27 May 2010
Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

In the Matter of: Cyber Security Certification Program, Docket No. PS 10-93

Dear Ms. Dortch:

This ex parte letter is intended to elaborate the ex parte presentation provided by Mr. Anthony M. Rutkowski, EVP for Regulatory Affairs and Standards of Yaana Technologies LLC, on 21 May 2010.

The presentation included the ontology of cybersecurity operational information, which is one of our research results that are closely related to the broad global industry effort in the ITU-T standards organizations, where Mr. Anthony M. Rutkowski is taking an active role as the Cybersecurity Rapporteur. This ontology can become a basis for a cybersecurity information exchange on a global scale, and can be used as a basis of discussion on building the framework of cybersecurity information exchange. The attached material elaborates the ontology and was presented for the 6th Annual Cyber Security and Information Intelligence Research Workshop held in April 2010. Note, in the ITU-T Study Group 17 meeting held in Geneva in April, this ontology was decided to be included in the appendix of CYBEX draft Recommendation.

We believe depicting cybersecurity operational information is helpful to expedite discussion on the advancement of cybersecurity. Hence, albeit the ontology itself does not answer any of the issues raised in the Cyber Security Certification Program Notice of Inquiry that is issued on 21 April 2010, we hope it would help advancing the discussion of the issues.

Pursuant to the Commission's rules, this ex parte letter is being filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

Takeshi Takahashi
Expert Researcher
National Institute of Information and Communications Technology
4-2-1 Nukuki-Kitamachi Koganei Tokyo,184-8795 Japan
tel: +81 42 327 5862
takeshi_takahashi@nict.go.jp

Youki Kadobayashi
Project Leader
National Institute of Information and Communications Technology
4-2-1 Nukuki-Kitamachi Koganei Tokyo,184-8795 Japan
youki-k@is.aist-nara.ac.jp

Attachment:
Proceedings of CSIIRW 2010: Building Ontology of Cybersecurity Operational Information

Building Ontology of Cybersecurity Operational Information

Takeshi Takahashi
National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi
Koganei
Tokyo Japan
takeshi_takahashi@nict.go.jp

Hiroyuki Fujiwara
Solution Crew Inc.
Shin-osaka Wako bldg 8F
4-6-18 Miyahara Yodokawa-ku
Osaka Japan
reisei@scw.co.jp

Youki Kadobayashi
Nara Institute of Science and Technology
Takayama 8916-5, Ikoma
Nara Japan
youki-k@is.naist.jp

ABSTRACT

Cyber threats come beyond the border of countries. However, most organizations are currently coping with them individually without global collaboration mainly due to the lack of global standard for cybersecurity information exchange format and framework. Albeit some countries possess their local standards to solve this problem, these standards are not orchestrated in order for each organization to fully collaborate each other. In order to build the basis of cybersecurity information exchange framework, this paper proposes an ontology of cybersecurity operational information. Based on the proposed ontology, it discusses on the coverage of existing cybersecurity information standards.

Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: General—Security and Protection; H.1 [Information System]: Models and Principles; K.6.5 [Management of Computing and Information Systems]: Security and Protection

General Terms

Security, Design, Theory

Keywords

cybersecurity, information sharing, ontology

1. INTRODUCTION

The widespread Internet is bolstering the immense development of cyber society, where various communications including private information sharing and business transactions are taken place. In the cyber society, a malware such as virus may attack any computers beyond the border of countries, and vulnerability of a system may be exposed to any attackers all over the world. However, countermeasures against those cyber threats are taken mostly by individual organization. Consequently, one organization in one country may be attacked by a malware whose countermeasure is already found and is implemented in another organization in another country. One of the biggest factors that prevent organizations to share information among one another is the absence of globally common format and framework for cybersecurity information exchange. Albeit some countries such as USA possess domestic standards for this purpose, most of the other countries do not possess that kind of standards.

Globally common format and framework for cybersecurity information exchange offer mainly two advantages. One advantage is that the cybersecurity level is expected to be improved significantly on a global scale. Since cybersecurity information can be shared on a global scale, the disparity of cybersecurity information availability among countries and organizations can be suppressed. Hence, no country and organization will be left behind in terms of cybersecurity information level. Another advantage is that security operation can be automated. Currently, most of security operations in most organizations are not automated and are largely dependent on human intervention. For instance, when one organization sends alert of some security flaws to another organization, a person in one organization needs to prepare email, which is then sent and received by another person in the corresponding organization. By advancing cybersecurity operation automation, cybersecurity operation cost in each organization will be suppressed drastically.

In order to build the basis of cybersecurity information exchange on a global scale, this paper proposes an ontology, a specification of abstracted world[1], of cybersecurity operational information. The proposed ontology is an outcome from our intensive discussions with cybersecurity operators and stakeholders in the USA, Japan and Korea. Albeit each cybersecurity operator runs slightly different operations, we succeeded in building a generalized ontology of cybersecurity operational information.

We took the following approach to build the ontology: Firstly, we defined domains for cybersecurity operations as mentioned in Section 2, identified the required entities to run the operations in each domain as mentioned in Section 3 and then introduced the proposed ontology as mentioned in Section 4. Based on the ontology, Section 5 discusses on the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
CSIIRW '10, April 21-23, Oak Ridge, Tennessee, USA
Copyright 2010 ACM 978-1-4503-0017-9 ...$5.00.

coverage of existing cybersecurity information standards.

2. OPERATION DOMAINS

This section defines cybersecurity operation domains that are required to secure the cyber society. Cybersecurity operations consist of 3 domains: Incident Handling Domain, IT Asset Management Domain and Knowledge Accumulation Domain.

Incident Handling Domain detects and responds incidents occurred in cyber society by monitoring incidents, computer events that composes the incidents, and attack behaviors caused by the incidents. For instance, it detects abnormality through the alert from detectors, then builds evidences by collecting various logs. Sometimes it provides alerts and advisories, e.g. early warnings against candidate threats, to user organizations.

IT Asset Management Domain runs cybersecurity operations inside each user organization such as installing, configuring, and managing IT assets in the organization. It covers both incident preventive operations and damage controlling operations in each organization.

Knowledge Accumulation Domain researches cybersecurity-related information. Then it generates reusable knowledge for the other organizations and accumulates them.

3. ENTITIES

Based on the operation domains defined in Section 2, this section identifies entities that are necessary to run cybersecurity operations in each domain. Note that the entities are defined from the viewpoint of functions. Hence an instance of an entity may be an instance of another entity.

In Incident Handling Domain, there exist two entities, i.e., Response Team and Coordinator, for its operation. Response Team is an entity that monitors and analyzes various kinds of incidents in cyber societies, e.g. unauthorized access, DDoS attack and phishing, and accumulates incident information. Based on the information, Response Team may implement countermeasures, e.g. registering phishing site addresses on black lists. Incident response team inside Managed Security Service Provider(MSSP) is its typical instance. Coordinator is an entity that coordinates with the other entities and addresses potential threats based on known incident and crime information. CERT Coordination Center(CERT/CC) is its typical instance.

In IT Asset Management Domain, there exist two entities, i.e., Administrator and IT Infrastructure Provider, for its operation. Administrator is an entity that administers the system of its organization. It possesses information on its own IT assets. IT administrator inside each organization is its typical instance. IT infrastructure Provider is an entity that provides IT infrastructure to each organization. IT infrastructure includes network connectivity, data server, and software as a service (SaaS). It possesses information on inter-organization networks, e.g. network topology information, specification of data servers and SaaS. Internet Service Provider (ISP) and Application Service Provider (ASP) are its typical instance.

In Knowledge Accumulation Domain, there exist 3 entities, i.e., Researcher, Product & Service Provider and Registrar, for its operation. Researcher is an entity that researches on cybersecurity and extract knowledge from the research, and accumulate it. Cybersecurity research teams in MSSP, e.g. X-force inside International Business Machines Corp. as well as Risk Research Institute of Cyber Space inside Little eArth Corporation Co., Ltd., are its typical instances. Product & Service Provider is an entity that possesses information on software, e.g. naming, versions, their vulnerabilities, their patches and configuration information. Software house and individual private software programmer are its typical instances. Registrar is an entity that classifies and organizes cybersecurity knowledge provided by Researcher and Product & Service Provider so that the knowledge can be used for another organization. NIST in the USA and IPA in Japan are its typical instances.

4. CYBERSECURITY OPERATIONAL INFORMATION

Based on the aforementioned operation domains and entities, this section proposes an ontology of cybersecurity operational information. Figure 1 describes an overview of the proposed ontology. Bar line describes the relationship of mutual reference while arrows describe information input from entity to knowledge base/database.

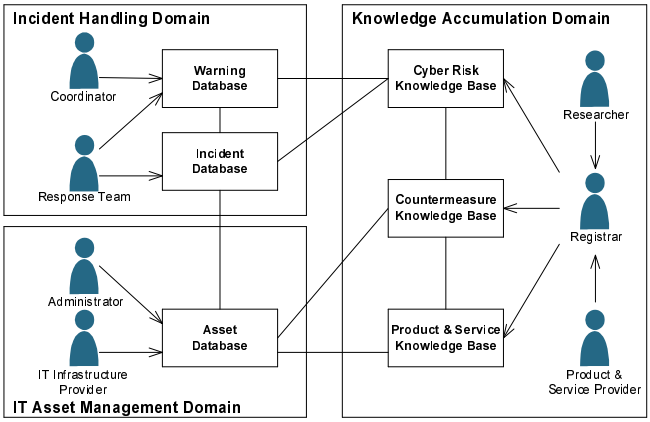


Figure 1: Overview of the Proposed Ontology

Each of the operation domains in the proposed ontology is elaborated respectively in the following subsections.

4.1 Incident Handling Domain

In Incident Handling Domain, there exist Incident Database and Warning Database.

Incident Database is a database that contains information on incidents provided by Response Team. It includes 3 records: Event Record, Incident Record and Attack Record. Event Record is a record of computer events. It includes information on packets, files and their transactions. Usually, most of the records are provided by computers automatically as computer logs. For instance, when a root user log in to a system, the log such as log-in time and date as well as terminal information will be provided by computers automatically. This log is one of Event Records. Incident Record is a record of incident that includes incident candidates. This record is derived from the record of several Event Records and their conjectures, which are created automatically and/or manually. Attack Record is a record of attacks that are based on the analyses of incidents. It describes the

sequence of the attacks. For instance, information such as how the attack was started, which part of IT assets were targeted, and how the damage of the attack was propagated are clarified.

Warning Database is a database that contains information on cybersecurity warnings provided by Response Team and Coordinator. The warnings are based on the Incident Database as well as Cyber Risk Knowledge Base

4.2 IT Asset Management Domain

In IT Asset Management Domain, there exists Asset Database. It is a database that accumulates information on the asset of each organization such as IT systems, subscribing cloud service list, and surrounding external network topologies. The information is provided by Administrator and IT Infrastructure Provider. It consists of two databases: Internal Asset Database and External Asset Database.

Internal Asset Database is a database that accumulates information on assets inside individual organization and contains information such as the list of softwares/hardwares, their configurations, status of resource usage, security policies including access control policies, security level assessment result, and intranet topology. I also contains the list of resources, e.g., data center and SaaS, each organization is utilizing outside their organization, the usage status/history of the resources as well as the contract information of the external resource usages. The information is provided by Administrator.

External Asset Database is a database that accumulates information on assets outside individual organization. It mainly contains external resource information and external network information. External resource information contains information on resources each organization is utilizing outside their organization such as the list and status of external cloud services (e.g. data center and SaaS). External network information contains information on networks with which each organization is connected with the other organizations such as their topology, routing information, access control policy, traffic status and the security level. The information is provided mainly by IT Infrastructure Provider and partly by Administrator.

4.3 Knowledge Accumulation Domain

In Knowledge Accumulation Domain, there exist 3 knowledge bases: Cyber Risk Knowledge Base, Countermeasure Knowledge Base and Product Knowledge Base. They accumulate knowledge on cybersecurity provided by Researcher and Product & Service Provider, then organized and classified by Registrar. Each of the knowledge bases are elaborated in the following sub sections.

4.3.1 Cyber Risk Knowledge Base

Cyber Risk Knowledge Base is a knowledge base that accumulates cybersecurity risk information and includes two knowledge bases, i.e., Vulnerability Knowledge Base and Threat Knowledge Base.

Vulnerability Knowledge Base is a knowledge base that accumulates known vulnerability information, which includes naming, taxonomy and enumeration of known vulnerability information. It also includes human vulnerabilities, which is vulnerabilities human IT users expose.

Threat Knowledge Base is a knowledge base that accumulates known threat information. It includes two knowledge bases: Attack Knowledge Base and Mis-use Knowledge Base. Attack Knowledge Base accumulates information on attacks which includes the information on attack patterns, attack tools (e.g. malware) and their trends. Trend information includes the information on past attack trend in terms of geography and attack target, for instance. It also includes statistical information of past attacks. Mis-use Knowledge Base accumulates information on mis-uses which is caused by users' inappropriate usage. The inappropriate usage includes both benign usage and malicious usage. Benign usage includes mis-typing, mis-recognition caused by inattentional blindness[3], mis-understanding, being caught by phishing traps. Malicious usage includes compliance violation such as unauthorized service usage and access to inappropriate materials.

4.3.2 Countermeasure Knowledge Base

Countermeasure Knowledge Base accumulates information on countermeasures to cybersecurity risks and contains 2 rule bases: Assessment Rule Base and Detection/Protection Rule Base. Assessment Rule Base is a rule base that accumulates known rules and criteria for assessing security level of IT assets as well as the checklist of configurations. Detection/Protection Rule Base is a rule base that accumulates known rules and criteria for detecting/protecting security threat. IDS/IPS signatures and detection/protection rules that follow the signatures are stored in this base, for instance.

4.3.3 Product Knowledge Base

Product Knowledge Base is a knowledge base that accumulates product information. It includes Version Knowledge Base and Configuration Knowledge Base. Version Knowledge Base is a knowledge base that accumulates version information of products and services, which includes naming and enumeration of product versions. Regarding the product, security patches are also included here. Configuration Knowledge Base is a knowledge base that accumulates product configuration information, which includes naming, taxonomy and enumeration of known configurations.

Based on the cybersecurity operational information mentioned in this section, the proposed ontology is described in Fig. 2.

5. DISCUSSION

Based on the proposed ontology, this section discusses on the coverage of existing cybersecurity information standards. The proposed ontology is capable of mapping major cybersecurity information standards as shown in Table 1.

Some cybersecurity information does not have any major standards that can describe it. For instance, no major standards can be found to describe External Asset Database. From the viewpoint of cloud security, the database takes important role. The necessity of having standards for this database should be discussed. Also, no major standards can be found to describe Mis-use Knowledge Base. Albeit many of cyber attacks exploit human vulnerability in reality, the knowledge on mis-use that is incurred by human vulnerability is not accumulated and not exchanged between organizations. The necessity of having standards for knowledge on human factors, e.g. enumeration of mis-use, should be discussed.

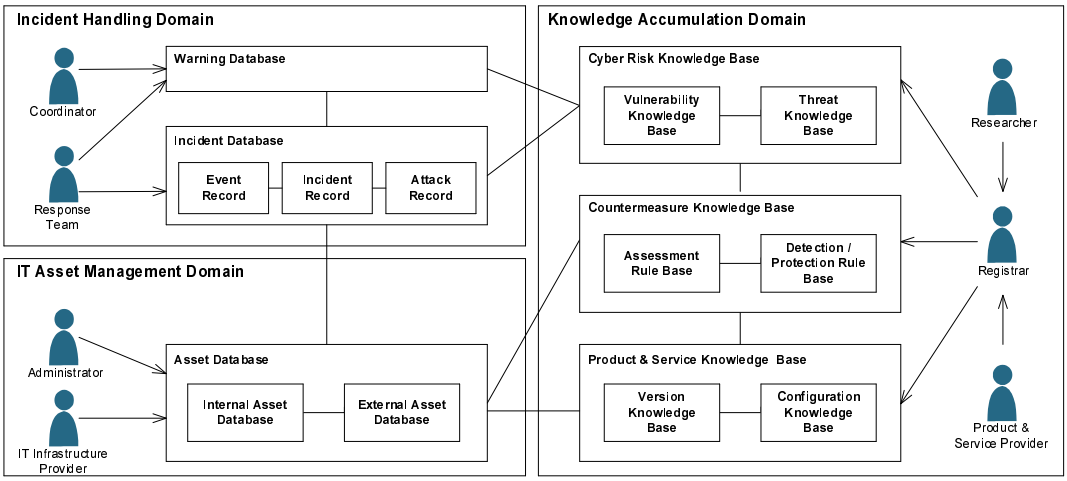


Figure 2: Proposed Ontology

Table 1: Major Cybersecurity Information Standards

Operation Domain	Information categories			Major standards
Incident Handling	Incident Database	Event Record		CEE[6]
		Incident Record		IODEF[4]
		Attack Record		-
	Warning Database			-
IT Asset Management	Asset Database	Internal Asset Database		ARF[6], CVSS[6]/CWSS[5] scores
		External Asset Database		-
Knowledge Accumulation	Cyber Risk Knowledge Base	Vulnerability Knowledge Base		CVE[6], CWE[6]
		Threat Knowledge Base	Attack Knowledge Base	CAPEC[6], MAEC[6]
			Mis-use Knowledge Base	-
	Countermeasure Knowledge Base	Assessment Rule Base		CVSS/CWSS formula, OVAL[6], XCCDF[6], OCIL[2]
		Detection/Protection Rule Base		-
	Product Knowledge Base	Version Knowledge Base		CPE[6]
		Configuration Knowledge Base		CCE[6]

On the other hand, these standards themselves are independent to one another and are not well-orchestrated. Without deliberate orchestration of these existing standards, automation of cybersecurity operations cannot be expedited. SCAP[6] orchestrates 7 of the existing standards in order to automate cybersecurity operations, and some security companies have already adopted SCAP for their internal cybersecurity operations. However, the coverage of the 7 existing standards are very limited at this moment, and future expansion is expected to fully advance the automation of cybersecurity operations.

6. CONCLUSION

This paper proposed an ontology of cybersecurity operational information based on intensive discussions with cybersecurity operators. The ontology can be used as a basis of discussion on building the framework of cybersecurity information exchange. Based on the ontology, this paper discussed on the coverage of existing cybersecurity information standards and pointed out that existing standards do not cover some information areas that might be very important in cyber society, and that automation of cybersecurity operations are provided in a very limited scope at this stage.

7. REFERENCES

[1] T. R. Gruber. Toward principles for the design of ontologies used for knowledge sharing. Int. J. Hum.-Comput. Stud., 43(5-6):907–928, 1995.

[2] M. Casipe et al.t. The Open Checklist Interactive Language (OCIL) Version 1.1. MITRE TECHNICAL REPORT MTR080368 R3, May 2009.

[3] P. Johansson et al. Failure to detect mismatches between intention and outcome in a simple decision task. Science, 310(5745):116, 2005.

[4] R. Danyliw, et al. The Incident Object Description Exchange Format. IETF Request For Comments 5070, dec. 2007.

[5] The MITRE Corporation. Common Weakness Scoring System (CWSS). http://cwe.mitre.org/cwss/index.html.

[6] The MITRE Corporation. Making Security Measurable. http://msm.mitre.org/.

Building Ontology of Cybersecurity Operational Information

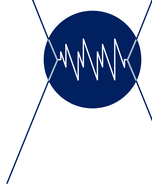
Takeshi Takahashi, National Institute of Information and Communications Technology, takeshi_takahashi@nict.go.jp
Hiroyuki Fujiwara, Solution Crew Inc., reisei@scw.co.jp
Youki Kadobayashi, Nara Institute of Science and Technology, youki-k@is.naist.jp

Background

- Cyber threats come beyond country borders while counter-measures are mostly taken by each organization alone
- That is caused by the lack of globally common information exchange format and framework

Cyber Threats

- **Threat comes beyond the borders of countries**
  - –An attacker can attack computers all over the world by simply pressing a return key
  - –It is also possible for an attacker to attack computers in country A by controlling computers in country B



Countermeasures

- **Countermeasures are most often implemented by individual organizations in isolation**
  - –Information is accumulated inside each organization
  - –Information sharing is usually very difficult
- **Significant man-power is required**
  - –Email, telephone calls and even face to face meetings are still the primary method for information exchange.
  - –The need for and reliance on human interaction consumes a lot of time

- By building them, we minimize information disparity on a global scale and can automate security operations
- Though various standards exist, there exists no basis for determining their applicability, coverage and effectiveness

Building & sharing cybersecurity information exchange format and framework

Minimizing the disparity of cybersecurity information availability on a global scale

- Developing countries, which currently have very little information and knowledge of cybersecurity, can become equal partners with developed countries
- The disparity will be even less once the automation mentioned below is implemented

Automating security operations

- Operation that is currently conducted by man-power will be automated
- Consequently, the cost of security operation (personnel cost etc.) will be significantly reduced
- At the same time, mistakes incurred by human operation can be avoided

- In order to build the discussion basis, we propose an ontology for cybersecurity operational information

Consideration

- By mapping existing standards to the proposed ontology, we discuss the necessity of further development of cybersecurity information standard.

Domains	KBs / DBs / Records			Existing standards
Incident Handling	Incident Database	Incident Record		IODEF
		Event Record		CEE
		Attack Record		
	Warning Database			
IT Asset Management	Asset Database	Internal Asset DB		ARF, CVSS/CWSS score
		External Asset DB		
Knowledge Accumulation	Cyber Risk KB	Vulnerability KB		CVE, CWE
		Threat KB	Attack	CAPEC, MAEC
			Mis-use	
	Countermeasure KB	Assessment RB		CVSS/CWSS formula, OVAL, XCCDF, OCIL
		Detection/Protection RB		
	Product KB	Version KB		CPE
		Configuration KB		CCE

Cloud Security

- External Asset Database does not have any major standards
- Product Knowledge Base lacks information on cloud services

Human Factors

- Mis-use does not have any major standards (for naming and enumeration etc.)
- Corresponding vulnerability, i.e., human vulnerability does not have any major standards

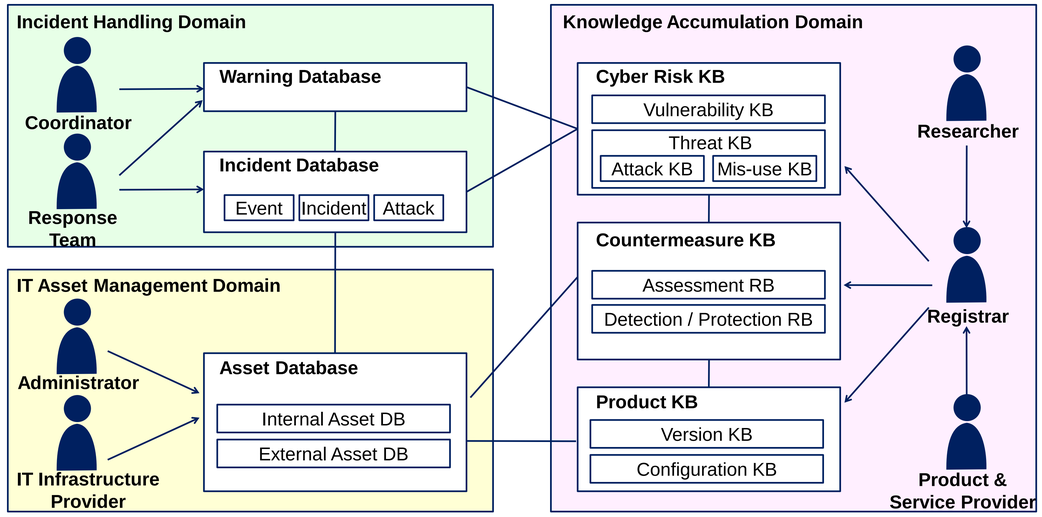
Operation automation

- SCAP covers many information categories
- Yet, further automation is possible

- Further development of cybersecurity information standard is required , especially in cloud security area, human factors, and cybersecurity operation automations

Proposed Ontology

- We propose an ontology for cybersecurity operational information



- The ontology was built following the 3 steps mentioned below

	Operation Domain		Overview of the operations
Step 1 **Design Operation Domain**	Cybersecurity Operation	Incident Handling	Monitors and detects incidents, then provides warnings and/or implements countermeasures
		IT Asset Management	Runs security operations inside user organizations
		Knowledge Accumulation	Researches, organizes and accumulates knowledge of cybersecurity

	Domain	Entity	Functions
Step 2 **Design Entity**	Incident Handling	Response Team	Monitors and analyzes incidents, and take countermeasures
		Coordinator	Coordinates various organizations to cope with incidents / provide warnings
	IT Asset Management	Administrator	Runs security operations inside each user organization
		IT Infrastructure Provider	Provides IT infrastructure for users such as network connectivity and SaaS
	Knowledge Accumulation	Researcher	Researches on cyber risks and extracts knowledge of cybersecurity
		Product & Service Provider	Researches on products and services and extracts cybersecurity knowledge
		Registrar	Organizes and classifies knowledge so that the other parties can reuse it

	Information category			Stored information
Step 3 **Design Cybersecurity Information**	Incident Handling	Incident Database	Event Record	• Artifacts that contain information on computer events
			Incident Record	• Artifacts that contain information on incidents and that is derived from the analysis on Event Records
			Attack Record	• Attack sequence derived from the analysis on Incident Record
		Warning Database		• Warning information based on the information of incidents
	IT Asset Management	Asset Database	Internal Asset DB	• Information on Asset inside each organization • Information on external resources each organization is using
			External Asset DB	• Information on external networks each organization is using • Information on the specifications and status of external resources
	Knowledge Accumulation	Cyber Risk KB	Vulnerability KB	• Knowledge of known vulnerabilities on cybersecurity
			Threat KB	• Knowledge of known cyber threats such as attacks and mis-uses
		Counter-measure KB	Assessment RB	• Knowledge of security level assessment rules for IT assets
			Detection/protection RB	• Knowledge of malicious attack detection and protection rules
		Product KB	Version KB	• Knowledge of product version
			Configuration KB	• Knowledge of product configuration