

Safety and Security

P. 054

Reinforce information security

0

Number of service suspensions

P. 057

Personal information protection

1

Number of incidents of personal information leaks

P. 059

Ensure stability and reliability of telecommunications services

100%

Stable service provision rate

Safety and Security

CSR Priority Activities	Medium-term Targets	CSR Quantitative Indicators	KPI	Target Achievement FY	Result (FY)		
					2017	2018	2019
Reinforce information security	Suspension of telecommunications services due to cyber attacks from the outside*1	Number of service suspensions	0	2020	—	—	0
	Number of incidents of personal information leaks due to cyber attacks from the outside*1	Number of incidents of personal information leaks	0	2020	—	—	1
Personal information protection	Zero incidents of personal information leaks	Number of incidents of personal information leaks	0	—	2	1	1
Ensure stability and reliability of telecommunications services*4	Provide stable telecommunications services free of major communications problems	Stable service provision rate*2	99.99%	—	100%	100%	100%
		Number of major accidents*3	0	—	0	0	0

*1 Newly established in fiscal 2020

*2 $[1 - \text{total hours under the impact of major accidents (number of affected users} \times \text{hours of major accidents)} / \text{total hours of major service provision (number of users} \times 24 \text{ hours} \times 365 \text{ days)}] \times 100\%$

*3 Number of accidents that led to a suspension of telecommunications services or a decline in communications quality that meet the following criteria regarding duration and number of people affected:

- Emergency call services (110, 119, etc.): at least 1 hour affecting at least 30,000 users
- Voice services other than emergency calls: at least 2 hours affecting at least 30,000 users, or at least 1 hour affecting at least 100,000 users
- Internet-related services (free of charge): at least 12 hours affecting at least 1 million users, or at least 24 hours affecting at least 100,000 users
- Other services: more than 2 hours affecting 30,000 users, or more than one hour affecting 1 million users

*4 Targets of statistics: Four telecommunications business companies (NTT East, NTT West, NTT Communications, and NTT DOCOMO)

Reinforce Information Security



Relevant GRI Standards: 102-12/103-2/203-2

Policies and Concepts

With the progressing digitalization of society and the economy and changes in international circumstances, security threats are becoming more serious and sophisticated, particularly cyber-attacks. Within this environment, the NTT Group has a responsibility to protect ICT service infrastructure and customers' basic rights, freedoms, and information assets, as well as to provide a sound foundation for the growth of the digital economy.

When formulating our medium-term management strategies in 2018, we made it our mission in terms of security to contribute to the building and development of a free, open, and safe ICT platform for supporting the infrastructure of the digital economy. We also made it our vision to realize the digital transformation of both customers and NTT itself, and for that reason, we will be chosen by customers.

In order to realize these, we will strive to engage in research and development that leverages the scale of the Group, realize superior abilities for early detection and rapid response, cultivate human resources who share the values of sincerity and advanced skill, and transcend profit-focused principles to transmit pioneering knowledge to society.

The appropriate handling of personal information is a focus of growing interest worldwide and it is also important to have countermeasures to large-scale, sophisticated cyber-attacks targeting things like international events. As a member of the global community building the digital society, the NTT Group will contribute to solving social issues through our security business.

NTT Group Information Security Policy

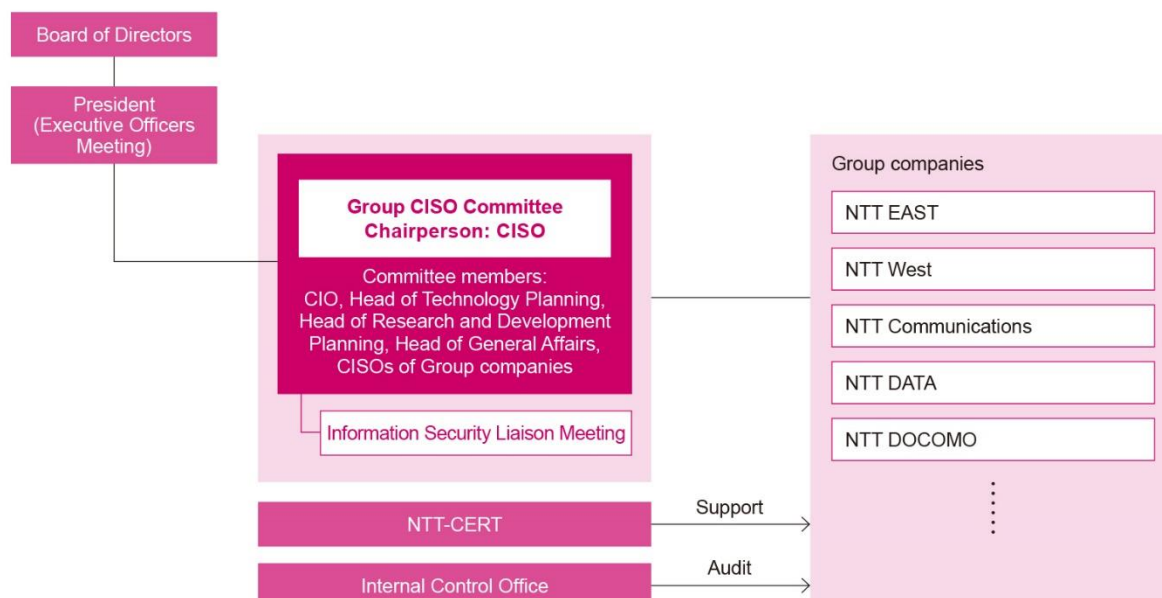
NTT Group will continue to provide safe and secure services and to be a trusted company, as a responsible carrier in the information and telecommunication industry. NTT Group will strive to ensure information security and contribute to the sound development of society in accordance with the following policies.

1. NTT Group will (a) be fully aware of the importance of information security in society, (b) strive to establish a safe, secure and convenient communication network environment and (c) strive to ensure information security.
2. All NTT Group employees, executives will (a) be fully aware that the protection of information is the basis of NTT Group's business activities and corporate social responsibility, (b) protect the secrecy of telecommunications and comply with relevant laws and regulations, including "the Act on the Protection of Personal Information".
3. NTT Group will continuously take necessary information security measures such as (a) establishing the information security management system, (b) taking strict security measures, both on the physical and technological aspects, in order to prevent unauthorized access and information loss, falsification, and leaks, (c) ensuring employee education, (d) providing appropriate supervision of outsourcing contractors.

📄 **NTT Group's Information Security Policy** <https://www.ntt.co.jp/g-policy/e/index.html>

Organization for Implementation

The NTT Group enforces information security management under the charge of the Chief Information Security Officer (CISO), and is thorough in its information security management. We have also established a Group CISO Committee, and formulate Group information security management strategies, plan and implement related measures, undertake human resources training, and otherwise engage in activities in collaboration with companies across the Group.



Main Initiatives

Strengthen Service Security

Information communication services are an important social infrastructure and a foundation for the digitalization of society and the economy, so to provide these services in a safe and secure manner, we are working to strengthen the security of telecommunications equipment, IT service environments, and all services provided by smart cities, smart buildings, and the like.

Global Cooperation within the NTT Group

With the integration of our global businesses, we are advancing global partnerships in the security field. This NTT Group cooperation includes many businesses and regions and incorporates an approach to risk-based management, the introduction of a framework that acts as a shared language, and the setting of standards that should be met by all Group members in regard to identification, defenses, detection, response, and recovery.

Engaging with and Contributing to the Global Community

We are engaging with the cybersecurity initiatives of governments and industries around the world, particularly in North America and Europe, by sharing information and best practices in regard to security threats and building a community of companies and organizations based on mutual trust.

Training Security Experts in the NTT Group

As a measure to enhance security personnel development with the aim of improving in terms of both quantity and quality, NTT Group companies are implementing human resource development measures based on the types and levels of security personnel.

NTT Group's Security Personnel Hierarchy

		Title	Job classification		
			Security management consulting	Security operation	Security development
Level	Advanced	Security master	Produce first-rate experts with best performance in the industry		
		Security principal			
	Intermediate	Security professional	Reinforce the pool of specialists with deep experience and judgment		
	Beginner	Security expert	Raise the level of workers who can do their work with the required knowledge		

Information Security Training

Each Group company seeks to raise information security literacy by organizing training for all employees as well as the employees of partner companies. Training is offered through e-learning, and all employees are obliged to participate in the course once a year. Looking ahead, we are considering unifying training content throughout the Group to provide employees with a standard level of knowledge on information security required in their business operations. By doing so, we will seek to enhance the security capabilities of the NTT Group and reinforce its human resources to deliver safe, secure services for our customers and society at large.

Research and Development Initiatives

In addition to advancing the technological development of service security, we are focusing on developing elemental security technologies. In 2019, we established a global research center for research into cybersecurity and encryption technology centered around some of the world's leading researchers.

Management of CSIRT

The NTT Group established NTT-CERT in 2004 to function as a computer security incident response team (CSIRT). This team collects information regarding security incidents associated with the Group. It then offers support for addressing these incidents, formulates measures to prevent recurrence, develops training programs, and provides security-related information. As a central element of the NTT Group's security initiatives, NTT-CERT provides a reliable venue for consultations regarding information security. The team also collaborates with organizations and specialists inside and outside the NTT Group to offer support for detecting and resolving security incidents, minimizing damages, and preventing occurrence. NTT-CERT is thereby contributing to better security for both the NTT Group and societies that are permeated by information networks.

Moreover, NTT-CERT coordinates with the United States Computer Emergency Readiness Team (US-CERT^{*1}) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC^{*2}) and is also a member of the Forum of Incident Response and Security Teams (FIRST) and the Nippon CSIRT Association,^{*3} which enables it to coordinate with domestic and overseas CSIRT organizations. This coordination makes it possible for NTT-CERT to share information on relevant trends and response measures. In addition, NTT-CERT participates in the cross-industry drills held by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to share expertise and gather information. NTT-CERT also plays a role in promoting the establishment of CSIRTs at Group companies and helping improve their response capabilities.

NTT-CERT will expand its collection of information on vulnerabilities and attacks to cover areas including the dark web and will strengthen its information analysis platform and further automate and enhance its response to cyber threats in order to continually respond to threats as they change.

^{*1} US-CERT: An information security preparedness organization under the Department of Homeland Security (DHS)

^{*2} JPCERT Coordination Center: An organization that collects reports inside Japan, supports responses, monitors situations, analyzes entry points, and reviews and provides advice on measures for preventing reoccurrences from a technical standpoint with regard to computer security incidents such as intrusions through the Internet or service interruptions

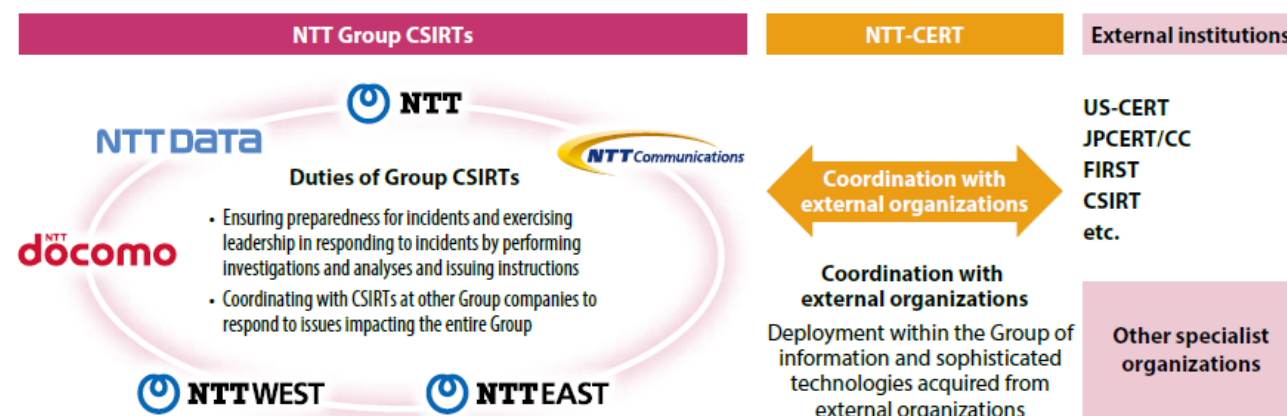
^{*3} NTT-CERT founded the Nippon CSIRT Association

📄 **NTT-CERT** <https://www.ntt-cert.org/index-en.html>

📄 **Nippon CSIRT Association** <https://www.nca.gr.jp/en/>

📄 **FIRST Forum of Incident Response and Security Teams** <https://www.first.org/>

NTT Group CSIRT Activities



Personal Information Protection



Relevant GRI Standards: 103-2

Policies and Concepts





The NTT Group has been entrusted with a considerable quantity of personal information, ranging from data on individual customers to that of corporate customers. In recent years, our customers' concern over protection of personal information has only increased. Meanwhile, the importance of enforcing personal information protection and information management is growing in terms of laws and regulations, as seen in the revision of Japan's Act on the Protection of Personal Information in 2017 and the enactment of the EU's General Data Protection Regulation (GDPR) in 2018.

Under these circumstances, personal information leakage could have various repercussions for the NTT Group in the operations of its businesses, including damage to its corporate value and loss of customers, which makes it essential to rigorously manage personal information as a top priority.

Organization for Implementation

Under the NTT Group Information Security Policy, we disclose on our website specific policies for protecting the personal information of customers and shareholders and policies for protecting personally identifiable information required by Japan's Social Security and Tax Number System. In this policy, we also define how we respond to requests for disclosure, correction, and suspension of use related to the personal information retained by the NTT Group. We have also put in place a security management system that ensures thorough and rigorous security practices, with the Chief Information Officer (CISO) placed in charge (see page 054).

Policy on Protecting Personal Information

-  **Policy on Protecting Personal Information of Customers** <https://www.ntt.co.jp/kojinjo/e/customer.html>
-  **Policy on Protecting Personal Information of Shareholders** <https://www.ntt.co.jp/kojinjo/e/shareholder.html>
-  **Policy on Protecting Specific Personal Information of Business Partners** https://www.ntt.co.jp/kojinjo/e/protection_bus.html
-  **Policy on Protecting Specific Personal Information of Shareholders** https://www.ntt.co.jp/kojinjo/e/protection_share.html

Main Initiatives

NTT has systematic security control measures, human security control measures, physical security control measures, and technical security control measures in place for handling our customers' personal information.

- (1) Systematic security control measures
We have created a statement outlining the building of management systems such as placing a person responsible for management of the committee and each organization, the establishment of internal regulations, management ledgers and process management charts, and other matters. Furthermore, we are also building management systems for handling ongoing improvements and the like.
- (2) Human security control measures
All employees who handle customers' personal information are informed and made aware of the importance of protecting this information, regardless of whether they are officers, regular employees, or temporary employees. We ensure employees conclude non-disclosure agreements and provide necessary auditing and supervision to ensure their effectiveness.
- (3) Physical security control measures
We enact various measures including controlling access to physical equipment which handles customers' personal information and the floors where these are kept, measures to prevent theft, measures to prevent damage to customers' personal information during incidents such as fires and lightning strikes, and the use of locks when taking out, moving, or storing systems and documents.
- (4) Technical security control measures
We have put in place various technical security control measures such as access management when accessing personal data including authentication, authority administration, control, and recording, countermeasures against viruses and malware in systems, measures for use when sending and receiving information including encryption and clarification of responsibility, and the monitoring of information systems.

Each domestic company in the Group has established a personal information protection system in line with its business and based on the revised Act on the Protection of Personal Information. We are consistently pursuing initiatives to protect information, including stringent measures on the physical and systems aspects of security and appropriate supervision of outsourcing contractors.

Main Initiatives of Domestic Group Companies

- Establishment of internal rules and regulations

- Employee training to ensure appropriate implementation of the above rules and regulations
- Establishment of an organization to promote information security management
- Establishment of a security management system for preventing illegal access to information or the loss, alteration, or information leakage as well as managing antivirus measures and the physical transfer of information

In addition, NTT Group companies that conduct business globally conform to the laws and regulations of the various countries.

To conform to the EU's General Data Protection Regulation (GDPR) enacted in May 2018, Group companies are promoting compliance following discussions within the NTT Group. They implement the measures necessary for the acquisition of personal information and its transfer outside of the EU, and, based on the EU regulation and other countries' regulations, are taking actions with respect to the sharing of employee information among NTT Group companies in Japan and overseas.

Establishment of Contact Points on Personal Information

NTT has set up the Customer Contact Point on Personal Information, and similar contact points for services related to personal information have been set up at each NTT Group company. Since NTT is a holding company that does not directly provide telecommunications services, inquiries regarding personal information related to services are redirected to the contact points of the operating companies concerned.

Additionally, inquiries regarding the handling of personal information under laws and regulations are redirected to the person responsible for information security at the operating companies concerned.

Nippon Telegraph and Telephone Corporation Customer Contact Point on Personal Information

Email: ntt.kojin.uz@hco.ntt.co.jp

 <https://www.ntt.co.jp/kojinjo/e/customer.html>

Ensure Stability and Reliability of Telecommunications Services



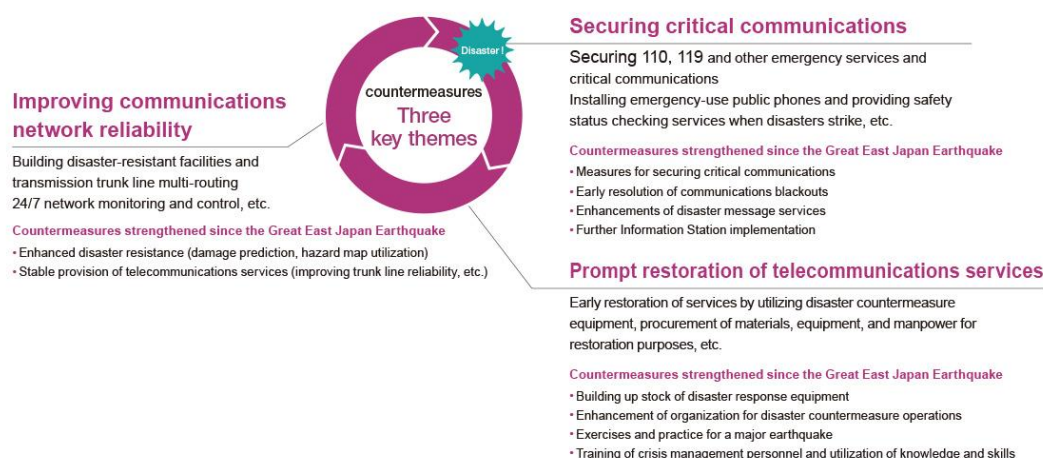
Relevant GRI Standards: 103-2/413-1/203-1

Policies and Concepts

As a corporate group with the mission of serving society by sustaining telecommunications infrastructure in normal times, the NTT Group is committed to building highly reliable telecommunications networks that connect people anytime, anywhere. Since telecommunications takes on a greater importance in the event of a disaster, we endeavor to secure the means of communication necessary for maintaining public order and for rescue and restoration operations at times of disasters, and for emergency communications, such as 110, 118, and 119. Japan is a country particularly prone to natural disasters such as earthquakes and typhoons. The importance of telecommunications networks was reaffirmed by the devastating Great East Japan Earthquake. Facing the possibility of an earthquake directly underneath Tokyo or the Nankai Trough off Japan's southern coastline, there is a pressing need for society to prepare for such potential disasters while ensuring the stability and reliability of its telecommunications infrastructure.

The NTT Group has defined three key themes for disaster countermeasures: securing critical communications, prompt restoration of telecommunications services, and improving network reliability. We have been strengthening efforts based on these themes since the Great East Japan Earthquake. We have also included Disaster Countermeasure Initiatives in our medium-term management strategy and are making a focused effort to further reinforce the communications infrastructure, seek proactive disaster response, and adequately provide information to the affected people.

NTT Group's Basic Policy on Disaster Countermeasures



Organization for Implementation

Five Group companies —NTT, NTT East, NTT West, NTT Communications, and NTT DOCOMO— are designated public institutions under the Basic Act on Disaster Control Measures. Accordingly, based on this Act, in preparation for a disaster, the NTT Group has formulated the Disaster Management Operation Plan for the purpose of smooth, appropriate implementation of measures to prevent damage. Each company has prepared their respective Disaster Management Operation Plan by organizing response efforts that are mobilized at the time of a disaster in a manner proportionate to the scope and circumstances of the situation. At the same time, we will maintain close contact with the relevant government institutions to ensure a smooth and appropriate recovery from the disaster and secure critical communications.

We are also taking measures in normal times to improve the reliability of our telecommunications infrastructure. To ensure that our telecommunications services operate without interruption at all times, we employ transmission trunk line multi-routing, have enacted blackout countermeasures for telecommunications buildings and base stations, and are making telecommunications buildings more quake-proof. In addition, we are expanding the assortment of power supply vehicles and other disaster response equipment that we have positioned throughout Japan and are repeatedly conducting training to prepare for major natural disasters. We are making a daily effort to secure the necessary emergency and critical communications.

■ **NTT Group Disaster Management Operation Plan** <https://www.ntt.co.jp/saitai/plan.html> (Japanese only)

Main Initiatives

Securing Critical Communications

To secure necessary communications in the event of a disaster, the NTT Group is implementing various response measures, including the installation of emergency-use public phones, a mobile phone lending service in affected areas, and providing means to confirm the safety of people in affected areas. We simultaneously install multiple lines to secure connections to

the headquarters of the police department, fire department, and coast guard to prepare against the possibility that the 110, 119 and 118 emergency call services may be damaged.

A major disaster could also lead to social disorder, such as the disruption of transport systems. In such an event, we would consider the overall situation, including whether other telecommunications carriers have put restrictions on mobile and fixed line phones and, if necessary, offer the use of public phones for free.*

* We will not charge carriers for which we have set call fees and will not settle payments between carriers for which we have set connection fees. For the specific names of carriers, please refer to the following websites. (Japanese only)

Free charge public phone policy for areas covered by NTT East <http://www.ntt-east.co.jp/info-st/saigai/index.html>
 Free charge public phone policy for areas covered by NTT West <https://www.ntt-west.co.jp/ptd/basis/disaster.html>

Providing Services for Easy Safety Status Checking and Information Gathering When Disaster Strikes

The NTT Group launches and provides the following services to enable people to confirm the safety of relatives and friends in areas hit by a major disaster that has disrupted phone connections.

Main Services

171 Disaster Emergency Message Dial	We store recorded voice messages left by users to confirm the safety of those in affected areas
Web 171 Disaster Message Board	We store text messages left by users via the Internet
Disaster Voice Messaging Service (i-mode/sp-mode/mopera U)	We deliver voice messages reporting the status of personal safety via mobile phone
Disaster Message Board Service (i-mode/sp-mode)	We store text messages left by users via mobile phone

When we launch these emergency services in the event of a disaster or other contingency, we promptly inform our customers through the mass media, website and other means.

By integrating the Web 171 Disaster Message Board with the Disaster Message Board Service for mobile and PHS phones (i-mode/sp-mode), we have also made it possible to conduct one-stop searches spanning both services from the companies providing those services. There are additional functions for notifying designated contacts by e-mail or voice when safety status information is posted. We are continuing to make improvements, such as by offering support in English, Chinese and Korean for the Web 171 Disaster Message Board, and in English for the Disaster Message Board Service (i-mode/sp-mode), increasing the number of messages that can be posted and extending message storage time.

With regard to the Web 171 Disaster Message Board, NTT East and NTT West agreed to collaborate with the disaster message boards operated by NTT DOCOMO, KDDI, and SoftBank to allow users to check each other's messages left with these carriers since August 2019.

Securing the Stability and Reliability of Telecommunications Services

The NTT Group is devoted to early restoration of telecommunications services by deploying and enhancing the functions of mobile power supply vehicles, portable satellite equipment and other mobile equipment as well as participating in disaster drills held in the respective regions. The NTT Group endeavors to build disaster-resistant communications infrastructure and maintain and operate it in a way that ensures its proper functioning at all times by conducting regular safety patrols, replacing devices as a preventive maintenance measure, and other such means, in an effort to develop disaster-resilient communication networks and equipment.

Ensuring the Disaster Resistance of Telecommunications Equipment

We also strive to enable telecommunications equipment housings, pylons and other facilities to withstand contingencies such as earthquakes, storms, flooding, fire and power outages in accordance with predetermined design standards.

Main Measures

- NTT's telecommunications buildings and pylons are designed to withstand earthquakes of a seismic intensity of 7 on Japan's intensity scale and 60 m/sec winds experienced during the strongest typhoons
- Our facilities are equipped with flood doors and other defenses according to location to prevent inundation of telecommunications equipment by tsunamis or floods
- We equip our telecommunications equipment rooms with fire doors or shutters
- Our telecommunications buildings and wireless base stations are fitted with backup power sources to keep them running for extended periods in the event of sudden power outages. As a further fallback, power supply vehicles can be hooked up to them to supply power
- We use trunk line multi-routing to ensure that our telecommunications services operate without interruption at all times
- We deploy large-zone base stations capable of covering wide areas during disasters and other emergency situations
- We install emergency power supply fuel tanks

Increasing the Resilience of Equipment and Speeding Up Our Response

In recent years, disasters of greater magnitude have had significant impact. To address the increased impact on telecommunications equipment and services, as well as the longer time required to resume operations, we are also

promoting additional initiatives toward such goals as increasing the resilience of our equipment and speeding up recovery.

Main Initiatives for Increasing the Resilience of Telecommunications Equipment

- Expansion in medium-zone base stations equipped to deal with disasters, such as blackout countermeasures
- Blackout countermeasures that use electric vehicles at base stations
- Centralized management and mobilization of approximately 400 power supply vehicles owned by the NTT Group
- Consideration of underground installation of power transmission cables and use of fixed line phones to deal with the impact of disasters

Main Initiatives for Speeding Up Service Recovery

- Advanced launch of recovery framework (national wide-area support system and other frameworks) based on damage prediction using AI
- Reinforcement of the recovery framework and recruitment of personnel, including the use of retired NTT employees

Initiatives for Bolstering Support for Disaster Victims

- Delivery of realistic and concise information, including status of damage to communications, status of recovery, location of charging stations, public phones in operation during disasters, information for visitors and foreign residents, and more to support evacuation and other activities
- Response to consultations on problems related to communications through emergency 113 call centers dispatched to affected areas
- Collaboration with local governments and other public offices for installing Wi-Fi and charging stations inside public phone booths to secure telecommunications during a disaster

Providing Stable Telecommunications Services in Normal Times

To consistently provide secure telecommunications services to our users, the NTT Group operates a system for monitoring its telecommunications networks, implements measures for preventing accidents and failures, and works to enhance the skills of personnel responsible for network maintenance and operations.

Initiatives for Maintaining Stable Telecommunications Services

- Operational system for monitoring and controlling the status of network operations on a real-time basis, 24-hours a day, 365 days a year
- Collection and analysis of performance data for telecommunications equipment under ordinary circumstances to identify and deal with signs of failure
- Development of system that enables a fast, accurate response to unexpected incidents, and revised procedures
- Application of lessons learned from past accidents to similar cases and thorough reinforcement of standard procedures based on an analysis of cases that may result in serious accidents
- Implementation of training and drills and development of related mechanisms for fostering personnel handling network maintenance and operations

Providing Stable Telecommunications Services to Address a Large Spike in Demand Due to the COVID-19 Pandemic

NTT and its major subsidiaries in the telecommunications business have formulated operation plans to execute their responsibilities as designated public institutions and contribute to preventing infections from the standpoint of respecting human life. The spread of infections has been accompanied by an increased demand for Internet use and telework, significantly increasing data traffic, particularly between stationary communication terminals during daytime weekdays. The NTT Group companies have designed their existing networks to meet peak nighttime traffic and are currently capable of providing network capacity for daytime traffic. We will continue to bolster our equipment to deliver stable telecommunications services.

Operation of mobile phone base stations and terminals (NTT DOCOMO)

For more than 60 years, research has been conducted worldwide on the impact of radio waves on the human body. As a result, standards and systems have been put in place for the safe use of radio waves not only in Japan, but around the world, too.

In 1990, Japan's Ministry of Posts and Telecommunications (presently the Ministry of Internal Affairs and Communications) established its own Radio Radiation Protection Guidelines for Human Exposure to Electromagnetic Fields (RRPG) as a set of reference values for the safety of radio waves on the human body based on the results of research conducted over the preceding 40 years both inside and outside Japan. The reference values of these guidelines are the same as those recommended by the World Health Organization (WHO). Radio waves below these reference values are recognized internationally as having no adverse effects on health.

Mobile base stations and terminals of NTT DOCOMO are operated at levels lower than the reference values of the RRPG. Services are provided in compliance with related laws and ordinances incorporating the RRPG, which ensures DOCOMO mobile phones can be safely used.

📄 **NTT DOCOMO Radio Wave Safety** <https://www.nttdocomo.co.jp/corporate/csr/network/radio/safe.html> (Japanese only)