2019 Cyber Security Report
Since its founding in 1875, Toshiba Group has been committed to contributing to society through its business while engaging with customers as an enterprise that supports people’s lives. At present, Toshiba operates in the Energy, Social Infrastructure, Electronic Devices, and Digital Solutions business domains. Providing safety and security in all these domains is the responsibility of Toshiba Group.

With the advancement of digitization, various types of information, including personal information, are increasingly accumulated in cyber-space. Such information is now indispensable to systems in physical space. Huge amounts of data collected from physical space are analyzed in cyber-space in order to generate new valuable information, which is fed back in physical space. Cyber-physical systems (CPS) provide this mechanism. Toshiba Group endeavors to enhance cyber security so as to properly safeguard cyber-physical systems, protect society from cyber-crimes, and utilize various types of information to benefit people’s lives. Toshiba pledges to support people’s lives and society using cutting-edge cyber security technologies, leveraging its experience and expertise in both the cyber and physical realms.

The purpose of the 2019 Cyber Security Report is to provide our customers, shareholders, suppliers, and other stakeholders with information about Toshiba Group’s initiatives to enhance cyber security. We will continue to devote ourselves to cyber security so that you can choose Toshiba’s products and services without any security concerns.

Message from the Chief Information Security Officer (CISO)

Cyber Security Envisioned by Toshiba

Since its founding in 1875, Toshiba Group has been committed to contributing to society through its business while engaging with customers as an enterprise that supports people’s lives. At present, Toshiba operates in the Energy, Social Infrastructure, Electronic Devices, and Digital Solutions business domains. Providing safety and security in all these domains is the responsibility of Toshiba Group.

With the advancement of digitization, various types of information, including personal information, are increasingly accumulated in cyber-space. Such information is now indispensable to systems in physical space. Huge amounts of data collected from physical space are analyzed in cyber-space in order to generate new valuable information, which is fed back in physical space. Cyber-physical systems (CPS) provide this mechanism. Toshiba Group endeavors to enhance cyber security so as to properly safeguard cyber-physical systems, protect society from cyber-crimes, and utilize various types of information to benefit people’s lives. Toshiba pledges to support people’s lives and society using cutting-edge cyber security technologies, leveraging its experience and expertise in both the cyber and physical realms.

The purpose of the 2019 Cyber Security Report is to provide our customers, shareholders, suppliers, and other stakeholders with information about Toshiba Group’s initiatives to enhance cyber security. We will continue to devote ourselves to cyber security so that you can choose Toshiba’s products and services without any security concerns.
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.
Message from the Chief Information Security Officer (CISO) ................. 1
Toshiba Group’s Manifesto on Cyber Security ................................ 2

**Chapter 1**

**Visions and Strategies**

Toshiba’s Cyber Security Visions ................................................. 4
Strategies for Enhancing Cyber Security Preparedness .................... 6
  Governance ............................................................................. 7
  Security Operations ................................................................ 9
  Human Resources Development ............................................. 10

**Chapter 2**

**Cyber Security Initiatives**

Security Measures for Internal IT Infrastructure .......................... 11
  Enhancing Prediction and Detection ....................................... 11
  Security Incident Response .................................................. 13
  Advanced Attack and Penetration Testing from Hackers’ Perspective 14
  Self-Audit and Security Assessment ...................................... 15
  Security Measures for Internet Connection Points .................... 16
  Enhancing the Security of Endpoints Using EDR Tools ............... 18

Security Measures for Products, Systems, and Services ............... 19
  Initiatives for Enhancing Product Security .............................. 19
  Prompt and Reliable Response to Security Vulnerabilities .......... 20
  Offering of Secure Products, Systems, and Services ............... 22
  R&D .................................................................................... 26
  Personal data protection ...................................................... 27
  Compliance with overseas laws and regulations ....................... 27
  External Activities ............................................................... 28
  Third-Party Assessment and Certification ................................ 29
  Pursuit of the Sustainable Development Goals (SDGs) ............. 32
  Toshiba Group Business Overview ....................................... 33
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 added value.

Toshiba Group engages in the social infrastructure business, including in the electricity, transportation, water treatment, and logistics sectors, and possesses extensive expertise and data in each sector. Toshiba Group is therefore well positioned to develop cyber-physical systems for the creation of new value by combining physical technologies cultivated through its long experience and the world’s leading image recognition and other cyber technologies. Cyber-physical systems will be utilized to facilitate digital transformation for 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. True to the venture spirit that has continued from one generation to the next since Toshiba was founded by Hisashige Tanaka and Ichisuke Fujioka, Toshiba Group aims to become a CPS technology enterprise that spurs technological innovation in diverse fields.
**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 myriad physical devices become interconnected via networks, cyber-threats are expanding from information systems to the industrial control systems and devices for social infrastructure that were not connected to the Internet before, exposing social infrastructure to the increasing risk of cyber-induced physical damage.

The mission of Toshiba Group is to support the business continuity of its customers and help realize a safe and secure society in the context of advances in CPS-based digital transformation. 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 the notion of conventional protection-oriented security measures to sustainable security solutions encompassing both information and control systems. Under these circumstances, based on the concept of “Security Lifetime Protection,” Toshiba Group endeavors not only to ensure protection via security-by-design 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 recovery from attacks. Furthermore, we endeavor to achieve 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.

This is to protect the security not only of its own information systems and production facilities but also of its products, systems, and services offered to customers.

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

---

| 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 |
| Personnel | Training and enhancement of necessary security personnel |

---

*Goals of Toshiba Group*
Toshiba Group has been pursuing strategies for enhancing its cyber security preparedness to ensure that the security management processes described above are implemented and improved in each business in a sustainable and continuous manner.

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 cyber security was delegated from the Chief Executive Officer (the then President and the current CEO of Toshiba Corporation). A chain of command was defined so that the CISO can directly communicate with the executives concerning cyber security risk, facilitate decision-making for grave security incidents that could affect business management, and promptly provide precise directions for major business-operating companies of the Group.

At the same time, in order to maintain consistent security measurement and thereby strengthen cyber security, Toshiba Group established the Cyber Security Center, which consolidates the security functions for information systems and those for products and services that had previously been promoted separately. Specifically, the Cyber Security Center consists of the CSIRT*1 responsible for addressing security risk concerning information assets and personal data and the PSIRT*2 responsible for managing security risk concerning products, systems, and services provided by Toshiba Group. The CSIRT and the PSIRT work in tandem to achieve the advanced cyber security needed as a manufacturer that supports social infrastructure. The CSIRT and the PSIRT cooperate to ensure that all systems at Toshiba’s factories and manufacturing facilities are properly secured, promote common use of processes and personnel to improve efficiency, 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 major business-operating companies of the Group have a point of contact serving as a liaison with the Cyber Security Center. Furthermore, Toshiba Group strives to prevent the introduction of cyber security vulnerabilities into products at the development stage, promptly address security vulnerabilities found in the shipped products, standardize the risk evaluation policy, incorporate security rules into in-house regulations, and establish security management systems at key group companies.

To strengthen security operations (such as prediction & detection, response & recovery, and protection), it is important to shift from reactive responses to proactive prediction and control. To achieve this shift, the Cyber Security Center promotes the collection, deployment, and utilization of internal and external threat intelligence. In addition, the Cyber Security Center considers that the protection must cover 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 connected to Toshiba’s network. The Cyber Security Center aims to realize extensive security monitoring and accurate detection and prediction while reducing the time required to deal with and recover from security incidents. To attain these goals, the Cyber Security Center is now preparing for full-scale operation of the Cyber Defense Management Platform (CDMP) designed to automate and increase the efficiency of security operations.

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 from R&D to technical support, and implementation assistance regarding cyber security technology. The Cyber Security Technology Center 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 courses on information security to manage and protect personal and other types of information and those on product security to ensure the security of products, systems, and services provided to customers.

The following sections describe our specific measures that are currently being implemented 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.

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.

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* 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 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.

* SIRT : Security Incident Response Team
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 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 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 CDMP will be extended to cover the systems of our customers and suppliers connected to Toshiba’s network. Specifically, the CDMP provides the functions shown below, some of which commenced operation in January 2019.

- **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 20)
- **Threat analysis function**
  - Preventing cyber threats by using threat intelligence
  - Improving the analysis accuracy by accumulating knowledge and using artificial intelligence
- **Evaluation and verification function**
  - 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 surrounding Toshiba Group is ever increasing. To address the threat, it is necessary to automate the response to and the recovery from the security incident detected. The CDMP accumulates knowledge and uses artificial intelligence to realize high-accuracy cyber security operations with slim resources so as to deal with new cyber threats that occur every day.
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 handle daily information properly 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 the General Data Protection Regulation (GDPR) of the European Union (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.

■ 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 describing the importance and methods of addressing product security risk.
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.

■ Information Security Handbook
In addition to the provision of the above education, Toshiba Group distributes the Information Security Handbook to all employees of Toshiba Group in Japan and abroad, which plainly describes the rules, regulations, and guidelines that they need to understand and act upon in the performance of their duties.
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. 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
Utilization

Scope of monitoring

Automatic protection

Log monitoring

Prevention

Internet

Firewall

Email gateway

Proxy

IPS/WAF

Internal networks

Firewall

Information systems

Production facilities & factories

Products and services for customers

TOSHIBA-SIRT

Incident response

SOC

Monitoring of security threats

Utilization

Cyber 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

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.

Security Incident Response

Security incidents include website tampering, targeted emailing, spam influx, unknown virus infection, and computer virus 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 computer virus. 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.
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

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 observes an average of roughly 2.5 million 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.

**Handling of suspicious emails**

Toshiba Group uses protective measures for both external cyber threats such as virus-infected emails and internal information leakage. To seize the inflow of harmful viruses 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 remote work 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 virus 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

Toshiba Group is now introducing EDR tools to detect and block unknown viruses, etc. that cannot be blocked by existing anti-virus software as well as sophisticated cyberattacks that cannot be detected at the entry point of the network.

- Detecting suspicious network activities due to the infection of unknown viruses 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

*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
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**

Under the cyber security management system, the PSIRT collaborates with quality assurance and procurement departments to enhance the security of the development process of products, systems, and services offered to customers as well as the security of third-party products for use in Toshiba Group’s products.

**Product Security Checklist**

Toshiba Group uses the Product Security Checklist that summarizes the security requirements to be checked at each product development stage. This checklist serves to remind product developers not to miss anything that should be considered in terms of security and thus helps ensure the security of Toshiba Group’s products.

<table>
<thead>
<tr>
<th>Inquiry</th>
<th>Definition of requirements</th>
<th>Design &amp; development</th>
<th>Manufacturing &amp; testing</th>
<th>Implementation &amp; inspection</th>
<th>Use</th>
<th>Disposal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Requirements for procurement</td>
<td>• Analysis of potential cyber threats and consideration of countermeasures</td>
<td>• Network control</td>
<td>• Source code vulnerabilities</td>
<td>• Product safety</td>
<td>• Collection of vulnerability information</td>
<td>• Notification of potential information leakage risk when a product is disposed of or transferred to another party</td>
</tr>
<tr>
<td>• Applicability of laws and regulations</td>
<td></td>
<td>• Known vulnerabilities</td>
<td>• Vulnerability test</td>
<td>• Go/no-go criteria for shipment</td>
<td>• System management and agreement with customers</td>
<td></td>
</tr>
<tr>
<td>• Risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

● Example of a secure development process and check items

**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.
Prompt and Reliable Response to Security Vulnerabilities

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 Rules 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 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.

---

<table>
<thead>
<tr>
<th>Sources of vulnerability information</th>
<th>Toshiba Group</th>
<th>Announcement of vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>External organizations</td>
<td>Toshiba</td>
<td>Customers</td>
</tr>
<tr>
<td>Users</td>
<td>TOSHIBA-SIRT</td>
<td>Toshiba’s websites</td>
</tr>
<tr>
<td>External third parties</td>
<td>PSIRT of key group companies</td>
<td>External announcement website</td>
</tr>
<tr>
<td>Websites, press reports, etc.</td>
<td>Each division</td>
<td></td>
</tr>
<tr>
<td>Development &amp; maintenance personnel</td>
<td>Group companies</td>
<td></td>
</tr>
</tbody>
</table>

*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. This system enables product divisions to provide prompt and reliable handling of vulnerability information while reducing the cost of doing so.
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

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
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 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, 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.
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 automatically encrypts the written data internally using AES, 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 Security Feature Set and TCG Opal SSC 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) for use by the U.S. government and under JCMVP (Japan CMVP) 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.

Toshiba Group’s Cyber Security Report 2019

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
e-STUDIO digital MFP series

Digital MFPs are now indispensable for office work as they act as a combination of multiple devices such as photocopier, fax, printer, and scanner. Digital MFPs incorporate data storage such as an HDD that allows the user to temporarily or permanently store document data as well as a document emailing function. Many office documents contain sensitive information, including personal data, privacy information, and corporate information. While such information must be safeguarded, it is necessary to avoid business interruption because of the inability to retrieve documents when necessary. It is crucial to prevent cyberattacks so as to safeguard confidential information stored in a digital MFP against leakage, falsification, and destruction.

To counter such threats, using the state-of-the-art cyber security measures is important. In the event of data leakage due to security negligence, enterprises and public organizations would lose social credibility and suffer compensatory and other monetary damages. Therefore, various security functions are required for digital MFPs to protect users’ information assets, such as user/card authentication, access control, a self-encrypting HDD with a wipe-out function, network traffic encryption, firmware integrity assurance, secure printing, audit logging, and wrong transmission prevention.

The e-STUDIO series is certified under ISO/IEC 15408, i.e., the Common Criteria (CC) for Information Technology Security Evaluation that is compliant with HCD-PP, the latest and highest security standard for MFPs. To protect data in MFPs, HCD-PP stipulates various security requirements equivalent to the FIPS 140-2 standard that is very difficult to comply with.

In addition to an encryption algorithm, FIPS 140-2 stipulates life-cycle requirements for encryption keys, including their generation, use, and disposal, as well as requirements for cryptographic modules. The acquisition of HCD-PP certification means that the e-STUDIO series is certified by a third-party organization as being equipped with security measures of the highest level. The HCD-PP-certified MFPs are expected to become increasingly disseminated since they provide robust security.

HCD-PP security features:
- User recognition and authentication
- Access control
- Encrypted communication
- Self-test
- Auditing
- Update verification
- Storage encryption
- Fax/network separation
- Overwrite erasure and complete wipe-out

Security features of the e-STUDIO digital MFP series

---

2 HCD-PP: Hard Copy Device-Protection Profile
3 FIPS 140-2: Federal Information Processing Standard 140-2
R&D

With the advancement of IoT and cyber-physical systems, 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 engages in the research and development of security technologies that make it possible to proactively perform advanced security management including security threat analysis, integration of state-of-the-art security technologies, incident prediction and detection, and response and recovery, as well as fundamental technologies such as enhanced cyberattack methodologies and advanced cryptography.

■ Prediction and detection (malware execution control)

Malware targets now include the control systems for critical infrastructure such as electric power systems, threatening the foundations of society. It was previously difficult to develop countermeasures for such threats while providing “24hours/365 days” service availability. In response, Toshiba has developed WhiteEgret™, a whitelisting malware execution control technology to protect control systems from 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.


■ Advanced cryptography (quantum-resistant public key cryptosystem)

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 the hard problem, we aim to provide encryption scheme required small keys which is less than or equal to as for RSA and thus to enables high-speed processing. We intend to apply public key cryptosystem to low-end devices.


■ 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.

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.

■ Personal data protection for product security
Toshiba Group operates in a wide range of industrial sectors, including Energy, Social Infrastructure, Electronic Devices, and Digital Solutions. The scope of personal data protection is expected to expand to include personal data handled by products and personal data that might be imparted in the course of maintenance work. Toshiba Group endeavors to promote personal data protection as part of product security.

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 local employees, establishment of in-house regulations, and data mapping. Toshiba Group is also educating all employees of Japanese group companies about an overview of the GDPR and the export of personal data out of Europe.

■ Compliance with the China Cyber Security Law
Bylaws and guidelines for the China Cyber 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 prepare to comply with the related laws and regulations.
External Activities

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

etc.
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             |
| Toshiba Products Marketing Inc.       |
| 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               |
| ES Toshiba Engineering Corporation                   |
| Toshiba TEC Solution Services Corporation             |
| Toshiba IT-Services Corporation                       |
| Toshiba Information Systems Corporation               |
| Toshiba Products Marketing Inc.                      |
| 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 and Life Service Corporation         |
| Toshiba Health Insurance Association                  |
| Toshiba Infrastructure Systems & Solutions Corporation |

As of March 31, 2019
### 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 that is operated by the Information-technology Promotion Agency, Japan (IPA) and those certified under certification schemes in other countries (as of March 2019).

<table>
<thead>
<tr>
<th>Product</th>
<th>TOE Class</th>
<th>Certification Number</th>
<th>PP and EAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOSHIBA e-STUDIO 2515AC/3015AC/3515AC/4515AC/5015AC with a fax unit (GD-1370U/GD-1370NA/GD-1370EU), and a FIPS hard disk kit (GE-1230)</td>
<td>Digital MFP</td>
<td>C0633</td>
<td>PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5516AC/6516AC/7516AC with a fax unit (GD-1370U/GD-1370NA/GD-1370EU) and a FIPS hard disk kit (GE-1230)</td>
<td>Digital MFP</td>
<td>C0632</td>
<td>PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5518A/6518A/7518A/8518A with a fax unit (GD-1370U/GD-1370NA/GD-1370EU) and a FIPS hard disk kit (GE-1230)</td>
<td>Digital MFP</td>
<td>C0631</td>
<td>PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 2010AC/2510AC with a fax unit (GD-1370U/GD-1370NA/GD-1370EU) and a FIPS hard disk kit GE-1230)</td>
<td>Digital MFP</td>
<td>C0629</td>
<td>PP(Protection Profile for Hardcopy Devices 1.0 dated September 10, 2015)</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 3508LP/4508LP/5008LP, Loops LP35/LP45/LP50 MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0566</td>
<td>EAL2&lt;sup&gt;+&lt;/sup&gt;</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5508A/6508A/7508A/8508A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0529</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5506AC/6506AC/7506AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0528</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 2008A/2508A/3008A/3508A/4508A/5008A MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0524</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 2505AC/3005AC/3505AC/4505AC/5005AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0523</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 2000AC/2500AC MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V1.0</td>
<td>Digital MFP</td>
<td>C0522</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5560C/6560C/6570C MULTIFUNCTIONAL DIGITAL SYSTEMS SYS V3.0</td>
<td>Digital MFP</td>
<td>C0491</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 5518A/6518A/7518A/8518A with a fax unit (GD-1370U/GD-1370NA/GD-1370EU) and a FIPS hard disk kit (GE-1230)</td>
<td>Digital MFP</td>
<td>C0490</td>
<td>EAL3+</td>
</tr>
<tr>
<td>TOSHIBA e-STUDIO 2000AC/2500AC with a fax unit (GD-1370U/GD-1370NA/GD-1370EU) and a FIPS hard disk kit GE-1230)</td>
<td>Digital MFP</td>
<td>C0489</td>
<td>EAL3+</td>
</tr>
</tbody>
</table>

---

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.
The following table lists major products certified under the Japan Cryptographic Module Validation Program (JCMVP) based on ISO/IEC 19790 that is operated by IPA and those certified under the Cryptographic Module Validation Program (CMVP) based on FIPS140-2 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 2019).

<table>
<thead>
<tr>
<th>Product</th>
<th>Certification Number</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5-inch MHZ2 CJ hard disk drive series with an encryption function</td>
<td>J0006</td>
<td>Level1</td>
</tr>
<tr>
<td>Toshiba Solutions' encryption library</td>
<td>F0001</td>
<td>Level1</td>
</tr>
<tr>
<td>Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)</td>
<td>F0022</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (THNSB8 model)</td>
<td>2807</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)</td>
<td>2769</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)</td>
<td>2709</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)</td>
<td>2707</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model)</td>
<td>2521</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX04S model)</td>
<td>2520</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive (AL14SEQ model)</td>
<td>2508</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model NA02)</td>
<td>2410</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Hard Disk Drive</td>
<td>2333</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba TCG Enterprise SSC Self-Encrypting Solid State Drive (PX model)</td>
<td>2262</td>
<td>Level2</td>
</tr>
<tr>
<td>Toshiba Secure TCG Opal SSC and Wipe technology Self-Encrypting Drive (MQ01ABU050BW, MQ01ABU032BW and MQ01ABU025BW)</td>
<td>2082</td>
<td>Level2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Certification</th>
<th>Product</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achilles Communication Certification</td>
<td>TOSMAP-DS/LX OWB</td>
<td>Level2</td>
</tr>
<tr>
<td></td>
<td>TOSMAP-DS/LX OWR</td>
<td>Level2</td>
</tr>
<tr>
<td>ISA Secure® EDSA (Embedded Device Security Assurance) certification</td>
<td>CIEMACTM-DS/nv (TO SDIC-CIEDS/nv) Unified Controller nv series type2</td>
<td>EDSA2010.1/ Level1</td>
</tr>
</tbody>
</table>
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. |

![Sustainable Development Goals](image)
## Toshiba Group Business Overview

### Company Overview

<table>
<thead>
<tr>
<th>Company Name:</th>
<th>TOSHIBA CORPORATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters Address:</td>
<td>1-1-1 Shibaura, Minato-ku, Tokyo 105-8001, Japan</td>
</tr>
<tr>
<td>Founded:</td>
<td>July 1875</td>
</tr>
<tr>
<td>Paid-in capital:</td>
<td>¥200,044 million</td>
</tr>
<tr>
<td>Consolidated Net Sales:</td>
<td>¥3,693.5 billion</td>
</tr>
<tr>
<td>Number of Employees: (consolidated)</td>
<td>128,697</td>
</tr>
<tr>
<td>Number of Shares Issued:</td>
<td>54,400 million shares</td>
</tr>
<tr>
<td>Stock Exchange Listings:</td>
<td>Japan: Tokyo and Nagoya</td>
</tr>
</tbody>
</table>

### Consolidated business results

#### Net sales

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>(¥ billion)</td>
<td>48,511</td>
<td>43,465</td>
<td>40,437</td>
<td>39,476</td>
<td>36,935</td>
</tr>
</tbody>
</table>

#### Changes in operating income and net income

<table>
<thead>
<tr>
<th>Year</th>
<th>2014 △725 △378</th>
<th>2015 △5,814</th>
<th>2016 △9,657</th>
<th>2017 820 △8,040</th>
<th>2018 △9,657 △5,814</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating income</td>
<td>364 △378</td>
<td>641</td>
<td>△354</td>
<td>△8,040</td>
<td>△9,657</td>
</tr>
<tr>
<td>Current-term net income</td>
<td>△10,133</td>
<td>△5,814</td>
<td>△9,657</td>
<td>△8,040</td>
<td>△9,657</td>
</tr>
</tbody>
</table>

### Main products and services

#### Energy systems and solutions

Thermal power generation systems, power transmission and distribution systems, photovoltaic, hydroelectric, and nuclear power generation systems

#### Infrastructure systems and solutions

Water supply and sewerage systems, broadcasting systems, radar systems, elevators, industrial light sources, compressors, instrumentation and control systems, environmental systems, road systems, station service automation systems, general lighting apparatus, business-use air conditioners, public transportation systems, industrial systems, etc.

#### Retailing and printing solutions

POS systems, multifunction printers, etc.

#### Storage and electronic devices solutions

Small-signal devices, power devices, optical semiconductor devices, mixed-signal ICs, image sensors, logic ICs, HDDs, semiconductor manufacturing systems, etc.

#### Industrial ICT solutions

IT solutions and services, etc.

#### Others

Logistics services, etc.
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:+81-3-5444-9210
e-mail : HDQ-TOSHIBA-SIRT@ml.toshiba.co.jp

Toshiba’s Cyber Security Website
https://www.toshiba.co.jp/security/en

Published in August 2019