Research about auto progress management system of cyber security training for education

1710021 Takuya Inoue

Information and communications technology are developing rapidly, almost all things in society have become dependent on the network. The 4th industrial revolution by IoT become a popular topic, and dependence on the Internet become further worse. But, as information and communication technologies become more familiar, the risks of cyber attacks become closer to us and serious. Cyber space is handy as well as very dangerous. A malicious attacker continually searches the Internet and looking for vulnerable computers. Besides, traps on malicious cyberspace, such as spam emails, fishing sites, and Forced Redirect to other WEB sites, are increasing day by day. However, we can prevent most of these attacks by appropriate measures. Even in case of damage caused by cyber attacks, if you take appropriate measures without panic, you can suppress the cost. Therefore, security education is essential.

However, education has not kept pace with the rapid development of technology now. Thus, not only the lack of security expert but also security literacy in everyone are sufficient. We focused on cyber defense training in this research to solve these problems. In cyber defense training, the management side executes cyber attacks against the training environment given to the students. Participants prevent cyber attacks by implementing security measures against the training environment and perform incident handling when incidents occur. By learning about the importance of countermeasures by experiencing the threat of cyber attacks through cyber defense training, at the same time, by making it a preliminary training in the event of actual damage, to deal with reality even in reality It is expected to become. However, technical training that undergo cyberattacks are difficult to hold due to problems of cost and labor, and only a limited number of people can attend. Besides, it is dependent on the individual's ability to learn the existing cyber defense training, whether learning elements are thin, and the purpose of the training will be experiences of cyber attack or learning of countermeasures and countermeasures. Therefore, it is essential to make cyber defense training easy for education.

The purpose of this research is to enable cyber defense training to be implemented by anyone by automating the progress management of learning cyber defense training. The progress of the training is aimed at reproducing the flexible pace according to the ability of the students and the training situation by automation like cyber defense training where cyber attacks are

executed manually. By automation, everyone can not only perform cyber defense training but also when and when attacks have been made clear, it will be easier to reflect. To realize flexible training, I thought that it would be necessary to have a function to judge the ability of students and a service to wait for the progress of the training. In general, the management side don't know the ability of students to operate cyber defense training. Therefore, judge the ability of the student by the success or failure of the cyber attack performed during the training. Also, in the training to manually complete a cyber attack, we will proceed with activities while inquiring about the situation of the students during the training and the case of the training environment. Therefore, the realization of flexible progression includes a function to diverge the progress of the practice according to the success or failure of the executed cyber attack, a role to make the training stand by in accordance with the operation situation of the student's service, It can be realized by the function to make the training progress wait until the action is done.

In this research, we proposed a cyber defense training progress management system DeTMan with these functions, designed and implemented it. DeTMan advances training according to prepared training scenario. In the training scenario, attacks to be executed, timing to achieve, and destinations according to success or failure of the attacks are described. Besides, we monitor the service before completing the offense, etc. When an abnormality is detected, we judge that some accident has occurred to the student and wait for the progress of the training. In addition to this, it is also possible to provide learning support such as displaying messages via WEB UI for students or making quizzes on behalf of attacks. Using DeTMan, we conducted experiments on the usefulness of DeTMan by actually making cyber attacks for learning purposes. By experiments, it was possible to reproduce various cyber attacks, and at the same time, it was found that cyber defense training could be held with less labor and expense compared with real defense training. Also, unlike actual defense training, we were able to confirm that learning elements can be offered to students during activities. By using DeTMan, it is possible to experience not only a verbal explanation about the cyber attack but also experience. Cyber attacks are not special things. They can learn something that the threats will attack at any moment, contributing to further enhancement of security education.