IIJ's Road to BCR Approval —Complying with EU GDPR and Beyond

In August 2021, we received notice of the long-awaited approval for IIJ's BCRs (Binding Corporate Rules) from LDI-NRW, the supervisory authority in North Rhine-Westphalia (NRW), Germany. Since the EU's GDPR (General Data Protection Regulation) came into force, 18 companies worldwide have received BCR approval (as of August 2021), IIJ being one of them. The five years since we started looking at BCRs as a means for complying with the GDPR have been eventful, and with the approval, we can now proudly say that our efforts so far have finally been recognized.

Here, I discuss why we chose the IIJ BCR approval route, what the road to acquiring that approval was like, and where we are headed from here.

4.1 Decision to Seek BCR Approval

The EU drafted the GDPR for the purpose of protecting personal data within the EEA (European Economic Area) in 2016, and it came into effect in 2018. The GDPR was the subject of a lot of speculation back when it was announced, and I remember some extreme arguments saying, for example. that it would harm the free distribution of information on the Internet.

The EU's objective was of course not to restrict the distribution of personal data on the Internet. Rather, it was calling for the appropriate use of data on people in the EU at a time when such information was already being used in countries everywhere. Where practices had been vague, the EU wanted to lay out clearer protections on personal data that had real effect. It was a truly advanced initiative to institutionalize such protections. I think that, even now, the policies and practices for personal data protection laid out in the GDPR have a lot to say about personal data protection in the information age.

With the rise of major platform operators, exemplified by GAFA, that use personal data to the hilt and Snowden's exposure of the US government's excessive surveillance practices, there was strong distrust within Europe about the US's use of personal data, and I think this is the real backdrop for what prompted the creation of the GDPR. I think, at its heart, this traces back to a marked difference in cultural values about personal data. This is something I will discuss later.

It became evident that the EU was pretty serious, but IIJ doesn't provide personal services on a global basis, and there was talk about the Japanese government's Personal Information Protection Commission working toward some sort of national certification from the EU anyway, so truth be told, we hadn't intended to actively pursue GDPR compliance. But as we worked through all the factors to consider, and with a proposal from Shinpei Ogawa, a director of IIJ Europe at the time, we came to the conclusion that seeking IIJ's own BCR approval would be advantageous.

We had four main reasons for embarking on our journey for IIJ's BCR approval.

■ We saw the need for global security governance

IIJ has been deploying group companies all over the world for some time, and doing business naturally requires us to address personal data protection and other factors in each country. In the past, however, we did not fully comprehend the situation in every country, so it was left up to each group company to mount its own response, and to be honest, we weren't able to address the issue of control on a group level. Creating IIJ's BCRs to comply with the GDPR and putting this into effect at group companies was crucial in enabling

us to implement control at a time when the situation around personal data was becoming more and more nuanced.

Alternatives to BCR were too complicated

An alternative to obtaining BCR approval as a means of meeting the GDPR requirements is to enter into SCC (Standard Contractual Clauses), a form of template contract, as necessary and perform data transfers on that basis. These contracts, however, must be meshed in the sense that there needs to be contracts between the controller (the party responsible for holding the personal data) and the processors (the parties who receive the personal data for processing), as well as between processors themselves. And if changes are made to how the data are processed, the contracts must be entered into again, so managing the contracts is cumbersome. It was easy to see that we would end up with quite a lot of contracts just with IIJ's own group companies, and given the nature of our business, in many cases information from our customers is deployed across each of our group companies' platforms. For these reasons, we were concerned about this approach eventually collapsing. IIJ's own BCR approval was really the only way to solve the problem.

GDPR represented a more advanced approach than Japan's own personal information protection practices

IIJ naturally implements internal controls for the protection of personal information and has acquired Japan's P Mark (Privacy Mark). Yet something that became eminently apparent as we started to understand more about the GDPR is that the EU's commitment is on another level. Japan's personal information protections certainly do comprise a range of carefully thought out measures, but the EU's approach was to tackle these difficult problems through sound reasoning and ideas, and to look ahead and start implementing responses to a range of issues that potentially lay down the track. We were honestly surprised at how far they were taking it. Japan was also naturally making an effort in that regard, and the EU did adopt an adequacy decision on Japan, but it is telling that supplementary rules were applied to transfers of personal data from within the EEA to Japan. This leads into the discussion that follows, but the approach of giving careful thought not just to the controller but also to the processors, and developing a framework with respect to the processors, is a fairly advanced one. The EU obviously implemented this because it felt it was necessary to protect personal data, but I think it also shows that they were somewhat prescient about how personal data would be handled in the Internet's cloud era.

It would enable protection of personal data on cloud services in addition to personal data held by IIJ

The EU's motivation for creating the GDPR was clearly to regulate the handling of personal data on the Internet by platform operators and the like within the EEA, to which end it sought to impose rules on business operators and the like that handle personal data so as to ensure that they do so properly in accord with EU standards. As such, the GDPR naturally applies not only to controllers responsible for managing personal data but also to processors who receive such data from controllers. I think the EU made such provisions explicit because it was seeking to confront what it saw as a less than appropriate state of affairs particularly with respect to the platform operators who process personal data. This potentially opened the way for outsourcing, such as cloud services, to comply with the GDPR by meeting the BCR conditions under the processor category. That is, it provided a way for controllers, the customers of such services, to prove that they use processors who have implemented proper protections.

IIJ Europe began looking seriously at GDPR compliance in January 2016, and IIJ's board of directors officially gave approval to start working toward BCR approval in May 2016. The approval was actually received on August 5, 2021, partly because of how long the review takes, but also due to the impact of Brexit and other subsequent events. While not all that many people were involved over that period, a number of internal units, led by the Risk Management Office, had a role to play, including the Business Risk Consulting Headquarters, the Global Business Division, and the Compliance Department, and we actually used a law firm when negotiating with the EU's supervisory bodies as well. Our efforts did finally pay off in the form of BCR approval. IIJ is the first global cloud vendor, not just in Japan but worldwide, to receive approval since the GDPR took effect.

But as with other aspects of data governance, obtaining approval is not the goal. Instead, it provides an opportunity to embark on new efforts to establish internal control for global data governance.

4.2 What are BCRs?

Below is a brief explanation of BCRs.

BCRs are data protection policies that are adhered to by an entire corporate group (these policies are also made known to the subjects of personal data and are thus widely disclosed) and embody rules that are binding on the group companies and their employees. The objective is data protection, but this is not so much about implementing technical security measures as it is about sharing information and educating employees on the basic principles and rules around the handling of personal data, creating an operating environment that allows employees to raise queries or complaints, and so forth. In that sense, the approach is akin to the efforts developed in Japan over the past many years around internal control for information security and personal information protection. That said, the EU's GDPR is the most stringent personal information protection regulation anywhere in the world, so obtaining BCR approval is by no means easy.

At the IIJ Group level, the IIJ Binding Corporate Rules appear at the very bottom of the privacy policy on IIJ Europe's website, and IIJ Group companies also link to this.

Once a corporate group's BCRs have been approved by the competent data protection authority in the EU, this certifies that, in terms of personal data protection under EU law, the group has appropriate safeguards in place, and under GDPR Article 46, Item 2(b), this allows it to legally transfer personal data fro within the EEA to locations outside of the EU.

Transfers of personal data from within the EEA to the outside of the EEA are in principle prohibited. There are a number of recognized ways of making it possible to do this, though. Among them, BCRs represent the strictest standards at the corporate level. As long as they comply with the BCRs, transfers of personal data outside the region to corporate groups that have BCR approval, or between companies within a group that has received approval, are recognized as being subject to the appropriate safeguards required by the GDPR.

Approval is obtained by submitting BCRs as stipulated in GDPR Article 47 to the competent data protection authority for approval. A rigorous review process that goes beyond the competent authority ensues. First, the competent authority reviews the BCRs with the assistance of supervisory authorities, and corrections are repeatedly made

in conjunction with the company under review. Once it is satisfied, the competent authority communicates with the EDPB (European Data Protection Board), part of the European Commission, the EU's executive branch, and submits a pre-review request to the ITES (International Transfer Expert Subgroup) meeting. ITES is made up of experts from the supervisory authorities of all EU member states. They may think that something should be done differently or that a particular rule is a little loose, and they accordingly send revision requests to the competent authority, based on which the corporate group revises the BCR draft. This process is repeated until it is apparent there are no further opinions on the pre-review, at which point the competent authority asks for an Opinion from a plenary meeting of the EDPB, the highest decision-making authority in this case, composed of representatives of all EU national data protection authorities. The Opinion is an official document of the EDPB, in accord with which the competent authority provides instructions to the corporate group to finalize the BCRs, and then grants final approval. This rigorous process means that obtaining BCR approval from your competent data protection authority in the EU takes quite a lot of effort and time.

In the IIJ Group's case, we submitted our BCRs to the UK's ICO (Information Commissioner's Office), our competent authority at the time, in October 2016. The impact of Brexit, however, means that the competent authority for us is now the supervisory authority in North Rhine-Westphalia (NRW), Germany. IIJ Europe (based in London) had been the IIJ Group's headquarters in the EU, but the UK's withdrawal from the EU meant that this role passed to IIJ Deutschland (based in Dusseldorf), and thus the supervisory authority in NRW, in which Dusseldorf is located, became the IIJ Group's competent authority. The norm in other countries is to have a single national authority, but with Germany being a federation, all 16 of its states have their own personal data protection supervisory authority.

The EU adopted an adequacy decision on Japan on January 23, 2019. The decision means the EU recognizes that Japan has personal information protection guarantees that are in line with those that apply in the EEA. This recognition from the European Commission was the result of work by Japan's Personal Information Protection Commission along with other stakeholders and no doubt came as a boon for many Japanese companies.

It does not mean, however, that all Japanese companies are now GDPR compliant.

First of all, the GDPR does not in principle allow the transfer of personal data out of the EEA, so the cross-border transfer rules must be observed when transferring data. The cross-border transfer rules, per GDPR Articles 45 and 46, allow such transfers under conditions including the following.

- The European Commission has adopted an adequacy decision on the country
- BCR approval has been acquired
- SCCs have been entered into
- In compliance with a (an industry) code of conduct approved by the EDPB

Put differently, only transfers of personal data out of the EEA pursuant to the GDPR are exempted. In addition, the Personal Information Protection Commission has published official notice that supplementary rules will apply to personal data transferred from within the EEA wherever the local rules are deemed inadequate. The EU's adequacy decision means that transfers of personal data from the EU

to Japan are permitted, but such data may not be further transferred from Japan to a third country. So the adequacy decision does not fully cover cases in which, for instance, an employee register is shared globally.

Japan's pursuit of an adequacy decision was the right approach for the nation to take, and an understandable one, in view of the circumstances of many Japanese companies' businesses, but it is unfortunate that it led to a sense that companies now no longer need to take any particular steps of their own with respect to the GDPR. Personal data protection is an extremely important issue for the Internet and other types of new information infrastructure, and we should not forget that the situation these days is such that even companies that do business mainly within Japan cannot ignore its impact.

4.3 Personal Data Protection Initiatives Around the World

As my mind became increasingly wound up in the various personal data protection initiatives out there, I was made acutely aware of differences in perspectives on personal data and astonished by just how different the cultural backgrounds can be. Norms around personal data in Japan merely represented Japan's own local perspective. My realization that there are rights and responsibilities with respect to personal data in other parts of the world that differ completely from those found in Japan was a very important insight that I gained from IIJ's BCR approval process. To be honest, I realized that IIJ's mindset as a traditional Japanese company simply would not cut it on the world stage. There exist multiple ideas about what is right and just when it comes to personal data around the world, and they will all no doubt have a major influence on the information society we live in going forward.

I will now briefly explain the background to the creation of the GDPR. An essential element is that the EU authorities are in opposition to the US in terms of privacy protection.

■ Historical background

The 9/11 terrorist attacks in the US were more than enough to shake the world's collective consciousness. After 9/11, the US embarked on a secret mass surveillance program and implemented mechanisms for installing backdoors in social media and other services in order to expose terrorists. These operations should only have been carried out under a court order, but in reality, as exposed by Edward Snowden in June 2013, the US had made it possible for intelligence personnel to freely snoop into people's privacy in the course of their intelligence activities. I think it was difficult for the American people to oppose this because the atmosphere was such that they felt compelled to allow the government to do what it needed to do for national security. I think Americans have a very strong sense of ownership about their country in the sense that they see the government as the people's representative and spokesperson, an attitude that dates back to the nation's founding. But then Snowden revealed that the US had been eavesdropping indiscriminately on embassies of the country's allies including Germany and France. This enraged the EU's member states and had major ramifications, the German government's axing of its Verizon contract, for instance.

The idea that the government is absolutely right does not exist in the EU. For more than a millennium, the European continent was again and again the scene of wars and conflicts that ultimately failed to settle national borders or territory. The rise of tyrants repeatedly led to tragic events—people oppressing those from different denominations within their own religion, for example, or

massacring other ethnic groups. The European Coal and Steel Community was created with the aim of establishing final national boundaries and securing a lasting peace after World War II. Gradually building its cooperation with the European Atomic Energy Community and the European Commission, it eventually grew to become the EU we know today. The EU operates on the premise that governments can also overstep and run wild, so when EU laws are passed, it is stipulated that independent, third-party supervisory authorities that have the power to enforce the law with respect to governments also be established. So the EU's privacy protection supervisory authorities strictly enforce the law with respect to privacy breaches not only over private-sector companies but also over governments and public agencies.

This difference in thinking means the US and the EU are basically incompatible in the world of privacy. But because they are each other's largest trading partner, people in the EU involved in the business of trade desire a good relationship with the US. Personal data is generally distributed as part of commercial activities and is thus inseparably linked with trade negotiations. In 2000, therefore, the EU created a framework called the EU-US Safe Harbor Principles, under which private-sector organizations were permitted to freely transfer personal data from the EU to the US provided they submitted a notification to the US Department of Commerce attesting that they had adequate security measures in place and will not pass personal data from the EU to third parties.

This collapsed in the wake of the Snowden expose. Snowden's revelations prompted doubt about the effectiveness of the Safe Harbor agreements in the mind of Austrian lawyer Max Schrems, who then filed a legal complaint in Ireland. The details are complex, but roughly speaking, under Facebook's Safe Harbor agreement, Facebook users' personal data was, for example, being transferred from Ireland (location of Facebook's EU headquarters) to the US. But as the Snowden expose revealed, the US government was able to freely view that data. This means, said the complaint, that Facebook is breaking the Safe Harbor agreement, and if the US government can legally spy on the services of private companies under US law, then the Safe Harbor agreement itself is pretty much meaningless in the first place. The Irish High Court, unable to make a decision, referred the matter to the Court of Justice of the EU (CJEU). In a shocking ruling, in October 2015 the CJEU declared the Safe Harbor Agreement invalid. This is known as the Schrems I decision. The inability to transfer personal data from the EU to the US represented an extreme impediment to trade, however, so economic proponents within the European Commission and the US Department of Commerce adopted a new special framework called Privacy Shield in August 2016. The Patriot Act, created after the 2001 terrorist attacks, expired in 2015, but the mechanisms for exposing terrorists arguably remained intact, albeit with increased transparency, under its successor, the Freedom Act. Privacy protection advocates within the European Commission claimed, therefore, that nothing had really changed, and debate about the validity of Privacy Shield thus continued to smolder on during and after 2017. Once the GDPR came into effect on May 25, 2018, Schrems immediately filed another suit claiming that it was illegal for US companies to transfer EU personal data to the US based on Privacy Shield. The case was settled in July 2020 with the ruling that Privacy Shield was also illegal. This is the Schrems II decision. Following Schrems II, the SCCs were also reviewed, and modernized SCCs were issued in June 2021.

The new SCCs provide extra protections that require companies and other bodies that transfer data to disclose information about access by public authorities in the destination country (whether the country has laws that allow the government requisition data and whether they are actually enforced).

Once personal data is transferred from one country to another, it is no longer protected by the origin country's laws, so various restrictions are thus imposed. Meanwhile, the EU does recognize a number of countries as offering adequately secure personal data protections. It refers to these as "adequate" countries (recognized by adequacy decisions), and they include Switzerland, New Zealand, and Argentina. Personal data can be transferred from the EU to these countries. Japan joined these ranks in January 2019. Japan's Personal Information Protection Act is not quite up to the GDPR standards, however, so personal data may only be transferred if certain supplementary rules are applied.

The Personal Information Protection Act is to be reviewed every three years to bring it up to speed with technological developments and other countries' laws and regulations, and thus it may approach parity with the GDPR going forward. On the other hand, Japanese personal data can also be transferred to the EU. As announced in January 2019, Japan and the EU reached a mutual agreement on the flow of personal data between each other's domains, and this means that Japan also recognizes the EU as having adequate protections. The only other place Japan recognizes in this manner is the UK. Given these developments, it does seem like the Japanese government's approach when it comes to protecting privacy is to strengthen individuals' rights and interests using the EU's GDPR as a reference.

Although the process is gradual, the revised Personal Information Protection Act, which was passed in June 2020 and will come into effect from April 1, 2022, also looks set to tighten Japan's protections and bring them closer in line with the GDPR. For instance, penalties will be raised from 300,000 yen and 500,000 yen to 100 million yen. Stronger information disclosure requirements will apply when personal data is provided to a third party in a foreign country (from the EU's perspective, this means when personal data is transferred out of its domain). Cookies will be subject to restrictions, although not quite to the extent as in the EU. And it will be mandatory to report personal data leaks that match certain patterns to the Personal Information Protection Commission and other bodies (preliminary report within 3–5 days and a final report within 30 or 60 days; incidentally, the GDPR mandates reporting within 72 hours).

Cultural background

In light of the above historical background, I see three major trends in personal data protection across the globe today.

One is a sort of public welfare idea that the sharing of big data will benefit people all over the world, which seems to be the mainstream view in the US. Another is the human rights assertion that says that the ability to manage your own personal data is a basic human right, which is the mainstream view in Europe. And then there is the security-oriented idea that the management of data within a country's own domain is its own national security issue, which is probably exemplified by China.

In the US, personal data is seen not only as holding convenience for the user but also as conveying benefits to a wide swath of other users, as exemplified by the rise of GAFA. This is evident from Google's mission, for instance,

which reads: "Our mission is to organise the world's information and make it universally accessible and useful." The history of American society is one of pioneering on the frontier, and this is possibly what embedded the idea of information sharing, including for the purposes of protecting national security, as an important part of its culture. In terms of its development strategy too, this seems to have led to a set of values that embrace the idea of de facto standards, the idea that prevalence itself is what makes a standard, something that has been a prominent factor in the Internet as well.

In Europe, on the other hand, personal data was at times something that could affect whether a person lived or died, so the ability of the subject of personal data to know and manage that data is seen as a right. Further, the development strategy is one of clarifying processes thought to have been developed as part of colonial policies, with standardization being pivotal to the global development of data protections.

In China, which exerts a significant influence on the world in recent times, the desire to maintain the nation is a crucial factor, and so naturally the thinking is that judgements about all sorts of information, including personal data, should be based on national security. Hence, China recommends its own country's services over those created in the US, and it imposes heavy restrictions on information flows between countries. And of course, the strategy is a nationalistic one: information flows involving China will take place under China's restrictions.

Of course, these are somewhat stereotypical characterizations. I think countries' information control strategies are carried out with an eye on any number of elements to do with the public interest, rights, and security, rather than emphasizing any single factor alone. But I think it's important to note that, broadly speaking, there are three major perspectives around personal data, each emerging from its own historical and cultural backdrop, and there is no unified mindset on personal data that applies across the entire world.

Closer to home in Japan (and while certainly not the mainstream world view), there is a culture of regarding information as being equivalent to value itself, a view that comes from the Japanese concept of kotodama, the belief that mystical powers dwell in words. So when it comes to personal data, people may feel that if someone knows information about you, they actually know you in some true sense. In older times, there was a cultural practice of hiding one's true name out of the belief that knowing someone's name would confer dominion over them. There is also a long-held idea that you should not utter unlucky thoughts (put misfortunes into words) because expressing information can somehow lead to the events it describes coming to pass (this is a deep rabbit hole to go down, so I will cut the discussion short here).

In any case, when it comes to personal data protection, this Japanese style of thinking, at least, is unlikely to pass muster elsewhere in terms of the mindset and meaning it implies and the weight of the belief. Of course, there is clearly no globally unified view, and this holds for the US mindset, the European mindset, and the Chinese mindset alike. In our information society, information is not just a set of symbols. There are historical and cultural backgrounds, and therefore each culture has its own principles, its own ideas about the right way to handle information, so when it comes to flows of information across national borders, there is a desire to ensure that the principles of each country or region involved are respected.

4.4 IIJ's Road to BCR Approval

IIJ was an early mover on BCR approval, but the process was full of twists and turns. The impact of Brexit in particular was significant, and the IIJ Group, which had aimed to obtain approval from the UKs ICO, did have to make a major strategic change along the way.

Table 1 provides a brief overview.

4.5 Looking Ahead

As discussed earlier, as the Internet spreads further, initiatives in personal data protection will no doubt continue to affect Internet-related companies and other companies in various ways. This process is a necessary part of the way society is adapting to facets of the information age, most notably the Internet, and even in Japan where attitudes can be indifferent, these changes are something that, sooner or later, we will be unable to ignore. Of course, even from my own experience, I cannot declare that every company should obtain BCR approval, but objectively speaking, there are many companies in Japan that do need it, and they will eventually be forced to take action of some sort.

Date	Organization	Action
Jan 2016	IIJ Europe	IIJ-EU receives CEO approval to start working toward GDPR compliance. Work begins in earnest.
Mar 2016	GDPR Office	Office set up by the Risk Management Office, Compliance Department, Global Business Division, and IIJ Europe.
Jun 2016	UK	Brexit prevails.
Jul 2016	GDPR Office	Decides on law firm.
Aug–Oct 2016	Risk Management Office	Creates BCR document.
Aug 2016	IIJ Europe	Starts GDPR compliance support consulting.
Oct 2016	GDPR Office	Submits BCRs to the Information Commissioner's Office (ICO), the UK's personal data protection authority.
Mar 2017	UK	Prime Minister signs a letter triggering Brexit.
Aug 2017	ICO	First communication that IIJ's BCRs are now under review. An ongoing process of revisions follows.
May 25, 2018	EU	GDPR comes into effect.
Jan 10, 2019	ICO	UK ICO's review is completed and submitted to the co-reviewers (Germany, Netherlands).
Feb 12, 2019	EDPB	Information on competent supervisory authorities post-Brexit is published. Appears we will not make it in time for Brexit.
Mar 1, 2019	LDI-NRW	Co-reviewer comments on IIJ's BCRs from the authority in NRW, Germany.
Mar 21, 2019	Dutch authority	Co-reviewer comments on IIJ's BCRs from the Dutch authority.
Mar 28, 2019	GDPR Office	Presents response to comments to ICO. Brexit deadline extended to Oct 31.
May 16, 2019	ICO	Co-reviewer provides notice that the review is complete. Pre-review by the EDPB ITES (International Transfers Experts Subgroup) meeting requested.
Jun 2019	UK	Prime Minister Theresa May resigns.
Jul 2019	UK	Boris Johnson becomes Prime Minister.
Jan 31, 2020	EU/UK	Britain withdraws from the EU. The transition period runs until end-2020.
Apr 2020	EDPB	Pre-review conducted by the EDPB ITES meeting under the ICO's guidance. Several rounds of revisions ensue.
Jun 2020	EDPB	Provides notice that ICO approvals made during the Brexit transition period are invalid.
Jul–Sep 2020	GDPR Office	The supervisory authority in NRW, Germany, where IIJ Deutschland is located, is appointed as the competent authority.
Sep 2020	GDPR Office	Formally requests the NRW authority to act as the competent authority.
Sep–Nov 2020	ICO/LDI-NRW	LDI-NRW takes over from ICO on IIJ's BCRs.
Dec 2, 2020	LDI-NRW	LDI-NRW officially becomes IIJ's competent authority.
Dec 31, 2020	UK	Completely withdraws from the EU.
Apr 2021	EDPB	Review at ITES meeting (review had progressed under ICO, so passage is smooth).
May 2021	GDPR Office	Creates a German-language version of the BCR document.
Jun 28, 2021	LDI-NRW	Submits BCR-C and BCR-P to the EDPB.
Jul 28, 2021	EDPB	Deliberates at a plenary meeting. All clear given.
Aug 2, 2021	EDPB	Discloses a positive official opinion on IIJ BCR-C/P.
Aug 5, 2021	LDI-NRW	IIJ BCR-C/P approved.

Table 1: IIJ's BCR Approval Process

The IIJ Group is also aware that it cannot rest on its laurels just because it has obtained BCR approval under the EU GDPR. We realize that, at the very least, we will also need to comply with the UK's requirements now that it is out of the EU, and that we will need to adhere with other personal data protection initiatives, including those in the US. The situation now is such that we could never keep up with all of the initiatives out there, but broad frameworks such as APEC CBPR, at least, are something we believe we should also look at complying with.

IIJ is also not immune to personal information breaches and other incidents, so I think we could be exposed to criticism along the lines of "look who's talking." But given the crucial role of personal information protection and other aspects of information security in our modern information society, I think there is a clear duty to address the issues in front of us. Organizations need to respond to the personal data protection and other practices found in different cultures while also enhancing their own information security capabilities.

Personal information protections and other information security measures are not something that can be thrown together overnight. They become meaningful only once they are established as part of organizational culture and everyday work practices. At the risk of being repetitive, obtaining BCR approval for IIJ was never our end goal. Our bigger objective was to use it as an opportunity to further bolster our internal controls around information security and privacy protection. We are proud to have taken a major, if not definitive, step toward that goal.

I think the IIJ Group's corporate mission can be described as the single-minded pursuit of business with the Internet at its core. Companies that specialize exclusively in global Internet infrastructure seem to have become rare these days. So, as a company that has helped drive the spread of the Internet, I think we have a responsibility to hold on to our Internet-centric perspective and continue making contributions as an infrastructure company for the information society age.

To be honest, IIJ BCR was a slog, and I honestly wouldn't recommend it to anyone. But I can say emphatically that I'm glad we did it because I believe it will be one key pillar supporting the type of Internet we envision.

Looking ahead, we will continue to strive for a safe and secure Internet.

Takamichi Miyoshi

Senior Fellow, DPO (Data Protection Officer), IIJ. Mr. Miyoshi joined Internet Initiative Planning Inc. (now Internet Initiative Japan Inc.) in April 1993. He worked on launching Internet services and the operation of service equipment/facilities. He later served in services development and strategic planning, going on to participate in numerous study groups set up by the Ministry of Internal Affairs and Communications and other agencies as Managing Director of IIJ. He has been in his current position since June 2015.