processing of those technologies themselves must be safely executed. Airpeak uses SoCs equipped with TrustZone, which is a secure software execution environment that is prepared in hardware as a part of the ARM processor architecture. TrustZone allows the positioning and execution of software in areas that are not accessible to regular software. Airpeak executes processing related to electronic keys and electronic certificates in TrustZone.

FOTA

FOTA (Firmware Over The Air) is a software update function via the internet that is commonly used in many situations on a daily basis. For example, FOTA is used for updating smartphone operating systems. When updating Airpeak, the firmware image positioned in the cloud for rewriting is encrypted and signed to ensure confidentiality and integrity. Figure 4 below shows an overview of this process.

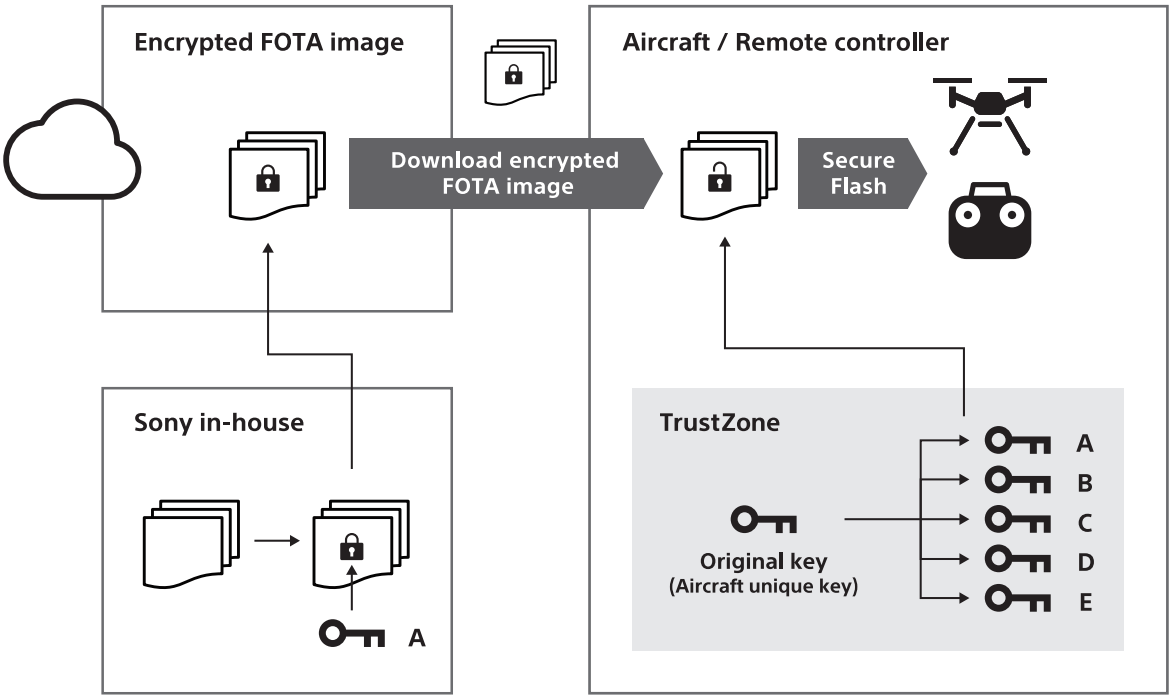

Figure 4

Airpeak writes an electronic key ring in the production line of the manufacturing base in order to realize application security. This electronic key ring is protected by TrustZone. The encryption technology used here corresponds to the FIPS 140-2 Level 3 standard* and functions as the Root of Trust for Airpeak's application security.

The firmware image for FOTA is encrypted using the keys prepared in the key ring written on this production line. Airpeak decrypts the updated image by using a protected key in TrustZone. After verifying the electronic signature, writing is performed to the flash memory.

**FIPS 140-2 Level 3: FIPS 140 is a federal standard of the United States that defines security requirements for cryptographic modules. FIPS 140-2 Level 3 is the second level from the top of the four levels defined for security requirements. Specific requirements of FIPS 140-2 Level 3 include the following: "Hardware must be resistant to physical tampering. Hardware must retain traces of physical tampering. There must be a physical or logical separation between the interfaces through which critical security parameters (CSPs; keys or value used to generate keys) enter/leave the cryptographic module and other interfaces. Operators must be authenticated. The authority of operators must be authenticated."*

Remote ID

When flying a drone (unmanned aerial vehicle) , it is required to install a “remote ID” that sends information such as the registration code of the drone via radio waves.

For Airpeak, by registering the aircraft on the Federal Aviation Administration (FAA) website, the registration code, etc., issued by the FAA via the mobile app “Airpeak Flight” will be written to Airpeak. At this time, TrustZone is used to securely store the serial number, registration code, and key for generating authentication information of the aircraft.

Additionally, it is possible to verify remote ID information that is repeatedly transmitted at a frequency of one time or more per second by transmitting that information using a remote ID capture (reception) device owned and operated by important facility managers such as the FAA and airport management companies, and using the registration system of the FAA. The Airpeak signature attached at the time of remote ID notification is generated using TrustZone and is therefore highly reliable.

This function was added after the product was released, but it is already available for use by updating with FOTA via the mobile application Airpeak Flight.

Communication security between aircraft and remote controller

The Airpeak remote controller and the Airpeak aircraft use extended Wi-Fi. Security at this layer employs industry standard WPA2-PSK (AES) encryption and authentication. A PSK (pre-shared key) is randomly generated each time the aircraft is initialized. Also, at the time of manufacturing, a unique key is generated for each aircraft, and the unique key is written to the aircraft before shipping. For this reason, no (connectable and controllable) remote controller is linked to the aircraft when the product is shipped. Instead, linking of the aircraft and the remote controller must first be performed by the user. The linking procedures are performed on a special band that is not supported by general Wi-Fi for devices such as computers and smartphones, so it is extremely difficult to attempt eavesdropping. Furthermore, in order to ensure that only one legitimate remote controller can be connected to the aircraft, Airpeak also uses the keys written to the aircraft and remote controller on the production line to perform mutual authentication in accordance with the RFC 4279 standard.

The aircraft and remote controller use the key written on the production line to generate their own respective session keys. They then use the session keys to perform mutual authentication, encryption of communication data, and integrity verification (secure channel communication). Additionally, the aircraft is equipped with a firewall, and access to the main unit is permitted only after the aforementioned mutual authentication. Even if the Wi-Fi pre-shared key is leaked, the communication security between the main unit and the remote controller is guaranteed by said mutual authentication. This prevents hijacking.

Cloud service

Airpeak provides an application environment for managing Airpeak on the cloud. There are two ways to access the environment. The first is to use the web application Airpeak Base, and the second is to access via the mobile application Airpeak Flight. In either case, the communication path is encrypted by https communication.

The cloud is constantly exposed to attacks such as DDoS, SQL injection, and cross-site scripting. A web application firewall is established in front of the application server and denies unauthorized access based on a predefined rule list. However, since the firewall alone is not enough to prevent DDoS attacks, the operation administrator constantly monitors the server for attacks. When an attack is detected, the administrator responds by immediately adding a new rule to the list based on the access source IP address, etc.

4. Operation

Network Security

Aircraft registration

When purchasing a new Airpeak or acquiring an Airpeak via transfer, etc., the user must first register for the aircraft cloud service. Through secure registration using an electronic certificate and TrustZone, the cloud service rejects registration requests from sources other than the legitimate Airpeak, and the Airpeak side discards any information generated by a non-legitimate cloud service. Therefore, no links are established with unauthorized devices or cloud services.\

User authentication

When actually flying the drone, the user must log in to the cloud service from the mobile application Airpeak Flight. Once the user is logged in, auxiliary data related to flight will be delivered from the cloud service side, and it will be possible to safely fly Airpeak. It is also possible to fly without logging in; however, for safety reasons, restrictions are placed on the flying distance and altitude.

The data exchanged when logged in includes anonymized user identifiers. These user identifiers are used to store the flight log associated with the user in the cloud service. Even if the Airpeak aircraft is lost during flight, the information stored in Airpeak alone is not enough to determine who had been flying Airpeak. This mechanism ensures privacy.

5. Maintenance

Online diagnosis and customer support

Airpeak's aircraft information (flight log) is securely stored in the cloud via https communication, and is securely managed using the operations described in the "Cloud service" section. Customer support is linked with the cloud service. Airpeak's condition can be diagnosed online and remotely by using the log stored in the cloud and the aircraft log information that the user uploads separately. This enables Sony to provide optimal support according to what has occurred.

Repair

Even during repairs, Sony's team performs work while strictly managing data related to user privacy. When a software update is required, writing of unauthorized software during repair services is prevented through a mechanism which only writes official firmware from Sony. This uses the same system as production lines at manufacturing bases.

6. Disposal, Retirement, and Transfer

Cloud service linkage

The cloud service is equipped with a function to delete user information and clear the link with the aircraft when the product is disposed of, retired from use, or transferred. Deletion and clearing can be done from the web app Airpeak Base.

On the other hand, hardware-related information (cumulative flight time, cumulative number of flights, etc.) will continue to be retained on the cloud service. If the product is transferred, etc., this information will be passed on to the next user. In regard to information such as the flight time and number of flights, the cumulative information for the aircraft and the cumulative information for the user are managed separately.

(This page intentionally left blank for editing purposes.)

SONY