Propose of a Mechanism to Avoid Personal Identification by Service Providers

1910065 Shinnosuke Kadwowaki

With the expand of the Internet, a variety of information is exchanged. This variety of information includes personal information. In addition, services such as social networking services and shopping website, which are based on the use of the Internet, have become an integral part of social life. When individuals use these services, the information exchanged may include personal information. Therefore, service providers can collect this personal information each time the service is used. Once the information is collected, the user has no control over it, so it is likely to remain with the service provider in the future. In order to prevent the collection of personal information, it is possible to separate the personal information from the transaction information for using the service, but if a lot of information is collected by the service provider, the personal information will be re-identified. One solution to this problem is to anonymize personal information and convert it into anonymously processed information. This anonymously processed information is information in which personal information is processed so that individuals are not identified. Personal information cannot be recovered from anonymized processed information. Identifying an individual from anonymously processed information is called re-identification.

This research proposed a mechanism to use services without identifying individuals by using an anonymous processing system that converts personal information into anonymously processed information. This anonymous processing system has four functions.The first function is to convert the data in the personal information field into anonymously processed information.The second function is to allow other service users to freely use the anonymously processed information records created in the first function. The third function is to increase the amount of anonymously processed information that is not based on service users' personal information. The fourth is a function that allows the processing system to use the service regardless of the service provider. Using these functions, anonymizing systems can dilute the relationship between personal service providers and personal information. This research also propose the use of multiple anonymous processing systems. By placing multiple anonymizing systems horizontally and vertically in a multilayered manner, the relationship between service providers and personal information is diluted compared to the case of a single system.

This research also propose an anonymity processing policy management system that relays between the above anonymity processing systems and service users. The anonymous processing policy management system manages

the personal information of service users by ID. There are three types of ID management: separate model, flat model, and sectoral model. There are three types of ID management: separate model, flat model, and sectoral model. In addition, this anonymous processing policy management system records which personal information is required for each service.

When a user selects a service he or she wants to use, the information necessary to use that service is input through the anonymity policy management system and the anonymity processing system. The anonymous processing policy management system has a one-to-one relationship with the user. From the anonymization policy management system to the anonymization system, the personal information record, the selected service, and the processing policy for anonymization are passed. Anonymity processing system can process anonymously.

Personal information that can be processed anonymously will be processed anonymously. After that, the next anonymizing system is given the record of personal information, the information of the service selected by the service user, and the record of personal information required by the service. The last anonymizing system gives the personal information to the service. In this way, by combining the anonymity processing policy management system and the anonymity processing system service, the relationship between users and their personal information will be diluted.

Even with the use of anonymized processing systems and anonymized processing policy management systems, there is still the problem of personal information required to use the service. However, this problem can be avoided by using settlement services or delivery boxes installed in front of stations that can be used by anyone.