Athens Institute

Working Paper No. 2025-2787-32

14 November 2025

Ontology-based System for Generating Information Security Policy

Kiyoshi Nagata

This paper should be cited as follows:

Nagata, Kiyoshi (2025) Ontology-based System for Generating Information Security Policy. Published by the Athens Institute: Working Paper No. 2025-2787-32, 14 November 2025. Pages 1-14

No.: 2025-2787-32
Date: 14 November 2025
DOI:
ISSN: 2241-2891

Previous Working Papers available at: www.atiner.gr/papers.htm

This series began in 2012 and was known as the Conference Paper Series until 2024. In 2025, the series was renamed and is now called the Working Paper Series.

Athens Institute (www.atiner.gr)
2025

Ontology-based System for Generating Information Security Policy

By Kiyoshi Nagata[*]

In any kind of organization, information security is indispensable for properly guaranteeing not only confidentiality but also integrity and availability while keeping them in balance. Although establishing an information security policy is effective as a means for that purpose, it is still a high hurdle especially for SMEs without neither personnel nor financial leeway. Thus, we have proposed a framework of a system for automatically generating an information security policy and tried to implement it in application programs, with the help of which the organization generate information security policies properly adjust to each organization. The system was proposed referencing an information security ontology corresponding to the organization based on the input organizational characteristics and reflecting them in a template. However, the specific ontology is incomplete, and no algorithm for reflecting it has been created. In this research, we aim to actually create an ontology for each organizational characteristic and implement a trial algorithm in an application program.

Keywords: *Information security policy, Organizational profile, Ontology-based System, Application program*

Introduction

The importance of information security in organizations is increasing, and in recent years, security breaches have become a problem, especially with the use of AI. In order to address these issues and maintain and develop the sustainability of organizational activities, not only technical responses but also measures that involve the organization as a whole are necessary.

The total rank of Japanese digital competitiveness in 2024 is 31st amongst 67 economies, and 7th even amongst 14 Asia-Pacific economies according to the IMD Word Digital Competitiveness ranking 2024[1]. These results are nearly identical to those in 2022. Amongst many refined factors for resulting the rank, “Cyber Security” is positioned as one aspect of “IT integration” in the “Future Readiness”, and Japan is ranked 45th, which is by no means good. The method for calculating this factor scores is not made clear just from the report, but by referring to the method for calculating “Government Cyber Security Capability”, it is likely based on one choice from “No” or “Not really” or “Somewhat” or “Mostly” or “Yes” as answer to the following questions:

> “Do organizations have sufficiently technologically skilled staff and resources to mitigate harm from cybersecurity threats?”

[*] Professor, Faculty of Business Administration, Daito Bunka University, Japan.

[1] https://imd.widen.net/s/xvhldkrrkw/20241111-wcc-digital-report-2024-wip (available: 04/05/2025)

In terms of preventive measures, we need to focus on the refined factor "(seize) Opportunities and threats (by cyber-attacks)" is positioned as one aspect of "Business agility" also in the "Future Readiness". Japan is ranked 67th, which is the worst amongst overall economies. This factor is considered to be closely related to the establishment of information security policy, which is the subject of this paper.

Although Japan's ranking in cybersecurity in the IMD reports is not heigh, Japan is in the top tier group "Role-modeling" in the ITU's cybersecurity index in the 5th edition of Global Cybersecurity Index (GCI) 2024[2]. GCI has 5 measures for each pillar such as "Legal", "Technical", "Organizational", "Capacity-development", and "Cooperation", and each measure is calculated by weighting averaged of score associated with ternary response within each pillar. Each measure has 20 scores as the full mark, and the index is calculated from the total score of them. Japan's total score is 97.58 which is 8th amongst 10 Asian countries in this top group. The worse scores comparing to other countries' scores are those in pillars "Cooperative (18.91)", "Capacity-development (19.07)", and "Technical (19.6)" while the best two countries, Indonesia and Republic of Korea, have 20 of all the measures.

There are differences between the two figures, IMD report is based on data from private research institutes, while ITU's one is based on responses from national agencies, but the figures show that Japan cannot be said to be leading the way in the field of information security which is an important factor for the business agility and the future development. One of the main reasons for this is the lack of awareness and communication regarding information security within and between organizations.

We believe that the establishment and publication of an information security policy that reflects the characteristics of the organization can help to solve this problem. But it is a particularly high hurdle for small or medium-sized enterprises (SMEs) with limited human and financial resources.

The final goal of our project is to create an application system that helps any type of organization to establish an information security policy which reflects characteristics of the organization and the purpose of their activities. For this purpose, we have implemented the creation process of the basic policy by presenting the template reflecting the organizational profile and also have proposed methods for the reflection of the characteristics of the organization obtained from its profile not only to the basic policy but also to the selection of countermeasures associated with identified critical assets. We believe that certain types of ontologies are very effective measures for representing characteristics of organizations, but it seems that there are no appropriate applications linking them with information security policy creation. Even though our project for ontology-based information policy creation is still in progress and the application program is not yet completed, the idea is novel, and we are sure that the application program that will be completed in the future will be useful.

The rest of this paper will be organized as follows. In the next section, we will consider the definition of information security policy by showing its current state of prevalence in Japan, especially among SMEs. In the following section, after

[2] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (available:2025/05/20)

a brief explanation of ontology, we will discuss the incorporation of ontology, and its implementation based on our previous research. Then describe the details of the proposed ontology-based query system in SPARQL reflecting the type and characteristics of an organization. Last part is the conclusion and our future works.

Information (Cyber) Security and Policy

In this section, we will look at the state of information security measures in Japanese SMEs, particularly in terms of establishing information security policies, referring to the report conducted by IPA (Information-technology Promotion Agency, Japan).

Information Security Measures for SMEs in Japan

According to the preliminary results of the 2024 survey on information security by SMEs and other businesses released by IPA[3], approximately 70% of SMEs in Japan do not have an organizational security system in place, which have increased from 49.2% in the 2021 survey "FY2021 Survey on Information Security Measures in Small and Medium-sized Enterprises (only in Japanese)"[4].

The percentage of companies "have not invested in information security measures" was 62.6%, up from 33.1% in the 2021 survey. The most common reason for not investing in information security measures was "Don't feel it's necessary (44.3%)" followed by "Can't see the cost-effectiveness (24.2%)" and "It's too costly (21.7%)". These results suggest that SMEs are reluctant to make information security investments due to limited financial resources.

Establishing Information Security Policy as Measures

The 2021 edition of the report by IPA includes a survey related to information security policies as organizational and operational security measures, so we will refer to that here.

Only 13.5% of 4074 organizations responded that they have documented information security policies (regulations and rules). This figure is low, but many of the contents that should be included in an organizational information security policy are described separately, such as "establishing management rules for general user accounts (28.2%)", "crushing/melting hard disks and other items when discarding them (17.2%)", and "locking up and managing information (on paper, etc.) (25.7%)".

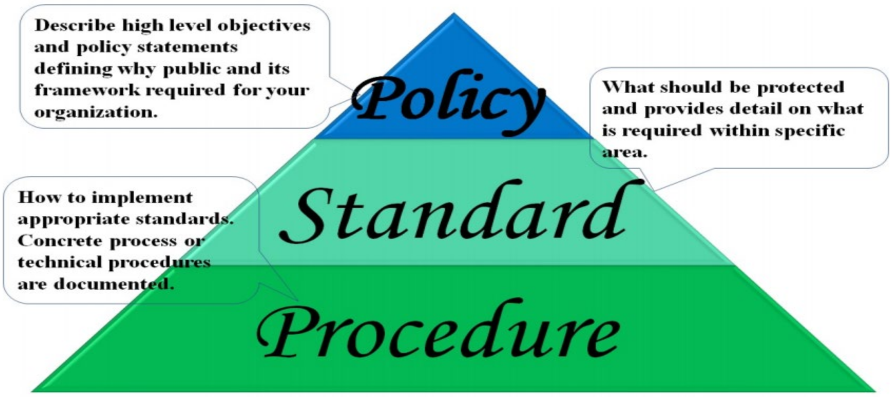
Out of the 550 organizations that responded that they have a documented information security policy, the document states as follows:

[3] https://www.ipa.go.jp/pressrelease/2024/press20250214.html (in Japanese) (available: 2025/05/20)
[4] https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf (in Japanese) (available: 2025/05/20)

1. Basic Policy (85.8%)
2. Confidentiality obligation (74.2%)
3. Appointment of person in charge (64.0%)
4. Detailed rules (countermeasures standards, implementation procedures, operation regulations, etc.) (53.3%)
5. Limits on personal use of equipment, email, and Internet access (50.5%)
6. Obligation to report loss (49.1%)
7. Clarification of access rights (46.0%)

In the three-layer policy model, Figure 1, which we have adopted (Nagata 2024, 2023), the above contents are concentrated in the top two layers, with documentation of them in the lowest layer. "Confidentiality obligation", "Appointment of person in charge", and "Obligation to report loss" are in the basic policy (the first layer), and others are in the standard (the second layer).

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

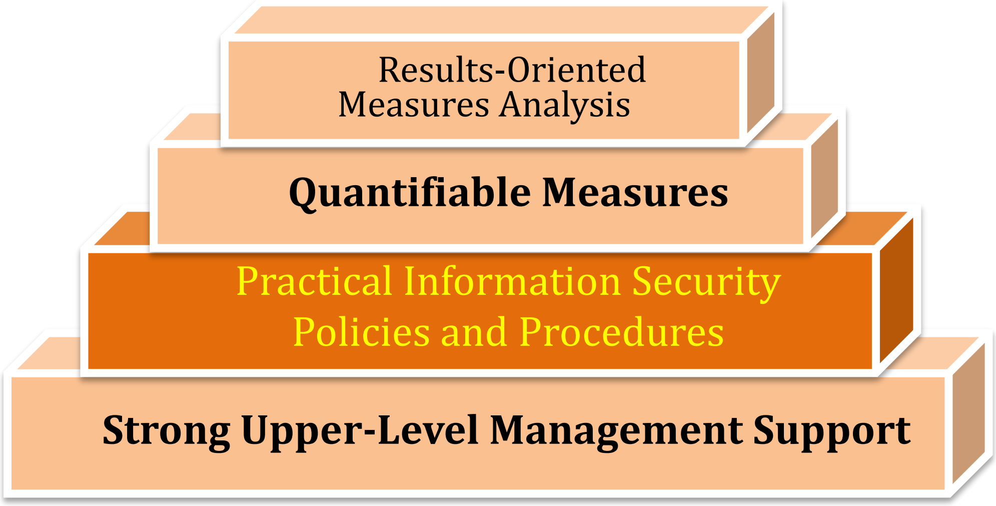

Describe high level objectives and policy statements defining why public and its framework required for your organization.
Policy
What should be protected and provides detail on what is required within specific area.
How to implement appropriate standards. Concrete process or technical procedures are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

NIST(National Institute of Standards and Technology) published the document "Measurement Guide for Information Security" consisting of two volumes. Volume 1 is on "Identifying and Selecting Measures"[5], and volume 2 is on "Developing an Information Security Measurement Program"[6]. In volume 2, the practical information security policies and procedures are positioned as the third layer of the Information security measurement program structure shown in Figure 2.

There is a statement on the information security policy as follows:

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v1.pdf (available: 2025/05/20)
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v2.pdf (available: 2025/05/20)

Figure 2. Information Security Measurement Program Structure in NIST. SP.800-55v2



> "Information security policies define the information security management structure, assign information security responsibilities, and reliably measure progress. The related procedures document management's position on implementing information security controls and the rigor with which they are applied.

The (basic) policy in the model of Figure 1 should include the statement about the top management support and responsibilities, and the risk analysis based on qualifiable measures and "Results-Oriented Measures Analysis" are necessary to establish the standard.

Ontologies and their Implementation

Here, we refer to the ontology itself and introduce some existing ontologies related to information security. Then describe our formerly proposed system for generating information security policy with ontologies.

Ontology and Some Ontologies

The term "ontology" is borrowed from philosophy and is defined as "a systematic explanation of existence". According to Thomas R. Gruber (Gruber 1993), "existence" in a knowledge-based system is exactly what can be expressed, and in that sense, "ontology is an explicit specification of conceptualization". From the perspective of the Semantic Web, Hendler (Hendler 2001) focused on the idea that ontologies provide a set of knowledge, and considered them to be a collection of basic concepts that include vocabulary and simple inference rules related to a specific task or domain.

Ontologies formalize concepts so that machines such as PCs can process knowledge and vocabulary that exists in the world, and enable access and processing via the Internet. In fact, many different types of ontologies have been created, and general-purpose ontologies are modified to be specialized for the intended domain and then republished to encourage reuse.

Dublin Core[7] is a metadata description for resources on the Web that was developed in Dublin, USA in 1995. It includes basic properties for describing bibliographic information such as titles, authors, dates, keywords, and languages for e-books and journals, as well as file formats.

FOAF (Friend Of A Friend)[8], as the name suggests, describes information about people and groups. It includes classes such as Person, Group, and Organization, and properties that represent their attributes, such as name, place of employment, projects they have participated in, and homepage. Based on the FOAF ontology, Edlira Kalemi and Edlira Martiri (Kalemi and Martiri 2011) have created an ontology, looking at people and communities in academic institutions and their characteristics[9].

Regarding IT asset ontology for information risk, A. Kayode Adesemowo et al. (Adesemovo et al. 2016) have proposed an ontology that divides information assets into "people", "networks", "services", "data", "hardware", "software", and "information". Almut Herzog and others from Linköping University in Sweden (Herzog et al. 2007) have proposed a "Cyber Security Ontology" that includes Assets, Threats, Vulnerabilities, Countermeasures, and Defense Strategies for achieving security goals such as confidentiality and integrity.

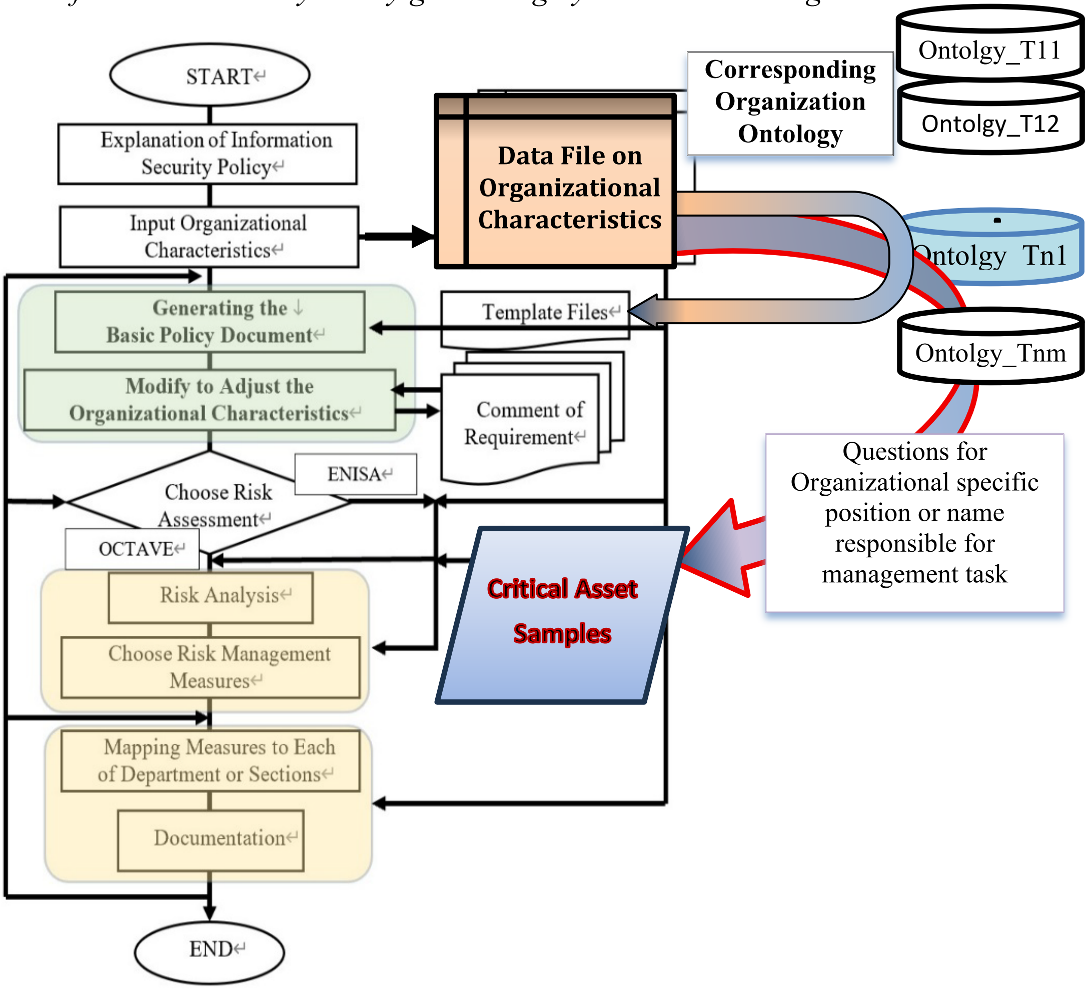
Protégé is an application software for creating original ontologies by combining, modifying, and adding to existing ontologies, and it is available for download as a free open-source program[10]. Natalya F. Noy and Deborah L. McGuinness (Noy and McGuinness 2001) have also compiled a guidebook on the basics of creating ontologies using Protégé.

For Implementation of Ontology

Figure 3 describes the modified total system for automatic generation of information security policies proposed in our previous papers (Nagata 2023, 2024). Parts that incorporate ontologies are both in the upper phase and lower phase, and here we consider especially the implementation of ontologies reflecting each of organizational type and characteristics into the critical assets sample extracting parts in the lower phase.

[7] https://www.dublincore.org/specifications/dublin-core/dcmi-terms/ (available:2025/05/20)
[8] http://xmlns.com/foaf/spec/ (available:2025/05/20)
[9] https://vocab.org/aiiso/ (available:2025/05/20)
[10] https://protege.stanford.edu/ (available:2025/05/20)

Figure 3. *Information Security Policy generating System with Ontologies*


START
Explanation of Information Security Policy
Input Organizational Characteristics
Data File on Organizational Characteristics
Corresponding Organization Ontology
Ontolgy_T11
Ontolgy_T12
Ontolgy Tn1
Ontolgy_Tnm
Template Files
Generating the Basic Policy Document
Modify to Adjust the Organizational Characteristics
Comment of Requirement
ENISA
Choose Risk Assessment
OCTAVE
Questions for Organizational specific position or name responsible for management task
Critical Asset Samples
Risk Analysis
Choose Risk Management Measures
Mapping Measures to Each of Department or Sections
Documentation
END

There have been several studies and implementations regarding the incorporation of ontologies into information security systems, and we will briefly touch on some of them here.

Stefan Fenz et al. proposed implementation of ontological mapping both of ISO/IEC 27001 and 27002 (Fenz et al. 2007, 2015). The paper states that information assets are modeled in ontology and then incorporated into applications in the process of considering controls based on ISO/IEC 27002.

Andrzej Uszok et al. developed KAoS, a policy and domain services framework based on W3C's OWL ontology language (Uszok et al. 2004). Although KAoS is not specified in information security policies, it is pioneering policy management framework incorporating with ontologies.

In order to establish ontology, Antonio De Nicola et al. proposed an ontology building methodology capitalizing the large experience drawn from a widely used standard in software engineering (Nicola et al. 2009). They name it the Unified Software Development Process or Unified Process for Ontology (UPON), in which the answer model for each competency question of requirement that the ontology should be able to answer is described in use-case mode and the analysis procedure proceeds according to the roles of Domain Expert (DE) and Knowledge Engineer (KE).

For an asset-based information system, Jehan Zeb et al. proposed to develop an ontology-supported information system (AIIS) (Zeb et al. 2015) where they described the methodology to develop ontologies such as "Tangible Capital Asset Ontology (TCA_Onto)" and "Transaction Domain Ontology (Trans_Dom_Onto)" in 10 steps. Here we refer only the first 4 steps involved in creating an ontology from the paper written by Jehan Zeb and Thomas Froese (Zeb and Froese 1016).

Step 1: The purpose, use, and users of the ontology were defined.
Step 2: A set of competency questions was developed so that the ontology should be able to answer.
Step 3: A preliminary taxonomy of various concepts was developed.
Step 4: Use was made of the existing ontologies and relevant concepts were captured.

Thus, the generation of a set of competency questions is very important for a system incorporating an ontology to operate effectively.

Preparation for Ontology-based Java Application Program

Our existing application program is written in Java language with a GUI implemented using the JavaFx library, and uses the Apache Jena library to reference and process ontologies appropriate for the organization type which is retrieved in the previous process. Show a list of information assets according to the type selected from the ontology of information risk created to answer each of competency questions. We need to create them corresponding to several organizational types and save them as files (top right in Figure 3). We must also prepare some files written in SPARQL, a query language for retrieving data from ontology.

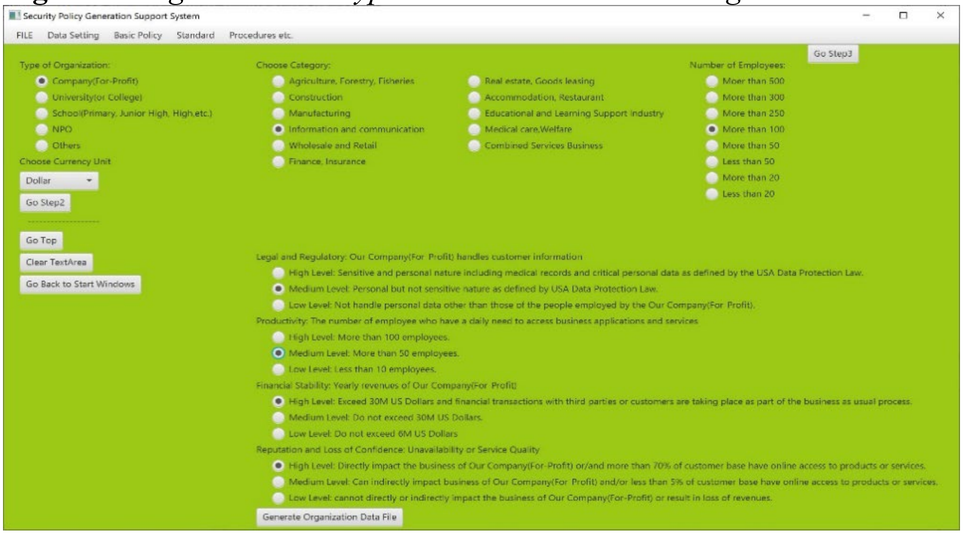
Describing Ontologies Proposed Ontology-based Query System

According to the flow in Figure 3, here we describe the proposed ontology-based query system in SPARQL reflecting the type and characteristics of an organization.

- ➢ The initial page is an explanation of "Policy", "Standard", and "Procedures etc.". When choosing one of them brief explanations come up.
- ➢ The type and the characteristic of organization is set when choosing the "Data Setting" in the menu bar, Figure 4.
  - ✓ In the top left, 4 types of organization are presented
  - ✓ In the top right, more precise types and size of organization are presented

- ✓ In the bottom right, the risk level according to 4 categories such as "Legal and Regulatory", "Productivity", "Financial Stability", and "Reputation and Loss of Confidence" are presented to select.

Figure 4. *Organizational Type and Characteristic setting*



Type of Organization:
● Company(For-Profit)
○ University(or College)
○ School(Primary, Junior High, High.etc.)
○ NPO
○ Others

Choose Currency Unit
Dollar

Choose Category:
○ Agriculture, Forestry, Fisheries
○ Construction
○ Manufacturing
● Information and communication
○ Wholesale and Retail
○ Finance, Insurance
○ Real estate, Goods leasing
○ Accommodation, Restaurant
○ Educational and Learning Support Industry
○ Medical care,Welfare
○ Combined Services Business

Number of Employees:
○ Moer than 500
○ More than 300
○ More than 250
● More than 100
○ More than 50
○ Less than 50
○ More than 20
○ Less than 20

Legal and Regulatory: Our Company(For Profit) handles customer information
○ High Level: Sensitive and personal nature including medical records and critical personal data as defined by the USA Data Protection Law.
● Medium Level: Personal but not sensitive nature as defined by USA Data Protection Law.
○ Low Level: Not handle personal data other than those of the people employed by the Our Company(For Profit).

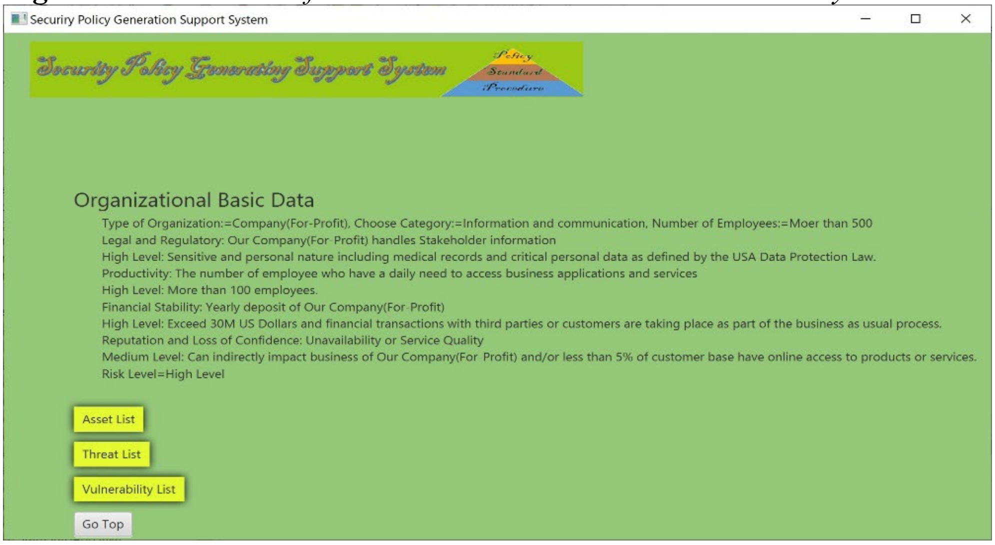
Productivity: The number of employee who have a daily need to access business applications and services
○ High Level: More than 100 employees.
● Medium Level: More than 50 employees.
○ Low Level: Less than 10 employees.

Financial Stability: Yearly revenues of Our Company(For Profit)
● High Level: Exceed 30M US Dollars and financial transactions with third parties or customers are taking place as part of the business as usual process.
○ Medium Level: Do not exceed 30M US Dollars.
○ Low Level: Do not exceed 6M US Dollars

Reputation and Loss of Confidence: Unavailability or Service Quality
● High Level: Directly impact the business of Our Company(For-Profit) or/and more than 70% of customer base have online access to products or services.
○ Medium Level: Can indirectly impact business of Our Company(For Profit) and/or less than 5% of customer base have online access to products or services.
○ Low Level: cannot directly or indirectly impact the business of Our Company(For-Profit) or result in loss of revenues.

- ➢ After confirmation, the organization type and characteristics are saved.
- ➢ According to the type and characteristic of organization, the system select the ontology file and chose list of "Asset" or "Threat" or "Vulnerability", Figure 5.

Figure 5. *Choose one of Asset List or Threat List or Vulnerability List*


Securiry Policy Generation Support System
Security Policy Generating Support System
Policy
Standard
Procedure
Asset List
Threat List
Vulnerability List
Go Top

Organizational Basic Data

Type of Organization:=Company(For-Profit), Choose Category:=Information and communication, Number of Employees:=Moer than 500
Legal and Regulatory: Our Company(For-Profit) handles Stakeholder information
High Level: Sensitive and personal nature including medical records and critical personal data as defined by the USA Data Protection Law.
Productivity: The number of employee who have a daily need to access business applications and services
High Level: More than 100 employees.
Financial Stability: Yearly deposit of Our Company(For-Profit)
High Level: Exceed 30M US Dollars and financial transactions with third parties or customers are taking place as part of the business as usual process.
Reputation and Loss of Confidence: Unavailability or Service Quality
Medium Level: Can indirectly impact business of Our Company(For Profit) and/or less than 5% of customer base have online access to products or services.
Risk Level=High Level

- ➢ Choose assets (or threats or vulnerabilities) from the presented list. Figure 6 represents the result of test query by SPARQL using the "Cyber Security Ontology" by Herzog et al.
- ➢ Represent property of selected assets (or threats or vulnerabilities), Figure 7, by consulting the ontology. Thus users understand the risk on

each of information assets and the relationship between asset and threat, or assets and vulnerabilities.

In the “Cyber Security Ontology” written in Turtle format, there are many classes concerning the information security issues such as “AccessControl”, “CPU”, “Internet”, “Cookies”, etc., and some of them have “rdfs:subClassOf” or “owl:onProperty” or “owl:someValuesFrom” properties.

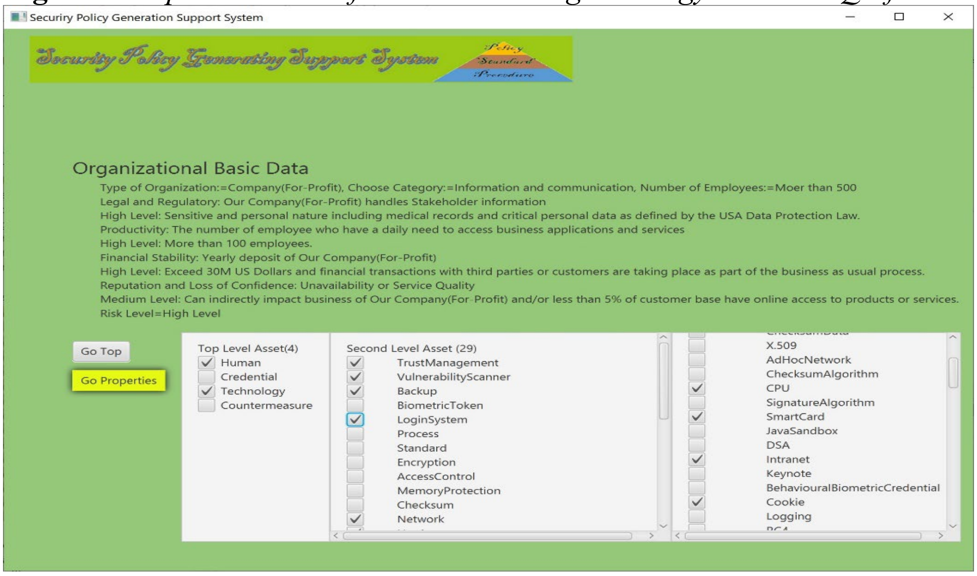
As an asset list, we put them into four categories such as “Human”, “Credential”, “Technology”, and “Countermeasure” as a top-level assets, and divide then in the second level and the third level. Each of asset may hava several properties and describtions.

For example, the “Backup” class is a subclass of (“rdfs:subClassOf”) “Countermeasure”, on property (“owl:onProperty”) of protects(“:protects”) some values from (“owl:someValuesFrom”) availability(“:_Availability”), data (“:_Data”), integraity (“:_Integrity”), and recovery(“:_Recovery”).

In order to see the class hierarchy and to extract the description and properties of a class, we need a small file of RDF in SPARQL such as the following:

```
SELECT DISTINCT ?yp ?yv
WHERE {
        :XXXX rdfs:subClassOf ?y.
        optional{ :XXXX dc:description ?desc}
        optional{ ?y owl:onProperty ?yp}
        optional{ ?y owl:someValuesFrom ?yv}
}
```

Figure 6. *Representation of Assets List using Ontology via SPARQL file*



Securiry Policy Generation Support System

Organizational Basic Data

Type of Organization:=Company(For-Profit), Choose Category:=Information and communication, Number of Employees:=Moer than 500
Legal and Regulatory: Our Company(For-Profit) handles Stakeholder information
High Level: Sensitive and personal nature including medical records and critical personal data as defined by the USA Data Protection Law.
Productivity: The number of employee who have a daily need to access business applications and services
High Level: More than 100 employees.
Financial Stability: Yearly deposit of Our Company(For-Profit)
High Level: Exceed 30M US Dollars and financial transactions with third parties or customers are taking place as part of the business as usual process.
Reputation and Loss of Confidence: Unavailability or Service Quality
Medium Level: Can indirectly impact business of Our Company(For-Profit) and/or less than 5% of customer base have online access to products or services.
Risk Level=High Level

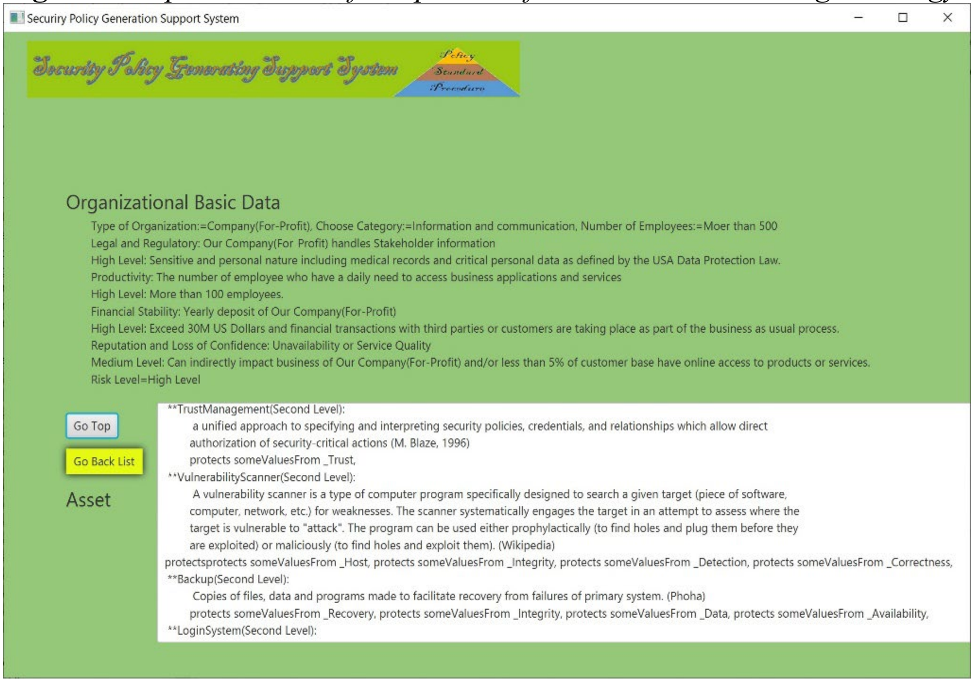
Top Level Asset(4)
☑ Human
☐ Credential
☑ Technology
☐ Countermeasure

Second Level Asset (29)
☑ TrustManagement
☑ VulnerabilityScanner
☑ Backup
☐ BiometricToken
☑ LoginSystem
☐ Process
☐ Standard
☐ Encryption
☐ AccessControl
☐ MemoryProtection
☐ Checksum
☑ Network

☐ X.509
☐ AdHocNetwork
☐ ChecksumAlgorithm
☑ CPU
☐ SignatureAlgorithm
☑ SmartCard
☐ JavaSandbox
☐ DSA
☑ Intranet
☐ Keynote
☐ BehaviouralBiometricCredential
☑ Cookie
☐ Logging

Figure 7 represents the result by applying SPARQL file for the chosen assets checked in the third level box. Descriptions on each of assets are represented in the text area from the turtle file of the "Cyber Security Ontology", and they can be helpful when considering security issues on the assets.

Figure 7. *Representation of Properties of each Assets also using Ontology*


Securiry Policy Generation Support System
Security Policy Generating Support System
Policy
Standard
Procedure
Go Top
Go Back List
Asset

Organizational Basic Data

Type of Organization:=Company(For-Profit), Choose Category:=Information and communication, Number of Employees:=Moer than 500
Legal and Regulatory: Our Company(For Profit) handles Stakeholder information
High Level: Sensitive and personal nature including medical records and critical personal data as defined by the USA Data Protection Law.
Productivity: The number of employee who have a daily need to access business applications and services
High Level: More than 100 employees.
Financial Stability: Yearly deposit of Our Company(For-Profit)
High Level: Exceed 30M US Dollars and financial transactions with third parties or customers are taking place as part of the business as usual process.
Reputation and Loss of Confidence: Unavailability or Service Quality
Medium Level: Can indirectly impact business of Our Company(For-Profit) and/or less than 5% of customer base have online access to products or services.
Risk Level=High Level

```
 **TrustManagement(Second Level):
      a unified approach to specifying and interpreting security policies, credentials, and relationships which allow direct
     authorization of security-critical actions (M. Blaze, 1996)
     protects someValuesFrom _Trust,
 **VulnerabilityScanner(Second Level):
      A vulnerability scanner is a type of computer program specifically designed to search a given target (piece of software,
     computer, network, etc.) for weaknesses. The scanner systematically engages the target in an attempt to assess where the
     target is vulnerable to "attack". The program can be used either prophylactically (to find holes and plug them before they
     are exploited) or maliciously (to find holes and exploit them). (Wikipedia)
protectsprotects someValuesFrom _Host, protects someValuesFrom _Integrity, protects someValuesFrom _Detection, protects someValuesFrom _Correctness,
 **Backup(Second Level):
      Copies of files, data and programs made to facilitate recovery from failures of primary system. (Phoha)
     protects someValuesFrom _Recovery, protects someValuesFrom _Integrity, protects someValuesFrom _Data, protects someValuesFrom _Availability,
 **LoginSystem(Second Level):
```

Discussion, Conclusion, and Future Works

This paper describes Japan's position in international competitiveness through information technology from IMD report 2024, and we noticed that information (or cyber) security is a critical factor not only in the IT integration but also in the business agility as Future readiness. Then we argue that the establishment of an information security policy is important in order to improve the state of information security which is one of the factors behind this competitiveness.

Although establishing proper information security is effective from the future readiness perspective, it is sometimes costly, and it also tends to be rigid system. Thus, we try to create an information security policy generating application program which helps and lead organizations to establish a proper and agile to current and future conditions.

An application program to support the creation of information security policies is currently under development, but here we propose to provide effective support system by using ontologies for organizational types and characteristics as part of the program and have created a program that implements the parts related to information assets in particular.

By creating actual programs and search files using SPARQL, we were able to determine what kind of ontologies would be needed, but the creation of individual ontologies remains as a future task.

References

Adesemowo, A. K., Solms, R., and Botha, R. A. 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*(London, UK, January 18-20, 2017), 173–187. DOI: 10.1007/978-3-319-51064-4_15.

Hendler, J. 2001. Agents and the Semantic Web, *IEEE Intelligent System*, 16(2), 30-37.

Herzog, A., Shahmehri, N., and Duma, C. 2007. An Ontology of Information Security, In *International Journal of Information Security and Privacy*, 1, 4, IGI Global, 1-23.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., and 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* (Melbourne, Australia, December 17-19, 2007), 381-388, DOI 10.1109/PRDC.2007.66.

Fenz, S., Plieschnegger, S., and Hobel, H. 2015. Mapping Information Security Standard ISO/IEC 27002 to an Ontology Structure, In *Information & Computer Security*, 24, 5, Emerald Publishing, 452-473, DOI 10.1108/ICS-07-2015-0030.

Gruber, T. R. 1993. A Translation Approach to Portable Ontology Specifications, In *Knowledge Acquisition*, Vol. 5, (2), 199-220, DOI: 10.1006/knac.1993.1008

Kalem, E. and Martiri, E. 2011. FOAF-Academic Ontology: A Vocabulary for the Academic Community, In *Proceedings of Third International Conference on Intelligent Networking and Collaborative Systems* (Fukuoka, Japan, 2011), 440-445, DOI: 10.1109/ INCoS.2011. 94.

Nagata, K., 2024, Establishing Information Security Policy as an Organizational Risk Management, The Future of Risk Management, Chapter 2. IntechOpen Series, Industrial Engineering and Management, Vol. 9, 17-37, ISBN: 978-0-85466-752-9, DOI: 10.5772/ intechopen.1001758

Nagata, K., 2023, Automatic Generating System of Information Security Policy. *Athens Journal of Technology and Engineering*, Vol. 10, Issue 4, 227-236, DOI: 10.30958/ ajte.10-4-3.

Nicola, A. D., Missikoff, M., and Navigli, R. 2009. A Software Engineering Approach to Ontology Building, In *Information Systems*, 34, 258-275, DOI: 10.1016/j.is.2008. 07.002

Noy, N. F. and McGuiness D. L. 2001. *Ontology Development 101: A Guide to Creating Your First Ontology*, Stanford Knowledge Systems Laboratory Technical Report KSL-01-05.

Uszok, A., Bradshaw, J.M., and Jeffers, R. 2004. KAoS: A Policy and Domain Services Framework for Grid Computing and Semantic Web Services. In *Trust Management. iTrust 2004*. Lecture Notes in Computer Science, 2995. Springer, Berlin, Heidelberg. 16–26. DOI: 10.1007/978-3-540-24747-0_2.

Zeb, J., Froese, T. and Vanier D. 2015. An Ontology-supported Asset Information Integrator System in Infrastructure Management, In *Built Environment Project and Asset Management*, Vol. 5, No. 4, 380-397, DOI: 10.1108/BEPAM-02-2014-0012.

Zeb, J. and Froese, T. 2016. An Ontology-Support Infrastructure Transaction Management Portal In Infrastructure Management, *Journal of Information Technology in Construction*, Vol. 21, 100-118, ISSN 1874-4753.