# Textbook for security response organisation (SOC/CSIRT)

 $\sim$  using X.1060  $\sim$ 

Appendix: mapping with FIRST CSIRT Services
Framework

Ver. 3.2.1 (en)

### 2025.10.17

NPO Japan Network Security Association (JNSA) Information Security Operation providers Group Japan (ISOG-J)

#### Revision history

2016/11/25	Ver.1.0
2017/10/03	Ver.2.0
2018/03/30	Ver.2.1
2023/2/13	Ver.3.0
	· align with ITU-T recommendation X.1060
2023/10/17	Ver.3.1
2024/10/17	Ver.3.2
2025/10/17	Ver.3.2.1 (en) English version, add this Appendix

#### Disclaimer

- The copyright of this document belongs to the Information Security Operation providers Group Japan (ISOG-J).
- Quotations are permitted under the Copyright Law to the extent that they are
  justifiable for the purpose of quotation. The quoted portion should be clear and the
  source clearly indicated, for example.
- In cases where the quotation is believed to exceed the permitted scope, ISOG-J
  may be contacted at info (at) isog-j.org.
- Company names, product names, and service names appearing in this document are generally registered trademarks or trademarks of the respective companies. The ®, TM and © marks are not indicated in this document.
- Neither ISOG-J nor the authors assume any responsibility for this guide document. Use at your own risk.

## **Table of Contents**

1.	Mapping with FIRST CSIRT Services Framework version 2.1.0	1
2.	Mapping with X.1060	33

## 1. Mapping with FIRST CSIRT Services Framework version 2.1.0

X.1060		FIRST CSIRT Services Framework version 2.1.0		
Service	Description	Service	Function	Purpose
A-1. Risk	The risk management service is to	N/A		
management	achieve coordinated activities			
	including A-2 to A-13 to direct and			
	control an organization with			
	regard to risk.			
A-2. Risk	The risk assessment service	9.4 Service:	9.4.1 Function:	Improve the identification of opportunities
assessment	provides a snapshot of the risk	Technical	Risk management	and threats, improve controls, improve loss
	level of an organization in terms of	and policy	support	prevention and incident management in
	assets, threats and security	advisory		conjunction with information security and
	measures.			other relevant functions.
A-3. Policy		7.5 Service:	7.5.1 Function:	Develop and maintain a policy that provides
planning	The policy planning service is	Vulnerabilit	Vulnerability	a framework and sets expectations for how a
	supporting all the activities of	y disclosure	disclosure policy	CSIRT handles and discloses vulnerabilities
	defining specific security policies,		and	and the mechanism(s) used to disclose the
	compiling the guidelines.		infrastructure	vulnerability.
			maintenance	
		8.1 Service:	8.1.1 Function:	Establish the context with which the
		Data	Policy	constituency and its assets should comply to
		acquisition	aggregation,	know what should be occurring on the

			distillation, and guidance	infrastructure.
		9.4 Service: Technical and policy advisory	9.4.3 Function: Policy support	Act as a trusted advisor on the development and implementation of policies by providing impartial, fact-based advice, considering the environment in which the advice may be used and any resource constraints that apply.
A-4. Policy management	The policy management service is to achieve periodic reviews for evaluation of policy and organization rules, to comply with new or external requirements (e.g., regulations and guidelines).	N/A		прод
A-5. Business continuity	The business continuity service supports the operational functions necessary to ensure correct implementation and execution of the business continuity plan of an organization.	9.4 Service: Technical and policy advisory	9.4.2 Function: Business continuity and disaster recovery planning support	Act as a trusted advisor on business continuity and disaster recovery by providing impartial, fact-based advice, considering the environment in which the advice may be used and any resource constraints that apply.
A-6. Business impact analysis	The business impact analysis service is to achieve a systematic assessment of the possible impacts	N/A		

			1
resulting from various events or			
scenarios. This service helps			
organizations understand the			
scale of loss that could occur. It			
may cover not only direct financial			
loss, but also other impacts, such			
as loss of stakeholder confidence			
and reputational damage.			
The resource management service	N/A		
plans resources (personnel,			
budget, systems, etc.) to support			
security activities and allocates			
them appropriately to each			
service.			
The security architecture design	N/A		
service is to establish an			
architecture to secure the			
business. Development and			
maintenance of CDC platforms			
(category G) can be achieved by			
compiling various security			
measurements that consider			
system design and constraints of			
	scenarios. This service helps organizations understand the scale of loss that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage.  The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service.  The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider	scenarios. This service helps organizations understand the scale of loss that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage.  The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service.  The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider	scenarios. This service helps organizations understand the scale of loss that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage.  The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service.  The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider

	business processes (e.g., supply		
	chain).		
A-9. Triage	The triage criteria management	N/A	
criteria	service is to set specific triage		
management	(response priority) criteria for		
	events (e.g., incidents,		
	vulnerabilities found, threat		
	information discovered) under the		
	agreed scope in the overall policy.		
A-10. Counter	The counter measures selection	N/A	
measures	service is to support all activities of		
selection	countermeasure selection for		
	triage criteria (A-9) and of the best		
	technologies with respect to all		
	dispositions of security.		
A-11. Quality	The quality management service is	N/A	
management	to check problems in the quality of		
	security activities, whether or not		
	they have a negative impact for		
	business (e.g., usability,		
	productivity) over a period of time		
	(e.g., one week or one month).		
A-12. Security	The security audit service	N/A	

audit	systematically and measurably			
	audits how an organization			
	implements security policies and			
	controls at a specific site or time.			
	CDC staff are indirectly involved			
	in audit activities in order to			
	provide necessary information and			
	evidence of implemented state of			
	controls.			
A-13.	The certification service supports	N/A		
Certification	activities necessary for an			
	organization to conform to various			
	standards and certification			
	schemes.			
B-1. Real-time	The real-time asset monitoring	5.2 Service:	5.2.1 Function:	Identify events directly related to other
asset	service is to supervise and analyse	Event	Correlation	potential or ongoing security incidents.
monitoring	systems status or suspicious	analysis		
	activities from logs and network			
	flows, and supporting triage as			
	incident or event for gathering			
	information needed.			
			5.2.2 Function:	Triage and qualify detected potential
			Qualification	information security incidents in order to

				identify, categorize, and prioritize true positives.
		8.2 Service:	8.2.2 Function:	Determine and confirm the details of the
		Analysis	Event detection	current situational picture for the
		and	(through alerting	constituency.
		synthesis	and/or hunting)	
B-2. Event	The event data retention service	N/A		
data retention	collects and centrally stores events			
	gathered in the process of security			
	monitoring and analysis.			
B-3. Alerting	The alerting and warning service	N/A		
and warning	notifies the internal function			
	involved of events that highlight			
	potential risks to information			
	assets (e.g., security devices alert,			
	security bulletins, vulnerabilities			
	and spreading threats).			
B-4. Handling	The handling enquiry on report	N/A		
enquiry on	service is to respond to enquiries			
report	about data and reports regarding			
	analysis.			
C-1. Forensic	The forensic analysis service	6.3 Service:	6.3.1 Function:	Compare information gathered from the
analysis	analyses digital evidence that is	Artifact and	Media or surface	artefact with other public and private

	gathered from security assets and	forensic	analysis	artefacts and/or signature repositories.
	relates to an event to assist in	evidence		
	determining what happened.	analysis		
C-2. Malware	The malware sample analysis	6.3 Service:	6.3.2 Function:	Perform in-depth static analysis of an
sample	service is to analyse malware,	Artifact and	Reverse	artefact to determine its complete
analysis	programs or scripts deployed by	forensic	engineering	functionality, regardless of the environment
	attackers that are found during	evidence		within which it may be executed.
	each forensic process.	analysis		
			6.3.3 Function:	Provide insight into the artefact's operation.
			Run time or	
			dynamic analysis	
C-3. Tracking	The service is the capability of an	6.3 Service:	6.3.4 Function:	Perform an analysis focused on identifying
and tracing	organization to track and trace the	Artifact and	Comparative	common functionality or intent, including
	source of any attacks on its	forensic	analysis	family analysis of catalogued artefacts.
	infrastructures, which is a critical	evidence		
	success factor to reduce further	analysis		
	occurrences and prevent security			
	incidents. An acknowledged ability			
	to track and trace both internal			
	and external attackers (e.g., cyber			
	attribution) can pre-empt future			
	attacks.			
C-4. Forensic	The forensic evidence collection	N/A		

evidence	service collects and conserves			
collection	digital electronic evidence related			
	to an assessed incident, and			
	develops and maintains validity of			
	evidence ("evidence chain of			
	custody").			
D-1. Incident	The incident report acceptance	6.1 Service:	6.1.1 Function:	Accept or receive information about an
report	service is to receive analytical	Information	Information	information security incident, as reported
acceptance	reports of operations. However, it	security	security incident	from constituents or third parties.
	may receive reports from another	incident	report receipt	
	organization within the company	report		
	or from an outside organization.	acceptance		
D-2. Incident		6.1 Service:	6.1.2 Function:	Initially review, categorize, prioritize, and
handling	The incident handling service is to	Information	Information	process a reported information security
	deal with accepted incidents and	security	security incident	incident.
	coordinates activities including D-	incident	triage and	
	3 to D-7.	report	processing	
		acceptance		
		6.5 Service:	6.5.4 Function:	Track the status of all communication and
		Information	Activities	activities.
		security	coordination	
		incident		
		coordinatio		

D-3. Incident classification	The incident classification service is to classify an incident to contribute to a common understanding of the types of incident that occur and what causes them.	n 8.2 Service: Analysis and synthesis  6.2 Service: Information security incident analysis	8.2.3 Function: Information security incident management decision support 8.2.4 Function: Situational impact 6.2.1 Function: Information security incident triage (prioritization and categorization)	Identify new insights during incidents that may help limit damage, mitigate future risk, or identify a newly created weakness.  Determine the expected potential impact of a given observation or possible observation to a situational picture.  Categorize, prioritize, and create an initial assessment of an information security incident.
			6.2.2 Function: Information collection  6.2.3 Function: Detailed analysis coordination	Intake, catalog, store, and track information related to the information security incident and all information security events that are considered to be part of it.  Initiate and track any other technical analysis in regard to an information security incident.

D-4. Incident	The incident response and	6.2 Service:	6.2.4 Function:	Identify the root cause of the information
response and	containment service is to contain	Information	Information	security incident, identifying the
containment	an incident before it spreads	security	security incident	circumstances that allowed the exploited
	through all resources and	incident	root cause	vulnerabilities to exist or that allowed the
	increases the damage to or impact	analysis	analysis	exploitation to succeed (including but not
	on them.			limited to user behavior).
		6.4 Service:	6.4.1 Function:	Define and enforce a plan to restore the
		Mitigation	Response plan	integrity of affected systems and return the
		and	establishment	affected data, systems, and networks to a
		recovery		non-degraded operational state, restoring
				the impacted services to full functionality
				without recreating the context of enabling
				the original security issue to be exploited
				again.
			6.4.2 Function: Ad	Implement measures that ensure an
			hoc measures and	information security incident does not
			containment	spread any further, i.e., remains confined to
				the currently affected system, users, and/or
				domains to ensure that no further losses
				(including leakage of documents, changes to
				databases or data, etc.) can occur.
D-5. Incident	The incident recovery service is to	6.4 Service:	6.4.3 Function:	Implement changes in the affected domain,
recovery	support the restoration of the	Mitigation	System	infrastructure, or network necessary to fix

	functionality of a target to its	and	restoration	and prevent this type of activity from
	normal system operability.	recovery		reoccurring.
			6.4.4 Function:	Enable the constituents to perform the
			Other information	required management and technical
			security entities	activities in order to successfully mitigate an
			support	information security incident and recover
				from it
D-6. Incident		6.5 Service:	6.5.1 Function:	Engage effectively with stakeholders and
notification	The incident notification service is	Information	Communication	establish appropriate multiple
	to communicate the occurrence of	security		communication channels providing the
	an incident to incident response	incident		required confidentiality.
	teams and other concerned groups.	coordinatio		
		n		
			6.5.2 Function:	Alert entities impacted by the information
			Notification	security incident or those that can
			distribution	contribute to the response to it and provide
				those entities with the required information
				to understand their role of involvement and
				any expectations that might exist regarding
				their cooperation and support.
			6.5.3 Function:	Keep communicating with the identified
			Relevant	entities and provide a suitable flow of
			information	available information in order to enable

			distribution	those entities to benefit from available insights and lessons learned, to apply improved responses or take new adhoc measures.
		6.6 Service: Crisis manageme nt support	6.6.1 Function: Information distribution to constituents	Provide established communication resources to help respond to the crisis.
			6.6.2 Function: Information security status reporting	Ensure that the crisis management team has a complete overview of current information security incidents and known vulnerabilities to consider this as part of its overall priorities and strategies.
			6.6.3 Function: Strategic decisions communication	Inform other entities in a timely manner about the impact caused by the crisis on currently open information security incidents.
		7.1 Service: Vulnerabilit y discovery / research	7.1.1 Function: Incident response vulnerability discovery	Identify a vulnerability that was exploited as part of a security incident.
D-7. Incident	The incident response report	6.5 Service:	6.5.5 Function:	Ensure that all involved entities within a

response	service is to achieve the completion	Information	Reporting	business have information about the status
report	and distribution of the report of a	security		of current activities so that further decisions
	closed incident response (if	incident		about the next steps to be taken are based on
	countermeasure efforts are	coordinatio		the best situational awareness available.
	protracted, it will be handed over	n		
	to the strategic management of			
	CDC (category A)). If CDC staff			
	need a report of current status			
	during handling of an incident,			
	this service distributes an interim			
	report.			
			6.5.6 Function:	Engage with the (public) media to be able to
			Media	provide accurate and easy-to-understand
			communication	factual information about ongoing events to
				avoid the spread of rumours and misleading
				information.
E-1. Network	The network information	N/A		
information	collection service is to receive an			
collection	overview of the network			
	configuration that is to be			
	protected.			
E-2. Asset	The asset inventory service is to	8.1 Service:	8.1.2 Function:	Provide knowledge of existing assets,
inventory	achieve information management	Data	Asset mapping to	ownership, baselines and expected activity

	relevant to the census of systems,	acquisition	functions, roles,	supports analysis functions that identify
		acquisition		
	assets and applications that		actions, and key	abnormal situational observations.
	constitute the overall business		risks	
	infrastructure within the scope of			
	CDC support.			
E-3.	The vulnerability assessment	7.1 Service:	7.1.3 Function:	Discover or search for new vulnerabilities as
Vulnerability	service is to examine networks,	Vulnerabilit	Vulnerability	a result of deliberate activities or research.
assessment	systems and applications to	y discovery /	research	
	identify vulnerabilities,	research		
	determines how they can be			
	exploited and recommends how			
	the risks can be mitigated.			
		7.6 Service:	7.6.1 Function:	Actively take information about known
		Vulnerabilit	Vulnerability	vulnerabilities and act upon that
		y response	detection /	information to prevent, detect, and
			scanning	remediate/mitigate those vulnerabilities.
E-4. Patch	The patch management service is	7.6 Service:	7.6.2 Function:	Remediate or mitigate vulnerabilities to
management	to support the installation of any	Vulnerabilit	Vulnerability	prevent them from being exploited, typically
	security patches required, while	y response	remediation	through the timely application of vendor-
	the availability of information			provided patches or other solutions.
	technology (IT) service is			
	maintained.			
E-5.	The penetration test service is to	7.6 Service:	7.6.1 Function:	Actively take information about known

Penetration	reveal security vulnerabilities that	Vulnerabilit	Vulnerability	vulnerabilities and act upon that
test	could be exploited by attackers and	y response	detection /	information to prevent, detect, and
	highlights possible methods of		scanning	remediate/mitigate those vulnerabilities.
	compromise (e.g., threat-led			
	penetration test).			
E-6. Defence	The defence capability against	9.3 Service:	9.3.1 Function:	Ensure an effective outcome of the exercise
capability	advanced persistent threat (ATP)	Exercises	Requirements	by concentrating on specific issues for the
against APT	attack evaluation service is to		analysis	given scope and focus of the exercise.
attack	measure the resistance of an			
evaluation	organization to targeted attacks			
	while conducting targeted email			
	training and social engineering			
	tests.			
			9.3.2 Function:	Specify and determine the internal and
			Format and	external resources and infrastructure
			environment	needed to conduct the exercise.
			development	
			9.3.3 Function:	Provide an opportunity for the target
			Scenario	audience to improve the efficiency and
			development	effectiveness of its services and functions,
				and its skills, knowledge, and abilities,
				through the handling of simulated
				cybersecurity events/incidents, including

				communications aspects
			9.3.4 Function:	Conduct drills/exercises allowing a CSIRT
			Exercise	team to increase its confidence in the
			execution	validity of an organization's CSIRT plan and
				its ability for execution.
			9.3.5 Function:	Perform a formal and objective analysis of
			Exercise outcome	the exercise, based on factual observations.
			review	
E-7. Handling	The handling capability on cyber-	9.3 Service:	9.3.1 Function:	Ensure an effective outcome of the exercise
capability on	attack evaluation service is to	Exercises	Requirements	by concentrating on specific issues for the
cyberattack	confirm whether actual security		analysis	given scope and focus of the exercise.
evaluation	response activities based on a			
	scenario that assumes an attack			
	has occurred can be activated and			
	whether the incident can be			
	brought to an end without delay			
	(called a cyber-attack response			
	exercise).			
			9.3.2 Function:	Specify and determine the internal and
			Format and	external resources and infrastructure
			environment	needed to conduct the exercise.
			development	
			9.3.3 Function:	Provide an opportunity for the target

			Scenario	audience to improve the efficiency and
			development	effectiveness of its services and functions,
				and its skills, knowledge, and abilities,
				through the handling of simulated
				cybersecurity events/incidents, including
				communications aspects
			9.3.4 Function:	Conduct drills/exercises allowing a CSIRT
			Exercise	team to increase its confidence in the
			execution	validity of an organization's CSIRT plan and
				its ability for execution.
			9.3.5 Function:	Perform a formal and objective analysis of
			Exercise outcome	the exercise, based on factual observations.
			review	
E-8. Policy	The policy compliance service is to	N/A		
compliance	support the verification of			
	conformity to and compliance with			
	predefined security policies.			
E-9.	The hardening service is to	N/A		
Hardening	optimize IT component			
	configuration to identify, evaluate			
	and apply systems security			
	configurations, and to mitigate or			
	eliminate the risk of attacks.			

F-1. Post-	The post-mortem analysis service	5.1 Service:	5.1.2 Function:	Manage the portfolio of detection use cases
mortem	describes resolution of an incident	Monitoring	Detection use case	through their entire lifecycle.
analysis	to ensure review and improvement	and	management	
	of the processes and tools for CDC	detection		
	staff.			
		6.2 Service:	6.2.5 Function:	Enable the usage of all available information
		Information	Cross-incident	to get the best understanding of the context
		security	correlation	and detect interrelationships that otherwise
		incident		would not have been recognized or acted
		analysis		upon.
F-2. Internal	The internal threat intelligence	6.3 Service:	6.3.4 Function:	Perform an analysis focused on identifying
threat	collection and analysis service is to	Artifact and	Comparative	common functionality or intent, including
intelligence	gather information (internal	forensic	analysis	family analysis of catalogued artefacts.
collection and	intelligence) on real-time analysis	evidence		
analysis	and incident response.	analysis		
		7.1 Service:	7.1.1 Function:	Identify a vulnerability that was exploited
		Vulnerabilit	Incident response	as part of a security incident.
		y discovery/	vulnerability	
		research	discovery	
		7.2 Service:	7.2.1 Function:	Accept or receive information about a
		Vulnerabilit	Vulnerability	vulnerability, as reported from constituents
		y report	report receipt	or third
		intake		parties.

		7.2.2 Function:	Initially review, categorize, prioritize, and
		Vulnerability	process a vulnerability report.
		report triage and	
		processing	
	7.3 Service:	7.3.1 Function:	Categorize, prioritize, and perform an initial
	Vulnerabilit	Vulnerability	assessment of a vulnerability.
	y analysis	triage (validation	
		and	
		categorization)	
		7.3.2 Function:	Understand the design or implementation
		Vulnerability root	flaw that causes or exposes the vulnerability
		cause analysis	to exist.
		7.3.3 Function:	Develop the steps necessary to fix
		Vulnerability	(remediate) the underlying vulnerability or
		remediation	mitigate (reduce) the effects of the
		development	vulnerability from being exploited.
	8.1 Service:	8.1.3 Function:	Collect of information to support the
	Data	Collection	Analysis and Interpretation service and/or
	acquisition		other CSIRT services.
	8.2 Service:	8.2.1 Function:	Analyze the information collected during
	Analysis	Projection and	data acquisition with the intent of
	and	inference	identifying current or predicting future
	synthesis		situational pictures.

F-3. External	The external threat intelligence	7.1 Service:	7.1.2 Function:	Learn about a new vulnerability from
threat	collection and evaluation service is	Vulnerabilit	Public source	reading public sources or other third-party
intelligence	to gather information (external	y discovery /	vulnerability	sources.
collection and	intelligence), such as new	research	discovery	
evaluation	vulnerabilities, attack trends,			
	malware behaviour and malignant			
	Internet protocol addresses or			
	domain information.			
		7.2 Service:	7.2.1 Function:	Accept or receive information about a
		Vulnerabilit	Vulnerability	vulnerability, as reported from constituents
		y report	report receipt	or third
		intake		parties.
			7.2.2 Function:	Initially review, categorize, prioritize, and
			Vulnerability	process a vulnerability report.
			report triage and	
			processing	
		7.3 Service:	7.3.1 Function:	Categorize, prioritize, and perform an initial
		Vulnerabilit	Vulnerability	assessment of a vulnerability.
		y analysis	triage (validation	
			and	
			categorization)	
			7.3.2 Function:	Understand the design or implementation
			Vulnerability root	flaw that causes or exposes the vulnerability

			cause analysis	to exist.
			7.3.3 Function:	Develop the steps necessary to fix
			Vulnerability	
				(remediate) the underlying vulnerability or
			remediation	mitigate (reduce) the effects of the
			development	vulnerability from being exploited.
		8.1 Service:	8.1.3 Function:	Collect of information to support the
		Data	Collection	Analysis and Interpretation service and/or
		acquisition		other CSIRT services.
		8.2 Service:	8.2.1 Function:	Analyze the information collected during
		Analysis	Projection and	data acquisition with the intent of
		and	inference	identifying current or predicting future
		synthesis		situational pictures.
F-4. Threat	The threat intelligence report	7.3 Service:	7.3.3 Function:	Develop the steps necessary to fix
intelligence	service is to compile internal and	Vulnerabilit	Vulnerability	(remediate) the underlying vulnerability or
report	external threat information and	y analysis	remediation	mitigate (reduce) the effects of the
	document it, including all details.		development	vulnerability from being exploited.
		8.3 Service:	8.3.2 Function:	Create results, artefacts, or findings that
		Communica	Reporting and	communicate critical information discovered
		tion	recommendations	or created during analysis to audiences in a
				manner and format that they will
				understand.
F-5. Threat	The threat intelligence utilization	7.5 Service:	7.5.2 Function:	Provide information to constituents (or the
intelligence	service is to achieve compilation	Vulnerabilit	Vulnerability	public) about a new vulnerability, so that

utilization	and dissemination of threat	y disclosure	announcement /	they can detect, remediate or mitigate, and
	information for all categories of		communication /	prevent future exploitation of the
	security response.		dissemination	vulnerability.
			7.5.3 Function:	Receive and respond to questions or reports
			Post-vulnerability	from constituents about a vulnerability
			disclosure	disclosure or document.
			feedback	
		8.1 Service:	8.1.4 Function:	Establish a reliable, consistent, and current
		Data	Data processing	set of data that can support CSIRT activities
		acquisition	and preparation	and the requirements of the analysis service.
G-1. Security	The security architecture	5.1 Service:	5.1.1 Function:	Manage log sources and sensors.
architecture	implementation service is to	Monitoring	Log and sensor	
implementatio	implement the security	and	management	
n	architecture designed by strategic	detection		
	management of CDC (category A)			
	by using assets.			
		8.3 Service:	8.3.3 Function:	Adapt the constituent environment based on
		Communica	Implementation	communications to be more prepared for or
		tion		react to changes in the situational picture.
G-2. Basic	The basic operation for network	5.1 Service:	5.1.1 Function:	Manage log sources and sensors.
operation for	security asset service is to operate	Monitoring	Log and sensor	
network	network devices, such as firewalls,	and	management	
security asset	intrusion detection	detection		

	system/intrusion prevention system (IDS/IPS), web application			
	firewall (WAF) and proxies.			
G-3. Advanced	The advanced operation for	5.1 Service:	5.1.2 Function:	Manage the portfolio of detection use cases
operation for	network security asset service is to	Monitoring	Detection use case	through their entire lifecycle.
network	create custom signatures of an	and	management	
security asset	organization for products with	detection		
	attack detection capabilities, such			
	as IDS/IPS and WAF, and applies			
	them if the signature provided by			
	the vendor is insufficient.			
			5.1.3 Function:	Manage of contextual data sources for
			Contextual data	detection and enrichment.
			management	
		8.3 Service:	8.3.3 Function:	Adapt the constituent environment based on
		Communica	Implementation	communications to be more prepared for or
		tion		react to changes in the situational picture.
G-4. Basic	The basic operation for endpoint	5.1 Service:	5.1.1 Function:	Manage log sources and sensors.
operation for	security asset service is to operate	Monitoring	Log and sensor	
endpoint	countermeasure products, such as	and	management	
security asset	anti-virus software, at endpoints.	detection		
G-5. Advanced	The advanced operation for	5.1 Service:	5.1.2 Function:	Manage the portfolio of detection use cases
operation for	endpoint security asset service is	Monitoring	Detection use case	through their entire lifecycle.

endpoint	to detect suspicious program	and	management	
security asset	activity within the endpoint using	detection		
	its protection product, and collects			
	and analyses registry status,			
	process execution, etc. If needed,			
	the service establishes customised			
	indicators of compromise to enable			
	endpoint detection.			
			5.1.3 Function:	Manage of contextual data sources for
			Contextual data	detection and enrichment.
			management	
		8.3 Service:	8.3.3 Function:	Adapt the constituent environment based on
		Communica	Implementation	communications to be more prepared for or
		tion		react to changes in the situational picture.
G-6. Basic	The basic operation for cloud	5.1 Service:	5.1.1 Function:	Manage log sources and sensors.
operation for	security products service is to	Monitoring	Log and sensor	
cloud security	operate security services in a	and	management	
products	cloud.	detection		
G-7. Advanced	The advanced operation for cloud	5.1 Service:	5.1.2 Function:	Manage the portfolio of detection use cases
operation for	security products service is to	Monitoring	Detection use case	through their entire lifecycle.
cloud security	create custom signatures of an	and	management	
products	organization for security services	detection		
	in a cloud with attack detection			

	capabilities. If the signature provided by a vendor is insufficient, the service applies custom signatures.			
			5.1.3 Function: Contextual data management	Manage of contextual data sources for detection and enrichment.
		8.3 Service: Communica tion	8.3.3 Function: Implementation	Adapt the constituent environment based on communications to be more prepared for or react to changes in the situational picture.
G-8. Deep analysis tool	The deep analysis tool operation service is to operate tools used in	N/A		
operation	deep analysis, such as digital forensics and malware analysis.			
G-9. Basic operation for analysis platform	The basic operation for analysis platform service is to operate analytical infrastructure that stores the log data required and enables the analysis to be performed routinely, mainly in real-time analysis, such as security information and event management (SIEM).	N/A		

G-10.	The advanced operation for	5.1 Service:	5.1.2 Function:	Manage the portfolio of detection use cases
Advanced	analysis platform service is to	Monitoring	Detection use case	through their entire lifecycle.
operation for	achieve more detailed and	and	management	
analysis	accurate analysis using the	detection		
platform	organization's own systems to			
	retain system logs and packet			
	capture data that commercial			
	SIEMs cannot capture, and			
	develops customized analysis			
	algorithms and logic for these			
	data, as well as the system.			
			5.1.3 Function:	Manage of contextual data sources for
			Contextual data	detection and enrichment.
			management	
G-11. Operates	The operates CDC systems service	N/A		
CDC/CSC	is to operate systems that perform			
systems	the tasks required for security			
	response operations, such as the			
	various security response tools			
	previously described, the			
	production of various reports, the			
	response to enquiries, and the			
	vulnerability management			

	system.			
G-12. Existing	The existing security tools	N/A		
security tools	evaluation service is to verify the			
evaluation	impact on other systems and			
	operations, mainly in terms of			
	availability, when upgrading or			
	changing the settings of existing			
	security-enabled tools.			
G-13. New	The new security tools evaluation	7.3 Service:	7.3.3 Function:	Develop the steps necessary to fix
security tools	service is to design and install new	Vulnerabilit	Vulnerability	(remediate) the underlying vulnerability or
evaluation	security assets, if new measures	y analysis	remediation	mitigate (reduce) the effects of the
	are needed in security activities.		development	vulnerability from being exploited.
H-1. Internal	The internal fraud response and	6.4 Service:	6.4.4 Function:	Enable the constituents to perform the
fraud response	analysis support service is to	Mitigation	Other information	required management and technical
and analysis	support the organization	and	security entities	activities in order to successfully mitigate an
support	responding to internal fraud when	recovery	support	information security incident and recover
	it is discovered, by organizing its			from it
	activities from the logs collected by			
	the security activities.			
H-2. Internal	The internal fraud detection and	N/A		
fraud detection	reoccurrence prevention support			
and	service is to analyse the details of			
reoccurrence	internal fraudulent activities that			

prevention	have been discovered, and			
support	considers whether it is possible to			
	detect them from the logs, and if			
	so, implements the detection logic.			
I-1. Awareness	The awareness service is to	9.1 Service:	9.1.1 Function:	Aggregate, collate, and prioritize
	precisely create awareness for the	Awareness	Research and	information that can be disseminated to the
	relevant staff across and in	build	information	constituency for the improvement of the
	relation to the CDC, promotes the		aggregation	security posture and prevention and
	utilization of the correct tools, best			mitigation of risks.
	practice, policies and resources to			
	ensure protection of the business			
	assets.			
			9.1.2 Function:	Use the information aggregated and
			Reports and	researched as being relevant to produce
			awareness	materials in different media with the goal of
			materials	reaching different audiences or delivering
			development	specific content in the best
				way possible.
			9.1.3 Function:	Disseminate security-related information to
			Information	improve awareness and implementation of
			dissemination	security practices.
			9.1.4 Function:	Develop and maintain relationships with
			Outreach	experts or organizations that may help or be

				part of the execution of the mission of the CSIRT.
I-2. Education	The education and training service	6.4 Service:	6.4.4 Function:	Enable the constituents to perform the
and training	is to support specialized training	Mitigation	Other information	required management and technical
	activities in the areas of security	and	security entities	activities inorder to successfully mitigate an
	for staff in the organizations that	recovery	support	information security incident and recover
	the CDC supports.			from it.
		9.2 Service:	9.2.1 Function:	Properly assess, identify, and document
		Training	Knowledge, skill,	what the constituency needs are in terms of
		and	and ability	requisite KSAs, to develop appropriate
		education	requirements	training and education materials and
			gathering	improve its skill level.
			9.2.2 Function:	Develop, using the constituency's KSA needs
			Educational and	as a basis, educational, instructional, and
			training materials	training material that is appropriate to the
			development	delivery methods identified as the best to
				reach different audiences or deliver specific
				content.
			9.2.3 Function:	Develop a formal process for content delivery
			Content delivery	that can help the CSIRT to best deliver the
				content to its constituency, based on the
				characteristics of different audiences and
				content.

			9.2.4 Function:	Develop a program for CSIRT staff,
			Mentoring	constituency members, or external trusted
				partners to learn from experienced staff
				through an established relationship.
			9.2.5 Function:	Help staff members successfully and
			CSIRT staff	appropriately plan and develop their
			professional	careers.
			development	
I-3. Security		9.4 Service:	9.4.4 Function:	Provide technical advice that can help the
consulting	The security consulting service	Technical	Technical advice	constituency to better manage risks and
	provides consultancy services to	and policy		threats and implement current operational
	the various business functions	advisory		and security best practices, while enabling
	with regards to security.			effective incident
				handling activities.
I-4. Security	The security vendor collaboration	N/A		
vendor	service is to build a direct line of			
collaboration	communication with the provider			
	of a security product or service			
	purchased, requests a response to			
	any deficiencies found in the			
	security response and exchanges			
	positive feedback on areas for			
	improvement.			

I-5.	The collaboration service with	7.4 Service:	7.4.1 Function:	Initial share or report new vulnerability
Collaboration	external security communities is	Vulnerabilit	Vulnerability	information with others who are to be
service with	to exchange information	у	notification/report	involved in the CVD process.
external	proactively by participating in	coordinatio	ing	
security	external communities. Such	n		
communities	information can reflect on the			
	security activities.			
			7.4.2 Function:	Conduct follow-on coordination and sharing
			Vulnerability	of information among the various
			stakeholder	stakeholders and participants involved in
			coordination	coordinated vulnerability disclosure (CVD)
				efforts.
		8.3 Service:	8.3.1 Function:	Inform constituents (and others) of the
		Communica	Internal and	current situational picture and how it may
		tion	external	be changing.
			communication	
			8.3.4 Function:	Assemble, normalize, and prepare
			Dissemination /	information and then share it with
			integration /	constituents and others outside the
			information	constituency.
			sharing	
			8.3.5 Function:	Ensure transfer of information is successful
			Management of	and useable.

			informa	tion	
			sharing		
			8.3.6	Function:	Improve the quality, timeliness, accuracy,
			Feedbac	k	and relevance of the data being received
					from internal and external sources.
I-6. Technical	The technical reporting service is	N/A			
reporting	to provide reports of the results of				
	monitoring and management				
	activities. These activities help to				
	show the security level of systems				
	and IT infrastructure.				
I-7. Executive	The executive security reporting	N/A			
security	service is to produce periodic				
reporting	reports and statistical analysis to				
	top management to highlight the				
	security level and indicators of				
	operational performance of an				
	organization.				

## 2. Mapping with X.1060

FIRST CSIRT	Services Framewo	ork version 2.1.0	X.1060	
Service	Function	Purpose	Service	Description
5.1 Service:	5.1.1 Function:	Manage log sources and sensors.	G-1. Security	The security architecture implementation
Monitoring	Log and sensor		architecture	service is to implement the security
and detection	management		implementation	architecture designed by strategic
				management of CDC (category A) by using
				assets.
			G-2. Basic	The basic operation for network security asset
			operation for	service is to operate network devices, such as
			network security	firewalls, intrusion detection
			asset	system/intrusion prevention system
				(IDS/IPS), web application firewall (WAF) and
				proxies.
			G-4. Basic	The basic operation for endpoint security
			operation for	asset service is to operate countermeasure
			endpoint	products, such as anti-virus software, at
			security asset	endpoints.
			G-6. Basic	The basic operation for cloud security
			operation for	products service is to operate security services
			cloud security	in a cloud.
			products	iii a ciouu.

5.1.2 Function:	Manage the portfolio of detection	F-1. Post-	The post-mortem analysis service describes
Detection use	use cases through their entire	mortem analysis	resolution of an incident to ensure review and
case	lifecycle.		improvement of the processes and tools for
management			CDC staff.
		G-3. Advanced	The advanced operation for network security
		operation for	asset service is to create custom signatures of
		network security	an organization for products with attack
		asset	detection capabilities, such as IDS/IPS and
			WAF, and applies them if the signature
			provided by the vendor is insufficient.
		G-5. Advanced	The advanced operation for endpoint security
		operation for	asset service is to detect suspicious program
		endpoint	activity within the endpoint using its
		security asset	protection product, and collects and analyses
			registry status, process execution, etc. If
			needed, the service establishes customised
			indicators of compromise to enable endpoint
			detection.
		G-7. Advanced	The advanced operation for cloud security
		operation for	products service is to create custom
		cloud security	signatures of an organization for security
		products	services in a cloud with attack detection
			capabilities. If the signature provided by a

			vendor is insufficient, the service applies custom signatures.
		G-10. Advanced operation for analysis platform	The advanced operation for analysis platform service is to achieve more detailed and accurate analysis using the organization's own systems to retain system logs and packet capture data that commercial SIEMs cannot capture, and develops customized analysis algorithms and logic for these data, as well as the system.
5.1.3 Function: Contextual data management	Manage of contextual dat sources for detection and enrichment.		The advanced operation for network security asset service is to create custom signatures of an organization for products with attack detection capabilities, such as IDS/IPS and WAF, and applies them if the signature provided by the vendor is insufficient.
		G-5. Advanced operation for endpoint security asset	The advanced operation for endpoint security asset service is to detect suspicious program activity within the endpoint using its protection product, and collects and analyses registry status, process execution, etc. If needed, the service establishes customised indicators of compromise to enable endpoint

				detection.
			G-7. Advanced	The advanced operation for cloud security
			operation for	products service is to create custom
			cloud security	signatures of an organization for security
			products	services in a cloud with attack detection
				capabilities. If the signature provided by a
				vendor is insufficient, the service applies
				custom signatures.
			G-10. Advanced	The advanced operation for analysis platform
			operation for	service is to achieve more detailed and
			analysis	accurate analysis using the organization's
			platform	own systems to retain system logs and packet
				capture data that commercial SIEMs cannot
				capture, and develops customized analysis
				algorithms and logic for these data, as well as
				the system.
5.2 Service:	5.2.1 Function:	Identify events directly related	B-1. Real-time	The real-time asset monitoring service is to
Event	Correlation	to other potential or ongoing	asset monitoring	supervise and analyse systems status or
analysis		security incidents.		suspicious activities from logs and network
				flows, and supporting triage as incident or
				event for gathering information needed.
	5.2.2 Function:	Triage and qualify detected	B-1. Real-time	The real-time asset monitoring service is to
	Qualification	potential information security	asset monitoring	supervise and analyse systems status or

6.1 Service: Information security incident report acceptance	6.1.1 Function: Information security incident report receipt	incidents in order to identify, categorize, and prioritize true positives.  Accept or receive information about an information security incident, as reported from constituents or third parties.	D-1. Incident report acceptance	suspicious activities from logs and network flows, and supporting triage as incident or event for gathering information needed.  The incident report acceptance service is to receive analytical reports of operations. However, it may receive reports from another organization within the company or from an outside organization.
	6.1.2 Function: Information security incident triage and processing	Initially review, categorize, prioritize, and process a reported information security incident.	D-2. Incident handling	The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7.
6.2 Service:	6.2.1 Function:	Categorize, prioritize, and create	D-3. Incident	
Information	Information	an initial assessment of an	classification	
security	security	information security incident.		The incident classification service is to
incident	incident triage			classify an incident to contribute to a common
analysis	(prioritization			understanding of the types of incident that
	and			occur and what causes them.
	categorizatio			
	n)			
	6.2.2 Function:	Intake, catalog, store, and track	D-3. Incident	The incident classification service is to

Information	information related to the	classification	classify an incident to contribute to a common
collection	information security incident		understanding of the types of incident that
	and all information security		occur and what causes them.
	events that are considered to be		
	part of it.		
6.2.3 Function	Initiate and track any other	D-3. Incident	The incident classification service is to
Detailed	technical analysis in regard to an	classification	classify an incident to contribute to a common
analysis	information security incident.		understanding of the types of incident that
coordination			occur and what causes them.
6.2.4 Function	Identify the root cause of the	D-4. Incident	
Information	information security incident,	response and	
security	identifying the circumstances	containment	The incident response and containment
incident roo	t that allowed the exploited		service is to contain an incident before it
cause analysis	vulnerabilities to exist or that		spreads through all resources and increases
	allowed the exploitation to		the damage to or impact on them.
	succeed (including but not		
	limited to user behavior).		
6.2.5 Function	Enable the usage of all available	F-1. Post-	
Cross-incident	information to get the best	mortem analysis	The post-mortem analysis service describes
correlation	understanding of the context and		resolution of an incident to ensure review and
	detect interrelationships that		improvement of the processes and tools for
	otherwise would not have been		CDC staff.
	recognized or acted upon.		

6.3 Service: Artifact and forensic evidence analysis	6.3.1 Function: Media or surface analysis	Compare information gathered from the artefact with other public and private artefacts and/or signature repositories.	C-1. Forensic analysis	The forensic analysis service analyses digital evidence that is gathered from security assets and relates to an event to assist in determining what happened.
	6.3.2 Function: Reverse engineering	Perform in-depth static analysis of an artefact to determine its complete functionality, regardless of the environment within which it may be executed.	C-2. Malware sample analysis	The malware sample analysis service is to analyse malware, programs or scripts deployed by attackers that are found during each forensic process.
	6.3.3 Function: Run time or dynamic analysis	Provide insight into the artefact's operation.	C-2. Malware sample analysis	The malware sample analysis service is to analyse malware, programs or scripts deployed by attackers that are found during each forensic process.
	6.3.4 Function: Comparative analysis	Perform an analysis focused on identifying common functionality or intent, including family analysis of catalogued artefacts.	C-3. Tracking and tracing	The service is the capability of an organization to track and trace the source of any attacks on its infrastructures, which is a critical success factor to reduce further occurrences and prevent security incidents. An acknowledged ability to track and trace both internal and external attackers (e.g., cyber attribution) can pre-empt future attacks.

6.4 Service:	6.4.1 Function:	Define and enforce a plan to	D-4. Incident	
Mitigation	Response plan	restore the integrity of affected	response and	
and recovery	establishment	systems and return the affected	containment	
		data, systems, and networks to a		The incident response and containment
		non-degraded operational state,		service is to contain an incident before it
		restoring the impacted services		spreads through all resources and increases
		to full functionality without		the damage to or impact on them.
		recreating the context of		
		enabling the original security		
		issue to be exploited again.		
	6.4.2 Function:	Implement measures that	D-4. Incident	
	Ad hoc	ensure an information security	response and	
	measures and	incident does not spread any	containment	The incident response and containment
	containment	further, i.e., remains confined to		service is to contain an incident before it
		the currently affected system,		spreads through all resources and increases
		users, and/or domains to ensure		the damage to or impact on them.
		that no further losses (including		the damage to of impact on them.
		leakage of documents, changes to		
		databases or data, etc.) can occur.		
	6.4.3 Function:	Implement changes in the	D-5. Incident	The incident recovery service is to support the
	System	affected domain, infrastructure,	recovery	restoration of the functionality of a target to
	restoration	or network necessary to fix and		its normal system operability.
		prevent this type of activity from		Too norman system operating.

		reoccurring.		
	6.4.4 Function: Other information security entities support	Enable the constituents to perform the required management and technical activities in order to successfully mitigate an information security incident and recover from it	D-5. Incident recovery	The incident recovery service is to support the restoration of the functionality of a target to its normal system operability.
			H-1. Internal fraud response and analysis support	The internal fraud response and analysis support service is to support the organization responding to internal fraud when it is discovered, by organizing its activities from the logs collected by the security activities.
6.5 Service: Information security incident coordination	6.5.1 Function: Communicatio n	Engage effectively with stakeholders and establish appropriate multiple communication channels providing the required confidentiality.	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.
	6.5.2 Function: Notification distribution	Alert entities impacted by the information security incident or those that can contribute to the response to it and provide those entities with the required	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.

	information to understand their		
	role of involvement and any		
	expectations that might exist		
	regarding their cooperation and		
	support.		
6.5.3 Function:	Keep communicating with the	D-6. Incident	
Relevant	identified entities and provide a	notification	
information	suitable flow of available		
distribution	information in order to enable		The incident notification service is to
	those entities to benefit from		communicate the occurrence of an incident to
	available insights and lessons		incident response teams and other concerned
	learned, to		groups.
	apply improved responses or		
	take new ad-hoc measures.		
6.5.4 Function:	Track the status of all	D-2. Incident	The incident handling service is to deal with
Activities	communication and activities.	handling	accepted incidents and coordinates activities
coordination			including D-3 to D-7.
 6.5.5 Function:	Ensure that all involved entities	D-7. Incident	The incident response report service is to
Reporting	within a business have	response report	achieve the completion and distribution of the
	information about the status of		report of a closed incident response (if
	current activities so that further		countermeasure efforts are protracted, it will
	decisions about the next steps to		be handed over to the strategic management
	be taken are based on the best		of CDC (category A)). If CDC staff need a

		situational awareness available.		report of current status during handling of an incident, this service distributes an interim report.
	6.5.6 Function: Media communicatio n	Engage with the (public) media to be able to provide accurate and easy-to-understand factual information about ongoing events to avoid the spread of rumours and misleading information.		The incident response report service is to achieve the completion and distribution of the report of a closed incident response (if countermeasure efforts are protracted, it will be handed over to the strategic management of CDC (category A)). If CDC staff need a report of current status during handling of an incident, this service distributes an interim report.
6.6 Service: Crisis management support	6.6.1 Function: Information distribution to constituents	Provide established communication resources to help respond to the crisis.	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.
	6.6.2 Function: Information security status reporting	Ensure that the crisis management team has a complete overview of current information security incidents and known vulnerabilities to consider this as part of its overall priorities and	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.

	6.6.3 Function: Strategic decisions communicatio n	strategies.  Inform other entities in a timely manner about the impact caused by the crisis on currently open information security incidents.	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.
7.1 Service: Vulnerability discovery / research	7.1.1 Function: Incident response vulnerability discovery	Identify a vulnerability that was exploited as part of a security incident.	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.
			F-2. Internal threat intelligence collection and analysis	The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
	7.1.2 Function: Public source vulnerability discovery	Learn about a new vulnerability from reading public sources or other third-party sources.	F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
	7.1.3 Function:	Discover or search for new	E-	The vulnerability assessment service is to

		Vulnerability	vulnerabilities as a result of	3.Vulnerability	examine networks, systems and applications
		research	deliberate activities or research.	assessment	to identify vulnerabilities, determines how
					they can be exploited and recommends how
					the risks can be mitigated.
				E-5. Penetration	The penetration test service is to reveal
				test	security vulnerabilities that could be
					exploited by attackers and highlights possible
					methods of compromise (e.g., threat-led
					penetration test).
				E-6. Defence	The defence capability against advanced
				capability	persistent threat (ATP) attack evaluation
				against APT	service is to measure the resistance of an
				attack	organization to targeted attacks while
				evaluation	conducting targeted email training and social
					engineering tests.
				E-7. Handling	The handling capability on cyber-attack
				capability on	evaluation service is to confirm whether
				cyberattack	actual security response activities based on a
				evaluation	scenario that assumes an attack has occurred
					can be activated and whether the incident can
					be brought to an end without delay (called a
					cyber-attack response exercise).
7.2	Service:	7.2.1 Function:	Accept or receive information	F-2. Internal	The internal threat intelligence collection and

Vulnerability report intake	Vulnerability report receipt	about a vulnerability, as reported from constituents or third parties.	threat intelligence collection and analysis	analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
			F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
	7.2.2 Function: Vulnerability report triage and processing	Initially review, categorize, prioritize, and process a vulnerability report.	F-2. Internal threat intelligence collection and analysis	The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
			F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
7.3 Service: Vulnerability	7.3.1 Function: Vulnerability	Categorize, prioritize, and perform an initial assessment of	F-2. Internal threat	The internal threat intelligence collection and analysis service is to gather information

analysis	triage	a vulnerability.	intelligence	(internal intelligence) on real-time analysis
	(validation and		collection and	and incident response.
	categorization)		analysis	
			F-3. External	The external threat intelligence collection and
			threat	evaluation service is to gather information
			intelligence	(external intelligence), such as new
			collection and	vulnerabilities, attack trends, malware
			evaluation	behaviour and malignant Internet protocol
				addresses or domain information.
	7.3.2 Function: Vulnerability root cause analysis	Understand the design or implementation flaw that causes or exposes the vulnerability to exist.	F-2. Internal threat intelligence collection and analysis	The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
			F-3. External	The external threat intelligence collection and
			threat	evaluation service is to gather information (external intelligence), such as new
			intelligence collection and	(external intelligence), such as new vulnerabilities, attack trends, malware
			collection and evaluation	behaviour and malignant Internet protocol
			Cvaiuation	addresses or domain information.
	7.3.3 Function:	Develop the steps necessary to	F-2. Internal	The internal threat intelligence collection and
	Vulnerability	fix (remediate) the underlying	threat	analysis service is to gather information
	remediation	vulnerability or mitigate		(internal intelligence) on real-time analysis

	development	(reduce) the effects of the vulnerability from being exploited.	collection and analysis	and incident response.
			F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
			F-4. Threat intelligence report	The threat intelligence report service is to compile internal and external threat information and document it, including all details.
			G-13. New security tools evaluation	The new security tools evaluation service is to design and install new security assets, if new measures are needed in security activities.
7.4 Service: Vulnerability coordination	7.4.1 Function: Vulnerability notification/re porting	Initial share or report new vulnerability information with others who are to be involved in the CVD process.	I-5. Collaboration service with external security communities	The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
	7.4.2 Function:	Conduct follow-on coordination	I-5.	The collaboration service with external

	Vulnerability stakeholder coordination	and sharing of information among the various stakeholders and participants involved in coordinated vulnerability disclosure (CVD) efforts.	Collaboration service with external security communities	security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
7.5 Service: Vulnerability disclosure	7.5.1 Function: Vulnerability disclosure policy and infrastructure maintenance	Develop and maintain a policy that provides a framework and sets expectations for how a CSIRT handles and discloses vulnerabilities and the mechanism(s) used to disclose the vulnerability.	A-3. Policy planning	The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines.
	7.5.2 Function: Vulnerability announcement / communicatio n / dissemination	Provide information to constituents (or the public) about a new vulnerability, so that they can detect, remediate or mitigate, and prevent future exploitation of the vulnerability.	F-5. Threat intelligence utilization	The threat intelligence utilization service is to achieve compilation and dissemination of threat information for all categories of security response.
	7.5.3 Function: Post- vulnerability disclosure	Receive and respond to questions or reports from constituents about a vulnerability disclosure or document.	F-5. Threat intelligence utilization	The threat intelligence utilization service is to achieve compilation and dissemination of threat information for all categories of security response.

	feedback			
7.6 Service: Vulnerability response	7.6.1 Function: Vulnerability detection / scanning	Actively take information about known vulnerabilities and act upon that information to prevent, detect, and remediate/mitigate those vulnerabilities.	E-3. Vulnerability assessment	The vulnerability assessment service is to examine networks, systems and applications to identify vulnerabilities, determines how they can be exploited and recommends how the risks can be mitigated.
			E-5. Penetration test	The penetration test service is to reveal security vulnerabilities that could be exploited by attackers and highlights possible methods of compromise (e.g., threat-led penetration test).
	7.6.2 Function: Vulnerability remediation	Remediate or mitigate vulnerabilities to prevent them from being exploited, typically through the timely application of vendor-provided patches or other solutions.	E-4. Patch management	The patch management service is to support the installation of any security patches required, while the availability of information technology (IT) service is maintained.
8.1 Service: Data acquisition	8.1.1 Function: Policy aggregation, distillation, and guidance	Establish the context with which the constituency and its assets should comply to know what should be occurring on the infrastructure.	A-3. Policy planning	The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines.

	8.1.2 Function: Asset mapping to functions, roles, actions, and key risks	Provide knowledge of existing assets, ownership, baselines and expected activity supports analysis functions that identify abnormal situational observations.		The asset inventory service is to achieve information management relevant to the census of systems, assets and applications that constitute the overall business infrastructure within the scope of CDC support.
	8.1.3 Function: Collection	Collect of information to support the Analysis and Interpretation service and/or other CSIRT services.	F-2. Internal threat intelligence collection and analysis	The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
			F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
	8.1.4 Function: Data processing and preparation	Establish a reliable, consistent, and current set of data that can support CSIRT activities and the requirements of the analysis service.	F-5. Threat intelligence utilization	The threat intelligence utilization service is to achieve compilation and dissemination of threat information for all categories of security response.
8.2 Service:	8.2.1 Function:	Analyze the information	F-2. Internal	The internal threat intelligence collection and

Analysis and synthesis	Projection and inference	collected during data acquisition with the intent of identifying current or predicting future situational pictures.	threat intelligence collection and analysis	analysis service is to gather information (internal intelligence) on real-time analysis and incident response.
			F-3. External threat intelligence collection and evaluation	The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.
	8.2.2 Function: Event detection (through alerting and/or hunting)	Determine and confirm the details of the current situational picture for the constituency.	B-1. Real-time asset monitoring	The real-time asset monitoring service is to supervise and analyse systems status or suspicious activities from logs and network flows, and supporting triage as incident or event for gathering information needed.
	8.2.3 Function: Information security incident management decision support	Identify new insights during incidents that may help limit damage, mitigate future risk, or identify a newly created weakness.		The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7.

	8.2.4 Function: Situational impact	Determine the expected potential impact of a given observation or possible observation to a situational picture.	D-2. Incident handling	The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7.
8.3 Service: Communicati on	8.3.1 Function: Internal and external communicatio n	Inform constituents (and others) of the current situational picture and how it may be changing.	I-5. Collaboration service with external security communities	The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
	8.3.2 Function: Reporting and recommendati ons	Create results, artefacts, or findings that communicate critical information discovered or created during analysis to audiences in a manner and format that they will understand.	F-4. Threat intelligence report	The incident response report service is to achieve the completion and distribution of the report of a closed incident response (if countermeasure efforts are protracted, it will be handed over to the strategic management of CDC (category A)). If CDC staff need a report of current status during handling of an incident, this service distributes an interim report.
	8.3.3 Function: Implementatio	Adapt the constituent environment based on communications to be more	G-1. Security architecture implementation	The security architecture implementation service is to implement the security architecture designed by strategic

	prepared for or react to changes		management of CDC (category A) by using
	in the situational picture.		assets.
		G-3. Advanced	The advanced operation for network security
		operation for	asset service is to create custom signatures of
		network security	an organization for products with attack
		asset	detection capabilities, such as IDS/IPS and
			WAF, and applies them if the signature
			provided by the vendor is insufficient.
		G-5. Advanced	The advanced operation for endpoint security
		operation for	asset service is to detect suspicious program
		endpoint	activity within the endpoint using its
		security asset	protection product, and collects and analyses
			registry status, process execution, etc. If
			needed, the service establishes customised
			indicators of compromise to enable endpoint
			detection.
		G-7. Advanced	The advanced operation for cloud security
		operation for	products service is to create custom
		cloud security	signatures of an organization for security
		products	services in a cloud with attack detection
			capabilities. If the signature provided by a
			vendor is insufficient, the service applies
			custom signatures.

	8.3.4 Function: Dissemination / integration / information sharing	Assemble, normalize, and prepare information and then share it with constituents and others outside the constituency.	I-5. Collaboration service with external security communities	The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
	8.3.5 Function: Management of information sharing	Ensure transfer of information is successful and useable.	I-5. Collaboration service with external security communities	The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
	8.3.6 Function: Feedback	Improve the quality, timeliness, accuracy, and relevance of the data being received from internal and external sources.	I-5. Collaboration service with external security communities	The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.
9.1 Service: Awareness build	9.1.1 Function: Research and information aggregation	Aggregate, collate, and prioritize information that can be disseminated to the constituency for the improvement of the security posture and prevention	I-1. Awareness	The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business

		and mitigation of risks.		assets.
	9.1.2 Function: Reports and awareness materials development	Use the information aggregated and researched as being relevant to produce materials in different media with the goal of reaching different audiences or delivering specific content in the best way possible.	I-1. Awareness	The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business assets.
	9.1.3 Function: Information dissemination	Disseminate security-related information to improve awareness and implementation of security practices.	I-1. Awareness	The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business assets.
	9.1.4 Function: Outreach	Develop and maintain relationships with experts or organizations that may help or be part of the execution of the mission of the CSIRT.	I-1. Awareness	The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business assets.
9.2 Service: Training and education	9.2.1 Function: Knowledge, skill, and	Properly assess, identify, and document what the constituency needs are in terms of requisite	I-2. Education and training	The education and training service is to support specialized training activities in the areas of security for staff in the organizations

ability	KSAs, to develop appropriate		that the CDC supports.
requirements	training and education materials		
gathering	and improve its skill level.		
9.2.2 Function:	Develop, using the constituency's	I-2. Education	
Educational	KSA needs as a basis,	and training	
and training	educational, instructional, and		The education and training service is to
materials	training material that is		support specialized training activities in the
development	appropriate to the delivery		areas of security for staff in the organizations
	methods identified as the best to		that the CDC supports.
	reach different audiences or		
	deliver specific content.		
9.2.3 Function:	Develop a formal process for	I-2. Education	
Content	content delivery that can help	and training	The education and training service is to
delivery	the CSIRT to best deliver the		support specialized training activities in the
	content to its constituency, based		areas of security for staff in the organizations
	on the characteristics of different		that the CDC supports.
	audiences and content.		
9.2.4 Function:	Develop a program for CSIRT	I-2. Education	
Mentoring	staff, constituency members, or	and training	The education and training service is to
	external trusted partners to		support specialized training activities in the
	learn from experienced staff		areas of security for staff in the organizations
	through an established		that the CDC supports.
	relationship.		

	9.2.5 Function:	Help staff members successfully	I-2. Education	The education and training service is to
	CSIRT staff	and appropriately plan and	and training	support specialized training activities in the
	professional	develop their careers.		areas of security for staff in the organizations
	development			that the CDC supports.
9.3 Service:	9.3.1 Function:	Ensure an effective outcome of	E-6. Defence	The defence capability against advanced
Exercises	Requirements	the exercise by concentrating on	capability	persistent threat (ATP) attack evaluation
	analysis	specific issues for the given scope	against APT	service is to measure the resistance of an
		and focus of the exercise.	attack	organization to targeted attacks while
			evaluation	conducting targeted email training and social
				engineering tests.
			E-7. Handling	The handling capability on cyber-attack
			capability on	evaluation service is to confirm whether
			cyberattack	actual security response activities based on a
			evaluation	scenario that assumes an attack has occurred
				can be activated and whether the incident can
				be brought to an end without delay (called a
				cyber-attack response exercise).
	9.3.2 Function:	Specify and determine the	E-6. Defence	The defence capability against advanced
	Format and	internal and external resources	capability	persistent threat (ATP) attack evaluation
	environment	and infrastructure needed to	against APT	service is to measure the resistance of an
	development	conduct the exercise.	attack	organization to targeted attacks while
			evaluation	conducting targeted email training and social
				engineering tests.

		E-7. Handling capability on cyberattack evaluation	The handling capability on cyber-attack evaluation service is to confirm whether actual security response activities based on a scenario that assumes an attack has occurred can be activated and whether the incident can be brought to an end without delay (called a cyber-attack response exercise).
9.3.3 Fund Scenario developme	target audience to improve the	E-6. Defence capability against APT attack evaluation	The defence capability against advanced persistent threat (ATP) attack evaluation service is to measure the resistance of an organization to targeted attacks while conducting targeted email training and social engineering tests.
		E-7. Handling capability on cyberattack evaluation	The handling capability on cyber-attack evaluation service is to confirm whether actual security response activities based on a scenario that assumes an attack has occurred can be activated and whether the incident can be brought to an end without delay (called a cyber-attack response exercise).

9.3.4 Function:	Conduct drills/exercises allowing	E-6. Defence	The defence capability against advanced
Exercise	a CSIRT team to increase its	capability	persistent threat (ATP) attack evaluation
execution	confidence in the validity of an	against APT	service is to measure the resistance of an
	organization's CSIRT plan and	attack	organization to targeted attacks while
	its ability for execution.	evaluation	conducting targeted email training and social
			engineering tests.
		E-7. Handling	The handling capability on cyber-attack
		capability on	evaluation service is to confirm whether
		cyberattack	actual security response activities based on a
		evaluation	scenario that assumes an attack has occurred
			can be activated and whether the incident can
			be brought to an end without delay (called a
			cyber-attack response exercise).
9.3.5 Function:	Perform a formal and objective	E-6. Defence	The defence capability against advanced
Exercise	analysis of the exercise, based on	capability	persistent threat (ATP) attack evaluation
outcome	factual observations.	against APT	service is to measure the resistance of an
review		attack	organization to targeted attacks while
		evaluation	conducting targeted email training and social
			engineering tests.
		E-7. Handling	The handling capability on cyber-attack
		capability on	evaluation service is to confirm whether
		cyberattack	actual security response activities based on a
		evaluation	scenario that assumes an attack has occurred

				can be activated and whether the incident can be brought to an end without delay (called a cyber-attack response exercise).
9.4 Service: Technical and policy advisory	9.4.1 Function: Risk management support	Improve the identification of opportunities and threats, improve controls, improve loss prevention and incident management in conjunction with information security and other relevant functions.	A-2. Risk assessment	The risk assessment service provides a snapshot of the risk level of an organization in terms of assets, threats and security measures.
	9.4.2 Function: Business continuity and disaster recovery planning support	Act as a trusted advisor on business continuity and disaster recovery by providing impartial, fact-based advice, considering the environment in which the advice may be used and any resource constraints that apply.	A-5. Business continuity	The business continuity service supports the operational functions necessary to ensure correct implementation and execution of the business continuity plan of an organization.
	9.4.3 Function: Policy support	Act as a trusted advisor on the development and implementation of policies by providing impartial, fact-based advice, considering the environment in which the advice	A-3. Policy planning	The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines.

		may be used and any resource		
		constraints that apply.		
	9.4.4 Function:	Provide technical advice that can	I-3. Security	
	Technical	help the constituency to better	consulting	
	advice	manage risks and threats and		The security consulting service provides
		implement current operational		consultancy services to the various business
		and security best practices, while		functions with regards to security.
		enabling effective incident		
		handling activities.		
N/A			A-1. Risk	The risk management service is to achieve
			management	coordinated activities including A-2 to A-13 to
				direct and control an organization with regard
				to risk.
N/A			A-4. Policy	The policy management service is to achieve
			management	periodic reviews for evaluation of policy and
				organization rules, to comply with new or
				external requirements (e.g., regulations and
				guidelines).
N/A			A-6. Business	The business impact analysis service is to
			impact analysis	achieve a systematic assessment of the
				possible impacts resulting from various
				events or scenarios. This service helps
				organizations understand the scale of loss

			that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage.
N/A		A-7. Resource management	The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service.
N/A		A-8. Security architecture design	The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider system design and constraints of business processes (e.g., supply chain).
N/A		A-9. Triage criteria management	The triage criteria management service is to set specific triage (response priority) criteria for events (e.g., incidents, vulnerabilities found, threat information discovered) under the agreed scope in the overall policy.
N/A		A-10. Counter measures selection	The counter measures selection service is to support all activities of countermeasure selection for triage criteria (A-9) and of the

		best technologies with respect to all dispositions of security.
N/A	A-11. Quality	The quality management service is to check
	management	problems in the quality of security activities,
		whether or not they have a negative impact
		for business (e.g., usability, productivity) over
		a period of time (e.g., one week or one month).
N/A	A-12. Security	The security audit service systematically and
	audit	measurably audits how an organization
		implements security policies and controls at a
		specific site or time. CDC staff are indirectly
		involved in audit activities in order to provide
		necessary information and evidence of
		implemented state of controls.
N/A	A-13.	The certification service supports activities
	Certification	necessary for an organization to conform to
		various standards and certification schemes.
N/A	B-2. Event data	The event data retention service collects and
	retention	centrally stores events gathered in the process
		of security monitoring and analysis.
N/A	B-3. Alerting	The alerting and warning service notifies the
	and warning	internal function involved of events that
		highlight potential risks to information assets

		(e.g., security devices alert, security bulletins,
		vulnerabilities and spreading threats).
N/A	B-4. Handling	The handling enquiry on report service is to
	enquiry on	respond to enquiries about data and reports
	report	regarding analysis.
N/A	C-4. Forensic	The forensic evidence collection service
	evidence	collects and conserves digital electronic
	collection	evidence related to an assessed incident, and
		develops and maintains validity of evidence
		("evidence chain of custody").
N/A	E-1. Network	The network information collection service is
	information	to receive an overview of the network
	collection	configuration that is to be protected.
N/A	E-8. Policy	The policy compliance service is to support the
	compliance	verification of conformity to and compliance
		with predefined security policies.
N/A	E-9. Hardening	The hardening service is to optimize IT
		component configuration to identify, evaluate
		and apply systems security configurations,
		and to mitigate or eliminate the risk of
		attacks.
N/A	G-8. Deep	The deep analysis tool operation service is to
	analysis tool	operate tools used in deep analysis, such as

	operation	digital forensics and malware analysis.
N/A	G-9. Basic	The basic operation for analysis platform
	operation for	service is to operate analytical infrastructure
	analysis	that stores the log data required and enables
	platform	the analysis to be performed routinely, mainly
		in real-time analysis, such as security
		information and event management (SIEM).
N/A	G-11. Operates	The operates CDC systems service is to
	CDC/CSC	operate systems that perform the tasks
	systems	required for security response operations,
		such as the various security response tools
		previously described, the production of
		various reports, the response to enquiries, and
		the vulnerability management system.
N/A	G-12. Existing	The existing security tools evaluation service
	security tools	is to verify the impact on other systems and
	evaluation	operations, mainly in terms of availability,
		when upgrading or changing the settings of
		existing security-enabled tools.
N/A	H-2. Internal	The internal fraud detection and reoccurrence
	fraud detection	prevention support service is to analyse the
	and	details of internal fraudulent activities that
	reoccurrence	have been discovered, and considers whether

		prevention	it is possible to detect them from the logs, and
		support	if so, implements the detection logic.
N/A		I-4. Security	The security vendor collaboration service is to
		vendor	build a direct line of communication with the
		collaboration	provider of a security product or service
			purchased, requests a response to any
			deficiencies found in the security response
			and exchanges positive feedback on areas for
			improvement.
N/A		I-6. Technical	The technical reporting service is to provide
		reporting	reports of the results of monitoring and
			management activities. These activities help
			to show the security level of systems and IT
			infrastructure.
N/A		I-7. Executive	The executive security reporting service is to
		security	produce periodic reports and statistical
		reporting	analysis to top management to highlight the
			security level and indicators of operational
			performance of an organization.

## Authors

Information Security Operations providers Group Japan (ISOG-J)

Security Operations Chaos WG (SOC-WG, WG6)

Shigenori TAKEI SCSK Security Corp.

/ leader of ISOG-J WG6

Kimitomo KAWASHIMA NTT DATA INTELLILINK Corp.

Hideto GOTO NTT DATA INTELLILINK Corp.

Supporters

Yuta NAKAMURA NTT TechnoCross Corp.

(Writing parties, in alphabetical order of company name)