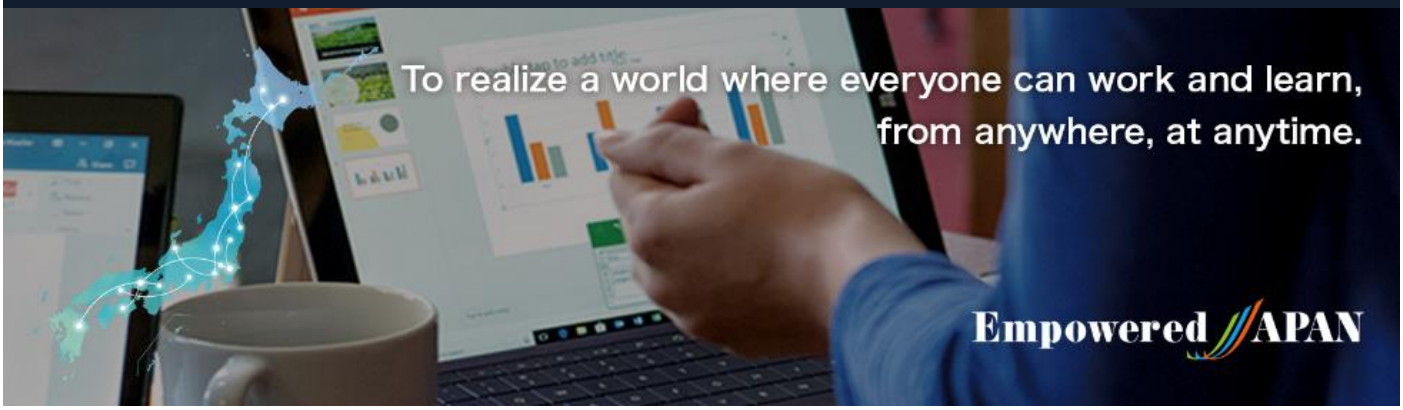
Empowered JAPAN Webinar Report



Empowered JAPAN Executive Steering Committee was established in 2018, “To realize a world where everyone can work and learn, from anywhere, at anytime.” To promote the true value of workstyle innovation including telework, the committee has been coordinating symposiums in both Tokyo and regional cities. And in collaboration with various local governments, Microsoft, and partners, the committee has been serving as an advisor to provide telework training for both corporate and individuals. In response to the spread of infection of corona virus (COVID-19) and the government announcement on February 25, 2020, which included the request to citizens to telework, the steering committee made the decision to launch a series of free webinars starting from March 17, 2020, to provide practical information for individuals and organizations across the nation, to telework and/or practice online education.

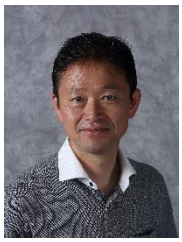
Category：IT tools and environment

Date：April, 16, 2020

Speaker：

Microsoft

Minoru Hanamura
Microsoft Corporation
Cybersecurity Solutions Group (CSG)
Chief Security Advisor



Mari Nakajima
Microsoft Japan
Corporate, External and Legal Affairs
Attorney

Privacy and Security of Microsoft Teams

With the swift advancement of teleworking, the use of online conference systems is also rapidly increasing. When using the systems, security and safety are as important as convenience. We will explain the security system efforts of "Microsoft Teams" that is one of the represented services.

Microsoft Corporation, which provides the service, has invested 100 billion yen each year for security measures, and employed 3,500 specialists from all over the world. According to Mr. Minoru Hanamura, who is one the specialists and resides in the U.S., information security has changed significantly over the last decade.

"In the past, the perimeter defense model, which protected important data by enclosing it in an internal trusted zone, was standard. However, it has limitations, and the company decided to use cloud." (Mr. Hanamura)

Using cloud makes it possible to consign a part of the security management responsibilities to cloud vendors. If you use an experienced vendor, you can eliminate the time spent on detecting and responding unauthorized accesses, as well as achieve efficient security measures.

The advancement of technologies made it possible to achieve both productivity and security, instead of choosing one or the other. With the advancement of technologies for security in biometric authentication, multi-factor authentication, conditional access, etc., an environment where work efficiency can be improved while safety is ensured, has become achievable.

Another major change is that the concept of security has shifted to assume defeat instead of defense. "Our attitude towards security was changed to challenge with resilience (quick recovery) on the assumption that security would be compromised regardless, instead of building iron walls. Meanwhile, the safety of each Microsoft service is progressing day and night." (Mr. Hanamura)

Empowered JAPAN Webinar Report

What kind of security measures are taken for the online meeting system Microsoft Teams, which is a popular tool for teleworking?

First, the product is designed with measures to protect data from being leaked in multiple stages. Teams has thorough countermeasures to block uninvited guests by setting the [Wait in lobby] option for guests outside your organization, prevent attacks from unauthorized access by multi-factor authentication, etc. Meeting and chat contents are all recorded and encrypted, and a certain control can be applied to internal data when sharing it with a participant outside the organization. Furthermore, Teams has AI that patrols chats and a function to prevent harassment. These measures comply with and are approved by more than 90 international regulatory standards and laws, and "aiming to achieve an environment which can guarantee the same level of safety as working at a company wherever you are." (Mr. Hanamura)

Now, how compliances including emergency measures are regulated? Ms. Mari Nakajima, who is a lawyer supporting companies using Microsoft products from a legal perspective at Microsoft Japan, explains using an overview.

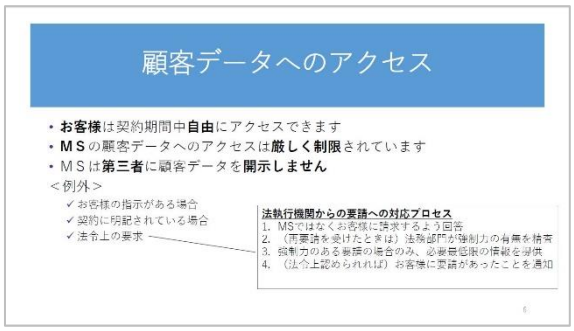
"Protecting clients' data is our top priority. Based on this policy, products and services are designed." (Ms. Nakajima)

One of the company's efforts is to explicitly express the stance that data belongs to the client. It is regulated that all clients have the right to their data related to meeting records, chats, etc. conducted with Microsoft Teams.

The purpose of using the client data (providing cloud service features, troubleshooting, etc.) is clearly stated in the contract, and using for other purposes including advertising is strictly prohibited.

Access from Microsoft is also strictly restricted, except when requested by the client, etc. "In that case, when and how data is accessed will be recorded, and the client can monitor it anytime." (Ms. Nakajima) A list of subcontractors involved in providing the service is also available online.

The company thoroughly complies with the policy "not disclosing information to third parties," except when instructed by the client or for a legal matter. When the police of judicial authorities legally make a request, first, the company suggests contacting the client directly. If they request again, the company verifies that they can legally force Microsoft. Only when they have legal force, the company provides the minimum amount of information, and notifies the client unless prohibited by law. Microsoft publishes a status and number of the actual cases, and makes efforts to disclose transparent information. "In the first half of 2019, we received 74 requests to disclose the clients' data worldwide and of those, 32 requests were replied with non-disclosure." (Ms. Nakajima)



The procedure for data deletion after the end of the contract is also clearly regulated. For 90 days after the contract ends, data is retained in an account with limited functions for allowing the client to extract data, however, after 90 days, the functions will be frozen. Data will be completely deleted within 180 days after the contract ends.

For more information on the above initiatives and related materials, see the Trust Center in the Microsoft website. You can also view general information including the laws and regulations for each country, etc.