TOSHIBA

Cyber Security Report

2022

Message from the Chief Information Security Officer (CISO)

Delivering safety and security to a remotely connected world

We have been engaged in a lengthy struggle to combat the COVID-19 pandemic; its impacts still persist, affecting all aspects of our lives, including work. As we have been urged to maintain social distancing to prevent the spread of coronavirus, many of us are feeling frustrated at being unable to enjoy the simple things in life. While praying for the speedy eradication of the coronavirus, we have learned how to come to terms with the pandemic, exploring “the new normal.”

Looking back over the past three years, we have utilized various forms of digital services more extensively than ever before. Connecting with people remotely is becoming increasingly the norm for us in all spheres of life as we interact with people via social media, do shopping online without going out, use home delivery services, take online classes, and telework most days of the week. When viewed from a different perspective, this situation is advantageous to those who are using the Internet for criminal purposes. It is therefore necessary to enhance the security of cyberspace in order to protect society from cybercrime.

Toshiba Group possesses extensive experience and expertise in *monozukuri*—the art, science, and craft of making things—cultivated for 147 years since its founding in 1875. By leveraging such experience and expertise, we would like to deliver safety and security not only in the physical world but also in a remotely connected world in accordance with the Basic Commitment of the Toshiba Group, "Committed to People, Committed to the Future."

The purpose of Cyber Security Report 2022 is to provide our customers, shareholders, suppliers, and other stakeholders with information about Toshiba Group’s initiatives to enhance cyber security. We hope it will allay any security concerns you may have so that you will select Toshiba’s products and services with confidence.

Executive Officer,
Corporate Senior
Vice President and CISO
Toshiba Corporation

Hideaki Ishii

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.

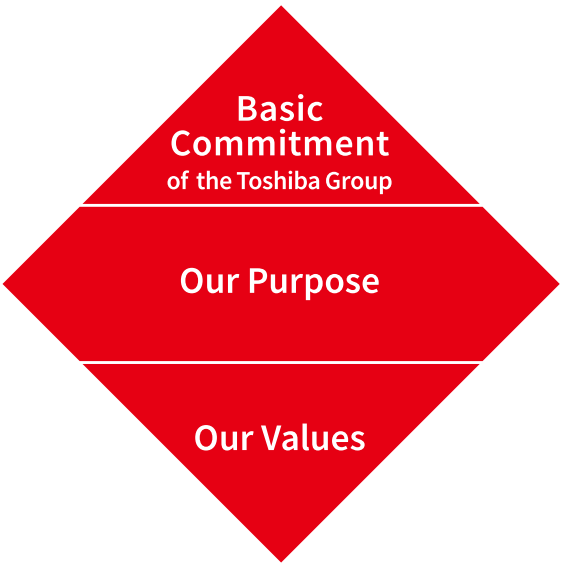
To protect society from invisible threats, Toshiba Group works with one accord to establish a robust **cyber security system**, comply with the related laws and regulations, and develop cyber security specialists while being committed to active and honest information disclosure to customers.

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.

2022 Cyber Security Report

Contents

Chapter 1

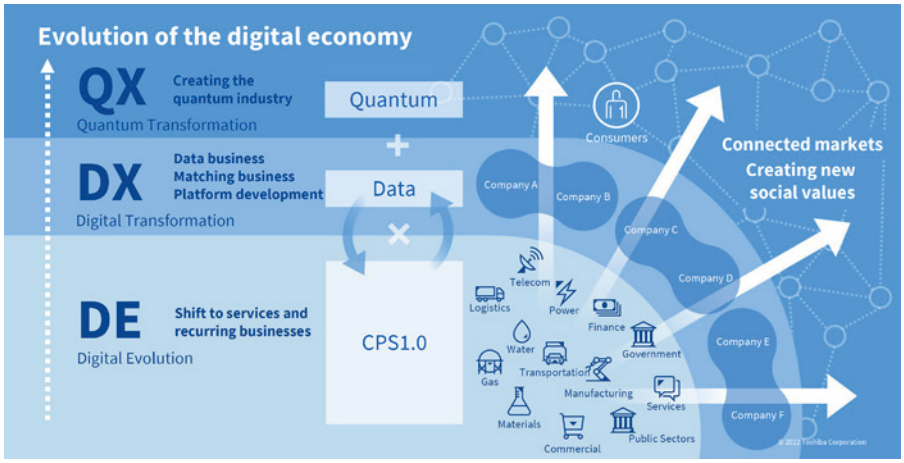
Visions and Strategies

In accordance with the Basic Commitment of the Toshiba Group, "Committed to People, Committed to the Future," Toshiba Group aims to realize a sustainable future. To this end, our priorities are: 1) developing infrastructure that helps maintain safe and secure lives for everyone, 2) realizing a connected data-driven society that helps promote social and environmental stability, and 3) shifting toward a carbon-neutral circular economy. The key to fulfilling these goals lies in digital technologies. As the transition to a digital economy progresses, many businesses will become connected to create new social value, transcending the barriers among different industrial sectors.
Cyber resilience is essential for the development of a digital economy. Accompanying the digitization of various social infrastructure, cyber threats are expanding, exposing them to the increasing risk of cyber-induced physical damage. To facilitate connections among various businesses across industries, it is crucial to ensure cyber security while securing the reliability of the data that will be traded and utilized. Furthermore, realization of secure network environments resistant to quantum computers is desired.
Toshiba Group possesses extensive expertise in each field of social infrastructure cultivated during more than 140 years and a high level of cyber security proficiency acquired through the operation of information systems supporting roughly 120,000 employees. As an enterprise promoting digitization, we consider that it is our responsibility to make the utmost use of our strengths to provide secure infrastructure and help create a securely connected data-driven society, thereby contributing to the realization of a circular, carbon-neutral economy.

Toshiba's Cyber Security Visions

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.



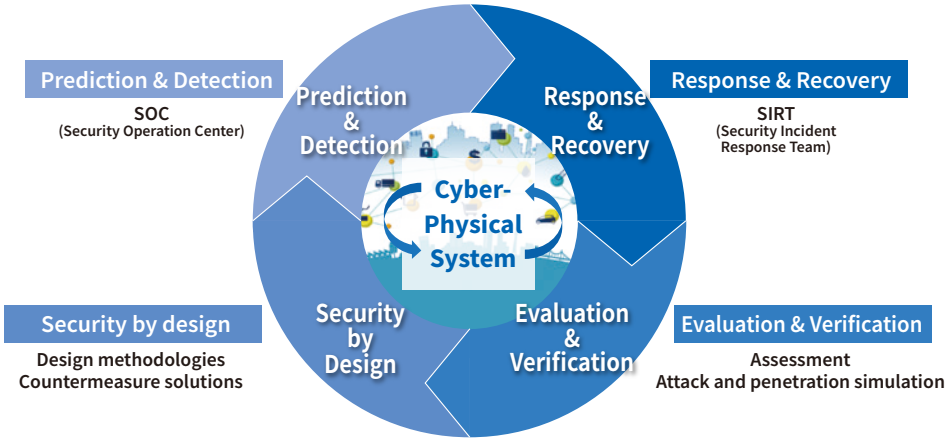
Source: FY2022 Toshiba Group Management Policy

Toshiba Group's cyber security visions

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

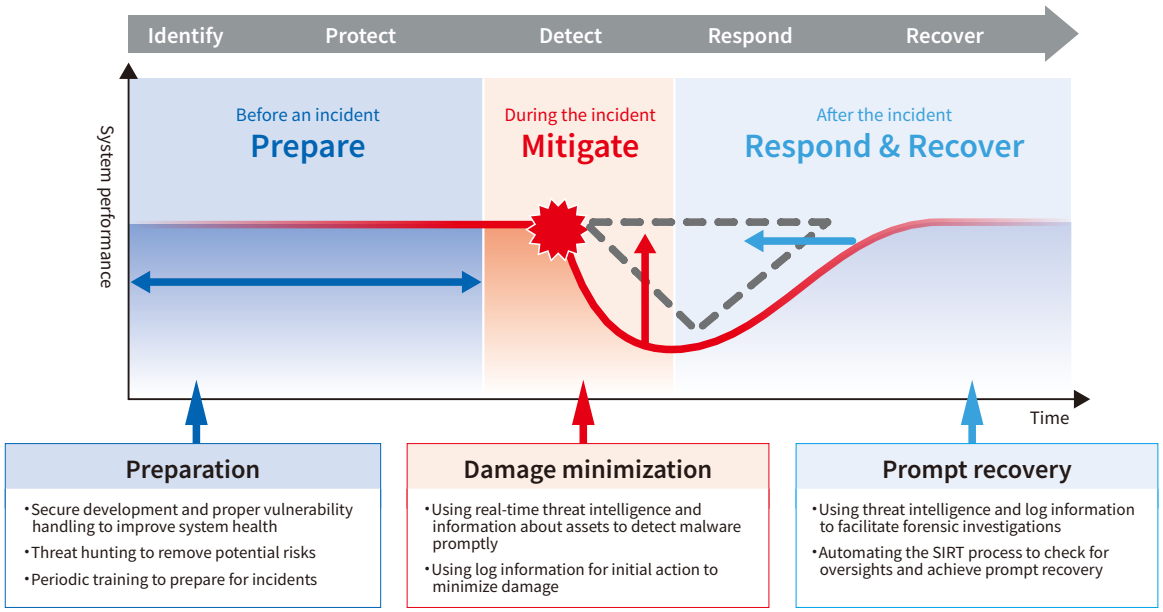
To realize this, Toshiba Group defines cyber security management as a series of organically connected processes from six perspectives: 1) Governance, 2) Design & Protection, 3) Prediction & Detection, 4) Response & Recovery, 5) Evaluation & Verification, and 6) Personnel. Toshiba Group has set its goals 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

Goals of Toshiba Group

Strategies for Enhancing Cyber Security Preparedness

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.

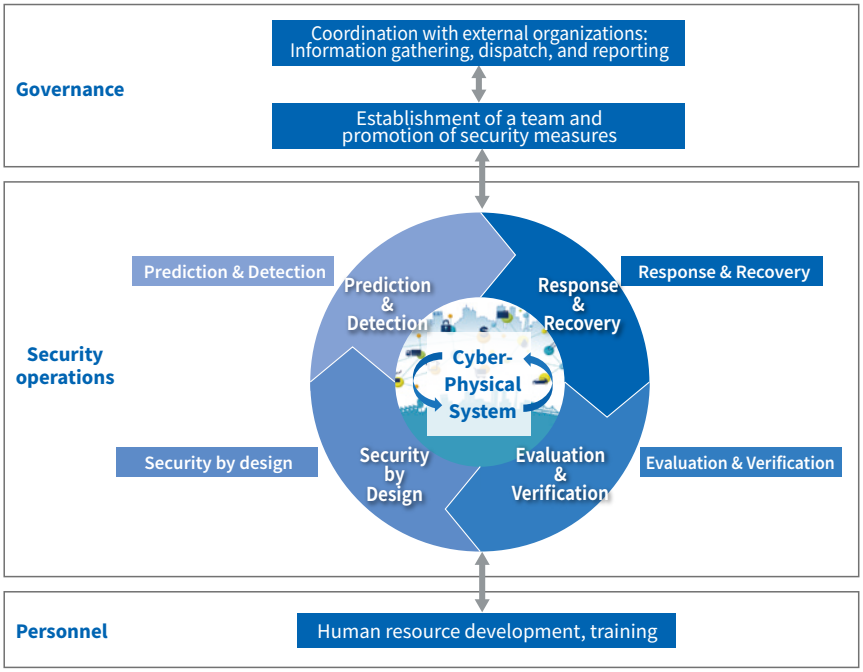
In order to facilitate the implementation of enhanced security measures, Toshiba Group is strengthening its organizational structure. First, to reinforce security governance, Toshiba Group set up the post of the Chief Information Security Officer (CISO) in November 2017, to whom the authority over information security was delegated from the Chief Executive Officer (CEO). 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.

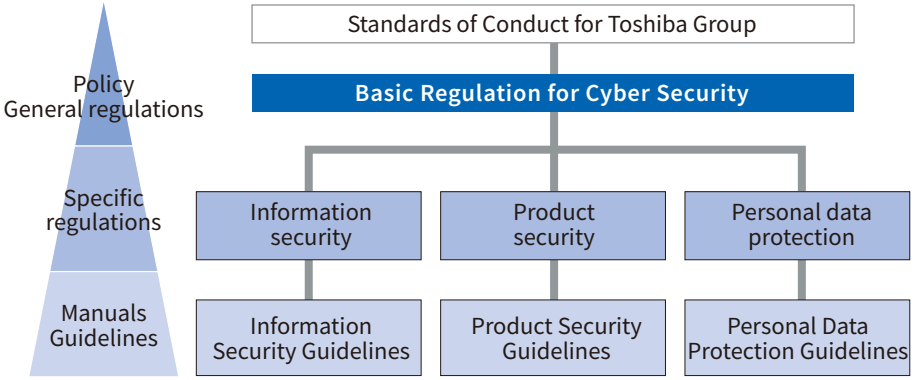
*1 Computer Security Incident Response Team
*2 Product Security Incident Response Team
*3 CDMP: Cyber Defense Management Platform
*4 Threat intelligence: A collection of information about cyber threat trends and cyberattacks by hackers that supports decision-making concerning cyber security

Governance

Toshiba Group has established the Basic Regulation for Cyber Security that stand above the regulations on information security, product security, and personal data protection. The purpose of the Basic Regulation for Cyber Security is to ensure the promotion of consistent security measures across Toshiba Group for its internal information systems; our products, systems, and services; and the personal data possessed by the Group.

Basic policy

Toshiba Group properly manages cyber security risk that could have a severe impact on corporate management and has 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 stable supply of high-quality products, systems, and services by cultivating a corporate culture that prioritizes safety and security and by protecting 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 the course of business activities, as its important assets and adopts a policy to manage all corporate information as confidential information and to ensure that the information is not inappropriately disclosed, leaked or used. In view of 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 also 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 in accordance with 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 in the course of 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 of each stakeholder and also an important asset for Toshiba, leading to 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.

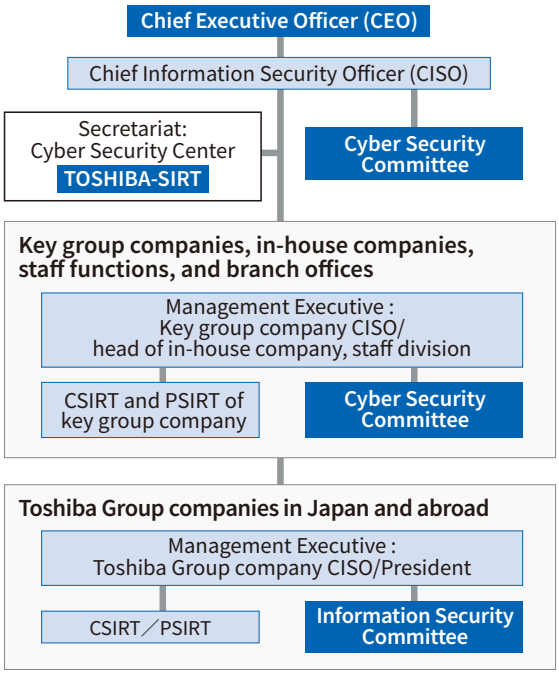
Toshiba's privacy policy: https://www.global.toshiba/ww/privacy/corporate.html

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.

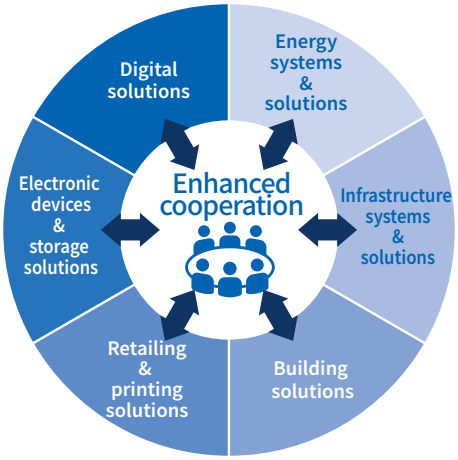


Cyber Security Management Structure

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, which require different cyber security frameworks. 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 so as to help resolve their respective issues.

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

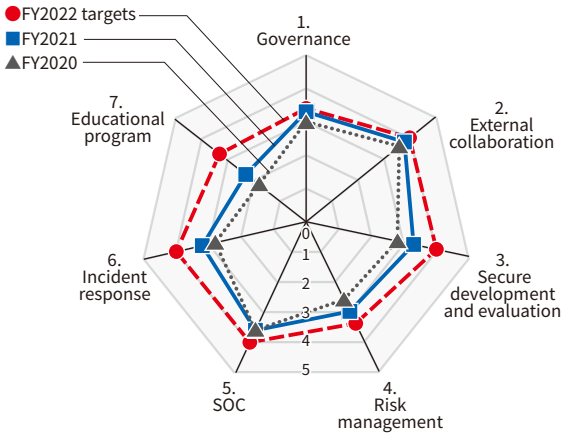


Self-assessment of cyber security management maturity

In order 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 Cybersecurity Management Maturity to include overseas group companies to enhance their cyber security management levels.



Results of cyber security management maturity self-assessment

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

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. In addition, in order to raise the security awareness of employees, we create a campaign poster to be displayed 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

February Cybersecurity Month

As Chief Information Security Officer (CISO) of Toshiba Group, I am very happy to share a short message for Cybersecurity Month.

1. Introduction

Although the COVID-19 pandemic seemed to be ebbing, the omicron variant is fueling another surge of infections, throwing the world into political and economic chaos. While the trajectory of the pandemic differs from country to country, it is likely to continue for a while. This is not the only threat we face cybersecurity incidents are also increasing. Recent ones include a cyberattack against a US oil pipeline, and a ransomware infection of a Japanese hospital. Techniques used in cyberattacks are becoming increasingly sophisticated, and the instigators are becoming shrewder.

Message for Cybersecurity Month from CISO

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.

Mitigating supply chain security risk

In recent years, the number of cyberattacks exploiting the vulnerabilities in supply chains has been increasing. It is therefore imperative to enhance the cyber security for the supply chains of both small and large companies.
In order to improve the security preparedness of not only Toshiba Group but also its partners with whom it shares information, Toshiba Group is implementing security measures from three perspectives: governance, operation, and human resources development.

(1)Human resources development (e-learning)
Toshiba Group provides e-learning programs for its employees to learn about cyber threats to supply chains, the supply chain risks that we need to anticipate, and possible countermeasures for these risks. Since we can act as both contractors and suppliers, the e-learning programs are designed to familiarize the employees with possible supply chain risks from both perspectives in order to ensure that appropriate security measures are always implemented.

(2)Assessment
As part of a survey of the systems and networks shared with partner companies, Toshiba Group regularly performs a security assessment to determine whether all the security measures stipulated in its in-house regulations are in place. In addition to in-house networks, we have commenced the assessment of production lines that tend to be separated from other networks.

(3)Security risk ratings
Some Toshiba Group companies have introduced a technique for quantitative cyber security assessment and visualization for the selection of partner companies. Generally called Security risk ratings, this technique is attracting much attention lately as a means of visualizing the risk of receiving cyberattacks.
From the viewpoint of an attacker, it performs information gathering (initial reconnaissance) as a preparation for an attack and scores the security measures that are in place at the company under assessment. Toshiba Group also assesses existing suppliers periodically and provides them with guidance and assistance as necessary in removing vulnerabilities. These efforts are intended to enhance the security of supply chains, including partner companies, and raise the security awareness of all parties involved.

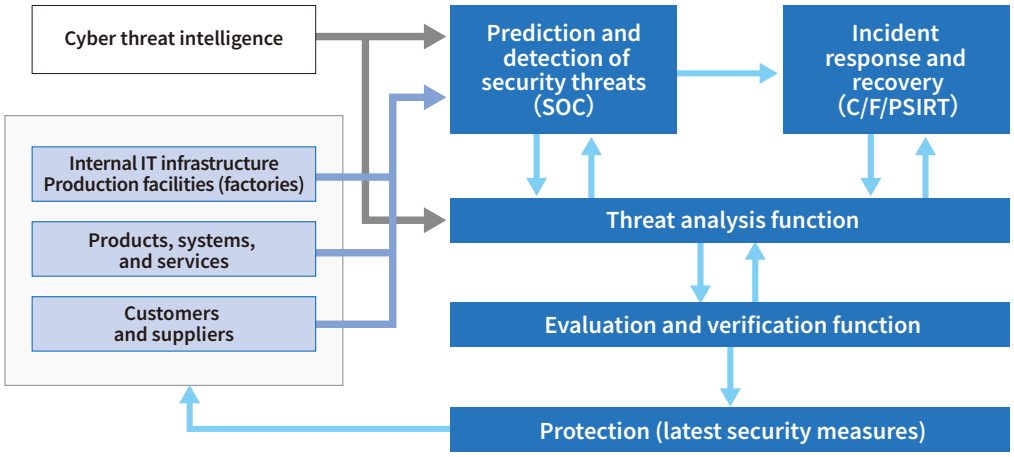
Security Operations

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

The purpose of the CDMP is to protect not only internal IT infrastructure but also production facilities and factories, as well as the products, systems, and services offered to customers. In the future, the coverage of the CDMP will be extended to include customers' and suppliers' systems connected to them. 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 ever-growing. Since resources are limited, Toshiba Group is endeavoring to automate the response to and the recovery from security incidents while accumulating knowledge and using artificial intelligence to realize high-accuracy security operations with slim resources. To automate the use of threat intelligence, and the investigation of and response to security incidents, we are working on the deployment of a platform called SOAR (Security Orchestration, Automation and Response). In addition, we are developing a dashboard to enable the CISO, CSIRT, and PSIRT of each group company to view their security states in real time. Its purpose is to let them grasp the security incidents that are occurring and how they are being dealt with and help them respond promptly.

Expediting a response to cyber security incidents

In the case of recent ransomware attacks and the attacks for information theft, endpoints*1 such as PCs and servers are often used as steppingstones for an attack. These cyberattacks are becoming cleverer than ever, making it increasingly difficult every year to fully protect the endpoints from all attacks. Therefore, based on the assumption that endpoints are constantly exposed to cyberattacks, it is becoming more important to grasp what is occurring at the endpoints and respond to cyberattacks as promptly as possible.
Under these circumstances, Toshiba Group has introduced an EDR*2 tool to detect and respond to sophisticated cyberattacks against endpoints. (See the section “Enhancing the Security of Endpoints Using EDR Tools” on page 19 in Chapter 2.)

The features of the EDR tool are as follows:

- Provides a powerful query to grasp the up-to-the-minute conditions of endpoints (security baseline assessment)
- Detects signs of suspicious behavior of the malware hidden in endpoints (early detection)
- Quarantines a network to prevent malware from spreading from the infected endpoint (damage minimization)

The EDR tool helps expediate a response to cyber security incidents.

∗1 Endpoints: PCs, servers, and other information systems connected to a network
∗2 EDR: Endpoint detection and response (also known as endpoint threat detection and response)

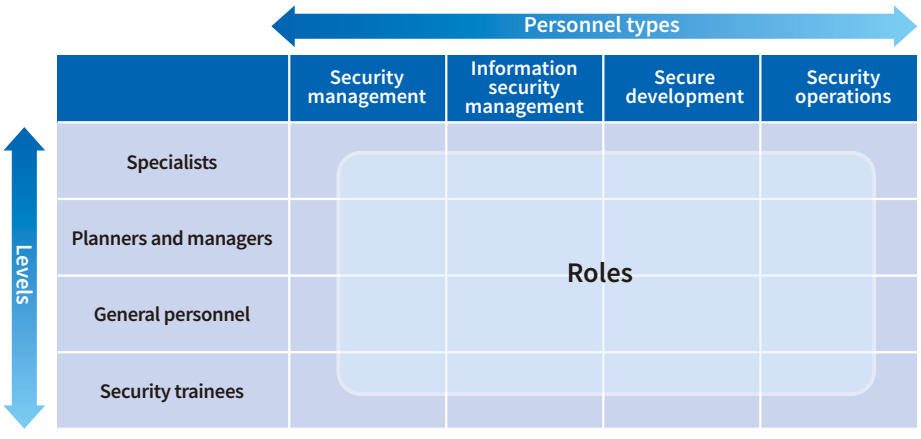
Human Resources Development

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

Toshiba Group defines several levels of security personnel, ranging from specialists who possess advanced skills to security trainees, including general personnel with added security knowledge*1. Personnel types are classified into business administration, management, development, and operations concerning cyber security*2. The roles that must be fulfilled are defined in terms of personal qualities required for each combination of personnel levels and types. In addition, Toshiba Group has a certification program to certify the qualified security personnel. Certification criteria include attendance of designated internal and external security education courses, acquisition of Registered Information Security Specialist or other security-related certifications, and job experience expected for a given role. To date, roughly 800 employees have been qualified.

∗1 Personnel with added security knowledge: The personnel whose main job responsibilities do not explicitly include security measures and who have sufficient cybersecurity literacy to engage in a type of work that entails a security risk unless sufficiently secured.
∗2 See the Skill Standards for IT Professionals (ITSS) from Information-technology Promotion Agency, Japan (IPA).



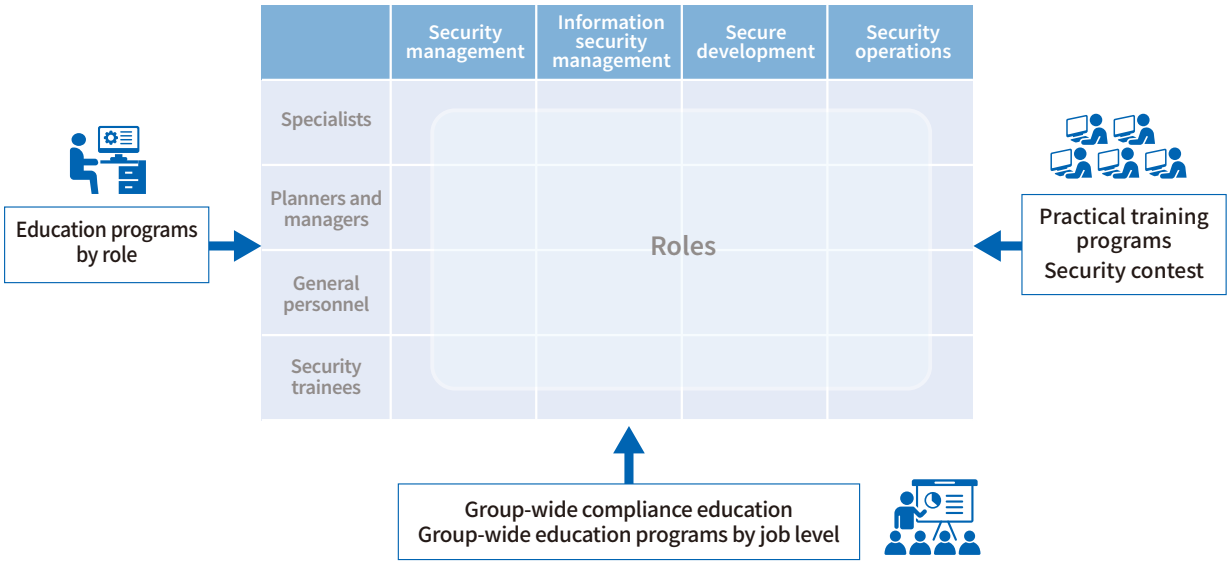
Qualities required for security personnel

Security education programs

In order to prevent information leakage, each employee must acquire knowledge necessary to properly handle the information encountered in the course of work and enhance awareness of security threats such as targeted attacks as well as security considerations for teleworking. To ensure the security of products, systems, and services offered to customers, all employees involved in products, such as sales, procurement, design, development, quality, and maintenance personnel, must understand the significance of product security vulnerabilities as well as the importance of preventing the introduction of vulnerabilities at the product development stage and promptly addressing security vulnerabilities found in the products shipped. To raise the security awareness and literacy of all officers and employees, Toshiba Group provides them with Group-wide compliance education programs (information security, personal information protection, and product security education programs) every year. These education programs are available in multiple languages for overseas employees. Toshiba Group also provides education programs at career milestones such as at the time of employment and promotion, which are organized according to job levels.

In addition, Toshiba Group has education and training programs according to the personal qualities required to fulfill the roles of security personnel. Toshiba Group also conducts e-learning courses about the basics of information and product security, the importance of supply chain security, threat analysis, and secure development techniques. Other training offerings include hands-on training designed to help acquire practical skills for vulnerability testing; training courses to develop specialists and highly skilled personnel capable of responding to security incidents promptly; and security courses for managers responsible for improving security quality at the time of product development. Toshiba Group also lets its employees enroll in external practical training programs such as the Core Human Resource Development Program offered by the Industrial Cyber Security Center of Excellence (ICSCoE) of Information-technology Promotion Agency, Japan (IPA).

Furthermore, Toshiba Group offers training programs designed to promote the use of the acquired knowledge and skills in daily work (e.g., incident response training) as well as a security contest for employees that aims to introduce, spread, and strengthen security practices.



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.

Establishment of privacy governance regulations

In July 2021, Toshiba established Privacy Governance Regulations, which stipulate a procedure for checking whether there is no risk of privacy infringement in conducting a business using personal data. The departments that plan such a business are required to apply for an evaluation, via their CSIRT, to the Privacy Risk Evaluation Committee, which consists of members from the related staff functions of Toshiba Corporation. In the case of projects that pose significant privacy risks, we seek advice from an external advisory board.

Privacy protection education for all employees

In 2021, Toshiba Group offered all its employees a class about the importance of privacy protection and a procedure for a privacy risk evaluation in addition to a class about personal information protection.

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.

Chapter 2

Cyber Security Initiatives

In order to enhance cyber security, Toshiba has consolidated information and product security functions that were separately promoted before. Chapter 2 categorizes Toshiba Group's IT infrastructure and its products, systems, and services, and describes Toshiba Group's initiatives for enhancing cyber security. Here, internal IT infrastructure includes factories and other production facilities in addition to PCs, servers, networks, and other equipment within Toshiba Group.

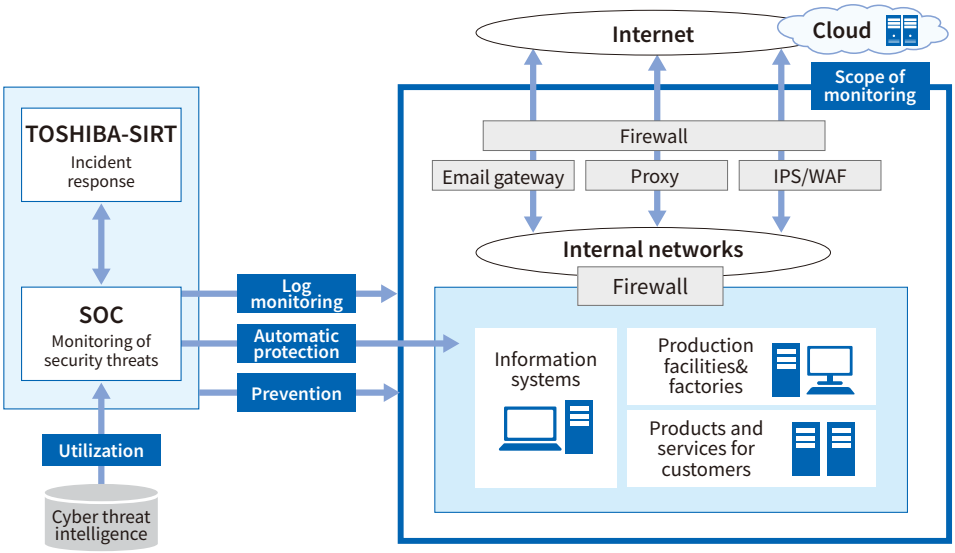
Security Measures for Internal IT Infrastructure

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

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

- 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

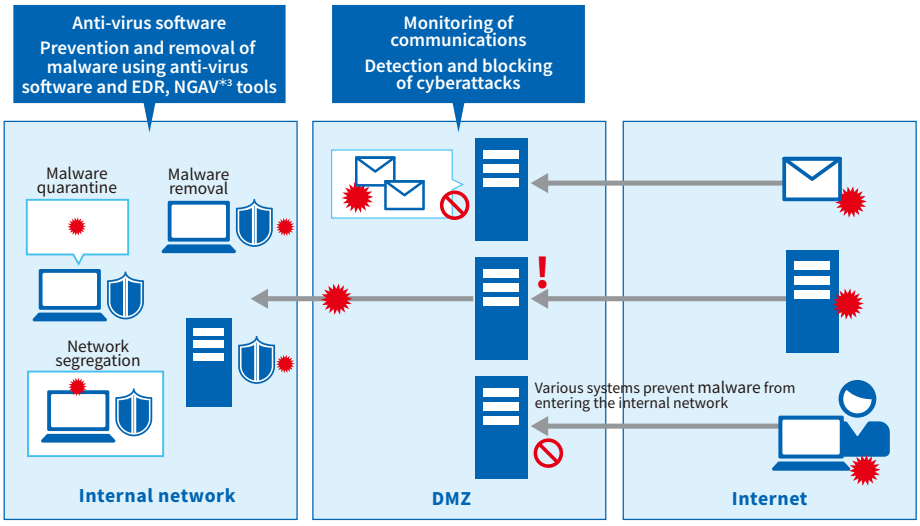
Prediction & Detection

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 Incident Response

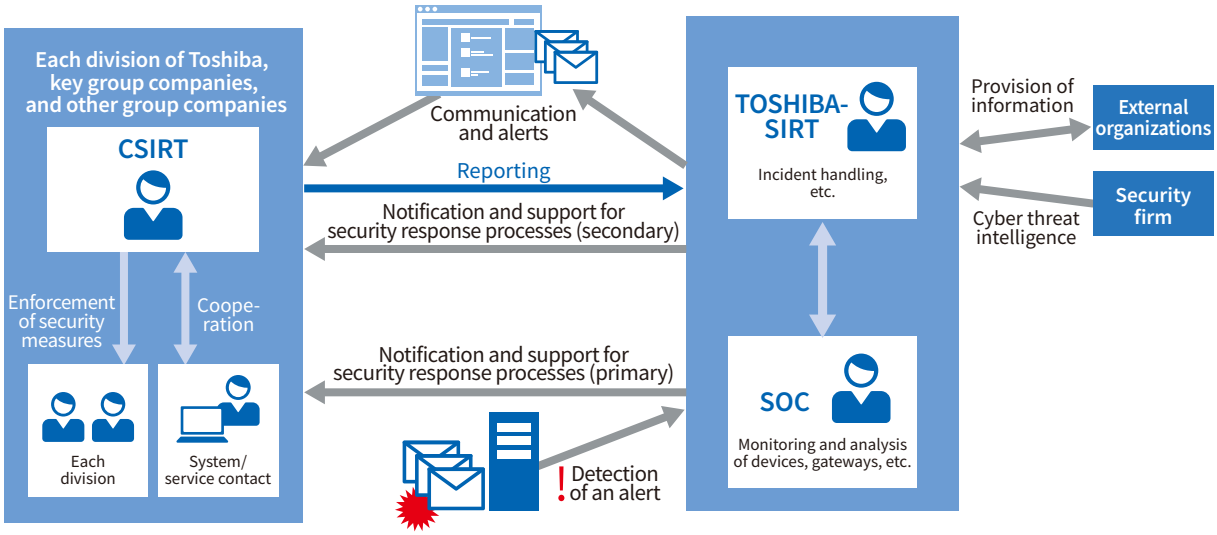
Response & Recovery

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

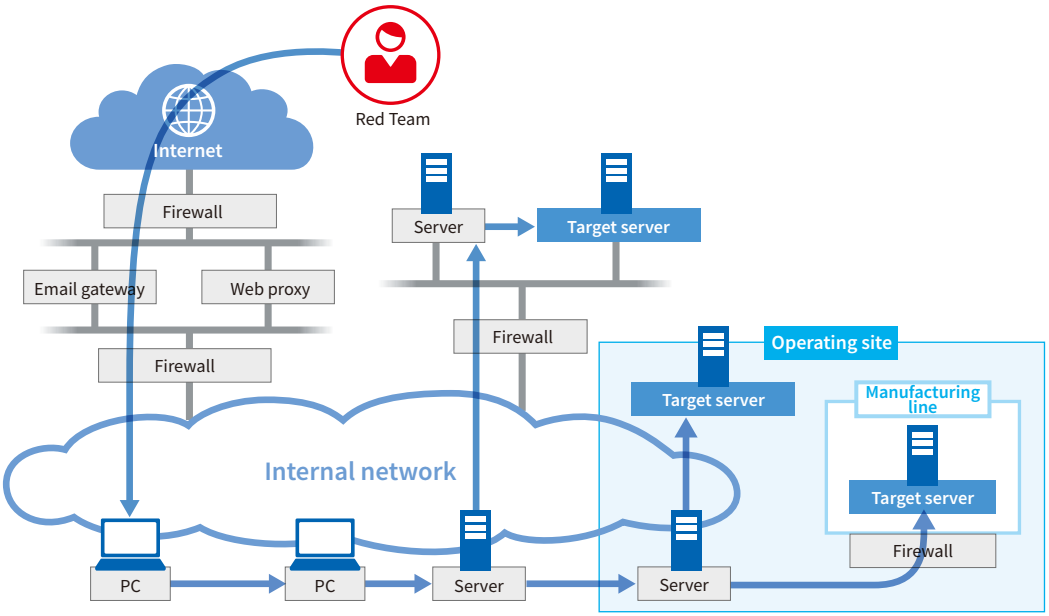
To promptly and accurately respond to vulnerabilities and incidents 24/7/365, Toshiba Group is now automating the response to vulnerability information, cyber threat intelligence, and security alerts. We have categorized security information and alerts and developed routine response patterns, ensuring 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, i.e., attacks that are uniquely destined for one specific enterprise or organization, are increasing, with cyber criminals focused on stealing its customer or confidential information. In the face of increasingly sophisticated cyber threats, Toshiba Group regularly takes an attack and penetration assessment from the Red Team* of a specialized cyber security firm in order to validate the effectiveness of its security measures.
In this assessment, the Red Team attempts to penetrate Toshiba Group's network using advanced tactics, techniques, and procedures of real-world hackers, in order to determine whether it is possible to reach a target server through a simulated attack. The purposes of this assessment are to verify the effectiveness of the current security measures, identify potential weaknesses against cyberattacks, and consider additional measures.

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

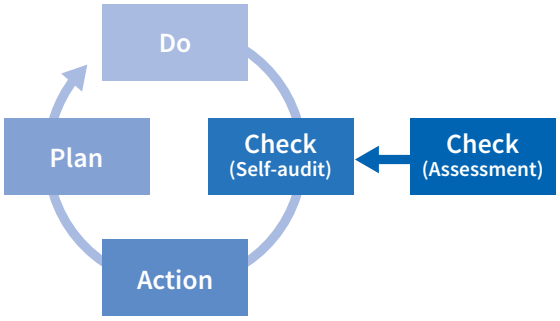


Outline of attack and penetration assessment

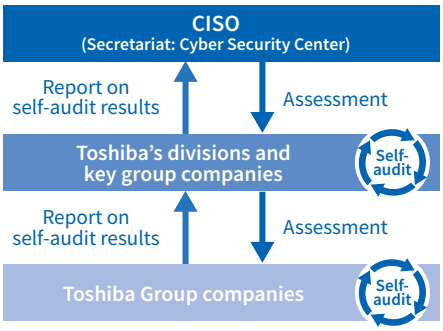
Self-Audit and Security Assessment

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.
The Cyber Security Center, which serves as a secretariat, assesses the results of the self-audit and improvement activities of each division and provides guidance and support if corrective action is required. 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.



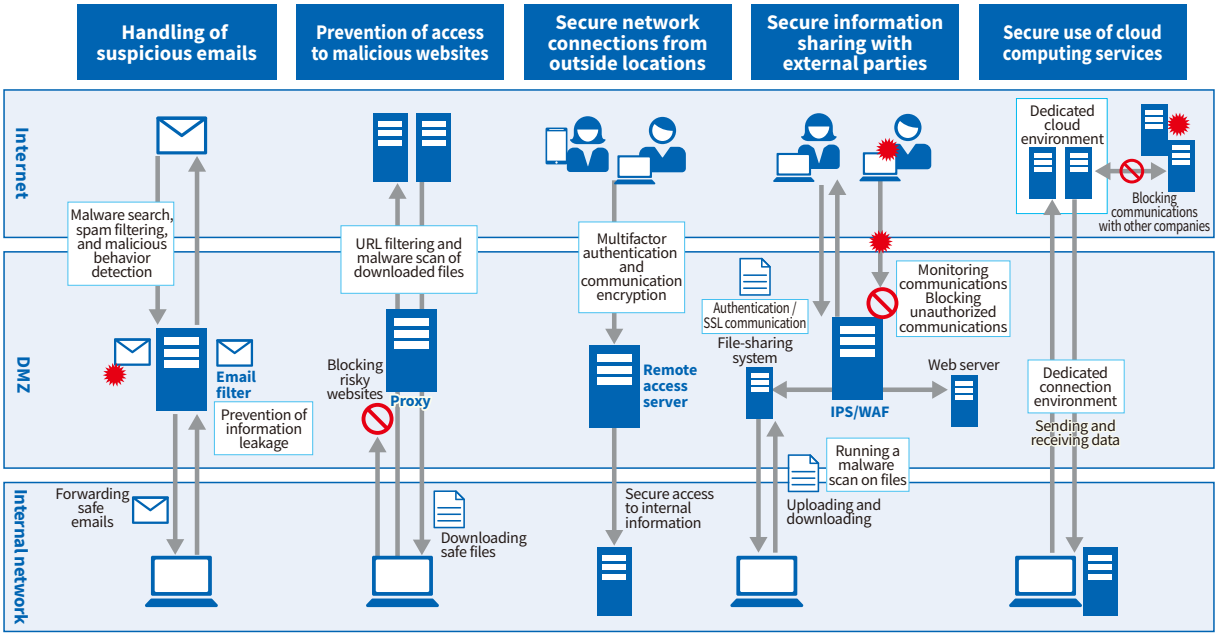
PDCA cycle based on a self-audit and assessment



Self-audit and assessment conducted by the entire Toshiba Group

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

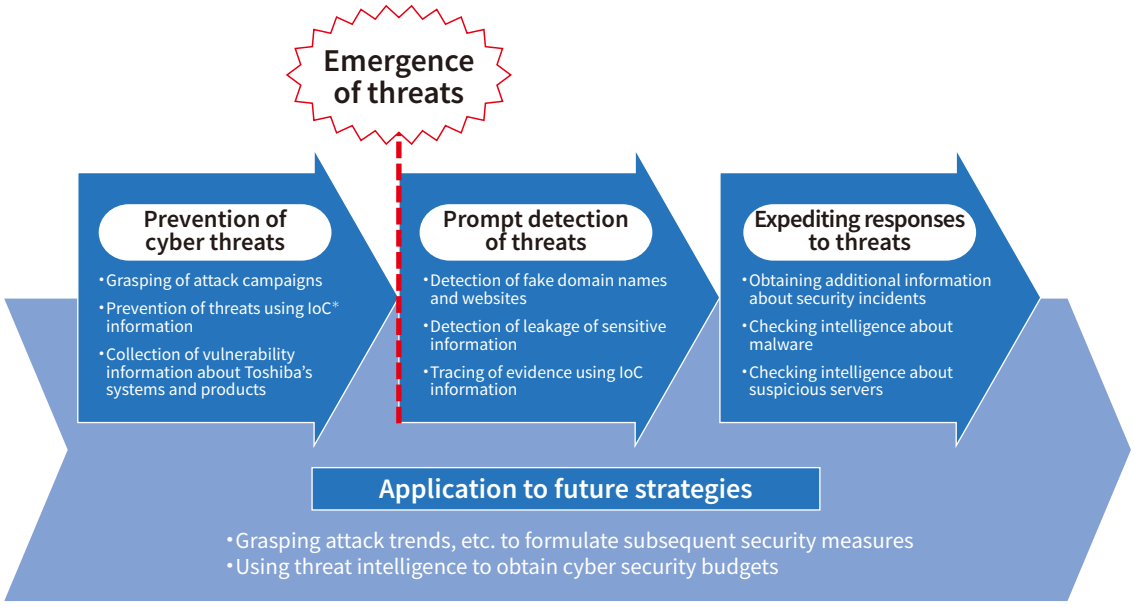
As cloud computing services are increasingly employed to improve work efficiency, the risk of information leakage, unauthorized access, and wrong settings increases. To alleviate this risk, Toshiba Group has established a secure private cloud environment in order to protect sensitive information from 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.

Utilization of Cyber Threat Intelligence

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 enhance the security quality of its products, systems, and services offered to 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.

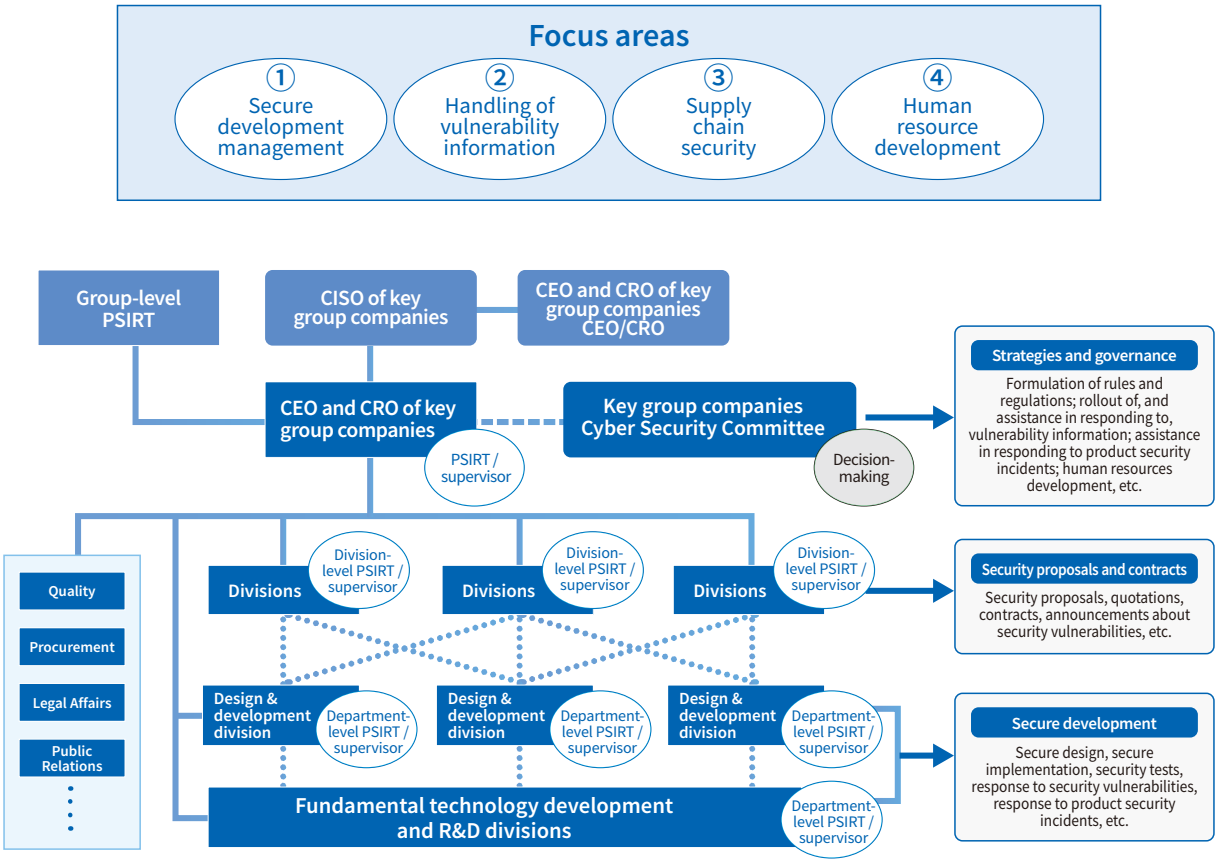
Initiatives for Enhancing Product Security

Security by design

In order to ensure the security of products, systems, and services offered to customers, Toshiba Group has established a product security management system as part of the cyber security management system. Under the product security management system, the PSIRT collaborates with quality assurance and procurement departments to enhance the security of product development processes as well as the security of third-party products for use in Toshiba Group's products.

Devising plans to enhance product security preparedness

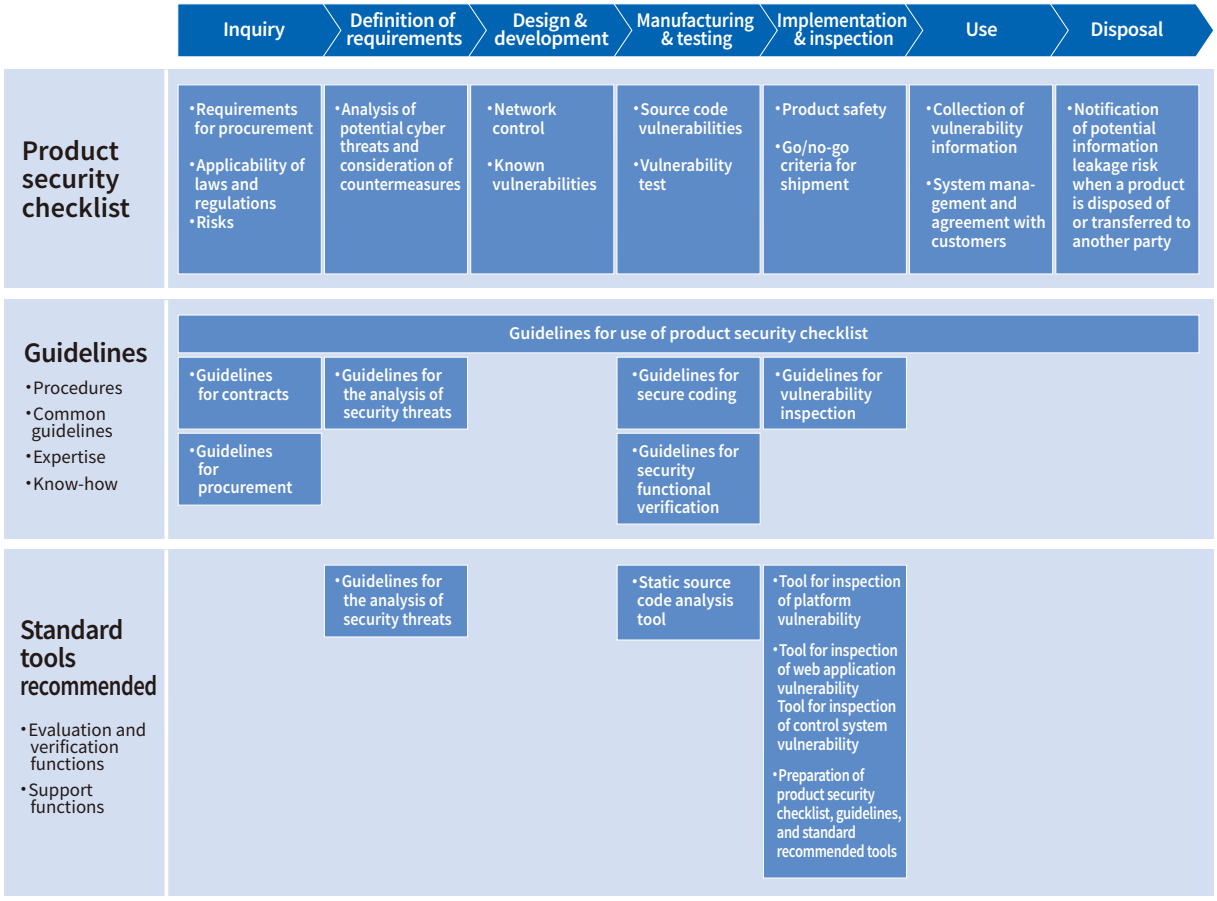
Toshiba Group has redefined four focus areas to strengthen its product security, considering the recent trends in product security and the situation of Toshiba Group, while setting mid-term objectives and visualizing the extent of their achievement. Based on this definition, Toshiba Group has devised 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

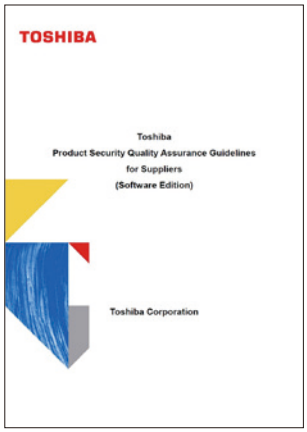
Preparation of product security checklist, guidelines, and standard recommended tools

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 provides the standard recommended tools and related support services that will come in handy when going through the checklists.



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

Toshiba Group is now preparing a product security guide to help suppliers understand its views on product security and to solicit their cooperation in the realization of secure products, systems, and services. This guide summarizes specific security requirements for suppliers in three areas: 1) supplier's security management system, 2) deliverables of software development, and 3) operation services to be contracted out. To communicate our security requirements, Toshiba Group provides suppliers with this guide before entering into business relations with them.



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

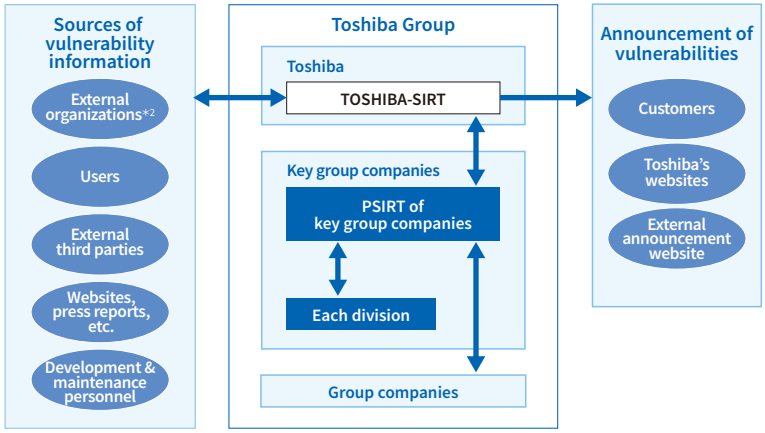
Prompt and Reliable Response to Security Vulnerabilities

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.

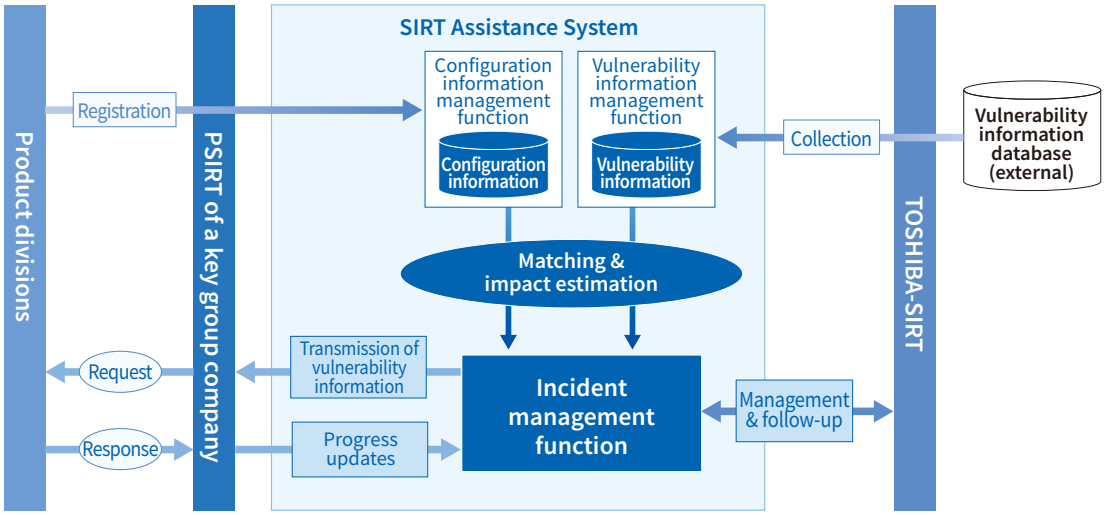


Toshiba Group's vulnerability handling system

*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

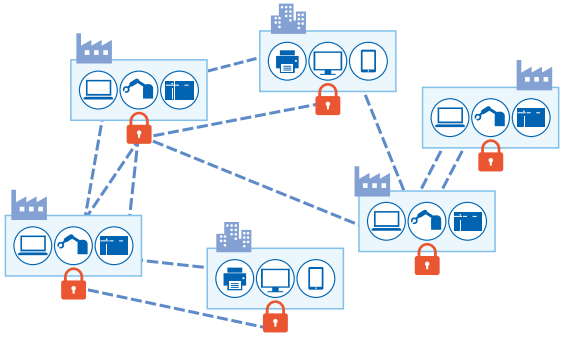
Column

A shift to a zero-trust security model in the new normal

As in 2021, the COVID-19 pandemic has continued to impact our work environments, making teleworking, remote meetings, and other online interactions the norm. As the way of working changes, the targets of cyberattacks have changed. In 2021, attacks that exploit teleworking and other "new normal" work styles were ranked third among 10 major security threats announced by Information-technology Promotion Agency, Japan (IPA)*1, with ransomware damage being ranked first. This indicates that attackers have adapted to the changes in people's working environments, posing an ever-greater threat to cyber security. Under these circumstances, it is imperative to reconsider the conventional approach to cyber defense.

The U.S. government's memorandum, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*2, released in January 2021 attracted plenty of attention as it states, "In the current threat environment, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data," and discusses a strategy for transition to a zero-trust security model. The National Cyber Security Centre (NCSC) of the United Kingdom also announced "Zero trust architecture design principles*3" last year while the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) of Japan released Cybersecurity Strategy 2021*4, discussing a zero-trust security model. According to a survey of Japanese companies conducted by Palo Alto Networks, Inc.*5, 88% of the respondents are interested in zero-trust architecture, indicating that it is attracting increasing attention both in the public and private sectors.

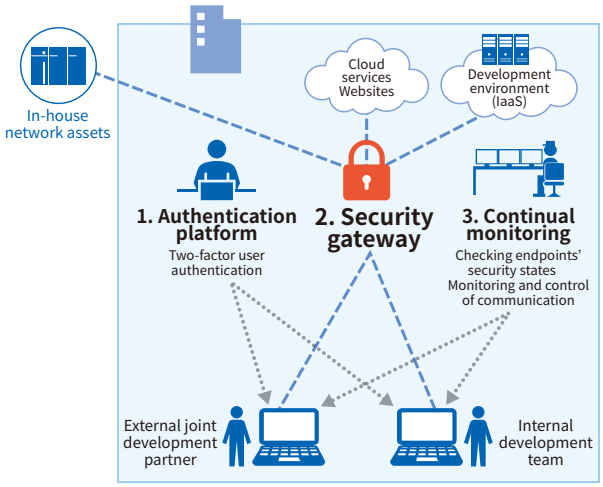
However, it is difficult to abandon existing perimeter-based defenses for in-house networks altogether and replace them with zero-trust networks because of the exorbitant costs and workloads required. So, one way to reduce the risk of this transition is to start with a single project or a zone within a "corporate perimeter" where it is easy to introduce a zero-trust model, gradually working toward full zero-trust implementation as you gain the understanding of network users.



Zero-trust networks

Toshiba Group's initiative

Since Toshiba Digital Solutions Corporation possesses a multitude of software development systems and resources on its internal network, it was previously separated from the outside world by a robust security perimeter. However, in view of the increasing number of joint development projects in the cloud, Toshiba Digital Solutions has established a zero-trust software development environment in order to improve development efficiency. This zero-trust implementation incorporates three principles that Toshiba Group considers essential for zero-trust networks: 1) authentication platform, 2) security gateway, and 3) continual monitoring. The company is planning to establish security policies and operational procedures based on these three principles while expanding zero-trust zones.



Zero-trust security model for software development sites

Perimeter-based defenses will become less effective in the future, making them unnecessary as zero-trust networks are created at each factory, laboratory, and asset-based unit. This means that a corporate network will become a collection of zero-trust zones. Attackers infiltrate a network with the help of internal accomplices or via overseas sites, subsidiaries, or supply chains. A zero-trust security model authenticates the reliability of the connecting device every time and keeps monitoring its behavior on the network. Therefore, a collection of zero-trust zones helps minimize security risk, making it possible to optimize the security level of supply chains.

*1 10 Major Threats to Information Security 2021
https://www.ipa.go.jp/security/vuln/10threas2021.html
*2 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
*3 https://www.ncsc.gov.uk/collection/zero-trust-architecture
*4 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf
*5 https://www.paloaltonetworks.jp/company/press/2021/palo-alto-networkssurveys-japanese-organizations-on-zero-trust

Offering of Secure Products, Systems, and Services

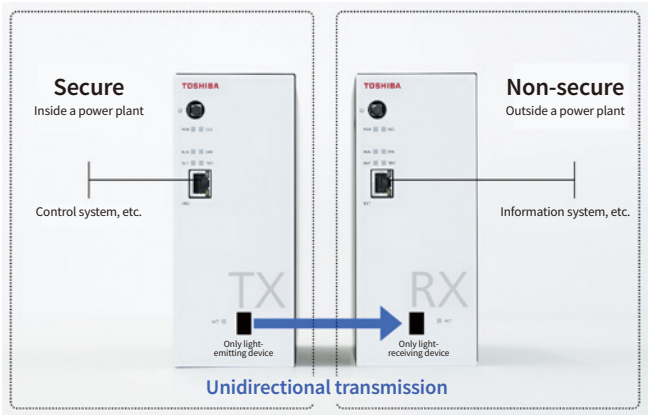
To meet the security requirements in the fields of energy, social infrastructure, electronic devices, etc., Toshiba Group provides various products, systems, and services for cyber security.

Unidirectional gateways: TOSMAP-DS™/LX OWB

Toshiba Energy Systems & Solutions Corporation

With the recent liberalization of the electricity market, the monitoring and control systems for power plants are becoming increasingly diverse, driving the need for efficient and advanced monitoring. For example, there is an increasing need for integrated remote monitoring and sophisticated analysis using operational data of power plants. To meet this need, it is necessary to fully protect the monitoring and control functions of power plants while sending data to external sites.
Against this background, Toshiba Energy Systems & Solutions Corporation has developed the TOSMAP-DS™/LXOWB unidirectional gateways that secure the network inside power plants. To protect the internal network, the TOSMAP-DS™/LXOWB physically blocks communications from the external world while allowing unidirectional data transmissions to the external world. Therefore, the TOSMAP-DS™/LXOWB provides robust network security.
The TOSMAP-DS™/LXOWB consists of a pair of separate transmitter (TX) and receiver (RX) units, with the TX unit having only a light-emitting device and the RX unit equipped only with a light-receiving device. This configuration clearly defines the network security boundary, physically allowing data to be transmitted in one direction only. The TOSMAP-DS™/LXOWB is designed in such manner that it can easily be added to an existing control system of a power plant to achieve advanced secure monitoring of its operation. With Achilles Communication Certification Level 2, the TOSMAP-DS™/LXOWB provides superior robustness* capable of detecting unknown security vulnerabilities. As a successor, we have also released the TOSMAP-DS™/LXOWR that is smaller and provides higher performance than the TOSMAP-DS™/LXOWB.

*Robustness: the property of being strong and unlikely to be affected by external



TOSMAP-DS™/LX OWB

TOSMAP-DS™/LX OWR

IoT security solution: CYTHEMIS™

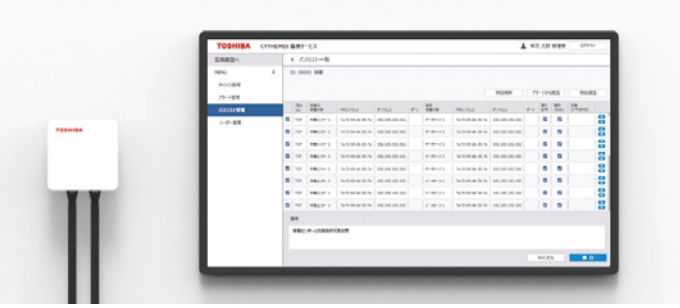
Toshiba Infrastructure Systems & Solutions Corporation

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

Accompanying the growing demand for personal data protection, the importance of information security of storage products is increasing. Toshiba provides hard disk drives (HDDs) suitable for various applications, including client HDDs for personal mobile devices and multifunction printers (MFPs), and enterprise HDDs for data centers.
Security requirements for HDDs include prevention of data leakage in the event of theft or loss. A function for wiping out all data is also required for HDDs to prevent data leakage after disposal.
To meet these customer requirements, we develop self-encrypting drives (SEDs). Toshiba's high-capacity, high-performance nearline HDDs for cloud data centers automatically encrypt the written data internally using AES*1, a standard encryption algorithm specified by the U.S. National Institute of Standards and Technology (NIST). These HDDs also support access control using the ATA*2 Security Feature Set (in the case of ATA models), TCG*3 Opal SSC*4, and TCG Enterprise SSC to prevent retrieval of protected data without password authentication. These features provide data leakage protection.
Furthermore, our HDDs for cloud data centers incorporate Cryptographic Erase that allows the user to instantaneously invalidate all data in the drive simply by changing a data encryption key without a costly overwriting process.
Certified under the Cryptographic Algorithm Validation Program (CAVP) based on FIPS PUB 140-3 of the U.S government (A1637, A1638, and A1645), the encryption algorithm of these HDDs provides a guaranteed security reliability. In addition, we are preparing to obtain CMVP*5 certification based on FIPS PUB 140-3 for the MG09*CP18/16TA*6. Under CMVP, a third-party organization evaluates the entire HDD unit as a cryptographic module in terms of its design, implementation, and operation.

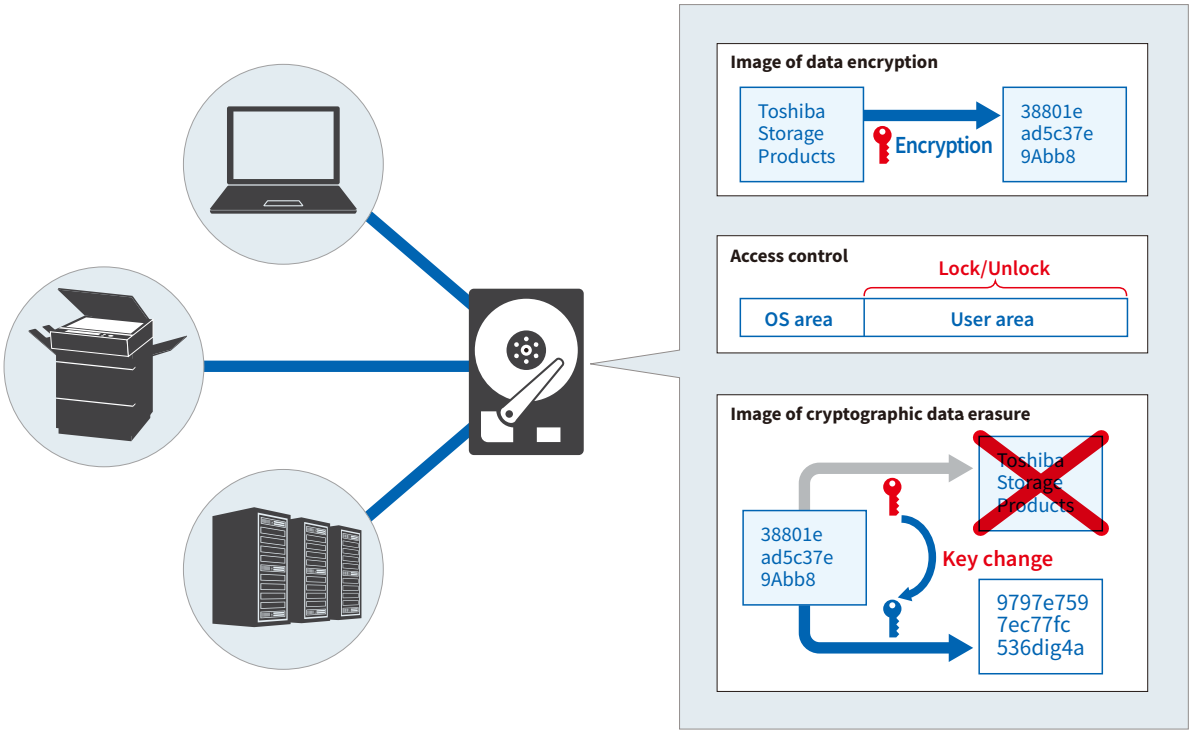


Image of security features of storage products

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

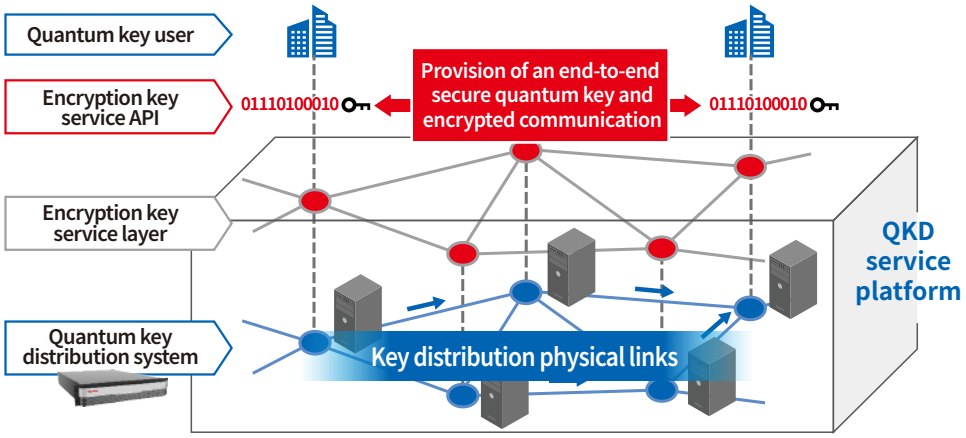
Quantum Key Distribution System

Toshiba Digital Solutions Corporation

Nowadays, information and communication networks represented by the Internet are essential in everyday life. With the ever-increasing spread of IoT, we will become more dependent on networks.
On the other hand, the progress of quantum computers is remarkable. Large quantum computers will appear at some point in the future. Because of their overwhelming computing power, quantum computers will be able to break modern encryption schemes that are widely used in the Internet, exposing computer networks to a greater risk of information leakage.
Quantum key distribution (QKD) is a technology to combat such a risk. QKD is theoretically unbreakable no matter how fast quantum computers run. It uses a single photon, an elementary particle of light, to distribute quantum keys for encryption in order to prevent eavesdropping by virtue of the principles of quantum mechanics.
Toshiba Group has been leading research on QKD for more than 20 years, setting a new record for the key rate (i.e., the number of quantum keys sent per unit of time).
Our QKD system will ensure secure quantum keys into the future. We have now commenced the demonstration of a QKD service in multiple cities around the world. Secure quantum keys can easily be used via a standardized application programming interface (API)*.
Our next step is to deploy this system on large networks to provide quantum key distribution services for many customers in various fields.

*ETSI GS QKD 014

Quantum key distribution system



QKD service platform

e-STUDIO5525AC/e-STUDIO5528A MFP series

Toshiba Tec Corporation

Widely used at offices and shops, multifunction peripherals (MFPs) incorporate the functionality of multiple devices, including a photocopier. Connected to a network, MFPs allow documents to be scanned and stored on the cloud and printed from the cloud. MFPs require security protection from cyberattacks in order to prevent leakage of and tampering with confidential information as well as data destruction and failures of the MFPs themselves.

Certified under ISO/IEC 15408*1 known as Common Criteria (CC), the e-STUDIO series of MFPs are compliant with HCD-PP*2, the latest and most stringent security standards for MFPs. HCD-PP stipulates security requirements for cryptographic modules that are equivalent to those of FIP PUB 140-2*3 of the U.S. government. Compliance with HCD-PP means that the e-STUDIO series provides the highest security level.

In addition, the e-STUDIO5525AC and e-STUDIO5528A series offer various security enhancements, including anti-malware, TPM*4 2.0, secure boot, and fingerprint authentication functions.

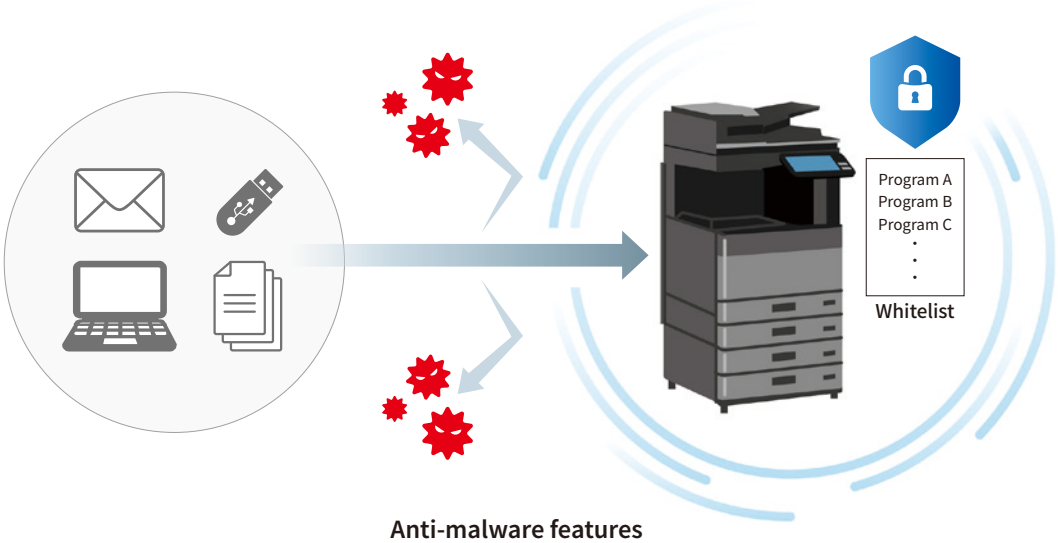
The anti-malware function allows the execution of only authorized, safe software to prevent malware infection.

TPM 2.0 enables secure storage of encryption keys and thus prevents the encrypted data from being compromised even in the event of a storage medium being stolen. Therefore, confidential information stored in an MFP can be protected. The secure boot function detects tampering with the boot program of an MFP.

Furthermore, the e-STUDIO5525AC and e-STUDIO5528A series support fingerprint authentication in addition to the conventional card-based and NFC authentication. The use of biometric information allows fast and secure personal authentication.

As a result of a cyberattack test at Toshiba's Corporate Research & Development Center, it was confirmed that these security features withstand possible cyberattacks that security experts expect.

As described above, the e-STUDIO series protects customers' information assets from various cybersecurity threats.



Anti-malware features

*1 ISO/IEC 15408 : International Organization for Standardization/International Electrotechnical Commission Standard 15408
*2 HCD-PP : Hard Copy Device – Protection Profile
*3 FIPS PUB 140-2 : Federal Information Processing Standard 140-2
*4 TPM : Trusted Platform Module

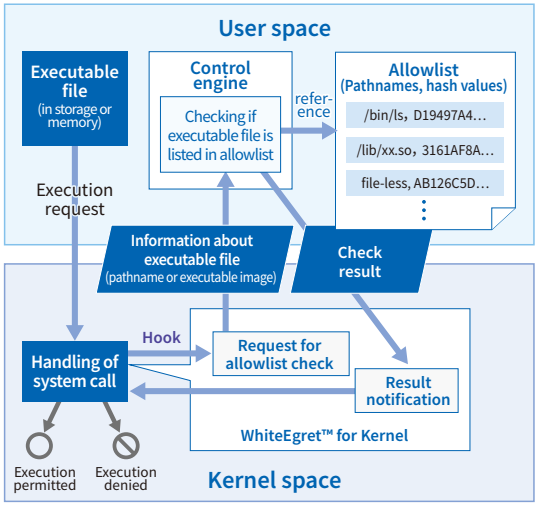
R&D

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

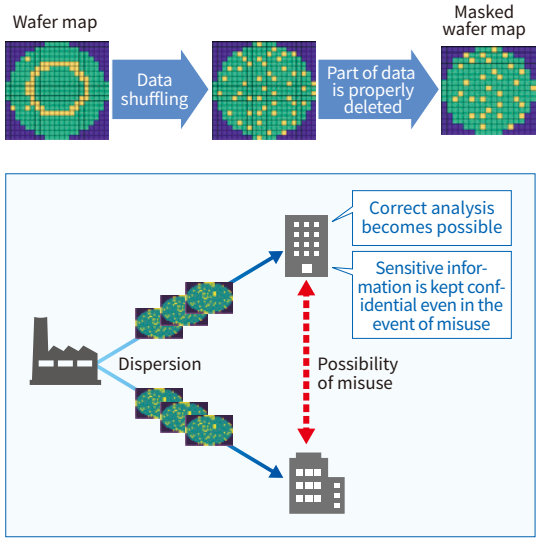


Data processing technology combining security and usefulness

Productivity improvement and other benefits can be obtained by properly analyzing and using industrial data such as wafer maps* in semiconductor manufacturing. However, furnishing external parties with such data to achieve full data utilization increases the risk of leakage of sensitive information contained in industrial data. Conversely, use of an encryption or other security technology makes it difficult to perform an analysis with a high degree of flexibility.
To resolve this dilemma, Toshiba has developed data masking technologies to ensure both security and analyzability.
These technologies are capable of protecting sensitive information by properly shuffling and deleting data, making data misuse impossible.

*Wafer map: Data showing the distribution of non-defective and defective chips on a silicon wafer

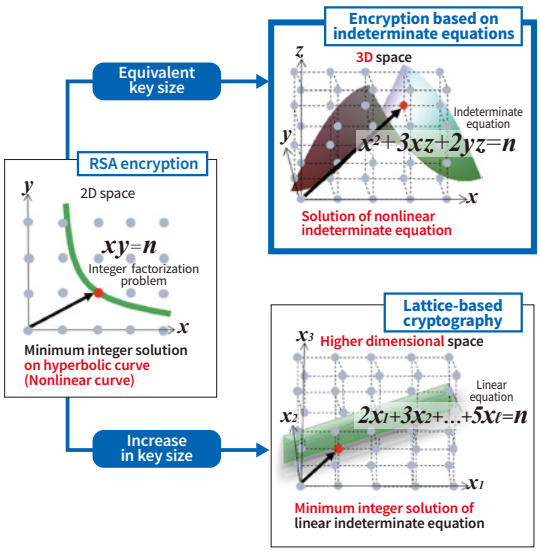
Reference: HANATANI Yoshikazu, et al. "Toward a secure and analyzable data masking method for wafer maps." SCIS2022 (in Japanese)



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.

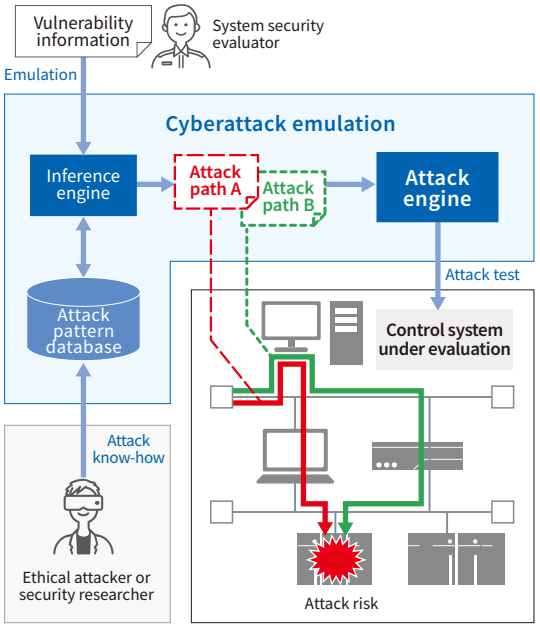
Reference: AKIYAMA Koichiro et al. "A Public-key Encryption Scheme Based on Non-linear Indeterminate Equations (Giophantus)," https://eprint.iacr.org/2017/1241, 2017



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.

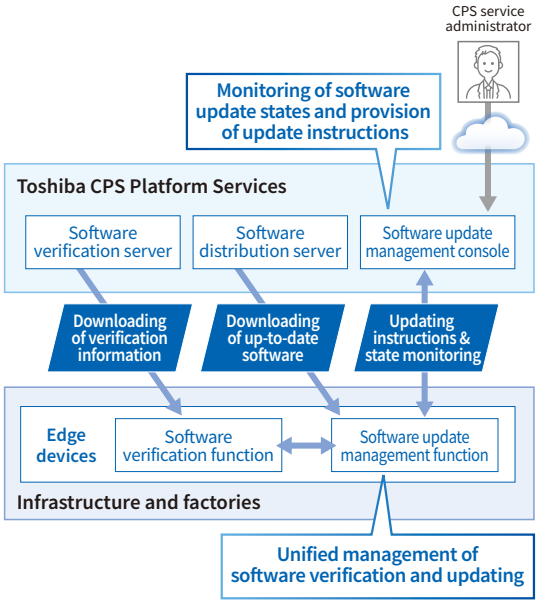
Reference: NAKANISHI Fukutomo, et al. "Automated Attack Path Planning and Validation (A2P2V)." BlackHat USA Arsenal 2021. https://github.com/pentest-a2p2v/



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



External Activities

As of March 31, 2022

Toshiba Group participates in various standardization 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, Industrial Security Action Group
- Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development
- 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)
- Japan Digital Trust Forum (JDTF)
- Factory Sub-working Group under Working Group 1 (Systems, Technologies and Standardization) of the Study Group for Industrial Cybersecurity at the Ministry of International Trade and Industry (METI)

etc.

Third-Party Assessment and Certification

As of March 31, 2022

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 Information Systems Corporation
Toshiba Infrastructure Systems & Solutions Corporation (SA Division at Komukai Complex)
Toshiba Information Systems (Japan) Corporation
Toshiba Digital Engineering Corporation (Oita Complex)
Toshiba Digital Engineering Corporation (Digital Engineering Division 2)
Toshiba Digital Engineering Corporation (Head Office Digital Engineering Division 3)
Toshiba Digital Solutions Corporation
Toshiba Digital Marketing Initiative Corporation
(Server Service Group and Application Service Group, Web Platform Department, Solutions Division)
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 Business Support Department,
TBLS Business Division and Shiba Daimon Juku, Human Resource Development Department
Toshiba Lifestyle Products & Services Corporation
TEC Information Systems Corporation
Enterprise Business System Solutions Corporation
SBS Toshiba Logistics Corporation
Chubu Toshiba Engineering Corporation (Headquarters, Yokohama Complex)

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 2022).

Product	TOE*2 Class	Certification Number	PP and EAL
TOSHIBA e-STUDIO330AC/400AC Model with a fax unit and a FIPS hard disk kit	Digital MFP	C0684	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO 2515AC/3015AC/3515AC/4515AC/5015AC with a fax unit (GD-1370J/GD-1370NA/GD-1370EU), and a FIPS hard disk kit (GE-1230)	Digital MFP	C0633	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO5516AC/6516AC/7516AC with a fax unit (GD-1370J/GD-1370NA/GD-1370EU) and a FIPS hard disk kit (GE-1230)	Digital MFP	C0632	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A with a fax unit (GD-1370J/GD-1370NA/GD-1370EU), and a FIPS hard disk kit (GE-1230) SYS V1.0	Digital MFP	C0631	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO5518A/6518A/7518A/8518A with a fax unit (GD-1370J/GD-1370NA/GD-1370EU) and a FIPS hard disk kit (GE-1230)	Digital MFP	C0630	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO2010AC/2510AC with a fax unit (GD-1370J/GD-1370NA/GD-1370EU) and a FIPS hard disk kit GE-1230)	Digital MFP	C0629	PP conformance (Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)
TOSHIBA e-STUDIO3508LP/4508LP/5008LP、Loops LP35/LP45/LP50 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0566	EAL2*3+
TOSHIBA e-STUDIO5508A/6508A/7508A/8508A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0529	EAL3+
TOSHIBA e-STUDIO5506AC/6506AC/7506AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0528	EAL3+
TOSHIBA e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0524	EAL3+
TOSHIBA e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0523	EAL3+
TOSHIBA e-STUDIO2000AC/2500AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0	Digital MFP	C0522	EAL3+
TOSHIBA e-STUDIO5560C/6560C/6570C MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	Digital MFP	C0491	EAL3+
TOSHIBA e-STUDIO557/657/757/857 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	Digital MFP	C0490	EAL3+
TOSHIBA e-STUDIO207L/257/307/357/457/507 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0	Digital MFP	C0489	EAL3+
TOSMART-GP1 (Supporting PACE PP-0499)	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-GP1 (Supporting PACE and BAC PP-0500)	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
Microcontrôleur sécurisé T6ND7 révision 4	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
Toshiba T6NE1 HW version 4	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-P080-AAJePassport	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
TOSMART-P080 ePassport 01.06.04 + NVM Ver.01.00.01	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
T6ND1 Integrated Circuit with Crypto Library v6.0	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+
FS Sigma Version 01.01.05	ICs, Smart Cards and Smart Card-Related Devices and Systems	—	EAL4+

*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): Software and hardware products to be evaluated TOE sometimes includes user's manuals, guides, installation procedures, and other documents written for administrators and users.

*3 EAL (Evaluation Assurance Level): Numerical rating as per ISO/IEC 15408 describing the depth and rigor of an evaluation. There are seven levels from EAL 1 to EAL 7, with EAL 1 being the most basic and EAL 7 being the most stringent.

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 that is operated by IPA and those certified under the Cryptographic Module Validation Program (CMVP) based on FIPS140-2*2 that is operated by the National Institute of Standards and Technology (NIST) of the U.S. and the Communications Security Establishment (CSE) of Canada (as of March 2021).

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 FIPS140-2: Federal Information Processing Standard that stipulates the security requirements for cryptographic modules that include both hardware and software components

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-CIEDS/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 frauld/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.

Toshiba Group Business Overview

As of March 31, 2022

Company Overview

Company Name: TOSHIBA CORPORATION

Headquarters Address: 1-1-1 Shibaura, Minato-ku, Tokyo 105-8001, Japan

Founded: July 1875

Paid-in capital: ¥200,869 million

Consolidated Net Sales: ¥3,337.0 billion(FY2021)

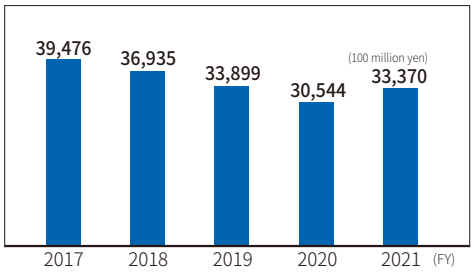
Number of Employees: (consolidated) 116,224

Number of Shares Issued: 433.14 million shares

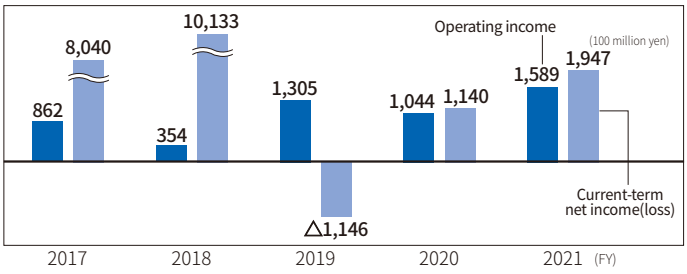
Stock Exchange Listings: Japan: Tokyo and Nagoya

Consolidated business results

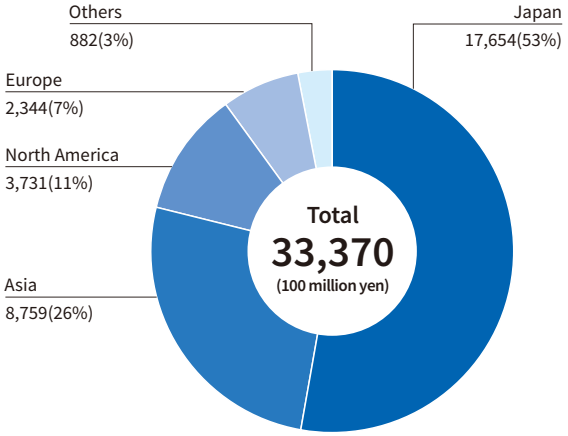
Net sales



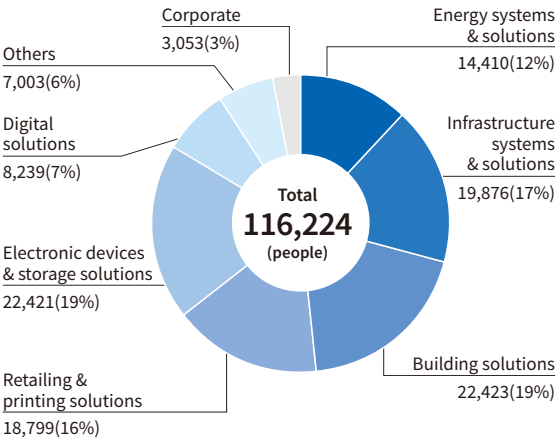
Changes in operating income and net income(loss)



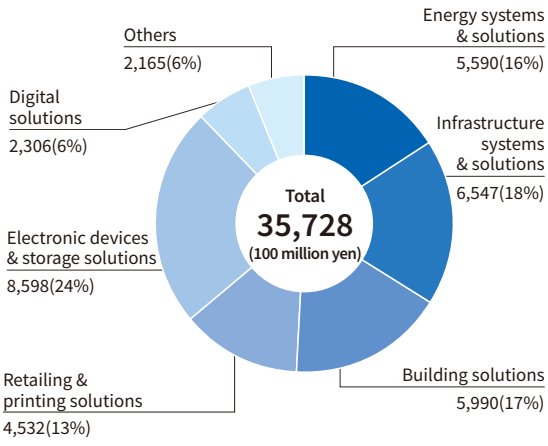
Net sales by region



Number of employees by segment



Net sales by segment



(Including an inter-segment elimination of 235,800 million)

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

Published in August 2022