

Chapter 3

Data Flow and Security Underpinning the 5G Age

Technological innovation in the ICT field, including 5G, as covered above, has been a huge driver of digitalization throughout society. Nevertheless, in order to solve social issues with digitalization in this way, it is essential that along with technological innovation, companies and other entities make use of the increasing amounts of digital data in circulation. While there have been persistent calls to make use of digital data, just how much progress has been made at present with the use of personal data and other forms of digital data?

Section 1 Data Circulation Accelerated by 5G

1. Explosive growth in data traffic volumes

(1) Transitions in data traffic volumes

Data traffic volumes in Japan continue to grow in concert with rapid digitalization. According to the estimation results¹⁸ for November 2019 compiled by MIC, the total download traffic of broadband subscribers in Japan reached about 12.7 Tbps, a year-on-year increase of 15.2 percent. The same data indicates that total upload traffic exceeded 1,500 Gbps, representing a yearly growth rate of 12.1 percent.

(2) Development of mobile growth

Mobile communication traffic is soaring with the prevalence of mobile phones and smartphones. According to MIC results¹⁸ of the previous estimate the total mobile communication download traffic in Japan is smaller than that for fixed-line communications, at 3,082 Gbps, but mobile's annual growth rate of 20.2 percent is outpacing that of fixed-line communications.

2. Changes accelerating data traffic volumes

Several factors are thought to be causing this increase in data traffic. These include larger content sizes, the

growth of IoT devices, the growth of 5G, and further digitalization prompted by the COVID-19 pandemic.

3. Current state of collection of personal data by companies

Data traffic growth in general is increasing the vol-

ume of personal data in circulation as well.

Section 2 Current State of and Issues with Digital Data Use

1. Current state of digital data use in Japan

(1) Current state of data use by Japanese companies

MIC conducted a survey in March 2020 of company employees to gauge the actual current use of digital data by Japanese companies.

a. Current state of data use

We first analyzed the types of data used in company activities (Figure 3-2-1-1). Compared to the survey conducted five years ago, there is greater use of sales records collected through POS or e-commerce and auto-collected data including MtoM data. This suggests companies are increasingly adopting IoT systems. In addition, use of telephone and other voice data has risen,

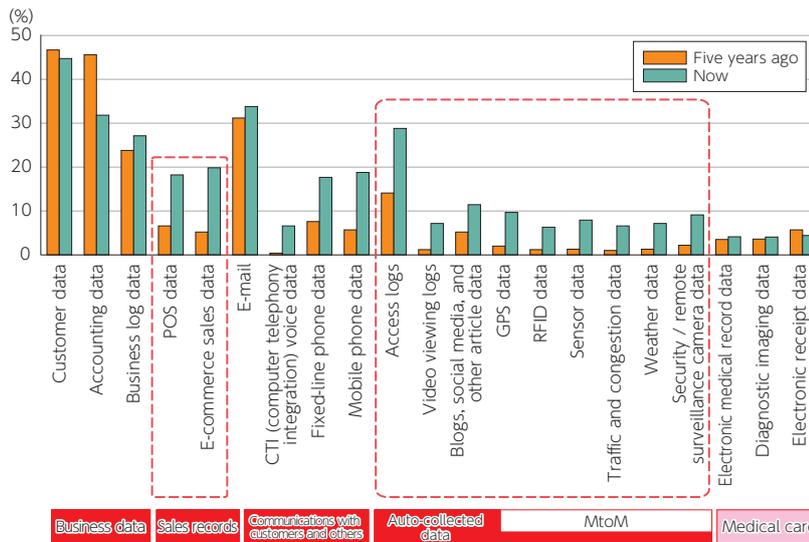
suggesting that, by data analyses, company management approaches has greatly been sophisticated over last five years.

The survey shows large companies use all forms of data at a higher rate than smaller companies. The use of GPS data, sensor data, and other IoT-related data in particular remains low at SMEs.

The operational domains where data are used the most are "business planning and organizational reform", "product and service planning and development", and "marketing" (Figure 3-2-1-2). Around 90 percent of large companies and more than half of SMEs use data in at least one operational domain. By industry, manufactur-

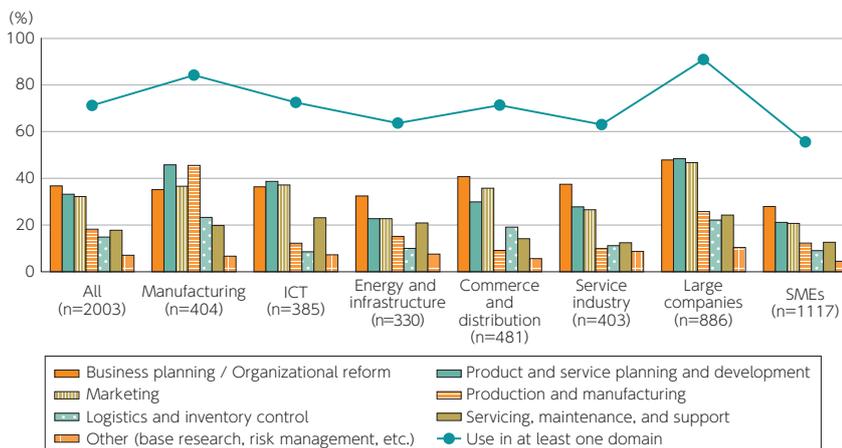
¹⁸ Ministry of Internal Affairs and Communications (2020). "Aggregate Results for Internet Traffic in Japan (November 2019)" (https://www.soumu.go.jp/main_content/000671256.pdf)

Figure 3-2-1-1 Data used in analyses



Source: "Survey on Measurements of the Economic Value of Digital Data and the Current Use of Digital Data", MIC (2020)

Figure 3-2-1-2 Operational domains that use data



Source: "Survey on Measurements of the Economic Value of Digital Data and the Current Use of Digital Data", MIC (2020)

ers are most likely to make use of data, while just over 60 percent of companies in energy and infrastructure and the service industry make use of data.

As for data analysis methods, "viewing data" and "tabulation" were the most common, at about 70 percent regardless of company size or industry (Figure 3-2-1-3). A considerable gap, however, was seen between large companies and SMEs regarding "statistical analyses" and "forecasting using machine learning, deep learning, or other artificial intelligence (AI) methods". In addition to pecuniary factors, personnel differences are also thought to account for this gap.

b. Outlooks on future data use

How do companies think about the use of data in the future?

When companies were asked for their plans to use data in each operational domain roughly three to five years from now, around 30 percent of companies that presently do not use data answered "would like to use

data in the future" for all domains (Figure 3-2-1-4). This reply rate was somewhat higher for the "servicing, maintenance, and support" domain. Nevertheless, although the replies include companies lacking the corresponding domain, the most common reply, ranging from 40 percent to around 50 percent, was "have no plans to use data in the future".

(2) Benefits of data use

a. Impact of digital data use on company businesses

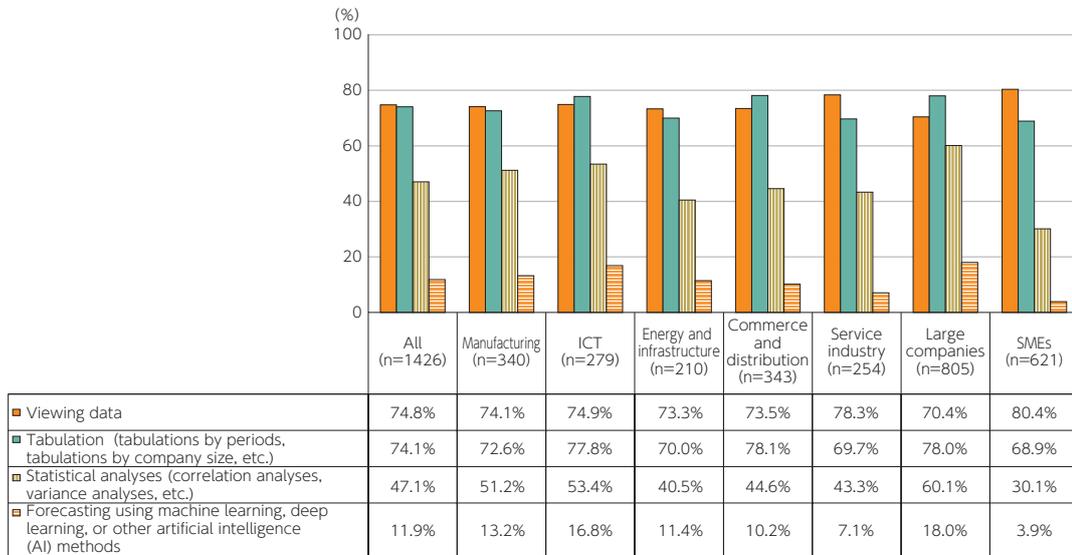
Multiple prior research papers have made it clear that digital data use does have benefits for company businesses.

b. Benefits of digital data use

The question is whether Japanese companies are seeing these benefits.

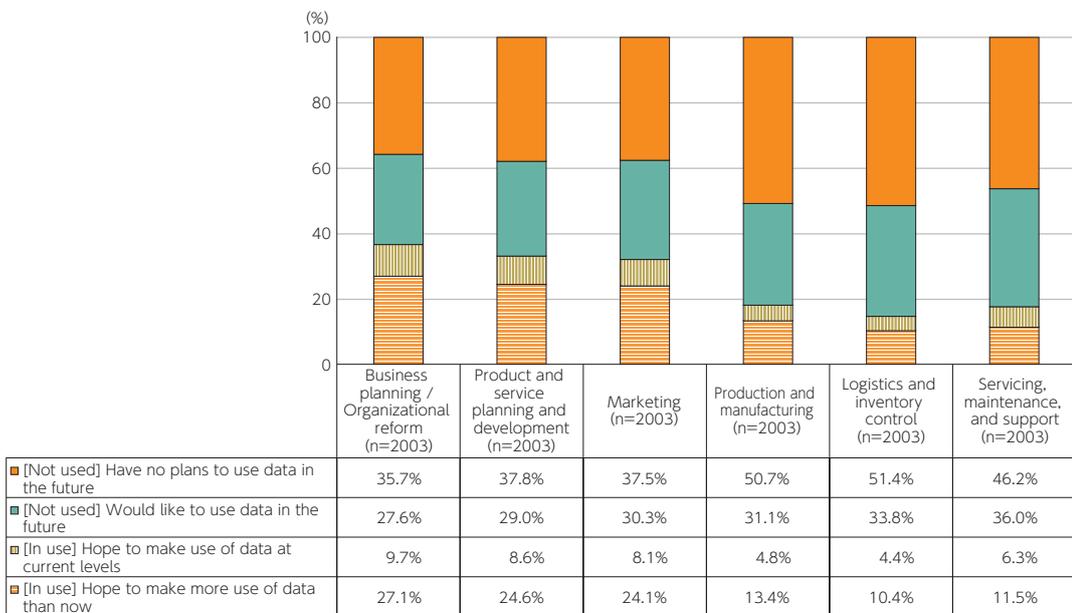
From the percentage of companies that use data in each operational domain and the percentage of companies that said the use of data was beneficial, we calculat-

Figure 3-2-1-3 Data analysis methods



Source: "Survey on Measurements of the Economic Value of Digital Data and the Current Use of Digital Data", MIC (2020)

Figure 3-2-1-4 Plans to use data in the future



Source: "Survey on Measurements of the Economic Value of Digital Data and the Current Use of Digital Data", MIC (2020)

ed the percentage of data-using companies that said data use was beneficial (the benefit achievement rate). The achievement rate was highest in the "production and manufacturing" domain, at 67 percent, followed by "lo-

gistics and inventory control", at 65 percent (Figure 3-2-1-5). From these calculations, the benefits of efficiency and optimization efforts using data are thought to more easily appear in these domains.

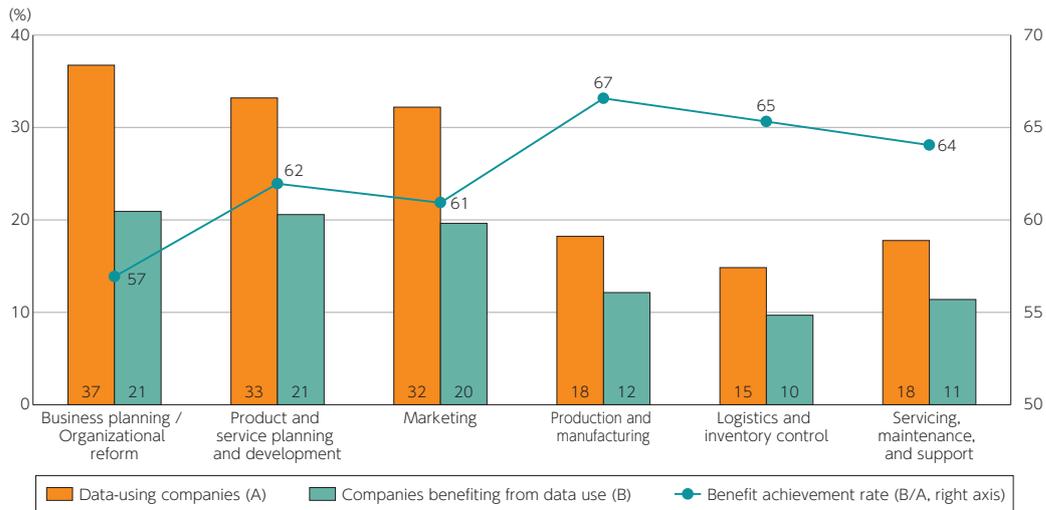
2. Comparisons with other countries

Use of digital data is on the rise in Japan, but what can be said of Japanese companies when compared to their overseas counterparts? Comparisons were made with U.S. and German companies based on a survey.

Companies were asked about their usage of non-personal data obtained from products and services, such as

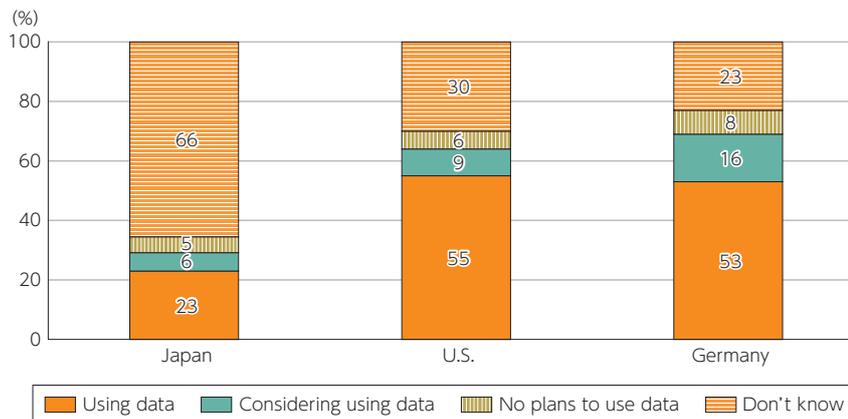
the operating status and usage status of products. Around 30 percent of Japanese companies answered either "using data" or "considering using data", whereas over 60 percent of U.S. and German companies answered either "using data" or "considering using data" (Figure 3-2-2-1).

Figure 3-2-1-5 Benefit achievement rates



Source: "Survey on Measurements of the Economic Value of Digital Data and the Current Use of Digital Data", MIC (2020)

Figure 3-2-2-1 Usage of non-personal data



Source: "Survey on Consumer Attitudes on Data Usage Environments", MIC (2020)

3. Promoting greater use of digital data

(1) Initiatives to share digital data among businesses

What are possible policies to encourage more digital data use?

One possibility is the construction of frameworks that facilitate data sharing. If companies could more easily access a broad range of data, presumably companies that couldn't obtain actionable data previously would make use of that data in their businesses. Companies in the surveyed countries, which included Japan, listed inconsistent data formats and assurance of data quality as two main issues with digital data use. Consequently, discussions of how to resolve these issues must be encouraged during the process of constructing data-sharing frameworks.

Initiatives in Japan designed to share digital data among businesses were included in the government's "Declaration to be the World's Most Advanced Digital Nation: A Basic Plan for the Advancement of Public and Private Sector Data Utilization",¹⁹ which was endorsed

by the Cabinet in June 2019.

Aside from government initiatives, similar movements are appearing among private companies. Data-sharing frameworks promoted by public and private initiatives should be monitored, as construction of such frameworks is expected to further activate data use. This is true despite numerous problems that need to be solved, such as how the framework will improve company earnings and how the framework will be structured to persuade consumers and companies to provide their data.

(2) Use of open data

a. Initiatives to solve social issues using open data

Other expected initiatives include the expanded future use of open data.

Civic tech movements — the use of technology to solve social issues led primarily by citizens — have gained attention, especially in measures to counter CO-

¹⁹ <https://cio.go.jp/data-basis>

VID-19. These civic tech movements have reformatted digital data obtained from multiple entities to make them more visible and understandable and are putting the data to use in various measures.

b. Initiatives to expand open data

The government promotes initiatives to expand the use of open data.

One example in Japan is the previously mentioned “Declaration to be the World’s Most Advanced Digital Nation: A Basic Plan for the Advancement of Public and Private Sector Data Utilization”. The declaration regards open data as the “starting point for data circulation” and

includes policies to encourage the national and local governments to make more data open.

Inconsistencies between open data formats have been an obstacle for citizens to collect and share COVID-19 information. Volunteer engineers put together a standard format for data on such statistics as the number of people who have tested positive and the number of tests administered in the “Definition Document of Open Data Parameters Related to COVID-19 Protection Measures”. After receiving the document, MIC promoted further open data measures by local governments and stronger cooperation with civic tech, along with providing information to municipalities.²⁰

Section 3 Future Use of Personal Data

1. New models for personal data circulation

Various new personal data circulation mechanisms have been proposed in recent years, such as personal data stores and data transaction markets. One leading example of an initiative taken in this country is personal data trust banks.

Personal data trust banks manage the data of individuals based on a contract or agreement with the individual. The businesses provide personal data to third parties according to the individual’s instructions or to conditions prespecified by the individual.

The Information Technology Federation of Japan be-

gan accreditations of personal data trust banks in the autumn of 2018 in a format compliant with the “Guidelines on Accreditation of Information Entrustment Functions Ver. 1.0”²¹ established by MIC and METI. As of March 2020, five companies have received accreditation, including normal accreditations for businesses already running personal data trust bank services and accreditations for businesses planning personal data trust bank services.

Scoring services are also being launched in Japan.

2. Consumer attitudes on data circulation

(1) Concerns about providing personal data

In connection with personal data use, we asked consumers what they thought about providing their personal data when it came to using services and applications provided by companies and other organizations. In all

countries, more than 60 percent of consumers had concerns about providing their personal data (total of those answering “very concerned” and “somewhat concerned”) (Figure 3-3-2-1).

3. Expanding the use of personal data

(1) Personal data trust banks are hoped to be the key to greater personal data circulation

a. Company awareness

Although personal data trust bank services have just started, new mechanisms governing data use and application — that could be called individual-directed data circulation — are expected to become platforms to drive the use and application of personal data.²²

We asked respondents in the U.S., Germany, and Japan about their awareness of these new data use models. Less than 10 percent of respondents in Japan knew of the models and understood their details, compared with around 20 percent in the U.S. and Germany. Furthermore, the awareness level among Japanese respondents

has barely changed between the previous survey and now.

b. Consumer attitudes

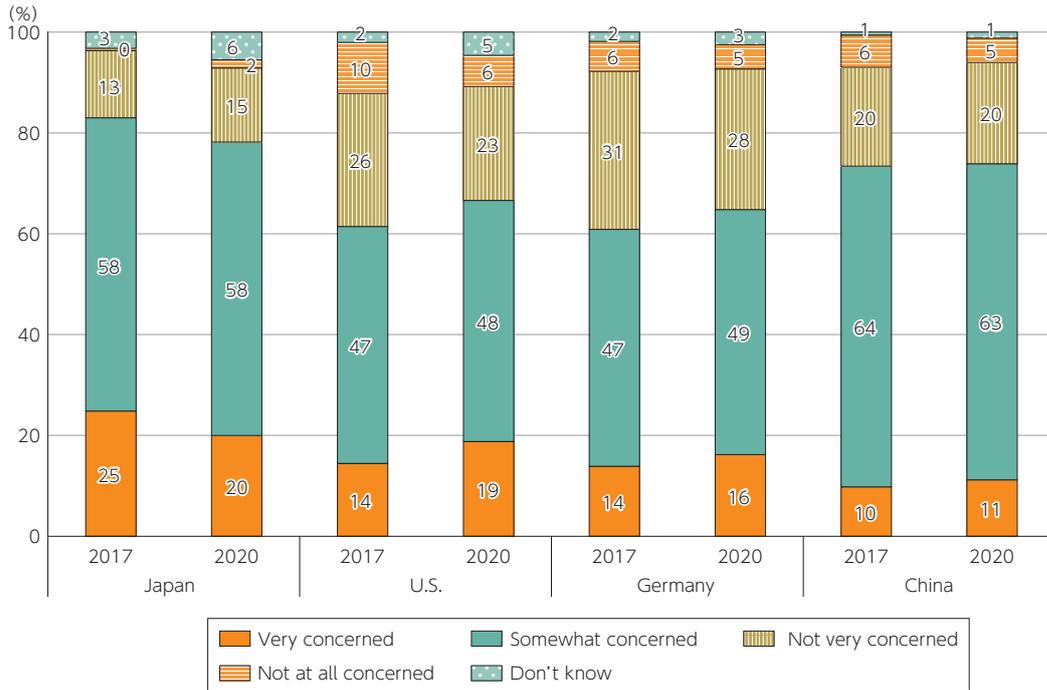
Looking at consumers’ intentions to use personal data management services, in Japan, those that said they “do not want to use” the services were roughly the same, percentage wise, as those that said they “want to use” the services. Still, the percentage that said they “want to use” was lower than in the U.S. and Germany, where the percentage was over half, and in China, where the rate was close to 80 percent (Figure 3-3-3-1). Nevertheless, more respondents answered “want to use” in all countries, including Japan, and less answered “do not want to

²⁰ Ministry of Internal Affairs and Communications (2020). “Request for the Provision of Statistical and Other Data Facilitating the Prevention of the Spread of COVID-19 Infections” https://www.soumu.go.jp/menu_news/s-news/02kiban01_04000143.html

²¹ https://www.soumu.go.jp/main_content/000607546.pdf

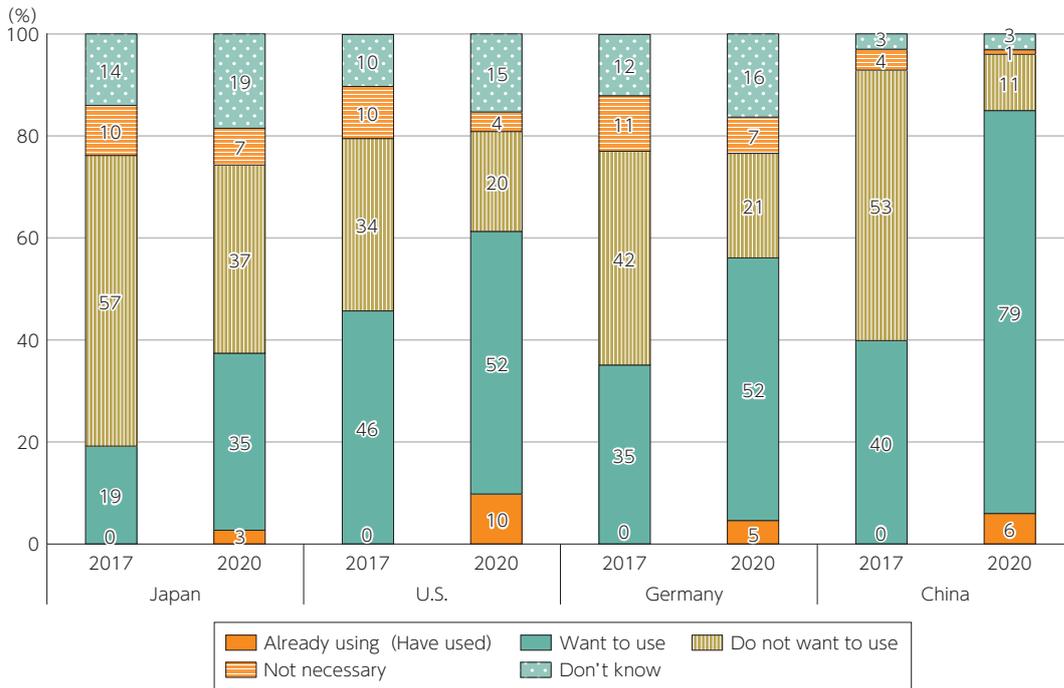
²² Based on an interview with an expert (Associate Professor Naoto Ikegai at Toyo University) in Ministry of Internal Affairs and Communications (2020) “Survey on Consumer Attitudes on Data Usage Environments”.

Figure 3-3-2-1 Concerns about providing personal data when using services and applications



Source: "Survey on Consumer Attitudes on Data Usage Environments", MIC (2020)

Figure 3-3-3-1 Consumer intention to use personal data stores or personal data trust banks



Source: "Survey on Consumer Attitudes on Data Usage Environments", MIC (2020)

use" than on the previous survey. The results show intentions to use personal data management services are rising.

We infer that the rise in consumer intentions to use personal data trust banks and similar services and the entrustment of more personal data in Japan will lead to an increase in personal data that companies can use. Nevertheless, the reality is there are factors obstructing

the expanded use of these services by companies and consumers. Therefore, to contribute to the further circulation of personal data by personal data trust banks, two things are thought to be critical: work to raise awareness among companies by, for example, publicizing the advantages of using personal data trust banks while providing secure and convenient services consumers can use without fear of security breaches.

(2) Further utilization of anonymously processed data

In addition to promoting personal data trust bank efforts, it can be said that the expansion of the use of anonymously processed data by companies is also expected to encourage the use of personal data by companies.

(3) Promoting digital transformations at Japanese companies

As we have seen, Japanese companies are not as advanced in the use of digital data, including personal data, as companies in the U.S. and Germany. Nevertheless, initiatives are making progress in assisting the use of digital data by companies, such as open data, anonymously processed information, and personal data trust bank initiatives. Furthermore, Japanese consumers' re-

sistance to the use of their personal data is slowly ebbing.

Based on the premise that digital data use brings positive benefits to company businesses, it is predicted that companies failing to achieve digital transformations will find it hard to survive due to digital disruptions amid competition with companies that have achieved digital transformations through advanced use of digital data. This tendency has probably increased all the more due to the dramatic leap in digitalization triggered by COVID-19. To cope with such situational changes in the international community, Japanese companies will have to apply various means to make greater use of digital data and press ahead with digital transformations.

Section 4 Cybersecurity in the 5G Age

1. Cybersecurity increasing in seriousness and complexity

The importance of handling the risks associated with cybersecurity is mounting as digitalization progresses. The "Cybersecurity Strategy",²³ endorsed by the Cabinet in 2018, stated that the potential for serious ramifications from cyber attacks will magnify exponentially as integration between cyber space and real space advances. For people to truly benefit from digitalization, it is vital that cybersecurity initiatives proceed hand-in-hand with advances in cutting-edge technologies and data application.

(1) Recent security concerns

Recent cyber attacks occurring around the world has widely been reported on the news. And still the range of attack vectors is diversifying year by year, and it is no longer an unusual occurrence for cyber attacks to bring services or servers to a standstill, steal or divulge information, or cause other significant damages.

a. Concerns about fraudulent smartphone payments

2019 saw a large increase in the use of cashless payments, in part because of a promotion program to receive a refund for payments made by cashless payment as an economic measure associated with the consumption tax increase in October 2019. Payments using smartphones also surged because of their ease and because of large promotions run by companies. Security concerns, however, have arisen in tandem with the increase in smartphone payments.

b. More extensive malware losses

Malware refers to malicious software or malicious code created with the intention of carrying out illegal or harmful actions. A characteristic of this sort of malware is that attack emails masquerade as normal business

emails by quoting real emails the attack victim had sent in the past.

Attack methods have grown more sophisticated than previous targeted emails. For example, attackers use the text of real emails sent previously to get the victim to trust that the malware email has been sent from a past correspondent. Attackers also craft attack emails based on emails of users who have already been attacked.

c. Growing sophistication of phishing attacks

Theft of personal information through phishing attacks also increased in 2019. According to statistics from the National Police Agency,²⁴ losses from illegal money transfers related to online banking soared from September 2019. Many of the losses are suspected to be the result of directing victims to phishing sites masquerading as financial institutions using short messaging services or email. There were 1,872 incidents in 2019, with losses totaling around 2.521 billion yen. This is the second largest number of incidents after 2014, which recorded the most incidents ever, and the total losses are considerably higher than last year.

(2) Implications of security concerns**a. Economic impacts**

In concert with the advancement of ICT in all parts of society, these cybersecurity concerns are having a direct impact both in cyber space and in our lives.

b. Impacts on people's livelihoods

The ramifications of cyber attacks in the real world are not limited to financial losses. Cyber attacks can impact not just cyber space but also many aspects of our real lives.

²³ <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf>

²⁴ National Police Agency (2020). "Threats in Cyberspace in 2019" (https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei_eng.pdf)

2. Rising cybersecurity risks in the 5G age

The “IoT/5G Security Comprehensive Measures”,²⁵ released by MIC in August 2019, pointed out several new risks associated with the start of 5G services. In particular, the expected growth in the IoT accompanying 5G expansion is likely to lead to even greater risks of cyber attacks in the future. The “Matters for Prompt Implementation to Strengthen Japan’s Cybersecurity [Urgent Recommendation]”,²⁶ released by MIC in January 2020, also advocates for the need to expand security

measures for IoT devices.

With the start of 5G commercialization, IoT device growth is expected to outstrip current rates. Despite this, there is a tendency to overlook the risks these devices present. This makes it all the more important to foster an awareness of the security risks when using IoT devices among users through such awareness-raising efforts as mentioned above.

3. New security risks

(1) Concern about supply chain risks

In addition to the security risks mentioned above, a new security concern that has surfaced in recent years is supply chain risks.

The “IoT/5G Security Comprehensive Measures”, established in 2019, cites examples of these risks, such as embedding unauthorized programs or firmware or tampering with legitimate programs or firmware during manufacturing or distributing ICT products and services. The document also mentions the possibility of the parties with contractual relationships such as consignment with insufficient cybersecurity measures being used as springboards for cyber attacks.

(2) Measures taken in Japan

To address supply chain risks, the Cybersecurity Measures Promotion Council and the Liaison Meeting of the Chief Information Officers (CIOs) of the Ministries and Agencies, at a joint meeting held in 2018, reached an understanding on obtaining and evaluating the information needed for procurement inspections.²⁷ This will serve as a new initiative to mitigate potential serious negative cybersecurity consequences when procuring information systems, devices, and services.

Furthermore, the decision was made to include the implementation of cybersecurity measures, including

supply chain risks, as a condition of approval of establishment plans for specified base stations when deploying fifth-generation (5G) mobile communication systems. It was also decided to add the same condition for local 5G licensing. And the Act on Promotion of Developing/Supplying and Introducing Systems Making Use of Specified Advanced Information and Communications Technologies, which was enacted in May 2020, requires the establishment of cybersecurity and other measures in order for businesses to receive special taxation exemptions.

Looking forward, there is almost certainly a need for more measures, in addition to the initiatives mentioned above, given the potential for vulnerabilities in software installed on devices and in the process of designing ICs and other hardware, as described in the “IoT/5G Security Comprehensive Measures”. One measure thought effective, as raised in the document, is the research, development, and application of technologies that harness big data and AI to detect potential vulnerabilities embedded in hardware.

Moreover, in light that attackers tends to single out businesses in supply chains without sufficient cybersecurity for attacks, it is necessary to further improve security measures including regional ICT services and networks as well.

4. Current state of security measures by companies

(1) Awareness of security measures

Japanese companies have a relatively high awareness of cybersecurity risks. For example, on a survey on personal data, companies were asked their top priority when collecting personal data. Close to 30 percent of Japanese companies said their top priority is “ensuring the security of collected data” — the most frequently selected answer option for the question. The percentage of companies choosing this answer was up significantly from the 2017 survey.

(2) Current state of security measures

What kind of measures are Japanese companies taking, which have these levels of awareness?

On a survey conducted by MIC, company employees in Japan, the U.S., and Germany were asked the security measures they thought are important to manage and store personal data securely. “Provision of security education and training to employees” and “access restrictions on personal data and management of access logs” were among the top-three answers in all three countries. “Restrictions on taking devices or storage media in or out of facilities or buildings where personal data is han-

²⁵ https://www.soumu.go.jp/main_content/000641510.pdf

²⁶ https://www.soumu.go.jp/main_content/000666176.pdf

²⁷ National Center of Incident Readiness and Strategy for Cybersecurity (2018). “Understanding on Government Procurement Policy and Procurement Procedures for IT Goods and Services”. (https://www.nisc.go.jp/active/general/pdf/chotatsu_moshiawase.pdf)

dled” was another top answer in Japan. Conversely, in the U.S., 30 percent of companies have introduced “storage and management of encrypted personal data” as measures to guard against risks after data has been exposed. U.S. companies also attach importance to “more rigorous subcontractor screening conditions and implementation of subcontractor monitoring and inspections” as measures that mitigate supply chain risks.

5. Necessity of further security measures

(1) Mounting cybersecurity risks

From the survey results presented above, we know that Japanese companies recognize the necessity of security measures and are moving ahead with security measures. Personnel shortages, however, are proving to be a long-term challenge for Japanese companies in the area of cybersecurity, a problem that has been raised in previous White Papers including the “2019 White Paper on Information and Communications in Japan”. As cybersecurity risks mount due to the growth of the IoT, driven by greater data usage and wider 5G application as well as the hosting of the Olympic and Paralympic Games, there is more concern than ever before that companies will be the targets of cyber attacks. Consequently, organizations must take greater security measures than ever before in order to protect themselves

Focusing on answers by Japanese companies, there appears to be less importance placed on security policy establishment and operation today, compared to the survey three years ago. On the other hand, companies are prioritizing security diagnoses and monitoring, information security audits, and the acquisition of PrivacyMark, ISMS, and other certifications, as security efforts to manage and store personal data securely in recent years.

from such attacks.

(2) Fostering a sense of security among consumers

In addition to these rising risks, companies must also pay attention to the elevated concerns consumers have about security assurance.

The use of data has many positive benefits for company businesses. But deficient security measures may make it much more challenging for companies to acquire the personal data they need in the future. Security measures are essential for consumers to feel secure about their data to be trusted to companies. A single security incident causes not only financial losses but also a loss of trust in the company. Therefore, to move ahead with data use in the 5G age, it is imperative to implement more rigorous security measures than in the past.