Building a Safe and Resilient Society

As a provider of telecommunications services, NTT DOCOMO pursues its mission of providing a communications environment that enables customers to use their mobile phones anytime and anywhere, and it strives to enhance customer security, safety, and comfort.
We set up the Network Division to spearhead our initiatives to ensure a consistently reliable network for customers by constructing and operating a total network service that includes communication devices and applications, securing communications during a disaster and guaranteeing the safety of radio waves used by mobile phones, and handling cyber security threats, which are becoming increasingly sophisticated and serious.

Materiality

Realize a Safe, Secure, and Resilient Society

Goal To fulfill our mission of providing a communications environment that can be used anytime, anywhere, and to ensure safe, secure, and comfortable communications for our customers

Sustainability Issues

- Deliver safe and stable services
- Ensure information security and privacy

Strategy

The NTT DOCOMO Group is committed to providing a network that its customers can always trust by ensuring stable service provision and pursuing network enhancement for 24/7 connectivity, giving consideration to radio wave safety, and responding to security threats.

Risks

Delays in network enhancement and stable service provision, as well as increasingly severe and frequent natural disasters, may affect the provision of services to our customers. Furthermore, information security threats such as cyber-attacks, data leaks, and fraudulent transactions in financial and payment services could lead to a decline in trust.

Opportunities

Considering technological trends, customer demands, and market trends, we will strengthen our network resilience, rapid recovery response, and information security to support the life infrastructure of our customers, leading to improved customer satisfaction and brand image.

FY2024 Initiatives

- To improve the quality of our telecommunications services, we increased the number of Sub6 base stations nationwide by 1.2 times compared to fiscal 2023. We also expanded facilities and base stations at large event facilities, major railway routes nationwide, and major urban centers.
- In fiscal 2024, we received 100,000 inquiries about signal quality. In addition to increasing base stations, we implemented DOCOMO repeaters and femtocells in indoor areas to improve signal quality.
- We introduced a wireless priority control function and launched a service that ensures stable communications even in congested areas and during busy hours.
- To ensure rapid network recovery in the event of a large-scale disaster, we established a new cooperative framework among eight telecommunications providers, including NTT DOCOMO, and began jointly using assets owned by each company (offices, accommodation, material storage areas, refueling bases, etc.), including ships.
- The NTT DOCOMO Group and Ishikawa Prefecture concluded a comprehensive partnership agreement with the aim of recovery, reconstruction, and regional revitalization following the 2024 Noto Peninsula Earthquake and Oku-Noto Heavy Rains.
- We expanded our security personnel certification system and strengthened human resource development.

Key FY2024 Results

P. 23 Metrics and Targets

Number of major accidents	Number of accidents in life infrastructure systems	Number of serious cyber-attack incidents	Number of serious information leaks
1	0	0	0

Provision of Network Services

Basic Philosophy

NTT DOCOMO is constantly improving its network services to consistently satisfy customers. Building base stations to expand our service areas offers connectivity to customers wherever they are, in the city, on the subway or in remote locations, or in relatively unpopulated areas. We also work to maintain a system that ensures connectivity around the clock, all year round, regardless of circumstances that may arise in the course of daily life or at special events.

We are improving connectivity during spikes in service demand and raising the reliability of our telecommunications services during network failures by implementing the network functions virtualization technology.

Overall Layout of NTT DOCOMO's Network

The NTT DOCOMO telecommunications network comprises the radio access network, core network, service platform, various mission-critical systems, and the operation system.

Expansion of the Service Area

Building Base Stations

NTT DOCOMO is actively expanding base station deployment to further improve call and communication quality and broaden service areas. For base stations for 5th generation (5G) mobile communications, we began providing commercial service on March 25, 2020. We had built approximately 51,000 stations by the end of March 2025 and continue to work on further enhancing the communication environment.

Prioritizing communication service quality improvement as a top priority, NTT DOCOMO increased the number of Sub6 base stations capable of high-speed, large-capacity communication by 1.2 times compared to the previous fiscal year in fiscal 2024. In addition to large facilities such as Tokyo Big Sight, Belluna Dome, and Suzuka Circuit, we increased equipment capacity and base stations in major urban centers and along railway routes nationwide, achieving all communication improvement targets.

DOCOMO's Communication Improvement Initiative Declaration FY2024 (in Japanese only)

DOCOMO's Approach to Installing Base Stations

Some neighbors are concerned about the effects of electromagnetic waves, while others are ambivalent about the construction of base stations. Therefore, prior to building a new base station, we provide detailed information to local residents in accordance with prevailing laws and regulations as well as to those residents in areas without such formal mandates, in accordance with NTT DOCOMO's internal rules. We also hold briefings and public hearings in advance to listen carefully to the opinions and concerns of local residents, and we only start construction after considering environmental impact and ensuring that the community will not be negatively affected.

We strive to minimize inconvenience by providing clear explanations and creating work schedules while considering the daily lives of local residents. During construction, we place top priority on the security and safety of residents, and our work includes efforts to support social infrastructures, such as improving the local emergency communication system.

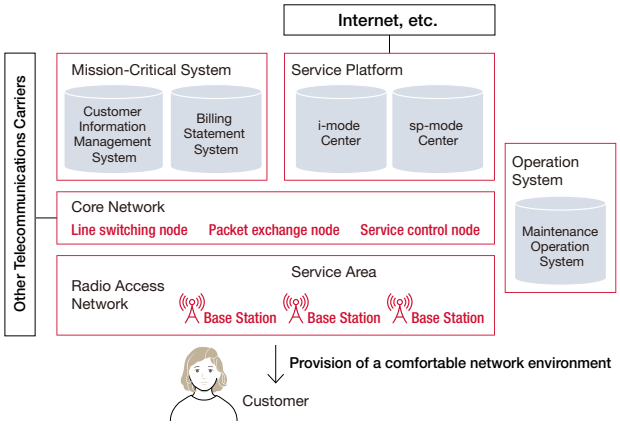
Inspecting and Improving Reception Quality

NTT DOCOMO broadly solicits customer information on mobile phone reception to ensure its communications quality and expand the coverage area. In fiscal 2024, we received approximately 100,000 customer inquiries and opinions.

To respond sincerely to customer feedback, we comprehensively monitor and evaluate reception by combining it with traffic data, app data, and AI-based estimates of perceived network quality. We are improving communications quality through these efforts while building more base stations in an effort to ensure a more stable environment for our mobile phone users.

For customers who request better indoor reception, we offer them solutions depending on the signal strength. Specifically, we are working to improve indoor signal strength by using DOCOMO repeaters that amplify signals or femtocells that transmit radio waves.

➤ DOCOMO's Network Layout



Ensuring the Quality of Communications Services during Large Events

Major events and exhibitions gather large numbers of customers in a single location. Local base stations may experience intermittent overloads causing spotty phone service when these customers use their mobile phones at the same time. NTT DOCOMO is taking various measures to prepare for the anticipated sudden concentration of communication traffic. In addition, we are systematically expanding the facility capacity of our networks in response to customer usage status.

Examples	Details
Events such as fireworks and concerts	• Disperse communication load by installing mobile base stations and Wi-Fi access points • Secure communication capacity by setting up base station facilities to cover the venue and modifying the software that controls the facilities

Enabling Communications in Remote or Relatively Unpopulated Areas

NTT DOCOMO has drawn up its Basic Policy on Area Expansion to strategically develop base stations in remote or relatively unpopulated areas. Our service coverage ratio in Japan for both 3G FOMA and 4G LTE has reached nearly 100%.

We also respond to temporary spikes at locations such as tourist spots that experience intermittent surges in visitor demand. These measures have helped climbers make rescue calls when they are hurt or lost and have increased the number of lives saved.

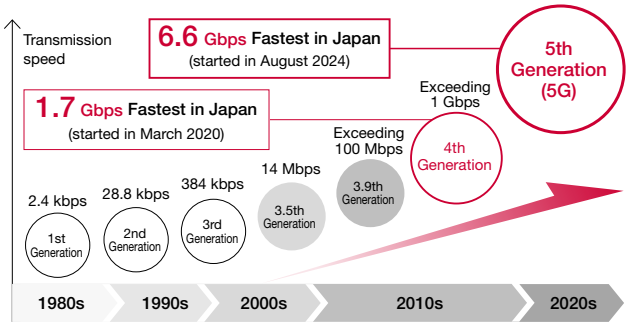
Examples	Details
During the Mt. Fuji climbing season	• Provide stable telecommunications services by installing a temporary base station at the summit
Mountain trails where radio waves are blocked by the surrounding terrain or foliage	• Install special antennas along mountain trails or compact base stations on the roofs of mountain huts
Using mobile phones in shinkansen tunnels	• Provide mobile phone service in all shinkansen tunnels in Japan

Overseas Use of Mobile Phones

NTT DOCOMO is enhancing its international roaming service so that customers can enjoy the convenience of using their mobile phones overseas. Our WORLD WING service allows customers to continue using the DOCOMO mobile phones they use in Japan within the areas covered by our overseas carrier partners while retaining the same phone number and email address. We have been expanding the number of countries and regions covered by our LTE-based, high-speed communication, LTE international roaming services, and our VoLTE international roaming services that offer high audio quality. As a result, mobile phones under contract with NTT DOCOMO can be used in over 200 countries and regions as of the end of June 2025.

Seeking High-Speed, Large-Capacity Communications

Starting with the first generation (1G) based on analog transmission in the 1980s, NTT DOCOMO has developed new generations of mobile communication systems roughly every decade. Over the years, we have dramatically increased transmission speeds and network capacity while also focusing on initiatives to provide more comfortable communications.



Note: Only available in some areas. Communication speeds represent maximum technical specifications for sending and receiving and do not indicate communication speeds under actual conditions. Communications are provided on a best effort basis and actual speeds may vary depending on the communications environment or network congestion.

➤ **Results of Effective Speed Tests**

	Download Speed	Upload Speed
Android™	70 Mbps–353 Mbps	10 Mbps–30 Mbps
iOS	63 Mbps–366 Mbps	10 Mbps–33 Mbps

Note: Effective speeds were measured in ten cities nationwide from January to March 2025 based on the guidelines established by the Ministry of Internal Affairs and Communications. Half of the results close to the median were within the above ranges. Effective speeds vary depending on customer location, time, and communication environment.

PREMIUM 4G

In December 2015, NTT DOCOMO launched PREMIUM 4G, a communication service using LTE-Advanced. The maximum downlink transmission speed of this service reached 1.7 Gbps as of March 2020, following the introduction of high-speed technologies such as carrier aggregation, 256 QAM, and 4×4 MIMO.

We are also monitoring customer traffic volume and expanding our service areas in major cities in Japan where traffic is concentrated. NTT DOCOMO will strive to provide networks for enjoying various content such as video, music, and SNS by meeting the needs of each individual customer.

Higher-Speed, Larger-Capacity Communications after Launch of 5G Services

NTT DOCOMO started 5G commercial service in March of 2020. While fully leveraging the strengths of 5G, including high speed, large capacity, low latency, and massive device connectivity, NTT DOCOMO will continue to be a leading global innovator in communications in realizing ever higher speeds, with its know-how in network operations and leading-edge technical development capabilities cultivated for more than 20 years.

By using three new frequency broad bands (3.7 GHz, 4.5 GHz, and 28 GHz) dedicated to 5G, we are able to provide high-speed, high-capacity communications.

Offering 5G Services Using SA (Standalone) Architecture

NTT DOCOMO has been offering 5G SA (Standalone) services to corporate customers since December 2021, with the introduction of 5GC (5G-Core), a core network device dedicated to 5G. 5G SA service enables even faster and larger capacity communications than standard 5G and is aimed at industrial development through the creation of solutions for a variety of industries and business categories.

In August 2022, NTT DOCOMO also started offering 5G SA as an optional service for customers who subscribe to NTT DOCOMO's 5G rate plans. The service locations were expanded mainly to major train stations and commercial facilities in fiscal 2022 and were broadened to include stadiums, universities, and airports in fiscal 2023. The 5G SA service is available on smartphones and delivers up to 6.6 Gbps download and 1.1 Gbps upload speeds*1. Prior to implementing network slicing*2 enabled by 5G SA, we introduced Wi-Fi Multimedia (WMM) in April 2024 to prioritize network traffic and ensure stable communications, even in congested areas and during high-volume periods, by preferentially assigning packets to certain users over general users. With the network slicing, we aim to leverage the unique potential of 5G to provide users with a network service that can flexibly correspond to each purpose and service.

*1 Indicate the fastest possible values based on technical standards and do not necessarily represent actual usage speeds. This is a best-effort service, and the actual speeds may vary depending on such factors as the communications environment and network congestion.
*2 Technology to divide and optimize the core network by service units such as use cases and business models in operating 5G networks.

Even Faster Communication Speeds

Since the launch of 5G services NTT DOCOMO has engaged in technical planning and R&D for the sophistication of 5G (5G Evolution) and introduction of 6G in the 2030s to seek even higher communication speeds. To realize 5G Evolution & 6G, we are taking on challenges in new areas such as the extension of ultra coverage to land, air, and sea and the development of ultra-low power consumption to help achieve carbon neutrality. We also aim to further evolve services to achieve ultra-high speed, larger capacity, ultra-high reliability, lower latency, and ultra-multiple connection, enabled by 5G.

P. 68 Expanding Connectivity across Land, Sea, and Air

Ensuring a Stable Network

Network Surveillance and Response to Network Failures

NTT DOCOMO strives to construct mechanisms for minimizing impact on its service when a problem arises in order to provide a reliable network that customers can depend upon anytime, anywhere.

Providing Year-Round Surveillance and Response for Network Facilities

NTT DOCOMO maintains network operation centers in Tokyo and Osaka that ensure connectivity by conducting surveillance of our network facilities and equipment, such as base stations, as well as monitoring the status of our service to customers nationwide, around the clock throughout the year. We are also committed to establishing mechanisms for preemptively addressing potential failures in network facilities that could interrupt its service to customers.

For example, we collect data on network facilities every day under normal operating conditions and are constantly analyzing the data. We analyze any anomalies as they arise to determine whether they may be warning signs of an impending failure, and we respond through such action as replacing faulty equipment in advance. We also use AI to identify failures that had been difficult to detect by conventional methods. We are continuously exploring new technologies and fine-tuning our systems to further improve customer satisfaction.

When informed of an abnormality, operators promptly respond by remotely controlling network facility and traffic routes to prevent any disruption in service. They also investigate the cause of the problem, and when the facility requires repairs due to physical or other damage, maintenance staff is dispatched to the site to quickly replace and repair the network equipment.

➤ Incidents of Serious Facility Failures

FY2021	FY2022	FY2023	FY2024
1	3	4	1

Scope: DOCOMO

NTT DOCOMO's Disaster Preparedness

Applying the Three Principles of Disaster Preparedness to Secure Communications in Times of Disaster

Mobile phones play a critical role in rescue operations, reconstruction, and confirmation of personal safety during disasters and emergencies. Since its founding, NTT DOCOMO has been continuously working to secure communications during disasters in accordance with its Three Principles of Disaster Preparedness: enhance system reliability, ensure essential communications, and rapidly restore communications services.

Applying lessons learned from the Great East Japan Earthquake, we formulated new measures for disaster preparedness and implemented them by the end of February 2012. In fiscal 2018, we announced and subsequently implemented a two-year project for additional measures amounting to 20 billion yen to bolster preparedness against frequent natural disasters. Moreover, we are strengthening our disaster preparedness to be better able to respond to the increasingly diverse natural disasters anticipated in the future.

➤ Three Principles of Disaster Preparedness

Three Principles of Disaster Preparedness

Enhance system reliability

- Reinforce equipment structures
  - Seismic measures (e.g., design that withstands an earthquake measuring a magnitude of 7 on the Japanese seismic scale)
  - Measures against storms and floods (e.g., installation of waterproof doors, tide plates)
  - Measures for fire prevention (e.g., installation of fire-proof shutters, doors)


Base station


Relay station

Ensure essential communications

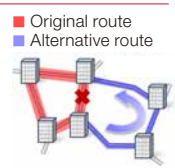
- 110, 119, 118 emergency calls
- Provide priority phone service to agencies dealing with essential communications during a disaster
- Control that separates voice calls and packet communication

Rapidly restore communications services

- Area restoration using emergency response equipment
  - Mobile base stations
  - Satellite-linked base stations
  - Mobile power generation vehicles, portable generators, etc.

➤ Initiatives for Disaster Preparedness

Disaster-Related and Other Events	Initiatives for Disaster Preparedness
Disruption of essential communications due to interrupted services	**Large-zone base stations (emergency base station to prepare for major disasters)** 105 locations nationwide (prefectural government offices, etc.) • Preventing power outages (engine) • Redundant transmission lines First operation in the Hokkaido Eastern Iburi Earthquake in 2018
	Medium-zone base stations (base stations prepared for natural disasters) 2,000 locations nationwide (disaster base hospitals, town halls, etc.) • Operate for 24 hours or more during a power outage • Redundant transmission lines Operated 62 stations during the torrential rains of July 2020
Batteries run out during prolonged power outage	**Reinforce emergency power sources** 14,000 locations nationwide (major public bodies, emergency shelters, etc.) • Can be used for at least 6 hours during a power outage Used batteries at 1,000 locations during Typhoon No.10 in 2020 Note: Including stations other than those that can use batteries for at least 6 hours
Interruption of transmission lines due to earthquake or torrential rains (fiber optic, etc.)	**Use of multiple transmission routes** 1,200 buildings nationwide • Securing multiple routes for transmission • Automatically switch to an alternative transmission line Automatically switched to an alternative transmission line during the torrential rains of July 2020



▶ Investment for disaster preparedness after the Great East Japan Earthquake

Cumulative total: over 100 billion yen

Disaster Management System

Under the NTT Group Disaster Preparedness Plan, the NTT DOCOMO Group stands ready with a system for efficiently conducting initial operations in accordance with the scope of disaster and recovery efforts. Our system is organized across departments so that it always facilitates an efficient response to disasters.

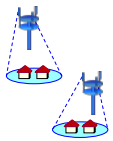
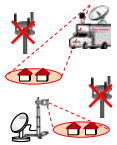
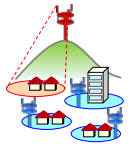
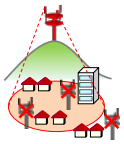
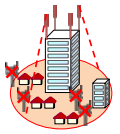
➤ **Internal System at the Time of a Disaster**

Scope	Internal System	Person in Charge	Past Disasters and Reference
Large	1st Degree Emergency Response	President and CEO	• The Great East Japan Earthquake
	2nd Degree Emergency Response	Senior Executive Vice President	• The 2024 Noto Peninsula Earthquake • Typhoon No. 21 of 2018, Hokkaido Eastern Iburi Earthquake (multiple disasters)
	3rd Degree Emergency Response	Executive officer	• Typhoon No. 10 of 2020 • Typhoon No. 15 of 2019 • Typhoon No. 21 of 2018 • Nankai Trough Earthquake Emergency Information "Warning against huge earthquakes," etc.
Small	Information Liaison	Head of Disaster Countermeasures Office	• Approaching typhoons, earthquakes with minimal impact, etc. • When a disaster is predicted, etc.
Before a disaster			

Internal System at the Time of a Disaster

NTT DOCOMO maintains emergency base stations to secure its networks in the event of a disaster. Depending on the level of damage, we implement measures such as setting up temporary base stations and remotely adjusting the transmission angle of radio waves from base stations.

➤ **DOCOMO's Emergency Base Stations**

	Mobile base station vehicles and portable base station devices	Medium-zone base stations	Large-zone base stations
Key Feature	**Respond to diverse natural disasters** Mobile base stations (vehicles and portable devices) that provide pinpoint relief for specific areas	**Respond to diverse natural disasters** Base stations that boost the capacity of existing stations to provide coverage for surrounding areas during a disaster	**Dedicated to major disasters** Provides wide-area coverage only when operations at most other base stations in the vicinity have been disrupted
Operation Overview	Normal state  ↓ Emergency 	Normal state Activated  ↓ Emergency Activated (wider coverage) 	Normal state Suspended  ↓ Emergency Activated 
Area Size (Radius)	Small (up to about 1 km)	Small (about 1 km) Medium (between 3 km to 5 km)	Large (about 7 km)
Emergency Operation	Requires time to transport and install	Instantly activated by remote control	Instantly activated by remote control

Large-Zone Base Stations

Large-zone base stations are specialized for emergencies to secure communications in heavily populated areas during widespread disasters and power outages. They provide 360-degree coverage across a seven kilometer radius, which is wider than that of a standard base station. Since 2011, NTT DOCOMO has installed large- zone base stations at 105 locations around Japan, and all are compatible with LTE, which boosts capacity by about three-fold. During the Hokkaido Eastern Iburi Earthquake, which struck in September 2018, we activated a large-zone base station for the first time, helping to restore communications to a wide area of Kushiro City.

Large-zone base station that secures communications in densely populated areas in times of disaster

Medium-Zone Base Station

Medium-zone base stations are built with foundations that are more robust than those of standard base stations and used as standard base stations under normal circumstances. They are able to cover adjacent areas by remotely expanding their service areas in the event of a disaster-related service interruption at neighboring base stations. To cover areas expected to suffer damage based on hazard maps, we had installed more than 2,000 medium-zone base stations in Japan. We also promote the nationwide deployment of medium-zone base stations to secure a means of communication in the suburbs of medium- size cities, disaster base hospitals, and coastal and mountainous regions. We activated 62 base stations during the torrential rains of July 2020.

Covering Areas Difficult to Access Rapidly

To diversify emergency recovery options in times of disaster, we are working to build shipboard base stations and fixed-line drone base stations while also strengthening our cooperation with related organizations to rescue people living in areas such as those difficult to access rapidly from maintenance sites.

When the Noto Peninsula Earthquake occurred on New Year's Day in 2024, NTT DOCOMO jointly operated shipboard base stations for the first time with KDDI Corporation and provided relief to two areas of Wajima City that had been severely damaged. With regard to cooperation with related organizations, we approached from the sea with the support of the Self Defense Forces to restore areas where land routes were closed.

The operation of drone relay stations allowed us to secure communication areas by amplifying radio waves in airspace and to strengthen our emergency recovery system.

Drone relay station

Introduction of Starlink

NTT DOCOMO introduced Starlink as a base station backhaul system following the Noto Peninsula Earthquake on January 1, 2024. Even if the fiber-optic connection to a base station is cut off due to an earthquake or other disaster, Starlink satellites can provide a temporary connection from the sky, making the system highly effective in times of disaster. Operating in a low orbit at approximately 550 km, much closer than conventional geostationary satellites, Starlink enables low-latency, high-speed communications. The system was put into practical use during a comprehensive disaster prevention drill in May 2024 and has since been deployed in multiple disasters, including Typhoon No. 10 and the Oku-Noto Heavy Rains in August and September 2024, and the Ofunato wildfires in February and March 2025.

Starlink Transforming Disaster Response: Connecting Disaster-Affected Areas through Rapid Recovery (in Japanese only)

Overview of DOCOMO's Response to Disasters

When the Noto Peninsula Earthquake struck on New Year's Day in 2024, our service was interrupted at up to 260 base stations due to power outages and transmission line cuts. As a result, service coverage in the six affected municipalities (Nanao City, Suzu City, Wajima City, Shika Town, Anamizu Town, and Noto Town) fell to 30% of normal levels. NTT DOCOMO immediately established an internal system after the disaster and began restoration activities the following day, engaging 10,000 people in the response.

Local access was hampered by aftershocks and accumulated snow in addition to traffic congestion and long distance travel due to the limited transportation routes on the peninsula. Under these circumstances, our employees rushed in from all over the country and managed emergency restoration at over 200 sites. In addition, we operated shipboard base stations, as mentioned earlier, and cooperated with related organizations. As a result, except for inaccessible areas, emergency restoration was completed on January 17 and area restoration was completed on March 21, except for Hegura Island in Wajima City.

We visited almost all emergency shelters (about 300 locations), both designated and undesignated, and provided evacuees with free battery charging services, free Wi-Fi services (d Wi-Fi, Starlink Wi-Fi), and free rental of DOCOMO public mobile phones. Furthermore, to support those living in emergency shelters over prolonged periods, we provided online medical consultations and video services to care for the physical and mental health of evacuees. This was NTT DOCOMO's first effort to support public mobile phones, online follow-up medical consultations, and video services.

➤ **DOCOMO's Principal Support for Areas Subject to the Disaster Relief Act**

Principal Support	Details of Concrete Support
Customers	• Activate unlimited data with disaster service • Free provision of mobile phone accessories • Special discount for purchasing mobile phones • Free of charge in place of some fees • Partial reduction in repair charges • Apply the mobile phone compensation service • Free mobile data recovery service • Free replacement of a phone • Relaxed subscription procedures • Free basic charge for DOCOMO Hikari, etc. • Free provision of some devices related to DOCOMO Hikari, etc. • Refund of basic charge for Hikari TV for DOCOMO • Extended fee payment deadline • Reissue of expired d POINTs
Local governments, etc.	• Lend mobile phones and satellite phones • Install multi-charger and Wi-Fi access points at emergency shelters

Working with National and Local Governments

The NTT DOCOMO Group, as a designated public body under Japan's Disaster Measures Basic Law, strives to prepare for disasters during normal circumstances and offer emergency response in the event of a disaster, under the NTT Group Disaster Preparedness Plan, with a view to facilitating the appropriate implementation of preparedness and response measures. During a disaster, we cooperate with government institutions through measures such as lending mobile phones to local governments to maintain essential communications. In addition, NTT DOCOMO signed mutual cooperation agreements with Japan's Cabinet Office, Ministry of Defense, the Japan Self-Defense Forces, and the Japan Coast Guard to allow for rapid recovery and relief activities during natural disasters. Under these agreements, NTT DOCOMO lends satellite phones and mobile phones to use in disaster recovery activities, and its emergency response equipment and personnel are quickly transported to affected areas by the Ground Self-Defense Forces and other public institutions.

In response to requests from related organizations following the Noto Peninsula Earthquake, we coordinated information during recovery activities and provided location information to assist with searching for missing persons. In providing the aforementioned online follow-up medical consultations, we worked to prepare for their implementation with the cooperation of the national and local governments, medical associations, and pharmacists associations.

Useful Services Available in Times of Disaster

In the event of a large-scale disaster, we provide a Disaster Message Board Service for people to confirm the safety of those in affected areas where a high volume of calls may disrupt mobile phone service. To enable customers to use the message board efficiently in the event of an emergency, we offer opportunities to try the service on the 1st and 15th of every month. We also provide an All Areas Disaster and Evacuation Information service for customers to receive area mail in remote locations via SMS.

Features of the Disaster Message Board Service

Someone in an affected area can easily post a message on the board to communicate their status, which can then be confirmed via the Internet from anywhere in the world. Two input options:

(1) Select from the following four message templates

I am safe. | There is damage. | I am home. | I am at an emergency shelter.

(2) Enter comments (up to 100 double-byte characters or 200 one-byte characters)

Features of the All Areas Disaster and Evacuation Information Service

- SMS notifications are transmitted to pre-registered users in specific areas or regions.
- Disaster and evacuation information from across Japan that has been transmitted in the previous three days can be reviewed on the webpage.

All Areas Disaster and Evacuation Information Service (in Japanese only)

Radio Wave Safety

Basic Philosophy

NTT DOCOMO operates and provides base stations and mobile phones in compliance with related laws and regulations and ensures that the level of radio wave emissions from them remains below the limits specified in the Radio-Radiation Protection Guidelines. Emissions below these levels are recognized around the world as having no adverse effect on human health, so users need not be concerned about the safety of DOCOMO's mobile phones.

Consideration for Radio Wave Safety

Radio-Radiation Protection Guidelines

The health effects of radio waves have been researched for over 60 years in Japan and abroad. The International Commission on Non-Ionizing Radiation Protection (ICNIRP), in cooperation with the World Health Organization (WHO), and the International Committee on Electromagnetic Safety (ICES) of the Institute of Electrical and Electronics Engineers (IEEE), established safety standard guidelines for the effect of radio waves on the human body. The guidelines have been adopted in many countries as international standards. The Radio Radiation Protection Guidelines, providing information consistent with these standards, have been established in Japan and are reviewed and amended as necessary to reflect the latest findings. The guidelines were amended in 2018 and 2024 to ensure the safe use of radio waves for 5G, and the relevant laws and regulations were also amended accordingly. NTT DOCOMO is fully committed to complying with the relevant laws and regulations, and the strength of radio

waves emitted by its mobile phone base stations and mobile phones is within standard values. Furthermore, it discloses the Specific Absorption Rate (SAR), the rate at which energy emitted by radio waves is absorbed by the human body, and power density (PD) for each mobile phone on its corporate website in its ongoing effort to ensure the safety of mobile phone use for customers.

Compliance Information on Radio Radiation Protection from Mobile Handsets

Collaborative Research on Radio Wave Safety

Since 2002, NTT DOCOMO has conducted experiments in collaboration with KDDI Corporation and SoftBank Corp. related to the possible impacts of radio waves on the human body at the cellular and genetic levels, and in 2007 we released a final report stating that the research had identified no impact. The report provided scientific evidence against the belief that radio frequency radiation could harm cell structure and function and possibly cause cancer, and it reconfirmed the safety of radio waves from mobile phones. The Ministry of Internal Affairs and Communications also engages in ongoing research on radio wave safety.

The Electromagnetic Environment Committee of the Association of Radio Industries and Businesses (ARIB) is currently conducting surveys and research on the safety of mobile phone radio waves to enhance public welfare associated with the use of radio waves. NTT DOCOMO actively participates in these initiatives as a regular member in support of the ARIB.

Radio Wave Safety (in Japanese only)

Explanation of Radio Wave Safety in 5G

We recognize the importance of again explaining the safety of radio waves to our stakeholders following the launch of 5G service in March 2020 in Japan. The NTT DOCOMO website offers evaluations and views of relevant domestic and international organizations on the safety of radio waves, as well as information on international guidelines that set radio wave safety standards, including those of the 5G band, on the human body. We disclose information including NTT DOCOMO's view on radio wave safety and answers to frequently asked questions so users can confidently use 5G.

Effects of Radio Waves on the Human Body and Standards and Systems for Safe Use (in Japanese only)

Opinions of DOCOMO and Major Organizations on the Safety of Radio Waves (in Japanese only)

Effect on Medical Electronic Devices and Ongoing Measures

Japan's Ministry of Internal Affairs and Communications and the Electromagnetic Compatibility Conference have confirmed that radio waves from mobile phones and other wireless devices may affect the functioning of medical electronic devices, including heart pacemakers, and have widely published their safety guidelines. Accordingly, we are working to ensure that users are fully aware of precautions when using mobile phones by providing information in the mobile phone users' manual and via the NTT DOCOMO website.

Information Security and Privacy Protection

Ensuring Information Security

Basic Philosophy

NTT DOCOMO recognizes that proper management of information is a vital management concern. To offer secure services to customers, we have declared our Information Security Policy as a guideline for initiatives on information security, and we are committed to thorough compliance with this policy and the Privacy Policy. In accordance with these policies, we have established an information management system and are continuously improving and strengthening the system.

The Information Security Policy applies to information management assets that consist of any information we obtain in the course of our corporate activities and all information NTT DOCOMO retains in connection with its operations.

➤ **Metrics for Information Security and Privacy Protection (DOCOMO Group)**

Metrics	Targets	FY2022	FY2023	FY2024
Number of major incidents caused by a cyber-attack*	0	—	0	0
Number of major information leaks	0	1	0	0

*Added to KPIs from 2023

Information Security Policy

NTT DOCOMO Privacy Policy

NTT DOCOMO Information Management System

In order to protect and appropriately manage all of the information assets we possess, we have established the Information Management Committee, chaired by the senior executive vice president, who also serves as the chief information security officer, chief privacy officer, and specific user information manager. We have also designated a person responsible for information management in each organization to establish a system for quickly implementing information security measures. The Information Management Committee meets at least twice a year with the following three primary roles:

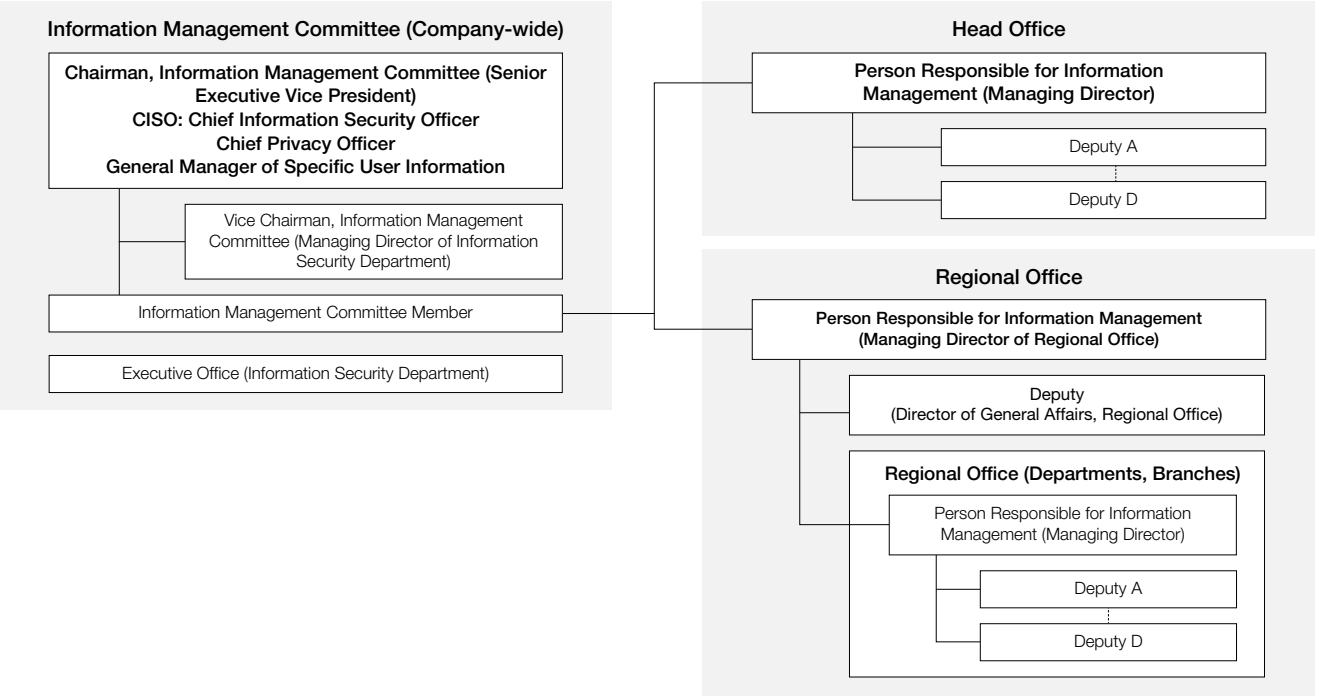
(1) Deciding, revising, and issuing notifications on the Information Management Principles and Information Management Rules

(2) Coordinating, determining, approving, and issuing notifications or public notices on the operation of information management regulations

(3) Issuing notifications or public notices on other specific guidelines for information management, and issuing instructions to each person responsible for information management

In the event of a major information security incident, we inform senior management and the Information Security Department of the head office. Moreover, a designated committee chaired by the president is set up to respond to the incident depending on the degree of impact.

➤ **Information Management System (DOCOMO)**



(As of July 2025)

Rigorous Enforcement of Information Security Rules

Information including personal data is rigorously managed in accordance with the NTT DOCOMO Information Management Rules, detailed regulations, manuals established in line with relevant laws and regulations, including the Telecommunications Business Law, the Act on the Protection of Personal Information, and other guidelines as stipulated by the relevant authorities. Such rules, regulations, and manuals also apply to NTT DOCOMO's outside contractors and partner companies, in addition to its employees.

If any of them use confidential information about communications, or confidential or personal information obtained in the course of duty, without a legitimate reason, and leak or attempt to leak such information, they will be subject to disciplinary action in accordance with our internal regulations.

Information Security Governance at Group Companies

To ensure thorough information management and prevent incidents at Group companies, we have established the DOCOMO Group Security Measures Manual based on the NTT DOCOMO Information Management Regulations. Each Group company has established the necessary systems for proper security management and adheres to the rules.

Furthermore, NTT DOCOMO's Information Security Department has established a division overseeing Group companies. The division monitors information security operations at each Group company, provides education and training on security, shares information on cybersecurity threats and countermeasures, and coordinates responses when incidents occur.

We have established the NTT DOCOMO Group CISO Meeting with NTT DOCOMO BUSINESS, NTT DOCOMO SOLUTIONS, and NTT DOCOMO Global, among Group companies. Comprised of the CISO of each company, it determines information security strategies and policies

for key measures. Based on these decisions, we manage information security measures and strengthen security personnel in an integrated manner.

Information Security Measures

Information Security Risk Management

We identify information security risks based on incidents that have occurred within the NTT DOCOMO Group and the NTT Group, the latest cyber-attack trends, global situations, the state of legal systems, and technological trends. We then assess, analyze, and implement countermeasures.

System Security Measures

The NTT DOCOMO Group is required to implement approximately 200 security measures for its systems based on frameworks such as the risk management framework outlined in SP800-37 issued by the U.S. National Institute of Standards and Technology (NIST). Security reviews and vulnerability assessments are conducted during the development phase.

For systems handling critical information such as personal data, NTT DOCOMO mandates measures including stricter rules for searching customer information, multi-factor authentication for system use, encryption of information system terminals and communication channels, and monitoring for unauthorized removal of information.

Eradicating Software Vulnerabilities

Software vulnerabilities are a major factor in providing a foothold for external attacks. As a countermeasure, systems are required to pass vulnerability assessments before going live, and regular vulnerability assessments are conducted after going live.

If new, high-risk software vulnerabilities are discovered, we promptly implement the necessary countermeasures to prevent unauthorized access, destruction, leaks, and falsification related to our information assets and to minimize damage in the event of such incidents.

Security Measures for Use of Public Cloud

To counter attacks due to improper configurations of highly flexible IaaS/PaaS or administrator ID leaks, we require centralized issuance of administrator accounts and constant monitoring and maintenance of security policies established for each cloud environment.

If a security policy is violated, prompt action is required after an alert is issued.

Response to Increasingly Sophisticated DDoS Attacks

DDoS attacks are an unavoidable threat when using the Internet, and the methods of these attacks are becoming increasingly sophisticated. In light of past DDoS attacks, NTT DOCOMO has implemented countermeasures against similar incidents to mitigate damage.

When an attack is detected, information on attack methods and more is shared among Group companies, and monitoring of each system is strengthened to respond to the attack. Depending on the attack's scale, information including detailed results of post-incident analysis is shared within the NTT Group, and the information is also shared with other companies in the industry and security vendors.

Preventing Unauthorized Use of Services

Attacks targeting personal services, including increasingly damaging phishing scams, are becoming more sophisticated and frequent each year. In response, NTT DOCOMO has established the Unauthorized Access Countermeasures Committee under the CISO to comprehensively strengthen efforts to anticipate and prevent unauthorized access, monitor the impact of attacks, and respond rapidly to incidents. In addition, when offering new services, we assess security risks, such as unauthorized use through account takeovers or information leaks, based on the characteristics of each service, and review whether appropriate countermeasures have been implemented.

Security Monitoring

We established the Security Operation Center (SOC) as a dedicated organization for security monitoring, operating 24 hours a day to detect signs of cyber-attacks and unauthorized use of services. We use Security Information and Event Management (SIEM), a system that aggregates logs from servers and network devices, enabling early detection of attacks through correlation analysis and anomaly detection using advanced AI-powered log analysis. In addition, we continuously gather information on attacks and responses, including improvements in detection and prevention methods.

Information Security Initiatives for Partner Companies, etc.

As one pillar for expanding its smart life business, NTT DOCOMO is promoting collaborations with other industries to address social issues. As collaboration and sharing of information with partner companies increases, NTT DOCOMO manages the efforts of partner companies by requesting that they comply with the Act on the Protection of Personal Information and follow guidelines issued by ministries and agencies as well as public organizations. Other measures taken to protect personal information include obtaining customer consent prior to sharing their personal information with partner companies.

Selection Criteria for Outsourced Companies Handling Personal Information

In the course of business operations, we may outsource tasks that involve handling personal information. We require that these outsourced companies implement information management measures equivalent to our own standards. Accordingly, we enter into contracts only with companies that

meet the selection criteria established by NTT DOCOMO. These criteria were formulated with reference to guidelines such as those from the Information-technology Promotion Agency, Japan (IPA) and the Guidelines Concerning the Act on the Protection of Personal Information (General Provisions).

When entering into a contract, we clearly stipulate conditions regarding security management measures, confidentiality, subcontracting, and other matters related to the handling of personal information. During the contract period, we monitor compliance with these rules and verify the actual implementation of security measures through on-site visits. Should any inadequacies be found in supervision, systems, or operational practices prove inadequate, we promptly implement corrective measures.

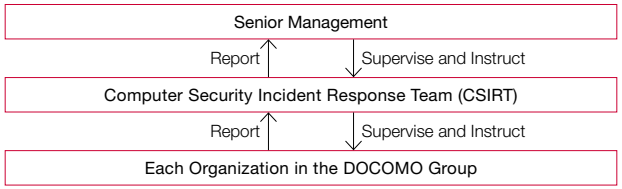
Raising Security Awareness and Ensuring Thorough Information Management at docomo Shops

We provide training on information security at least once a year for docomo Shop staff and provide additional education resources through quarterly issued Security News, a compilation of security issues the shops are likely to experience.
Also, since customer information is often handled and the risk of information leakage is high at the point of sales, we conduct rigorous audits once every three months in addition to monthly self-inspections to ensure that information is being managed appropriately.

Response to Security Incidents

The NTT DOCOMO Group maintains a Computer Security Incident Response Team (CSIRT) as a specialized department for responding to security incidents. In the event of a serious incident, the CSIRT takes the lead in responding in accordance with the Response Manual and in close cooperation with related internal and external organizations and senior management. In normal times, the CSIRT monitors attacks on our facilities and collects information on domestic and international trends to prepare for incidents.

➤ Security Incident Response System



External Collaboration

We are a member of security organizations such as the Nippon CSIRT Association, the Forum of Incident Response and Security Teams, ICT-ISAC JAPAN, the JPCERT Coordination Center, and the Japan Cybercrime Control Center. We collect information on domestic and overseas security trends and reflect it in security measures, employee training, and incident responses. Furthermore, NTT DOCOMO shares information about incidents that occur within the NTT DOCOMO Group and the countermeasures taken with these organizations, contributing to society including other companies.

Threat Intelligence Analysis

NTT DOCOMO collaborates with external security vendors to collect threat intelligence on the types, trends, and methods of increasingly sophisticated cyber-attacks. We focus our analysis primarily on attack trends targeting critical infrastructure businesses, such as telecommunications, helping to predict potential cyber-attacks against NTT DOCOMO.

Incident Response Training

NTT DOCOMO conducts annual internal training simulating incidents that occur in the services it provides. The training involves management, service departments, customer support departments, and public relations departments to establish a response system and confirm procedures.

We also actively participate in drills hosted by supervisory agencies and public institutions, as well as NTT Group internal drills, to improve our practical capabilities in the event of an incident.

We conduct annual training on targeted attack emails for NTT DOCOMO Group executives, employees, and partner employees (including temporary staff) to maintain vigilance and to ensure that all personnel confirm the reporting procedures in the event of an incident.

Information Security Training and Fostering Awareness

NTT DOCOMO provides ongoing regular education and training to enhance information security literacy among all employees to appropriately manage information assets. These efforts include an e-learning course for raising awareness of information security and cyber security. Education and training are provided in accordance with the learning program framework in the DOCOMO Information Management Training Guidelines. Executives, and Group and partner employees, including temporary staff, are all required to participate in the program.

Furthermore, we have expanded role-specific training programs. For instance, upon assuming their positions, presidents of Group companies are required to complete the NTT Group's common security training for presidents, while system security training and annual exams are mandatory for system administrators.

Strengthening Security Personnel

Japan faces a shortage of over 110,000 cybersecurity personnel, and the situation is expected to become even more serious in the future as cyber-attacks grow more sophisticated and digitalization advances. The NTT DOCOMO Group is therefore working to expand its pool of security personnel with advanced specialized skills while also raising the security

skill level of all personnel involved in providing safe and secure services.

Security Personnel CoE (Center of Excellence)

We have established the Security Personnel CoE, a framework jointly operated by the information security and human resources departments and are taking a strategic approach to recruiting, developing, and assigning security professionals. We aim to systematically and continuously nurture experts with advanced expertise who can play active roles in various domains, including strengthening NTT DOCOMO's information security, contributing to safer services for individual customers, and helping resolve security challenges faced by corporate customers.

New Graduate Recruitment and Advanced Security Training Program

NTT DOCOMO hires new graduates with strong potential to contribute in the security field. After joining the Company, these recruits receive 3 to 12 months of specialized training in security technologies at N.F. Laboratories, a subsidiary of NTT DOCOMO BUSINESS dedicated to developing security professionals. They then spend one to two years working in security-related operations, acquiring a uniformly high level of information security knowledge and skills required for their roles.

After completing the program, they are assigned to positions that align with their interests and aptitudes, enabling them to make immediate contributions. We hired 35 individuals in fiscal 2024 and 52 in fiscal 2025, and plan to further expand recruitment in the coming years.

Internal Security Certification System

The NTT DOCOMO Group encourages and supports its employees in obtaining national and private-sector certifications to acquire the security expertise necessary to provide safe, secure, and stable services, as well as the security skills required for promoting IT use and digital transformation.

We also certify personnel with specific qualifications and job-related skills, such as the IPA's Registered Information Security Specialist and the former Information Security Specialist qualifications, the ISC2's Certified Cloud Security Professional and Certified Information Systems Security Professional, and ISMS Auditor, as intermediate and advanced security professionals. Recognizing that intermediate and above security professionals contribute to strengthening and maintaining security in all organizations and operations, we are working to increase the number of certified personnel by setting medium-term targets.

➤ **Major Certification Systems and Number of Certified Personnel (DOCOMO Group)** (Persons)

Certification System	Target	FY2023	FY2024
Security Intermediate/ Advanced Certification	2,160	1,715	1,755

Information Security Audits

NTT DOCOMO conducts information security audits on two fronts: through system security audits for the development and operation of information systems and operational security audits for the use of information systems and services. In both audits, the internal audit division conducts information security audits of all organizations from a position independent of business execution in order to continuously confirm the proper management and implementation of security measures. Based on the audit results, the internal audit division rectifies and provides advice on security measures and, as required, recommends proposals for improving security measures to the information security division.

The internal audit division formulates audit plans after evaluating and assessing the risks of audit targets by leveraging its accumulated expertise and closely monitoring changes, such as internal and external information security breaches and evolving security requirements within the Group.

System Security Audits

System security audits to verify the technical security measures in place for systems owned by the Group are conducted at least once a year for departments that develop and operate these systems, the risks of which have been deemed high through a risk-based evaluation. In fiscal 2024, we conducted 21 audits on general technical security measures and provided recommendations for improvements. The internal audit division offered specific guidance as needed and gathered evidence to confirm that the necessary corrections were completed.

Operational Security Audits

Operational security audits are conducted at least once a year, with audit targets selected through a risk assessment of each organization. These audits examine the implementation of organizational, human, and physical security measures.

In fiscal 2024, we audited 61 items, including those concerning the transfer of personal information with contractors and the handling of information equipment. We identified areas for improvement and provided guidance on corrective actions, which the internal audit division later confirmed as completed.

Auditor Independence

The internal audit division submits proposals for internal audit plans directly to the Board of Directors for approval, and audit results are also reported directly to the representative directors and the Board. This ensures that auditors can perform audits independently from business operations.

In addition, we have established a rule that auditors cannot audit the division they previously belonged to within a specified period, further safeguarding their independence.

Protection of Data Privacy

Establishing the Guidelines and Structure for Protecting Personal Information

NTT DOCOMO believes that recognizing the importance of personal information and ensuring thorough protection represent a vital business responsibility. We disclose our Private Policy, which clearly states our commitment to ensuring security and reliability for customers.

In December 2019, we reformulated the policy based on the behavioral principles P. 103 set forth in the Personal Data Charter P. 103, revising its structure and wording to make it simpler and easier to understand, without changing the scope of personal data processing. In fiscal 2023, we continued to revise the policy as needed in response to the revised Act on the Protection of Personal Information, etc., in order to protect the personal information of our customers.

In the course of obtaining, using, or providing personal information or handling anonymized information, we comply with the Act on the Protection of Personal Information and other relevant laws and regulations and respond promptly to revisions under an established management system for protecting personal information. In addition, we appropriately and carefully handle the information in accordance with internal rules. Through our Privacy Policy, we inform our customers about the content of the personal information handled, statements requiring customer approval for the use of data, and policy on disclosure to third parties and other information. docomo Shops obtain information required for contracts after clearly stating the intended use of such information. Any personal data we provide to a third party is strictly limited to the scope permitted by law or with customer consent.

We formulated the GDPR Compliance Manual in compliance with the EU General Data Protection Regulation (GDPR), which came into effect in May 2018 as a new framework for personal information in the E.U., setting out rules pertaining to personal data. In April 2019, we also formulated the Information Management Regulations (Handling of EU Personal Data) as an internal regulation that stipulates the handling of personal information in the E.U. In the event of a serious incident involving the leakage of personal information or data theft or loss, we report through the corporate website.

Personal Information Management

At NTT DOCOMO, the number of employees with access to systems that manage customer information is kept to the minimum, and the information accessible to each employee is specified and limited. Biometric authentication* is required to use the system, and access logs are regularly reviewed. We seek to ensure the accuracy and security of personal information by implementing rational measures that address risks such as illegal access to personal information, and leakage, loss of, or damage to personal information.

*Biometric authentication confirms the identity of an individual by identifying physical characteristics such as fingerprints and facial as well as voice features.

Use of Personal Data

Progress related to AI and IoT has led to the creation of diverse products and services that utilize big data. Initiatives in place to create new value are gaining momentum throughout society. Guided by its corporate philosophy of "creating a new world of communications culture," NTT DOCOMO takes on the challenge of constantly innovating to realize an affluent future. We will leverage our customers' personal data and data on various products and experiences as well as technologies such as AI that produce diverse insights from the collected data. We will then generate and society as a whole. Meanwhile, we believe our mission is to protect and pay due consideration to customer privacy as well as to comply with prevailing laws and regulations when using personal data that is particularly important to the customer. NTT DOCOMO will continue to live up to the trust of its customers by handling personal data with a sense of responsibility.

In August 2019, we published the Personal Data Charter as a Company policy on the use of data to ensure the continued provision of new value to customers and society by leveraging data while maintaining the optimal privacy protection for customers. We set out the six behavioral principles in the charter and use data in accordance with these principles. In July 2022, NTT DOCOMO transferred its corporate business to NTT DOCOMO BUSINESS and publicly declared its compliance with the Personal Data Charter. In April 2024, in light of changes in the environment surrounding personal data, we partially revised the Charter from the following three perspectives.

- Privacy considerations for children and senior citizens
- Privacy considerations at NTT DOCOMO Group companies
- Security measures at contractors

DOCOMO's Use of Personal Data, which clearly and simply explains how personal data is used through illustrations. Moreover, we provide the Personal Data Dashboard on our website, allowing customers to confirm the main items of their consent to the handling of personal data and to set and change their own settings to a certain extent.

We will continue our efforts to protect data privacy by pursuing the protection and appropriate handling of personal data.

NTT DOCOMO Personal Data Charter
DOCOMO's Use of Personal Data (in Japanese only)
Personal Data Dashboard (in Japanese only)

NTT DOCOMO Personal Data Charter—Behavioral Principles for Innovation Creation

Guided by our corporate philosophy of "creating a new world of communications culture," NTT DOCOMO is pursuing innovation toward the goal of realizing a richer future we have never seen before. Innovation, as we perceive it, is about connecting various goods and services that are relevant to people's everyday lives to deliver comfort and excitement that exceed customers' expectations. We also seek solutions to various societal issues to create a future where everyone can enjoy affluence beyond borders and across generations.

From safety and security to health tips, education and all sorts of entertainment in everyday life, we will provide the optimal information catered to the needs of each and every customer as we take steps toward the future. We will also promote various business innovations that are consistent with these goals and other initiatives aimed at solving various social challenges.

We will work to create the future described above together with customers in harmony with society without being complacent with the status quo. We will aim to create new value and provide returns to customers and society by utilizing customers' personal data as well as data derived from various goods and services, adopting artificial intelligence and other new technologies that generates various insight and wisdom from such data.

When we utilize the valuable personal data of customers, we believe it's our mission to protect customers' privacy and ensure due attention to customers, as well as to abide by all relevant laws and regulations. Some customers may have anxiety or concerns about our utilization of their personal data. As we have always done, we will continue to handle personal data with responsibility going forward with a strong resolve to gain the trust and confidence of customers. We will value our "ties" with customers more than ever and listen to their voices with sincerity. What is most important for us is to constantly consider and communicate the new value that we can deliver to customers and society through the utilize of data and the optimal way to protect the privacy of each customer.

To realize "continual new value delivery to customers and society through the utilization of data" and "optimal privacy protection for customers," we will make decisions adhering to our behavioral principles set forth below when we handle customers' personal data in various scenes of our corporate activity

Six Behavioral principles of the NTT DOCOMO Personal Data Charter

Behavioral principles

Value communication with customers and ensure transparency

- Ensure transparency to have our customers understand how their personal data is obtained and utilized.
- Upon the acquisition and utilization of personal data, we will consider diversity such as customers who are children and seniors and work to gain customers' understanding through easy-to-understand explanation using plain expressions, summary and video presentations.
- We will strive to eliminate customers' concerns and questions and improve our communication for their peace of mind.

Think about customers' profit and contribution to society

- We will delivery new value to customers and society through the utilization of personal data.
- Upon the utilization of personal data, we will always be mindful if it leads to customers' benefit or contribution to society and refrain from any data utilization that could undermine customers' confidence.
- When we provide services and products, etc. targeting children, we will give due consideration to the children's interests.
- Acquisition and utilization of personal data shall be executed in a proper and lawful manner paying due attention to the feelings of customers.

Honor the wishes of each and every customer

- Each customer has different views regarding the utilization of their personal data. In view of such difference, we will offer customers with options for the utilization of personal data (including means for opt-out, etc.) considering the nature or the utilization conditions of the data in question.
- We will strive to make the options simple and easy to understand.

Be attentive to customers' privacy when allying with partners

- When personal data or its anonymized version or statistics version derived out of such data is provided to external partners such as partner businesses and group companies for open innovation aimed at creating new value to customers and society, we will ensure compliance with relevant laws and regulations and pay due attention to customers' privacy.
- When information is provided to partners, depending on the nature of information, we will follow the most adequate method, e.g., confirming the trustworthiness of the recipient, or setting limitation on the way information is provided or utilized, etc.

Protect personal data by adopting proper security measures

- We will protect valuable customer information employing proper organizational/personnel/physical/technical measures internally and by our entrustees to prevent leakage, theft, alteration of data or any other accidents.
- We will perform a regular review on information security and implement measures to mitigate security risks as necessary.

Implement and operate a structure for customers' privacy protection

- In accordance with the concept of privacy-by-design, we will be mindful of customers' privacy whenever we develop new products and services.
- To ensure thorough consideration to privacy, we will provide training, education and information sharing with the relevant persons who handle customers' personal data on an ongoing basis.
- We will implement and operate a governance mechanism to assess the impact on customers' privacy in personal data utilization, including the establishment of a specialized advisory body that will assess the impact on privacy.

The content and operation of the behavioral principles will be reviewed and modified from time to time so we can continue to live up to the trust and confidence of customers.

Privacy Impact Assessment System

NTT DOCOMO has established and is operating a Privacy Impact Assessment (PIA) system under the behavioral principles in the NTT DOCOMO Personal Data Charter, as well as frameworks and systems for legal compliance and safety management governing the use of key personal data of customers. Under the system, we evaluate whether customer privacy is taken into consideration from the planning stage of projects and services that use personal data, and we are committed to protecting the privacy of our customers.

Specifically, when implementing such projects and services that use personal data, the department handling them evaluates the items from a privacy perspective. When certain criteria are met, such as the nature and usage of personal data, an assessment is conducted by the PIA Council, a specialized advisory body established within the Company.

Evaluation is focused on whether there are violations of the principles of action of the NTT DOCOMO Personal Data Charter and whether they will be accepted by customers and society. The PIA Council has so far evaluated more than 600 projects and services that use personal data, and then worked to review and improve them as necessary based on the evaluation results. In fiscal 2024, we conducted 85 evaluations.

Case 1

When providing Caboneu record, a service that uses customer location information and service usage data to quantify their eco-action, evaluation was based on whether the explanation of data use was easy for customers to understand and whether the customer's intention could be reflected.

Case 2

To acquire and use new data such as smartphone usage data when enhancing the existing Health Mileage functions, evaluation was based on whether the explanation of data use was easy to understand and on the benefits it would bring to customers and society.

What privacy measures are in place? (in Japanese only)

➤ Number of PIA Meeting Agenda Items for Past Four Years (cases)

FY2021	FY2022	FY2023	FY2024
124	113	76	85

With the transfer of NTT DOCOMO's corporate business to NTT DOCOMO BUSINESS in July 2022, the Company has also publicly declared its compliance with the Personal Data Charter and introduced PIA initiatives.

Employee Education and Awareness Raising

NTT DOCOMO provides training at least once a year for all employees and executives, including temporary staff, and an e-learning course suited to each career level from the perspective of information security and privacy protection. In addition, it conducts awareness and educational activities regarding the Personal Data Charter at least once a year, and NTT DOCOMO Group companies also implement similar initiatives for employees who handle customers' personal data.

Response to Generative AI

Background of Generative AI Governance

NTT DOCOMO has been advancing the digital transformation of business operations and providing value-added services with generative AI. Various types of generative AI can create text, images, videos, and voices. Selecting the appropriate method can significantly enhance the efficiency of tasks previously performed manually and bring ideas to life in unexpected ways. On the other hand, the social risks associated with generative AI are diversifying and occurring more frequently following its introduction, including unintended discrimination, unreasonable behavioral restrictions and inducements, infringement of intellectual property rights, and the generation and dissemination of false information and misinformation.

The NTT Group has established basic policies and regulations for the use of AI, including the NTT Group AI Charter, to address concerns about generative AI while promoting enhanced competitiveness and safety in a comprehensive manner. In line with these policies and regulations, NTT DOCOMO has established the DOCOMO Generative AI Guidelines.

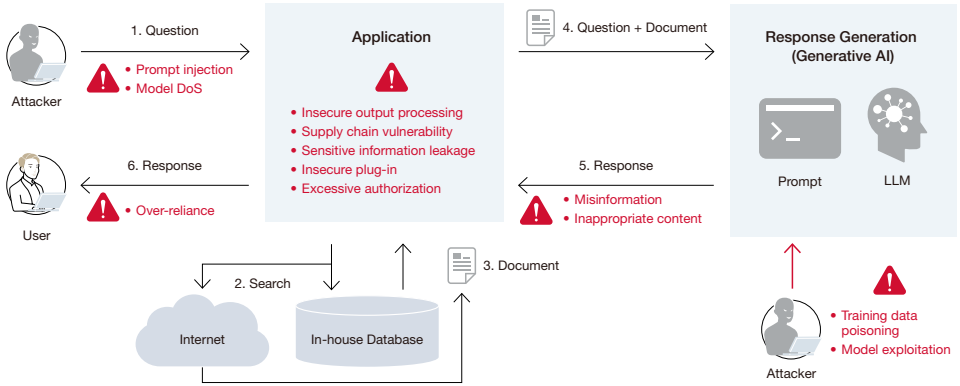
NTT Group AI Governance

Positioning the DOCOMO Generative AI Guidelines

The DOCOMO Generative AI Guidelines aim to properly assess the risks associated with generative AI, prevent potential risks, and mitigate the impact of any such risks on business if they occur, and to promote active use and value creation opportunities.

As shown in the diagram on the right, it is crucial to manage the risks of using generative AI, which include not only the generative AI model itself but also its applications and users. Therefore, the Docomo Generative AI Guidelines outline the measures to be taken for each risk under three roles: model developer, generative AI service provider, and generative AI user.

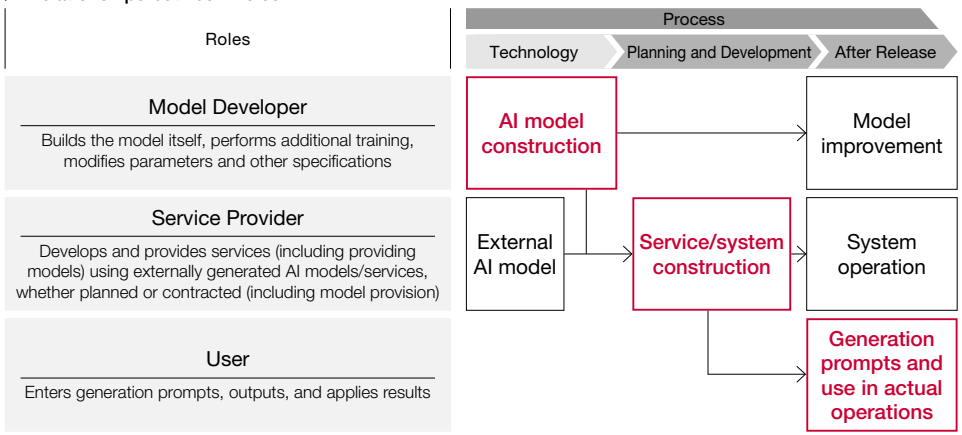
➤ Risks of Using Generative AI



Roles and Countermeasure Standards in the DOCOMO Generative AI Guidelines

These guidelines define three roles based on specific tasks, as shown in the diagram, with countermeasure standards established for each role. Specifically, compliance requirements for additional learning methods, such as Retrieval-Augmented Generation (RAG), are outlined for service providers.

➤ Relationships between Roles



Internal Review Process for DOCOMO Generative AI Guidelines

NTT DOCOMO has established an internal review process in cooperation with the risk management division to ensure the implementation of standardized countermeasures for each role and to enhance the stability of quality. In addition, we have broadly classified risk items into five categories. The risk management division reviews each risk concerning the associated countermeasure, while the Corporate Planning Department conducts cross-sectional management.

Five Risk Countermeasures

- **Selection of Generative AI Models and Services**
Selection of a technology that can reduce the risk of attacks from third parties resulting from unauthorized access caused by tampering with learning data

- **Protection Against Managed Information Leakage**
Prevention of managed information from being learned by the Large Language Model (LLM) and thereby being included in outputs when the LLM is used by third parties

- **Protection of Personal Data**
Confirmation of legal and regulatory compliance, such as the Act on the Protection of Personal Information, and operation of a Privacy Impact Assessment system

- **Prevention of Intellectual Property Infringement**
Addressing infringement of third-party intellectual property rights in LLM learning and use of generated materials

- **Deterrence of Input and Output of Misinformation and Unethical Content**
Tuning and operational framework considering the reputation risk associated with the dissemination of incorrect answers from LLMs

To further improve the stability of quality when creating systems and services using generative AI, we implement a cross-sectional review process for risk countermeasures at each phase of planning and development. This process is managed comprehensively and carried out by the Corporate Strategy & Planning Department.

➤ Internal Review Process