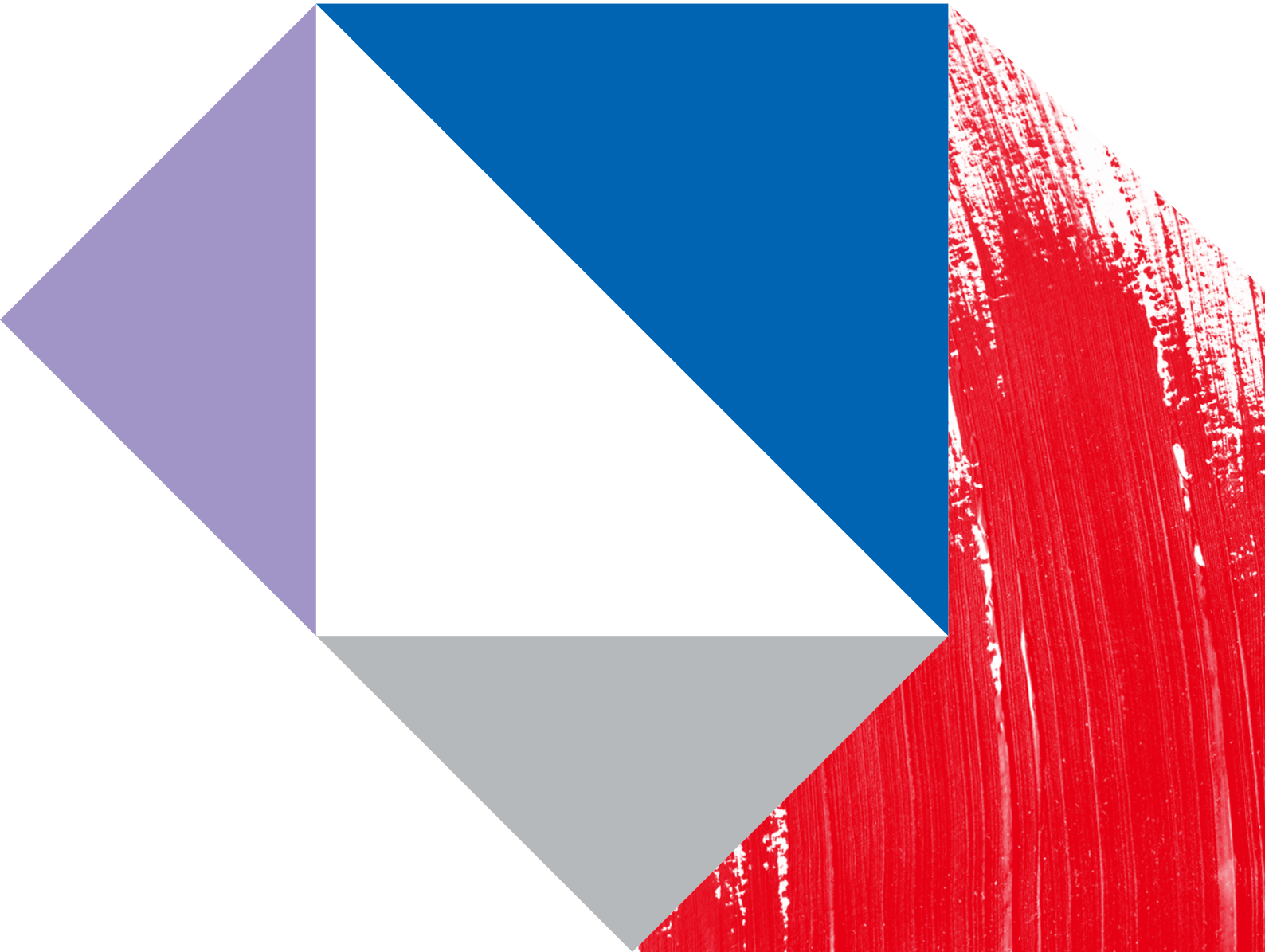
TOSHIBA

2020 Cyber Security Report



Message from the Chief Information Security Officer (CISO)

Delivering safety and security to everyone in the cyber and physical worlds

In recent years, ICT technology has been evolving in various fields and becoming progressively integrated into our everyday lives. In particular, digital technology has enabled information sharing and communication beyond physical space, transforming our lifestyles and social infrastructure. Toshiba Group possesses extensive experience and expertise in monozukuri—the art, science and craft of making things—cultivated for 145 years since its founding in 1875. We are currently committed to providing solutions in the fields of energy, social infrastructure, electronic devices, and digital products by combining this expertise with digital technology. The paramount priority for our business operations is to deliver safety and security to everyone.

Accompanying the progress of IoT technology, cyber space typified by the Internet is becoming fused with the physical space where we live. In response to this change in the social environment, Toshiba Group aims to support people's lives through cyber-physical system (CPS) technology. CPS analyzes huge amounts of data collected from physical space in cyber space in order to generate valuable intelligence and feeds it back to physical space. Therefore, enhancing the security of cyber space helps provide increased protection of physical space. Toshiba Group is committed to offering secure CPS to protect against formidably sophisticated and diverse cyberattacks and thereby ensure the safety and security of people's lives.

The purpose of Cyber Security Report 2020 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 Vice President and CISO
Toshiba Corporation

Hideaki Ishii

TOSHIBA

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. We possess extensive experience and expertise cultivated through more than 140 years of monozukuri—the art, science and craft of making things—in a wide range of fields, including the design, development, and operation of electricity supply facilities, public transportation systems, semiconductor devices, and large-scale plants. The breadth of our experience and expertise is a definite advantage in confronting cyber-crime. 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 also 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.

2020 Cyber Security Report

Contents

Chapter 1

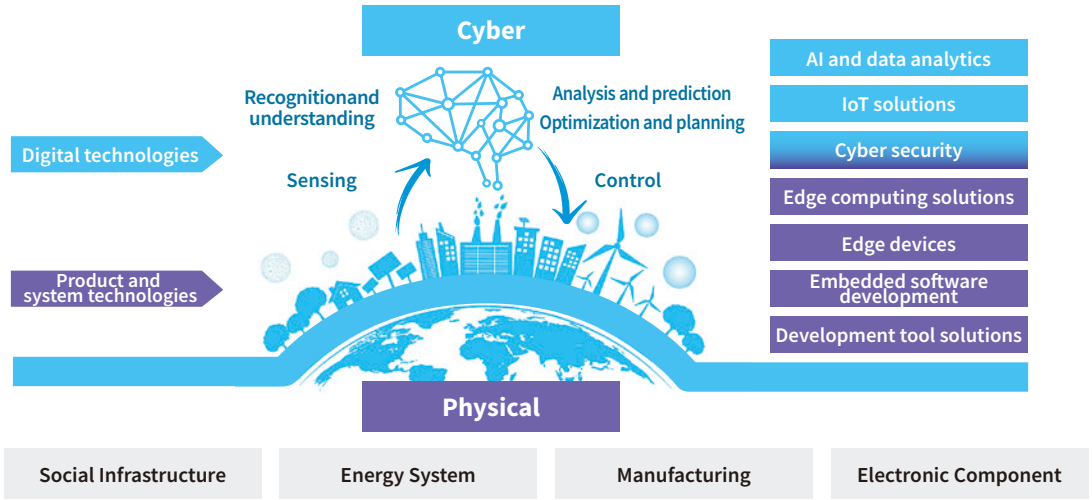
Visions and Strategies

Toshiba Group aims to become one of the world's leading cyber-physical systems (CPS) technology enterprises through integration of cyber and physical technologies so as to fulfill its role in solving social issues. On the other hand, with digital transformation spurred by the progress of the Internet of Things (IoT), a myriad of physical devices are becoming connected to the network, increasing the threat of cyberattacks. Within the purview of this threat now are not only information systems but also industrial control systems and products, exposing social infrastructure to ever-greater risk of cyber-induced physical damage.

Toshiba Group possesses extensive expertise in the physical realm cultivated through more than 140 years of experience in various business areas as well as know-how for information security acquired from the operation of information systems supporting roughly 130,000 employees. As an enterprise promoting cyber-physical integration, we consider that it is our responsibility to combine both cyber and physical expertise to enhance cyber security, aiming to ensure the safety and security of our products, systems, and services and to support customers' business continuity.

Toshiba's Cyber Security Visions

CPS technology enterprise envisioned by Toshiba Group



A cyber-physical system (CPS) is a mechanism to collect physical data, analyze the collected data in cyber space using digital technology or translate them into easy-to-use information or knowledge, and feed it back to the physical realm so as to create new value.

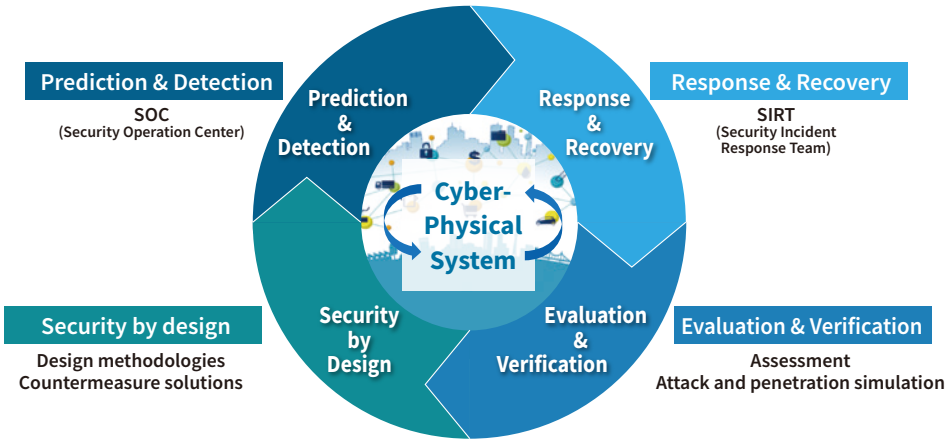
Toshiba Group possesses extensive knowledge and expertise in social infrastructure and other sectors as well as a huge amount of data accumulated through business activities over many years. Toshiba Group also has world-leading cyber technology. Therefore, with the aim of becoming a CPS technology enterprise capable of spurring technological innovation in various fields, Toshiba Group is endeavoring to combine physical technologies cultivated since its founding with cyber technologies in order to realize cyber-physical systems that will create new value. Cyber-physical systems will be utilized to facilitate digital transformation of social infrastructure in order to solve social issues such as growing energy demand, depletion of natural resources, climate change, concentration of the population in urban areas, an increase in logistics, population aging, and labor shortages.

Toshiba Group's cyber security visions

Digital transformation is progressing in a wide range of industrial and social sectors through the use of cyber-physical systems incorporating IoT, AI, cloud, and other digital technologies. However, as a myriad of physical devices become interconnected via networks, cyber threats are expanding to include control systems and devices for social infrastructure, exposing them to the increasing risk of cyber-induced physical damage. Even under these circumstances, the mission of Toshiba Group remains the same—to support the business continuity of its customers and help realize a safe and secure society. To fulfill this mission, it is essential to accurately assess the convenience of cyber-physical systems 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.

In view of this, Toshiba Group is endeavoring to enhance cyber security not only for internal information systems and production systems at its factories and other manufacturing facilities but also for its products, systems, and services to be offered to customers. Furthermore, Toshiba Group endeavors not only to ensure protection via security by design* at the design and development stages but also to predict and be prepared for security risks by constantly monitoring internal and external security threats. Toshiba Group quickly responds to security incidents to minimize damage and expedite business recovery from attacks. We also emphasize "security lifetime protection," a concept that stresses 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 design and development processes.

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



Security Lifetime Protection

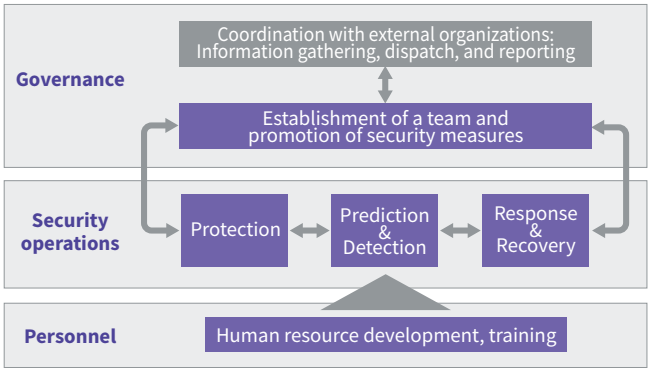
To realize this, Toshiba Group defines cyber security management as a series of organically connected processes from six perspectives: 1) governance, 2) protection, 3) prediction and detection, 4) response and recovery, 5) evaluation and verification, and 6) personnel. Toshiba Group has set its goals as "Toshiba Cyber Security Visions" from these perspectives. We endeavor to enhance our cyber security initiatives to become a trusted partner for our customers so that they can use our products and services without any security concerns.

Governance	Continuously increasing the maturity level of cyber security management through PDCA cycles
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 been pursuing strategies for enhancing its cyber security preparedness to achieve sustainable operation and continual improvement of the cyber security management processes. Here, "cyber security preparedness" means a state of being fully prepared for extensive security risks. Specifically, it encompasses three elements: 1) governance to clarify decision-making processes and a chain of command, 2) security operations, including prediction & detection, response & recovery, and protection, 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 as shown in the figure at right.



Cyber security management processes

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 (the then President and the current CEO of Toshiba Corporation). 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 risk concerning information assets and personal data stored in in-house information systems and the PSIRT*2 responsible for managing security risk concerning products, systems, and services provided by Toshiba Group. The CSIRT and PSIRT cooperate to ensure that all systems at Toshiba's factories and manufacturing facilities are properly secured. Furthermore, the CSIRT and the PSIRT work in tandem to achieve the advanced cyber security needed as a manufacturer in order to promote common use of processes and personnel and share their expertise with each other. 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 serving as a liaison with the Cyber Security Center, promoting the sharing of internal and external information. The Cyber Security Center also 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.

To strengthen security operations such as prediction & detection, response & recovery, and protection, the Cyber Security Center is developing the Cyber Defense Management Platform (CDMP). In view of the ever-increasing threat to Toshiba Group, the Cyber Security Center now needs to protect not only internal IT infrastructure but also factories and other production facilities as well as products, systems, and services, and in the future, customers' and suppliers' systems. However, since security personnel are limited, it is necessary to realize high-accuracy security operations even with minimal personnel. The CDMP realizes extensive security monitoring and accurate detection and prediction while automating the tasks required to deal with and recover from security incidents. Furthermore, the Cyber Security Center actively promotes the collection and utilization of internal and external threat intelligence, accumulation of knowledge, and utilization of artificial intelligence (AI) in order to reduce the time required for and improve the accuracy of threat detection and response. The Cyber Security Center is shifting from reactive responses to proactive prediction and control in order to minimize the impact of security risk 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 reinforce security personnel. The roles of the Cyber Security Technology Center encompass R&D, technical support, and implementation assistance regarding cyber security technology. It cooperates with the Cyber Security Center to provide assistance in relation to security technologies during product development, develop fundamental security technologies, and train and reinforce specialized personnel. In order to improve the security level of the entire Toshiba Group, we have also established an education system to provide all employees with adequate education. It consists of information security courses on the management and protection of personal and other types of information and product security courses on ensuring the security of products, systems, and services.

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

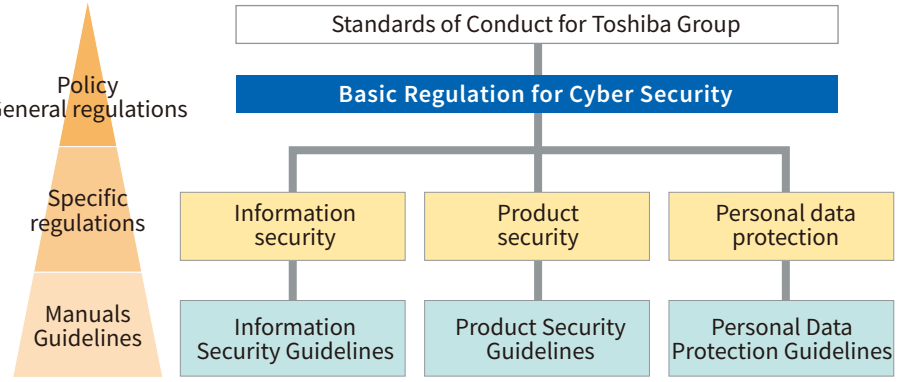
*1 Computer Security Incident Response Team
*2 Product Security Incident Response Team

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. This section provides an outline of these regulations and our cyber security management system.

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.

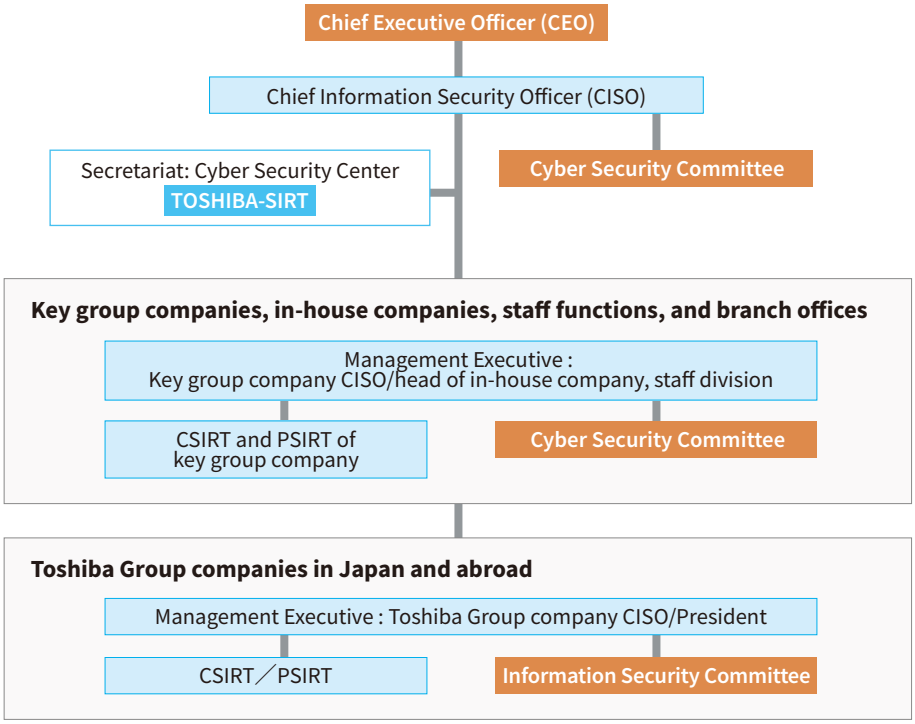
Toshiba's privacy policy: http://www.toshiba.co.jp/privacy/index.htm

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 and planning cyber security schemes and measures, which are discussed by the Cyber Security Committee. 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. The Cyber Security Committee discusses matters necessary for thorough cyber security management of the entire Toshiba Group and how to respond to cyber security incidents that could develop into a major crisis.

Each key group company overseeing other subsidiaries also has a CISO, who is responsible for the promotion 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 subsidiaries operating under its umbrella. In addition, 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

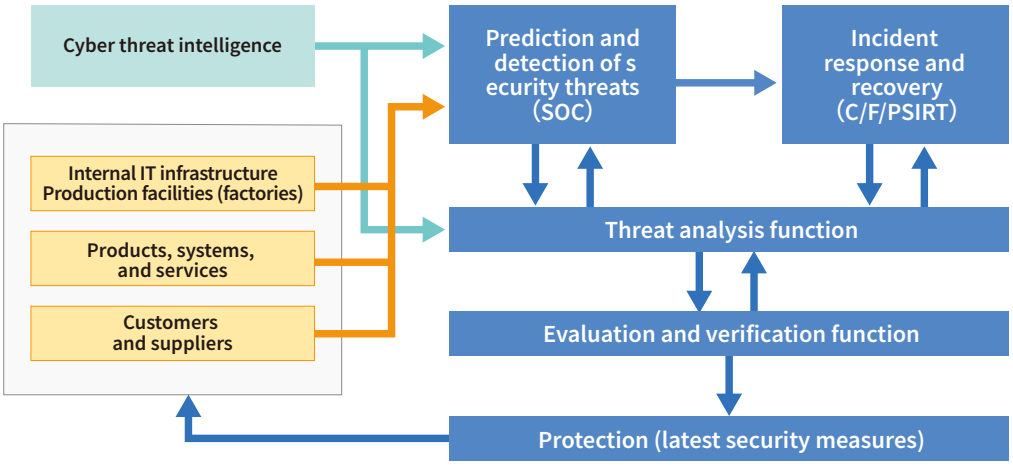
Security Operations

This section describes the initiatives undertaken by Toshiba Group to enhance its security operations. Toshiba Group is currently developing a security management platform called the CDMP*1 with the aim of increasing the accuracy and speed of security risk detection and response. 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.



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

Cyber Defense Management Platform (CDMP)

The CDMP consists of the following functions:

- Prediction and detection of security threats (SOC)
  ⇒ Detecting security incidents by monitoring system states (see page 11)
- Incident response and recovery (C/F/PSIRT)
  ⇒ Responding to security incidents and recovering the affected systems (see pages 13 and 22)
- Threat analysis function
  ⇒ Preventing cyber threats by using threat intelligence (see page 19)
  ⇒ 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 14)
- Protection
  ⇒ Protection using state-of-the-art security measures (see page 16)

The threat to Toshiba Group is ever increasing. Since resources are limited, Toshiba Group is endeavoring to automate the responses to and the recovery from security incidents while accumulating knowledge and using artificial intelligence to realize high-accuracy security operations with slim resources. To realize automation, we are working on the deployment of a platform called SOAR (Security Orchestration, Automation and Response).

Human Resources Development

This section describes Toshiba Group's programs for the development of cyber security personnel. In order to enhance security consciousness, Toshiba Group provides education on information security, personal data protection, and product security for all employees. In addition, Toshiba Group endeavors to develop highly-skilled security personnel responsible for improving security quality at the product development stage and for responding to security incidents.

Education on information security and personal data protection

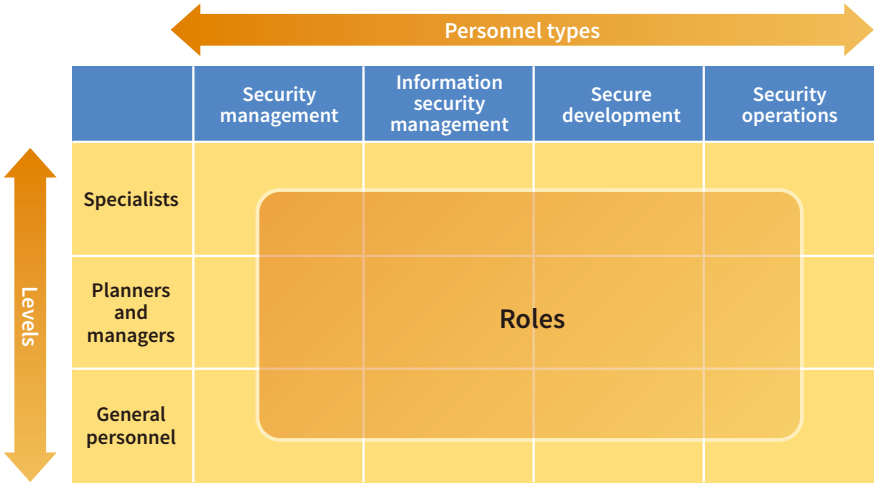
To prevent information leakage, each employee must acquire knowledge necessary to properly handle the information encountered in the course of work and enhance awareness of security threats such as targeted attacks. Toshiba Group provides all officers and employees with e-learning programs every year incorporating the latest information, including on adequacy decision concerning the transfer of personal data obtained from countries in the EU, which are available in multiple languages for overseas employees. Toshiba Group also provides education about information security and personal data protection at career milestones such as at the time of employment and promotion.
Toshiba Group has created the Information Security Handbook that plainly describes the rules, regulations, and guidelines that all employees of Toshiba Group need to understand and act upon in the day-to-day performance of their duties.

Product security education

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. In addition to information security education, Toshiba Group provides all officers and employees with e-learning programs every year addressing product security risk.

Training of advanced security personnel

In addition to the above education, Toshiba Group provides training for security personnel according to the types of their tasks and levels while defining the qualities of security personnel required. Training security personnel so as to ensure they possess the necessary specialized knowledge and expertise is not the only goal of human resource development. Toshiba Group also endeavors to train personnel so that they are capable of enhancing product security at the development stage and promptly responding to security vulnerabilities and incidents. In addition, Toshiba Group provides product security education for those in managerial positions.In order to ensure that product security practices are properly implemented in each department, Toshiba Group also provides product security education for those in managerial positions while endeavoring to develop cyber security personnel with extensive specialized knowledge and expertise capable of enhancing product security quality at the development stage and promptly responding to security vulnerabilities and incidents.



Qualities required for security personnel

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.

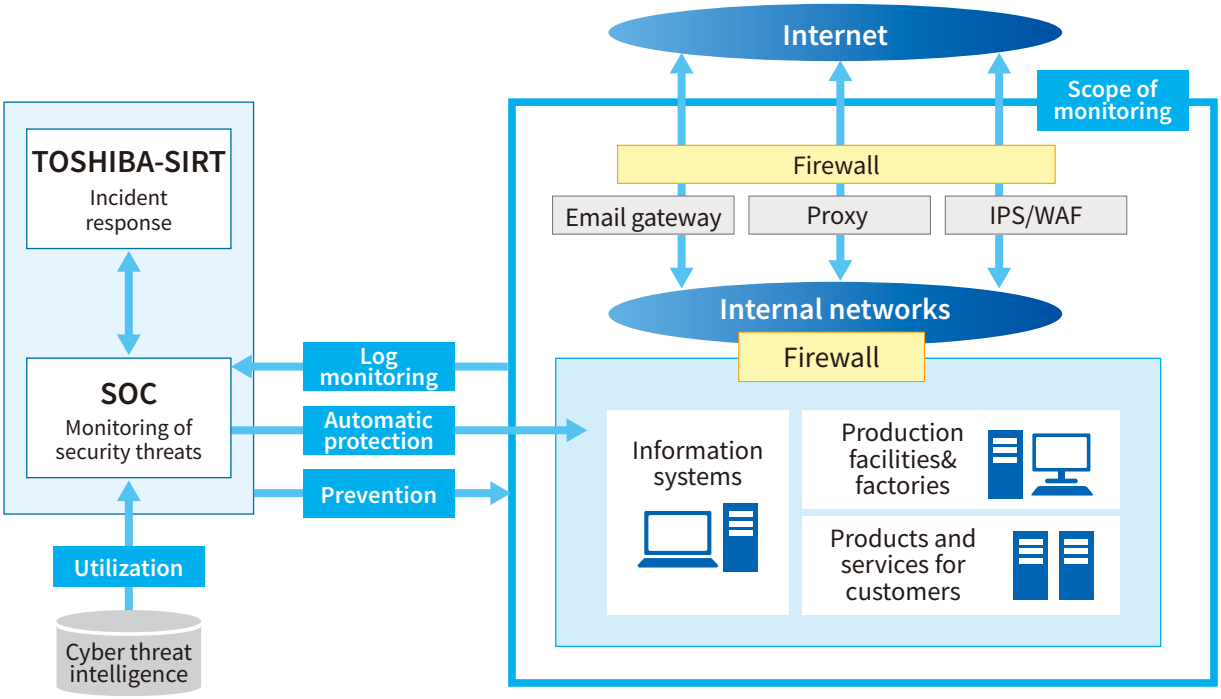
Security Measures for Internal IT Infrastructure

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 are shifting 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. In order to detect security risks promptly and accurately, the Security Operation Center (SOC) monitors the Internet gateway, PCs, servers, and other IT systems, factories, and customer services, and immediately responds to an alert in order to minimize damage. SOC uses external threat intelligence to prevent cyberattacks and enhance the security of all the organizations of Toshiba Group.
Specifically, SOC is enhancing the following measures:

- 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

Security Incident Response

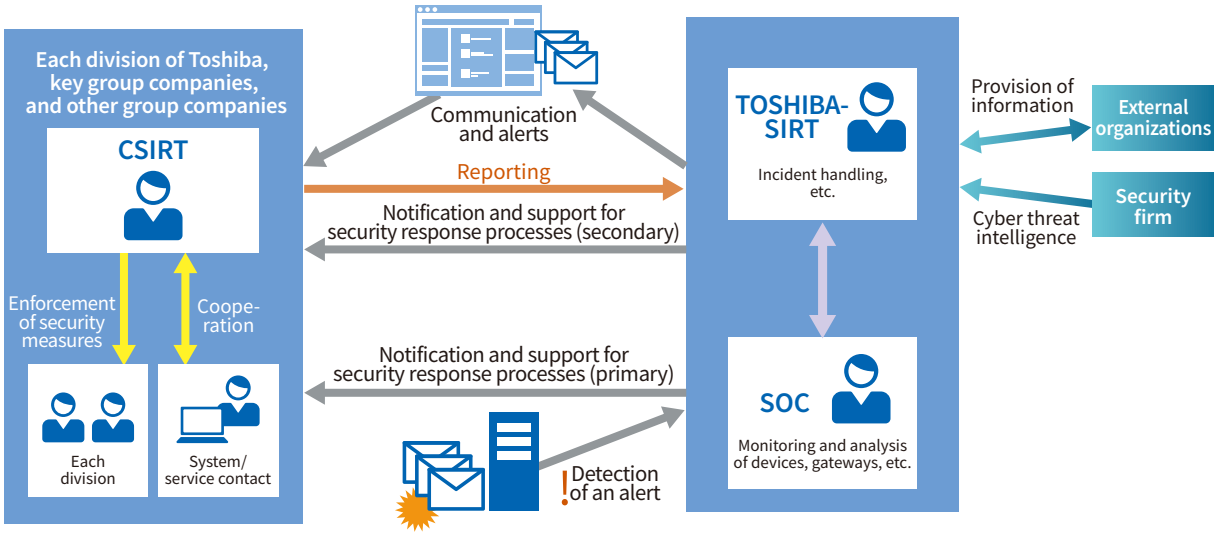
Response & Recovery

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 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 the CSIRT of the divisions of Toshiba and the CSIRT of each group company 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 the CSIRT of each division and group company, 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, TOSHIBA-SIRT has predefined response procedures, which are continually reviewed and improved through training and actual response to security incidents. Business could be affected by some security measures, for example, a disconnection of a network to prevent the spread of a malware. Even for such measures, TOSHIBA-SIRT has established predefined procedures and the criteria for their implementation, which have been disseminated throughout the Group so as to be able to respond promptly to any incidents and thereby minimize damage.

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.

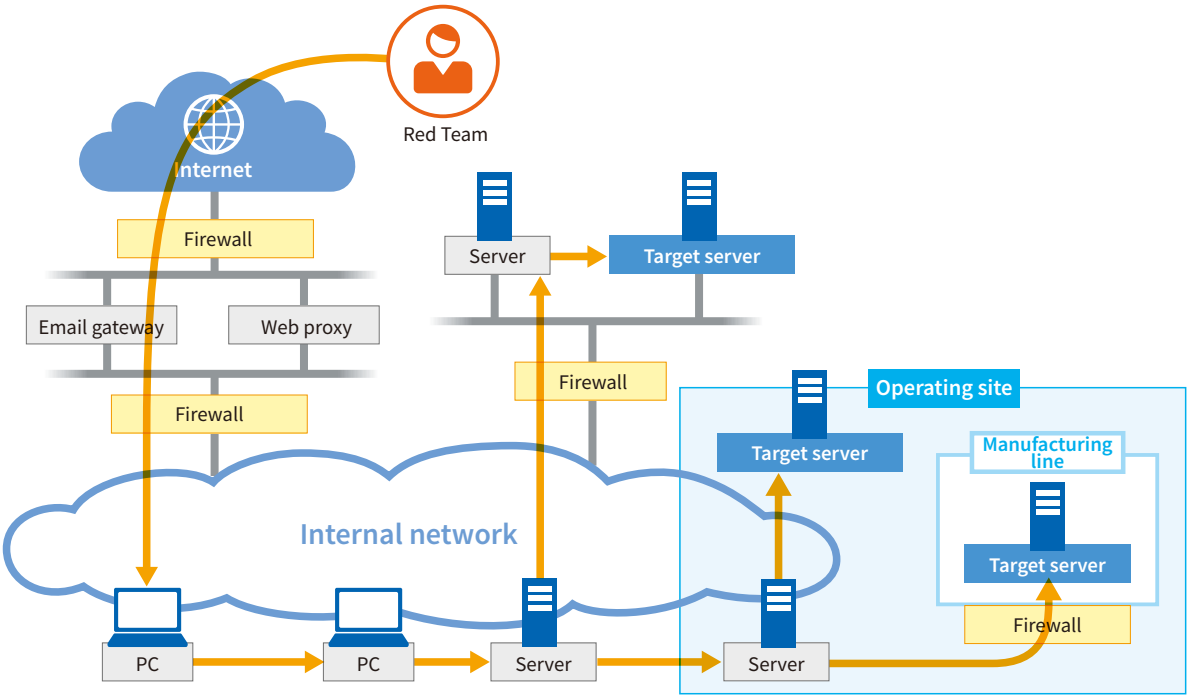
Advanced Attack and Penetration Assessment from Hacker's Perspective

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 has taken 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. We will continue to take such an assessment periodically.

In this assessment, the Red Team attempts to penetrate Toshiba Group's network using advanced tactics, techniques and procedures of real-world attackers, 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.

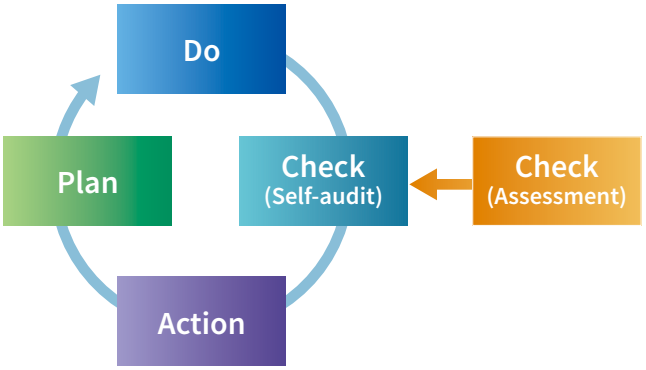
＊Red Team: An independent team that provides real-world attack simulations designed to assess the effectiveness of security systems and measures of an organization



Self-Audit and Security Assessment

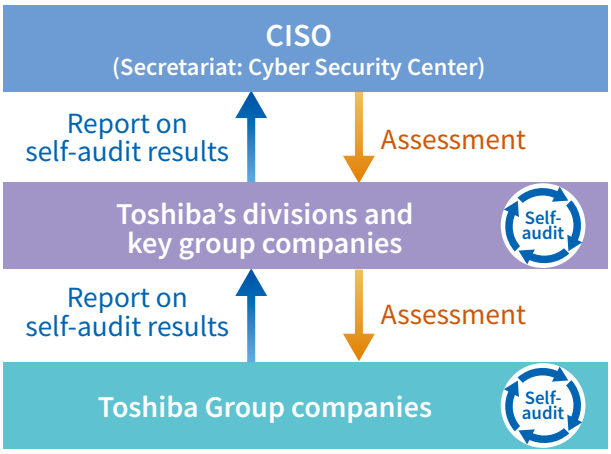
Evaluation & Verification

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



PDCA cycle based on a self-audit and assessment

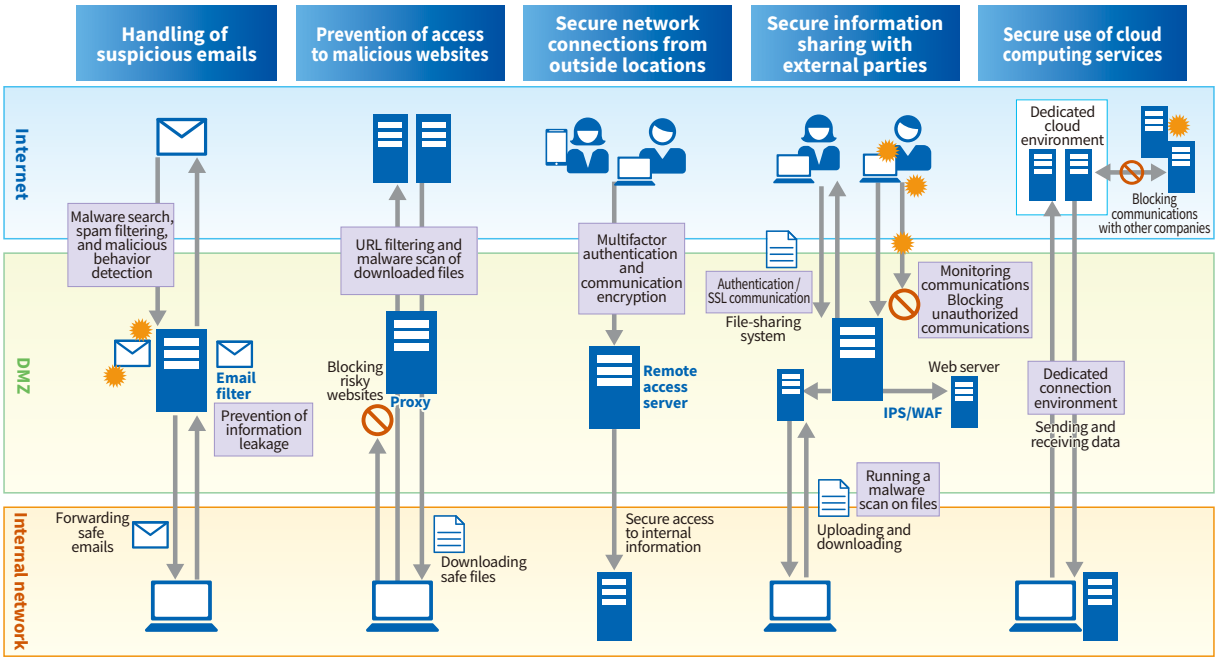
The Cyber Security Center, which serves as a secretariat, assesses the results of the self-audit and improvement activities of each division and provides guidance and support if corrective action is required. Toshiba Group companies in Japan and abroad conduct a self-audit every year. The Cyber Security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



Self-audit and assessment conducted by the entire Toshiba Group

Security Measures for Internet Connection Points

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 remote work as a means of promoting work style innovation.



- 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 such as malware-infected emails and internal information leakage. To seize 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 an average of roughly 500,000 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 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.

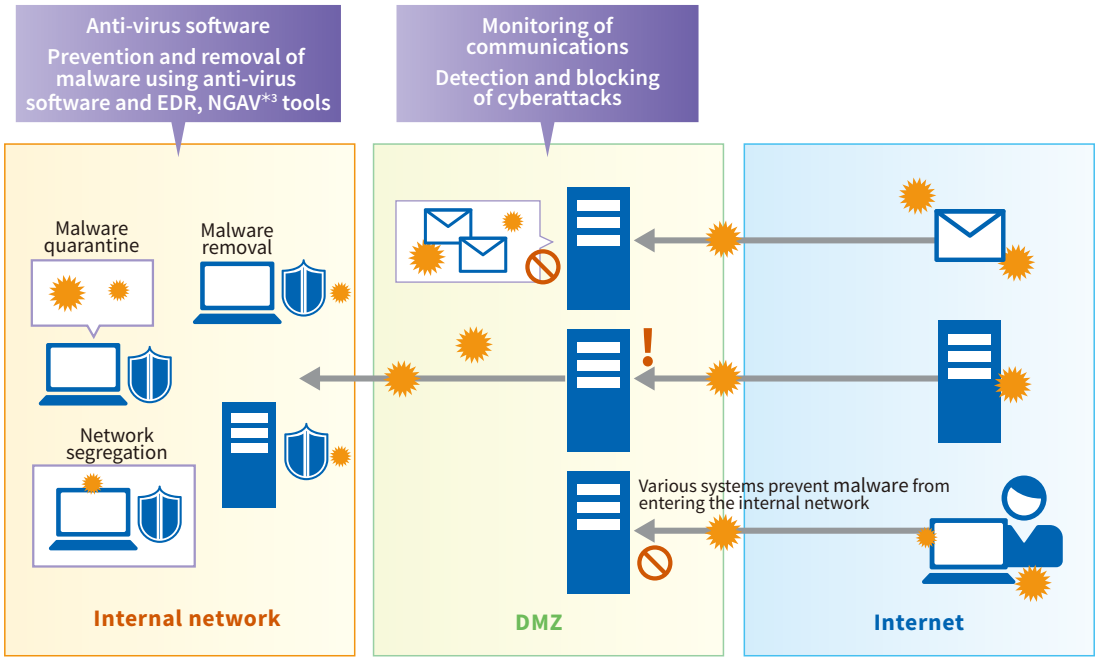
In addition to these common security measures, Toshiba Group keeps track of the settings of security devices and the network logs of the operating sites having their own Internet connection points. For protection from cyberattacks, Toshiba Group employs not only common measures but also additional measures 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.

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

Security by design

Toshiba Group has completed the installation of EDR tools on all PCs and servers in Japan, which are capable of detecting and blocking unknown malware that cannot be blocked by existing anti-virus software as well as sophisticated cyberattacks that cannot be detected at the Internet gateway. We will continue to deploy EDR tools overseas.

- Detecting suspicious network activities 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
- Tracking the causes and scope of damage from the collected operating log



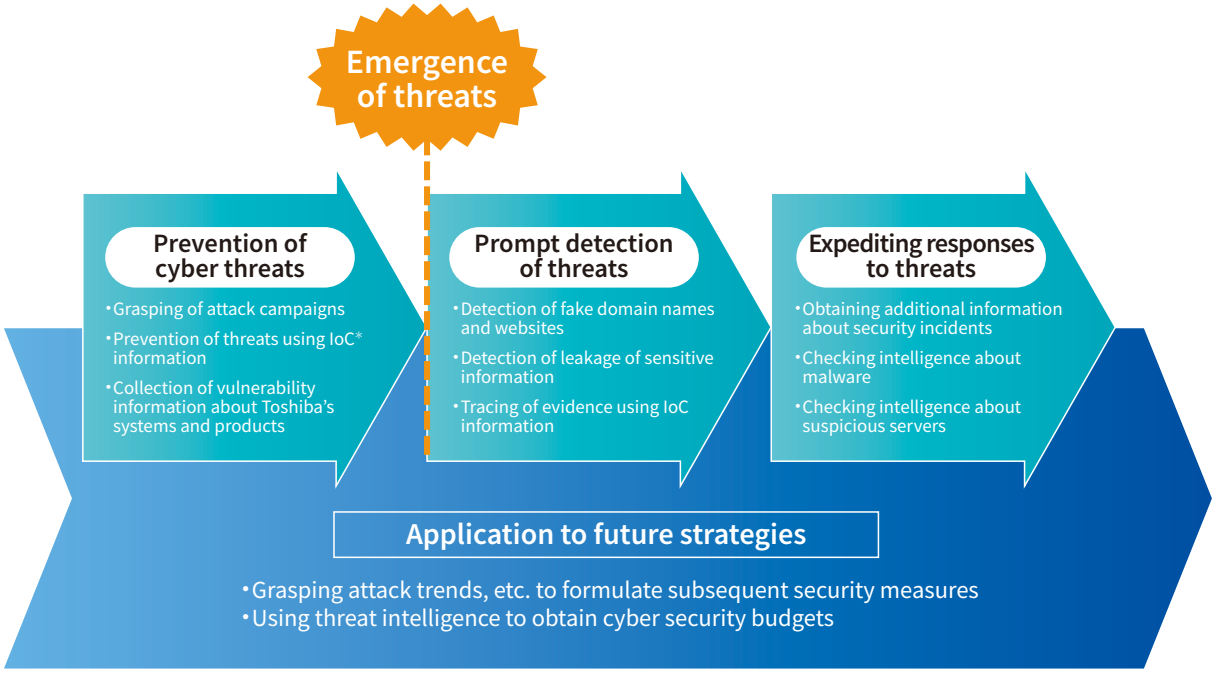
Introduction of EDR tools

*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
*3 NGAV: Next-generation anti-virus

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 prevent cyber threats to Toshiba Group and to promptly detect and respond to cyber threats if they materialize. We also use intelligence about cyberattack trends to formulate future security strategies.



＊IoC：Indicator of Compromise

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.

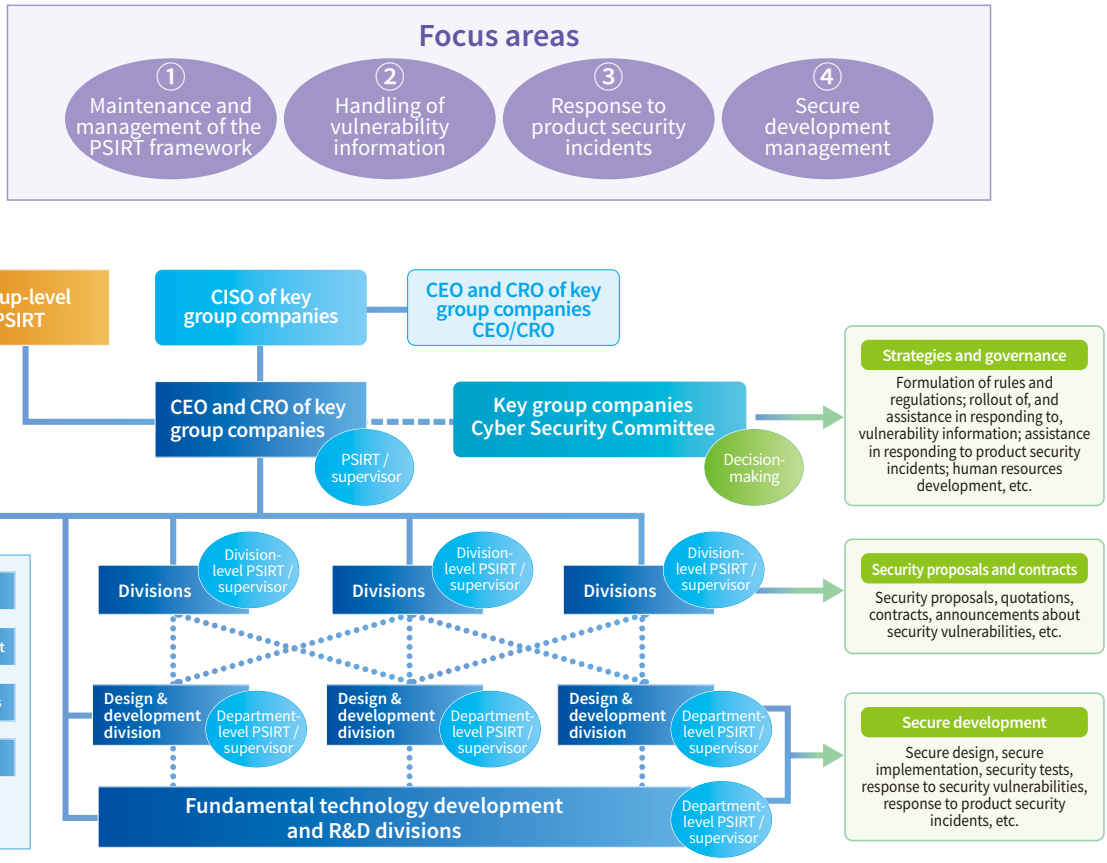
Initiatives for Enhancing Product Security

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

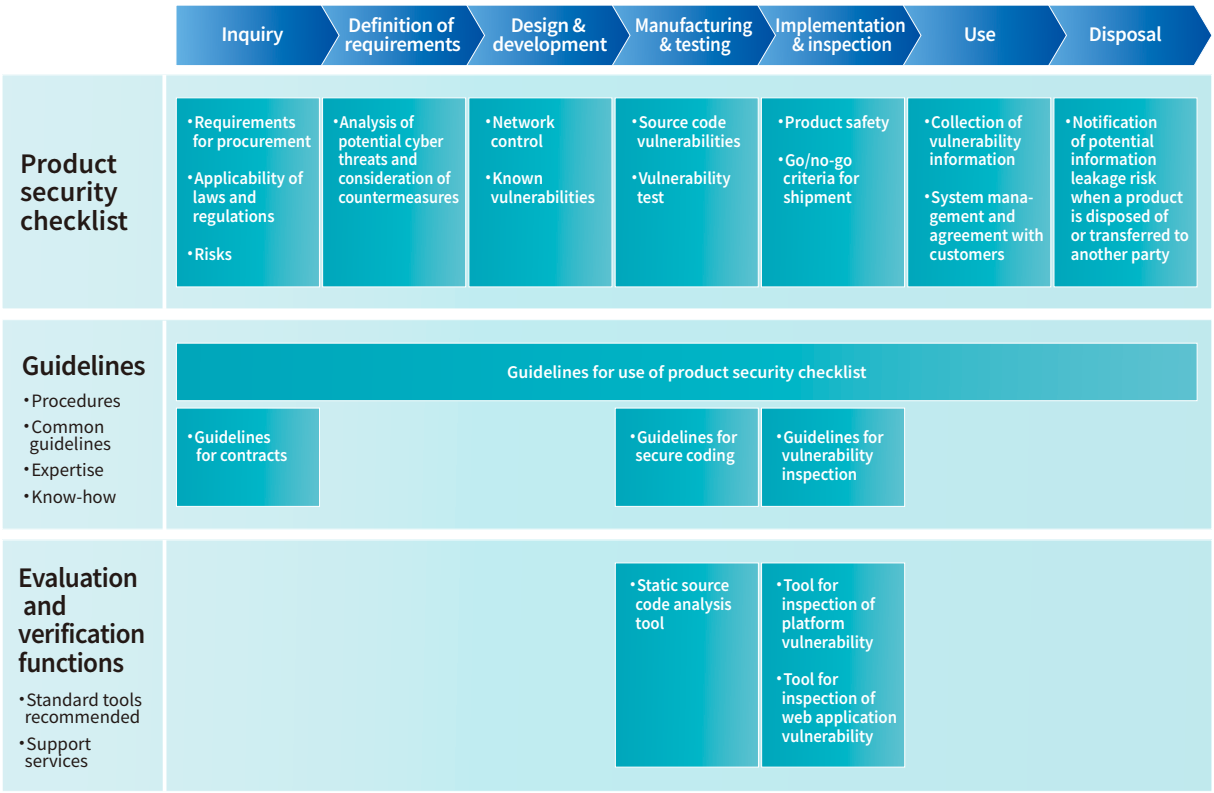
Toshiba Group defines four focus areas to strengthen its product security. Based on this definition, Toshiba Group has devised plans to enhance its product security preparedness according to risk-based priorities. Toshiba's product security management system covers all group companies. This product security 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 ensuring autonomous operations of each group company.



Product security management system

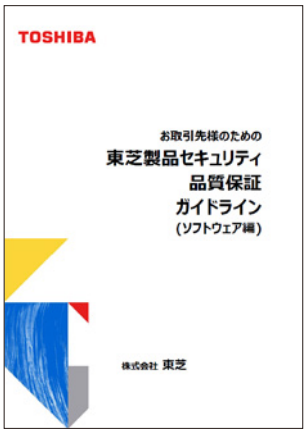
Preparation of product security checklist, guidelines, and standard recommended tools

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. Toshiba will provide the group companies with the standard recommended tools and related support services as part of the menu of evaluation/verification functions.



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

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)

Prompt and Reliable Response to Security Vulnerabilities

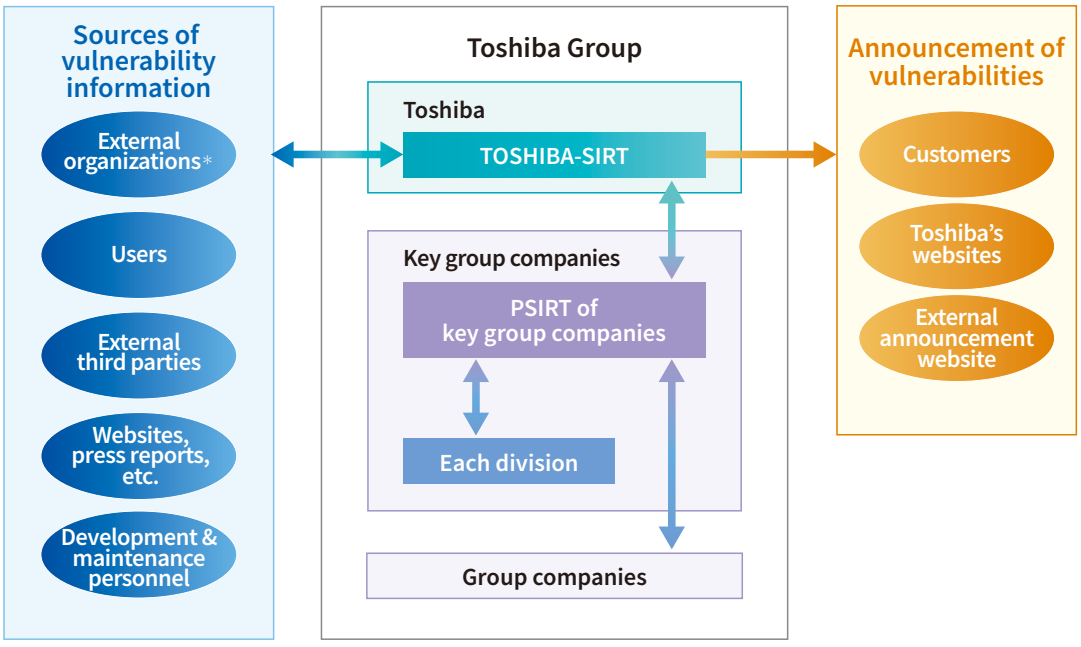
Response & Recovery

Toshiba Group has a product vulnerability response system in place to provide a consistent and prompt 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 (MITI) of Japan, Toshiba Group actively collects vulnerability information in cooperation with external organizations. 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.

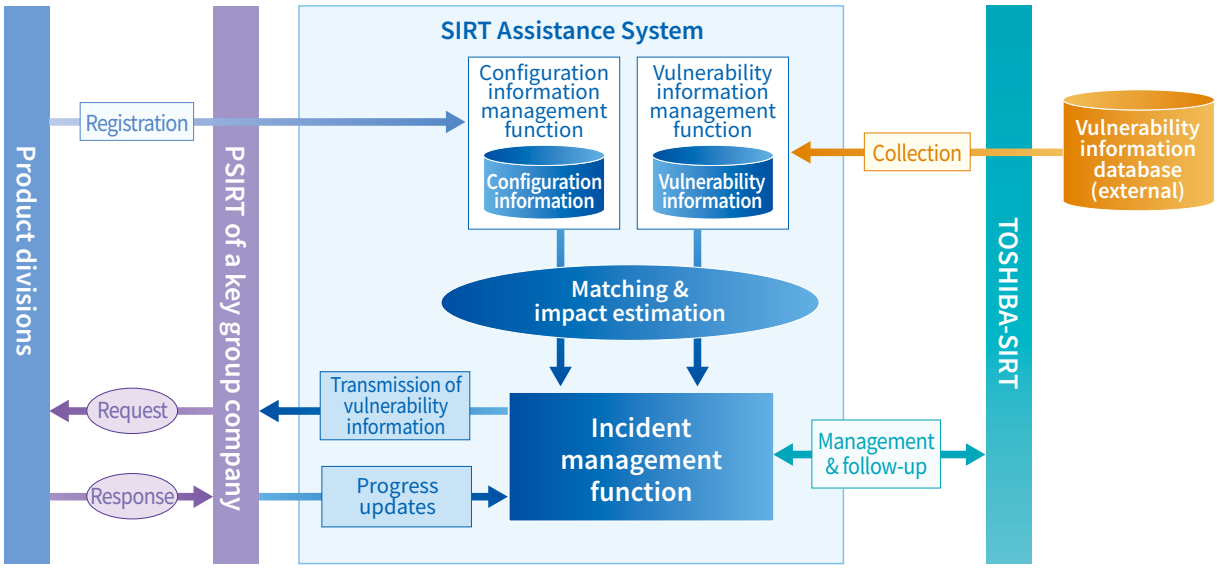


* External organizations: JPCERT/CC, JVN, ICS-CERT, etc

Toshiba Group's vulnerability handling system

Vulnerability handling process

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



Summary of the SIRT support system

Offering of Secure Products, Systems, and Services

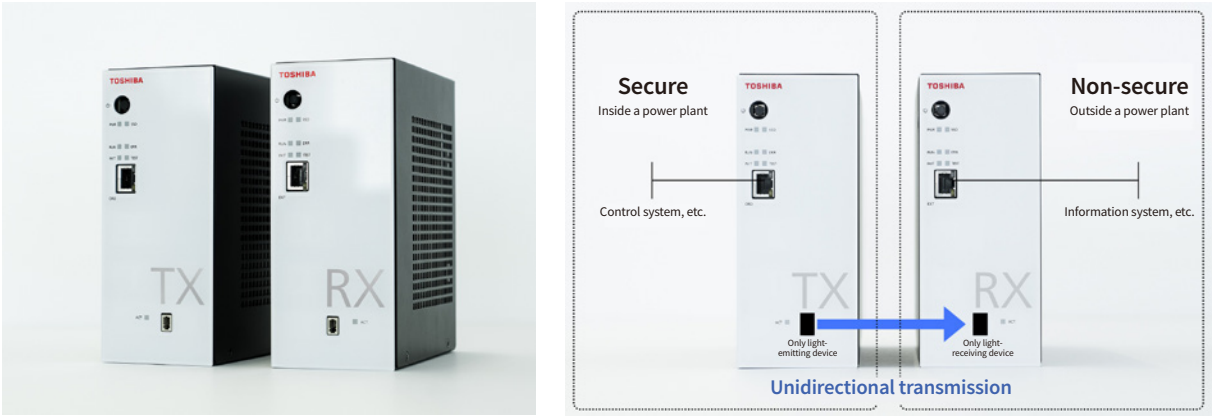
To meet the security requirements in the fields of energy, social infrastructure, electronic devices, etc., Toshiba Group provides various products, systems, and services for cyber security.

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

Industrial controller certified to ISASecure® EDSA*1: Unified Controller nv series type2

Toshiba Infrastructure Systems & Solutions Corporation

As cyberattacks against critical infrastructure become prevalent, the security measures and management of mission-critical control systems are becoming increasingly important. The Unified Controller nv series from Toshiba Infrastructure Systems & Solutions Corporation is widely used for social infrastructure and industrial applications. The type2 is a secure control system incorporating various security functions that is specifically designed for use in Toshiba's CIEMAC™-DS/nv instrumentation control system for general industrial applications.

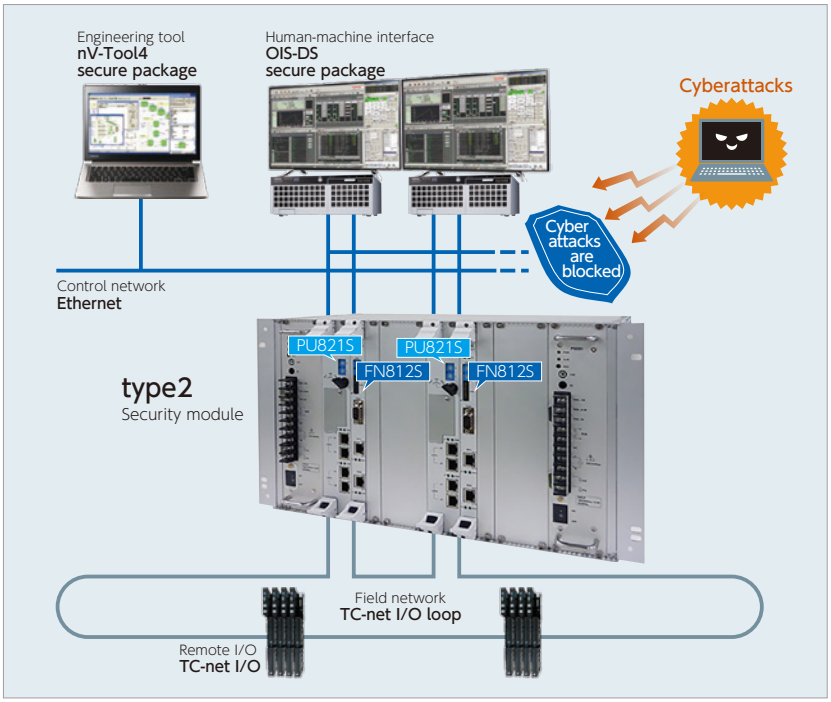
ISASecure® EDSA is a security certification program for embedded control systems operated by ISCI*2 in the United States as a scheme owner. The EDSA certification is increasingly required by enterprises as one of the procurement conditions. As the ISASecure® EDSA certification is expected to be integrated into the IEC 62443 series, it is attracting a lot of attention from various industries. The EDSA certification consists of three elements: Software Development Security Assessment (SDSA), Functional Security Assessment (FSA), and Communication Robustness Testing (CRT). The Unified Controller nv series type2 received an EDSA certificate from CSSC*3, an internationally recognized third-party certification laboratory.

The security module of the Unified Controller nv series type2 provides functions such as encryption of communication channels, control data, and parameters as well as authentication. These security functions provide robust protection against external cyberattacks during control operations while maintaining communication links with an engineering tool and a human-machine interface.

The Unified Controller nv series type2 makes it possible to securely configure the CIEMAC™-DS/nv instrumentation control system.

With the advent of the IoT era, the functions and roles expected of control systems and components are increasing. Therefore, construction of safe and secure systems is becoming increasingly important. We will continue to expand our portfolio of secure and highly reliable products in order to contribute to the realization of a safe, secure, reliable, and sustainable society.

Unified Controller nv series type2



Example of control system configuration

*1 ISASecure® EDSA: Embedded Device Security Assurance program for control systems provided by the ISA Security Compliance Institute
*2 ISA Security Compliance Institute: An organization founded by a consortium of ISA members to provide EDSA certification
*3 CSSC: Control System Security Center

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 Electronic Devices & Storage Corporation 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. Our HDDs incorporate adequate security features according to their intended applications.

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 requirements, we develop self-encrypting drives (SEDs).

The MQ01ABU***BW series*1 automatically encrypts the written data internally using AES*2, a standard encryption algorithm specified by the U.S. National Institute of Standards and Technology (NIST). The MQ01ABU***BW series also supports access control using the ATA*3 Security Feature Set and TCG*4 Opal SSC*5 to prevent retrieval of protected data without password authentication. These features provide data leakage protection.

Furthermore, the MQ01ABU***BW series incorporates Cryptographic Erase that allows the user to instantaneously invalidate all data in the drive simply by changing a data encryption key as well as Wipe technology, our proprietary data encryption technology to wipe out all data without a costly overwriting process. The security level of the MQ01ABU***BW series is certified through an accredited third party under the Cryptographic Module Validation Program (CMVP) (#2082) for use by the U.S government and under JCMVP (Japan CMVP) (#F0022) for use by the Japanese government. These certifications are security requirements for self-encrypting HDDs for digital MFPs and therefore simplify a digital MFP vendor's acquisition of security certification.

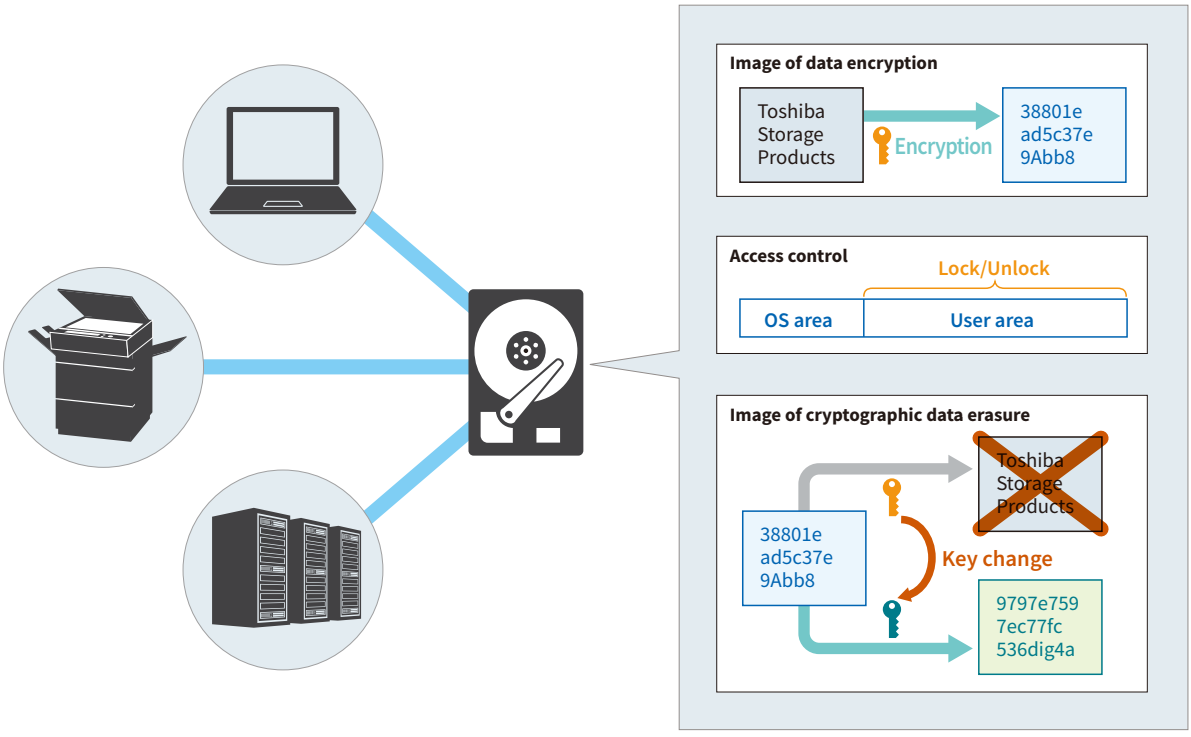


Image of security features of storage products

*1 MQ01ABU***BW series : MQ01ABU050BW/MQ01ABU032BW
*2 AES : Advanced Encryption Standard
*3 ATA : Advanced Technology Attachment
*4 TCG : Trusted Computing Group
*5 SSC : Security Subsystem Class

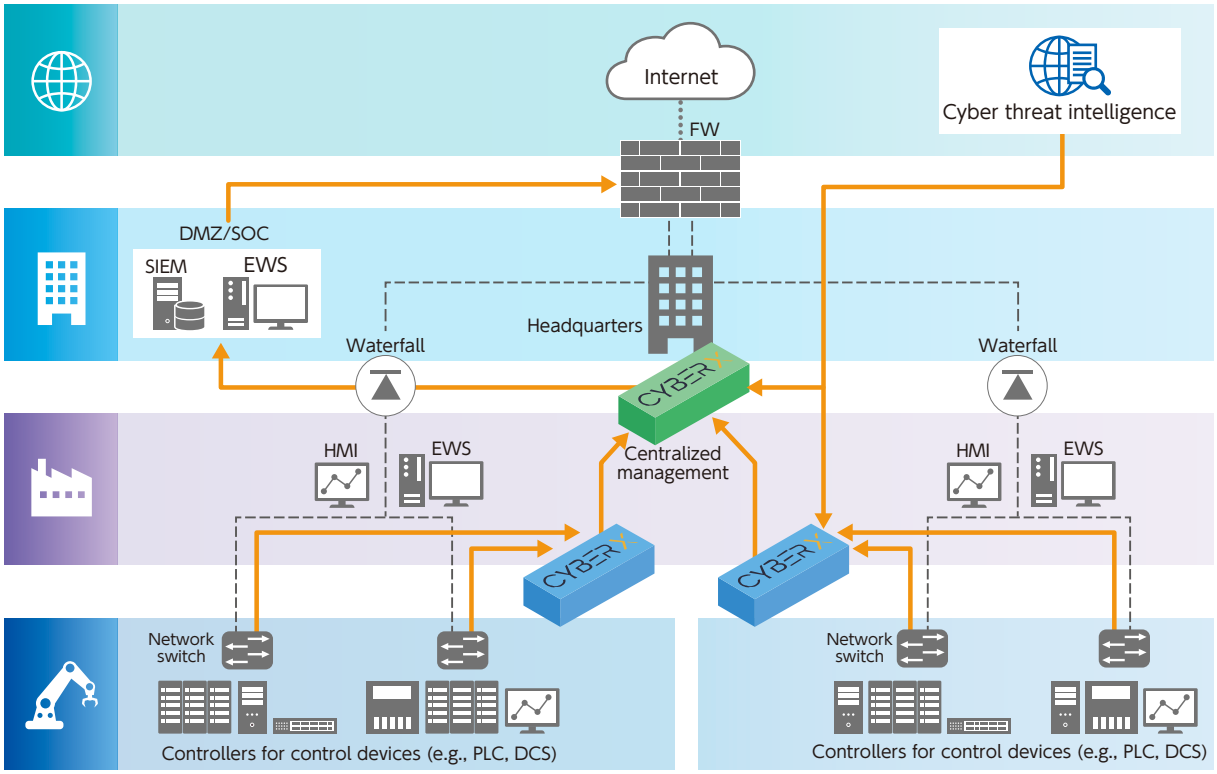
The CyberX platform, a cyber security platform for control systems

Toshiba Digital Solutions Corporation

The CyberX platform is a cyber security platform that provides a solution to the identification of control system assets, cyber security implementation, and integrated management. It is utilized by more than 3000 social infrastructure facilities around the world, including energy and industrial installations.
The CyberX platform provides real-time functions for grasping the up-to-the-minute conditions of a control network whose management was previously document-based; monitoring for unauthorized access to the network; and detecting and analyzing the causes of abnormal network traffic. These functions make it possible to reduce asset management costs and system downtime.

Features of the CyberX platform include the following:

1. Analyzing network traffic through identification and visualization of assets to learn information assets, detect devices on a network automatically, and display a network topology map (i.e., network interconnections) in real time
2. Collecting and analyzing information as necessary to automatically generate a list of assets and a summary report on device and network vulnerabilities in a system as well as possible countermeasures for each of the detected vulnerabilities
3. Detecting security threats to and abnormal conditions of a control system as per the control protocol and assisting in the analysis of security incidents to enable prompt operations
4. Identifying the conditions of an entire control system to predict existing dangerous attack paths based on the information about the vulnerability of all assets so as to support the formulation of countermeasures



Example of the CyberX platform configuration

- The CyberX platform is a product from CyberX Inc.
- SIEM: Security information and event management
- DMZ: Demilitarized zone
- Waterfall: The Waterfall Unidirectional Gateway is a system developed by Waterfall Security Solutions Ltd.

CT-5100 card settlement terminal series

Toshiba Tec Corporation

Payment and settlement methods are becoming diverse. Payment by credit card is one of the most widely used methods of payment. For credit card payment transactions, clients' sensitive information is transmitted, including a credit card number and personal information. Should any of the sensitive information be intercepted and misused, credit card users would suffer serious damage. Therefore, the Japanese government designates credit card settlement services as one of the 14 critical infrastructure sectors that could have a significant impact on people's lives. Before the Payment Card Industry Security Standards Council (PCI SSC) was established in 2006 by five international payment brands to develop security standards, card settlement terminals had been manufactured according to manufacturers' individual standards. One of the security standards developed by the PCI SSC is PCI PTS (Payment Card Industry PIN Transaction Security), which is the highest security certification for card settlement terminals that require a PIN (personal identification number) to work.

The PADCT-5100 PIN pad for the CT-5100 card settlement terminal series is certified as conforming to PCI PTS 4.1 for secure PIN entry. PCI PTS specifies a wide range of requirements, including those for security functions of the software and hardware comprising a card settlement terminal as well as product management.

In addition, the CT-5100 uses a closed operating system (OS) instead of an open OS such as Android and Linux. All the embedded software modules incorporate authentication and encryption functions, making the CT-5100 robust against external hacking attacks. Its tamper-resistant function provides protection against external malicious attacks, allowing merchants to use the CT-5100 without security concerns.

The revision of the Installment Sales Act of Japan that came into effect in June 2018. This revision obligates credit card merchants to strengthen the security measures for credit card transactions. It also requires merchants that handle in-store credit card transactions not to retain credit card information (or to achieve a state equivalent to a non-retaining state) or otherwise to comply with PCI DSS. There are two methods for not retaining credit card information. One method allows card information to be processed by credit card companies without passing through in-store POS terminals and networks. The other method allows card information to pass through in-store POS terminals and networks, but uses an encryption scheme to make it impossible for merchants to access card numbers and decrypt them. The CT-5100 and PADCT-5100 support both methods.

Left : CT-5100 (main unit)
Right : PADCT-5100 (PIN pad with IC card reader/writer)

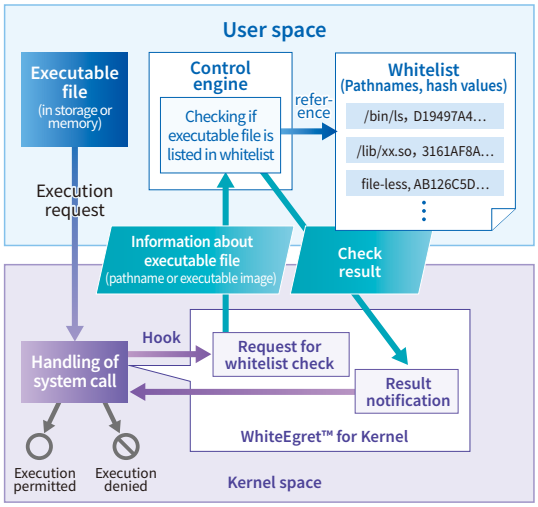
R&D

With the advancement of IoT and cyber-physical systems (CPS), cyberattacks are becoming increasingly sophisticated and diversified. To protect critical infrastructure from unknown cyberattack threats in a zero-trust environment and realize a safe and secure society, Toshiba is deploying the latest security technologies based on security threat analysis, incident prediction and evaluation. Toshiba also engages in the research and development of state-of-the-art security management technologies, including those for the monitoring and detection of, response to, and recovery from security incidents, as well as technologies for advanced cyberattacks and data encryption that support such security management. Toshiba strives to stay ahead of evolving cyber security threats with 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 is reported to be targeting control systems for critical infrastructure such as electric power systems, threatening the foundations of society.
In response, Toshiba has developed WhiteEgret™, a whitelisting malware execution control technology to determine whether to invoke an executable using a standard Linux® function. WhiteEgret™ makes it possible to protect control systems from both known and unknown malware. WhiteEgret™ provides protection not only from conventional file-based malware but also from file-less malware that has shown signs of a potential epidemic in recent years.

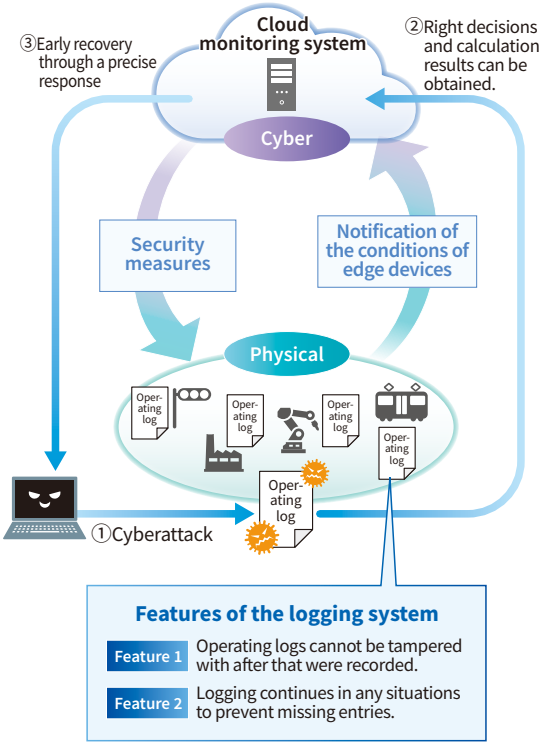
Reference: Haruki. H. et al. "Cybersecurity Technologies Ensuring Safe, Secure, and Long-Term Operation of Control Systems for Infrastructure." Toshiba Review 73(5), September 2018



Embedded logging system

Stable operation is required for social infrastructure systems over the long term. In order to detect abnormal behaviors and signs of failure, operating logs are gathered from edge devices in the field for remote monitoring via the cloud. In the event of a successful cyberattack against a social infrastructure system, the attacker might not only steal highly confidential information such as operating information but also tamper with an operating log, making it impossible to grasp system conditions correctly. In the worst-case scenario, this might make it impossible to detect system instability and consequently lead to an accident.
To prevent such a situation, Toshiba has developed a logging system for edge devices using virtualization technology that is robust against the tampering with or missing entries from an operating log due to a cyberattack.

Reference: DAN Jiang, et al.
"Proposal for a secure logging system for embedded systems (in Japanese)," SCIS2020



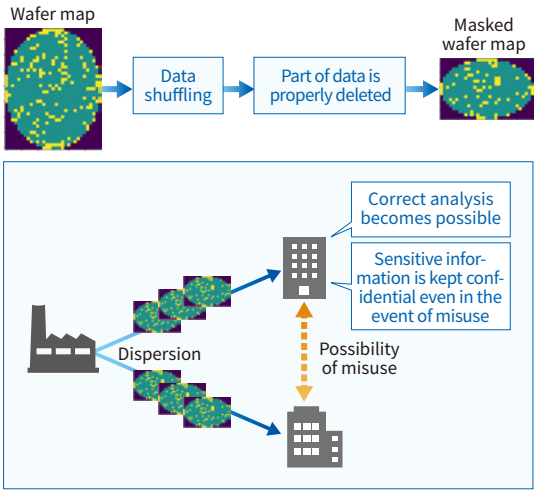
Data processing technology combining safety and usefulness

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 safety measure makes it difficult to perform an analysis with a high degree of flexibility.

To resolve this dilemma, Toshiba is developing data masking technologies to ensure both safety and analyzability.

As part of this effort, we have developed a technology capable of protecting sensitive information by shuffling and deleting part of data, making data misuse impossible.

Reference: WADA Hiroho, et al. "Initial Study on Secure and Analyzable Data Masking Methods for Wafer Map (in Japanese)." SCIS2020

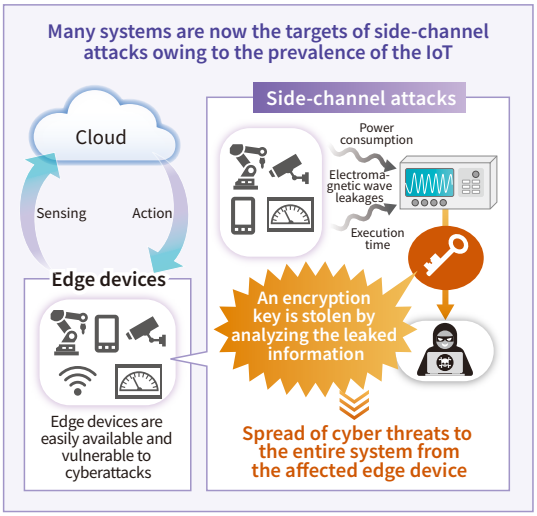


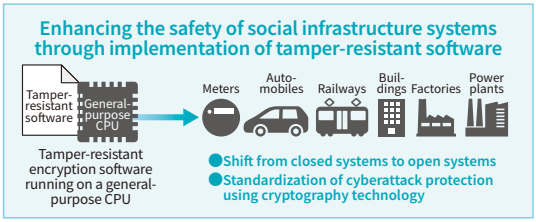
Cyberattack evaluation technology

Technologies for cyber and physical attacks are becoming increasingly sophisticated and diverse. To protect social infrastructure systems (cyber-physical systems) from unknown threats, it is necessary to understand the latest attack technologies.

In response, Toshiba is developing a technology to evaluate and analyze the attacking methods for physical devices and systems, including remote cyberattacks against control systems and side-channel attacks that physically exploit unintended physical information leakage from cyber-physical systems (CPS). Furthermore, we are developing proactive cyber security technologies such as a malware execution control technology by incorporating the cyberattack evaluation technology during the product development process. We are also working on the R&D of tamper-resistant implementation technologies to protect physical devices against side-channel attacks.

Reference: KOMANO Yuichi, et al. "Threat Estimation of Side-Channel Attacks against the IoT Devices: Evolution of Attack Environments and Perspective of Countermeasures (in Japanese)," SCIS2019



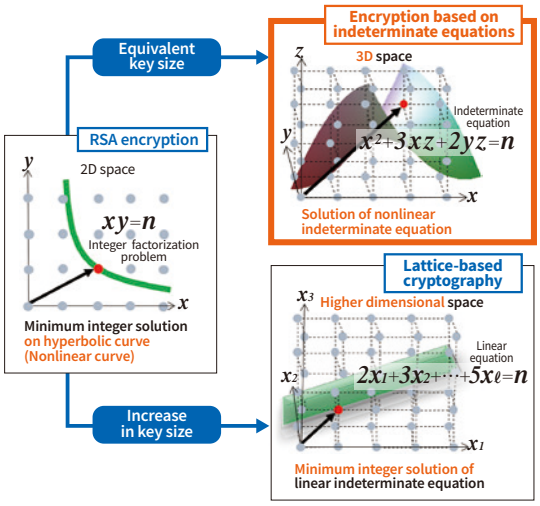


Quantum computing-resistant cryptography

Quantum computers capable of computing large size integers are expected to have the ability to break the current public key cryptography.

In response, Toshiba has developed an encryption scheme whose security depends on solving indeterminate equation problems that are much harder than integer factorization problems used in the current RSA algorithm. By using hard problems, we aim to achieve an encryption scheme with a key length as short as or shorter than RSA keys in order to enable high-speed processing. We intend to apply public key cryptosystems to edge devices with limited resources.

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

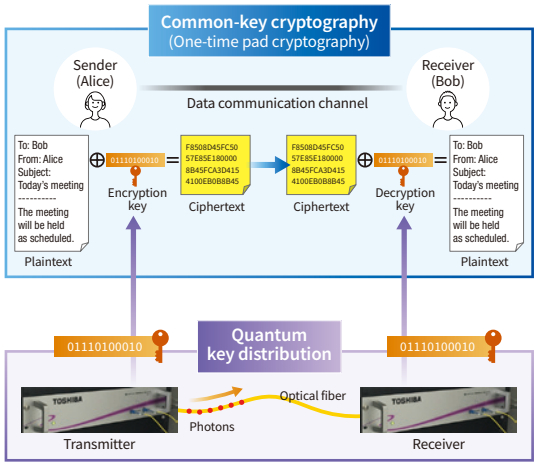


Quantum cryptographic communications

Toshiba engages in research and development of quantum cryptography, a next-generation cryptography technology based on the principles of quantum mechanics. Toshiba has developed the high speed and stable photon detection technologies, etc. for quantum cryptography. We have succeeded in generating quantum encryption keys at a rate exceeding 10 Mbps for the first time in the world. Toshiba is now conducting field trials in Japan and the United Kingdom, aiming to achieve practical use of quantum cryptography for various applications and use cases, including medical care, finance, and communications infrastructure.

As a member of ITU-T, ISO/IEC JTC1, ETSI, etc., Toshiba also engages in international standardization activities concerning technologies related to quantum cryptography.

Reference: http://www.toshiba.co.jp/qkd/en/index.htm



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 each organization is at the center of promoting personal data protection (see page 8). 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 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 perform first-hand inspections of the divisions and group companies that handle high-risk personal data 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. Outsourcers are now 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 May 2018, the GDPR became enforceable in Europe. Led by Toshiba's regional headquarters in Europe, Toshiba Group companies are responding to the GDPR in various ways, including through the education of employees, establishment of in-house regulations, and data mapping.

Compliance with the China Cyber Security Law

Bylaws and guidelines for the China Internet Security Law, which came into effect in June 2017, have been established. As a result, law enforcement concerning illegal acts is now becoming common. In response, Toshiba's regional representative subsidiaries in China are collecting information so as to comply with the related laws and regulations.

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

Thailand promulgated PDPA in May 2019. To ensure that local subsidiaries comply with PDPA, Toshiba has created templates for in-house regulations concerning PDPA and provided it for the local subsidiaries.

External Activities

As of March 31, 2020

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 two subcommittees (SCs) of ISO/IEC JTC 1, partaking in the following standardization activities:

- ISO/IEC JTC1/SC17 Cards and personal identification
- ISO/IEC JTC1/SC27 IT security techniques
- ISO TC68/SC2,SC6,SC7 Information security techniques for financial services
- ISO TC292/WG4: Authenticity, integrity and trust for products and documents
- IEC TC65/WG10: General-purpose control systems
- Institute of Electrical and Electronics Engineers (IEEE) 802.21 WG: Security authentication for multicast communications
- ETSI SCP (European Telecommunications Standards Institute Smart Card Platform): Activities for standardization for European telecommunications
- Global Platform: 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.

- Information-technology Promotion Agency, Japan (IPA), 10 Major Security Threats Authors' Association, etc.
- Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA)
- Japan Electronics and Information Technology Industries Association (JEITA),
- Communications and Information network Association of Japan (CIAJ), ICT Network Equipment Security Committee, etc.
- 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)

etc.

Third-Party Assessment and Certification

As of March 31, 2020

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 IT-Services Corporation
Toshiba Information Systems (Japan) Corporation
Toshiba Infrastructure Systems & Solutions Corporation
Toshiba Digital Solutions Corporation
Toshiba TEC Solution Services Corporation
Japan Systems Corporation
Kyushu Toshiba Engineering Corporation
Enterprise Business System Solutions Corporation
Chubu Toshiba Engineering
Toshiba TEC Corporation
Toshiba Development & Engineering Corporation
TEC Information Systems Corporation
Toshiba Information Systems Corporation
Toshiba Digital Marketing Initiative Corporation

Acquisition of the PrivacyMark certification

Toshiba Information Systems (Japan) Corporation
Toshiba Plant Systems & Services Corporation
Toshiba Digital Solutions Corporation
Kyushu Toshiba Engineering Corporation
Toshiba TEC Solution Services Corporation
Toshiba IT-Services Corporation
Toshiba Information Systems Corporation
Toshiba Information System Products Inc.
Toshiba Automation Systems Service Co., Ltd.
Toshiba Office Mate
Toshiba Digital Marketing Initiative Corporation
Toshiba I.S. Consulting Corporation
Toshiba Business Expert Corporation
Toshiba Health Insurance Association
Toshiba Infrastructure Systems & Solutions Corporation

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 2020).

Product	TOE*2 Class	Certification Number	PP and EAL
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(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(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	C0631	PP(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(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(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+
TOSMART-P080 ePassport 01.06.04 + NVM Ver.01.00.01	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+
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 2020).

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 C	2769	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type A	2709	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model) Type B	2707	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type A	2521	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model) Type B	2520	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)	2508	Level2
Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model NA02)	2410	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 Communication 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 highlights large-scale cyberattacks and massive incidents of data fraud/theft among the top five risks in terms of likelihood. Therefore, the manufacturing industry spurring digital transformation 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, 2020

Company Overview

Company Name: TOSHIBA CORPORATION

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

Founded: July 1875

Paid-in capital: ¥200,175 million

Consolidated Net Sales: ¥3,389.9 billion

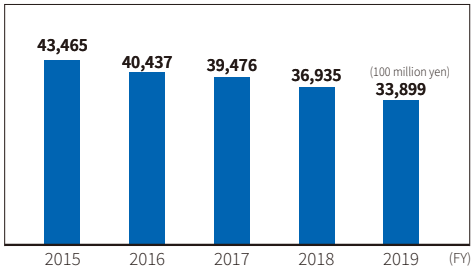
Number of Employees: (consolidated) 125,648

Number of Shares Issued: 455 million shares

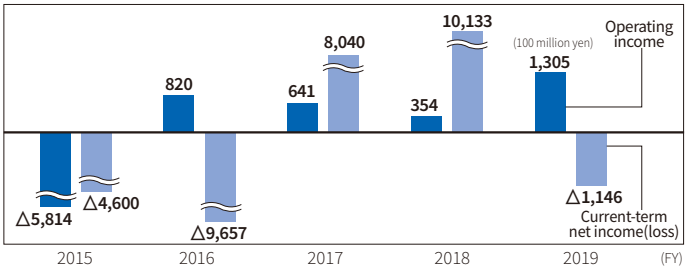
Stock Exchange Listings: Japan: Tokyo and Nagoya

Consolidated business results

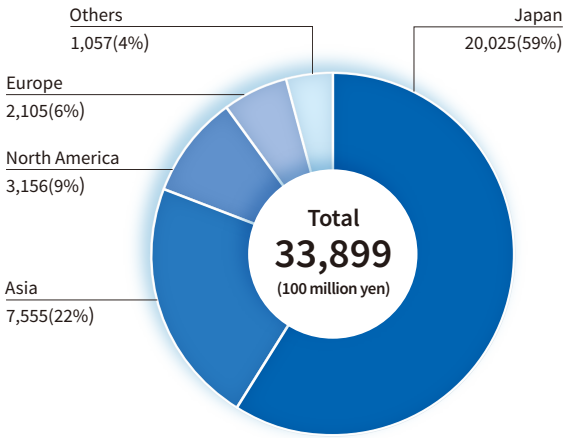
Net sales



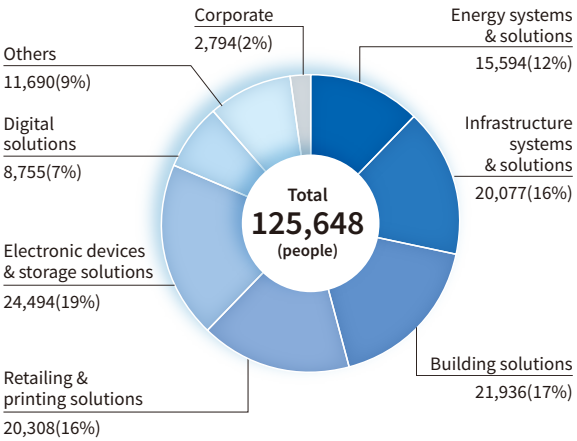
Changes in operating income and net income(loss)



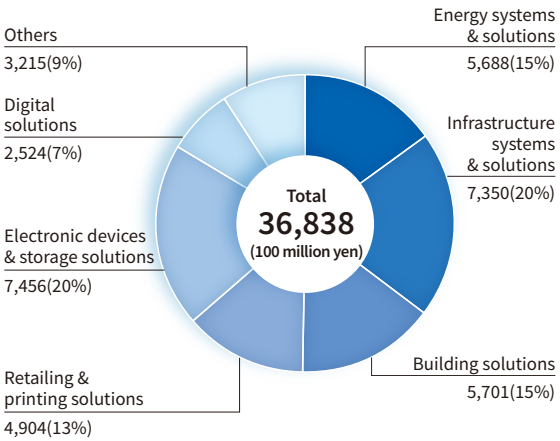
Net sales by region



Number of employees by segment



Net sales by segment



(Including an inter-segment elimination of 293,900 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.toshiba.co.jp/security/en

Published in September 2020