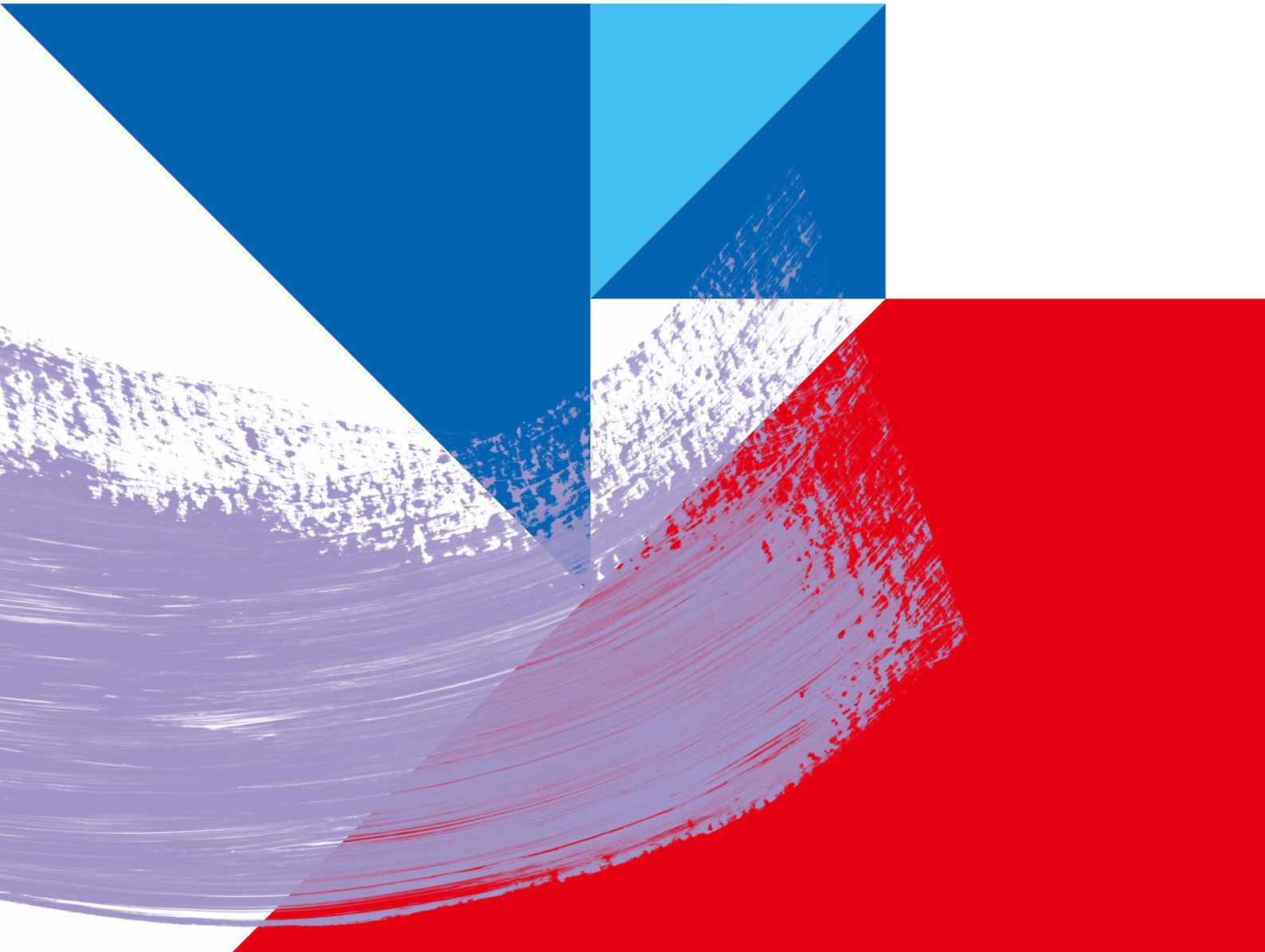
TOSHIBA

Cyber Security Report

2023



Message from the Chief Information Security Officer (CISO)

Improving the resilience of social infrastructure as a whole

As typified by automobiles and TV, our lives and social infrastructure are becoming more and more convenient with digitization and network connection. The wave of digitization has also reached industrial fields such as factory operations, construction, and agriculture, and we are seeing the results of productivity improvement and labor saving. Toshiba Group's vision is to promote the digitization of society, industry, and conditions in people's lives, create new services, and contribute to building a sustainable society. To realize this vision, it is important to implement cyber security initiatives to properly protect and manage collected data.

We must strengthen security in cyberspace to protect society, social infrastructure, and industry from cybercrime. However, as cyberattacks become more sophisticated and risks increase, it is becoming hard to completely eliminate attack damage, no matter how prepared one may be. Hence, the growing importance of "resilience," that is, the ability to respond promptly and appropriately when an incident occurs to minimize damage and recover quickly.

Based on Toshiba Group's management philosophy— "Committed to People, Committed to the Future"—we want to provide peace of mind not only in the physical world, but also in digital space, using the knowledge and experience we have gained through 148 years of continuous manufacturing since our founding in 1875. The purpose of this report is to provide our customers, shareholders, business partners, and all other stakeholders with an understanding of the efforts implemented by Toshiba Group in strengthening cyber security. We sincerely hope that this report will inspire your trust in our products.

Yutaka Sata

Executive Officer,
Corporate Senior Vice President and CISO
Toshiba Corporation

Toshiba Group's Manifesto on Cyber Security

With unwavering determination to protect society from invisible threats

With rapid digitization of everyday life, cyber-crimes have become common nowadays. All of a sudden, anyone could be deprived of their valuable assets or involved in an outrageous crime.

As an enterprise that supports people's lives, Toshiba Group has endeavored to afford **safety and security** to society and its customers. Leveraging extensive experience and expertise cultivated through more than 145 years of history, we offer electricity supply, public transportation, and other infrastructure services as well as data services using cutting-edge digital technologies. We would like to contribute to the betterment of people's lives and culture in both physical and cyber realms. As these services can be a target of cyberattacks, security enhancement is one of the most crucial issues.

To protect society from invisible threats, Toshiba Group works with one accord to establish a robust **cyber security system**, comply with the related laws and regulations, and develop cyber security specialists while being committed to active and honest information disclosure to customers.

We accord the highest priority to the protection of customers' privacy. Therefore, we consider it crucial to properly manage personal data acquired through our business activities in order to prevent its leakage and unauthorized use. In the event of a security incident, we will do our utmost to **minimize damage**, identify its cause, and expedite the recovery of the affected system.

With firm resolve, we commit ourselves to protecting society from invisible threats.

The Essence of Toshiba

The Essence of Toshiba is the basis for the sustainable growth of the Toshiba Group and the foundation of all corporate activities.

The Essence of Toshiba comprises three elements: Basic Commitment of the Toshiba Group, Our Purpose, and Our Values.

With Toshiba's Basic Commitment kept close to heart, we clarified our purpose – the difference that Toshiba Group makes in society – together with our values, the shared beliefs that guide our actions.

Basic Commitment of the Toshiba Group

Committed to People,
Committed to the Future.

At Toshiba, we commit to raising the quality of life for people around the world, ensuring progress that is in harmony with our planet.

Our Purpose

We are Toshiba. We have an unwavering drive to make and do things that lead to a better world.

A planet that's safer and cleaner.
A society that's both sustainable and dynamic.
A life as comfortable as it is exciting.

That's the future we believe in.
We see its possibilities, and work every day to deliver answers that will bring on a brilliant new day.

By combining the power of invention with our expertise and desire for a better world, we imagine things that have never been – and make them a reality.

That is our potential. Working together, we inspire a belief in each other and our customers that no challenge is too great, and there's no promise we can't fulfill.

We turn on the promise of a new day.

Our Values

Do the right thing

We act with integrity, honesty and openness, doing what's right—not what's easy.

Look for a better way

We continually strive to find new and better ways, embracing change as a means for progress.

Always consider the impact

We think about how what we do will change the world for the better, both today and for generations to come.

Create together

We collaborate with each other and our customers, so that we can grow together.

2023 Cyber Security Report

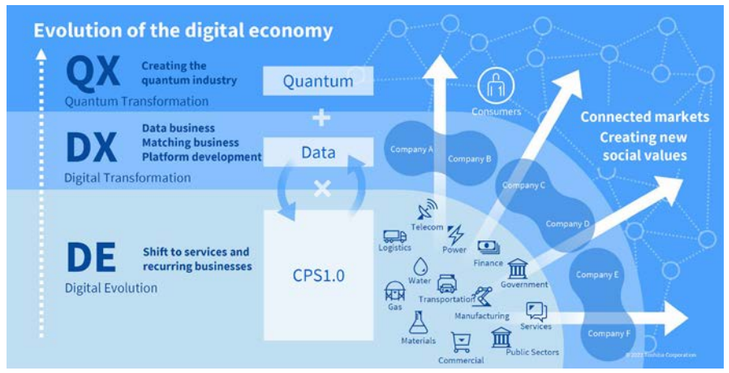
Contents

Visions and Strategies

Based on Toshiba Group's management philosophy of "Committed to People, Committed to the Future," our goal is to create a sustainable future, which we aim to achieve by building infrastructure that enables everyone to enjoy safe and secure lives, establishing a connected data society that achieves social and environmental stability, and realizing a carbon-neutral circular economy, digitalization of infrastructure, and quantization. An important key to fulfilling this vision is the adoption of digital technology, and we believe that with the development of the digital economy, new social value will be created by connecting various businesses and transcending the boundaries between different industries. Cyber resilience is essential for the development of the digital economy. As the digitization of various infrastructure advances, there is an increasing risk of cyberattacks having a physical impact on social infrastructure. It is essential to ensure security in order to connect various businesses across industries, and ensuring the reliability of data that is distributed and used is also an important issue. Furthermore, it is desirable to achieve safe network environments with security capable of withstanding even quantum computers. Exercising our responsibility as an enterprise that promotes digitization, we are engaged in cybersecurity-strengthening initiatives that contribute to the realization of a sustainable, carbon-neutral circular economy by providing safe and secure infrastructure and building a securely connected data society.
In these efforts, we combine our extensive knowledge of infrastructure rooted in a wide range of business areas and cultivated over Toshiba Group's history of more than 145 years with the know-how of security operations for information systems supporting approximately 110,000 employees.

Digitization strategies for the realization of a carbon-neutral circular economy

For many decades, Toshiba Group has been engaged in major national infrastructure projects, including those related to electric power, railways, water supply, and sewage treatment. Toshiba Group has formulated three strategies for digital evolution (DE), digital transformation (DX), and quantum transformation (QX) to adapt to profound changes that will occur as digitization accelerates toward the realization of a circular, carbon-neutral economy. DE, the first step of digitization, focuses on the decoupling of the hardware and software of infrastructure to make it possible to network diverse infrastructure systems and add various software applications to create new services. The next stage is DX, which requires the standardization of software layers so that all software can communicate with any hardware and software applications from third parties, thereby facilitating the development of platforms. Toshiba Group aims to develop a data business in order to create new services using personal and industrial data derived from platforms. As we aim to become an enterprise capable of contributing to the realization of a circular, carbon-neutral economy, the final stage beyond DX is to lead the way to QX, or quantum-inspired approaches to interconnecting platforms across industries to find the optimum solution for complex problems in the carbon neutrality assumption, etc.



Source: FY2022 Toshiba Group Management Policy

Response to supply chain risks

In order to realize a carbon-neutral circular economy, digitization of infrastructure, and quantization, we need to work even more closely with our customers and business partners than ever before. Moreover, there is a greater need than ever to strengthen measures against supply chain risks, so as not to increase security risks to each other's business.
The supply chain means the process that covers the entire product lifecycle, from procurement of the product's raw materials and parts, to manufacturing, sales, use, and disposal. This process involves multiple companies, and cyberattacks that exploit this system are called "supply chain attacks." According to the "10 Major Threats to Information Security for 2023 (Organization Edition)" selected by the Information-technology Promotion Agency (IPA) based on conditions of information security incidents and threats, "attacks that exploit weaknesses in the supply chain" have now been moved up in rank from 3rd place in 2022 to 2nd place, and the social impact of supply chain risks is increasing.
Specific examples of supply chain risks include tampering and embedding of unauthorized programs and firmware in the manufacturing and distribution processes of ICT products and services, and the exploitation of companies with contractual relationships such as business partners and subcontractors that have insufficient cyber security measures, which are then used as stepping stones to deliver ransomware, etc. and cause damage. As a manufacturer that provides products to customers and as a procurer that commissions suppliers, Toshiba Group is engaged in the following efforts for supply chain security: 1) vulnerability management of shipped products, 2) utilization of attack surface survey, and 3) human resource development and enlightenment.

1) Vulnerability management of shipped products
Currently, the number of software-vulnerability-related new registrations put out by the IPA is about 4,000 every quarter. Unless we understand which of our products contain vulnerable software components and which do not, we cannot implement appropriate countermeasures. For this reason, whenever necessary, Toshiba Group matches the configuration information of product software components with the vulnerability information published by IPA and other organizations. If software with vulnerabilities is detected, we notify the product department of the results. Additionally, we have commenced building a system based on SOAR* to manage the response status of each department. Furthermore, by visualizing the number of new vulnerability notifications, the response status of each product, the vulnerabilities whose response deadlines are approaching, and so forth, we are able to share the information on circumstances not only with development divisions, but also with upper management, administrative divisions, and other departments throughout the entire company, and we are promoting the use of this shared information as an indicator for cyber security management.

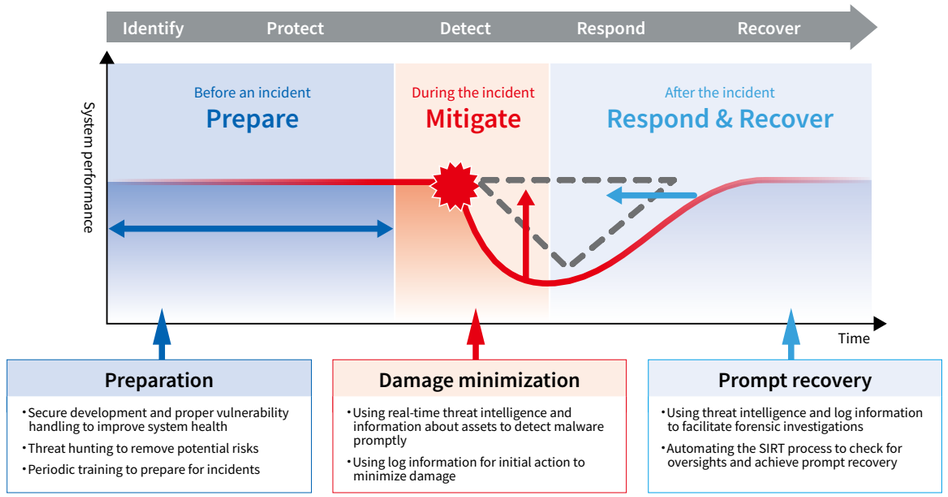
2) Utilization of attack surface survey
We had been distributing Toshiba Group product security quality guidelines to subcontractors to whom we outsource software development, and conducting inspections of new business partners, regular voluntary inspections, and on-site inspections. However, in addition to the high cost of inspections, it was difficult to actually find security holes through voluntary inspections alone, making it difficult to achieve thorough management. Therefore, we have now focused attention on the attack surface survey, which objectively evaluates a company's security level, and we are currently carrying out partial utilization of this. The attack surface survey automatically investigates the status of security measures for externally accessible networks, applications, endpoints, etc., as well as the application status of patches. It observes vulnerabilities hidden in information assets available to the public (such as whether vulnerable services are open to the Internet, whether old operating systems and browsers are being used, etc.), calculates the probability of a breach occurring in the organization/business, and visualizes the security level. Based on this information, we can request subcontractors to make corrections, and can thereby expect to reduce security holes.

3) Human resource development and enlightenment
Supply chain security needs to be understood not only by designers and operational engineers, but also by upper management, sales personnel, and staff, so we are conducting e-Learning for "Supply Chain Security Education" throughout Toshiba Group. Additionally, some business units are conducting cyber security training and taking steps to strengthen their incident response capabilities in order to ensure that the procedures to be followed by each responsible person in the event of a cyber incident can be reliably carried out according to the manual.

※SOAR：Security Orchestration, Automation and Response

Efforts toward realization of cyber resilience

Toshiba Group has adopted a high-level security philosophy called “cyber resilience” in order to achieve comprehensive solutions for information, product, control, and data security. The word “resilience” means the ability to withstand or recover quickly from difficult conditions. The purpose of cyber resilience is to be prepared for cyberattacks and other security incidents so as to minimize their impact and facilitate prompt recovery from any incidents.
Toshiba Group has defined parameters that must be met to increase cyber resilience and thereby minimize the impact of security incidents on infrastructure systems. There are three parameters represented by PMR: P for “prepare,” M for “mitigate,” and R for “respond & recover.” P denotes preparations for cyber security incidents; M signifies mitigation of a loss caused by an incident; and R indicates the time required to deal with and recover from an incident. To become cyber-resilient, it is necessary to promote P and M and reduce R.



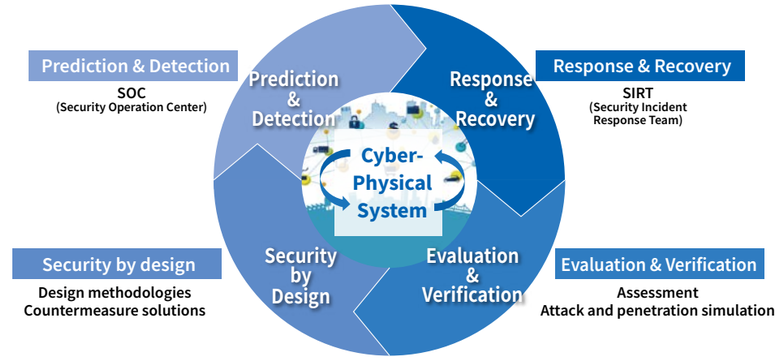
Cyber resilience

Toshiba Group is strengthening its cyber security preparedness with the aim of achieving cyber resilience. Here, “cyber security preparedness” means a state fully prepared for extensive security risks. Specifically, it encompasses three elements: 1) governance to clarify decision-making processes and a chain of command in order to promote P and M, 2) security operations, including prediction & detection, response & recovery, and protection, in order to promote M and reduce R, and 3) personnel responsible for the implementation and enhancement of these operations. These three elements should be enhanced and regularly maintained so that they are implemented in an orchestrated manner.
With the evolution of CPS systems, not only information systems but also development environments, production apparatus, and operation systems for social infrastructure and industrial systems as well as some of their control systems will migrate to the cloud. Physical systems will be controlled from cloud platforms in cyberspace. Then, the conventional software-defined perimeter (SDP) security model will become inappropriate and unreliable since it is designed on the assumption that all devices within a notional "corporate perimeter" can be trusted. Therefore, a zero-trust architecture, a security model that always verifies individual resources (e.g., people and devices) without respect to location is becoming essential. Under zero trust, each of the devices connected to a network is authenticated and monitored in real time. Therefore, a zero-trust policy requires an automated and sophisticated security operation. In response to these circumstances, Toshiba Group is taking proactive action to support the evolution of CPS systems through the “Energy × Digital” and “Infrastructure × Digital” strategies.

Toshiba Group’s cyber security vision

With the recent progress of digitization in many areas of industry and society, the targets of cyberattacks are expanding to include control systems and devices for social infrastructure, exposing them to the increasing risk of cyber-induced physical contingencies such as cyber hijacking and forced shutdown. Under these circumstances, the mission of Toshiba Group is to provide greater support than ever before for its customers’ business and society and help realize a safe and secure sustainable society. To fulfill this mission, it is essential to accurately assess the convenience of digital technologies and the risk of cyber threats and accordingly shift the focus from conventional protection-oriented security measures to sustainable security solutions encompassing both information and control systems.
To keep up with the evolution of digitization, Toshiba Group is endeavoring to step up cyber security not only for internal information systems and production systems at its factories and other facilities but also for its products, systems, and services offered to customers. Its initiatives are aimed not only to enhance security via security by design* at the design and development stages but also to predict and be prepared for security risks at the operational stage by constantly monitoring internal and external security threats. Toshiba Group quickly responds to security incidents to minimize damage and expedite business recovery in the event of an incident. We also emphasize “security lifetime protection,” a concept stressing the importance of sustainable security that incorporates the evaluation and verification of up-to-the-minute security threats and their countermeasures as well as feedback to the design and development processes of products and services.

*Security-by-design: A product development approach that focuses on security at the planning and design stages



Security Lifetime Protection

To realize this, Toshiba Group defines cyber security management as a series of organically connected processes from six perspectives: 1) Governance, 2) Design & Protection, 3) Prediction & Detection, 4) Response & Recovery, 5) Evaluation & Verification, and 6) Personnel. Toshiba Group has set its goals as “Toshiba Cyber Security Visions” from these perspectives. To attain these goals, we endeavor to enhance our cyber security initiatives so as to remain a trusted partner for our customers through the provision of our products and services.

Governance	Continuously increasing the maturity level of cyber security management through PDCA cycles
Design & Protection	Proper implementation of product and system development processes to prevent vulnerabilities
Prediction & Detection	Real-time detection of internal and external security threats that could affect Toshiba Group or its products
Response & Recovery	Prompt minimization of damage and swift business recovery in the event of security incidents
Evaluation & Verification	Evaluating and verifying products and systems so as to be prepared to respond to new vulnerabilities
Personnel	Training and enhancement of necessary security personnel

Toshiba Group’s cyber security vision

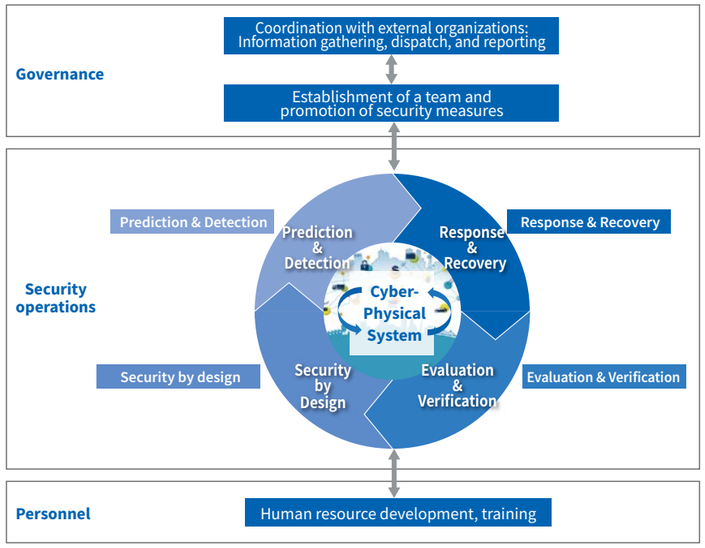
In order to put these goals into practice, starting with consideration of security governance, we began by establishing Toshiba Group's Chief Information Security Officer (CISO) in November 2017. CISO assumes full responsibility for the management of cyber security risks and facilitates decision-making for grave security incidents that could affect business management. A chain of command was defined so that CISO can promptly provide precise directions for group companies.

At the same time, Toshiba Group established the Cyber Security Center, which consolidates the CSIRT*1 responsible for addressing security risks concerning information assets and personal data stored in in-house information systems and the PSIRT*2 responsible for managing security risks concerning products, systems, and services provided by Toshiba Group. The CSIRT and PSIRT cooperate to ensure that all systems at Toshiba's factories and other facilities are properly secured. The Cyber Security Center strives to enhance the cyber security governance of Toshiba Group, incorporating security rules into in-house regulations, establishing security management systems at group companies, addressing cyber security vulnerabilities at the product development and post-shipment stages, and standardizing the risk evaluation policy. In addition, the Cyber Security Center provides a single channel of contact for security-related organizations in Japan and abroad while group companies have a point of contact for liaison with the Cyber Security Center, promoting the sharing of internal and external information.

To strengthen security operations such as prediction & detection, response & recovery, and protection, the Cyber Security Center is currently developing a security management platform called the Cyber Defense Management Platform (CDMP)*3. The purpose of CDMP is to increase the accuracy and expediency of security risk detection and response and thereby enhance cyber resilience. The CDMP is designed to automate the "prediction and detection" and "response and recovery" processes and actively use threat intelligence*4 in order to minimize the impact of security risks on corporate activities.

In April 2019, Toshiba Group established the Cyber Security Technology Center at the Corporate Research & Development Center, where in-house security experts are gathered to enhance security technologies. The roles of the Cyber Security Technology Center encompass R&D, technical support, and implementation assistance regarding cyber security technology.

In order to develop security personnel across Toshiba Group, Toshiba Group provides education on information security, personal data protection, and product security for all employees with the aim of enhancing security consciousness. In addition, Toshiba Group endeavors to improve security quality at the product development stage while offering education and qualification programs designed to develop security personnel responsible for dealing with security incidents.



Cyber security management framework

The following sections describe the specific measures that we are currently implementing in relation to governance, security operations, and human resource development.

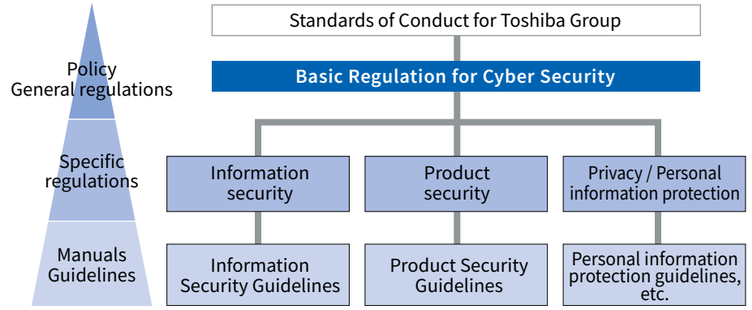
*1 Computer Security Incident Response Team
*2 Product Security Incident Response Team
*3 CDMP: Cyber Defense Management Platform
*4 Threat intelligence: A collection of information about cyber threat trends and cyberattacks by hackers that supports decision-making concerning cyber security

Governance

To promote consistent Group-wide measures against risks related to Toshiba Group's information systems, our products, systems, and services (hereinafter collectively referred to as "products"), and privacy and personal information protection, we have established the Basic Regulation for Cyber Security, under which we have established rules for information security, product security, privacy, and personal information protection.

Basic policy

Toshiba Group properly manages cyber security risks that could have a severe impact on corporate management and have a management system in place that is designed to cope with various types of cyberattacks. In addition, Toshiba Group endeavors to maintain social trust and establish supply chains that enable a stable supply of high-quality products by cultivating a corporate culture that prioritizes safety and security and providing thorough protection of information about customers, suppliers, and individuals.



Toshiba Group's regulations related to cyber security

Basic policy on information security management

Toshiba Group regards all information, such as personal data, customer information, management information, technical and production information handled during business activities, as its important assets and adopts a policy to manage all corporate information as confidential information and ensure that the information is not inappropriately disclosed, leaked, or used. Given this, Toshiba has a fundamental policy "to manage and protect such information assets properly, with top priority on compliance." The policy is stipulated in the chapter "Corporate Information and Company Assets" of the Standards of Conduct for Toshiba Group, and managerial and employee awareness on the same is encouraged.

Basic policy on product safety and product security

In keeping with the Standards of Conduct for Toshiba Group on Product Safety and Product Security, Toshiba Group endeavors to comply with relevant laws and regulations, to ensure product safety and product security, and to proactively disclose reliable safety information to our customers. Furthermore, we continually research safety-related standards and technical standards (UL Standards*1, CE Marking*2 ,etc.) required by the countries and regions where we distribute products and display the safety compliance of our products by the relevant standards and specifications.

*1 UL standards: Safety standards established by UL LLC (Underwriters Laboratories Inc.) that develops standards for materials, products, and equipment and provides product testing and certification
*2 CE marking: A certification mark that indicates conformity with the safety standards of the European Union (EU). The CE marking is required for products sold within the European Economic Area (EEA).

Privacy policy

Toshiba Group protects personal data obtained from its stakeholders during business activities appropriately in accordance with the Personal Information Protection Act, the related laws and regulations, national guidelines, and other rules, recognizing that personal data is an important asset for each stakeholder and an important asset for Toshiba, leading to the creation of new value. In addition, Toshiba Group endeavors to implement, maintain, and continually improve its personal data protection management system as per in-house regulations.

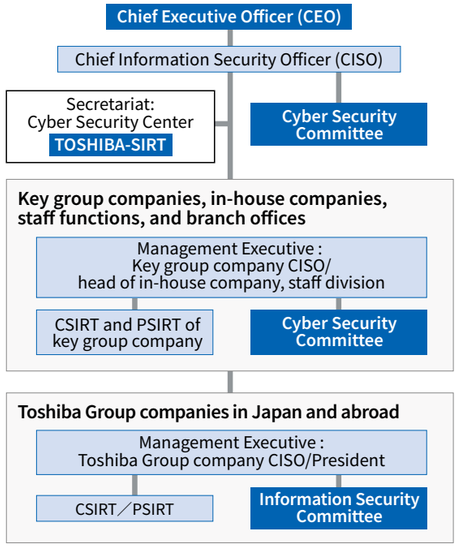
Toshiba's privacy policy: https://www.global.toshiba/ww/privacy/corporate.html

Management system

To promote cyber security measures, Toshiba Group has established a cyber security management system under the direction of the CISO. The TOSHIBA-SIRT*1 assists the CISO in reviewing the following matters to be discussed by the Cyber Security Committee: the basic policy, project team, and action plans for the cyber security management of the entire Toshiba Group and how to respond to cyber security incidents that could develop into a major crisis. The TOSHIBA-SIRT, which has the functions of both CSIRT and PSIRT, supervises the cyber security measures of the entire Toshiba Group and provides support for all group companies in Japan and abroad.

Each key group company overseeing other subsidiaries also has a CISO, who is responsible for the implementation of security measures consistent with those of Toshiba Group and the establishment of a cyber security management system for the company. The CISO of each key group company assumes the responsibility for its own cyber security and that of the domestic and overseas subsidiaries operating under its umbrella. The CSIRT of each company is responsible for implementing information security measures and responding to information security incidents whereas the PSIRT is responsible for implementing product security measures and responding to product vulnerabilities. The Cyber Security Committee*2 discusses matters necessary for the implementation of cyber security measures at key group companies and how to respond to cyber security incidents that could develop into a crisis.

*1 SIRT: Security Incident Response Team
*2 : In some cases, other committees perform the same functions.

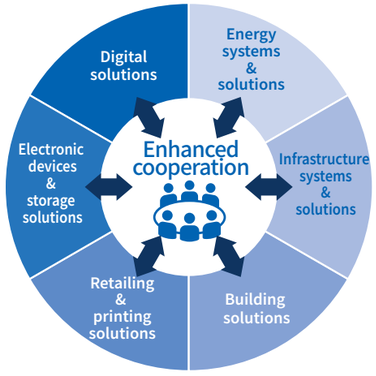


Cyber Security Management Structure

Toshiba Group CISO meetings

Toshiba Group holds quarterly Toshiba Group CISO meetings where the CISOs of key group companies formulate and review its cyber security policies and measures. Toshiba Group operates in a wide range of industrial sectors, including energy, social infrastructure, electronic devices, and digital solutions, and the cyber security measures required for each of these are not necessarily uniform. Therefore, at the Toshiba Group CISO meeting, we discuss cyber security strategies and policies common to the entire Toshiba Group while the CISOs of key group companies share the initiatives and issues of each group company to help resolve their respective issues.

To combat increasingly sophisticated cyberattacks, key group companies are enhancing cooperation to strengthen the overall cyber security capabilities of Toshiba Group.



Global security governance system

A worldwide security assurance framework for the entire Toshiba Group is becoming increasingly important in promoting business globally. In reality, Toshiba Group experienced a security incident in which an attack against one of its overseas subsidiaries affected a subsidiary in another country.

Toshiba Group has a cyber security management system to facilitate the implementation of cyber security measures (page 10). Toshiba Corporation communicates security instructions to all its subsidiaries via key group companies to ensure that they are properly implemented. Each key group company is responsible for the cyber security of itself and all the subsidiaries operating under its umbrella.

As opposed to the hierarchical cyber security management system, the Security Operation Center (SOC) and Toshiba PSIRT provide centralized monitoring of and response to cyber threats against internal IT infrastructure for all group companies in Japan and abroad. They perform correlational analysis of all the incidents affecting internal IT infrastructure while collecting all the information concerning security incidents, thereby facilitating early detection of and response to security incidents.

In addition, some regions and countries are tightening laws and regulations concerning information security and personal information protection, sometimes making it necessary to employ different measures tailored to their specific requirements. Therefore, Toshiba Group keeps track of the related laws and regulations around the globe so as to be able to adapt to any legal and regulatory changes promptly.

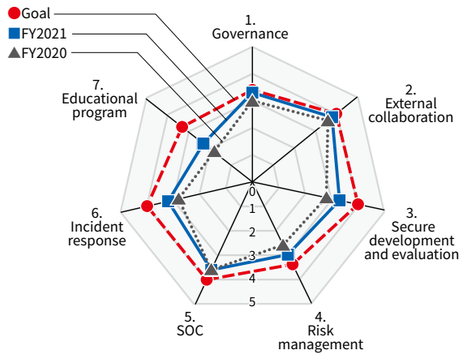
Self-assessment of cyber security management maturity

To enhance the cyber security management level, Toshiba Group sets maturity goals and performs self-assessment designed to elevate the level of goal management. Maturity assessment is intended to visualize the gaps between current conditions and goals so that each group company can implement countermeasures to steadily improve its cyber security management maturity.

We assess both the information security level of the CSIRT and the product security level of the PSIRT. The basis of this assessment includes the SIM3*1 maturity model that is widely used worldwide, the Cybersecurity Management Guidelines of the Ministry of Economy, Trade, and Industry (METI) of Japan, and the Cybersecurity Framework of the U.S. National Institute of Standards and Technology (NIST*2). Maturity levels are graded on the scale of 1-5 in respect to 1) governance, 2) external collaboration, 3) secure development and evaluation, 4) risk management, 5) SOC, 6) incident response, and 7) educational program.

Since 2020, we have expanded the Self-Assessment of Cyber Security Management Maturity to include Toshiba Group companies outside Japan, and have been pressing forward with the strengthening of cyber security management systems overseas.

*1 SIM3: Security Incident Management Maturity Model
*2 NIST: National Institute of Standards and Technology



Results of cyber security management maturity self-assessment

Activities for raising cyber security awareness

Endorsing Cybersecurity Month observed by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) of Japan, Toshiba Group observes February as Cybersecurity Month. The CISO of Toshiba Group delivers a message for Cybersecurity Month, focusing on cyber security trends of the year, including considerations for information security and the security measures for the products that Toshiba Group ships. To raise the security awareness of employees, we also post this information on the in-house web portal.
To ensure cyber security, it is crucial to keep track of the latest trends and share information among all parties concerned. Therefore, we have formed a community to disseminate and share information, including domestic and international news on cyber security, vendor reports, news releases from industry associations, media reports about national policies, and press releases.


This message will be sent to employees of all Toshiba Group overseas companies.

To employees of Toshiba Group companies

A business email compromise? First, suspect that it is.
Next, consult with your colleague or superior and check with the sender.

Stay alert! Are the sender's name and email address legitimate?

Consult! Did you talk to your colleague or superior about the suspicious email?

Check! Did you call the sender or send a new email to the address that you know is legitimate?

Yutaka Sata, General Executive and CISO
Toshiba Corporation

February - Cybersecurity Month

Toshiba Group endorses initiatives by the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) to raise cybersecurity awareness, and we observe February as Cybersecurity Month. Every employee is requested to understand that threats to cybersecurity are increasing, that cyberattacks are becoming more sophisticated, and to pay closer attention to cybersecurity.

1. Introduction
In our turbulent world, cyberattacks on governments and businesses are an ever-growing threat. We should all be aware of this, more concerned about cybersecurity, and prepared for any emergency. As February is Cybersecurity Month, I ask you to review your cybersecurity practices.

Message for Cybersecurity Month from CISO (Excerpt)

Donation of “The Poop Cyber Security Workbook,” in collaboration with Bunkyosha, to public elementary schools throughout Japan

As part of our activities for raising awareness of the threat of cyber risks lurking around us and the importance of cyber security to prevent them, Toshiba Group has collaborated with the publishing company Bunkyosha Co., Ltd. to create “The Poop Cyber Security Workbook, supported by TOSHIBA”*1 that allows children to learn about cyber security in a fun way, which we have made available on our website.*2 We also made this workbook into a booklet and donated approximately 83,000 copies to public elementary schools around Japan to raise children’s awareness of security issues.
In recent years, with cyberattacks increasing at an alarming pace, the need for people to protect themselves with cyber security is being emphasized like never before. In this workbook, we have adopted themes that are familiar to children to help them recognize the significance of cyberattacks that endanger them and understand the cyber security that can protect them against such attacks. In the workbook, the character Unko Sensei presents special lessons to help children understand the necessity of cyber security. In addition, the workbook introduces “hackers for justice (white hat hackers)” who protect society from cyberattacks, and promotes the role and importance of the security industry. Through this workbook, Toshiba Group is helping to raise children’s security awareness, protecting them from the threat of cyberattacks, and working to realize a safe and secure Internet society.

*1 The Poop Workbook Series: A series of children’s workbooks published by Bunkyosha Co., Ltd. since March 2017. These workbooks are designed to lower the hurdles of learning with the keyword “poop,” a magic word that makes children happy just by saying it, so that they can learn while having fun. Since 2020, the publishers have been developing educational workbooks, booklets, Internet apps, and videos on a variety of topics in collaboration with various companies, administrative agencies, local governments, and other organizations.
https://unkogakuen.com/books
*2 The Poop Cyber Security Workbook: Scheduled to be released by February 14, 2024
https://www.global.toshiba/jp/cybersecurity/corporate/unkodrill.html

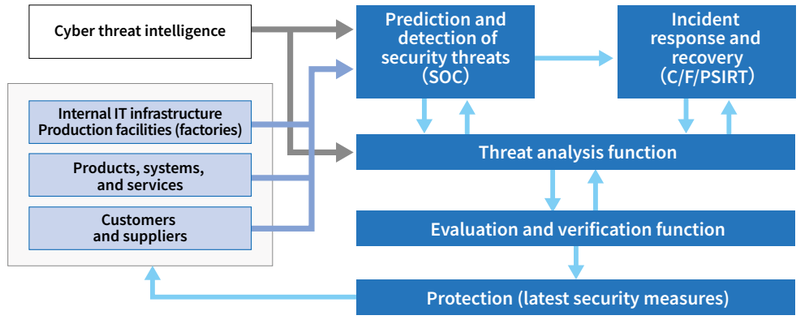
Security Operations

This section describes the initiatives undertaken by Toshiba Group to enhance its security operations. At present, Toshiba Group is developing a security management platform called the CDMP*1 with the aim of increasing the accuracy and expediency of security risk detection and response in order to enhance its cyber resilience. The CDMP is designed to automate the “prediction and detection” and “response and recovery” processes and actively use cyber threat intelligence*2 in order to minimize the impact of security risk on corporate activities.

*1 CDMP: Cyber Defense Management Platform
*2 Cyber threat intelligence: A collection of information about cyber threat trends and cyberattacks that supports decision-making concerning cyber security

CDMP overview

We believe that the purpose of the CDMP is to protect not only internal IT infrastructure, but also production facilities such as factories and the products provided to customers, and in the future this will be extended to include customer and business partner systems that share connections with these.
Specifically, the CDMP provides the functions shown below, some of which commenced operation in January 2019.



Cyber Defense Management Platform (CDMP)

•SOC：Security Operation Center
•C/F/PSIRT：Computer/Factory/Product Security Incident Response Team

The CDMP consists of the following functions:

- Prediction and detection of security threats (SOC)
  ⇒ Detecting security incidents by monitoring system states (see page 18)
- Incident response and recovery (C/F/PSIRT)
  ⇒ Responding to security incidents and recovering the affected systems (see pages 14, 20, 26)
- Threat analysis function
  ⇒ Preventing cyber threats by using threat intelligence (see page 23)
  ⇒ Improving the analysis accuracy by accumulating knowledge and using artificial intelligence
- Evaluation and verification
  ⇒ Evaluating and verifying products and systems from the hackers’ perspective (see page 21)
- Protection
  ⇒ Protection using state-of-the-art security measures (see page 22)

The threats in cyberspace are constantly growing. Since resources for responding to these threats are limited, Toshiba Group is endeavoring to automate the response to and the recovery from security incidents while accumulating knowledge and using AI to achieve high-accuracy security operations with limited resources. In regard to automation, we are promoting the introduction of an automation platform called SOAR,*1 on which we are utilizing threat intelligence, and we are progressing with automation of incident investigation and response.
In addition, we are promoting new initiatives such as developing a dashboard to enable the CISO, CSIRT, and PSIRT personnel of each group company to grasp the security incidents and response status within their companies and help them respond promptly, and utilizing ASM*2 solutions to identify those IT assets open to the public that are at risk of cyberattacks.

*1 SOAR: Security Orchestration, Automation and Response
*2 ASM: Attack Surface Management

Information security incident response training

The purpose of information security incident response training is to minimize the impact of incidents on business by ensuring the smooth sharing of information and appropriate response flow among relevant departments when an incident actually occurs. As an example of response training, imagining that a PC has become infected with malware, the PC that is assumed to be infected is actually isolated from the network, its logs are checked, and we verify whether communication between related organizations is properly carried out according to the predetermined response flow for when an incident occurs. We take the findings and issues learned from this training and utilize them in the next training, and we continue to promote initiatives to achieve cyber resilience, such as conducting training that includes overseas group companies and follow-up education.

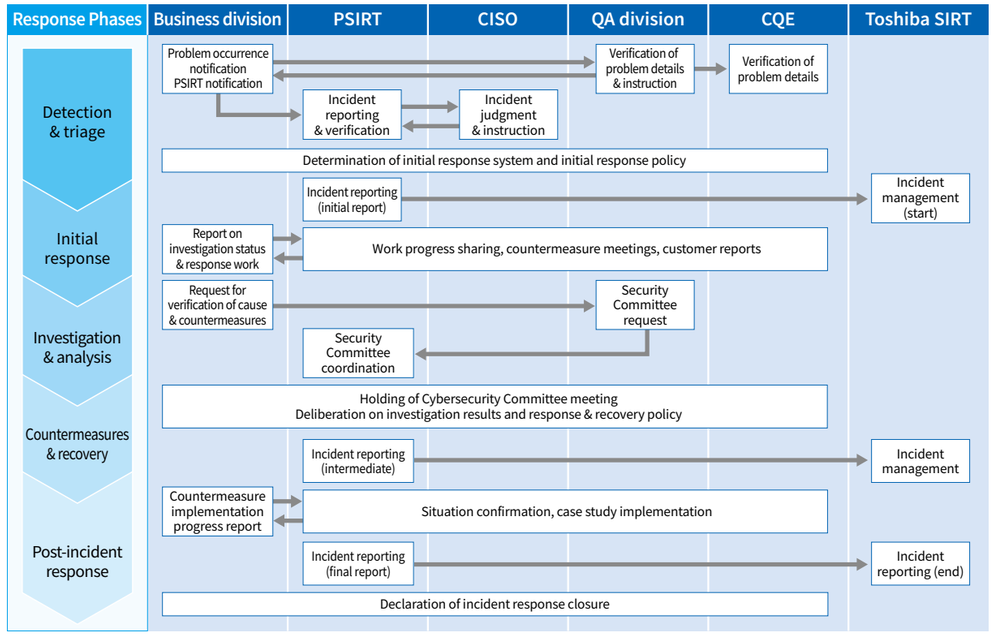
Product security incident response training

Product security incident response training is conducted to confirm whether systems and flows, such as information sharing, communication pathways, decision points, and advance preparations, are in place to appropriately respond to actual incidents. The purpose is to improve those systems and flows through training and to minimize the impact of security incidents on business. For training, in regard to products that may encounter security incidents and the nature of those incidents within business divisions, we first create response scenarios that include communication methods, flows, and target times in the event of an incident, in accordance with the rules of Toshiba and its key Group companies. After that, we carry out communications and mock meetings according to the scenario, measure the implementation time, and identify points for improvement in the response system and flow. By repeating such training, we can verify that the response system and status of establishing the response flow are adequate.
The EU Cyber Resilience Act, published on 15 September 2022, includes time constraints in its vulnerability response requirements, such as mandated reporting to ENISA* within 24 hours of becoming aware of an actively exploited vulnerability or occurrence of a security incident. It is expected that these requirements will be included in the laws of other countries at some point in the future, and so it is essential to confirm the status of establishing a response system.
In light of these circumstances, in the future, we plan to increase the number of training organizations, including overseas subsidiaries, and expand the scope of training to include more departments and relevant parties with related roles.

* The European Union Agency for Cybersecurity

Incident response training: Implementation example

As an example, this section will describe the details of a training which was held in Toshiba Digital Solutions Corporation, one of our Group companies. Toshiba Digital Solutions is not only providing digital solutions in the fields of manufacturing, logistics & distribution, finance & insurance, media, power & social infrastructure, but also provides digital solutions to the government and municipal offices.
During a response of an incident, there are three important things: 1. Get the correct information, 2. Share these information with the relevant person/departments, 3. Prioritize the response activities. If there is something wrong with the product or service which was provided to a customer, a notification will be sent from the business division to the QA division. If this problem is related to a product security incident, for example, if it was caused by a cyberattack, it's necessary to contact PSIRT*1 as well.
At this time, the training covered the whole Response phases in the following figure. Each of the relevant departments—the business division, the QA division, PSIRT, CISO*2, CQE*3, and Toshiba SIRT (Cyber Security Center)—participated in this training. Additionally, we created a scenario of all necessary procedures from past experiences. Each department checked about their roles in this training, and all of the participants executed the procedures following the scenario. An outline of the departments and the flow of procedures is as below.



Outline of departments participating the product security incident response training and the flow training procedures

Through the questionnaire of this training, there are many comments shows the effectiveness of the training. Such as "It was an opportunity to experience my own role in an incident response," and "Although there was a scenario, I still think it's important to practice in real" and "I keenly felt the necessity of changing the target departments and conducting regular training exercises."
It is not enough for a single Business division to conduct training just once. Rather, it is important to repeatedly conduct training that involves other Business divisions. We will take the findings and issues learned from this training and utilize them in the next training.

*1 PSIRT: Product Security Incident Response Team
*2 CISO: Chief Information Security Officer
*3 CQE: Chief Quality Executive

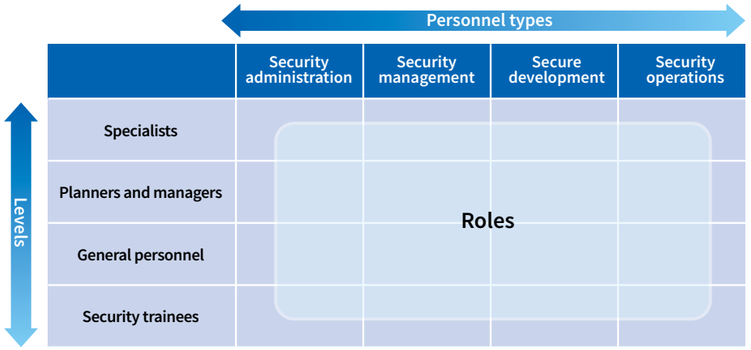
Human Resources Development

This section describes Toshiba Group's programs for the development of cyber security personnel. Our initiatives are threefold: 1) defining personal qualities required for security personnel, 2) provision of security training programs based on this definition, and 3) a security certification program to qualify the employees who possess the required knowledge, expertise, and practical skills in the field of cyber security.

Personal qualities required for security personnel and security certification program

For each combination of security personnel level*1 and security personnel type*2, the roles that must be fulfilled are defined in terms of the personal qualities required for security personnel. Toshiba Group also has a security certification program to certify such security personnel. Certification criteria include attendance of designated internal and external security education courses, acquisition of Registered Information Security Specialist certification or other security-related certifications, and suitable job experience for performing the defined role. To date, roughly 2,000 employees have received certification.

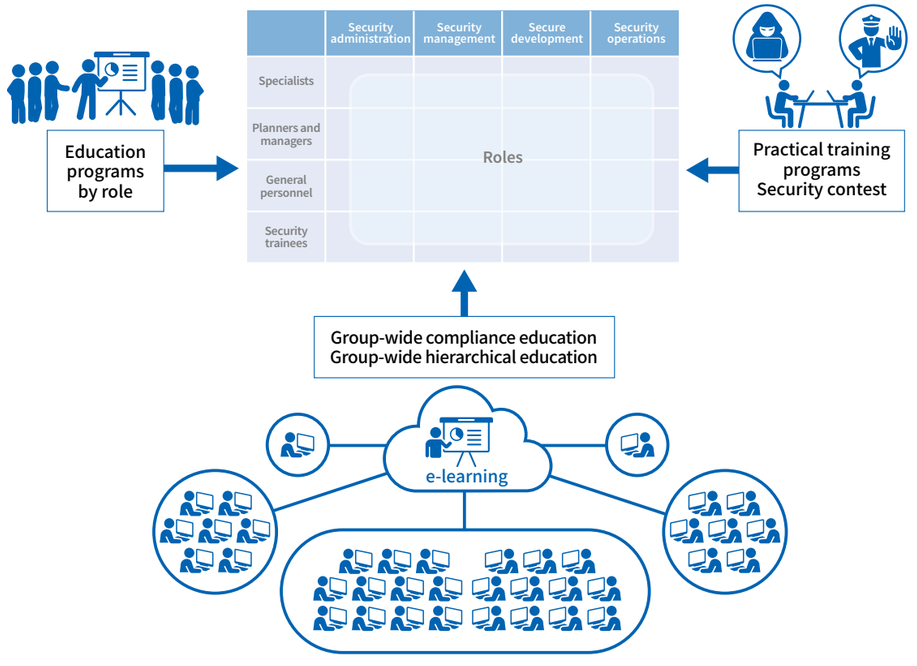
*1 Security personnel level: Ranges from specialists who possess advanced skills to security trainees, including personnel with added security knowledge (personnel whose main job responsibilities do not explicitly include security measures, but who have sufficient cyber security literacy to engage in the type of work that entails security risk unless sufficiently secured).
*2 Security personnel type: Classified into business administration, management, development, and operations concerning cyber security (see Skill Standards for IT Professionals [ITSS], compiled by the Information-technology Promotion Agency, Japan [IPA]).



Qualities required for security personnel

Security education programs

In order to prevent information leakage, each employee must acquire the knowledge necessary to properly handle the information encountered in daily work and be keenly aware of security threats such as targeted attacks and security considerations for teleworking. Additionally, to ensure the security of products provided to customers, all employees involved in products, such as sales, procurement, design, development, quality, and maintenance personnel, must understand the seriousness of product security vulnerabilities. Furthermore, personnel must understand the importance of preventing the introduction of vulnerabilities at the product development stage and promptly addressing security vulnerabilities found in products that have already been shipped, and must put this understanding into practice. Therefore, to raise the security awareness and literacy of each and every one of our personal, we conduct annual Group-wide compliance education training (information security/personal information protection and product security education) for all executive officers and employees of Toshiba Group. These training programs are available in multiple languages for overseas employees. We also provide personnel with hierarchical education programs at career milestones, such as when they join the company or when they receive a promotion, according to their various roles.
In addition, Toshiba Group also provides education and training corresponding to the various roles defined according to the personal qualities required for security personnel. Toshiba Group also conducts e-learning courses on the basics of information and product security, the importance of supply chain security, threat analysis, and secure development techniques. Other training programs include hands-on training to help personnel acquire practical skills for vulnerability testing, training courses to develop specialists and highly skilled personnel capable of responding to vulnerabilities and security incidents promptly, and product security courses for managers responsible for improving security quality at the time of product development. We also send personnel to external practical training programs, such as the Core Human Resource Development Program offered by the Industrial Cyber Security Center of Excellence (ICSCoE) of the Information-technology Promotion Agency of Japan (IPA).
Furthermore, we carry out several other initiatives such as training programs designed to promote the use of acquired knowledge and skills in daily work (e.g., incident response training) and a security contest for Toshiba Group employees that aims to introduce, spread, and strengthen security-related skills. This security contest has been held annually since 2020 and has approximately 70 participants from various departments each year. It is conducted as a quiz-style contest in which participants strive to answer problems prepared by the organizer, and it is becoming established as an opportunity to acquire and test security skills.



Privacy Governance* Initiatives

Toshiba Group provides data services. Public demand for privacy protection is growing as the utilization of personal data expands.
Prior to the launching of a business using personal data, Toshiba Group has established a system and rules for the identification and evaluation of privacy risks. Minimizing privacy risks is crucial for using personal data for business purposes. Toshiba Group will also educate its employees on privacy protection in order to raise their awareness about privacy.

Publication of privacy statement

Through our data service business, Toshiba Group is implementing a strategy to turn that data into forms that have value and realize our vision of a society in which people can effectively utilize that data in their various activities beyond the framework of business operations, etc.
Based on this strategy, Toshiba has established and released the "Toshiba Group Privacy Statement" in anticipation of our proactive use of data in future Group business operations and in our efforts to strengthen governance of personal data. This statement declares our management stance regarding the use of personal data in our data service business.

Privacy statement

https://www.global.toshiba/ww/cybersecurity/corporate/privacystatement.html

External advisory board on privacy

Toshiba has an external advisory board on privacy consisting of external, independent specialists in order to receive advice from a neutral and fair perspective.

* Privacy governance: Establishing and implementing a system for proper management of privacy risks and organizational efforts for privacy issues

Personal Data Protection

Toshiba Group protects personal data obtained from its stakeholders in the course of business activities appropriately, recognizing that personal data is an important asset of each stakeholder and also an important asset for Toshiba, leading to creation of new value.

Establishment of in-house regulations and a management system, and education

To properly manage and handle personal data, Toshiba has established the Toshiba Personal Data Protection Program. Its group companies have also established similar programs. To observe and implement the rules defined in the regulations, the cyber security management system composed of all divisions of the company is promoting personal data protection (see page 10). Toshiba also educates all officers, regular employees, and temporary staff every year about the handling of personal data and safety management practices.

Identification and management of personal data

To identify personal data owned by each organization, Toshiba maintains and periodically checks and updates its personal data management database. We assess the risks involved based on the contents and volume of personal data and manage them accordingly. We also conduct a self-audit concerning personal data protection and take corrective action if any improvements are required.

Selection and supervision of outsourcees entrusted with the handling of personal data

When the handling of personal data is contracted out, the outsourcer will be held responsible for inadequate supervision of the outsourcee in the event of leakage of any personal data. After cases of data leakage from outsourcees were reported in the press, protection of personal data became a social issue. Since then, outsourcers have been required to supervise outsourcees. Toshiba Group stipulates the rules and guidelines for the selection of outsourcees so that only those capable of properly safeguarding personal data will be selected. Toshiba Group periodically ensures that personal data are properly managed and handled by outsourcees.

Compliance with Overseas Laws and Regulations

In recent years, many countries have enacted or revised legislation on personal data protection. In Toshiba Group, regional headquarters in the United States, China, Europe, and Asia are spearheading compliance activities according to the business risks involved.

Compliance with the General Data Protection Regulation (GDPR)

In order to comply with the EU GDPR, Toshiba's regional headquarters in Europe and other Toshiba Group companies implement various measures, including employee education, establishment of in-house regulations, and data mapping. Following the withdrawal of the United Kingdom from the EU, the transition period ended at the end of December 2020. Prior to the end of the transition period, European subsidiaries and Japanese group companies of Toshiba Group concluded the Toshiba Intra-Group Data Sharing Agreement (IGDSA) in October 2020 in order to establish a contractual basis for the cross-border sharing of personal data.

Compliance with China's Personal Information Protection Law (PIPL)

After the China Cyber Security Law that came into effect in June 2017, China enforced the Data Security Law (DSL) in September 2021, followed by the Personal Information Protection Law (PIPL) in November 2021. In response, Toshiba's regional representative subsidiary in China is collecting information about the new laws while developing templates for in-house regulations, contracts, and training materials to be provided for the local subsidiaries.

Compliance with Thailand's Personal Data Protection Act (PDPA)

In Thailand, the Personal Data Protection Act (PDPA) came into effect in June 2022. To ensure that local subsidiaries comply with the PDPA, Toshiba's regional representative subsidiary for the Asian region has created templates for in-house regulations, contracts, and training materials and provided them for the local subsidiaries.

Cyber Security Initiatives

In order to enhance cyber security, Toshiba has consolidated information and product security functions that were separately promoted before. This chapter describes Toshiba Group's initiatives for enhancing cyber security, divided into security measures for internal IT infrastructure and security measures for products. Here, internal IT infrastructure includes factories and other production facilities in addition to PCs, servers, networks, and other equipment within Toshiba Group.

Security Measures for Internal IT Infrastructure

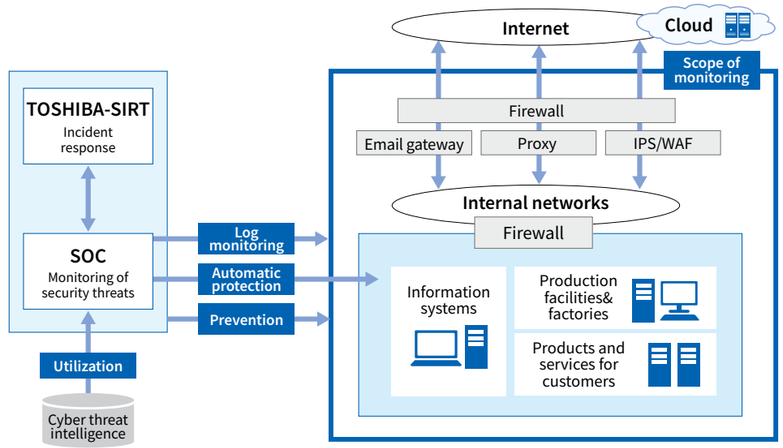
As cyberattacks are becoming increasingly sophisticated and ingenious, Toshiba Group is committed to proper management of customers' information assets. At Toshiba Group, the SOC is responsible for the prediction and detection of security threats while the CSIRT is dedicated to the response to and recovery from cyber security incidents. In addition, all the organizations of Toshiba Group in Japan and abroad perform an annual self-audit and security assessment and receive guidance.

Enhancing Prediction and Detection

Prediction & Detection

Previously, Toshiba Group prioritized the deployment of firewalls, intrusion prevention systems (IPS), and proxies at the Internet gateway to prevent attackers from breaching an internal network because all information assets to be protected used to be located only in the internal network. However, in view of the increasing reliance on public cloud services as a means of improving work efficiency and promoting work style innovation, the boundary between internal and external networks is becoming obscure. In addition, cyberattacks have shifted from random attacks on mass targets to targeted attacks on one specific organization designed to steal its confidential information or disrupt its business, exposing enterprises to an increased risk of cyberattacks. Under these circumstances, Toshiba Group is strengthening the following measures to detect security risks promptly and accurately and respond to them immediately:

- Expanding the scope of monitoring to cover not only IT systems but also factories and customer services
- Detecting not only external cyberattacks but also the internal spread of cyber intrusions and suspicious activities
- Standardizing and automating responses in the event of an alert being detected
- Risk-based security management using external threat intelligence



Security prediction and detection provided by the SOC

- SIRT (Security Incident Response Team): Has both CSIRT and PSIRT functions
- SOC (Security Operation Center): An organization that monitors networks and devices 24/7/365, detects and analyzes cyberattacks, and provides advice about how to respond to them
- Firewall: A security barrier that controls communication ports to prevent software from performing unintended communications
- Gateway: Hardware or software that interfaces one network to another
- Proxy: A computer system that acts as an intermediary for communications between the Internet and an internal network
- Intrusion prevention system (IPS): A device or software that detects and blocks an intrusion into an internal network
- Web application firewall (WAF): A form of firewall that detects and blocks cyberattacks attempting to exploit vulnerabilities of Web applications

Enhancing the Security of Endpoints*1 Using EDR*2 Tools

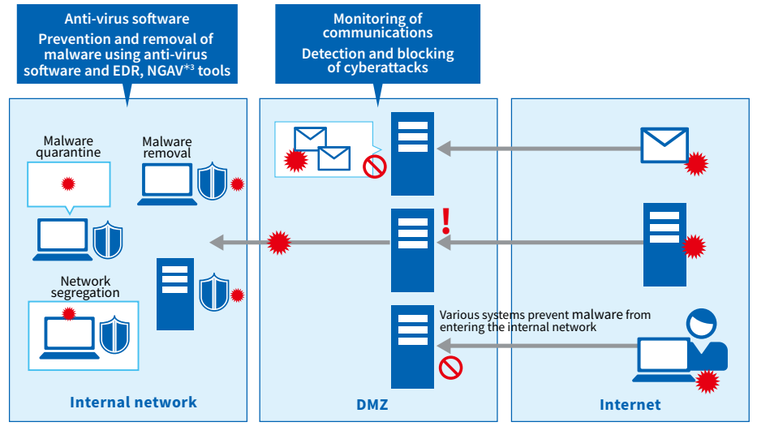
Prediction & Detection

Toshiba Group is installing EDR tools on all PCs and servers in Japan and abroad, which are capable of detecting and blocking unknown malware that cannot be blocked by antivirus software as well as sophisticated cyberattacks that cannot be detected at the Internet gateway.

Introduction of EDR tools

- Detecting and blocking suspicious behavior of endpoints due to the infection of unknown malware that cannot be detected by existing anti-virus software
- Ability of the SOC to remotely quarantine the infected computers without disconnecting them from a network and remove security threats
- Tracking the causes and scope of damage from the collected operating log
- Using external threat intelligence to grasp endpoint vulnerabilities and implement countermeasure

*1 Endpoints: PCs, servers, and information devices connected to a network
*2 Endpoint detection and response: Detection of and response to security threats at endpoints

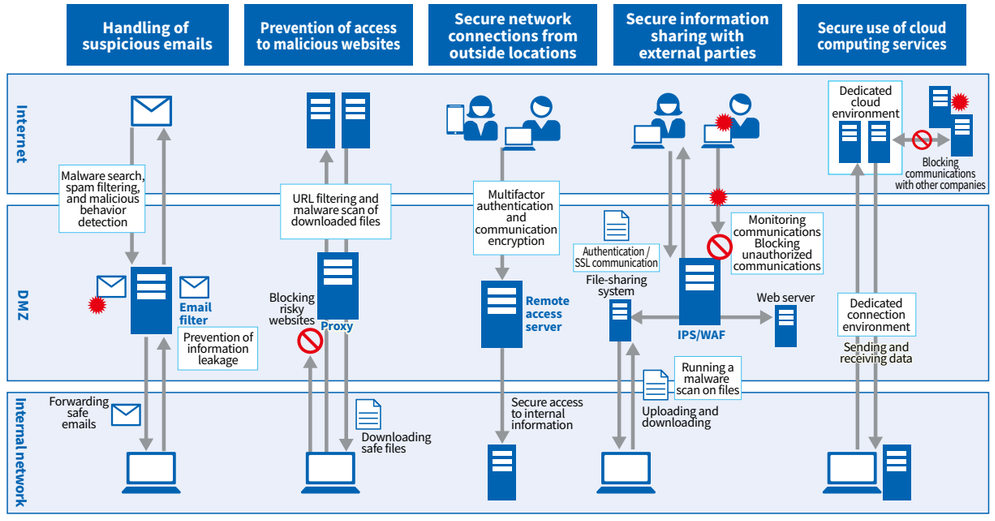


Introduction of EDR tools

- NGAV (Next Generation Anti-Virus)
- DMZ (demilitarized zone): A subnetwork added between an organization's secure internal network and an untrusted external network such as the Internet

Security Measures for Internet Connection Points

Toshiba Group observes tens of millions of attempted cyberattacks per day. To detect and block cyberattacks, Toshiba Group has security devices such as Web application firewalls (WAFs) and intrusion prevention systems (IPS) at the interface between internal and external networks. This section describes our countermeasures for various security risks implemented at the Internet connection points.



Security measures for Internet connection points

- DMZ(demilitarized zone): A subnetwork added between an organization's secure internal network and an untrusted external network such as the Internet
- Proxy: A computer system that acts as an intermediary for communications between the Internet and an internal network
- Intrusion prevention system (IPS): A device or software that detects and blocks an intrusion into an internal network
- Web application firewall (WAF): A form of firewall that detects and blocks cyberattacks attempting to exploit vulnerabilities of Web applications
- Spam: Unsolicited junk emails sent in bulk

Handling of suspicious emails

Toshiba Group uses protective measures for both external cyber threats from virus-infected emails and internal threats of information leakage. To counter the inflow of harmful malware from an external environment, Toshiba Group employs behavior detection, sender domain authentication, and spam filtering to execute email attachments and email-embedded links in a safe environment. Consequently, Toshiba Group blocks hundreds of thousands of suspicious emails per day. In order to prevent information leakage from inside, Toshiba Group has implemented a tool to encrypt email attachments and prevent erroneous email transmissions, and has implemented email monitoring for external domains.

Preventing access to malicious websites

Toshiba Group uses proxy servers to reduce the risk of accessing malicious websites on the Internet while employing a malware checker and a URL filter and monitoring logs to prevent access to such websites. In the event of suspicious network activity, the computer concerned is identified from an access log. If access to particular websites is necessary for work purposes, it is permitted via user authentication so that access restrictions do not impede business.

Secure network connections from outside locations

Toshiba Group provides salespersons and those on business trips with an environment that allows their PCs and smartphones to securely connect to the internal network via the Internet at hotel rooms and elsewhere. Multifactor authentication is used to prevent unauthorized access while all user communications are encrypted. In addition, virtual desktops are utilized for telework and working from home (WFH) as a means of promoting work style innovation.

Secure information sharing with external parties

Toshiba Group makes the most use of websites to share and disseminate information to external parties. Access control and malware scanning allow us to securely exchange files with customers and suppliers. Our websites and servers that allows public access are subjected to periodic security assessment while security measures are promptly implemented to check for vulnerabilities and protect against increasing cyber threats.

Secure use of cloud computing services

As cloud computing services are increasingly employed to improve work efficiency, the risk of information leakage, unauthorized access, and wrong settings increases. To alleviate this risk, Toshiba Group has established a secure private cloud environment in order to protect sensitive information from various threats. To use public cloud services, users are required to submit an application. We permit the use of public cloud services only when their security policy meets our requirements. Toshiba Group periodically checks whether there are any changes to the service features and methods used.

In addition to these common security measures, the operating sites that have their own Internet connection points monitor the settings and logs of security devices. For protection from cyberattacks, Toshiba Group employs not only common measures but also additional measures according to the importance of business and information. At present, these measures are primarily designed for information systems. In the future, we will leverage such expertise to enhance the security of our factories and customer services.

Security Incident Response

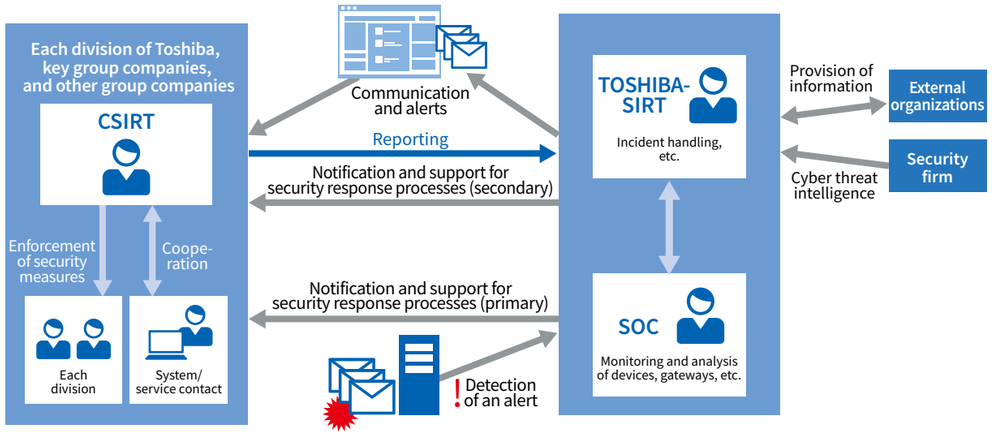
Response & Recovery

As per the cyber security management system, a CSIRT* is organized in each division of Toshiba, key group companies, and all the subsidiaries operating under their controls worldwide so as to be prepared to respond accurately and promptly in the event of a security incident. When an alert is detected, the SOC directly notifies the CSIRT of each division and group company of the alert in order to respond promptly while acting in concert with the TOSHIBA-SIRT.

*CSIRT: Computer Security Incident Response Team

Roles of the CSIRT

The CSIRTs of the division and of the group company supervising a given system are responsible for dealing with the security vulnerabilities and incidents involving that system. They ensure the implementation of various security measures to fix vulnerabilities and other issues and respond to security incidents in cooperation with IT and manufacturing departments. The TOSHIBA-SIRT is responsible for coordinating with each CSIRT to ensure that various security measures are properly implemented across the entire Toshiba Group and for minimizing damage in the event of a security incident. In particular, the TOSHIBA-SIRT deals with security incidents involving email and other shared systems, provides support for each CSIRT, and addresses security incidents that require cooperation of multiple divisions.



Outline of the security incident response procedure

Security Incident Response

Security incidents include website tampering, targeted emailing, spam influx, unknown malware infection, and malware spreading. For all types of potential security incidents, the TOSHIBA-SIRT has predefined response procedures, which are continually reviewed and improved through training and actual response to security incidents. After dealing with a security incident, the TOSHIBA-SIRT identifies its root cause and implements an improvement measure to prevent recurrence of similar incidents.

Automation initiatives

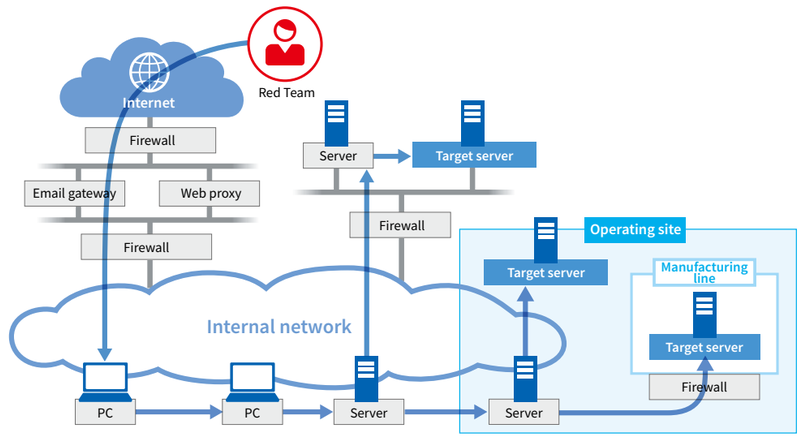
To respond 24/7/365 to vulnerabilities and incidents promptly and accurately, Toshiba Group is now automating the response to vulnerability information, cyber threat intelligence, and security alerts. We have categorized security information and alerts and developed routine response patterns, ensuring that any security incident can be handled by anyone, anytime. Furthermore, our automation initiatives include analyzing the relationships among the detected security alerts and cyber threat intelligence, identifying the root causes of the alerts, and establishing optimum response procedures.

Advanced Attack and Penetration Assessment from Hacker's Perspective

Evaluation & Verification

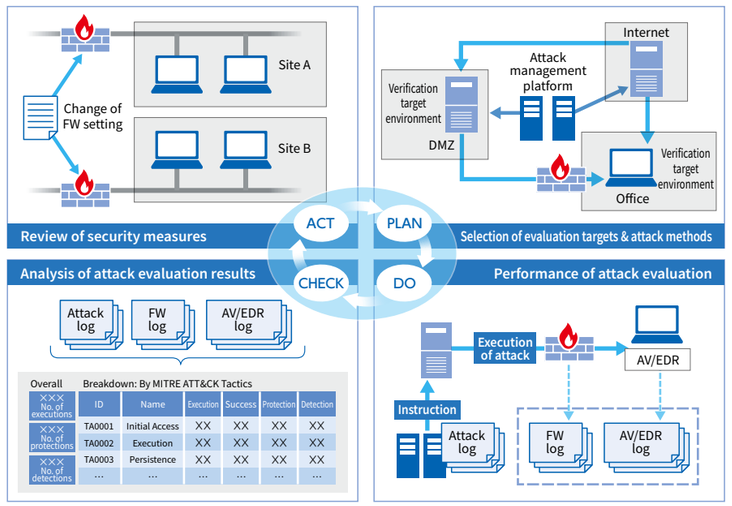
Targeted attacks focused on stealing customer or confidential information from a specific company or organization are increasing. In the face of these increasingly sophisticated cyberattack threats, Toshiba Group regularly undergoes attack and penetration assessment by the Red Team*1 of a specialized cyber security firm and examines security measures using attack (BAS*2) tools in order to validate the effectiveness of our security measures.
In this attack and penetration assessment, the Red Team attempts to infiltrate Toshiba Group's network using the same advanced tactics and techniques of actual hackers, in order to determine whether it is possible to reach a predetermined target server through a simulated attack. This also allows us to verify the effectiveness of the current security measures, identify potential weaknesses to cyberattacks, and consider additional measures.

*1 Red Team: An independent team that provides real-world attack simulations designed to assess the effectiveness of security systems and measures of an organization
*2 BAS: Breach and Attack Simulation



Outline of attack and penetration assessment

In the use of attack simulation tools, simulated cyberattacks equivalent to those in the real world are carried out between devices in the verification target environment, the examiners check whether security measures such as network security and endpoint security work properly, and we verify the effectiveness of Toshiba Group's security measures and make improvements.

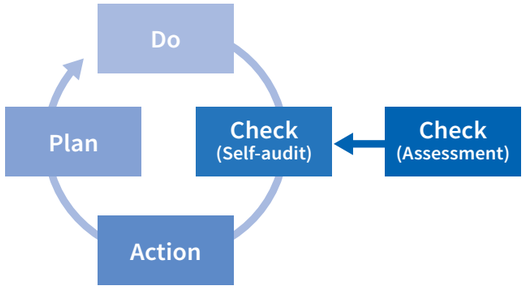


AV: Antivirus, EDR: Endpoint Detection and Response, FW: Firewall

Self-Audit and Security Assessment

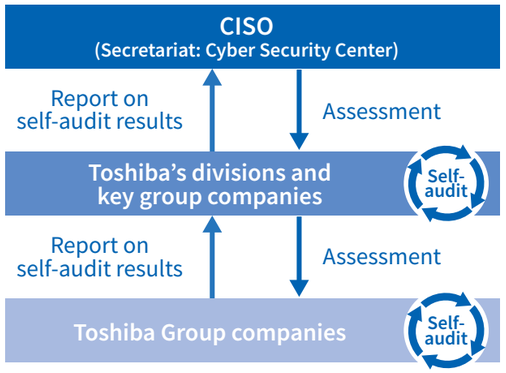
Evaluation & Verification

As Toshiba Group operates in various business sectors, it is important for each division to establish an iterative PDCA cycle on its own in order to ensure the information security of the entire group. Therefore, each division conducts a self-audit every year to determine whether it conforms to the internal rules and endeavors to correct problems, if any.



PDCA cycle based on a self-audit and assessment

The Cyber Security Center (secretariat) assesses the results of the self-audit and improvement activities of each division and provides guidance and support if corrective action is necessary. Toshiba Group companies in Japan and abroad conduct a self-audit every year. The Cyber Security Center assesses its results from a third-party perspective to evaluate its validity so as to help enhance the information security level of each group company.



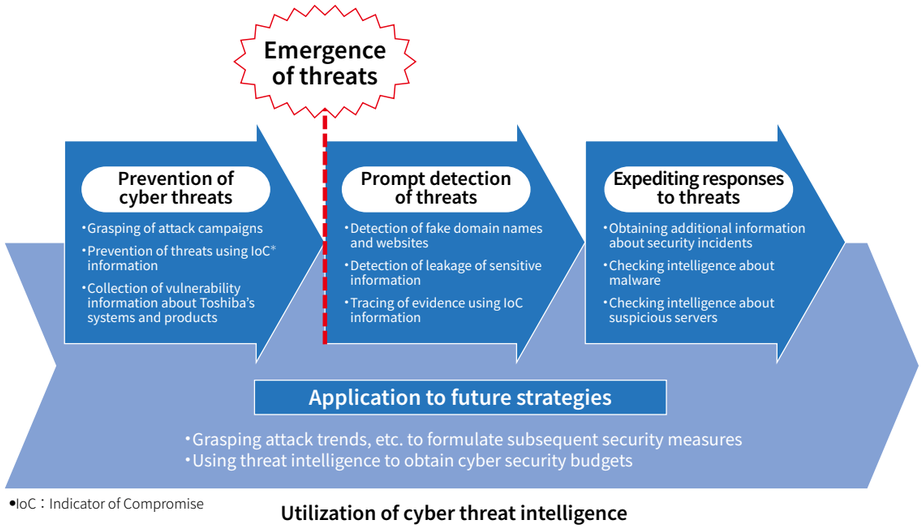
Self-audit and assessment conducted by the entire Toshiba Group

Utilization of Cyber Threat Intelligence

Prediction & Detection / Security by design / Response & Recovery / Evaluation & Verification

Toshiba Group actively utilizes cyber threat intelligence to enhance the sophistication of its security operations. Threat intelligence collectively refers to all types of intelligence data about attacks by hackers, trends in cyber threats, security vulnerabilities, etc. that can be used for the prevention and detection of cyber threats. Toshiba Group obtains cyber threat intelligence from various sources, including public organizations and external threat intelligence service providers.

We utilize such threat intelligence to analyze possible impact on Toshiba Group and its urgency and employ proxies, firewalls, EDR tools, etc. as necessary. Threat intelligence helps prevent cyber threats to Toshiba Group and to promptly detect and respond to cyber threats if they materialize. In addition, we use intelligence about cyberattack trends to formulate future security strategies.



•IoC：Indicator of Compromise

Utilization of cyber threat intelligence

Security Measures for Products, Systems, and Services

Toshiba Group engages in various initiatives to ensure the security quality of the products we provided to our customers. In addition, Toshiba Group has established a product security incident response team (PSIRT) system to promptly respond to vulnerabilities found in its products in cooperation with external organizations.

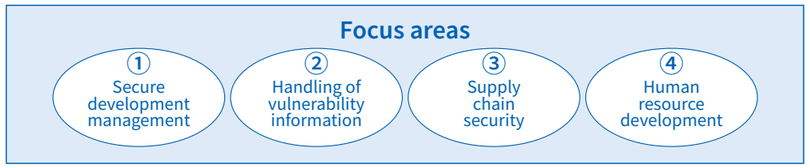
Initiatives for Enhancing Product Security

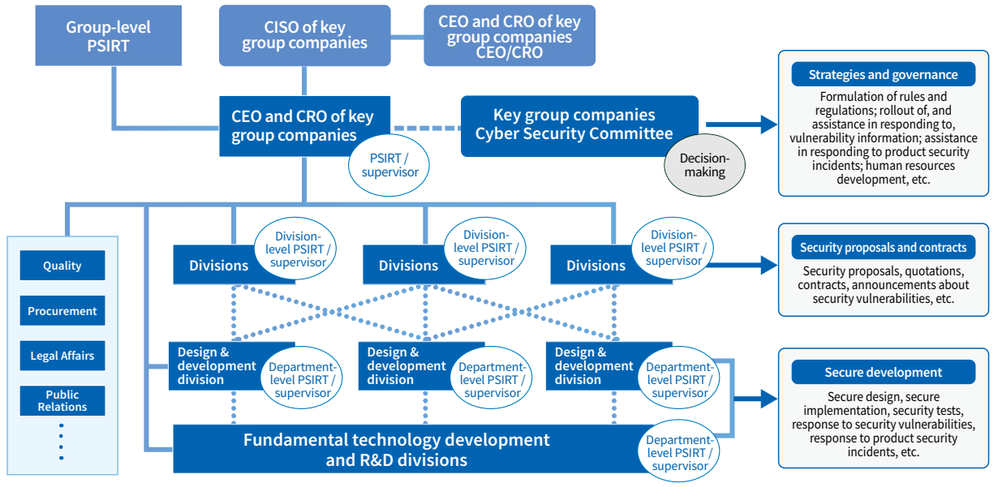
Security by design

In order to ensure the security of the products we provide to our customers, we have established a product security management system as part of our cyber security management system. Under this product security management system, the PSIRT collaborates with quality assurance and procurement departments to ensure the security of product development processes as well as the security of third-party products used in Toshiba Group's products.

Devising plans to enhance product security preparedness

Toshiba Group has redefined four focus areas to strengthen its product security, considering the recent trends in product security and the situation of Toshiba Group, while setting mid-term objectives and visualizing the extent of their achievement. Based on this definition, Toshiba Group has devised plans to enhance its product security preparedness according to risk-based priorities. Toshiba's product security management system covers all group companies. This product security management system makes it possible to effectively communicate group-wide measures to all business units and product design and development divisions of each group company while endeavoring to achieve autonomous operations of each group company promptly.

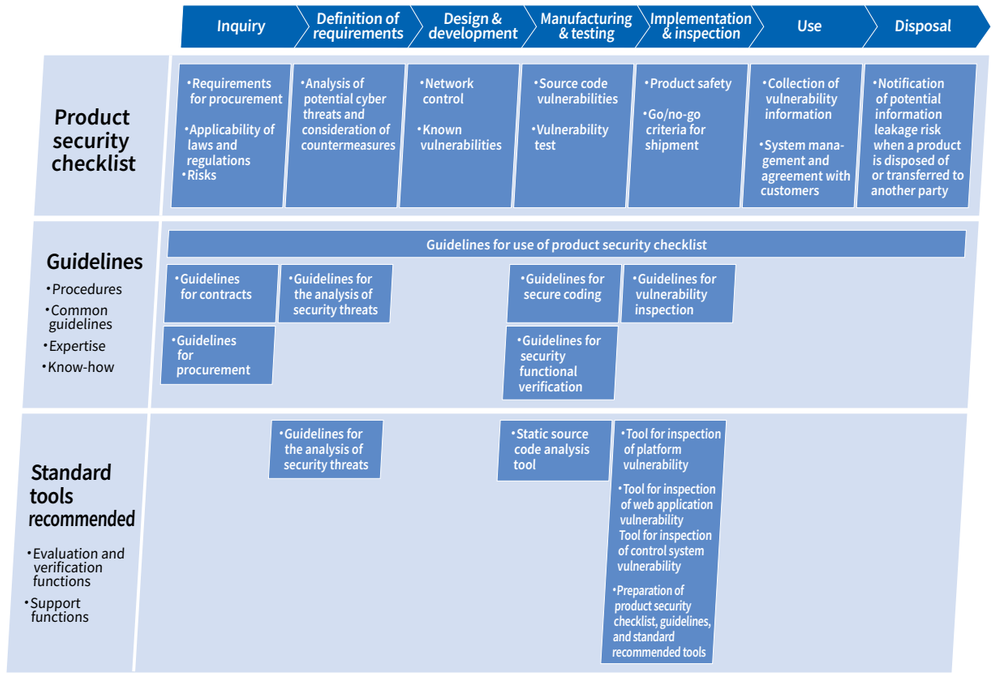




Product security management system

Preparation of product security checklist, guidelines, and standard recommended tools

Toshiba Group is preparing product security checklists that summarize the security requirements to be checked at each product development stage as well as common guidelines and standard recommended tools for Toshiba Group corresponding to each of the checklists. They serve to remind product developers not to miss anything that should be considered in terms of security and help ensure consistent security responses regardless of differences in the experience, expertise, and proficiency of individual staff members. As part of the menu of evaluation/verification functions, Toshiba Group will provide the standard recommended tools and related support services that will come in handy when going through the checklists.



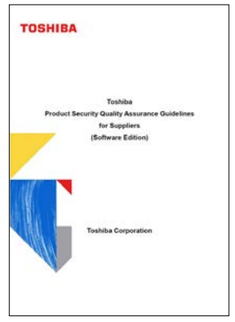
Initiatives to strengthen product security in the supply chain

In collaboration with business partners, Toshiba Group develops a wide variety of products, including social infrastructure products, and provides them to customers. Once an incident occurs in a product, it can have a major impact not only on customers, but also on society as a whole. In order to ensure product security, we believe it is important to implement risk-based operations and carry out security measures across the entire supply chain, including our business partners.

In order to objectively judge the security risks of products, we have defined the "Criteria for Security-Critical Products" for determining whether they have potential to develop into major crisis risks that will greatly impact society, such as products for critical infrastructure as defined in the "Cybersecurity Policy for Critical Infrastructure Protection" established by the National center of Incident readiness and Strategy for Cybersecurity (NISC) and products that handle personal information, and we have made it a rule to assess products according to these criteria at the time of procurement.

We are also preparing security guidelines to help suppliers understand Toshiba Group's approach to product security and to solicit their cooperation in ensuring the provision of secure products. These guidelines define specific security requirements for suppliers in three areas: 1) supplier's security management system, 2) software product development deliverables, and 3) outsourced operation services. By providing these guidelines to suppliers from the moment of entering into business relations with them, we make clear the security requirements of Toshiba Group.

Through these efforts, Toshiba Group is working to strengthen product security throughout the entire supply chain.



Toshiba Product Security Quality Assurance Guidelines for Suppliers (Software Edition)

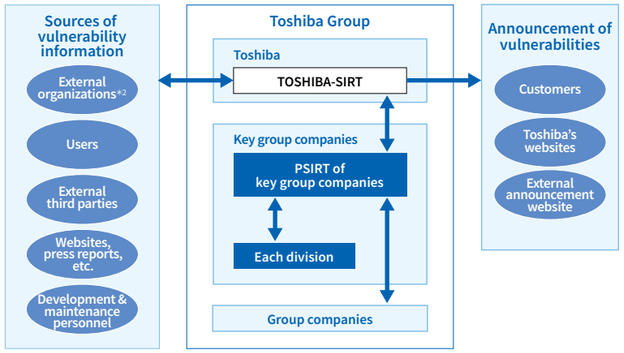
Prompt and Reliable Response to Security Vulnerabilities

Response & Recovery

Toshiba Group has a product vulnerability response system in place to provide a prompt and consistent response to vulnerability information, contributing to reducing the business risk of customers using its products, systems, and services. As a member of the Information Security Early Warning Partnership established as per the Standards for Handling Software Vulnerability Information and Others, a directive of the Ministry of Economy, Trade and Industry (METI) of Japan, Toshiba Group actively collects vulnerability information in cooperation with external organizations. In June 2021, Toshiba Group joined the Common Vulnerabilities and Exposure (CVE®)*1 program as a CVE Numbering Authority (CNA) so as to be able to respond to vulnerabilities found in its products more promptly.
In addition, Toshiba Group has established the Product Security Risk Handling Manual, in-house regulations that describe specific procedures for handling vulnerability information so that vulnerability information is dealt with in a consistent manner across Toshiba Group. We also provide all employees with an e-learning program to raise their awareness of security throughout the product life cycle.

Vulnerability handling system

The TOSHIBA-SIRT is responsible for handling information about the vulnerabilities of the products, systems, and services offered by Toshiba Group. The TOSHIBA-SIRT serves as a sole channel of contact for internal and external parties regarding the handling of vulnerability information. The TOSHIBA-SIRT provides prompt and consistent responses to vulnerability information in cooperation with the PSIRT of key group companies of the Group. If any vulnerability could have a severe impact on customers' businesses, Toshiba Group announces and deals with the vulnerability in an appropriate manner, taking social impact into consideration.

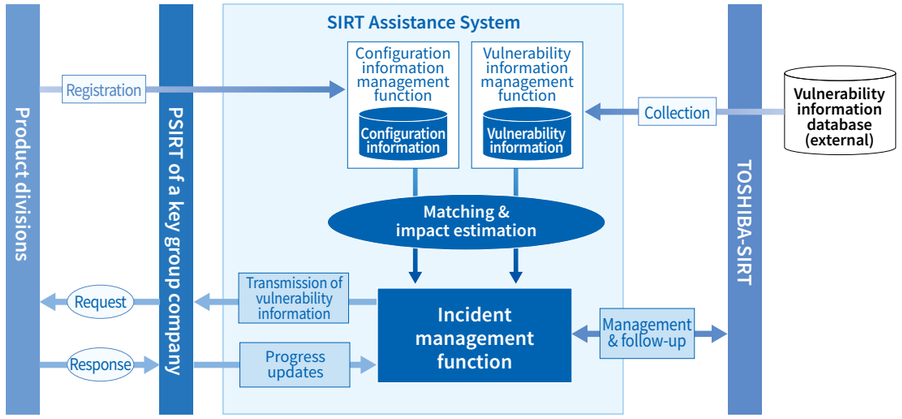


Toshiba Group's vulnerability handling system

*1 CNA: An organization that assigns CVE IDs to the vulnerabilities found in a predefined range of products and publishes CVE Records on these vulnerabilities
http://www.cve.org/About/Overview
*2 External organizations: JPCERT/CC, JVN, ICS-CERT, etc.

Vulnerability handling process

When vulnerability information is received from an external source, the key group company concerned needs to identify the affected products, determine the level of impact, and accordingly take necessary action. To cope with ever-increasing product vulnerabilities, Toshiba Group has developed the SIRT Assistance System, leveraging its expertise in vulnerability handling. Product divisions utilize this system with the aim of providing prompt and reliable handling of vulnerability information.



Summary of the SIRT support system

Offering of Secure Products, Systems, and Services

To meet the security requirements in the fields of energy, social infrastructure, electronic devices, etc., Toshiba Group provides various products, systems, and services for cybersecurity.

Cybersecurity training service for energy businesses

Toshiba Energy Systems & Solutions Corporation

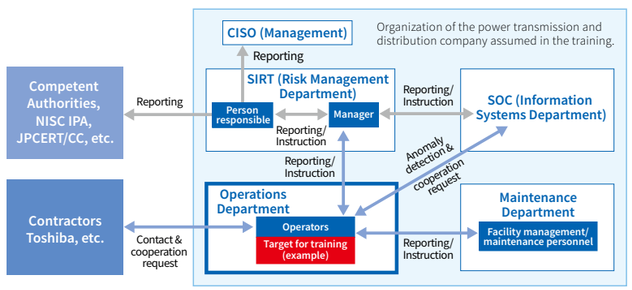
Previously, control systems for critical infrastructure such as electricity, gas, and water supply were designed and operated as closed networks that were physically separated from office networks, and since customized communication protocols are often adopted, cybersecurity is something that has been considered unrelated to these systems. In recent years, however, with the expansion of the networking on these control systems, the adoption of standard protocols, and the rapid advances in information and communication technology, the scope of cyberattacks[*1,*2] has expanded to include such control systems. For control systems, integrity and availability are vital to ensure stable and reliable operation of system ; and so, in addition to responses and countermeasures to prevent cyberattacks, it is necessary to minimize the impact in the event of a cyberattack and to recover as soon as possible.

To this end, we have developed a security training system for infrastructure operators to help them respond to cyberattacks on control systems (Figure 1). This training system uses a control system simulator to allow operators and supervisors in the operation department to experience what a cyberattack on the control system looks like. Assuming the organization shown in Figure 2, through inter-organizational communication between the operations department, the risk management department (Security Incident Response Team [SIRT]), the information systems department (Security Operation Center [SOC]), and the maintenance department, we monitor and analyze threats to the system, and provide training on how to respond to cyberattacks, identify and eliminate the causes, and recover from cyberattacks. By using a simulator, our training system can implement various scenarios such as DoS attacks and ransomware with the possibility of accidents and failures, without the actual control system (Figure 3). Trainees can actually experience what it is like to deal with various types of cyberattacks that haven't been realized without a simulator before, and can learn how to respond to incidents in a precise and organized manner.

We will continue to promote the provision of services using this training system to operators in the energy sector, expand the incident scenarios that strengthen SIRT and SOC response training, and strive to provide wide-ranging contributions to human resource development such as improving security knowledge and incident response capabilities.

*1 Large-scale blackouts caused by cyberattacks on electric power companies
*2 Gas pipeline shutdowns due to ransomware attacks

(Figure 1) Security training system



(Figure 2) Example of an operator's organizational structure (in the case of power transmission and distribution)

(Figure 3) Trainees' action in the training

IoT security solution: CYTHEMIS™

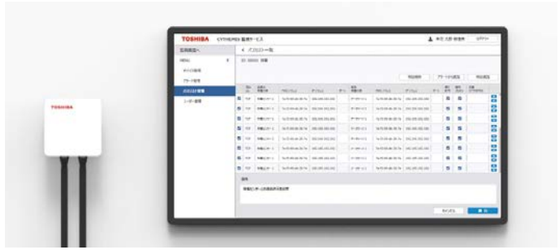
Toshiba Infrastructure Systems & Solutions Corporation

In addition to the IoT networking of factories, the use of the IoT has been increasing recently in R&D fields, as typified by materials informatics, a field of study in which cloud computing is used to accelerate and improve the efficiency of the R&D of materials as the IoT helps enhance the analysis capability and facilitate the shared use of measurement data and research systems. Since the COVID-19 pandemic has made teleworking the new norm for all employees, it has become essential to connect research systems to a network. However, unlike typical PCs, many of the PCs that control the research systems are customized, making it difficult to add new security measures to them or update their operating system. In this case, it is necessary to simply forgo the networking option or use a USB memory or other device to move data between two research systems, thereby degrading the efficiency of R&D work. In response to these circumstances, Toshiba Infrastructure Systems & Solutions Corporation has developed CYTHEMIS™, a solution that enables secure networking of such research systems and thus facilitates the use of the IoT.

CYTHEMIS™ is a packaged solution that consists of small external devices connected to a network and a centralized management system. These small devices act as a firewall for each research system to ensure secure communication. They filter network communications between research systems, provide two-way authentication, encrypt the transmitted data, and let through only the authorized network traffic to the permitted destinations. Since these devices block unauthorized network traffic, they prevent the lateral movement of malware within the enterprise network even in the event of intrusion and thus protect research systems with potential vulnerabilities. Research systems could also be infected with malware during maintenance work. Even in that case, the centralized management system and external devices cooperate to prevent the malware from spreading from the infected system. In this respect, CYTHEMIS™ plays the role of an external endpoint detection and response (EDR) tool. From the perspective of a network administrator, CYTHEMIS™ can be regarded as a solution that enables previously unnetworkable systems to be networked without modifying the existing network environment while minimizing the workload required for security management.

At first, CYTHEMIS™ can be used simply to transfer data within a closed environment and use research systems remotely. The use of CYTHEMIS™ can subsequently be expanded to use the cloud or collaborate with external parties just by modifying the settings of the management system.

When IoT and CPS systems become the norm, it will become essential to ensure exact mirroring of data between cyber and physical spaces and identify the entity at the other end of a communication. Instead of protecting the boundary of a network, CYTHEMIS™ authenticates all the entities involved to secure each communication, thereby contributing to the realization of a society where IoT and CPS systems are widely used.



CYTHEMIS™

Implementation of security features in storage products

Toshiba Electronic Devices & Storage Corporation

In recent years, with the growing demand for personal data protection, the importance of information security of storage products is increasing. Toshiba's hard disk drive (HDD) product lineup includes not only products for personal mobile devices, but also products designed for various fields, such as products for digital multifunction printers (MFPs) and enterprise products for data centers and other operations. We provide HDDs with appropriate information security technology to meet the needs of each field.

Security requirements for storage products include protection and deterrence functions to prevent data leakage due to theft or loss of HDDs. A function for completely erasing all data is also required to prevent data leakage after disposal.

To meet these customer requirements, we develop and provide self-encrypting drives (SEDs). Our high-capacity, high-performance nearline HDDs for cloud data centers automatically encrypt and store data when they are input. For data encryption, we use AES*1, a standard encryption algorithm established by the US National Institute of Standards and Technology (NIST). Our HDDs also support access control functions using the ATA*2 Security Feature Set (for ATA devices), TCG*3 Opal SSC*4, and TCG Enterprise SSC to prevent acquisition of protected data without password authentication. These functions achieve data protection and leakage prevention.

Furthermore, in regard to the complete erasure of data at the time of disposal, our MDDs are equipped with a technology called Cryptographic Erase that can instantly invalidate data cryptographically by changing the encryption key of the data, thereby achieving the invalidation of all data without the need to overwrite it at cost.

The cryptographic algorithm implemented in our HDDs has been certified by the cryptographic algorithm test CAVP*5 (A1637, A1638, A1645) based on the US government's FIPS PUB 140-3, guaranteeing high reliability. Moreover, for our MG09*CP18/16TA*6 products, we are progressing with the acquisition of CMVP*7 certification based on FIPS PUB 140-3, the US government's cryptographic module certification that started in 2020, and a third-party organization carries out multi-faceted evaluation of the entire HDD unit as a cryptographic module in terms of its design, implementation, and operation.

*1 AES: Advanced Encryption Standard
*2 ATA: Advanced Technology Attachment
*3 TCG: Trusted Computing Group
*4 SSC: Security Subsystem Class
*5 CAVP: Cryptographic Algorithm Validation Program
*6 MG09*CP18/16TA: MG09SCP18TA, MG09ACP18TA, MG09SCP16TA, MG09ACP16TA
*7 CMVP: Cryptographic Module Validation Program

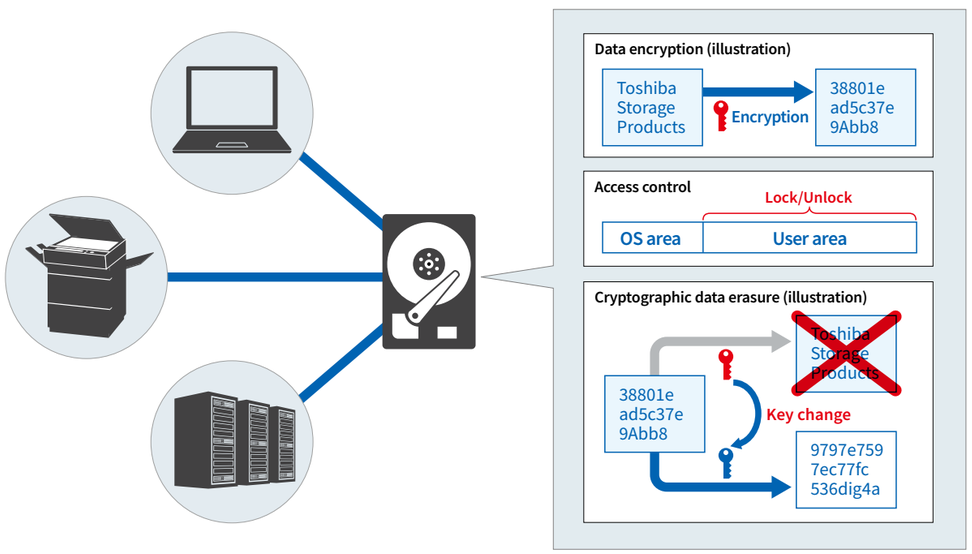


Image of security features in storage products

Cyber security compliance (ISO/SAE 21434) for in-vehicle semiconductor products

Toshiba Electronic Devices & Storage Corporation

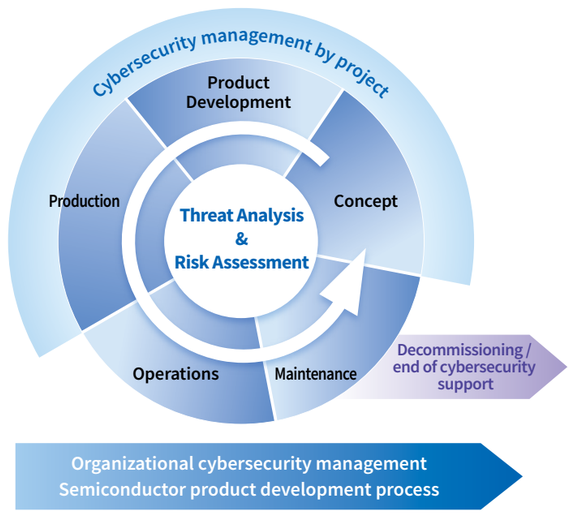
In addition to CASE*1, which is the goal of the automotive industry, as automobiles are being transformed into mobility services, such as the promotion of MaaS*2 occurring primarily in developed countries, and as software is becoming an increasingly prominent aspect of automobile functions, strengthening cybersecurity measures for in-vehicle E/E systems*3 is an urgent issue. In international law, WP.29 of the United Nations Working Group has already approved and enacted regulations for vehicle cybersecurity (UN Regulation No.155 [UN-R155] and No.156 [UN-R156]). These regulations require Cyber Security Management System (CSMS) and Software Update Management System (SUMS) certification in order for automobile manufacturers to get vehicle type approval, and throughout the supply chain, semiconductor suppliers are also required to provide evidence of CSMS and SUMS compliance and explanations of management methods.

CSMS compliance is achieved in large part by complying with ISO/SAE 21434, the international standard for automotive cybersecurity engineering. This standard defines the procedures necessary to achieve sustainable security throughout the entire product life cycle, from planning,*4 through concept, product development, production, operations, maintenance, and decommissioning / end of cybersecurity support, as shown in the diagram below.

We develop and sell semiconductor products for in-vehicle E/E systems such as powertrain, safety, and body systems. Through the establishment of development processes and internal regulations that conform to ISO/SAE 21434, we ensure CSMS compliance for the entire product life cycle of these automotive E/E system semiconductors that we supply, thereby contributing to continuous security risk management for automobiles.

In regard to the development process, using the existing semiconductor product development process ISO 9001 as a base, we have implemented an automotive grade hardware and software quality management process based on IATF 16949 and Automotive SPICE, a functional safety management process based on ISO 26262, and a cybersecurity management process based on ISO/SAE 21434 as an add-on to the other processes, allowing us to achieve seamless cybersecurity support throughout the development process. Our ISO/SAE 21434-conforming development process has been evaluated for compliance with standards by an external agency and we have received certification. We have achieved continuous monitoring of security threats and response to incidents through cooperation with Toshiba Group's CSIRT/PSIRT activities. Going forward, in order to meet SUMS compliance, we will implement development process conformity with ISO 24089, which was officially issued recently, and provide semiconductor products that help to keep automotive systems up-to-date and secure.

*1 CASE = Connected, Autonomous, Shared, Electric
A medium-term strategy used by automakers to transform into mobility service providers.
*2 MaaS = Mobility as a Service; a next-generation mobility service that seamlessly connects conventional public transportation with ride sharing, bicycle sharing, etc. using IT.
*3 In-vehicle E/E systems = automotive Electric/Electronic systems
*4 Cybersecurity plan included in cybersecurity management by project



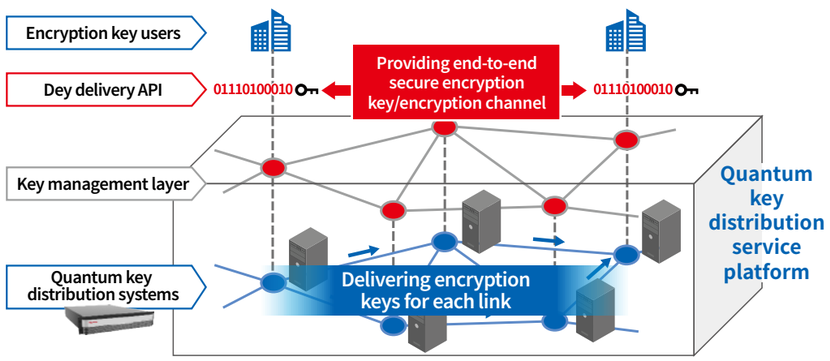
Management of cybersecurity risks throughout the product life cycle

Quantum key distribution system

Toshiba Digital Solutions Corporation

These days, information communication networks such as the Internet have become an indispensable part of our lives. With the ever-increasing spread of IoT, it is likely that we will become even more dependent on such networks.
On the other hand, the development of quantum computers in recent years is remarkable. When large-scale quantum computers emerge at some point in the future, their overwhelming computational power will easily break the encrypted communications now widely used on the Internet and other networks, and there is a danger that important information will be leaked.
Quantum key distribution is a technology designed to combat this problem. This technology is theoretically unbreakable, no matter the speed of quantum computers or any other type of high-speed computer that may emerge. By placing the encryption keys for cryptographic communication on photons, the smallest unit of light, this technology utilizes the principle of quantum mechanics to prevent encryption keys from being leaked during communication.
Toshiba Group has been conducting research on quantum key distribution for more than 20 years, and has constantly been in the lead, setting new world records for cryptographic key delivery speed (i.e., the amount of cryptographic keys that can be sent per unit time). Currently, in multiple cities around the world, we are pressing forward with the demonstration and establishment of a quantum key distribution service that can safely supply cryptographic keys. We are also actively participating in the standardization of quantum key distribution so that secure cryptographic keys can easily be used from various applications.
Going forward, we will continue to expand this system to large-scale networks to provide quantum key distribution services that can be used by many different customers.

Quantum key distribution system

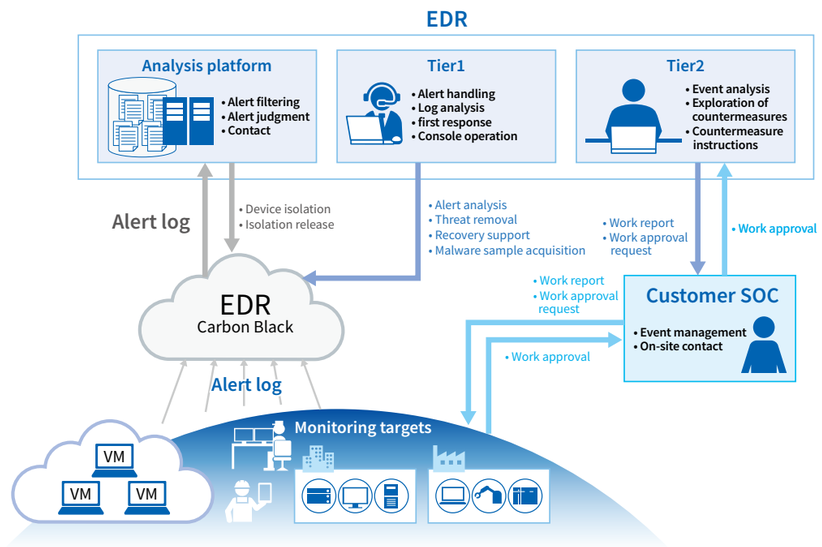


Quantum key distribution service platform

EDR tool Carbon Black and MEDR security operation service

Toshiba Digital Solutions Corporation

In recent years, cyberattacks have become more sophisticated and malicious, and it is becoming increasingly difficult to prevent endpoints, such as personal computers, from being infected with malware and ransomware simply by installing antivirus software.
On the other hand, due to recent changes in work styles, work is now being done in various environments such as with telecommuting and mobile environments outside the office, and the conventional concept of a secure internal network is giving way to the concept of a zero-trust network that does not presuppose a perimeter defense network with firewalls and intrusion detection systems.
In this age of changing circumstances and environment, security measures for endpoints are becoming ever more important in order to prevent leaking of information handled in business and to avoid business interruptions due to malware infection, etc.
In order to detect cyberattacks and malicious intrusions to endpoints in this environment, it is effective to implement Endpoint Detection & Response (EDR) that is able to constantly monitor the behavior of personal computers and other terminals and immediately alert and isolate any suspicious behavior.
As deployed of EDR solution, we have begun handling VMware Carbon Black Cloud, and we are supporting its use in our customers' environments. This tool has been installed in more than 140,000 terminals throughout Toshiba Group, protecting our business and information from various cyberattacks both day and night.
When operating EDR, the large volume of alerts detected by EDR solutions on a daily basis requires efficient identification of problems and appropriate responses based on the latest attack methods and trends.
Through combined use of the Managed EDR (MEDR) service, a security operation service for VMware Carbon Black Cloud, you can operate efficiently with advanced expertise and information.



EDR tool Carbon Black and MEDR security operation service

Payment terminal CT-6100/PICT-6100 series

Toshiba Tec Corporation

The CT-6100/PICT-6100 series, released in December 2022, is a compact and user-friendly payment terminal that integrates a pin pad and a contactless reader/writer. In addition to magnetic cards and contact ICs, payments can be made via touch payment, electronic money, and bar code reading.
In payment services, if attacks on payment terminals lead to the leaking and exploitation of credit card numbers, personal information, etc., not only could users suffer enormous damage, but terminal manufacturers may also face lawsuits for damages and suffer loss of social credibility. It is therefore necessary for payment terminal designs to address these risks. The CT-6100/PICT-6100 series has a carefully devised product structure that makes it difficult to hack and has a tamper detection configuration that can detect unauthorized access to the internal components.
In the payment terminal industry, the PCI Security Standards Council (PCI SSC*1) has established the PCI-PTS*2 security standard in order to publicly certify that appropriate security performance is provided. PCI-PTS stipulates the requirements for software and hardware security functions and product management needed for payment terminals that require personal identification number (PIN) input, and the certification standards are regularly reviewed to keep up with the latest attack methods. As it is best for a payment terminal to comply with the latest certification standards when it is released, PICT-6100 has acquired the latest PCI-PTS certification, V6.0.*3
Furthermore, as our own measures to enhance security, the layout of the button display on the touch panel for entering the PIN code is randomly changed each time, and a privacy screen protector film is used to reduce the risk of other people peeping at the screen. This also eliminates the need for protruding parts to shield the buttons, achieving both security and good design. These enhanced security features ensure that customers can enjoy long-term use of the product with peace of mind.

＊1 Payment Card Industry Security Standard Council
＊2 Payment Card Industry PIN Transaction Security
＊3 At the time of product development

• J-Debit is a registered trademark of NTT Data Corporation and JCB Co., Ltd.
• UnionPay is a registered trademark of CHINA UNIONPAY Co., Ltd.
• CARDNET and JET-STANDARD are registered trademarks of Japan Card Network Co., Ltd.
• Other service names mentioned in the text are registered trademarks of their respective companies.

CT-6100　　PICT-6100

Integrated card reader/writer

e-BRIDGE SKY Suite™ for Service (Portal, Device Management, Meter Collector, AppShowcaseSetting)

Toshiba Tec Corporation

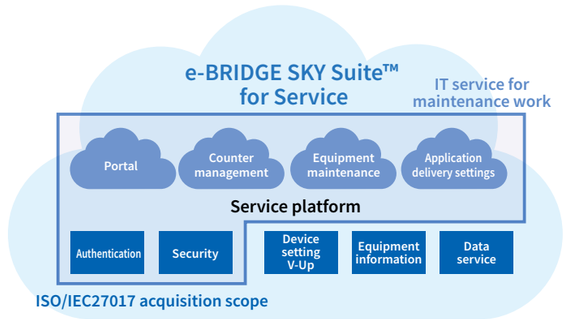
In recent years, improving the efficiency of device management and maintenance services has become an issue for digital multifunction peripherals (MFPs). e-BRIDGE SKY Suite™ for Service (hereinafter referred to as eSS for Service) is a cloud service designed to solve this issue. Customer data is collected daily from the MFP via our cloud connection service, e-BRIDGE Cloud Connect, and stored in eSS for Service. eSS for Service can collect customer data not only from MFPs, but also from approximately 500,000 edge devices such as printers and barcode printers. Customer data, including MFP setting information and copy count information, is provided to service engineers and end users via web applications, and is utilized in various operations.
In providing cloud services that utilize such customer data like this, it is necessary to improve safety and reliability and reduce security risks so that users can use them with peace of mind. In particular, data protection, access control, and ensuring privacy are especially important. In establishing an information security management system for this cloud service, we acquired ISO/IEC27017 international standard certification in October 2022. ISO/IEC 27017 applies the initiatives of ISO/IEC 27001, which is for information security management systems, to cloud services. By clarifying risks and implementing countermeasures, not only can security risks be reduced, but the appeal of these initiatives can be broadly demonstrated.
ISO/IEC27017 defines more than 100 security requirements. The following are concrete examples of measures to satisfy those requirements.

1. Use of HTTPS communication to ensure the safety of data on communication channels
2. Protecting cloud environments with CNAPP (Microsoft Defender™ for Cloud)
3. Secure publication of content and API using LB, CDN and WAF (Azure™ Front Door)
4. Efficient authentication and authorization across multiple services using customer ID management on the cloud (Azure™ ADB2C)
   CNAPP: Cloud Native Application Protection Platform
   LB: Load Balancer
   CDN: Content Delivery Network
   WAF: Web Application Firewall

By implementing measures such as these we have achieved the protection of data and systems. In addition, by conducting a website security diagnosis once every six months and always maintaining up-to-date security, we are able to provide secure services that users can use with peace of mind.

＊ Azure and Microsoft Defender are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
＊ This service is not available under this name, e-BRIDGE SKY Suite™, in the European region.

Screenshot of top page for e-BRIDGE SKY Suite™



Schematic diagram of e-BRIDGE SKY Suite™ for Service

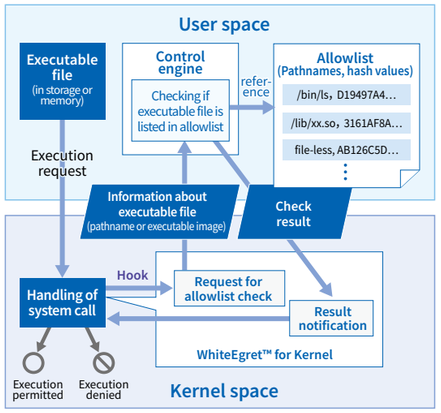
R&D

To protect social infrastructure from increasingly sophisticated and diverse cyberattacks, Toshiba is engaged in R&D on cutting-edge security management technologies as well as advanced cyberattacks and data encryption to support such security management. Toshiba strives to stay ahead of evolving cyber security threats by means of proactive operation in order to continue delivering Toshiba-standard safety and security quality cultivated through its experience in the social infrastructure business.

Malware execution control

Nowadays, malware targets control systems for critical infrastructure such as electric power systems, threatening the foundations of society.
In response, Toshiba has developed WhiteEgret™, an allowlisting malware execution control technology to determine whether to invoke an executable using a standard Linux® interface. WhiteEgret™ makes it possible to protect control systems from both known and unknown malware. In addition, WhiteEgret™ incorporates container-based virtualization technology that is increasingly used for control systems and provides protection from new file-less malware.

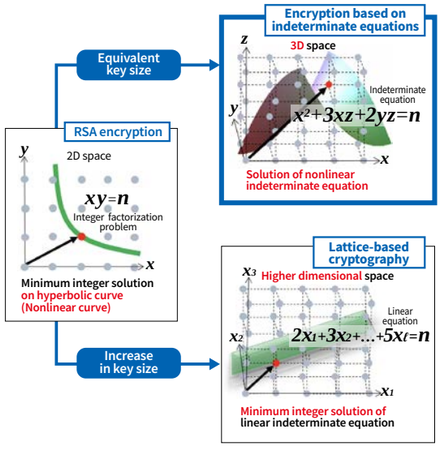
Reference: KANAI Jun, et al. "Allowlisting Execution Control Solution Ensuring Security of Container-Based Virtualization Technologies." Toshiba Review 77(3), May 2022



Quantum computing-resistant cryptography

Quantum computers capable of processing large integers are expected to have the ability to break the widely used public key cryptography.
In response, Toshiba has developed an encryption scheme whose security depends on the problem of solving an non-linear indeterminate equation problem that is much harder than integer factorization problem used in the current RSA algorithm. By using the hard problem, we aim to achieve an encryption scheme with a key length as short as or shorter than RSA keys. We intend to apply public key cryptosystems to edge devices with limited resources.

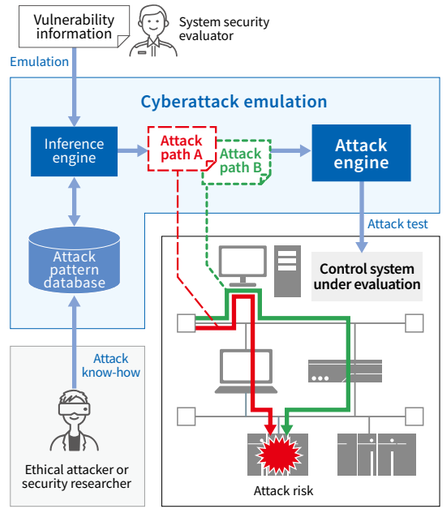
Reference: AKIYAMA Koichiro et al. "A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus)," https://eprint.iacr.org/2017/1241, 2017



Cyberattack emulation technology

In the face of increasingly vicious cyberattacks against the control systems that support social infrastructure, it is becoming crucial to evaluate their risks and implement appropriate countermeasures.
Under these circumstances, Toshiba has developed a cyberattack emulation technology that evaluates the risk of receiving cyberattacks based on the information about vulnerabilities in a system. Since this technology identifies the paths that an intruder might take to gain access to the innermost control device in a control system, it allows security personnel to implement effective security measures based on the emulation results. Cyberattack emulation makes it possible to determine the risk of an attack with high accuracy and validate the effectiveness of security measures.

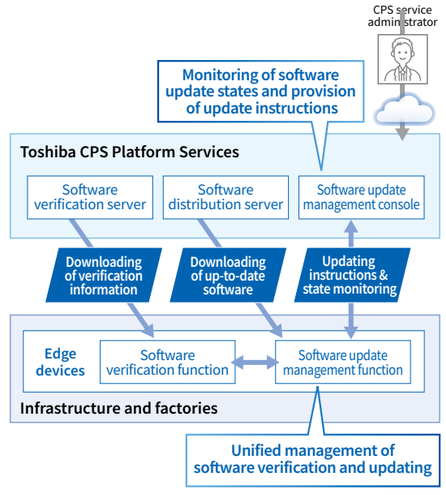
Reference: TODA Kosuke, et al., "Cyberattack Emulation Technology for the Automation of Cyber-attack Path Planning and Validation," SCIS2023



Secure software update technology

In the case of cyber-physical systems (CPS), the risk that their edge devices might be attacked by malicious third parties via the Internet is increasing. To prepare for such cyberattacks, it is necessary to keep the software running on the edge devices up to date. In recent years, however, the number of cyberattacks that exploit a software update function has been increasing, making it necessary to pay meticulous attention to its specifications and implementation.
Against this background, Toshiba analyzed possible threats to the existing software update function and developed a secure software update technology based on the insights obtained from the analysis and open-source implementation.

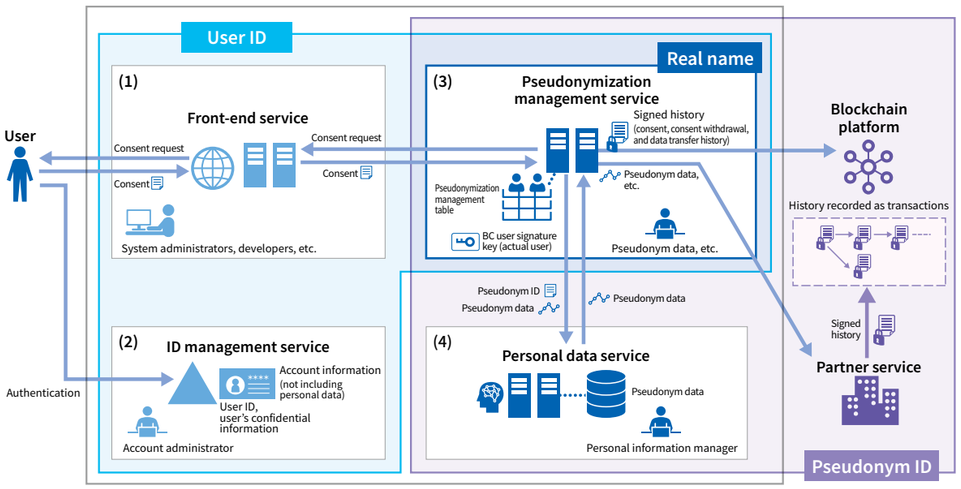
Reference: MINAMI Keisuke, et al. "Security Functions of HABANEROTS IoT Platform Service to Protect Edge Devices against Cyberattacks." Toshiba Review 76(5), September 2021



A data management platform with high transparency

The utilization of personal genomic information and medical information is expected to lead to the personalized disease prevention and treatment according to the constitution and medical conditions of each individual. However, since sensitive personal information can be inferred from genomic and medical information, it is essential to have secure data management that complies with laws and guidelines according to data attributes. Furthermore, it is desirable to have highly transparent data management, so that individuals can feel secure in providing data and using the services.
For these reasons, Toshiba has developed a genomic information platform that achieves a high level of security and transparency. The provided data are stored in a pseudonymized state, thereby improving security; the determination of whether or not the data can be used based on the conditions for use recorded on the blockchain; and the usage history is recorded on the blockchain, thereby increasing the transparency of data management.

Reference: HANATANI Yoshikazu, et al., "Development of a Data Distribution Platform for the Proper Use of Genomic Information", CSS2021



Structure of genomic information platform

External Activities

As of March 31, 2023

Toshiba Group participates in various standardization activities and other external activities concerning cyber security so as to help realize a secure cyber-physical society.

International standardization activities

Major de jure international standardization bodies include the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Together, the ISO and the IEC form a joint technical committee called ISO/IEC JTC 1 (Joint Technical Committee 1). Toshiba Group is a member of three subcommittees (SCs) of ISO/IEC JTC 1, participating in the following standardization activities:

- ISO/IEC JTC1/SC17 Cards and security devices for personal identification
- ISO/IEC JTC1/SC27 Information security, cybersecurity and privacy protection
- ISO/IEC JTC1/SC41 Internet of things and digital twin
- ISO TC292/WG4: Authenticity, integrity and trust for products and documents
- IEC TC65/WG10: Industrial-process measurement, control and automation
- ETSI SCP (European Telecommunications Standards Institute Smart Card Platform): Activities for standardization for European telecommunications
- GlobalPlatform: Technology for the management of multi-application IC cards

SIRT activities

FIRST

The Forum of Incident Response and Security Teams (FIRST) is an international community formed through relationships of trust, consisting of universities, research institutes, enterprises, and government bodies. Toshiba Group joined the FIRST in January 2019.

Nippon CSIRT Association (NCA)

The Nippon CSIRT Association (NCA) is a Japanese organization that handles computer security incidents. Toshiba Group joined the NCA in 2014.

Other activities

Toshiba Group participates in various external activities for exchanging information about, and promoting dissemination of, cyber security. Toshiba Group also delivers presentations at seminars and academic conferences held in Japan.

- Communications and Information network Association of Japan (CIAJ), ICT Network Equipment Security Committee, etc.
- Japan Institute for Promotion of Digital Economy and Community (JIPDEC)
- Japan Information Security Audit Association (JASA)
- Initiative for Cyber Security Information Sharing & Partnership of Japan (J-CSIP), Critical infrastructure equipment manufacturing company Special Interest Group
- Electronic Commerce Security Technology Research Association (ECSEC)
- Control System Security Center (CSSC)
- Robot Revolution & Industrial IoT Initiative (RRI) Industrial Security Action Group
- Cyber Risk Intelligence Center - Cross-Sector Forum (CRIC CSF)
- Cybersecurity Council of the National center of Incident readiness and Strategy for Cybersecurity (NISC)
- Technical member of the Japan Electricity Information Sharing and Analysis Center (JE-ISAC)
- Ministry of Economy, Trade and Industry (METI) Study Group for Industrial Cybersecurity: Working Group 1 (Systems, Technology, Standardization) Factory Sub-working Group
- Japan Network Security Association (JNSA)

etc.

Third-Party Assessment and Certification

As of March 31, 2023

Toshiba Group promotes the utilization of third-party assessment and the acquisition of certification concerning information security management, personal data protection, and products.

Acquisition of the Information Security Management System (ISMS) certification (Toshiba Group and Toshiba-brand companies)

Toshiba IT-Services Corporation
Toshiba I.S. Corporation
Toshiba Infrastructure Systems & Solutions Corporation (SA Division at Komukai Complex)
Toshiba Information Systems (Japan) Corporation
Toshiba Digital Engineering Corporation
Toshiba Digital Solutions Corporation
Toshiba Digital Marketing Initiative Corporation
Toshiba Tec Corporation (Shizuoka Business Center [Mishima])
Toshiba Tec Corporation (Shizuoka Business Center [Ohito])
Toshiba Tec Solution Services Corporation
Toshiba Development & Engineering Corporation
Toshiba Business Expert Corporation (TBLS Business Division, Business Support Division, Human Resources Development Division, Shiba Daimon Juku)
Toshiba Lifestyle Products & Services Corporation
TEC Information Systems Corporation
Enterprise Business System Solutions Corporation
SBS Toshiba Logistics Corporation

Acquisition of the PrivacyMark certification (Toshiba Group and Toshiba-brand companies)

Toshiba I.S. Consulting Corporation
Toshiba IT-Services Corporation
Toshiba Information Systems Corporation
Toshiba Infrastructure Systems & Solutions Corporation
Toshiba Health Insurance Association
Toshiba Automation Systems Service Co., Ltd.
Toshiba Information Systems (Japan) Corporation
Toshiba Data Corporation
Toshiba Digital Engineering Corporation
Toshiba Digital Solutions Corporation
Toshiba Digital Marketing Initiative Corporation
Toshiba TEC Solution Services Corporation
Toshiba Business Expert Corporation
Toshiba Plant Systems & Services Corporation
Mizuho-Toshiba Leasing Company, Limited
UT Toshiba Co., Ltd.

Acquisition of IT security evaluation and certification

The following table lists major products certified under the Japan Information Technology Security Evaluation and Certification Scheme (JISEC) based on ISO/IEC 15408[*1] that is operated by the Information-technology Promotion Agency, Japan (IPA) and those certified under certification schemes in other countries(As of March 31, 2023).

Product	TOE[*2] Class	Certification Number	Applicable PP
TOSHIBA e-STUDIO4525AC/5525AC/6525AC Model SYS V2.1, with FAX unit and FIPS hard disk kit	Digital copier	C0776	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2525AC/3025AC/3525AC Model SYS V2.1, with FAX unit and FIPS hard disk kit	Digital copier	C0775	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2020AC/2520AC Model SYS V2.1, with FAX unit and FIPS hard disk kit	Digital copier	C0774	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO5528A/6528A Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0760	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO4525AC/5525AC/6525AC Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0759	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2528A/3028A/3528A/4528A Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0758	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2525AC/3025AC/3525AC Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0757	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2020AC/2520AC Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0756	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO 2018A/2518A/3018A/3518A/4518A/5018A Model SYS V2.0, with FAX unit and FIPS hard disk kit	Digital copier	C0747	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO 2515AC/3015AC/3515AC/4515AC/5015AC Model SYS V2.0, with FAX unit and FIPS hard disk kit	Digital copier	C0746	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO330AC/400AC Model SYS V1.0, with FAX unit and FIPS hard disk kit	Digital copier	C0684	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC Model SYS V1.0, with FAX unit (GD-1370J/GD-1370NA/GD-1370EU) and FIPS hard disk kit (GE-1230)	Digital copier	C0633	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO5516AC/6516AC/7516AC Model SYS V1.0, with FAX unit (GD-1370J/GD-1370NA/GD-1370EU) and FIPS hard disk kit (GE-1230)	Digital copier	C0632	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A Model SYS V1.0, with FAX unit (GD-1370J/GD-1370NA/GD-1370EU) and FIPS hard disk kit (GE-1230)	Digital copier	C0631	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO5518A/6518A/7518A/8518A Model SYS V1.0, with FAX unit (GD-1370J/GD-1370NA/GD-1370EU) and FIPS hard disk kit (GE-1230)	Digital copier	C0630	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)
TOSHIBA e-STUDIO2010AC/2510AC Model SYS V1.0, with FAX unit (GD-1370J/GD-1370NA/GD-1370EU) and FIPS hard disk kit (GE-1230)	Digital copier	C0629	Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015 (Authentication ID: JISEC-C0553)

*1 ISO/IEC 15408: An international standard for the evaluation of products and systems related to information technology to determine whether they are properly designed and implemented in terms of information security

*2 TOE (Target of Evaluation): TOE refers to products such as software and hardware that are subject to evaluation. TOE may include manuals (user's manuals, guides, installation procedures, etc.) for relevant administrators and users.

Acquisition of cryptographic module validation

The following table lists major products certified under the Japan Cryptographic Module Validation Program (JCMVP) based on ISO/IEC 19790,*1 which is implemented by IPA, and those certified under the Cryptographic Module Validation Program (CMVP) based on FIPS 140-2,*2 which is implemented by the National Institute of Standards and Technology (NIST) of the U.S. and the Communications Security Establishment (CSE) of Canada (as of March 31, 2023).

Product	Certification Number	Level
2.5-inch MHZ2 CJ hard disk drive series with an encryption function	J0006	Level1
Toshiba Solutions' encryption library	F0001	Level1
Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	F0022	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (THNSB8 model)	2807	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type B	2707	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)	2508	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive	2333	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)	2262	Level2
Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)	2082	Level2

*1 ISO/IEC 19790: Information technology – Security techniques – Security requirements for cryptographic modules. An international standard for their testing and certification

*2 FIPS 140-2: The U.S. Federal Information Processing Standard that stipulates the security requirements for cryptographic modules that include both hardware and software components, used by U.S. federal government ministries and agencies.

Acquisition of other security certifications

Certification	Product	Level
Achilles Communications Certification	TOSMAP-DS/LX OWB	Level2
	TOSMAP-DS/LX OWR	Level2
ISA Secure® EDSA (Embedded Device Security Assurance) certification	CIEMACTM-DS/nv (TOSDIC-CIE DS/nv) Unified Controller nv series type2	EDSA2010.1 Level1

Pursuit of the Sustainable Development Goals (SDGs)

The Global Risks Report 2019 from the World Economic Forum cites large-scale cyberattacks and massive incidents of data fraud/theft among top five risks by likelihood. In pursuit of digital transformation, manufacturing industry is required to enhance cyber security of information technology (IT), operation technology (OT), and the Internet of Things (IoT). Toshiba Group offers its views on the security of products and systems throughout their life cycles and endeavors to enhance its cyber security system so as to contribute to the SDGs from the following four angles:

Goal 9: Innovation
We promote security measures from both cyber and physical perspectives to counter increasingly sophisticated cyberattacks.

Goal 11: Smart cities
We support the safety and security of social infrastructure for smart cities through security technology.

Goal 12: Sustainable consumption and production
We establish the reliability of supply chains, aiming at value creation by global value chains.

Goal 17: Partnership
We continuously adopt state-of-the-art security measures through partnership with global security vendors.

Business Overview of Toshiba Group

As of March 31, 2023

Company Overview

Company name: TOSHIBA CORPORATION

Location of head office: 1-1-1 Shibaura, Minato-ku, Tokyo, Japan

Founded: July 1875

Capital: ¥200,869 million

Consolidated net sales: ¥3,361.7 billion (FY2022)

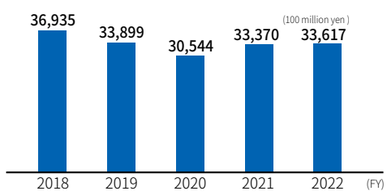
Number of employees (consolidated): 106,648

Total number of shares issued: 433.14 million shares

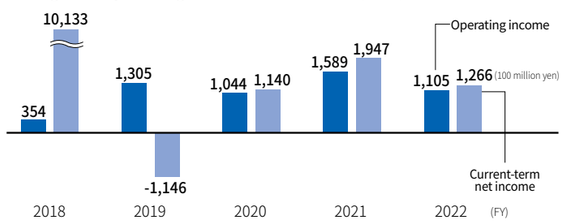
Stock Exchange Listings: Japan: Tokyo and Nagoya

Performance (Consolidated)

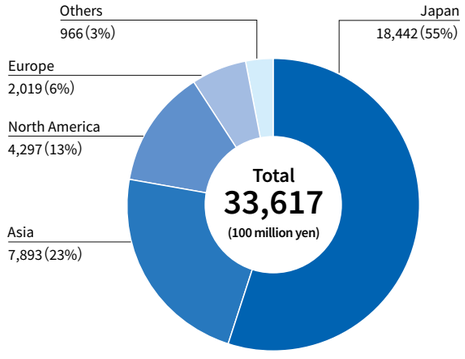
Sales trends



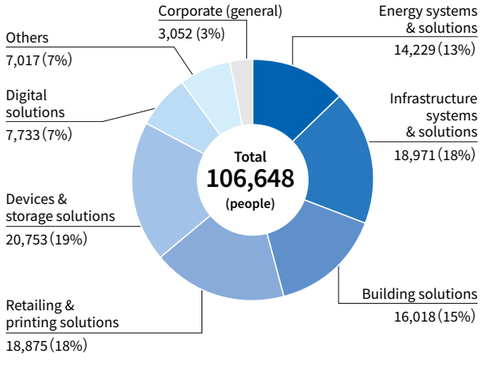
Changes in operating income/net income (loss)



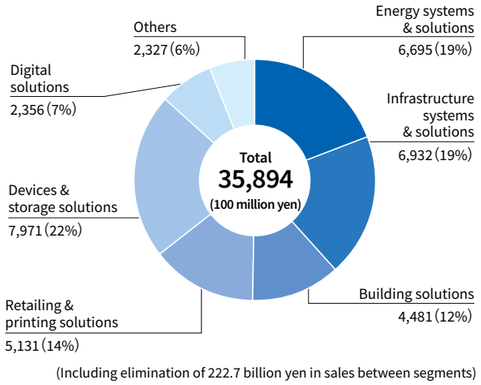
Sales by region



Number of employees by segment



Sales by segment



(Including elimination of 222.7 billion yen in sales between segments)

Committed to People, Committed to the Future.

Toshiba Corporation

1-1, Shibaura 1-chome, Minato-ku, Tokyo,105-8001, Japan

Contacts:

Corporate Technology Planning Division, Cyber Security Center

TEL:+81-3-3457-2128　FAX:+81-3-5444-9213

e-mail : HDQ-TOSHIBA-SIRT@ml.toshiba.co.jp

Toshiba's Cyber Security Website

https://www.global.toshiba/ww/cybersecurity/corporate.html

"Committed to People, Committed to the Future." is the Basic Commitment of the Toshiba Group.

Published in August 2023