

[]

(Network-Based Intrusion Detection: NIDS) 가
가 (Resource) ,
(Process) .
(signature) ,
(Intrusion)
(Misuse Detection)가 .
(Attack) , 가(Expert)가
가
가
(Traffic)
(Statistics-Based Anomaly Detection) .
가
가
(Artificial Intelligence) .
(Knowledge) , 가 (Expert
System) (Classification) .
(Machine Learning)
(Supervised Learning)
(Unsupervised Learning) ,
(

(Tree), (Instance), (Weight value), IF THEN (Rule))
 가
 (Cluster) , 가 .
 ,
 ,
 ,
 (Decision Tree), (Nural Network), IBL(Instance Based
 Learning) , (Clustering) .

DARPA 가 1998 3
 가 가 .
 (ETRI)
 (KISA) ,
 가

가 (Error Rate)
 70% ,
 40% 가 90%
 가
 (DARPA Data Set)

(Modeling)

가

가

(

, chlee@konkuk.ac.kr)