# FY 2026 Briefing Session for Senior Management and Personnel

## Request for Self-Evaluation and Implementation of the Automotive Industry Cybersecurity Guidelines


Japan Automobile Manufacturers Association, Inc.

ICT Subcommittee
General Policy Committee

Procurement Subcommittee
Supply Chain Committee

Japan Auto Parts Industries Association

Cyber Security Subcommittee
DX Management Committee

Supply Chain Subcommittee
Organizational Affairs Committee


September, October 2026

# Today's Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# Today's Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# 1-1. Today's Briefing Session

- ✓ Today's session is intended to provide an overview of the growing global trend of security incident damage, and to make the following two requests.
  1. **Use the "Automotive Industry Cybersecurity Guidelines" to assess and enhance the security level of your organization.**
  2. **Include suppliers in the process in order to enhance security across the entire supply chain.**

- ✓ Using actual damage case studies, this session will help participants understand the importance of improving security levels across the entire supply chain **while deepening the knowledge of security measures among senior management and personnel**. The **submission method for self-evaluation results** using the Automotive Industry Cybersecurity Guidelines will also be explained.

- ✓ This session will also include a case study of a **cyberattack on a small or medium-sized enterprise**, presented as special content*. *This special content is available exclusively to attendees of this briefing session.

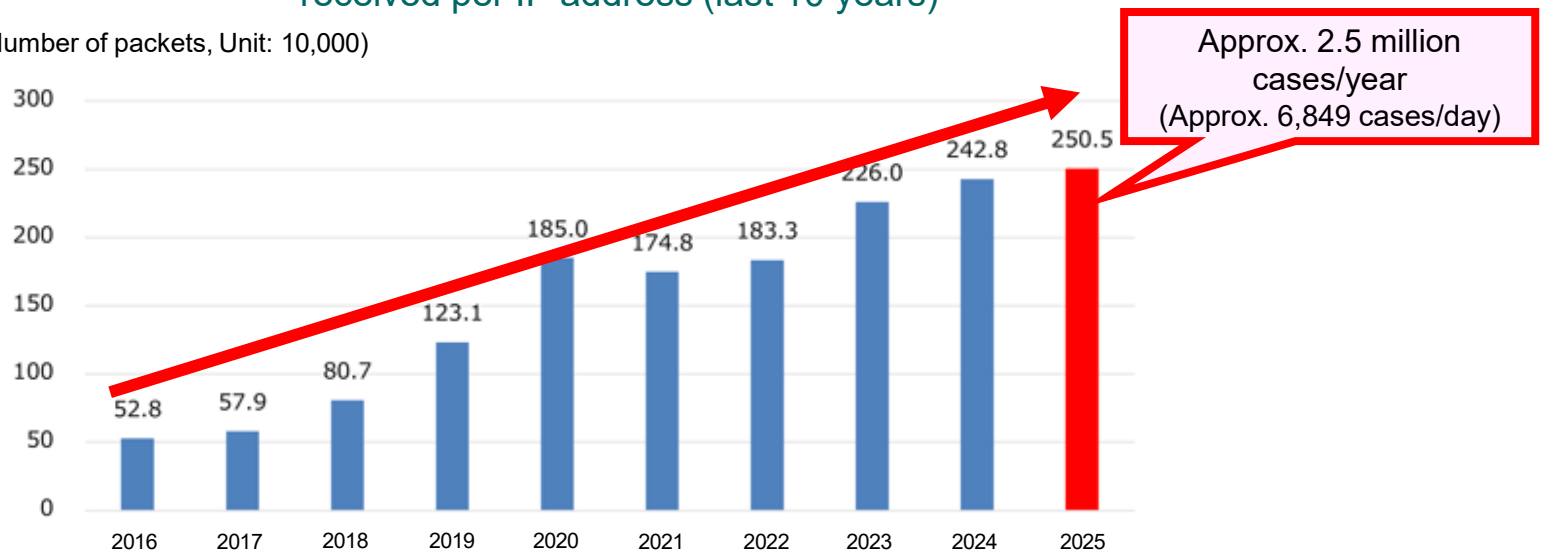
- ✓ We sincerely hope this briefing will provide valuable insights for all participating organizations.

# 1-2. Global Situation

Every device connected to the internet faces about **7,000 cyberattacks daily**. These **attacks are becoming increasingly complex and sophisticated each year, with further escalation expected**.
In addition, **by industry, manufacturing continues to account for the largest share of damage**, representing 40% of all cases and **making it the most targeted industry overall**.
**Cybersecurity is a critical issue for all organizations,** making it **essential to adopt a proactive approach to threats, viewing them as urgent and personal.**

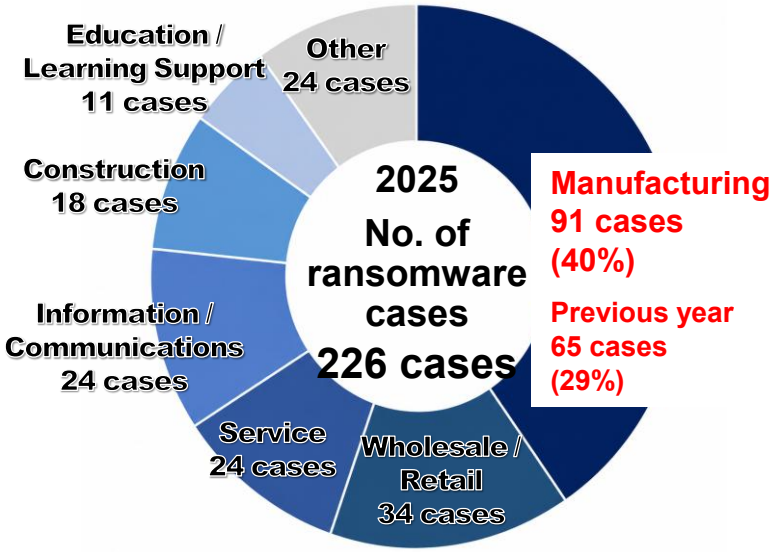
Annual number of cyberattack related communications received per IP address (last 10 years)

(Number of packets, Unit: 10,000)




Source: National Institute of Information and Communications Technology (NICTER) Observation Report 2025

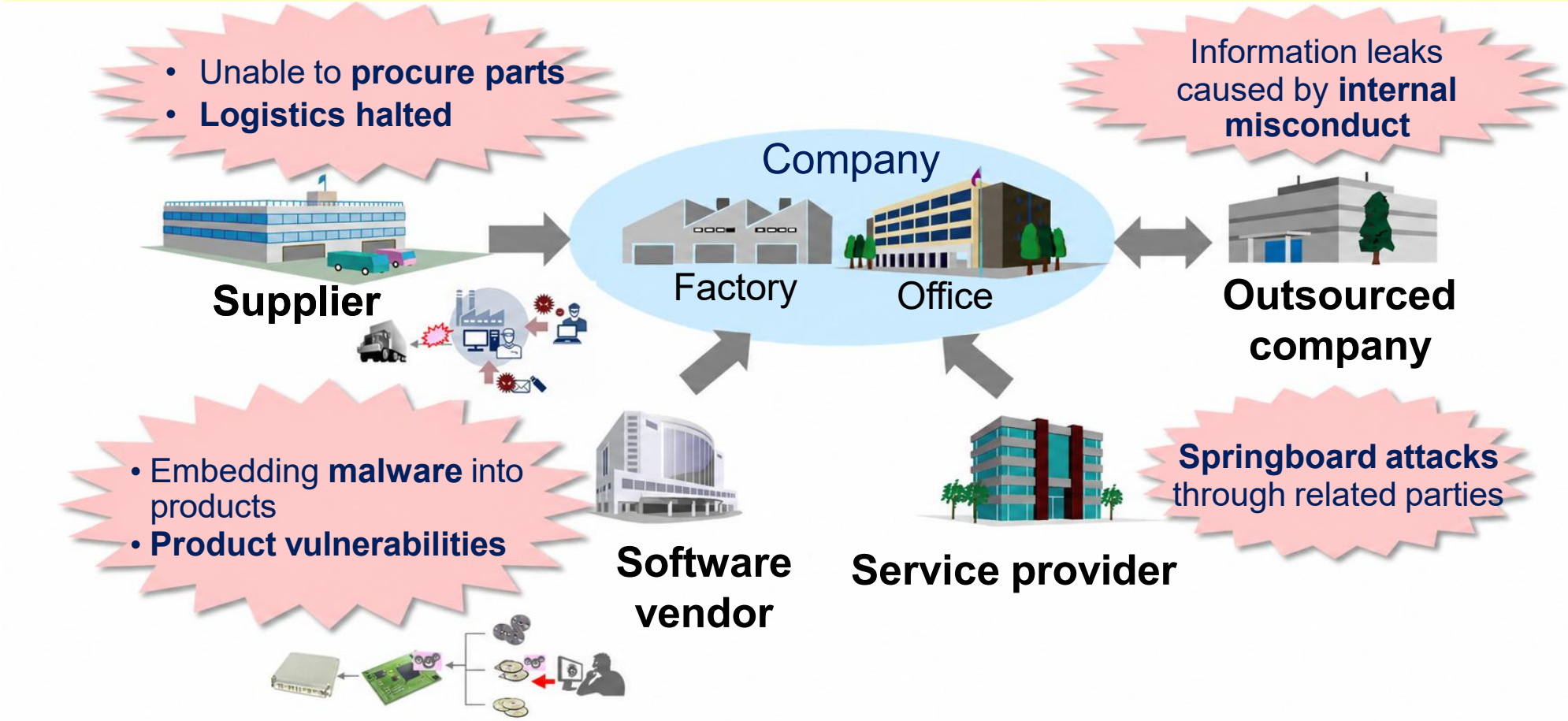
Number of reports by industry




Source: “Situation of Threats in Cyberspace in 2025”, National Police Agency

# 1-3. Security Risks in the Supply Chain

As the industry continues to evolve and the amount of data grows, **protecting just one's own organization is no longer enough**.
**Attackers consistently exploit weaknesses within the supply chain, highlighting the need for thorough risk management across the entire supply chain.**



# 1-4. Security Promotion Activities in the Automotive Industry Supply Chain

**Activities undertaken by the automobile industry are guided by the country's overall policy.**
**Industry-standard guidelines are set** to enhance security across the industry.
We are collaborating with relevant companies in the industry to improve security levels.

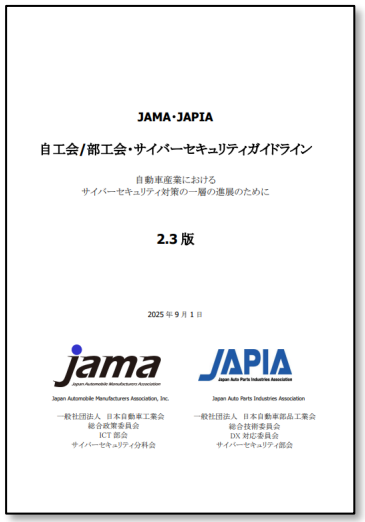
**[Standard Model]**

**Ministry of Economy, Trade and Industry: Cyber Physical Security Framework (CPSF)**

Industry-by-industry review

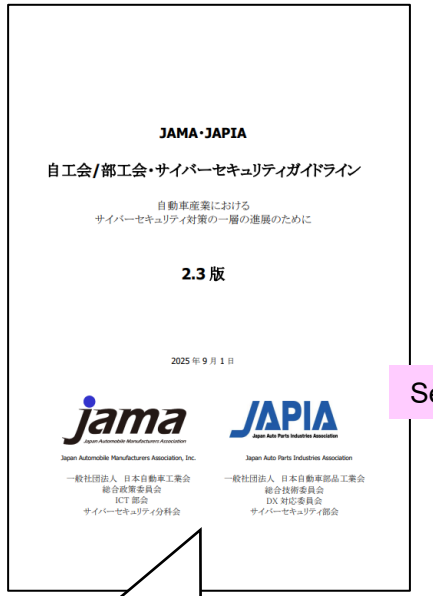
- **Building industry** (elevator, energy management system)
- **Electricity industry**
- **Defense industry**
- **Automotive industry**
- **Smart home industry**
- **Other connected industries**

Formulation of security guidelines for the supply chain


JAMA・JAPIA
自工会/部工会・サイバーセキュリティガイドライン
自動車産業における
サイバーセキュリティ対策の一層の進展のために
2.3 版
2025 年 9 月 1 日

# 1-5. Specific Activities

In FY 2019, **JAMA and JAPIA collaboratively established industry standard cybersecurity guidelines** in alignment with the METI's CPSF.
Beginning in March 2021, **the automotive industry has been requested to conduct self-evaluations and enhance its cybersecurity levels**.
→ Companies will use these self-evaluation results to **identify priority areas and take steps to enhance their security levels**.




JAMA and JAPIA have **jointly developed security guidelines for the automotive industry**

Automobile manufacturer

Self-evaluation request
+
Request for deployment to business partners of each company

Tier 1 Supplier

Self-evaluation request
+
Request for deployment to business partners of each company

Tier 2 Supplier

Self-evaluation results
Submit

Self-evaluation results
Submit

Self-evaluation results
Submit

+

Compile / Publish

Industry average

Results announcement website

**Requests for deployment to each company in the supply chain**; JAMA collects industry-wide evaluation

Companies **identify priority issues by comparing industry averages** with their **self-evaluation results**

[Support Activities]

- Explanatory guide
- Seminars for senior management and personnel
- Inquiry support (Via chatbot, etc.)
- How-to guide
  Security measures for SMEs
  Guide to enhancing security

# Future Outlook

## — SCS Evaluation System —

# 1-6-1. Outline of the SCS Evaluation System (taken from METI materials)

**Problem**

| | |
|---|---|
| METI's Understanding of the Issue | 1) Customers: It is difficult to judge to what degree suppliers have implemented countermeasures<br>2) Suppliers: It is difficult to respond to varying levels of countermeasures required by different customers |

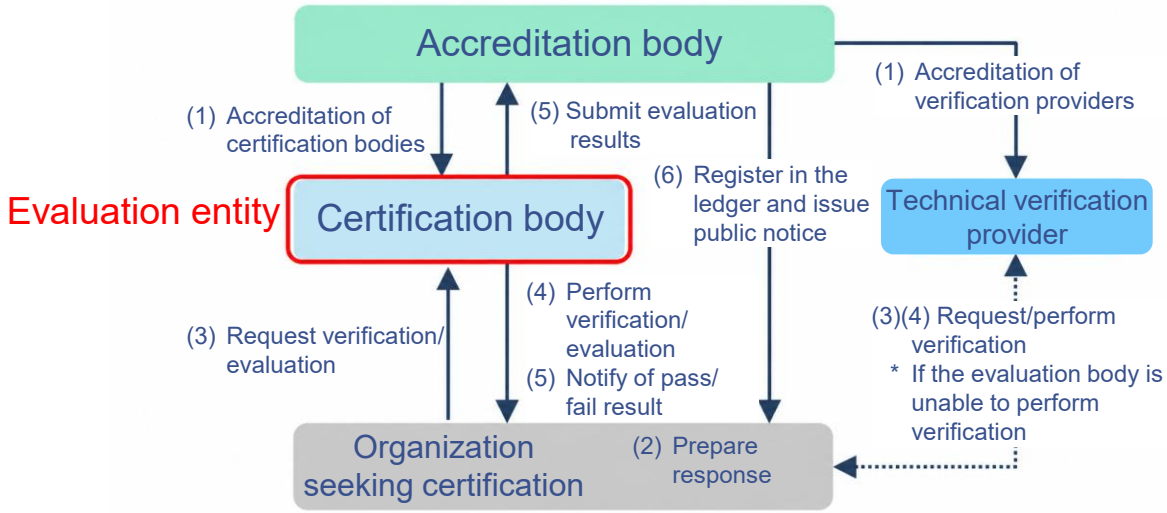
**Measure**

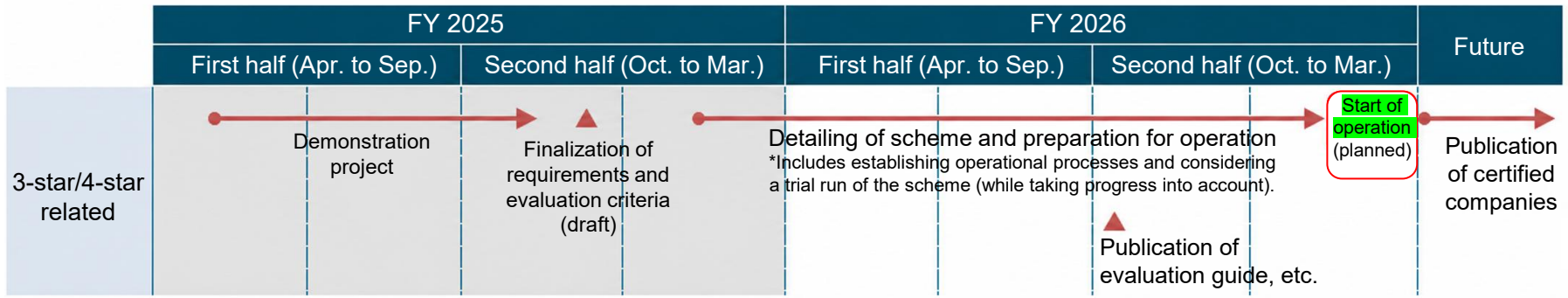
Establish a national evaluation scheme that clearly rates the status of countermeasures using common criteria (3-star, 4-star, 5-star)

(Note: This scheme is not a legal requirement. Participation is entirely voluntary for each company.)

- The 3-star and 4-star tiers are scheduled to come into use around the end of FY2026.
- Criteria and scheme details for the 5-star tier will be considered from FY2026 onward.

## 4-star Evaluation Scheme



# 1-6-2. Response Policy for the SCS Evaluation System (JAMA/JAPIA)

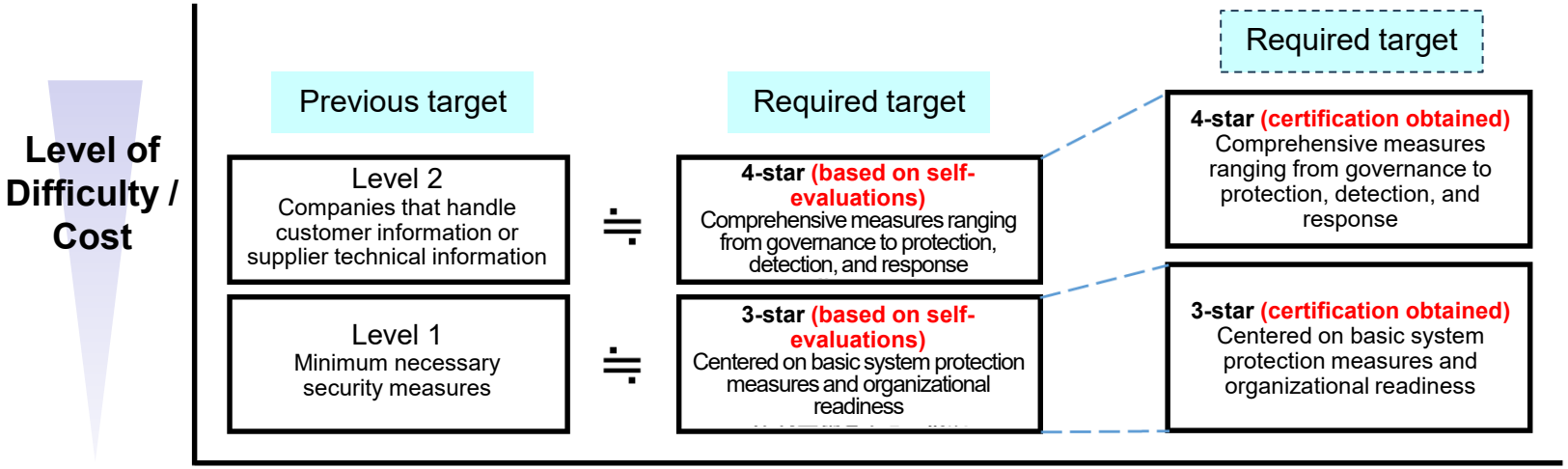
Below is an overview of how JAMA and JAPIA have organized their response policy for the SCS Evaluation System.

- **Vision for the Automotive Industry**

  Ultimately, we believe the industry should consolidate under the new national system (while avoiding any double standards).

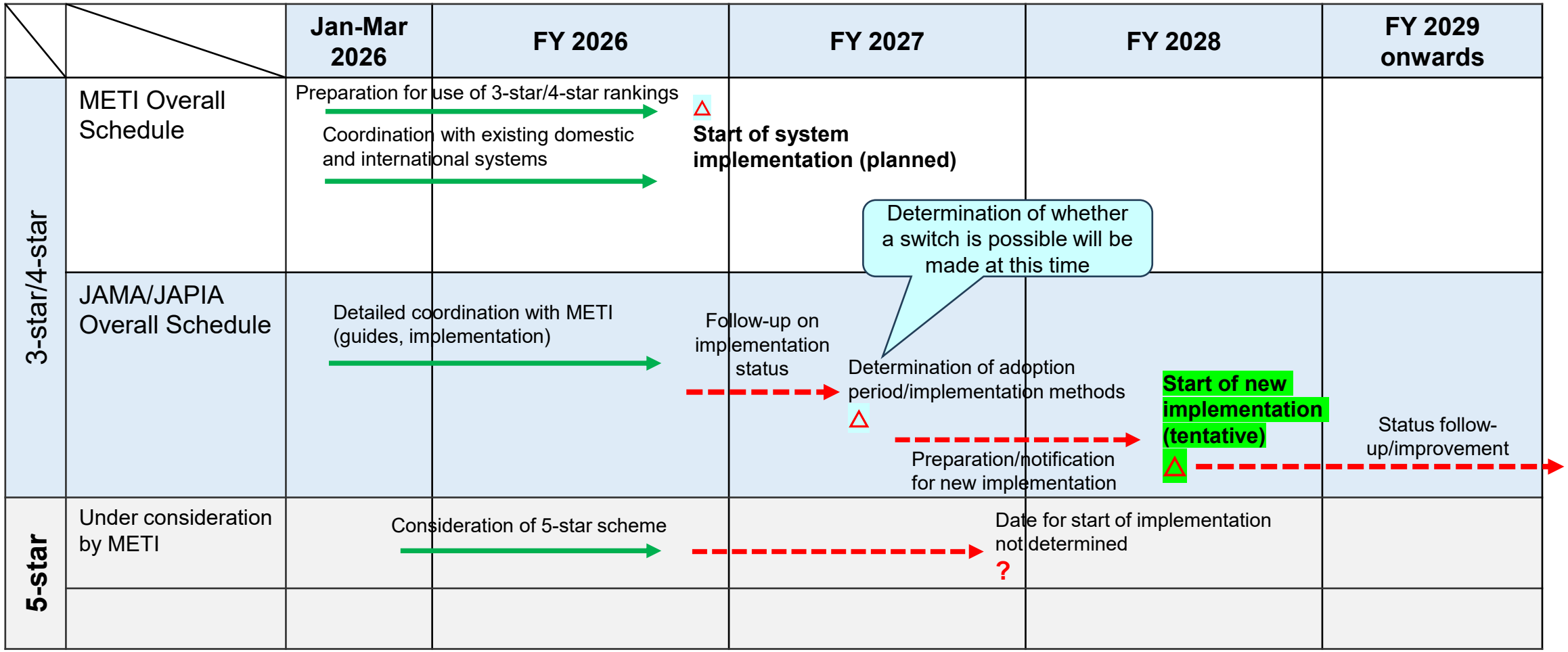
- **How the Automotive Industry Will Use the New System**

  1) The only guidelines companies will need to follow will be those for the new system (switch from the Automotive Industry Guide to the guide for the new system).
  2) As before, each company will be asked to conduct a self-evaluation and submit their results based on the guide for the new system. JAMA will continue to compile and analyze self-evaluation results and publish those results, as it has done previously.
  3) Obtaining 3-star or 4-star certification will not be mandatory, but will be at each company's discretion.



# 1-6-3. Overall Schedule for Transitioning to the New System (Draft)
*Still under consideration

Current transition plan draft (including an outline of interim checkpoints)



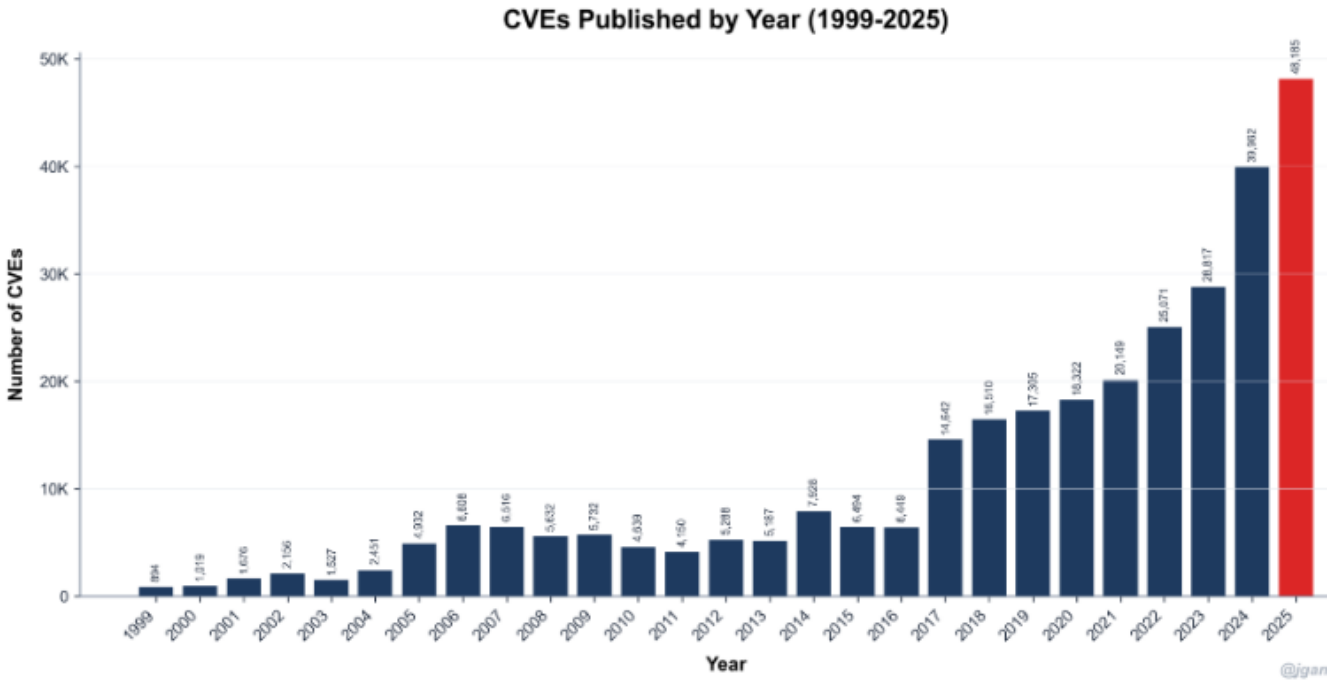
# Urgent Issue

## — Responding to High-Performance AI —

# 1-7-1. Threat Awareness: Growing Threats from High-Performance AI

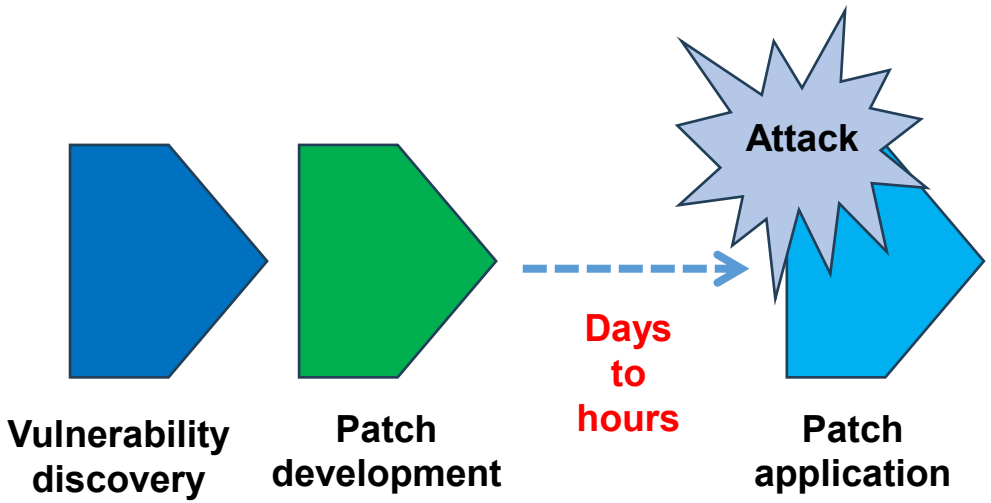
High-performance AI excels at discovering vulnerabilities and generating sophisticated attack codes, and as it continues to advance, it raises the risk that conventional assumptions will be fundamentally upended.

- **Number of vulnerabilities: Total number of vulnerabilities discovered thus far**
  **⇒ Already discovered in large numbers, with sharp increases expected**




- **Timeline: This enormous volume must now be addressed in an extremely short period**

**(Lead time until attack)**
**Until now: Weeks to months**
**From now: Hours to days**




Source: 2025CVEBlog/blog_final.md at main/jgamblin/2025CVEBlog/GitHub

# 1-7-2. Preparing for Growing Threats from High-Performance AI

- With rapid advances in AI technology, its use in cyberattacks is dramatically accelerating attack speed and expanding attack scale, resulting in increased threats to cybersecurity.
- In particular, so-called “high-performance AI” is expected to rapidly improve cybersecurity capabilities such as vulnerability discovery and remediation, meaning the automotive industry must also take action in response.

🔷**We first request that prompt action be taken on the items below (see the "Urgent Message" posted on the JAMA website):**

**1) Respond promptly to discovered vulnerabilities**

Proactively gather vulnerability-related information, set priority levels for discovered vulnerabilities based on their business criticality and severity of associated risk, and respond promptly in accordance with those priorities. (In particular, patches should be applied to externally facing systems as the top priority.)

**2) Ensure that response efforts are led from the top of the organization**

Cybersecurity risks should be recognized as management risks, with the necessary resources being secured and the response carried out under the leadership of executive management.
(Specific examples: Securing the framework, man-hours, and budget needed to respond to vulnerabilities; developing a BCP in case of intrusion)

# Today’s Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# Incident Summary

ASKUL Corporation, a major B2B e-commerce company, suffered a cyberattack in October 2025, suspending its e-commerce site and logistics operations. **Recovery took approximately 4 months**, and **roughly 740,000 customer records were leaked.**

**By using resources such as JAMA/JAPIA guidelines to check security requirements, companies can identify weak points while understanding their risks, enabling them to then take countermeasures against those risks.**
**Cyberattacks are no longer a matter of "if", but of "when".**

**The first step toward preparedness is treating cyberattacks as a personal risk**

# About ASKUL Corporation

| | |
|---|---|
| **Company name** | ASKUL Corporation |
| **Main businesses** | E-commerce business: Mail-order services for office supplies, daily necessities, and other products<br>• B2B e-commerce sites: ASKUL and SOLOEL ARENA<br>• B2C e-commerce site: LOHACO |
| **Details** | • Offers products ranging from specialized items for the manufacturing and construction industries to medical supplies.<br>• **Most logistics-related operations have been automated.** |
| **Supply chain** | ASKUL LOGIST, a subsidiary, **has been contracted by the brands Muji and LOFT to handle logistics operations for their official e-commerce sites** |

**ASKUL is a core supply chain company responsible for the logistics of business supplies and other goods**

# Case Study Overview

Ransomware infection **stopped the company's systems**, with damage ultimately extending to a **full suspension of business**

## Impact on systems

- ✓ **Encryption of logistics and internal systems**
- ✓ **Encryption of backup files**
- ✓ **Compromised external cloud service accounts (inquiry management system)**

## Impact on business

- ✓ **Suspension of order receipt and shipping for ASKUL, SOLOEL ARENA, and LOHACO**
- ✓ **Suspension of automated warehouse equipment and picking systems**
- ✓ **Full suspension of shipping operations at multiple logistics centers**

**Furthermore, the impact of order and shipping suspensions extended to the supply chain**

**e.g., Ryohin Keikaku Co., Ltd., LOFT Co., Ltd.**

# Impact on Management

The business suspension also had a major impact on financial results:

| Extraordinary loss (Q2) | Operating loss (Q2) | Personal information leak |
|---|---|---|
| **5.22 billion yen** | **▲2.995 billion yen** | **Approx. 740,000 records** |
| **System failure response costs Logistics infrastructure maintenance, investigation, and recovery, etc.** | **Monthly sales during peak month Down ▲95.1% YOY** | **Including approximately 15,000 business-partner records** |

**Cyberattack countermeasures are a management issue that determines business continuity and corporate value**

# Timeline

| | |
|---|---|
| **June 5, 2025** | Initial intrusion from outside the company, exploiting an account issued to an outsourcing contractor |
| **October 19, 2025** | **Ransomware activated**, files encrypted, deleted, and leaked.<br>**Order receipt and shipping operations for ASKUL and other services suspended.** |
| **October 20, 2025** | Requested support from external specialist organizations. Started detailed investigation. |
| **October 29, 2025** | **Order acceptance via manual operation using fax**<br>(Limited to specific locations and items) |
| **November 12, 2025** | **Order acceptance resumed on some websites**, including ASKUL.<br>Shipping locations and order scope gradually expanded. |
| **February 13, 2026** | Key e-commerce service functions **restored to pre-incident levels** |

# Initial Response Timeline

The initial response focused on **network isolation and password changes**, and was carried out swiftly.

| | |
|---|---|
| **Morning of October 19, 2025** | **Ransomware activated**, files encrypted, deleted, and leaked |
| **October 19, 2025** | **Isolation of suspected infected systems and physical disconnection of networks.**<br>Began changing all passwords. |
| **October 19, 2025 at around 2 PM** | Set up a response headquarters within the head office |
| **October 19, 2025 at around 4:30 PM** | **Order receipt and shipping operations for ASKUL and other services suspended** |
| **October 20, 2025** | Requested support from external specialist organizations. Started detailed investigation.<br>Checked for unintended data changes, program releases, and timestamp anomalies. |
| **October 22, 2025** | **Unauthorized access to an external cloud service occurred** |
| **October 23, 2025** | Completed password changes for key external cloud services |
| **October 24, 2025** | **Applied multi-factor authentication to administrator accounts**, changed passwords for key accounts, and updated EDR signatures |

# Key Points of This Case – What Went Wrong

The problems behind ASKUL's cyberattack damage are as follows:

**Initial intrusion**

**Misuse of contractor account**

**Detection**

**Damage went unnoticed for 4 months after intrusion**

**Recovery**

**It took 4 months from damage discovery until recovery**

**Why did the cyberattack on ASKUL occur, and how did it result in such extensive damage?**

# (1) Initial Intrusion – How did the intrusion occur?

The point of entry **was the leaked ID and password of an administrator account issued to a contractor, which was then misused.**

## Problem #1

- ✓ **Although multi-factor authentication was generally implemented, this particular account was an exception where it had not been set up.**

## Results

- ✓ **Anyone who knew the ID and password could access the system as a legitimate user.**
- ✓ **The attacker had already succeeded in breaching the internal network as of June 2025.**

**Because management was not unified, the point where oversight was weakest became the point of entry**

# (2) Detection – Why wasn't the intrusion noticed?

After the intrusion, the attacker **spent approximately 4 months gaining access privileges across the entire** internal network.

## Problem #2

- ✓ **EDR (threat detection software) had not been installed on the servers at the data center where the breach occurred.**
- ✓ **Mechanisms for automatically detecting suspicious activity were insufficient.**

## Results

- ✓ **The attacker's presence and activities went undetected for almost 4 months.**
- ✓ **The damage went unnoticed until the ransomware was executed and the system was encrypted.**

**Servers without EDR installed became a monitoring blind spot, allowing the attacker to remain undetected**

# (3) Recovery – Why Did It Take So Long?

It took **almost four months** for e-commerce services to recover to pre-incident levels.

## Problem #3

- ✓ **Backup data existed, but part of it was stored online (connected to the network).**
- ✓ **Logs on affected devices were erased during an OS update, leaving no logs from the time of the breach.**

## Results

- ✓ **The attacker gained control of and encrypted backup files before executing the ransomware.**
- ✓ **Identifying the intrusion route and scope of damage was difficult.**
- ✓ **A system rebuild (clean reinstall) was carried out as an unavoidable measure.**
- ✓ **It took almost four months for e-commerce services to recover.**

**No business continuity preparations had been made in anticipation of a cyberattack**

# Problems and Required Actions in This Case Study #1

| Phase | Problems | Examples of actions required | Example JAMA/JAPIA Cybersecurity Guidelines |
|---|---|---|---|
| **(1) Initial intrusion** | **Multi-factor authentication had not been implemented for the contractor account**.<br>* Anyone who knew the ID and password could log in as a legitimate user. | **Implement multi-factor authentication** for internet-accessible systems and systems storing critical data, and verify configuration statuses (cloud services, VPNs, etc.). | **18 Authentication/Approval, No. 120**<br>"Multi-factor authentication is implemented for systems that can be used from the internet" |
| | | **Check the status** of security measures **at key contractors.**<br>***Supply chain management/measures** | **8 Information security requirements between companies, No. 42**<br>"Have a grasp of the **status of security measures of business partners** that handle important confidential information" |
| **(2) Detection** | **No mechanism to detect suspicious activity, such as EDR, had been implemented** on the servers. | **Implement an activity tracking system, such as EDR**, on PCs and servers.<br><br>After implementation, **regularly check EDR installation status and keep the version up to date.** | **22 Malware Countermeasures, No. 138**<br>"A **behavior tracking system has been introduced** that allows for the **acquisition of detailed histories** at endpoints and remote response after malware infection" |

# Problems and Required Actions in This Case Study #2

| Phase | Problems | Examples of actions required | Example JAMA/JAPIA Cybersecurity Guidelines |
|---|---|---|---|
| **(3) Recovery status** | No measures had been taken, **such as storing backup files in an environment isolated from the network**.<br><br>**Logs were not securely managed,** such as by being stored in an isolated environment. | **Perform backups in preparation for cyberattacks** (e.g., the 3-2-1-1 rule, immutable backups).<br><br>**Store on a dedicated log collection server or similar system** and **control access** to that server. | **24 Backup/Restore, No. 148**<br>“Backups are performed at **appropriate times**”<br>*e.g., by storing backups offline<br><br>**9 Access rights, No. 53**<br>“Access logs **are securely stored and managed in an access-controlled state**” |

**Has your company implemented these measures?**

# Cyberattack Demo

Let’s see how easily an attacker can gain access and carry out an attack without prior preparedness or countermeasures in place...

# Summary

1. Recognize **cyberattack countermeasures** as a **management issue** that determines business continuity and corporate value.
2. Use the **JAMA/JAPIA Guidelines** and other resources to reliably perform **risk assessments** and **implement risk countermeasures**.
3. Realize that **preparing for cyberattacks in advance** is essential to preventing intrusion and the spread of damage.

**Cyberattacks are no longer a matter of "if", but of "when"**

**The first step toward preparedness is treating cyberattacks as a personal risk**

# In conclusion: Actions to be taken immediately

**1. First, know where your company currently stands**

Using the JAMA/JAPIA guidelines and other resources to check the status of countermeasures is the first step.

**2. Secure resources for any countermeasures that are lacking**

Countermeasures only move forward once senior management gets involved and secures the personnel, budget, and structure needed.

**3. Continuously review cybersecurity as a management issue**

This is not a one-time effort. Continue regularly reviewing the check sheet and making improvements.

**Please take that first step, whether it be today or tomorrow**

# Appendix — Reference Literature & List of Terms

# Sources

ASKUL Corporation, “Report on Investigation Results of the Ransomware Attack's Impact and Initiatives to Strengthen Safety (System Outage Due to Ransomware Attack – 13th Report)”

https://pdf.irpocket.com/C0032/PDLX/O3bg/N4O3.pdf

(Last accessed on July 22, 2026)

ASKUL Corporation, “Consolidated Financial Results for the Second Quarter (Interim Period) of the Fiscal Year Ending May 2026 [Japanese GAAP]”

https://pdf.irpocket.com/C2678/ikpa/wnGE/HEKP.pdf

(Last accessed on July 22, 2026)

# List of Terms

| Term | Definition |
|---|---|
| Ransomware | Malware (malicious software) that encrypts systems or files and demands payment in exchange for restoring them. Once infected, data becomes inaccessible, creating a risk of a complete suspension of business. |
| Multi-factor authentication (MFA) | A mechanism that verifies identity at login using multiple factors in addition to a password, such as a smartphone notification or biometric authentication. Even if an ID and password are leaked, unauthorized login becomes much more difficult. |
| EDR (Endpoint Detection and Response) | Security software that detects and logs suspicious activity on PCs and servers in real time and supports early detection of and response to cyberattacks. |
| Backup | Storing copies of data on a separate device or medium in preparation for data loss or destruction.<br>Storing backups in an environment isolated from the network (e.g., an external HDD or dedicated storage) can help prevent encryption damage caused by ransomware. |

# Today's Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# 3-1. Analysis of Self Evaluation Results for FY 2025

- ✓ In FY2025, 4,032 companies conducted a self-evaluation (an increase of 898 companies YOY).
  *This is the highest number of participating companies to date.
- ✓ Average scores for all Level 1 through Level 3 items showed improvement compared to FY 2024.

| Fiscal year | Total number of valid responses | Average score |
|---|---|---|
| 2025 | **4,032 companies** | **Level 1 item: 83.13** / 100 points **(83.1%)**<br>**Level 2 item: 126.14** / 148 points **(85.2%)**<br>**Level 3 item: 41.24** / 58 points **(71.1%)** |
| 2024 | **3,134 companies** | **Level 1 item: 82.80** / 100 points **(82.8%)**<br>**Level 2 item: 123.47** / 148 points **(83.4%)**<br>**Level 3 item: 39.34** / 58 points **(67.8%)** |
| 2023 | **3,240 companies** | **Level 1 item: 81.84** / 100 points **(81.8%)**<br>**Level 2 item: 120.00** / 148 points **(81.1%)**<br>**Level 3 item: 42.91** / 58 points **(74.0%)** |

FY 2025 Average Score Details

| Target level | No. of companies | Average score | | | |
|---|---|---|---|---|---|
| | | Level 1 item | Level 2 item | Level 3 item | Total |
| Level 1 | **989 companies** | **63.32** / 100 points **(63.3%)** | - | - | **63.32** / 100 points **(63.3%)** |
| Level 2 | **1,704 companies** | **87.25** / 100 points **(87.3%)** | **121.20** / 148 points **(81.9%)** | - | **208.45** / 248 points **(84.1%)** |
| Level 3 | **1,339 companies** | **92.52** / 100 points **(92.5%)** | **132.43** / 148 points **(89.5%)** | **41.24** / 58 points **(71.1%)** | **266.18** / 306 points **(87.0%)** |
| | Total | **83.13** / 100 points **(83.1%)** | **126.14** / 148 points **(85.2%)** | **41.24** / 58 points **(71.1%)** | - |

# 3-2. Requests for FY 2026

- ✓ In order to consistently monitor your progress, we request that you conduct a self-evaluation similar to the one completed in FY 2025.
  **Submission deadline: December 31, 2026**
- ✓ We request that this initiative be extended to a broader range of suppliers, thereby fostering its growth throughout the automotive industry.

**1) Self-evaluation by companies and submission of results to JAMA**

**2) Request to business partners**
***Self-evaluation and submission of results to JAMA**

# 3-3. Achievement Level and Timeline Expected by JAMA and JAPIA

**Targets for FY 2026**

The automotive industry has moved towards its target of achieving Levels 1 and 2 by the end of FY 2025.
In FY 2026, we request that targets be aimed for:

✓**Companies that have already achieved Levels 1 or 2 ➞ Maintain and improve the status quo**

* Automobile manufacturers, leading Tier 1 companies, and organizations with advanced technology and expertise are encouraged to strive for Level 3.

✓**Companies that have not achieved Levels 1 or 2 ➡ Achieve Level 1 or 2 in FY 2026**

* While this may pose some challenges, we kindly ask that you meet all Level 1 requirements by the end of FY 2026 and work to fulfill Level 2 requirements to the best of your ability.

[Security Level Definitions in the Automotive Industry Cybersecurity Guidelines]

| | |
|---|---|
| Lv. 3 | **Exemplary level (implementation of best practices)** |
| Lv. 2 | **Requirements for companies handling customer information and supplier technical information** |
| Lv. 1 | **Minimum necessary security measures**, regardless of the scale or type of information handled |

# 3-4. Self-Evaluation and Report Submission Guidelines

Please assess your security posture according to the FY 2026 Automotive Industry Cybersecurity Guidelines and submit your report based on the following guidelines.

| Item | | Description |
|---|---|---|
| 1 | JAMA check sheet for self-evaluations | • The details of checks to be performed are the same as for FY 2025.<br>• **Please obtain and use Checklist V2.3 from the following site on the JAMA website:** Automotive Industry Cybersecurity Guidelines \| JAMA Japan Automobile Manufacturers Association |
| 2 | Submission deadline | • **Please submit by December 31, 2026.** |
| 3 | Submission methods (JAMA/requester) | • Before proceeding, please confirm the submission method outlined in the website referenced in section 1 above.<br>**1. Apply through the URL for submitting the FY 2026 check sheet by accessing the website referenced in section 1 above.**<br>**2. Alternatively, submit the check sheet using the destination URL provided via email.** |
| 4 | Supplementary information | • Companies that receive a request for self-evaluation are requested to ask their Tier 1 suppliers to perform self-evaluations. Additionally, they should request that these suppliers extend this self-evaluation request to their Tier 1 suppliers. |

# Today's Agenda

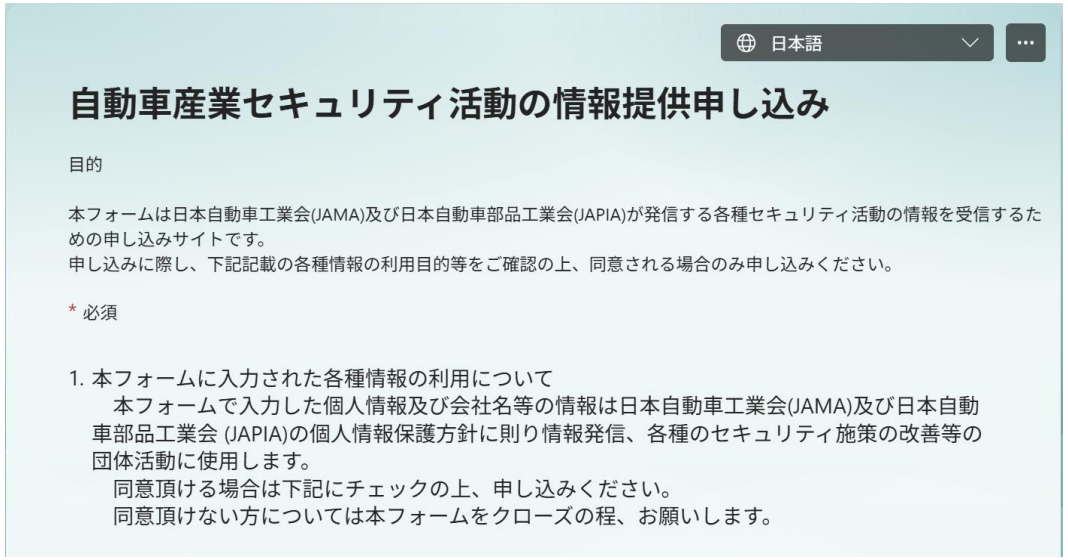
| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# 4-1. Applying for Information on Automotive Industry Security Activities

- ✓ From the last fiscal year, JAMA and JAPIA have regularly disseminated information on information security activities and other JAMA/JAPIA initiatives **aimed at enhancing cybersecurity measures across the automotive industry**.
- ✓ Emails will be sent to those who select **“Request Information”** on the **“Apply for Information on Automotive Industry Security Activities”** page of the official JAMA website.

**Application form for receiving information for automotive industry suppliers**

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_supply_chain.html




**[Information to be provided]**

- ✓ Information on Automotive Industry Cybersecurity Guideline Self-Evaluations
- ✓ Information on self-evaluation request briefing sessions, etc.

# 4-2. Sending of Email Newsletters

- ✓ From the last fiscal year, **e-mail newsletters have been sent out aimed at revitalizing security activities across the entire automotive industry**.
- ✓ **Emails will be sent** to those who select **“Request Information”** on the **“Apply for Information on Automotive Industry Security Activities”** page of the official JAMA website.
- ✓ **Subscribers will receive security-related tips and information on JAMA and JAPIA initiatives.**

## ■ Details

- Introduction of security measures and alerts, etc.: Passwords, log management, encryption, alerts ahead of extended holidays, etc.
- Security news, such as information on major reported incidents, cyberattack trends, emerging risks, and current phishing emails
- Security vulnerability alerts, such as notifications on critical vulnerabilities or brief descriptions of countermeasures
- Announcements, such as information on events and other notices from JAMA

*Topics are selected based on feedback from surveys conducted at the time of sending.

## ■ Email frequency

Although only three issues were sent in total during the last fiscal year, six issues are planned for this fiscal year, with one being sent every other month.

# 4-3. Chatbot for Inquiries Regarding Automotive Industry Cybersecurity Guidelines (Overview)

## A chatbot has been established for inquiries regarding Automotive Industry Cybersecurity Guidelines

- ◆ Chatbot access (JAMA website)
  Chatbot URL: Chatbot for inquiries regarding Automotive Industry Cybersecurity Guidelines
- ◆ Availability period: September 1, 2026 to January 15, 2027
  *The guideline submission deadline is December 31, 2026
- ◆ Cost: Free
- ◆ Application: Inquiries regarding Automotive Industry Cybersecurity Guidelines

Assistance will be provided by this chatbot, which was trained on past inquiries regarding issues faced when carrying out self-evaluations using the guidelines.

# 4-4. Consultation Desk (Usage Example)

You can ask chatbot questions that are either specific or abstract.

**Example of specific question**

**Please provide information on Guideline #1.**

jama

**Below is information on Guideline #1.**

- Details of guideline #1
- The purpose of Guideline #1 is to have companies demonstrate basic concepts and policies regarding security and enhance awareness of information security within their organization.
- Specifically, an in-house information security policy must be established and communicated within the organization.

**Example of abstract question**

**What security measures can be taken without spending any money?**

jama

- **Security measures that can be taken without spending money**
- We recommend starting with the simple measures described in the Guidelines that can be implemented within your company. Specifically, this involves formulating confidentiality rules and explaining these to employees, such as when joining or leaving the company.
- You can also make use of the “Cybersecurity Rescue Team” service provided by the Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA). This service makes it possible to implement security measures at a relatively low cost.
- It is also essential to conduct regular security training and education within the company to enhance employee security awareness.

Please refer to these measures when proceeding with your own security measures.

**Relevant documentation**

- Document name: JAMA/JAPIA Cybersecurity Guidelines V2.2
- See page: P5
- FAQ number: 99

Note: Although the chatbot is limited in what answers it can provide, we hope it can be used to solve any problems you may face in promoting self-evaluations.

# 4-5. Improvement Support Activities

## Helping SMEs improve their security with this one handbook!

**The Reality for SMEs (Challenges Revealed by the Survey)**

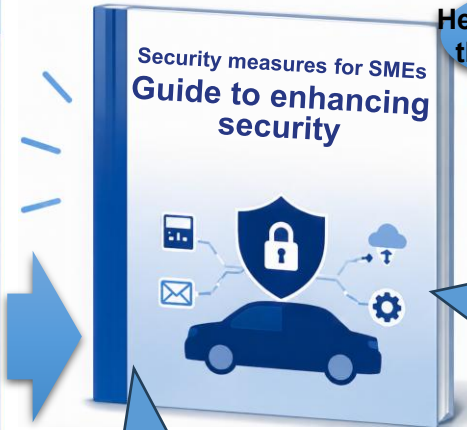
**Senior management doesn't understand**
It is viewed as low priority, making it difficult to move initiatives forward

**Inadequate security personnel**
No one or not enough people have specialized knowledge

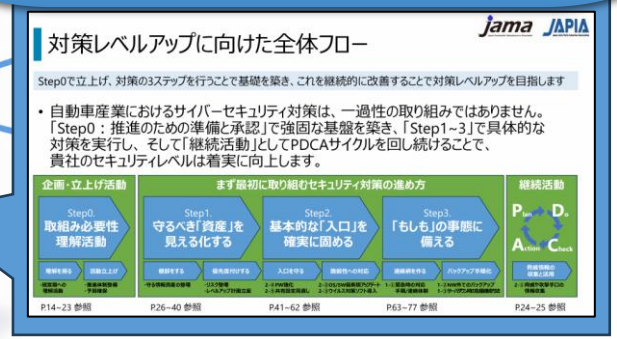
**Securing a budget is difficult**
The need is felt, but there is no room to allocate funds to investment

**We don't know where to start**

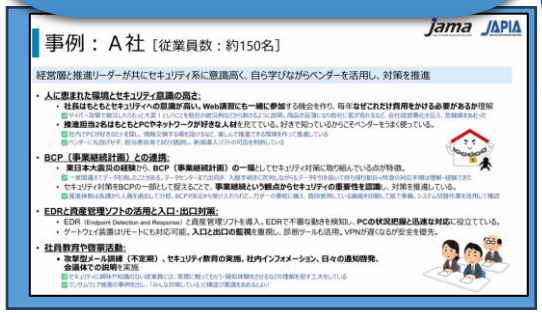
**Please be sure to give it a read first!**




**Helps address problems while assisting users in taking the first step toward implementing countermeasures**




**Delivering real voices from the field. Case studies included!**





**Find information to help your company through the real initiatives of others!**

These case studies are not theoretical exercises, but are proven paths to success, put into practice by companies in the same position as yours.

## Security measures are nothing out of the ordinary.

This handbook clearly explains everything from what can be addressed with limited resources right away, as well as a reliable path for steady improvement.

**Start with what you can, beginning with this one handbook!**

**Download this handbook from the JAMA website.**

https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_Security_LevelUp_Handbook.pdf

# Today's Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# 5-1. Special Content

## ■ Message

**A reality that suddenly struck one day.**
**Lessons learned from that experience, and the changes that followed.**

Miyaki Co., Ltd. will share its firsthand experience and the lessons learned from it, for the benefit of others in the automotive industry.
Please listen with the understanding that this could happen just as easily at your company tomorrow.

## ■ Speaker Introduction

Miyaki Co., Ltd.
Masayuki Yamamoto, Executive Officer, Management Administration Department
Yoshinobu Suzuki, Chief, Systems Section, Corporate Planning Division, Management Administration Department

# Today's Agenda

| | |
|---|---|
| 1 | Introduction |
| 2 | The importance of cybersecurity measures –Introducing recent case studies– |
| 3 | Request for Self-evaluation for FY 2026 |
| 4 | Forthcoming activities and the application process for information on automotive industry security activities |
| 5 | Special Content *Exclusive for briefing session attendees |
| 6 | Summary |

# 6-1. Briefing Session Summary

**[Global Situation]**

- Manufacturing has the highest number of incidents of any industry. This is no longer “someone else's problem”.
- Defenses at your company alone are not enough. Risk management is required across the entire supply chain.

**[Trends in Systems and Threats]**

- METI and IPA are scheduled to have the SCS Evaluation System implemented by the end of FY 2026. As an industry, the guidelines will be unified into a single guideline from FY 2028.
- The misuse of AI is spreading attacks that are faster and larger in scale. Response speed is what determines the outcome.

**[Recent Case Study: ASKUL]**

- A ransomware attack suspended e-commerce and logistics operations, with recovery taking approximately four months, and resulting in roughly 740,000 records of personal information being leaked.
- Damage could have been minimized by thoroughly implementing basic measures such as multi-factor authentication, EDR, and backups.

**[Self-evaluation Status]**

- In FY 2025, a record 4,032 companies conducted self-evaluations, and an improvement in average scores was also seen.
- In order to consistently monitor your progress, we request that you conduct a self-evaluation in FY 2026 as well.

# 6-2. Today's Requests

## 1. Conduct and submit a self-evaluation

- Conduct a self-evaluation using Automotive Industry Guidelines Check Sheet V2.3 and submit it by December 31, 2026.
  (The target is to achieve Levels 1 and 2. Companies that have already achieved these should aim for Level 3.)

## 2. Extend to the entire supply chain

- Request that Tier 1 suppliers also conduct self-evaluations, and extend this action further down the supply chain.

## 3. Ensure proactive involvement from senior management

- Position security as a management issue, and secure personnel, budget, and structure faster than ever before.

## 4. Implement reliable basic measures

- Thoroughly implement basic measures such as early response to vulnerabilities, patch application, backup preparation, and multi-factor authentication.

# 6-3. In Conclusion

**Know where your company currently stands before taking that first step.**

1. Assess your company's risk by checking the status of countermeasures via self-evaluation with the guidelines.
2. Have senior management get involved in securing the personnel, budget, and structure needed for any countermeasures that are lacking.
3. Rather than treating this as a one-time effort, conduct regular reviews while continually making improvements.

**We will work together with everyone in raising security levels across the entire supply chain. Thank you for your attention.**