3-5 Cybersecurity Information Exchange Techniques: Cybersecurity Information Ontology and CYBEX

TAKAHASHI Takeshi and KADOBAYASHI Youki

Cyber threats cross country borders, but most organizations are currently coping with them individually without global collaboration mainly due to the lack of global standards for cybersecurity information exchange framework and format. Though there exist multiple local or community standards to solve this problem, they are not orchestrated in order for each organization to fully collaborate each other. To build the basis of cybersecurity information exchange framework, this paper proposes a cybersecurity operational information ontology. It also discusses the standardization activities on cybersecurity information exchange, such as CYBEX and its ensembles, and its effectiveness from the standpoint of expediting cybersecurity information exchange and streamlining cybersecurity operations.

Keywords
Cybersecurity, Ontology, Information exchange, CYBEX

1 Introduction

As Internet access has become more widespread globally, cyber society has been developing rapidly in recent years. However, security in cyber society, i.e., cybersecurity, is still in the process of developing. Though cyber threats cross country borders, countries and organizations are currently coping with them individually without global collaboration. Despite the fact that malicious users can attack computers all over the world by executing prepared software, the countermeasures for attacks are implemented by individual countries or organizations separately. In addition, information exchange/sharing that is needed for the cooperation between countries/organizations is currently implemented by e-mail, telephone, and face-to-face meetings on as-needed basis, and is therefore very inefficient and takes time and manpower.

One of the causes of this situation is the lack of a common global framework and format for information exchange. To cooperate and implement cybersecurity countermeasures, countries/organizations need to share such framework and format. Such framework and format eliminate regional disparities of available cybersecurity information on a global scale. This will enable countries that are still in process of developing cybersecurity and have not accumulated much information (hereafter developing countries) to obtain information more easily, and also significantly reduce cyber attacks that utilize computers in such countries to target computers in advanced countries. The format and framework also automate cybersecurity operations. Such automation will reduce the needed manpower for the operations and also avoid errors that can be caused by relying on human hands. Moreover, facilitating the automation will further promote the elimination of the above-mentioned regional differences in cybersecurity information on a global basis.

Though there are various standards for information exchange format, different regions have different standards, and a collective framework has not yet been established. For this reason, in the current situation it is not

possible to argue the completeness of cybersecurity based on the existing standards, and it is difficult to improve inefficient cybersecurity operations. To cope with this issue and build the basis of global cybersecurity information exchange, this paper proposes a cybersecurity operational information ontology. An ontology is a conceptualized model of the world and is expected to facilitate information sharing/reuse between software. The proposed ontology is based on the result of discussions/reviews with the actual cybersecurity operation providers in Japan, the USA, and Korea. Though cybersecurity operations vary depending on the provider, we have succeeded in building a common ontology of cybersecurity operational information by abstracting operations.

The rest of the paper is organized as below: Chapter **2** introduces the cybersecurity information ontology, Chapter **3** introduces the standardization activities of cybersecurity information exchange techniques, such as CYBEX, Chapter **4** discusses the effectiveness of CYBEX, and Chapter **5** concludes this paper.

2 Cybersecurity information ontology

The proposed cybersecurity information ontology is built by defining operation domains, roles required in each of the domains, and then the information that these roles handle.

2.1 Operation domains

This section defines three domains for cybersecurity operation that are needed to maintain security in cyber society. They are the Incident Handling, IT Asset Management, and Knowledge Accumulation domains.

Incident Handling domain: This domain monitors incidents, events that constitute the incidents, and attack behaviors caused by the incidents to detect individual incidents that are occurring in cyber society and respond to them. For instance, it detects anomalies through warning notifications from anomaly detection devices and collects various logs to build up evidence. This domain's operation also includes providing early warnings and advice to user organizations.

IT Asset Management domain: This domain runs the necessary cybersecurity operations within each user organization such as installing, configuring and managing IT assets. It also runs operations for both prevention and post-incident measures within organizations.

Knowledge Accumulation domain: This domain conducts research on cybersecurity and accumulates the obtained knowledge in a form that can be reused by other organizations. Consequently it consolidates the knowledge to be widely shared between organizations.

2.2 Roles

We define the roles required to run cybersecurity operations in the aforementioned domains. The Incident Handling domain has Response Team and Coordinator roles, the IT Asset Management domain has Administrator and IT Infrastructure Provider roles, and the Knowledge Accumulation Domain has Researcher, Product & Service Provider, and Registrar roles. We have defined these roles from a functional viewpoint. Therefore, it should be noted that an instance of a certain role could be an instance of another role.

Administrator: This role manages the system of each user organization and owns IT asset information within the organization. IT administrators within an organization are the typical instance of this role.

IT Infrastructure Provider: This role provides IT infrastructure to each organization. The IT infrastructure includes network connectivity, data centers, and SaaS. The internet service provider (ISP) and application service provider (ASP) play this role.

Response Team: This role monitors and analyzes various incidents in cyber society such as illegal accesses, DDoS attacks, and phishing to accumulate incident information. Based on this information, this role will implement countermeasures, for instance, adding the addresses of

phishing sites to a blacklist. The incident handling team in a security management service provider is its typical instance.

Coordinator: This role coordinates entities and responds to potential threats based on the information of known incidents and crimes. Computer Emergency Response Team/Coordination Center (CERT/CC) is its typical instance.

Researcher: This role conducts research on cybersecurity information and extracts the obtained knowledge. For instance, cybersecurity research team in an MSSP such as X-force of IBM and Risk Research Institute of Cyber Space (RRICS) of LAC are its typical instances.

Product & Service Provider: This role possesses information of products and services of software and hardware such as identifiers, versions, vulnerabilities, patches and configuration information. Software houses and individual software developers are its typical instances.

Registrar: This role classifies and organizes cybersecurity knowledge provided by the Researcher and the Product & Service Provider, and provides the information in a form that can be reused by other organizations. NIST in the USA and IPA in Japan are its typical instances.

2.3 Cybersecurity information

Based on the aforementioned operation domains and roles, this section defines the information required for cybersecurity operations. Figure 1 shows the outline of the proposed ontology. Taking account of the information provided by each role, this section defines four databases and three knowledge bases.

Incident database: This database stores accumulated information on incidents such as event records, attack records, and incident records. An event record is a record of computer events that includes packets, files and their processing. Generally it is automatically provided as a computer log. An attack record contains information of attacks such as actual attack sequences. This record will require more details with the progress of incident analysis. An incident record is a general record of a particular incident such as computer states and situation of damage. It is generated from event records and assumed/estimated information. Attack information is linked to this record. Based on this record, the administrators judge the harmful effects and need for countermeasures.

Warning database: This database stores accumulated information on cybersecurity warnings, which is created based on the incident database and Cyber Risk knowledge base.

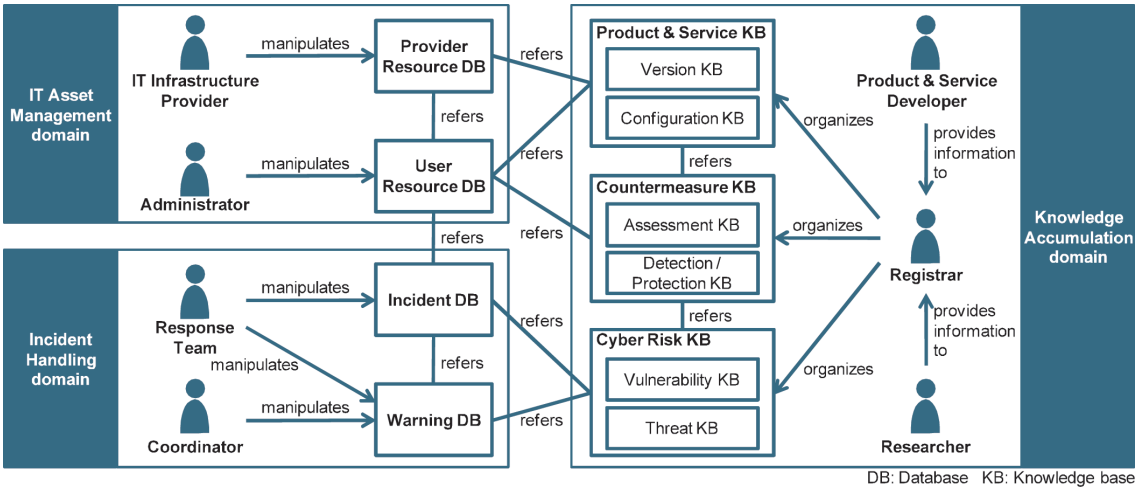

Fig.1 *Cybersecurity operational information ontology*

User organizations can take necessary countermeasures based on this information.

User Resource database: This database stores accumulated information required to manage the assets of each user organization, such as a list of software/hardware and their configurations, status of resource usage, security policies, security level assessment result, and intranet topology. It also contains information of a list of subscribed cloud services as described later and record of service usage.

Provider Resource database: This database stores accumulated information on the assets that individual organizations use outside their organizations, mainly on external networks and external cloud services. External network information contains the information related to networks that connects each organization to other organizations, including inter-organization network topology, routing information, access control policy, traffic status and security level. External cloud service information includes the information of cloud service providers and their services, service specifications, workload information and security policy information of each cloud service.

Cyber Risk knowledge base: This knowledge base contains accumulated information on cybersecurity risks and includes the Vulnerability and Threat Knowledge bases. The former accumulates information of known vulnerabilities including naming conventions, classification and enumeration of vulnerability information, as well as vulnerabilities caused by configuration errors. The latter accumulates information of known cybersecurity threats including attack patterns, attack tools, trends and statistics of attacks, as well as threats of misuse that could be caused by users' inappropriate usage whether it is benign or malicious.

Countermeasure knowledge base: This knowledge base accumulates information on cybersecurity countermeasures and contains two knowledge bases: the Assessment and Detection/Protection knowledge bases. The former accumulates information of security level assessments on IT platforms, such as rules and criteria for assessment and checklists, and the latter accumulates the existing knowledge of detecting/protecting from security threats, such as IDS/IPS signatures and detection/protection rules that are compliant with the signatures.

Product & Service knowledge base: This knowledge base accumulates information on products and services, and contains two knowledge bases: the Version and Configuration knowledge bases. The former contains naming conventions of identifiers and enumeration of each version of products/services, and also includes security patches for products. The latter accumulates configuration information of products/services, such as the naming conventions, classification, and enumeration of configurations, as well as usage guidelines.

For further details on the ontology, refer to [1].

3 Cybersecurity information exchange standards

The ontology has built a platform to discuss who should own information and what kind of information needs to be exchanged. Building the platform, however, does not mean that it can facilitate information exchange, and therefore it is necessary to build a framework to realize information exchange based on this platform. As one of the initiatives to achieve this, ITU-T has been working on cybersecurity information exchange techniques (CYBEX).

CYBEX is defined by Recommendation ITU-T X.1500 "Overview of cybersecu-

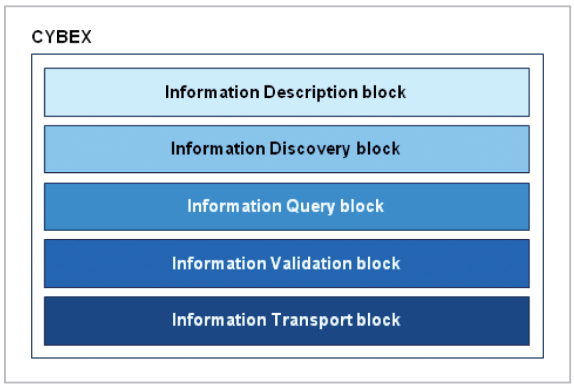

Fig.2 CYBEX's functional blocks

rity information exchange," which provides a framework to structure cybersecurity information and exchange cybersecurity information over networks.

CYBEX consists of five main functional blocks: the Information Description, the Information Discovery, Information Query, Information Validation, and Information Transport blocks. These functional blocks work together to enable cybersecurity information exchange between organizations (Fig. 2).

Information Description block: This block defines the expression/description format of cybersecurity information. A number of useful regional standards are already in use, even though they are not recognized as international standards. Table 1 shows typical standards that were built by the initiatives of MITRE, FIRST, NIST and IETF. CYBEX framework incorporates these standards. Our proposed ontology, which is mentioned in the Appendix of the Recommendation ITU-T X.1500, can also clearly explain the role of these standards as shown in Fig. 3.

Information Discovery block: This block identifies/finds the location of the cyber security information that is described by the aforementioned Information Description block. There are two methods to achieve this: central management and distributed management. CYBEX defines a discovery method that uses OID for the former and one that uses RDF for the latter. Further details are described in the Recommendation ITU-T X.1570, one of the recommendations of X.1500 series.

Information Query block: This block defines the method to request information or request to add/modify/delete information to the owner organization, after the cybersecurity information has been structured and the owner has been identified. This method is called SYIQL which is an extension of SQL, and can perform secure queries similar to SQL operations. However, as CYBEX is not based on the premise of the use of SYIQL, users could implement arbitrary scheme other than SYIQL.

Information Validation block: This block checks whether the information and the sender of the information can be trusted prior to sending the required information over network. Specifically, it confirms the identity of the communicating parties to secure the authenticity. When a company starts a business with a new company, it is normal to check the information that confirms the identity of the new partner such as the corporate registry, in order to secure the authenticity. Similar to this, the EVCERT technique that confirms the identity of the sender of the information is used when receiving cybersecurity information to check

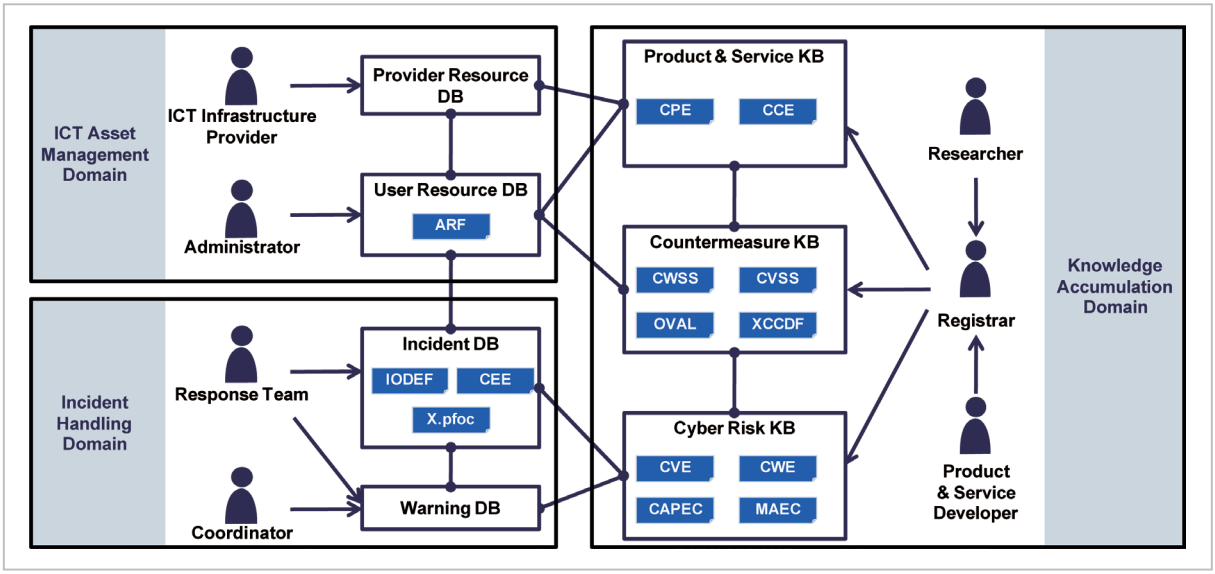

Fig.3 *Cybersecurity operational information ontology and CYBEX family recommendation*

the authenticity of the sender.

Information Transport block: This block transmits cybersecurity information over a network, and defines the required functions for the protocols for that purpose. A transport method that uses BEEP is proposed and its proof-of-concept implementation is already available[2].

As described above, CYBEX links these five blocks to describe information, identify the organization that possesses the information, send queries to them, and secure the authenticity of the organization in order to realize information exchange.

For further details on CYBEX, refer to [3][4].

Table 1 *Major cybersecurity information specifications*

Specification Name	Description
CVE	Defines the description format for vulnerability information
CAPEC	Defines the description format for attack pattern information
CCE	Defines the description format for configuration information
CPE	Defines the naming scheme for IT platforms including software
OVAL	Defines a language to describe configuration
CEE	Defines the description format for computer events
MAEC	Defines the description format for malware

4 Evaluations and Discussions

This chapter discusses the usability and applicability of the proposed ontology and CYBEX.

4.1 Needed cybersecurity information to support the cloud environment

As an example that shows how the ontology functioned as a platform to discuss cybersecurity information, we introduce a case example of listing up cybersecurity information required for a cloud environment. The detailed discussion can be found in [1], but in conclusion, as Table 2 shows, it is possible to list up the information that should be managed by each database. Such list contains both the information that is newly required for cloud environments and that has become more important than before. The list can be a base for discussion of the necessity of standards for new information description formats, some of which have been considered for incorporation into CYBEX in future.

4.2 Streamlining operations

The ontology and CYBEX facilitate streamlining cybersecurity operations since they can convert various types of cybersecurity information into machine-readable format. Some use cases of what can be streamlined are introduced below.

Inter-organizational information sharing: Traditionally information is shared by the use

Table 2 *A set of cybersecurity information that becomes more important in cloud environments*

KBs/DBs	Needed cybersecurity information
User Resource DB	Cloud service subscription, user identity, data access control policy, resource dependency, security level information
Provider Resource DB	Subscriber identity information, service security level information
Incident DB	Data provenance, data placement log, incident/event information
Warning DB	Data incident warning
Cyber Risk KB	Impact range of vulnerabilities, configuration vulnerabilities
Countermeasure KB	Measurement schemes to handle virtual machines, multiple machine environments
Product & Service KB	Service enumeration/taxonomy, service configuration

Note – DB: Database, KB: Knowledge Base

of telephone, e-mail, and face-to-face conversations or meetings. This is very inefficient considering that malicious users can attack computers all over the world in no time. However, with the use of the ontology and CYBEX, when it becomes possible to convert cybersecurity information into machine-readable format, certain information could be instantly shared with numerous computers in the world in theory. Though there are still some operational issues, we recognize that this will improve the efficiency of inter-organizational information sharing one step further.

Information and knowledge accumulation: When more cybersecurity information becomes available in machine-readable format or in organized form with additional meta information such as classification and ID, it will be possible to organize information based on this data. With traditional operation methods, operators have to manually record the information they obtained through human communication, and add an ID and classify the information according to their judgment; however, if all these tasks are omitted, it will not only improve the efficiency of operations, but also eliminate the need to consider the difference of IDs and classification methods between operators.

Language-agnostic information sharing: It is possible to add meta information such as classification to the cybersecurity information exchanged by CYBEX. The classification method itself is expected to be established as a standard like CWE. IDs for the classification are language-agnostic such as numbers and alphabet, and therefore, cybersecurity information is searchable regardless of the language of the information. In the past, the whole database needs to be translated prior to the search, but the IDs changed that; only the search result of the database needs to be translated. In addition, if the part of the information is already translated by another organization, it is possible to ask them to share the information. Though some language issues still remain, we consider CYBEX will be able to move this problem closer to a solution.

Our research also contributes to operation design for inter-organizational information sharing, increases time to spend on improvement of operation quality, reduction of human errors when exchanging information, improvement of operation quality of developing operators, and the potential for the system to support decision making by operators. For further details, refer to [4].

4.3 Global cybersecurity

Currently cybersecurity threats are increasing in those developing countries. According to the Symantec report published in April 2010, there has been a significant increase in malicious activities in developing countries such as Brazil, Poland, India, and Russia, which are all in the top 12 countries of such activities. Especially in 2009, Brazil overtook Germany and rose to third place. These countries have been seeing a rapid spread of broadband services in recent years; but on the other hand, they lag behind in terms of security awareness and countermeasures. As the number of these countries increases, more computers in such countries may become hotbeds for bots which could become serious threats for computers in advanced countries. Thus, it is necessary to consider cybersecurity from the global standpoint to secure cybersecurity in Japan. To achieve this, the present cyber society has to face to cybersecurity in developing countries.

When our ontology and CYBEX become more widespread and available to use globally, security information can be shared in these developing countries where the information was not available before. As a result, it can be expected that the number of affected computers will be significantly reduced in developing countries. Conversely, our intention is to expand the use of CYBEX to reduce disparities in cybersecurity information and security levels across the world.

5 Conclusions

This paper proposed a cybersecurity operational information ontology to facilitate inter-

organizational cybersecurity information sharing and cooperation, as well as introducing global standardization activities related to CYBEX. The ontology and CYBEX are tools to facilitate information sharing, and in order for these tools to be used, countries/organizations need to raise awareness for cybersecurity and also utilize CYBEX. We will always have to consider how we can make countries/organizations use our ontology and CYBEX, and what we need to do to achieve this.

As previously described, CYBEX is expected to streamline cybersecurity operations. In the meantime, it is important to review cybersecurity operations and create a new image of them so that the advantages of implementing CYBEX will become apparent, and motivation to install CYBEX will be raised. By doing so, we expect CYBEX to become more widespread.

Though CYBEX focuses on information exchange, it is necessary in the future to consider how to generate the information to be exchanged, and how to use the exchanged information effectively. As a part of this activity, we have been studying traceback technology[5] that tracks cybersecurity incidents and collect information. Through above activities, we contribute to global cybersecurity, which as a result will allow us to make a significant contribution to cybersecurity in Japan.

Acknowledgements

We would like to extend my gratitude to Professor Yoichi Shinoda (Japan Advanced Institute of Science and Technology), Mr. Hiroshi Takechi (Little eArth Corporation Co., Ltd.), Mr. Toshifumi Tokuda (IBM Japan), Dr. Kazumasa Enami (Vice President of National Institute of Information and Communications Technology), Yukio Takahashi (Director General, Network Security Research Institute), and Shin'ichiro Matsuo (Director of Laboratory, Network Security Research Institute) for their continuous support for our research.

References

1 T. Takahashi, Y. Kadobayashi, and H. Fujiwara, "Onto-logical approach toward cybersecurity in cloud computing," International Conference on Security of Information and Networks, ACM, Sep. 2010.

2 Cybex Information Exchange Tool (cybiet) — A Cybex Discovery and Cybex BEEP profile implementation, Sourceforge.net, http://cybiet.sourceforge.net/

3 A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, and S. Adegbite, "CYBEX — The Cybersecurity Information Exchange Framework (X.1500)," ACM SIG-COMM Computer Communication Review, ACM, Oct. 2010.

4 Takeshi Takahashi, Hiroshi Takechi, and Youki Kadobayashi, "Security operations evolving with CYBEX," atmark IT, [Online]. Available: http://www.atmarkit.co.jp/fsecurity/index/index_cybex.html

5 T. Takahashi, H. Hazeyama, D. Miyamoto, and Y. Kadobayashi, "Taxonomical Approach to the Deployment of Traceback Mechanisms," Baltic Conference on Future Internet Communications, IEEE, Feb. 2011.

(Accepted June 15, 2011)

TAKAHASHI Takeshi, *Ph.D.*

Researcher, Security Architecture Laboratory, Network Security Research Institute

Cybersecurity

KADOBAYASHI Youki, *Ph.D.*

Guest Expert Researcher, Network Security Research Institute/Associate Professor, The Graduate School of Information Science, Nara Institute of Science and Technology

Cybersecurity, Internet Engineering