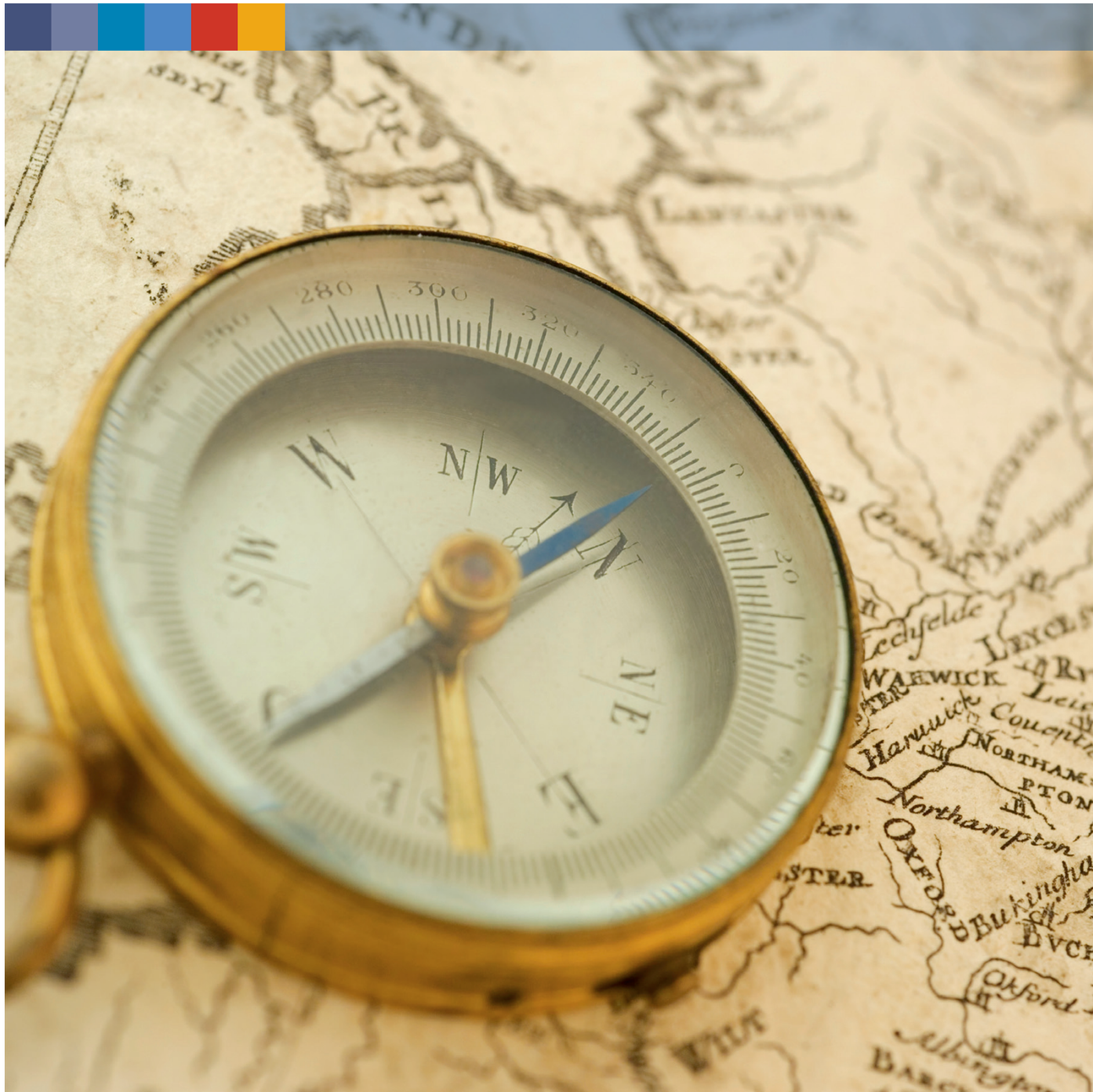
NTT DATA
Global IT Innovator

Information Security Report 2016



NTT DATA Corporation

Toyosu Center Bldg., 3-3, Toyosu 3-chome,
Koto-ku, Tokyo 135-6033, Japan
Tel: + 81 3 5546 8202
www.nttdata.com

Mission

【Mission Statement】
Mission of the NTT DATA Group

NTT DATA uses information technology to create new paradigms and values, which help contribute to a more affluent and harmonious society.

Information Security Report 2016

C O N T E N T S

Applicable Period and Timing of This Report

- This report applies to all information covered by the NTT DATA Group.
- This report applies to information security initiatives current at the end of December 2015 unless otherwise noted.

Scope of This Report

NTT DATA Group
Consolidated subsidiaries : 263 *Current as of September 30, 2015

Inquiries

NTT DATA Corporation
Toyosu Center Building Annex 3-3-9, Koto-ku, Tokyo 135-8671
TEL: +81-50-5546-2545
URL: http://www.nttdata.com/

Message from the CISO

The NTT DATA Group's thinking on Information Security

Information security with the goal of providing safe and secure IT services

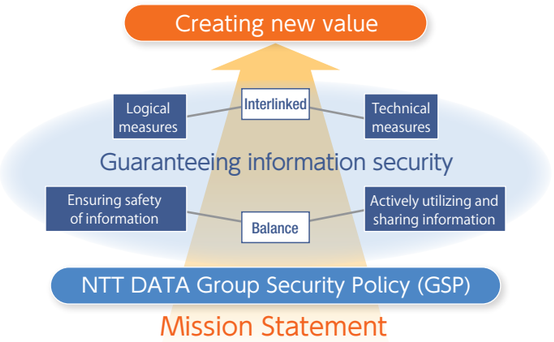
In recent years, with everything becoming connected through Internet, the "IoT" (Internet of Things) world, which can be subject to monitoring and control, has been expanding rapidly. This, in turn, has ushered in a new age where response to new security risks has become all the more pressing, causing every company and employee to become fully aware of those risks and to seek counter-measures for protecting information assets. In fact, new attacks targeting the IoT, like attacks on vehicle and POS systems, consumer electronics and so on, are being carried out in rapid succession. Cyber attacks like targeted attacks are becoming increasingly more common and sophisticated while DDoS attacks against companies and government agencies, as well as direct damage to businesses by ransomware, are on the rise. In anticipation of the 2020 Tokyo Olympics, cyber attacks are only expected to increase and to have an ever heavier impact on society.

Against this backdrop, the NTT DATA Group, in order to continue to a partner trusted by customers, is developing on a global scale information security-related management measures including preparation and improvement of rules and guidelines, informing and training of employees, business partner and temporary staff, inspections by audit in line with its "information security policy." Furthermore, in addition to the introduction of new measures for thoroughly ensuring in-house information security, we are focusing our efforts on information security measures in a variety of ways with the aim of enhancing the security services we offer our customers. Providing safe and secure IT is essential to the realization of the NTT DATA Group's mission statement of contributing to building a more affluent and harmonious society by creating new "paradigms" and "values" through information technology. To this purpose, we will detail in this document a series of in-house security initiatives as well as information security services that can contribute to solve the issues affecting our customers. We hope that this document will be of help, however slightly, to all of you who will read it and that it will help to further improve confidence in the NTT DATA Group.

NTT DATA Corporation
Representative Director and
Senior Executive Vice President CISO
Satoshi Kurishima

Information Security Policies

By maintaining an appropriate balance between "ensuring safety of information" and "actively utilizing and sharing information", the NTT DATA Group promotes the circulation of knowledge throughout the entire group and provides brand new value to customers.
Both (1) logical measures covering the development of rules and providing training and educational activities related to information security, and (2) technical measures for preventing information leakage or the installation of thin-client PCs are required for adequately "ensuring safety of information" and "actively utilizing and sharing information".



Establishment of Information Security Policy

Unauthorized use of information and information leakage resulting from security breaches can cause serious trust problems. Starting from December 1998, NTT DATA has established an "Information Security Policy" to properly handle information assets and to ensure information security.
Additionally, in recognition of the importance of protecting personal information, we established a "Personal Information Protection Policy" in July 2001. The policy sets forth in-house compliance rules for the proper handling of personal information. It is constantly being revised and improved upon to keep up with the progress of information technology and with changes in society.

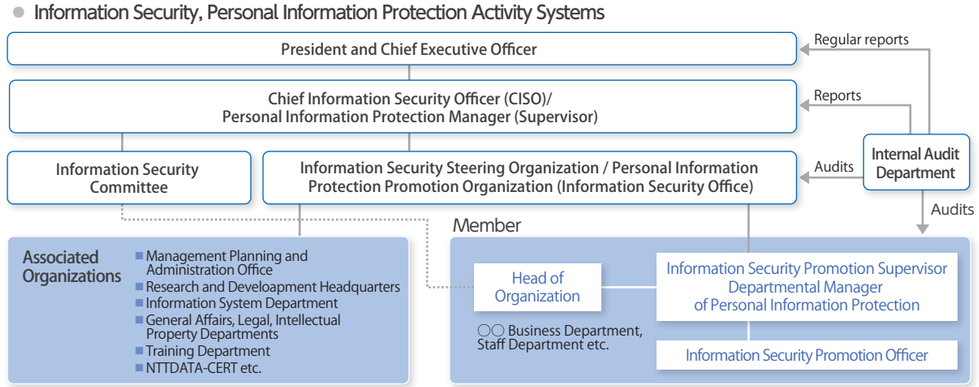
Policy for Commissioning Business

NTT DATA has established rules to prevent information security incidents at partner companies which have been commissioned work, including software development work.
When entrusting work which involves handling confidential information and personal information, we always receive confidentiality pledges and verify the degree to which security measures have been implemented.

Checking the state of systems and countermeasures
When selecting trade partners, we always verify the state of our partners' security measures, through interviews and similar means, in accordance with the designated standards.

Introduction of rules and agreement on the level of measures
After presenting the rules related to security management and the protection of personal information, we ask partner companies to agree to the level of measures expected of them.

● Information Security, Personal Information Protection Activity Systems



Information Security Strategies

The NTT DATA Group has defined information security strategies for achieving management policies and minimizing information security risks. Based on the information security strategies, NTT DATA make proposals for concrete information security measures (action plans) and implement them.

Our Position on Management Policies and Corporate Management

The NTT DATA Group has made "Global TOP 5" and "Improvement of Corporate Value" its Medium-Term Management Policy.
More specifically, the following three key measures have been put forward as part of the Medium-Term Management Policy.

- **Expansion of new fields and reinforcement of product competitiveness**
- **Expansion, enhancement and reinforcement of global business**
- **Pursuit of overall optimization**

In the Medium-Term Management Policy, risks related to information security are deemed the risks with the greatest potential impact on business management.
The "various consequences of information security incidents, including the release or leakage of information" are considered the greatest risk, and NTT DATA, as a company that provides information systems, is committed to guaranteeing information security and protecting personal information.

Balancing Ensuring Safety with Active Use of Information

To better respond to the increasing globalization of customers, the NTT DATA Group has also implemented global management to ensure the spread of knowledge to each and every employee of Group companies, and to create a work environment that allows the expertise of the entire group to be applied in full.
The objectives of the NTT DATA Group Security Policy (GSP), ensuring safety of information and actively utilizing and sharing information, are essential as a partner that supports customer reform. More specifically, ensuring the safe distribution of knowledge on a global scale, and implementing efforts for preventing incidents related to information security from occurring are essential for stopping the leakage or release of customer's valuable information.
To this end, it is essential that we are aware of our responsibility as professionals dealing with information and ensure that information security is always taken into consideration when taking actions.
In FY 2015, NTT DATA has set the following three information security strategies, and has implemented the necessary measures to achieve them.

Priority 1
Enhancement and strengthening of security measures
Enhancing and strengthening measures on a global level

Priority 2
Promotion of the security of commercial systems
Thoroughly preventing internal wrongdoing and strengthening response capabilities to cyber attacks

Priority 3
Upgrading of preventive measures and improvement of ability to respond to accidents
Improving accuracy in detecting unknown malware and enhancing response capabilities in case of accidents

● Key Measures in Information Security Strategy

Information Security
Management System

Information Security Management System

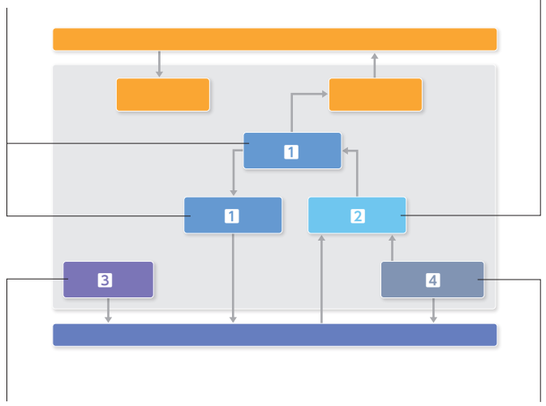
The NTT DATA Group has built an information security management system and has established an information security governance in order to deal with information security risks.
Each organization plays a specific role in ensuring information security, monitoring the direction and state of implementation of measures taken by each business unit running working areas and projects, and finally evaluating results. It also implements backup measures like inspections and emergency response.
Additionally, we are committed to the timely and accurate disclosure of information regarding the results and conditions of each organization. We acknowledge as our stakeholders a variety of parties including all our customers, shareholders and investors, as well as all our suppliers and employees and their families, and we exercise our social responsibility as a good corporate citizen by having the IR department deal with all shareholders and investors, and the employees of the sales department deal with customers. Furthermore, we consider all initiatives aimed at the establishment of information security as one of our responsibilities towards society and in 2008 we created and released the first information security report as a systems integrator.

1 Information Security Committee
[Assessment] [Steering]

The Information Security Committee sets information security strategies for the NTT DATA Group with the aim of minimizing information security risks and ensuring safe utilization and sharing of information.
Furthermore, it evaluates as a whole the information security implementation activities for each fiscal year, which are based on information security strategies, taking into consideration monitoring information for each activity, the results of internal audits and other factors. Each activity is reviewed based on the results of the evaluation, and proposals are made for new information security strategies.
The Information Security Committee is overseen by the Representative Director and Senior Executive Vice President and CISO (Chief Information Security Officer) and is held regularly with the managers of each sector in attendance (held a total of 65 times as of December 2015).

2 Information Security Office
[Monitoring]

Established as the special group for implementing information security activities throughout the NTT DATA Group.
This group conducts individual information security activities based on information security strategies, as well as monitoring of the implementation state of each information security activity.



3 Internal Audit Department
[Auditing]

The Internal Audit Department at NTT DATA conducts internal auditing related to information security.
This involves information security audits of each sector from a perspective that is completely independent of business procedures.
Results of audits are relayed to the Information Security Office, and improvements or reviews of systems or activities are implemented whenever required.

4 NTT DATA-CERT
[Backups]

Established in the Information Security Office and operates as the Special NTT DATA Group Security Incident Response Team (CSIRT)* Collects and analyzes information, and devises the appropriate response for preventing security incidents from occurring. Provides emergency response in the event that a security incident does occur.

* CSIRT (Computer Security Incident Response Team) is an incident response team comprised of security specialists. The team collects and analyzes information on security incidents, security-related technologies and vulnerabilities, and conducts activities for effective response and training.

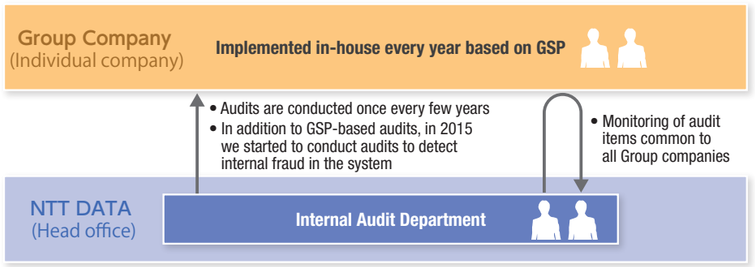
Information Security Governance

Framework of Audit and Monitoring

NTT DATA established the NTT DATA Group Security Policy (GSP) in FY2006 and has been applying it to all NTT DATA Group companies in order to promote information security thoroughly. For this purpose, we have established a framework of audit and monitoring for all Group companies including overseas ones.
We have been conducting information security audits from the three perspectives of "thoroughness of basic operations", "protection against external attacks" and "protection against internal fraud".
In future, we will focus more on audits against external attacks and internal fraud, while continuing the audit of basic operations.

1	Thoroughness of basic operations	We check the state of security management in the organization based on GSP and control information systems handling personal information.
2	Protection against external attacks	We verify the state of systematic security measures of Group companies against cyber attacks from the outside because in resent times the techniques of the attacks have evolved and become more sophisticated.
3	Protection against internal fraud	We are committed to preventing internal fraud by verifying the state of the information system's countermeasures.

● Internal Audit System



Global Governance

In the NTT DATA Group's overseas bases, we have been conducting solutions-centered business operations in North America, EMEA (Europe, Middle East and Africa), APAC (Asia-Pacific) and China since FY 2012. In conjunction with this, we have also been restructuring the operational framework for information security.

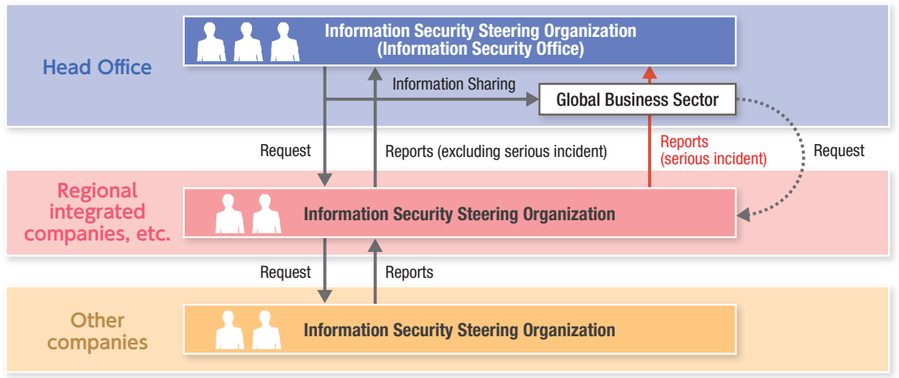
Cooperation for supporting global security

In order to ensure the global governance of information security, we have established an information security governance framework consisting of three levels of Information Security Steering Organization placed in headquarters, regional integrated companies and other companies.
Information Security Steering Organization at each level closely cooperate with each other and play a role in the preparation and development of information security policy, in the monitoring of information security measures, emergency response and measures for the prevention of incidents.

Conduction of incident response workshops

With the goal of strengthening global governance, in FY 2015 we have particularly focused our efforts on ensuring that initial response to accidents can be properly carried out on site. In order to achieve this goal we have conducted a series of workshops.
Targeting Group companies in Japan and overseas, we have implemented training based on initial response guidelines in many parts of the world. This has contributed to furthering understanding of the purpose of initial response and of what each employee must do when responding to incidents as well as to deepening the knowledge of the goals and methods of today's cyber attackers through the study of actual incidents which have taken place in the NTT DATA Group.

● Structure of Information Security Governance



Platform for a Safe and Secure Commercial System

Ensuring the Security of Commercial Systems

In recent years, cyber attacks on information systems such as unauthorized access via Internet, internal intrusions by means of malware (so called targeted attacks), etc., have increased in intensity. In order to respond to these attacks, in addition to dealing with all the known vulnerabilities (security deficiencies) of information systems relying on the latest information available, it is also important to devise measures for detecting threats and for neutralizing damage in consideration of the attack methods. On the other hand, given the parallel occurrence of internal malfeasance episodes, such as the unauthorized appropriation of large quantities of personal information or of information tied to large amounts of cash, there is also a definite need for sound operational management of this important information.
The NTT DATA Group, in order to thoroughly ensure the prevention of internal malfeasance as well as to strengthen its capabilities to respond to cyber attacks against commercial systems built and operated for its customers, is taking the following 4 steps of (1) building appropriate security measures starting from the development stage, of (2) establishing periodic vulnerability checks (security diagnosis) for operating systems, of (3) setting up a framework for promptly responding to detected critical vulnerabilities and of (4) ensuring sound operational management of important information.

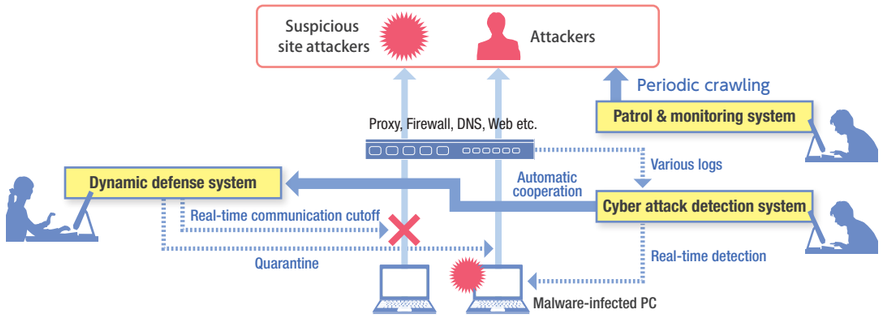
Dealing with the latest security technology trends

The NTT DATA Group, in connection with implementing the above steps, in addition to promptly sharing information on the latest security technology trends and vulnerability information, will apply the above-mentioned response to developing and operating commercial systems and will strive to provide systems which can be used safely and securely.

Information Security System Platform

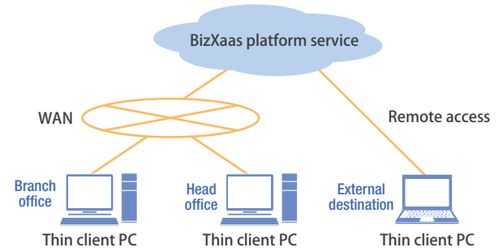
In-house IT Platform for Minimizing Risks

NTT DATA conducts risk analysis for internal operation systems on an ongoing basis and actively introduces security measures to its internal IT platform for dealing with the information security risks posed by new threats. At present, the security measures consist of three systems, “patrol & monitoring system”, “cyber attack detection system” and “dynamic defense system”. These systems are developed and operated by NTT DATA.
The patrol & monitoring system crawling Web sites on a regular basis in order to detect Web falsification at an early stage. The cyber attack detection system incorporates in real time the logs of network devices and security devices into a database, detects cyber attack by using in-house developed detection patterns and identifies malware-infected PCs. Using information provided by the cyber attack detection system, the dynamic defense system cuts off communication between suspicious sites and PCs and isolates malware-infected PCs.



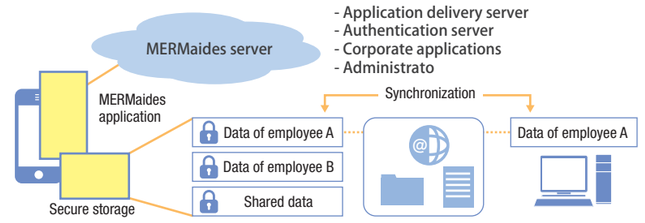
Thin client “BizXaaS Office” DaaS

“BizXaaS Office” is a service which provides employees with a PC environment in the cloud. It prevents information leakage from PCs by aggregating the client environment in the cloud and replacing PCs with thin client PCs, thus additionally allowing to save power in the office. Moreover, as a telework-promoting solution, it also operates in-house desktop services.



“MERMaides” mobile platform

It effectively protects information by isolating business data within a mobile device and encrypting the business applications and data stored therein. Furthermore, by linking up with existing authentication systems via the mobile gateway feature and by seamlessly performing synchronization with internal e-mail and business systems, it allows one to conduct business anytime and anywhere.



NOSiDE quarantine system

The NOSiDE quarantine system inspects computers accessing the Internet. It protects computers from cyber attacks exploiting vulnerabilities via the Internet. Also it prevents malwares from leaking information to the Internet. The system allows compliant computers to access external sites. On the contrary it prohibits noncompliant computers from accessing them.

“ETRANPOT” Information distribution infrastructure

This is a system for securely transferring files between customers associated with NTT DATA and NTT DATA Group companies. Files cannot be stored outside a predetermined time period and only parties which have been invited from within a company can send files from outside the company.

Management of the CSIRT

NTT-DATA CERT

The NTT DATA Group, operates "NTTDATA-CERT" as an internal CSIRT for preventing the occurrence of incidents through its normal activities, promptly detecting incidents and carrying out rapid and accurate emergency response.

Activities in anticipation of new security risks

NTTDATA-CERT, which aggregates in-house CSIRT activities which had been independently conducted in each business division since the year 2000, was launched in July 2010. Its main activities include the collection, analysis and dissemination of a wide range of security-related information, such as the methods of the latest attacks, the circumstances of incidents, etc., as well as the monitoring of communication, emergency response, research and development and cooperation with external sources. With the objectives and modus operandi of cyber attacks changing every year, we spare no effort to become able to respond to the latest risks.

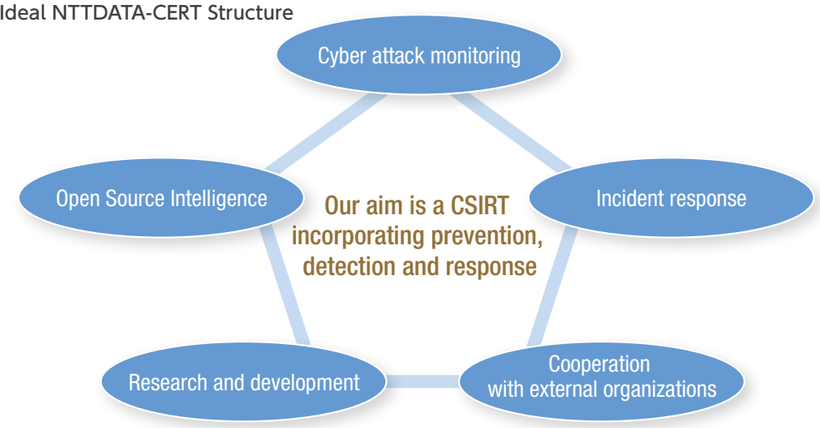
Wide range of activities in cooperation with inside and outside organizations

The range of NTTDATA-CERT activities is not limited to the NTT DATA Group. It collaborates in a wide range of ways with external security organizations like the CSIRTs of member companies of the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and the Nippon CSIRT Association (NCA).
This makes it possible to rapidly share security-related information as well as to promptly detect and respond to information security incidents.

Activities using OSINT

In running NTTDATA-CERT, we have adopted the open-source intelligence (OSINT) approach of actively using legally available information like reports, papers and technical documents released by government agencies and the mass media. This information, collected on a daily basis, is then analyzed by NTTDATA-CERT technicians expert in information analysis in order to predict security trends and results are then passed on to the various NTT DATA Group companies in the form of security-related news or quarterly reports.
Additionally, this information is used for formulating NTT DATA Group's security strategies and measures, such as the strengthening of cyber attack monitoring, and for defining the next research and development themes.

● Ideal NTTDATA-CERT Structure



Security Experts

Human Resource Development in the NTT Group

With information security threats getting more diverse and sophisticated, the number of technicians engaged in information security in companies in Japan currently stands at about 265,000 people. According to estimates by the Information Technology Promotion Agency (IPA), this number is about 80,000 people short. Against this backdrop, the NTT Group, in order to intensify the training of security experts within the Group, has set the goal of bringing the number of security experts in Japan to about 10,000 individuals from the current 2,500 individuals by 2020.

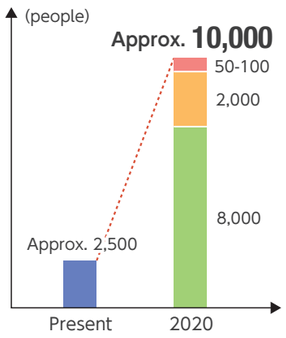
Since securing and training security experts has been recognized as an urgent need even within NTT DATA, we will continue to promote training as well as cooperation with external experts.

Training policies matching our role

The NTT Group divides its security experts into the three categories of security management consulting, security operation and security development, with each category being further subdivided into three distinct levels. Every NTT Group company is similarly committed to human resources training policies matching our role.

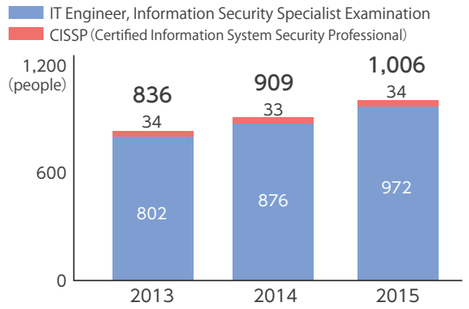
● Strengthening of Security Experts Training in the NTT Group

Level	Title	Job classification: Security management consulting / Security operation / Security development
Advanced	Security Master / Security Principal	Produce first-rate experts with the best performance in the industry
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



Acquisition of Qualification within NTT DATA

NTT DATA is promoting the training of human resources specializing in information security. As of January 2016, we have enrolled 972 individuals certified as Information security specialists by the IPA and 34 individuals who have obtained the CISSP international certification (Information Security Professional certification qualification).



Overall Outlook of Solutions

The Future of Information Security

At present we are faced with growing demands for enhancing cyber security measures against Advanced Persistent Threat attacks, preventing information leakage resulting from internal fraud and protecting specific personal information like "My number" data. Add to this that in the future information security will probably continue to become more and more complicated. At NTT DATA, we are anticipating the future of information security, concentrating our efforts on the automation of cyber security countermeasures by SIEM as well as on network technology enabling the IoT to protect itself autonomously.

In the future, information security measures for products connected by sensor to the IoT, like vehicles, drones, smart meters and so on, will not only protect information assets, as they have until now, but will also take on the fundamental role of protecting people's lives. At NTT DATA, we are working to create systems which balance providing convenience to customers with ensuring their safety, not only through technology but also in the way we run our operations.

New security technology initiatives

Given current social trends, 2020 will be a watershed year in the world of information security. Cities will become places where the physical plane of people and devices will merge with cyberspace. NTT DATA is committed to developing new technologies in view of this novel concept of protecting every aspect of such an environment. Among the myriad of new technologies, the key to the future of information security is probably going to lie with AI (artificial intelligence). AI will play a central role, not only in SIEM and IoT self-protecting network technology, but also in all major technologies that NTT DATA has been developing in view of 2020, including automatic vehicle operation, defense technology globally linking together each company's threat intelligence, etc. Furthermore, interlinking with AI will also be vital to minimize information leakage by automated incident response.

Additionally, we are also working on medium-to-long-term research and development including utilization and reliable device authentication of wearable devices, improvement of forensic technology, etc. The one element in common to all these technologies is the desire to ensure the necessary degree of security for people to lead safe and secure lives.

4 Categories of Solutions

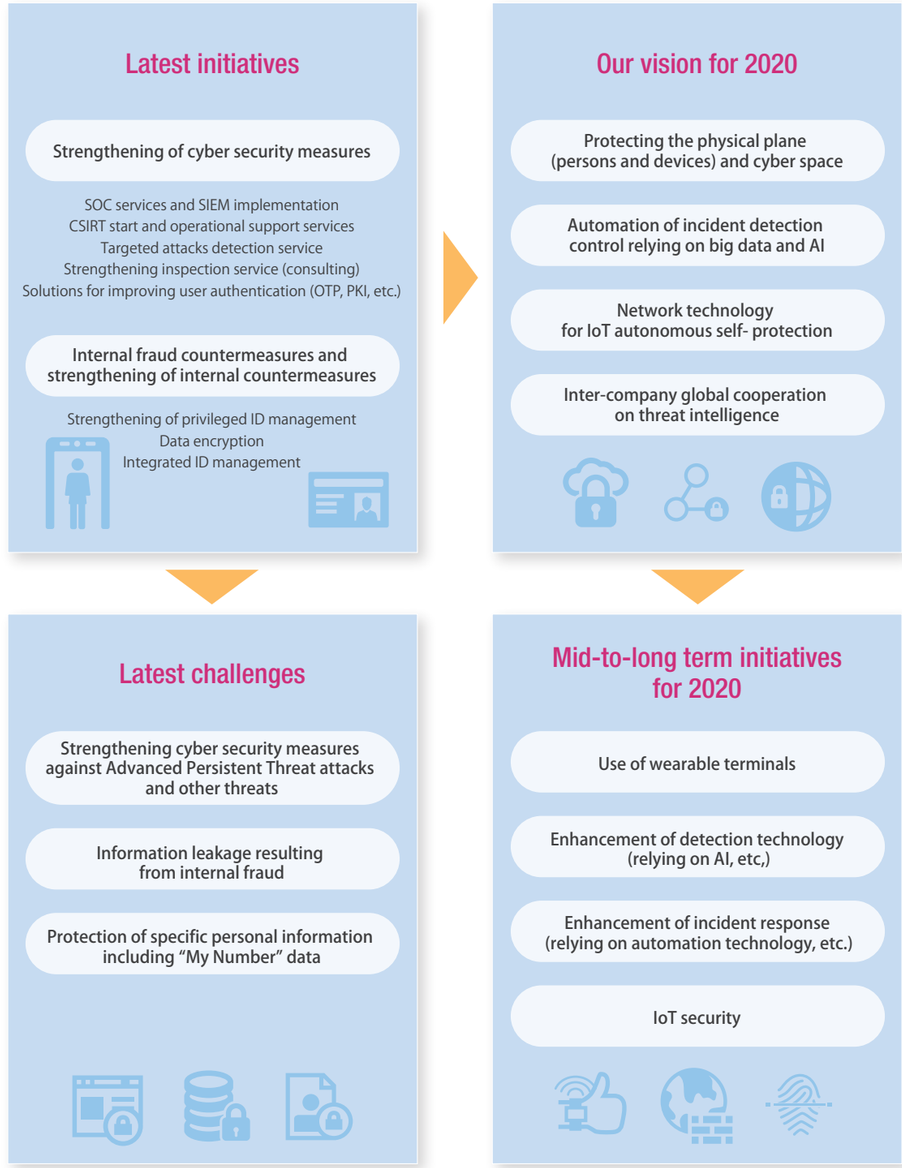
The solutions offered by NTT DATA to solve every aspect of our customers' security challenges can be roughly divided into four general categories.

Against cyber attacks, our line-up of solutions for each process offers, first, "Identify" and "Protect," and then "Detect" and "Respond and Recover." This allows us to perform all stages in one stop, from analyzing existing conditions to proposing and executing solutions tailored to our customers.

● 4 Categories of Solutions

Consulting on analysis of existing conditions and planning of countermeasures	Introduction and operation of security tools	SOC and security monitoring services	Incident response support
[IDENTIFY]	[PROTECT]	[DETECT]	[RESPOND and RECOVER]
● Inspections for strengthening cyber security ● Strengthening defense against targeted attacks ● PCI DSS total service	● Multi-factor authentication technology ● Integrated ID management ● Network security diagnostic services	● Targeted attacks detection service ● SOC service ● SIEM introduction and implementation support services	● CSIRT implementation support service and operation support service ● Forensic Lab ● Security and incidents emergency services

● Future Aspect of Information Security



Overview of Solutions

◎ Consulting on analysis of existing conditions and planning of countermeasures

Inspections for strengthening cyber security	By bringing to light the state of customers' cyber security measures and by clarifying measures to be implemented in the future, as well as their degree of priority, we help customers come up with the optimal cyber security plan. With a rapidity of response that makes it possible to implement measures in as little as two months, we bring to light the state of measures targeting known threats as well as new threats, helping establish the newest and best security level at all times. Verifying the conditions of security measures based on know-how obtained from actual security incidents is a feature unique to NTT DATA services.
Strengthening defense against targeted attacks	We help reduce the probability of attacks by repeatedly implementing training sessions simulating Advanced Persistent Threat attacks, appraisal of existing conditions through training and education of employees. In addition, assuming that a certain percentage of attacks will end up being successful, we also help formulate so called "exit measures" for preventing leakage of internal information. Linking together the system checks aimed at preventing information theft, their respective results and the proposing of solutions and services for strengthening resistance is another feature unique to NTT DATA services.
PCI DSS total service	As Japan's first QSA (PCI SSC certified Examining Authority), we provide global standard security to fit our customers' systems focusing PCI DSS compliance support consulting. As part of our total support from the planning stage to the final check prior to inspection, we provide a variety of solutions to solve the problems identified in the course of gap analysis and system testing. In the inspection and reporting stages, we carry out on-site surveys as QSA. We will continue to check day-to-day compliance and support the early detection and resolution of problems even after certification.

◎ Introduction and operation of security tools

"BXA (BizXaaS-Authentication)" Multi-factor authentication technology	We offer secure and reliable personal authentication requiring the user to be in possession of a token. In the event a password is stolen via the Web, that password can no longer be used after one minute, thus preventing unauthorized login by impersonators. As a response against the illegal remittance attacks by malware recently denounced as a threat, it is also possible to provide a new one-time-only password that proved effective against malware attacks after login. This technology boasts a spectacular track record with more than 80 financial institutions and more than 30 corporations having adopted it in Japan.
"VANADIS Identity Manager" Integrated ID management	As an entirely made-in-Japan software, it achieves integrated ID management by meticulously supporting typically Japanese business practices like concurrent information and Japanese organizational structure. Featuring a wide range of functions, including Provisioning functions, Group-management functions, Single Sign-on functions, etc., it can be adjusted to suit each customer's organizational situation. In addition to being equipped with an interface functioning with a variety of systems, it can also be set up in a short period of time through an established framework. Being based on NTT DATA in-house-developed software, its reliability is backed by a track record reaching back more than 10 years.
Network security diagnostic services	We inspect the customer's' network system of network devices and servers using a variety of techniques to assess whether a security problem exists. We then report on the impact that detected problems have on customers' services and propose corrective measures in order to improve the system and prevent security incidents in the future. Other features unique to NTT DATA services include removal of false positives both with the help of tools and manually by highly-skilled technicians, conduction of thorough and accurate inspections as well as original and easy-to-understand reports submitted by technicians.

◎ SOC and security monitoring services

"PatoLogphin" Targeted attacks detection service	By analyzing proxy logs, this service detects Advanced Persistent Threat attacks against an office environment (malware infection) which would otherwise be difficult to detect with existing security products like anti-virus software, firewalls, IDS / IPS, etc. Since malware detection takes place at the pre-infection stage preceding actual infection, detection and countermeasures can be implemented before any damage, for example information leakage, is caused. This service does not require purchasing any new security products and it can be used right away.
SOC service	As part of the Managed Security Service, we conduct comprehensive monitoring of IDS / IPS, firewalls, DB firewalls, Web application firewalls (WAF) and the likes. Monitoring, failure correspondence, monitoring, analysis, monthly reports, etc., are conducted by professional analysts skilled in monitoring, failure response, detection alerts, etc. It is also possible to combine sandbox-type systems against unknown malware which detect malware from Web traffic and e-mail traffic with Advanced Persistent Threat attacks detection services.

SIEM introduction and implementation support services	By monitoring and analyzing logs in an integrated and interrelated way through Security Information and Event Management, it is possible to identify potential risks that can not be detected by monitoring with security equipment alone. With more than 300 data sources supported, we monitor application data and protocol anomalies as well as database activities. We conduct advanced rule-based and risk-based correlation analysis which makes it possible to promptly assess situations and identify threats by bringing them to light.

◎ Incident response support

CSIRT implementation support service and operation support service	As emergency measure in the event of an incident had occurred, we help set up and operate a CSIRT (Computer Security Incident Response Team) for ensuring damage control and prompt recovery. Relying on NTT DATA's vast experience in CSIRT implementation and operation, we set up and operate CSIRTs in the best suitable way for our customers' organization by providing information on the system's definitions and construction as well as its security. Furthermore, by opening CSIRTs to the outside, we promote cooperation with external CSIRTs with the additional effect of allowing the sharing of useful information.
Forensic Lab	The Forensic Lab not only promotes the development of forensics-related technologies but also provides assistance for those customers who require forensic help. Relying on academic researches on the latest trends in forensics, we offer tool-assisted collection and reporting of evidence, malware analysis, product log analysis, etc., to meet our customers' requests. We analyze behaviors after deliberately infecting systems with malware and we also possess an environment (Honeynet) for verifying how the various security products used by our customers respond to attacks, thus contributing to advancing forensic accuracy.
Security and incidents emergency services	In the event of a security incident, we will provide on-site assistance by offering advice on every stage of the process, from first response to full-scale response and damage minimization. When an emergency is reported, we provide initial advice by phone or e-mail. Next, as part of on-site first response, we provide guidance on how to investigate occurring circumstances and prevent damage from spreading, and then formulate and conduct causal analysis and planning of corrective measures as part of a full-scale response; finally, we assist with recovery and recurrence prevention. This service can also be used to obtain second opinions in order to carry out a more appropriate response.

External Communication

NTT DATA has been actively promoting external communication in order to contribute to the promotion of information security measures for the whole of society.
More specifically, in addition to providing statistical information on incidents involving disclosure of personal information in companies, we have been suggesting approaches and measures related to the changes in risk and incident trends of personal information.
Furthermore, in addition to measures for preventing information leakage due to human error, we have also been spreading awareness on the need for cyber attack countermeasures by calling attention to the increased damage resulting from cyber attacks.
Some of this information was even quoted in "National cyber security strategy" (guidelines concerning the disclosure of information on cyber security breaches and risks) published in March 2015 by the Government agency : National center of Incident readiness and Strategy for Cyber Security (NISC).
We have also submitted reports on security to teams studying local government information security measures under the supervision of the Ministry of Internal Affairs and Communications.

● 2015 Security Reports

No.	Date of Issue	Title
1	Jan 2015	Caution on using wireless LAN in hotels! What are Darkhotel attacks?
2	Feb 2015	How not to get involved in crimes perpetrated through "Tor"
3	Mar 2015	Malware installed in brand new PCs? On Lenovo's Superfish
4	Apr 2015	How to use Internet Banking safely
5	May 2015	Increase in ransomware for demanding ransom money!
6	July 2015	Can cars be illegally remote-controlled !? IoT Security requirements
7	Aug 2015	Alert level up! Latest trends of "targeted attacks" and relative countermeasures
8	Sep 2015	Are the sites you always visit really safe? - How to avoid falling victims of your favorite sites-
9	Oct 2015	On the challenges of using AI in the security sector
10	Nov 2015	Infection routes of Android™ malware and relative countermeasures
11	Dec 2015	Coming soon!? Freedom from overtly complex passwords

Contributing to Invigorate the Security Sector

NTT DATA has also been active in organizing lectures featuring guest speakers throughout Japan. In FY 2014 and FY 2015 we conducted lectures at seminars sponsored by the Japan Network Security Association (JNSA) and the Ministry of Economy, Trade and Industry in every district in Japan. Furthermore, we held lectures on scouting security personnel and on CSIRT at the "ISS SQUARE horizontal workshop" organized by the Institute of Information Security as well as at the InternetWeek professional internet technology seminar.
In addition, we have had a hand in planning "security camps" organized by the Ministry of Economy, Trade and Industry for discovering and nurturing young and talented cyber security personnel since their inception in 2004. In 2015, we were also deeply involved in running and chairing the camps.

Our Aim: The Creation of a Safe and Secure Society

NTT DATA has been working to spread, and create awareness of, security measures by promoting external communication through the above-mentioned provision of information, lectures featuring guest speakers and participation in external activities,. Through such efforts, we aim to boost the entire security sector by creating new information security concepts and trends as well as to build a safe and secure society.

Information Security Education and Training

Education and Training Activities for an Information Security-Oriented Mind Set

For a sustained implementation of information security, it is essential that each employee, officer, business partners and temporary staff be aware of their responsibilities as professionals handling information. NTT DATA has been striving to train professionals by promoting understanding of rules and conducts and by creating an information security-oriented mind set through ongoing information security education and training.

Additionally, in order to maintain the security level of the entire group above a certain level, NTT DATA has been providing the necessary tools so that each Group company can carry out education on information security and protection of personal information in line with the NTT DATA Group Security Policy (GSP) and has been working to raise awareness of the overall NTT DATA Group security.

Introduction of Multiple-language e-learning Courses

In 2014, with the aim of helping NTT DATA employees around the world acquire the necessary security knowledge and to act on it, we started to provide information security education in multiple languages.
Information security education in the e-learning format is available in six languages (Japanese, English, Chinese, German, Italian and Portuguese) and 9 patterns. More than 40,000 Group employees have already taken advantage of it. Educational materials have been brushed up and properly translated with the cooperation of the regional headquarters' information security officer and information promotion officer. Not stopping at implementation, we have also been analyzing results and working to strengthen weaknesses.

Expansion of Educational Activities in Overseas Group Companies

We have been actively promoting security education and training even in overseas Group companies and we have been conducting GSP indoctrination and security training targeting all companies.
As our main initiative concerning overseas Group companies in FY 2015, we held an incident workshop by NTTDATA-CERT in the APAC zone and China. After the conclusion of the workshop, we conducted testing in order to assess the penetration rate of understanding.

Workshop held in China

Results of FY 2014/2015 Information Security Training

Target	Content and Format	Number of Participants	
All employees	**Information Security and Personal Information protection IBT** (e-learning)	Improved understanding of information security policy/Understanding of basic conduct in case of information security accidents/Proper handling of laptop PCs or small portable media/Basic stance on personal information/ Handling of personal information/Understanding of internal rules/improving awareness on the subject of personal information * FY 2014/2015 results: 100% of employees	
All employees (optional)	**Information Security Workshop**	Workshop on the subject of information security and personal information in response to individual requests * FY 2014 and FY 2015: once each	
Each management level	**Information Security lectures** (classroom instruction)	Description of the knowledge, differences in roles and responsibilities, approach, and required items for each employment position, including new employees, mid-career employees, division managers, and department managers Acquiring knowledge for improving understanding and implementation of information security	
Business partners and temporary staff (required)	**Support to Information Security Policy education**	Provides training of content that should be known by partners working at NTT DATA related to the protection of personal information, and information security rules at NTT DATA Training is required when using company systems, and regularly training is essential * Available in multilingual format (English, Japanese, Chinese)	
Business partners and temporary staff (new partners)	**Information Security Training handbook**	Handbook that outlines how to deal with information security and personal information when working within the NTT DATA, distributed by contract from the NTT DATA Group. The handbook is for new NTT DATA Group partners. * Available in multilingual format (English, Japanese, Chinese)	
Group company employee, business partners, and temporary staff	**GSP security training IBT** (e-learning)	Improving NTT DATA Group Security Policy understanding/Methods to deal with personal information/Description of the NTT DATA Group Security Policy (GSP) * Available in multilingual format (English, Japanese, Chinese) * FY 2014 results: 124 companies, 37,044 individuals	* FY 2015 results: 94 companies, 31,770 individuals
	Personal Information Protection training IBT (e-learning)	Approach related to personal information protection, training for information security rules that should be known as new NTT DATA Group partners * FY 2014 results: 65 companies, 23,962 individuals	
Internal Auditors	**GSP Internal Auditor training** (offline training)	Training for conducting information security audits training with simulated audits * Available in a multilingual (English, Chinese, Japanese) format that can be completed by employees at their desks * FY 2014 results: 89 companies, 399 individuals. FY 2015 results: 86 companies, 431 individuals	

Information Security Activities

1998	December	"Information Security Policy" developed
2000	February	Greater venture systems (NTT DATA INTRAMART CORPORATION established)
	March	Accounting system using consolidated balance sheets started from the March quarter
	June	Information security policy assessments started
2001	February	"Standard Security Policy (SSP)" developed
	June	"Personal Information Protection Regulations" developed
	July	"Personal Information Protection Policy" announced
	September	First BS7799 certified in Japan
2002	September	Training (CISP) started for partners
	October	NTT DATA Group Security Agreement (GSA) established
2003	June	Acquired Privacy Mark Certification
	July	Established system for regional subsidiaries (system incorporating nine regional subsidiaries)
2005	June	P2P software checks became available for remote connection PCs
	November	Started TSF operation
2006	July	Started trials of Telework
	September	Declaration received from all Employees at NTT DATA (ensuring that users delete work related information from their own PCs, and prohibiting work on their own PCs)
	October	Declarations required from all Employees working within the NTT DATA Group
	November	Declarations required from subcontractors
2007	April	ISMI Certification obtained for the head office building
	July	Thin client services started
	December	Email filtering service started
2008	February	Telework system started
	March	First "2008 Information Security Report" as system integrator published
	April	NTT DATA Group Security Policy (GSP) published
	November	"Information Security Improvement Month" established
2010	March	"2010 Information Security Report" published
	July	"7 Wise Conditions for Basic Security Activities" established
	July	NTTDATA-CERT established
2011	April	Joined NTTDATA-CERT FIRST
	May	Internal connection service for smartphones started
	June	NTT DATA Social Media Policy announced
	July	Office computers switched to notebook PCs following restrictions to power consumption
2012	February	Training for targeted email attacks (for executives and management level)
	March	"Information Security Report 2012" issued
	July	Training for targeted email attacks (for employees)
2013	April	New governance system run by operating companies started
	June	Online storage service application system introduced
	October	"Forensic Laboratory" established
2014	March	"2014 Information Security Report" issued
	May	Start of security training from the Aichi Prefectural Police
	August	The Group's shared security platform becomes operative
2015	April	Start of real-time detection of unknown malware
	August	Rules for handling My Number data enacted

Company Profile (as of September 30, 2015)

[Name] **NTT DATA Corporation**

[Head Office] Toyosu Center Building, 3-3, Toyosu 3-chome, Koto-ku, Tokyo 135-6033, Japan

[Established] May 23, 1988

[President and CEO] Toshio Iwamoto, President and Chief Executive Officer

[Business Areas]
- System integration
- Networking system services
- Other business activities related to the above

[Number of Employees] 80,132 (consolidated) 11,378 (non-consolidated)

[Capital stock (consolidated)] 142,520 million yen

[Net sales (consolidated)] 743,200 million yen

[Ordinary income (consolidated)] 31,200 million yen

[Consolidated subsidiaries] 263

[Participating groups] (excerpt)
JAPAN CARD DATA SECURITY CONSORTIUM
Security Camp Executive Committee
Information Security Operation providers Group Japan (ISOG-J)
Nippon CSIRT Association
JASA - Cloud Information Security Promotion Alliance (JCISPA)
Japan Network Security Association (JNSA)
NPO Institute of Digital Forensics
Information Security Technology study group (IST)
NPO Japan Information Security Audit Association (JASA)
Security Promotion Realizing sEcurity meAsures Distribution (SPREAD)
Electronic Commerce Security Technology Research Association (ECSEC)
Japan Smartphone Security Forum (JSSEC)
Japan Data Communications Association
Japan Society of Security Management (JSSM)
Japan Information Security Management Systems User Group (J-ISMS UG)

[State of Global Offices]
EMEA (Europe, the Middle East, Africa) 81 cities 17,700 employees /APAC (Asia-Pacific) 25 cities 12,000 employees
China 13 cities 3,500 employees / AMERICAS (North America) 61 cities 14,000 employees