

Cyber Security First Step for Introducing IIoT to the Factory

-Security Guide for Businesses Implementing IIoT-



JPCERT Coordination Center

August 2018

Table of Contents

Foreword	2
Introduction	3
For Business Owners and Managers	5
IIoT Cyber Security Approach	7
IoT Installation Process: Roles and Responsibility of Third-Party Vendors	9
Elements of IIoT: Cyber Security Navigation Map	13
Securing IoT Devices	14
Securing Intra-Factory IoT Network (LAN).....	16
Securing Server.....	19
Securing External Network (WAN)	22
Securing Cloud Service	23
Glossary	24
References	25

Foreword

With Internet of Things (IoT), Industrial IoT (IIoT), and Industry 4.0, systems and facilities of the factories are now connected with various networks as industrial technology evolves. In the new era of connected technology, cyber security is becoming a new issue, and the production at the factory should not be held due to insecure environment. We hope this document will help securing the IIoT environment.

JPCERT Coordination Center (JPCERT/CC)

Introduction

Industrial Internet of Things (IIoT) are utilized in the production industry for various purposes. For example, IIoT sensors are used for visualizing operating conditions. Other devices are used to analyze operation data and predict malfunction. Analyzed data is used for automated control of the devices.

On the other hand, implementation of IIoT devices connects various devices in the factory with each other. This situation creates new threats, and cybersecurity measures are now a new requirement.

<Possible risks caused by cyber attacks against IIoT devices>

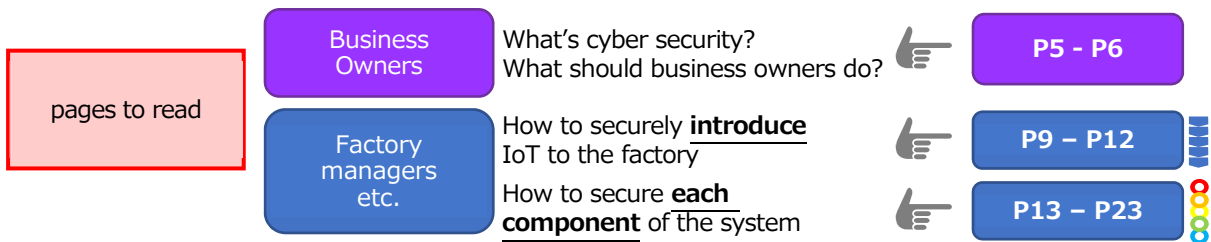
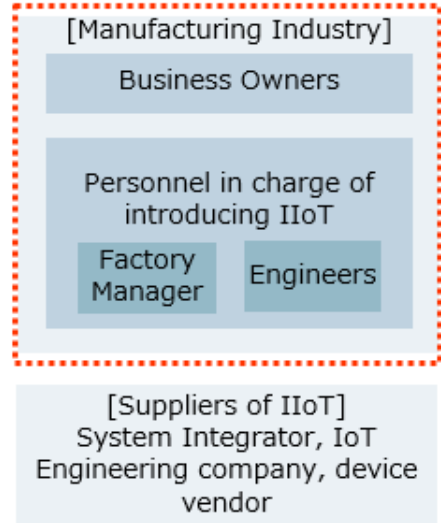
- Factory machines suspended or controlled remotely
- Defective products produced and dispatched based on falsified test data
- Delayed anomaly detection due to altered operation data
- Clients affected by suspended factory operation

Cyber attacks against IIoT devices may impact not only to the company's production and reputation, but also supply chain as a whole.

The Purpose of this document is to provide basic guide to cyber security for introducing IIoT devices to a factory. **Audience** of this document are business owners, factory managers, system administrators, and factory engineers.

This document is focused on basics of cyber security measures for introducing IIoT devices to the factory. For cyber security measures required during operation of the factory after installing IIoT devices, please refer to documents on the reference page. This document can also be used as security requirements of the specification when ordering, for example, construction of an IIoT system.

Audiences



For Business Owners and Managers

IIoT devices are introduced for various purposes in the manufacturing industry.

In the past, cyber security of the facilities was assured by operating devices in the isolated network environments. However, with the introduction of IIoT, this is no longer the case. Various devices are now connected to the network. This increases the risk of cyber attacks from the external environment, and therefore cyber security measures are now needed.

If a cyber attack affects production plan or product quality, the result may be reduced sales or loss of brand reputation.

Case 1 :

In June 2017, a Danish container shipping company A.P. Moller-Maersk was affected by malware (ransomware) NotPetya, which cost Maersk \$200 to 300 mil to recover from the damage.

Case 2 :

In June 2017, a Japanese automobile company suffered from Wannacry infection in one of the factories. Production was suspended until next day.

In addition, it is possible for the malware (virus) that affected a system to spread out to business partners' systems. An asset owner can fall a victim, and inadvertently, a steppingstone for another attack. There are cases where the companies require their business partners to practice cyber security measures as part of their contract.

It is possible that, in the future, factories of the supply chain are connected by IIoT or other technologies, allowing production of each factory to be monitored and controlled automatically. When this happens, the companies not meeting the cyber security requirement of the supply chain may not be allowed do business in the supply chain.

It is crucial that the cyber security countermeasures are implemented with IIoT devices when they are installed. Additional cost may be necessary to implement cyber security measures later, especially after once the operation has started due to necessity for changing the environment.

It is important for the business owners and managers to be aware that the cyber security measures are the important element of investment when introducing IIoT devices to the factory. It is recommended to ensure any required resources

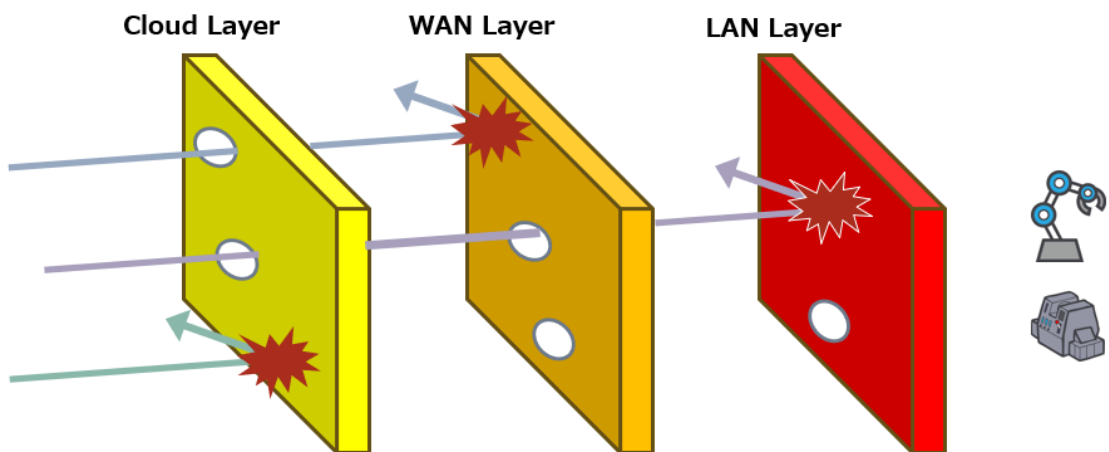
(budget, personnel, etc.) and assign personnel in charge to conduct adequate cyber security measures. This document can be used as one of the references when doing so.

IIoT Cyber Security Approach

Layered protection is the essential for IIoT. IIoT devices have limited functions and capacities, and therefore security measures that can be taken on these devices are limited. Considering that IIoT devices have a long life cycle, assuring individual protection for the devices is not enough to mitigate the risks.

Layered protection is effective not only for the IIoT devices, but also for the networks that the IIoT devices are connected to. Many cyber attacks can be prevented by protecting each network layer, such as cloud layer, WAN layer, Intra-factory IoT network layer, and device layer.

However, there are still possibilities of advanced and persistent attacks which exploit unexpected security holes. In addition to layered protection, it is also important to be ready to detect and investigate anomalies (e.g. support from security vendors).



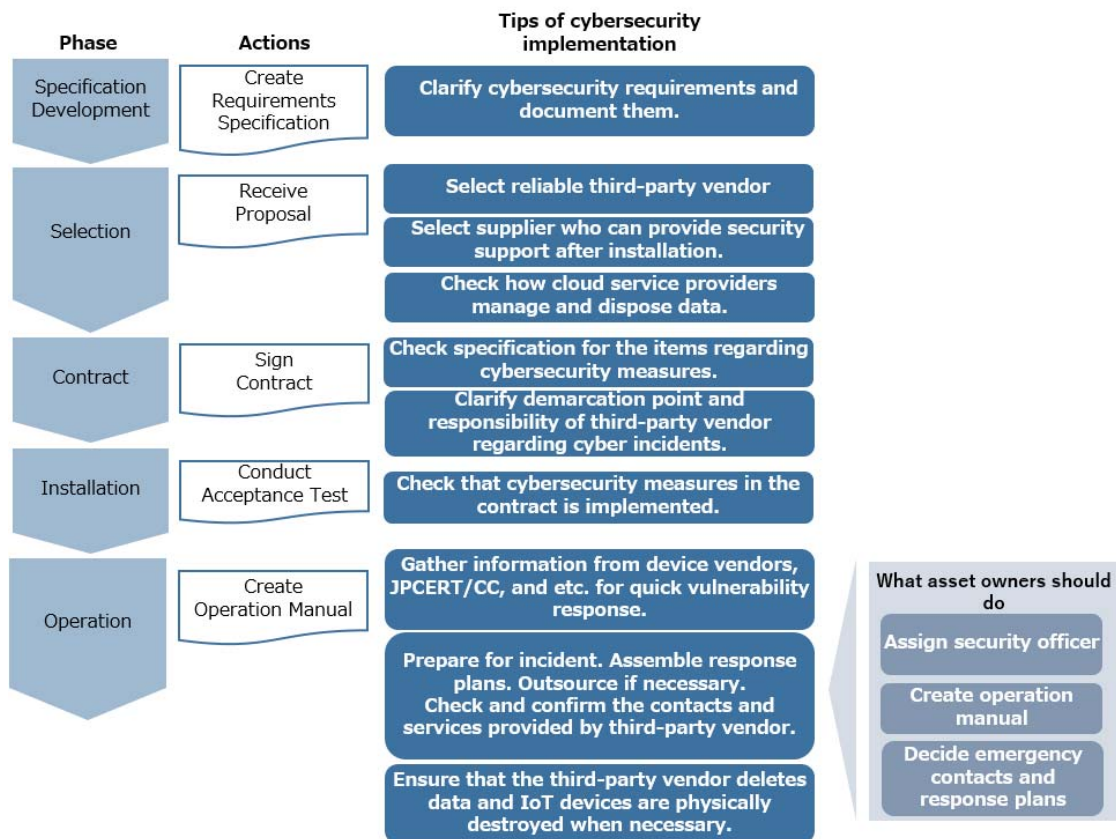
Entry point of the threats depend on the network structure. It is important to consider the network structure and decide which cyber security measures need to be prioritized.



Protection and assuring data and validity of analysis results are important for **“IoT connected within a company”** where the operational data and production control data are analyzed and feedbacked to factories for the purpose of efficient production. In addition, for the **“IoT connected with external partners”** where different companies and organizations create a supply chain and process chain for manufacturing and maintenance of products comprised of large number of parts, it is also important to assure the reliability of the partner(s).

IoT Installation Process: Roles and Responsibility of Third-Party Vendors

When introducing the IIoT to the factory, cyber security measures must be prepared in each step of the introduction process. Cyber security requirements should be discussed and included in the specification when purchasing devices, systems and services from third-party vendors (e.g. systems integrator, hardware vendor, cloud service provider). Check that the cyber security measures are implemented by the third-party vendor. Roles of the third-party vendor and the services provided during the operation phase should be clearly stated.



P – 1 Specification Development

1. Clarify cyber security requirements

When creating a requirement specification, specify “what must be protected (e.g. data, availability)” on the existing system and on new IIoT system, and summarize security measures to be taken depending on the device usage and system structure. The required specification must be documented and presented to the third-party vendor¹.

P – 2 Selection

1. Select a third-party vendor

Select a reliable third-party vendor who can provide strong support. Choose a reliable company that is third-party certified (e.g. ISMS, CSMS), has cyber security practices disclosed, and clearly states security support policies.

2. Select hardware

Select a vendor that provides long support period since IIoT devices are likely to have long life cycle. Also, before introducing IIoT devices to the environment, consider whether device replacement is necessary at the end of supported life cycle.

3. Select a cloud service

Select a cloud service vendor who performs adequate cyber security measures to prevent data breaches and falsification. Also make sure that they manage the data properly and all data will be deleted at the end of the service.

P – 3 Contract

1. Document requirements

Cyber security requirements must be documented in the contract with the third-party vendor. Security support period and summary of services should be documented on the maintenance contract of the IIoT devices.

2. Clarify demarcation point and responsibility

Identify the demarcation point and responsibility and make provision for the security incidents that happened to, was caused by, and affected the third-

¹ Recommended reference for stating security requirements.

“Non-Functional Requirements Grade Usage Guide” by IPA

<https://www.ipa.go.jp/files/000028844.zip>

party vendor. Document it in the contract, including how the third-party vendor is responsible for losses and damages to their business partners.

P – 4 Installation

1. Implement cyber security measures

Conduct an acceptance test when system is delivered. Thoroughly inspect and confirm that all cyber security measures stated in the contract is implemented. Check with the third-party vendor if there is anything unclear.

P – 5 Operation

1. Assign a cyber security officer

Management executives must assign a cyber security officer, with adequate authority and resource, to keep the level of cyber security. Cyber security measures need constant review and updates to correspond to changes in business and new threat.

2. Create operation manual

Include important cyber security subjects in the operation manual².

3. Train employees

There are cases where operators at the factory have little or no knowledge of IT. When introducing IIoT to a factory, train the operators with basic knowledge of IT, IIoT, and cyber security.

4. Manage IoT devices (assets)

Gather information routinely from device vendors, JPCERT/CC, and other sources to quickly respond to cyber security risks such as vulnerabilities and to identify what should be protected. Also, prepare and use the list³ of IoT

devices with their model number, software version, and support period for routine inventory. In addition, given that cyber security related operation (e.g. anti-theft measures, measures for unauthorized use, applying patches, checking logs, etc.) and settings of IoT devices require routine review,



² Recommended reference for creating operation manual.

“Guideline for Security Operation of Control System” by NECA

https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline_en.pdf

³ Recommended reference for creating list of assets for inventory.

“J-CLICS Step2” Chapter 1 by JPCERT/CC

https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline_en.pdf

decide how often they should be reviewed.

5. Prepare for incidents

Structure the operation so that communication logs and IoT device logs are checked regularly. This enables early stage detection of incidents. Quick response is the key to reducing loss or damage caused by the incident. Prepare incident response plan and procedures in advance. Third party commission may be a choice if an asset owner does not have enough resource.

When recovering from the incident or investigating the cause of the incident, manager of the factory should be able to cooperate with other departments of the company, such as persons in charge of IT and cyber security.

Also, identify the emergency contacts and specific supports that are available from third-party vendors such as system integrator and cloud service vendor.

6. Dispose data

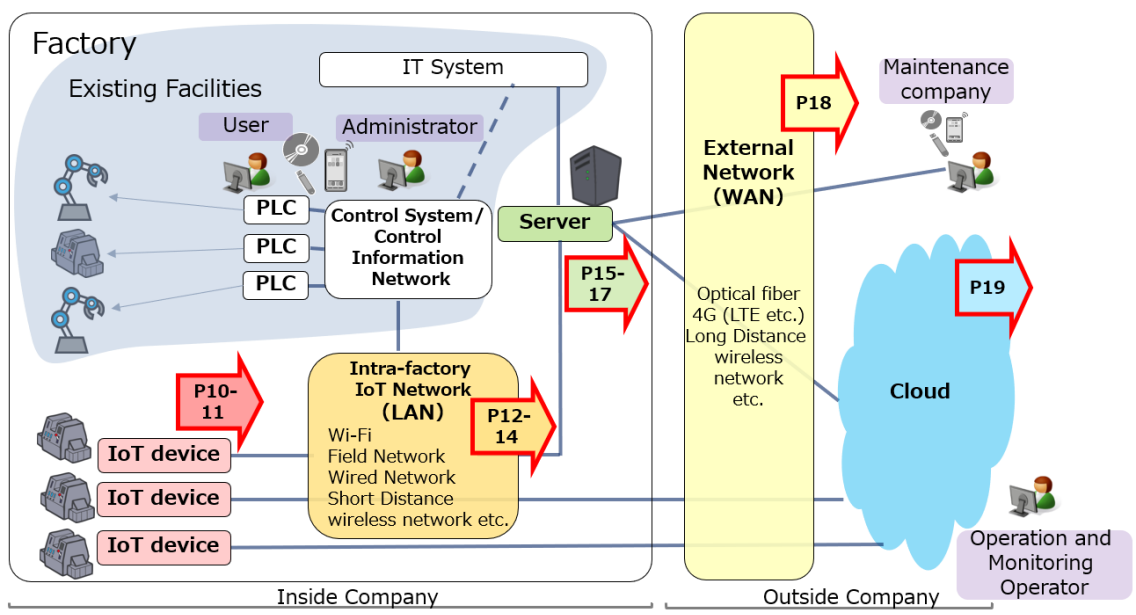
Credentials and other data left on disposed IoT devices can be leveraged for cyber attacks or unauthorized use by a third party. To prevent such incidents, make sure that all data are deleted from devices and cloud servers or have devices physically destroyed. This should be included in the operation manual.



If a cyber attack occurs, the affected company will be questioned of its management responsibility for cyber security, by its customers, business partners, and perhaps from society. Keep a record of conducted cyber security measures and store log data so that they can be used as evidence.

Elements of IIoT: Cyber Security Navigation Map

The diagram below shows the elements of a typical IIoT system. Please refer to the pages which correspond to each element.



Navigation Map

- Securing IoT Devices
p.10-11
- Securing Intra-Factory IoT Network (LAN)
p.12-14
- ※Connection with Control Systems and Control Information Systems included in this part.
- Securing Server
p.15-17
- Securing External Network (WAN)
p.18
- Securing Cloud Service
p.19

Securing IoT Devices

Possible risks of insecure IoT devices

- An unauthorized insider may physically access an IoT device and steal sensitive data such as production data and technical information. Information leakage or unauthorized data transmission to other machines due to operational error is possible, too.
- Malicious programs may intrude into a factory's internal network during maintenance and exploit vulnerabilities of IoT devices, which leads to data falsification, data deletion, or IoT device failure.


D - 1 Choose IoT devices with security features

Choose the IoT devices with security features, since it will be difficult to implement security measures to IoT devices after system introduction.

Specific examples	<ul style="list-style-type: none"> ● Choose IoT devices with security features. This may include products that are designed to be secure, products that are vulnerability tested, and products with functional safety. ● Choose IoT devices which are supported by vendor or manufacturer after installment.
-------------------	--

D - 2 Change default username and password

Default username and password of the devices can easily be found. They are most likely to be in the user's manuals available from vendors and manufacturers, which can be found on the Internet. Therefore, default credentials must be changed when introducing the device to the factory.

Specific examples	<ul style="list-style-type: none"> ● Change default username and password. ● Enable authentication feature for accessing configuration screen of the IoT devices. ● Use strong password⁴. 	
-------------------	---	---

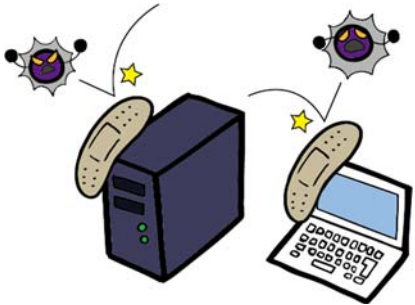
⁴ More than 8 characters with letters, numbers, and symbols. (NECA, "Guideline for Security Operation of Control System")

https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline_en.pdf

At least 10 characters with upper case letter, lower case letter, number, and symbol. (NISC "Information Security Handbook for Network Beginners") https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf

D - 3 Manage vulnerabilities of the IoT devices

Vulnerability management is important because vulnerabilities can be exploited to cause malware infection or unauthorized access. Carefully consider the vulnerability management especially when IoT devices are directly connected to the Internet.

Specific examples	<ul style="list-style-type: none"> ● Update software to the latest version upon implementation. ● Vulnerabilities are discovered constantly. Prepare maintenance plans to update the software during operation. ● If vulnerability responses cannot be conducted regularly on the system, investigate workarounds and mitigation, clarify the risk in case of exploit, and plan how to handle the incident. 	
-------------------	--	--

D - 4 Take anti-theft measures

Physical anti-theft measures must be taken, since many IoT devices are small and easily carried.

Specific examples	<ul style="list-style-type: none"> ● Attach wire-locks to IoT devices. ● Keep IoT devices in the locked cabinet.
-------------------	--

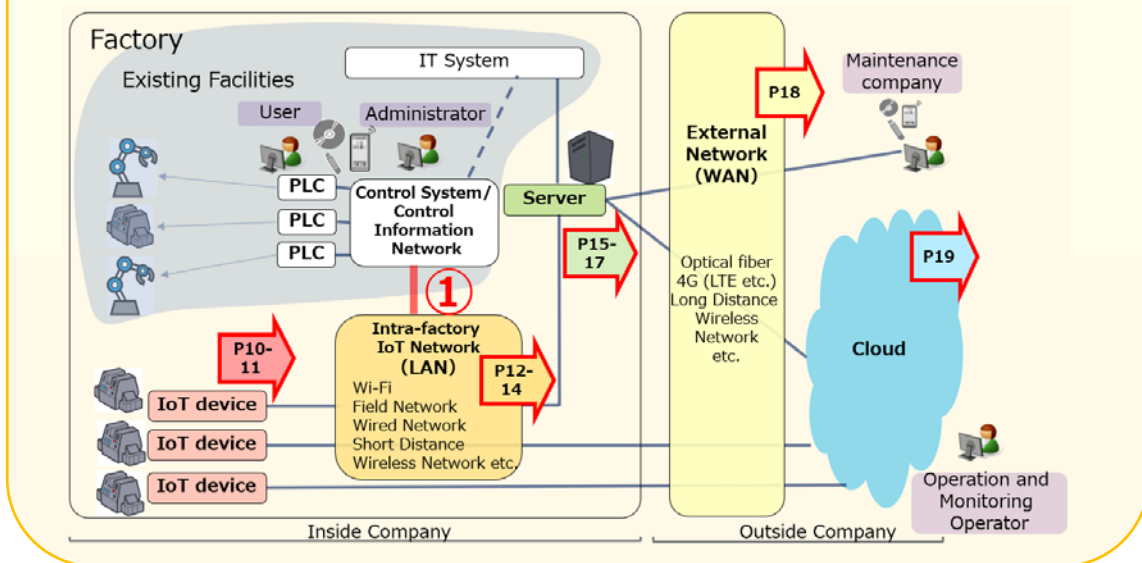
D - 5 Manage IoT devices and peripheral devices

External storage devices must be secured. There are cases where malware infection was caused via USB flash drives in the factory facilities.

Specific examples	<ul style="list-style-type: none"> ● List, record, and manage the peripherals such as USB flash memory used in the factory. These peripherals must be kept in the locked cabinet. ● Check external storage device with anti-virus software. Use USB flash drives that can be scanned for malware. ● Physically block the USB and serial ports and disable them.
-------------------	--

Securing Intra-Factory IoT Network (LAN)

Point When connecting the factory's IoT network with existing control system network (see ① in the figure below), it should be done with extreme caution. In most cases, the devices in the control system network are vulnerable. They are usually either isolated or have strictly limited communication to keep them secure. However, IIoT is expected to be used with the Internet connection such as external cloud service. This has potential for intrusion from external network, which can result in the factory operations being delayed or suspended.



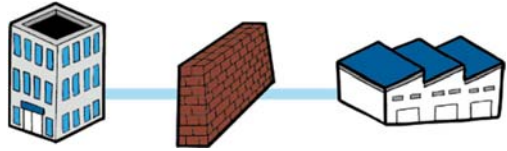
Possible risks of insecure intra-factory IoT network (LAN)

- Malware can enter LAN and intercept communication data. This could lead to leakage of production data and technical information.
- Malware can spread to LAN and manipulate communication data. This could lead to error in analyzed data, which can cause operators to misjudge the situation or cause malfunction of the control system.
- Malware infection of an IoT device can spread via LAN and increase damage.

L - 1 Limit communication between networks to minimum


Office PCs have higher risks of malware infection since they are connected to external network to send/receive e-mails and browse websites. Therefore, it is crucial to separate IT network (business network) from intra-factory IoT network. If it is necessary to connect these networks for any reason,

security measures must be placed at the boundary of IT and intra-factory IoT networks.

<p>Specific examples</p>	<ul style="list-style-type: none"> When connecting IT (business) network with intra-factory IoT network, install a router or firewall between these networks and allow only communications that are necessary. Do not forget to review these settings when there is any change in the system. 
--------------------------	---

L - 2 Change default username and password

There are cases where default username and password are written in the manuals provided by manufacturers or vendors, which are available to the public. Default username and password must be changed when installing the device.

<p>Specific examples</p>	<ul style="list-style-type: none"> Change the default password of the network devices when installing them. If the device supports authentication for accessing configuration screen, enable it. Also, disable access to authentication screen from WAN. Choose a strong password⁵. 
--------------------------	--

L - 3 Limit access to the network devices

It is essential to avoid access from unauthorized devices to the network, since risk of sniffing and manipulating communication increases with unauthorized devices connected to network.

<p>Specific</p>	<ul style="list-style-type: none"> Physically block the unused ports of the network devices.
-----------------	---

⁵ More than 8 characters with letters, numbers, and symbols. (NECA, "Guideline for Security Operation of Control System")

https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline_en.pdf

At least 10 characters with upper case letter, lower case letter, number, and symbol. (NISC "Information Security Handbook for Network Beginners")

https://www.nisc.go.jp/security-site/campaign/files/aj-sec/handbook-all_eng.pdf

examples	<p>Also have them disabled by configuration.</p> <ul style="list-style-type: none"> ● Check physical ports (e.g. serial port, console port) of the network devices on a regular basis to make sure that unnecessary devices are not connected. ● Network devices can be configured to enable services such as SSH and SFTP for management and maintenance. Enable only services that are required. ● Configure the network devices so that the radio waves are transmitted only to an appropriate area. (Avoid placing any access point near the window, adjust transmit power, etc.)
----------	--

L - 4 Encrypt wireless network

It is easy to intercept wireless network. Secure communication such as encrypted communication should be used in order to protect sensitive information from leakage.

Specific examples	<ul style="list-style-type: none"> ● Encrypt wireless network. Choose most secure encryption method and protocol available on the device.
-------------------	--

L - 5 Detect anomaly and monitor the intra-factory IoT network

Monitor intra-factory IoT network communication to enable quick response to anomaly.

Specific examples	<ul style="list-style-type: none"> ● Monitor network communication and send alerts when an anomaly is detected. Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) as needed.
-------------------	--

○ Securing Server

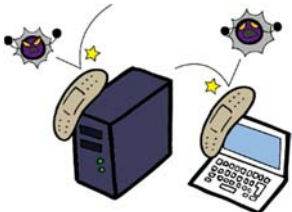
Servers may be installed to IIoT network to avoid delay in communication with external network (e.g. cloud service) or to enable fast and complicated application processing by having the server to process them instead of IoT devices.

Possible risks of insecure server

- Data may be stolen or deleted as a result of unauthorized access.
- Malware may be installed on the server. Data might be altered or program might be overwritten, affecting operation of the factory.


S - 1 Apply vulnerability countermeasures to servers

Vulnerability countermeasures are crucial since vulnerabilities can leverage unauthorized access or malware infection. Plan regular maintenance and consider how to apply patches.

Specific examples	<ul style="list-style-type: none"> ● Apply patches upon installation so that OS and applications are operating at their latest version. ● Vulnerabilities are found constantly. Provide vulnerability response procedure to test for possible effects of the patches on the system before applying patches. Apply patches on a regular basis. Plan and provide methods for gathering information on patches and applying patches. 	
-------------------	---	---

S - 2 Change default username and password

Default username and password are most likely to be found in the manuals available from vendors and manufacturers, which are available to the public. Username and password must be changed when introducing a server to the factory.

Specific examples	<ul style="list-style-type: none"> ● Change username and password of server and server applications when installing them to the system. ● Choose a strong password. 	
-------------------	---	---

S - 3 Manage user accounts and privileges

Restrict each user account to least privileges (e.g. creating accounts and folders, read/write/delete data) required. This will reduce the risk of unauthorized access.

Specific examples	<ul style="list-style-type: none"> ● Limit privileges of each account to minimum features required. ● Allow minimum users with administrator and root privileges. ● Check and revise user account privileges periodically as part of operation. Change or delete privileges of the accounts, depending on how the accounts are used. Delete user accounts that are not used. ● Configure account lockout feature. For example, lock out the accounts which failed to login certain number of times.
-------------------	---

S - 4 Secure external storage devices

Peripherals including USB flash drives must be secured. There are cases of malware infection via external storage devices such as USB flash drives. Since external storage devices are used in IoT environment, they must be kept secure.

Specific examples	<ul style="list-style-type: none"> ● List, record, and manage the peripherals such as USB flash memory used in the factory. The peripherals must be kept in the locked cabinet. ● Check external storage devices with anti-virus software or use the devices that can be scanned for malware. ● Consider using tools and software which restrict usage of USB flash drives to only those permitted. ● Physically block USB ports that are unused.
-------------------	---

S - 5 Disable unused ports and services

Risk of unauthorized access can be reduced by disabling unused physical ports, logical ports, and services of server.

Specific examples	<ul style="list-style-type: none"> ● Unused physical ports (e.g. LAN, USB, serial) must be physically disabled, for example, by using blocker. ● Configure OS to disable services that are not necessary for operation (e.g. FTP).
-------------------	--

S - 6 Check logs on server routinely

A server, which is continuously running, can be a foothold for attackers. Some servers have higher priority set to keep them operating, rather than having their vulnerabilities patched. Such unpatched servers may already be penetrated. Early detection of unauthorized access can be expected by routinely checking the server logs.

Specific examples	<ul style="list-style-type: none"> ● Configure server to retain logs when installing. Compress files to save disk space if necessary. ● Check logs routinely. Consider outsourcing it if necessary. ● Store half to one-year of logs in a separate storage such as DVD-ROM. ● Configure to have alert sent to person in charge when anomaly is observed.
-------------------	--

S - 7 Protect servers from malware

Anti-virus measures are essential for prevention, early detection, and quick response to malware infection via USB flash drives and external network. Potential damages caused by malware can be minimized.

Specific examples	<ul style="list-style-type: none"> ● Install anti-virus software to detect and remove malware. If blacklist-based anti-virus software is used, keep it up to date. When updating the software or pattern list, use a secured USB flash drive that is checked that it is safe.
-------------------	--

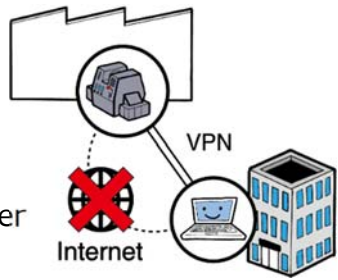
○ Securing External Network (WAN)

Possible risks of insecure external network

- Information may be leaked by an unauthorized access to intra-factory network from the Internet.
- Communication with cloud service may be interrupted by DDoS attack to router, firewall, and other gateway devices.

W - 1 Choose secure connection to external network

It is important to keep the Internet usage to minimum to reduce the risk of attack from WAN.

Specific examples	<ul style="list-style-type: none"> ● Use VPN or dedicated line (including LTE) for connection with external network. ● Apply strict firewall and router filter settings if Internet VPN is in use. 	
-------------------	--	--

W - 2 Restrict communication between internal and external network to minimum

As in common IT systems, it is essential to restrict communication between LAN and WAN to minimum to prevent information leakage or unauthorized access from outside.

Specific examples	<ul style="list-style-type: none"> ● The communication between internal and external network must be restricted to minimum, for example, by using firewalls and routers. Configure firewall and routers so that only necessary communication, such as communication to cloud service or communication for remote maintenance, are allowed. For example, communication from external network should be limited only to remote maintenance purposes. Communication to external network should be limited to specific cloud service. ● If permanent connection between external and internal network is not required, connect them only when needed. For example, if the communication with cloud service is only required during operating hours, turn off the communication device during closed hours.
-------------------	--

Securing Cloud Service

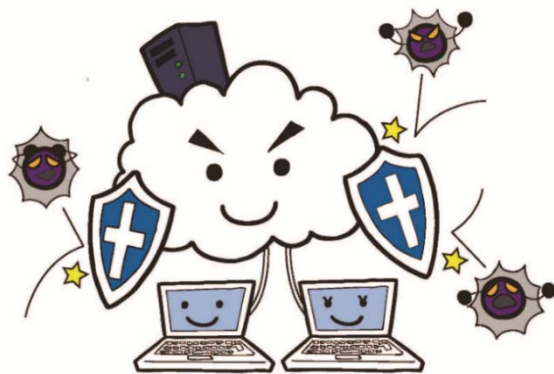
Possible risks of insecure cloud service

- Cyber attacks against the cloud server may result in information leakage and falsification of data on the cloud server.
- Cloud service disruption can affect the factory operation, such as being unable to process data obtained from IoT devices at the factory.

C - 1 Check security policy of the cloud service

Inappropriate management of cloud server, including unpatched vulnerabilities, can lead to cyber attacks via cloud service, which has risk of affecting operation of the factory. Cyber security measures and policies of the cloud service providers must be checked by users independently.

Specific examples	<ul style="list-style-type: none"> • Check the cloud service provider’s whitepaper, policy, contract, etc. to see if they have adequate cyber security measures. Third-party certifications such as ISMS Cloud Security Certification will be a useful reference, too. • When using a cloud service, use fixed IP address service. Configure communication equipment at the factory so that it only communicates to designated IP addresses, in this case, a fixed IP address of the cloud service, and discard external connection requests as necessary. • Check logs routinely to detect any anomaly in the cloud service. Use alert notification service as necessary.
-------------------	---



Glossary

Term	Definition
CSMS	Cyber Security Management System. Cyber Security management system policies and procedures for Industrial Control Systems based on IEC 62443-2-1.
DDoS attacks	Distributed Denial of Service attack. Cyber attacks which cause denial-of-service status by sending massive or malicious packet to network devices and servers.
Firewall	A device installed between two different networks which separates communication that is allowed and blocked.
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
Internet VPN	Virtual Private Network. Method of virtually creating an environment equivalent to dedicated line on the Internet.
ISMS	Information Security Management System Policies and procedures for managing an organization's sensitive data, standardized as ISO 27001.
LAN	Local Area Network. Network within a site.
VPN	Virtual Private Network. Method of virtually creating an environment equivalent to dedicated line on the Internet or a closed network.
WAN	Wide Area Network. Network which connects geographically remote sites.
Vulnerability	Security holes that software and hardware has
Security by Design	Planning and designing by expecting cyber security risks and insuring mitigation.

References (as of August 2018)

[IoT in general]

- IoT Acceleration Consortium, IoT Security Working Group “IoT Security Guideline Ver 1.0” (April 2017) [English]
http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf
- National Center of Incident Readiness and Strategy for Cybersecurity (NISC), “General Framework for Secure IoT systems” (August 2016) [English]
https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

[IoT developers]

- Information-technology Promotion Agency (IPA), “IoT Safety/Security Development Guidelines 2nd ed.” (September 2017) [English]
<https://www.ipa.go.jp/files/000053920.pdf>
- IPA “Guidance for Designing Security in IoT Development” (December 2017 revision) [Japanese]
<https://www.ipa.go.jp/files/000052459.pdf>
- IPA, “IoT Safety/Security Design Tutorial” (July 2016) [English]
<https://www.ipa.go.jp/files/000053921.pdf>

[IoT users (factory)]

- Ministry of Economy, Trade, and Industry (METI), “CPS/ IoT Security Response Manual” (March 2017) [Japanese]
http://www.meti.go.jp/policy/mono_info_service/mono/smart_mono/H28SmartFactory_DataProfile_Security_Report.pdf
- METI/NEDO “IoT Security Response Manual Industrial Safety Version” (April 2018) [Japanese]
http://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/security_manual.pdf

[Industrial Control System]

- SICE/JEITA/JEMIMA/JPCERT Coordination Center “J-CLICS” (December 2016) [English]
J-CLICS Guidance Step1
https://www.jpCERT.or.jp/english/cs/J-CLICS_STEP1_guide_en.pdf
J-CLICS Check List Step1
https://www.jpCERT.or.jp/english/cs/J-CLICS_STEP1_checklist_en.pdf

J-CLICS Guidance Step2

https://www.jpCERT.or.jp/english/cs/J-CLICS_STEP2_guide_en.pdf

J-CLICS Check List Step2

https://www.jpCERT.or.jp/english/cs/J-CLICS_STEP2_checklist_en.pdf

- Nippon Electric Control Equipment Industries Association (NECA) “Guideline for Security Operation of Control System” (August 2013) [English]
https://www.neca.or.jp/wp-content/uploads/control_system_security_guideline_en.pdf

[Small and Medium Businesses]

- IPA “Information Security Guideline for SMB 2.1 ed” (January 2017) [Japanese]
<https://www.ipa.go.jp/files/000055520.pdf>

Copyright Notice

The copyright of this document is owned by JPCERT/CC.

If you wish to quote, reproduce or re distribute the document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp).

JPCERT/CC shall not be responsible for any loss or damage caused in relation to the information of this document.