2020 Capstone Design

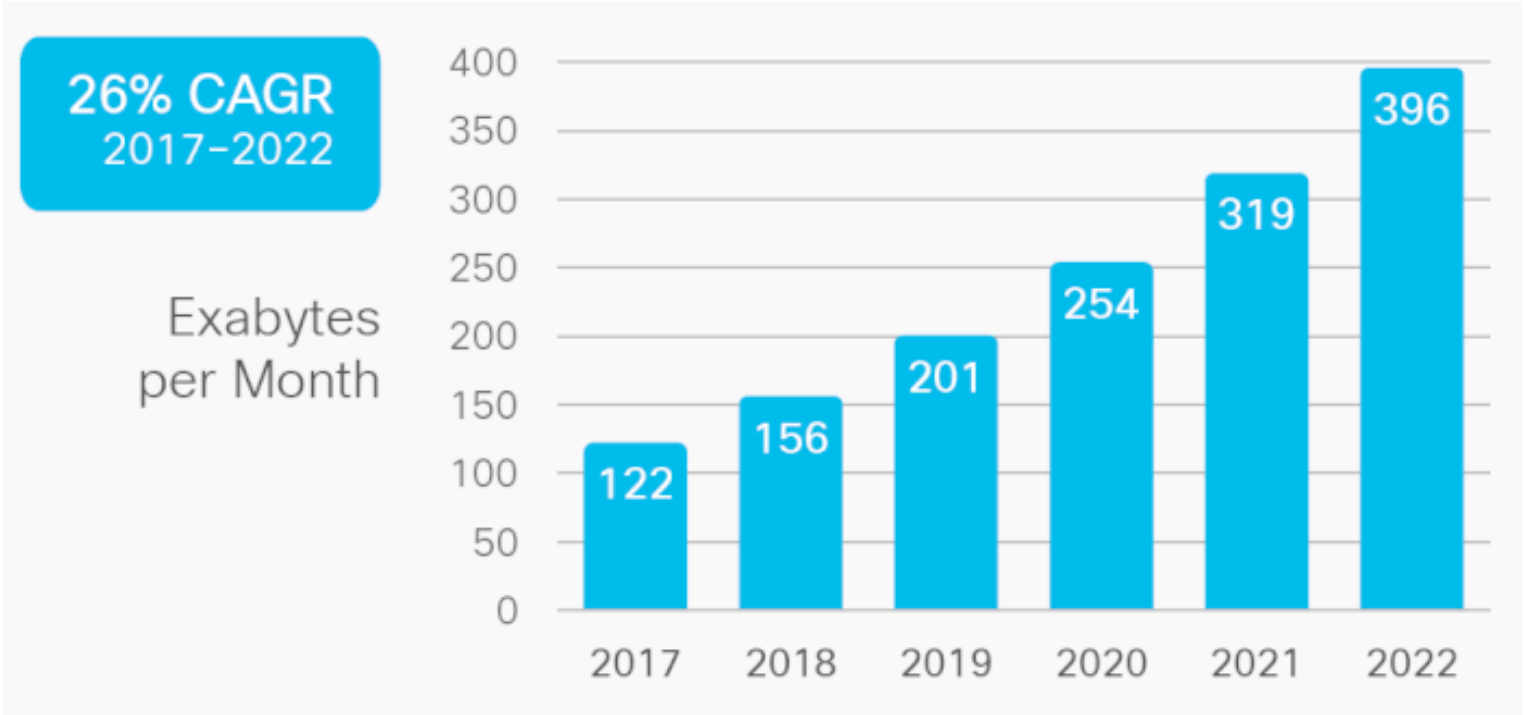
SEMO : Security Monitoring Platform

7조 Do Mo!(Do Monitoring!)

CONTENTS

SEMO : Security Monitoring Platform

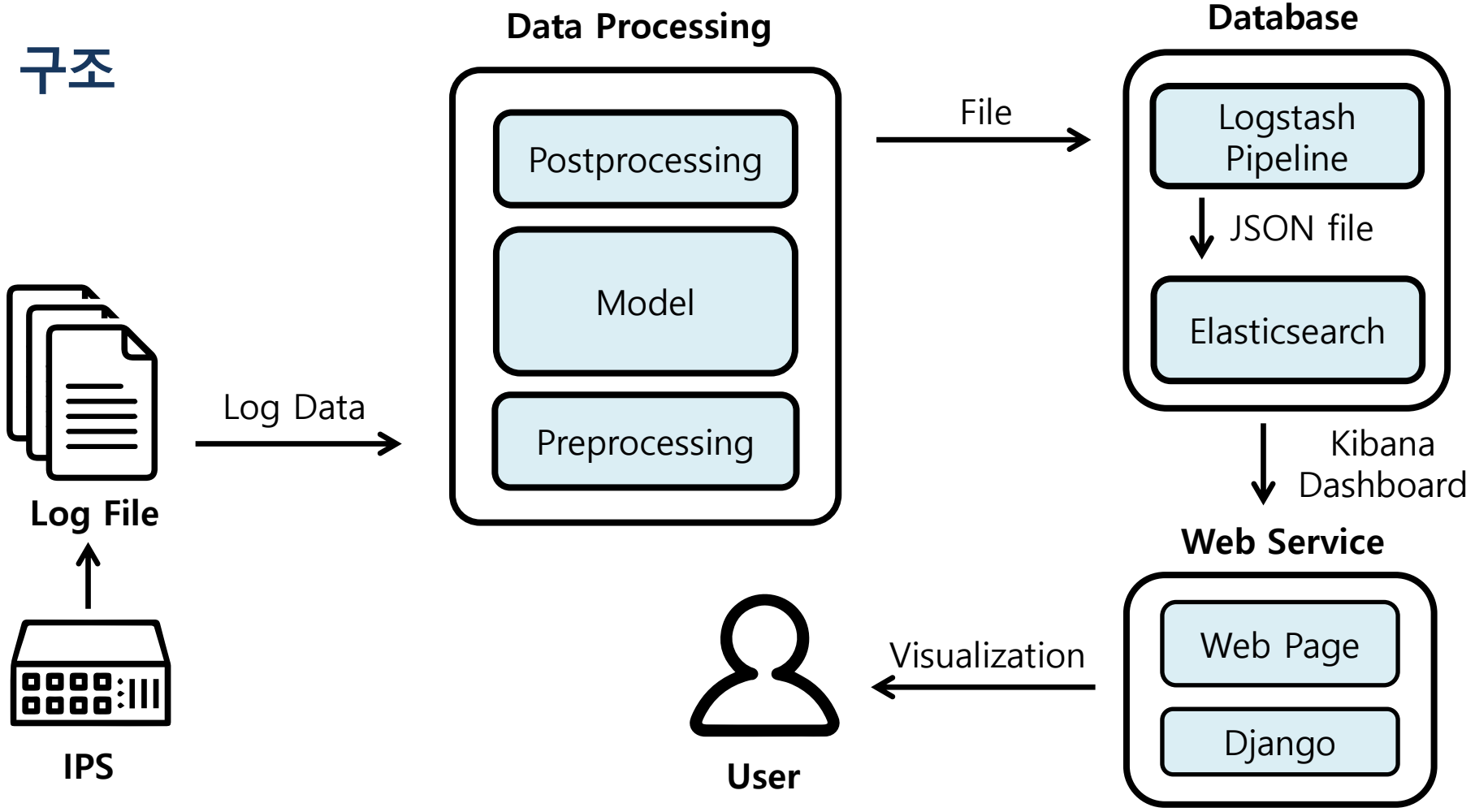
01 프로젝트 소개



전세계 월별 IP 트래픽 전망
(출처 : Cisco VNI Global IP Traffic Forecast, 2017–2022)

01 프로젝트 소개

시스템 구조



01 프로젝트 소개

프로젝트 목표

“보안 업무 효율성 향상”

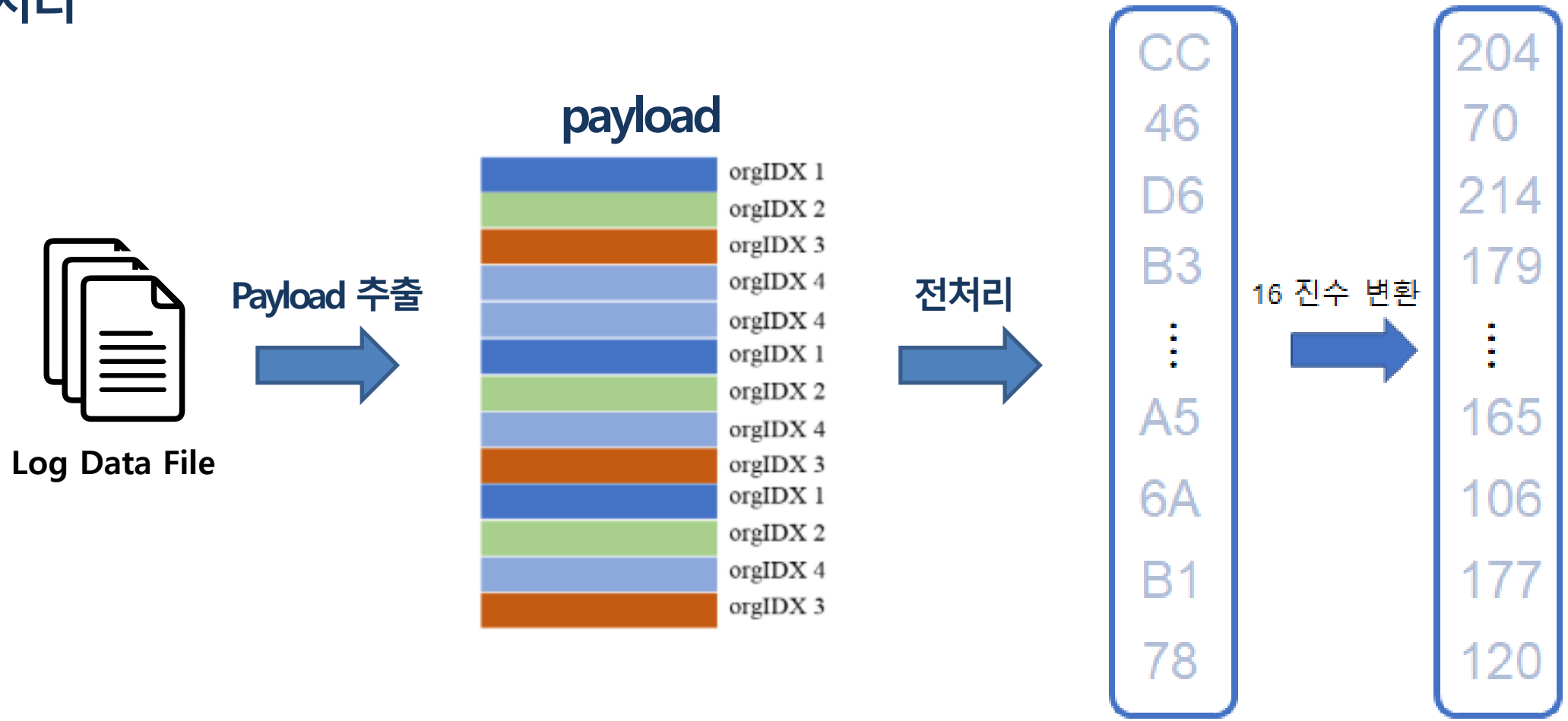
“Best Practice 제공”

CONTENTS

SEMO : Security Monitoring Platform

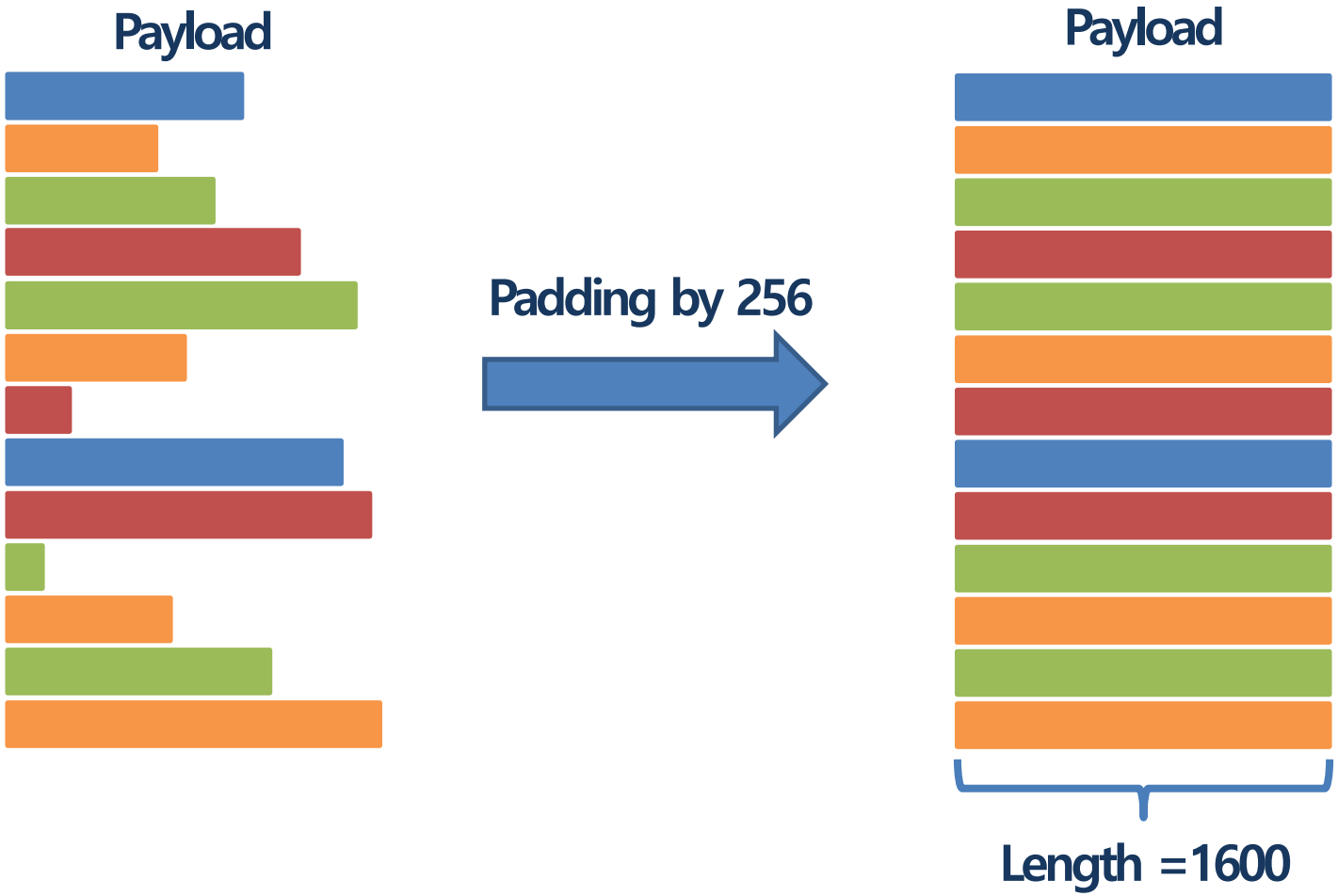
02 수행 내용

전처리


payload
orgIDX 1
orgIDX 2
orgIDX 3
orgIDX 4
orgIDX 4
orgIDX 1
orgIDX 2
orgIDX 4
orgIDX 3
orgIDX 1
orgIDX 2
orgIDX 4
orgIDX 3
Log Data File
Payload 추출
전처리
CC
46
D6
B3
A5
6A
B1
78
16 진수 변환
204
70
214
179
165
106
177
120

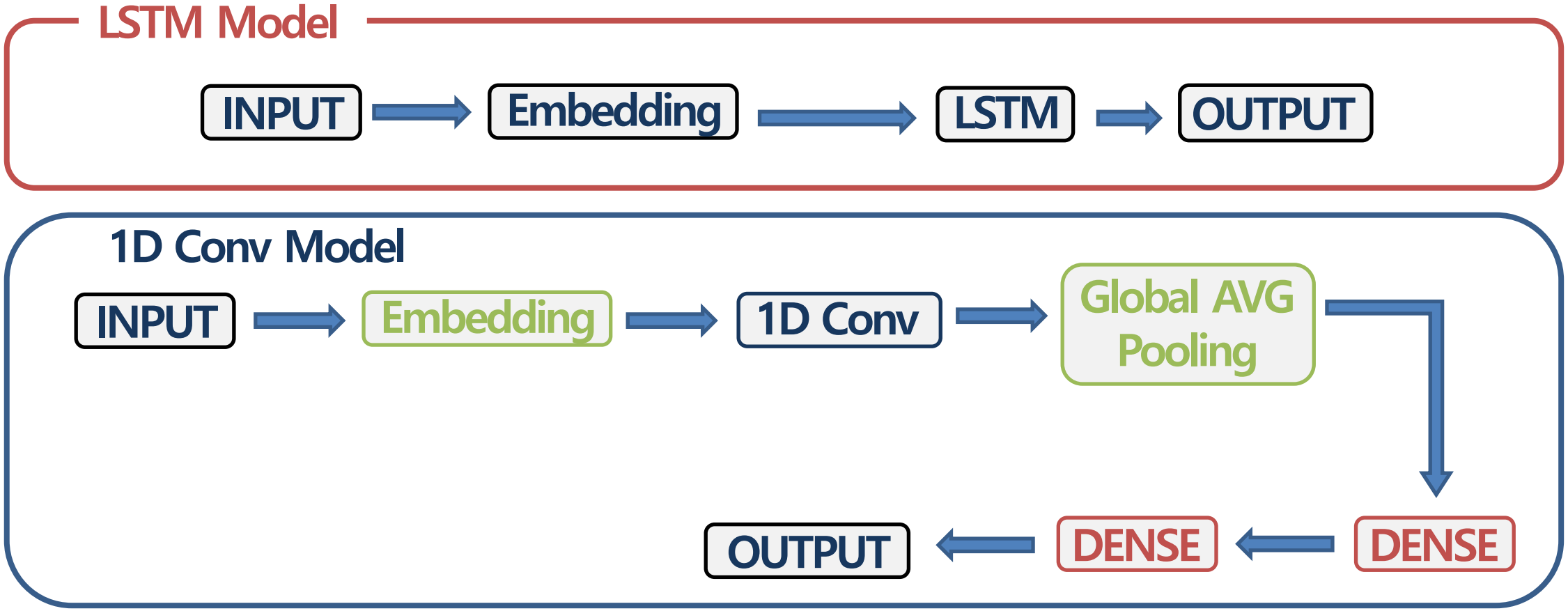
02 수행 내용

전처리 [Padding]



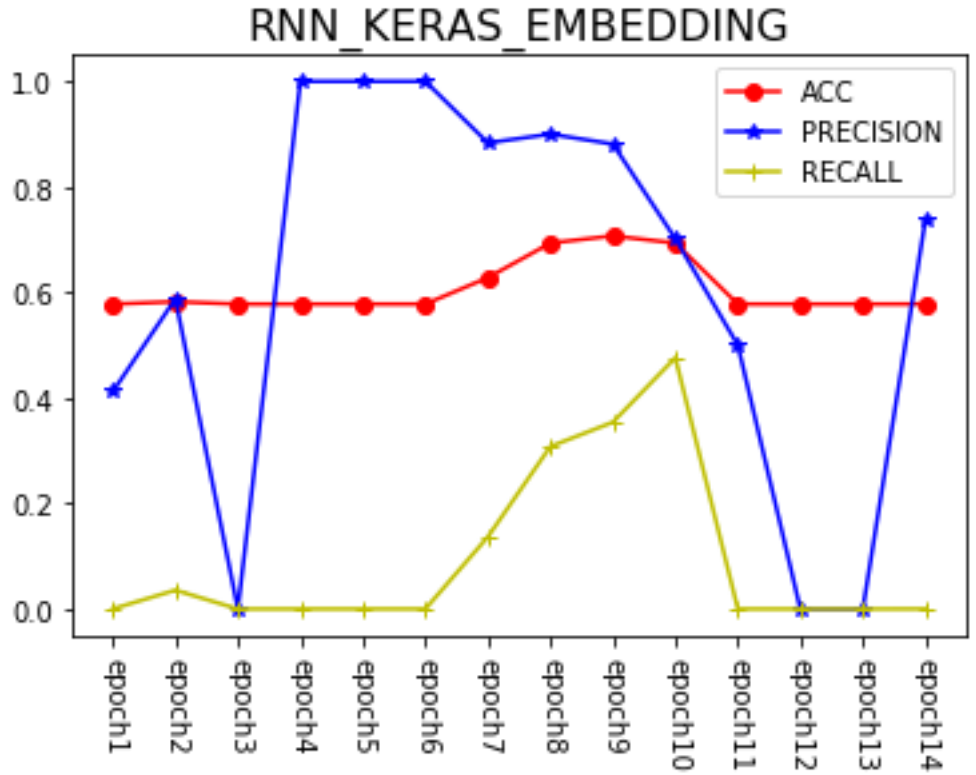
02 수행 내용

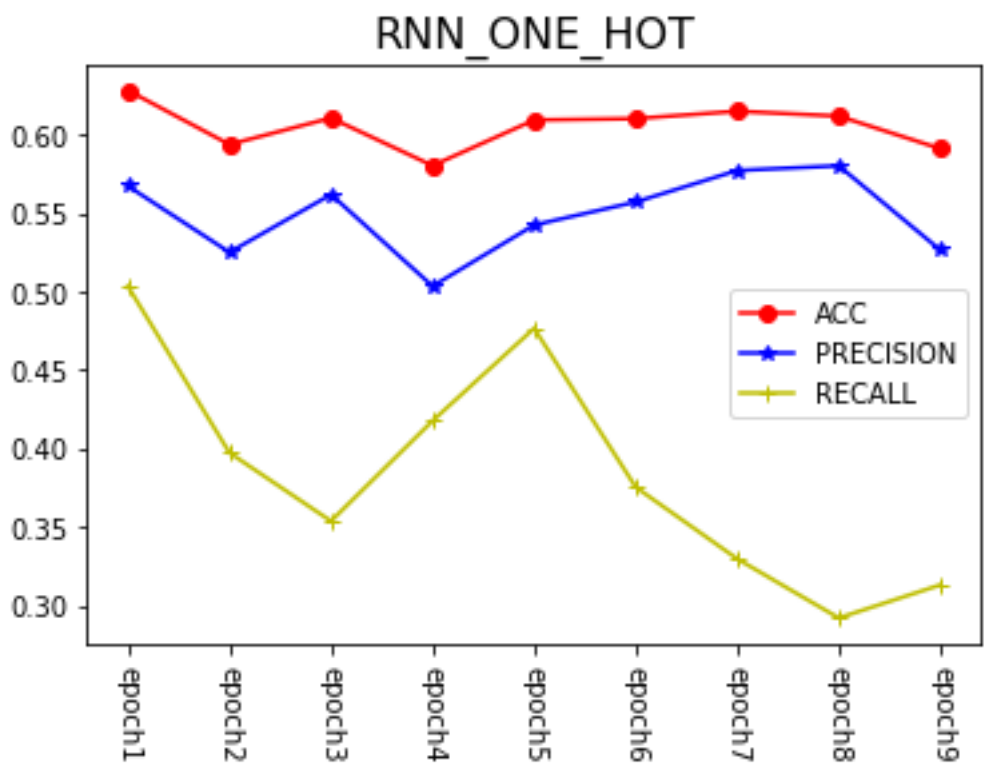
모델 선정


LSTM Model
INPUT
Embedding
LSTM
OUTPUT
1D Conv Model
INPUT
Embedding
1D Conv
Global AVG Pooling
DENSE
DENSE
OUTPUT

02 수행 내용

모델 선정





➔ 임베딩 기법을 바꿔가며 실험을 진행했으나, 훈련이 안되는 것으로 판단
➔ 비교적 안정적인 1dConv로 모델 결정

02 수행 내용

1D Conv

임베딩 중요성에 관한 실험

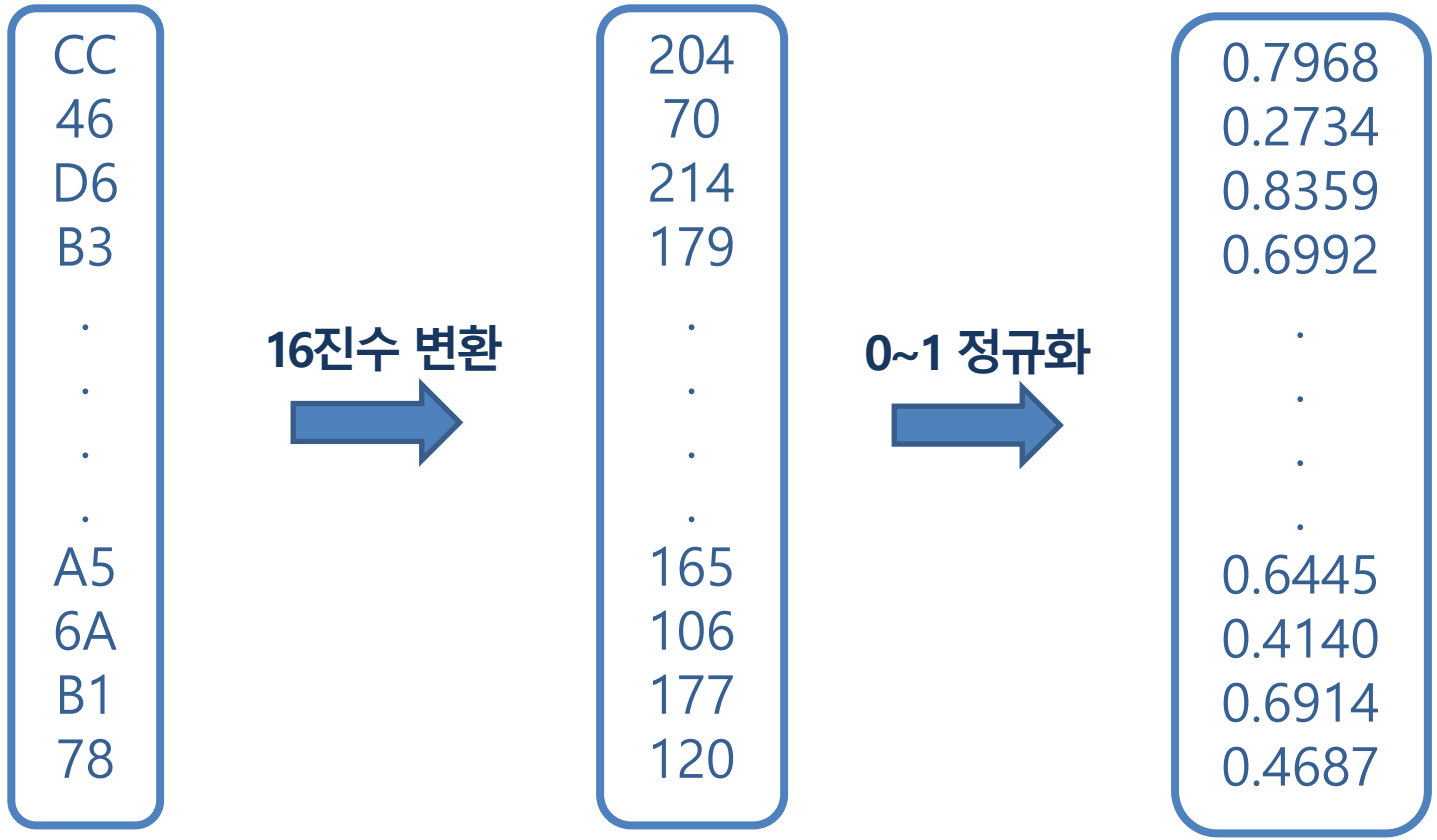
1. 0~1로 정규화

2. One-Hot encoding

3. Keras Embedding layer

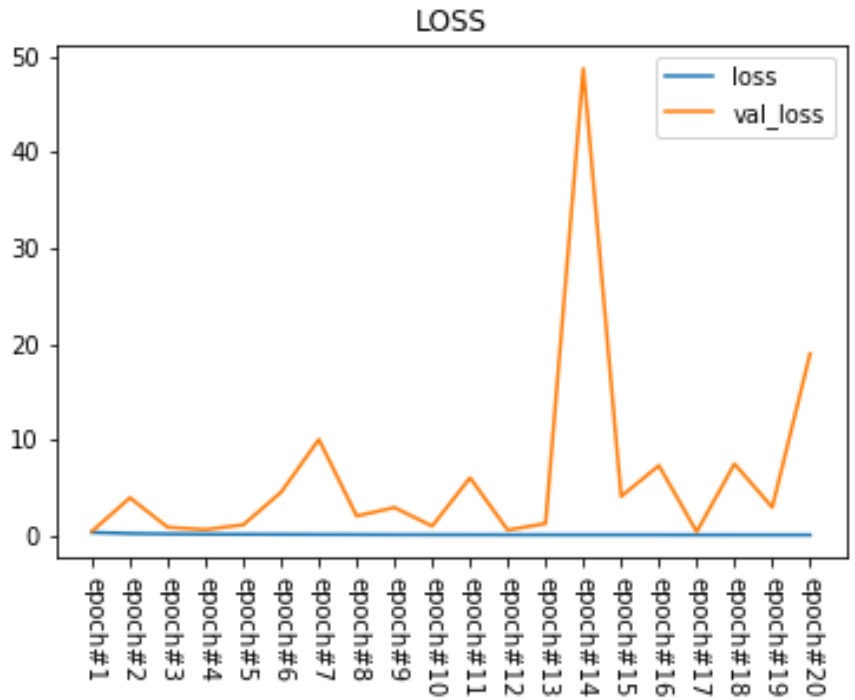
02 수행 내용

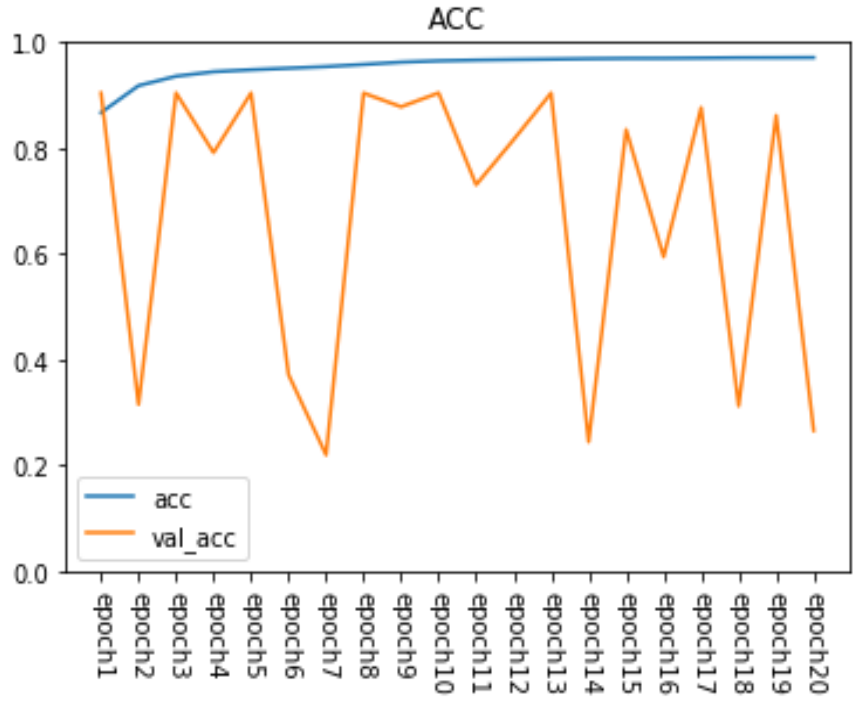
1D Conv [0~1 정규화]



02 수행 내용

1D Conv [0~1 정규화]

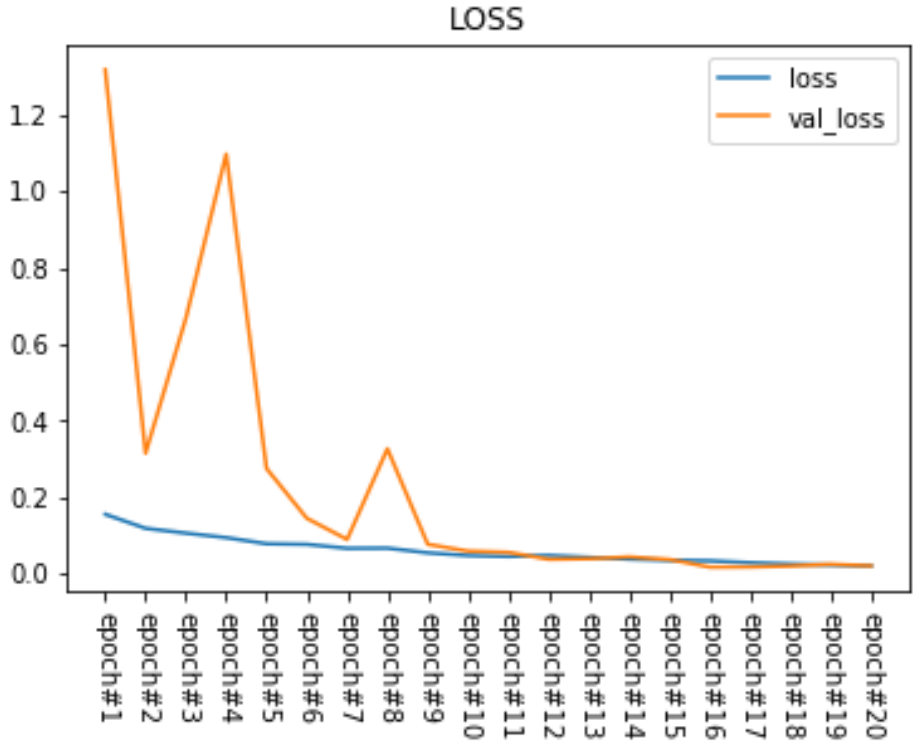


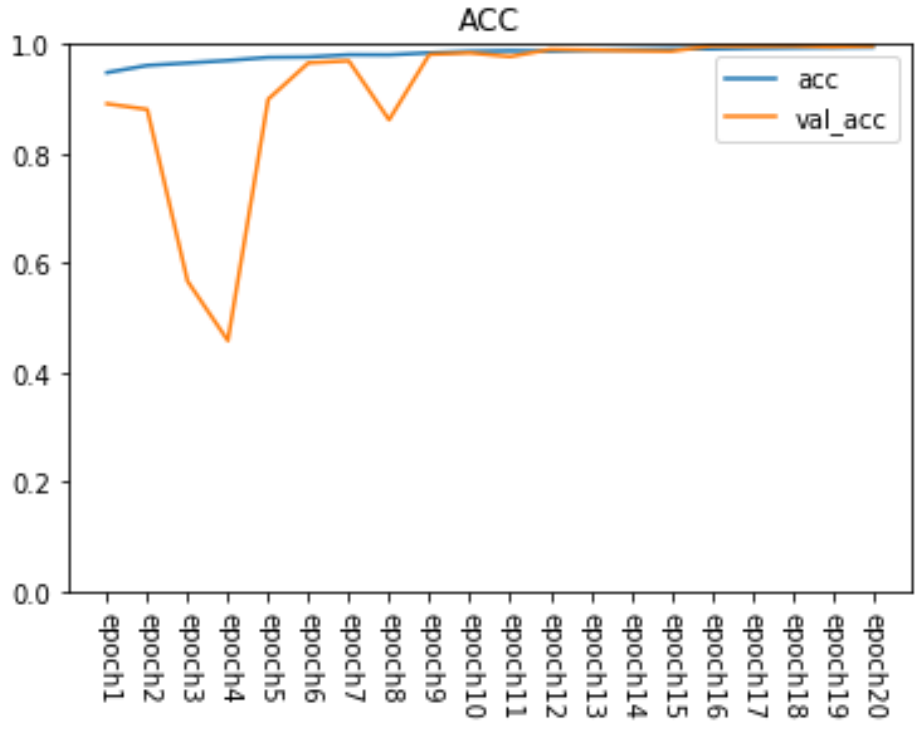


➔ Validation Loss 와 Accuracy가 불안정

02 수행 내용

1D Conv [one-hot]

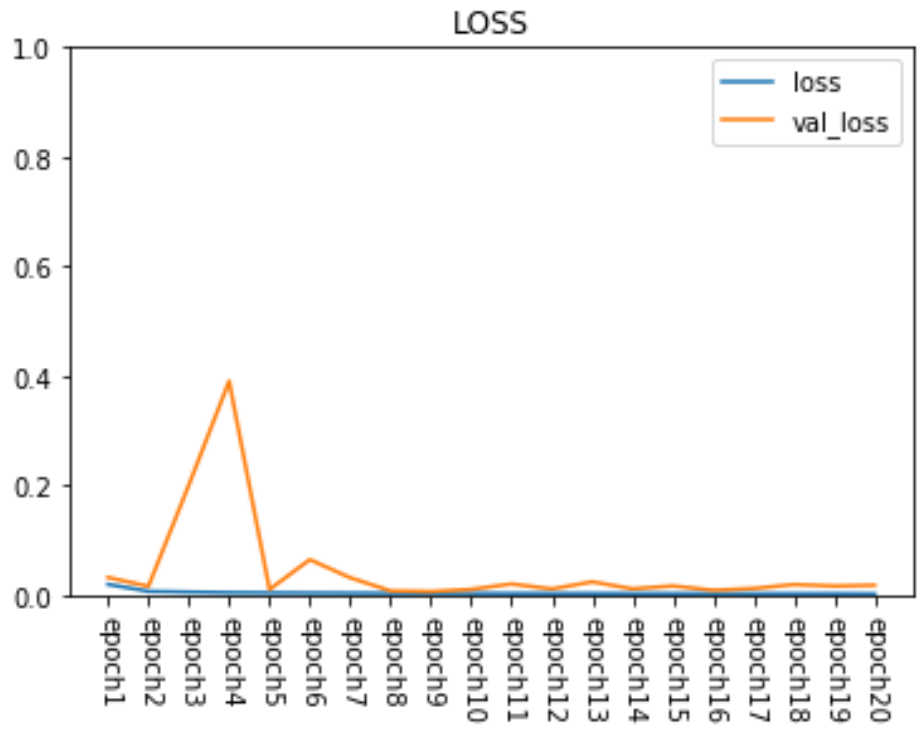


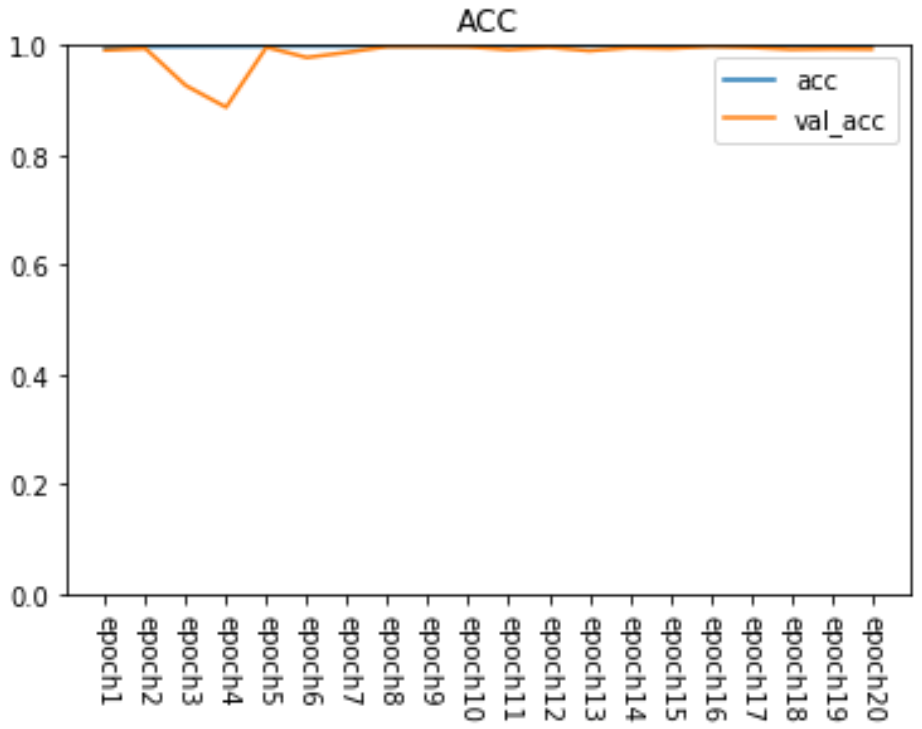


➔ Train과 Validation이 비교적 안정적이나 무거운 구조

02 수행 내용

1D Conv [keras embedding]





➔ Train Loss가 더욱 빨리 수렴

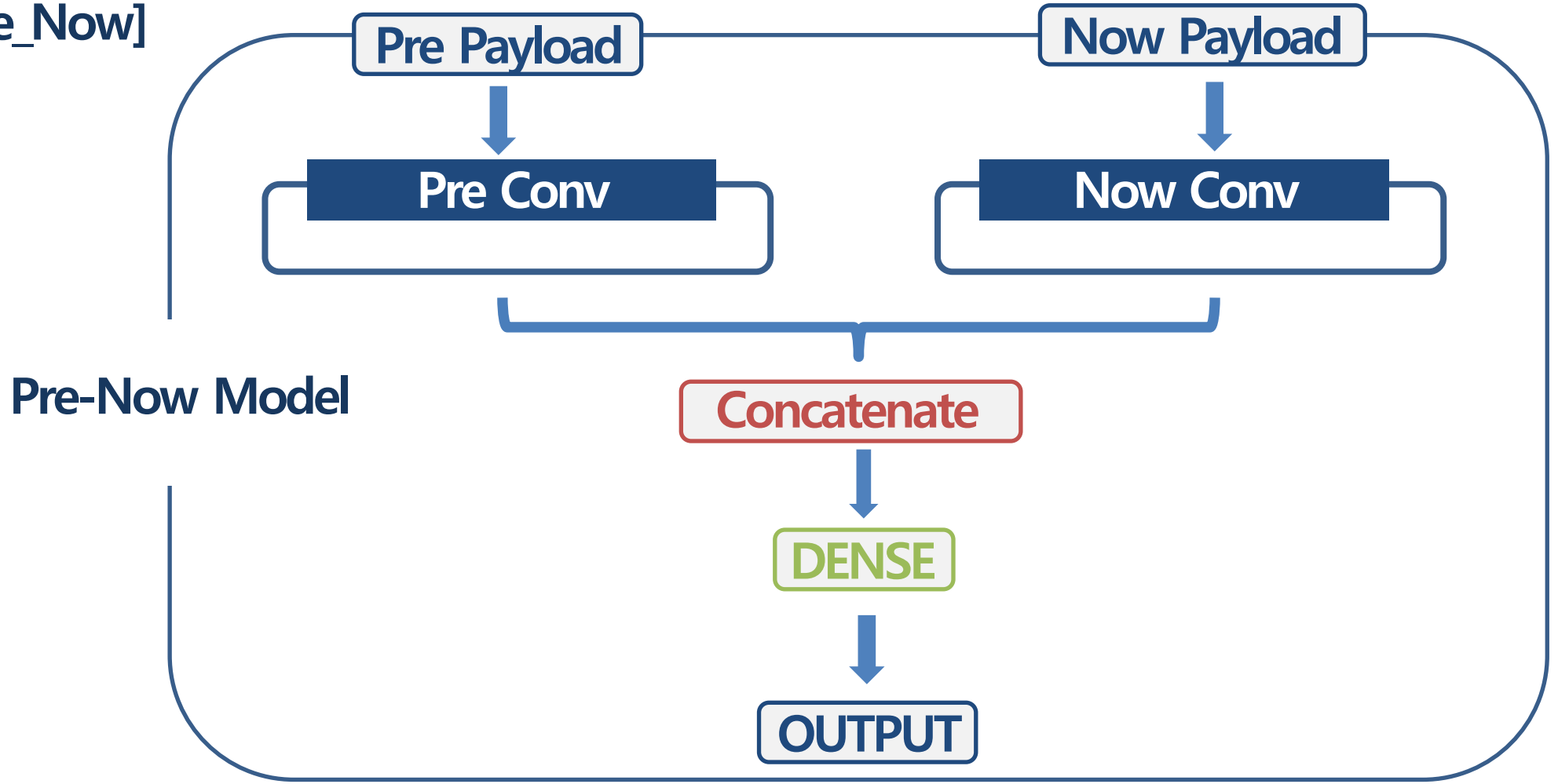
02 수행 내용

전처리 [Pre_Now]

➔ 하나의 페이로드 학습 시 같은 기관의 이전 페이로드 고려하여 학습

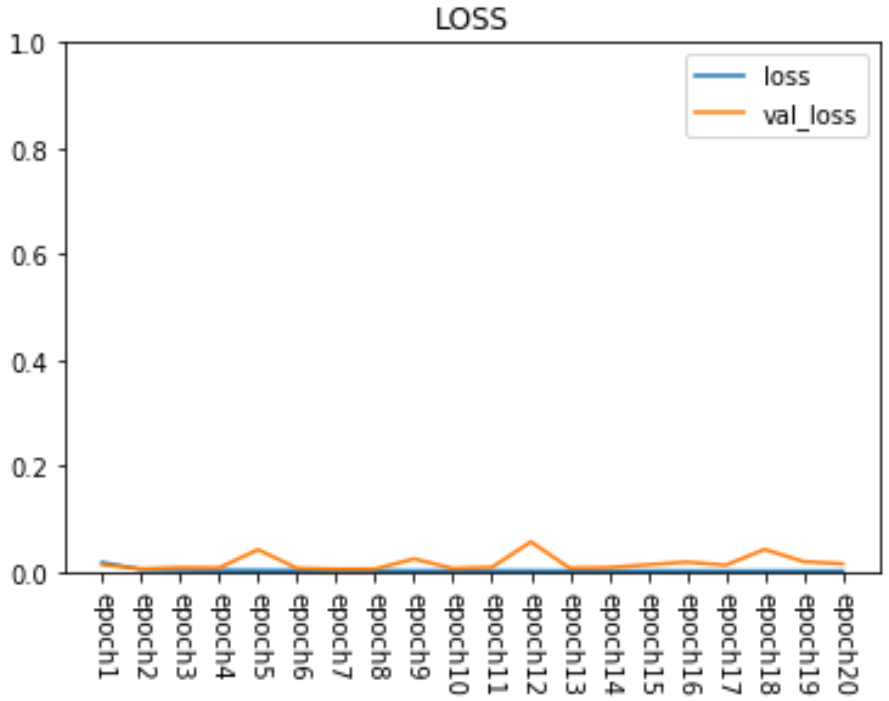
02 수행 내용

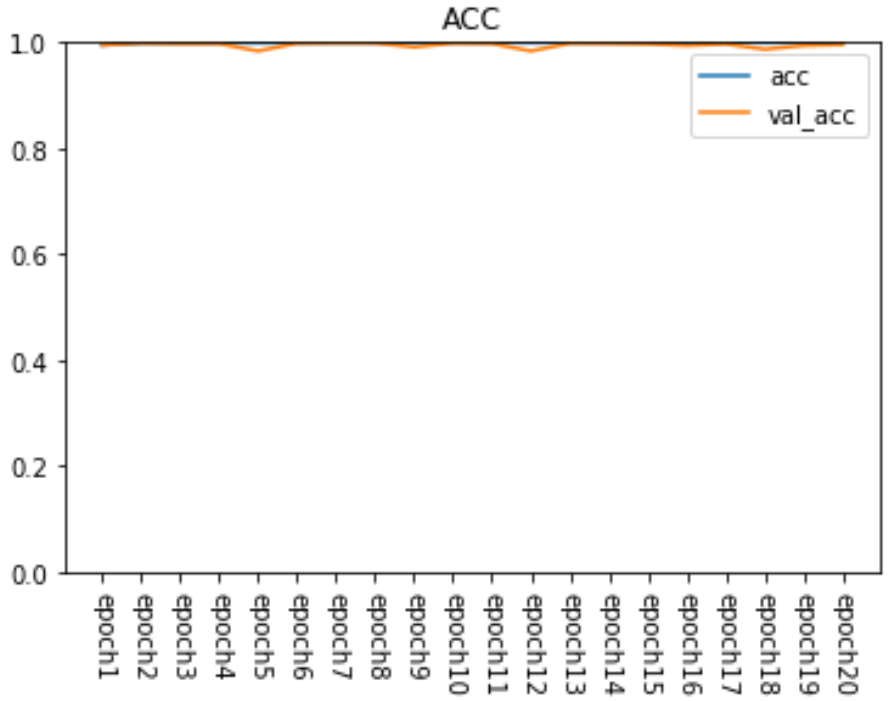
모델 [Pre_Now]



02 수행 내용

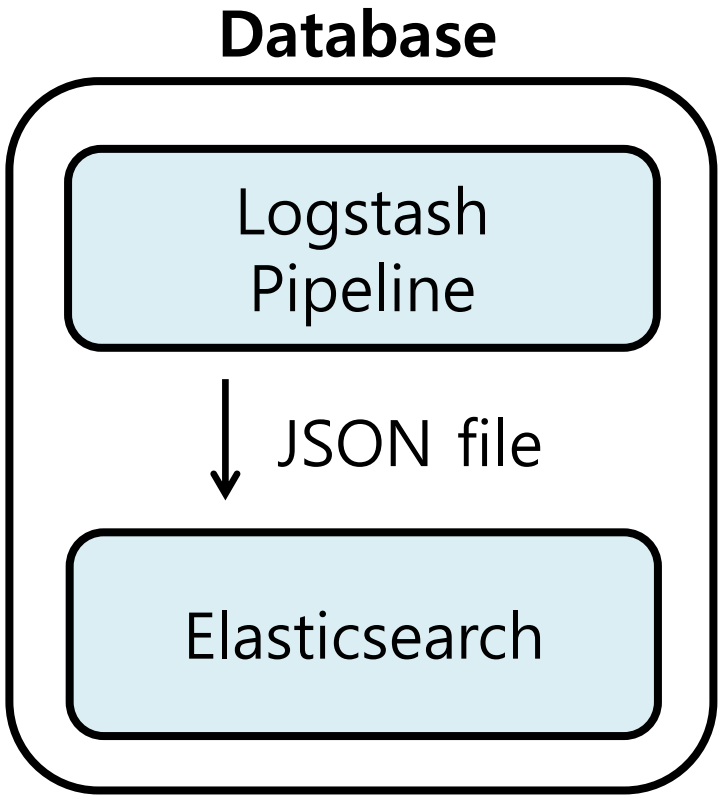
모델 [Pre_Now]





02 수행 내용

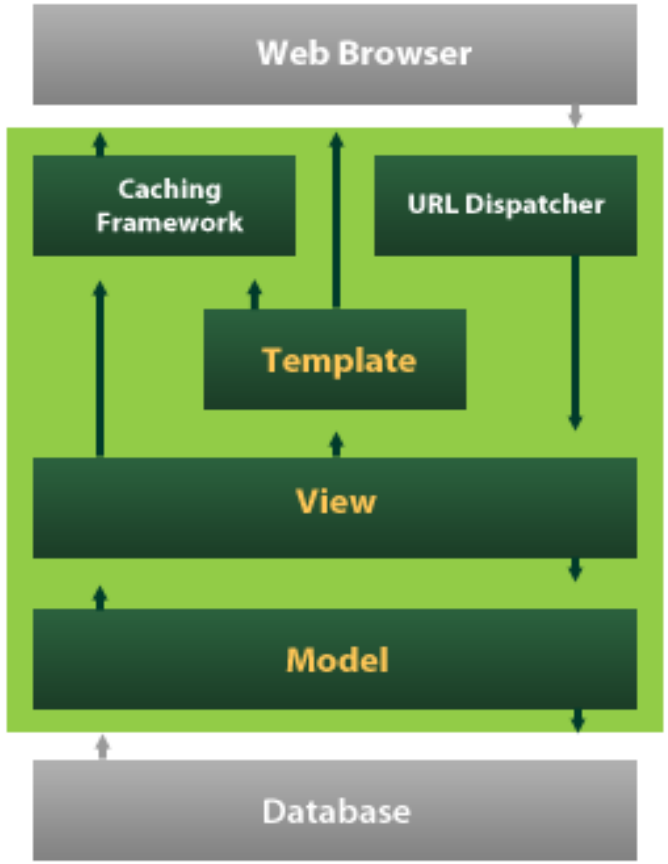
ELK



Kibana

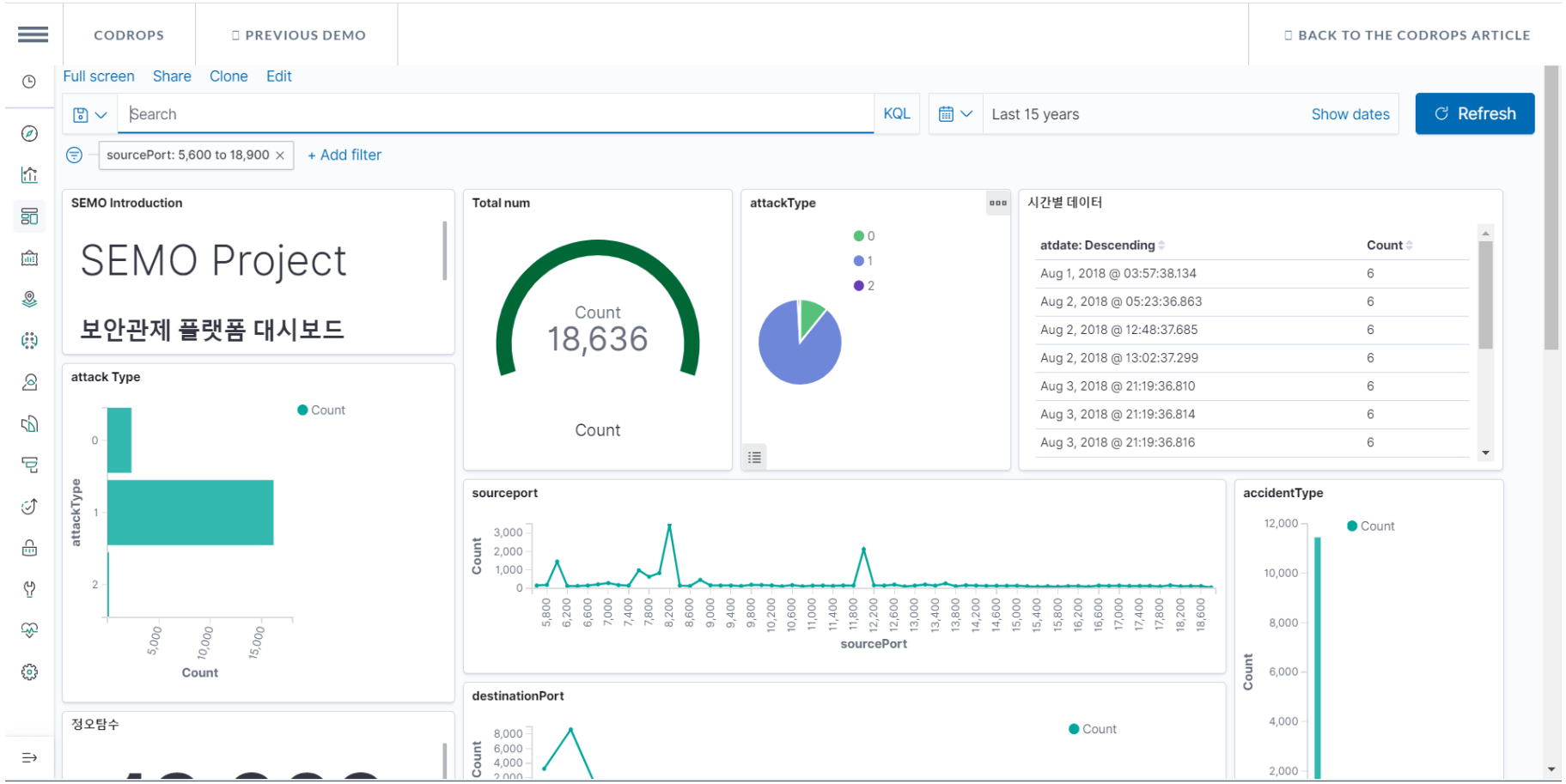
02 수행 내용

WEB - Server



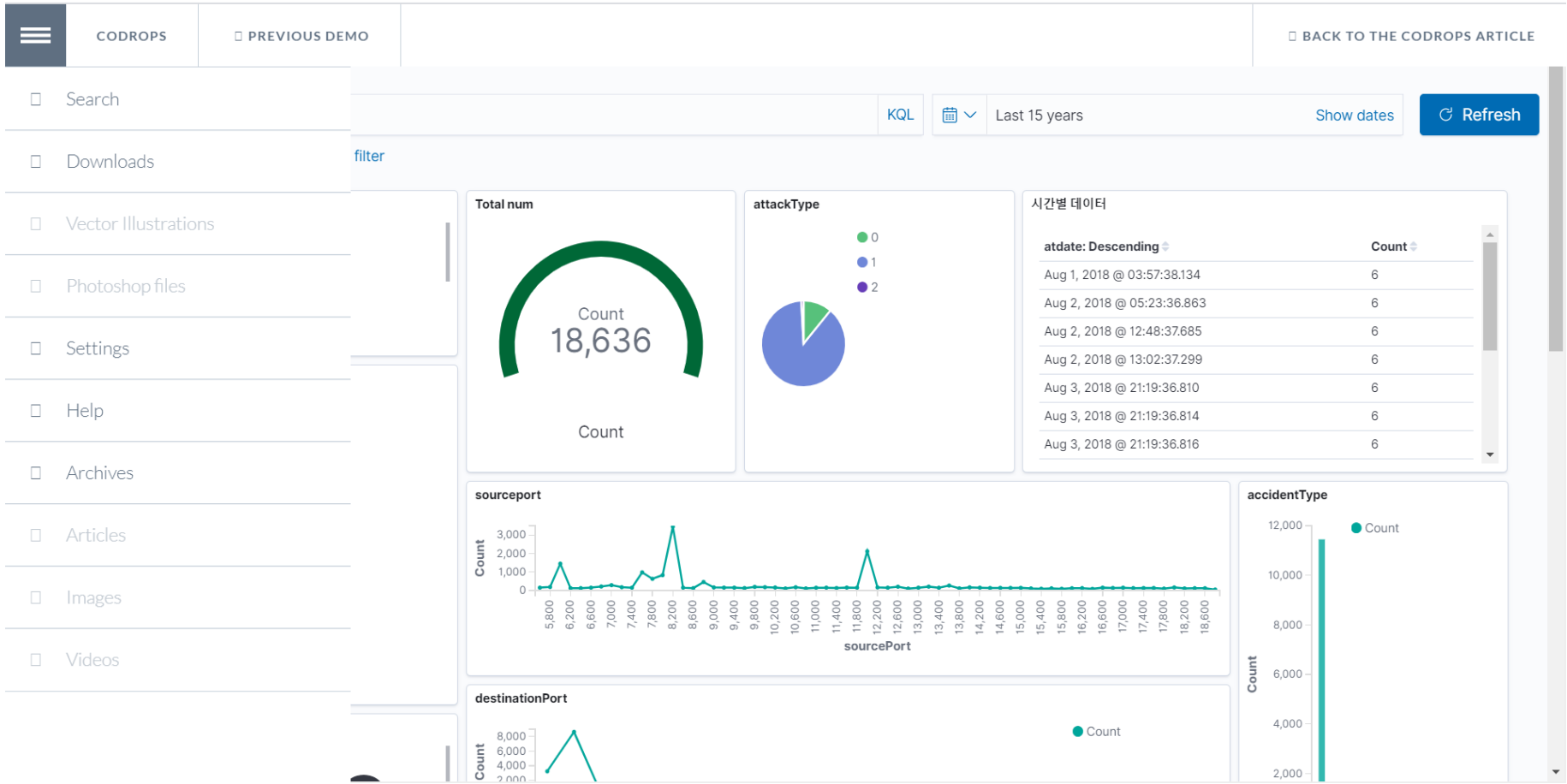
02 수행 내용

WEB – Front / ELK - Kibana



02 수행 내용

WEB – Front / ELK - Kibana

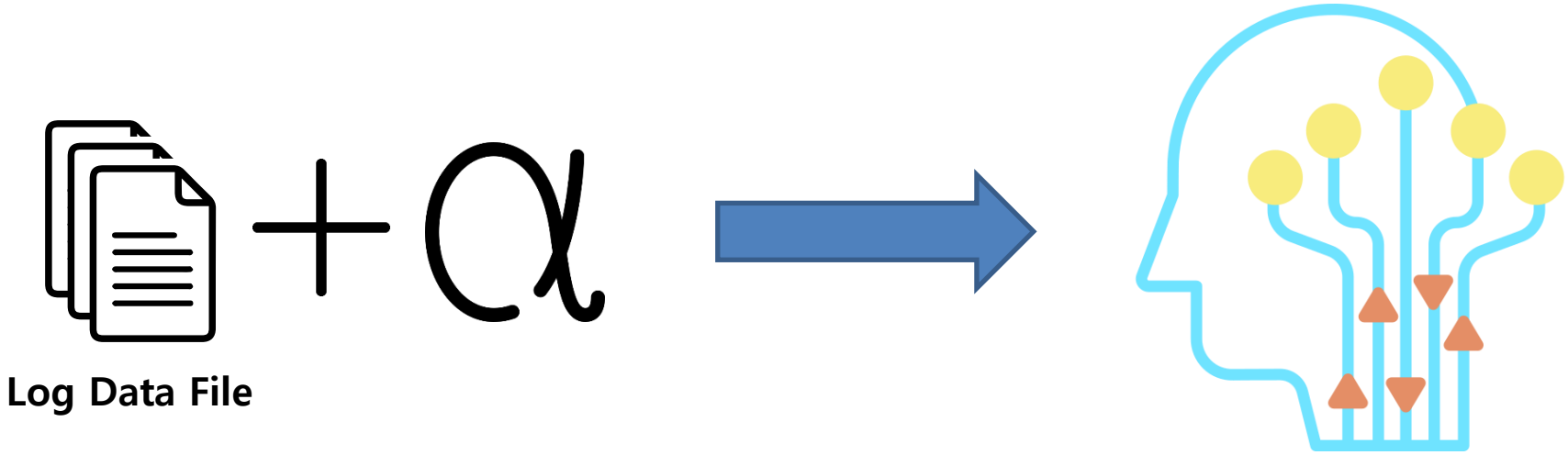


CONTENTS

SEMO : Security Monitoring Platform

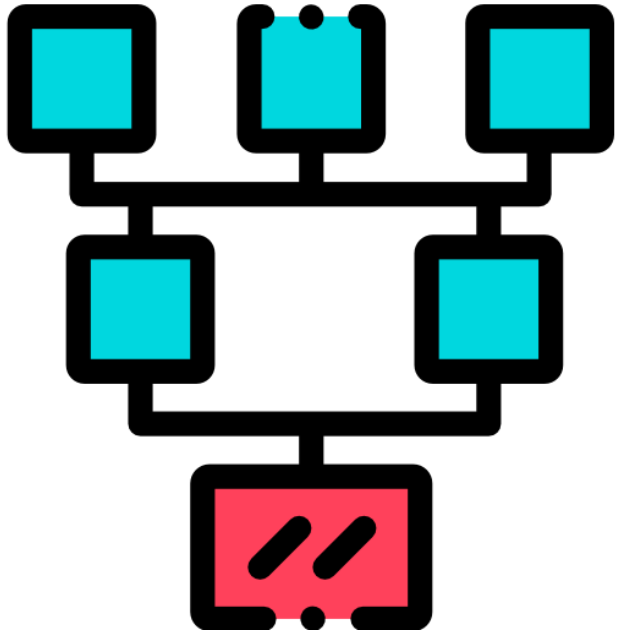
03 향후 계획

모델



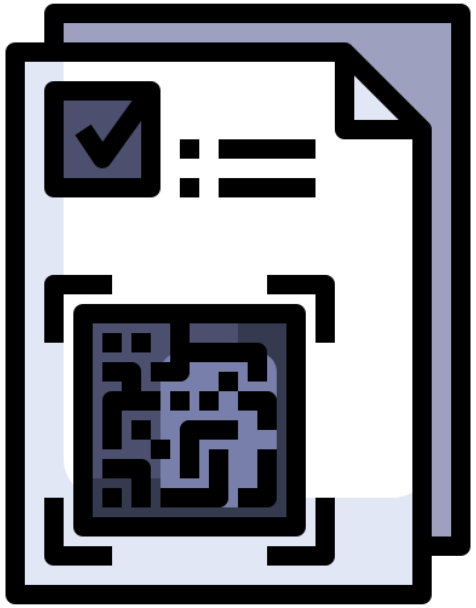
03 향후 계획

모델



03 향후 계획

ELK



03 향후 계획

WEB – Front

THANK YOU