Japan Computer Emergency Response Team Coordination Center



JPCERT CC®

# J-CLICS Guidance

STEP 1

## For All Users of Industrial Control Systems

Japan Computer Emergency Response Team Coordination Center

March 7, 2013

## About This Guide

This guide is provided as a supplement to J-CLICS (Check List for Industrial Control Systems of Japan). Its purpose is to clarify and explain the measures referred to in each checklist question.
This guide explains the meaning (background and purpose) of the questions listed on the checklist and how to implement specific countermeasures, so you can use it to more accurately judge whether you should mark each question with a ✓ or a X as well as to design and implement effective measures for the questions you mark with an X.

### Content of This Guide

This guide has been prepared so that the sections for each question can be read independently of one another. Rather than reading the entire guide, you may read only those sections necessary for you to understand particular questions.
The guide uses the following format to provide information to help you obtain a deeper understanding of each question:

**Background and Purpose**
An explanation of the background and purpose of the J-CLICS question.

**Potential Risks**
Examples of potential risks if what the J-CLICS question asks is not met. You can eliminate or reduce these risks by implementing the measures described in the next section (Explanations and Implementation Examples).

**Explanations and Implementation Examples**
A detailed explanation of the J-CLICS question and examples of countermeasures you can take to fulfill the requirements described in the relevant question. Provided measures are strictly generalized examples. Using them as a guide, you must consider which measures are best for each work site.

**References**
Information sources related to the J-CLICS question, such as books, papers, and websites that you may use to better understand the question.

**Supplement**
Supplementary information pertaining to the J-CLICS question that may be useful when reviewing or implementing measures. This supplement appears at the end of each question.

## Acknowledgments

J-CLICS was created through the cooperation of the SICE/JEITA/JEMIMA Security Working Group (WG) and the Joint Council of J-CLICS Users based on the items in the Japanese version of SSAT (SCADA Self-Assessment Tool), which is freely distributed by the JPCERT Coordination Center.

**People Who Collaborated in the Creation of J-CLICS**
**(Affiliations as of the publication of this guide, titles omitted)**

| | |
|---|---|
| Takayuki Arai | Yokogawa Electric Corporation (JEMIMA) |
| Yuuji Umeda | Toshiba Corporation (JEMIMA) |
| Hiromichi Endo | Hitachi, Ltd. (JEMIMA) |
| Shirou Kitaura | The Japan Gas Association |
| Takushi Kitagawa | The Federation of Electric Power Companies of Japan |
| Satoshi Kubo | Fuji Electric Co., Ltd. (JEMIMA) |
| Satoshi Kuboya | Azbil Corporation (JEMIMA) |
| Yoshiaki Shimizu | Fuji Electric Co., Ltd. (JEMIMA) |
| Hiroyuki Sugitani | Mitsubishi Chemical Engineering Corporation |
| Kenji Takatsukasa | Fuji Electric Co., Ltd. (JEITA) |
| Naoto Takamune | Mitsui Chemicals, Inc. |
| Seiji Takita | Japan Electric Measuring Instruments Manufacturers' Association |
| Tsutomu Yamada | Hitachi, Ltd. (SICE) |
| Hidehiko Wada | Yokogawa Electric Corporation (JEITA) |
| Souichi Watanabe | Mori Building Company |

**Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA)**
The Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) PA/FA Measurement and Control Committee Security Research Work Group researches and studies the future impact of and initiatives on security in the manufacturing sector, and provides feedback and valuable information to JEMIMA member companies.

**Japan Electronics and Information Technology Industries Association (JEITA)**
The Japan Electronics and Information Technology Industries Association (JEITA) Control and Energy Management Technical Committee researches and studies issues and solutions in order to disseminate and promulgate industrial control system security measures, and defines and proposes visions for safe, secure factory and plant operation.

**The Society of Instrument and Control Engineers (SICE)**
The Society of Instrument and Control Engineers (SICE) Technical Committee on Instrument and Control Networks in the Technical Division on Industrial Applications researches and studies the implementation of the latest IT technologies, standardization activities, and industrial control system security technologies at industrial sites in order to coordinate information concerning the industrial control systems field.

# Table of Contents


**Introduction**

About This Guide ..... 2

Acknowledgments ..... 3

**1. Physical Security**

Question No. 1-1 ..... 6

Question No. 1-2 ..... 8

Question No. 1-3 ..... 10

Supplement ..... 13

**2. Equipment Connection Procedures**

Question No. 2-1 ..... 16

Question No. 2-2 ..... 19

Supplement ..... 21

**3. Passwords and Accounts**

Question No. 3-1 ..... 23

Question No. 3-2 ..... 25

Question No. 3-3 ..... 27

Supplement ..... 29

**4. Ensuring of Responsiveness**

Question No. 4-1 ..... 32

Supplement ..... 34

**5. Third-party Risk Management**

Question No. 5-1 ..... 36

Supplement ..... 38

**6. Continuous Evaluation and Improvement (Kaizen)**

Question No. 6-1 ..... 40

Supplement ..... 42

**Appendix A**

Information Security Reference Materials ..... 44

# 1. Physical Security

Question No. 1-1

**Is access to the control room restricted to authorized personnel?**

---

Question No. 1-2

**Are visitors to the control room always accompanied by an authorized person?**

---

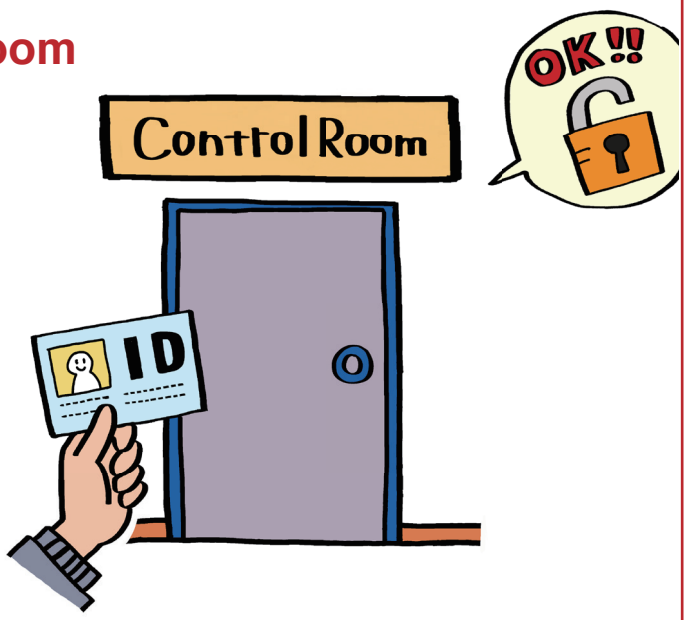
Question No. 1-3

**Is access to the control room managed (regular checking by record and by administrator)?**

---

## Question No. 1-1

# Is access to the control room restricted to authorized personnel?




In order to ensure that only authorized personnel can access the control room (where control equipment or operation terminals are located) and operate the equipment, access must be appropriately managed so as to restrict entry to and exit from the control room to authorized personnel.

## Background and Purpose

The control room contains equipment that is critical to the operation and setup of the industrial control system. Sensitive data that must be protected may also be handled there. To prevent control equipment from being operated in an unauthorized manner and to prevent leaks of sensitive data, it is important to restrict access to the control room to authorized personnel.

## Potential Risks

If someone with malicious intent enters the control room, he or she can physically access to the equipment there, and may operate the equipment without authorization, leak information, physically destroy the equipment, or steal the equipment. In addition, if unauthorized personnel enter the control room, they may perform careless or accidental operations or make changes that could impact the operation of the industrial control system, which may result in malfunction or stoppage of the industrial control system.

## 1. Physical Security

Question No. 1-1

## Explanations and Implementation Examples

To manage access to the control room, you can implement the following measures.

(A) Establish rules.

(1) Establish and enforce rules to restrict access to the control room to authorized personnel.

(2) Create a list of personnel authorized to enter the control room and disseminate the list to relevant parties.

(3) Post a notice at the entrance to the control room that states that entry is restricted to authorized personnel.

(4) Ensure that visitors are always accompanied by an authorized person. Refer to Question No. 1-2 for more information on measures pertaining to accompanying visitors.

(B) Require identification to be worn.

Distribute identification (ID cards, etc.) to all authorized personnel and require authorized personnel to wear identification.

If someone who is not wearing identification attempts to enter the control room, ask the person to identify himself/herself and check that the person is authorized to enter.

(C) Introduce access management equipment.

Install a locking device that authenticates people via ID cards, PINs, or other means in order to restrict access to the control room to authorized personnel.

(D) Log access to the control room.

Log every access to the control room and save the logs for a set period of time. The length of time to save the access logs should be set and managed in accordance with company policy. Refer to Question No. 1-3 for more information on measures pertaining to access management.

(E) Review access authorization.

Immediately review access permissions whenever authorized personnel are transferred to ensure that the appropriate personnel have been granted the appropriate permissions. Regularly check the validity of the authorized personnel list and update it as necessary.

**References**

- ISO/IEC 27001: A.9.1.1 Physical security perimeter
- ISO/IEC 27001: A.9.1.2 Physical entry controls

Question No. 1-2

# Are visitors to the control room always accompanied by an authorized person?


If visitors are allowed to access the control room (where control equipment or operation terminals are located) during the course of work, ensure that they are accompanied by an authorized person who is familiar with the rules of the control room, that they do not operate or connect to any equipment without authorization, and that they do not bring in or take out any equipment.

## Background and Purpose

The control room contains equipment that is critical to the operation and setup of the industrial control system. Sensitive data that must be protected may also be handled there. To prevent visitors from operating equipment without due reason or without authorization as well as to prevent photographing, duplication, and removal of sensitive data, control room visitors must always be accompanied by an authorized person.

## Potential Risks

Once a visitor is allowed to enter the control room, he or she may gain physical access to all equipment in the room. Such a person may leak sensitive data or accidentally operate or make changes to equipment, which could impact the operation of the industrial control system and lead to malfunction or stoppage of the industrial control system.

## Explanations and Implementation Examples

To manage visitors' access to the control room, you can implement the following measures.

(A) Establish rules.

Establish and enforce rules for visitors who access the control room. Explain the rules to visitors and instruct them to comply with the rules before they enter the control room. Have an authorized person accompany visitors while they are in the control room to ensure the rules are followed.

**Examples of rules**

(1) Whenever a visitor enters the control room, he or she must inform an authorized person of his or her purpose of entry and obtain permission to enter.

(2) Visitors must listen to an explanation of emergency response procedures and act in accordance with such procedures.

(3) Visitors must always carry out their work in the control room while accompanied by an authorized person. Visitors must always obtain permission from an authorized person in the following instances:

- If touching equipment in the control room
- If taking photos, shooting video, or recording audio in the control room
- If bringing anything in or taking anything out of the control room (the authorized person shall identify the item(s) brought in before the visitor enters or exits the control room)

(4) As a general rule, recording media (USB memory devices, CDs, DVDs, magnetic tape, etc.) and portable information devices (cameras, mobile phones, etc.) may not be brought into the control room. If data must be brought in or taken out of the control room, visitors must make a request to do so to the authorized person and follow the authorized person's instructions.
(In such a case, the authorized person will review the relevant content or data and perform a virus scan. Devices that can read/write data shall be subject to having their content verified and transferred to a USB memory device provided for use and the like upon the visitor's entry to and exit from the control room.)

(5) As a general rule, laptops and other information devices may not be brought into the control room. If an information device must be brought into the room, the visitor must make a request to do so to the authorized person and follow the authorized person's instructions. (The authorized person shall lend the visitor a PC to use and verify the content upon the visitor's entry to and exit from the control room.)

(6) Feature phones and smartphones may not be used in the control room. If necessary, take measures to have the reception desk and so forth keep such devices before the visitor enters in the control room.

(B) Require visitor ID cards to be worn.

Distribute ID cards that display the visitor ID number and scope of authorized access and require that visitors to wear such ID cards. If you encounter any visitors who are not accompanied by an authorized person or anyone who is not wearing an ID card, instruct the person to exit the control room and contact security.

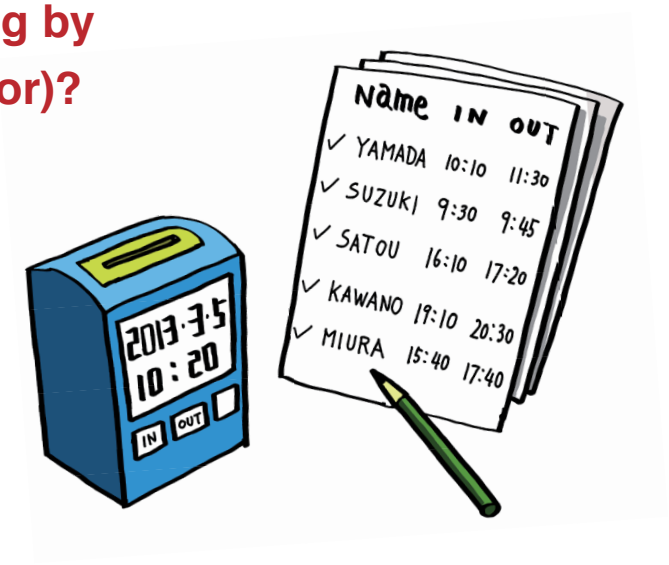
**References**

- ISO/IEC 27001: A 6.2.2 Addressing security when dealing with customers
- ISO/IEC 27001: A.9.1.5 Working in secure areas
- ISO/IEC 27001: A.10.7.1 Management of removable media

## Question No. 1-3

# Is access to the control room managed (regular checking by record and by administrator)?

In order to ensure that only authorized personnel enter the control room (where control equipment or operation terminals are located), it is important to regularly check the access status and periodically check the access logs.




## Background and Purpose

The control room contains equipment that is critical to the operation and setup of the industrial control system. Sensitive data that must be protected may also be handled there. It is crucial that people who are not authorized to access the control room be prevented from performing unnecessary or unauthorized operations as well as photographing, duplicating, and removing sensitive data. To prevent access to the control room by unauthorized personnel, log the person's identity, time of entry, time of exit, and purpose of visit, and periodically review these access records. Access records can be used as an audit trail and to assist in an investigation if a security incident or accident occurs.

## Potential Risks

Without access logs, any defects in access management are left unsolved. This leads to overlooking of the entry of unauthorized personnel or items into the control room, and may cause a security incident or accident. Moreover, when a security incident or accident occurs, without access logs it becomes more difficult to identify the cause and extent of effects and may make it hard to respond and take appropriate measures. Not having logs also renders it impossible to determine whether access to the control room is being managed appropriately and further increases the difficulty of discovering and rectifying access management problems.

## Explanations and Implementation Examples

To manage control room access logs, you can implement the following measures.

(A)Establish rules.

(1) Establish and enforce rules on recording access to the control room by authorized personnel.

Authorized personnel access log examples

- Log times of entry and exit to the access management system in combination with an electric lock and an ID card or PIN.
- Record access using time cards.
- Record access in a logbook or notebook. In such a case, always follow approval procedures.

(2) Establish and enforce rules on visitor access authorization and logging.

Visitor access log examples

- Name and affiliation of the visitor
- Name, affiliation, and contact information of the person(s) being visited
- Purpose of the visit and description of any work to be done
- Scope of access authorization and equipment to be operated
- Entry time, expected exit time, and actual exit time
- If information devices (PCs, USB memory devices, etc.) are to be brought in, their content
- If a PC, USB memory device, or something else is to be lent, its content
- Name and signature of approval of the authorizing party
- Access authorization ID card (name tag) number
- Visitor's signature on the rules consent form

(3) Establish and enforce rules on authorizing and logging bringing in/taking out recording media/information devices to/from the control room.

Log examples of bringing in and taking out recording media and information devices

- Name and affiliation of the person responsible for bringing in or taking out the item
- Type, name, and lot number of the recording media or information device
- Purpose and description of the work to be done with the item brought in or taken out
- Content of data stored on the recording media or information device
- Extent to which the item will be connected to the network, media, or equipment
- Time the item is brought in and time the item is taken out
- Applicable rules (perform a virus scan, etc.) and details of work to be done (virus scanning software, etc.)
- Name and signature of approval of the authorizing party
- Check and signature of approval when the item is brought in and when the item is taken out

(B) Introduce access management equipment.

Install a locking device that authenticates people via ID cards, PINs, or other means in order to restrict access to the control room to authorized personnel. Install and operate such devices in accordance with the company policy.

## 1. Physical Security

Question No. 1-3

(C) Manage access with surveillance cameras.

Install surveillance cameras at the entrance to the control room to record all who access the room. Install and operate such cameras in accordance with the company policy.

(D) Store access logs.

(1) Log every access to the control room and save the logs for a set period of time.

(2) If using an authentication device to manage access to the control room, save the device logs.

(3) Set and manage the access log retention period in accordance with the company policy.

(E) Periodically review access logs.

(1) Periodically review the content of access logs to check that nothing suspicious has occurred.

(2) If something suspicious or insufficient is found in the logs, contact the relevant parties to check whether or not there is a security issue.

**References**

- ISO/IEC 27001: A.9.1.1 Physical security perimeter
- ISO/IEC 27001: A.9.1.2 Physical entry controls

## 1. Physical Security

### Supplement Question No. 1-1

**Bringing Information in or out of the Control Room**

It is desirable to define rules on and manage bringing in and taking out of items that can spread viruses or leak information, including memory devices (USB memory devices, USB hard drives, etc.), recording media (CDs, DVDs, magnetic tape, etc.), portable information devices (mobile phones, etc.), and information devices (laptops, etc.)

**Example rules on bringing data in and taking data out of the control room**

(1) Before bringing memory devices (USB memory devices, USB hard disk, etc.) into the control room, ensure that doing so is absolutely necessary.
(2) Copy only the minimum amount of necessary data onto the USB memory device.
* Before copying data, format the provided USB memory device to ensure that no unnecessary data remains on the device.
* Disable AutoRun and use a USB memory device that has a write-protect switch.
(3) Allow the USB memory device to be taken into the control room only after running a virus scan and disabling AutoRun.
(4) Turn on write protection before bringing the USB memory device into the control room (Cover the write-protect switch with a sticker and so forth to help ensure that the switch does not get turned off).
(5) After use, initialize the USB memory device by formatting or other means to completely remove the data.

From a security perspective, it is preferred to use read-only DVD-R and CD-R media as the means of bringing data into the control room. Allowing information devices such as laptops to be brought into the control room is dangerous. It is desirable never to allow devices to be brought into the control room from the outside for any reason. If a PC is necessary to carry out work in the control room, provide an alternative such as lending visitors a PC for use in the control room instead of allowing them to bring their own PCs. Before and after each use, initialize the PCs that have been lent out to visitors by restoring from a backup of the environmental settings in order to always keep clean conditions. If there is no other choice but to bring in a laptop from the outside for operational requirement (in the control room environment in which a wireless LAN has been introduced), ensure that no wireless access point scanning software, hacking tools, or password analysis tools are installed on the laptop.

### Supplement Question No. 1-2

**Sensitive Data in the Control Room**

The control room contains information that should be handled with care. Such information must be organized and managed properly to prevent visitors from seeing it. Particularly sensitive data such as passwords and the locations of keys should be checked that it is not disclosed.

## 1. Physical Security

**Examples of managing sensitive data in the control room**

(1) Do not allow visitors to go near equipment that displays sensitive data.
(2) Use security filters to prevent visitors from peeking at the content of monitors.
(3) Lock storage cabinets that contain sensitive data to prevent visitors from easily accessing their content.
(4) Set up printers in locations that are not easily accessible to visitors in order to prevent information from being leaked through printed materials. Alternately, collect all printed materials immediately after printing and never leave at the printer.
(5) To prevent sensitive data leaks from materials discarded in the trash, pay sufficient attention to the disposal of sensitive materials so that visitors cannot easily take away trash.

### Control Room Equipment Lock and Key Management

Control panels, racks, and other equipment in the control room must be properly locked to prevent unauthorized operation of equipment by visitors.

**Examples of lock and key management**

(1) Do not use the same key for multiple areas.
(2) Do not lend keys to visitors; have the accompanying authorized person perform unlocking and locking as necessary.

**Supplement** Question No. 1-3

### Control Room Access Logs

Logging access to security areas such as the control room provides important clues in the event a security incident or accident occurs. In addition to keeping a record of the time visitors enter, we also recommend recording the time they exit. Moreover, you must consider how to prevent access log falsification and tampering.

**Examples of countermeasures against log falsification and tampering**

(1) Make a carbon copy of the access log document when filling in records.
(2) Use a ball-point pen when filling in records.
(3) Review the content of the document when visitors leave.
(4) Have the approving party and the authorized person being visited sign the document.

### Installation of Surveillance Cameras (CCTV)

Recording actual entry to and exit from the control room using surveillance cameras or another type of physical monitoring system provides useful information for analysis in the event a security incident or accident occurs. Physical monitoring systems can also help deter crime.

**Examples of surveillance camera introduction**

(1) Install surveillance cameras in conspicuous places where they can easily be seen at the entrance to the control room and other security areas as well as at important facilities where no personnel are regularly stationed. (Having visible surveillance cameras helps deter unauthorized entry and operation.)
(2) Always set the internal clocks of surveillance cameras to the exact time. (If the internal clock is set to an incorrect time, it will not be possible to properly check the recordings, causing them to lose their value as evidence.)
(3) Regularly review the recorded video to ensure that no unauthorized access to the control room or operation of important equipment has been overlooked.

# 2. Equipment Connection Procedures

Question No. 2-1

**Are procedures followed to check that equipment has not been infected with a virus before connecting it to the industrial control system network?**

---

Question No. 2-2

**If industrial control system equipment is installed in the same rack as information system equipment, is each piece of equipment labeled (with a tag, sticker, etc.) to identify the system to which that equipment belongs?**

---

## Question No. 2-1

# Are procedures followed to check that equipment has not been infected with a virus before connecting it to the industrial control system network?


To prevent computer virus infections, it is important to establish and follow procedures for running virus scans on equipment (information devices such as laptops, memory devices such as USB memory devices and USB hard disks, recording media such as CDs and DVDs, and portable information devices such as mobile phones) before connecting them to the industrial control system or control network.

## Background and Purpose

Memory devices (USB memory devices, USB hard disks, etc.), recording media (CDs, DVDs, magnetic tape, etc.), information devices (laptops, etc.) and portable information devices (mobile phones, etc.) are all possible means of transmitting computer viruses. Because viruses that target industrial control systems and spread through such devices have been discovered in recent years, extra precautions and countermeasures will be necessary in future.

## Potential Risks

Virus infections of industrial control system equipment may adversely affect the operation of the industrial control system, possibly leading to a serious situation such as a complete shutdown of operations. Destructive activities of viruses may induce information leaks and system data corruption. Also, removing a virus may require the system to be stopped or software to be reinstalled, incurring significant costs and damaging the brand image.

## 2. Equipment Connection Procedures

Question No. 2-1

## Explanations and Implementation Examples

To prevent virus infections, you can implement the following measures.

(A) Establish rules.

(1) Before setting up PCs that connect to the industrial control system or control network, develop and follow test procedures to prevent virus infections.

- Ensure that the OS and all software are up-to-date. Patch and update if necessary.
- Ensure that virus definitions are up-to-date before scanning for viruses.
- Perform a virus scan in advance to ensure that the equipment is not infected with a virus.
- Ensure that unnecessary services and communication functions have been disabled. (Port scanning tools and vulnerability inspection tools may be used.)

(2) Develop and follow procedures to prevent sensitive data leaks when removing equipment that has been connected to the industrial control system or control network. Define procedures to completely erase or physically destroy hard disks as necessary.

(3) As a general rule, prohibit information devices (laptops, etc.), memory devices (USB memory devices, USB hard disks, etc.), and recording media (CDs, DVDs, magnetic tape, etc.) from being brought in from the outside and from being connected to the industrial control system or network.

(4) Prohibit USB connections for charging or power supply purposes (music players, feature phones, smartphones, fans, LED lights, etc.)

(5) If information equipment is brought in for operational requirement, request to do so in writing in advance and submit the equipment for inspection before bringing it in. Undergo a check by a third party when bringing equipment into or taking it out. Keeping written records of what equipment is brought into the control room will help identify the infection route should an infection occur.

**What to include in written requests**

- Name and affiliation of the requesting party
- Name and affiliation of the authorizing party
- Date and time the equipment is to be brought in and the period it will be brought in for
- Name and type of equipment to be brought in
- Purpose of and work to be done with the equipment to be brought in
- Equipment or network to connect to
- Potential risks
- Applicable rules and procedures
- Matters to be checked when the equipment is brought in and the results of checking; name and affiliation of the checking party
- Matters to be checked when the equipment is taken out and the results of checking; name and affiliation of the checking party
- Versions of the antivirus software and pattern file used

(6) Cover any USB ports and other connection ports that will not be used in the course of the work with stickers and so forth to prevent them from being used to connect to equipment.

## 2. Equipment Connection Procedures

Question No. 2-1

(B) Set up a PC to detect viruses.

**Examples of introducing a PC to detect viruses**

(1) Set up a PC dedicated to virus scanning of memory devices (such as USB memory devices and USB hard disks) as well as recording media (such as CDs and DVDs).

(2) Do not connect the virus scanning PC to the network in order to prevent it from becoming infected via the network. Use virus detection software that can be updated offline (while not connected to the network).

(3) Before running a scan, update that the OS and virus detection software on the virus scanning PC to ensure that they are up-to-date.

(4) Boot the virus scanning PC from optical media (such as a DVD) without mounting a hard disk.

(5) Before and after using the virus scanning PC, run a virus check on it to ensure that it has not become infected with a virus.

(C) Set up USB memory devices restricted to use in the control room.

Connecting memory devices such as USB memory devices and USB hard disks brought in from the outside to control equipment or networks is dangerous because they could be infected with viruses. Memory devices brought in from the outside may also lead to information leaks. You can reduce such risk by providing USB memory devices for use exclusively inside the control room and copying only the necessary data to such USB memory devices.

**Examples of handing of USB memory devices dedicated for use by visitors**

(1) As USB memory devices dedicated for use by visitors, use USB memory devices equipped with a write-protect switch and turn on write protection except when writing to the device.

(2) In order to prevent virus infections, turn off AutoRun of the PC that the USB memory device will be connected to.

(3) Connect any equipment owned by a third party to the virus scanning PC to check whether or not it has been infected with a virus.

(4) Before use, connect the USB memory device to the virus scanning PC to check whether or not it has been infected with a virus.

(5) Use the virus scanning PC to copy the necessary data from the equipment being brought in to the USB memory device.

(6) After use, connect the USB memory device to the virus scanning PC in order to reinitialize (format) the device and completely erase its data.

(D) Set up PCs restricted to use in the control room.

Connecting laptops that are brought into the control room to control equipment or networks is dangerous because they could be infected with viruses. Laptops brought in from the outside may also lead to information leaks. If use of a PC is unavoidable to carry out work, lend a PC restricted to use in the control room instead of allowing visitors to bring their own PCs in.

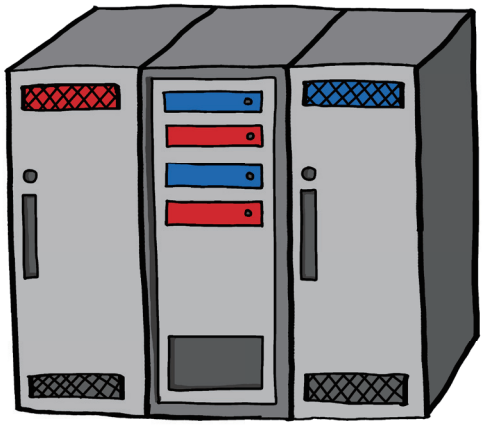
(Related to: Supplement - Question No. 1-1)

**Reference**

• ISO/IEC 27001: A.9.2 Equipment security

## Question No. 2-2

# If industrial control system equipment is installed in the same rack as information system equipment, is each piece of equipment labeled (with a tag, sticker, etc.) to identify the system to which that equipment belongs?



To prevent unauthorized operation and misuse as well as erroneous connection to the industrial control system, it is important to clearly identify industrial control system equipment and draw attention.

## Background and Purpose

Equipment and cables are likely to become mixed up in an environment where many pieces of equipment are installed. Such mistakes during system maintenance have a high risk of affecting system security and availability.

PCs and other equipment that are used daily and which have a high risk of becoming infected by viruses are connected to the IT network. For this reason, if you connect the IT system and the industrial control system via a network in an unintended manner, or if you connect equipment to be used with the industrial control system (such as USB memory devices or PCs restricted to use in the control room) to the IT system, the industrial control system may become infected with a virus, thereby affecting system operation. It is effective to draw attention by identifying and labeling industrial control system components and network cables as such to prevent them from being mistaken for part of the IT system.

## Potential Risks

Erroneous operation or erroneous connection due to confusion with other systems may lead to stoppage of the industrial control system or abnormal operation. Accidentally connecting the industrial control system to the IT system network could cause the industrial control system to become infected by a virus, thereby affecting industrial control system operation.

## 2. Equipment Connection Procedures

Question No. 2-2

## Explanations and Implementation Examples

To prevent erroneous operation and erroneous connection, you can implement the following measures.

(A) Establish rules.

Establish rules on handling industrial control system equipment, change approval procedures, and abnormality response. Hold seminars and so forth to explain and inform personnel thoroughly of these rules.

(B) Separate equipment on different racks and keep it locked up.

Install by management classification (the IT system, industrial control system, etc.) in a different area or on a different rack and lock each up with separate keys. Restricting physical access to equipment prevents accidents due to misidentification.

(C) Label equipment and cables.

Label the equipment and cables that belong to the industrial control system. Include a warning on the label stating that unauthorized use is prohibited to draw attention. To prevent unauthorized operation and improper response, include the administrator's contact information and describe what to do if an abnormality occurs. Use red or another color that stands out to increase the labels' efficacy.

(D) Seal open ports and terminals.

Physically seal open ports and terminals to prevent erroneous connection and attach a label stating that connection is prohibited to draw attention.

(E) Cover switches, etc.

To prevent erroneous operation, use labels to draw attention to power switches and so forth. The efficacy of labels can be increased by adding a statement to the effect that operation is prohibited.

(F) Color-code network cables.

To prevent erroneous connection, use different colored cables to connect to each network. Combine color coding with labeling to increase the efficacy of both approaches.

**Reference**

• ISO/IEC 27001: A.9.2.1 Equipment siting and protection

## 2. Equipment Connection Procedures

### Supplement Question No. 2-1

**Disposal of Recording Devices**

When disposing of memory devices (USB memory devices, USB hard disks, etc.), recording media (CDs, DVDs, magnetic tape, etc.), or recording devices (HDDs in laptops, etc.), measures must be taken to prevent information leaks. Initializing (formatting) or deleting data from memory devices may only rewrite the management area of the hard disk but not actually erase the data area; thus, it may be possible to restore information that was thought to have been erased. Physically destroying the equipment is the most reliable method of erasing data. Before disposing of equipment, use a tool or other implement to destroy the equipment so that their data can no longer be restored.

Destroy optical media such as CDs and DVDs using scissors or a specialized shredder before disposal. If a hard disk cannot be physically destroyed, use a tool to completely erase the data on the disk. Completely erasing all data on a hard disk typically takes a long time (from a few hours to several dozen hours). It is recommended to check the time required noted in the tool's instruction manual in advance.

Flash memory devices such as USB memory devices and SSDs use a special writing algorithm due to write cycle limitations. It may not be possible to erase data on flash memory devices simply by formatting them or overwriting them multiple times. To completely erase data from these devices, a special tool must be used or the device must be physically destroyed.

### Supplement Question No. 2-2

**Locking Up PCs Without a Rack Mount**

Erroneous operation of or erroneous connection to not rack-mountable PCs can be prevented by mounting them to a rack using a rack mount kit or by placing them on a lockable shelf and keeping them locked up. Locking up equipment is an effective way to prevent virus infections due to the inadvertent connection of a USB memory device or other equipment.

# 3. Passwords and Accounts

Question No. 3-1

**Is there an industrial control system password policy in place that stipulates a required password strength and expiry period?**

Question No. 3-2

**Are strong passwords used?**

Question No. 3-3

**Is the password to the industrial control system changed regularly?**

Question No. 3-1

# Is there an industrial control system password policy in place that stipulates a required password strength and expiry period?


It is important to establish a password policy that specifies the number of characters to be used in passwords, the types of characters that can be used, when passwords expire, and other details related to password management and strength.

## Background and Purpose

Many industrial control systems that feature computers and control equipment are strictly managed using passwords and subjected to measures for preventing unauthorized access to the system. However, because a person who merely knows the correct password can access the system to view critical data and manipulate equipment at will, people with malicious intent attempt to use a variety of means to discover or crack passwords. (The administrator password, which enables access to the entire system, is particularly sought after.)

Therefore, to prevent attacks on industrial control systems by means of industrial control system passwords and password management, a password policy that defines how to properly configure and use very strong passwords must be established.

Having a password policy means nothing if it is not followed. In addition to establishing a password policy, it is critical that everyone follows it.

## Potential Risks

Without a password policy, passwords will not be appropriately configured and managed, which increases the risk of passwords becoming compromised.

A compromised password can lead to unauthorized access to the industrial control system, theft of operational data or other important information, or rewriting of control equipment program code and specified values (parameters). This may result in changes to the industrial control system's behavior and huge losses if the system is stopped. If the system is critical infrastructure, the impact on society may be immeasurable.

## 3. Passwords and Accounts

Question No. 3-1

## Explanations and Implementation Examples

A password policy must be established that addresses topics such as configuring, changing, and otherwise managing passwords used in the industrial control system. In the event a password policy cannot be enforced due to the system's specifications or operational status, protect the system from access by unauthorized personnel by bolstering physical security measures, such as by implementing access and locking management.

(A) Create a password policy.

Develop and document a password policy. Password policies should include requirements such as those listed in the following examples.

(1) Use a password that satisfies the following conditions:

- Use a character string that you can remember. (Do not use a character string that is difficult to enter without checking a written note or hint.)
- Do not use character strings that can be found in a standard dictionary (English words, romanizations of Japanese words found in a dictionary, etc.) or strings that are commonly used in passwords.
- Do not use character strings related to the user of the password or that can be inferred from easily discoverable information about the user (names, dates of birth, phone numbers, car license plate numbers, etc.)
- Use a character string that combines the four types of characters: lowercase letters, uppercase letters, numbers, and symbols.
- Make character strings as long as possible (at least eight characters). If the target piece of equipment does not enable passwords to be at least eight characters, use the maximum number of allowed characters.

(2) Change passwords periodically and also change passwords after they have been used a certain number of times. Do not reuse old passwords.

(3) Do not show your password to anyone or share with anyone.

(4) Do not reuse passwords.

(5) If there is a possibility that someone may have come to know your password, change it immediately.

(6) Strictly manage the administrator password as sensitive data.

- Under normal circumstances, only the administrator should know the administrator password.
- Prepare a means of obtaining the administrator password in an emergency when the administrator is not present.

(B) Comply with the password policy.

Understand and comply with the requirements of the password policy.

(1) Follow the password configuration rules.

(2) Comply with password expiration periods.

(3) Comply with the method used to manage password information.

(4) Implement technical measures.

(5) Thoroughly educate and train all relevant employees.

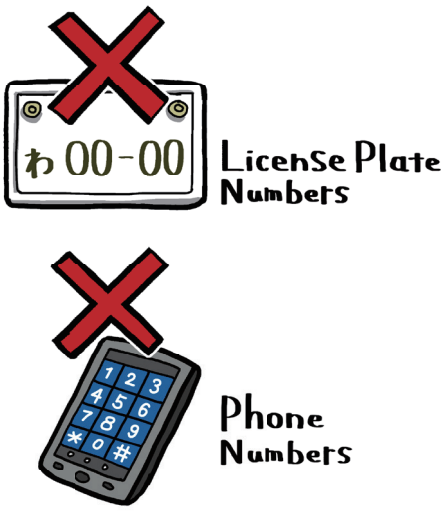
**Reference**

- ISO/IEC 27001: A.11.3.1 Password use

Question No. 3-2

# Are strong passwords used?

In order to prevent unauthorized access, passwords should be character strings that cannot be easily analyzed or guessed.




## Background and Purpose

A password is a combination (string) of characters. Strings can always be cracked by trying all possible combinations using methods known as dictionary attacks and brute-force attacks (refer to the Supplement: Question No. 3-2). If the attacker knows an individual's address, phone number, date of birth, or similar information, a common password cracking technique is to use that information to attempt to guess the password. Passwords with fewer characters are easier to crack and thus short passwords cannot be said to be secure. Increasing a password's length and including different types of characters can exponentially increase the time required to crack it.

To help prevent unauthorized access, avoid using words that appear in standard dictionaries as well as commonly used passwords and instead use strings of characters that seem like nonsense to third parties.

## Potential Risks

If a password is short or easy to guess, it is also easy to crack.

A cracked password can lead to unauthorized access to the industrial control system, theft of operational data or other important information, or rewriting of control equipment program code and specified values (parameters). This may result in changes to the industrial control system's behavior and huge losses if the system is stopped. If the system is critical infrastructure, the impact on society may be immeasurable.

## 3. Passwords and Accounts

Question No. 3-2

### Explanations and Implementation Examples

It is important that passwords be as long as possible (at least eight characters) and difficult to guess.
The following are not appropriate passwords:

- Many kinds of names, phone numbers, and dates of birth
- Words (such as English words) that can be found in a standard dictionary
- The name of the account or anything that can be inferred from the name of the account
- The same letter or number repeated in succession
- The temporary password provided when the account was created

When setting a password, consider doing the following:

- Use both uppercase and lowercase letters.
- Include both numbers and symbols.
- Use a string that cannot be found in a dictionary
- Use as long a string as possible (at least eight characters recommended).

Example: H!elZl2o

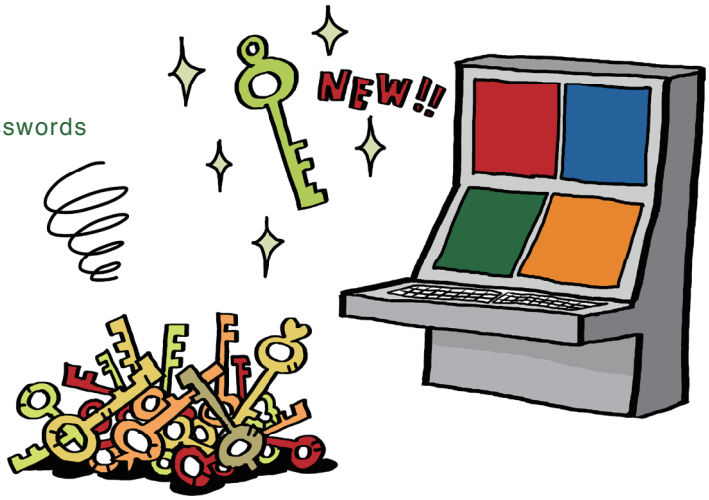
**References**

- IPA: Password Management and Cautions
  http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html (Japanese)
- Creating a strong password - Accounts Help
  https://support.google.com/accounts/answer/32040?hl=en
- ISO/IEC 27001: A.11.3.1 Password use

Question No. 3-3

# Is the password to the industrial control system changed regularly?

To prevent unauthorized access, passwords should be changed regularly.




## Background and Purpose

When someone with malicious intent successfully steals or cracks a password, that person is unlikely to publicize said fact so that he or she can continue to secretly access the system. However, regularly changing passwords revokes the ability to use stolen or cracked passwords.
Given enough time, all passwords can be cracked using password cracking tools. Continuing to use the same password without changing it means it is only a matter of time before the password is cracked through a brute-force attack or similar means. Therefore, changing passwords regularly is an effective means of avoiding security accidents and incidents.

## Potential Risks

A cracked or stolen password can lead to unauthorized access to the industrial control system, theft of operational data or other important information, or rewriting of control equipment program code and specified values (parameters). This may result in changes to the industrial control system's behavior and huge losses if the system is stopped. If the system is critical infrastructure, the impact on society may be immeasurable.

## 3. Passwords and Accounts

Question No. 3-3

## Explanations and Implementation Examples

Passwords should be changed regularly. In particular, administrator passwords with various special permissions should be changed more frequently than general user passwords.

(A) Establish rules.

Establish and follow rules on changing passwords regularly. In systems where passwords cannot be changed routinely, change passwords during inspections. In addition, prevent access to the control room by unauthorized personnel by bolstering physical security measures, such as by implementing access and locking management.

(B) Use password expiration functionality.

Some OSes enable you to set expiration dates for passwords. You can use this function to prompt users to change their passwords regularly.

(C) Implement education and training.

Explain to all users the importance of changing passwords and encourage them to do so regularly.

**References**

- IPA: Password Management and Cautions (Japanese)
  http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html
- ISO/IEC 27001: A.11.3 .1 Password use

## 3. Passwords and Accounts

### Supplement Question No. 3-1

**The Importance of Having Users Manage Passwords**

Technical measures (such as configuring OS settings) can be taken to set when passwords should expire and minimum character restrictions. However, no matter what technical measures are taken and how strong passwords are, any password becomes useless if it is written down on a sticky note and stuck next to an operation terminal. Each staff member must remain aware of security at all times during the course of daily work.

**Password Management Measures**

The administrator password must never be known by anyone but the administrator. However, you must also prepare a method for obtaining the administrator password to respond in an emergency when the administrator is not present. The following method uses an envelope to store the administrator password for use in an emergency.

**Storing the Administrator Password in an Envelope**

(1) Have the administrator write down the password on a piece of paper and seal it in an envelope.
(2) Store the sealed envelope in a lockable storage cabinet. Have the department strictly manage the key.
(3) If an emergency occurs, remove the envelope from the storage cabinet, open the envelope, and use the password.
(4) After the password has been used, have the administrator change the password.
*Check the envelope regularly to ensure that it remains sealed. Change the password immediately if the envelope has been opened.

**Alternate Measures If Not Using Passwords**

Access management using a password may be impossible due to the system's specifications or operational status. In such a case, protect the equipment from unauthorized personnel by bolstering access and locking management of the control room (where control equipment or operation terminals are located). Please refer to Question No. 1-1 for more information on access management.

### Supplement Question No. 3-2

Sometimes users write passwords on sticky notes and stick them near operation terminals to avoid forgetting them. However, because there may be some insiders with malicious intent, this sort of behavior is dangerous and should be corrected if discovered.
In addition, people are not the only ones who crack passwords. There exist software and tools with the ability to illegally obtain passwords. Such software monitors and records keyboard input. Using tools, hackers attempt to log in by trying different words listed in a dictionary or combinations of numbers and letters; such attacks are known as dictionary attacks and brute-force attacks, respectively. A password is more likely to be cracked if it is made up of a combination of letters and numbers that are easy to guess character string or is a commonly used in a password.

**How to Generate Strong, Memorable Passwords**

Mixing numbers and symbols into a large, random string of characters makes for a strong password, but the drawback is that such passwords are difficult to remember and handle. As shown on the following page, there are ways to create passwords that are both strong and memorable such as using independently determined passphrases and password generation rules.

## 3. Passwords and Accounts

**Password Generation Using Passphrases**

Generate a long password from a memorable sentence (phrase). This applies to systems that allow long passwords. Even though this method uses words that can be found in a dictionary, the combination of multiple words increases the password's resistance to dictionary attacks. Combine with numbers to further strengthen the password.

Example: Create a passphrase from a memorable phrase.
Phrase: "One day I met a bear in the woods"
Password: "1OneDay2I3Met4Abear5Inthe6Woods"

**Password Generation using Individual Generation Rules**

By deciding upon personal password generation rules in advance, users can generate a random password from a memorable phrase or word. By following their own independent rules, it is possible for users to generate passwords that are hard to guess based on well-known words or phrases. Passwords can be further strengthened by devising rules for mixing in uppercase letters, symbols, and numbers.

Example No. 1: Generate a seemingly random password from a memorable phrase.
Phrase: "One day I met a bear in the woods"
Step 1: Replace certain letters with similar-looking or sounding numbers: "1 d4y 1 m3t 4 b34r 1n th3 w00ds"
Step 2: Capitalize the first letter of each word and remove the spaces: "1D4y1M3t4B34r1nTh3W00ds"

Example No. 2: Generate a seemingly random password from a memorable word.
Word: "2-propanol"
Step 1: Capitalize the first letter of the word: "2-Propanol"
Step 2: Rearrange the letters in alphabetical order: "2-alnooPpr"
Step 3: Rearrange the letters again so that the vowels and consonants alternate: "2-lanoPopr"
* When creating a password using a passphrase or password generation rules, you must strictly protect the generation rules and the base word or phrase from becoming known by others. If someone may have learned of any of these, you must change the generation rules and the word or phrase.

**Supplement** Question No. 3-3

**Password Change Cycles**

Under the following conditions, it takes about 250 days to analyze and crack an eight-character-long password made up of upper and lower case alphanumeric characters (62 possible characters in total). In such a case, a password that is changed once per year may be discovered before it is changed again.

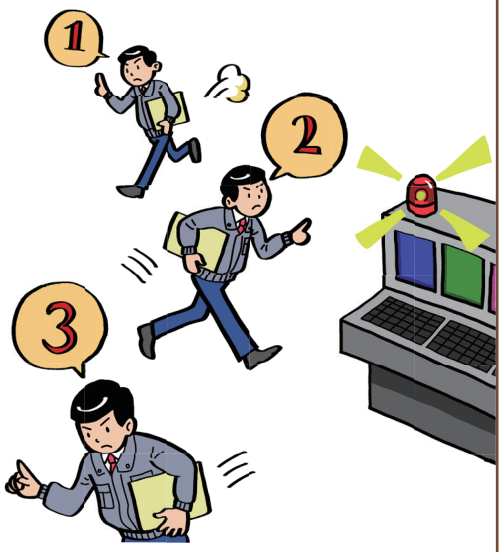
**Conditions**

- Use a password analyzing tool on an average PC that can test 10 million combinations per second.
- An eight-character-long password made up of upper and lower case alphanumeric characters has 218,304,105,584,896 possible combinations.
  Configuring the system so that accounts are locked after a certain number of failed login attempts and prohibiting users whose accounts have been locked from logging in without going through the process of unlocking their accounts may deter mechanical attacks and significantly extend the time to crack passwords.

# 4. Ensuring of Responsiveness

Question No. 4-1

**Do you understand the procedure for monitoring the security of an industrial control system and what to do in the event of an alert or an abnormality? Are you conducting drills to prepare for such incidents?**




## Question No. 4-1

# Do you understand the procedure for monitoring the security of an industrial control system and what to do in the event of an alert or an abnormality? Are you conducting drills to prepare for such incidents?

To minimize the damage from an attack on a control system, it is important to monitor for unauthorized access and attacks. In addition, to prevent any damage from spreading, it is also important to understand the monitoring procedure and what to do in the event of an alert or an abnormality, as well as to conduct drills to make sure that you will not panic in the event of an emergency.

## Background and Purpose

Just as robbers (burglars) in real life search for houses that are easy to break into and look for doors that are easy to open, people who want to harm an industrial control system search in advance to see whether the industrial control system they plan to attack has any weaknesses.
There are various ways a hacker can search for system vulnerabilities, but by analyzing the logs (e.g. access logs and event logs) stored on equipment such as a network device or a server, you can learn what kind of searches hackers are performing on your systems. It is also possible to estimate to what extent hackers have managed to breach your system and what operations they have performed. Furthermore, if you can respond quickly as soon as suspicious access is detected, you can prevent the theft of important data, unauthorized rewriting of control programs, and system shutdowns resulting from unauthorized operations.
It is important to understand the methods required to respond to security incidents and to conduct regular drills on these methods (procedures) in order to be able to respond quickly and accurately when suspicious access is detected or during an attack.

## Potential Risks

Even if you understand the procedures for monitoring unauthorized access and other security accidents or incidents and you understand what to do in the event of an alert or an abnormality, there is no guarantee that you will be able to respond accurately in an emergency if you have never actually carried out these procedures.
If you notice that your system might be under attack but just let time pass without responding, the damage will only spread. Mistaken responses or measures can also lead to secondary damage or accidents.
Just as with evacuation drills conducted to prepare people for how to respond to earthquakes and fires, it is important to experience the process of responding to a security incident before one actually happens.

## 4. Ensuring of Responsiveness

Question No. 4-1

## Explanations and Implementation Examples

(A) Understand monitoring procedures.

Activities done in the course of security monitoring range from monitoring of logs to physical investigation of connections of suspicious wiring or network equipment. The following list contains standard surveillance targets. All monitoring should be conducted according to the organization's monitoring procedures.

**Standard surveillance targets**

- Firewall and server access logs and event logs
- Log in and log out times (point to check: records of logging in at unusual times of day)
- Password change logs (point to check: whether passwords have been changed without users remembering)
- Logs of attempts to access information by users without access privileges
- Various industrial control system operation logs
- Intrusion detection system logs
- Access logs for controlled areas with important control equipment, such as the control room (where control equipment or operation terminals are located)
- Unauthorized connection of wiring or network equipment (routers, switching hubs, etc.)
- Changes in network load (point to check: very high load compared to normal)
- Whether or not any unauthorized processes are running

(B) Practice responding to alarms and abnormalities.

Practicing in the production environment may affect the system in operation, so preparation of a separate environment comparable to the production environment is ideal for the purpose of practice. If you cannot prepare a separate practice environment, another option is to change the settings of the production environment to the extent that the system is not affected. Even just visualizing operations being performed in front of terminals or equipment in one's head is a more effective method of practice compared to seeing the procedures for the first time and trying to follow them after an abnormality has occurred.

**References**

- ISO/IEC 27001: A.10.6 Network security management
- ISO/IEC 27001: A.10.10 Monitoring

## 4. Ensuring of Responsiveness

Supplement Question No. 4-1

### Setting the Exact Time

When analyzing logs collected from various monitored devices (network equipment, servers, etc.), the causal relationships and the order in which events occur will be analyzed based on the times recorded in the logs. For this reason, it is very important to set the exact time on each piece of monitored equipment. Some methods for setting the exact time are to use a radio clock or GPS, or to synchronize the equipment with an NTP (Network Time Protocol) server also called a time server.

### Security Monitoring Products and Services

The following products and services can be used for security monitoring.

(A) FW: Firewall

Software or hardware that monitors communication with the outside and allows only necessary communication to pass through.

(B) IDS: Intrusion Detection System

Software or hardware with the ability to detect unauthorized communication. Other products can also block unauthorized communication, but an IDS changes the firewall settings to block communication that it determines to be suspicious. For this reason, even when the IDS blocks communication, data that has been stolen may reach its destination, allowing the attack to be successful.

(C) IPS: Intrusion Prevention System/Intrusion Protection System

Software or hardware with the ability to stop unauthorized communication. Detecting whether data transmissions are suspicious by not sending data to its destination until the transmission has been determined to be valid can prevent data stolen in attacks from reaching its destination. However, erroneous detection may cut off normal access or allow unauthorized access. A high detection accuracy is necessary to avoid affecting network usage.

(D) UTM: Unified Threat Management

UTM refers to integrated security equipment with virus scanning, intrusion detection and prevention, and other features in addition to firewall capabilities. UTM products may be used instead when virus scanning software cannot be installed on control equipment or servers.

(E) Outsourcing of Security Monitoring

Collecting, managing, and analyzing security-related logs requires your understanding of security in addition to your knowledge of the network and system. When analyzing logs, it sometimes becomes necessary to analyze traces of unauthorized access using control equipment logs in addition to those of IDS, server equipment, etc., while keeping in mind the causal relationships between events instead of focusing only on a single point of entry, such as the firewall. Because such log monitoring requires highly skilled workers and a significant number of man-hours, outsourcing of security monitoring to companies that provide security monitoring services can also be an effective option. Many security monitoring services can provide efficient analysis using their knowhow in similar cases. Outsourced security monitoring services will send necessary monitoring logs to security monitoring centers on dedicated lines 24 hours a day, 365 days a year and prepare reports on the results of analysis conducted by their monitoring personnel; they will also cause communication to stop in the event of an alarm or abnormality.

# 5. Third-party Risk Management

Question No. 5-1

**Are the rules for ensuring remote connection security followed?**

Question No. 5-1

# Are the rules for ensuring remote connection security followed?

In order to prevent virus infections and information leaks, it is important to comply with the rules for connecting the industrial control system to the outside (remote connections). In this guide, remote connection refers to connecting industrial control system equipment or a management console to the Internet, or connecting such equipment or console to an Internet-connected PC or server.

## Background and Purpose

Remote connection to an industrial control system incurs the risks of virus infections, information leaks, and unauthorized operation from the outside. Even if industrial control system equipment cannot be used to access the Internet or read email, if such equipment is connected to a PC or server with such capabilities, it will be possible to access the industrial control system via the Internet through the connected PC or server. Similar risks emerge if the industrial control system communicates with an industrial control system at another location in order to carry out functions over an Internet connection. You must also exercise caution if the industrial control system uses an Internet database or web service.

Remote connections should be avoided as much as possible. Thoroughly demonstrate the necessity of any remote connections used for operational requirement. It is crucial to strictly manage remote connections to restrict them to the minimal scope and ensure that remote connection approval procedures are followed and preventive measures are taken to prevent virus infections and information leaks.

## Potential Risks

Remote connection makes it possible to access equipment in the control room (where control equipment or operation terminals are located) from the outside. This could result in virus infections, unauthorized operation, information leaks, or other damage.

## Explanations and Implementation Examples

To manage remote connection, you can implement the following measures.

### (A) Establish rules.

Establish and thoroughly disseminate rules on remote connection.

(1) Define procedures for requesting, approving, and repealing remote connection privileges.

(2) Define connection destination requirements. If necessary, define pre-connection review procedures and Restrictions on connection destination networks (intranet, no connecting to the Internet, etc.), connection equipment, and connection protocols.

(3) Define procedures for regularly reviewing the necessity of each connection and repeal connection privileges for remote connections that are no longer necessary.

(4) Define contract requirements pertaining to connection destination security. If necessary, submit a confidentiality agreement or a signed note of assurance and define response procedures and compensation coverage in the event of a security accident or incident.

(5) Define technical requirements for remote connections. If necessary, define requirements for communication authentication, terminal authentication (use of digital certificates), firewall configuration, account password management, and communication equipment management. In addition, define how logs should be saved to keep records of communication and operations for future verification purposes.

### (B) Minimize the number of connections.

Carefully consider why and for what work remote connections are needed and restrict connection partners, connected devices, connection times, remote object protocols, connection bandwidth (line speed), and connection destination privileges to the minimum necessary.

Examples

(1) Use the MAC address or IP address filter functions of communication equipment (routers, etc.) to restrict which devices can connect.

(2) Use the protocol filter function of communication equipment to allow only necessary protocols.

(3) If the connection does not need to be always available, cut off the physical connection to the line by turning off the power to the communication equipment when it is not in use (This can reduce the risk of attacks from the outside).

(4) Confirm why and for what work the connection is needed, and set operation privileges on the industrial control system to the minimum necessary. Do not grant excessive privileges to remote users (administrative privileges to communication and control equipment, etc.).

### (C) Review communication logs.

Review the logs of communication equipment and control equipment to operate both periodically as well as before and after remote connections are made in order to ensure that all rules are followed, that no unnecessary operation or communication has occurred, and that there are no abnormalities with the equipment or communication. If any problem is discovered, promptly investigate the cause and implement countermeasures.

**References**

- ISO/IEC 27001: A.10 Communications and operations management
- ISO/IEC 27001: A.11.4.2 User authentication for external connections

## 5. Third-party Risk Management

Supplement Question No. 5-1

### Managing Remote Connection Risks

You must assume that a connection destination with only an SLA or contract is outside the scope of management and you must consider all risks and countermeasures.

**Matters to consider**

- Impact and industrial control system security measures in the event the connection destination equipment becomes infected with a virus (Define settings for routers, firewalls, and others to ensure security)
- Impact in the event a person with malicious intent operates the connection destination equipment
- Measures for early detection of abnormal states (monitor communication and connected equipment)
- Risk of information leaks through remote connections
- Impact and response procedures in the event an abnormality occurs with the communication line while work is being done via a remote connection
- Impact and industrial control system security measures in the event the communication line is cut or response speed decreases

### Connecting from a Laptop or Remote Terminal

Although this question focuses primarily on problems and solutions when connecting the industrial control system to outside equipment and services, remote connections may also be used to access and remotely operate or maintain the industrial control system from outside terminals. With the widespread use of mobile devices, in the future there will likely be more systems that can monitor and operate industrial control systems from smartphones. It is advisable to establish security measures and rules for this sort of remote connection if necessary.

# 6. Continuous Evaluation and Improvement (Kaizen)

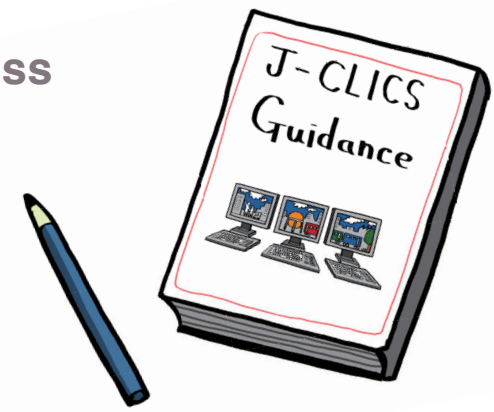
Question No. 6-1

**Do you regularly use J-CLICS (or any other checklist prepared within the company or other industry associations, etc.) to self-assess the control system's security?**

Question No. 6-1

# Do you regularly use J-CLICS (or any other checklist prepared within the company or other industry associations, etc.) to self-assess the control system's security?

In order to maintain and improve security, it is important to regularly perform security self-assessments and update related documents (rules, procedure manuals, management records, etc.) and security measures.




## Background and Purpose

The effectiveness of security measures changes daily as business and organizations change, technology advances, and new attack methods are discovered. Using the PDCA cycle (Plan, Do, Check, Act) to regularly check and make improvements is vital for maintaining the effectiveness of in-place security measures. Advances in technology may also make it possible to select lower-cost measures. Regularly performing self-assessments and reviewing security are important for increasing the efficiency of security and reducing costs.

## Potential Risks

If impractical rules and documents, and new methods of attack are discovered and if obsolete security measures are left unchanged, such measures become a point of weakness and incur attacks and operational confusion. This increases the risk of adverse effects on the industrial control system's operation. Leaving obsolete rules and measures as they are not only makes helpless to the latest attacks but is also a primary reason that unnecessary costs are incurred.

## 6. Continuous Evaluation and Improvement (Kaizen)

Question No. 6-1

### Explanations and Implementation Examples

Regularly perform security self-assessments as well as review and update security measures.

(A) Establish rules.

Establish and enforce rules on regularly carrying out security self-assessments.

(1) Select someone to be responsible for security assessments and reviews.

(2) Determine when to perform self-assessments (yearly, after updating the system, during periodic inspections, at security accidents or incidents, etc.).

(B) Implement security self-assessments.

Use the J-CLICS checklist (or an equivalent checklist prepared in-house or by an industry association) to perform a self-assessment and document the results. Clarify the following matters.

(1) Evaluation results and reasons for evaluation for each checklist item

(2) Countermeasures and their implementation status for each checklist item

(3) For items not yet addressed satisfactorily, the reason why and response plan

(C) Assess and review security measures.

Evaluate and review the details and results of security measures and update them if necessary.

**Examples of what to evaluate**

- Are security measures in place and enforced?
- Are security measures functioning effectively?
- Are the costs of security measures reasonable?
- Is the impact of security measures on work reasonable?
- Are more effective or less expensive measures available?
- Are the rules and content of documents consistent with the current operation, systems, organization, and personnel structure?

**Reference**

- ISO/IEC 27001: A.5.1.2 Review of the information security policy

## 6. Continuous Evaluation and Improvement (Kaizen)

**Supplement** Question No. 6-1

**How to Evaluate Security Measures**

Response time and costs in the event of a security incident or accident and the number of such occurrences can be recorded as an index for evaluating security measures. If no security incident or accident has actually occurred, it may be possible to assess by assuming such incident or accident, investigating the hypothetical damage, response procedure, response time and cost, and comparing the difference between having measures in place and not having them in place.

# Appendix A

## Information Security Reference Materials

### Information Security Reference Materials

The following lists documents and websites where you can learn more about information security.
(Website information (URLs) is current as of January 2013.)

#### 1. References on Information Security

- JPCERT/CC website

  https://www.jpcert.or.jp/english/cs/controlsystemsecurity.html
  https://www.jpcert.or.jp/english/
  Regarding industrial control system security, the following kinds of helpful information on incident response are available.

  Guidelines, standards, and similar documents
  Related tools
  Presentation materials
  Information introducing the information sharing community and other communities
  Security alerts
  Vulnerability-related advisory
  Other information

  You can also use the website to submit a request for consultation from JPCERT/CC on how to respond in the case of an incident.

- JPCERT/CC Information on Industrial Control System Security

  https://www.jpcert.or.jp/ics/ics-community.html (Japanese)
  Information that JPCERT/CC collected and organized, news and trend on the control system security, examples of threats, reference information on standards and rules, etc. are provided to participants of the industrial control system security community.

- Information-technology Promotion Agency (IPA) Website

  http://www.ipa.go.jp/index-e.html
  The IPA website provides information on emergency responses related to information security, materials on information security measures, seminar and event information, notifications and consultation information, and information on software engineering.

- IPA Control System Security

  http://www.ipa.go.jp/security/controlsystem/index.html (Japanese)
  Information on the security of industrial control systems used in critical infrastructure can be found here.

#### 2. Standards and Guidelines

- Information Security Management Guide—JIS X 5080:2002 (ISO/IEC 17799:2000) (Japanese)

  Co-authored by Yoshiyuki Hirano, Masahiro Mizumoto, Kenichiro Yoshida, and the Japanese Standards Association.

- ISO/IEC 17799: 2005 (JIS Q 27002: 2006) Code of Practice for Information Security Management (Japanese)

  Co-authored by Koji Nakao, Yoshiyuki Hirano, Kenichiro Yoshida, Hatsumi Nakano, and the Japanese Standards Association.
  This is the handbook to ISO/IEC 17799: 2005 on information security management. The handbook discusses measures that should be carried out for information security management.

- GOOD PRACTICES GUIDE - PROCESS CONTROL AND SCADA SECURITY

  Prepared by the Center for Protection of National Infrastructure (CPNI). Translated by JPCERT/CC.
  https://www.jpcert.or.jp/ics/information02.html (Japanese)
  In outlining the need for process control and SCADA system security and revealing the difference between process control or SCADA system security and IT security, this guide demonstrates the seven stages to handle process industrial control system security and the principles behind good practices in each stage.

• Japanese Version of SSAT (SCADA Self-assessment Tool)

Developed and created by the Centre for Protection of National Infrastructure (CPNI). Japanese version developed by JPCERT/CC.

https://www.jpcert.or.jp/ics/ssat.html (Japanese)

JPCERT/CC has developed a security self-assessment tool that is focused on monitoring and industrial control systems using SCADA developed by the UK-based CPNI. You can use this tool in conjunction with the Good Practices Guide - Process Control and SCADA Security to obtain a deeper understanding of industrial control system security.

### 3.Vulnerability Information

• Vulnerability countermeasure information portal site: JVN (Japan Vulnerability Notes)

https://jvn.jp/en/

JVN stands for "the Japan Vulnerability Notes." It is a vulnerability information portal site designed to help ensure Internet security by providing vulnerability information and their solutions for software products used in Japan.

• Common Vulnerabilities and Exposures (CVE)

http://cve.mitre.org

This is the vulnerability information website operated and managed by the US-based MITRE Corporation that administers CVE. The website provides information on vulnerabilities found in software. Each vulnerability is assigned a CVE-ID; these IDs are used internationally.

• Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

http://www.us-cert.gov/control_systems/ics-cert/

Operated by the US Department of Homeland Security (DHS), ICS-CERT is an incident response organization that focuses on industrial control systems. The ICS-CERT website provides newsletters, advisories, reports, and other information on industrial control system security.

### 4.Information on Information Security Policies

• Ministry of Economy, Trade and Industry

http://www.meti.go.jp/policy/netsecurity/index.html (Japanese)

This website provides information on security policies from METI. Information on government security policies, various reports, guidelines, and so forth are posted here

• National center of Incident readiness and Strategy for Cybersecurity (NISC)

http://www.nisc.go.jp/eng/index.html

The website of the National center of Incident readiness and Strategy for Cybersecurity posts various conference materials, security-related investigation reports, and information on relevant laws.

• Ministry of Internal Affairs and Communications

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html (Japanese)l

Investigation reports, public relations documents, and other information pertaining to security can be viewed at the information security policy website.

• National Police Agency

http://www.npa.go.jp/cyber/ (Japanese)

On its cybercrime countermeasures website, the NPA posts information on its efforts to prevent and crack down on cybercrime, cybercrime statistics, and how to contact it for a consultation on cybercrime as well as other information.

## Copyright Notice