On Designing a Cybersecurity Educational Program for Higher Education

Eunyoung Kim
School of Knowledge Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi, Ishikawa, Japan
+81-761-51-1740
kim@jaist.ac.jp

Razvan Beuran
School of Information Science
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi, Ishikawa, Japan
+81-761-51-1241

ABSTRACT
Cybersecurity education is critical for preparing current and future IT professionals to deal with the multitude of security threats that occur worldwide on an ever-increasing scale. We believe that this issue can be addressed most effectively at the level of higher education, which provides the best balance of existing skills and available resources as needed for such highly-technical topics.

In this paper we present first of all a methodology for designing a cybersecurity educational program, so that it becomes easier for all interested parties to design such programs, which helps extending the global scale of cybersecurity education. Secondly, we describe in detail how we applied our methodology to design an appropriate cybersecurity program for the case of higher education in Japan, followed by a discussion of the current state of our endeavor.

CCS Concepts
• **Social and professional topics → Professional topics → Computing education→Model curricula**

Keywords
Cybersecurity Education; Curriculum Design; Pedagogical Methods; Educational Content

1. INTRODUCTION
Given the scale of cybersecurity threats in the present world, and their growing tendencies, it is obvious that the readiness of current and future IT professionals needs to be considerably improved. As cybersecurity is often associated with the defense industry, most of the cybersecurity education programs have been led so far by the governmental units of individual countries or agencies with defense-related contracts [1]. However, given the need to extend the scale of cybersecurity education, we assert that it needs to be considered as an interdisciplinary field of study based on information security, and that the various advances in education theory should be applied to this area as well in order to improve the effectiveness of education process.

As the first step in this endeavor, we have created a methodology for designing cybersecurity educational programs. Our method takes into account all the related aspects, including an educational framework built along relevant dimensions (institution, users and externals), as well as suitable pedagogical models. Such a custom design approach is necessary in order to make sure that the resulting educational program matches well with the profile of the institution, the needs of the students, and the requirements from the industry.

Our methodology can be applied to any interested institutions, thus, it could help the cybersecurity educational program designers in the global scale. We have applied it to the case of higher education in Japan, as we consider that higher education is the most appropriate setting for cybersecurity education and training programs, given that students have the right amount of technical skills and available resources for dealing with the associated education and training content.

As ongoing work, the cybersecurity educational program that we designed will be integrated with the training system CyTrONE that we have already developed at the Cyber Range Organization and Design (CROND) NEC-endowed chair at Japan Advanced Institute of Science and Technology (JAIST) [2]. CyTrONE has many features to support and facilitate cybersecurity training, hence it will constitute an ideal platform on which the educational content will be deployed, as well as for conducting the associated hands-on training activities.

The main contributions of our paper are:

- Propose a methodology for designing a cybersecurity educational program that takes into account the needs and requirements of all the concerned parties, and utilizes appropriate pedagogical models to ensure maximum education effectiveness;
- Present the manner in which we applied the methodology to the case of higher education in Japan, including details on the decisions we have made at each step and their rationale.

The remainder of this paper is organized as follows. In Section 2 we review the works related to our research. In Section 3, we present our proposed methodology for cybersecurity educational program design. This is followed by a detailed description of the way in which we applied this method for the case of higher education in Japan (Section 4), and the current status of our endeavor. Finally, this paper ends with conclusions, acknowledgments, and references.

2. RELATED WORKS
As major parts of our daily life are exposed to cyber networks, there is an increasing need for establishing the cybersecurity education programs in higher education. Numerous researchers and educators have made a tremendous effort to build educational programs for fostering cybersecurity professionals in the fields of

ICETC 2018, October 26–28, 2018, Tokyo, Japan

ACM ISBN 978-1-4503-6517-8/18/10…$15.00
https://doi.org/10.1145/3290511.3290524

defense, criminology, policy, computer science and engineering, and so on [3, 4]. As a result, a number of educational programs have been designed and implemented in the higher education level. NIST developed the Cybersecurity Framework, which provides a guideline for building a program for cybersecurity from the industry perspective [5]. Many organizations support educational activities by sharing the cybersecurity resources in the form of virtual labs [6], communities of practice (CoPs) [7] and competitions [8].

Integrated curriculum strategies in cybersecurity education have been proposed as a holistic approach based on integrative learning theory [9]. In this approach, four dimensions—curriculum development, experiential learning method, assessment, and building a community of practice—were defined as key elements of the holistic cybersecurity educational model.

Henry [10] designed a cyberspace education framework that aims to meet the national demand in Australia for reinforcing the maturity of cybersecurity education. There are five dimensions in his framework: education type, level of expertise, the field of education, purpose, application. In addition, he proposed a curriculum created based on his framework.

Apart from the frameworks that help in setting the goals and designing the curriculum of cybersecurity educational programs, specific pedagogical models and methods must be considered. Pedagogical models are often associated with learning styles, and there are numerous studies defining the types of learning and the adequate teaching methods [11, 12]. In cybersecurity education, the Kuzmina-Bespalko-Popovsky (KBP) pedagogical model [13] was proposed through the blending of Russian and American pedagogical approaches. KBP was already applied to a number of cybersecurity educational programs as both conceptual and operational pedagogical model in developing a specific course that aligns with the purpose of the curriculum. Also, Yuan et al. [14] proposed the Process Oriented Guided Inquiry Learning (POGIL) model to enhance both the technical skills and the soft ones, such as communication, attitude, team work. On the other hand, as information technology, including IoT, evolves quickly and it spreads rapidly into our daily life, we need a new cybersecurity education approach to cope with the new threats [15].

3. METHODOLOGY FOR DESIGNING AN EDUCATIONAL PROGRAM

Educational program design is a complex process in general, and one of our goals is to simplify this process, so that it becomes easier to design such programs. This will help expand the scope of cybersecurity education so as to meet the needs of educational institutes, students, as well as the industry and global society.

Our methodology for designing the cybersecurity educational programs is consist of establishing an education framework, selecting appropriate pedagogical methods, and developing educational content accordingly. The methodology can be explained as a sequence of steps that guarantee the creation of an effective educational program. The six steps of our methodology are (see also Figure 1):

1) Review the existing programs in the field, so as to determine their strengths and weaknesses;
2) Define the educational framework, in order to decide the dimensions that the educational process should address (i.e., decide *which perspectives* should be considered for education);
3) Design the outline of the curriculum by integrating the information and decisions made in the previous two steps;
4) Select the appropriate pedagogical methods that match the educational framework and curriculum (i.e., decide *how* the content should be taught);
5) Develop education content in accordance with the above curriculum and pedagogical methods;
6) Test the education content in realistic class settings, and revise the curriculum, pedagogical methods and content as needed.

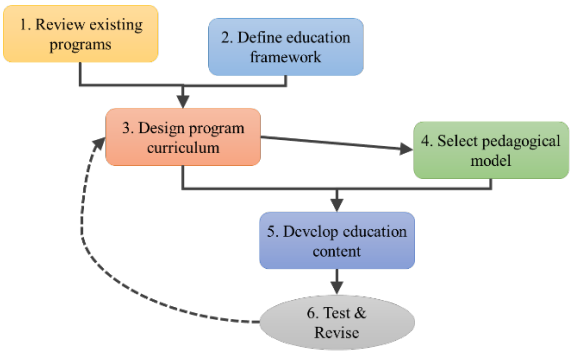

Figure 1. Educational program design methodology.

Our focus is on cybersecurity education and training, therefore in the remainder of this section will illustrate how our methodology can be applied to this field. However, cybersecurity can be considered simply as a case, since we believe that our methodology is general enough to be applied to other areas too.

3.1 Reviewing Existing Programs

The first step of our methodology is to review the current education programs, with the main goal of determining what are their strengths and weaknesses. We recommend that this review is done as widely as possible within the limits of the available time, covering also related areas which are not higher education per se, such as technical training and so on.

3.2 Defining the Education Framework

Based on our review of current frameworks, approaches and strategies for designing the curriculum of cybersecurity education program, we concluded that there is a lack of viewpoints from participants (users), such as learners (direct users) and stakeholders (indirect users), and external elements, such as rapidly changing advanced technologies (e.g. IoT, AI, etc.) and the public policy. We suggest an extended framework for developing the curriculum, which includes following three dimensions:

1) *Institutional dimension*: Includes the education type, level of expertise, the purpose of the program, field of education [10], decided based on the nature of the institution that provides the cybersecurity education program; according to the institutional dimension, the range of academic subjects can be determined.
2) *Users dimension*: Contains two sub-dimensions, learners and stakeholders, and takes into account the often-neglected modern demands and characteristics of the beneficiaries, such as the case of new generations who grew up with massive use of information technology, or for innovative

companies who require prompt solutions to their cybersecurity issues.

3) *External dimension*: Accounts for the latest technological changes that have shaped game-changing shifts in our society; a state-of-the-art educational program must enable students to cope with upcoming innovations in information technology.

3.3 Designing the Program Curriculum

The framework defined in the previous section enables us to apply a multi-dimensional approach in designing the curriculum for cybersecurity education and training. In practical terms, we suggest to make the decision of the specific subjects and topics of the curriculum based on a survey of faculty, industry, and students.

In our framework, the institutional viewpoint emphasizes fundamental learning aspects, such as theories and critical thinking, the users' viewpoint reiterates the applications and management of the skills learned, which accounts for the training part, and the external dimension might enhance the motivation to learn. A sample curriculum design matrix is shown in Table 1.

Table 1. A sample outline of the curriculum design

<table>
<tr><td></td><td>Institutional dimension</td><td>Users dimension</td><td>External dimension</td></tr>
<tr><td rowspan="2">Semester 1</td><td>Introduction to OOO</td><td>Application of OOO</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Development of OOO, Management of OOO</td></tr>
<tr><td rowspan="2">Semester 2</td><td rowspan="2">Theories in OOO</td><td>Techniques and tools in OOO</td><td></td></tr>
<tr><td colspan="2">Invited lecture series</td></tr>
<tr><td>Semester 3</td><td colspan="2">Research project</td><td>Special topics in OOO</td></tr>
<tr><td>Semester 4</td><td>Master thesis</td><td colspan="2">Internship</td></tr>
</table>

3.4 Selecting the Pedagogical Model

The framework can guide us to make decisions on the scope of the educational program, however, it does not show how to operate it, e.g. by considering the dynamics of the institution, faculty, students, related industries, trends in information technology, job market, and public policies. Several pedagogical models and methods have been suggested for handling the questions on how to educate the students. In cybersecurity education, various types of learning methods have been implemented and reviewed including role-based [5], scenario-based [16], competency-based [17], game-based [18], challenge-based [8], experiential, problem-based and inquiry-based [19]. It is hard to say that one specific learning or teaching style is more effective than the others, hence we recommend to apply multiple methods in accordance with the conditions of the instructors and classroom.

After deciding the curriculum topics and courses, one should develop an evaluation method to assess the learning level in connection with the purpose of the educational program. One of the most widely used model is Bloom's taxonomy [20], which determines the level of learning from knowledge, comprehension, application, analysis, synthesis, and evaluation. This taxonomy has been revised many times by other researchers [21, 22], and can be redefined if needed according to the goal of the educational program.

Besides formal learning, the institution should also provide the environments for informal learning. In Japan, the concept of "ba" was introduced as a space for sharing and creating organizational knowledge, encouraging informal learning [23].

3.5 Developing the Educational Content

After defining the educational framework, curriculum design, and selection of pedagogical models and methods, we must integrate these steps to develop the educational content. At this stage, we recommend the educators to organize a seminar to understand the educational framework and its dimensions, and the suitable pedagogical methods, then facilitate a workshop to generate the educational content collectively in accordance with the structure of the curriculum. Finally, the generated content should be managed as the resource of education, and reorganized and from an instructional point of view.

3.6 Testing and Revising

Testing the effectiveness of the resulting educational program can be conducted in various forms. Many education-related resources describe assessment methods and the results from the collected data. However, at this stage, we consider that it is most important to follow a trial-and-error procedure in order to enhance both the teaching and learning environments.

Educational program development is a continuous process by its nature, and educators should play both roles of course/educational program designer and practical instructor. The dyadic interaction of those two roles enables them to improve the quality of learning.

4. APPLYING THE METHODOLOGY TO CYBERSECURITY EDUCATION IN JAPAN

In this section, we illustrate the manner in which we have applied the proposed methodology to design a cybersecurity educational program for the case of Japanese higher education. The following subsections provide details for each of the six steps of the methodology.

4.1 Japanese Program Review

For the purpose of our research, we have identified the following categories of related programs: academic programs, training programs, and competitions.

As a representative academic program, we mention enPiT-security (also known as SecCap) started in April 2013 by a consortium of five Japanese universities, and now available both for graduate and undergraduate students [24]. The goal of SecCap is to develop the basic skills needed by IT security engineers through courses and hands-on activities regarding security-related aspects of operating systems, software, networks, as well as malware-related countermeasures and technologies.

Another relevant resource is the course "Computer Network Security" which is being taught at Osaka University. This program is being conducted with reference to a book published by the professors who give the course, which thus represents a rich source of information regarding it [25]. This course provides a comprehensive view of the current network security issues, and also includes elements of practical training.

Regarding training programs and competitions, we have already published a detailed report that emphasizes their characteristics [26]. Training programs can be either paid and technical, such as Secure Eggs by NRI SecureTechnologies [27], or free and less-technical, such as the CYDER program conducted by the National Cyber Training Center [28].

Competitions are mainly aimed at motivating and attracting young people towards cybersecurity professions and are typically free. However, they vary considerably in their scope and approach, some contests being very technical, such as SECCON, which is being conducted in Capture The Flag (CTF) style [29]. Other competitions have a greater focus, such as the Hardening Project, which uses the realistic scenario of managing a virtual e-commerce company as background [30].

4.2 Education Framework Definition

Following the discussion in Section 3.2, we propose the following education framework for cybersecurity higher education:

1) *Institutional dimensions*: (i) Level of expertise: Basic to intermediate; (ii) Purpose: Generalist; (ii) Fields of educations: Technical and managerial.
2) *Users dimensions*: (i) Learners: Generation Z and millennial (digital natives); (ii) Industry requirements: Based on the skill map developed by the Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development (CRIC-CSF) established by the Japan Business Federation [31].
3) *External dimensions*: (i) Advances in technology: IoT, AI, etc.; (ii) Social system: Changes in policy, social trends, etc.

4.3 Program Curriculum Design

By taking into account the characteristics of the proposed education framework we have created an example outline of the curriculum for Mater program as outlined in Table 2. The details of each course will be decided and further refined by taking into account the details of dimensions of the framework, e.g. the CRIC-CSF skill map of the users dimension.

Table 2. A sample outline of the proposed curriculum

<table>
<tr><th></th><th>Institutional dimension</th><th>Users dimension</th><th>External dimension</th></tr>
<tr><td rowspan="2">Semester 1</td><td>Introduction to information security</td><td>Cybersecurity management</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Cryptography</td></tr>
<tr><td rowspan="3">Semester 2</td><td>Cyber network architectures</td><td rowspan="2">Business intelligence programming</td><td rowspan="2"></td></tr>
<tr><td>Theories in software engineering</td></tr>
<tr><td colspan="2">Invited lecture series</td></tr>
<tr><td rowspan="2">Semester 3</td><td colspan="2">Cyber network protections and tools</td><td rowspan="2">Special topics in cybersecurity</td></tr>
<tr><td colspan="2">Research project</td></tr>
<tr><td rowspan="2">Semester 4</td><td rowspan="2">Master thesis</td><td>Internship</td><td></td></tr>
<tr><td colspan="2">Competitions</td></tr>
</table>

4.4 Selecting the Pedagogical Methods

As mentioned in Section 3.4, one pedagogical model cannot suit all goals. Consequently, we propose to use a collection of pedagogical methods depending on the dimensions of the educational framework. Figure 2 illustrates how the correspondence between each dimension and selected pedagogical models. The instruction method will vary accordingly, for instance by using competitions in response to the "digital native" characteristics of the learners.

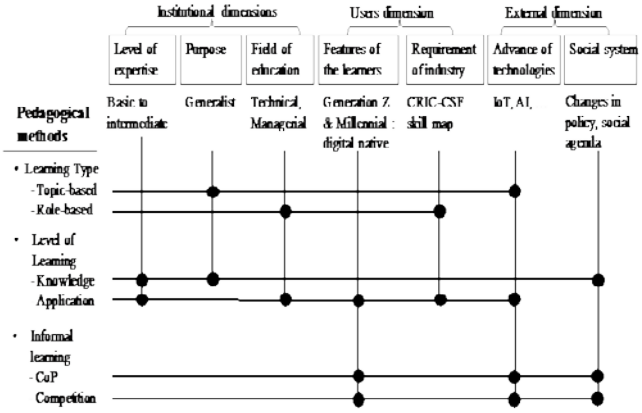

Figure 2. Example of how to integrate the education framework and pedagogical methods

4.5 Educational Content Development

Once the program curriculum and the pedagogical model are decided and integrated as described so far, the next step is to develop the educational content. This is the most time-consuming part of the design process, and it is an ongoing activity for us. Our approach is to take a top-down technique, starting from the curriculum, then going lower to courses and lessons until it becomes possible to discuss individual key concepts, as well as questions that verify whether students master them or not.

4.6 Test and Revise

The goal of our endeavor is not to develop a cybersecurity educational program for our university, JAIST, but to create a program that can be applied, under some assumptions, by any interested institutions. Therefore, we plan to make all the resources associated with the educational program publicly available, including any associated training content. Consequently, the test and revise step in our methodology will be composed of two stages:

- *Stage 1*: Given that our university has numerous students involved in research related to security and networks, the prototype of educational content will be tested via an optional course for the students interested in improving their knowledge and skills related to cybersecurity. Their feedback will be then used to revise the program content (and even the curriculum and/or pedagogical model if needed).
- *Stage 2*: Next, we shall make the educational program and its resources in public, and the feedback from any institution that uses the program will be utilized to further improve it iteratively. We have already received expressions of interest from several of the technical colleges in Japan that are united under the governing body of the National Institute of Technology, which includes 55 national public colleges all over Japan.

5. CONCLUSION

In this paper we have presented a methodology for designing a cybersecurity education program that comprises the following steps: (i) review of existing programs; (ii) defining the education framework; (iii) design of the program curriculum; (iv) selection of appropriate pedagogical methods; (v) development of educational content in accordance with the curriculum and pedagogical methods; (vi) test & revision of the educational content. For each step we detailed the issues that one is expected

to encounter and provided the advice for making the necessary decisions.

As a conceptual paper, this study has limitations as it lacks empirical data to support the proposed methodology. However, the above method was applied to the case of Japanese higher education, especially for the master program, for which we have conducted an in-depth review of existing education and training programs and defined a suitable education framework. We have also designed an outline of curriculum for the program that takes into account these aspects and selected several suitable pedagogical methods based on the dimensions of the framework.

In a future study, we will assess the education framework through collecting data from existing education and training programs. We are now in the process of developing the educational content in accordance with these elements. Once the education content will be finalized, we shall proceed with internal testing at our university, JAIST, followed by a public release of all the related resources.

Although in this paper we did not demonstrate the effectiveness of the proposed educational program and its content for the learners, we have shown the process of designing the educational program and its content. Therefore, other educators can follow this process and give constructive feedback to each other for enhancing the teaching as well as learning experiences.

6. ACKNOWLEDGMENTS

This work was partially supported by JSPS KAKENHI Grant Number 17K00478.

7. REFERENCES

[1] Kessler, G. C. and Ramsay, J. Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, 2 (2013), 35.

[2] Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y. and Shinoda, Y. CyTrONE: An Integrated Cybersecurity Training Framework. In *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP 2017)* (Porto, Portugal, February 19-21, 2017).

[3] Martini, B. and Choo, K. R. Building the next generation of cybersecurity professionals (2014).

[4] McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K. and Impagliazzo, J. Toward curricular guidelines for cybersecurity. In *Proceedings of the Proceedings of the 45th ACM technical symposium on Computer science education* (Atlanta, Georgia, USA, 2014). ACM.

[5] Toth, P. and Klein, P. A Role-Based Model for Federal Information Technology/Cyber Security Training. *NIST Special Publication*, 800 (2013), 16.

[6] Locasto, M. E., Ghosh, A. K., Jajodia, S. and Stavrou, A. The ephemeral legion: producing an expert cyber-security work force from thin air. *Communications of the ACM*, 54, 1 (2011), 129-131.

[7] Nobles, C. and Burrell, D. *Using Cybersecurity Communities of Practice (CoP) to Support Small and Medium Businesses*. Academic Conferences and publishing limited, 2018.

[8] Cheung, R. S., Cohen, J. P., Lo, H. Z. and Elia, F. *Challenge based learning in cybersecurity education*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2011.

[9] Abraham, S. and Shih, L. Instructional Perspective: Towards an Integrative Learning Approach in Cybersecurity Education (2015).

[10] Henry, A. P. Mastering the Cyber Security Skills Crisis: Realigning Educational Outcomes to Industry Requirements. *ACCS DISCUSSION PAPER*, 4 (2017).

[11] Kolb, A. Y. and Kolb, D. A. Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education. *Academy of Management Learning & Education*, 4, 2 (2005), 193-212.

[12] Franzoni, A. L., Assar, S., Defude, B. and Rojas, J. *Student Learning Styles Adaptation Method Based on Teaching Strategies and Electronic Media*. 2008.

[13] Endicott-Popovsky, B. E. and Popovsky, V. M. Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. *ACM Inroads*, 5, 1 (2014), 57-68.

[14] Yuan, X., Yang, L., He, W., Ellis, J. T., Xu, J. and Waters, C. K. Enhancing Cybersecurity Education Using POGIL. In *Proceedings of the Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (2017). ACM.

[15] William Butler, W. V. M., Helen G. Barker *The Evolving Internet of Things (IoT) Requires New Approaches by Colleges and Universities in Educating All Students in Cyber Security*. IEEE Standards University E-Magazine, 2016.

[16] Carlton, M. *Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills*. Nova Southeastern University, 2016.

[17] Sabeil, E., Manaf, A. B. A., Ismail, Z. and Abas, M. Cyber forensics competency-based framework-review. *International Journal of New Computer Architectures and their Applications (IJNCAA)*, 1, 4 (2011), 991-1000.

[18] Giannakas, F., Kambourakis, G. and Gritzalis, S. *Cyberaware: A mobile game-based app for cybersecurity education and awareness*. IEEE, 2015.

[19] Weiss, R., Turbak, F., Mache, J., Nilsen, E. and Locasto, M. E. *Finding the Balance Between Guidance and Independence in Cybersecurity Exercises*. USENIX, 2016.

[20] Bloom, B. S. and Krathwohl, D. R. *Taxonomy of Educational Objectives: Volume 2 Affective Domain*. David McKay Company Incorporated, 1971.

[21] Anderson, L. W., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. E., Pintrich, P. R., Raths, J. and Wittrock, M. C. A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives, abridged edition. *White Plains, NY: Longman* (2001).

[22] Fink, L. D. *Creating significant learning experiences: An integrated approach to designing college courses*. John Wiley & Sons, 2013.

[23] Nonaka, I. and Konno, N. The concept of "ba": Building a foundation for knowledge creation. *California management review*, 40, 3 (1998), 40-54.

[24] *enPiT University Consortium, enPiT-Security (SecCap) Program (in Japanese)*. https://www.seccap.jp/.

[25] Yagi, T., Akiyama, M. and Murayama, J. *Computer Network Security*. Corona Publishing, 2015.

[26] Beuran, R., Chinen, K., Tan, Y. and Shinoda, Y. *Towards Effective Cybersecurity Education and Training*. IS-RR-2016-003, Japan Advanced Institute of Science and Technology (JAIST), Ishikawa, Japan, 2016.

[27] Nomura Research Institute Secure Technologies *Secure Eggs Training Program(in Japanese)*. http://www.nri-secure.co.jp/service/learning/secureeggs.html.

[28] NICT National Cyber Training Center *Cyber Defense Exercise with Recurrence (CYDER) Training Program (in Japanese)*. https://cyder.nict.go.jp/.

[29] Japan Network Security Association *Security Contest SECCON (in Japanese)*. http://seccon.jp/.

[30] Web Application Security Forum *Hardening Project (in Japanese)*. http://wasforum.jp/hardening-project/.

[31] Industry Cross-Sectoral Committee for Cybersecurity Human Resources Development (CRIC-CSF) *Final Report of Stage 1*. http://cyber-risk.or.jp/sansanren/index.html.