Textbook for security response organisation (SOC/CSIRT)

～ using X.1060 ～

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

Table of Contents

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 management	The risk management service is to achieve coordinated activities including A-2 to A-13 to direct and control an organization with regard to risk.	N/A		
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 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-3. Policy planning	The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines.	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.
		8.1 Service: Data acquisition	8.1.1 Function: Policy aggregation,	Establish the context with which the constituency and its assets should comply to 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		
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		

	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.			
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	N/A		

	business processes (e.g., supply chain).			
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 management	The quality management service is 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).	N/A		
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. Certification	The certification service supports activities necessary for an organization to conform to various standards and certification schemes.	N/A		
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.	5.2 Service: Event analysis	5.2.1 Function: Correlation	Identify events directly related to other potential or ongoing security incidents.
			5.2.2 Function: Qualification	Triage and qualify detected potential information security incidents in order to

				identify, categorize, and prioritize true positives.
		8.2 Service: Analysis and synthesis	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-2. Event data retention	The event data retention service collects and centrally stores events gathered in the process of security monitoring and analysis.	N/A		
B-3. Alerting and warning	The alerting and warning service 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).	N/A		
B-4. Handling enquiry on report	The handling enquiry on report service is to respond to enquiries about data and reports regarding analysis.	N/A		
C-1. Forensic analysis	The forensic analysis service analyses digital evidence that is	6.3 Service: Artifact and	6.3.1 Function: Media or surface	Compare information gathered from the artefact with other public and private

	gathered from security assets and relates to an event to assist in determining what happened.	forensic evidence analysis	analysis	artefacts and/or signature repositories.
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 Service: Artifact and forensic evidence analysis	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.
			6.3.3 Function: Run time or dynamic analysis	Provide insight into the artefact's operation.
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.	6.3 Service: Artifact and forensic evidence analysis	6.3.4 Function: Comparative analysis	Perform an analysis focused on identifying common functionality or intent, including family analysis of catalogued artefacts.
C-4. Forensic	The forensic evidence collection	N/A		

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

		n		
		8.2 Service: Analysis and synthesis	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.
			8.2.4 Function: Situational impact	Determine the expected potential impact of a given observation or possible observation to a situational picture.
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.	6.2 Service: Information security incident analysis	6.2.1 Function: Information security incident triage (prioritization and categorization)	Categorize, prioritize, and create an initial assessment of an information security incident.
			6.2.2 Function: Information collection	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.
			6.2.3 Function: Detailed analysis coordination	Initiate and track any other technical analysis in regard to an information security incident.

D-4. Incident response and containment	The incident response and containment service is to contain an incident before it spreads through all resources and increases the damage to or impact on them.	6.2 Service: Information security incident analysis	6.2.4 Function: Information security incident root cause analysis	Identify the root cause of the information security incident, identifying the circumstances that allowed the exploited vulnerabilities to exist or that allowed the exploitation to succeed (including but not limited to user behavior).
		6.4 Service: Mitigation and recovery	6.4.1 Function: Response plan establishment	Define and enforce a plan to restore the integrity of affected systems and return the affected data, systems, and networks to a 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 hoc measures and containment	Implement measures that ensure an information security incident does not 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 recovery	The incident recovery service is to support the restoration of the	6.4 Service: Mitigation	6.4.3 Function: System	Implement changes in the affected domain, infrastructure, or network necessary to fix

	functionality of a target to its normal system operability.	and recovery	restoration	and prevent this type of activity from 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-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 Service: Information security incident coordinatio n	6.5.1 Function: Communication	Engage effectively with stakeholders and establish appropriate multiple communication channels providing the required confidentiality.
			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 information to understand their role of involvement and any expectations that might exist regarding their cooperation and support.
			6.5.3 Function: Relevant information	Keep communicating with the identified entities and provide a suitable flow of available information in order to enable

			distribution	those entities to benefit from available insights and lessons learned, to apply improved responses or take new ad-hoc measures.
		6.6 Service: Crisis management 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: Vulnerability 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 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.	Information security incident coordination	Reporting	business have information about the status of current activities so that further decisions about the next steps to be taken are based on the best situational awareness available.
			6.5.6 Function: Media communication	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.
E-1. Network information collection	The network information collection service is to receive an overview of the network configuration that is to be protected.	N/A		
E-2. Asset inventory	The asset inventory service is to achieve information management	8.1 Service: Data	8.1.2 Function: Asset mapping to	Provide knowledge of existing assets, ownership, baselines and expected activity

	relevant to the census of systems, assets and applications that constitute the overall business infrastructure within the scope of CDC support.	acquisition	functions, roles, actions, and key risks	supports analysis functions that identify abnormal situational observations.
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.	7.1 Service: Vulnerability discovery / research	7.1.3 Function: Vulnerability research	Discover or search for new vulnerabilities as a result of deliberate activities or research.
		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-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.	7.6 Service: Vulnerability response	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-5.	The penetration test service is to	7.6 Service:	7.6.1 Function:	Actively take information about known

Penetration test	reveal security vulnerabilities that could be exploited by attackers and highlights possible methods of compromise (e.g., threat-led penetration test).	Vulnerability response	Vulnerability detection / scanning	vulnerabilities and act upon that information to prevent, detect, and remediate/mitigate those vulnerabilities.
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.	9.3 Service: Exercises	9.3.1 Function: Requirements analysis	Ensure an effective outcome of the exercise by concentrating on specific issues for the given scope and focus of the exercise.
			9.3.2 Function: Format and environment development	Specify and determine the internal and external resources and infrastructure needed to conduct the exercise.
			9.3.3 Function: Scenario development	Provide an opportunity for the target audience to improve the efficiency and 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: Exercise execution	Conduct drills/exercises allowing a CSIRT team to increase its confidence in the validity of an organization's CSIRT plan and its ability for execution.
			9.3.5 Function: Exercise outcome review	Perform a formal and objective analysis of the exercise, based on factual observations.
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 Service: Exercises	9.3.1 Function: Requirements analysis	Ensure an effective outcome of the exercise by concentrating on specific issues for the given scope and focus of the exercise.
			9.3.2 Function: Format and environment development	Specify and determine the internal and external resources and infrastructure needed to conduct the exercise.
			9.3.3 Function:	Provide an opportunity for the target

			Scenario development	audience to improve the efficiency and 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: Exercise execution	Conduct drills/exercises allowing a CSIRT team to increase its confidence in the validity of an organization's CSIRT plan and its ability for execution.
			9.3.5 Function: Exercise outcome review	Perform a formal and objective analysis of the exercise, based on factual observations.
E-8. Policy compliance	The policy compliance service is to support the 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		

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

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

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 Service: Vulnerability discovery / research	7.1.2 Function: Public source vulnerability discovery	Learn about a new vulnerability from reading public sources or other third-party sources.
		7.2 Service: Vulnerability report intake	7.2.1 Function: Vulnerability report receipt	Accept or receive information about a vulnerability, as reported from constituents or third parties.
			7.2.2 Function: Vulnerability report triage and processing	Initially review, categorize, prioritize, and process a vulnerability report.
		7.3 Service: Vulnerability analysis	7.3.1 Function: Vulnerability triage (validation and categorization)	Categorize, prioritize, and perform an initial assessment of a vulnerability.
			7.3.2 Function: Vulnerability root	Understand the design or implementation flaw that causes or exposes the vulnerability

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

utilization	and dissemination of threat information for all categories of security response.	y disclosure	announcement / communication / dissemination	they can detect, remediate or mitigate, and prevent future exploitation of the vulnerability.
			7.5.3 Function: Post-vulnerability disclosure feedback	Receive and respond to questions or reports from constituents about a vulnerability disclosure or document.
		8.1 Service: Data acquisition	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.
G-1. Security architecture implementation	The security architecture implementation service is to implement the security architecture designed by strategic management of CDC (category A) by using assets.	5.1 Service: Monitoring and detection	5.1.1 Function: Log and sensor management	Manage log sources and sensors.
		8.3 Service: Communication	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-2. Basic operation for network security asset	The basic operation for network security asset service is to operate network devices, such as firewalls, intrusion detection	5.1 Service: Monitoring and detection	5.1.1 Function: Log and sensor management	Manage log sources and sensors.

	system/intrusion prevention system (IDS/IPS), web application firewall (WAF) and proxies.			
G-3. Advanced operation for network security asset	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.	5.1 Service: Monitoring and detection	5.1.2 Function: Detection use case management	Manage the portfolio of detection use cases through their entire lifecycle.
			5.1.3 Function: Contextual data management	Manage of contextual data sources for detection and enrichment.
		8.3 Service: Communication	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-4. Basic operation for endpoint security asset	The basic operation for endpoint security asset service is to operate countermeasure products, such as anti-virus software, at endpoints.	5.1 Service: Monitoring and detection	5.1.1 Function: Log and sensor management	Manage log sources and sensors.
G-5. Advanced operation for	The advanced operation for endpoint security asset service is	5.1 Service: Monitoring	5.1.2 Function: Detection use case	Manage the portfolio of detection use cases through their entire lifecycle.

endpoint security asset	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.	and detection	management	
			5.1.3 Function: Contextual data management	Manage of contextual data sources for detection and enrichment.
		8.3 Service: Communication	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-6. Basic operation for cloud security products	The basic operation for cloud security products service is to operate security services in a cloud.	5.1 Service: Monitoring and detection	5.1.1 Function: Log and sensor management	Manage log sources and sensors.
G-7. Advanced operation for cloud security products	The advanced operation for cloud security products service is to create custom signatures of an organization for security services in a cloud with attack detection	5.1 Service: Monitoring and detection	5.1.2 Function: Detection use case management	Manage the portfolio of detection use cases through their entire lifecycle.

	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: Communication	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 operation	The deep analysis tool operation service is to operate tools used in deep analysis, such as digital forensics and malware analysis.	N/A		
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. 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 Service: Monitoring and detection	5.1.2 Function: Detection use case management	Manage the portfolio of detection use cases through their entire lifecycle.
			5.1.3 Function: Contextual data management	Manage of contextual data sources for detection and enrichment.
G-11. Operates CDC/CSC systems	The operates CDC systems service is to operate systems that perform 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	N/A		

	system.			
G-12. Existing security tools evaluation	The existing security tools evaluation service is to verify the impact on other systems and operations, mainly in terms of availability, when upgrading or changing the settings of existing security-enabled tools.	N/A		
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.	7.3 Service: Vulnerability analysis	7.3.3 Function: Vulnerability remediation development	Develop the steps necessary to fix (remediate) the underlying vulnerability or mitigate (reduce) the effects of the vulnerability from being exploited.
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.	6.4 Service: Mitigation and recovery	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
H-2. Internal fraud detection and reoccurrence	The internal fraud detection and reoccurrence prevention support service is to analyse the details of internal fraudulent activities that	N/A		

prevention support	have been discovered, and 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 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 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 and mitigation of risks.
			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.
			9.1.3 Function: Information dissemination	Disseminate security-related information to improve awareness and implementation of security practices.
			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-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 that the CDC supports.	6.4 Service: Mitigation and recovery	6.4.4 Function: Other information security entities support	Enable the constituents to perform the required management and technical activities inorder to successfully mitigate an information security incident and recover from it.
		9.2 Service: Training and education	9.2.1 Function: Knowledge, skill, and ability requirements gathering	Properly assess, identify, and document what the constituency needs are in terms of requisite KSAs, to develop appropriate training and education materials and improve its skill level.
			9.2.2 Function: Educational and training materials development	Develop, using the constituency's KSA needs as a basis, educational, instructional, and training material that is appropriate to the delivery methods identified as the best to reach different audiences or deliver specific content.
			9.2.3 Function: Content delivery	Develop a formal process for 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: Mentoring	Develop a program for CSIRT staff, constituency members, or external trusted partners to learn from experienced staff through an established relationship.
			9.2.5 Function: CSIRT staff professional development	Help staff members successfully and appropriately plan and develop their careers.
I-3. Security consulting	The security consulting service provides consultancy services to the various business functions with regards to security.	9.4 Service: Technical and policy advisory	9.4.4 Function: Technical advice	Provide technical advice that can help the constituency to better manage risks and threats and implement current operational and security best practices, while enabling effective incident handling activities.
I-4. Security vendor collaboration	The security vendor collaboration service is to build a direct line of 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.	N/A		

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 Service: Vulnerability coordination	7.4.1 Function: Vulnerability notification/reporting	Initial share or report new vulnerability information with others who are to be involved in the CVD process.
			7.4.2 Function: Vulnerability stakeholder coordination	Conduct follow-on coordination and sharing of information among the various stakeholders and participants involved in coordinated vulnerability disclosure (CVD) efforts.
		8.3 Service: Communication	8.3.1 Function: Internal and external communication	Inform constituents (and others) of the current situational picture and how it may be changing.
			8.3.4 Function: Dissemination / integration / information sharing	Assemble, normalize, and prepare information and then share it with constituents and others outside the constituency.
			8.3.5 Function: Management of	Ensure transfer of information is successful and useable.

			information sharing	
			8.3.6 Function: Feedback	Improve the quality, timeliness, accuracy, and relevance of the data being received from internal and external sources.
I-6. Technical reporting	The technical reporting service is to provide 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 security reporting	The executive security reporting service is to produce periodic reports and statistical analysis to top management to highlight the security level and indicators of operational performance of an organization.	N/A		

2. Mapping with X.1060

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

	5.1.2 Function: Detection use case management	Manage the portfolio of detection use cases through their entire lifecycle.	F-1. Post-mortem analysis	The post-mortem analysis service describes resolution of an incident to ensure review and improvement of the processes and tools for CDC staff.
			G-3. Advanced operation for network security asset	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 operation for cloud security products	The advanced operation for cloud security products service is to create custom signatures of an organization for security 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 data sources for detection and enrichment.	G-3. Advanced operation for network security asset	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 operation for cloud security products	The advanced operation for cloud security products service is to create custom signatures of an organization for security 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.
5.2 Service: Event analysis	5.2.1 Function: Correlation	Identify events directly related to other potential or ongoing security incidents.	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.
	5.2.2 Function: Qualification	Triage and qualify detected potential information security	B-1. Real-time asset monitoring	The real-time asset monitoring service is to supervise and analyse systems status or

		incidents in order to identify, categorize, and prioritize true positives.		suspicious activities from logs and network flows, and supporting triage as incident or event for gathering information needed.
6.1 Service: Information security incident report acceptance	6.1.1 Function: Information security incident report receipt	Accept or receive information about an information security incident, as reported from constituents or third parties.	D-1. Incident report acceptance	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: Information security incident analysis	6.2.1 Function: Information security incident triage (prioritization and categorization)	Categorize, prioritize, and create an initial assessment of an information security incident.	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.
	6.2.2 Function:	Intake, catalog, store, and track	D-3. Incident	The incident classification service is to

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

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: Mitigation and recovery	6.4.1 Function: Response plan establishment	Define and enforce a plan to restore the integrity of affected systems and return the affected data, systems, and networks to a 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.	D-4. Incident response and containment	The incident response and containment service is to contain an incident before it spreads through all resources and increases the damage to or impact on them.
	6.4.2 Function: Ad hoc measures and containment	Implement measures that ensure an information security incident does not 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-4. Incident response and containment	The incident response and containment service is to contain an incident before it spreads through all resources and increases the damage to or impact on them.
	6.4.3 Function: System restoration	Implement changes in the affected domain, infrastructure, or network necessary to fix and prevent this type of activity from	D-5. Incident recovery	The incident recovery service is to support the restoration of the functionality of a target to its normal system operability.

		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: Communication	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: Relevant information distribution	Keep communicating with the identified entities and provide a suitable flow of available information in order to enable those entities to benefit from available insights and lessons learned, to apply improved responses or take new ad-hoc measures.	D-6. Incident notification	The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.
	6.5.4 Function: Activities coordination	Track the status of all communication and activities.	D-2. Incident handling	The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7.
	6.5.5 Function: Reporting	Ensure that all involved entities within a business have information about the status of current activities so that further decisions about the next steps to be taken are based on the best	D-7. Incident response 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

		situational awareness available.		report of current status during handling of an incident, this service distributes an interim report.
	6.5.6 Function: Media communication	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.	D-7. Incident response 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.
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.

		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.	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 research	vulnerabilities as a result of deliberate activities or research.	3.Vulnerability assessment	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).
			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).
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 (validation and categorization)	a vulnerability.	intelligence collection and analysis	(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.
	7.3.2 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 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.
	7.3.3 Function: Vulnerability remediation	Develop the steps necessary to fix (remediate) the underlying vulnerability or mitigate	F-2. Internal threat intelligence	The internal threat intelligence collection and analysis service is to gather information (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/reporting	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 / communication / 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.	E-2. Asset inventory	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.	D-2. Incident handling	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: Communication	8.3.1 Function: Internal and external communication	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 recommendations	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: Implementation	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 in the situational picture.		management of CDC (category A) by using assets.
			G-3. Advanced operation for network security asset	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 operation for cloud security products	The advanced operation for cloud security products service is to create custom signatures of an organization for security 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 requirements gathering	KSAs, to develop appropriate training and education materials and improve its skill level.		that the CDC supports.
	9.2.2 Function: Educational and training materials development	Develop, using the constituency's KSA needs as a basis, educational, instructional, and training material that is appropriate to the delivery methods identified as the best to reach different audiences or deliver specific content.	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 that the CDC supports.
	9.2.3 Function: Content delivery	Develop a formal process for content delivery that can help the CSIRT to best deliver the content to its constituency, based on the characteristics of different audiences and content.	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 that the CDC supports.
	9.2.4 Function: Mentoring	Develop a program for CSIRT staff, constituency members, or external trusted partners to learn from experienced staff through an established relationship.	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 that the CDC supports.

	9.2.5 Function: CSIRT staff professional development	Help staff members successfully and appropriately plan and develop their careers.	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 that the CDC supports.
9.3 Service: Exercises	9.3.1 Function: Requirements analysis	Ensure an effective outcome of the exercise by concentrating on specific issues for the given scope and focus of the exercise.	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).
	9.3.2 Function: Format and environment development	Specify and determine the internal and external resources and infrastructure needed to conduct the exercise.	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).
	9.3.3 Function: Scenario development	Provide an opportunity for the target audience to improve the efficiency and effectiveness of its services and functions, and its skills, knowledge, and abilities, through the handling of simulated cybersecurity events/incidents, including communications aspects	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: Exercise execution	Conduct drills/exercises allowing a CSIRT team to increase its confidence in the validity of an organization's CSIRT plan and its ability for execution.	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).
	9.3.5 Function: Exercise outcome review	Perform a formal and objective analysis of the exercise, based on factual observations.	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).
9.4 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: Technical advice	Provide technical advice that can help the constituency to better manage risks and threats and implement current operational and security best practices, while enabling effective incident handling activities.	I-3. Security consulting	The security consulting service provides consultancy services to the various business functions with regards to security.
N/A			A-1. Risk management	The risk management service is to achieve coordinated activities including A-2 to A-13 to direct and control an organization with regard to risk.
N/A			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			A-6. Business impact analysis	The business impact analysis service is to 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 management	The quality management service is 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).
N/A			A-12. Security audit	The security audit service 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.
N/A			A-13. Certification	The certification service supports activities necessary for an organization to conform to various standards and certification schemes.
N/A			B-2. Event data retention	The event data retention service collects and centrally stores events gathered in the process of security monitoring and analysis.
N/A			B-3. Alerting and warning	The alerting and warning service 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).
N/A			B-4. Handling enquiry on report	The handling enquiry on report service is to respond to enquiries about data and reports regarding analysis.
N/A			C-4. Forensic evidence collection	The forensic evidence collection service collects and conserves digital electronic evidence related to an assessed incident, and develops and maintains validity of evidence ("evidence chain of custody").
N/A			E-1. Network information collection	The network information collection service is to receive an overview of the network configuration that is to be protected.
N/A			E-8. Policy compliance	The policy compliance service is to support the 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 analysis tool	The deep analysis tool operation service is to operate tools used in deep analysis, such as

			operation	digital forensics and malware analysis.
N/A			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-11. Operates CDC/CSC systems	The operates CDC systems service is to operate systems that perform 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.
N/A			G-12. Existing security tools evaluation	The existing security tools evaluation service is to verify the impact on other systems and operations, mainly in terms of availability, when upgrading or changing the settings of existing security-enabled tools.
N/A			H-2. Internal fraud detection and reoccurrence	The internal fraud detection and reoccurrence prevention support service is to analyse the details of internal fraudulent activities that have been discovered, and considers whether

			prevention support	it is possible to detect them from the logs, and if so, implements the detection logic.
N/A			I-4. Security vendor collaboration	The security vendor collaboration service is to build a direct line of 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.
N/A			I-6. Technical reporting	The technical reporting service is to provide 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 security reporting	The executive security reporting service is to produce periodic reports and statistical 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）