# Cyber Security Education Practice in Credit Transfer System among National Institutes of Technology

K. Yonemura*,[a], T. Kaeriyama[b], Y. Wakaba[c], M. Maruyama[a], T. Okamoto[c] and M. Yamazaki [d]

[a] National Institute of Technology, Kisarazu College, Information and Computer Engineering, Kisarazu, Japan
[b] National Institute of Technology, Kisarazu College, Mechanical Engineering, Kisarazu, Japan
[c] National Institute of Technology, Kisarazu College, Electrical and Electronic Engineering, Kisarazu, Japan
[d] National Institute of Technology, Kisarazu College, Kisarazu, Japan

*yonemura@j.kisarazu.ac.jp

## Abstract

**Cybersecurity education in engineering education is becoming increasingly important, and the cybersecurity human resource development project that began at KOSEN in 2015 has entered its mature phase. The author has been responsible for the practical technical aspects of this project and has developed many cyber security educational materials. Lectures using the developed educational materials have been practiced and educational effectiveness has been measured. The relationship between educational effectiveness and motivation has also been examined, and the latest research results show that a high educational effectiveness can be expected if the motivation score of the students in the course is 4 or higher (on a scale of 1 to 5 points). In 2022, KOSEN started a credit transfer system among national institutes of technology, and National Institute of Technology, Kisarazu College, which is the base college of this project, offered "Information Security Exercise," which is the author's subject and enables students to learn about vulnerabilities in web applications through practical exercises. Thirty-seven students from National Institute of Technologies across Japan received credits for the course. In light of previous research results, the 37 students were classified into two groups according to their motivation scores on a pre-course questionnaire: the ultra-high motivation group (mean: 4.48) and the high motivation group (mean: 4.00) (analysis of variance showed a significant difference in mean scores (F(1,35)=11.37, p <.005)). Students' scores on cybersecurity skills and knowledge (operational and construction, knowledge and law, certification, vulnerability, and defense in depth) were obtained by questionnaire before and after the course. Analysis of variance showed that both the highly motivated group (Fs(1,100)>=10.65, ps<.005) and the ultra-highly motivated group (Fs(1,75)>=17.20, ps<.001) showed significant score increases on all five items. To examine consistency with the learning content, we also analyzed the magnitude of score increase for the five items and found a significant difference between the magnitude of score increase for vulnerability and the other items (ts(140)>=3.705, ps<.0003). These results confirm that the assumed skill improvement was appropriately practiced, and replicate that a motivation score of 4 or higher is highly effective for learning. To effectively utilize these results in other subjects, it is important to set goals based on appropriate historical background and to prepare prior learning to further increase interest.**

**Keywords:** *Credit Transfer System among National Institutes of Technology, Cyber Security Education Practice, Motivation, Information Security Exercise*

## Introduction

As cyber-attacks intensify, cyber security education is becoming increasingly important in engineering education around the world; KOSEN education, which emphasizes the acquisition of practical skills from the age of 15, fits well with Cybersecurity Body of Knowledge (CyBoK) advocated by Awais et al. (2018), who also advocate the importance of the technical aspects. Therefore, KOSEN became a target of national policy support, and the Cyber Security Human Resource Development Project (K-SEC) was initiated at KOSEN in 2015, and a faculty development project was launched within the project in 2019, with Kisarazu National College of Technology in charge of the project. The reason for launching the faculty development project is simple: if faculty members become stronger, students will also become stronger. In this project, practical training was conducted to improve the skills of faculty and staff, and the experience was used to develop teaching materials to foster students with a high skill level.

In 2022, K-SEC will be reborn as a cyber security field in COMPASS 5.0, a part of the "Society 5.0 Future Technology Human Resource Development Project" that KOSEN has started since 2020, and is expected to be further deepened and developed. Kisarazu National College of Technology has been a base school supporting Kochi National College of Technology, the core school of K-SEC, from the time K-SEC was established, but in COMPASS 5.0, it has become a full base school along with Kochi National College of Technology. The author has played a central role in the practical technical aspects of this human resource development project and has developed many cyber security educational materials together with the project team members. The author has also implemented the developed educational materials in lectures at his own college of technology, and has measured their educational effects. In addition, he has examined the relationship between educational effectiveness and motivation, and his latest results show that a motivation score of 4 or higher (on a scale of 1 to 5) for students can be expected to have high educational effectiveness (e.g., Yonemura et al., 2023).

In the same year of 2022, KOSEN started a credit transfer system among national colleges of technology, and Kisarazu National College of Technology, which serves as a base school for the cyber security human resource development project, began offering the author's course, Information Security Exercise. The Information Security Exercise is an introductory course to learn about vulnerabilities of web applications through practical exercises in a wide range of cyber security fields. Many technical college students from all over Japan had the opportunity to apply for the course, and in the end, 37 students received credits.

This paper describes the outline and practical methods of the Information Security Exercise, a course related to the Cyber Security Human Resource Development Project, which is a new trial for KOSEN and is expected to be challenging, and the effects obtained by the participants. The lecture will also include a discussion on the relationship with the motivation of the participants. The degree of skill improvement on vulnerability in the cyber security field learning items (defined as a total of 5 items), which was the goal of the project, was higher than the other 4 items. The high effectiveness of the priority items while obtaining considerable educational effects from the high level of motivation was demonstrated, which also led to confirmation of the validity of the content of the practical exercises. The findings have the potential to be applied not only to KOSEN education and education in the field of cybersecurity, but also to engineering education in higher education institutions more broadly, contributing to the advancement of engineering education as a whole in a lasting manner.

## Materials and Methods

The lecture "Information Security Exercise" in the credit transfer system for national colleges of technology in FY2022 was held in the second semester, specifically from October 2022 to February 2023. The materials were distributed by Microsoft Teams. Seventy students from all over Japan wished to take the course, regardless of their departmental grade. In the end, 37 students earned credits. No timetable was set; materials were added once a week, and each student worked on the lectures and exercises in his/her own free time. Questions were asked using individual chats, and content that needed to be made available to all participants was posted in the form of messages on Teams and made available to all.

The themes of the lecture materials were as follows:

- Construction of a target server to learn about vulnerabilities in web applications
- SQL injection attacks and defense exercises
- Directory traversal attacks and defense exercises
- Attacks and defense exercises for OS command injection
- Bind Shell and Reverse Shell
- Final assignment in the form of Capture the flag

Each participant prepared a virtual machine on his/her own PC, installed an OS, and built a target server. Then, in a closed network environment within the PC, the attacker's PC connected to the target server was also prepared as a virtual machine, and an attack defense exercise against web application vulnerabilities was conducted. The skills and knowledge acquired through the lectures were used for the final exam, Capture the flag.

In measuring the effectiveness of the education of students, which has been promoted as part of the cyber security human resource development project to date, skill check questionnaires on skills and knowledge in the field of cyber security have been conducted before and after attending lectures using the developed teaching materials (e.g., Yonemura et al., 2022; Yonemura et al., 2021) Furthermore, in the process of conducting educational effectiveness measurement research, we have conducted a study examining the relationship between motivation and educational effectiveness (e.g., Yonemura et al., 2023). In this study, we followed the above format that we have promoted in the past and had the participants answer the same skill-check questionnaire and motivation questions before and after the course. Responses were based on self-assessment.

The skill check questionnaire included items for monitoring and discussing the growth of skills before and after the course. The items were set by the steering members based on the knowledge system SecBOK by Uehara et al. (2019) and the experience of cybersecurity training (e.g., MIC, 2016) in which the steering members of the faculty development project participated (e.g., Yonemura et al., 2023; Yonemura et al., 2022; Yonemura et al., 2021).

Scores are on a 5-point scale from 1 to 5, based on respondents' self-assessment: 1 is "not knowledgeable," 2 is "knows," 3 is "can teach (knows well)," 4 is "can operate," and 5 is "can troubleshoot (can operate at a higher level)."

There are five major categories of responses, each with four or five sub-categories. The major item "Operation and Construction" includes five sub-items such as "OS (Linux / Windows)," "Server (Web server, mail server, DB server)," "Database and access privileges," "User and administrator access control," and

"HTML / JavaScript / PHP / CGI. The major category "Knowledge and Law" includes five subcategories: "OS (Linux / Windows)," "Risk Causes (physical factors, technical factors, human factors)," "Unauthorized Access Prohibition Law and Personal Information Protection Law," "CVE," and "Cyber Kill Chain. The major category "Certification" has four subcategories: "Certificates," "Cookies," "Protocols (HTTP, TCP/IP, IPSec)," and "Basic Authentication. The major category "Vulnerability" has five subcategories: "SQL Injection," "OS Command Injection," "XSS," "Exploits," and "Security Assessment, Vulnerability Assessment, and Penetration Testing. Finally, the major item "Defense in depth" has five sub-items: "Anomaly detection, tamper detection," "Firewall," "DMZ," "IDS, IPS," and "WAF.

Based on the discussion by Jaaska et al. (2022) that Game Based Learning (hereafter GBL) methodology as an educational method may increase student motivation and learning effectiveness, Yonemura et al. (2023) positioned cybersecurity educational materials as Game Based Learning and quantitatively examined the amount of motivation required for effective learning. The participants were asked to answer four questions related to motivation: "Interest in learning cyber security," "Difficulty in learning cyber security on your own," "Are you looking forward to taking the course," and "Expectations for improving your skills after taking the course. Respondents were asked to rate the degree to which they thought about each question on a 5-point scale: 100%, 75%, 50%, 25%, and 0%. A score of 100% was set at 5, followed by 4, 3, and 2, and a score of 0% was set at 1 when we analyze the data. The results showed that a motivation score of 4 was the boundary line separating effective skill development from ineffective skill development, suggesting that an average of 75% or more in the degree of thought to the four questions leads to effective skill development. Since the purpose of this study was also to observe the possibility that motivation contributes to effective learning, the same questions were answered before the course was taken.

## Results and Discussion

The 37 students who eventually received credit were divided into two groups according to their motivation scores from the pre-course questionnaire. Based on previous research findings (e.g., Yonemura et al., 2023), we positioned these two groups as the ultra-high motivation group (mean score 4.48, 16 students) and the high motivation group (mean score 4.00, 21 students). Figure 1 shows the mean motivation scores of the two groups after classification. The ultra-high motivation group is on the left and the high motivation group is on the right. All 37 students were highly motivated, as they had voluntarily requested elective courses and had earned credits for them. The high motivation group was further divided into two groups: the high motivation group and the high motivation group. A one-factor analysis of variance with score as a factor showed a main effect of score for both groups (F(1,35)=11.37, p<.005), so we decided to proceed with the analysis for each group, judging that the positioning by score was appropriate.

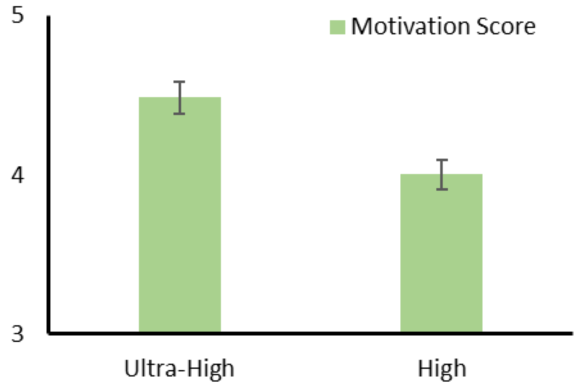

Figure 1 The average of motivation scores for each group when 37 participants were divided into two groups according to motivation score (error bars indicate standard error).

Scores on cybersecurity skills and knowledge of the students who took the course were also obtained through questionnaires before and after the course. The skills and knowledge were the five categories that have been used as indicators in previous studies: operation and construction, knowledge and law, certification, vulnerability, and multilayer defense. We focused on this point because the perspective is whether differences in skill development occur in the two groups we classified.

Figure 2 shows the average of the self-assessment scores of the five skill items before and after the course for the 21 participants in the highly motivated group. Similarly, Figure 3 shows the average of the self-assessment scores of the five skill items before and after the course for the 16 participants in the ultra-high motivation group.

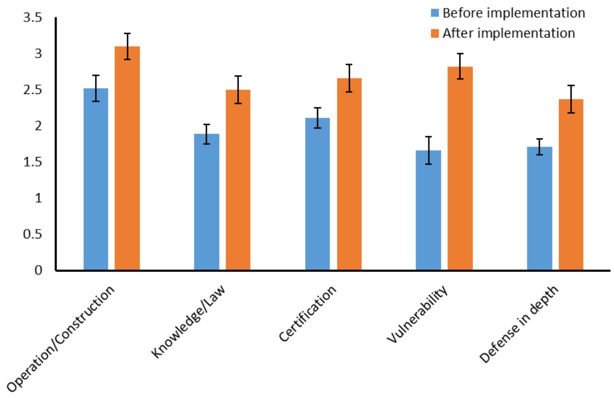

Figure 2 The average of self-rated scores of the five skill items before and after the course for the 21 highly motivated group members (error bars indicate standard errors).

For the highly motivated group, a two-factor analysis of variance with skill items and pre- and post-attendance as factors revealed main effects for skill items (F(4, 80)=13.76, p<.001) and pre- and post-attendance (F(1,20)=24.05, p<.001). The interaction was also significant (F(4,80)=7.32, p<.001). Since the focus was on which of the five skill items had a significant learning effect before and after the course, a simple main effect test for the interaction confirmed that significant learning effects were obtained for all five skill items (Fs(1,100)>=10.65, ps<.005). ps<.005).

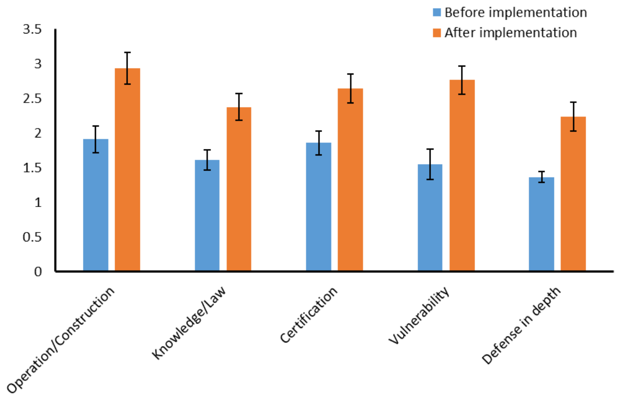

Figure 3 The average of self-rated scores of the five skill items before and after the course for the 16 participants in the ultra-high motivation group (error bars indicate standard errors).

Similarly, in the ultra-high motivation group, a two-factor analysis of variance with skill items and pre- and post-course as factors showed main effects for skill items (F(4, 60)=5.98, p<.001) and pre- and post-course (F(1,15)=37.65, p<.001). The interaction was also significant (F(4,60)=2.64, p<.05). As with the highly motivated group, since the focus was on which of the five skill items had a significant learning effect before and after the course, a simple main effect test on the interaction confirmed that significant learning effects were obtained for all five skill items (Fs(1,75)>=17.20, ps<.001).

These results confirm the results obtained in the previous paper that a motivation score of 4 or higher is associated with a high learning effect. A new point of view in this study was to examine whether there is a difference in learning effectiveness when groups are further classified into groups with a motivation score of 4 or higher. However, since both groups obtained exactly the same results, i.e., significant learning effects were obtained for all five skill items, a so-called ceiling effect occurred, and no differences between the two groups could be confirmed.

In order to examine whether the content of the prepared study and the corresponding skill items grew, we then conducted a two-factor analysis of variance on the score increase for the five items, with the two motivation groups and the growth of the five skill items as factors. A main effect for growth in skill items was found (F(4,140)=8.23, p<.001), but no main effect was found for the motivation group (F(1,35)=1.07, p=031). The interaction was also not significant (F(4,140)=0.95, p=0.44). Since a main effect was found for the growth of the skill items, multiple comparisons confirmed a significant difference with the other four items for the score increase on vulnerability (ts(140)>=3.71, ps<.0003).

This result suggests a high level of skill building and knowledge acquisition on vulnerability, a skill item intended by those who developed and provided the educational materials. However, no difference in learning effects was observed between the two motivation groups.

Although it was not possible to confirm the difference between the two motivation groups due to the occurrence of the ceiling effect, it was confirmed that the assumed skill improvement was appropriately implemented and effective for all participants, and that a motivation score of 4 or higher is sufficient for a high learning effect to be obtained. In order to effectively utilize the results of this study in other subjects, practices in other fields, and other higher education institutions, we conclude that two points are necessary: setting goals based on appropriate historical background and preparing prior learning to further increase interest, since a high motivation score may be an important point.

## Conclusions

The development of cyber security personnel is becoming increasingly important in engineering education around the world. kosen has been promoting a cyber security personnel development project since 2015, and our Kisarazu National College of Technology is the base school for the project. in 2022, KOSEN launched an inter-KOSEN credit transfer system. The author, who is in charge of the technical aspects of the project, opened an "Information Security Exercise" course that allows students to learn about vulnerabilities of web applications in a practical manner in order to develop cyber security human resource development by utilizing this system.

While promoting the project and conducting educational effectiveness measurement research, the latest research results had obtained that a motivation score of 4 or higher (on a scale of 1 to 5) indicates a high learning effect. Therefore, we aimed to replicate this result in this course under the KOSEN inter-KOSEN credit transfer system.

When we compared the educational effects of the cyber security skills and knowledge items for 37 participants in the "Information Security Exercise" course offered in the second semester of 2022 before and after the course, we confirmed the high educational effects associated with high motivation scores, thus reproducing the findings we had obtained previously. In addition, the cyber security educational materials used in this study were intended to improve skills related to vulnerability, and skill improvement was observed as intended, suggesting the appropriateness of the content of the practice.

In other words, by having students attend lectures with high motivation, high educational effects can be obtained and skills can be improved as intended. Although this framework and its results are limited to education at KOSEN and the field of cybersecurity at this time, the effects of increasing motivation may be applicable to all educational settings in light of the theory of Jaaska et al. In addition, since learning in the cybersecurity field contains many elements of Game Based Learning, there is a high possibility that the findings can be generalized to fields that have elements of Game Based Learning.

In conclusion, we believe that by working to motivate students by setting goals based on appropriate historical backgrounds and preparing for prior learning to increase interest, it will be possible to increase the effectiveness of education not only in engineering education at KOSEN, but also in all engineering fields at higher education institutions.

In the future, we would like to examine the differences in educational effectiveness due to further subdivided groupings within a motivation score of 4 or higher, which could not be confirmed this time. By focusing on the points in the range of scores where many learners stay, and by zooming in, a more detailed analysis of the same range will be possible, so we will prepare questions that take this into account and conduct a detailed analysis at the next course opening.

The results obtained are expected to make a significant contribution to the analysis and application of new educational effectiveness measures.

## Acknowledgements

This research was partially supported by JSPS KAKENHI Grant Number 20K03113 and KOSEN Security Educational Community.

## References

Awais, R., George, D., Howard, C., Emil, L., Andrew, Makayla, L. & Claudia, P. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, 16, 96–102.

Jaaska, E., Lehtinen, J., Kujala, J. & Kauppila, O. (2022). Game-based learning and students' motivation in project management education. *Project Leadership and Society.* 3, 1-13.

Ministry of internal affairs and communications. (2016) Cyber Defense Exercise with Recurrence (CYDER). Retrieved from *https://cyder.nict.go.jp*.

Uehara, T. et. al., (2019). Security Body of Knowledge (SecBoK2019). Retrieved from *https://www.jnsa.org/result/2018/skillmap/.*

Yonemura, K., Kobayashi, H., Oyama, S., Fukuda, T., Hirano, M., Shiraisi, K., Hayashi, N., Moriyama, H., Okamura, S., Doi, S., Kaeriyama, T., Nakata, R., Hashimoto, M., Sato, J., Taketani, H., Yamada, S., Izumi, S., Okamoto, H., Fujimoto, Y., Sakamoto, Y., Maruyama, M., Noguchi, K. & Kishimoto, S. (2023). Motivation in Teaching Expert Development Project by KOSEN Security Educational Community. *in Proc. 2023 IEEE Global Engineering Education Conference (EDUCON)*, Kuwait, Kuwait, 1-9.

Yonemura, K., Kobayashi, H., Shiraisi, K., Fukuda, T., Hirano, M., Moriyama, H., Sato, J., Taketani, H., Oyama, S., Yamada, S., Izumi, S., Okamoto, H., Fujimoto, Y., Sakamoto, Y., Noguchi, K. & Kishimoto, S. (2022). Teaching Expert Development Project by KOSEN Security Educational Community. *in Proc. 2022 IEEE Global Engineering Education Conference (EDUCON)*, Tunis, Tunisia, 1642-1650.

Yonemura, K., Kobayashi, H., Sato, J., Taketani, H., Oyama, S., Yamada, S., Izumi, S., Okamoto, H., Fujimoto, Y., Sakamoto, Y., Noguchi, K., and Kishimoto, S. (2021). Cybersecurity Teaching Expert Development Project by KOSEN Security Educational Community. *in Proc. 2021 IEEE Global Engineering Education Conference (EDUCON)*, Vienna, Austria, 468–477.