Manual for Handling Digital Assets Left by the Deceased

— *Digital End-of-life Planning to Eliminate Problems When the Time Comes* —

ISEDA Atsushi
Japan Digital Shuukatsu (End-of-Life Planning) Association Representative

1. Introduction

In Japan, a declining birthrate and aging population is intensifying at a speed unprecedented in the world. The country is already a super-aged society (a society in which the ratio of elderly persons aged 65 years or older is greater than 21%) with its ratio of elderly persons to the total population reaching 28.1% in 2018.

Against this background of a super-aged society, the expression "end-of-life planning" has come into popular use to describe the making of advanced preparations or the putting of one's affairs in order mostly by elderly people before one's life comes to an end. Indeed, end-of-life planning has become a social phenomenon in Japan centered about the elderly. Given the declining birthrate and aging population, parents are increasingly saying, "I do not want to be a burden to my children," and they are now less likely to live with their children and to have opportunities for exchanging information. These developments all lie behind increasing concerns about "end-of-life planning" in society.

In this way, it can be said that Japan, as a country that has clearly become a super-aged society, is seeing the gradual formation of a culture that anticipates and prepares for "death" in the form of "end-of-life planning" (at the same time, while the need for end-of-life planning is recognized, there are still many people who find the topic of death too difficult to handle and who cannot take the first step in making preparations).

Up to now, end-of-life planning has generally focused on matters associated with the funeral, gravesite, and inheritance. However, with the spread of digital devices such as personal computers and smartphones in the wake of the Internet boom, the issue of "digital assets" is attracting increased attention as they can pose problems when the user of a digital device dies.

In this article, I would like to explain what the term "digital assets" means with a focus on pre-death measures (end-of-life planning). I point out here that the processing of digital assets is a problem that becomes entangled not only with the inheritance system of each country but also with the legal system itself with respect to digital assets. Recent years have seen a growing movement in enacting or legislating laws in relation to digital assets in a variety of countries such as the Fiduciary Access to Digital Assets Act (FADAA) in the United States, but there has been no such legislation in Japan as yet. Given the inheritance system in Japan, I would here like to consider what kind of pre-death measures could be taken (end-of-life planning) in Japan where no legal system in relation to digital assets exists.

2. What are Digital Assets?

2.1 Definition and types of digital assets

Here, to differentiate from ordinary articles left by a deceased person, I would like to define a digital asset of a deceased person as "an intangible thing that can be understood, for the most part, only via a digital device." Now, on the basis of this definition, digital assets can be divided into two types in terms of properties: offline data and online data.

Offline data, as the word "offline" implies, is a digital asset that can be understood or processed without relation to an Internet environment, or in other words, "data." In more concrete terms, offline data can be thought of as a Word or Excel file stored on a personal computer or photos taken with a smartphone.

On the other hand, online data, as the word "online" implies, is a digital asset that assumes an Internet environment to be understood or processed, and in this sense, is an "account." Specifically, online data can be thought of as an account on an Internet service such as a social networking service (SNS), Amazon, etc.

2.2 Inheritance of digital assets

(1) Introduction

Before I explain how digital assets should be handled, I would first like to describe how digital assets are inherited in the first place. Furthermore, as described below, it must be kept in mind that processing in relation to inheritance is completely different between offline data and online data.

(2) Inheritance of offline data

A Legal considerations of inheriting offline data

To begin with, can offline data be inherited? The answer is "no." This may come as a surprise, but being digital data, no ownership or other property rights are recognized for offline data, so it is not, as a consequence, a target of inheritance.

I will explain this in detail below (the following includes somewhat specialized content and may be skipped if so desired).

First, from the perspective of Japan's Civil Code, the object (target) of property rights including ownership is limited to tangible entities (things that occupy a part of space whether they be a liquid, gas, or solid). In short, no property rights including ownership are recognized for anything that is a not a tangible entity.

In this regard, it cannot be said that offline data (so-called

"data") is a "thing that occupies a part of space," so it is not a "tangible entity" (but rather an "intangible").

As a result, property rights including right of ownership to offline data cannot be considered and any heirs (family of the deceased) cannot inherit ownership of the deceased's offline data. (I here omit discussion on intellectual property rights.)

B Processing of offline data

Now, given that the family of the deceased (heirs) cannot inherit offline data, can they process that data? The answer is "yes." However, given that rights to offline data are not recognized and that offline data is therefore not the target of inheritance as explained above, why then is the family of the deceased able to process offline data itself? Constructing a theory to explain this presents a problem.

In this regard, while conceptualizing (creating) a new right similar to property rights can be considered, this problem can be solved by existing inheritance practices. I will explain this below.

Since offline data is stored in the memory portion of a digital device, it has no independent existence without that digital device. The offline data and digital device can therefore be called an integrated entity. Consequently, if it is understood that the owner of that digital device can process or handle any digital data (offline data) within the device, the problem that no one may handle that offline data can be avoided.

Furthermore, since it is quite rare in a will to prepare an article stating which persons will inherit which digital devices, then, in the absence of any wording to the effect of "all other possessions will be inherited by so-and-so," each digital device will enter into a shared state among the heirs if no legacy division conference is held. As a result, it can be said that each heir can access that digital data on the grounds of Article 249 of Japan's Civil Code.

C Summary

No ownership rights are recognized for offline data, and it is therefore not a target of inheritance. However, it can be said that offline data in each digital device can be handled as desired by inheriting digital devices storing offline data.

(3) Inheritance of online data

A Rights of online data

In contrast to offline data, online data assumes the existence of an Internet environment as well as that of a third party. In other words, online data can be thought of as a relationship between a service provider and a user, which, in reality, is none other than a "contract." This means that online data should be the target of inheritance in the usual sense.

B Online data and exclusive nature

However, the presence or absence of "exclusive nature," while not much of a problem in ordinary inheritance processing, is a problem in the case of online data. I will explain this below.

To begin with, "exclusive nature" is a property by which rights or obligations belong to an individual and are not transferable to a third party (including an heir) thereby excluding them from inheritance. An example that should clarify this property is the right to receive social benefits.

In general, the content of an Internet service account (contract) is specified in the user agreement for each service.

Most Internet services, moreover, include statements of the kind presented below in which contract content assumes an exclusive nature.

Consequently, if an exclusive nature as described above has been specified in the user agreement, that account (contract) is something that cannot be inherited.

C Summary

Since online data is, in essence, a "contract," it can be treated as a target of inheritance, but if the content of that data is judged to have an exclusive nature, it falls outside the scope of inheritance. Caution should therefore be taken in the case of online data.

3. Pre-death Measures for Digital Assets (Digital End-of-life Planning)

3.1 Need for digital end-of-life planning

(1) Introduction

Pre-death measures are essential in the case of digital assets. I will explain the need for digital end-of-life planning below.

(2) Characteristics of digital assets

I defined a digital asset of a deceased person as "an intangible thing that can be understood, for the most part, only via a digital device." In short, if the inside of a digital device cannot be accessed and its content checked, it would be difficult to determine even the existence of that content.

At the same time, recent digital devices come equipped with a "password lock function" as standard. This function requests a previously set login password when someone attempts to gain access to a digital device thereby preventing a third party other than the user from accessing the content of that device.

It is not uncommon for a user of a password lock function to refrain from conveying that password to anyone else. Consequently, there are a very high number of cases in which a digital device cannot be accessed even if the device itself can be found.

(3) Lack of a legal system surrounding digital assets

There are no laws at present describing how to handle digital assets for protecting heirs, which means a situation with no legally established benefits in the case of digital assets.

Moreover, as for the accounts (the content thereof) of users of Internet services, there are not even self-imposed regulations by industry organizations, which means a situation in which the handling of such accounts relies on the discretion of each business operator.

(4) Importance of digital assets

In modern society, digital devices have made deep inroads into our daily lives. In fact, it is no exaggeration to say that a person could live their life with a single smartphone.

On the other hand, important information has come to be stored with digital devices. This important information in its entirety becomes "digital assets" on the death of the user.

The processing of digital assets looks to increase in importance from here on.

(5) Summary

As described above, the characteristics of digital assets are such that it can be extremely difficult to specify their existence without being able to gain access into that digital device. On the other hand, though password functions are installed in key digital devices and used by many people, the situation is such that access cannot be gained into a digital device when that need arises if no password is available to a third party such as the user's family.

In addition, a legal system in relation to digital assets has yet to be legislated in Japan, so no means of relief exists if problems should arise with digital assets. At the same time, the processing of digital assets looks to become increasingly important in the years to come.

As a result, digital end-of-life planning is essential as a means of self-protection.

3.2 Specific methods for digital end-of-life planning

(1) Password sharing as the first thing to do

In digital end-of-life planning, the first thing to do above all else is to share one's login passwords for each of one's digital devices. This is because the capability of gaining accessing into a digital device significantly raises the possibility that the family of the deceased will notice the existence of the deceased's digital assets.

However, while some people have no problem with informing someone else about their passwords just in case something should happen to oneself, the reality is that there are many people who do not want to share their passwords while still alive.

With this being the case, I recommend that the following methods be considered.

Method 1: Prepare an "ending note" (similar to a living will) and give it to one's family

To begin with, we can consider the preparation of an ending note that includes the passwords of all of one's digital devices. This ending note should then be placed in an envelope and sealed, and instructions should be left to one's family to open the envelope if anything should happen to oneself.

An important point here is that, if the envelope should then at some time be opened, the situation with those digital devices can be easily understood, so some form of after-the-fact measures can be taken.

Column

How to deal with data that you do not want others to see

On the one hand, there is a data in your personal computer or smartphone that should be passed on, but on the other, there is data that you do not want your family to see for a variety of reasons.

In the case of data not meant for others' eyes, there are many people who simply say, "Just destroy all of your computers and smartphones." However, it is also said that sacrificing data that should be passed on and destroying your digital devices is not only unrealistic but a huge loss as well.

If you have data that you do not want your family to see, I recommend that you ask them to physically destroy that data through a data erasure (data wipe) process on each hard disk after clearly specifying the data that you want to save and pass on to them (no doubt the readers of this article have a variety of technical knowledge in this regard). It could be argued that doing such a thing will arouse suspicion, but building human relationships with your family so that you can request such a thing and carry it through is part of digital end-of-life planning. It should be kept in mind that there is an "analog" aspect to digital end-of-life planning involving such human relationships with one's family members since they are also obliged to perform some processing.

However, a disadvantage of this method is that the contents of those digital devices can be easily seen, so there are no doubt many people who would have absolutely no desire to use this method.

Method 2: Prepare a piece of paper listing each password and make it noticeable to one's family after death

The next method that should be considered is to prepare a piece of paper listing each password with an ending note included. Then, instead of passing the paper to one's family beforehand, it should be placed in a wallet or purse, bankbook, etc. that would probably be checked by one's family after one's death thereby making it noticeable to them at that time. Here, using pasteboard with the size of a credit or debit card should make it easy for a family member to notice.

However, compared with Method 1 above, the possibility of discovering such an item beforehand is low but not zero. To therefore lower the possibility of being discovered to the utmost limit, a method that places that paper in a bank safe-deposit box can be considered. However, care should be taken in this case since having one's family learn about one's passwords in a timely manner may be difficult since inheritance procedures must be firmly followed.

Method 3: Using other services

Recent years have seen an increase in software and web services related to digital end-of-life planning. The use of such services can be viewed as one approach to end-of-life planning.

(2) Measures that should be taken for offline data

If, at minimum, one's computer and smartphone login passwords are shared, then the family of the deceased can check the contents of those devices and understand to some extent the nature of any digital assets.

In the end, however, this simply means that the inside of the deceased's digital devices can be accessed—it does not guarantee that any data that needs to be passed on will be transferred in a timely manner. It can be said that searching through data on the digital devices of another person is extremely difficult for the family despite being "family." This is because it is difficult for a third party to understand how the deceased organized and used what types of files.

For this reason, if one has time to spare, the family should be informed not only of passwords but also of the storage locations of data that the family will likely need when the worst happens (for example, information in the form of "folder with the name OOO on the desktop" could be provided). It would also be a good idea here to clearly indicate how each set of data should be processed (for example, this information could take the form of "I need the data in this folder to be passed on to client X (telephone number 090-XXXX-XXXX)"). This approach is particularly essential if the data used in one's business exists on one's digital devices since that data should be passed on as soon as possible after one's death. I would like managers of small and medium-sized businesses and sole proprietors in particular to give these measures special attention.

(3) Measures that should be taken for online data

In the case of Internet service accounts, that is, online data, several dozens of contracts can be considered even for one individual if we include temporary accounts.

While it is not necessary to comprehensively process all such online data, accounts related to property (financial institutions such as Internet banks and online brokers, cryptocurrency exchanges, etc.) and accounts that charge fees should be handled in such a way that they can be reliably passed on to heirs or cancelled. As for the former, the names of the financial institutions in question and any methods for processing cryptocurrency (since there are probably many cases in which the family of the deceased has never used cryptocurrency) should be shared, and for the latter, IDs and passwords should be fully shared.

Additionally, I would recommend that one think about the way in which accounts with SNSs such as Facebook are to be handled after one's death (such as whether to use a memorial account).

4. Problems with Digital Assets

4.1 Introduction

The following describes problems that can occur if no digital end-of-life planning is performed as pre-death measures.

4.2 Unlocking the password lock on a digital device

While it is desirable if passwords can be shared between the deceased and the family of the deceased through digital end-of-life planning, not doing so means that the family will not be able to access the inside of the digital devices of the deceased.

In such a case, the family can request a company specializing, for example, in data restoration to unlock any password locks. The table can be used as a reference for such purpose.

Compared with smartphones, password locks on personal computers can be unlocked (data can be restored) at a relatively low price with a high probability of success. This being the case, it would probably be best to leave data needed by the family on a computer rather than on a smartphone.

On the other hand, the flip side of enhanced security on smartphones is a low probability of success in unlocking passwords and a high price for doing that. In addition, there are many cases in which the deceased opted for a smartphone equipped with a security function that initializes the data on the device (wipes the data clean) if the wrong login password is entered more than a certain number of times. Consequently, while there is no problem in particular with the family of the deceased trying to guess the password to a certain device from the deceased's birthdate, for example, they should stop doing so if they fail two or three times in a row and think about requesting the services of an appropriate business. Note that when a function like the one described above is being used, failing to guess and input the correct password any number of times may, in the end, lower the probability of

successfully unlocking the login password lock.

4.3 Problems with online data

(1) Introduction

In the case of Internet service accounts, determining the existence of online data is extremely difficult if it cannot be searched for inside of a digital device.

I would now like to introduce problems that have occurred when online data could not be passed on.

(2) Inheriting services of Internet financial institutions

The existence of accounts with Internet financial institutions (in particular, online brokers) is also entwined with establishing a comprehensive listing of the estate in inheritance proceedings, and as such, it is said to be a serious problem that can create difficulties in inheriting assets.

Additionally, if the deceased had been involved in foreign exchange (FX) transactions, significant fluctuations in the exchange rate could require the family of the deceased to make an additional margin deposit. (In one actual case, the family was required to deposit about one million yen.)

It is fine if the deceased had previously talked about trading stocks through an online broker, but it often happens that FX transactions are kept hidden from the family, so there are many cases in which such accounts had been established unknown to the family.

It can therefore be said that checking for the existence of online brokerage accounts is an absolute necessity for the family.

In this regard, it may be possible to identify any securities trading accounts of the deceased by making a request for disclosing registered subscriber information to the Disclosure Request Business Center of the Japan Securities Depository Center (JASDEC), so using this service should be considered.

(3) Internet services for business use

It appears that opportunities for using Internet services for business use have been increasing in recent years, and that many sole proprietors in particular have been contracting and using such services on an individual basis.

If it happens that the deceased had used such a service, it must be kept in mind that the account in question may not be transferable to the family because of its exclusive nature. For example, given that a contract had been made with a certain cloud service and data needed for business had been stored on the cloud, if the account then disappears due to the death of the user, it's possible that that data will never be retrievable again for business purposes.

For this reason, when using an Internet service for business purposes, a necessary measure to take is to store that data locally (offline) labeled with the name of the company.

In addition, there are many Internet services that will treat the data of a deceased user as exclusive in nature and process it accordingly even if that data had not been used for business purposes. Consequently, when entering into contracts on an individual basis, it is advisable to check carefully whether any data can be passed on if anything should happen to oneself.

5. Conclusion

Most people on hearing the words "end-of-life planning" are likely to say, "It's still too early for that!" and put off dealing with it until later.

They say, "I'm not going to die tomorrow, so tomorrow is fine to start planning," but "tomorrow" keeps coming and going, and the day one one's death is sure to come. "I should have taken care of this earlier!" ……. One day, it may be too late for regrets.

Before thinking about how to plan for one's funeral, arrange for one's gravesite, and other troublesome things, I would like you to put aside just ten seconds right now. Take a pen and write down your computer and smartphone login passwords on a piece of paper and give it to your family.

My sincere desire in writing this article is to eliminate the difficulty in dealing with digital assets for everyone.

Cover Art

Shinrei Yaguchi no watashi

Utagawa Toyokuni III (1786~1865)

Collection of the Art Research Center (ARC)
Ritsumeikan University
Object number: arcUP2851