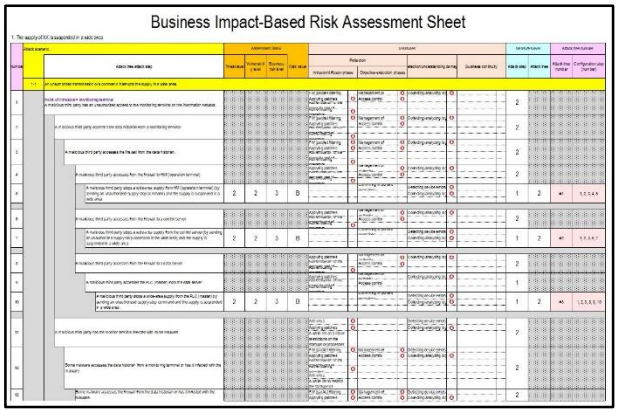
IPA Better Life with IT



Security Risk Assessment Guide for Industrial Control Systems

Quick Guide, 2nd Edition

Information-technology Promotion Agency, Japan
IT Security Center (ISEC)

October 2019

Security Risk Assessment Guide for Industrial Control Systems (ICS) - 2nd Edition

”Guide” and “Practical Example”

【Table of Contents】

1. Role and Importance of Risk Assessment in Security
2. Overview and Procedure of Risk Assessment
3. Preparing for Risk Assessment (1)
   - Deciding Assessment Objects -
4. Preparing for Risk Assessment (2)
   - Risk Value, Evaluation Factors and Criteria -
5. Conducting Risk Assessment (1)
   - Asset-based Risk Assessment -
6. Conducting Risk Assessment (2)
   - Business Impact-based Risk Assessment -
7. Interpreting and Utilizing Risk Assessment Results
8. Security Test
9. Additional Criteria for Specific Security Controls

Reference, Appendixes

2nd Edition published in Oct. 15, 2018

Guide

380 pages

Practical Example

94 pages

Download available at : https://www.ipa.go.jp/security/controlsystem/riskanalysis.html (in Japanese only)

Role and Importance of Risk Assessment
～Effective to Maintain and Improve Security of ICS～

「Risk Assessment」: Process to clarify the risk level using ①②③ as the evaluation factor

① Importance (value) of assessment objects (assets and businesses), magnitude and impact of potential consequence
② Supposed threat to assessment objects and its likelihood of occurrence
③ Susceptibility to the potential threat when it occur (vulnerability to the threat)

Process		Definition in ISO/IEC 27000:2018（JIS Q 27000:2019）
Risk Assessment		Overall process of risk identification, risk analysis and risk evaluation
	Risk Identification	Process of finding, recognizing and describing risks
	Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk
	Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
Risk Treatment		Process to modify risk

Importance and Effectiveness of Risk Assessment

- Achieve effective risk reduction
- Enable effective investment（additional security controls, identifying what and where to test for testing to be effective）
- Provide a foundation for PDCA cycle and continual security enhancement

Risk Assessment Methods and Challenges
～Various Methods and Issues～

Risk Assessment Methods

Assessment Methods			Estimated Man-hour	Effectiveness
Baseline Approach (checklist-based)			Small	△
Informal Approach (knowledge and experience-based)			Small	×？
Detailed Risk Assessment	Asset-based		Medium	○
	Scenario-based	Attack Tree Analysis（ATA）	Large	○
		Fault Tree Analysis（FTA）	Large	○
Combined Approach			Large	◎

What makes Detailed Risk Assessment challenging ?

- ”I don’t know any specific method or procedure of risk assessment.”
- ”I’ve heard risk assessment requires a lot of man-hours but I’d like to avoid it.”

➡ The Guide will give you answers to these problems.

Two Types of Detailed Risk Assessment

Asset-based and Business Impact-based Risk Assessment

★ Asset-based Risk Assessment

Conduct risk assessment for each asset (server, operator HMI, network device, etc.) which makes up ICS using three evaluation factors, ‘importance (value)’, ‘threat’ and ‘vulnerability’.

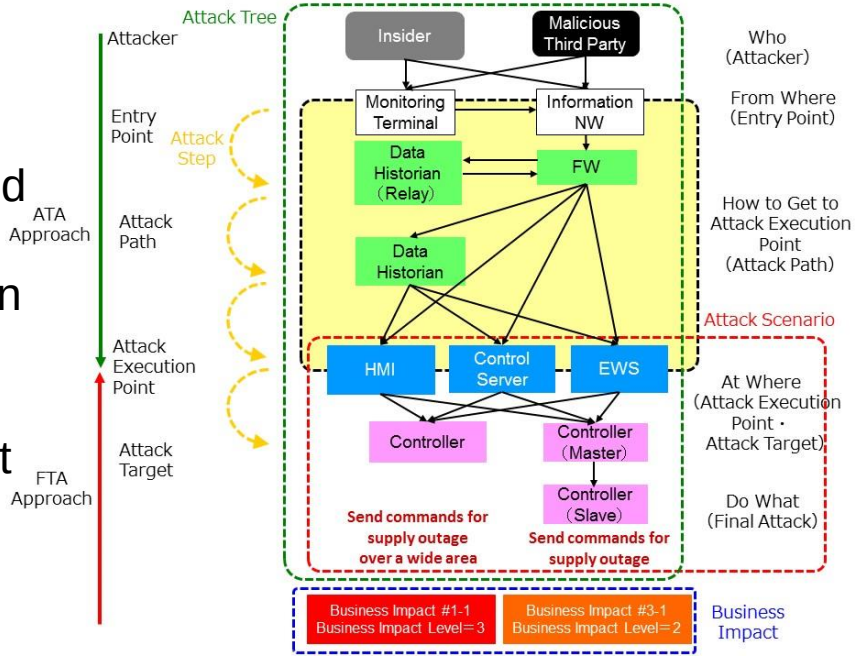
⇒ Enable to comprehensively evaluate threats against and security status of assets.

★ Business Impact-based Risk Assessment

Conduct risk assessment for business (service and functions) realized by ICS. Define the business consequences to be avoided and brainstorm attack scenarios and trees that could cause the consequences, then analyze their risk using three evaluation factors, 'business impact', 'threat', and 'vulnerability’.

⇒ Enable to evaluate a chain of attacks that lead to business consequence.
(Fusing ATA and FTA advantages)

⇒ Desktop Penetration Testing

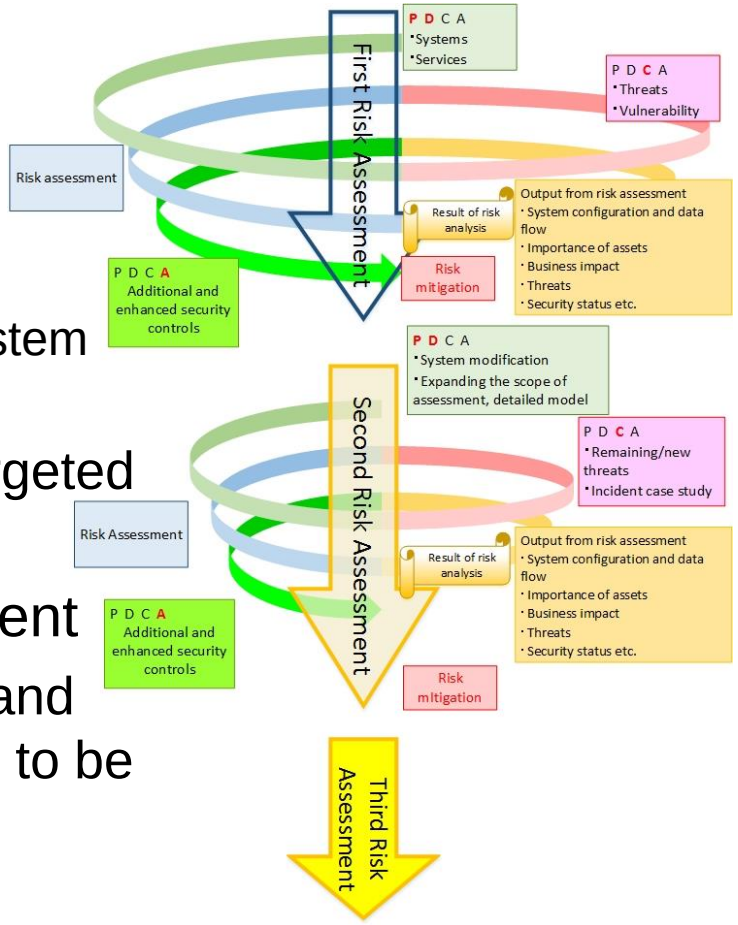


1. Role and Importance of Risk Assessment in Security

Guide
p.16-23

Explain the Role, Importance, and Necessity of ICS Risk Assessment

- Necessity of Securing ICS
  - Change in systems and components
  - Connection with external networks, use of storage media to transfer data
  - Characteristics of ICS (e.g. long device/system life expectancy)
  - Surge of reports about vulnerabilities, targeted cyberattacks, malware infections, etc.
- Role and Importance of Risk Assessment
  - A process to identify the level of threats and impacts to the systems and the business to be protected .
  - Imperative to secure ICS

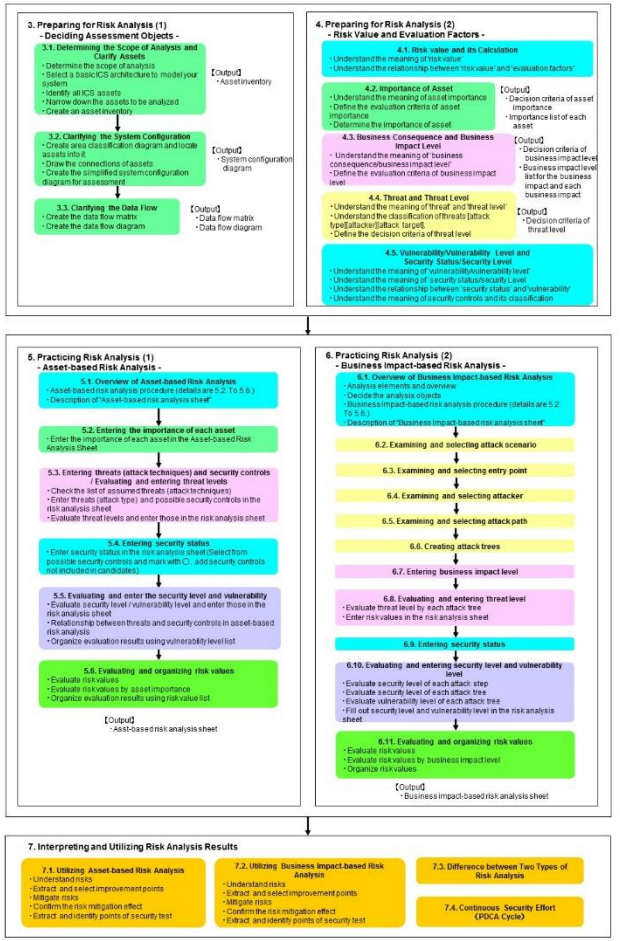


2. Overview and Procedure of Risk Assessment

Guide p.24-41

Introduce Risk Assessment Methods and How to Use this Guide

- Overview of Risk Assessment
  - Baseline Approach
  - Informal Approach
  - Detailed Risk Assessment
  - Combined Approach
- Procedure of Detailed Risk Assessment
  - Asset-based Risk Assessment
  - Business Impact-based Risk Assessment
- How to Use The Guide
  - Structure of this guide
  - Recommendations for conducting risk Assessment



3. Preparing for Risk Assessment (1)
～Deciding Assessment Objects～

IPA

Guide
p.42-43

Know Yourself : Analyze and Understand Your ICS

【Preparatory Works and Outputs】

Section	Preparatory Works	Outputs
3.1	• Determine the scope of assessment and specify assets	• Asset inventory
3.2	• Clarify the system configuration (including network configuration)	• System configuration diagram
3.3	• Clarify the data flow	• Data flow matrix • Data flow diagram

3. Preparing for Risk Assessment (1)

3.1. Determining the Scope of Assessment and Specify Assets

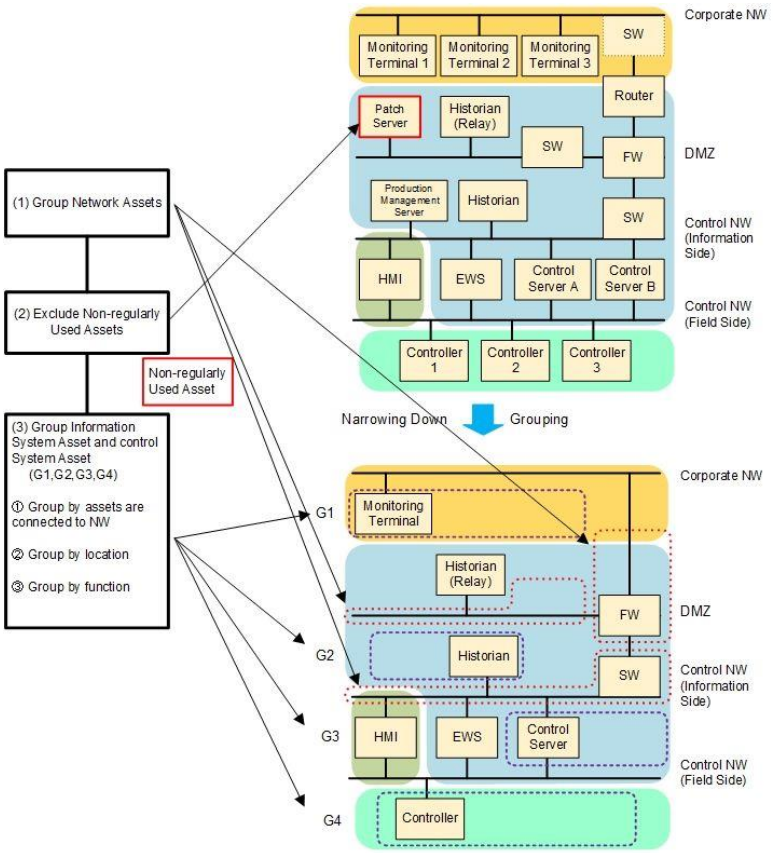
Guide p.44-62

- Determine the scope of assessment
- Select a basic ICS architecture (ref: NIST SP800-82) to model your system
- Identify all ICS assets
- Narrow down the assets to be analyzed
- Create an asset inventory

【Asset Inventory】

No.		1	2	3	4	5	6	7	8
Asset		Monitoring Terminal	Firewall	DMZ	Data Historian (Relay)	Controll Server	EWS	Controller (Master)	Field NW
Asset Type	Informatin System Asset	○	○		○	○	○		
	Control System Asset							○	
	Network Asset			○					○
Function	Data Input / Output	○					○		
	Data Storage				○				
	Command Issuance	○				○	○	○*1	
	Gate		○						
Type of Network				LAN					Leased Line
Location		Control Room	Server Room	Server Room	Server Room	Server Room	Server Room	Field	Filed
Connected NW	Corporate NW	○	○						
	DMZ		○		○				
	Control NW(Information Side)		○			○	○		
	Control NW(Field Side)					○	○	○	
	Others								
Connected NW of Management Port		×	Corporate NW	×	×	×	×	×	×
Operation I/F		○	×		○	○	○	×	
USB Port／Communicatin I/F		○(USB)	○(LAN)		○(USB)	○(USB)	○(USB)	○(USB)	
Regularly-used external media		×	×		×	×	○	×	
Wireless Function		×	×	×	×	×	×	×	×
Regularly-used／Non-regularly used		Regularly	Regularly	Regularly	Regularly	Regularly	Regularly	Regularly	Regularly
Data Type / Data Path		Described in Data Flow Matrix							
System Vendor／Device Manufacturer		ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/HH	ABY/CCJ
OS／Version		Windows	Proprietary		Windows	Windows	Windows	Proprietary	
Protocol		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP,Proprietary	TCP,UDP	Proprietary	Proprietary
Security Controls		Described in Asset-based Analysis Sheet							

【Example of Asset Narrowing Down Procedure】

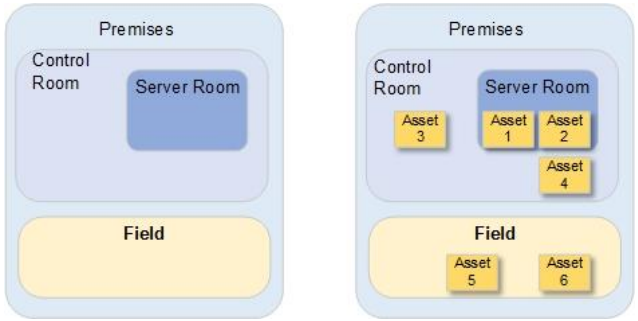


3. Preparing for Risk Assessment (1)

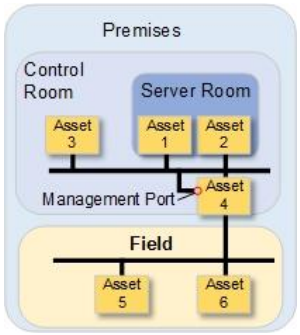
3.2. Clarifying the System Configuration

Guide p.63-77

- Create area classification diagram and locate assets into it

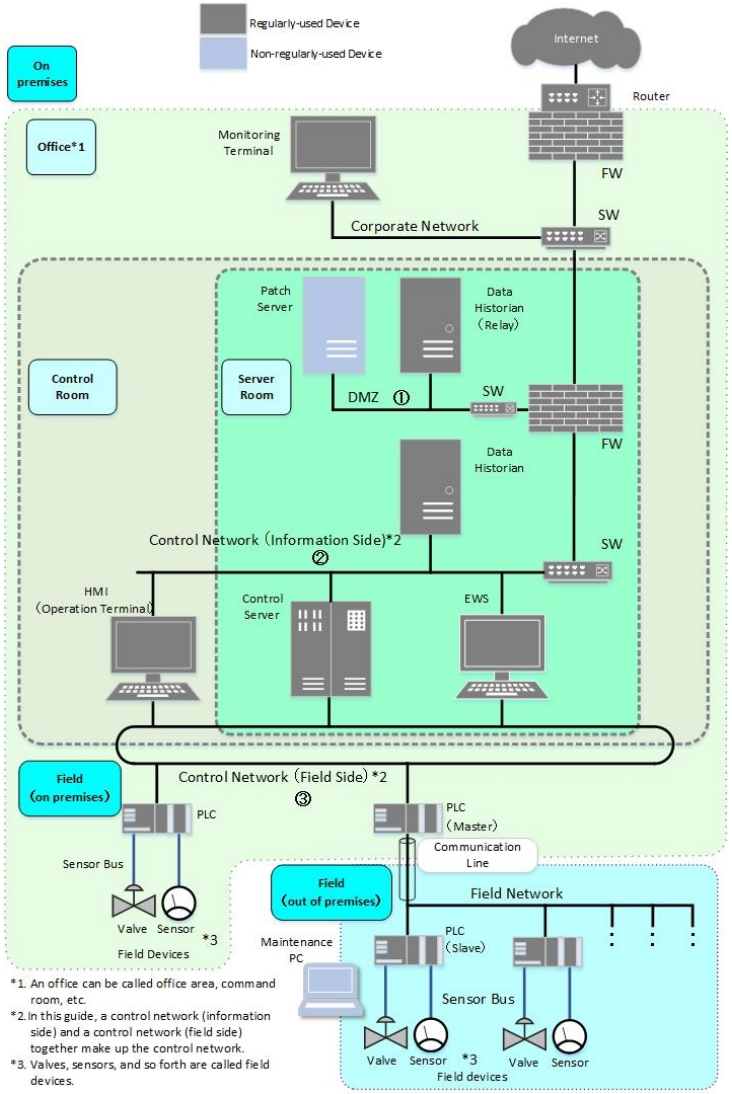


- Draw the connections between assets



- Create the simplified system configuration diagram for assessment

→



3. Preparing for Risk Assessment (1)

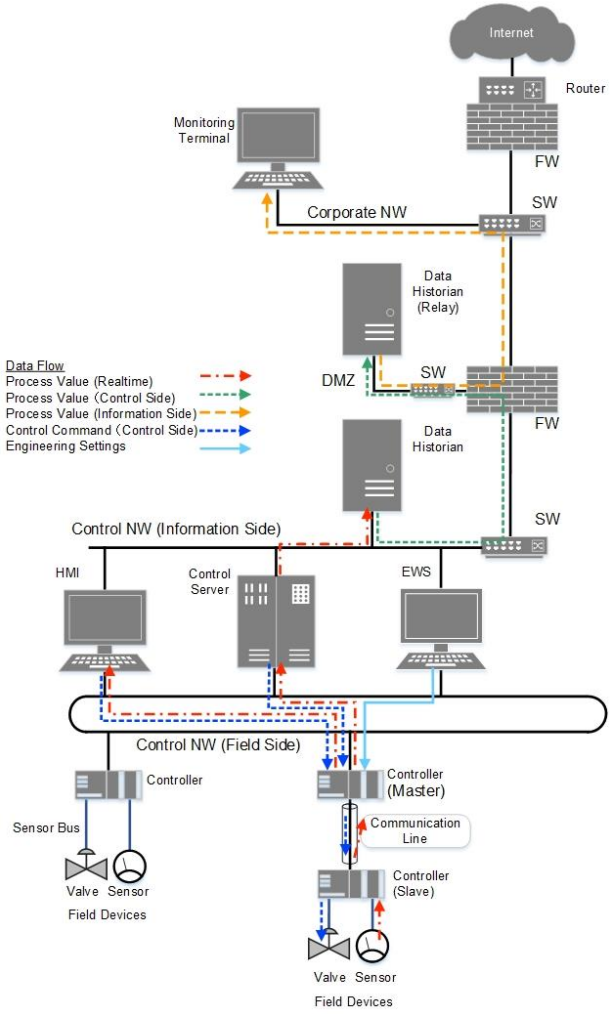
3.3. Clarifying the Data Flow

Guide p.78-89

- Create Data Flow Matrix
  - Organize what data flow from what device to what device

to→ P:Process Value C:Control Command S:Engineering Settings ↓from	Monitoring Terminal	FW	Data Historian (Relay)	Data Historian	EWS	Control Server	HMI	Controller (Master)	Controller (Slave)
Monitoring Termial	■								
FW	P	■							
Data Historian (Relay)		P	■						
Data Historian		P		■					
EWS					■			C	
Control Server				P		■		C	
HMI							■	C	
Controller (M)						P	P	■	C
Controller (S)								P	■

【Data Flow Diagram】



- Create Data Flow Diagram
  - Add data flow to system configuration diagram

4. Preparing for Risk Assessment (2)
～Risk Value, Evaluation Factors and Criteria～

IPA

Guide p.90-91

Understand the 'Risk Value' and 'Evaluation Factors' and Define Part of Criteria Yourself

【Preparatory Works and Outputs】

Section	Preparatory Works (excerpt)	Outputs
4.1	• Understand the meaning of 'risk value' • Understand the relationship between 'risk value' and 'evaluation factors'	
4.2	• Define the evaluation criteria of asset importance • Determine the importance of asset	• Evaluation criteria of asset importance • List of the assets and their importance
4.3	• Define the evaluation criteria of business impact level • Identify the business consequence	• Evaluation criteria of business impact level • List of the business impact level and each business impact
4.4	• Understand the meaning of 'threat' and 'threat level' • Define the evaluation criteria of threat level	• Evaluation criteria of threat level
4.5	• Understand the relationship between 'security status' and 'vulnerability'	

4. Preparing for Risk Assessment (2)
4.1. Risk Value and its Calculation

Guide p.92-93

- Risk Value
  - A value that represents relative risk of the asset/business against an specified threat calculated based on the importance of asset/business impact, likelihood of occurrence (threat), and acceptability of the threat (vulnerability).

【Risk Value Classification】

Risk Value	Definition
A	Risk is very high.
B	Risk is high.
C	Risk is medium.
D	Risk is low.
E	Risk is very low.

【Relationship between Risk Assessment Methods and Evaluation Factors】

Risk Assessment Method	Evaluation Factors			
	Asset Importance	Business Consequence	Threat	Vulnerability
Asset-based	○	–	○	○
Business Impact-based	–	○	○	○

4. Preparing for Risk Assessment (2)
4.2. Importance of Asset

Guide p.94-102

- Importance of Asset
  - One of the evaluation factors in asset-based risk assessment
  - Considering the value as an system asset, the potential business impact by attack, and the influence on business continuity

    (1：low～3：high)

【Evaluation Criteria for Importance of Asset (example)】

Evaluation Value	Evaluation Criteria
3	•When the asset is attacked, the system would stop for a long time. •When data is leaked from the asset, a huge financial loss would occur. •When the asset is attacked, large-scale human/environmental damage would occur.
2	•When the asset is attacked, the system would stop for a period of time. •When data is leaked from the asset, some financial loss would occur. •When the asset is attacked, medium-sized human/environmental damage would occur.
1	•When the asset is attacked, the system would stop for a short period of time. •When data is leaked from the asset, a small financial loss would occur. •When the asset is attacked, small-scale human/environmental damage would occur.

4. Preparing for Risk Assessment (2)

4.3. Business Consequence and Business Impact Level

Guide p.103-107

- Business Impact Level
  - One of the evaluation factors in business impact-based risk assessment
  - The magnitude of business impact caused by threat (1:small～3:large)

【Evaluation Criteria for Business Impact Level (example)】

Evaluation Value	Evaluation Criteria
3	Business consequence is large. 【e.g.】 •When it occurs, the whole system is affected. •Impact to company's business may be fatal or persistent.
2	Business consequence is medium. 【e.g.】 •When it occurs, only a part of the system is affected. •Impact to company's business may be Large or long-term.
1	Business consequence is small. 【e.g.】 •When it occurs, only a small part of the system is affected. •Impact to company's business may be less than medium or temporary.

4. Preparing for Risk Assessment (2)

4.3. Business Consequence and Business Impact Level

Guide p.103-107

- Business Consequence
  - Events and situations that hinder the stable operation and continuation of the organization's business
  - Defined by each organization based on the scope of impact when it occurs and magnitude of impact on business operations

#	Business Consequence	Description	Business Impact Level
1	Wide Area XX Supply Outage	Cyber attack on XX manufacturing facility, XX supply facility, etc. could result in supply outage over a wide area, largely affecting society, and causing huge financial loss such as compensation costs, and loss of credibility.	3
2	Limited Area XX Supply Outage	Cyber attack on XX manufacturing facility, XX supply facility, etc. could result in supply outage in a limited area, affecting society, and causing financial loss such as compensation costs, and loss of credibility.	2
3	Supply of Off-spec Product XX	Cyber attack on XX manufacturing facility, XX supply facility, etc. could result in supply of XX which doesn't meet defined specifications/standards, affecting society, and causing financial loss such as compensation costs, and loss of credibility.	2
4	Destruction of Equipment/Facility	Cyber attack on XX manufacturing facility, XX supply facility, etc. could result in destruction of the equipment/facility, affecting society, causing casualties (employees and/or neighbors) and financial loss such as compensation costs, and loss of credibility.	3
5	Facing Huge Cost for Remediation	Although cyber attack did not cause XX supply outage, the insufficiency of current security controls was revealed, and a huge cost for the remediation is required.	1

4. Preparing for Risk Assessment (2)
4.4. Threat and Threat Level

Guide p.108-119

- Threat Level
  - One of the evaluation factors and common in both types of risk assessment
  - The likelihood of occurrence of the potential threat in each risk assessment (1: low ～ 3: high).

【Decision Criteria of Threat Level / example】

Evaluation Value	Evaluation Criteria
3	Likelihood of threat occurrence is high. 【e.g.】 •Attacks are likely to be attempted by individual attackers who may or may not be skillful. •Attacks are likely to be attempted on assets on externally accessible network (e.g. DMZ, corporate network).
2	Likelihood of threat occurrence is medium. 【e.g.】 •Attacks are likely to be attempted by attackers who have a certain level of skill. •Attacks are likely to be attempted on assets on internal network (e.g. control network (information side).
1	Likelihood of threat occurrence is low. 【e.g.】 •Attacks are likely to be attempted by nation-state attackers (military intelligence or state-sponsored hackers). •Attacks are likely to be attempted on assets on a specific restricted network (e.g. control network (field side)).

4. Preparing for Risk Assessment (2)

4.4. Threat and Threat Level

Guide p.108-119

【Threats (attack techniques) to assets (devices) (excerpt)】

#	Threats（attack techniques)	Description	Examples
1	Unauthorized Access	Hack into a devices via network and execute an attack.	● Abuse of credentials acquired fraudulently (unauthorized login) ● Intrusion to devices having no authentication mechanism ● Exploitation of inherent vulnerabilities in devices ● Abuse of wrong device settings (unnecessary processes and ports etc. are left enabled or open)
2	Physical Intrusion	Intrude into a restricted area (where equipment is installed, etc.) , or unlock a device to which the access is physically limited (a device installed in a rack or a box, etc.) .	● Unauthorized intrusion into the premises/control room/server room ● Unauthorized unlocking of rack/installation box
3	Fraudulent Operation	Access the device and fraudulently operate it to execute an attack.	● Abuse of credentials acquired fraudulently (unauthorized login) ● Intrusion to devices having no authentication mechanism ● Exploitation of inherent vulnerabilities in devices
4	Unintentional adverse Operation	Induce an incorrect operation of the insider (a person with privilege to access the device among employees and business partners) and execute an attack. Connect an authorized medium or device to the device, and an action equivalent to an attack is executed as a consequence.	● Opening a malicious email/attachment ● Bringing in a legitimate medium which is infected with malware
5	Connecting Unauthorized Medium/Device	Bring in some unauthorized media or device (CD/DVD, USB device etc.) and connect it to the device to attack.	● Connecting malicious media/device ● Read from the medium/ Write to the medium
6	Unauthorized Execution of Process	Fraudulently execute a process existing in the target device, such as legitimate programs, commands, services etc.	● Unauthorized execution of program/command ● Unintentionally enabling services
7	Malware Infection	Infect and execute malware on the target device	
8	Data Theft	Steal data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	● Theft of control data
9	Data Modification	Modify data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	● Modification of control programs ● Modification of control parameters
10	Data Destruction	Make information (software, credential configuration settings, confidential information such as an encryption key) stored in the device unusable.	● Deletion of control data ● Encryption of control data
11	Issuing Malicious Command	Send malicious control commands (set point change, power off, etc.) or malicious data to other devices.	● Unauthorized execution of control command / data transmission instruction ● Modification of transmission data
12	Shutdown	Halt the function of device.	● Unauthorized execution of commands to stop function/device/system

4. Preparing for Risk Assessment (2)

4.5. Vulnerability/Vulnerability Level and Security Status/Security Level

Guide p.120-130

- Vulnerability Level
  - One of the evaluation factors and common in both types of risk assessment
  - The likelihood of occurrence of the potential threat in each risk assessment (1: low ～ 3: high).

Evaluation Value		Evaluation Criteria
Vulnerability Level	Security Level	
3	1	The likelihood of accepting a threat is high at its occurrence. Since no security controls against threats are not implemented, the likelihood of attack being successful is high. 【e.g.】 •In the past incidents, it was confirmed that attacks making use of vulnerability occurred and was successful to cause impact.
2	2	The likelihood of accepting a threat is medium at its occurrence. Some security controls against threats are implemented but are not sufficient. The likelihood of attack being successful is medium. 【e.g.】 •Since common security controls are implemented, whether the attack is successful depends on attacker's skill level. •In the past incidents, it was confirmed that attacks making use of vulnerability occurred but no major impact was caused.
1	3	The likelihood of accepting a threat is low at its occurrence. Since effective and multi-layered security controls against threats are implemented sufficiently, the likelihood of attack being successful is low. 【e.g.】 •Since effective and multi layered measures are implemented, the likelihood of attack successful is low. •In the past incidents, no attacks occurred that made use of vulnerability.

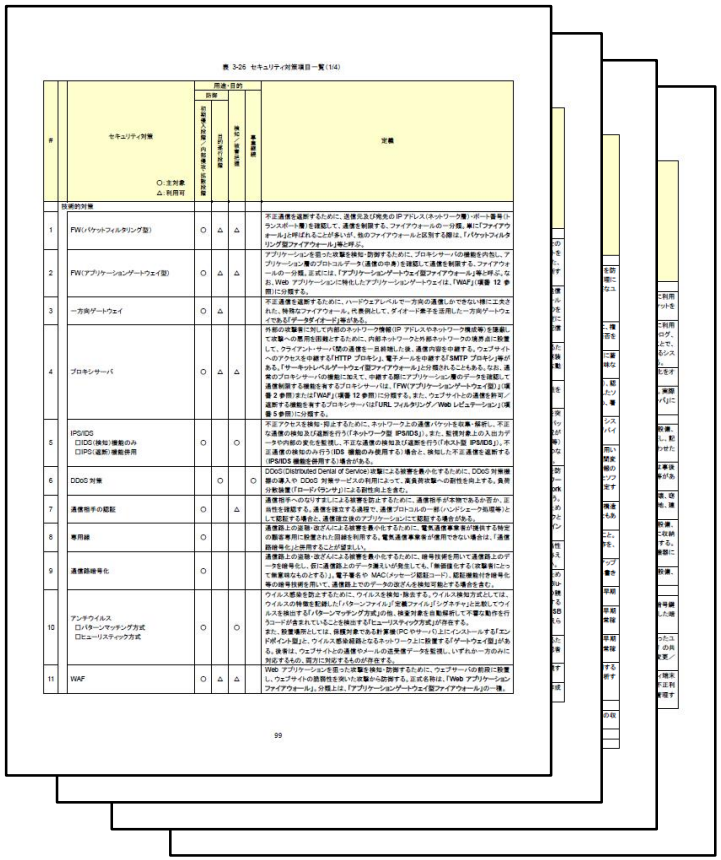
4. Preparing for Risk Assessment (2)

4.5. Vulnerability/Vulnerability Level and Security Status/Security Level

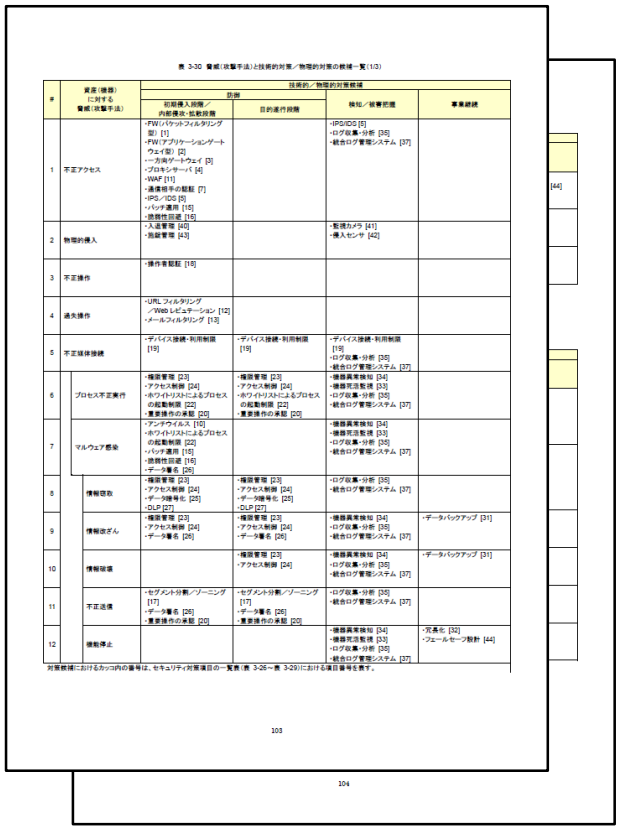
Guide p.120-130

Lists of "Security Controls" and Mapping to “Threats (Attack Techniques)"

【List of Security Controls（47 controls）】



【Mapping of Security Controls to Threat (Attack Techniques) 】

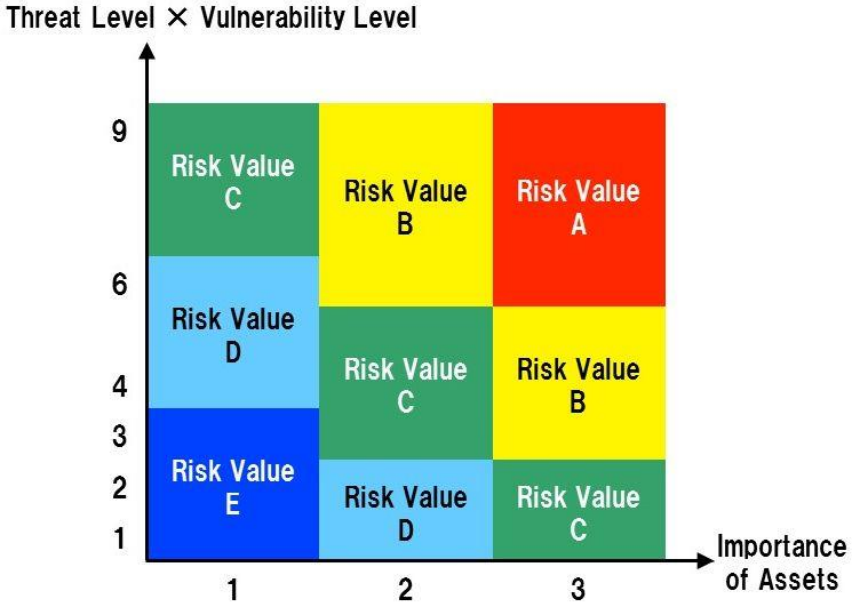


5. Conducting Risk Assessment (1)
Asset-based Risk Assessment

Guide
p.131-169

Assessment method focusing on assets that make up ICS
～Evaluate the assumed direct threats to assets and the sufficiency of security controls implemented～

- For the assets making up ICS which should be protected, calculate the magnitude of the risk of each asset (risk value) from
  - Importance (value) of the asset
  - Threat level
    (likelihood of threat occurrence)
  - Vulnerability level
    (likelihood of accepting a threat at its occurrence)



5. Conducting Risk Assessment (1)
Asset-based Risk Assessment

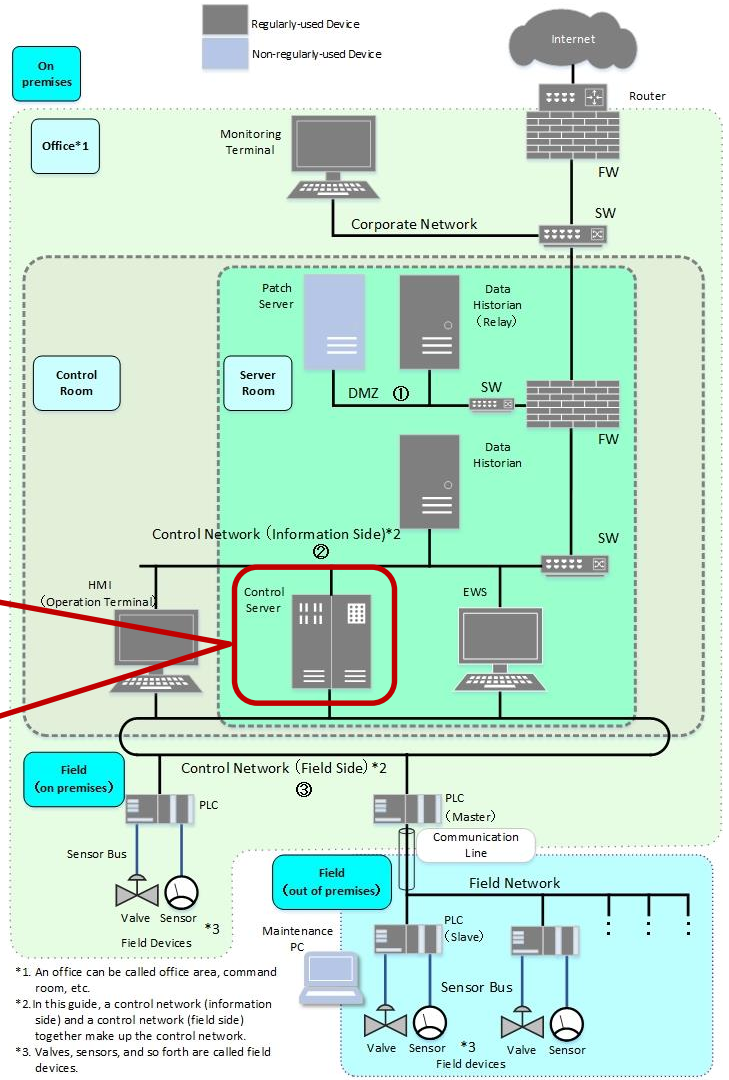
Guide p.131-169

- List threats (attack techniques) and available security controls, based on asset type (“information asset”, “control asset”, “network asset”) per asset
- Check which security controls are implemented for each asset
  → Vulnerability level

Threats (attack techniques)
Unauthorized Access
Malware Infection
Data Modification
Shutdown etc.

Security Status
Authentication of Connecting Entity
Whitelist
User Authentication
Privilege Management etc.

Vulnerability Level for each threat



5. Conducting Risk Assessment (1)
Asset-based Risk Assessment

Guide p.133-136

- Example of the completed sheet of Asset-based Risk Assessment

Asset-based Risk Assessment Sheet

[Legend] ○: Implemented / ×: Not Implemented / Greyout : Threats not considered in the asset / Green characters: additional information of the security measure

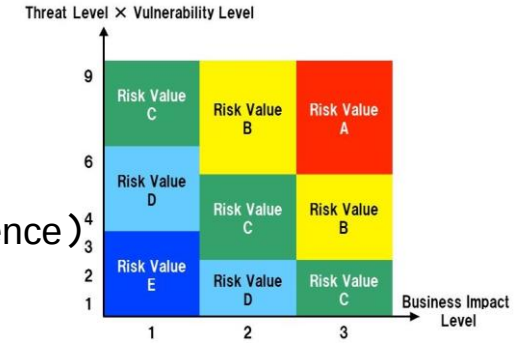
No.	Asset Type	Assessment Object	Evaluation Factor				Threat (Attack Technique)	Description	Security Controls						Security Level
									Protection				Detection / Consequence Identification	Business Continuity	
			Threat Level	Vulnerability Level	Importance of Asset	Risk Value			Intrusion / Diffusion Phase		Objective Achievement Phase				Per Threat
1	Information System Asset	**Control Server**	2	2	3	B	Unauthorized Access	Hack into a devices via network and execute an attack.	FW (Packet Filtering type) FW (Application Gateway type) Unidirectional Gateway Proxy Server WAF Authentication of Connecting Party ○ IPS／IDS Patch Application Vulnerability Avoidance				IPS／IDS Logging／Analysis Integrated Log Management System		2
2			2	1		C	Physical Intrusion	Intrude a restricted area (where equipment is installed, etc.) , or unlock a device the access to which is physically limited (a device installed in a rack or a box, etc.) .	Physical Access Control (IC card, Biometric Authentication) ○ Lock-up／Key Management ○				Surveillance Camera ○ Intrusion Sensor ○		3
3			2	2		B	Fraudulent Manipulation	Intrude by direct operation of the console of the device etc. and execute an attack.	Operator Authentication (ID/Pass) ○						2
4			2	3		A	Incorrect Operation	Induce an incorrect operation of the insider (a person with privilege to access the device among employees and business partners) and execute an attack. Connect an authorized medium or device to the device and an action equivalent to an attack is executed as a consequence.	URL Filtering／Web Reputation Mail Filtering						1
5			2	3		A	Connecting Unauthorized Media/Device	Connect illegally brought malicious medium (CD/DVD, USB device etc.) to the device and execute an attack.	Device Connection and Usage Restriction		(same as left)		(same as left) Logging／Analysis Integrated Log Management System		1
6			3	2		A	Unauthorized Execution of Process	Fraudulently execute a process existing in the attack target device, such as legitimate programs, commands, services etc.	Privilege Management ○ Access Control Process Run Limitation by Whitelist ○ Approval of Critical Operations		(same as left) (same as left) (same as left) (same as left)		Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System		2
7			3	1		B	Malware Infection	Infect and execute malware on the target device.	Anti Virus Process Run Limitation by Whitelist ○ Patch Application Vulnerability Avoidance Digital Signature				Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System		3
8			3	2		A	Data Theft	Steal data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	Permission Management ○ Access Control Data Encryption DLP		(same as left) (same as left) (same as left) (same as left)		Logging／Analysis Integrated Log Management System		2
9			3	2		A	Data Modification	Modify data (software, credential, configuration settings, confidential information such as an encryption key) stored in the device.	Permission Management ○ Access Control Digital Signature		(same as left) (same as left) (same as left)		Device Anomaly Detection Logging／Analysis Integrated Log Management System	Data Backup ○	2
10			2	2		B	Data Destruction	Make information (software, credential configuration settings, confidential information such as an encryption key) stored in the device unusable.			Privilege Management ○ Access Control		Device Anomaly Detection Logging／Analysis Integrated Log Management System	Data Backup ○	2
11			3	3		A	Malicious Command	Send malicious control commands (set point change, power off, etc.) or malicious data to other devices.	Segmentation／Zoning Digital Signature Approval of Critical Operations		(same as left) (same as left) (same as left)		Logging／Analysis Integrated Log Management System		1
12			3	3		A	Shutdown	Halt the function of device.					Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System	Redundancy Fail-safe Design	1
13			1	3		B	Denial-of-service Attack	Requests processing that exceeds the processing capability of the device by DDoS attacks, etc., and interferes with the normal operation of the device.	Anti DDoS Solution				Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System	Redundancy Fail-safe Design	1
14			1	2		C	Theft	Steal device or equipment.	Lock-up／Key Management ○		(same as left)		(同左)		2
15			3	3		A	Information theft by disassembling stolen and discarded equipment	A stolen device or a discarded device is disassembled, and information (software, authentication information, configuration setting information, confidential information such as an encryption key) stored in the device is stolen.	Tamper Resistant Obfuscation Secure Deletion		(same as left) (same as left) (same as left)				1

6. Conducting Risk Assessment (2)
Business Impact-based Risk Assessment

Guide
p.170-252

Scenario-based detailed risk assessment using attack tree
～Evaluate the assumed attacks on business and sufficiency of the security control～

- Attack Scenario
  - A scenario embodies an attack that leads to a business consequence that should be avoided.
  - Each scenario should include attack execution point, attack target, and a final attack.
- Attack Tree
  - An attack tree depicts a series of attack procedures that realize an attack scenario.
  - In addition to the attack execution point, attack target, and final attack embodied in an attack scenario, each attack tree should include the attacker, entry point and assets on attack path (from the entry point to the attack execution point).
- Calculate the magnitude of the risk of each attack tree (risk value) from
  - Threat level (likelihood of attack tree occurrence)
  - Vulnerability level (likelihood of accepting attack tree at its occurrence)
  - Business impact level (magnitude of business impact)



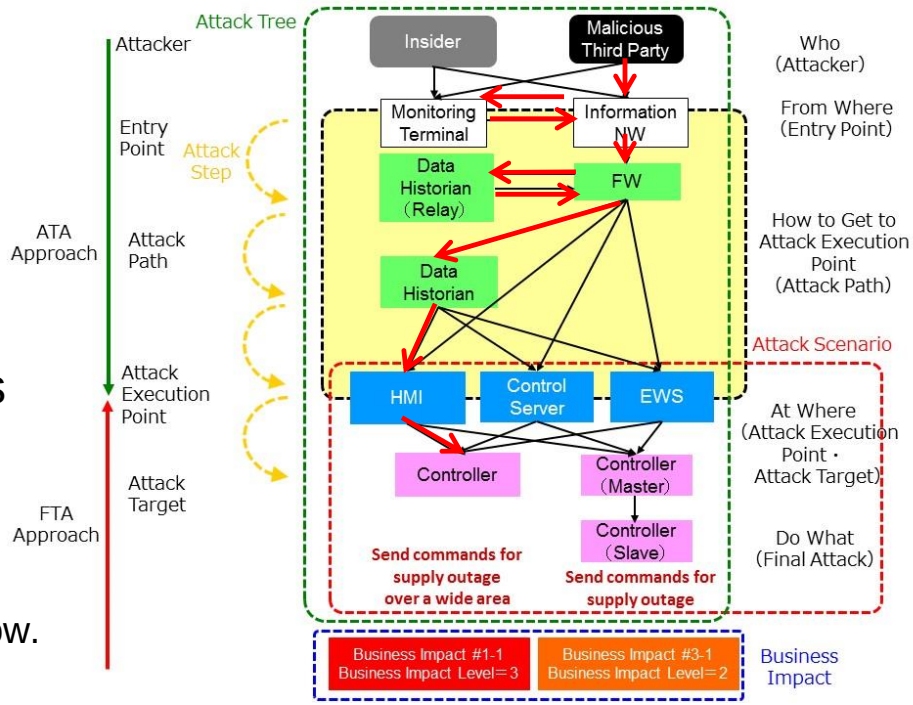
6. Conducting Risk Assessment (2)
Business Impact-based Risk Assessment

Guide p.170-252

- Structure of Attack Tree

[attack tree example]

A malicious outsider hacks into the monitoring terminal on the corporate NW, and through the data historian (relay), FW and data historian, reaches to the HMI (attack execution point), and then executes the final attack command to the controller (attack target) to cause wide area supply outage.



This example will be shown as below.

A malicious outsider gains unauthorized access to the monitoring terminal.	Attack Step	Attack Tree
A malicious outsider gains unauthorized access to the data historian (relay) from the monitoring terminal.	Attack Step	
A malicious outsider gains unauthorized access to the data historian from the data historian (relay).	Attack Step	
A malicious outsider gains unauthorized access to the HMI from the data historian.	Attack Step	
A malicious outsider sends commands from the HMI to the controller for causing wide area supply outage.	Final Attack Step	

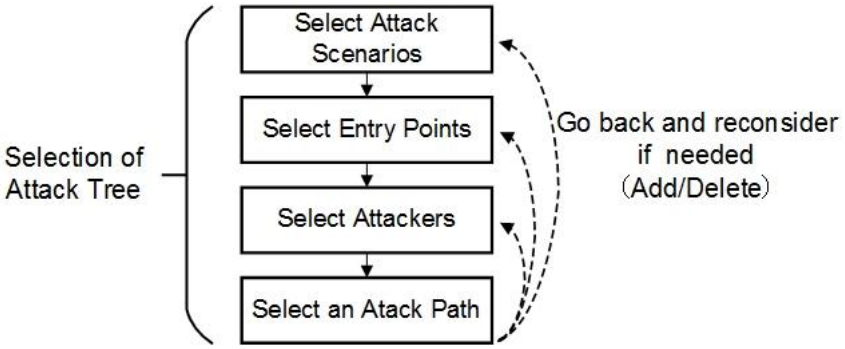
6. Conducting Risk Assessment (2)
Business Impact-based Risk Assessment

Guide p.170-252

- Selection of Assessment Objects(1)

【When NOT Selected】
(Scope = Blue Square)
Analyze all business impacts, attack scenarios, entry points, attackers, attack paths

【When Selected】
(Scope = Red Squares)
Preferentially analyze attack scenarios, entry points, attackers and attack paths that have a high potential to cause significant business consequence.



6. Conducting Risk Assessment (2)
Business Impact-based Risk Assessment

Guide p.170-252

- Selection of Assessment Objects (2)

【 Entry point of physical access: Points to consider for prioritization (example)】

#	Points to consider for prioritization
1	Whether the device has a USB port, communication interface, or wireless function which can be used.
2	Whether the device has a regular operation to transfer data via USB memory, DVD, or Laptop PCs etc. from/to the device.
3	Whether the device is an attack execution point.
4	Whether the device has an operation interface such as a keyboard, touch panel, or switches etc.
5	Whether the device is a regularly-used device.

【 Entry point of physical access: Selection Criteria (example)】

＜ Selection Criteria 1＞ Select a device that has a regular operation to transfer data via external storage media such as USB memory, DVD, or laptop PCs.
＜ Selection Criteria 2＞ Select a device that is the attack execution asset in attack scenarios and has an operation interface.

6. Conducting Risk Assessment (2)
Business Impact-based Risk Assessment

Guide p.170-252

- Example of the completed sheet of Business Impact-based Risk Assessment

Business Impact-based Risk Assessment Sheet

1. XX Supply Outage Over a Wide Area

No.	Attack Scenario: Attack Tree／Attack Step	Evaluation Factor: Threat Level	Vulnerability Level	Business Impact Level	Risk Value	Security Controls: Protection: Intrusion／Lateral Movement		Protection: Mission Execition Phase	Detection／Impact Identification		Business Continuity	Security Level: Attack Step	Attack Tree	Attack Tree Number	Component Steps (No.)
1-1	Wide area supply outage occurs by conducting unauthorized and malicious operations.														
1	**Network Attack Entry Point : Monitoring Terminal** A malicious outsider gains unauthorised access to the monitoring terminal.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	○ ○ ○		Logging／Analysis Integrated Log Management System			2			
2	A malicious outsider gains an authorised access to the data hystorian (relay) from the monitoring terminal.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	● ● ●		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring			1			
3	A malicious outsider gains an authorised access to the data hystorian from the data hystorian (relay).					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	● ●		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring			1			
4	A malicious outsider gains an authorised access to HMI from the data hystorian.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	○ 		IPS/IDS Logging／Analysis Integrated Log Management System Device Alive Monitoring			2			
5	A malicious outsider sends commands from HMI to the controller for causing wide area supply outage.	2	2	3	B	Segmentation／Zoning Digital Signature Approval of Critical Operations			Logging／Analysis Integrated Log Management System			1	2	#1	1,2,3,4,5
6	**Physical Attack Entry Point : HMI** An insider enters into the control room.					Physical Access Control (IC card) Lock up／key Management	● ●		Surveillance Camera Intrusion Sensor Logging／Analysis Integrated Log Management System	○ ○		1			
7	An insider logs on to HMI.					Operator Authentication			Logging／Analysis Integrated Log Management System			1			
8	An insider accidentally connects a USB media infected with malware to the HMI, then the HMI is infected with malware.					Anti Virus (Media) Anti Virus (HMI) Poet Lock Process Run Limitation by Whitelist Patch Application Vulnerability Avoidance Digital Signature			Device Anomaly Detection Device Alive Monitoring Logging／Analysis Integrated Log Management System			1			
9	The malware executes operations for causing wide area supply outage.	2	3	3	A	Segmentation／Zoning Digital Signature Approval of Critical Operations			Logging／Analysis Integrated Log Management System			1	1	#2	6,7,8,9
1-2	Wide area supply outage occurs by sending legitimate commands to controllers.														
10	**Network Attack Entry Point : Corporate NW** A malicious outsider gains unauthorized access to FW via corporate NW.					FW Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	○ ○ ○ ○		IPS/IDS Log Collection／Analysis Integrated Log Management System Device Alive Monitoring			2			
11	A malicious outsider gains access to EWS via FW.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management	○ 		IPS/IDS Log Collection／Analysis Integrated Log Management System Device Alive Monitoring			1			
12	A malicious outsider gains access to the master controller via EWS.					Authentication of Connecting Party Patch Application Vulnerability Avoidance Privilege Management			Log Collection／Analysis Integrated Log Management System Device Anomaly Detection			1			
13	A malicious outsider sends supply outage commands from the master contoller to the slave controllers.	2	2	3	B	Segmentation／Zoning Digital Signature Approval of Critical Operations			Log Collection／Analysis Integrated Log Management System			1	2	#3	10,11,12,13

7. Interpreting and Utilizing Risk Assessment Results

IPA

Guide
p.253-281

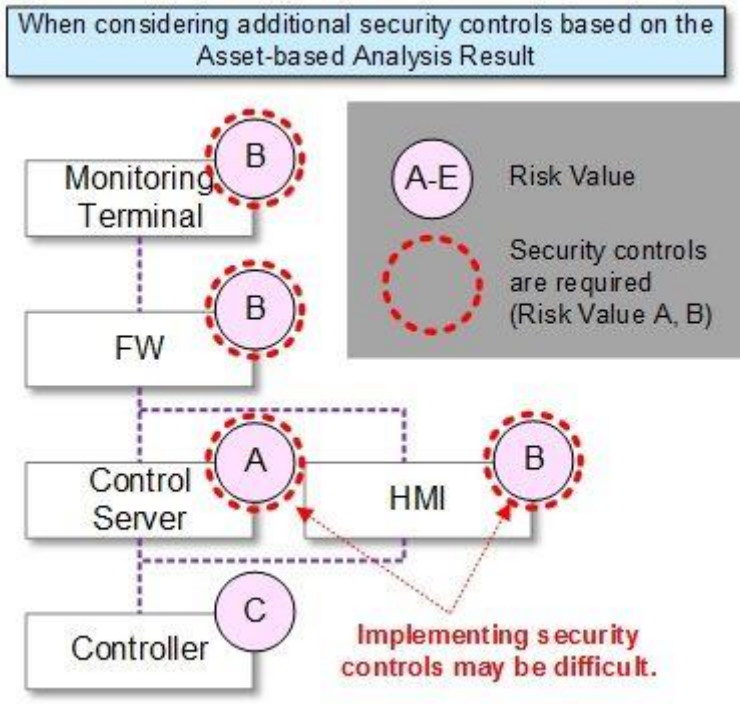
New Steps towards improving ICS security

- Objectives for interpretation and utilization of risk assessment results
  - Locate security weaknesses and lower the risk value as much as possible as a step to mitigate the risk to cyberattacks
- Utilization of risk value
  - Understand risks
  - Select points of improvement
  - Mitigate risks
  - Confirm the risk mitigation effect
  - Extract and select best places to perform security
- Difference between two types of risk assessment in how to utilize the result
- Toward continuous security effort (PDCA cycle)

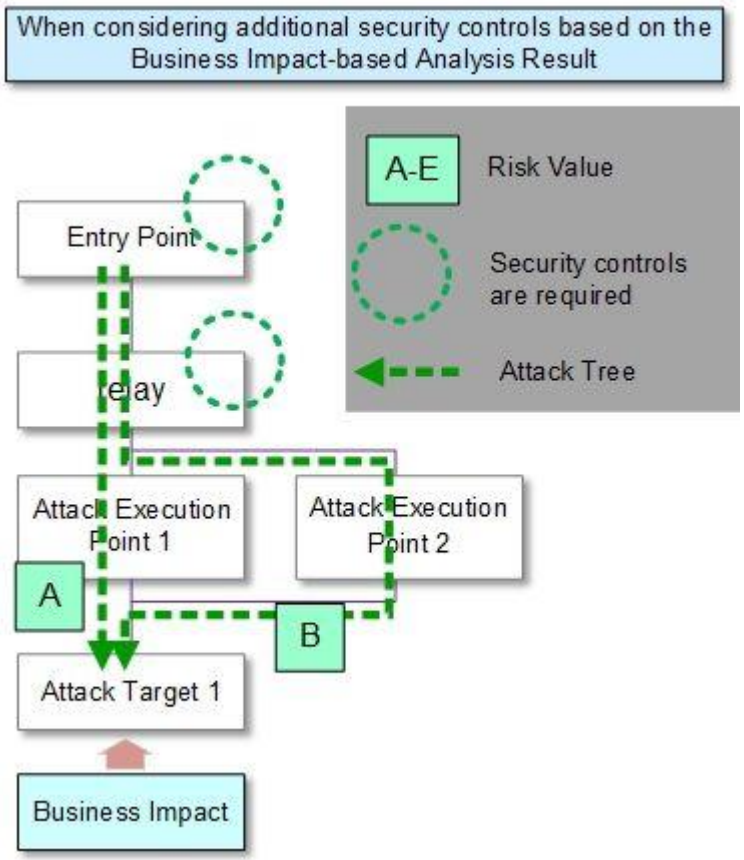
7. Interpreting and Utilizing Risk Assessment Results

Difference between Two Types of Risk Assessment

Guide p.277-279



Consider security controls for assets regardless of the connection between assets



Consider security controls for selected assets somewhere on the attack path

8. Security Test

Guide
p.282-301

Verify whether security controls work as they should, and their robustness against threats

- Roles of Security Test (Objectives and Expected Effects)
  - Verification of ICS risk assessment results on actual devices
  - Survey of the as-is control system
- Types, Objective, and Target of Security Test

Objective	Target of Test		
	Network	OS／Middleware	Application
Detect known-vulnerabilities	•Vulnerability scan（System inspection）		•Vulnerability scan（Web application inspection）
Detect unknown-vulnerabilities	•Fuzzing		
			•Source code inspection
Verify intrusion feasibility	•Penetration test		
Verify suspicious communications	•Packet capture		
Verify unauthorized network devices	•Network discovery •Wireless Scanning		

9. Additional Criteria for Specific Security Controls

Guide p.302-307

Confirm and evaluate the implementation status of specific security issues in more detail

- Selection of cryptographic technology and its application
- Targeted attack protection
- Insider threat protection
- Firewall settings
- Secure use of external storage media

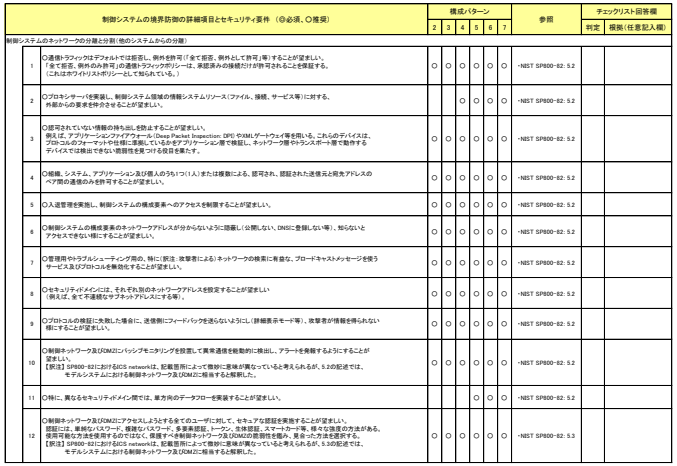
- Provide security requirements for each issue as a checklist
  - Security requirements
    - Labeled as “required” or “recommended”
  - Reference
    - Provide mapping to related international standards, industry standards, etc.
  - Intended answerer (such as “CEO”, “IT Dept.”, “HR Dept.”) (only for “insider threat protection checklist”)

Can be used for any information systems, not limited to ICS

Appendixes

Guide
p.310-378

- Firewall Architectures for Network Segmentation
  - Definition of Firewalls
  - Types of Firewalls
  - Firewall implementation architectures
- Checklist for Specific Security Controls
  - Cryptographic Technology Checklist
  - Targeted Attack Protection Checklist
  - Insider Threat Protection Checklist
  - Firewall Settings Checklist
  - External Storage media Checklist
- List of ICS Incidents
- Glossary
- Key Updates from the First Edition



制御システムの境界防御の詳細項目とセキュリティ要件（◎必須、○推奨）		構成パターン							参照	チェックリスト回答欄	
		2	3	4	5	6	7			判定	根拠（任意記入欄）
制御システムのネットワークの分離と分割（他のシステムからの分離）											
	1 ○通信トラフィックはデフォルトでは拒否し、例外を許可（「全て拒否、例外として許可」等）することが望ましい。 「全て拒否、例外のみ許可」の通信トラフィックポリシーは、承認済みの接続だけが許可されたことを保証する。 （これはホワイトリストポリシーとして知られている。）	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	2 ○プロキシサーバを実装し、制御システム領域の情報システムソース（ファイル、接続、サービス等）に対する、 外部からの要求を仲介させることが望ましい。				○	○	○		・NIST SP800-82: 5.2		
	3 ○認可されていない情報の持ち出しを防止することが望ましい。 例えば、アプリケーションファイアウォール（Deep Packet Inspection: DPI）やXMLゲートウェイ等を用いる。これらのデバイスは、 プロトコルのフォーマットや仕様に準拠しているかをアプリケーション層で検証し、ネットワーク層やトランスポート層で動作する デバイスでは検出できない悪意性を見つける役目を果たす。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	4 ○組織、システム、アプリケーション及び個人のうち1つ（1人）または複数による、認可され、認証された送信元と宛先アドレスの ペア間の通信のみを許可することが望ましい。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	5 ○入退管理を実施し、制御システムの構成要素へのアクセスを制限することが望ましい。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	6 ○制御システムの構成要素のネットワークアドレスが分からないように隠蔽（公開しない、DNSに登録しない等）、知らないと アクセスできない様にすることが望ましい。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	7 ○管理用やトラブルシューティング用の、特に（訳注：攻撃者による）ネットワークの検索に有益な、ブロードキャストメッセージを扱う サービス及びプロトコルを無効化することが望ましい。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	8 ○セキュリティドメインには、それぞれ別のネットワークアドレスを設定することが望ましい （例えば、全て不連続なサブネットアドレスにする等）。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	9 ○プロトコルの検証に失敗した場合に、送信側にフィードバックを送らないようにし（詳細表示モード等）、攻撃者が情報を得られない 様にすることが望ましい。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	10 ○制御ネットワーク及びDMZにパッシブモニタリングを設置して異常通信を能動的に検出し、アラートを発報するようにすることが 望ましい。 【訳注】SP800-82におけるICS networkは、記載箇所によって指すのに意味が異なっていると考えられるが、5.2の記述では、 モデルシステムにおける制御ネットワーク及びDMZに相当すると解釈した。	○	○	○	○	○	○		・NIST SP800-82: 5.2		
	11 ○特に、異なるセキュリティドメイン間では、単方向のデータフローを実装することが望ましい。					○	○		・NIST SP800-82: 5.2		
	12 ○制御ネットワーク及びDMZにアクセスしようする全てのユーザに対して、セキュアな認証を実施することが望ましい。 認証には、単純なパスワード、複雑なパスワード、多要素認証、トークン、生体認証、スマートカード等、様々な強度の方法がある。 使用可能な方法を使用するのではなく、保護すべき制御ネットワーク及びDMZの悪脅性を鑑み、見合った方法を選択する。 【訳注】SP800-82におけるICS networkは、記載箇所によって指すのに意味が異なっていると考えられるが、5.3.2の記述では、 モデルシステムにおける制御ネットワーク及びDMZに相当すると解釈した。	○	○	○	○	○	○		・NIST SP800-82: 5.3		

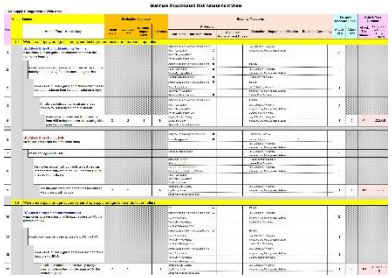
Practice Example of Risk Assessment for ICS

Practical Example p.1-94

Complete implementation example of risk assessment for a typical ICS

Includes:

① Asset Inventory ② System Configuration Diagram
③ Data Flow Matrix ④ Data Flow Diagram
⑤ Evaluation Criteria for Importance of Assets
⑥ List of the Assets and their Importance
⑦ Evaluation Criteria of Business Impact Level
⑧ List of Business Consequences
⑨ Evaluation Criteria of Asset Level
⑩ Threat Levels and Reasoning ⑪ Table of Threat Levels
⑫ Risk Assessment Sheet for Asset-based Risk Assessment
⑬ Table of Risk Values ⑭ List of Attack Scenarios
⑮ List of Attack Paths
⑯ Risk Assessment Sheet for Business Impact-based Risk Assessment
⑰ Table of Risk Values
⑱ Result of Risk Assessment (Improvement Measures for Risk Mitigation)



Risk Assessment Sheet formats are available at following URL. (in Japanese only)
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

In Short:

It's a practical guide to risk assessment that is important to enable radical improvement of ICS security

- Promote better understanding of the whole picture and procedure of risk assessment
- Provide concrete procedures and guidance to conduct risk assessment

- Introduce two types of detailed risk assessment methods
  - Asset-based, Business Impact-based
- Provide materials for risk assessment
  - Risk assessment sheet (format, examples)
  - List of threats (attack techniques) and security controls
  - Detailed checklist for specific security controls
- Present how to use risk assessment results
  - How to consider additional security controls to mitigate risk
  - Security test to complement risk assessment

Cybersecurity Incidents of ICS

Reference documents of Security Risk Assessment Guide for ICS

Incidents #1～#3

A series of reference document "Cybersecurity Incidents of ICS"

- Published in July, 2019
- Overview and attack procedures of cybersecurity incidents
- Able to utilize documents for creating attack trees and formulating security controls
- Cybersecurity incidents featured in each document
  - #1 : Cyber Attack on Ukrainian Power Grid (2015)
  - #2 : Cyber Attack on Ukrainian Power Grid (2016)
  - #3 : Malware Attack on Safety Instrumented System (SIS) (2017)

Documents are available at following URL. (in Japanese only)

https://www.ipa.go.jp/security/controlsystem/incident.html

Key Updates from the 1st Edition

Guide p.376-378

- Reflection of Feedback
- Reduction of Man-hours by Reviewing Risk Assessment Methods

  【Asset-based – Reduction of man-hours by simplifying assessment method】

  – Instead of mulling threats against and available security controls for each asset from scratch, the 2nd edition enables to choose them based on the asset type, in addition to grouping the assets just once in the preparation stage only.

  【Business impact-based – Reduction of man-hours by presenting selection criteria for assessment object】

  – Instead of listing all possible attack trees, the 2nd edition presents a way to select and preferentially analyze their important attack trees that their business consequence is high if the attacks succeed, and are likely to be targeted by attackers.
- Expanded Explanations on the Basics of Risk Assessment
  – Strictly defined the meaning of the evaluation factors and their evaluation values in risk assessment, and the risk value (risk level) obtained as a result of risk assessment