Athens Journal of Technology & Engineering 2023, 10: 1-10
https://doi.org/10.30958/ajte.X-Y-Z

Automatic Generating System of Information Security Policy

By Kiyoshi Nagata[*]

Information is indispensable in any organization, and its security must be properly guaranteed. At present, information security in an organization includes not only confidentiality but also integrity and availability, and means a balance between them. Establishing an information security policy is effective as a means for that purpose, but it is considered to be a high hurdle for organizations such as SMEs, which have neither personnel nor financial leeway, to tackle it. We thought that a system to help establish information security policies was necessary, so we proposed a framework and tried to implement it in application programs. At present, the creation process of the basic policy by presenting the template and the creation of the organizational profile are implemented. In this paper, we propose a method to reflect the characteristics obtained from the organization profile not only in the basic policy but also in the following countermeasure standards and implement it in the application program.

Keywords: *security policy, information asset, ontology, generation system, SMEs*

Introduction

According to the IMD Word Digital Competitiveness ranking 2022[1], the total rank of Japan is 29th amongst 63 counties, and 8th even amongst 14 Asia-Pacific counties. In the report, they say that the cybersecurity capabilities both at the company and governmental level have become very important factor, then the result reflects those factors facilitating the strengthening of capabilities to protect digital infrastructure from cyber-attacks. As one of subfactors for the ranking evaluation, "Cyber security" rank of Japan is 45th which dropped the overall evaluation value along with other indicators values.

Bartlett (2019) investigates Japanese cyber-security policy making process by adopting Campbell's four categorizations (Campbell 2014). According to his result, Japan's cybersecurity policy was swayed by the motives of each organization before 2010, and it was finally affirmed after 2011 where new set of provisions aiming explicitly at improving the cybersecurity of small-and medium-sized enterprises (SMEs) were implemented regarding information technology. Although more than 30% of 195 Japanese SMEs assumed information security risks as a risk that makes business continuity difficult, only 19.6% of SMEs cited awareness of cyber security as a reason for increasing IT investment over the next five years (2022 White Paper on Small and Medium Enterprises in Japan).

[*] Professor, Daito Bunka University, Japan.

[1] https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/.

From the ISTR (Internet Security Threat Report 2019 [2] , attacks on organizations with 250 or fewer employees are no less common than those on larger organizations, and it claims that “Employees of smaller organizations were likely to be hit by email threats-including spam, phishing, and email malware than those in large organization. They claim that “Smaller organizations can be held hostage when faced with cyberattacks since they have fewer IT security resources to avoid or respond to complex attacks”.

Even if the government establishes a cybersecurity policy and provides financial assistance, it is difficult for SMEs to cope with the shortage of IT engineers with advanced knowledge. Moreover, it is true that the cause of cyber security breaches is not necessarily the lack of advanced IT technology. Together with MIC (Ministry of Internal Affairs and Communications) and NPSC (National Public Safety Commission), METI (Ministry of Economy, Trade and Industry) published a report title “Occurrence of unauthorized computer access and research and development of technology related to access control functions” (in Japanese)[3], in which the number of the identification code theft type unauthorized access that have been cleared from 2018 to 2022 was listed by method. These are top three means of stealing amongst 482 cases: “Taking advantage of the lax password setting and management of authorized users” (230), “committed by a former employee or an acquaintance who was in a position to know the identification code” (41), and “Leakage from authorized users or by social engineering” (38). These problems are not due to the lack of advanced IT technology, but due to the lack of information security awareness and recognition.

In order to cope with information security issues mentioned above, establishing information security policy is essential and principal mean. Ministry of Education of Japan (MEXT) issued a notice to encourage national universities to develop and publish security policies, and raised the importance to private universities. Then almost all the universities and colleges published information security policy statements on their website.

Although we could not find out any results of a fact-finding survey on the status of information security policy development in SMEs in Japan, the survey report titled “Cyber Security Breaches Survey 2019: Statistical Release”[4] conducted by the Department for Digital, Culture, Media and Sport in UK pointed out that only 32% of micro and small firms with less than 49 employees established the cybersecurity policy while 71% of medium firms and 74% of large firms did.

With the aim of establishing information security, especially in SMEs, we tried to construct a support system for information security policy developing (Nagata and Kigawa 2019). We proposed the framework and created prototype, however the system development as an actual application is still underway. In this paper, we propose a method of creating a basic policy document suitable for each organization by incorporating ontology.

[2] https://www.academia.edu/14479611/INTERNET_SECURITY_THREAT_REPORT.

[3] https://www.meti.go.jp/press/2020/03/20210304003/20210304003-1.pdf.

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf.

The rest of paper organized as follows; our former works and some general issues on security management and policy are described along with the review of some papers on cybersecurity applying ontology in the next section. And the outline of our proposed system is explained as the methodology in the following section. The last section is on the discussion, and the conclusion and future works.

Literature Review

In this section, we will review some of papers or issues on the information security management including our former works, and on cybersecurity related ontology in the following two subsections.

Former Works and Issues on the Information Security Management

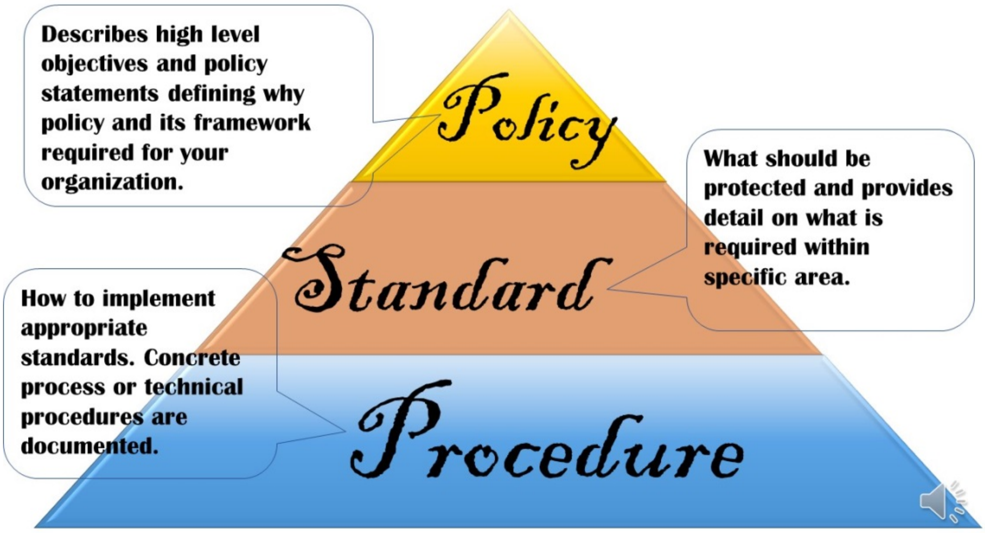
One of well-known ISMS frameworks is ISO/IEC 27000 family[5] some of which are based on BS7799. In 3.1.24 of the latest version of ISO/IEC 27002: 2022 quoting the ISO/IEC 27000:2018, 3.53, the policy is determined as "intentions and direction of an organization, as formally expressed by its top management". Since ISO/IEC 27002 is the guideline for organizational information security standards and management by giving code of practice for information security controls, policy is handled as one of controls in parallel with some of others such as asset classification, personal security, physical and environmental security, etc.

However, the information security policy is sometimes considered as the comprehensive and integrated system for implementing ISMS where various types of controls and measures are incorporated. In an issue titled "Information security policy sample"[6] published in 2016 by Japan Network Security Association, five layers model is adopted. Zinatullin (2016) shows four layers model consisting of "Policy", "Standard", "Guideline", and "Procedure", where "(Basic) Policy" is defines as a document providing a high-level overview of how organizational processes should operate in a secure manner. He also described "Standard" as regulation for the approach to security in the designated scope by preventing them from implementing conflicting or redundant solutions, and "Procedure" as a set of basic steps aiding the implementation of policies and standards. Here we adopt much simpler model of three layers, with "Basic Policy", "Standard", and "Procedure" shown in Figure 1 with short descriptions.

[5] https://www.iso.org/standard/iso-iec-27000-family.

[6] https://www.jnsa.org/result/2016/policy/data/policy_gaiyou.pdf.

Figure 1. *Tree-Layer Model for Information Security Policy*

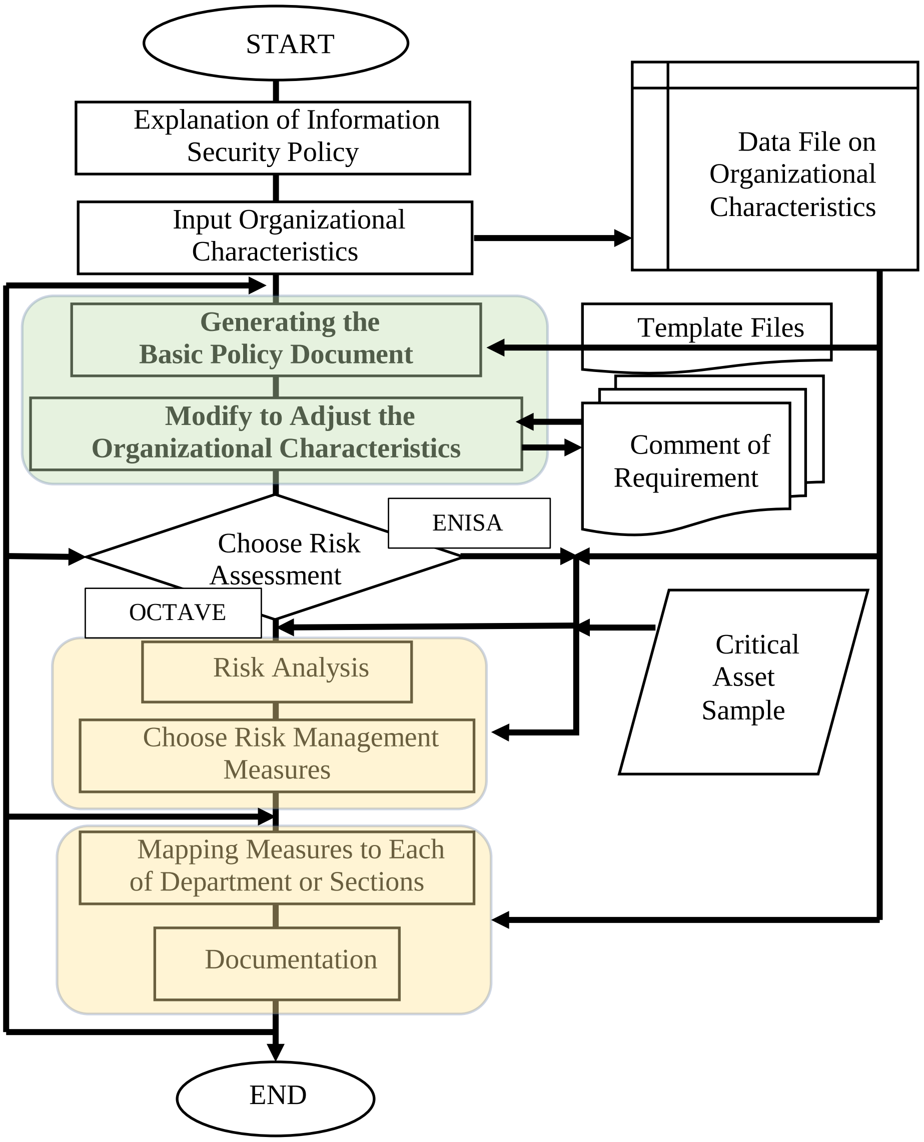

Describes high level objectives and policy statements defining why policy and its framework required for your organization.
Policy
What should be protected and provides detail on what is required within specific area.
Standard
How to implement appropriate standards. Concrete process or technical procedures are documented.
Procedure

According to the model, we proposed to construct a supporting system for generating the security policy, and an initial program was created as a prototype (Nagata and Kigawa 2019). The flow of our proposed system is depicted in Figure 2.

- At first, the information security policy is explained to those who are responsible for the organization in several media such as text, audio, video, etc.
- Organizational characteristics are input, and they will be used in each stage.
- Basic policy is generated using template consisting of several items by referring organizational data file and displayed with some comment on requirement when adopting this expression or word.
- If going on standard stage, choose one of risk analysis methods from OCTAVE (Alberts et al. 2005) or ENISA. Although the analyzing process is somewhat different depending on the method, they output a set of mitigation controls. We have proposed some system for evaluation of risks and find out a set of proper mitigation controls (Nagata et al. 2009). To identify information related assets, we will prepare a list of possible ones (Nagata 2012).
- On procedure stage after information risk analysis, summarize and document the procedures for each department, and the document will be completed after hearing the opinions of each department.
- Over all security policy usually equipped with PDCA cycle. The arrows from down to up in the left part represent it.

In our previous works, we implemented the total framework and the generation and modification process, as shown in the first shaded parts in the figure 2, in a Java application program. Basic policy document is generated by presenting several candidate sentences that reflect the basic organization data and enumerate them, and then correcting them by policy creators. However, the organizational data refection process is just replacement of some terms such as "company" instead of "school" or "university", "client" instead of "student", etc.

Figure 2. *Overall Flow (Former System)*


START
Explanation of Information Security Policy
Input Organizational Characteristics
Data File on Organizational Characteristics
Generating the Basic Policy Document
Template Files
Modify to Adjust the Organizational Characteristics
Comment of Requirement
Choose Risk Assessment
ENISA
OCTAVE
Critical Asset Sample
Risk Analysis
Choose Risk Management Measures
Mapping Measures to Each of Department or Sections
Documentation
END

Source: Nagata et al. 2019.

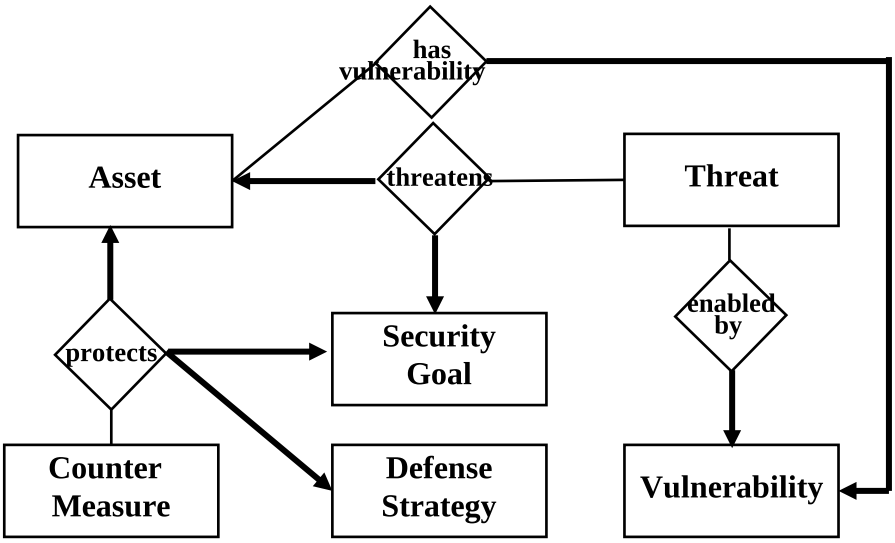
Here we propose to incorporate ontology-based system for sample sentence creation process by which the organization's characteristics will be more reflective.

Review of Some Ontology-Based Information Security Management Systems

Gruber (1993) noted that "ontology is an explicit specification of a conceptualization. The term is borrowed from philosophy, where an ontology is a systematic account of existence. For knowledge-based systems, what "exists" is exactly that which can be represented." He also claimed that sharing common understanding of the structure of information among people or software agents is one of the more common goals in developing ontologies. Noy and McGuiness (2001) published a guide for ontology development where an ontology is denoted as a formal explicit description of concepts in a domain of discourse, properties of each concept describing various features and attributes of the concept, and restrictions on slots.

Herzog et al. (2007) gave a security ontology built upon classical components of risk analysis, and their relations to each other. Figure 3 is a graphical description of overview of the security ontology that depicts only core concepts and core relations from the original one.

Figure 3. *Core Concepts and Core Relations of the Security Ontology Overview*



Source: Herzog et al. 2007.

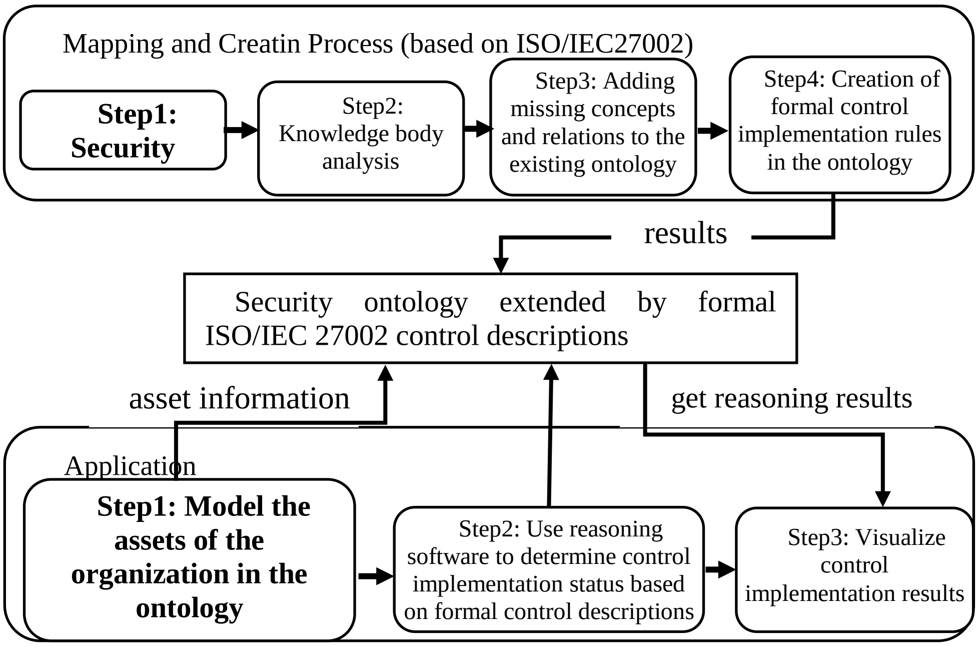
Since the organization's information assets play a central role in establishing an information security policy as an ISMS, creating a detailed information asset ontology becomes important. Zeb et al. (2015) proposed an ontology-supported asset information integrator system (AIIS) which can help industry experts to exchange the tangible capital assets information and transform the way they were exchanged at that time between the municipal and provincial governments in Canada. In the paper, they presented the ontology development methodology in ten steps as the hybrid version of former works.

Adesemowo et al. (2016) published a paper on IT assets ontology aiming to assist in determining inherent attribute of IT assets that can assist in the process of IT assets risk value assessment. They divide Assets into Personnel, Network, Services, Data, Hardware, Software, and Information. For ontology creation, "IT Asset" class is divided into "TangibleAsset" and "IntangibleAsset" classes according to which properties, "tangible" or "intangible", they have.

As application of ISMS policy implementation of policy ontology, Fenz et al. proposed an ontological mapping of ISO/IEC 27001 (Fenz et al. 2007) and

ISO/IEC 27002 (Fenz et al. 2015). Figure 4 is the overview of creating security ontology based on ISO/IEC 27002. We stress the first steps in each process with bold face letters, as these initial steps are related to our proposing system.

Figure 4. *Overview of Mapping ISO 27002 in the Ontological Structure and Applying the Results*


Mapping and Creatin Process (based on ISO/IEC27002)
Step1: Security
Step2: Knowledge body analysis
Step3: Adding missing concepts and relations to the existing ontology
Step4: Creation of formal control implementation rules in the ontology
results
Security ontology extended by formal ISO/IEC 27002 control descriptions
asset information
get reasoning results
Application
Step1: Model the assets of the organization in the ontology
Step2: Use reasoning software to determine control implementation status based on formal control descriptions
Step3: Visualize control implementation results

Source: Fenz et al. 2015.

Pereira and Santos (2012) represented the conceptual framework for information security ontology which is somehow different from that of Fenz et al. (2015). Although they have Asset, Threat, Vulnerability, and Control as common classes, relations between two of them are distinct. For instance, "Control, protect, Asset" in Pereira and Santos, whereas "Control (is) implemented (in) Asset" in Fenz et al. (2015). Thus, the configuration of the ontology will vary depending on the adopted criteria, organizational characteristics, purpose, way of thinking, and etc.

Almost all the policy-based ontologies aim to present mitigation measures for risks and threats and means to compensate for vulnerabilities. For that purpose, it is necessary to create a detailed ontology that matches the characteristics of the organization. Nicola (2009) proposed Unified Process for Ontology (UPON) for building a large-scale ontology in four workflows such as Requirements, Analysis, Design, Implementation, and Test by domain expert and knowledge expert. Their methods, UPON, may be helpful for creating a precise ontology.

KAoS by Uszok et al. (2004) is a pioneering policy management framework using semantically rich ontological representation and reasoning composed of three layers, "Human Interface Layer", "Policy Management Layer", "Policy Monitoring and Enforcement Layer". Basic form of KAoS policy is as follows:

[Actor] is [constrained] to perform [controlled action] (which ha [any attributes])

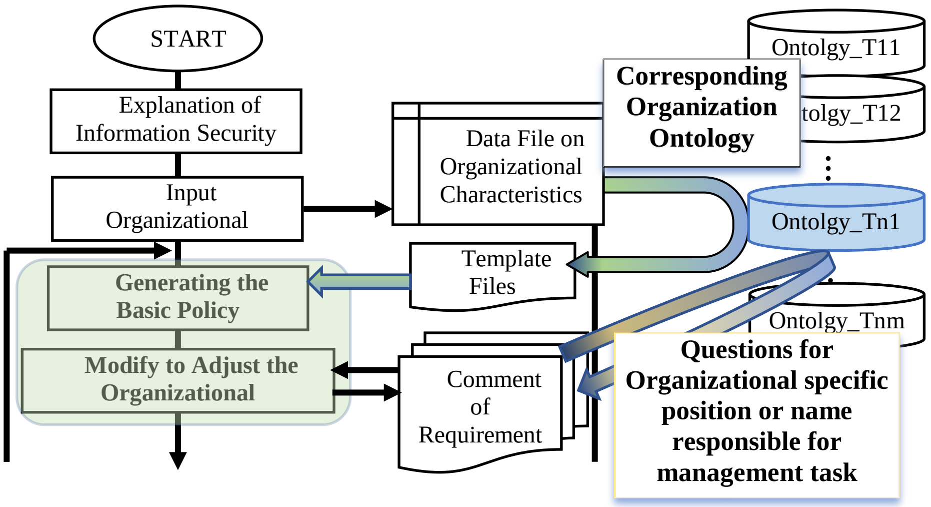
Implementing the enforcement system of OWL policies using the KAoS policy framework into multi-agent systems built on top of the JDK1.4 is also discussed (Tonti et al. 2004).

Proposing System

Although several methodologies mentioned in the previous section are useful and effective for organizational information security establishment, these are concerned with the creation of ontologies that reflect policies and the methodology of automatically configuring means to ensure information security using ontologies. Here we aim to automate the stage of creating basic policy statements in the upper part of the Figure 2.

Figure 5 depicts the newly proposed part of the system for creating general basic statement by applying organization related ontology. In the upper part, the system queries corresponding ontology by using input organizational essential data, then constructs set of candidate phrases of basic policy. Policy makers try to adjust or modify the represented policy with help of the ontology again in the lower part.

Figure 5. *Improved Version of the First Stage of our Former System*


START
Explanation of Information Security
Input Organizational
Data File on Organizational Characteristics
Corresponding Organization Ontology
Ontolgy_T11
tolgy_T12
Ontolgy_Tn1
Ontolgy_Tnm
Template Files
Generating the Basic Policy
Modify to Adjust the Organizational
Comment of Requirement
Questions for Organizational specific position or name responsible for management task

In the above diagram, the organizational ontology also plays an important role, but what is needed here is for creating basic policies phrases, not the detailed ontology that is treated in many studies. For the process, ontologies for different types of organizations must be created in advance. We describe the method for the ontology creating.

Step 1. Gather the set of sample phrases of basic policy. Then classify them into each of typical items in our former implemented system, such as “Concept and Purpose”, “Scope of Application”, “Definition of terms”, “Composition/ Positioning”, “Management system”, “Role/responsibility”, and “Basic requirements”.

Step 2. Analyze sample policy to get competency questions (CQ) for ontology. For example, if there is a sample phase reading “The CEO serves as chairman of the

information protection committee and is responsible for information security within the organization", then CQs will be like as follows:
CQ1: "Is there a body for ensuring information security"
CQ2: "Who serves as chairman of the ISMS committee?"
CQ3: "Is the chairman ultimately responsible for ISMS?"
Step 3. Configure each of ontologies according to type of organization. These types of organization are pre-determined relatively broadly according to business conditions, such as universities, high schools, manufacturing industries, distribution industries, etc., as well as their scale and management style. Then create an ontology that will be common to each of these types.

In step 3, we can apply existing ontologies for general matters such as FOAF ontology for academic organizations (Kalem and Martiri 2011).

Conclusion & Future Works

We proposed automated basic information security policy statement generation system for embedding into existing Java application program. The key point is to apply ontology, and unlike existing research, we also propose a method of creating competency questions from sample sentences and configure an ontology which can respond to them.

We use Tree-Tagger for language structure analysis, in the CQ generation process, and then configure ontologies according to type of organization by using Protégé. In our renewal Java application, we will include a SPARQL (Simple Protocol and RDF Query Language) engine, e.g. ARQ, and adopt some readability indexes (DuBay 2004) for evaluating the representing sentences.

However, ontology configuration is a time-consuming and skill intensive process, and the validity assessment of the prepared statement will be necessary. About the readability index we did not explain, there is also the problem of which index to choose.

Although application programming by Java is still in the development stage, we think that the direction for proceeding to the countermeasure standard creation stage following this basic policy stage is indicated.

References

Adesemowo AK, Solms R, Botha RA (2016) ITAOFIR: IT asset ontology for information risk in knowledge economy and beyond. In *Proceedings of 11th International Conference, Global Security, Safety and Sustainability: The Security Challenges of the Connected World 2017*, 173–187. London, UK, January 18-20, 2017.

Alberts C, Dorofee S, Stevens J, Woody C (2005) In *OCTAVE-S implementation guide*, Version 1.0, CMU/SEI-2003-HB-003.

Bartlett B (2019) How Japanese cybersecurity policy changes. In *Harvard Program on U.S.-Japan Relations Occasional Paper Series 2019-01*. Weatherhead Center for International Affairs, Harvard University.

Campbell JC (2014) *How policies change: the Japanese Government and the aging society*. Princeton University Press.

DuBay WH (2004) *The principles of readability*. Costa Mesa California: Impact Information.

Fenz S, Goluch G, Ekelhart A, Riedl B, Weippl E (2007) Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In *Proceedings of 13th IEEE International Symposium on Pacific Rim Dependable Computing,* 381–388. Melbourne, Australia, December 17-19, 2007.

Fenz S, Plieschnegger S, Hobel H (2015) Mapping information security standard ISO/IEC 27002 to an ontology structure. *Information & Computer Security* 24(5): 452–473.

Gruber TR (1993) A translation approach to portable ontology specifications. *Knowledge Acquisition* 5(2): 199–220.

Herzog A, Shahmehri N, Duma C (2007) An ontology of information security. *International Journal of Information Security and Privacy* 1(4): 1–23.

Kalem E, Martiri E (2011) FOAF-academic ontology: a vocabulary for the academic community. In *Proceedings of Third International Conference on Intelligent Networking and Collaborative Systems,* 440–445. Fukuoka, Japan, 2011.

Nagata K (2012) Construction of effective database system for information risk mitigation. *Security Enhanced Application for Information Systems,* INTECH Open Access Publisher, Chapter 6, 111–130.

Nagata K, Kigawa Y (2019) Construction of support system for information security policy. In *Proceedings of the 20th Asia Pacific Industrial Engineering and Management Systems Conference 2019*, 942–947. Kanazawa, Japan, December 2-5, 2019.

Nagata K, Kigawa Y, Cui D, Amagasa M (2009) Method to select effective risk mitigation controls using fuzzy outranking. In *Proceedings of the 9th International Conference on Intelligent Systems Design and Applications*, 479–484. Pisa, Italy, November 30 - December 2, 2009.

Nicola AD, Missikoff M, Navigli R (2009) A software engineering approach to ontology building. *Information Systems* 34: 258–275.

Noy NF, McGuiness DL (2001) *Ontology development 101: a guide to creating your first ontology*. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05.

Pereira T, Santos H (2012) An ontology approach to information security management. In *Proceedings of the 7th International Conference on Information Warfare and Security,* 368–375. Seattle, Washington, USA, March 22-23, 2012.

Tonti G, Montanari R, Bradshaw JM, Bunch L, Jeffers R, Suri N, et al. (2004) Automated generation of enforcement mechanisms for semantically-rich security policies in Java-based multi-agent systems. In *Proceedings of IEEE First Symposium on Multi-Agent Security and Survivability,* 11–20. Drexel, PA, USA, 2004.

Uszok A, Bradshaw JM, Jeffers R (2004) KAoS: A policy and domain services framework for grid computing and semantic web services. In *Trust Management. iTrust 2004,* 16–26. Lecture Notes in Computer Science, 2995. Berlin, Heidelberg: Springer.

Zeb J, Froese T, Vanier D (2015) An ontology-supported asset information integrator system in infrastructure management. *Built Environment Project and Asset Management* 5(4): 380–397.

Zinatullin L (2016) *The psychology of information security*. IT Governance Publishing.