Title	APT
Author(s)	,
Citation	
Issue Date	2016-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/13629
Rights	
Description	Supervisor: , ,

Japan Advanced Institute of Science and Technology

2015 to August 2015 for conduct behaviour for legitimate user, and change to Read/Write TSL from September 2015 to November 2015 for conduct behaviour for attacker. And comparison of the TSL by FAST. "fspeek" experiment is the correct anomaly detection by FAST as a result of the experiment. And "fspeek" could detect at an early stage than the conventional method. Because the attacker is assumed to be a long-term lurk within the system. As a result, "fspeek" could shorten the period until detecting the intrusion of the attacker.

As the future works, FAST is required verification of detection accuracy in the case of change the various parameters. In addition, it is required to reduce the amount of data of the TSL. Because long-term TSL is required for the FAST.

2015 to June 2015 (TSL A) is referred to as a group A. Read only TSL from July 2015 to November 2015 (TSL B) is referred to as a group B. TSL A include exploratory file access is referred to as a group A_n. TSL B include exploratory file access is referred to as a group B_n. "n" of A_n and B_n represents the number of times per day of file access that mix to read only TSL. I putting "n" =(1,2,3,4,5,6,8,12), calculating the area of each TSL. I conduct paired T-test to define null hypothesis as "no difference between the groups". As an experimental result, in case of significance level =10%, paired T test(B,A_3),(B,A_4),(B,A_6),(B,A_8),(B,A_{12}),(A,B_6),(A,B_8),(A,B_{12}) are significantly different.