Tomorrow, Together

KDDI

おもしろいほうの未来へ。

au

Cybersecurity Annual Report 2023

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 2023.

Referenced Documents

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

Website

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

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/

Message from the Information Security Chairperson

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. However, accompanying this, the risks associated with information security and privacy have grown increasingly complex and diverse. Cyberattacks and other criminal activities in cyberspace by threat actor groups are increasing and getting more and more sophisticated every day.

In 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 working on the introduction of automated AI-driven technologies for analyzing and monitoring cyberattacks. In addition, 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.

Furthermore, the KDDI Group is actively engaged in the development and utilization of AI. Specifically, there’s a company-wide initiative to promote the use of Generative AI across various divisions. On the other hand, since the utilization of AI covers a wide variety of fields, we have established guidelines and other measures, taking into account that the benefits and risks posed by AI are different in each field.

KDDI will continue to evolve responses to increasingly complex and sophisticated emerging threats to ensure ethics, social acceptance, safety, and reliability. This commitment allows us to provide services that users can rely on. This report introduces KDDI’s security initiatives. We appreciate your interest and time in reading through this report.

Senior Managing Executive Officer, Director, CTO and Executive Director, Chairperson of the information Security Committee

Kazuyuki Yoshimura

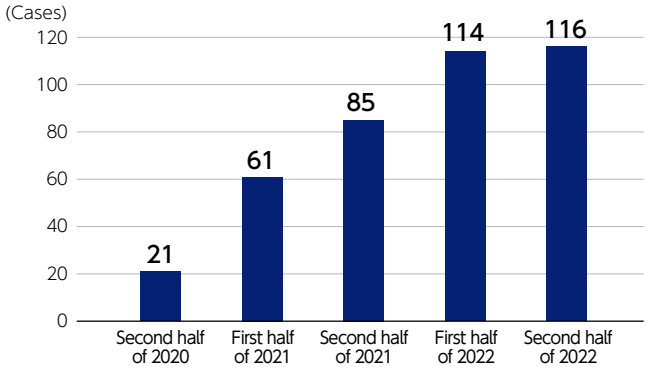
Apr. 2023	CTO (Current position)
Jun. 2022	Senior Managing Executive Officer, Director (Current position)
Apr. 2021	Managing Executive Officer, Director
Jun. 2020	Executive Officer, Director
Apr. 2020	Executive Officer Executive Director, Technology Sector (Current position)

Cyberattacks/Cyberthreats Trends

1 Today's Cyberattacks

Damage from cyberattacks targeting companies and organizations continues unabated. The trend in the reported cases of ransomware damage announced by the National Police Agency shows that security incidents are on the rise year by year, as shown in the graph on the right. In recent years, attacks exploiting vulnerabilities across a wide range of products and utilizing methods that are difficult to detect by monitoring systems have increased. Attack methods have become more sophisticated and cunning. Furthermore, a business model has been established in which attackers are rewarded for carrying out cyberattacks on behalf of others. There are confirmed instances of attacker groups structured similarly to corporations, divided into multiple departments, indicating the commercialization of cyberattacks.

The Trend in Reported Cases of Ransomware Damage in Corporations and Organizations (Announced by the National Police Agency)

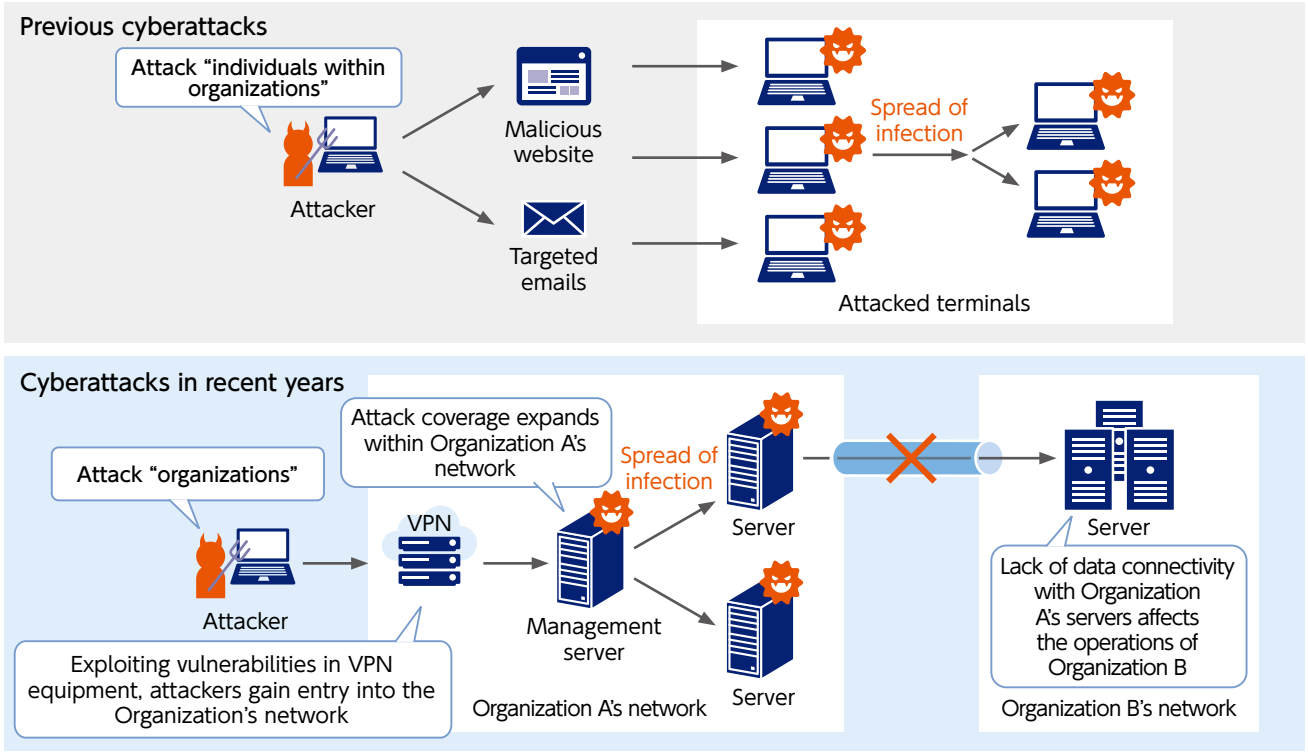


Source: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf (Japanese site only)

Cyberattacks targeting organizations have traditionally focused on attacking web services publicly available on the Internet or targeting individuals within organizations using email. However, in addition to this, attacks targeting Virtual Private Network (VPN) equipment and supply chain attacks, which infiltrate target organizations through less secure Group companies or business partners, are also on the rise. As a result, it can be said that the range of targets for cyberattacks is expanding.

The actions of attackers after intrusion vary, but encrypting data through ransomware infections and demanding money are particularly prevalent tactics. Incidents where business operations are suspended due to ransomware infections have been reported both domestically and internationally.

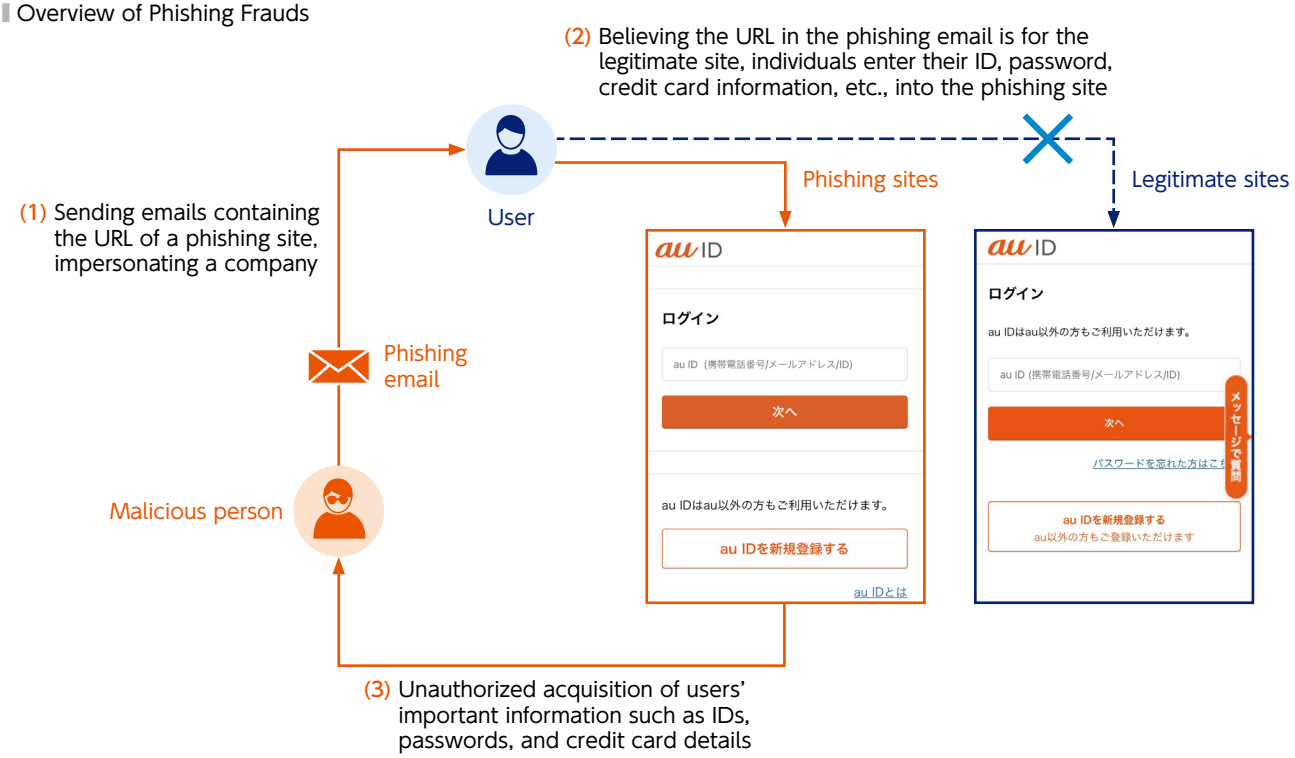
Changes in Cyberattacks



2 Unauthorized Use of Services

In addition to cyberattacks targeting companies and organizations, phishing frauds targeting individual customers have become a social issue and have been covered by various media. Attackers send emails or SMS messages disguised as real companies or well-known services, using methods to lure customers to fake websites, through which they steal personal information such as authentication credentials and credit card details. The methods using phishing sites have become increasingly sophisticated each year, making it difficult to determine the authenticity of emails or fake websites based solely on their appearance.

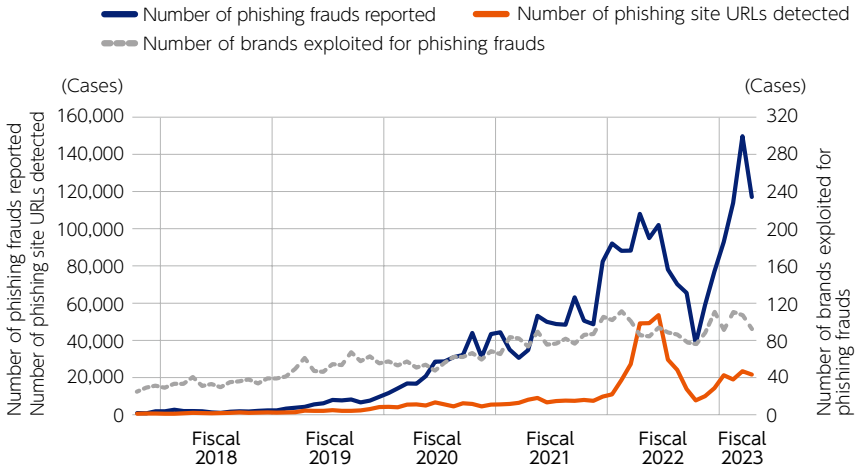
Overview of Phishing Frauds



Cyberattacks/Cyberthreats Trends

Furthermore, the trick of having malicious malware installed on smartphones to cause damage has also become commonplace. If customers fall for such tricks and have their personal information stolen or install malware, it ultimately results in financial losses. As specific examples of damage, authentication information for cashless payment services and Internet banking has been stolen, leading to unauthorized money transfers from customers' accounts or incidents of fraudulent use on e-commerce sites and gaming platforms. These damages may occur both in physical stores and online. According to announcements from the National Police Agency and industry groups, cases of fraudulent money transfers involving credit cards and Internet banking have surged in recent years. This is believed to be linked to the increasing prevalence of phishing frauds. As a result, there is a demand for strengthening measures against fraudulent activities, including phishing frauds, among businesses that provide digital services.

Number of Phishing Frauds in Japan



Source: Created by KDDI using data provided by Council of Anti-Phishing Japan

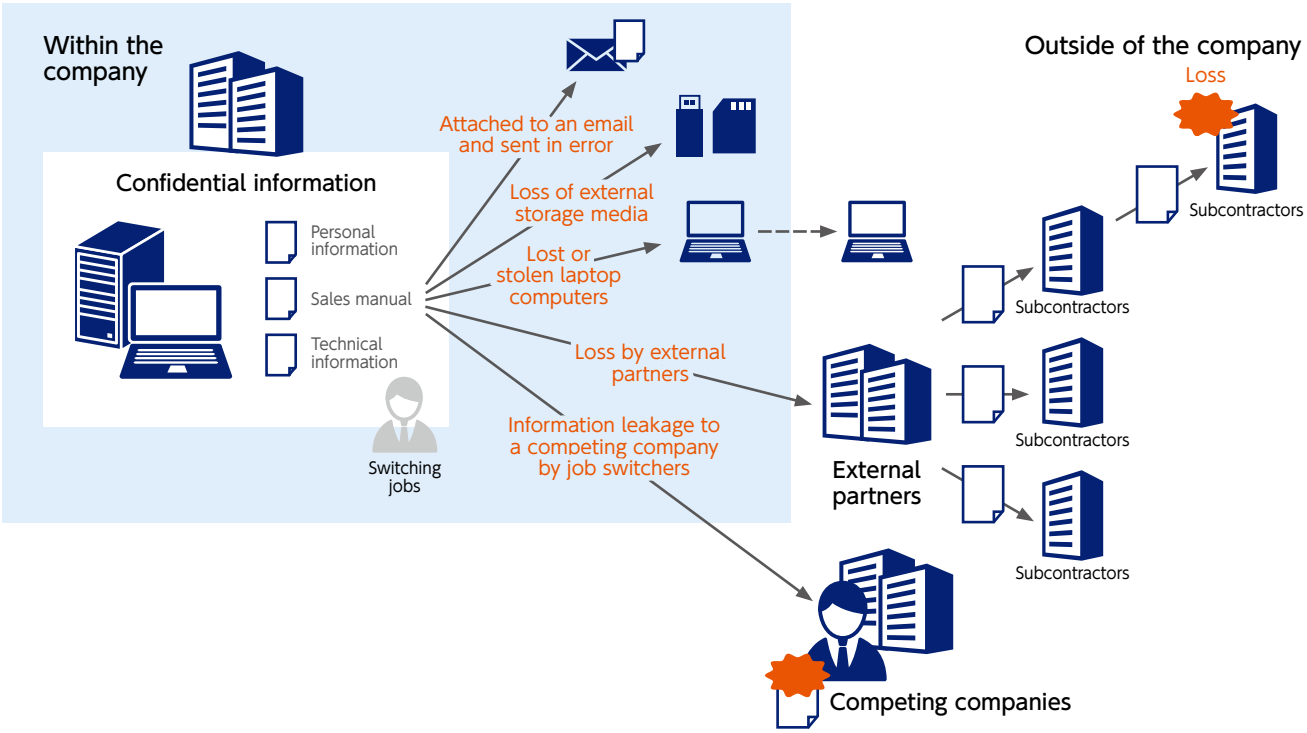
3 Personal Information Leaks

The risk of leakage of personal information held by companies is also increasing. This is due to changes in social structures, such as the progress of digitization and the widespread adoption of telework. In order to reduce initial investments and operating costs, the use of cloud services has become common in businesses. However, the risk of attackers targeting misconfigurations in cloud services, leading to the leakage of data to external parties, has also increased. Furthermore, the proliferation of telework has increased the risk as employees access the network from insecure environments. Additionally, there is a risk of information leakage from retirees due to increased workforce mobility, as well as cases of personal information loss by external partners and instances where employees of companies' external partners take customer information. These situations highlight lurking risks in various scenarios. According to the annual report for fiscal 2022 by the government's Personal Information Protection Commission JAPAN, the number of reported cases has surged from 1,042 in the previous fiscal year to 4,217*1, a nearly four-fold increase, partly because reporting of data breaches by businesses has become mandatory.

In addressing the urgent risk of information leakage for companies, the focus is not only on protecting against cyberattacks on their own systems but also on addressing internal information leaks and ensuring security measures throughout the entire supply chain, including external partners.

*1 Reference: Overview of the Annual Report for fiscal 2022 by the Personal Information Protection Commission JAPAN
https://www.ppc.go.jp/files/pdf/050609_annual_report_gaiyou.pdf (Japanese site only)

Patterns of Confidential Information Leaks

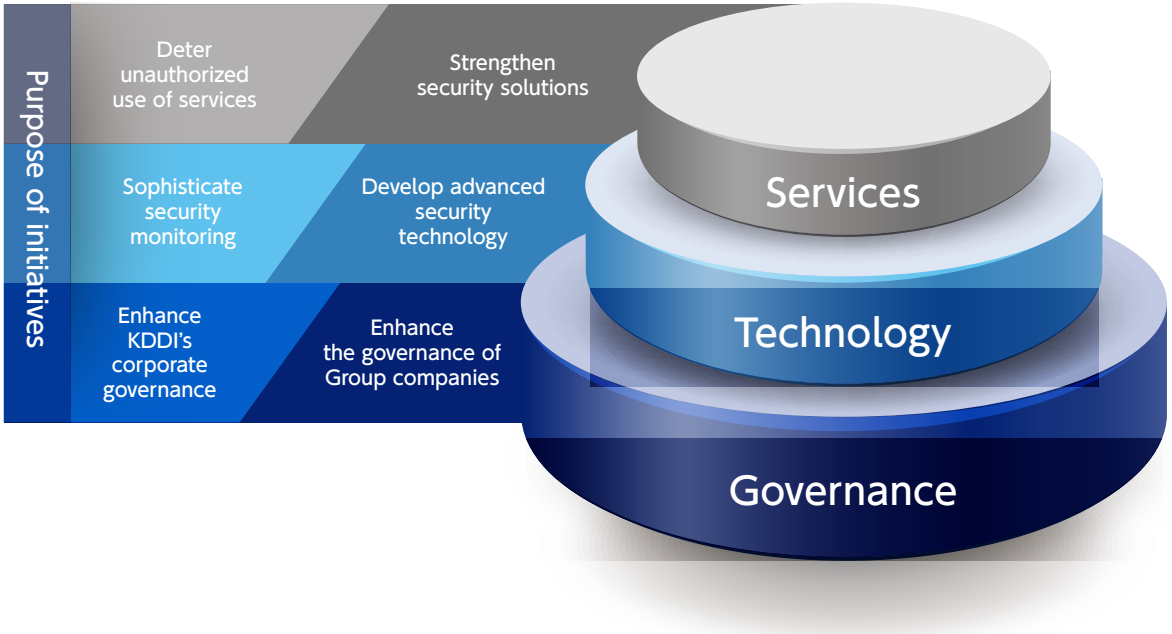


Initiatives for Cybersecurity

KDDI is an infrastructure company that supports the information foundation of society and plays a role that contributes to the public interest. Therefore, we strongly recognize our direct involvement in customers' lives and have set forth connecting "Lives," "Day-to-Day Lives," and "Hearts and Minds" as our mission. To achieve this mission, we are actively promoting initiatives aimed at providing safe and secure telecommunication services. On the other hand, with the recent development of the digital society, we also recognize the increasing global impact of evolved cyberattacks, leading to external leakage of highly confidential information and unauthorized use of services. These cyberattacks are now being recognized as significant risks, comparable to natural disasters and climate change. In this situation, it is an urgent issue for KDDI to enhance measures against new cyberattack methods to provide customers with safe and secure telecommunication services.

In response to the intensification of cybersecurity attacks, KDDI recognizes the need to further strengthen its commitment to cybersecurity. We are actively engaged in the initiatives placing emphasis on three perspectives: governance, technology, and services.

Three Perspectives in Initiatives for Cybersecurity



	Purpose	Initiatives
Governance	Enhance KDDI's corporate governance	Establishment of AI governance; digital transformation (DX) of ISMS operation
	Enhance the governance of Group companies	Strengthening security governance for Group companies
Technology	Sophisticate security monitoring	Visualization of cyberattack indicators; construction of a threat intelligence platform
	Develop advanced security technology	Detection of C&C servers through information analysis; consideration of the use of software component tables in the telecommunication field World's fastest processing of encryption; building an IoT security infrastructure with digital twin technology
Services	Deter unauthorized use of services	Improvement of phishing site detection accuracy; advanced detection of unauthorized use
	Strengthen security solutions	Initiatives in security business: Proposal and provision of managed trust; support for security measures

The emphasis on governance by companies brings numerous benefits, including the strengthening of risk management, ensuring compliance, and fulfilling social responsibilities. Therefore, KDDI aims to build a robust foundation for security governance, enhance governance across the KDDI Group, and earn trust from society.

Additionally, technological advancements are crucial to our security initiatives, playing a significant role in contributing to and supporting the enhancement of security. KDDI strives for the development of advanced security technology, laying the foundation for technology to enhance security and address ever-evolving threats.

The services provided by KDDI are utilized by many customers and have a significant impact on society. We consider protecting our services and maintaining security to be part of KDDI's social mission. To ensure that customers can use our services with confidence, we constantly refine our technology and expertise to address the latest threats. We also dedicate efforts to deter unauthorized use of our services. Furthermore, as a means to help customers address security-related issues, we also provide security solutions and consulting services.

KDDI considers security to be one of the top-priority issues to be addressed and aims to build a better future by promoting these initiatives to provide a safe and secure environment.

Information Security Governance

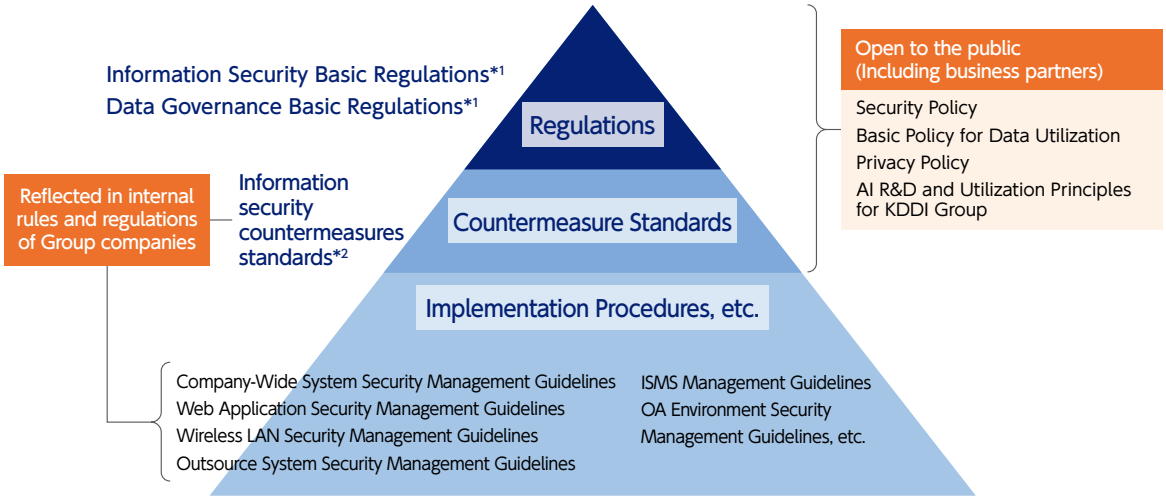
In response to increasingly sophisticated and skillful cyberattacks, the KDDI Group recognizes information security risk management as a critical issue and is working to strengthen information security governance.

In this chapter, we provide an overview of KDDI's initiatives to enhance information security governance, including policies on information security, the information security framework, the information security management cycle, information security audits, and information security education.

1 Policies on Information Security

KDDI's internal documents on information security policies 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 countermeasure standards to ensure compliance with those regulations, and the third level provides implementation procedures, etc. Especially in the regulations and countermeasure standards, we handle customer information and corporate confidential information strictly. Our goal is to gain the trust of customers and other stakeholders by consistently implementing appropriate protective measures. For this reason, we have established and adhere to externally published versions of a Security Policy and Privacy Policy.



*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.

Security Policy

KDDI acknowledges proper information management as a critical management issue and is committed to ensuring information security. Specifically, we are establishing the information security management framework, implementing information security measures, and developing internal regulations. These are part of the Security Policy, which establishes the basic policy for 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. The term "personal data" used here 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. Furthermore, based on this Basic Policy for Data Utilization, KDDI establishes the KDDI Privacy Policy*2 as guidelines for handling personal data.

*1 https://www.kddi.com/english/corporate/kddi/public/privacy-portal/
*2 https://www.kddi.com/english/corporate/kddi/public/privacy/

Information Security Governance

Governance of Generative AI

KDDI has established the "AI R&D and Utilization Principles for KDDI Group" to further enhance the value of customer experience and contribute to the sustainable development of society through the use of artificial intelligence (AI). In these principles, the KDDI Group establishes nine guidelines that AI developers and AI users within the KDDI Group should adhere to. The contents consider not only aspects of security and privacy but also ethical and societal acceptance, as well as the responsibilities as service providers. Moreover, we have established the "AI Development Guidelines" as a set of guidelines that define the measures required to realize AI service development based on these principles. We are also actively promoting risk assessment activities in accordance with these guidelines. At the KDDI Group, we will establish AI governance based on these principles, aiming to build a foundation for utilizing AI services. By doing so, we actively promote the integration of various AI technologies, including Generative AI, into internal business processes. Additionally, drawing on insights gained from these activities, we will work towards realizing AI research and development and safe and secure AI service provision for our customers.

- News Release on August 30, 2021: Establishment of the "AI R&D and Utilization Principles for KDDI Group"
  https://news.kddi.com/kddi/corporate/newsrelease/2021/08/30/5356.html (Japanese site only)
- News Release on May 25, 2023: 10,000 employees have started using "KDDI AI-Chat"
  https://news.kddi.com/kddi/corporate/newsrelease/2023/05/25/6741.html (Japanese site only)

Path to Introducing Generative AI
Discussion with project managers in charge of Generative AI introduction

Security Management Department,
Information Security Division
Hirokazu Sasaki

Smart Office System Department,
Information Systems Division
Tatsunori Hirano

What motivated you to engage in the establishment of Generative AI governance, and what challenges did you overcome before implementation?

Sasaki: The Information Systems Division, involved in improving KDDI employees' productivity and enhancing the internal environment, is considered the "offensive" domain. On the other hand, the establishment of security governance in my role is likened to the "defensive" domain. While the "offensive" and the "defensive" are inherently opposing domains, both share a common understanding that "Generative AI has a significant impact on business, giving rise to business transformation." As a result, we were able to promptly advance the establishment of Generative AI governance.

Hirano: KDDI started exploring services that utilize Generative AI for internal use. However, due to risks like information leakage and copyright issues, I realized that considering them solely within the Information Systems Division would be challenging. To achieve this, we collaborated with the Information Security Division and engaged in discussions concerning anticipated risks and corresponding countermeasures. I believe that by establishing usage rules and implementing the deployment of awareness-raising content for internal users, we have been able to launch the service while ensuring both safety and security.

Sasaki: Among KDDI employees, there are not only those who use Generative AI as end-users but also individuals who engage in advanced usage, such as incorporating it into their own services for provision. To help these individuals understand the risks of Generative AI and ensure its correct usage, our awareness-raising content have incorporated matters to be considered based on their respective standpoints.

Please share any measures or prospects that should be implemented in the future in tandem with the development of Generative AI.

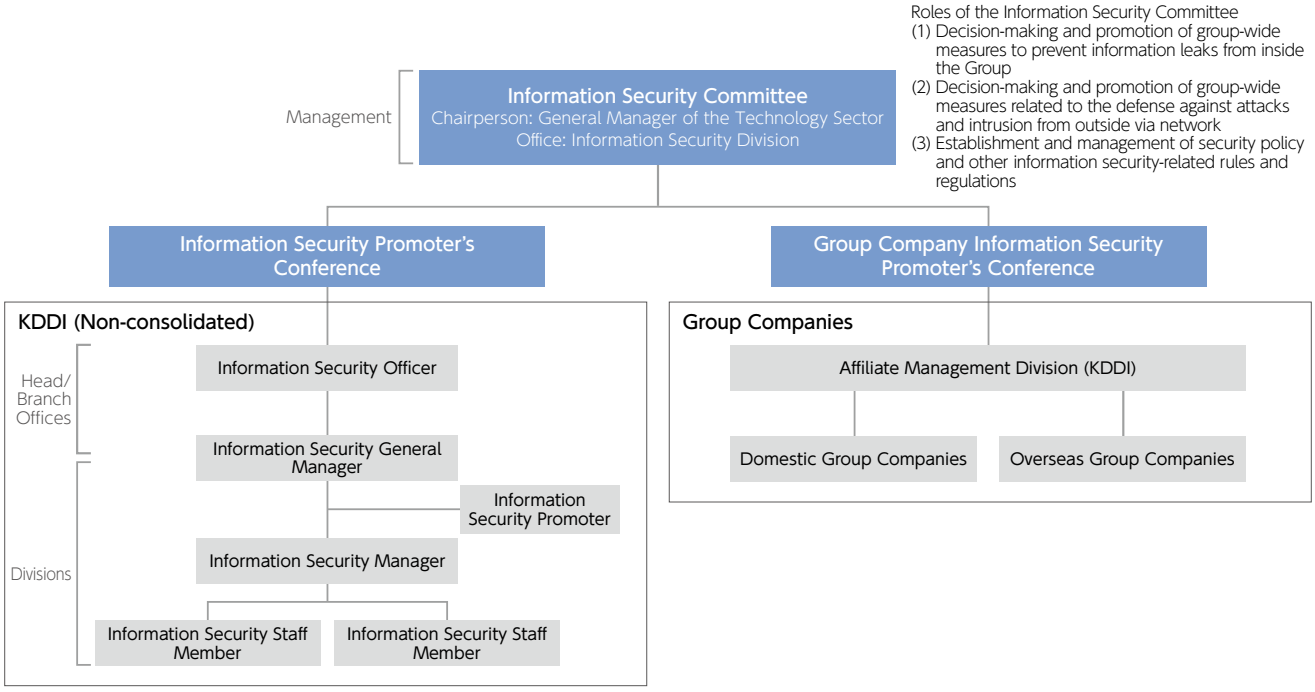
Hirano: I believe that Generative AI can significantly contribute to improving business productivity. In the future, we would like to actively enhance the internal environment by utilizing Generative AI, while deepening collaboration between the IT and security divisions.

Sasaki: At present, various individuals in the Company are not only using natural language conversational AI but also attempting to utilize code generation AI and image generation AI, incorporating them into their own services. The immediate challenge is to conduct appropriate risk assessments for these various types of Generative AI so that KDDI employees can use and provide safe and secure services. As the division in charge of governance, I would like to collaborate more closely with the user division and consider establishing rules that represent a mutual compromise.
Additionally, as rules and regulations for AI usage are being developed globally, KDDI will strive to accurately capture these trends and reflect them in our internal rules. This effort aims to ensure that AI services provided by KDDI are recognized as safe and secure not only internally but also socially.

2 Information Security Framework

KDDI has established the Information Security Committee, with a member from the management level serving as the chairman and heads of sales, technology, and corporate divisions as members, to ensure unified information security throughout KDDI and the KDDI Group. Additionally, there are Information Security Promoter's Conference composed of representatives from each division within KDDI and KDDI Group companies assigned to the Information Security Committee, as well as the Group Company Information Security Promoter's Conference. This framework enables not only a precise understanding of the status of information security management but also prompt development of measures to enhance information security throughout the KDDI Group. Each Group company has also established an information security management system to reduce and prevent risks of information security and cybersecurity. They conduct risk assessment, analysis, and implement countermeasures and responses.

Information Security Management Framework



Information Security Governance

3 Information Security Management Cycles

KDDI has obtained ISMS certification (ISO/IEC 27001: 2013)*1, and has implemented the information security management cycle. In this cycle, we formulate an Information Security Policy in the planning phase and, following the information security management cycle (PDCA cycle) below, conduct checks, reviews, and improvements.

*1 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.

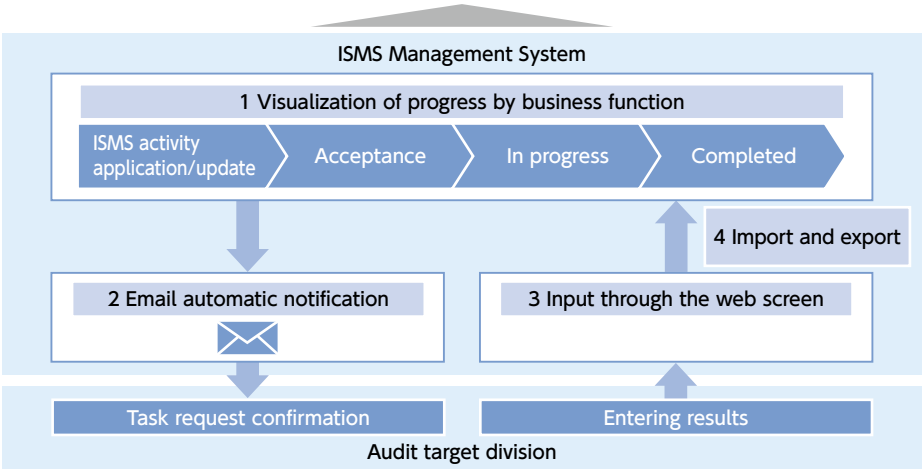
Overview of the Information Security Management Cycle

- **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.

In ISMS activities, it is necessary to regularly assess risks and promptly implement necessary countermeasures to protect various information assets. Additionally, responding swiftly to new threats is essential. These activities were individually managed by personnel in each division; however, with technological advancements and changes in the environment, there was the potential for an increased burden on the responsible individuals. Therefore, with the introduction of the ISMS management system, it became possible to centrally manage information assets and monitor progress through a common database (DB) and visualization of business processes.

In the future, data will be accumulated, analyzed, and utilized in stages, and risk assessment will be conducted based on pattern classification according to the nature of the business and the handled data. This will lead to effective risk management.

Functional items	Function overview/Supplementary information
Visualization of progress by business function	Visualization of progress is possible based on processes such as application and approval
Email automatic notification	Automated delivery of request emails, etc., is possible based on progress
Input through the web screen	Selection input and content confirmation are possible from the menu screen. Additionally, blank fields can be detected
Import and export	Import/export of information asset ledgers is possible. Additionally, updates from the web screen are also possible after importing into Excel
Visualization of activity status and registration information	Automated aggregation of activity status based on progress and the visualization of registration information for each organization are possible



4 Information Security Audits

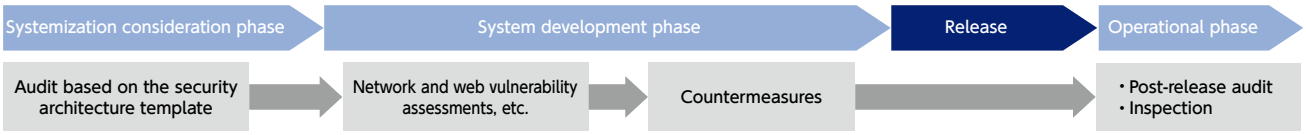
KDDI conducts the following three audits to confirm compliance with information security-related guidelines and ensure proper operations.

System Security Audits

At KDDI, when constructing or modifying systems, audits are conducted by specialized department auditors to investigate whether the work is in accordance with the "Company-Wide System Security Management Guidelines."
In the audit, we use the security architecture template that breaks down the contents written in the Security Management Guidelines into implementation-level details. There are several hundred audit items, and if the requirements are not met, corrective action is requested from the system architect personnel. For the Security Management Guidelines and security architecture templates used in audits, we regularly revise them based on the latest cyberattack methods and strive to enhance the security level.

The flow of security audits is as shown in the diagram below. In the systemization consideration phase, audits are conducted, both in writing and face-to-face, based on the security architecture template. In the system development phase, we conduct network and web vulnerability assessments, implementing measures against vulnerabilities prior to release. Furthermore, we have implemented security monitoring systems such as Intrusion Detection Systems (IDS), and in case of detection, we have established a responsive framework for immediate action. After the system release, we conduct regular audits and inspections as appropriate during the operational phase to ensure that security is appropriately maintained.

Flow of Security Audits



ISMS Internal Audits

KDDI conducts audits on each department and related companies within the scope of ISMS certification, following the "ISMS Management Guidelines" and the "Integrated ISMS Internal Audit Procedures." The audits are carried out by auditors selected from specialized departments or internal organizations. ISMS internal audits confirm that the information security-related norms to be complied with in the KDDI 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 part or all 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. KDDI aims to further strengthen its initiatives in information security to appropriately protect important information, including customer data.

Information Security Governance

5 Information Security Training

Employee Security Awareness and Training

KDDI has established a security human resource development program and is committed to systematic security human resource development to protect customer data and the services we provide from cyberattacks. In this program, we actively encourage the acquisition of the national certification "Registered Information Security Specialist (Cybersecurity Specialist)" operated by the Information-technology Promotion Agency, Japan (IPA). We provide support for certification preparation, including specialized training and learning assistance. As of April 2023, the number of certified individuals within the KDDI Group is 274, making it one of the largest in the country.

Number of Registered Information Security Specialists: 274

* Based on the IPA public directory, those registered with the employer's name "KDDI Corporation" are extracted.
* Aggregate for April 2023

Human resource development is a crucial initiative aimed at fostering employee growth and showcasing the high level of the Company. The goal is to enhance KDDI's expertise and technical capabilities through an increase in certified individuals. Additionally, we conduct stratified e-learning and group-based information security training for a target audience of 11,000 employees, continuously working on improving the security awareness and skills of our 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.

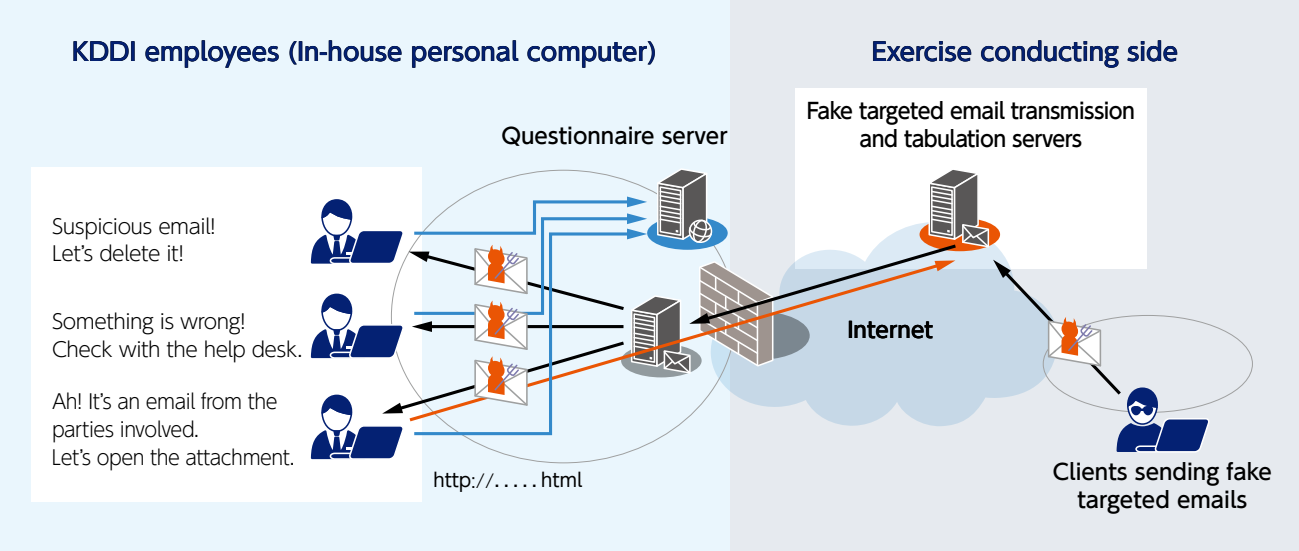
Example of Information Security Training

Content	Target	Implementation method
Security training for new employees	New employees	Group-based training
Basic security training	All employees	e-learning
Security training for line managers	Line managers	e-learning/ Group-based training

Incident Response Exercises

KDDI conducts regular exercises simulating targeted email attacks to promptly and appropriately confirm information-sharing methods and incident response flows, in the event of an incident, such as a cyberattack. When an actual incident occurs, we will establish a response headquarters based on the scale of the incident and collaborate with relevant divisions to implement appropriate measures. Therefore, in training exercises, not only the security-related divisions but also divisions such as those related to systems and public relations participate according to their roles. This is because there is a possibility that these divisions may be the source of incidents or may need to disseminate information externally. In incident response exercises, we continuously follow the cycle of "scenario creation," "conducting exercise," and "feedback/improvement." 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.

Example of an Exercise Using a Fake Targeted E-mail



(1) Scenario creation

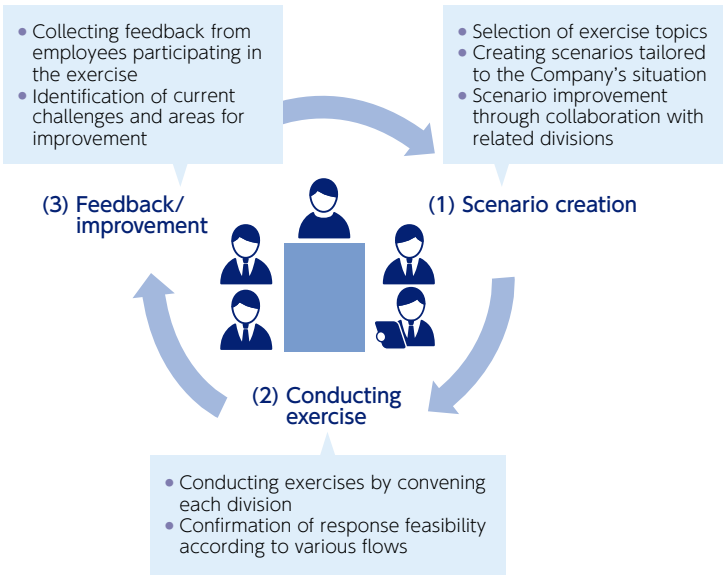
The exercise-related will conduct scenario creation. In scenario creation, exercises are conducted using subjects such as ransomware, which is currently a social issue. To ensure that the created scenario reflects situations that could actually occur, we collaborate with the system-related divisions, which could be the source of incidents in the scenario. Together, we work to improve the scenario.

(2) Conducting exercise

We convene each division and, assuming that an incident has actually occurred, engage in communication and take various actions in response to the incident. In this way, participating divisions in the exercise confirm whether they can fulfill their roles within the predetermined incident response flows. Practical exercises are conducted, including the use of online meetings for remote information sharing between divisions to align with actual on-site incident response.

(3) Feedback/improvement

After the exercise, we gather feedback from participating employees to identify current challenges and areas for improvement. We aim to improve these aspects and enhance our ability to respond to cyberattacks by continuously conducting ongoing incident response exercises targeting various topics and numerous divisions.



Measures for Enhancing Security

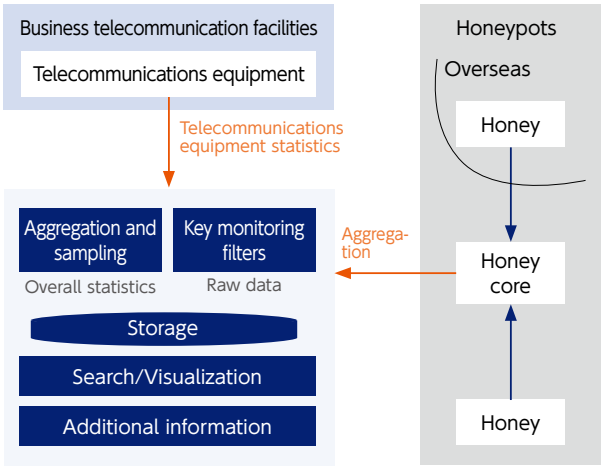
1 Advanced Monitoring Technology

To protect the information entrusted by our customers and the data we handle, we continually monitor for cyberattacks. The monitoring system has the capability to analyze various logs and detection information from security devices to predict and anticipate attacks. It also has the function of collecting information from various information agencies, security research organizations, and security experts engaged in information dissemination. Additionally, monitoring functions for the early detection and response to suspicious access are integrated into both personal computers and servers. To leverage these functions, we are actively working on the introduction of DX and AI. This enables us to respond quickly in case any signs of an attack are detected.

■ Attack Telecommunication Observation System

At KDDI, we actively monitor trends in online attacks, visualize indicators of potential attacks, and implement proactive countermeasures. To accomplish this, various telecommunications equipment and honeypots are installed in KDDI's telecommunications network. Information from these sources is aggregated, sampled, and subjected to correlational analysis. By leveraging the attack telecommunication observation system, KDDI has the capability to understand and anticipate attacks across the entire KDDI network and among corporate customers in its security monitoring operations. This enables KDDI to provide added value related to cybersecurity, unique to a telecommunications company, to its own and corporate customers.

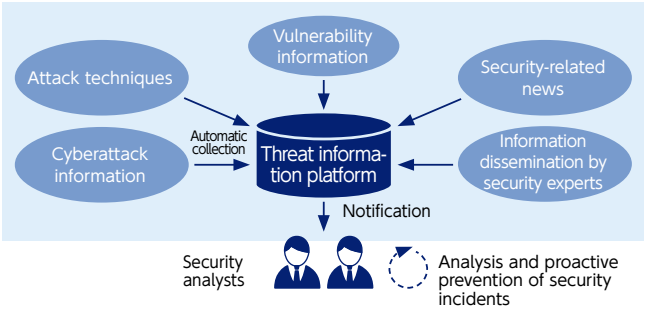
Overview of the Attack Telecommunication Observation System Developed by the KDDI Group



■ Threat Information Platform

Cybersecurity is a rapidly evolving field, and in the event of the disclosure of critical vulnerabilities or attack codes, prompt implementation of countermeasures is necessary. Therefore, it is crucial to gather the latest vulnerability information promptly in security operations. In traditional methods, security analysts had to manually collect and analyze information, assess priorities, and raise awareness within the Company. However, with the "threat information platform" developed in 2022, we automatically collect cyberattack information, attack techniques, vulnerability details, security-related news, and information disseminated by security experts.

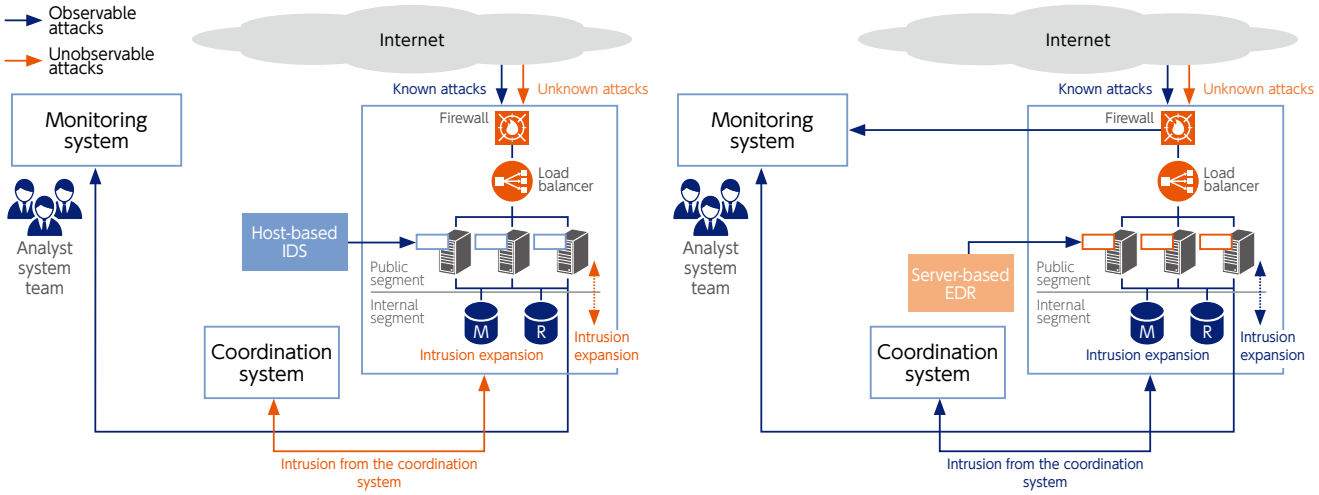
The use of this threat information platform automates the information collection tasks previously performed by security analysts, improves the quality of security operations, and contributes to the proactive prevention of security incidents.



Server-Based Endpoint Detection and Response (EDR)

In recent years, cyberattacks have become more sophisticated and advanced. For this reason, traditional perimeter-type defense methods alone cannot completely prevent cyberattacks, necessitating measures based on the "premise of intrusion." In addition, the lead time for attackers has shortened, and the time from initial intrusion to the achievement of attack objectives has decreased. On the other hand, as the time from initial intrusion to breach detection has lengthened, early detection of breaches and rapid response have become crucial in security operations. Against this background, many organizations are deploying Endpoint Detection and Response (EDR) as a security solution in addition to traditional antivirus software. By integrating powerful AI technology into EDR, they are establishing an environment that enables a swift response to incoming attacks on business personal computers and servers. As a result, it becomes possible to detect attacks from both within and outside KDDI, enhancing the level of security monitoring and expanding the scope of surveillance. It also enables proactive prevention of security incidents and facilitates prompt security incident response.

Present issues	Details of countermeasures
Detects only known events and security incidents. Unable to detect internal intrusions after the breach.	Implement server-based EDR and aggregate logs.



Measures for Enhancing Security

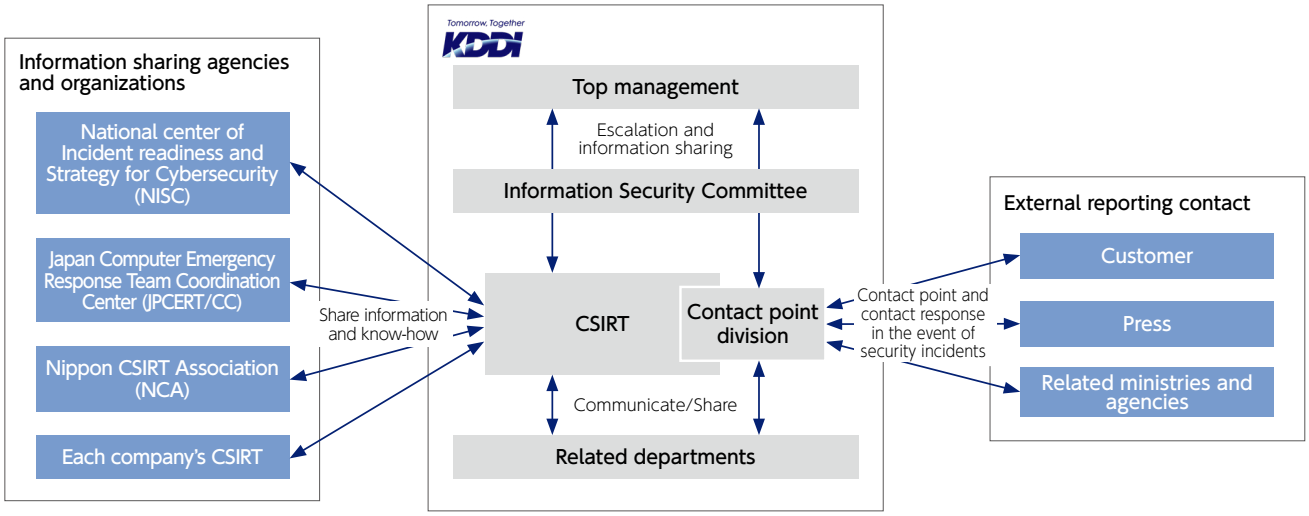
2 Introduction of Security Measures

Computer Security Incident Response Team (CSIRT) Initiatives

CSIRT is a specialized organization dedicated to responding to security incidents that occur within an organization. CSIRT plays a role not only in responding to crises but also in coordinating internal and external activities, collecting and analyzing threat intelligence and vulnerability information, and establishing an effective response system for security incidents, even during normal times. KDDI established CSIRT in 2013. In the event of security incidents, CSIRT collaborates with related internal divisions to conduct cause investigations, preserve evidence, and ensure organizational control towards resolving the situation. In 2018, we also began working with an external organization, KDDI Digital Security*1. Under normal circumstances, we also collect information on cyberattacks and vulnerabilities to prevent future security incidents. Furthermore, we closely collaborate with external security organizations such as the National center of Incident readiness and Strategy for Cybersecurity (NISC), ICT-ISAC, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), as well as communities like the Forum of Incident Response and Security Teams (FIRST) and the Nippon CSIRT Association (NCA).

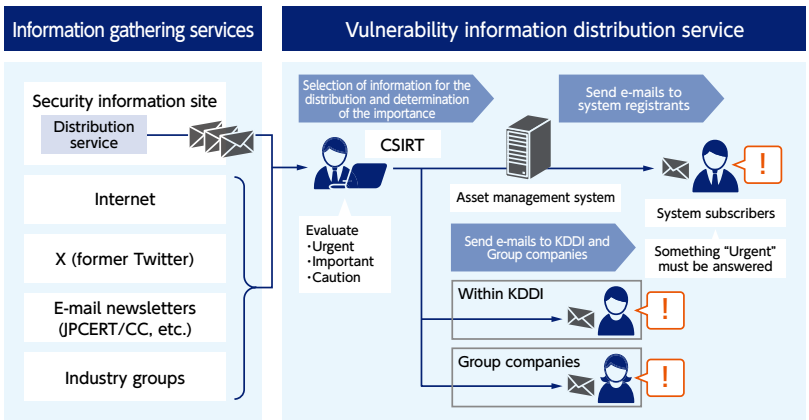
*1 KDDI Digital Security Inc. (KDSec) is a company established by KDDI and LAC Co., Ltd., and it is a leading company in the field of information security. By combining KDDI's ICT solutions with LAC's advanced security analysis and technical capabilities, the Company is dedicated to providing comprehensive security solutions and strengthening security measures for the KDDI Group.

Structure of Coordination Framework with Information Sharing Agencies and External Reporting Contacts



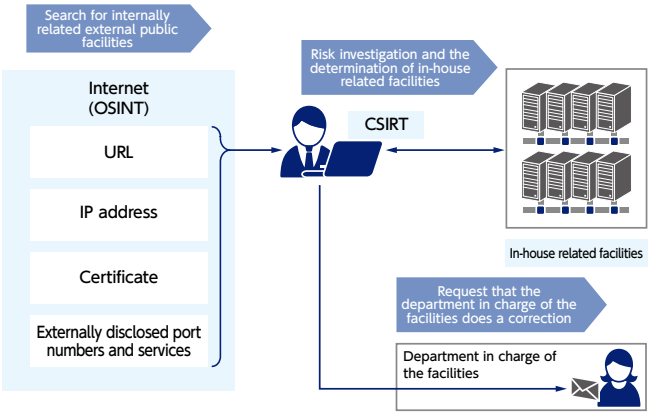
■ Vulnerability Information Collection and Distribution

In CSIRT, vulnerability information obtained from security information sites and other sources is disseminated to the internal system construction and operation staff. Each responsible person then confirms the impact. If there is an impact, the results are reported to CSIRT, and we collaborate to implement countermeasures. In addition, since April 2017, we have introduced a cybersecurity management system that centrally manages the configuration information of all systems. Currently, using the cybersecurity management system, we automatically determine the systems to be corrected and distribute vulnerability information directly to the relevant system construction and operation staff. This enables a quick and efficient response.



External Attack Surface Investigation and Corrective Action

CSIRT recognizes that, within organizations promoting digital transformation (DX), there is a tendency for externally exposed devices—especially those supporting Virtual Private Network (VPN) and Remote Desktop Protocol (RDP)—to become targets for attackers as the attack surface expands with the advancement of initiatives. These devices have vulnerabilities and management deficiencies, posing a significant threat of unauthorized access through authentication bypass or password information leakage. There have also been reported cases of actual attacks on companies. In CSIRT, proactive investigations are conducted from the perspective of attackers to reduce the risk of cyberattacks exploiting externally exposed equipment. We identify hosts that are challenging to pinpoint through regular vulnerability assessments or have management deficiencies. We then focus on reviewing their public status and correcting configuration issues. Specifically, we explore in-house related facilities that are externally exposed by leveraging information publicly available on the Internet, such as Open Source Intelligence (OSINT), URLs, and certificates. Through this investigation, we evaluate the risk of attacks and the management status of our facilities. Based on the investigation results, we promptly implement corrective measures for hosts with high risks and take precautions to prevent attackers from exploiting externally disclosed equipment. In this manner, CSIRT actively takes measures to enhance the organization's security and enables companies to promote DX safely.



Security Monitoring Initiatives

To protect the services and information we provide to our customers, our security analysts at the 24/7, 365-days-a-year Security Operations Center (SOC) monitor for unauthorized access and falsification. In this monitoring, we leverage information from Intrusion Detection System and EDR to detect suspicious activities. Trained security analysts use Security Information and Event Management (SIEM) to monitor and analyze logs generated by each security monitoring device, detecting signs of attacks. If a dangerous security incident is detected, they promptly contact CSIRT and the relevant divisions within the Company, instructing them to take action. Furthermore, internal monitoring is conducted to detect events related to internal misconduct, such as the unauthorized removal of information by employees. This protects our customers' services, information, and internal confidential data from various security threats.

At the KDDI Group, there is also a focus on the in-house development of various systems related to security operations, such as the Cybersecurity Management System and security information infrastructure.

Measures for Enhancing Security

The Cybersecurity Management System manages asset information for each system and handles the distribution of vulnerability information related to assets, as well as ticket management for various response scenarios. The implementation of the Cybersecurity Management System has achieved the streamlining of asset management. Additionally, the security information infrastructure is designed for the collection, storage, investigation, analysis, and visualization of security information. Its centralization of information allows for the effective implementation of security measures.

At the KDDI Group, we ensure the enhancement of security measures and customer trust by incorporating technology in-house through internal development, thereby achieving more efficient and high-quality business operations.

■ Countermeasures Against DDoS Attacks

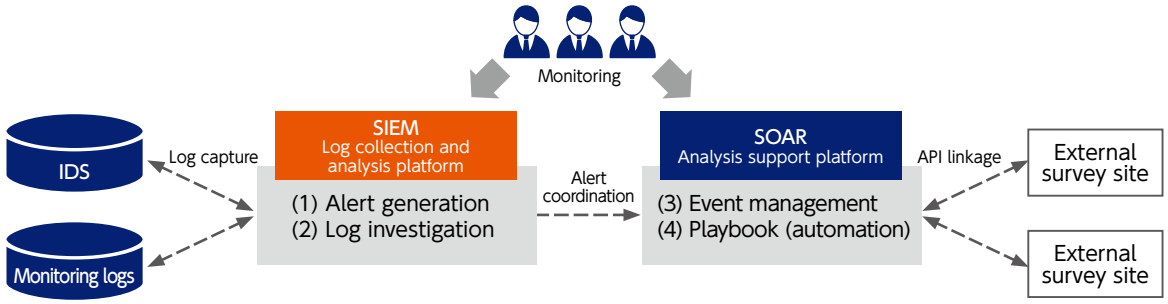
At KDDI, we develop and operate systems to address Distributed Denial of Service attacks (DDoS attacks). If an attack is detected, automatic countermeasures are taken according to predetermined rules. However, as needed, KDDI Digital Security collaborates with the operational monitoring division of our telecommunication facilities to implement appropriate measures. In DDoS countermeasures, we are also actively involved in gathering and verifying information related to technologies such as AI. This enables us to grasp the latest technologies and techniques, swiftly detect the characteristics of attacks, and respond accordingly. Through these efforts, KDDI is able to protect the telecommunication network and provide stable telecommunication services. We minimize service outages and interruptions caused by DDoS attacks, providing a safe environment for our customers.

■ Technology Development to Support Advanced Security Monitoring

To protect its business and corporate networks from cyber threats, the KDDI Group is leveraging cutting-edge technologies to advance its security monitoring systems. This involves utilizing monitoring equipment and systems such as Security Information and Event Management (SIEM), Security Orchestration Automation, and Response (SOAR), and Intrusion Detection System.

In the realm of cybersecurity analysis support platforms, the integration of highly skilled monitoring personnel and the automation of monitoring processes enables the efficient analysis of vast amounts of logs, thereby achieving high-quality security monitoring. Furthermore, this analysis support platform is implemented not only for KDDI (non-consolidated) but also across KDDI Group companies worldwide to collect and analyze security events. This ensures the overall security of the entire KDDI Group.

The KDDI Group ensures the reliable protection of customer networks by leveraging the latest security technologies and enhancing the sophistication and efficiency of security monitoring systems. Additionally, through global deployment, we centrally manage security for the entire KDDI Group, providing a safer environment.



Strong Partnerships for Sharing the Latest Cyberattacks Information Through Data Analysis

Against constantly evolving cyberattacks, KDDI's Information Security Divisions and KDDI Digital Security are collaboratively promoting initiatives to analyze trends of DDoS attacks using actual data and share information.

Security Operations Division 1, KDDI Digital Security Inc.
Atsushi Ushida (left)

Security Operations Division 1, KDDI Digital Security Inc.
Hikaru Oishi (middle)

System Security Department, Information Security Division
Yuuta Miura (right)

What background led to the launch of collaborative initiatives to analyze DDoS attacks?

KDDI aggregates a substantial amount of traffic data for each telecommunication facility but faced the challenge of not having enough manpower to dedicate time to analyzing DDoS attacks. On the other hand, at KDDI Digital Security, there is a strong emphasis on training analysts to analyze cyberattacks that primarily target KDDI through network channels. As the challenges and requirements of both parties aligned, we decided to launch collaborative initiatives in data analysis. In addition, leveraging KDDI Digital Security's expertise in collecting global threat information, we prepare regular reports that interweave public attack data with actual detection data, fostering information sharing between the two parties.

What advantages do you think there are in trend analysis of cyberattacks through data analysis?

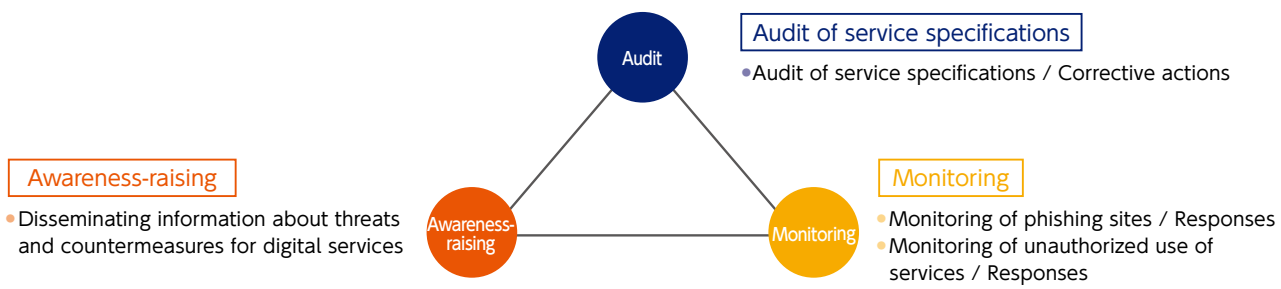
DDoS attacks are one of the oldest cyberattack methods, and techniques like "TCP SYN Attack" have been used as effective attacks for over 20 years. On the contrary, at present, attacks exploit a wide range of ports, and diverse attack communications from what appears to be botnets exploiting IoT devices are observed. Consequently, defending against these attacks can be challenging. However, by understanding the trends of DDoS attacks through data analysis, it becomes possible to automatically control and implement countermeasures. This allows for the prevention of the expansion of damage caused by attacks and enables early recovery. In other words, data analysis is a valuable tool for defending against DDoS attacks and has become an indispensable element in security measures.

Looking to the future, what kind of security initiatives do you plan to take?

As the trends in DDoS attack techniques change daily, we have begun to observe telecommunications where the complete scope of the attack is difficult to discern. To enable analysts to analyze such communications, we plan to incorporate advanced visualization technologies to understand the overall picture of the attack and implement appropriate security measures.

SSIRT Efforts

Service Security Incident Readiness & response Team (SSIRT) is an organization established to address new threats arising from the digitization of services, a necessity also recognized by NISC. In 2018, KDDI established SSIRT to address new risks as a digital service provider. A specialized team with expertise is actively working on three measures: "audit of service specifications," "monitoring," and "awareness-raising." Furthermore, activities to expand this initiative to the entire KDDI Group are also underway.

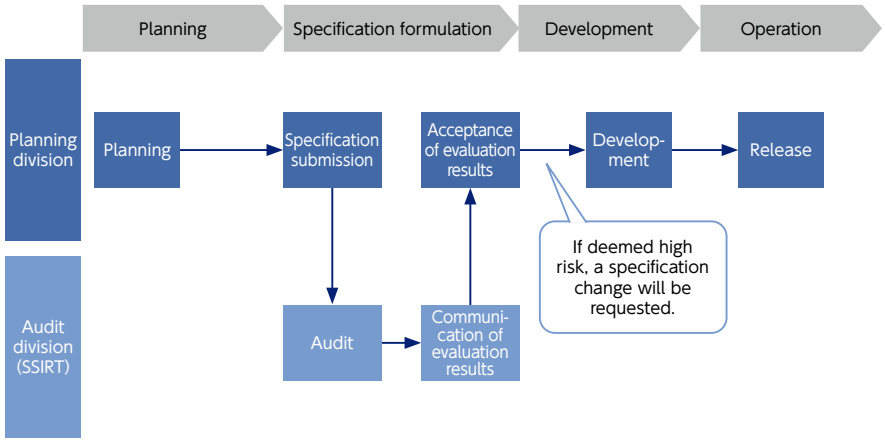


Measures for Enhancing Security

Countermeasures Against Unauthorized Use of Digital Services

■ Audit of Service Specifications

When we provide a new service or add or change 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.



Aiming to Provide Smartphone Apps that Customers Can Use with Peace of Mind

With the widespread use of smartphones, a diverse range of applications is being provided. Tasks that were traditionally performed on personal computers can now be done on smartphones, making people's lives increasingly convenient. However, smartphones store a significant amount of personal information, and because they are constantly carried, it becomes possible to acquire and accumulate a large amount of information, such as location data. Therefore, I sometimes feel anxious that those applications access information within my smartphone and retrieve it. Furthermore, there is a possibility of information leakage due to vulnerabilities in applications.

At KDDI, we provide many apps to make it more convenient for customers to use au services. Considering the background mentioned earlier, we believe it is necessary to offer applications that customers can use with confidence. Therefore, at KDDI, we have established guidelines as company regulations for the development and provision of smartphone apps. It is mandatory to conduct vulnerability and privacy audits before releasing the app. The vulnerability assessment conducts diagnostics in accordance with the "Android Application Secure Design/Secure Coding Guidebook" issued by the Japan Smartphone Security Association (JSSEC) and the mobile security guidelines issued by the Open Worldwide Application Security Project (OWASP).

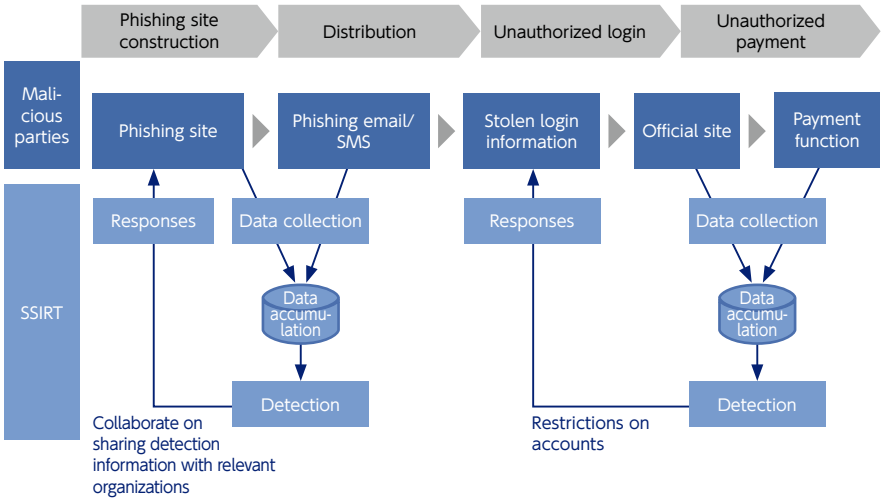
Furthermore, concerning privacy, we create a privacy policy in accordance with the Smartphone Privacy Initiative (SPI) issued by the Ministry of Internal Affairs and Communications, and additionally, undergo an audit by third-party organizations recommended by SPI. In this review, we confirm the transmission of data as stated in the privacy policy and ensure transparency in the data we collect. Additionally, in conducting the examination, we have developed dedicated assessment tools and perform evaluations. We also conduct similar assessments for third-party applications available on au Pay Market. As a result, the cumulative total of examinations has surpassed 13,000 cases to date. Moving forward, we will continue to work towards providing smartphones that customers can use with confidence by making appropriate revisions to the guidelines in preparation for new threats.

In charge Security & Privacy Guidelines Audit
Service Development Department 1, Business & Services Development Division
Teruaki Honma

Monitoring

As a measure against phishing frauds, SSIRT conducts two types of monitoring. One is the “monitoring of phishing sites.” This involves detecting the occurrence of phishing sites based on information obtained from the Internet. Upon detection, collaboration with relevant authorities occurs to implement measures, such as preventing customer access. The other is “monitoring of unauthorized use of services.” It involves analyzing information such as system logs to determine whether logins or transactions are legitimate actions by genuine customers or if they are unauthorized activities due to account takeover.

If deemed unauthorized, it imposes restrictions on the account. SSIRT conducts these round-the-clock monitoring activities to address them and ensure that customers do not fall victim to any harm. Additionally, we conduct daily data analysis, expand the scope of data under analysis, and strengthen monitoring capabilities to enhance early detection of new irregularities and improve detection accuracy.



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. Furthermore, we collaborate with external organizations such as the Council of Anti-Phishing Japan and the Japan Cybercrime Control Center (JC3), advancing information sharing on the latest techniques and countermeasures, while also strengthening response capabilities.

Measures for Enhancing Security

Initiatives for Audits to Provide a Secure Service
SSIRT Member Discussion

System Security Department
Information Security Division
Satsuki Nishioka

System Security Department
Information Security Division
Takuya Katou

Please discuss recent trends in the unauthorized use of the service.

Nishioka: Unauthorized logins to other people's online accounts once targeted some services, such as Internet banking on personal computers. However, with the widespread use of smartphones making online shopping and bank transfers easier and more convenient, incidents of unauthorized use have also increased. Phishing frauds, utilizing emails or SMS messages that impersonate legitimate organizations to extract login information, are a primary trick of malicious parties. Following unauthorized logins, it has been confirmed that they proceed to make unauthorized purchases or transfers without the user's knowledge.

Katou: If users are deceived by phishing frauds and enter their account information or passwords on a phishing site, malicious parties can then log in using that information. Some services implement measures against unauthorized logins, such as sending two-factor authentication codes. However, users being deceived into entering even such codes, allowing unauthorized logins on phishing sites.

Nishioka: The tricks are becoming increasingly clever every day. Despite companies taking measures, the current situation is characterized by the development of tactics that can overcome these measures, in my opinion.
As KDDI also provides various services, including au PAY and au PAY Market, we are not unrelated to such damages. We monitor phishing sites and unauthorized use in response to these issues. Additionally, as part of initiatives to enhance the security of the service itself, we also conduct security audits.

What aspects is your team conscious of when working on audits?

Katou: In the audit of service specifications, we assess the magnitude of risks of unauthorized use by considering two factors: susceptibility to targeting by malicious parties and the potential severity of damage if exploited. Additionally, when a certain level of risk is anticipated, we develop necessary countermeasure proposals and request the enhancement of measures from the service planning division. Security measures involve a trade-off between safety and convenience, and as we prioritize safety, we strive to achieve the best possible balance between both aspects.

Nishioka: The susceptibility to being targeted by malicious parties and the severity of the damage depend on the balance between the effort malicious parties put into committing fraud and the benefits they can gain. In other words, it depends on the motivation of the malicious parties to execute unauthorized use itself. Therefore, the key is to prevent an increase in the motivation of malicious parties. To achieve this, it is effective in terms of governance to establish uniform rules, add authentication based on these rules through audits, and limit the amount of money that can be used. However, when it comes to measures against unauthorized use of the service, it is challenging to avoid compromising the convenience of legitimate customers with this approach.

Katou: Therefore, instead of uniform rules, we are promoting specific measures with a flexible approach for each individual strategy, focusing on the motivation of malicious parties while establishing certain standards, such as guidelines. For this purpose, it is necessary to be well-versed in trends of unauthorized use of services both domestically and internationally, so we strive for daily information gathering through activities such as participation in business associations and researching overseas news.

Nishioka: In the future as well, it is anticipated that the behavior of malicious parties will change in accordance with societal shifts. Despite these changes, we hope to contribute by continuously adapting and providing safe, user-friendly services.

3 Measures for Strengthening Governance

Reconstruction of KDDI Group Security Governance

In fiscal 2011, KDDI established the "KDDI Group Information Security Standards" for its Group companies and encourages each Group company to achieve compliance with these standards. In this way, we are working to improve the security level of KDDI Group companies and enhance information security governance. Additionally, as the number of Group companies increases, there is a demand for establishing security governance tailored to the business types and scales of each company. As a result, in October 2023, we revised the KDDI Group Information Security Standards and are providing support for each company to build security systems tailored to their respective business types and scales. This is intended to unify and strengthen the security system throughout the KDDI Group.

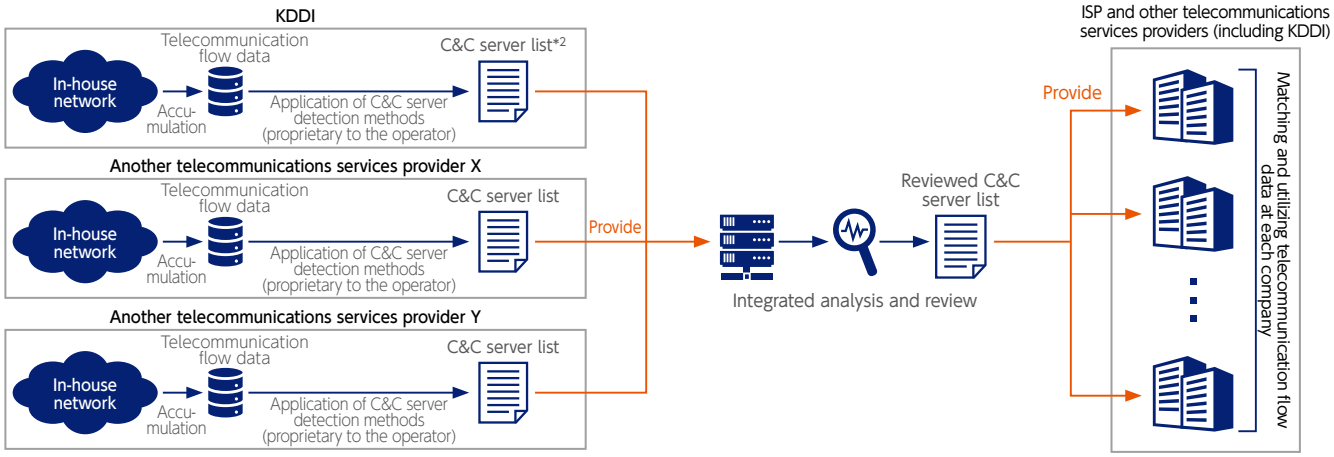
Advanced Technology

1 Command and Control (C&C) Server Detection Research

With changes in societal trends, including the rise of telework, there has been a growing number of Internet-connected devices such as IoT devices, smartphones, and PCs. Recently, cyberattacks that infect terminals with malware and exploit them as means for information theft, such as DDoS attacks and phishing, have also increased in scale. The server that issues instructions for cyberattacks to terminals infected with malware is commonly known as a Command & Control Server (hereinafter C&C Server). As a telecommunications services provider, KDDI needs to proactively understand the operational status of C&C Servers, with the perspective of developing appropriate responses to such servers in the future. In light of this background, at KDDI, we collaborate with multiple major telecommunications services providers and others, and have been entrusted with projects from the Ministry of Internal Affairs and Communications since fiscal 2022. We are engaged in an initiative to detect C&C servers through extensive analysis of data known as flow information*1 within the traffic flowing through our own network.

In fiscal 2023, we are working to enhance the analysis methods to more precisely detect C&C servers based on insights and issues identified during the analysis of fiscal 2022. Additionally, we are collaborating on initiatives to share information about C&C servers detected by major telecommunications operators, including KDDI, with other entities. This collaboration aims to promote not only security measures in the domestic telecommunications business but also to ensure the safety and reliability of KDDI's information and telecommunication network.

*1 Associated information such as sender and receiver IP addresses, ports, timestamps, excluding the content within the traffic.



*2 Consists of IP addresses and port numbers and does not fall within the scope of telecommunications confidentiality

Cybersecurity Pioneered by Data Scientists

I have been involved in information security tasks since April 2023, but before that, I worked for five and a half years at KDDI Research, Inc., engaging in research on data analysis and AI. The C&C Server Detection Project involves analyzing our own telecommunication flow data and narrowing down IPs with a high likelihood of being C&C servers. This initiative aligns well with the specialized field I was involved in at the KDDI Research, Inc. However, when I actually participated in the project, I realized that even within the domain of data analysis, there are challenges unique to the cybersecurity field.

For example, when collecting a dataset, obtaining comprehensive label information about whether this IP is a C&C server is extremely challenging. Certainly, for challenges like these, machine learning approaches, such as semi-supervised learning and unsupervised learning, are viable options, and we intend to explore them further in the future. Additional approaches from different perspectives are also necessary. Through this project, we expect not only to contribute to the development of the project itself by promoting the sharing and standardization of label information built by each telecommunication service provider but also to gain insights into the analysis of telecommunication flow data from each company.

Ultimately, through this project, we aim to enhance the overall data analysis capabilities related to cybersecurity within the Company, and we hope to contribute to the establishment of cybersecurity at KDDI.

In charge of C&C Server Detection Project, Security Management Department, Information Security Division
Yutaro Mishima

Advanced Technology

2 Demonstration Project for Software Bill of Materials (SBOM) Implementation

With the advancement and diversification of telecommunication system functions, the core software architecture has evolved into complex combinations of various software components. On the other hand, there have been cyberattacks targeting malicious code injection and vulnerabilities in software components, and the risk of similar attacks impacting telecommunication systems has become apparent. Responding promptly to vulnerabilities becomes challenging when the software configuration within a telecommunication system is unknown. Consequently, the significance of a Software Bill of Materials (SBOM), which compiles a list of components, version information, etc., is rapidly increasing.

Against this background, KDDI was commissioned by the Ministry of Internal Affairs and Communications to undertake the "Contracted Survey for the Introduction of SBOM in the Telecommunications Field" project and established a framework to collaborate on this project with KDDI Research, Inc., Fujitsu Limited, NEC Corporation, and Mitsubishi Research Institute, Inc. In this project, our focus will be on organizing technical and operational issues related to the introduction of SBOM in the field of telecommunication, with the aim of achieving prompt responses to vulnerabilities through the utilization of SBOM.

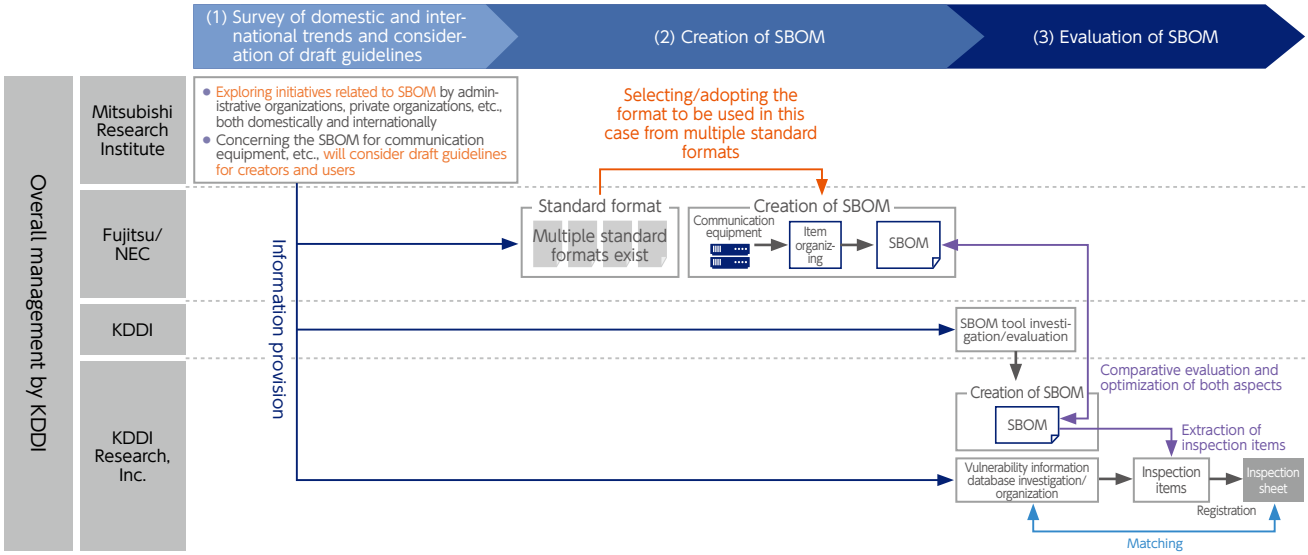
In this project, KDDI will assume overall responsibility for enhancing cybersecurity in the telecommunications field, with each company sharing responsibility for implementing the following steps (1) to (3).

(1) Survey of Domestic and International Trends and Consideration of Draft Guideline (Handled by: Mitsubishi Research Institute)
We will explore the use cases of SBOM in domestic fields beyond the telecommunications sector and examine initiatives related to SBOM by administrative organizations, private entities, and other organizations, primarily in Europe and the United States. Furthermore, to organize key points for creating and utilizing SBOM in the telecommunications sector, we will consider draft guideline for both creators and users.

(2) Creation of SBOM (Handled by: Fujitsu/NEC)
We will select multiple communication devices for wireless access networks and core networks for 5G and 4G LTE. Additionally, after determining the format to be used in the demonstration project based on industry-proposed standard formats, we will categorize the "items specific to the telecommunications field." Subsequently, we will create a comprehensive and high-quality SBOM, ensuring there are no omissions for the mentioned equipment.

(3) Evaluation of SBOM (Handled by: KDDI/KDDI Research, Inc.)
We will use multiple SBOM creation tools selected based on considerations such as functionality, accuracy, cost, etc., to generate an SBOM for the equipment identified in (2). Furthermore, we will assess accuracy by comparing the SBOM created by the tool with the one generated for the equipment identified in (2). Additionally, we will develop an inspection sheet to check vulnerabilities from the SBOM and validate the appropriate vulnerability management methods through comparisons with external vulnerability information databases.

In the midst of anticipated changes in the cybersecurity landscape, we will continue to strive towards contributing to the enhancement of cybersecurity to deliver stable telecommunication services that support our customers' lives.



3 Achieved the World's Fastest 2 Tbps Performance with Rocca-S

The ultra-high-speed common key cryptosystem "Rocca-S" has achieved a processing performance of 2 Tbps, making it the fastest in the world

When we use smartphones or PCs to access the Internet daily, the content is usually encrypted and protected from being seen by others. For example, when registering as a member or making inquiries online, encryption technology called SSL/TLS is used to protect input information, such as personal data, from being viewed by third parties. Examples of specific encryption methods include the following.

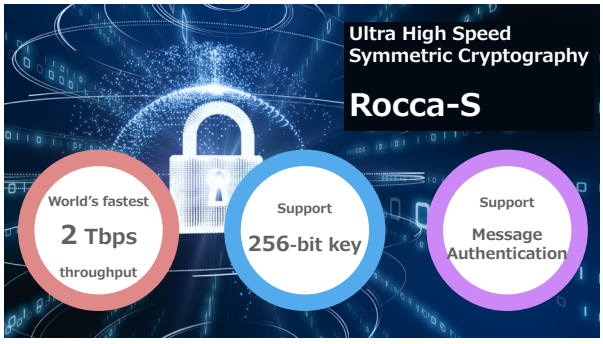
- Encryption of software and hard disk data using a password
- Encryption of Wi-Fi communications to prevent the contents of a neighbor's communication from being read, even if they are using the same signal.
- Encryption of input information during online membership registration
- Encryption of address, name, and payment information on online shopping sites

Until now, cryptography has been used to protect various types of data, but new encryption techniques will be necessary in the era Beyond 5G/6G, which represents the next generation of 5G. One of the challenges is adapting to our communications speed of the Beyond 5G/6G era. The current communication speed of 5G is at most around 10 Gbps, but it is said to surpass 100 Gbps in the Beyond 5G/6G era. With the current common key cryptosystem, the processing performance is limited to several tens of Gbps at most, and at this rate, the encryption process will become a bottleneck in the communication process. Therefore, there is a demand for common key cryptosystem with processing performance equivalent to or greater than the communication speed of Beyond 5G/6G. The other challenge is adapting to quantum computers. Quantum computers utilize the principles of quantum mechanics to process multiple pieces of data simultaneously, enabling them to quickly solve complex calculations that would take a significant amount of time on current computers. However, with its introduction, current public-key cryptography, including RSA encryption, has been shown to be breakable within a practical timeframe. For a long time, quantum computers were considered theoretical and were said to be difficult to achieve; however, with the research and development efforts of many organizations, the possibility of their realization is increasing.

Considering such future scenarios, the National Institute of Standards and Technology (NIST) in the United States has been seeking new public-key cryptography capable of withstanding attacks from quantum computers since 2016 and is actively working on its standardization. Regarding a common key cryptosystem as well, it is necessary to lengthen the key to ensure resistance against decryption by quantum computers. Currently, 128-bit keys are common, but it is considered necessary to use 256-bit keys, which are twice as long. Longer keys can slow down the encryption process, driving the demand for a common key cryptosystem that balances security and performance.

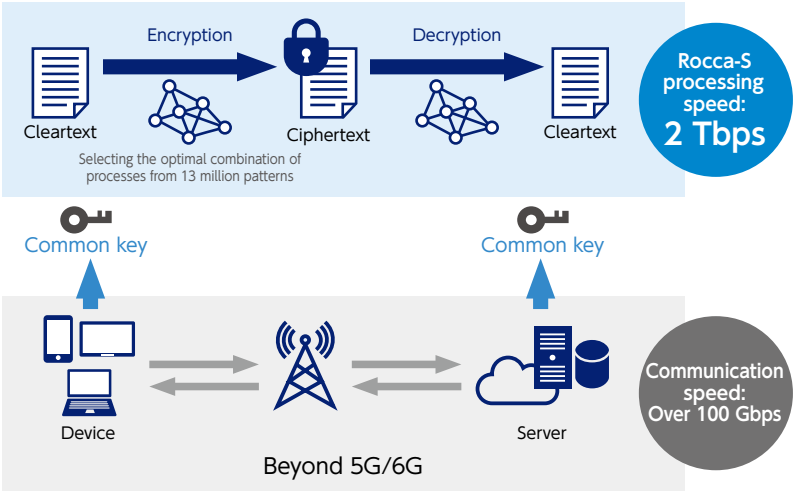
Therefore, KDDI Research, Inc., in collaboration with University of Hyogo, has developed a new common key cryptosystem called "Rocca-S," excelling in both processing speed and the capability to handle quantum computer resistance. Through this Rocca-S, we were able to simultaneously address two challenges: resistance to quantum computers and processing speed. While conventional encryption methods encrypted data by processing it sequentially, Rocca-S achieved acceleration by simultaneously performing multiple processes. Specifically, in hardware implementation, it achieves 2 Tbps, and in software implementation on commercially available PCs, it has achieved a speed of 200 Gbps as of August 2023, currently the world's fastest. It also records speeds of over 90 Gbps on smartphones. Additionally, Rocca-S is designed to support 256-bit keys in preparation for decoding by quantum computers, and its security against known attacks has been verified. Furthermore, it has a function to detect whether the data has been tampered with in the process, achieving significant progress in terms of security.

Characteristics of Rocca-S



Advanced Technology

Rocca-S achieves maximum acceleration through parallel processing, simultaneously handling multiple blocks and ensuring an even distribution of the computational workload across each block. Furthermore, by utilizing components of the current standard encryption AES in the mixing process, it becomes possible to achieve fast software implementation using dedicated hardware instructions (such as AES-NI) on servers, PCs, and smartphones.



In the design process of Rocca-S, we evaluated all 13 million possible configurations derived from the original idea and selected the optimal method. Through several months of computer simulations, we identified the four safest samples from among the 13 million possibilities. Subsequently, we implemented and tested the four samples, ultimately selecting the one with the highest performance as Rocca-S. As of August 2023, Rocca-S is recognized as the world's fastest encryption method, and its technological development is supported by the Ministry of Internal Affairs and Communications. Going forward, with the aim of further acceleration, we will expedite research toward practical implementation and strive to establish Rocca-S as an international standard for the Beyond 5G/6G era.

The Forefront of Encryption Technology: Researchers' Challenge to Achieve a Balance Between Acceleration and Security

With the evolution of infrastructure, why is there a demand for high-speed encryption?

Fukushima: Currently, in telecommunication systems like 5G, customer data exchanges are protected through encryption. Until now, the processing performance of encryption has surpassed communication speeds, limiting cases where the processing performance of encryption becomes an issue. However, with the anticipated launch of 6G services around 2030, a significant improvement in communication speed is expected. As a result, there is a possibility that encryption processing may fall behind in its current state. Therefore, high-speed encryption is required to ensure that encryption does not hinder communication performance. Rocca-S achieves world-leading performance with 200 Gbps in software implementation and over 2 Tbps in hardware implementation, significantly surpassing the targeted communication speed for 6G.

Please share any challenges you faced in designing the world's fastest Rocca-S.

Nakano: In cryptography design, security is more important than anything else. Reducing processing will improve performance; however, it may also reduce security, making it extremely challenging to achieve both high performance and security. In this research and development, our goal was to create encryption that is overwhelmingly faster than other alternatives. Therefore, we prepared 13 million samples for high-speed encryption and verified the security of each one. After more than 3 months of continuous computer verification, we found only four qualified samples that met the security criteria. Due to the significant impact on safety and performance with even slight changes in the internal structure, finding the optimal samples was challenging.

What kind of verification was conducted for the security of Rocca-S?

Nakano: We meticulously verified the security against existing attacks one by one. In addition to attacks by conventional computers, the system has also been confirmed to be secure against quantum computer attacks.

Finally, what is your outlook for the future?

Fukushima: In the future, we aim to actively pursue the international standardization of Rocca-S and strive for its widespread adoption as the standard encryption for the 6G era worldwide. We will continue to promote research and development that contributes to further advancements in communication technology and the improvement of reliability.

Security Division, KDDI Research, Inc. Yuto Nakano (left)
Security Division, KDDI Research, Inc. Kazuhide Fukushima (right)

4 IoT Security Infrastructure through Digital Twin

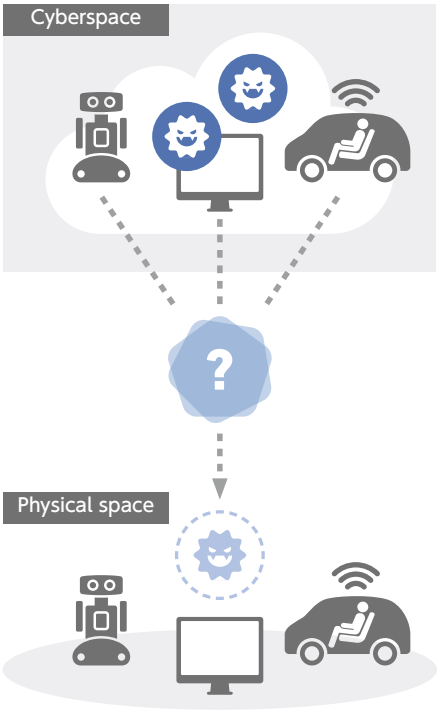
With the progress of Beyond 5G, the integration of cyberspace and physical space is anticipated. This may increase the impact of cyberattacks as they extend into the physical space. Furthermore, with the advancement of digital twin technology, it has become possible to replicate the conditions of physical space in cyberspace. This enables the analysis and simulation of the movements of objects and humans. At KDDI, we are conducting research and development to leverage this digital twin for cybersecurity measures. This allows us to understand the impact of cyberattacks occurring in physical space and implement appropriate countermeasures.

Today, IoT devices have become pervasive throughout society and are utilized in various locations, including critical infrastructure. In such circumstances, it is crucial to identify products that have exploitable vulnerabilities found in commonly used software and hardware across numerous IoT devices. Understanding where and in what situations these vulnerabilities are incorporated and used becomes essential.

However, as shown in the image on the left side of Figure 1, it is currently difficult to identify which products and where they are being used, even if one finds vulnerable network devices in cyberspace. In our research, as shown in the image on the right side of Figure 1, simulations reproduced by the digital twin are linked to each other and share security information through the digital twin wide-area collaboration platform, which is constructed and operated in various locations. We then aim to build a system that can identify and notify the presence of dangerous devices through information on the physical space that each digital twin understands, and assess their impact so that appropriate countermeasures can be taken.

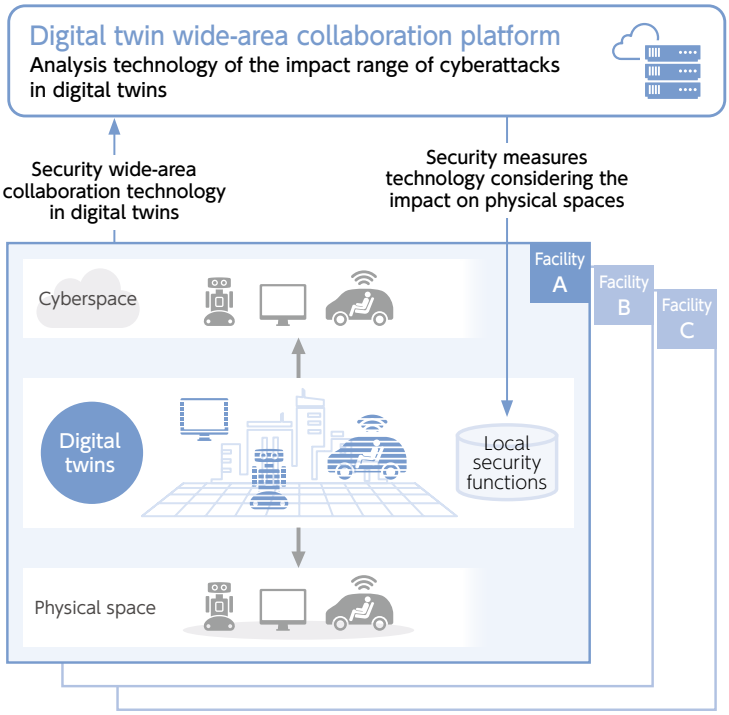
Figure 1 The World Aimed at Through the Utilization of Security in Digital Twins

As-Is (before digital twin utilization)



It is difficult to determine which physical spaces are affected by attacks in cyberspace, and there is a concern that a risk to physical spaces may expand.

To-Be (after wide-area collaboration of digital twins)



By leveraging Digital Twins and their wide-area collaboration, it becomes possible to map cyberattacks in cyberspace to physical spaces, minimizing their impact.

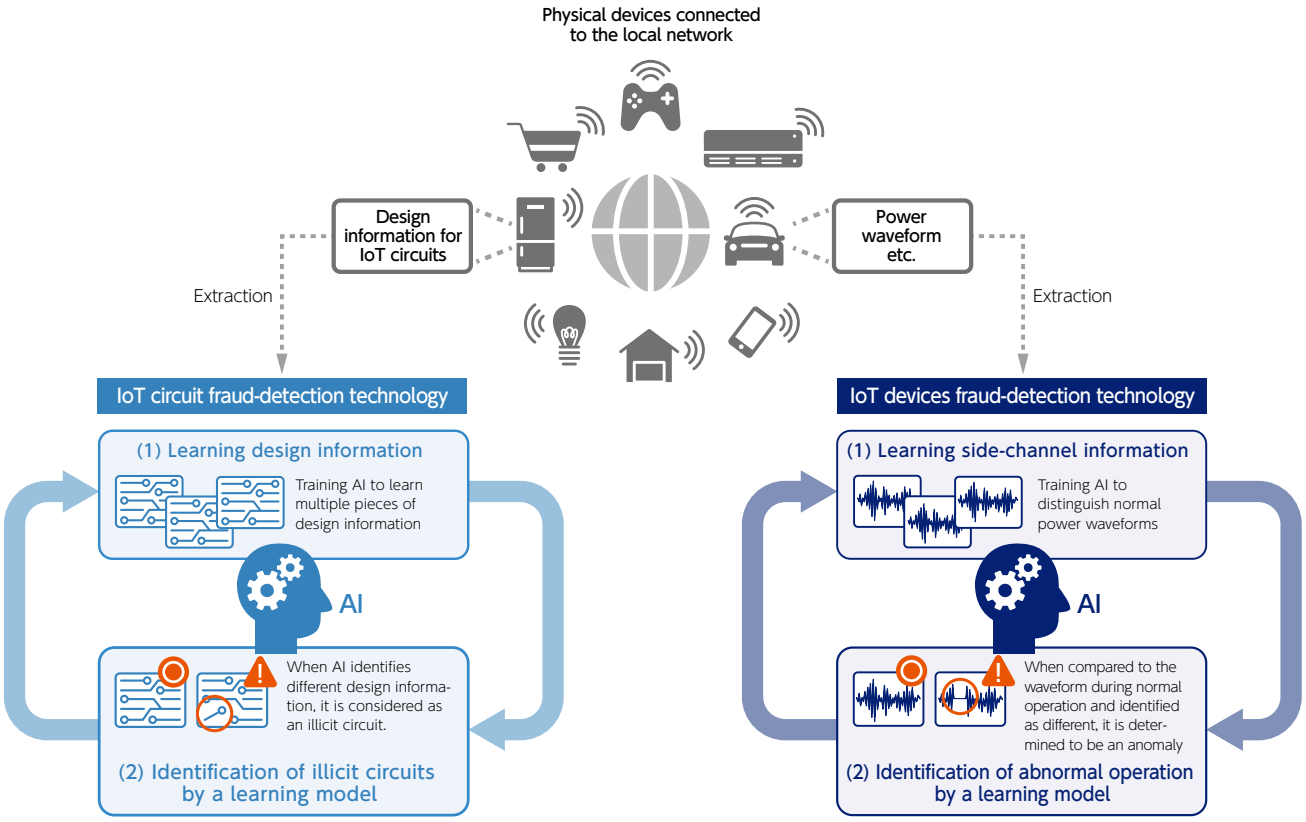
Advanced Technology

In this research, various study challenges include the advancement of observation techniques in cyberspace, understanding threat information related to hardware such as illicit IC chips, consideration of the utilization and collaboration of Digital Twins, and practical demonstrations in a production environment. This research and development effort is led by KDDI Research, Inc.: Yokohama National University, Waseda University, and Shibaura Institute of Technology.

In the Beyond 5G era, the use of IPv6 with its extensive address space is expected to further increase, making it challenging to search for network devices and discover vulnerable devices in cyberspace. Additionally, upon discovering a network device with vulnerabilities, it is necessary to identify the associated product and understand the extent of the vulnerability's impact, as well as possible countermeasures. We are conducting R&D on search technology for IPv6-enabled IoT devices, as mentioned earlier, and device profiling technology that enables us to identify the product and version information of devices based on the search results, as well as to understand the functions of the devices.

In recent years, the incorporation of illicit hardware components has raised concerns regarding supply chain security. Detecting these illicit components and identifying the products into which they have been integrated are significant challenges. Therefore, in addition to research and development on techniques for detecting illicit circuits from the circuit information of IC chips (Figure 2, left) and for detecting anomalous operations from power waveforms during the operation of IoT devices (Figure 2, right), efforts are underway to construct a repository that maintains the relationship between hardware components and products. This initiative aims to accurately identify the products affected when illicit components are discovered.

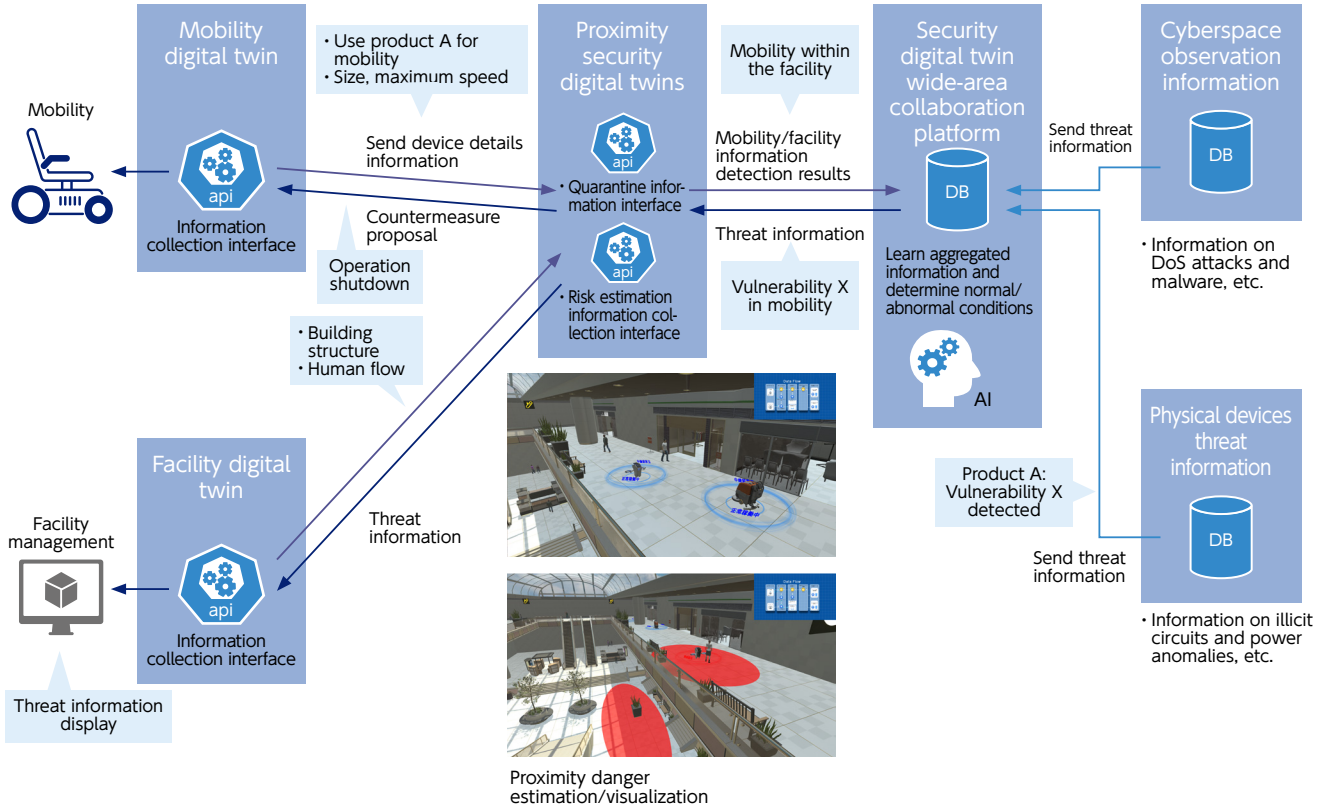
Figure 2 Physical Device Fraud-Detection Technology



The figure (Figure 3) illustrates the configuration of the prototype currently under development as a platform to share threat information grasped through such technologies with digital twins from various locations and to utilize it for security measures. When vulnerable software or illicit hardware components are detected, information about the products in which they are installed is shared across numerous service digital twins through the security digital twin wide-area collaboration platform and proximity security digital twins. The goal is to capture and detect the identified products on digital twins, assess the extent of their impact based on usage and surrounding conditions, and take appropriate measures.

For example, if a problematic network controller causing a decline in communication functionality is discovered, the urgency of the response may vary depending on the type of product in which it is integrated. There may be cases where the response urgency is low, while on the other hand, situations may arise where an urgent response is necessary, such as when it is integrated into a network-controlled vehicle. By utilizing digital twins, the impact of newly discovered vulnerability information and threat intelligence can be evaluated based on the specific conditions at each site where it may have an effect. This allows for the prioritization of countermeasures and supports the selection of appropriate mitigation measures. We are working on the establishment of mechanisms for information sharing and utilization in collaboration with other research institutions participating in this research project.

Figure 3 Cyber-Physical Coordinated Security Infrastructure Through Digital Twins



Initiatives in Security Business

1 Managed 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.

As part of its workstyle reform efforts, KDDI has been promoting initiatives to realize diverse work styles in stages since around 2005. Against this backdrop, we began considering implementing Zero Trust in the fall of 2019 to ensure the protection of devices and cloud services used for telecommuting and teleworking. Due to the COVID-19 pandemic, however, the number of employees telecommuting and teleworking quadrupled, and the number of videoconferences held increased dramatically by more than 70 times, so the perimeter-type defenses no longer sufficed for business operations. Therefore, we have accelerated our plans to introduce Zero Trust and are implementing the system on a company-wide basis.

Considering both "convenience" and "security"

Company-wide implementation (in Japan) ahead of schedule
1,000 units in the 2H plan → 14,000 units after revision

Improved connectivity and stability
No more disconnections and a safe environment for business meetings

Improved work efficiency
Smooth operation, as efficient as when working at the office

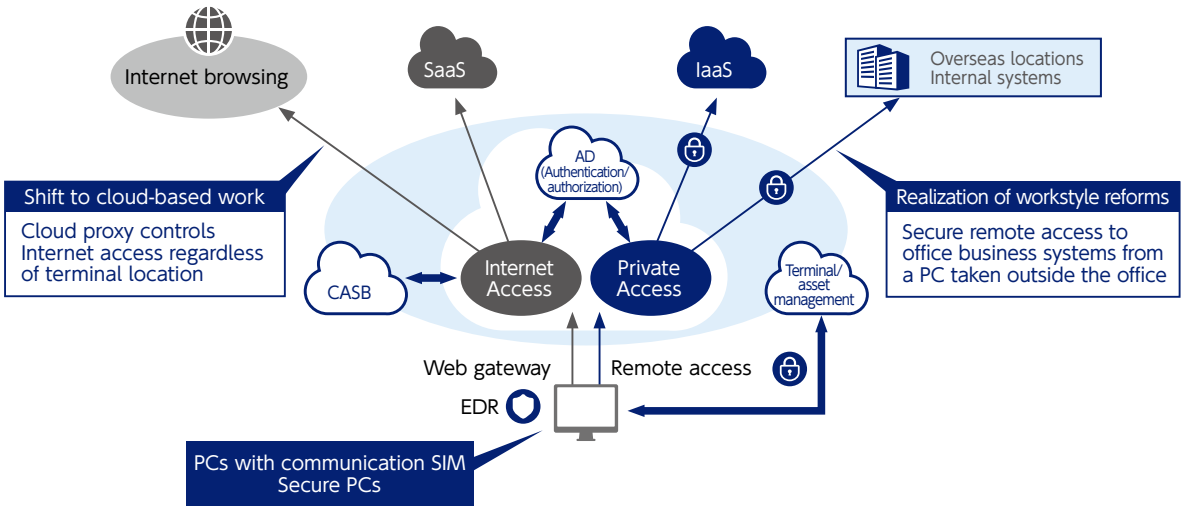
Shift to cloud-based work
Work from any terminal at any location

Improved security
Remote control available in case of loss of device, ensuring security

We began installing and distributing a total of 13,800 devices throughout the Company in November 2020, and completed the implementation of Zero Trust at our domestic locations by February 2021. The combination of cloud solutions allowed for rapid implementation and has provided stress-free operations for both teleworkers and office workers. Based on the know-how cultivated in Japan, we then introduced Zero Trust to our overseas subsidiaries over the next several years, expanding the system to 49 overseas locations in 22 countries.

Structure of KDDI's Zero Trust Model

We have created an environment where PCs equipped with LTE SIM and FAT PCs can securely connect to cloud environments and internal resources anytime, anywhere, with solutions such as SWG, endpoint security, and CASB, which are Zero Trust components.



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

Supporting Security Measures for Customers in Japan and Overseas

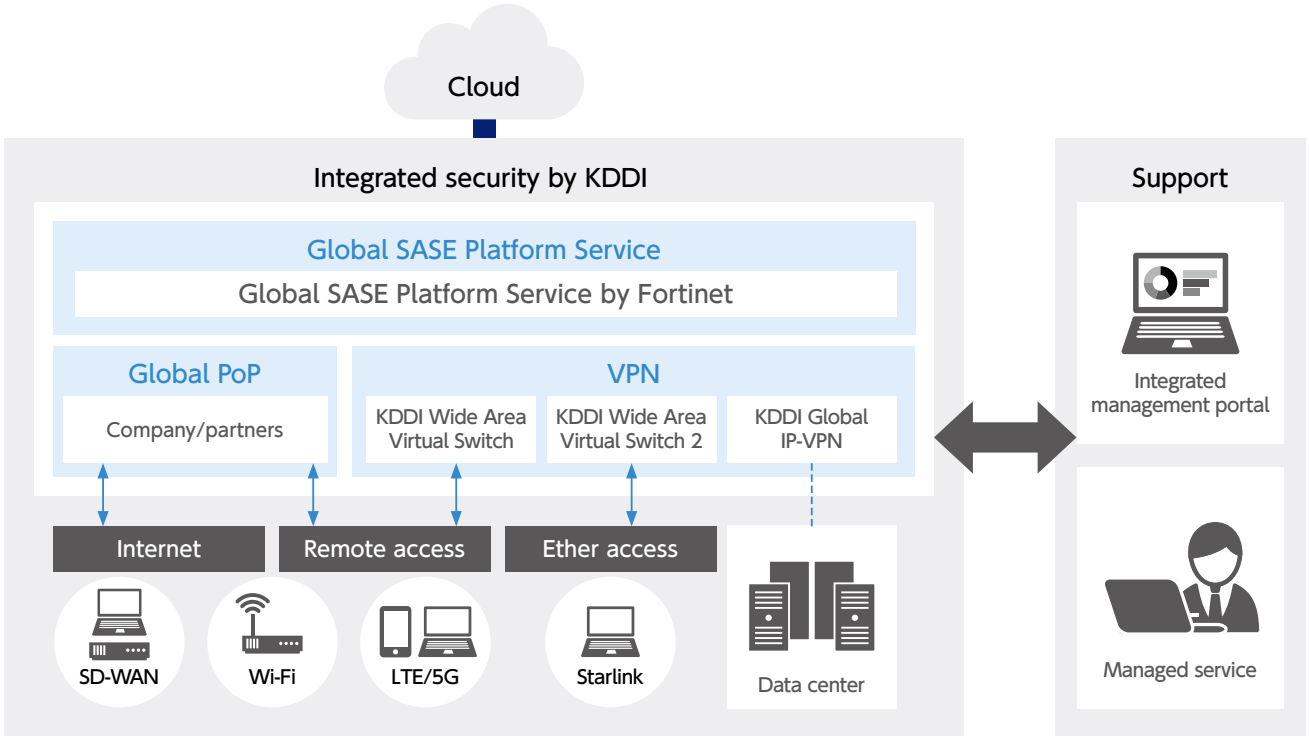
KDDI provides one-stop support for corporate customers' security measures both in Japan and overseas, from consulting to system integration and operational support, leveraging the know-how KDDI has internally cultivated.

Consulting	System integration	Operational support
Support for planning and concept development	Promotion of project management	Agency services for IT operations
Research and assessment of security, cloud migration, etc.	Support for provision, design, and construction of network/cloud/security components	IT help desk services
Support for compliance with overseas laws and regulations		Managed security services

Initiatives in Security Business

Global SASE Platform Service by Fortinet

Besides realizing a high-security environment of remote access from Japan and overseas, we provide one-stop services from examination to implementation, operation, and maintenance at domestic and overseas locations. We deploy key security features such as Secure WEB Gateway, Zero Trust Network Access, a next-generation dual-mode Cloud Access Security Broker, and Firewall-as-a-Service.



2 LAC Managed Service

The “KDDI Security Solution by LAC” integrates the knowhow 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. LAC Co., Ltd. (LAC) 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, LAC has been involved in the development of fundamental systems that support Japanese society, including the financial and manufacturing industries. In recent years, it has also been engaged in the latest IT services suited to the DX era, such as AI, cloud computing, and teleworking. In over 25 years since the launch of Japan’s first information security service, LAC has consistently expanded its position as a leading company in the field of information security. It remains at the forefront of the latest cyberattack countermeasures and incident response, including the Japan Security Operation Center (JSOC), one of the largest facilities of its kind in Japan, alongside cyber emergency centers, vulnerability assessments, penetration testing, and IoT security.

Status of the Group and Third-Party Evaluation

1 Security Incident Record

Number of Serious Incidents Related to Information Security

KDDI is working to enhance information security throughout the Group and reduce information security risks.

Regarding information leaks, regardless of whether they are intentionally or inadvertently caused, we strictly deal with them in accordance with the employment regulations and ensure that all employees are fully aware of and comply with these regulations.

Number of Serious Incidents Related to Information Security

Item	Boundary	Coverage (fiscal 2022)	Unit	Fiscal 2018	Fiscal 2019	Fiscal 2020	Fiscal 2021	Fiscal 2022
Service interruptions of telecommunication services due to external cyberattacks	Non-consolidated	—	Cases	0	0	0	0	0
Personal information leakage due to external cyberattacks				0	0	0	0	0
Personal information leaks				0	0	0	0	0

2 Third-Party Evaluation and Certification

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 (ISMS) global standard certification (ISO/IEC 27001: 2013) *1 are as follows.

Group Companies with ISMS Certified Organizations

KDDI Corporation

Mobile Business

OKINAWA CELLULAR TELEPHONE COMPANY
SORACOM, INC.

Fixed-line Business

Chubu Telecommunications Co., Inc.

Content & Media Business

mediba Inc.

Research & Development of Cutting-Edge Technology

KDDI Research, Inc.
KDDI Technology Corporation

Network Construction, Operation and Maintenance

KDDI Engineering Corporation
Japan Telecommunication Engineering Service Co., Ltd.*2

Contact Center and IT Solution Business

Altius Link, Inc.

Sales & Marketing

KDDI MATOMETE OFFICE CORPORATION*2
KDDI MATOMETE OFFICE KANSAI CORPORATION*2
KDDI MATOMETE OFFICE CHUBU CORPORATION*2
KDDI MATOMETE OFFICE HIGASHINIHON CORPORATION*2
KDDI MATOMETE OFFICE NISHINIHON CORPORATION*2

DX-Related Business

iret Inc.
KDDI Web Communications Inc.

KDDI's Directly Operated Shops

KDDI PRECEDE CORPORATION

Special Subsidiary

KDDI Challenged Corporation*2

Other

KDDI Group Foundation*2
KDDI Pension Fund*2
KDDI Health Insurance Society*2

Overseas Subsidiaries and Offices

KDDI EUROPE Ltd.
KDDI Deutschland GmbH
KDDI FRANCE SAS
KDDI HONG KONG LIMITED
KDDI Asia Pacific Pte Ltd
TELEHOUSE Deutschland GmbH
TELEHOUSE International Corp. of Europe Ltd. Paris Branch
TELEHOUSE International Corporation of Europe Ltd.
TELEHOUSE BEIJING Co., ltd
TELEHOUSE BEIJING BDA Co., ltd
Mobicom Corporation LLC

*1 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

1 Corporate Overview (As of March 31, 2023)

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
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, Representative Director CEO
Makoto Takahashi

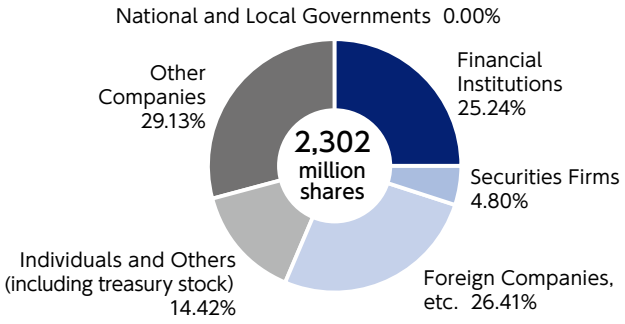
Capital
¥141,852 million

Number of Employees
49,659 (consolidated)

2 Stock Information (As of September 30, 2023)

SE Code	9433
Number of Shares Authorized	4,200,000,000 shares
Number of Shares Issued and Outstanding	2,302,712,308 shares
Number of Shareholders	429,078 shareholders

Breakdown of Shareholding by Investor Type



Major Shareholders

Name of Corporate Entity	Number of Shares Held	Shareholding ratio*1 (%)
The Master Trust Bank of Japan, Ltd. (Trust Account)	342,866,800	16.37
KYOCERA Corporation	335,096,000	16.00
TOYOTA MOTOR CORPORATION	253,094,600	12.08
Custody Bank of Japan, Ltd. (Trust Account)	145,769,400	6.96
STATE STREET BANK WEST CLIENT - TREATY 505234	32,653,275	1.55
JPMorgan Securities Japan Co., Ltd.	25,097,071	1.19
SSBTC CLIENT OMNIBUS ACCOUNT	22,172,909	1.05
JP MORGAN CHASE BANK 385781	22,090,633	1.05
Mitsubishi UFJ Morgan Stanley Securities Co., Ltd.	19,647,001	0.93
STATE STREET BANK AND TRUST COMPANY 505103	18,533,969	0.88

*1 KDDI holds 208,402,549 shares of treasury shares but is excluded from the major shareholders listed above. The shareholding ratio is calculated after deducting the shares of treasury stock.
The shares of treasury stock does not include the Company's shares owned in the Board Incentive Plan trust account (1,074,019 shares). The shareholding ratio is calculated after rounding down to the second decimal points.

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