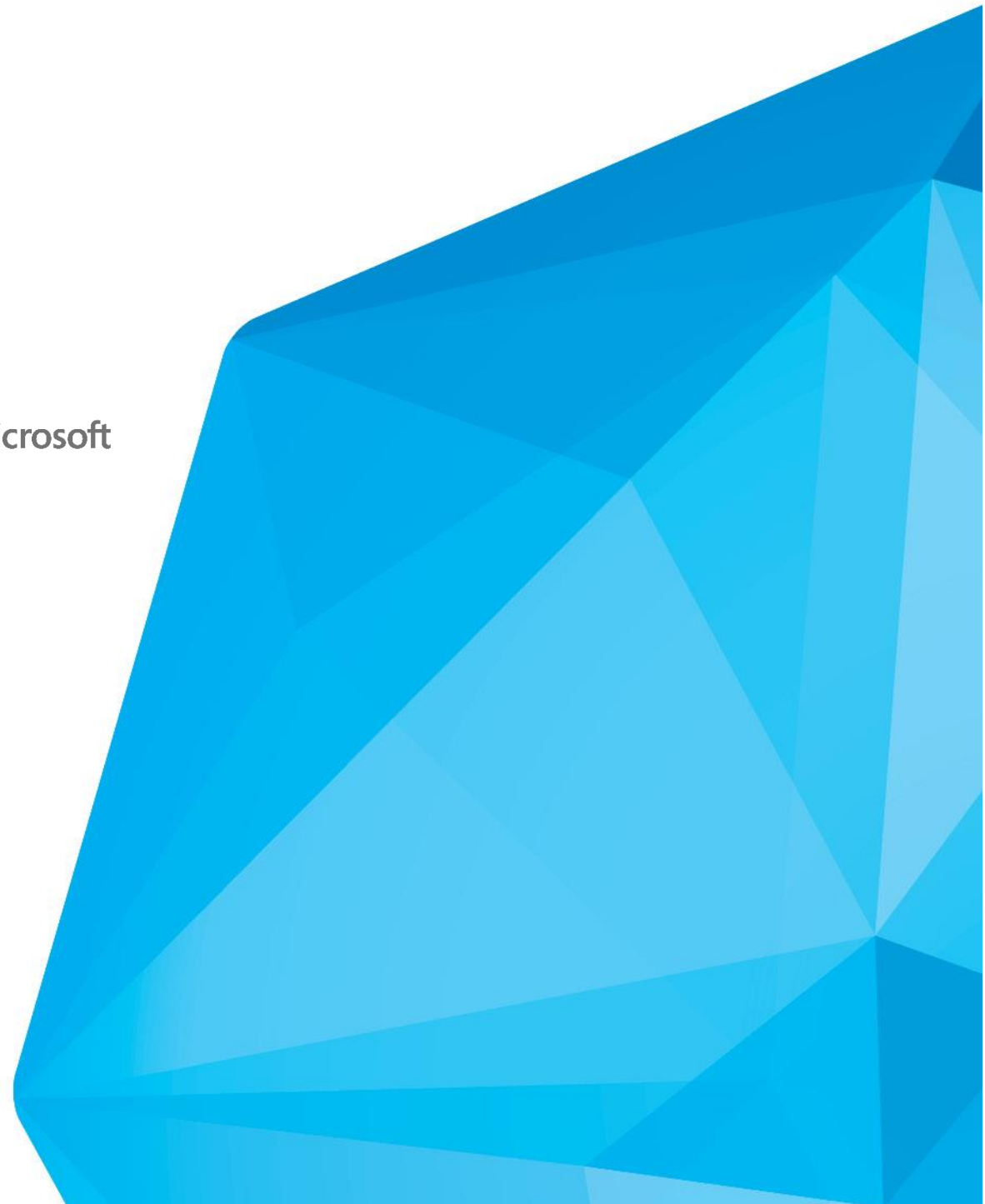
Microsoft Azure Compliance

In the context of Japan Security and Privacy Requirements



Disclaimer

October 2017

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.

This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.

The information contained in this document must not be construed as legal advice. Customers must seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.

Audience

This white paper is intended for IT decision makers in Japan, and provides them with information about how Microsoft Azure addresses their country's compliance, security, and privacy requirements.

Authors

Frank Simorjay
Eric Tierling
Peter Foote (Cadence Preferred)

Contributors and Reviewers

Arisa Hirashima
Katie Jackson
Stevan Vidich
Katie Look

Executive Summary

Microsoft Azure is a trusted cloud-based platform that provides Microsoft customers with the ability to realize the benefits of cloud computing. This white paper addresses questions posed by customers in Japan who are considering a move to the cloud. Questions about the security of cloud data, where data is stored, how it is used, and who can access it are common. These types of questions usually relate to one of three areas – compliance, privacy, and security.

For customers who are concerned about compliance in Japan, there are no laws that prevent the use of cloud computing. However, there are questions that are raised by customers about how some recent Japanese legislation would apply to the use of cloud computing. Regarding the Act on the Protection of Personal Information (APPI), recently enforced from 30 May 2017, and the My Number Act, enforced from January 2016, there is guidance provided by the government on the use of cloud computing. With regard to concerns on security, Azure meets the Cloud Security Mark (Gold) standard, the first Japanese security accreditation for cloud service providers (CSPs), and the Center for Financial Industry Information Systems (FISC) Security Standard v8, a set of security policies and standards used by major financial institutions in Japan. This support means customers can have confidence knowing they comply with Japanese legislative and certification requirements when deploying data to the cloud.

With the global nature of the cloud, customers want to know their privacy is assured. Microsoft Azure sets and adheres to stringent privacy standards such as ISO/IEC 27018, which, among other things, assures customer data is never used for advertising. Should customers have concerns over data sovereignty, Azure provides complete control over where their data lives by allowing them to choose from 34 Azure regions (as of the time of this publication) in Asia, the Americas, and Europe. In addition, Microsoft does not provide any third party with direct or unfettered access to customer data, and always attempts to redirect government requests for data to the customer. Finally, tenant isolation and strict access controls help ensure that, by default, only customers can access their data.

Security is increasingly a primary focus for customers when contemplating the cloud. Microsoft Azure provides multiple levels of security, starting with physical protection of datacenter locations to protect against physical intrusion, power failure, and network outages. Azure uses encryption to protect data in transit and at rest, and extensive monitoring and logging provides operational staff and customers with visibility into the environment. Microsoft designs and operates Azure using security best practices, which are embodied in programs such as the Microsoft Security Development Lifecycle (SDL), Microsoft Operational Security Assurance (OSA), and an "assume breach" strategy. Together, these programs and strategies help ensure that Azure is resilient to attack. Microsoft has received ISO/IEC 27001 security certification, which validates the benefits of this approach.

Although Microsoft Azure addresses the compliance, privacy, and security requirements that Japan identifies, some requirements are the responsibility of the customer, such as controlling administrator passwords, and it is important for customers to understand the shared responsibilities associated with Microsoft Azure.

Table of Contents

Introduction

This paper is written for IT decision makers in Japan who are considering whether to move their data to Microsoft Azure, and answers several typical questions:

- Does Microsoft Azure meet Japanese compliance requirements?
- Where is data stored and who can access it?
- What is Microsoft doing to protect data?
- How can a customer verify that Microsoft is doing what it says?

The content is divided into three main sections:

- *Japanese compliance requirements*. This section focuses on how Azure meets legislative and certification requirements.
- *Key privacy principles*. This section provides technical information on how Azure addresses key privacy principles for customers located in Japan, such as data location and government requests.
- *Key security principles*. This section provides technical information on how Azure addresses key security principles for customers located in Japan, such as encryption and security best practices.

Understanding how Azure shares responsibility with customers to meet Japanese security and privacy requirements is an important step toward moving data to the cloud.

Shared responsibilities between Microsoft and customers

When moving data to the cloud, it is important to remember that some security and privacy requirements are the responsibility of the customer, some are shared, and some are the responsibility of the cloud service provider (CSP). Read the Shared responsibility in cloud computing white paper to learn more about the responsibility for each cloud-based solution.

1. Japanese compliance requirements

As part of its declaration in 2013 to be "the world's most advanced IT nation," the Japanese government strongly endorsed cloud computing with comments like "*Going forward, the ability to obtain government services electronically will be the norm, and comprehensive utilization of cloud computing will make possible the creation of convenient lifestyles where anyone can obtain one-stop electronic government services from anywhere, at any time, using any type of terminal.*"[1] Since then, Japan has progressed to be one of the most advanced markets for technology adoption in the Asia-Pacific region, and indeed the world.

More recently, Japan has continued this tradition of using the latest technology solutions as part of its Tokyo 2020 Olympic Games. In the Games Foundation Plan for Technology, it states that part of the mission is to "showcase Japanese innovation beyond 2020 by developing cutting-edge technology for the Games."[2]

[1] Declaration to be the World's Most Advanced IT Nation, p24.
[2] Tokyo 2020 Games Foundation Plan February 2015, p125.

The remainder of this section provides details about how Microsoft Azure addresses Japan's legislative and certification requirements for cloud computing.

Act on the Protection of Personal Information (APPI)

In 2003, the Japanese government passed the Personal Information Protection Act (PIPA) (Japanese) to ensure the protection of personal information of its citizens. Since then, the IT landscape has changed significantly, including a more pervasive use of computing in everyday life, the growth of big data, and a greater adoption of cloud computing, resulting in cross-border data transfers. To address the need to use personal data for business while protecting privacy, the Japanese government released an amendment to the PIPA, titled "The Act on the Protection of Personal Information" (APPI) (Japanese, English). Enforced from 30 May 2017, it addresses several areas including:

- The establishment of the Personal Information Protection Commission (PPC)
- A clearer definition of personal information
- Restrictions on personal data transfer to a third party in a foreign state[3]

Microsoft Azure compliance for APPI

Although APPI provides specific obligations where data is transferred to a third party, these obligations do not apply if the third party does not "handle" personal data. The Q&A document issued by the Personal Information Protection Commission provides that it is not construed as "handling" personal data if (i) the third party stipulates in the agreement that it does not "handle" personal data, and (ii) it establishes a proper access control system.[4]

Microsoft Azure meets these requirements because Microsoft provides in its Online Services Terms (OST) that (i) the customer, not Microsoft, owns the customer data, (ii) Microsoft commits to only use the data for the purpose of providing the services to the customer, not for any advertising or similar commercial purposes, and (iii) Microsoft Azure has robust access control systems in place, as per the "Key security principles" section later in this paper.

Consequently, Microsoft Azure does not conflict with the APPI and does not cause any additional obligation under the APPI on customers, such as a consent from an individual owner of personal data.

My Number Act

The My Number Act[6] was enforced from January 2016. It assigns a unique 12-digit number — called the Social Benefits and Tax Number, Individual Number, or My Number — to every

[3] Outline of the amended Personal Information Protection Act p3.
[4] Q&A on the Guidelines concerning the Act on Protection of Personal Information (Japanese).
[6] The "My Number" Act is officially called the "Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure" (Japanese, English).

resident of Japan, whether Japanese or foreign. More information can be found at the Japan Government Cabinet Office website (Japanese, English).

The Personal Information Protection Commission (PPC) has issued "My Number guidelines" (Japanese) and "Q&A" (Japanese) to ensure that organizations properly handle and adequately protect My Number data as required by law.

Microsoft Azure compliance for My Number

The same analysis outlined in the "Microsoft Azure Compliance for APPI" section applies to Microsoft Azure compliance for My Number.[7] Therefore, Microsoft Azure does not conflict with the My Number Act and does not cause any additional obligation under the My Number Act on customers, such as a consent from an individual My Number owner.

Cloud Security Mark (CS Mark Gold)

The Cloud Security Mark is the first Japanese security standard to validate cloud service providers (CSPs), and is based on ISO/IEC 27017, an international code of practice for information security controls. CS Mark is maintained by the Japan Information Security Audit Association (JASA), a nonprofit organization established by the Ministry of the Interior and the Ministry of Economy, Trade, and Industry. CS Mark audits includes approximately 1,500 controls covering areas such as information security management, physical and development security, personnel security, business continuity, disaster recovery, and incident management. More information about the CS Mark standard can be found at the JASA website (Japanese).

Microsoft Azure compliance for CS Mark

In December 2015, Microsoft received a 3 year, CS Mark Gold accreditation (Japanese) for Azure infrastructure as a service (IaaS), Azure platform as a service (PaaS), and Office 365 software as a service (SaaS), making it the first global CSP to receive this accreditation across all three classifications. More information about Azure compliance for CS Mark can be found at the Microsoft Trust Center.

Center for Financial Industry Information Systems (FISC)

The finance industry has some of the strictest security standards in Japan. In collaboration with the Bank of Japan, the Financial Services Agency, and Japanese member corporations, the Center for Financial Industry Information Systems (FISC) established guidelines for the security of banking information systems. The latest guidelines, FISC Security Guidelines v8 (Japanese), were released in 2015 and audit more than 300 controls covering computer systems, contingency planning, security policies, and standards.

Microsoft Azure compliance for FISC

Although the application of these guidelines in a cloud computing environment is not required

[7] My Number Q&A Q3-12 (Japanese) and Q3-13 (Japanese).

by regulation, most financial institutions in Japan that implement cloud services have built information systems that satisfy these security standards, and it can be very difficult to justify diverging from them. Therefore, Microsoft has used outside assessors to validate that Azure meets FISC version 8 requirements. Banking and non-banking customers can have confidence using Azure knowing that it complies with some of the strictest security controls in Japan. More information about Azure compliance for FISC can be found at the Microsoft Trust Center.

2. Key privacy principles

This section provides technical information about how Azure addresses key privacy principles for customers located in Japan, such as data location and government requests.

Microsoft does not use customer data for advertising

Microsoft takes privacy very seriously and never uses enterprise customer data for marketing or advertising purposes. This policy is written into Microsoft Online Services Terms and affirmed by Azure certification to international privacy standard ISO/IEC 27018. Microsoft was the first major cloud service provider to incorporate the ISO/IEC 27018 privacy code of practice. Additional information is available in this 5-minute video: Privacy interview with Brendon Lynch, Microsoft Chief Privacy Officer.

Azure provides logical tenant isolation

Microsoft logically segregates storage and processing for different customers through specialized technology engineered to help ensure that customer data is not combined with anyone else's data, and to help prevent one malicious or compromised customer from affecting the service or data of another. Microsoft also takes strong measures to protect customer data from inappropriate use, access, or loss. Additional safeguards include proper controls for administrative access, such as secure user authentication.

For customers with an existing Azure subscription, additional information about tenant isolation is available in the "Office 365 Tenant Isolation" white paper, located on the Service Trust Portal (STP) and available both in English and Japanese. The STP offers access to a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft Azure, risk assessments, security best practices, and other similar materials.

Microsoft has transparent data-use policies and uses independent audits

The Microsoft Online Services Privacy Statement uses straightforward, transparent language to provide clarity around Microsoft data-use policies. Azure also undergoes independent audits against international standards such as ISO/IEC 27001, ISO/IEC 27018, and CSA CCM 3.0.1, so customers can have confidence that Microsoft is honoring its commitments. Additional compliance reports are available on the Service Trust Portal.

Customers choose the region where their data lives

Customers have complete control over where their data is stored because they choose which

region best meets their compliance needs. Currently, there are 34 Azure regions, including:

- *Asia*: Japan (Osaka, Tokyo), Korea (Seoul, Busan), Singapore, Hong Kong, China (Shanghai, Beijing), India (Pune, Chennai, Mumbai), and Australia (New South Wales, Victoria).
- *Americas*: United States (California, Illinois, Iowa, Texas, Virginia x 2, Washington, Wyoming), United States Government (Iowa, Virginia), United States Department of Defense (Central, East), Canada (Toronto, Quebec), and Brazil (Sao Paulo state).
- *Europe*: Ireland, Netherlands, Germany (Frankfurt, Magdeburg), United Kingdom (London, Cardiff).

In addition, Microsoft has announced another 6 Azure regions, specifically:

- US Government (Arizona, Texas), France (two regions – to be announced), South Africa (Cape Town, Johannesburg).

Additional information is available on the Azure Regions webpage.

Customers control access to their data

Microsoft has provided a self-service model for customers to access and manage their data. When Microsoft engineers or subcontractors need access to customer data, such as when troubleshooting an issue, they must be explicitly granted access by the customer, and access is revoked when it is no longer necessary. The operational processes and controls that govern access to and use of customer data are protected by strong controls and authentication, such as multi-factor authentication, which helps limit data access to authorized personnel only.

Customers may extract their data upon termination of their subscription

If a customer chooses to end a subscription to a service, they are given 90 days to extract their data, after which Microsoft follows stringent standards in purging customer data from systems under its control.

How Microsoft responds to government requests

Microsoft does not provide any third party (including law enforcement, other government entity, or civil litigant) with direct or unfettered access to customer data except as directed by the customer. When a government or law enforcement request for customer data is received, Microsoft policy is as follows:

- Always attempt to redirect the third party to obtain the requested data from the customer. For valid requests that cannot be redirected to the customer, Microsoft discloses information only when legally compelled to do so, and only to the extent specified in the legal order.
- Promptly notify customers of any third-party request and provide a copy, unless legally prohibited from doing so.

Microsoft never provides any government with its encryption keys or the ability to break its encryption. Additional information is available on the Microsoft Transparency Hub and Principles, Policies and Practices FAQ webpages.

Microsoft sets and adheres to stringent privacy standards

Microsoft cloud privacy is grounded in the Microsoft Privacy Standard (which details Microsoft core privacy requirements and practices) and the Microsoft Security Development Lifecycle (which addresses privacy requirements in the process of developing software). Microsoft backs those protections with strong contractual commitments to safeguard customer data. Additional information is available in this 5-minute video: Interview with Brad Smith, General Counsel, Microsoft: Security & Privacy in the Cloud.

3. Key security principles

This section provides technical information about how Azure addresses key security principles for customers located in Japan, such as encryption and security best practices.

Azure provides encryption for data in transit and data at rest

Microsoft Azure provides capabilities to help protect data both in transit and at rest. For data in transit, Azure uses the Transport Layer Security (TLS) protocol to encrypt connections between customer and Microsoft datacenters. TLS provides strong authentication, message privacy, integrity (by enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, ease of deployment, and ease of use. Perfect Forward Secrecy is also used so that each connection between client systems and Azure uses unique keys. In addition, Azure Virtual Networks provide the ability to use the industry-standard IPsec protocol to encrypt traffic between corporate VPN gateways and Azure, as well as between the virtual machines (VMs) located on virtual networks.

For data at rest, customers have a number of encryption options available to them, such as hard disk encryption for Windows VMs using BitLocker, and SQL database encryption using Transparent Data Encryption. Azure implements encryption using strong symmetric and asymmetric keys for encrypting and protecting confidentiality of data:

- Software-based AES-256 for symmetric encryption/decryption
- 2048-bit or better for asymmetric keys
- SHA-256 or better for secure hashing

Additional information is available in the Data Protection in Azure white paper (39 pages) and the Is your data safe at rest? video (5 mins).

Microsoft designs and operates Azure using security best practices

From the start, Microsoft designed Azure with security in mind. By taking advantage of the Microsoft Security Development Lifecycle (SDL) during the Azure development process, security concepts such as attack surface reduction and threat modeling are built into the service. From an operations perspective, Microsoft Operational Security Assurance, the "assume breach" strategy, and a global incident-response presence help ensure the Azure infrastructure is resilient to attack.

Vulnerabilities present a significant risk to any information system, particularly those that are

exposed to the Internet. One of the initial steps to reducing risk is to understand threats, exploits, and vulnerabilities that target a region. The Microsoft Security Intelligence Report provides intelligence for 106 regions including Japan that can be used to better understand regional risk and exploits used by malicious entities. It is also important for customers to understand that when using Microsoft Azure they must ensure that the IaaS services they use are patched in a timely manner. Improved patch and vulnerability management is often cited as one of the main benefits of moving to the cloud.

Azure provides infrastructure protection

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all. Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft online services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards such as ISO/IEC 27001 for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Third parties undergo a review process and an approved vendor list is established and used. These vendors are required to comply with Microsoft security policies and are audited for compliance.

Azure uses an "assume breach" strategy

One key operational best practice that Microsoft uses to harden Microsoft Azure is known as the "assume breach" strategy. A dedicated team of software security experts simulate real-world attacks at the network, platform, and application layers, testing the ability of Azure to detect, protect against, and recover from breaches. Microsoft has also established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure. Constantly challenging the security capabilities of the service can help Microsoft stay ahead of emerging threats.

Customers can take advantage of datacenter redundancy

Customers may opt for in-country storage for compliance or latency considerations, or out-of-country storage for security or disaster recovery purposes. Data may be replicated within selected geographic regions for redundancy. Microsoft recommends replication of workloads across Azure regional pairs to benefit from Azure's isolation and availability policies.

Customers have visibility of their data through monitoring and logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Customers can protect their networks

Management workstations and external or less-trusted interfaces of a service should be

identified and have appropriate protections to defend against attacks through them. If an interface is exposed to consumers or outsiders and is not sufficiently robust, it could be subverted by attackers to gain access to the service or data within it. If the exposed interfaces include private interfaces (such as management interfaces), the impact may be more significant.

Conclusion

Microsoft strives to be transparent in its compliance, security, and privacy practices. In addition, Microsoft offers meaningful privacy choices and responsibly manages the data that it stores and processes. The Microsoft commitment to security and privacy of customer data is backed by the Microsoft Online Services Privacy Statement, which describes the specific privacy policy and practices involving customer data in Microsoft enterprise cloud services.

For customers who are concerned about compliance, the use of Microsoft Azure does not conflict with Japanese legislation, including the Act on the Protection of Personal Information (APPI) and My Number Act. In addition, it meets the Cloud Security Mark (Gold) standard, and the Center for Financial Industry Information Systems (FISC) Security Standard v8. This support means customers can have confidence knowing they comply with Japanese legislative and certification requirements when deploying data to the cloud.

Microsoft believes that Azure can provide secure and compliant cloud services to meet the needs of government and commercial customers of all sizes.