Building High-quality Social Communication Networks

Highly Convenient, Stable, and Trustworthy Networks and Security

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE | 11 SUSTAINABLE CITIES AND COMMUNITIES | 13 CLIMATE ACTION | 16 PEACE, JUSTICE AND STRONG INSTITUTIONS

Communication networks are essential lifelines for society. Based on these networks, SoftBank Corp. consistently provides the latest high-quality services to ensure stable connectivity to highly reliable information and communication services at all times.

To provide better service, we are advancing the nationwide rollout of 5G, which started service in March 2020. We are also developing non-terrestrial networks (NTN solutions), most notably stratosphere-based high-altitude platform stations (HAPS). NTN solutions provide communications networks from space and the stratosphere so that anyone, anywhere can connect.

To maintain our communications infrastructure in the event of a disaster, we strive to be well prepared and reinforce disaster prevention and mitigation initiatives. We are strengthening initiatives to maintain lifelines in order to provide stable communication services under any circumstances.

Furthermore, as cyberattacks—including attacks on supply chains and on remote work environments resulting from workstyle reforms—grow increasingly sophisticated and complex, we constantly monitor the ways they are changing and proactively use cutting-edge technologies to guard against them. In addition to maintaining sophisticated security environments, we are working to further enhance our systems for 24/7 security monitoring and implementing immediate response. We also carry out training to instill a strong awareness of security in all employees. As for the handling of customer data, we have launched a Privacy Center website that provides a dashboard by which customers can check and manage how their information is used, putting customer privacy first.

SoftBank Corp. will create new value and contribute to the creation of sustainable communities and industrial development by combining 5G and networks with cutting-edge technologies and wide-ranging customer contact points.

Social Issues

- Maintenance and management of high quality networks
- Prevention and rapid restoration of infrastructure disruption by natural disasters
- Response to sophisticated cyberattacks

Value Creation

(1) Prepare sustainable life infrastructure
(2) Construct robust communications infrastructure to contribute to disaster prevention and mitigation
(3) Promote data security and privacy protection initiatives

Risks and Opportunities

Risks

- Loss of new business opportunities requiring 5G with ultra-high-speed, large-capacity, ultra-low latency and massive device connectivity
- Increasing response costs, deterioration of customer trust or loss of subscribers due to network outages or delays in disaster recovery
- Deterioration of customer trust or loss of subscribers due to the improper use or leakage of personal information

Opportunities

- Increased ARPU and revenue reflecting communications speed and capacity increases, through the nationwide expansion of 5G coverage
- Development of new industries and services that use 5G, such as automated driving and telemedicine
- Increased customer satisfaction through high communications quality and dependable security

KPIs

(1)
- 5G deployment plan: Expansion of 5G standalone (SA) coverage: Smartphone SA in key areas of all prefectures (FY2026)
- Number of major network accidents: Zero
- High-capacity optical submarine cable: Start of operation (FY2023)

(2)
- Tohoku Route: Commercial operation start (end of FY2023)
- Maintain and enhance equipment and materials for disaster response and recovery: Maintain at least 200 mobile base station vehicles/portable mobile base stations; maintain at least 80 mobile power supply vehicles; maintain at least 200 portable satellite antennas; strengthen cooperation with external organizations involved in disaster recovery

(3)
- Number of major accidents involving information security: Zero (annually)
- Number of major accidents involving privacy issues: Zero (annually)
- Helping customers understand how their personal information is handled: Addition of a privacy dashboard setting function; disclosure of information handling of application/website usage details

Main Businesses and Initiatives

- Broad rollout and quality enhancement of 5G
- Participate in submarine cable projects
- Eliminate regional communications disparities by expanding networks
- Advance initiatives to prevent network accidents
- Support network monitoring and operation with AI
- Secure communications service environments in the event of a disaster (using mobile base stations, portable satellite antennas, drones, etc.)
- Build frameworks for quickly restoring communications environments after disasters
- Disaster recovery countermeasures, including creating three-route backbone networks
- Operation and management using advanced security systems and tools
- Promote the protection and appropriate use of personal information
- Thoroughly educate employees and build secure environments and facilities

Building High-quality Social Communication Networks

Key Person Interview

Hideyuki Tsukuda

Executive Vice President & CTO

Offering New Services with Progress in 5G Technology

Under our "Beyond Carrier" strategy, we are working to further reinforce the foundations of our communications business while using the latest technologies to promote the digital transformation (DX) of industry and help solve social issues. We launched nationwide commercial 5G service in March 2020, followed by 5G standalone ("5G SA") commercial service in October 2021. By doing so, we have realized ultra-high speed, large-capacity, ultra-low latency and massive device connectivity not previously feasible. Beginning in March 2023, we now also offer private 5G, enabling network slicing and network services customized to the needs of companies.

Going forward, by expanding 5G SA and offering private 5G (shared type and dedicated type) to meet even more industry needs, we will realize a wide range of unprecedented services.

Disaster Readiness and Creating Safe and Reliable Communications Environments

SoftBank Corp. regards communications infrastructure as a vital lifeline. In recent years, fueled by climate change, major natural disasters have been occurring frequently around the world. We are implementing numerous measures to minimize the impact on communications services when disaster strikes, such as deploying tethered balloon radio relay systems, wired power feed drone wireless relay systems, mobile base station vehicles and mobile power supply vehicles. Through such efforts to ensure network redundancy and deal with power outages, we strive to provide stable communications services.

We also prioritize the reinforcement of information security and customer privacy protection. To strengthen information security, we use cutting-edge security systems to guard against increasingly sophisticated cyberattacks. To protect customer privacy, we conduct training for employees and provide a dashboard via our Privacy Center website that enables customers to check and change their privacy settings so that their personal data is not used in unwanted ways.

Building a Ubiquitous Network with NTN Solutions

SoftBank is aiming to expand its communications network coverage both on land and into the sky through a ubiquitous network (multi-layered network) that combines existing terrestrial mobile networks with satellites (low Earth orbit and geostationary) and stratosphere-based high-altitude platform stations (HAPS). As all companies and industries around the world are increasingly required to digitally transform and automate, connectivity needs are expected to further diversify. In collaboration with partner companies, SoftBank Corp. aims to contribute to society by creating a ubiquitous network that allows various communication methods all around the world to seamlessly connect.

Working to Offer Next-generation Infrastructure

SoftBank Corp. is working to evolve its existing communications infrastructure to provide next-generation infrastructure that will help realize the society of the future. Data centers in Japan are currently concentrated in urban areas and, consequently, so is data processing and the requisite power consumption. By building data centers around the country, we can better distribute data processing and power use, enabling the use of locally produced power and thereby solving this structural issue. Going forward, in addition to continuing to provide stable communication networks, we seek to continuously create new value using cutting-edge technologies to help solve social issues across a diverse range of fields.

Value Creation 1 Prepare Sustainable Life Infrastructure

By maintaining safe and resilient infrastructure centered on the 5G network and protected by advanced security, SoftBank Corp. provides convenient and reliable communications services. As the foundation connecting people, goods and information, our networks support social and economic activity. Aiming to further evolve this infrastructure, we will continue to advance technological development to solve issues and help provide new value.

Initiatives for the Rapid Deployment of 5G Networks

SoftBank Corp. has been accelerating its development of 5G base stations. We are advancing a variety of research and other initiatives aimed at utilizing the full potential of 5G technologies, such as developing services that leverage its high speed and large capacity, as well as fundamental research related to ultra-high reliability, low latency and massive device connectivity.

Forms of 5G Use

In addition to public 5G—the service generally referred to by "5G"—forms of 5G use include local 5G, in which private 5G networks are individually set up, and private 5G, which entails the exclusive use of a part of public 5G service. Furthermore, there are two types of private 5G, namely the shared type, in which the 5G environment is shared with public 5G, and the dedicated type, in which the 5G environment is set up and operated on the customer's premises.

On March 29, 2023, SoftBank Corp. launched its Private 5G service for enterprises. SoftBank's Private 5G is a shared-type managed service that can be customized based on the needs of specific companies, local governments and other organizations.

Local 5G and Public 5G

Local 5G refers to private 5G networks built by companies other than telecommunications carriers or municipalities specifically for use in a certain area, building or facility. Compared with public 5G, local 5G networks are less likely to be affected by communications problems in other areas or network congestion.

Private 5G, meanwhile, is like local 5G in that it entails building individual networks for companies and municipalities. However, entities using Private 5G will not have to go through the burdensome process of obtaining a radio license, as with normal local 5G. Instead, SoftBank Corp., as a telecommunications carrier, will install network infrastructure tailored to the project's requirements at base stations on the grounds of the company or municipality and handle maintenance and operations. In this way, Private 5G will offer the advantages of creating individually optimized 5G networks with less hassle.

Private 5G is expected to advance the use of 5G even by companies that previously had to forgo using local 5G due to the hassle or cost. In the "new normal" era, needs for technologies that allow work to proceed without human operators being onsite, such as remote control and automation, are growing. The use of 5G in this area and in remote work will enable smoother, more efficient business operations.

As we enter the full-fledged digital era, 5G is expected to play a major role in advancing digital transformation (DX). By offering 5G services tailored to customer businesses and needs, we will help customers increase their efficiency and competitiveness, thereby contributing to sustainable social development.

Public 5G Telecommunications carrier's licensed spectrum	Private 5G (Shared type) Telecommunications carrier's licensed spectrum	Private 5G (Dedicated type) Telecommunications carrier's licensed spectrum	Local 5G Local 5G spectrum
Telecommunications carriers operating 5G environments nationwide	Operated by sharing the 5G environment with public 5G	Set up and operated by SoftBank on customer premises	Companies and local governments individually build 5G environments
Setup/operation: SoftBank Installation: Nationwide	Setup/operation: SoftBank Installation: Nationwide	Setup/operation: SoftBank Installation: On customer premises	Setup/operation: Customers Installation: On customer premises

Building High-quality Social Communication Networks

Value Creation 1 Prepare Sustainable Life Infrastructure

Providing Stable Telecommunications Services

Telecommunications networks are the basis of information and communication services. In order to stably operate these networks, SoftBank Corp. stations technicians at network centers nationwide to maintain wireless base stations, mobile phone transmission lines and equipment within the network centers. The operating status of telecommunication networks and wireless base stations is monitored 24 hours a day, 365 days a year by expert engineers at the Network Operations Center.

We hold Maintenance Pro Contests every year to promote the horizontal roll-out to other divisions of operational improvement measures implemented at our nationwide network centers and the Network Operations Center, aiming to improve the reliability and efficiency of operations. In addition, we are certified by international standards such as those for Integrated Management Systems, Quality Management Systems, and IT Services Management Systems. We have established a system for continuous operational improvements to maintain and enhance the quality of our services.

In FY2022, there were no serious network accidents that fall under Article 57 of the Ordinance for Enforcement of the Telecommunications Business Act.

Building Safe Base Stations

As part of our ongoing safety management and accident prevention activities, we hold an annual national safety convention with relevant construction companies. In 2022, we held the event in the metaverse for the first time. To ensure safety, we conducted safety “pulse” surveys, held accident prevention study groups, monitored construction companies, and shared examples of safe and unsafe practices by distributing hazard prediction support booklets. We also held safety awards to commend the stable operations and robust safety management know-how of business partners that have maintained long accident-free records.

To safely complete the major project of building the 5G network, we continue to reinforce on-site safety patrols and thoroughly educate construction staff. In addition, we provide messaging about heightening safety awareness and implementing safety awareness initiatives aimed at eliminating accidents.

National safety convention in the metaverse

Radio Wave Safety

Providing Information Regarding Radio Wave Safety

Radio waves are used in a wide range of fields. In addition to mobile phone service, these include emergency wireless systems, satellite broadcasting, navigation systems, wireless LAN networks and IoT devices. Indeed, radio waves are used in innumerable ways that are essential to everyday life.

SoftBank Corp. studies the effects of radio waves on human health and published information about the safety of radio waves so that customers who are worried about the impacts of electrical waves from base stations and mobile phones can use their mobile phones and smartphones with peace of mind.

Policy Regarding Radio Wave Safety

To prevent negative health effects, the strength of radio waves emitted by base stations and mobile phones is regulated by Japan’s Radio Act and other laws and regulations. Enterprises that use radio waves, including SoftBank Corp., adhere to these laws and regulations.

Specifically, SoftBank Corp. provides services in line with its Policy Regarding Radio Wave Safety and Topical Absorption Policy for Mobile Phones and Other Devices.

➔ Details

Building High-quality Social Communication Networks

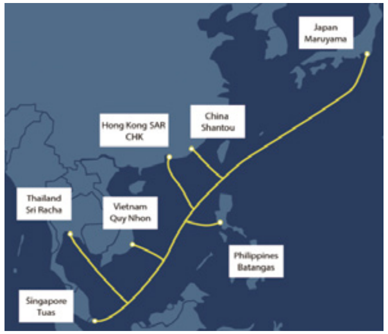
Value Creation 1 Prepare Sustainable Life Infrastructure

Building Overseas Networks

SoftBank Corp. is part of the Asia Direct Cable (ADC) project to build an optical submarine cable with a total length of approximately 9,400 km connecting Japan, China, Hong Kong, the Philippines, Vietnam, Thailand and Singapore. The project aims for completion and the start of operations within 2023.

The cable will feature multiple pairs of high capacity optical fibers and is designed to carry more than 140 Tbps of traffic. ADC's high capacity will allow it to meet rapidly increasing demand for Internet traffic in the Asia-Pacific region driven by 5G, IoT, AI and cloud services. The operation of the ADC will also provide additional network redundancy in the region, realizing highly reliable communications and enabling more flexible response to changes in connectivity demand.

SoftBank Corp. will provide the SoftBank Maruyama Cable Landing Station, located in Minamiboso City, Chiba, for the ADC cable landing in Japan. Serving an important role as a data center and international communications hub, this station provides landing services for many submarine cables, including JUPITER, a trans-Pacific optical submarine cable already in operation. Through connections to cables like ADC and Jupiter and the creation of connection facilities, SoftBank Corp. will continue to stably offer service to meet traffic demand in the Asia-Pacific region and provide an important gateway for international submarine cables in Japan.



ADC system route map

An Industrial Revolution in the Sea with Beyond 5G

Aiming to power an industrial revolution in the sea with 5G, a team comprising researchers from SoftBank Corp. and researchers under Professor Shinpei Gotoh of Tokyo University of Marine Science and Technology, with the cooperation of Koichiro Shibata, Vice Principal of Hokkaido Akkeshi Shoyo High School, successfully demonstrated the remote control of an underwater robot in real time, a world-first.*

Acoustic communication has conventionally been used for submarine communication. However, the slow transmission speed and low amount of information transmitted with such technologies present numerous issues, including difficulties with precise positioning, real time communication and security. Visible light communication technology has gained attention as a potential solution to these issues, but this technology requires the precise reception of light signals with extremely high directionality, necessitating high-precision optical tracking technology. In the recent demonstration experiment, the research team used optical camera communication (OCC) technology, which does not require high-precision optical tracking technology and can establish communications with just imprecise tracking using a camera trained on a communications target. Furthermore, using wireless communications via the communications satellites of Thuraya Telecommunications Company—a non-terrestrial network (NTN) that extends coverage to the open sea and polar regions—we were able to freely control two underwater robots operating in narrow spaces beneath the thick ice covering Lake Akkeshi, where terrestrial network signals do not reach, from the SoftBank Corp. Head Office in Minato-ku, Tokyo, some 930 kilometers away.

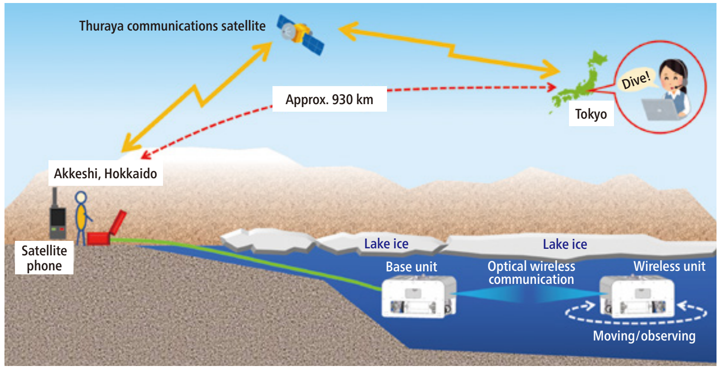


Diagram of robot control demonstration test using NTN and OCC

The commercialization of this technology will reduce the burden of field surveys for data collection, observation, equipment monitoring and maintenance even in regions and waters that are difficult to access. Furthermore, the use of OCC and underwater laser communication technology that employs high-precision optical tracking and is capable of medium- and long-range, high-volume communications will enable stable, real time communications with robots, even in very shallow waters where positioning with conventional acoustic communications is difficult. As such, these technologies are expected to be useful in fishery surveys under sea and lake ice. And, because they are not readily impacted by hydrographic or weather conditions, these submarine wireless communication technologies have great potential for creating infrastructure, such as submarine lighthouses, making them promising for use in next-generation marine logistics.

Underwater optical wireless communication technology will enable the construction of practical submarine wireless communication networks, which are expected to yield major economic impacts, such as increasing efficiency in marine industries and creating new industries. To make this technology even more practical and reliable, SoftBank Corp. and Tokyo University of Marine Science and Technology plan to first work on its practical application in the polar regions and around the Izu-Ogasawara islands through demonstration tests in the Antarctic Ocean and elsewhere. In order to realize an industrial revolution in the sea through Beyond 5G, we aim to establish a global undersea communication network by realizing short- and medium-range one-to-one and many-to-many optical wireless communications within a communication distance of 10 to 100 meters, as well as long-range one-to-one submarine optical wireless communications over a communication distance of several hundred meters or more.

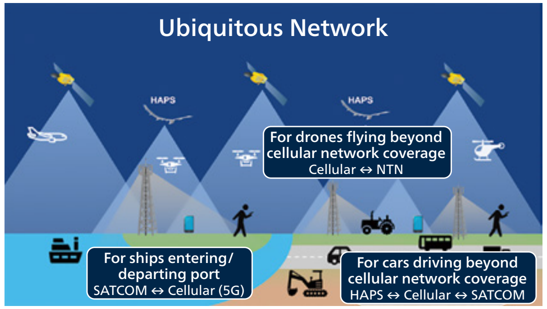
* At March 3, 2023 (SoftBank and Tokyo University of Marine Science and Technology survey)

Building High-quality Social Communication Networks

Value Creation 1 Prepare Sustainable Life Infrastructure

NTN Solutions

SoftBank Corp. has made closing the global digital divide part of its mission. Accordingly, we aim to build a ubiquitous network that combines non-terrestrial networks (NTNs) that provide telecommunications connectivity from space and the stratosphere with terrestrial mobile networks. By doing so, we aim to enable seamless connection to a variety of communications from anywhere on Earth. As elements of the ubiquitous network, we plan to roll out OneWeb, HAPS and other NTN solutions.


Ubiquitous Network
HAPS
HAPS
For drones flying beyond cellular network coverage
Cellular ↔ NTN
For ships entering/ departing port
SATCOM ↔ Cellular (5G)
For cars driving beyond cellular network coverage
HAPS ↔ Cellular ↔ SATCOM

Providing High-speed, Low-latency Communications with OneWeb

OneWeb high-volume, high-speed satellite communication services are provided using satellites in low Earth orbit at an altitude of 1,200 km, closer to the surface of the Earth than geostationary satellites. These satellites are launched into one of 12 orbits, in which they circle the Earth every two hours. Placing large numbers of satellites in low Earth orbits that are closer to ground than geostationary satellites enables OneWeb to offer higher speed and lower latency than conventional satellite communications.

In April 2021, SoftBank Corp. and OneWeb LLC, which provides OneWeb, agreed to collaborate on deployment in Japan, and preparations for service launch are under way. Following the completion of its global constellation in early 2023, OneWeb is on track to deliver full global coverage by the end of 2023. In response to this achievement, SoftBank Corp. has commenced preparations for providing satellite communication services utilizing OneWeb in Japan.

Note: The future provision of this service is under consideration and subject to change.

HAPS: Providing Service to an Area 200 km Wide from Unmanned Aircraft

The stratosphere-based high-altitude platform station (HAPS) is a means of providing terrestrial communication services from unmanned aircraft that remain aloft in the stratosphere for long periods at an altitude of 20 km. One HAPS aircraft can provide service to a much wider area than a terrestrial base station, with a land coverage diameter of about 200 km, enabling spot provision of mobile signal to sparsely populated areas, like islands and mountainous regions. Furthermore, after natural disasters, HAPS can provisionally restore communication by flying aircraft over the affected areas.

Radiowave Propagation Simulator Developed for HAPS

In November 2022, SoftBank Corp. and HAPSMobile Inc., its subsidiary established to develop the HAPS business, developed a radiowave propagation simulator that implements the HAPS Radiowave Propagation Prediction Method that became part of the International Telecommunication Union Radiocommunication Sector (ITU-R)'s global standard in October 2021 based on contributions from SoftBank and HAPSMobile. The simulator will make it possible to analyze radiowave propagation with greater accuracy and efficiency for HAPS service rollouts.

This radiowave propagation simulator can analyze radiowave propagation loss by utilizing weather data, such as variations by latitude and longitude in atmospheric temperatures and rainfall intensity, and geographical information that includes terrain and buildings, making it possible to accurately analyze radiowave propagation in regions around the world.

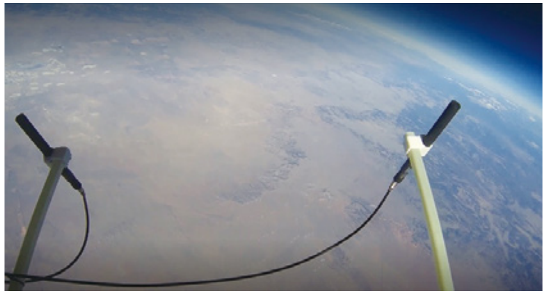
Utilizing this simulator, SoftBank Corp. and HAPSMobile will further study radiowave propagation analysis and system design.

Development of Next-generation Lithium-metal Battery Pack and Successful Demonstration in the Stratosphere

In October 2022, SoftBank Corp. developed a battery pack for HAPS using a next-generation lithium-metal battery cell. The next-generation lithium-metal battery cell was developed jointly with Enpower Japan Corp. and boasts a specific energy of 439 Wh/kg. Furthermore, in cooperation with ENAX Inc., SoftBank Corp. successfully reduced the weight of the pack components, including a constraint mechanism, heaters and insulation materials, bringing the companies much closer to building a battery pack with a specific energy of 300 Wh/kg.

SoftBank Corp. and HAPSMobile Inc. conducted a charge-discharge cycle test of the battery pack in the stratosphere from January 30 to February 2, 2023. The pack demonstrated the same level of regular operation in the stratosphere at extremely low temperatures of around -60 °C as shown during the ground tests, a first for such battery packs.

In the near future, SoftBank Corp. aims to develop a large battery pack as a power source for HAPS operation. In addition to HAPS, SoftBank Corp. will consider using such packs for industrial drone applications.



Demonstration in the stratosphere

Building High-quality Social Communication Networks

Value Creation 2 Construct Robust Communications Infrastructure to Contribute to Disaster Prevention and Mitigation

Communications infrastructure is one of the most important lifelines in the event of a disaster. To ensure stable communications services no matter the circumstances, SoftBank Corp. is building disaster-resilient communications networks and systems to effect rapid recovery in the event of damage. Using AI and ICT, we quickly collect and communicate information on disasters to help keep people safe and mitigate harm after disasters strike.

Disaster Response

Structure Based on Disaster Response Agreements

To assist swift restoration efforts in the event of a major disaster or emergency, SoftBank Corp. has entered into disaster response agreements with Japan’s Ministry of Defense and the Japan Coast Guard for the purpose of securing communications and mutually cooperating in a wide range of areas. As communications are a necessary means of assisting life-saving activities following a disaster, SoftBank Corp. provides satellite phones, ordinary mobile phones and other communication equipment to the Ministry of Defense and the Japan Coast Guard.

Furthermore, the Ministry and Coast Guard provide logistics assistance and the use of their facilities and equipment so that SoftBank Corp. can better secure communications and work toward restoration in affected areas.

In preparation for emergencies, we conduct training around Japan in collaboration with the Ground Self-Defense Force and Coast Guard. SoftBank Corp. will continue to work closely with the Ministry of Defense, the Japan Coast Guard and other related institutions to ensure disaster preparedness and carry out its responsibilities to society as a telecommunications carrier.

Disaster Management Structure

Disaster Operation Plan

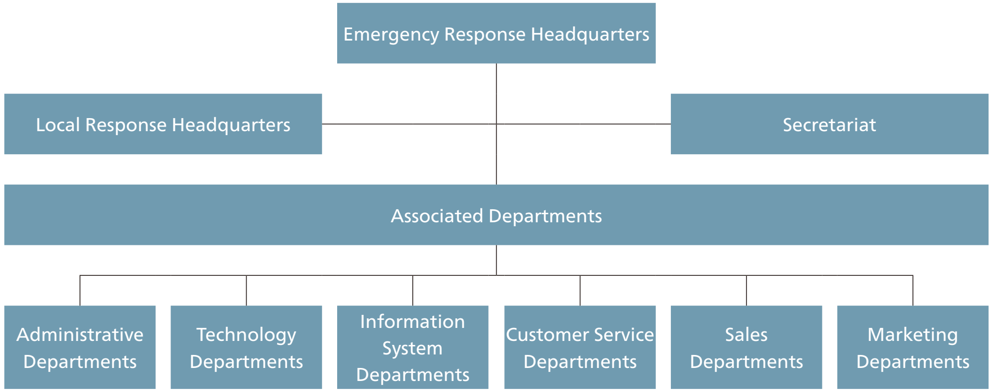
Under Japan’s Basic Act on Disaster Management, SoftBank Corp. is a designated public institution as determined by the national government and therefore has formulated a Disaster Management Operation Plan. SoftBank Corp. has established systems for disaster prevention and preparedness, and in the case of disasters, responds in accordance with the Disaster Management Operation Plan while working closely with relevant institutions.

Internal Systems

To respond swiftly in the event of a disaster, SoftBank Corp. has prepared and thoroughly disseminated response manuals, developed an emergency contact system and deployed emergency supplies.

Comprehensive Response Manuals	If a facility is likely to be damaged by a disaster, we have designated measures to minimize the impact on services and ensure a prompt recovery (by such means as the creation of disaster response manuals).
Emergency System and Contact Network	We have established a system able to quickly respond to telecommunications network failures in the event of a disaster and maintain an emergency contact network in preparation for emergencies.
Disaster Response Equipment and Disaster Supplies Deployment	To quickly restore communication networks, SoftBank Corp. maintains repair supplies and spare equipment, as well as stockpiles of such daily necessities as drinking water and food at its locations across Japan. We also have disaster response equipment (emergency generators, etc.) deployed nationwide.
Emergency Response Headquarters	In the event of a major disaster or other emergency, personnel from each division gather and analyze information on impacts and damage in their areas of responsibility. Depending on the extent of the impacts, an Emergency Response Headquarters may then be established to take action to rapidly restore operations.

Emergency Response Headquarters Structure


Emergency Response Headquarters
Local Response Headquarters
Secretariat
Associated Departments
Administrative Departments
Technology Departments
Information System Departments
Customer Service Departments
Sales Departments
Marketing Departments

Building High-quality Social Communication Networks

Value Creation 2 Construct Robust Communications Infrastructure to Contribute to Disaster Prevention and Mitigation

Disaster Response

Deploying Mobile Power Supply Vehicles

We have mobile power supply vehicles deployed across Japan to provide power to base stations in the case of power outages in a disaster. We aim to maintain at least 80 mobile power supply vehicles. As of March 2023, we have 91 deployed nationwide, striving to provide continuous service.

Mobile power supply vehicle

Mobile Power Supply Vehicles by Region

(as of March 2023)

Hokkaido	6	Kinki	11
Tohoku	9	Chugoku	6
Kanto	18	Shikoku	7
Shinetsu	2	Kyushu	13
Hokuriku	5	Okinawa	4
Tokai	10	Total	91

Deployment of Mobile Base Station Vehicles and Portable Mobile Base Stations

SoftBank Corp. deploys mobile base stations to rapidly restore service in disaster-stricken areas where base stations have been damaged or have lost power. We aim to maintain more than 200 mobile base stations of various types across Japan in preparation for emergencies in order to assist in the recovery of areas affected by disasters.

Mobile Base Station Vehicle

Mobile Base Station Vehicles

Small Mobile Base Station Vehicles

When transmission lines are damaged by disasters, these temporary base stations provide an entrance to the satellite network. Thanks to their high mobility, small vehicles are typically the first to reach the scene of disasters.

Medium Mobile Base Station Vehicles

These temporary base stations provide an entrance to the satellite network when transmission lines are damaged by disasters or use ground transmission lines if available.

Large Mobile Base Station Vehicles

These temporary base stations provide an entrance to the satellite network when transmission lines are damaged by disasters or use ground transmission lines if available. Capable of carrying the most simultaneous voice calls of all mobile base station vehicles, the large vehicles are all equipped to use SoftBank 4G LTE.

Mobile Base Station Vehicles by Region

(as of March 2023)

	Small	Medium	Large
Hokkaido	1	4	2
Tohoku	1	4	3
Kanto	2	13	10
Shinetsu	0	3	1
Hokuriku	1	2	2
Tokai	1	6	6
Kinki	1	6	4
Chugoku	1	4	2
Shikoku	1	3	2
Kyushu	1	7	3
Okinawa	0	2	1
Total	10	54	36

Portable Mobile Base Stations

We have deployed 200 portable mobile base stations that can provide an entrance to the satellite network nationwide. Of these, 100 can be mounted on vehicles.

Portable mobile base stations

Building High-quality Social Communication Networks

Value Creation 2 Construct Robust Communications Infrastructure to Contribute to Disaster Prevention and Mitigation

Disaster Response

Deploying Portable Satellite Antennas

These collapsible auto-acquiring satellite antennas can be used to quickly set up temporary satellite-based communication links. Equipped to support high-speed communications, by using high-speed satellite circuits, these antenna systems can be used as an alternative to optical fiber lines. We currently have 282 of these antennas deployed across Japan.

Portable satellite antenna

Portable Satellite Antennas by Region

(as of March 2023)

Hokkaido	14	Kinki	24
Tohoku	16	Chugoku	22
Kanto	57	Shikoku	26
Hokuriku	10	Kyushu	73
Tokai	18	Okinawa	22
Total			282

Microwave Links

Base station antennas are set up in locations with clear lines of sight to one another (free of obstacles that could block radio waves), and wireless signals in the millimeter wave or microwave bands are used for communication in place of optical fiber connections.

Coordination with National and Local Governments

Disaster Drills

To ensure rapid response in the event of a major disaster, SoftBank Corp. regularly conducts disaster drills in coordination with local governments, the Ground Self-Defense Force, the Ministry of Defense and the Japan Coast Guard. We participate alongside other lifeline providers, such as power companies, in supply packing drills with the Self Defense Force and Coast Guard, as well as drills held by local governments, including comprehensive disaster drills and drills for helping people who cannot reach their homes in a disaster. Through these drills, participants confirm emergency contact systems and coordination procedures, aiming to enable smooth collaboration when an actual disaster strikes.

We also conduct disaster recovery drills to confirm restoration methods and procedures for specific situations and cases to improve our ability to provide continuous communications services under any circumstances. To quickly restore service in areas with poor communications service or no service when base stations have been damaged, lost power or been cut off from the network by a disaster, we have a variety of equipment, including mobile base station vehicles and portable base stations, deployed across the country. These facilities switch power sources to emergency batteries during power outages, and we have emergency generators at our maintenance centers around the country for use should these power sources be insufficient, such as during prolonged power outages. We regularly conduct drills on the use of this equipment.

Wired Power Feed Drone Wireless Relay System

In collaboration with the Tokyo Institute of Technology and Futaba Corporation, SoftBank Corp. has developed a wired power feed drone wireless relay system for deployment to quickly restore lifeline mobile phone service when a base station has been damaged by a disaster. These have been positioned at key locations across Japan to provide back-up communication channels for use in a disaster. The new system began operation in July 2022. In preparation to provide temporary connections after disasters, the system was first deployed to SoftBank Corp.'s network centers in the Kanto area, with plans to expand its use nationwide going forward.

The wired power feed drone wireless relay system is equipped with both wireless relay equipment and a wired power supply system. It comprises wireless relay equipment on the ground (the main unit) and on a drone (the extension), with communications between the two via optical fiber using radio on fiber (RoF) technology. The connection between the mobile network and the base station wireless transmission equipment connected to the main unit is, in most deployments, by satellite, enabling the rapid establishment of a temporary service area regardless of any damage from disasters to permanent base stations or other ground-based equipment. Because the system can use LTE (2.1 GHz) communications, by positioning the drone 100 m off the ground, it can provide a service area with a radius of more than 3 km in suburban areas, or more than 5 km in more open areas.

Building High-quality Social Communication Networks

Value Creation 2

Construct Robust Communications Infrastructure to Contribute to Disaster Prevention and Mitigation

Coordinating with National and Local Governments

Reconstruction of Base Stations

Should a base station become inoperable due to damage to the facility or communications equipment in a disaster, it is rebuilt in the same place after checking the safety of the ground and foundations and confirming that users are present to use the base station.

Loaning Devices to Local Governments

SoftBank Corp. has deployed satellite phones, mobile phones and tablets at locations across Japan for use as a means of communication in disaster areas for relief and recovery activities. We have established a structure whereby these devices can be loaned free of charge to local governments, public organizations, NPOs and other organizations. After the heavy rains beginning July 14 and August 3, 2022, as well as after Typhoon No. 15 of 2022, we loaned out mobile phones, Wi-Fi systems and other devices in disaster-stricken areas. As of March 2023, we have a total of 101 devices out on loan.

➔ Disaster and Reconstruction Support P. 202-203

Support for Securing Means of Communication at Evacuation Centers

When disaster strikes, we provide evacuation centers with mobile phones and land-line phones for calls. As an additional form of assistance, we provide facilities for use free of charge that include charging services during power outages and Wi-Fi systems (00000JAPAN) that allow users to access the Internet via their personal computers or smartphones. These added means of communication help evacuees confirm the safety of friends and family members, as well as gather information on support.

Securing Communications When Disaster Strikes

In a major disaster, mobile phone, and Internet and network device access surges in the affected areas as customers try to confirm the safety of their family and friends. The resulting network congestion can cause difficulties with regular communications and even such important communications as emergency calls designated under the Telecommunications Business Act (calls to the telephone numbers 110 and 119 in Japan).

To prevent a large-scale network system failure caused by congestion, SoftBank Corp. may temporarily restrict communications services as necessary in proportion to the scale of the congestion in order to protect and maintain certain essential communications services.

When a disaster impacts mobile phone service, SoftBank Corp. quickly establishes a Disaster Response Headquarters. We gather personnel from all over the country and bring in mobile base station vehicles, portable base stations, portable satellite antennas, mobile power supply vehicles, portable generators and other equipment to ensure the supply of power and help secure the area.

Going forward, to minimize the damage caused by natural disasters, SoftBank Corp. will strive to construct robust communications infrastructure that contributes to disaster prevention and mitigation.

Services Providing Peace of Mind When Disaster Strikes

SoftBank Corp. provides information on disasters and disaster prevention, as well as notifications and services that help secure a means of communication for customers when disaster strikes.

■ Yahoo! JAPAN Disaster Alert App

The Yahoo! JAPAN Disaster Alert app promptly alerts customers with push notifications about sudden heavy rains or earthquakes, including evacuation orders. This free disaster prevention app provides information regarding the user's current location and up to three other user-specified locations in Japan so that users can receive information about places they are planning to travel or where their families reside.

■ Disaster Prevention Notebook

The Disaster Prevention Notebook service offers content useful not only for disaster readiness, but also for everyday life, including articles and information about disaster readiness supplies.

防災手帳
いのちを守る、日頃の備え
防災タイムライン
未設定
自宅周辺の想定危険度や、災害時の防災行動を確認しましょう。

■ Emergency Alert Emails

This service broadcasts earthquake early warnings and tsunami warning messages issued by the Japan Meteorological Agency as well as disaster and evacuation information issued by national and local governments to customers in the affected areas.

■ Disaster Message Board Service

This service enables customers to store and send messages to the people with whom they want to communicate if voice calls surge when disaster strikes and it becomes difficult to connect.

■ Emergency Call Location Notification

When emergency calls (110, 118 and 119 in Japan) are placed from a SoftBank mobile phone, information about the location where the emergency call was placed is automatically provided to the emergency operator.

Value Creation 3 Promote Data Security and Privacy Protection Initiatives

SoftBank Corp. monitors and operates networks using the latest technologies and conducts thorough security education for employees, doing its utmost to ensure the confidentiality of communications and protect customer information. By understanding information security risks and proactively working to protect the privacy of customers' personal data, we strive to contribute to the realization of a society in which telecommunications can be used safely and with peace of mind.

Information Security and Privacy Protection

Policy

SoftBank Corp. has formulated and adheres to the Information Security Policy and Personal Data Protection Policy so that it can keep the trust of customers and the wider community by implementing far-reaching and advanced solutions to counter the risk of information leaks. We endeavor to maintain information security by appropriately handling and protecting our information assets from a variety of threats.

Information Security Policy

■ Information Security Policy Management

1. Creation of an information security management system

SoftBank Corp. has created a highly secure information security management system in an effort to protect all the information assets it holds and comply with information security-related laws, regulations and other standards to consistently earn the trust of society.

2. Appointment of a Chief Information Security Officer

SoftBank Corp. has established the Information Security Committee and appointed a Chief Information Security Officer (CISO). By proactively using this framework, we are able to ensure an accurate understanding of the company-wide information security status and promptly take necessary measures.

3. Maintenance of internal rules regarding information security

SoftBank Corp. has established internal rules based on the Information Security Policy to clearly indicate its stance on the handling of personal information and all information assets, and to make everyone within and outside the company aware of its strict position on information leaks.

4. Audit system maintenance and enhancement

SoftBank Corp. maintains a system for conducting internal audits to ensure compliance with the Information Security Policy and other rules and regulations. We also strive to conduct ongoing external audits to obtain more objective evaluations. These regular audits verify that our employees are complying with security policies.

5. Realizing a system for thorough information security measures

SoftBank Corp. will realize a system that reflects thorough measures to prevent unauthorized intrusion, leakage, falsification, loss, destruction and obstruction of information asset usage. In terms of countermeasures, we thoroughly manage access to data and systems by granting access rights based on the "need to know principle"* and limiting the database access rights of employees working in high-security areas.

* Need to know principle: Information is provided only to those people with a need to know, and is not provided to those without a need to know.

6. Improving information security literacy

SoftBank Corp. provides thorough security education and training to employees so that everyone involved with information assets can conduct their work with information security literacy. We also provide ongoing education and training to enable responses to constantly changing conditions.

7. Outsourcer management system enhancement

When concluding business outsourcing contracts, SoftBank Corp. thoroughly examines outsourcer qualifications and requests that outsourcers maintain security levels equal to or higher than those of SoftBank Corp. In addition, to confirm that security levels are being maintained appropriately, we continuously review outsourcers and work to strengthen agreements.

■ Scope of the Information Security Policy

The "information assets" covered by this policy include information obtained or known through the ordinary course of SoftBank Corp.'s business as well as all information held by the company for business purposes. All SoftBank Corp. directors, employees and temporary staff engaged in handling and controlling information assets, as well as outsourcers and their employees who handle SoftBank Corp. information assets, must comply with the Information Security Policy.

Building High-quality Social Communication Networks

Value Creation 3

Promote Data Security and Privacy Protection Initiatives

Information Security and Privacy Protection

Information Security System

SoftBank Corp. has an information security management system in place to ensure adherence to laws and regulations regarding information security, safeguard its information assets and defend against cyberattacks. SoftBank Corp. has formulated its Information Security Policy to be followed by employees and established the position of Chief Information Security Officer (CISO). We have also established the Information Security Committee (ISC), chaired by the CISO, and the SoftBank Computer Security Incident Response Team (SoftBank CSIRT). These bodies review policies as needed to adapt to changes in the security environment and technological innovation, and share information helpful for planning information security and cybersecurity measures.

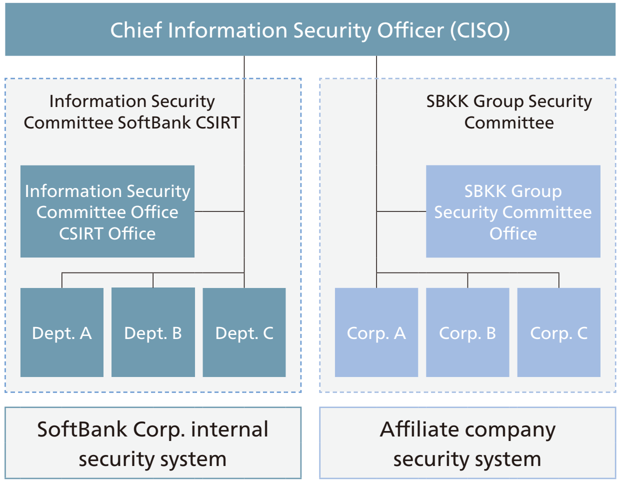
When an information security breach causes a system failure, the system operation head and the CISO coordinate to assess the situation, evaluate responses and restore the system. Additionally, in the event of serious issues, we establish an Emergency Response Headquarters headed by the CEO and promptly report to the Ministry of Internal Affairs and Communications and other appropriate authorities as mandated by laws and regulations.

Information Security Committee

The Information Security Committee (ISC), chaired by the CISO, is composed of each division's person in charge of information security. It is a cross-functional organization that seeks to promote and manage various initiatives for information security. In order to ensure the effective execution of initiatives, we have set up the Information Security Committee Office (ISC Office) to help plan and swiftly implement information security measures.

■ Roles of the ISC

- Sharing of information beneficial to information security activities
- Company-wide sharing of measures and plans related to information security activities
- Company-wide monitoring and improvement of information security status
- Information security education and training
- Coordinating information security initiatives across departments


Chief Information Security Officer (CISO)
Information Security Committee SoftBank CSIRT
Information Security Committee Office CSIRT Office
Dept. A
Dept. B
Dept. C
SBKK Group Security Committee
SBKK Group Security Committee Office
Corp. A
Corp. B
Corp. C
SoftBank Corp. internal security system
Affiliate company security system

SoftBank CSIRT

SoftBank CSIRT was established to prevent security incidents and minimize damage by quickly responding when security incidents occur. SoftBank CSIRT deals with security incidents related to the services SoftBank Corp. provides. Overseen by the CISO, the team consists of members from the Security Department and members appointed by the heads of other departments. The CSIRT Office works with the Information Security Committee Office and related organizations, both inside and outside the company, to support the team.

In order to prevent security incidents, SoftBank CSIRT addresses system vulnerabilities (information collection and analysis, making response requests and reviewing of response status), formulates security rules, provides security training and sends warnings about potential security issues. To prepare for and respond to any incidents that should occur, the team has established an incident response flow and carries out incident response training.

Security System of Affiliate Companies

SoftBank Corp.'s affiliate companies (subsidiaries and affiliates) have risk management structures in place, mitigating information security and cybersecurity risks and preventing incidents. They also assess, analyze and respond to security risks.

The SBKK Group Security Committee, headed by the CISO and comprising members in charge of information security management at affiliate companies, shares information on threats and solutions regarding information security. The Committee also executes security training and drills, and coordinates responses when incidents occur. Additionally, the SoftBank Affiliate Company Security Guidelines stipulate matters to be observed and the governance structure necessary for group companies to manage security appropriately.

Value Creation 3

Promote Data Security and Privacy Protection Initiatives

Protecting Customer Information

We take measures to protect our customers from information leaks and cyberattacks so that they can use our services with peace of mind.

Security Measures

To protect our various information assets, including customer information, we have a security governance structure in place, providing security checks and advice when services are developed and launched internally. We also conduct security tests prior to their release and during operations. Furthermore, we run the Security Operation Center (SOC), which monitors services and equipment, establish regulations, collaborate internally and with other organizations, and review our solutions and consider new ideas by referring to the Cybersecurity Framework (CSF) of the U.S.-based National Institute of Standards and Technology (NIST) and the CIS Controls of the U.S.-based Center for Internet Security (CIS).

Rigorous Information Management

SoftBank Corp. has established tiered security areas ranging from level 1 to 5 in its facilities, applying strict controls in accordance with each level. Levels 3 and above are considered high-security areas. Especially important data, such as personal information and confidential communications, are exclusively handled in these areas.

For example, at the Customer Support Center, which is designated as a high-security area, we strictly control security under the rules specifically designed for these areas, using security guards and passes to manage entry and exit to the facilities while restricting prohibited items from the facilities.

Additionally, our operations fully adhere to ISO 27001, the international standard for information security management systems. We undergo an external audit twice a year based on ISO 27001 to confirm that our information security management is appropriately run, including compliance with our Privacy Policy.

Security Monitoring

To protect customer information and the equipment used to provide telecommunication services, security analysts monitor security at our Security Operation Center (SOC) 24 hours a day, 365 days a year.

As measures against cyberattacks, we monitor for DoS attacks* on our telecommunications service equipment and infiltration into devices connected to our equipment, detect malware infections of our employees' computers and their access to unauthorized websites, and watch for attacks that could exploit vulnerabilities in our in-house systems. We also take steps to deter the theft of data and unauthorized device use.

* DoS attack: Denial of service attack, in which a flood of data is directed at a target site to disrupt its systems so that they cannot function normally

Protecting the Usage Environment of Customers

We offer a variety of security measures to protect customers from viruses, spyware, one-click fraud and other hazards to provide a pleasant experience when using our mobile phone, smartphone and Internet services.

- **Viruses**

Smart Security powered by McAfee® protects customers' smartphones from viruses. This service detects viruses that can infiltrate smartphones through installed applications, e-mail attachments and microSD memory cards.

- **One-click Fraud**

SagiWall/Internet SagiWall detects dangerous websites, such as those designed for one-click fraud schemes, when customers use the Internet. This service constantly monitors websites being browsed and displays a warning screen when a user attempts to access a suspected dangerous website.

- **Security Protection**

BB Security is a service for users of the SoftBank Hikari and SoftBank Air home Internet services that constantly maintains the latest security environment for their smartphones and computers.

- **Sniffing/Hacking**

Security Checker protects customers' smartphones when they are connected to a telecommunications network, such as through public Wi-Fi, by safeguarding their important data and detecting such hazards as sniffing and wiretapping.

Spam Mail

To protect against malicious e-mails, such as spam and fake bills unexpectedly sent to mobile phones or smartphones, we provide our customers with spam filters as a standard feature. These filters automatically sort e-mails based on our accumulated database of spam to block the receipt of malicious emails. We have also set up a reporting center where our customers can report any spam e-mails they have received by simply forwarding them. When it is confirmed that spam has been sent from a SoftBank registered address, we may take strict measures against the address owner, including suspension or cancellation of service.

Building High-quality Social Communication Networks

Value Creation 3 Promote Data Security and Privacy Protection Initiatives

Protecting Customer Information

Unauthorized Access

Cases of malicious third parties gaining unauthorized access to personal information as a result of virus infection or accessing URLs sent in e-mails are increasingly common. This personal information can include bank account numbers, credit card numbers, and login IDs and passwords. We are strengthening security to protect our customers' personal information by preventing the use of such information to gain unauthorized access to the My SoftBank and My Y!mobile member sites, where members can confirm and change fees and contract details.

■ Passcodes

Customers can change their settings to require the passcode they specified when signing their contract when logging into My SoftBank or My Y!mobile.

■ One-time Passwords

When a customer uses SoftBank or Y!mobile Matomete Shiharai payment options, an SMS (a text) is sent to their phone with an authorization code. This code is valid for one time only and is only known to the registered user.

■ Unauthorized Access

In order to prevent unauthorized access, such as identity impersonation, when a customer attempts to use certain options available on the My SoftBank or My Y!mobile membership sites, we may send a SMS or e-mail to confirm the usage status of their mobile phone.

Collaborative Cybersecurity

As an operator of communications infrastructure vital to society and as a company providing innovative services by integrating telecommunications with cutting-edge technologies, SoftBank Corp. works with various external organizations to help improve security across society. The Computer Security Incident Response Team (CSIRT) represents SoftBank Corp. in collaborations with external organizations.

Information Sharing with Local and Overseas CSIRT

SoftBank CSIRT is a member of security organizations both in Japan and overseas, engaging in discussions on common security themes and issues with the CSIRTs of other companies to study effective responses and solutions.

▼ Memberships

Nippon CSIRT Association

FIRST
(Forum of Incident Response and Security Teams)

ICT-ISAC Japan

Incident Response Coordination and Joint Exercises

In the event that an incident occurs at multiple organizations from a single cause, or an incident at one organization also affects other organizations, we coordinate and implement a response with the CSIRTs of other companies, as needed, to address the issue.

To ensure a quick response to incidents, we regularly conduct joint exercises with the CSIRTs of other companies, verifying how we will work together when incidents occur.

Through these efforts we aim to minimize the impact caused by incidents and mitigate any harm.

Receiving Reports of Security Vulnerabilities

We work to improve the security of our websites and services in various ways, including vulnerability tests. SoftBank CSIRT welcomes reports from engineers outside the group on any vulnerability they have discovered in our website or services, using information received in cooperation with the relevant department or individuals to address the issue.

Value Creation 3 Promote Data Security and Privacy Protection Initiatives

Protecting Customer Information

Ongoing Security Enhancement

In response to the spread of digital devices and increasingly sophisticated cyberattacks, we strive to continuously strengthen security by adopting new technologies and methods, raising employee awareness through education, and training security specialists.

Personnel Measures

■ Employee Training

In order to ensure appropriate handling of information in ordinary operations and to raise awareness of information security and cybersecurity, we provide classroom training, regular e-learning programs and security drills for executives and employees while updating security rules on an ongoing basis.

With particular focus on the topics of protecting personal information, the confidentiality of communications and preventing internal wrongdoing, we implement ongoing internal training to improve our employees' knowledge and ethics. Useful materials and educational videos on information security are available on the company intranet for employees to access at any time. In FY2022, we designated a Group Security Month for group companies, implementing intensive training in an effort to raise group-wide awareness.

■ Training of Security Experts

Our security experts work hard not only to collect and share information on security threats and solutions, but also to improve their technical skills and knowledge so that they can guard against ever-changing security threats. We encourage our security experts to obtain security qualifications to build their expertise.

Qualifications Held by Our Security Experts

CISSP, Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Registered Information Security Specialist (RISS), GIAC qualifications, CEH, AWS Certified Security - Specialty, among others.

Technological Measures

■ Monitoring Technology

While the early detection of incidents is becoming increasingly difficult due to the growing complexity of attack techniques in recent years, the number of detected incidents is constantly rising. SoftBank Corp. strives to improve the quality of monitoring by continuously upgrading detection methods, implementing analysis and solutions leveraging threat intelligence (information useful to detecting and blocking attacks), and automating response operations so that no signs of attack are missed.

■ Monitoring of Threats and Attacks

By monitoring communication log data collected from digital devices and equipment, such as servers, we anticipate and identify threats from multiple angles, including suspicious communications inside or outside of our organization and potential malware infections. We have built information-sharing frameworks with security organizations we belong to and with security vendors to ensure we are aware of the latest developments by reviewing incidents at other companies and reports on vulnerabilities and attacks.

We aim to detect increasingly sophisticated and complex attacks as early as possible by implementing security information and event management (SIEM) to detect the latest attacks by collecting log data and performing correlation analysis.

■ Monitoring of Telecommunication Networks Security

Since telecommunications networks serve as social infrastructure, expectations for their reliability and quality are far higher than ever before. SoftBank Corp., as a telecommunications provider, performs various kinds of monitoring to provide a stable telecommunications network. Monitoring security is one part of this effort.

5G networks offer not only higher speeds but also ultra-low latency and massive device connectivity. Thanks to these features, 5G is expected to be applied across a wide variety of new use cases, like remote operations and autonomous driving. SoftBank Corp. is building an even more advanced security monitoring system to respond to changes in data traffic caused by DDoS attacks* and to deal with cyberattack attempts to access 5G equipment.

* DDoS attacks: Distributed denial-of-service attacks, a form of cyberattacking a specific device by overwhelming it with a simultaneous flood of data traffic from multiple devices

5G Network Features and Use Cases

Ultra-low latency: Remote-controlled robots, autonomous driving, telemedicine—all previously considered difficult due to latency.

Massive device connectivity: Powerful acceleration of IoT that will revolutionize industries and society, with more things and sensors connected to networks.

Building High-quality Social Communication Networks

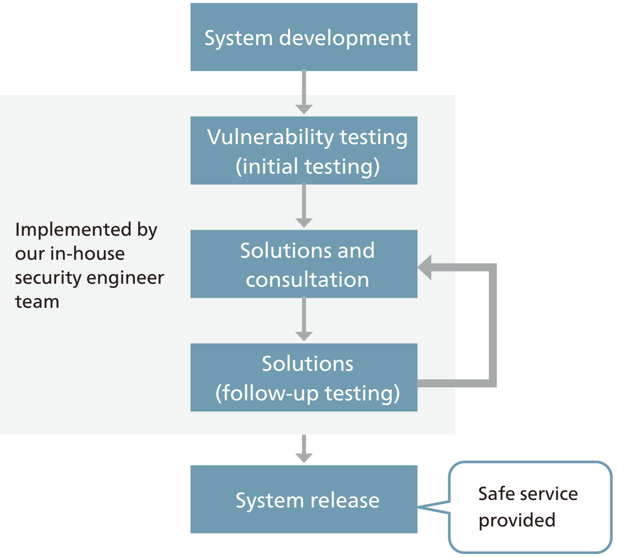
Value Creation 3 Promote Data Security and Privacy Protection Initiatives

Protecting Customer Information

Security Testing

If we launch services with flawed system settings or latent vulnerabilities, attacks on our network and systems could result in harm to customers. Our security engineer team carries out thorough vulnerability testing and issues instructions to address any vulnerabilities detected so that we can provide safe services.

Since new vulnerabilities can emerge even after the release of a service, we continue vulnerability testing and follow-ups to minimize security risks.


System development
Vulnerability testing (initial testing)
Implemented by our in-house security engineer team
Solutions and consultation
Solutions (follow-up testing)
System release
Safe service provided

Enhancing the Internal Security Environment

We seek to protect against increasingly sophisticated attacks by proactively adopting the most advanced technologies, such as mobile device management (MDM) and endpoint detection and response (EDR), which are becoming standard security solutions. Additionally, we carry out targeted attack e-mail simulation exercises and other measures to help strengthen our internal network security.

Information Security Incident Status

The number of serious information security breaches in FY2022 was zero. In order to prevent serious information security incidents, we will continue to conduct training and implement initiatives to prevent security breaches.

Cybercrime Prevention Educational Activities

BBSS Corporation issues a monthly report on Internet fraud as part of its cybercrime prevention and educational activities. The report is based on analyses of data on fraud websites detected and collected by the SagiWall® security software that protects against online fraud. It highlights techniques used by fraud sites, including the emergence of new sites, their characteristics, the latest fraud techniques and key considerations for harm prevention.

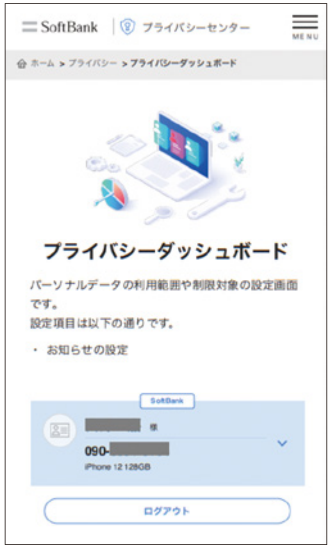
In March 2023, SagiWall detected 5,778,392 fraud websites, up 673,820 from February.

By publishing the monthly Internet fraud report, BBSS is helping to prevent harm from increasingly sophisticated cybercrime.

Privacy Protection Initiatives

Privacy Center Website

SoftBank Corp. aims to enable convenient and comfortable living through the appropriate use of customers' personal data in a variety of applications. We have set up the Privacy Center website to provide clear explanations of our initiatives in this area, including the ways we acquire, use and protect customer information. In addition, we provide a dashboard that allows customers to check and manage the use of their information.


SoftBank | プライバシーセンター

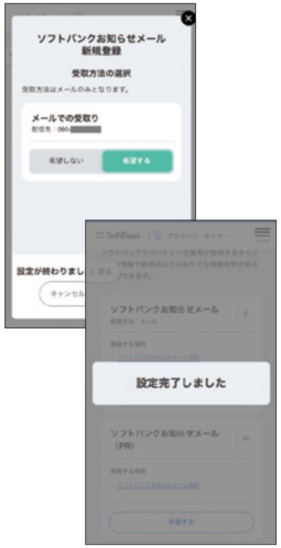
ホーム > プライバシー > プライバシーダッシュボード

プライバシーダッシュボード

パーソナルデータの利用範囲や制限対象の設定画面です。
設定項目は以下の通りです。

・ お知らせの設定

SoftBank
[redacted] 様
090-[redacted]
iPhone 12 128GB


ソフトバンクお知らせメール
新規登録

受取方法の選択

受取方法はメールのみとなります。

メールでの受取り
配信先：090-[redacted]

希望しない | 希望する

設定が終わりまし

SoftBank | プライバシーセンター

ソフトバンクお知らせメール

ソフトバンクお知らせメール（PR）

設定完了しました

Building High-quality Social Communication Networks

Value Creation 3

Promote Data Security and Privacy Protection Initiatives

Privacy Protection Initiatives

Personal Data Protection Action Guidelines

SoftBank Corp. uses the customers' personal data to enhance customer quality of life and solve social issues. We take the utmost care in the handling and protection of personal data.

1. We respect the wishes of our customers to the greatest extent possible.
   Personal data is our customers' valuable information. By allowing customers to manage how and for what their data is used, we respect customer wishes and avoid using their data in undesired ways.
2. We explain in a manner that is easy to understand from the customer's perspective.
   We strive to explain our approach to and methods of using personal data in ways that customers will easily understand, using clear language, illustrations and other tools.
3. We strictly manage our customers' valuable data.
   We maintain thoroughgoing security to protect personal data from increasingly diverse cyberattacks and other threats 24 hours a day, 365 days a year.
4. We handle personal data within proper systems.
   We build dedicated company-wide structures to handle personal data appropriately from a variety of perspectives, including laws and regulations, popular opinion and customer sentiment. We also proactively implement training and education for employees in cooperation with partner companies.
5. We use personal data in efforts to resolve social challenges.
   By using customer data, we work to resolve a wide range of social challenges, aiming to create a prosperous society in which everyone can live in comfort.

Personal Data Protection Policy

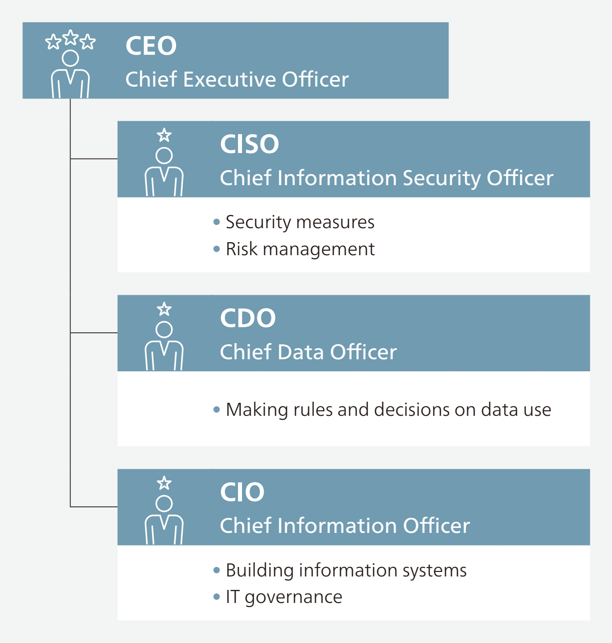
SoftBank Corp. handles the personal data of customers and various other stakeholders. We take the utmost care in the handling of such personal data, endeavoring to give due consideration to the rights of customers and other stakeholders. In addition to strictly complying with the following laws and regulations, guidelines set by the government and other norms, taking the initiative in protecting privacy, we have joined an accredited personal information protection organization (the Japan Data Communication Association) as a covered business operator.

- Act on the Protection of Personal Information
- Telecommunications Business Act (provisions on confidentiality of communications)
- Guidelines for Protection of Personal Information in Telecommunications Business
- Personal information protection management systems - Requirements (JIS Q 15001)

Personal Data Protection Framework

■ Structure

SoftBank Corp. has built a company-wide framework for protecting the personal data of customers and other parties. We practice integrated management of personal data from the three perspectives of data management, information security and information systems, with designated officers responsible for each.


CEO
Chief Executive Officer
CISO
Chief Information Security Officer
• Security measures
• Risk management
CDO
Chief Data Officer
• Making rules and decisions on data use
CIO
Chief Information Officer
• Building information systems
• IT governance

Building High-quality Social Communication Networks

Value Creation 3 Promote Data Security and Privacy Protection Initiatives

Privacy Protection Initiatives

Rules

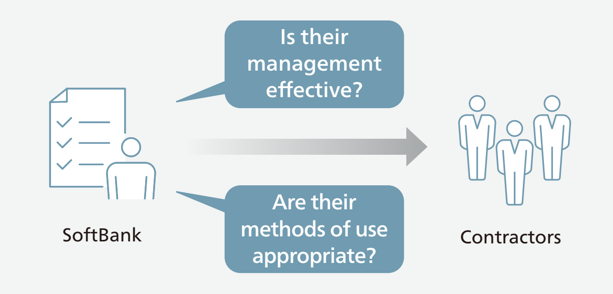
SoftBank Corp. has established internal regulations regarding the handling of personal data, clearly stating its policy in this area. We ensure internal awareness of our strict stance against the leakage, loss, and damage of personal data. In the event of such an incident, we take appropriate measures, including disciplinary action, based on the employment regulations.

In addition, all SoftBank Corp. employees and temporary staff who handle such personal receive training once a year to ensure the appropriate handling of such data.

Outsourcing

SoftBank Corp. sometimes outsources all or part of its operations that involve handling personal data, including customer inquiry response for various services, facility maintenance and fee-related operations. We thoroughly screen the qualifications of contractors when forming outsourcing agreements. Safety management measures, confidentiality, terms of subcontracting and other matters related to the proper handling of personal data are set out in such outsourcing agreements. Throughout the period of outsourced operations, we regularly monitor outsourced work to ensure appropriate oversight.

When performing operations outsourced to SoftBank Corp. from other companies, we use any provided personal data only within the scope necessary to complete the purpose of the outsource agreement.


Is their management effective?
SoftBank
Are their methods of use appropriate?
Contractors

Security Measures

In order to prevent leaks of personal information and other such incidents, SoftBank Corp. takes necessary and appropriate safety management measures, such as access control, restrictions on the removal of information from designated areas, and measures to prevent unauthorized access from the outside.

In order to make security measures effective, SoftBank Corp. thoroughly enforces compliance with the Personal Information Protection Management System and carries out risk assessments on a regular basis. When a risk is discovered, SoftBank Corp. takes appropriate measures and conducts monitoring to minimize the risk. There is also a system in place to internally audit whether personal data is properly protected.

Cyberattack Defense

We implement wide-ranging cyberattack countermeasures, such as monitoring for DoS attacks on our telecommunications service equipment, malware infections of employee computers and access to unauthorized websites.

Constant Monitoring by Specialists

Our Security Operation Center (SOC) provides specialized security monitoring 24 hours a day, 365 days a year.

Preventing Data Theft

We grant only the minimum necessary data access privileges to employees and collaborators, and activity on work computers is monitored and logged.

Data Storage Limitation

We set limits on how long personal data is stored based on the period needed to achieve its purpose of use (including legally required storage periods).

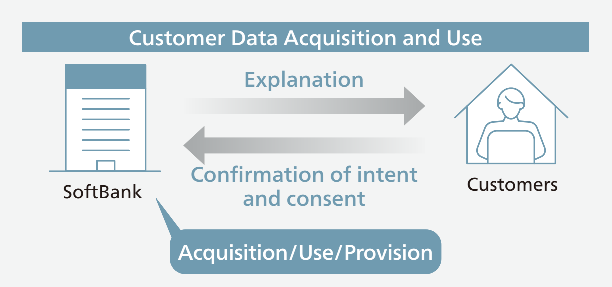
Privacy Protection Initiatives

Privacy Protection and Consideration for Customers

Appropriate Acquisition, Use, Provision and Publication of Personal Data

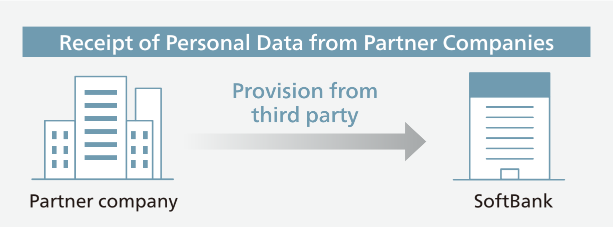
In consideration of privacy, SoftBank Corp. limits the acquisition, use and provision of personal data. When acquiring personal data, SoftBank Corp. clearly specifies the purpose of use via legal and fair means, such as in writing (on application forms, etc.), on screen (on websites, etc.) or verbally. In addition, SoftBank Corp. uses, provides and publishes personal data in an appropriate manner, taking into consideration business content and scale. In particular, the handling of sensitive information is based on the consent of the individual and limited to the extent necessary for business execution, except when otherwise stipulated by law.

Customer Data Acquisition and Use



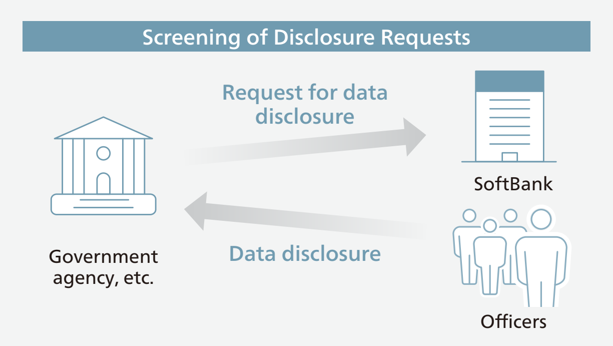
In addition, personal data is retained for the period required to achieve its purpose of use (including legally required storage periods). Personal data received from third parties is handled in compliance with laws and regulations, with respect for the privacy principles of the provider, and in adherence to the conditions stipulated in any agreement separately executed between the provider and SoftBank Corp.

Receipt of Personal Data from Partner Companies



When a government agency requests personal information, the Chief Data Officer (CDO) confirms the validity of the request. When providing personal data to a third party, SoftBank Corp. obtains the consent of the individual as required by law.

Screening of Disclosure Requests



In the event of human rights violations related to personal data, we promptly investigate and take necessary corrective actions. In the event of human rights violations related to personal data as a result of providing personal data to a third party, SoftBank Corp. takes necessary measures, such as setting up a point of contact to provide remedy to affected individuals.

Handling of Communications Information

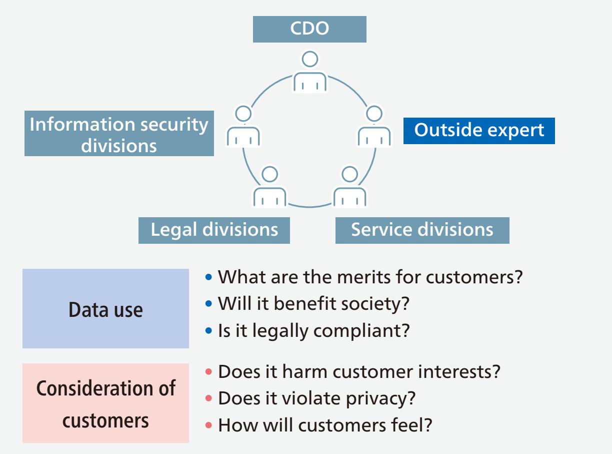
SoftBank Corp. manages personal data related to the confidentiality of communications especially strictly. We do not acquire, store, use or provide information pertaining to the confidentiality of communications, such as communication history, call history or caller information, except when necessary to provide telecommunications services, when the customer has given consent, when required by law or when there is other justifiable cause for noncompliance with the law.

Information pertaining to the confidentiality of communications is promptly deleted after handling.

When providing telecommunications subscriber information to third parties, including outsourcing contractors, we comply with Article 4 of the Telecommunications Business Act and other related provisions regarding the protection of the confidentiality of communications.

Privacy Impact Assessment

When SoftBank Corp. utilizes personal data, a team of experts that includes an outside expert assesses the impact of said data use. The multifaceted assessment covers not only laws and regulations, but also merits to customers, contribution to society, and disadvantages and negative sentiment caused for customers, in order to confirm that the use of data will provide safety and security to customers.


CDO
Information security divisions
Outside expert
Legal divisions
Service divisions
Data use
• What are the merits for customers?
• Will it benefit society?
• Is it legally compliant?
Consideration of customers
• Does it harm customer interests?
• Does it violate privacy?
• How will customers feel?

Building High-quality Social Communication Networks

Value Creation 3 Promote Data Security and Privacy Protection Initiatives

Privacy Protection Initiatives

Reporting and Future Initiatives

In FY2022, there were no legal violations resulting in disciplinary action from the authorities (such as personal information leaks or use outside of the intended purpose), complaints or other major accidents involving privacy.

We will continue to make revisions and improvements in order to protect the personal data of our customers and other stakeholders.

SoftBank Corp. may revise all or part of the contents of the Personal Data Protection Policy. Any significant changes are announced in an easy-to-understand manner on our website.

■ Scope of the Personal Data Protection Policy

The Personal Data Protection Policy applies to all subjects of personal data acquisition by SoftBank Corp., including customers and the employees of SoftBank Corp. and of business partners.

The Personal Data Protection Policy applies to all personal data acquired by SoftBank Corp. unless otherwise specified.

Provision to Overseas Third Parties

When permitted by customer consent or by laws and regulations, SoftBank Corp. may provide customers' personal data to overseas third parties (including when outsourcing operations). When transferring data to other countries, we consider systems for protecting personal data in the countries in question and provide personal data only if they meet standards equivalent to those in Japan.

Specifically, we implement safety management measures according to the following two categories.

1. Countries and regions with personal information protection systems equivalent to those in Japan (the European Union, etc.)
   We thoroughly screen the qualifications of enterprises to which we provide data. Safety management measures, confidentiality, terms of subcontracting and other matters related to the proper handling of personal data are set out in contracts with such enterprises. We regularly monitor the handling of personal data to ensure appropriate oversight.
2. Countries and regions without personal information protection systems equivalent to those in Japan
   Aside from handling data in the countries and regions described in 2. above, in operations elsewhere, we do not store data and we have in place measures to ensure adequate data protection, including mechanisms for viewing data without storing it, and the use of security rooms with strict entry and exit control.

   In addition, every year, we confirm the status of systems that could impact the handling of personal data, based partly on information published by Japanese government agencies.

SoftBank AI Ethics Policy

Under the "Beyond Carrier" strategy, SoftBank Corp. is moving beyond its previous framework as a telecommunications carrier, using cutting-edge technologies, such as AI and IoT, to provide innovative services and advance DX.

The use of AI, in particular, has been expanding across all industries in recent years. Going forward, uses of AI are expected to continue diversifying, and AI technologies are forecast to continue growing more sophisticated.

However, AI is a technology that requires ethical considerations and caution, as it may, for example, lead to discriminatory evaluation and selection, depending on how it is utilized.

Against this backdrop, SoftBank Corp. has established the SoftBank AI Ethics Policy in order to appropriately utilize AI to provide safe services that customers can use with confidence.

Specifically, the policy lays out guidelines covering six areas: "Principle of Human-Centeredness," "Respect for Fairness," "Pursuit of Transparency and Accountability," "Ensuring Safety," "Privacy Protection and Security" and "Development of AI Human Resources and Literacy." We will conduct business operations and develop services in line with these guidelines.

We have also set up a system by which the SoftBank AI Ethics Policy may be applied by group companies. As of June 1, 2023, 56 companies have applied the policy and established internal guidelines with more specific rules. Going forward, we will continue to work within the group to strengthen the framework, including the establishment of an external committee consisting of AI experts.

➔ Details