Title	状態遷移モデルを活用したサイバー防御演習における振る舞い解析の高度化に関する研究
Author(s)	梅内, 翼
Citation	
Issue Date	2022-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/17626
Rights	
Description	Supervisor: 篠田　陽一, 先端科学技術研究科, 修士（情報科学）

Research on the Advancement of Behavior Analysis in Cyber Defense Exercise using State Transition Model

2010014 Umeuchi Tsubasa

In recent years, with the development and spread of information and communication technologies, cyber security measures have become a challenge for many organizations, while a significant shortage of human resources with skills in cyber security is considered to be a problem. In response to this situation, the importance of cyber defense exercises conducted in a virtual space, which is constructed for the purpose of conducting cyber security exercises, has been recognized as a means of acquiring incident response skills. A cyber defense exercise is an exercise aimed at empirically acquiring incident response skills through detection and response to attacks on hosts and systems assigned to the participant, and recovery from failures caused by attacks.

The purpose of the cyber defense exercises conducted on the cyber range is to provide participants with knowledge and skills on incident response through the exercise. To achieve this, it is essential to reflect on what kind of behavior led to a successful defense against the attacks executed in the exercise.

In this study, based on the assumption that the changes brought to the cyber range by the behavior of the participants are considered as differences, we propose a method to systematically extract the differences by integrating the progress of the cyber defense exercise with the state transition model and a method for automatically analyzing the differences that led to the successful defense of the attacks executed in the exercise among the extracted differences.

As a result of our experiments, we verified that it is possible to analyze such differences accurately and in a realistic time. On the other hand, we also found concerns about the coverage of the sources where the differences are extracted, the reproducibility of the behavior, the performance of the analysis algorithm, and the existence of differences that cannot be observed on the cyber range.