



2020 Capstone Design

# SEMO : Security Monitoring Platform

7조 Do Mo!(Do Monitoring!)

# CONTENTS

01

---

프로젝트 소개

02

---

수행 내용

03

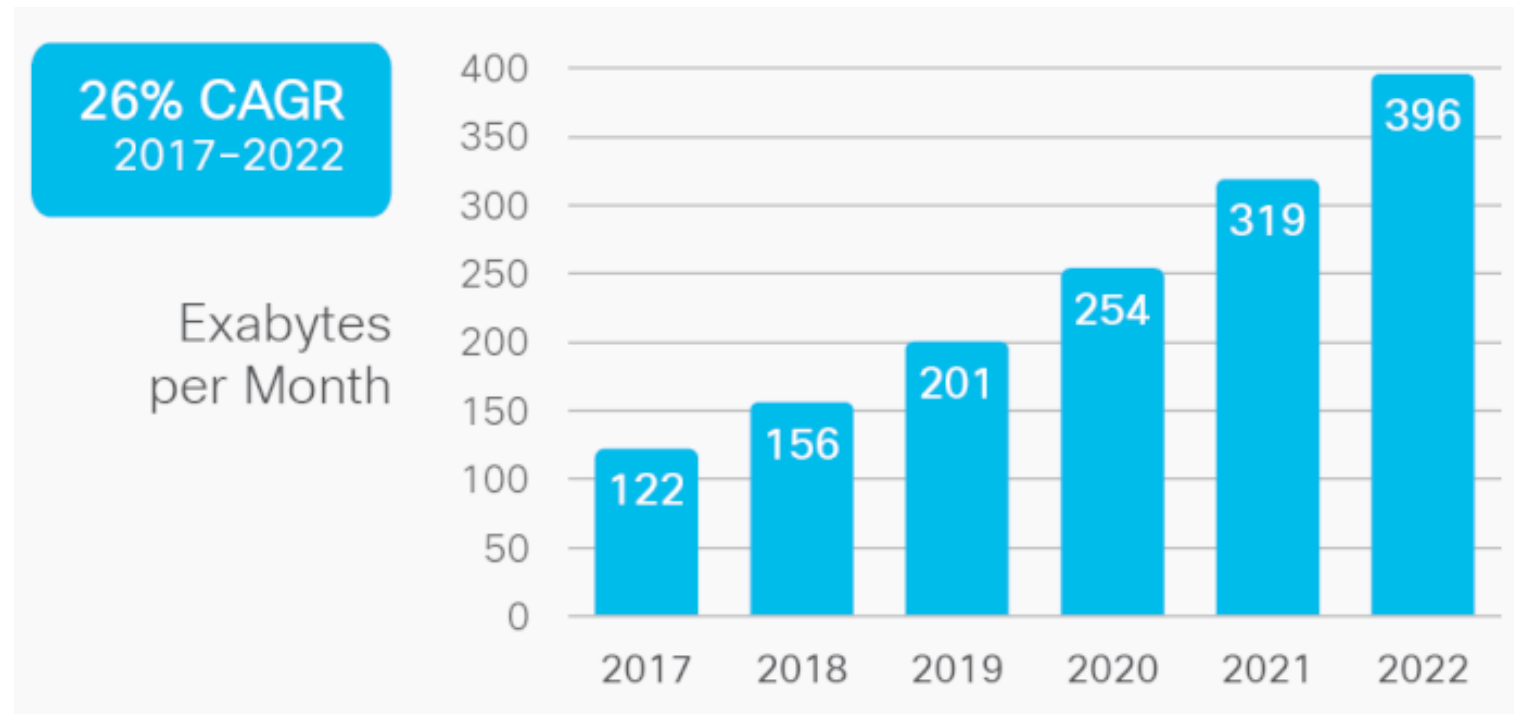
---

향후 계획

---

SEMO : Security Monitoring Platform

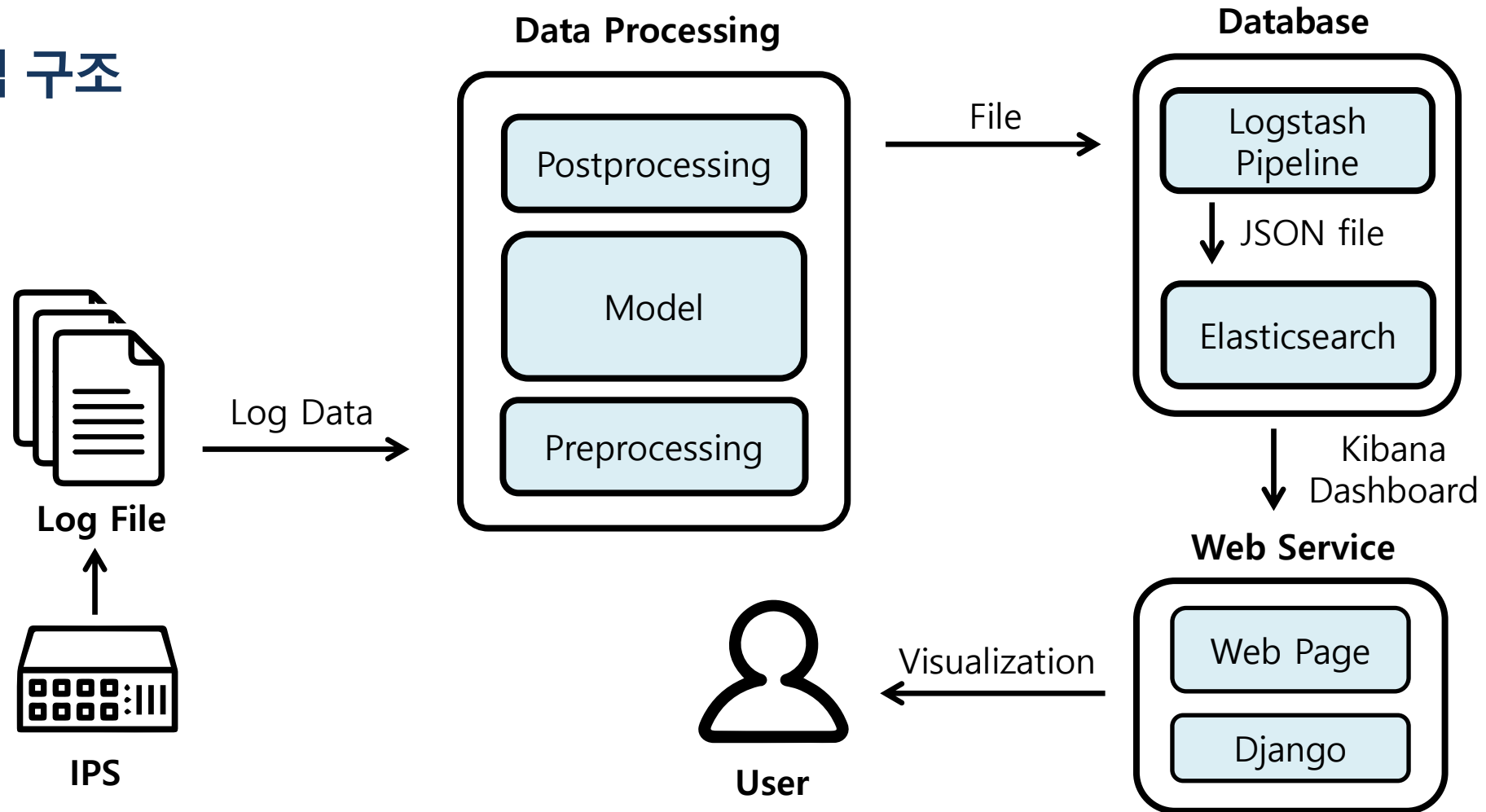
# 01 프로젝트 소개



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

01

---

프로젝트 소개

02

---

수행 내용

03

---

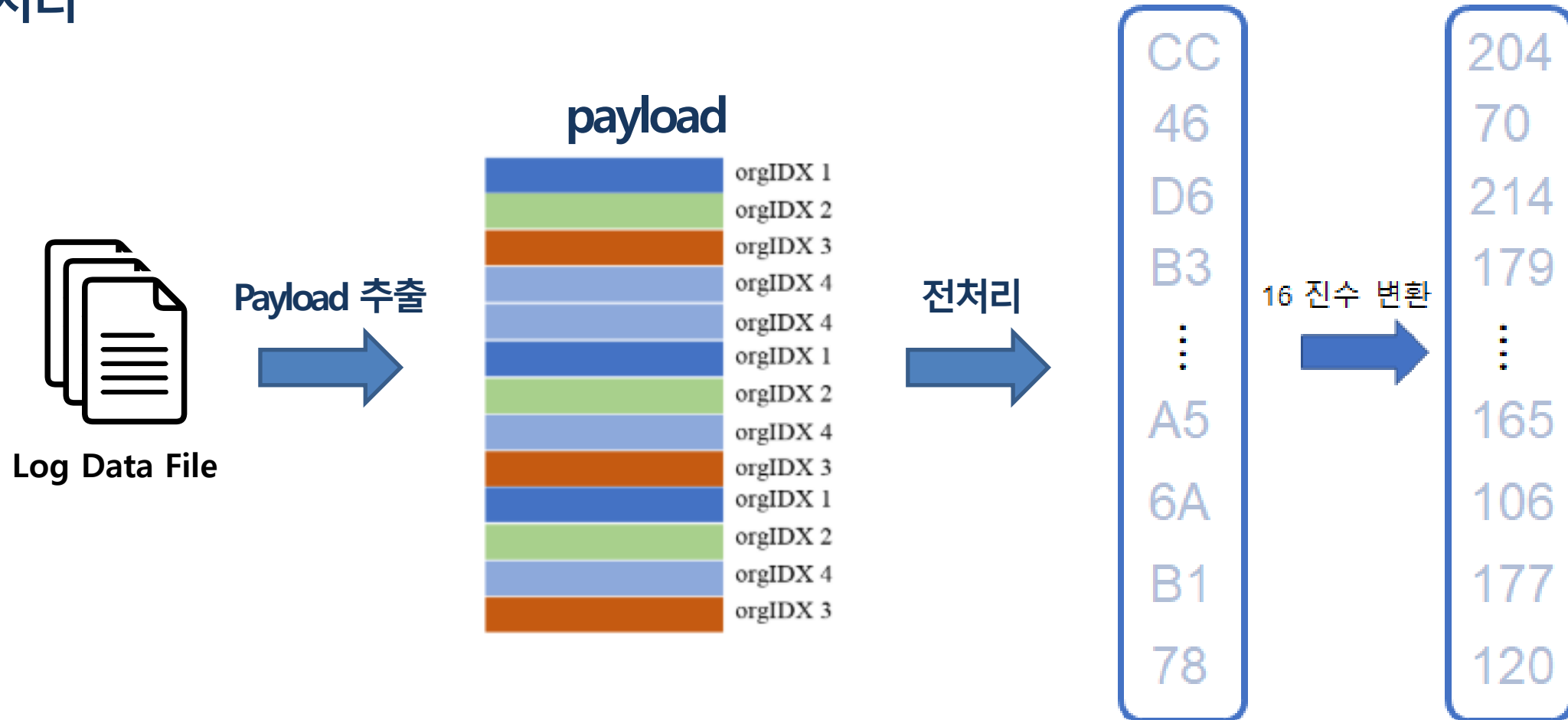
향후 계획

---

SEMO : Security Monitoring Platform

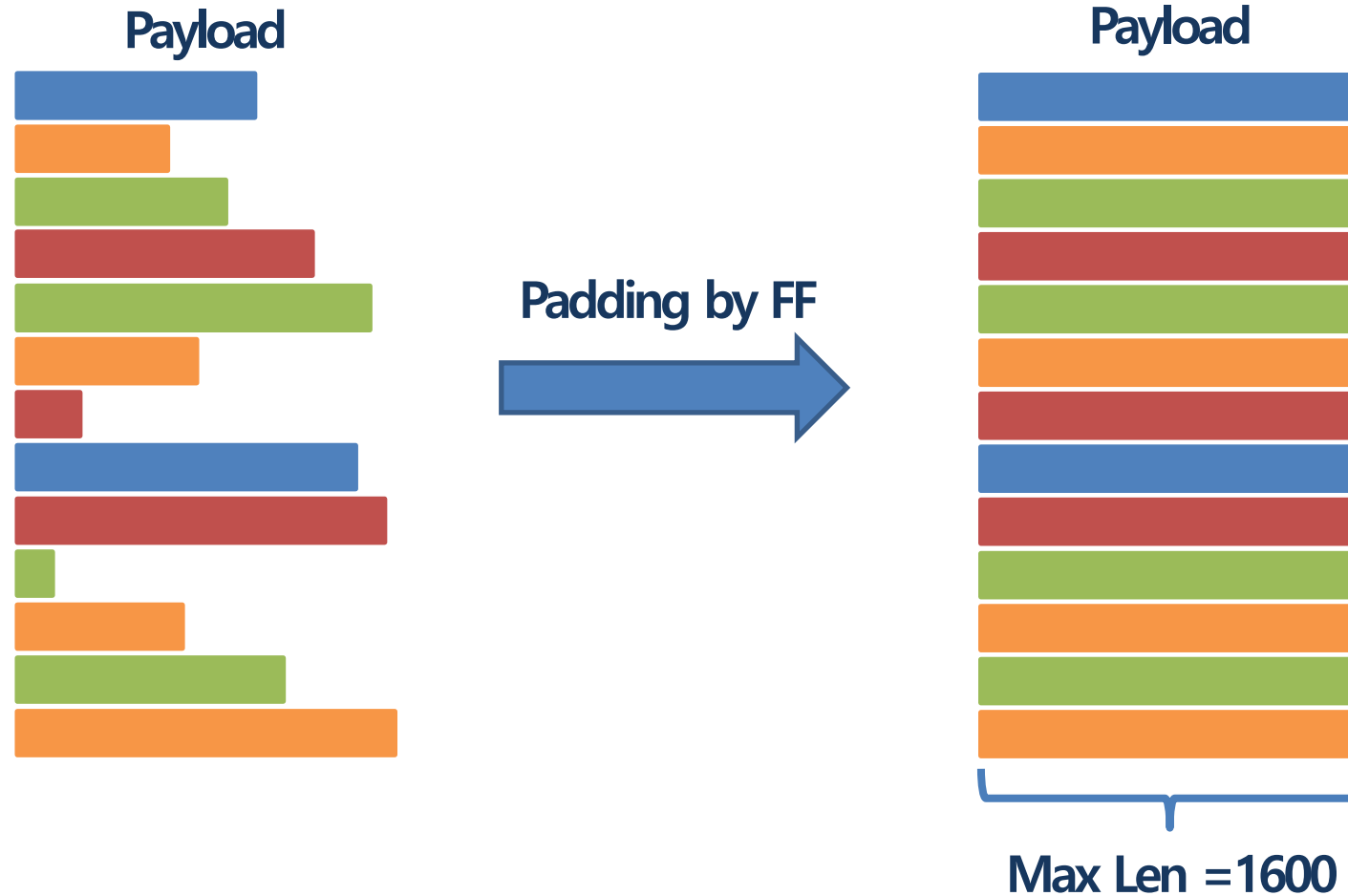
# 02 수행 내용

## 전처리



# 02 수행 내용

## | 전처리 [ Padding ]





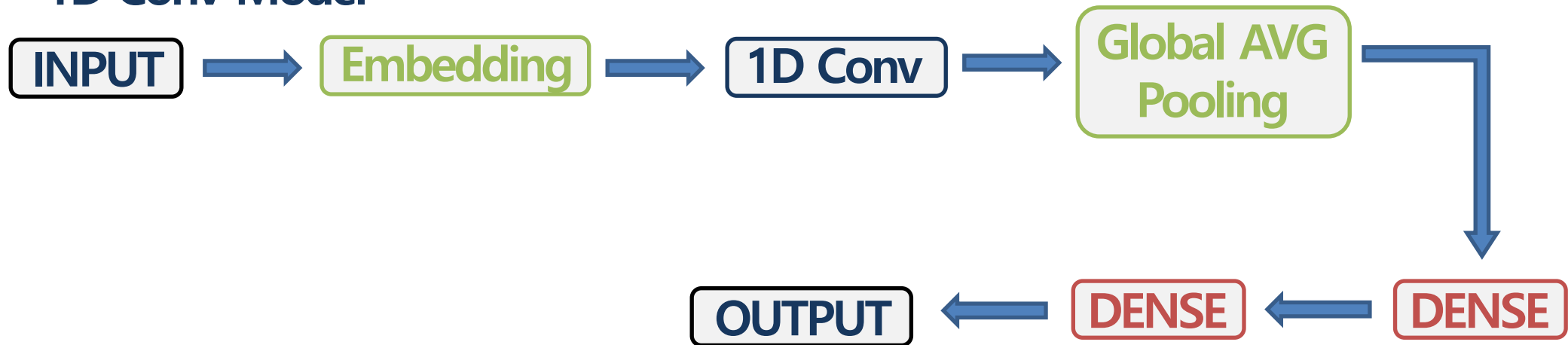
# 02 수행 내용

## 모델 선정

### LSTM Model

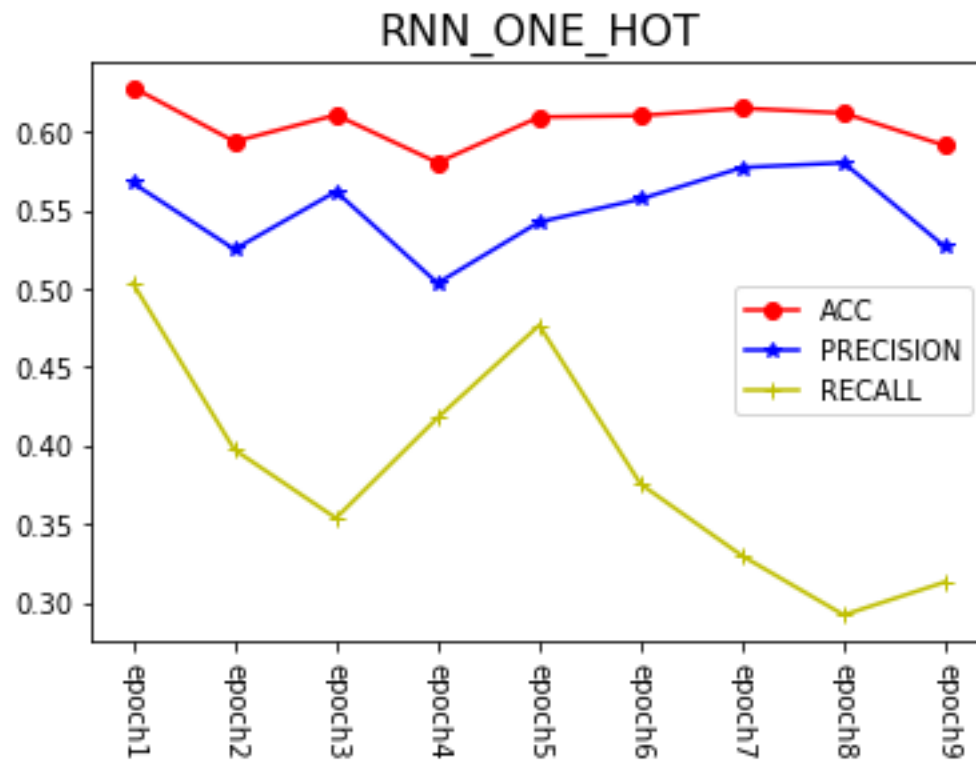
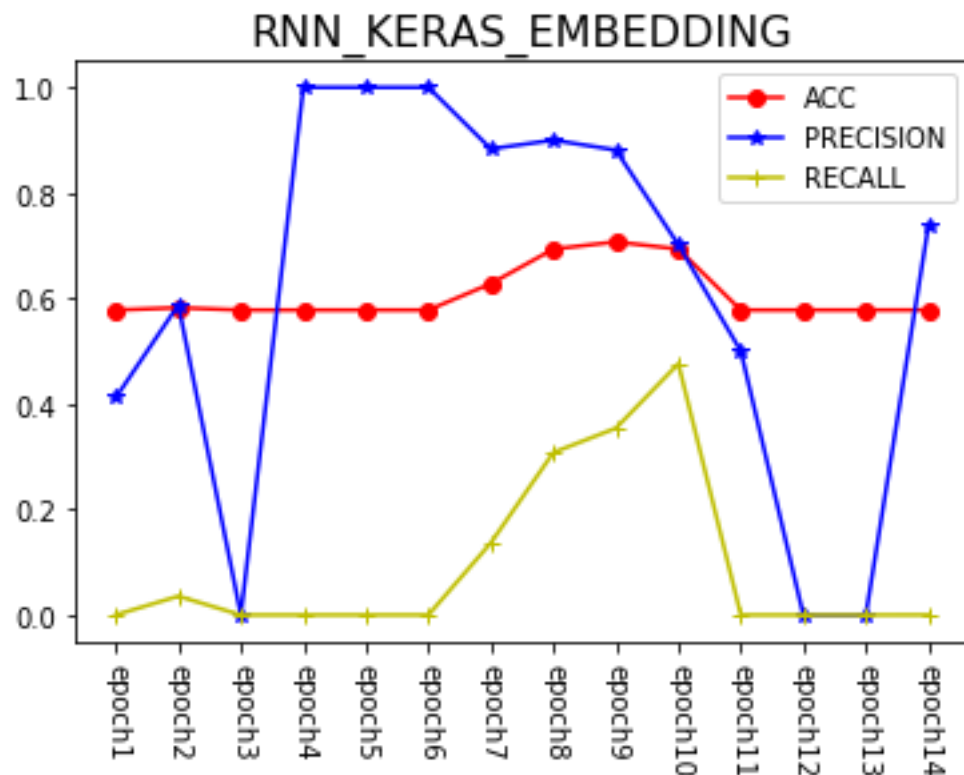


### 1D Conv Model



# 02 수행 내용

## 모델 선정



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

# 02 수행 내용

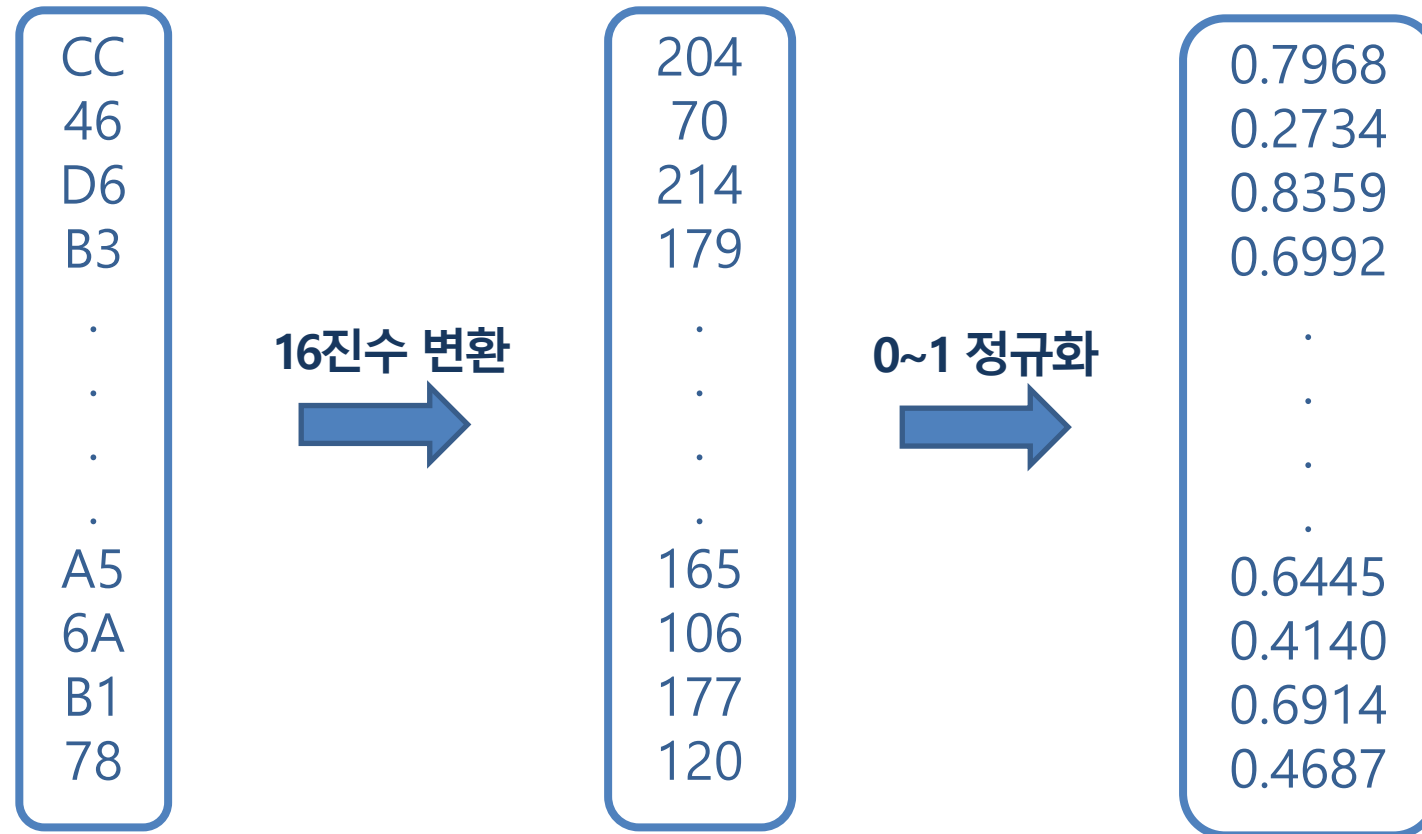
## | 1D Conv

### 임베딩 중요성에 관한 실험

1. 0~1로 정규화
2. One-Hot encoding
3. Keras Embedding layer

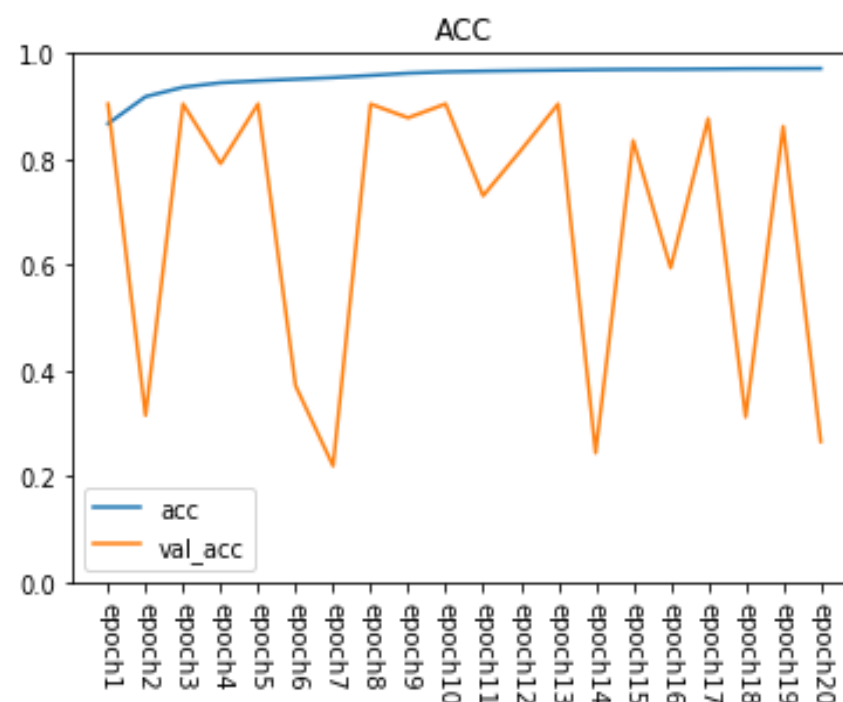
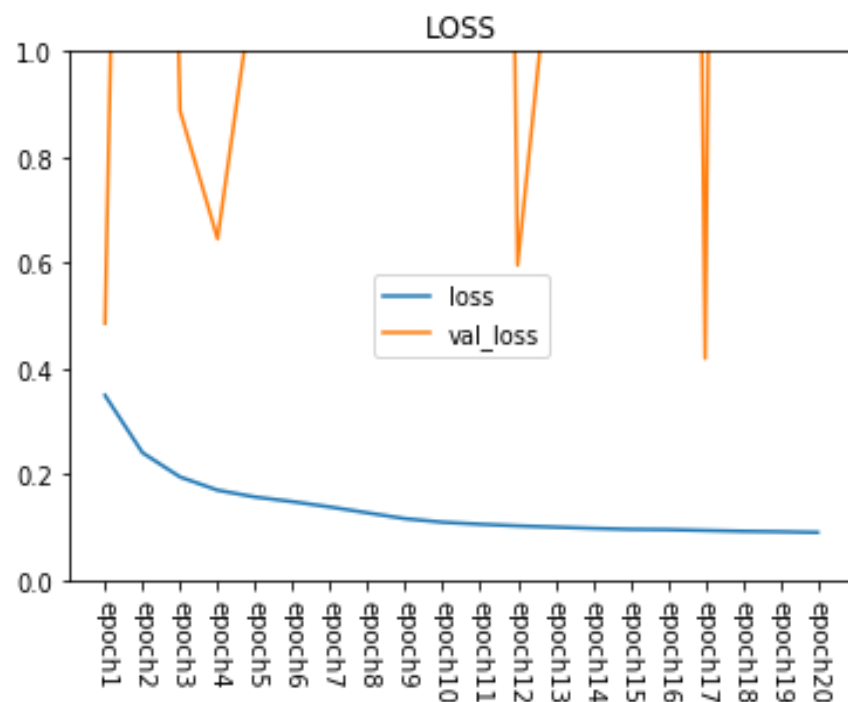
# 02 수행 내용

## | 1D Conv [0~1 정규화]



# 02 수행 내용

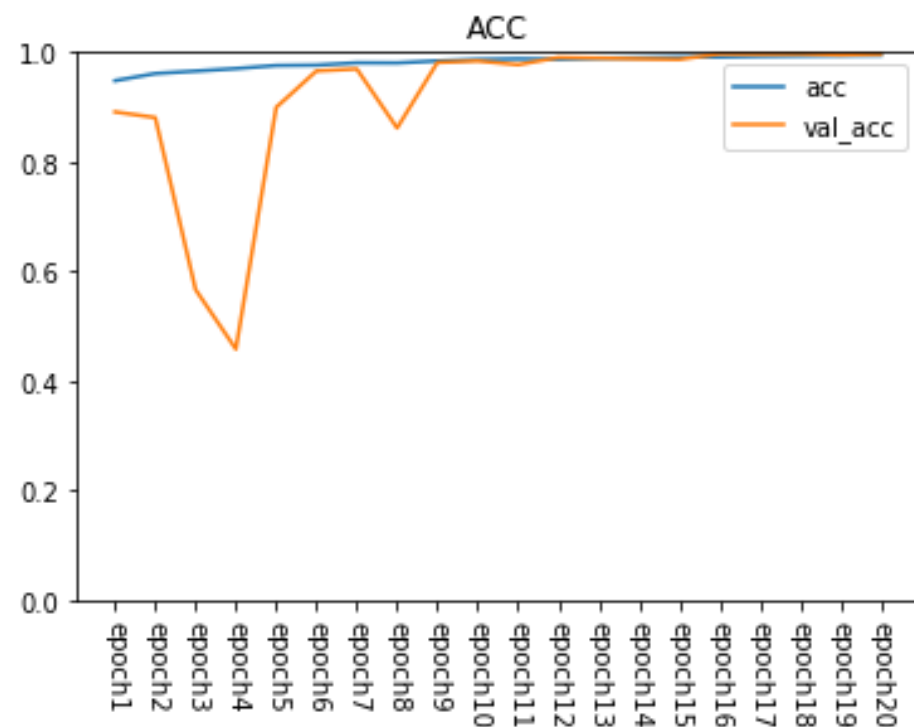
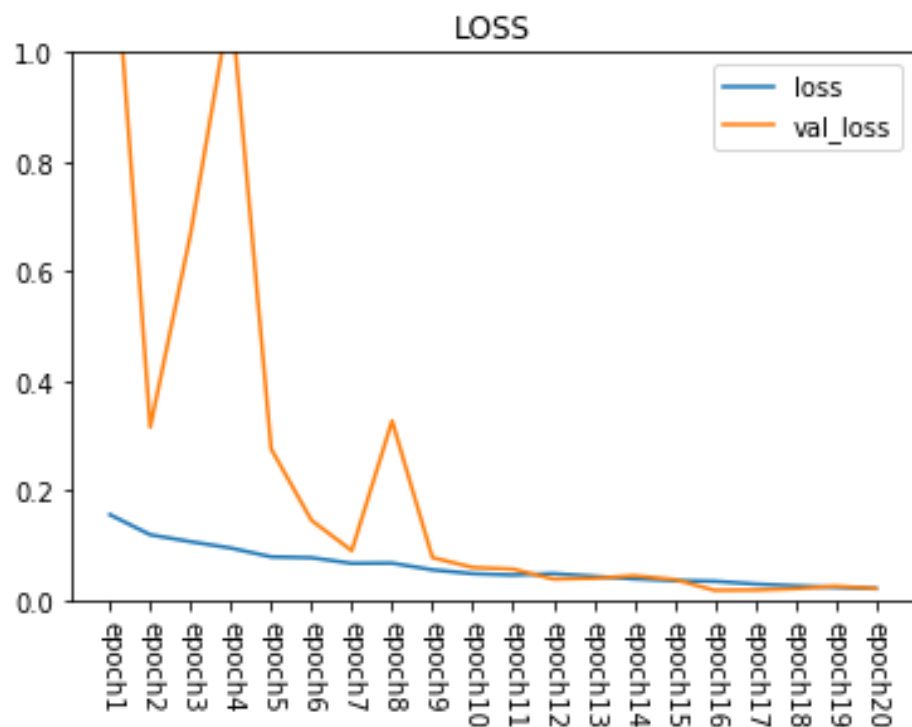
## 1D Conv [0~1 정규화]



➔ Validation Loss 와 Accuracy가 불안정

# 02 수행 내용

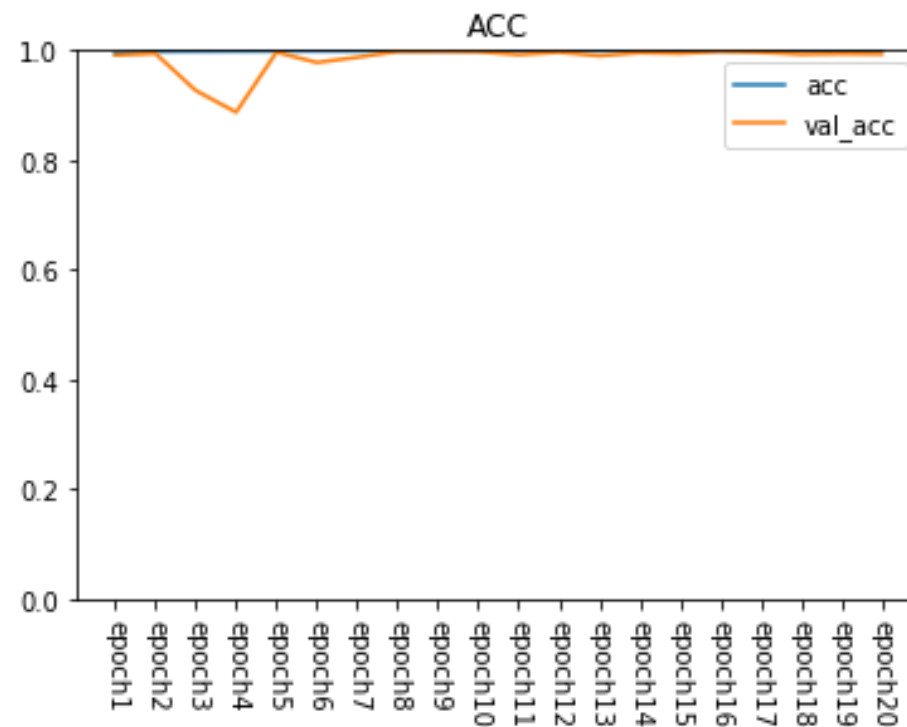
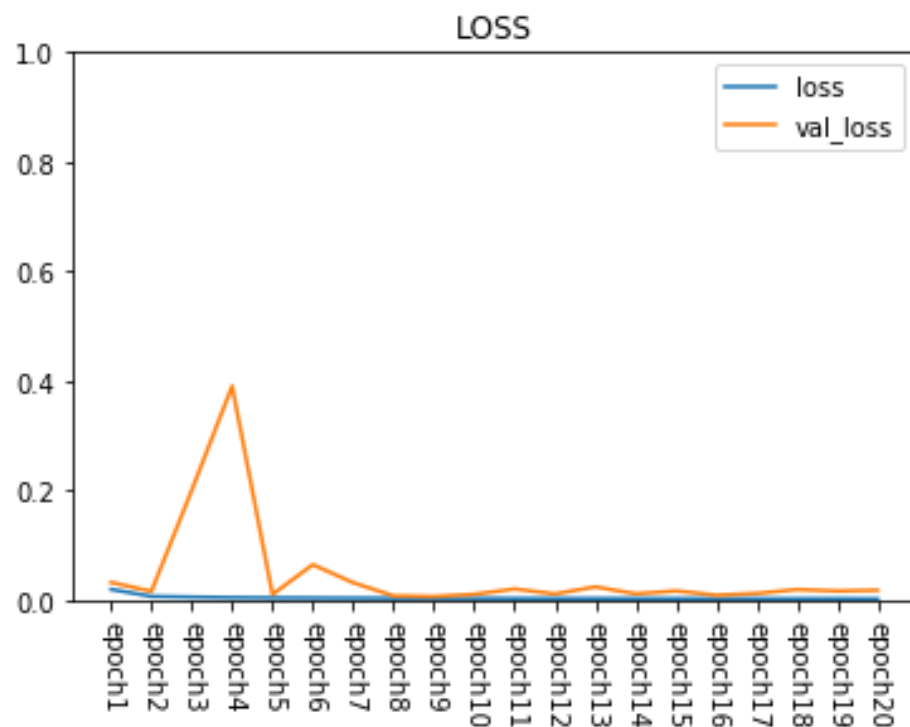
## 1D Conv [one-hot]



➔ Train과 Validation이 비교적 안정적이나 무거운 구조

# 02 수행 내용

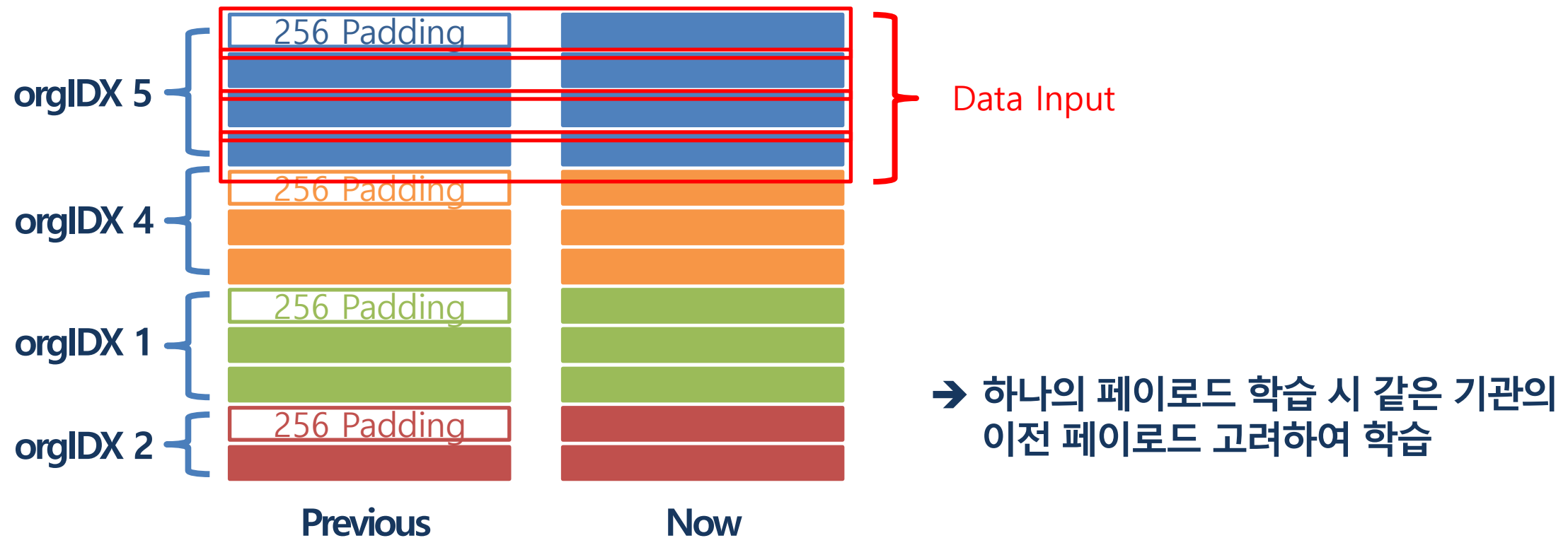
## 1D Conv [keras embedding]



➔ Train Loss가 더욱 빨리 수렴

# 02 수행 내용

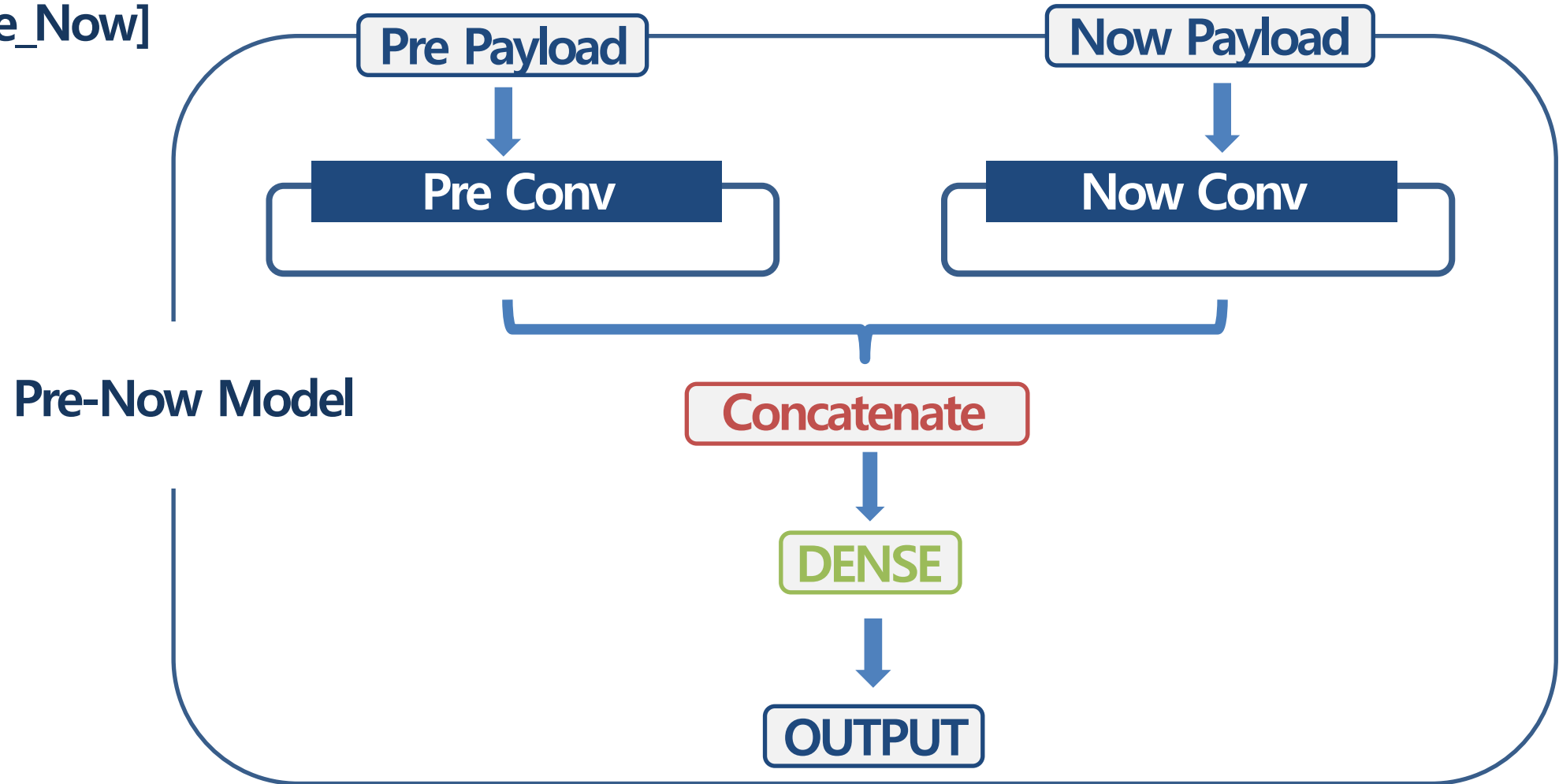
## 전처리 [Pre\_Now]





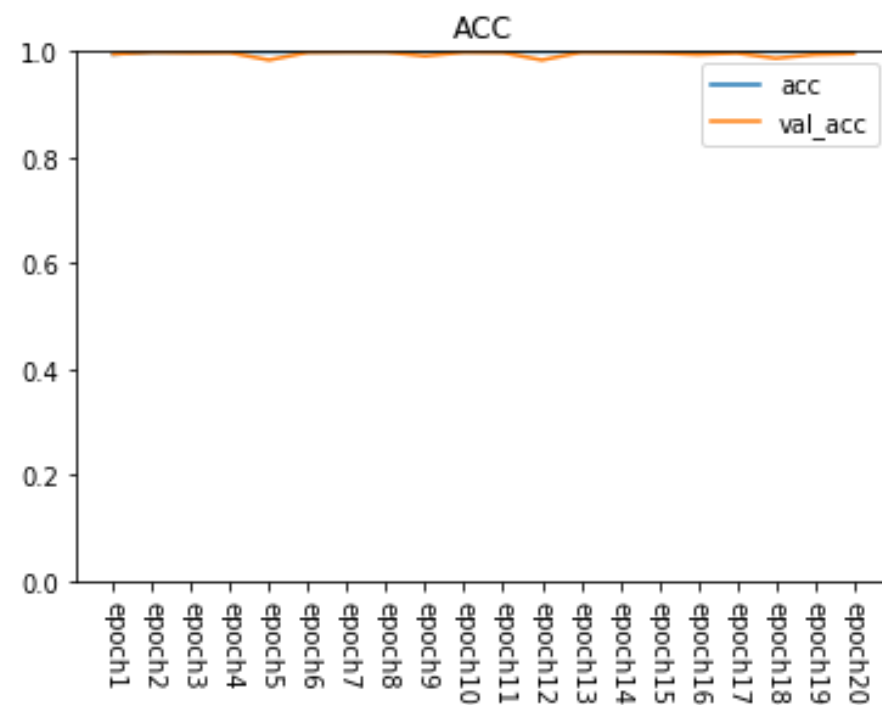
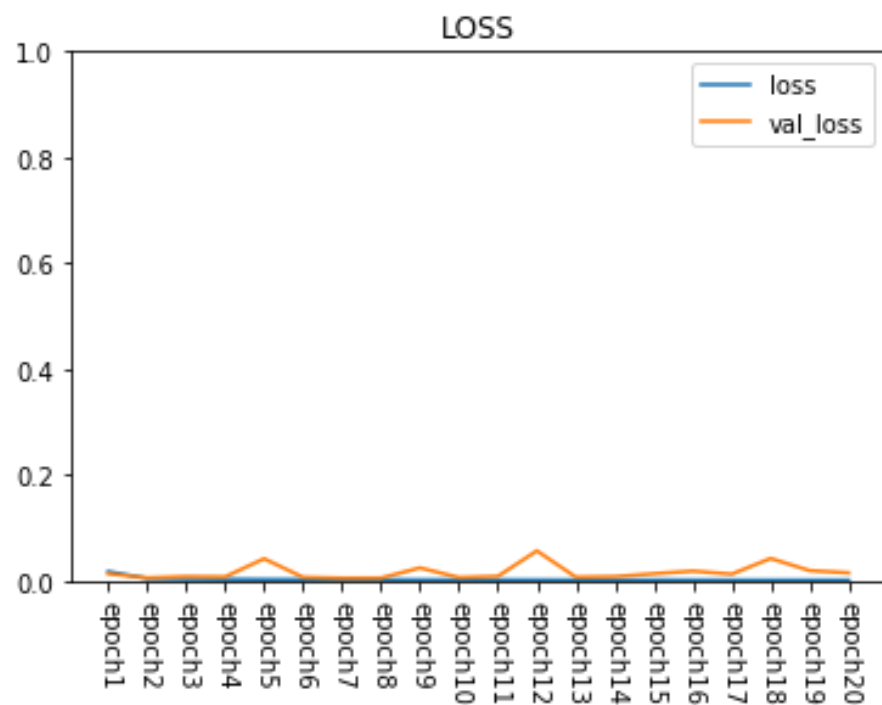
# 02 수행 내용

모델 [Pre\_Now]



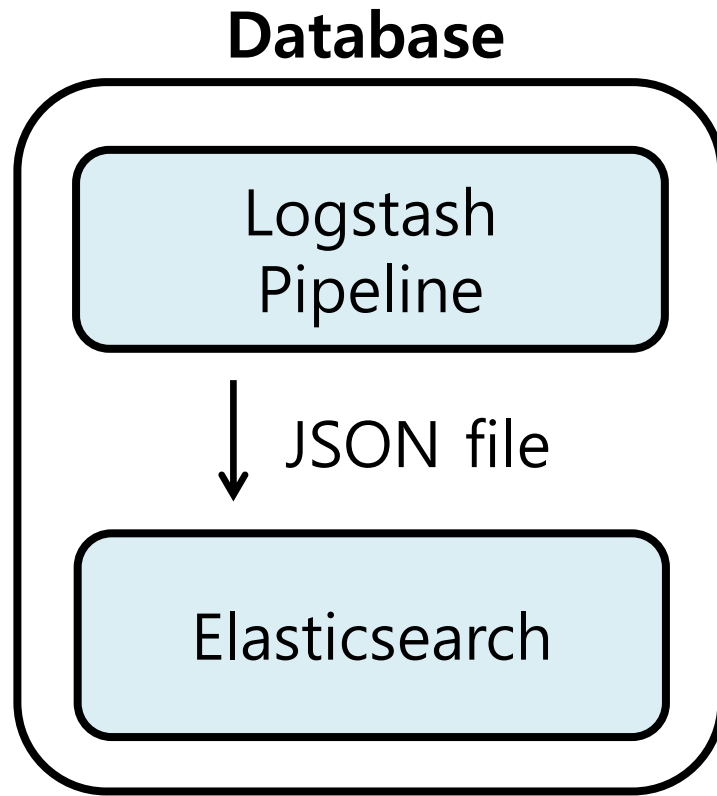
# 02 수행 내용

## 모델 [Pre\_Now]



# 02 수행 내용

## | ELK

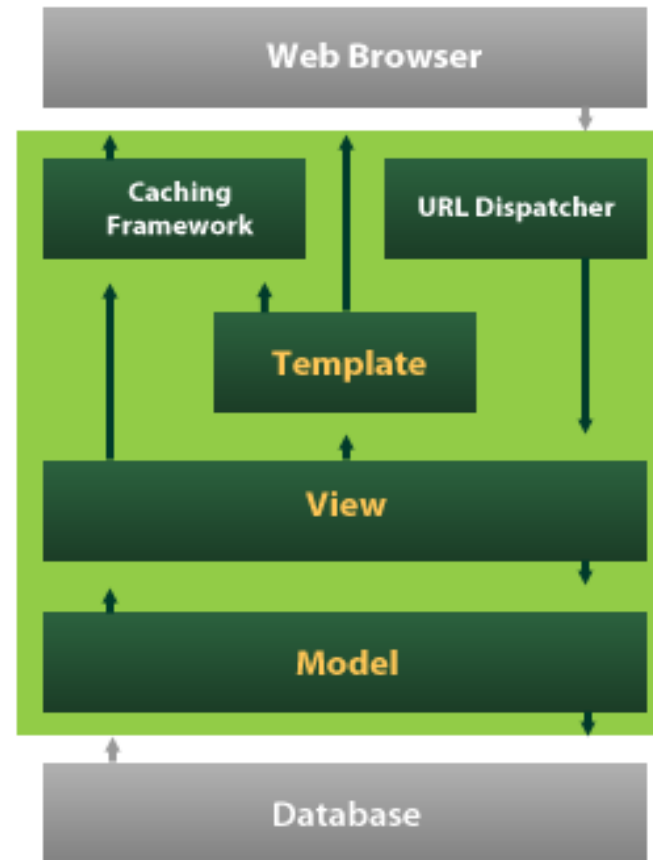


## Kibana

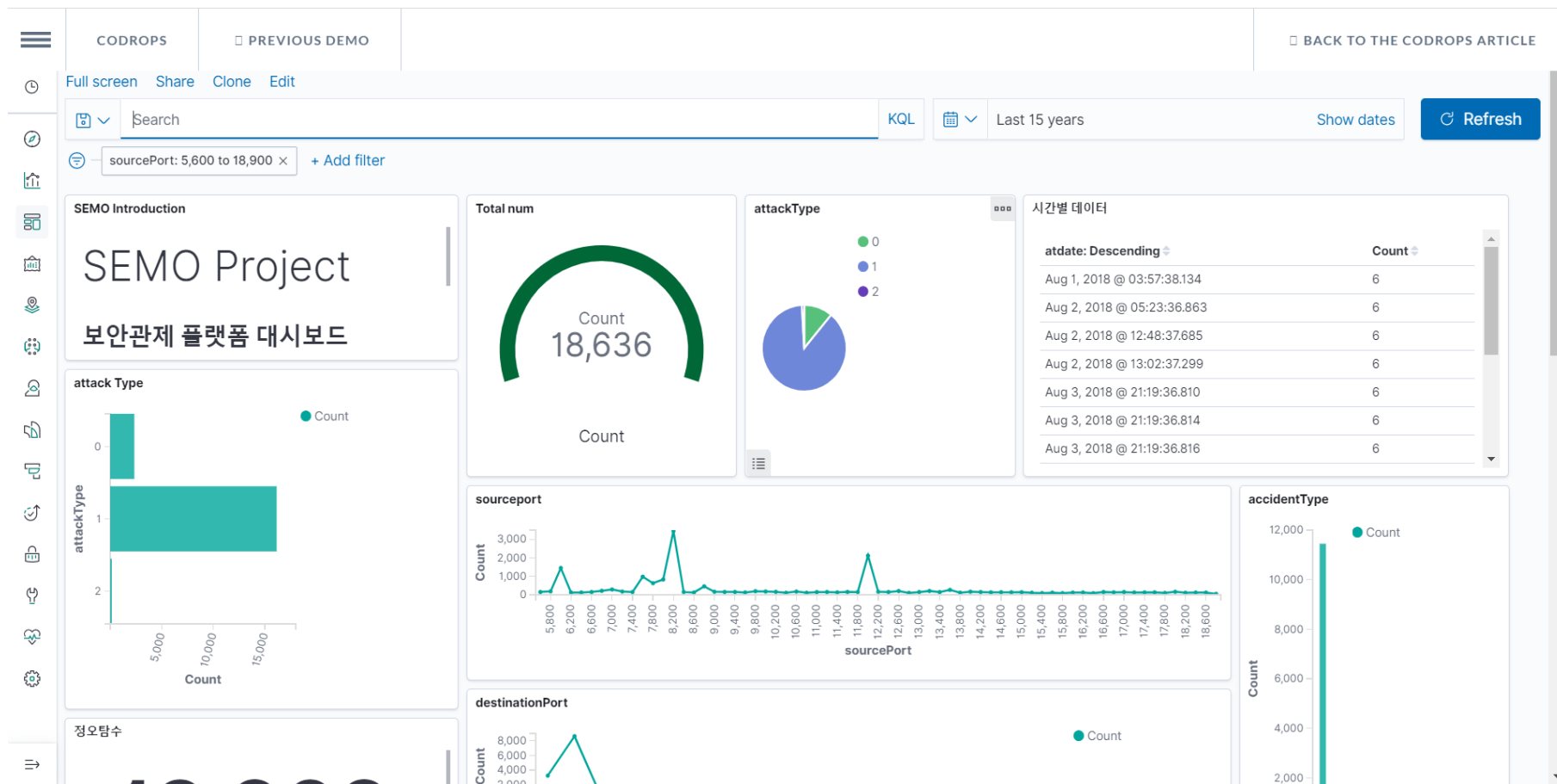


# 02 수행 내용

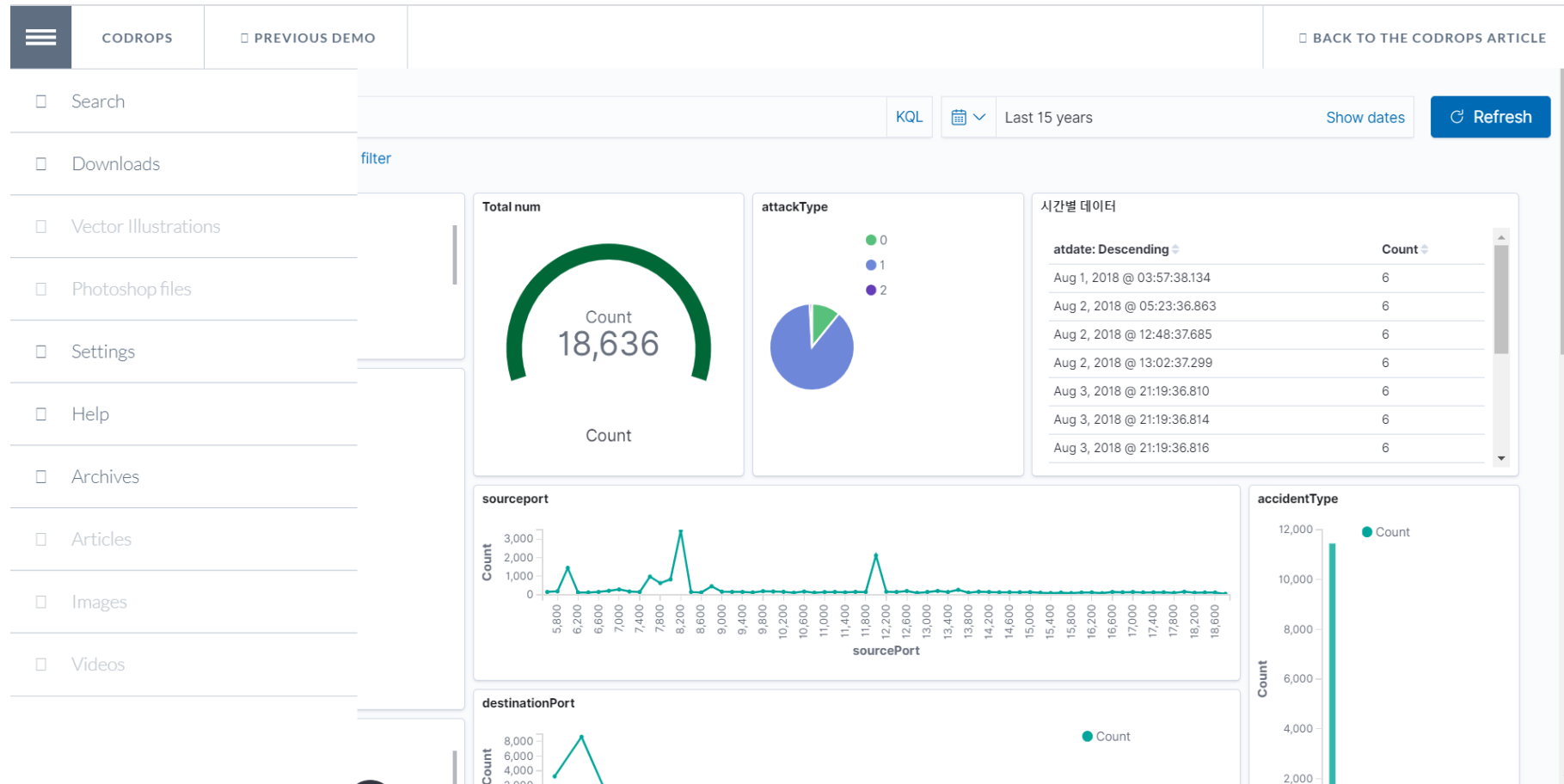
## WEB - Server



## WEB – Front / ELK - Kibana



## WEB – Front / ELK - Kibana



# CONTENTS

01

---

프로젝트 소개

02

---

수행 내용

03

---

향후 계획

---

SEMO : Security Monitoring Platform

# 03 향후 계획

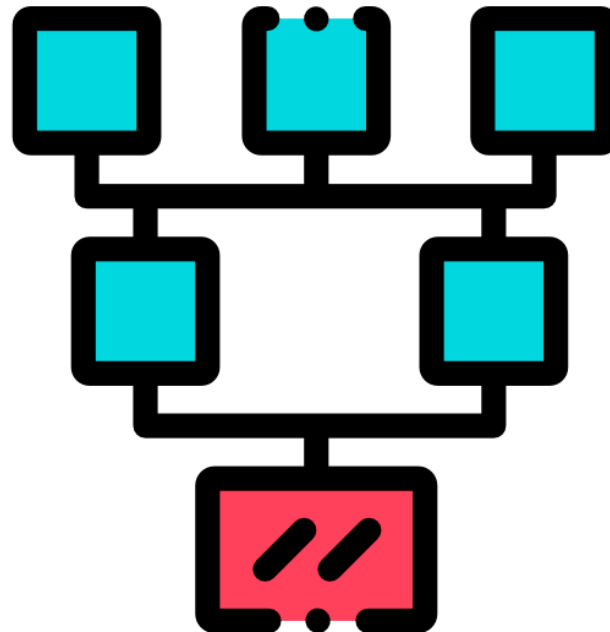
## | 모델





# 03 향후 계획

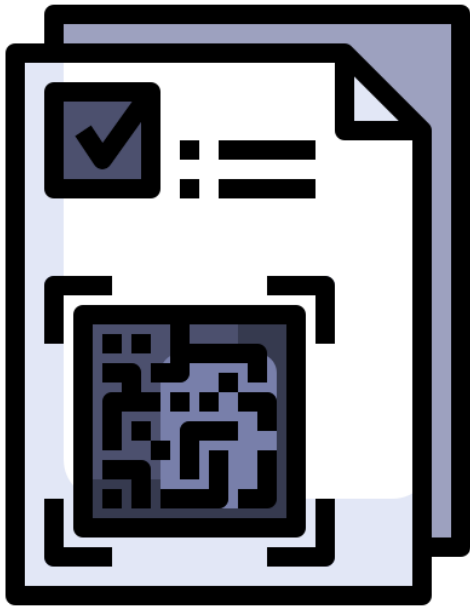
## | 모델



# 03

## 향후 계획

| ELK



# 03 향후 계획

## WEB – Front



**THANK  
YOU**