Tomorrow, Together

KDDI

おもしろいほうの未来へ。

au

Cybersecurity Annual Report 2022

KDDI VISION 2030

The creation of a society in which anyone can make their dreams a reality, by enhancing the power to connect.

Contents

Editorial Policy

This report was published to introduce the KDDI Group's information security activities to our stakeholders and to improve their reliability in our business.

Period Covered

Unless otherwise stated, this report covers information security initiatives through the end of September 2022.

Referenced Documents

Ministry of Economy, Trade and Industry
"Information Security Report Model"

Website

KDDI
https://www.kddi.com/

KDDI Security Portal
https://www.kddi.com/english/corporate/kddi/public/security-portal/

KDDI Sustainability
https://www.kddi.com/english/corporate/sustainability/

Research & Development (R&D)
https://www.kddi.com/english/corporate/r-and-d/

Information Security Chairperson's Message

As KDDI VISION 2030, KDDI delivers the message, "The creation of a society in which anyone can make their dreams a reality, by enhancing the power to connect" and is working on a diverse range of businesses to develop a fruitful communication society. Information security is key in this pursuit. As the responsibility of an enterprise that plays a role in core infrastructure, KDDI positions information security as a critical issue for delivering stable telecommunications services at all times.

The proliferation of smartphones, the development of big data and AI technologies, and the corporate progress in digital transformation have led to the creation of new services using various information, which also comes with intricate and diversified risks in information security and privacy. Cyberattacks and other criminal activities in cyberspace by malicious hacker groups are increasing and getting more and more sophisticated every day.

Amid such circumstances, in order to protect telecommunications facilities from unauthorized access, tampering, targeted attacks, and other cyberattack threats, KDDI's security engineers are on vigilant duty round-the-clock for monitoring while we are simultaneously developing automated AI-driven technologies for analyzing and monitoring cyberattacks. Furthermore, KDDI regularly works in collaboration with CSIRTs in Japan and abroad, as well as other relevant organizations, to collect and analyze vulnerability information and attack trends to set up stronger security measures.

KDDI will continue to provide services that users can rely on as being safe by keeping up the development of our combat against increasingly sophisticated and complex emerging threats. This report introduces KDDI's security initiatives. We appreciate your interest and time in reading through this report.

Senior Managing Executive Officer, Director
and Executive Director, Technology Sector
and Information Security Chairperson

Kazuyuki Yoshimura

Jun. 2022 Senior Managing Executive Officer, Director (Current position)
Apr. 2021 Managing Executive Officer, Director
Jun. 2020 Executive Officer, Director
Apr. 2020 Executive Officer
Executive Director, Technology Sector (Current position)

Cybersecurity Trends

Despite the advances in security technologies, frameworks, laws and regulations in recent years, cyberattack methods have become increasingly sophisticated and complex, with an ongoing repetitive exchange of attacks and countermeasures.

Although investments in security are increasing year by year and a variety of security measures are being introduced, there is no end to the number of security incidents that raise public concern, such as large-scale personal information leaks, confidential information breaches that threaten management, and business shutdowns due to ransomware. In addition, there have been numerous incidents, both in Japan and overseas, of the types of attack that "could have been prevented with strict management." Examples include cyberattacks that do not necessarily use sophisticated methods, the misuse of unpatched equipment, the leakage of unencrypted information to the outside world, and incidents due to password and ID leaks.

Evolution of Cyberattacks and Necessary Protective Measures

Until the early 2000s, the main purpose of cyberattacks was to generate publicity and self-gratification, mainly by targeting individuals using computer viruses, worms, macro viruses, Trojan horses, and other methods that can enter terminals and trigger unexpected behaviors. Meanwhile, attacks targeting corporate clients began to occur, and zero-day attacks using undisclosed vulnerabilities were also seen. Endpoint countermeasures such as personal firewalls and anti-virus for terminal defense have been adopted as the main response to these attacks.

In the 2010s, attackers started targeting specific companies and governments, with the damage caused by cyberattacks becoming increasingly severe. A typical example is the cyberattack on the pension management system of the Japan Pension Service, in which personal information was leaked due to a virus infection triggered by a targeted e-mail. Mail isolation, which isolates suspicious mail, is considered a practical response to such targeted attacks. Perimeter-type defenses such as NGFW/IDS/ISP/WAFs are an effective way to prevent DDoS and various injection attacks, and should be implemented in conjunction with endpoint measures.

Characteristics of Recent Attacks and Necessary Protective Measures

Since the late 2010s, ransomware attacks, cryptojacking to unearth crypto assets (virtual currency), and the distribution of attack tools via the dark web have further strengthened the trend toward the industrialization of cyberattacks for the purpose of acquiring money and other assets. Cyberattacks have also been used by certain groups and countries as a tool to assert their politics and beliefs, and as a means of intellectual property theft and intelligence activities. The scale of damage also continued to grow. WannaCry ransomware, which spread in 2017, infected 300,000 PCs in 150 countries by exploiting a vulnerability in the file-sharing protocol SMBv1, causing damage to major Japanese companies, including the suspension of factory production and the suspension of order and supply systems with business partners. To counter the spread of ransomware and other attacks through such automated infection activities, a Zero Trust security model is effective, which is based on the concept of maintaining a secure state by verifying all access each time, both inside and outside the company's network.

Global Social Issues

As the demand for security measures increases, the shortage of security field human resources is becoming an issue not only in Japan but also worldwide. (ISC)² reported*1 that there was a shortage of 2.72 million security field human resources worldwide and 40,000 in Japan in 2021.

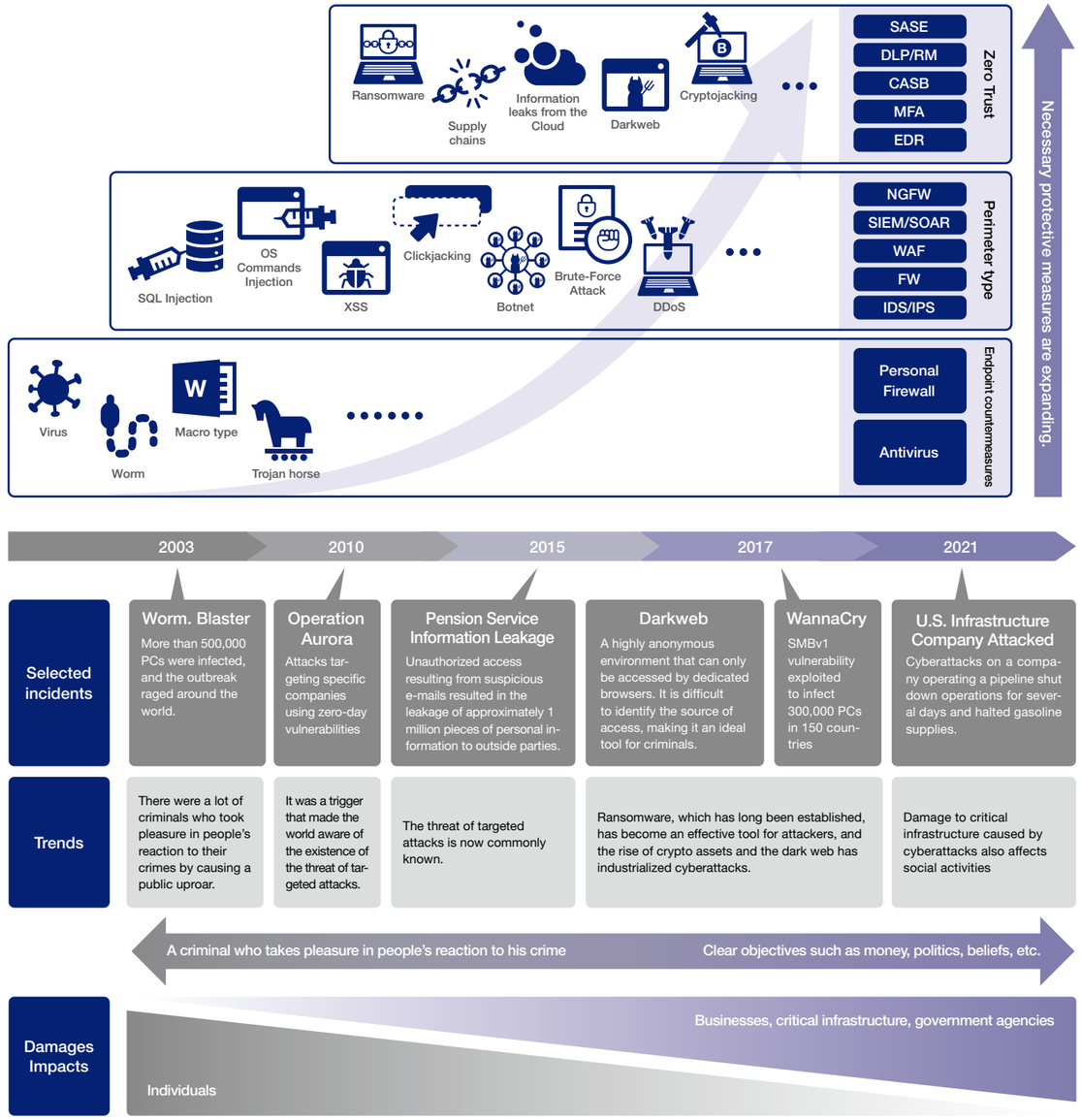
Meanwhile, cyberattacks have become more closely related to the real world than ever before due to the use of ICT technology in the critical infrastructure (digital transformation) and the penetration of IoT, and cyberattacks*2 involving human lives and critical infrastructure operations are occurring.

As described above, cyberattacks have become more sophisticated and complex in recent years, and their impacts have become extremely serious. In order to prevent damage to the critical infrastructure from cyberattacks, it is necessary to address security measures, including human resource development, as an issue for society as a whole.

*1 "A Resilient Cybersecurity Profession Charts the Path Forward - (ISC)² CYBERSECURITY WORKFORCE STUDY-", 2021, https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

*2 Cases of cyberattacks involving human lives and critical infrastructure operations

July 2019	A hospital in Alabama, U.S.A., suffered a ransomware attack that rendered all computers unusable for eight days. As a result, it was no longer possible to monitor the fetal heartbeat in the delivery room, and a newborn who was born during that time became severely disabled and died nine months later.
September 2020	A ransomware attack on the University Hospital of Düsseldorf, Germany, resulted in a patient requiring emergency transport to another hospital more than 30 km away from the planned destination, delaying urgent treatment and subsequently resulting in a confirmed death.
May 2021	Colonial Pipeline, a company that operates a pipeline system in the US, was shut down for several days by a cyberattack. This disrupted gasoline supplies, causing social disruption and leading to an increase in the average price of gasoline.



Information Security Governance

In response to increasingly sophisticated and skillful cyberattacks, the KDDI Group has positioned information security risk management as a critical issue and is working to strengthen information security governance. This chapter provides an overview of KDDI's information security promotion framework, internal regulations for information security, information security management cycle, information security audits, and information security training.

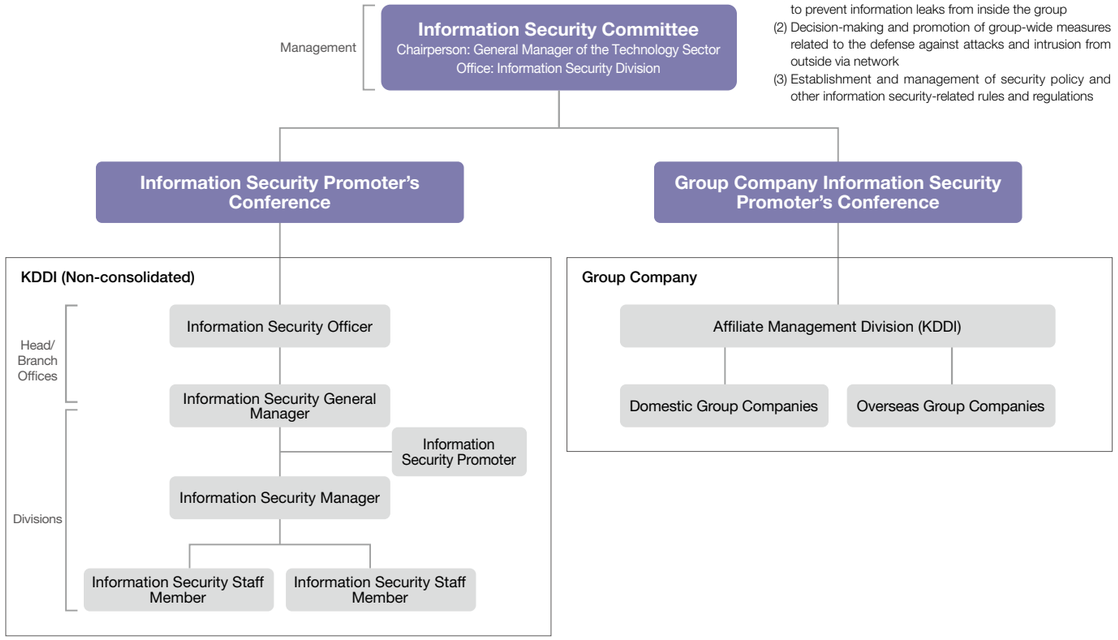
1 Information Security Promotion Framework

To ensure uniform information security throughout KDDI and the KDDI Group, we have established the Information Security Committee, chaired by General Manager of the Technology Sector and includes members from the management level, along with managers of sales, technology and corporate divisions.

Under the Information Security Committee, KDDI has established the Information Security Promoter's Conference and the Group Company Information Security Promoter's Conference, which consists of representatives from each department of KDDI non-consolidated basis and KDDI Group companies. This framework not only enables precise understanding of the status of information security management, but also promotes swift deployment of information security enhancement measures throughout the group.

Each group company has also established an information security management system. Furthermore, they work hard to reduce and prevent risks related to information security and cybersecurity, as well as evaluate and analyze risks and implement countermeasures and responses.

Information Security Management Framework



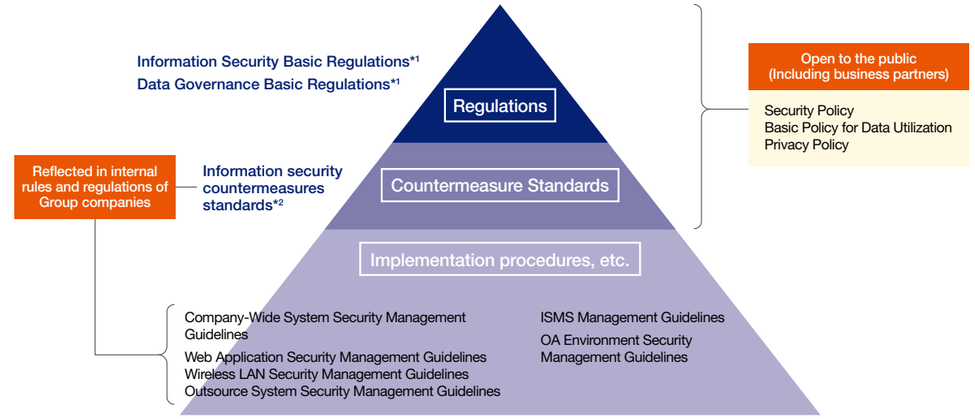
Roles of the Information Security Committee
(1) Decision-making and promotion of group-wide measures to prevent information leaks from inside the group
(2) Decision-making and promotion of group-wide measures related to the defense against attacks and intrusion from outside via network
(3) Establishment and management of security policy and other information security-related rules and regulations

2 Internal Regulations on Information Security

KDDI's internal documents on information security consist of the three layers shown in the figure below.

On the first level, we have established "Information Security Basic Regulations," which define our basic policies on information security, and "Data Governance Basic Regulations," which define our basic policies on data governance. The second level has standards for measures to ensure compliance with those standards, and the third level provides implementation procedures, etc.

In particular, we strictly handle customer data and confidential company information in accordance with our regulations and countermeasure standards, and always take appropriate protective measures against the risk of information leaks. To gain the trust of our customers and other stakeholders, we have established and adhere to a Security Policy and Privacy Policy, both of which are available to the public.



*1 Complies with Safety and Reliability Standards Appendix 3: Guideline for the Formulation of Information Security Policy (Ministry of Internal Affairs and Communications), Information Security Policy Sample Revision (JNSA), etc.
*2 Complies with Safety Standards for Ensuring Information Security in the Telecommunications Field (TCA), etc.

Open to the Public (Including business partners)

Security Policy

KDDI acknowledges proper information management is a critical management issue, and to ensure information security, formulated the Security Policy, which establishes the basic policy for information security, including the information security management framework, implementing information security measures, and establishing internal regulations on information security.

▶ https://www.kddi.com/english/corporate/kddi/public/security/

Basic Policy for Data Utilization and Privacy Policy

KDDI may obtain and use our customers' personal data to contribute to improving the value of their experience and to the sustainable development of society through our business activities, which include the provision of various services and products. "Personal data" includes data related to an individual, not limited to personal information as defined in the Act on the Protection of Personal Information (hereinafter referred to as "Personal Information Protection Act").

In recognition of the importance of personal data, KDDI has established the Basic Policy for Data Utilization*1 as clear guiding principles for our course of action to ensure the protection of personal data. KDDI sets forth the privacy policy*2 as guidelines for handling personal data based on the Basic Policy for Data Utilization.

*1 https://www.kddi.com/corporate/kddi/public/privacy-portal/ (Japanese site only)
*2 https://www.kddi.com/english/corporate/kddi/public/privacy/

Information Security Governance

3 Information Security Management Cycles

KDDI has obtained ISMS certification (ISO/IEC 27001: 2013)*1, and formulates an Information Security Policy at the planning stage as part of the information security management cycle, and also checks, reviews, and makes improvements according to the following information security management implementation cycle (PDCA cycle).

*1 ISMS certification (ISO/IEC 27001: 2013) A third-party conformity assessment scheme for information security. It was established with the goal of contributing to widespread improvements in information security and encouraging companies to target levels of information security that can be trusted around the world.

Overview of the Information Security Management Cycle

- **Plan (Plan)**
  Identify information assets, organize risks and issues, and formulate an Information Security Policy that defines information security measures suited to the organization and company's situation.
- **Introduction/Operation (Do)**
  Disseminate information to all employees and provide training and other education as necessary. By having employees act in accordance with the Information Security Policy, we aim to maintain the desired level of information security.
- **Inspection/Assessment (Check)**
  The Information Security Policy itself will be assessed regularly based on the situation and problems in the field after its introduction, as well as on the social context. It also conducts audits to ensure compliance.
- **Review/Improvement (Act)**
  Review and improve the Information Security Policy with reference to the contents of the inspection and assessment.

4 Information Security Audits

KDDI conducts the following three audits to confirm that information security-related guidelines are complied with and properly operated.

System Security Audits

When new telecommunications facilities are installed or renovated, audits are conducted by specialized department auditors to ensure compliance with the "Company-Wide System Security Management Guidelines."

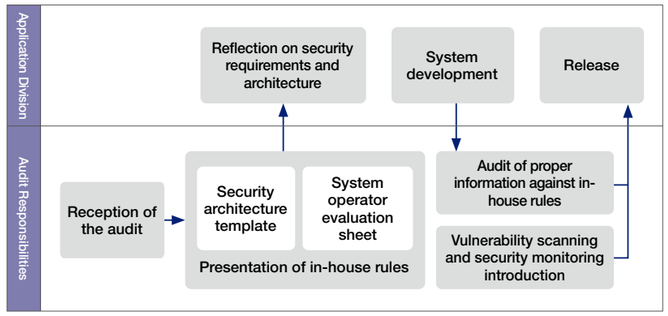
The security architecture template, which comprises the information contained in the Security Management Guidelines in a question-and-answer table format, is used for the audit. There are hundreds of audit requirements, and if a system does not comply with the mandatory requirements, the system architect will be asked to correct the situation.

As the speed of business accelerates, the number of systems to be audited, including reaudits, is increasing every year due to an increase in the number of systems released within a short period of time and the addition of functions and upgrading of equipment of systems audited in the past. We are efficiently responding to this trend by improving our daily operations and developing tools.

The operational flow of a security audit is shown in the figure on the right. First, the system configuration is confirmed with a preliminary questionnaire. Next, a written audit is conducted using the security architecture template.

Based on the results of written audits, network and web vulnerability assessments are conducted prior to release, and security monitoring mechanisms such as Intrusion Detection Systems (IDS) will also be implemented.

Operational Flow of a Security Audit



ISMS Internal Audits

Audits are conducted on each department within the scope of KDDI ISMS certification and on related companies in accordance with the "ISMS Management Guidelines" and "Integrated ISMS Internal Audit Procedures" by specialized departments or auditors selected from each organization within the company.

ISMS internal audits confirm that the information security-related norms to be complied with in the KDDI ISMS are properly operated and that all information security management activities are systematically implemented. We also confirm that ISMS activities have penetrated the audited organization and are being effectively implemented; if not, corrective action is required.

In addition, the results of ISMS internal audits and the results of ISMS activity effectiveness evaluation based on analysis of ISMS records are reported at management reviews for review and improvement.

Audits of External Partners

In cases where KDDI outsources all or part of its operations, KDDI conducts an audit of its external partners at least once a year to ensure that the same level of security as that of KDDI is appropriately maintained; the management system is also reviewed. In addition to the above, special audits of external partners are conducted by auditors from specialized divisions.

5 Information Security Training

Employee Security Awareness and Training

KDDI conducts annual e-learning security training for all employees. By continuously learning about the latest cyber threat trends, information leak cases, and their countermeasures, we aim to raise awareness of information security and improve skills to prevent incidents.

In addition, targeted email attack exercises that imitate cyberattacks are conducted on a regular basis. These exercises aim to continuously improve the security literacy of employees, each time raising the difficulty level of the emails sent as well as revising the exercise method.

Other security training is provided by level, such as basic information security training for all new employees and security management training for line managers, to prevent security incidents.

Information Security Governance

Training of Security Specialists

In order to protect our customers' data and the services offered from cyberattacks, it is necessary to develop human resources related to cybersecurity. KDDI is also engaged in systematic training at each level of employees' skills.

Engineers specializing in security participate in security training programs at external professional organizations to enhance their security expertise and deepen their professional skills in daily practice and exercises to respond to unknown attacks and incidents.

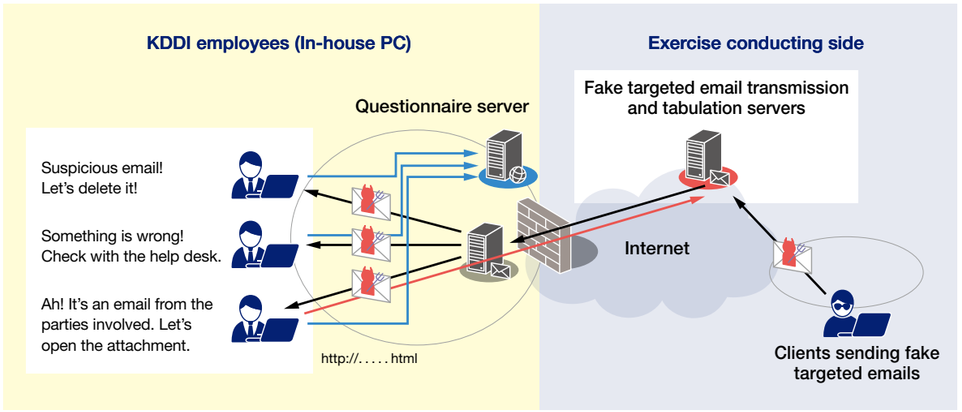
In addition, KDDI has established an in-house human resources development program that encourages employees to obtain the "Registered Information Security Specialist" national certification administered by the Information-technology Promotion Agency, Japan (IPA), and KDDI has one of the largest numbers of such registered individuals in Japan.

Moreover, we regularly conduct in-house cyberattack response exercises. Through collecting and analyzing the results of each exercise and the feedback from participating employees, we strive to maintain and improve employees' security awareness and cyberattack response capabilities.

Skills and Reference Standards Required for Security Field Human Resources

The vision for human resources	Skills possessed	Reference standard/ Reference qualification
Security specialists	• Security monitoring of facilities and systems related to the rendering of the provision of telecommunications services (hereinafter referred to as "facilities and systems") • Security audits of facilities and systems • Conducting rapid damage mitigation, investigation, etc. in the event of cyberattacks on facilities and systems	ITSS LV5-7
IT technicians (servers, networks, apps, devices, etc.)	• Design and construction of security quality systems • Secure operation of facilities and systems	Equivalent to ITSS LV3-4
Non-technical human resources (system users, etc.)	• Security literacy as a baseline • Information asset management based on ISMS	Equivalent to ITSS LV1-2

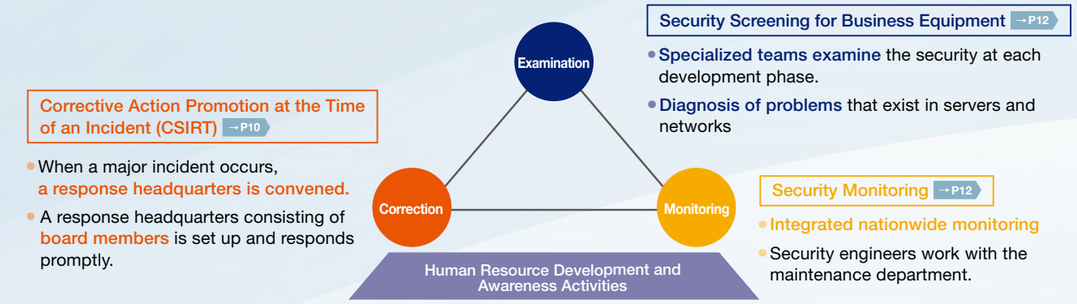
Example of an Exercise Using a Fake Targeted E-mail



Cyberattack Countermeasures

KDDI is continuously strengthening its security measures against cyberattacks based on three main measures: "Corrective action promotion at the time of an incident (CSIRT)," "Security screening for business equipment," and "Security monitoring."

This chapter introduces specific initiatives for the three measures.



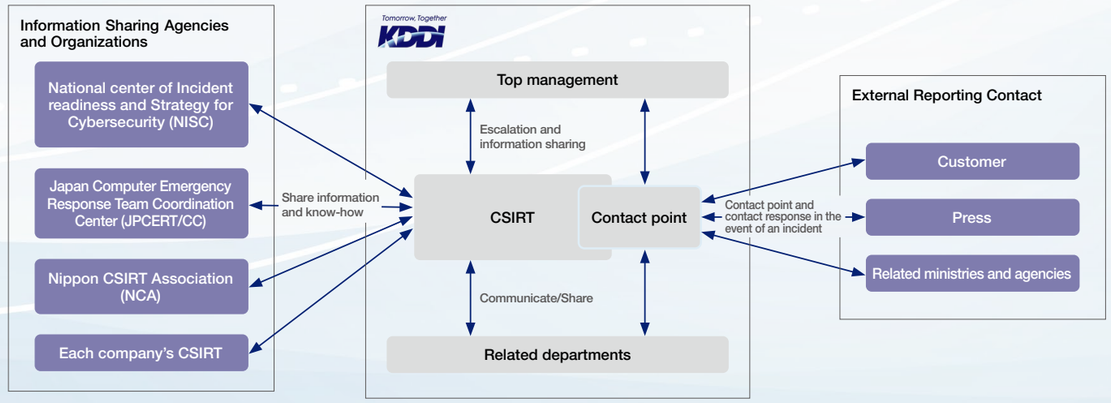
Corrective Action Promotion at the Time of an Incident (CSIRT)

What Is CSIRT?

CSIRT is a common name for a specialized organization that acts within an organization to respond to security incidents. KDDI established KDDI-CSIRT in 2013, and KDDI Digital Security*1 was added to KDDI-CSIRT in 2018.

When an incident occurs, KDDI-CSIRT cooperates with relevant internal departments to investigate the cause, preserve evidence, etc., as well as implement internal controls to bring the situation under control. During normal times, we also collect various information on cyberattacks and vulnerabilities to prevent future security incidents. We also participate in external security organizations, such as the Cabinet Cyber Security Center, ICT-ISAC, and JPCERT/CC, as well as the Forum of Incident Response and Security Teams (FIRST), a CSIRT community, and the Japan CSIRT Council, and we establish close inter-organizational cooperation.

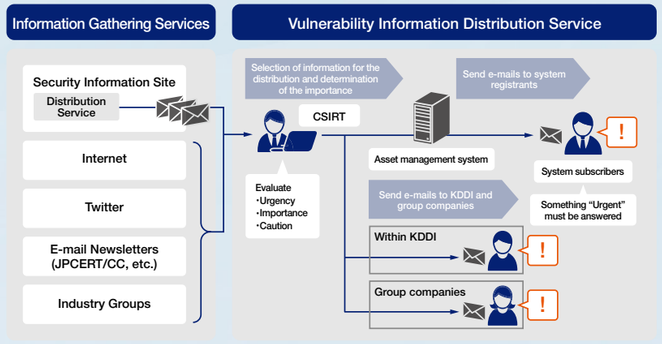
*1 KDDI Digital Security was established by LAC Co., Ltd., a leading company in the information security field, and KDDI. By combining KDDI's ICT solutions with LAC's advanced security analysis and technical capabilities, the company provides customers with comprehensive security solutions and work to strengthen security measures for the KDDI Group.



Cyberattack Countermeasures

CSIRT Activities <Vulnerability Information Collection and Distribution>

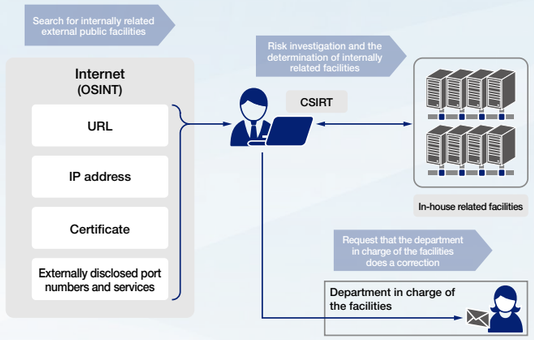
Vulnerability information obtained from security information sites, etc., is deployed company-wide by KDDI-CSIRT to confirm whether or not the system is affected. If there is an impact, we have KDDI-CSIRT report the results and work together to address the issue. In addition, we have built an asset management system that centrally manages the configuration information of all systems, automatically determines the systems to be corrected, and distributes the vulnerability information directly to the relevant system construction/operation staff.



External Attack Surface Investigation and Corrective Action

As corporate IT assets are expanding year by year, the number of areas targeted by attackers (attack surfaces) is also increasing. In particular, the number of externally exposed devices supporting Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) to connect to the corporate network environment from the home has increased rapidly in recent years, in line with the increase in remote work. Attackers attempt to break into a company's internal network by exploiting poorly managed, externally exposed equipment.

KDDI-CSIRT reduces the risk of attacks from entities who exploit external public devices by utilizing OSINT (Open Source Intelligence), i.e., information available on the Internet such as URLs and certificates, is used to search for internal equipment that is open to the public. This allows us to assess the risk of attacks against our facilities as well as the state of management, such as whether services or content that can be abused by attackers have been mistakenly disclosed, and promptly take corrective action to prevent attackers from abusing externally disclosed equipment.



Security Screening for Business Equipment

KDDI strives to take appropriate security measures during equipment procurement to ensure the safe provision of services to customers. In order to ensure a safe and reliable network, it is important to strengthen 5G security, and at the end of March of this year, the government established security guidelines for 5G SA systems, to which KDDI has responded by revising our internal regulations during periodic diagnoses and audits.

In addition to the security measures common to all general systems, the internal regulations also specify requirements for security measures specific to 5G SA systems. By conducting security audits based on the regulations, we confirm the implementation status of countermeasures against the risk of information leakage from inside and attacks from outside, and take corrective actions if a high risk is determined to exist.

KDDI will continue its efforts to provide secure services by regularly reviewing its internal regulations for equipment procurement and updating the necessary security measures.

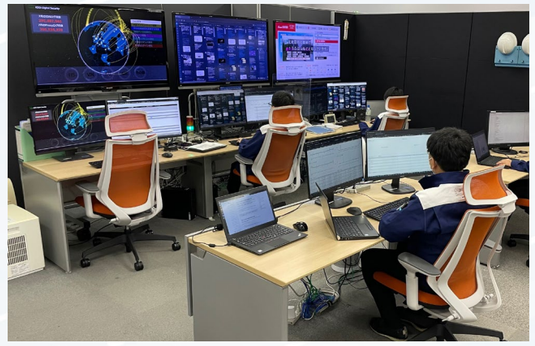
Security Monitoring

To protect the services and information we provide to our customers, our security analysts monitor unauthorized access and falsification 24 hours a day, 365 days a year, at KDDI's Security Operation Center (KDDI-SOC).

Professionally trained security analysts monitor and analyze the log from each security monitoring device to find signs of attacks in the vast number of logs.

If they discover dangerous incidents, such as unauthorized access or falsification, they promptly contact CSIRT and relevant departments within the company and instruct them to take action.

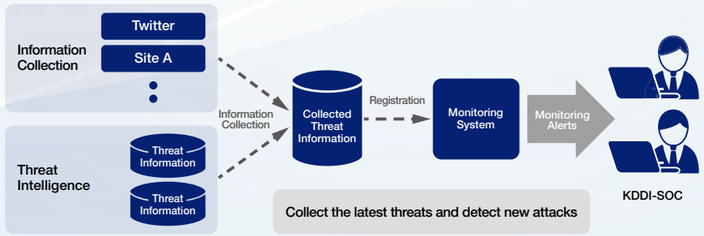
In recent years, there has been an increasing number of cases of unauthorized intrusion into office automation environments through targeted e-mails and other means to obtain important corporate information. KDDI has introduced SIEM/SOAR and EDRs to monitor and respond to suspicious activities. We also monitor daily for internal fraud, such as the unauthorized removal of information by employees, to protect our customers' services and information, as well as confidential internal information, from various security threats.



Continuous Threat Intelligence Collection

KDDI-SOC collects information on a daily basis in order to respond to the latest security threats. Information is collected from not only public information sources such as Twitter, but also threat intelligence information.

Information collected that may be useful for security monitoring is registered in the monitoring system and is collected on an ongoing basis so that the latest threats can also be detected.

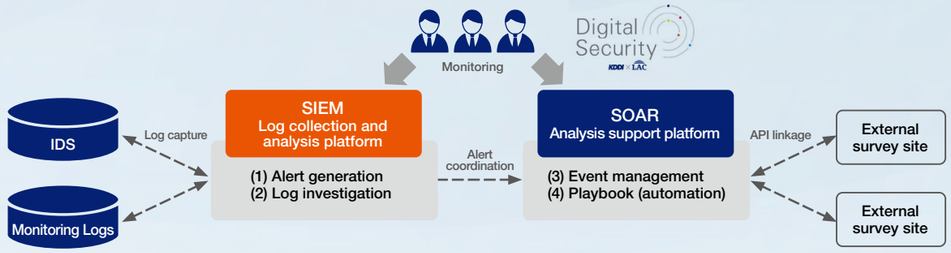


Technology Development to Support Advanced Security Monitoring

To protect its business and corporate networks from cyber threats, KDDI Group is applying cutting-edge technologies to further advance its security monitoring systems.

Using a cybersecurity analysis support platform that applies monitoring equipment and systems such as SIEM, SOAR, and IDS, we efficiently analyze huge amounts of logs and conduct high-quality security monitoring by combining the judgment of highly skilled monitoring personnel with the automation of the monitoring process.

The cybersecurity analysis support platform collects and analyzes security events collected by SIEMs, which are deployed not only at KDDI (non-consolidated) but also at KDDI Group companies around the world to ensure the security of KDDI Group worldwide.



DDoS Countermeasures

We also develop and operate systems to deal with DDoS attacks.

When an attack is detected, we automatically respond according to predetermined rules, and if necessary, the SOC and the operation and monitoring department of our telecommunication facilities work together to respond.

This protects KDDI's telecommunication network and enables us to provide stable telecommunication services.

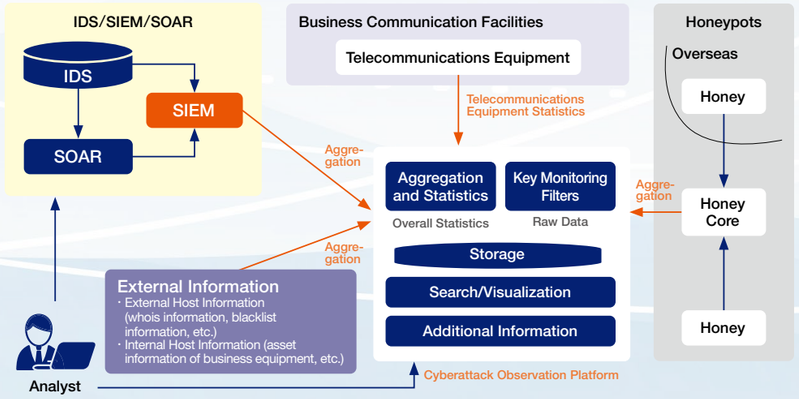
Development of a Security Upgrading System

Cyberattacks are becoming more organized, complex, sophisticated, and faster. To respond to such cyberattacks, we research, analyze, and evaluate cutting-edge technologies and industry trends, incorporate technologies that can be applied at KDDI, and develop systems for use in security operations.

Example of a Security Operation System Developed by KDDI Group

- **Observation system for attack communication through KDDI's communication network**

This system is designed to understand attack trends, visualize behavior that indicates signs of an attack, and proactively take countermeasures. Information from a wide variety of monitoring devices installed in the KDDI commercial network is aggregated, sampled, and correlatively analyzed to understand and predict attacks across the entire KDDI network.



Measures to Protect Personal Information

In order to further ensure that we properly handle customer information, KDDI has established an internal body dedicated to this purpose, has a third party assess our handling of the information, offers the privacy management functions by customers, has adopted a privacy impact assessment (PIA) conducted before a service is introduced, and takes other actions.

Upgrading Internal Systems

KDDI has established the Data Governance Office as the organization that is responsible for upgrading and operating the utilization of personal data. KDDI has also established the Data Governance Board, chaired by the President and Representative Director, as the decision-making body for privacy and data governance, and has built a system to review and approve privacy protection and other initiatives.

Organization	Data Governance Office
	Secretariat
An approval and deliberative body	Data Governance Board (Chairperson: President and Representative Director)
Role	● Planning of medium- to long-term strategies for data use ● Planning data governance strategies and implementing measures ● Responding to domestic and international privacy legislation ● Privacy governance internal penetration activities

Conducting Third-Party Assessments

We receive third-party opinions on whether KDDI is handling data appropriately with regard to our data utilization efforts. Based on these opinions, KDDI has established an advisory board consisting of experts in various fields in order to further promote the improvement of customer experience and achieve continuous development of society.

The contents of the Advisory Board's discussions are also available on the Privacy Portal*1.

Reference: (Advisory Board Members as of September 5, 2022)

Akira Morita	Representative Director [Chairperson] The General Incorporated Association Next Generation Fundamental Policy Research Institute
Toshiko Sawada	Chairperson The General Incorporated Association EC Network
George Shishido	Professor Graduate Schools for Law and Politics, The University of Tokyo
Harumi Shinohara	CP Design Consulting Co.,Ltd./Public Interest Incorporated Association Nippon Association of Consumer Specialists
Ryoji Mori	Lawyer Cyber Law Japan Eichi Offices

*1 https://www.kddi.com/corporate/kddi/public/privacy-portal/advisory-board/ (Japanese site only)

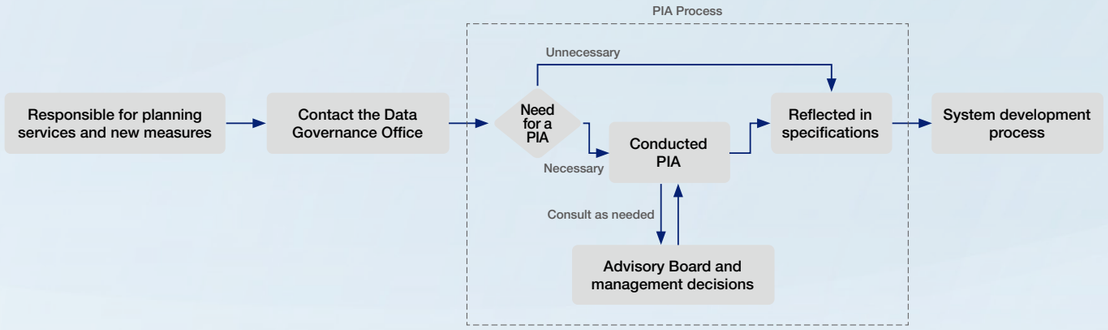
Offering Customers Privacy Management Capabilities

We offer the aforementioned "Privacy Portal," which provides customers with a more comprehensive and easier access functionality of how their personal information is handled.

Measures to Protect Personal Information

Privacy Impact Assessment (PIA)

PIAs are incorporated into the business process, and workflow is implemented so that risk assessment can be conducted when planning and reviewing new services.



Initiatives to Develop and Utilize AI Safely and Securely

To further enhance the value of the customer experience and contribute to the sustainable development of society through the use of artificial intelligence (AI), KDDI, in cooperation with the KDDI Research, Inc., formulated the "AI R&D and Utilization Principles for KDDI Group*1" on August 30, 2021, as part of "KDDI Accelerate 5.0." Based on these principles, the KDDI Group will promote the research, development, and utilization of AI so that customers can use our services safely through internal awareness-raising initiatives.

*1 AI R&D and Utilization Principles for KDDI Group (https://www.kddi.com/english/corporate/kddi/public/ai_principles/)

Countermeasures Against Unauthorized Use of Services

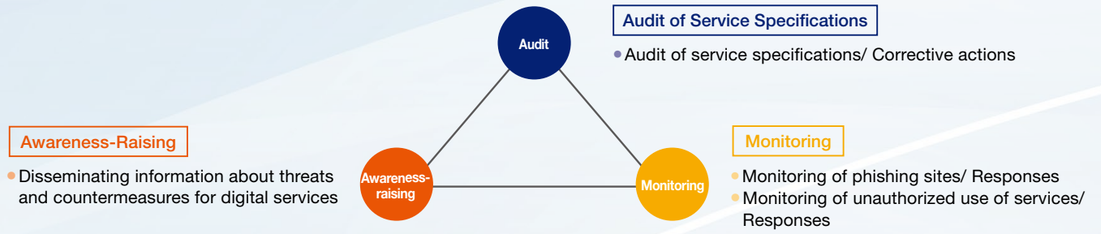
SSIRT Efforts

Service Security Incident Readiness & response Team (SSIRT) is an organization whose necessity is being discussed by the National center of Incident readiness and Strategy for Cybersecurity(NISC) as a system to respond to new threats generated by the digitization of services. KDDI was one of the first to adopt it, forming KDDI-SSIRT in 2018.

In recent years, while the spread of smartphone payment services has made our lives more convenient, criminals intent on stealing money have been impersonating legitimate users to take advantage of opportunities to commit fraud.

If the damage caused by such fraud is due to inadequacies in the service specifications of the operator, there is a risk that the service may be forced to terminate.

SSIRTs with specialized knowledge are working on countermeasures to these new risks as a digital service provider. In this chapter, we will introduce the measures that SSIRT is working on in the three measures of "audit of service specifications," "monitoring," and "awareness-raising."



Audit of Service Specifications

When KDDI-SSIRT provides a new service or adds or changes a function, SSIRT audits the service specifications in advance. Through these audits, we identify service specification inadequacies and potential for abuse, and work to correct specifications and reduce the risk of abuse so that customers can use KDDI services safely and securely.

Monitoring

Monitoring of Phishing Sites

In the past few years, with the intent to commit fraud, there has been a rapid increase in the number of phishing frauds in which fraudsters steal customers' passwords and personal information by sending e-mails and SMSs that appear to be from a real company or KDDI and guiding customers to fake websites that look exactly like the real websites.

Our measures against such phishing frauds include not only our previous anti-spam measures, but also efforts to monitor the occurrence of phishing sites. We are working with relevant agencies to deal with the phishing sites we discover and stop our customers from becoming the victims of phishing.

Monitoring of Unauthorized Use of Services

SSIRT has a round-the-clock surveillance system to deal with fraudulent activities to identify any unauthorized activities that take over authorized user accounts through phishing frauds and other means. We are further strengthening our efforts to prevent customers from being victimized.

Awareness-Raising

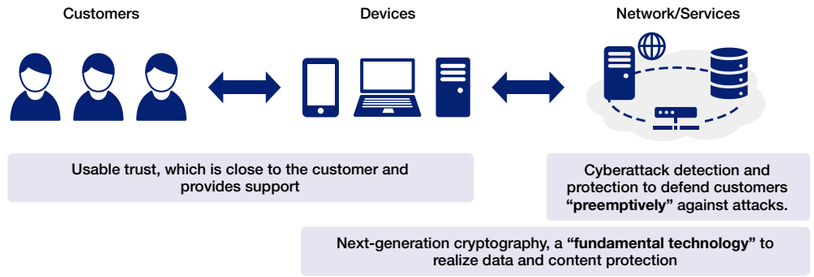
KDDI posts phishing frauds and other criminal techniques on the KDDI website and provides information on matters that customers should be aware of and effective countermeasures when using digital services. We also support the purpose of the annual "CYBER BOUSAI" event, in which multiple Internet companies and others across different industries cooperate to raise awareness of fraud among customers, and participate in this event every year. We will continue our efforts to disseminate easy-to-understand information in the hope of making as many customers as possible aware of the threats posed by digital services and the countermeasures to these threats.

Promotion of Research and Development

Research and Development at KDDI Research, Inc.

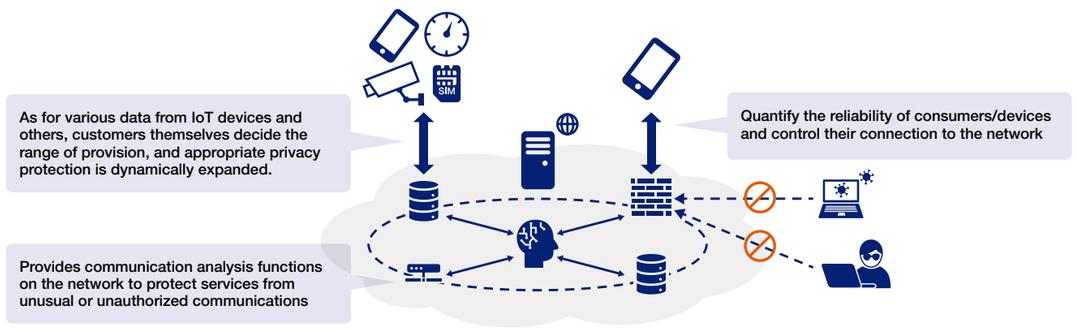
KDDI is studying to realize the optimal countermeasures to all kinds of service threats using telecommunications for the B5G/6G era. The following figure shows the research and development initiatives of the Security Division of KDDI Research, Inc. Usable trust technologies include security countermeasures based on human psychology and behavioral analysis, as well as privacy protection technologies that consider customer preferences. Cyberattack detection and protection enables AI to efficiently analyze big security data to realize proactive countermeasures that anticipate attacks. As next-generation cryptography, we will study symmetric cryptography for ultra-high speed and large capacity for the B5G/6G era and post-quantum cryptography for the quantum computing era.

Research and development at the Security Division of KDDI Research, Inc.



The following initiatives are being promoted as technologies to enhance network reliability. First, unauthorized users are prevented from entering the network by quantifying the trust level of service users and devices and controlling network connections based on trust relationships among users and devices. Second, advanced traffic analysis technology is used to accurately detect abnormal or unauthorized communications and control these appropriately, including through blocking, even for new types of devices. Additionally, to ensure the reliability of the devices that make up the network, we are conducting demonstration experiments on an infrastructure for multilayer interoperability that enables hardware verification in the supply chain and the sharing of verification results. Also, technology that allows customers to control the use of their data is an important function to protect their privacy, and from a privacy-by-design perspective, it should be used on telecommunications network as a common function. By making this control available as a default function in telecommunications network, each service can apply appropriate privacy protection measures based on a customer's consent and privacy preferences, thereby ensuring appropriate data usage. As shown in the figure below, we aim to provide a wider range of unified security and privacy measures by making these technologies seamlessly applicable to various services on our telecommunications network.

Security Infrastructure That Has Security and Privacy Functions Inside



We are also conducting research and development of AI-based attack detection and defense technologies. In the WarpDrive project, which aims to advance web security measures technology, a large amount of web access information was collected and accumulated, and eight domestic security research organizations collaborated to build and operate an infrastructure for analysis and research, producing several promising results. We will continue to simultaneously accumulate and collaborate security big data and promote research and development of AI-based cybersecurity measures in B5G/6G. Additionally, we will use AI to validate the security of many hardware and software products efficiently.

On the other hand, we also work on countermeasures to attacks on AI as a critical issue to ensure that AI does not bring new vulnerabilities. Attacks against AI have rapidly become more sophisticated in recent years, and methods to create malware that cleverly mislead AI's judgment have appeared. As the use and application of AI progress, threats from attacks are anticipated to become more apparent. We will continue to promote research and development on measures against such technologies. Furthermore, to effectively use AI, we are also improving next-generation homomorphic encryption with sophisticated and high-speed functions that can be used for integrated analysis.

Security Evaluation of Post-Quantum Cryptography

We are also studying next-generation cryptography for the B5G/6G era.

Asymmetric cryptography is the fundamental technology that supports secure telecommunications systems and is used in everyday life, such as online shopping and smart cards. However, large-scale quantum computers are anticipated to improve the efficiency of cryptanalysis significantly. We thus require post-quantum cryptography, a public-key cryptography that protects against cryptanalysis attacks using quantum computers. Post-quantum cryptography is currently being selected by the National Institute of Standards and Technology, United States (NIST-PQC competition).

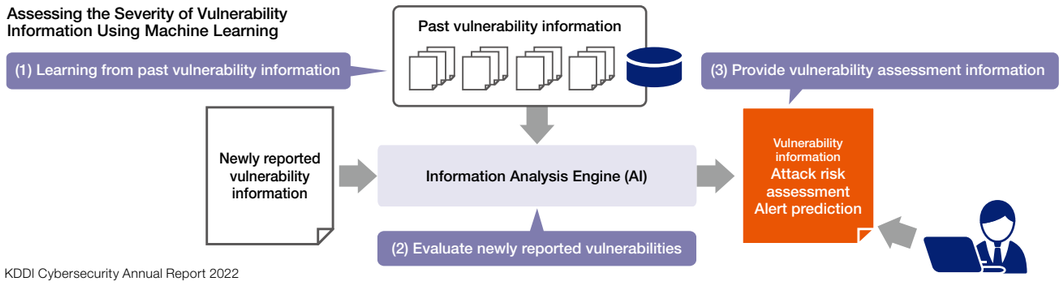
In February 2022, KDDI became the first company in the world to solve a 550-dimensional Syndrome Decoding problem (hereinafter referred to as the SDP) in a worldwide cryptanalysis competition, "decodingchallenge.org." The SDP is the security basis of code-based cryptography, including Classic McEliece, which was selected as a fourth-round candidate for the NIST-PQC completion. We need to clarify the limit of the solvable dimension of code-based cryptography to select the secure key size of the cryptography as post-quantum cryptography. The 550-dimensional SDP is the most challenging problem among those solved throughout the competition. We optimized the process and data structure of the solving algorithm and implemented multi-threaded and multi-core parallelization with approximately 3 million threads per GPU. As a result, the GPU-parallelized algorithms achieved 226 times faster than the original algorithm and solved the 550-dimensional SDP in 13 days.

Promotion of Research and Development

Vulnerability Response Support

Many cyberattacks are carried out by exploiting the system vulnerabilities caused by software bugs, etc. Failure to take action, such as by applying patches to newly discovered vulnerabilities, may lead to serious cyber damage. However, about 20,000 vulnerabilities are discovered each year. Even if we focus on "urgent" vulnerabilities indicated by Common Vulnerability Scoring System (CVSS), which measures severity of the vulnerability on a scale of 0 to 10 and score of 9 or higher corresponds to "urgent", over 2,000 vulnerabilities are discovered annually. This makes it difficult to collect detailed information on vulnerabilities that are discovered one after another, understand their content and impact, and take appropriate countermeasures. Therefore, KDDI has been conducting research to automate the collection and analysis of vulnerability-related information. Using the analysis system, called Vuldate, developed as a result of this research, since June 2022, KDDI has been providing information to member companies of ICT-ISAC Japan, an organization established to share and analyze cybersecurity-related information for businesses in the information and communications field. The flow of Vuldate's operation is shown in Figures (1) through (3). First, an analysis model is built using past vulnerability information as training data, which is then imported into the AI information analysis engine (1). When a new vulnerability is reported, AI provides vulnerability assessment information on "attack risk assessment," which indicates the likelihood of an attack code being created to exploit the vulnerability, and an "alert prediction," which indicates whether the vulnerability is subject to alert. AI also automatically collects and organizes information related to the vulnerability from Internet news sites and SNS sites to support information system staff in making vulnerability response decisions, as described in (2) and (3). Improving security by promptly responding to vulnerabilities is an issue that must be addressed by society as a whole, and KDDI is contributing to the realization of a safe and secure information-based society by providing Vuldate to the ICT-ISAC.

Assessing the Severity of Vulnerability Information Using Machine Learning



Usable Security That Is Close to Customers and Achieves Precise Countermeasures

KDDI also focuses on customer behavior as an important measure point to prevent security incidents and damage. Even if a system can prevent security incidents when it functions as expected at the time of design, accidents and damage can still occur if the configuration and usage procedures are incorrect. From a security perspective, the ability to properly use a system depends on multiple factors, including the literacy of the customer and the circumstances under which the system is used. In these complex situations, efforts to provide warnings and uniform procedures for proper use have limited ability to prevent accidents.

Therefore, we are researching security technologies that are tailored to the customers who use our services to realize the safe use of systems without any stresses and depending on the literacy of the customer and the situations in which they use the systems. Specifically, we are working on "understanding customers" and "mechanisms to trigger appropriate security measures."

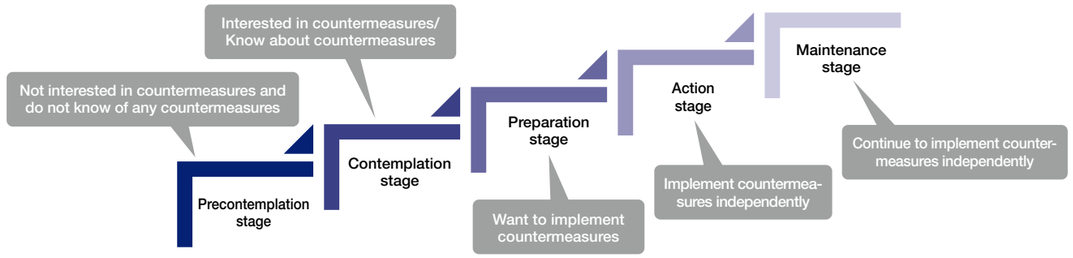
One example of our research on "understanding customers" is the Security Behavior Stage Model shown in the figure below. This model defines five stages of security behavior from the "Precontemplation stage" to the "maintenance stage." These stages are based on the behavioral change stages used in the health field and the differences in customer attitudes, such as interest in security measures and the status of usual measures. The results of this research will make it possible to accurately identify and classify the status of customers and contribute to research to elucidate the factors that will improve their attitudes toward security measures (i.e., make customer attitudes move in the upper right direction in the figure as a highly desirable state). Additionally, we are also engaged in research to establish a psychological scale to accurately estimate whether appropriate security measures are being taken using a limited number of questions. The results have been accepted for publication at the high-level international conference, SOUPS 2022*1.

Concerning research on "mechanisms to trigger appropriate security measures," we aim to develop practical means to effectively alert customers to security measures and risk avoidance and encourage them to comply with these measures according to their circumstances as determined through the research results mentioned above. So far, we have verified the effectiveness of technology to optimize the wording of update notifications, screen design, and the timing of notifications for PC OS updates.

Through such research, we aim to generate technology that realizes precise security measures with less burden on customers and along with their sense of satisfaction.

*1 https://www.usenix.org/conference/soups2022/presentation/sawaya-poster

Security Behavior Stage Model



Security Solutions for Corporate Customers

Managed Zero Trust

What Is Zero Trust Security?

The "Zero Trust" concept of secure information system design has been attracting significant attention in tandem with the penetration and establishment of telework. It is no longer unusual for teleworkers to bring home laptops or other devices loaned by the company and connect to the company network via a public Internet connection. The use of cloud computing is expanding at an accelerating pace, and the traditional "perimeter-type defenses" to ensure cybersecurity is no longer viable for business and operations. In other words, it is no longer acceptable to take security measures on both internal and external boundaries and utilize information assets only within the boundaries, under the assumption that the internal network is kept secure. Zero Trust is a concept that maintains security by verifying every instance of access both inside and outside the company network. It is attracting attention as an ideal next-generation security concept.

Flexible "Workstyle" and Decentralized "Places of Work"

What Is KDDI's Proposal for "Managed Zero Trust"?

KDDI offers a variety of products and services for each of the six components required to realize Zero Trust, operations, cloud applications, security, IDs, networks, and devices, and combines these in the optimal manner to provide one-stop support for safe, secure, and diverse workstyles.

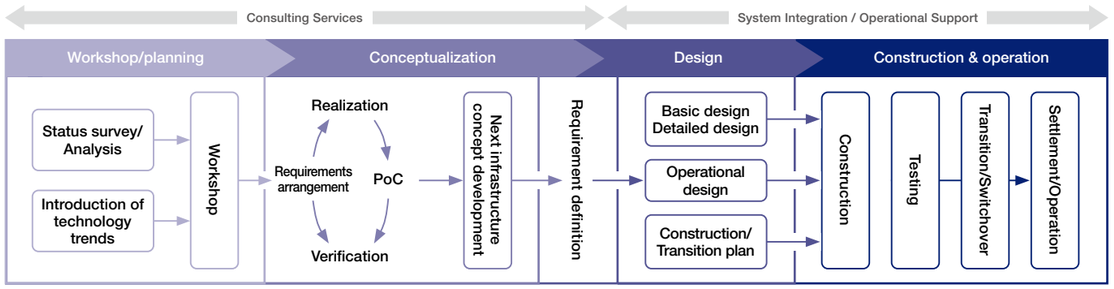
The Six Components of Managed Zero Trust

Security Assessment

We provide security assessments and vulnerability assessments and penetration testing to visualize security issues and risks and support the formulation of countermeasure plans for improvement. To address such concerns as difficulty in gathering and sorting information and uncertainty about where to start when establishing a Zero Trust, the "Zero Trust Maturity Assessment" visualizes the status of Zero Trust measures and provides a quantitative evaluation of measure priority and effectiveness in a short period (about one month) and at no cost.

Consulting Services

Implementing Zero Trust is a review of the entire IT infrastructure environment. We offer a list of consulting services to support the formulation of specific concepts in a step-by-step manner. We support the formulation of specific concepts with an eye toward our customers' goals.



One-Stop Support for Post-Introduction Operations

KDDI provides total support for post-implementation burdens, including inquiries from employees, tuning to cloud updates, and security operations.

Supporting administrative operations with customer business support

Contents of Support
- Help desk outsourcing (Centralized receipt of all types of inquiries from end-users)
- Account and device management
- Configuration work on behalf of the client

System and service operations to support operational stability and efficiency

Contents of Support
- Service desk (Centralized receipt of service delivered by administrators)
- System and service monitoring
- Failure notification and responses to emergency recovery
- Visualization and reporting
- Configuration work on behalf of the customer (Policy and parameter settings, various console operations on behalf of the administrator)

Security operations support and threat prevention

Contents of Support
- Log monitoring and risk analysis
- Securiy improvements
- Security notification
- Incident response (Quarantine, blocking, reporting of specific devices and accounts)

Third-Party Evaluation and Certification

KDDI Security Solutions by LAC

LAC (LAC Co., Ltd.) provides services to solve a variety of social and business issues with its extensive experience in system integration, cybersecurity, and the latest technologies. Since its inception, the company has been involved in the development of fundamental systems that support Japanese society, including the financial and manufacturing industries. In the more than 25 years since the launch of Japan's first information security service, the LAC has continued to grow as a leading company in the information security field, remaining at the forefront of the latest cyberattack countermeasures and incident response measures, including the use of Security Operation Center (JSOC), which is one of the largest such facilities in Japan, cyber emergency centers, vulnerability assessments, penetration testing, and IoT security.

The "KDDI Security Solution by LAC" integrates the know-how of KDDI and LAC, a top-class company in information security, to provide a full range of security solutions through consulting, security diagnosis, and security monitoring and operation.

ISMS Certification Status

The KDDI Group is actively involved in third-party evaluations and certifications related to information security.

The major companies that contain organizations that have acquired the Information Security Management System Global Standard ISMS (ISO/IEC27001) certification*1 are as follows.

Group Companies with ISMS Certified Organizations

KDDI Corporation

Mobile communication market

OKINAWA CELLULAR TELEPHONE COMPANY

SORACOM, INC.

Fixed-Line Telecommunications Business

Chubu Telecommunications Co., Inc.

Internet-related Business

BIGLOBE Inc.

Content & Media Business

mediba Inc.

Research & Cutting-edge Technology Development

KDDI Research, Inc.

Network Construction, Operation and Maintenance

KDDI Engineering Corporation

Japan Telecommunication Engineering Service Co., Ltd.*2

Contact Center and IT Solution Business

KDDI Evolva Inc.

Sales & Marketing

KDDI MATOMETE OFFICE CORPORATION*2

KDDI MATOMETE OFFICE KANSAI CORPORATION*2

KDDI MATOMETE OFFICE CHUBU CORPORATION*2

KDDI MATOMETE OFFICE NISHINIHON CORPORATION*2

KDDI MATOMETE OFFICE HIGASHINIHON CORPORATION*2

DX-related business

iret Inc.

KDDI Web Communications Inc.

KDDI's Directly Operated stores

KDDI PRECEDE CORPORATION

Special Subsidiary

KDDI Challenged Corporation*2

Other

KDDI Group Foundation*2

KDDI Pension Fund*2

KDDI Health Insurance Society*2

*1 ISMS certification (ISO/IEC 27001: 2013) : A third-party conformity assessment scheme for information security. It was established with the goal of contributing to widespread improvements in information security and encouraging companies to target levels of information security that can be trusted around the world.
*2 Included in the applicable scope of ISMS certification for KDDI Corporation.

KDDI Group Overview

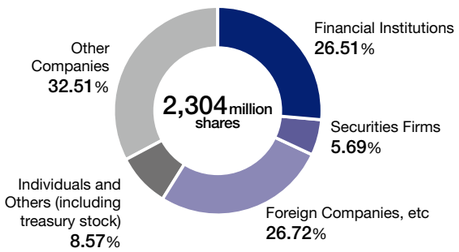
Corporate Overview (As of March 31, 2022)

Company Name	**KDDI CORPORATION**
Date of Establishment	**June 1, 1984 (The KDDI CORPORATION was established in October 2000 through the merger of DDI CORPORATION, KDD Corporation, and IDO CORPORATION.)**
Business Objective	**Telecommunications business**
Head Office	**Garden Air Tower, 10-10, Iidabashi 3-chome, Chiyoda-ku, Tokyo 102-8460, Japan**
Registered Place of Business	**3-2, Nishi-Shinjuku 2-chome, Shinjuku-ku, Tokyo 163-8003, Japan**
President	**Makoto Takahashi**
Capital	**¥141,852 million**
Number of Employees	**48,829 (consolidated)**

Stock Information (As of March 31, 2022)

SE Code	**9433**
Number of Shares Authorized	**4,200,000,000 shares**
Number of Shares Issued and Outstanding	**2,304,179,550 shares**
Number of Shareholders	**341,622 shareholders**

Breakdown of Shareholding by Investor Type



Major Shareholders

Name of Corporate Entity	Number of Shares Held	Ratio of Voting*1 (%)	Shareholding Ratio*2 (%)
The Master Trust Bank of Japan, Ltd. (Trust Account)	357,949,400	16.13	15.53
KYOCERA Corporation	335,096,000	15.10	14.54
Toyota Motor Corporation	316,794,400	14.28	13.74
Custody Bank of Japan, Ltd. (Trust Account)	130,021,300	5.86	5.64
STATE STREET BANK WEST CLIENT - TREATY 505234	31,085,775	1.40	1.34
Barclays Securities Japan Limited	28,453,600	1.28	1.23
Mitsubishi UFJ Morgan Stanley Securities Co., Ltd.	24,555,562	1.11	1.06
JPMorgan Securities Japan Co., Ltd.	23,590,296	1.06	1.02
STATE STREET BANK AND TRUST COMPANY 505103	22,595,124	1.02	0.98
JP MORGAN CHASE BANK 385781	21,868,304	0.99	0.94

*1 The ratio of voting is calculated excluding treasury stock (85,058,340 shares as of March 31, 2022). In addition, the Company's shares held by the Executive Remuneration BIP Trust Account, and the Stock Grant ESOP Trust Account (3,920,592 shares as of March 31, 2022) are included in the number of shares with voting rights, but the Company does not exercise its voting rights on these shares. The ratio of voting is calculated by rounding off to the second decimal place.
*2 Shareholding ratio is calculated after rounding down to the second decimal place.

KDDI CORPORATION
https://www.kddi.com/english/