JAMA/JAPIA

JAMA/JAPIA Cybersecurity Guidelines

—Further Development of Cybersecurity Measures in the Automobile Industry—

Ver. 2.0

April 1, 2022

Japan Automobile Manufacturers Association, Inc.

Japan Automobile Manufacturers Association General Policy Committee
ICT Subcommittee
Cyber Security Subcommittee

Japan Auto Parts Industries Association

Japan Auto Parts Industries Association
IT Committee
Cyber Security Subcommittee

Revision History

Edition	Date Issued	Revision Details
Ver. 0.9	March 31, 2020	First version
Ver. 1	December 1, 2020	Issued as Ver. 1 based on the trial version Ver. 0.9
Ver. 2	April 1, 2022	In addition to the items that should be prioritized across the entire automobile industry—regardless of company size—formulated in the first version, Version2 was formulated by adding items that should be aimed at as a standard and items that should be aimed at as the final goal, depending on the information handled.

Table of Contents

1. Background and Purpose

The automobile industry is currently entering a once-in-a-century period of technological change—as represented by the acronym CASE (Connected, Autonomous, Shared & Services, Electric)—during which the entire industry is promoting the utilization of information technology to realize a mobile society. However, as more information systems managed by companies, such as IT infrastructure environments and factory control systems, are connected to the Internet, the threat of internet-based cyberattacks to in-house IT environments is increasing and concerns in recent years regarding cyberattacks on supply chains—including unauthorized access by attackers to the networks of affiliated companies and business partners in the process of reinforcing security measures, attacks via B2B networks, or unauthorized embedding of programs into software or products used by target companies—have shown that the cybersecurity risks faced by the automobile industry are growing more serious in nature.

In order for the automobile industry to realize a mobile society that is safe, secure, and prosperous while achieving sustainable development in an environment where cybersecurity risks are increasing, it is essential for the entire industry to gain an accurate understanding of the cybersecurity risks it faces and take appropriate measures against those risks.

Furthermore, in response to these evolving cybersecurity risks, Japan's Ministry of Land, Infrastructure, Transport and Tourism (MLIT) has required that the industry harmonize its cybersecurity measures using a cybersecurity certification system (UN WP29, CS/SU certification). Likewise, in order to improve supply chain security levels, Japan's Ministry of Economy, Trade and Industry (METI) has introduced its "Cyber/Physical Security Framework (CPSF)" which requires the creation of standard industry guidelines for the information systems field.

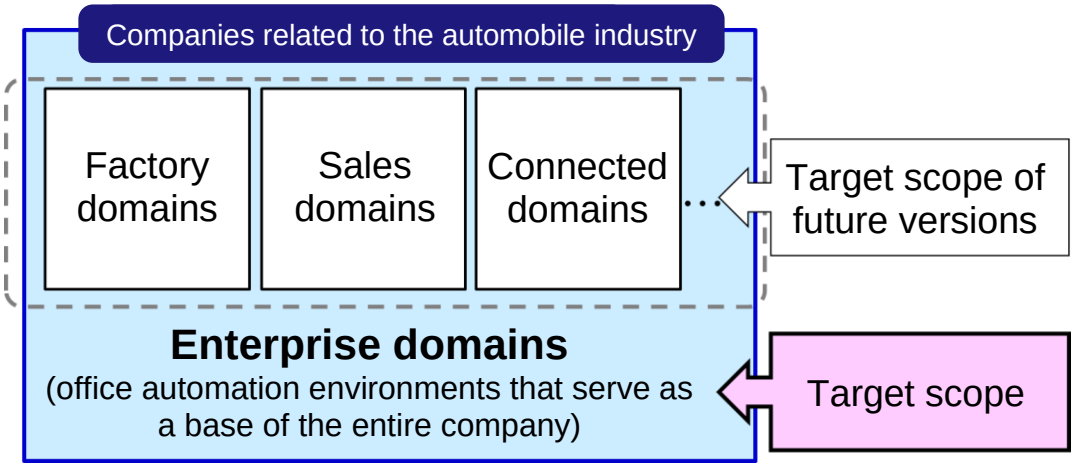
These guidelines—which are based on the background described above and take the unique cybersecurity risks faced by automobile manufacturers and companies that make up supply chains in the automobile industry into consideration—seek to clarify a three-year framework for cybersecurity measures and industry-wide self-assessment criteria aimed at enhancing cybersecurity measures throughout the entire automobile industry while promoting efficient inspections of cybersecurity levels.

2. Intended Audience for These Guidelines

These guidelines are intended for all companies related to the automobile industry, with the assumed readers being officers and employees of the following departments involved in security operations at each company.

- CISOs (Chief Information Security Officers)
- Risk Management Departments
- Audit Departments
- Security Support Departments
- Information System Development/Operation Departments
- Data Management Departments
- Purchasing/Procurement Departments responsible for supply chain management
- Other security-related departments (HR, Legal, General Affairs)

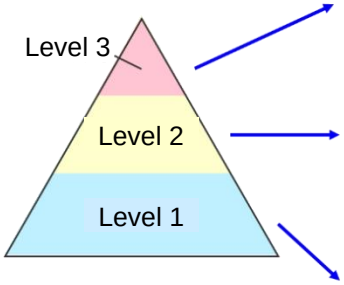
The scope of these guidelines is enterprise domains common to all operations (office automation environments that serve as a base for business operations), regardless of specific operations domain.



<Figure: Domains subject to the automobile industry cybersecurity guidelines>

3. Structure of These Guidelines

Because improving the security of the entire automobile industry supply chain is considered a priority, these guidelines were structured by narrowing down important items that should be prioritized across the entire automobile industry—regardless of company size—to enable their use by all companies, including small and medium-sized enterprises. Version2 was formulated by adding items that should be aimed at as a standard and items that should be aimed at as the final goal, depending on the information handled.



Level	Definition	Companies that Should Aim to Achieve Each Level
Lv3	Items that the automobile industry should be aiming for at this point* *April 2022	• Companies that should be indexed on behalf of the automobile industry from the perspective of company scale/technology level, or a company aiming to do so ◆All items from Lv1 to 3 achieved
Lv2	Items that the automobile industry should be aiming for as standard	Companies for which any of the following apply: • Companies that handle confidential information outside the company (technology, customer information, etc.) in the supply chain • Companies with in-house technology/information important for the automobile industry • Companies with a reasonable scale/share that can have a significant impact on the industry supply chain due to an accidental supply suspension, etc. ◆All items from Lv1 and 2 achieved
Lv1	The minimum of what should be implemented in the automobile industry	• All companies related to the automobile industry ◆All items from Lv1 achieved

<Figure: Definitions of security levels in the automobile industry cybersecurity guidelines>

Furthermore, a checklist is attached as an appendix to be used for confirming achievement status.

- Guidelines (this document)
  This document clarifies the background and purpose of these guidelines and includes descriptions on the scope of these guidelines, their structure, how they are to be utilized, requirements/conditions for achievement, as well as a glossary.

- Appendix: Checklist
  A checklist to be used for confirming requirements and conditions for achievement

These guidelines are centered on the “Cyber/Physical Security Framework (CPSF)” from Japan’s Ministry of Economy, Trade and Industry (METI) and were created by benchmarking “NIST Cybersecurity Framework v1.1”, “ISO 27001”, “AIAG Cyber Security 3rd Party Information Security 1st Edition” and “Guidelines for Information Security Measures for Small and Medium-sized Enterprises (IPA)”.

4. How to Utilize These Guidelines

We propose that these guidelines be used by all companies that support the automobile industry supply chain to improve security within their own organizations. This can be done by using them on a regular (once or more per year recommended) or as-needed basis to check for gaps in basic security measures.

Furthermore, the implementation of security measures based on common guidelines coupled with the subsequent assessment of those measures is expected to simplify and enhance the effectiveness of assessment processes aimed at constructing a chain of security and trust between companies and their business partners.

<Assumed method of utilization>

(1) Establishment of security policies at companies and implementation of security measures

The requirements and achievement criteria shown in the attached checklist can be referenced by companies in their efforts to establish security policies and implement security measures.

(2) Utilization of guidelines to construct a chain of trust in the automobile industry

By using a common security checklist to confirm the implementation status of security measures, these guidelines can be used to construct a chain of security and trust for B2B transactions in the complex automobile industry.

(3) Utilization of guidelines by companies for security education/training activities

These guidelines can be used by companies to assess the state of their in-house security, as well as for security education and training activities.

<Addition of information on the area in charge>

When it is unclear who is in charge of answering within the organization, the name of the area in charge (function) has been added for each countermeasure as reference information for when deciding the person in charge. Please refer to this information when deciding on an evaluator.

5. Requirements and Conditions for Achievement

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
1 Policies	As a company, demonstrate basic concepts and policies regarding security and enhance awareness of information security within the organization	An in-house information security policy shall be established and communicated within the organization	1	Lv1	An in-house information security policy is established	・An in-house information security policy shall be established and documented
			2	Lv2	The details regarding the in-house information security policy are checked and reviewed as necessary	[Rule(s)] ・Details are checked and reviewed as appropriate based on environmental changes both inside and outside the company [Frequency] ・The details regarding the information security policy are checked and reviewed as necessary -Once or more per year *There will be a separate, prompt response if a significant change occurs
			3	Lv1	The information security policy is communicated within the organization	[Rule(s)] ・The in-house information security policy shall be in a format that is easily accessible [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・The in-house information security policy shall be communicated within the organization regularly and whenever revised

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
2 Rules for handling confidential information	Prevent the leakage of confidential information by defining rules for handling confidential information and communicating those rules within the organization	In-house rules to ensure security for confidential information shall be defined	4	Lv1	Non-disclosure rules in the company are established and enforced	[Rule(s)] ・Non-disclosure rules shall be established and documented ・Explanations regarding non-disclosure rules are provided when new employees (including outside employees) join the company ・Confidential information shall not be carried outside the company when an employee resigns or their contract date expires [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.)
			5	Lv2		[Rule(s)] ・A letter of commitment for non-disclosure shall be submitted (excluding outside employees)
			6	Lv2	A non-disclosure agreement is entered into with the dispatching/transferring company for temporary and transferred employees	[Rule(s)] ・For non-disclosure, a statement shall be included stating that information obtained in the course of business will not be divulged [Timing] *When to enter into a contract for confidentiality obligations ・Before starting business
			7	Lv2	The necessary confidential information, IT equipment/devices, etc., is collected when an employee resigns or their contract date expires	[Standards] ・A checklist or form shall be created for the list of items to be collected ・Procedures shall be prepared and utilized that prevent collection omissions ・It shall be checked that collection is done in accordance with the procedure, and the procedure shall be corrected as necessary [Items to be collected] -Information (printed materials, storage media) -IT equipment/devices (PCs, smart devices) -Access rights (ID, keys) *In addition to the above, each company shall determine what items will be necessary to collect [Confirmation of collection status, frequency of procedure correction] -Once or more per year
			8	Lv1	Rules for the usage of IT equipment/devices employed for business operations are defined and communicated within the organization (including rules for personal devices [BYOD])	[Rule(s)] ・Rules for the usage of IT equipment/devices (computers, servers, communications equipment, storage media, smart devices, etc.) shall be established that include procedures for starting/ending usage, items to be observed/prohibited during usage, and procedures for when such equipment/devices are lost ・Rules for the usage of IT equipment/devices shall be in a format that is easily accessible [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Rules shall be communicated within the organization regularly and whenever revised

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
3 Compliance	As a company, comply with laws regarding information security	In-house rules shall be established to ensure compliance with laws regarding information security (Examples of laws: Act on the Protection of Personal Information, Unfair Competition Prevention Act)	9	Lv1	To ensure compliance with laws regarding information security, rules are established and education/communication are provided within the organization	[Rule(s)] ・In-house rules shall be established to ensure compliance with laws regarding information security ・Established in-house rules shall be communicated within the organization and education provided on those rules [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] (Training) ・Whenever a new employee joins the company and once per year (Communication within the organization) ・Rules shall be communicated within the organization regularly and whenever revised
			10	Lv2	For companies with personal information, there are in-house rules stipulated that are specifically for the handling of personal information	[Rule(s)] ・In-house rules shall be established regarding the handling of customer personal information [Details for clarification] ・Establish a personal information management system ・Notify and clearly indicate purpose of use at the time of acquisition ・Use within the scope of consent of the individual ・Do not provide to a third party without the consent of the individual ・Requests for disclosure, correction, suspension of use, deletion, etc., by the individual shall be responded to ・Rules for the handling of personal information shall be established ・Information shall be collected regarding information security laws and regulations such as the Act on the Protection of Personal Information, GDPR, and Unfair Competition Prevention Act ・Procedures for responding to information leaks ・Established in-house rules shall be communicated within the organization and education provided on those rules [Applies to] ・Those in charge of handling personal information [Frequency] (Training) ・Whenever a new employee joins the company and once per year (Communication within the organization) ・Rules shall be communicated within the organization regularly and whenever revised

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			11	Lv1	Rules are reviewed as necessary in accordance with changes to laws	[Frequency] ・Once per year, or when a serious information security incident/accident occurs
			12	Lv2		[Frequency] ・Compliance with in-house rules are checked and correction is carried out as necessary
4 System (Normal)	Clarify systems and roles for information security and thoroughly enact and reinforce measures for cybersecurity and protecting against data leakage	A system for managing information security risks for use in normal situations shall be constructed to enable the collection and sharing of information without incident	13	Lv1	The system, roles and responsibilities (incl. information security officers) during normal situations are clarified	[Rule(s)] ・The roles and responsibilities of the executive that presides over information security (CISO, etc.) and those of the department in charge of information security shall be clarified ・A list of contact persons shall be established
			14	Lv2		[Rule(s)] ・Understanding that information security risks have a significant impact on management, a system shall be established that enables systematic management decisions
			15	Lv1	The system for normal situations is reviewed regularly or as necessary	[Frequency] ・Once per year, or when a serious information security incident/accident occurs ・Or, when changes are made to the department or officer responsible for protecting/managing various information, including customer information, due to company reorganization, etc.
			16	Lv1	New methods of cyberattacks or leaking information are detected and corresponding security measures are shared with departments in the company A system is in place for monitoring and analyzing cyberattacks and signs	[Rule(s)] ・In accordance with the system for normal situation, examples of information security incidents/accidents and corresponding security measures shall be shared with departments in the company [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Once per year, or when a serious information security event/incident occurs either inside or outside the company
			17	Lv2		[Rule(s)] ・Build a system that will utilize public and non-public information regarding cyberattacks and vulnerabilities ・Allow for detection of cyberattacks and signs using correlation analysis, and build a system that can derive the appropriate responses from analysis results *Correlation analysis: A method for finding signs and traces of information security incidents/accidents by analyzing complex logs, etc.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
5 System (adverse situations)	Clarify systems and roles for information security and minimize damage in the event of an incident/ accident to enable recovery to normal operations as quickly as possible	A system for responding to information security incidents/accidents and its corresponding officers shall be clarified	18	Lv1	A system for responding to information security incidents/ accidents and its corresponding roles and responsibilities is clarified	[Rule(s)] ・The roles and responsibilities of the executive that presides over information security (CISO, etc.) and those of the department in charge of information security shall be clarified ・Criteria for information security incidents/accidents shall be clarified, as shall contact persons inside/outside the company and contact routes thereof
			19	Lv1	Information security incidents/accidents that occur are responded to and an overview of the accident and its impact/response measures are recorded	[Rule(s)] ・An initial response flow for information security incidents/accidents shall be established ・A reporting format for information security incidents/accidents shall be established
			20	Lv1	The system for adverse situations is reviewed regularly or as necessary	[Frequency] ・Once per year, or when a serious information security incident/accident occurs, etc.

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
6 Procedures in adverse situations	Same as above	Positioning information security incidents/accidents in the company's business continuity plan or emergency response plan	21	Lv3	A business continuity plan or emergency response plan is created for the company that includes information security incidents/accidents	[Standards] ・Devise a countermeasure plan based on the response history for security incidents/accidents and risk assessment results ・It shall be confirmed that the measures are implemented in accordance with the countermeasure plan [Details of the countermeasure plan] -Descriptions of measures (what kinds of measures should be taken for what events) -Schedule (start and end times and the period required for each process of the countermeasure) [Countermeasure progress confirmation] -Once or more per year
			22	Lv3	The business continuity plan or emergency response plan for the company that includes information security incidents/accidents is checked regularly and revised as necessary	[Frequency] ・Once or more per year
		Procedures for addressing information security incidents/accidents at an early stage shall be clarified	23	Lv2	The scope of information security incidents/accidents is clarified and communicated throughout the company	[Rule(s)] ・The following scopes shall be clarified [Details for clarification] -Events treated as accidents/incidents -Accident/incident levels [Applies to] ・Communicating to executives, employees, temporary employees, and seconded employees
			24	Lv1	Procedures (initial procedures, system recovery procedures, etc.) for responding to information security incidents/ accidents are defined	[Rule(s)] ・If necessary, the organization shall include the following response procedures (1) Procedures for reporting discovery of incidents/accidents, (2) Initial procedures, (3) Investigation/response procedures, (4) Recovery procedures, (5) Final reporting procedures
			25	Lv3	Procedures (initial procedures, system recovery procedures, etc.) for responding to information security incidents/accidents are checked regularly and revised as necessary	[Frequency] ・Once per year and when a serious incident/accident occurs
			26	Lv1	Procedures for responding to malware infections are defined	[Rule(s)] ・If necessary, the organization shall include the following procedures in responding to malware infections (1) Procedures for reporting discovery of incidents/accidents, (2) Initial procedures, (3) Investigation/response procedures, (4) Recovery procedures, (5) Final reporting procedures
			27	Lv2	Procedures for responding to malware infection are checked regularly and revised as necessary	[Rule(s)] ・The content of education/training shall be reviewed based on attack trends, world trends, etc. [Frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
7 Daily education	Have employees understand the risks surrounding malware and confidential information, as well as the correct handling methods thereof, in order to prevent information security incidents/accidents	Employees shall be educated to be aware of risks	28	Lv1	In-house education is provided regarding malware infections via email	[Rule(s)] ・Education on preventing malware via email shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. ・Review the content of training and improve the content of the next training [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) who use email [Frequency] ・Whenever a new employee joins the company and once or more per year
			29	Lv1	In-house education is provided regarding internet connections	[Rule(s)] ・Education on preventing malware during online browsing shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. ・Review the content of training and improve the content of the next training [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) who use the internet [Frequency] ・Whenever a new employee joins the company and once or more per year
			30	Lv1	Education is provided regarding the handling of information based on confidentiality classification	[Rule(s)] ・Education regarding definitions of confidentiality classifications and the handling thereof shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. ・Review the content of training and improve the content of the next training [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Whenever a new employee joins the company and once or more per year
			31	Lv2	Training on targeted emails is being implemented	[Rule(s)] ・Training on targeted emails shall be implemented ・Include in the training content what to do if an email is opened ・Review the methods and content of training and improve the content of the next training [Applies to] ・Those who use email [Frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			32	Lv2	Education is provided to information security managers in each department regarding measures to take and management methods within the organization	[Rule(s)] ・Education shall be provided regarding measures to take and management methods within the organization ・Review the content of training and improve the content of the next training [Applies to] ・Information security managers or promoters in each department *If an information security manager has not been appointed, the department manager [Frequency] ・Once or more per year
			33	Lv2	Opportunities are provided for corporate management to understand their roles and responsibilities with regard to information security	[Rule(s)] ・A forum is provided for corporate management to understand their roles and responsibilities ・Review the content of explanations and improve for the next iteration [Applies to] ・Corporate management, executives [Frequency] ・Once or more per year
			34	Lv2	Company-wide enlightenment activities are carried out	[Rule(s)] ・Opportunities shall be provided to reaffirm the importance of information security throughout the company [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Once or more per year
			35	Lv2	Enlightenment activities are carried out for particularly important risks and rules in each workplace	[Rule(s)] ・Reminders shall be given regarding particularly important rules and risks in the activity units (department, section, etc.) set by each company ・Review the content of enlightenment and improve the next iteration [Applies to] ・Employees and outside employees (temporary employees, etc.) whose understanding of workplace-specific risks and compliance with rules are especially important [Frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			36	Lv2	Have a concrete grasp of training and enlightenment implementation status with numerical values, etc.	[Rule(s)] ・Have a concrete grasp of the attendance and level of understanding for training and enlightenment sessions with numerical values, etc. [Target education, enlightenment] ・Education and enlightenment judged to be important by each company [Frequency] ・Once or more per year
			37	Lv3	Security education is provided to personnel involved in the procurement of information systems so that they can instruct suppliers	[Rule(s)] ・Education shall be provided via distributing/posting educational materials, e-Learning, group education, etc., in order for personnel to acquires skills for security guidance tailored to the characteristics of suppliers [Applies to] ・Personnel related to procurement of information systems [Frequency] ・Once or more per year
	Make advanced preparations for prompt and appropriate responses aimed at preventing further damage to enable prompt recovery when an information security incident/accident occurs	Education/training on information security incidents/accidents that have an impact within or across organizations, and methods of minimizing their impact, shall be provided	38	Lv1	Education/training for responding to information security incidents/accidents is provided	[Rule(s)] ・Education and training on responding to information security incidents/accidents shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. [Applies to] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Whenever a new employee joins the company and once or more per year
			39	Lv3	Education/training for responding to information security incidents/accidents across organizations is provided	[Rule(s)] ・Education and training on responding to information security incidents/accidents across organizations shall be provided by distributing/posting educational materials, e-Learning, or group education, etc. [Applies to] ・Security-related departments [Frequency] ・Once or more per year
			40	Lv1	Education/training content is reviewed as necessary	[Frequency] ・Before/after education and training, or once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
8 Information security requirements between companies	Prevent the leakage of confidential information in the supply chain and enable prompt response to accidents	Information security requirements for the supply chain shall be clarified	41	Lv3	The flow of goods and data is shared with suppliers	[Rule(s)] ・Must be able to identify important suppliers ・Must be able to identify the flow of goods and data ・An overview of transactions shall be illustrated and shared with the supplier [Applies to] ・Suppliers with which business occurs
			42	Lv3	Have a grasp of the status of security measures of business partners that handle important confidential information	[Rule(s)] Grasp the state of countermeasures of business partners by referring to the following examples: ・Create a checklist and receive answers from business partners ・Visit business partners and carry out inspections [Target companies] ・Subsidiaries, suppliers, etc., that provide and share important confidential information of the company Example: Companies that share "top secret" confidential information [Frequency] ・Once or more per year
			43	Lv3	Confidential information, access rights, etc., are collected or disposed of at the end of a contract	[Rule(s)] ・A checklist for confidential information, access rights, etc., to be collected shall be created ・Use the checklist at the end of a contract to collect confidential information, access rights, etc. ・Confirm that collection or disposal has been carried out without omission, and make corrections as necessary [Target companies] ・Subsidiaries, suppliers, etc., that provide and share confidential information [Frequency] ・Once or more per year
			44	Lv1	Methods of handling confidential information between companies are clarified	[Rule(s)] ・Methods of handling confidential information shall be exchanged before starting business [Applies to] ・Companies that share confidential information
			45	Lv3	Regular checks are made to see if there are any issues with how confidential information between companies is handled and revisions are made as necessary	[Frequency] ・Once or more per year
			46	Lv1	Roles and responsibilities when an information security incident/ accident occurs are clarified with other companies	[Rule(s)] ・When sharing confidential information, the roles and responsibilities of each company when an information security incident/accident occurs shall be documented
			47	Lv3	The text for roles and responsibilities with other companies in the event of an information security incident/accident is checked regularly and revised as necessary	[Frequency] ・Once or more per year
			48	Lv3	Have a grasp of the state of handling of other company's important confidential information in the company	[Rule(s)] ・The history of handling other company's important confidential information in-house shall be recorded and stored ・Confirm that recording and storage is done appropriately, and make corrections as necessary [Frequency of recording, checking storage status, correcting] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
9 Access rights	Prevent unauthorized access to confidential areas or systems due to inadequacies in access right settings	Access rights (room and system access rights) shall be managed appropriately	49	Lv1	Rules for managing access rights (room and system access rights) in the event of personnel transfers are defined	[Rule(s)] ・Management rules shall be defined to include the following: ・An application/approval system shall be used for issuing, changing, and revoking access rights ・Granted room entry permissions and access rights shall be limited to the scope necessary ・Methods of taking inventory for room entry rights and access rights shall be defined ・Applications and ledgers for granted room entry permissions and access rights shall be managed [Applies to] ・Systems used for business operations and user IDs for logging onto computers ・Locations or rooms in which considerations for confidentiality are required
			50	Lv2		[Rule(s)] ・For systems handling important information, clarify the conditions for granting access rights ・Setting of access rights should be carried out under strict management by clarifying the requirements and settings for the system administrator. ・Systems handling important information should have an environment in which authority is not concentrated on individuals, such as by separating the authority of those using information and system administrators. ・Monitor the operation/usage state for systems handling important information.
			51	Lv1	Access rights are issued, changed, disabled, or revoked in accordance with management rules	[Rule(s)] ・Inspections of the compliance status of the management rules defined in No. 49 shall be performed
			52	Lv1	An inventory of access rights is taken regularly or as necessary	[Rule(s)] ・In accordance with the rules defined in No. 49, an inventory of access rights shall be taken regularly or as necessary
			53	Lv2	Access logs are securely stored and managed in an access-controlled state	[Rule(s)] ・Logs are kept for an appropriate period so that matters required by laws and regulations can be met. ・To protect logs from threats, access restrictions, etc., are applied to the items and systems that store logs

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
10 Management of information assets (information)	Appropriately manage information assets to prevent the leakage of confidential information	Confidentiality classifications for information assets shall be set and understood, and information managed in accordance with those confidentiality classifications	54	Lv1	Management rules are defined for information based on confidentiality classification	[Rule(s)] ・Management rules shall be defined to include the following: ・Identification of confidentiality ・Determinations of levels for confidentiality classifications and their application ・Classification-based handling methods ・Handling area classifications and restrictions [Applies to] ・Information assets (information)
			55	Lv2	Management rules for information based on confidentiality classification are reviewed regularly or as necessary	[Rule(s)] ・The details of management rules are checked and improved as necessary [Frequency] ・Once or more per year
			56	Lv1	A list is created of information assets (information) with high confidentiality classifications	[Rule(s)] ・This list shall include the target information, administrator name, department name, storage location, storage period, persons disclosed to, contact persons, etc. [Target information] ・Information assets applicable to a high level of confidentiality among the confidentiality classifications defined in No. 54
			57	Lv2	The created list of information assets (information) with high confidentiality classifications is reviewed regularly or as necessary	[Rule(s)] ・The details of the list are checked and corrected as necessary [Frequency] ・Once or more per year
			58	Lv1	Management of information assets (information) is performed in accordance with management rules based on confidentiality classification	[Rule(s)] ・Inspections of the compliance status of the management rules defined in No. 54 shall be performed and corrective actions taken in the event irregularities or violations are found [Frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
11 Management of information assets (equipment/devices)	Appropriately manage IT assets to reduce the risks associated with information security incidents/accidents and shorten response times when an information security accident occurs	IT equipment/devices owned by the company and information (version information, administrator, administrating department, location installed, etc.) on the OS and software used by the equipment/device shall be managed appropriately	59	Lv1	Management rules for IT equipment/devices, OS, and software are defined based on importance	[Rule(s)] ・Management rules shall be defined that include equipment/device adoption, installation, network connections, application of security patches, etc.
			60	Lv1	A list is created of IT equipment/devices and information (version information, administrator, administrating department, location installed, etc.) on OS and software	[Rule(s)] ・A list of information for IT equipment/devices, OS and software shall be created that includes version information, administrators, administrating departments, locations installed, etc.
			61	Lv2	A list of IT equipment/devices and information (version information, administrator, administrating department, location installed, etc.) on OS and software is reviewed regularly or as necessary	[Frequency] ・Once or more per year
			62	Lv1	Management of information assets (equipment/devices) is performed in accordance with management rules based on importance	[Rule(s)] ・Management shall be performed in accordance with management rules defined in No. 59. Corrective actions shall be taken in the event irregularities or violations are found [Frequency] ・Once or more per year
			63	Lv3		[Rule(s)] ・Regularly check that devices and installed software are genuine by using serial numbers and hash values according to importance [Frequency] ・Once or more per year (when taking inventory of assets, etc.)
			64	Lv2	Unauthorized installation of applications on smart devices is restricted, and installation status is checked regularly	[Rule(s)] ・Applications that can be installed are defined, and installation status is checked regularly. [Applies to] ・Company-supplied smart devices [Confirmation frequency] ・Once a year
			65	Lv2	At the time of disposal (including at the end of a lease), the data on the storage medium is erased	[Rule(s)] ・When disposing of information assets (equipment) (including at the end of a lease), delete the data so that it cannot be restored ・Keep a record of having erased the storage area of information assets (equipment) or a vendor disposal certificate *Disc formats are not possible as data may be recovered [Applies to] -Servers, company-supplied client PCs, smart devices, external storage media

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
12 Risk response	Identify information asset security risks and take organizational measures as a company to minimize impacts to operations	Measures for information security risks shall be taken within the organization (organizational operations also include outsourced operations)	66	Lv1	Risks are identified when the three elements of information assets—confidentiality, integrity, and availability—cannot be ensured	[Rule(s)] ・The impact on operations when an information security incident/accident occurs to the target information asset shall be understood in terms of scope of impact and frequency of occurrence [Applies to] ・Information assets identified in No. 56 [Viewpoints] ・External threats ・Company vulnerabilities *Consider threats and vulnerabilities caused by business partners as necessary ・Value of information assets [Methods] ・Determine the target information and information systems ・Establish evaluation rules for each viewpoint and risk level rules that take those into consideration ・For each piece of information and information system, determine the risk level from the evaluation from each viewpoint [Frequency] ・When reviewing important information assets or once or more per year
			67	Lv3	Development standards are established that describe security requirements and they are regularly reviewed	[Rule(s)] ・Security development standards shall be established for information systems ・Check that development is proceeding in accordance with development standards ・Regularly review the content of the development standards [Frequency of review] ・Once a year
			68	Lv1	Impacts on operations and their measures are reported to management as necessary and shared with internal departments involved in security operations	[Rule(s)] ・Methods of measures for the impact on operations understood in No. 66 and plans thereof shall be formulated and reported/shared ・Any instructions received from executives when reporting shall be shared with relevant departments [Applies to] ・Chief Information Security Officer, related departments [Frequency] ・Once or more per year
			69	Lv1	Management of measures for impacts on operations are performed in accordance with formulated plans	[Rule(s)] ・In addition to appropriately implementing the measures and plans created in No. 68, it shall be confirmed that any impact to operations was reduced, and corrective actions taken for any irregularities that are discovered [Applies to] ・Impact to information asset operations [Frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
13 Understanding details of business transactions and methods	Prevent information leakages, etc., during the course of business transactions by clarifying what methods are used to exchange information assets and with what business partners	Information assets exchanged over the course of business transactions with each business partner, as well as the methods used for such transactions, shall be understood	70	Lv1	A list is created for the information exchanged with each company and the methods used (methods of exchanging information, such as for receiving/sending orders)	[Rule(s)] ・This list shall include information assets exchanged/used during transactions, as well as how they are handled, and mutually understood by the business partner [Applies to] ・Business partners with which important information assets (such as the highly confidential information assets defined in No. 54) are shared [Frequency] ・When starting business transactions or when changes are made to information exchanged and methods used
			71	Lv3	The list of information exchanged with each company and the methods used (methods of exchanging information, such as for receiving/sending orders) is reviewed regularly or as necessary	[Frequency] ・Once or more per year
		Managing information security risks regarding the procurement of IT equipment	72	Lv3	Security requirements for the procurement of IT equipment are established and communicated within the organization	[Rule(s)] ・A list shall be made of the security requirements for procuring equipment ・Security requirements can be easily confirmed when procuring equipment [Applies to] [Equipment] ・IT equipment connected to the internal network [Communication] ・Executives, employees, outside employees (including temporary employees, etc.) [Frequency] ・Information shall be communicated within the organization regularly and whenever the security requirements for procuring equipment are revised
			73	Lv3	Security requirements for the procurement of IT equipment are shared with the provider, and results of the evaluation at the time of purchase are recorded and stored	[Rule(s)] ・Security requirements are clearly stated in the purchase contract, etc. ・When procuring equipment, security requirements are evaluated and the results are stored ・There are regular checks confirming the storage of check results [Applies to] ・IT equipment connected to the internal network [Frequency of checking storage status] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
14 Understanding the statuses of external connections	Ensure safety and trust when using external information systems, while enabling prompt response to information security incidents/accidents	For relations with affiliated organizations (including suppliers, etc.), understand the communication network structure for your own organization and monitor the status of cooperation with other organizations as well as the flow of data	74	Lv2	Network and data flow diagrams are created, and communication with affiliated organizations (including suppliers, etc.) are monitored	[Standards] ・Network diagrams shall be created [Scope] -Networks where the company's own IT equipment/devices exists [Frequency of review] -Once or more per year <Addition> [Standard] ・Data flow diagrams shall be created [Scope] -Data within the company exchanged over the network between affiliated organizations [Standard] ・Communication with affiliated organizations shall be monitored [Scope] -Data exchanged on the network between affiliated organizations [Frequency] -Always
			75	Lv2	Network and data flow diagrams are reviewed regularly or as necessary	[Frequency] ・Once or more per year
		External information systems (such as those of customers, subsidiaries, affiliated companies, contractors, cloud services, external information services) shall be clarified and their usage status managed appropriately	76	Lv1	Rules for using external information systems connected to organizational assets are defined	[Rule(s)] ・Usage rules shall be defined to include the following: ・Non-disclosure agreements are entered into with entities that connect with external information systems ・Security requirements for using external information systems are defined ・Service details are checked to conform that security requirements for using external information systems are met and evidence of the approval thereof is saved
			77	Lv1	A list of external information systems that are used is created	[Rule(s)] ・A list of external information systems shall be created
			78	Lv1	The list of external information systems is reviewed regularly or as necessary	[Rule(s)] ・In addition to regularly taking inventory, new external information systems shall be added to the list and those for which usage has stopped removed from the list [Frequency] ・Once or more per year and whenever use of new system starts or use of a system stops

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
15 In-house connection rules	Minimize damage, such as that caused by information leakage and malware infections, by appropriately managing the usage of internal networks	When connecting to internal networks, measures shall be implemented to minimize unauthorized usage of information systems and IT equipment/devices For remote work environments, measures are taken to prevent security incidents (primarily information leakage and spoofing)	79	Lv1	Rules for connecting IT equipment/devices used for business to internal networks are defined	Connection rules for equipment/devices such as computers and servers: [Rule(s)] ・Rules regarding connections to internal networks shall be defined [Applies to] ・All equipment/devices that connect directly to in-house networks ・Including standard company equipment/devices and equipment/devices brought in from the outside Additional rules for connecting from external to internal networks: [Rule(s)] ・Rules for using remote access shall be defined [Applies to] ・All equipment/devices that connect to internal networks from outside the company via public internet or leased lines
			80	Lv3	There is a system that restricts connections to the internal company network, except for authorized devices	[Rule(s)] ・A system shall be introduced to detect and block connections other than those from authorized devices [Applies to] ・Devices connecting to the company network
			81	Lv3	A system has been introduced as a measure against internal information leakage that can automatically detect abnormal behavior by combining multiple logs	[Rule(s)] ・It must be possible to detect the unauthorized removal of information by analyzing logs related to information ・It must be possible to be alerted in the event of unauthorized removal of information
			82	Lv2	Rules have been established and are operated under regarding conditions for confidential information and IT equipment/devices used in remote work	[Rule(s)] ・Rules shall be established and communicated within the company regarding conditions for confidential information and IT equipment/devices used in remote work ・Confirm compliance with rules and make corrections as necessary [Targets for communication] -All employees, temporary employees, and seconded employees working remotely [Timing for communication] -Before the start of remote work [Content of rules] -IT equipment/devices that are permitted to be used in remote work *Including application and approval methods as necessary -Confidentiality classifications and types of files that can be downloaded to personally owned terminals [Frequency for checking the content of rules and compliance status] -Once or more per year
			83	Lv2	Rules have been established and are operated under regarding working remotely	[Rule(s)] ・Rules shall be established and communicated within the company regarding working remotely ・Confirm the details of rules and compliance status, and make corrections as necessary [Targets for communication] -All employees, temporary employees, and seconded employees working remotely [Timing for communication] -Before the start of remote work [Frequency of checking and correcting the content of rules and compliance status] -Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
16 Physical security	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Physical security measures shall be implemented for areas where equipment such as servers are installed	84	Lv1	Persons with access to areas where equipment such as servers are installed are defined	[Rule(s)] ・Persons with access to areas where equipment such as servers are installed shall be defined
			85	Lv1	Locks or other devices are used to restrict access to areas where equipment such as servers are installed	[Rule(s)] ・Areas where equipment such as servers are installed shall be locked ・If servers are installed in an area where locking is not possible, servers shall instead be installed on a dedicated rack that is then locked ・An administrator responsible for locking shall be designated
			86	Lv2	Records of entry into areas where equipment such as servers are installed are kept and checked regularly	[Rule(s)] ・Records for entry into/exit from areas where equipment such as servers are installed shall be obtained and stored [Items to be recorded] ・Entry/exit date and time ・Name of the individual (name, affiliation, contact information, etc.) ・Reason for entering ・Approved by [Storage period] ・Six months
			87	Lv2	Unauthorized intrusions and suspicious behavior in areas where equipment such as servers are installed is monitored	[Rule(s)] ・Items brought in/taken out are checked when entering or leaving ・The behavior of visitors is monitored
		Measures are taken to prevent security incidents (primarily unauthorized intrusion, unauthorized removal, information leakage, and suspicious behavior) with regard to entering or exiting the company	88	Lv2	Rules are established, communicated within the company, and operated under regarding entry and exit	[Rule(s)] ・Rules regarding entering and exiting the company shall be defined ・Entry/exit rules shall be communicated within the company ・Confirm the details of entry/exit rules and compliance status, revising and re-informing employees as necessary [Targets for communication] ・All personnel entering/exiting the company [Content of entry/exit rules] ・Areas with restricted entry are defined ・Application and approval when entering/exiting ・Identity confirmation measures when entering/exiting (wearing employee ID cards, entry permits, etc.) ・Rules for issuing entry permits and gate passes [Frequency of checking and correcting the content of entry/exit rules and compliance status] ・Once or more per year
			89	Lv2	Access to important areas and rooms are restricted, and entry/exit records are stored	[Rule(s)] ・Entry into and exit from important areas and rooms shall be restricted ・Entry/exit records for important areas and rooms shall be obtained and stored [Items to be recorded] ・Entry/exit date and time ・Name of the individual (name, affiliation, contact information, etc.) ・Reason for entering ・Approved by [Record storage period] ・Six months or more
			90	Lv2	Unauthorized intrusions and suspicious behavior is monitored	[Rule(s)] ・Unauthorized intrusions and suspicious behavior shall be monitored for important locations in the company ・Confirm that monitoring is functioning normally and make corrections as necessary [Frequency of confirming and correcting monitoring status] ・Once or more every six months

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
		Place restrictions on items carried in/taken out	91	Lv2	Rules for what can be carried into the company are clarified and operated under	[Rule(s)] ・Rules for carrying items into the company shall be defined ・Check the content of carry-in rules and compliance status, and make corrections as necessary [Applies to] ・Employees, temporary employees, seconded employees, and individuals from outside the company [Target items] ・Computers, tablets, smart devices, cameras, external storage media *If there are other recordable items, judgments should be made by each company [Content of carry-in rules] ・Areas and items subject to carry-in restrictions ・Application and approval methods for carrying items into the company ・Storage and control methods for carry-in records (retention period: six months) [Frequency of checking and correcting the content of carry-in rules and compliance status] ・Once or more per year
			92	Lv2	Rules for what can be carried out of the company are clarified and operated under	[Rule(s)] ・Rules for carrying items out of the company shall be defined ・Check the content of carry-out rules and compliance status, and make corrections as necessary [Applies to] ・Employees, temporary employees, seconded employees, and individuals from outside the company [Target items] ・Computers, tablets, smart devices, cameras, external storage media, printed materials (confidential documents such as diagrams) *Other necessary items should be judged by each company [Content of carry-out rules] ・Application and approval methods for carrying items out of the company ・Storage and control methods for carry-out records (retention period: six months) [Frequency of checking and correcting the content of carry-out rules and compliance status] ・Once or more per year
			93	Lv2	Measures are taken to raise awareness of carry-in/carry-out rules	[Rule(s)] ・Measures shall be taken to raise awareness of carry-in/carry-out rules [Implementation frequency] ・Once or more every six months

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
		Video and audio recording in the company, measures are taken to prevent security incidents (primarily information leakage)	94	Lv2	Rules are established and operated under regarding photography in the company	[Rule(s)] ・Rules regarding photography within the company shall be defined ・Confirm the details of photography rules and compliance status, and make corrections as necessary [Content of photography rules] ・Items and areas subject to photography restrictions ・Application and approval procedures for photography ・Storage of photography applications, action records (retention period: six months) *Areas with no restrictions on photography can also be set up (Example: Areas for meeting with individuals from outside the company) [Frequency of checking and correcting the content of photography rules and compliance status] ・Once or more per year
			95	Lv3	Rules are established and operated under regarding the recording of audio	[Rule(s)] ・Rules regarding audio recording shall be defined ・Confirm the details of audio recording rules and compliance status, and make corrections as necessary [Content of audio recording rules] ・Definitions of meetings (including face-to-face and remote) and areas where audio recording is restricted ・Application and approval methods for audio recording *It is also possible to make distinctions regarding the need for applications and approval based on meeting type and area [Frequency of checking and correcting the content of recording rules and compliance status] ・Once or more per year
			96	Lv3	Measures are taken against information leakage due to eavesdropping	[Rule(s)] ・Measures shall be taken against information leakage due to eavesdropping [Implementation frequency] ・Once or more per year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
		Measures shall be taken to understand what should be targeted for countermeasures when a vulnerability is discovered and to prevent information leakage, etc., using external storage media	97	Lv2	Standard PC configuration/setting rules are defined, and if there is a change to these standard configuration/setting rules, the change is made after approval	[Rule(s)] ・Standard PC configurations (software and version) and settings shall be defined ・There is an approval system for changes to the configuration or setting [Applies to] -OS, office software, browsers, and anti-virus software for company-supplied PCs
			98	Lv2	What software is allowed to be/prohibited from being used on PCs is defined, the unauthorized installation of software is prohibited, and there are regular checks for violations	[Rule(s)] ・A list of allowed/prohibited software in the company shall be created and communicated within the organization ・Unauthorized installation of software shall be restricted ・Software installation status shall be checked regularly *No confirmation is required if installation is restricted by the system [Applies to] -Company-supplied client PCs [Examples of software to be restricted] -Software tied to information leakage -Software with serious vulnerabilities -Apps suspected of being malware/spyware [Confirmation frequency] -Once a year [Targets for communication] -Executives, employees, temporary employees, and seconded employees
			99	Lv2	There is a system that restricts exporting data from PCs	[Rule(s)] ・A system limiting the export of data shall be introduced [Applies to] -Company-supplied client PCs
			100	Lv2	For important data that would interfere with business if it were damaged by malware (data encryption, etc.), rules are established and communicated that it is stored outside of PCs	[Rule(s)] ・Important data shall be stored in a location other than client PCs [Targets for communication] -Executives, employees, temporary employees, and seconded employees

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
		For systems that store and use important information, measures are taken to minimize the damage caused by human error regarding setting mistakes	101	Lv2	Unnecessary features on servers are disabled Use of default user IDs is stopped Default passwords are changed	[Rule(s)] ・Unnecessary services and daemons shall be disabled ・Use of default user IDs shall be stopped ・Default passwords shall be changed
			102	Lv2	Managing departments have carried out the necessary settings for confidentiality management on smart devices	[Rule(s)] ・Passwords shall be set ・A data deletion function is set in the case of being lost
17 Communication control		Communication is controlled to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	103	Lv2	A firewall is installed at the boundary between the internet and the internal company network to restrict communication	[Rule(s)] ・A system shall be introduced to restrict internal and external network communication [Introduction location] -Boundaries between internal and external networks [Items to be restricted] -The IP addresses of connection sources and connection destinations -Communication ports
			104	Lv2	Firewall filtering settings (communication permissions/blocking settings) are recorded, with regular checks for unnecessary settings	[Rule(s)] ・Filtering settings for internal and external network communications shall be recorded ・Periodically check for unnecessary filtering settings ・Delete unnecessary filtering settings [Items to be recorded] ・Applicant name, IP addresses of connection source and destination, communication direction, protocol, port number, usage, registration date, expiration date [Confirmation frequency] ・Once a year
			105	Lv2	Remote access IDs are managed with regular checks for unnecessary IDs	[Rule(s)] ・The issuing, changing, and deleting of remote access IDs are carried out through an application/approval system ・There shall be regular checks for unnecessary IDs ・Unnecessary IDs are deleted [Confirmation frequency] ・Once a year

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			106	Lv2	Networks are separated according to business and data importance.	[Rule(s)] ・Systems shall be classified according to business content and data importance, and they shall be installed in dedicated network segments [Applies to] ・External public servers
			107	Lv2	Configured so that there is no effect on the production environment when developing or testing	[Rule(s)] ・The development environment and test environment shall be separated from the production environment [Applies to] -Important in-house servers, important external public servers *Targets are decided up by each company according to risk
			108	Lv2	Access to malicious websites is restricted	[Rule(s)] ・Access to malicious websites shall be restricted [Applies to] ・Client PCs, web gateways
			109	Lv2	A Web Application Firewall (WAF) is installed for web applications published on the internet	[Rule(s)] ・WAF (Web Application Firewalls) shall be installed [Applies to] ・Important external public web applications
			110	Lv2	Measures are implemented to continue the service of websites and systems published on the internet even if subjected to DDoS attacks	[Rule(s)] ・A system shall be introduced to continue service in the event of a DDoS attack [Applies to] ・Important external public websites, DNS servers
			111	Lv2	Communication is encrypted to prevent eavesdropping and tampering with communication via the internet	[Rule(s)] ・Internal and external network communications shall be encrypted [Applies to] ・Remote access communication from outside the company ・Communication with authentication between the user and an external public server
			112	Lv2	Communication between terminals and wireless LAN access points is encrypted	[Rule(s)] ・Communication between terminals and access points shall be encrypted ・Do not use cryptographic technology that has been compromised according to CRYPTREC [Applies to] ・In-house wireless LANs

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
18 Authentication /Approval	・Prevent information leakage/unauthorized modification and ensure stable information system operation by preventing unauthorized usage or unauthorized operation/modification of information systems ・Enable the causes of information leakage, unauthorized modification, or system stoppages to be investigated	Authentication and approval measures shall be used for information systems and IT equipment/devices	113	Lv1	Unique user IDs are assigned to each person	[Rule(s)] ・User IDs shall not be shared ・If the sharing of user IDs is unavoidable, it shall be possible to identify the user of the shared ID [Applies to] ・User IDs for logging onto systems and computers used for business operations
			114	Lv1	Different rights are granted to user IDs and system administrator IDs	[Rule(s)] ・System managers and officers shall be defined ・Employees with administrative rights shall be limited ・The minimal rights necessary for roles to be performed shall be granted ・System administrators shall not be allowed to operate using administrative rights in production environments ・Administrator passwords shall be set appropriately [Applies to] ・All servers, network devices
			115	Lv1	Rules for the setting of passwords are defined and communicated within the organization	[Rule(s)] ・Number of digits, letter combinations, and expiration dates shall be defined ・Easily guessed passwords, such as repeated numbers or letters, shall be avoided ・If it is found that a password has been leaked, the password shall be changed [Applies to] ・Passwords for logging onto systems and computers used for business operations [Targets for communication] ・Executives, employees, temporary employees, and seconded employees
			116	Lv2	Rules for the setting of passwords for external information systems are defined and communicated within the organization	[Rule(s)] ・Target passwords shall not be set in external web services *If the same authentication platform (SSO, etc.) is used, this does not count as being reused [Target passwords] ・Passwords when logging into PCs ・Mail system passwords (Microsoft 365, etc.) [Targets for communication] ・Executives, employees, temporary employees, and seconded employees
			117	Lv1	An inventory of user IDs and system IDs is taken regularly or as necessary, during which unnecessary IDs are deleted	[Rule(s)] ・Rules for implementing inventory taking that clearly specify when such inventory taking is to take place shall be defined and unnecessary IDs deleted [Applies to] ・User IDs and system administrator IDs for logging onto systems and computers used for business operations

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			118	Lv2	Procedures for issuing, changing, and deleting user IDs are set in place	[Rule(s)] ・There shall be an application/approval system for the issuing, changing, and deleting of user IDs [Applies to] ・User IDs for logging onto systems and computers used for business operations
			119	Lv2	Manager approval is obtained for the granting/changing/deleting of administrative rights and for changing the settings of servers and network devices	[Rule(s)] ・There shall be an application/approval system for the granting, changing, and deleting of administrative rights ・There shall be an application/approval system for changing the settings of servers and network devices ・Server administrative rights shall be managed (additions, changes, modifications) ・Individuals who can use administrative rights on network devices shall be controlled
			120	Lv3	Multi-factor authentication is implemented for systems that can be used from the internet	[Rule(s)] ・There shall be at least two forms of authentication implemented (knowledge/possession/biometric) for authentication via the internet [Applies to] ・Systems that handle information with a high level of confidentiality ・Privileged accounts ・Remote access
			121	Lv2	Session time-outs are implemented for important systems	[Rule(s)] ・Session time-outs shall be implemented for important systems [Applies to] ・External public systems, important internal systems
			122	Lv3	Monitoring of authentication logs is implemented	[Rule(s)] ・Monitoring of authentication logs shall be implemented and it shall be possible to detect suspicious authentication [Applies to] ・PCs, server authentication logs, database access logs for important systems [Frequency] ・Once or more a month

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
19 Applying patches and updates	Reduce the risk of unauthorized access and malware infection	Avoid using devices, operating systems, and software that is no longer supported	123	Lv2	The use of operating systems and software that is no longer supported is avoided	[Rule(s)] ・Supported OS and software shall be used ・If an OS or software that is not supported must be used, reduce the risk of vulnerabilities being exploited as practicable as possible [Applies to] ・OS, browser, office software for company-supplied PCs ・Server OS, middleware ・OS and applications for company-supplied smart devices ・OS and firmware of network devices in contact with the internet
		Implement measures to prevent unauthorized access using vulnerabilities	124	Lv1	Security patches and updates are properly applied for information systems, IT equipment/devices, and software	[Rule(s)] ・The applying of security patches and updates shall have defined rules and deadlines ・If they cannot be applied for an unavoidable reason, record the reason why it cannot be applied [Applies to] ・PCs, smartphones, tablets, servers, network devices, software, etc. -OS, browser, office software for company-supplied client PCs -Server OS, middleware -OS and applications for company-supplied smart devices -OS and firmware of network devices in contact with the internet
			125	Lv2	A management system and management process has been set in place for vulnerabilities	[Rule(s)] ・The roles and responsibilities of the departments in charge from collecting vulnerability information to responding shall be clarified ・The sources, tools, and frequency for collecting vulnerability/threat information shall be defined ・Criteria and procedures for determining the necessity of responding to the collected information shall be defined ・Correspondence history shall be recorded and checked monthly
			126	Lv3	For servers that are open outside of the company, vulnerability diagnoses before and after production are carried out, and measures are taken against identified vulnerabilities	[Rule(s)] ・Platform vulnerabilities shall be diagnosed ・The rules and lead time for determining the necessity of dealing with vulnerabilities shall be defined ・Diagnosis and response results shall be stored [Applies to] ・External public server OS, middleware [Diagnosis frequency] ・Before production: One or more times ・After production: Twice a year and when a major system change takes place ・When a high-impact vulnerability is made public

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			127	Lv3	For in-house servers, vulnerability diagnoses before and after production are carried out, and measures are taken against vulnerabilities	[Rule(s)] ・Platform vulnerabilities shall be diagnosed ・The rules and lead time for determining the necessity of dealing with vulnerabilities shall be defined ・Diagnosis and response results shall be stored [Applies to] ・Important internal server OS, middleware [Diagnosis frequency] ・Before production: One or more times ・After production: Once a year and when a major system change takes place
			128	Lv3	Application vulnerability diagnoses are carried out for web applications published on the internet	[Rule(s)] ・Web application vulnerabilities shall be diagnosed ・The rules and lead time for determining the necessity of dealing with vulnerabilities shall be defined ・Diagnosis and response results shall be stored [Applies to] ・Important external public web applications [Diagnosis frequency] ・Before production: One or more times ・After production: When a major application change takes place

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
20 Data protection	Reduce the risk of unauthorized access and malware infection	The data of information systems and IT equipment/devices is being protected	129	Lv3	The data of IT equipment/devices and information systems is properly encrypted	[Rule(s)] ・Data on personal computers and storage media taken outside the company shall be encrypted ・The databases for important systems shall be encrypted
			130	Lv2	Data received from the outside is confirmed safe	[Rule(s)] ・Real-time scans using anti-virus software shall be implemented ・A system shall be introduced for checking the safety of files received from the outside in a secure virtual environment
21 Office tool-related	Reduce the risk of unauthorized access and malware infection	The data of information systems and IT equipment/devices is being protected	131	Lv2	Measures are implemented to prevent information leakage due to email transmission	[Rule(s)] ・When sending confidential information by email, measures shall be implemented to prevent information leakage
			132	Lv2	Measures are implemented to prevent erroneous email transmission	[Rule(s)] ・Measures shall be implemented to prevent erroneous email transmission [Applies to] ・Mail sent to addresses outside of the company
			133	Lv2	Emails sent outside the company are audited, and users are informed that auditing is taking place as a way to combat internal fraud	[Rule(s)] ・Implement email auditing and communicate within the organization that auditing is taking place [Applies to] ・Mail sent to addresses outside of the company [Targets for communication] ・Executives, employees, temporary employees, and seconded employees
			134	Lv2	Prohibitions and restrictions on the use of websites and web applications are clarified and communicated within the organization	[Rule(s)] ・The following shall be clarified and communicated within the organization: -Do not post company information on social media without permission -Do not upload business data to web services without permission [Targets for communication] ・Executives, employees, temporary employees, and seconded employees
			135	Lv2	Establish and disseminate usage rules for sharing files with affiliated companies and business partners (including the use of cloud services)	[Rule(s)] ・The following shall be clarified and communicated within the organization: -When sharing files outside the company, share only with trusted parties -File transfers outside the company using a method that does not leave a transmission history are prohibited *File sharing: Uploading a file to a specific location and allowing a specific individual to access the file *File transfer: Sending a file directly to a specific individual [Targets for communication] ・Executives, employees, temporary employees, and seconded employees

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
22 Malware countermeasures	Prevent information leakage, unauthorized modifications, and system stoppages due to malware infections	Anti-malware measures shall be implemented to quickly detect security abnormalities	136	Lv1	Software (anti-virus software) is used on computers and servers to detect malware and provide notifications	[Rule(s)] ・Anti-virus software shall be used on each computer and server ・Scans shall be performed by specifying scan scopes and frequencies appropriate for the equipment/device [Applies to] ・All computers and servers connected to networks
			137	Lv1	Anti-virus software pattern files are updated regularly	[Applies to] ・Same as No. 136 [Pattern file update frequency] ・Once or more on days computers/servers are booted and used
			138	Lv3	A behavior tracking system has been introduced that allows for the acquisition of detailed histories at endpoints and remote response after malware infection	[Rule(s)] ・An endpoint countermeasure system shall be introduced [Applies to] ・Company-supplied client PCs ・Servers [System requirements] ・Can obtain terminal operation history, program execution history, registry change history ・Can remotely investigate terminals ・Can remotely disconnect from the network ・Can recover after infection
			139	Lv2	Malware checks are implemented at email gateways to prevent malware infection by email	[Rule(s)] ・A malware check function shall be introduced at the email gateway
			140	Lv2	Extension restrictions are enforced by a system to prevent malware intrusion from email attachments	[Rule(s)] ・A function restricting specific extensions shall be introduced at the email gateway
			141	Lv2	Malware checks are implemented at web gateways to prevent malware infection by viewing malicious websites	[Rule(s)] ・A malware check function shall be introduced at the web gateway

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
23 Detecting unauthorized access	Prevent information leakage, unauthorized modifications, and system stoppages due to unauthorized access and intrusions	Build a system to constantly monitor unauthorized access to the network	142	Lv2	A system is introduced to constantly monitor the content of communications and detect/block and notify regarding unauthorized access in real time	[Rule(s)] ・A system shall be introduced that detects/blocks unauthorized access in real time [Applies to] ・Communications from the internet to the company ・Communications from within the company to an unauthorized server [Introduction location] ・Boundaries between internal and external networks
		Logs shall be acquired so that intrusion and leak routes can be investigated in the event of a security incident or accident	143	Lv2	Logs required for investigation when an incident occurs are being obtained	[Rule(s)] ・The following logs shall be obtained and stored [Logs to be obtained (retention period)] -Email transmission/reception logs (6 months) Items: Date and time, destination email address, sender email address -Firewall logs (6 months) Items: Date and time, source IP address, destination IP address -Proxy server logs (6 months) Items: Date and time, requester IP address, URL -Remote access logs (6 months) Items: Date and time, connection source IP address, user ID -Authentication server logs (6 months) Items: Date and time, connection source IP address, user ID, success/failure -Endpoint (PC, server) operation logs (6 months) Items: Date and time, host name, user ID, IP address, operation details *Also includes the use of cloud services *If using a cloud service that cannot meet the regulations for retention period, each company shall determine the period according to risk
			144	Lv3	Application operation logs are obtained for important systems	[Rule(s)] ・User and administrator operation logs shall be obtained [Applies to] -Important systems *Applicable systems are judged by each company according to risk [Log items to be acquired] -User ID, time stamp, operation details (login, logout, addition/deletion, etc.) [Retention period] -6 months *If using a cloud service that cannot meet the criteria for the retention period, each company shall determine the period according to risk

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
		Take measures to promptly detect and block cyberattacks in order to curb damage caused by targeted attacks and other such cyberattacks	145	Lv2	A system is introduced to analyze logs and detect cyberattacks	[Rule(s)] ・A system shall be introduced to constantly analyze logs and given notification when an abnormality is found [Analysis targets] -Proxy servers, IPS/IDS, firewalls, endpoints, or a combination thereof [Monitoring period] -24 hours a day, 365 days a year [Functional requirements] -Incident alerts are issued immediately -Breaking incident reports are created and notifications given
			146	Lv2	Measures are implemented to block communication between malware that has intruded into the company and unauthorized servers	[Rule(s)] ・A system shall be introduced to block communication from within the company to unauthorized servers
			147	Lv3	For websites published on the internet, a system is introduced to detect site falsification and checks are made regularly	[Rule(s)] ・A system shall be introduced to detect website falsification [Applies to] ・Important external public websites
24 Backup/Restore	Minimize the impact of system stoppages and data loss on business operations, and enable operations to resume quickly	Measures shall be taken to minimize the damage to important information and impact to system operations caused by cyberattacks	148	Lv1	Backups are performed at appropriate times	[Rule(s)] ・Data, etc., subject to back up and backup frequencies shall be defined
			149	Lv1	Restore procedures are established	[Rule(s)] ・Restore procedure manuals shall be established for each type of data, etc., subject to backup
			150	Lv1	Alternative means that can be used to perform business operations in the event of a system stoppage are prepared	[Rule(s)] ・Viable alternative means shall be established for use in the event systems are down [Applies to] -Systems requiring a high level of availability (short allowable downtime) *Targets are determined by each company according to risk [Example measures] -Use of analog tools (fax, etc.) -Use of external information systems such as cloud services

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievement Criteria
			151	Lv2	Backup restore tests on important data and systems are implemented	[Rule(s)] ・It shall be confirmed that restoration is possible according to specified restoration procedures [Applies to] ・Important data and systems [Frequency] ・When constructing systems, making changes, regularly (determined according to risk)
			152	Lv2	Disaster prevention and environmental countermeasures are implemented in locations where equipment such as servers are installed	[Rule(s)] ・Measures shall be taken against fires, floods, and power outages ・Temperature and humidity shall be controlled
		Anticipating a security incident, the data necessary for recovery meeting business continuity requirements are prepared.	153	Lv2	For systems that are important for business continuity, data and procedures are prepared that satisfy recovery points and recovery times for each system according to necessity	[Rule(s)] ・Transaction logs and backups that can be used to restore to the required recovery point shall be stored. Procedure manuals shall be prepared that allow for restoration within the required recovery time [Applies to] ・Systems important for business continuity

6. Glossary

No.	Term	Description
1	BYOD	Refers to employees using personal portable devices to perform work. (BYOD: Bring Your Own Device)
2	CASE	An acronym that expresses trends in the automobile industry. Connected: Connecting cars and data to analyze information and provide services Autonomous: Automation that automatically gets drivers and vehicles to their destinations Shared: As in “Ride-sharing” Electric: Electrification aimed at popularizing electric vehicles that are 100% powered by electricity
3	CIO	The person responsible for establishing and implementing IT strategies within a company or organization. Acronym for "Chief Information Officer".
4	CISO	The person responsible for implementing effective security measures within a company or organization. Makes decisions and takes action regarding cyberattacks and security incidents/accidents. Acronym for "Chief Information Security Officer".
5	CS/SU regulations	Regulations regarding Cybersecurity (CS) and Software Updates (SU) being considered for adoption in UN WP29. A revised proposal was released in September 2019 and work is underway for its adoption.
6	CSIRT	A specialized team that investigates and responds to computer security-related incidents and accidents within a company or organization. Acronym for "Computer Security Incident Response Team".
7	DDoS attack	An attack that prevents the provision of regular service by sending a large number of packets from multiple computes to the target web server, etc. Acronym for "Distributed Denial of Service".
8	DMZ	Refers to a segment on a network created between an internal network and an external network, such as the internet. Acronym for "DeMilitarized Zone".
9	HTTPS	A communication standard between a server with a webpage and a terminal (PC, smartphone, etc.) with a browser. An encrypted and secure version of the traditional HTTP. It is entered at the beginning of a web address. Acronym for "Hyper Text Transfer Protocol Secure".
10	IPA	IPA (Information-technology Promotion Agency) is an independent administrative agency in Japan that conducts research/provides information on computer viruses and security.

No.	Term	Description
11	IPS/IDS	Systems that detect and prevent unauthorized access to a network. IPS is an acronym for "Intrusion Prevention System". IDS is an acronym for "Intrusion Detection System". Unlike firewalls, which protect using IP addresses, port numbers, etc., IPS/IDS checks the content of packets, making it effective in preventing attacks such as DoS and Syn floods that cannot be prevented by firewalls.
12	JVN	An organization that provides information and measures for vulnerabilities found in software, etc., used in Japan. Acronym for "Japan Vulnerability Notes".
13	MAC address	A unique identifier for the network adapters of network equipment, computers, and servers applied at the manufacturing stage.
14	OEM	Automobile manufacturers. Acronym for "Original Equipment Manufacturer".
15	OS	Acronym for “Operating System”. Refers to the basic software on which computers run. Examples include Microsoft Windows, Apple macOS, and Linux.
16	SOC	An organization that monitors networks and devices, detects and analyzes cyberattacks, and gives advice on countermeasures. Acronym for "Security Operation Center".
17	TLS	One protocol (communication procedure) for transmitting and receiving encrypted data on TCP/IP networks such as the internet. The successor to SSL. Acronym for "Transport Layer Security".
18	UN WP29	The 29th working party of the World Forum for Harmonization of Vehicle Regulations. As the world’s only organization dedicated to the harmonization of vehicle regulations, it conducts activities such as the study of regulation proposals.
19	VPN	A technology that builds a virtual dedicated line on public internet that allows for the same secure communication as on an intranet. Acronym for "Virtual Private Network".
20	Windows Update	A function that delivers programs to repair Windows vulnerabilities.
21	Access rights	System usage authority settings for system users and user groups. Access rights are used to control access and allow or deny usage based on settings.
22	Variant	Malware created by modifying a portion of a malicious program, worm, etc., that has already appeared.
23	Appliance	Dedicated equipment used for specific functions and applications.

No.	Term	Description
24	Encryption scheme	Encryption is a method of converting information into a form that cannot be understood by third parties. Various encryption schemes for performing such encryption exist, such as WPA, WPA2, and WPA3 in the case of wireless LAN, and encryption schemes that are secure must be selected.
25	External information service	An information service that does not own information equipment within the organization. Such services may be provided online or via other related organizations.
26	Availability	Property of information being accessible to required users when necessary.
27	Integrity	Property of information being complete and accurate.
28	Confidentiality classification	Classifications of confidentiality. Examples include “Top secret” and “Company secret”.
29	Confidential information	Information owned by a company that is not scheduled for external disclosure. Disclosure of such information could result in a loss to the company.
30	Confidentiality	Refers to information that is not to be used or disclosed without permission.
31	Compromised	Being in a state of danger due to some change in circumstances. Example: Decryption technology has evolved due to a dramatic increase in computing power, and so cryptography is compromised.
32	Cloud service	An information service that does not own information equipment within the organization. Services are mainly provided online. (includes some external information services)
33	Cyber/Physical Security Framework	A framework established by Japan’s Ministry of Economy, Trade and Industry (METI) in April 2019 that summarizes the overall picture of security measures required for industry.
34	Cyber intelligence	Efforts taken to respond to advanced cyberattacks, such as "analyzing and understanding the intent and ability of an attacker," "predicting potential threats to the organization," and "evaluating the probability of predictions and taking appropriate measures."
35	Cybersecurity risk	The risk of cyberattacks causing problems such as leakage or unauthorized modification of electronic data or the risk of IT systems and control systems not fulfilling their intended functions, etc.
36	Supply chain	In general, a series of processes starting with the procurement of raw materials/parts for products and including manufacturing, inventory control, delivery, sales, and consumption.
37	IT equipment/device	Equipment and devices used for processing and transmitting information. Includes computers, servers, smartphones and their peripheral devices.

No.	Term	Description
38	Information asset	Important information owned by a company that is to be protected and the equipment/devices used to handle such important information. Examples: Information assets (information): Confidential information, personal information, etc. Information assets (equipment/devices): Servers, computers, network equipment, OS, software, etc.
39	Information security incident/accident	Refers to when vulnerabilities inherent in information assets have been exploited and manifested by various threats facing information assets.
40	Initial response	The first actions or operations performed when an information security incident/accident occurs.
41	Snapshot	Extracted source code, files, directories, database files, etc., from a particular point in time.
42	Spyware	Malware that collects and automatically sends information about the user in an unintended manner.
43	Control system	An information system used for controlling industrial processes such as manufacturing, product sales, production and sales. Control systems include supervisory control and data acquisition systems (SCADA) used to manage geographically dispersed assets, distributed control systems(DCS), and systems that perform control using local programmable logic controllers (PLC) that are smaller in scale than both SCADA and DCS systems.
44	Vulnerability	Information security flaws that occur due to program defects or design errors.
45	Security patch	Programs that resolve defects caused by problems and vulnerabilities found in software.
46	Security policy	The intention and orient for organizational security as officially expressed by top management and the regulations established by the organization for implementing security measures based on that intention and orient.
47	Software	Programs used to operate information systems. These often refer to applications used for performing certain tasks.
48	Deep learning	One of the machine learning technologies used in artificial intelligence. Refers to technology that allows a computer to automatically discover desired features from large amounts of data, without human intervention.
49	Daemon	Of the programs that run on Unix-based operating systems such as UNIX, Linux, and Mac OS X, refers primarily to those programs that run in the background.

No.	Term	Description
50	Transaction data log	A sequential record of changes made to a database kept in order for the database management system, etc., to maintain consistency with multiple related processes. It is used for rollback processing and to restore from backups in the event of a failure.
51	Authentication	The use of methods to ensure that the identity of an entity is as claimed.
52	Hash value	A fixed-length value obtained from the underlying data by a fixed calculation procedure. One of its characteristics is that the same value can always be obtained from the same data with a constant length regardless of the length of the original data. Due to that characteristic, it can be used as a short code representing the characteristics of the original data.
53	Packet filtering	A filtering method that performs checks based on specific rules to ensure correct communication, potentially by checking the consistency of the context of the communication sessions. Packets determined to be invalid are discarded.
54	Targeted email training	Training aimed at improving the ability to detect attacks and raising the security awareness of an organization by sending mock attack emails targeting specific companies and having them learn through these mock attacks.
55	Firmware	Software for controlling hardware in electronic devices such as computers.
56	Restore	The act of returning data to its normal operating state using backup data when a failure occurs.
57	Behavior detection	A method for detecting malware from the behavior and characteristics of a program, instead of from conventional detection using pattern files.
58	Black list	A method of designating and defining dangerous targets, then preventing attacks from those targets.
59	Malware	A generic name for malicious software and code created with the intention of dishonest and harmful operation. Includes computer viruses, worms, spyware, etc.
60	Wireless LAN	Networks established using wireless technology instead of physical cables. Also referred to as “Wi-Fi”.
61	Ransomware	A compound word combining "Ransom" and "Software," malware that exploits software and demands a ransom for data.

Afterword

In recent years, the number of cyberattacks targeting not only corporate IT environments but also supply chains is increasing, and the cybersecurity risks facing the automobile industry are becoming more serious.

In order for the automobile industry to realize a mobility society that is safe, secure, and prosperous while achieving sustainable development in such an environment, it is essential for the entire industry to gain an accurate understanding of the cybersecurity risks it faces and take appropriate and continuous measures against those ever-increasing risks.

For this reason, the Japan Automobile Manufacturers Association (JAMA) and Japan Auto Parts Industries Association (JAPIA) have jointly formulated these security guidelines—which take the unique cybersecurity risks faced by automobile manufacturers and companies that make up supply chains in the automobile industry into consideration—to clarify a framework for cybersecurity measures and industry-wide self-assessment criteria aimed at enhancing cybersecurity measures throughout the entire automobile industry while promoting efficient inspections of cybersecurity levels.

These guidelines are expected to assist in enhancing cybersecurity measures throughout the entire automobile industry.

Contributing Committee Members (shown in alphabetical order of company name)

Japan Automobile Manufacturers Association
General Policy Committee / ICT Subcommittee / Cyber Security Subcommittee / CS Guidelines Study Taskforce

Role	Company Name	Name
Leader	Toyota Motor Corporation	Toshiya Ban
Sub-Leader	Nissan Motor Corporation	Shuntaro Torii
Sub-Leader	Honda Motor Co., Ltd.	Atsushi Kubo
Committee Member	Suzuki Motor Corporation	Hideaki Suzuki
Committee Member	Subaru Corporation	Hidemasa Ito
Committee Member	Daihatsu Motor Co., Ltd.	Nobuyuki Sakata
Committee Member	Toyota Systems Corporation	Noboru Taniguchi
Committee Member	Honda Motor Co., Ltd.	Akitoshi Honda
Committee Member	Mazda Motor Corporation	Kazuhiro Kikuchi
Committee Member	Mitsubishi Motors Corporation	Kenji Taki

Japan Auto Parts Industries Association
IT Committee / Cyber Security Subcommittee

Role	Company Name	Name
Subcommittee Chair	DENSO Corporation	Shunjiro Goto
Deputy Subcommittee Chair	Hitachi Astemo, Ltd.	Takayuki Nakao
Deputy Subcommittee Chair	Marelli Corporation	Kenichi Suzuki
Committee Member	Aisan Industry Co., Ltd.	Kenji Niina
Committee Member	Aisin Corporation	Hiroyuki Onishi
Committee Member	Aisin Corporation	Masataka Rokujo
Committee Member	ALPS ALPINE Co., Ltd.	Hiroyuki Ando
Committee Member	NOK Corporation	Tsubasa Motozawa
Committee Member	NOK Corporation	Toshiyuki Nagasawa
Committee Member	KYB Corporation	Hidetomo Sugo
Committee Member	Koito Manufacturing Co., Ltd.	Yasushi Noyori
Committee Member	JTEKT Corporation	Takashi Hikosaka
Committee Member	Stanley Electric Co., Ltd.	Tomoaki Tanaka
Committee Member	DENSO Corporation	Koji Hara
Committee Member	Tokairika Co., Ltd.	Naoki Masuda
Committee Member	Toyoda Gosei Co., Ltd.	Yukiyoshi Matsui
Committee Member	Toyota Boshoku Corporation	Mitsuhiro Osako

Committee Member	Transtron Inc.	Yuji Sho
Committee Member	NGK Spark Plug Co., Ltd.	Hiroaki Kato
Committee Member	NGK Spark Plug Co., Ltd.	Hiromitsu Yamashita
Committee Member	NHK Spring Co., Ltd.	Koji Suzuki
Committee Member	Hitachi Astemo, Ltd.	Naruki Toshima
Committee Member	Mitsuba Corporation	Yusuke Irie
Committee Member	Yazaki Corporation	Katsunori Uematsu

Contact address: Vehicle Safety and Environmental Division, Japan Automobile Manufacturers Association, Inc. (JAMA)

Jidosha Kaikan, 1-30, Shiba Daimon 1-chome, Minato-ku, Tokyo 105-0012 Japan

TEL:03-5405-6125 FAX:03-5405-6136