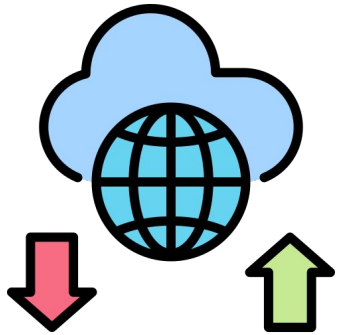
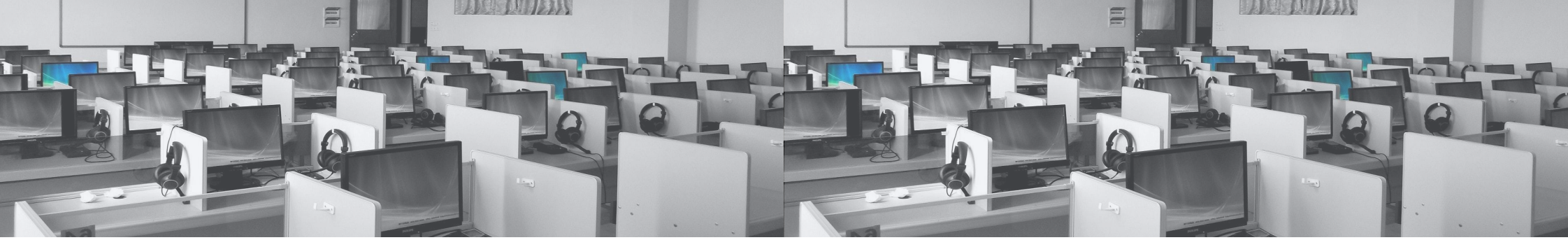
NAVER Cloud

# 2024년도 모의
# 행정·공공기관 정보시스템
# 클라우드 전환·통합 사업

## 구축결과 발표 – 3팀



T&T 으뜸정보기술



# C/O/N/T/E/N/T

# 1

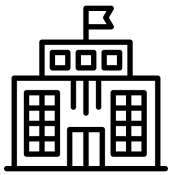
# 프로젝트 소개

1. 프로젝트 목적 및 범위
2. 수행 전략

# 1. 프로젝트 목적 및 범위

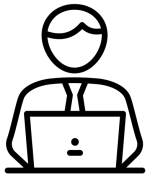
정부, 공공기관은 일반 기업보다 더 많은 공무원과 시민들이 사용하는 내부, 외부 웹서비스와 앱들이 있습니다. 때문에 공공부문에서도 기업처럼 클라우드를 통한 서비스 효율화와 비용 절감, 유연한 서비스 개발의 필요성이 높아지고 있습니다.

## 행정·공공기관 정보시스템 클라우드 전환·통합



공공기관

- IT 인프라 및 유지 관리에 대한 비용 절감
- 필요에 따라 리소스를 조절하여 비용 효율성 증가
- 효율적인 기관 내 다양한 프로세스 및 업무 관리
- 체계적인 데이터 보안 및 백업 관리
- 타 기관 협업 용이 및 효율적인 정보 공유 및 커뮤니케이션



공무원

- 업무 효율성 증가 및 업무 처리시간 단축
- 인공지능, 빅데이터 등 첨단 기술을 도입하여 업무 자동화 및 혁신 촉진
- 새로운 기술 및 솔루션 습득 및 전문성 향상

시민

- 공공기관의 더 나은 품질의 서비스 제공으로 만족도 향상
- 공공기관의 업무 투명성이 높아져 시민들의 신뢰성 증가
- 공공기관과 소통하고 참여할 수 있는 채널 다각화

# 1. 프로젝트 목적 및 범위

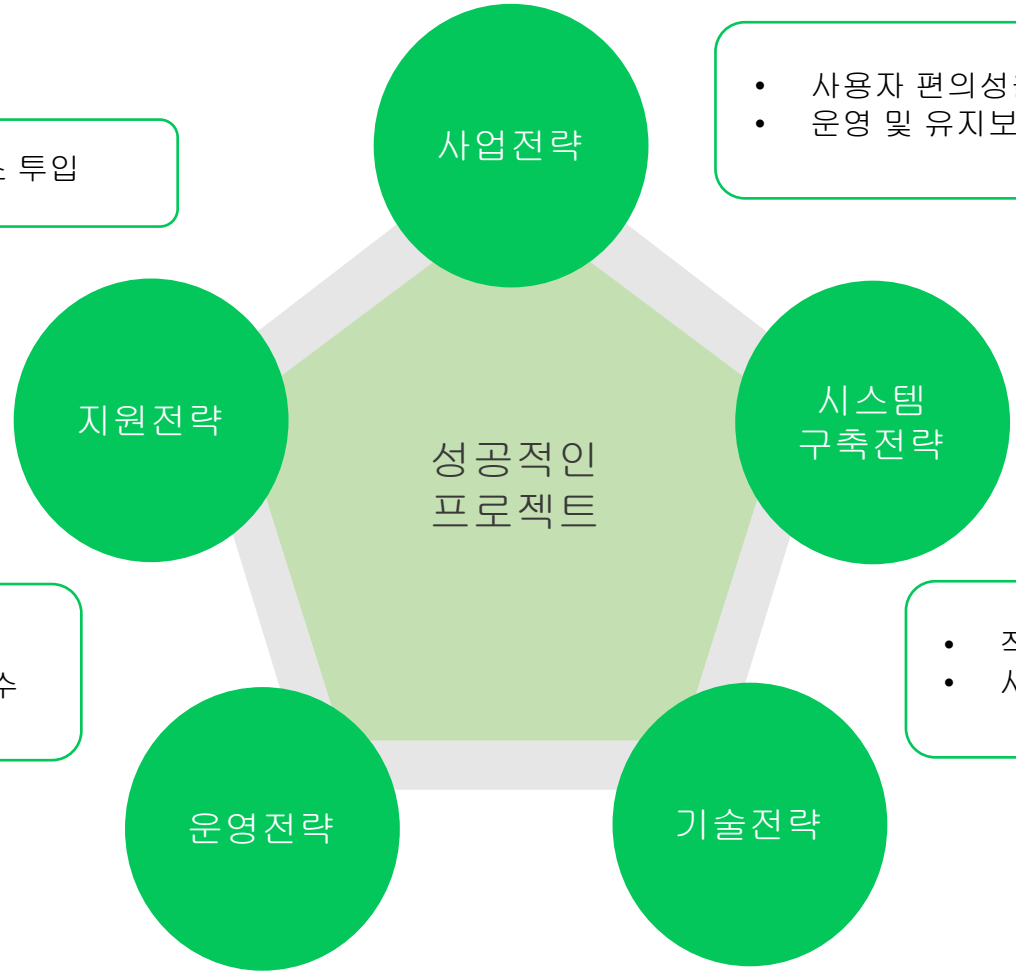
| | |
|---|---|
| 프로젝트 기간 | 2024. 01. 16. ~ 2024. 01. 19. |
| 대상 업무 | **천문우주지식정보시스템** 클라우드 서비스 전환 (Naver Cloud) |
| 주요구성 사항 | 천문 관련 정보(해달출몰시각, 음양력, 태양 고도각 등) 제공 및 티커 서비스 신청 |

## 프로젝트 일정

| | |
|---|---|
| 2024. 1. 16 | 서비스 환경 분석, 아키텍처 설계, 클라우드 구축 계획 수립 |
| 2024. 1. 17 | 전환 환경 구성, CSP 환경 구성, 보안 및 관제 환경 구성 |
| 2024. 1. 18 | 데이터 이관, 클라우드 구축 결과 보고 |
| 2024. 1. 19 | 성능 테스트, 취약점 점검, 서비스 전환 |

NAVER CLOUD PLATFORM

# 2. 수행 전략




- 사용자 편의성을 고려한 시스템 구축
- 운영 및 유지보수를 통한 체계적인 기술 이전

- 적용 기능 기술 분석 및 적극적 활용
- 시스템 호환성 및 활용도 고려

- DB 구축 능력 확대
- 소프트웨어 개발 방법론을 적용한 시스템 구축

- 비상연락 체계 유지
- 시스템 운영 담당자의 절차 준수

- 전문 기술자 적재적소 투입

# 2

# 프로젝트 준비 부문

1. 팀 조직 구성현황
2. 프로젝트 구축 순서

NAVER CLOUD PLATFORM

# 1. 팀 조직 구성

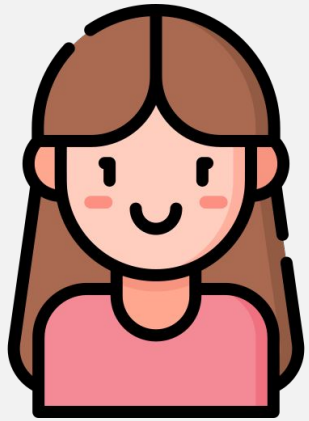
**Team Member**

임 은 채

**Team Leader**

구 동 한

**Network**



문 지 은

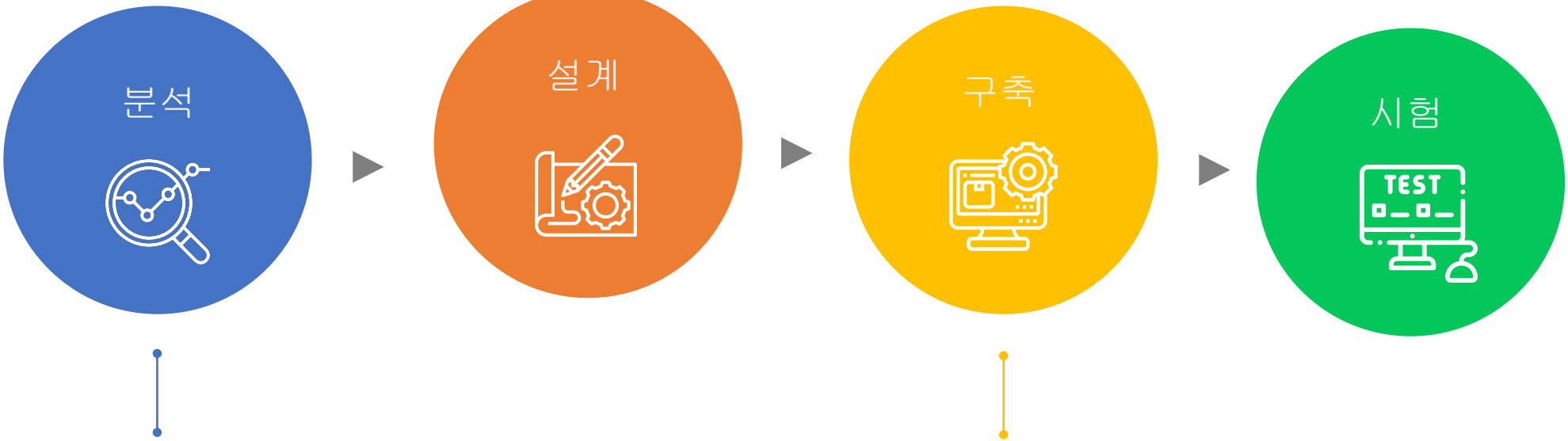
**Operate**

정 수 호

**Infra**

NAVER CLOUD PLATFORM

# 2. 프로젝트 구축 순서




설계 분석
서비스 환경 분석

아키텍처 설계
클라우드 구축 계획
수립

환경 구성
데이터 이관

성능 테스트
취약점 점검

# 프로젝트 수행 부문

3

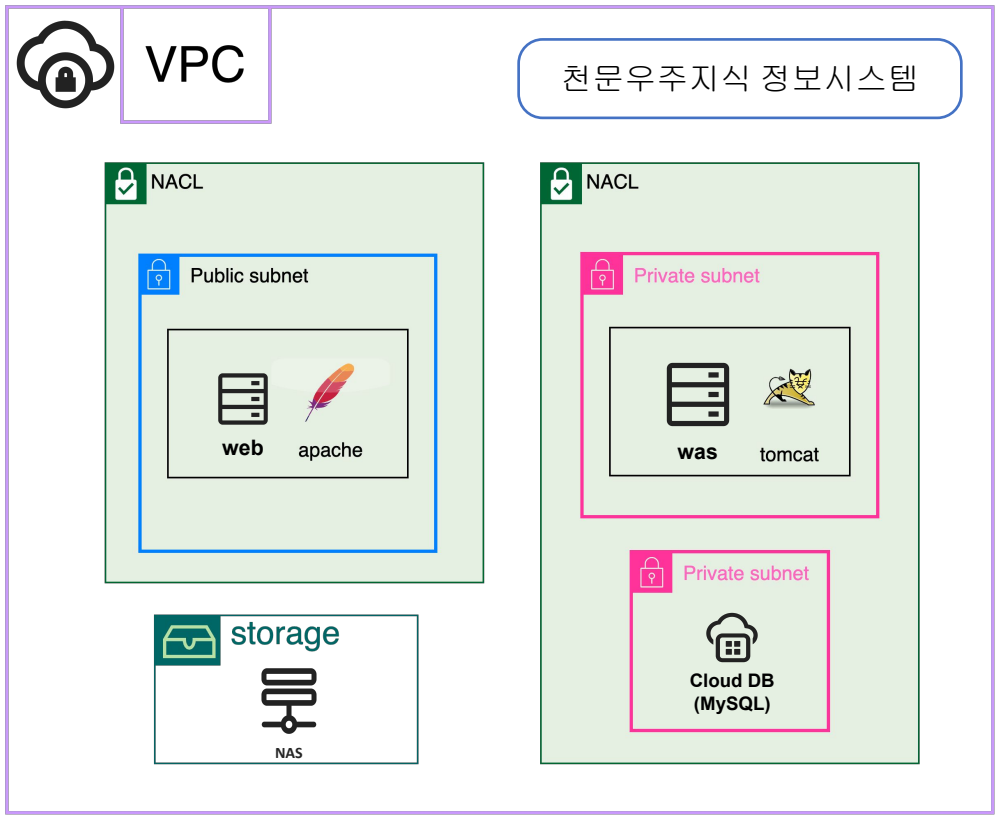
1. 서버 구축 방안
2. 네트워크 구축 방안
3. 데이터 이관
4. 인프라 구축 방안

NAVER CLOUD PLATFORM

# 1. 서버 구축 방안

클라우드 환경에 서버를 생성하여 시간과 비용 측면에서 효율적이며 많은 서버 지원이 필요한 경우 적합

## 네이버 클라우드 플랫폼의 시스템 서버 구조




간편하게 구축하고 사용한 만큼 지불하는 종량제 서버

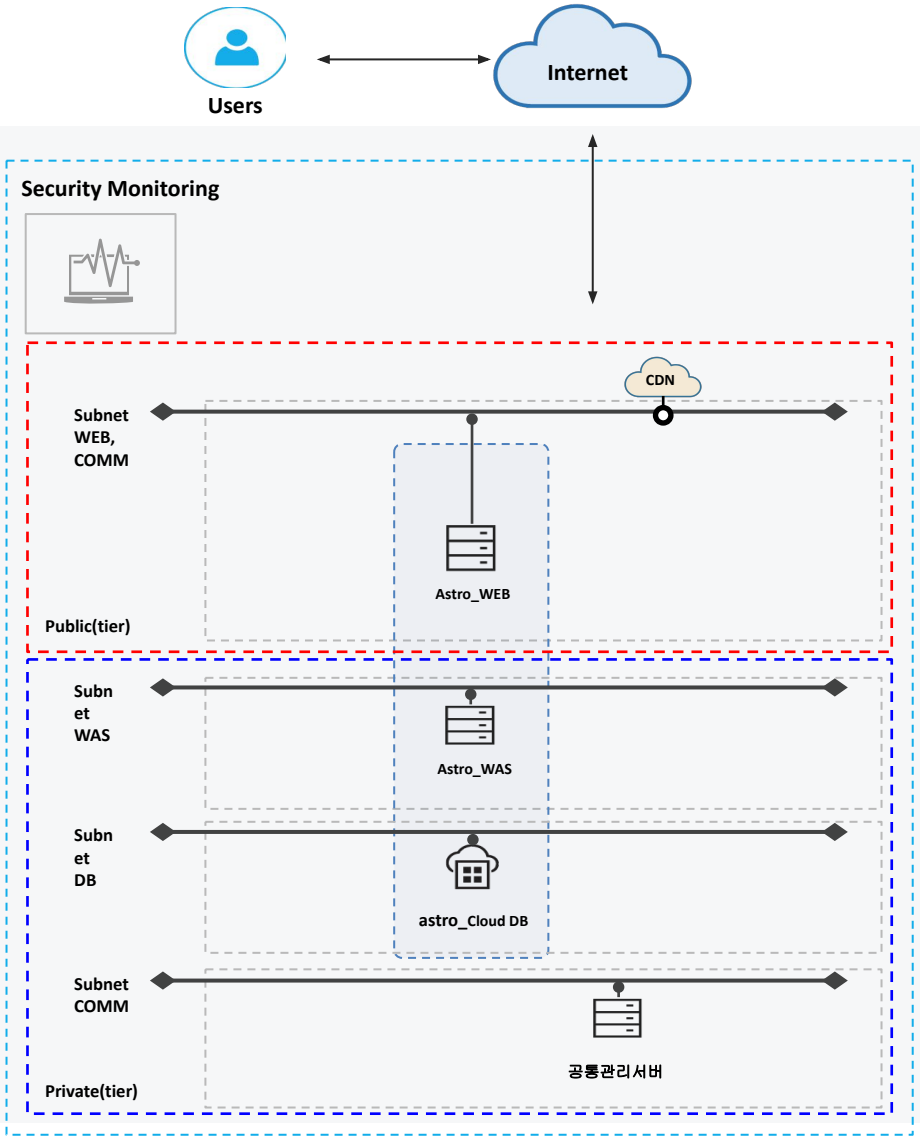
| 강력한 보안 | 모니터링기능 | 효과적인 비용관리 |
|---|---|---|
| astro_web | astro_was | astro_db |
| 인터넷망 (Public subnet) | 내부망 (Private subnet) | 내부망 (Private subnet) |
| Linux Centos 7.8 | Linux Centos 7.8 | Linux Centos 7.8 |
| CPU:2core Memory:4GB Disk:50GB(SSD) | CPU:2core Memory:4GB Disk:50GB(SSD) | CPU:2core Memory:4GB Disk:50GB(SSD) |
| SW Apache | SW Apache-tomcat 10.0.6 Open-idk 1.8 | SW Mysql 5.7.40 |

NAVER CLOUD PLATFORM

# 2. 네트워크 구축 방안

네트워크 서브넷(Subnet) 기능을 통한 네트워크의 용도별 세분화가 가능

## NCP 네트워크 인프라 구성




용도에 따라 네트워크를 세분화하여(서브넷) 네트워크를 구성

보안 강화를 위한 3-Tier 및 Web, WAS, DB서버가 분리된 구조로 전환

| 시스템명 | 이름 | CIDR | 위치 |
|---|---|---|---|
| 천문우주지식정보 시스템 | Public_Web | 172.16.10.0/24 | Public |
| | Private_WAS | 172.16.20.0/24 | Private |
| | Private_DB | 172.16.50.0/24 | Private |

보안 강화를 위한 NACL과 ACG

Access Control Group(ACG)과 Network Access Control List(NACL)은 각각 서버와 서브넷의 인바운드/아웃바운드 트래픽을 제어

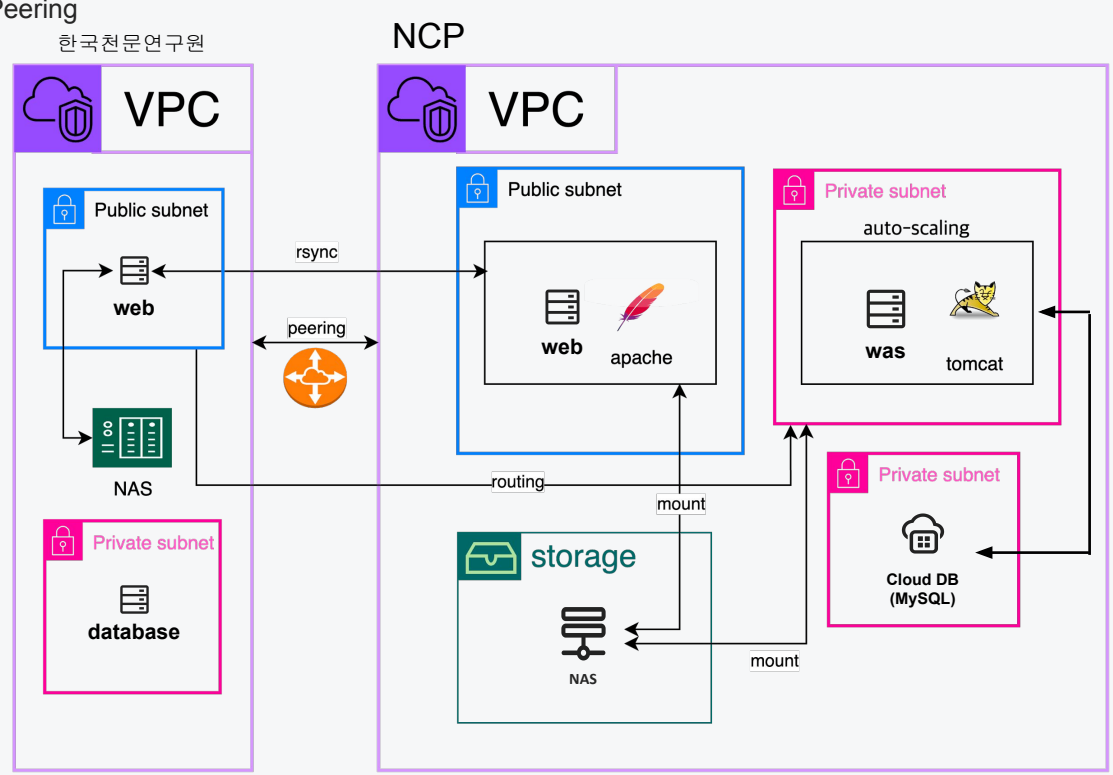
NAVER CLOUD PLATFORM

# 3. 데이터 이관

네트워크, 서버, 스토리지, 라우팅 메커니즘을 통한 데이터 이관을 설계합니다.

## 데이터 이관을 위한 아키텍쳐 구성

### 데이터 이관을 위한 VPC Peering




VPC 피어링을 이용한 VPC 간 통신

- 천문우주지식 정보시스템에서 Naver Cloud Platform 서버로의 데이터 이관을 위해 VPC Peering을 사용함

VPC 피어링(peering)을 이용하면 사설 IP를 기반으로 통신할 수 있어 서비스를 공용 인터넷에 노출하는 일 없이 안전한 통신 수단을 확보할 수 있습니다.

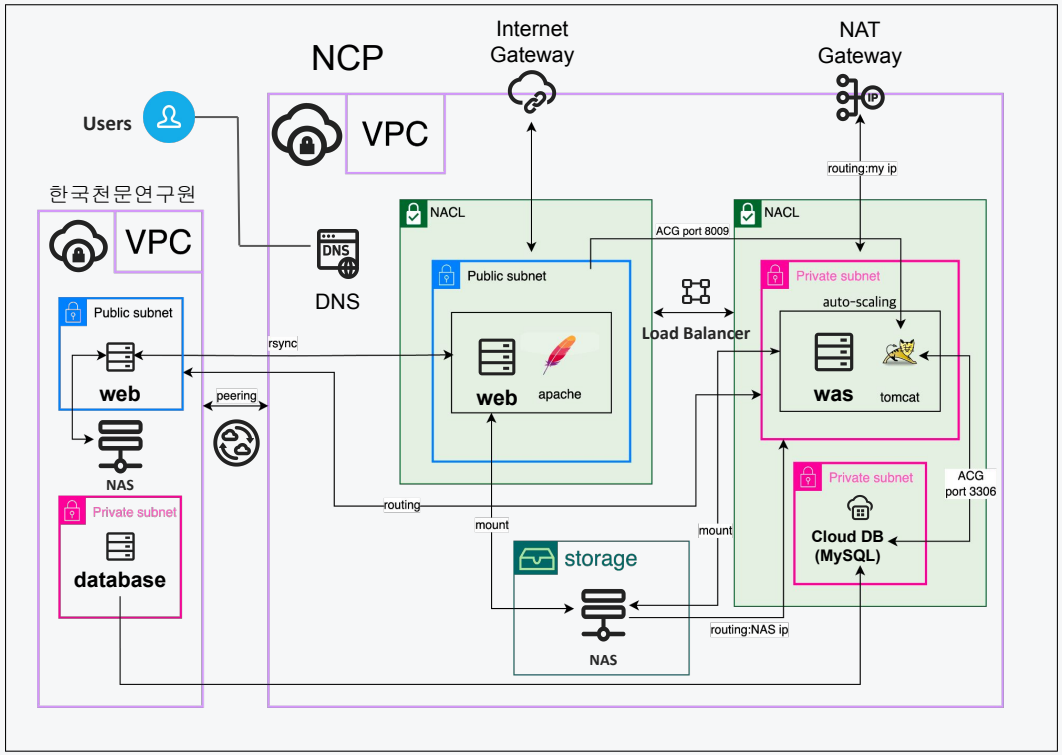
NAVER CLOUD PLATFORM

# 4. 인프라 구축 방안

네트워크, 서버, 스토리지, 라우팅 메커니즘을 통한 다양한 영역의 서비스 부하 분산을 설계할 수 있습니다.

## 부하 분산 서비스를 위한 다양한 기능 제공 방안

### 부하 분산을 위한 기본 아키텍처




**Loadbalancer 와 Autoscaling을 활용한 부하 분산**

- WAS 서버에 auto-scaling 기능을 추가하여 최대 용량을 5개로 늘리고, 로드밸런서를 추가하여 헬스체크를 가능하게 함으로써 부하 분산을 설계

**Mysql을 이용한 완전 관리형 클라우드 데이터베이스**

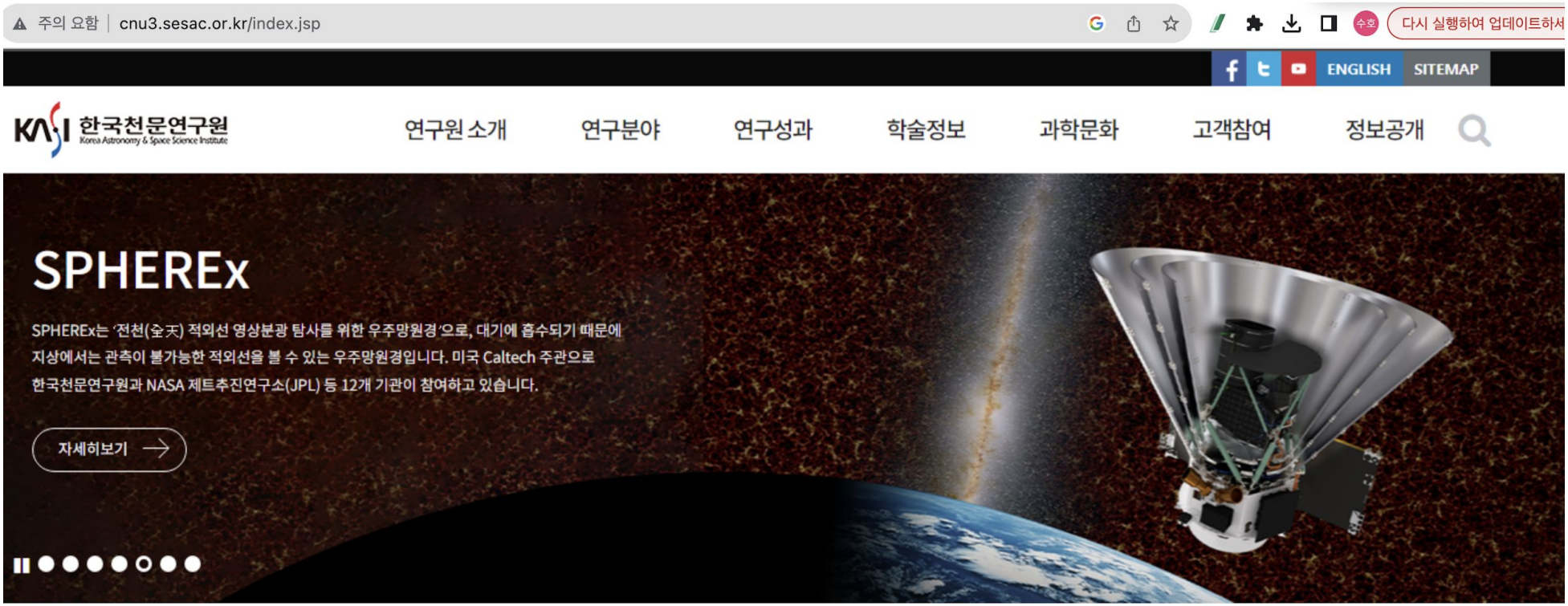
- Naver CLOUD PLATFORM에서 제공하는 Cloud DB for mysql 을 사용하여 DB를 기존 서버와 분리하여 운영. DB와 WAS,WEB 서버와 연동을 통해 읽고, 쓰기를 가능하게 함

**데이터베이스 읽기/쓰기 분리**

데이터베이스를 마스터-슬레이브 구조로 구축. 복제한 슬레이브 데이터베이스는 최대 10대까지 확장할 수 있으며 로드 밸런서와 연동하여 데이터베이스 읽기 쿼리의 부하를 마스터 슬레이브 복제를 통해 분산할 수 있습니다

NAVER CLOUD PLATFORM

# 구축 완료된 페이지 (한국천문연구원 홈페이지)



# 프로젝트 관리 부문

4

1. 보안 구성 (인프라)
2. 데이터 이관
3. 테스트 및 점검

# 2. 정보시스템 관리

접근제어(서버/DB) 구성 및 db 암호화

- public (NACL)

| 우선순위 | 프로토콜 | 접근 소스 | 포트 | 허용여부 |
|---|---|---|---|---|
| 0 | TCP | 0.0.0.0/0 (전체) | 80 | 허용 |
| 1 | TCP | 0.0.0.0/0 (전체) | 22 | 허용 |
| 100 | TCP | 168.131.0.0/16 | 22 | 허용 |
| 101 | ICMP | 168.131.0.0/16 | | 허용 |
| 198 | ICMP | 0.0.0.0/0 (전체) | | 차단 |

| 적용 서브넷 |
|---|
| public-web (125210) |
| sub-nat (125378) |

| 우선순위 | 프로토콜 | 목적지 | 포트 | 허용여부 |
|---|---|---|---|---|
| 0 | TCP | 0.0.0.0/0 (전체) | 1-65535 | 허용 |
| 1 | UDP | 0.0.0.0/0 (전체) | 1-65535 | 허용 |
| 2 | ICMP | 0.0.0.0/0 (전체) | | 허용 |

# 1. 보안 구성 (인프라)

- private (NACL)

| 우선순위 | 프로토콜 | 접근 소스 | 포트 | 허용여부 |
|---|---|---|---|---|
| 0 | TCP | 172.16.0.0/16 | 22 | 허용 |
| 100 | ICMP | 172.16.0.0/16 | | 허용 |
| 198 | ICMP | 0.0.0.0/0 (전체) | | 차단 |
| 199 | TCP | 0.0.0.0/0 (전체) | 22 | 차단 |

- outbound : public과 동일

| 적용 서브넷 |
|---|
| private-was (125213) |
| private-db (125214) |
| sub-lb (125707) |

# 1. 보안 구성 (인프라)

- public (ACG)

| 프로토콜 | 접근 소스 | 허용 포트 |
|---|---|---|
| TCP | 0.0.0.0/0 | 22 |
| TCP | 168.131.0.0/16 | 22 |
| TCP | 0.0.0.0/0 | 80 |
| ICMP | 0.0.0.0/0 | |

- outbound : 동일

| 적용 Network Interface ( 서버 ) |
|---|
| nic-3776594 (astro-web) |

# 1. 보안 구성 (인프라)

- private (ACG)

| 프로토콜 | 접근 소스 | 허용 포트 |
|---|---|---|
| TCP | nia3-vpc-auto-acg(152939) | 8009 |
| TCP | 172.16.0.0/16 | 22 |
| ICMP | 172.16.0.0/16 | |

- outbound : 동일

| 적용 Network Interface ( 서버 ) |
|---|
| nic-3777172 (astro-was) |
| nic-3782384 (was-5257komt4r4) |

# 1. 보안 구성 (인프라)

- mysql db (ACG)

| 프로토콜 | 접근 소스 | 허용 포트 |
|---|---|---|
| TCP | 0.0.0.0/0 | 3306 |
| TCP | cloud-mysql-d7tp6(152958) | 3306 |

| 프로토콜 | 목적지 | 허용 포트 | 적용 Network Interface ( 서버 ) |
|---|---|---|---|
| TCP | cloud-mysql-d7tp6(152958) | 3306 | nic-3776623 (astro-db-001-451h) |

- mysql db 암호화

# 2. 데이터 이관

File 및 DB 데이터 이관
정합성 검증

○ 데이터 이관

| 정보시스템명 | 연결서버명 | 이관유형 | 이관용량 (GB) | 이관 방식 |
|---|---|---|---|---|
| 천문우주지식정보 | astro_Web<br>astro_WAS<br>astro_DB | File Data<br>File Data<br>DB Data | 10 이하<br>10 이하<br>10 이하 | File Copy(Rsync)<br>File Copy(Rsync)<br>Migration Tool |

- AS-IS 정보시스템 중지 후
To-Be 시스템으로 Data 이관

- 실제 이관된 데이터 (약 400GB)

```
4096 Jan 18 16:40 .
  17 Jan 18 12:53 ..
4096 Jan 18 10:57 backup
4096 Jan  8 09:46 data
8259 Jan 12 09:15 failure_image.jpg
4096 Jan 18 10:56 files
6425 Jan 18 15:18 gstecN-3.sql
4096 Jan 18 10:56 html
4096 Jan 18 10:57 images
 113 Jan 15 12:00 index.html
1235 Jan 18 15:35 index.jsp
 329 Jan  4 10:11 index_test.jsp
8259 Jan 11 16:55 main_logo.png
 636 Jan  4 15:07 mysql.jsp
4096 Jan 18 11:01 sites
4096 Jan 17 18:57 .snapshot
0103 Jan 11 16:55 sub_page.png
4096 Jan 18 11:05 tempFile
2167 Jan  4 14:49 test.jsp
4096 Jan 18 11:02 tmeplate
4096 Jan 18 11:02 tomcat
4096 Jan 18 13:07 web
4096 Jan 18 11:00 Web-home
4096 Jan 18 11:01 WEB-INF
```

# 2. 데이터 이관

– 정합성 검증

| 구분 | 검증방법 | 세부 검증 내용 | 작업자 |
|---|---|---|---|
| File Data | 파일 개수 검증 | 파일 개수 동일 여부 확인<br># find "디렉토리명" -type f | TBD |
| | 디렉토리 개수 검증 | 디렉토리 개수 동일 여부 확인<br># find "디렉토리명" -type d | |
| DB Data | Table Row 개수 검증 | Table Row 수 동일 여부 확인 | |

※ 데이터 정합성의 검증방법은 기관담당자와의 사전 협의를 통하여 검증방안을 도출함(데이터 총 건수 확인, 특정 칼럼 데이터 합산 값 비교, 특정 쿼리 수행 결과 비교 등)

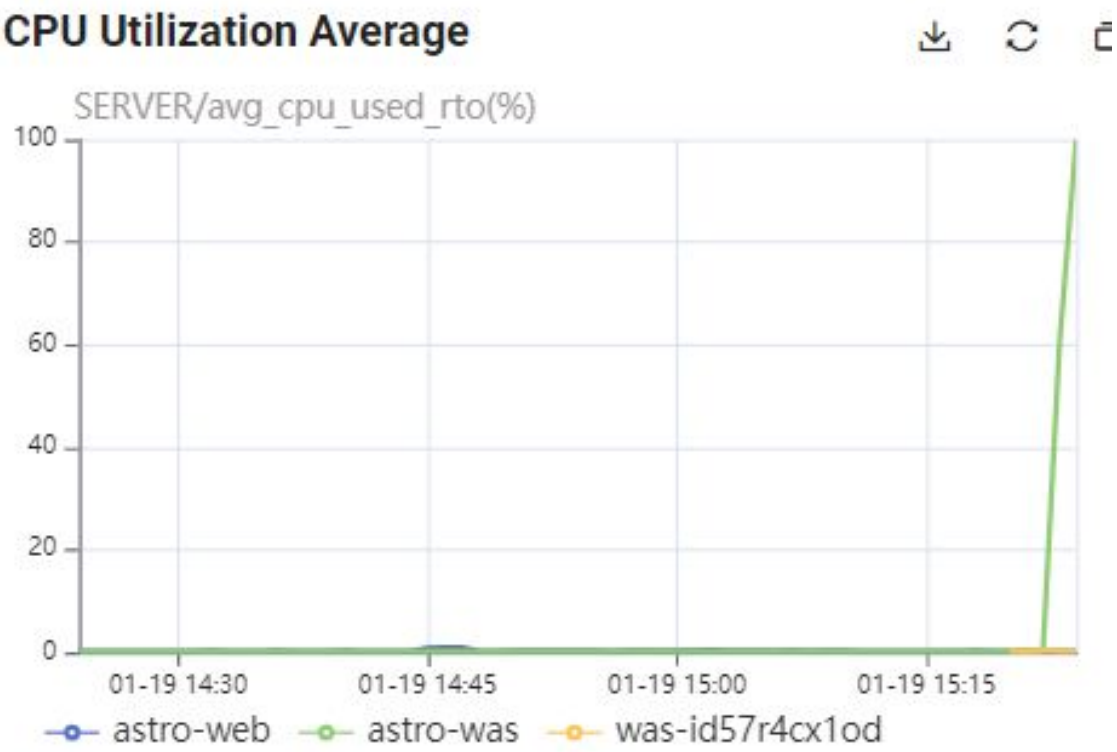
# 3. 테스트 및 점검

**cpu 부하 테스트**

- Stress Tool

```
[root@astro-was ~]# stress --cpu 2 --timeout 300 --verbose
```

서버 증가 또는 감소 확인을 위해 300 초동안 cpu 코어 2 개에 부하를 발생시킵니다.



# 3. 테스트 및 점검

**System Security Checker**

- OS Security Checker

**서버 운영 체제에 대한 보안 취약점을 점검** Region 통합 서비스

파일 접근 권한 관리, 계정 관리 등 서버의 운영 체제에 대한 보안 설정상 취약점은 없는지 꼼꼼하게 점검하고 그에 대한 결과 레포트를 제공합니다.

| Total | Good | Critical | Major | Minor | Exception |
|---|---|---|---|---|---|
| 37 | 27 | 10 | - | - | 1 |

| | |
|---|---|
| Title | 패스워드 복잡성 설정 |
| Risk level | Critical |

Mitigation method

```
Linux - RHEL7 기준
Step 1) /etc/security/pwquality.conf 파일 수정
  # 각 항목에서 -1 값은 반드시 해당하는 문자를 비밀번호에 포함시키도록 강제함.
  # 문자 조합 선택 (2 또는 3개 이상)
  lcredit=-1 (영문 소문자)
  ucredit=-1 (영문 대문자)
  dcredit=-1 (숫자)
  ocredit=-1 (특수문자)
  # 비밀번호 길이 설정
  minlen=8 (최소 패스워드 길이 설정)
```

# 3. 테스트 및 점검

– WAS Security Checker

Summary

| Total | Good | Critical | Major | Minor | Exception |
|---|---|---|---|---|---|
| 12 | 10 | - | 2 | - | 1 |

| | |
|---|---|
| Description | 주기적으로 보안 패치를 적용하지 않으면, 알려진 취약점 등으로 서버 침해가 발생할 위험이 높아집니다. 주기적으로 보안이 향상된 버전으로 업데이트 하는 것을 권고합니다. |

| | |
|---|---|
| Title | 최신 패치 적용 |
| Risk level | Major |

다. jar 파일을 통한 버전 확인

```
Server version: Apache Tomcat/10.0.6
Server built:   May 8 2021 15:24:15 UTC
Server number:  10.0.6.0
OS Name:        Linux
OS Version:     3.10.0-1127.10.1.el7.x86_64
Architecture:   amd64
JVM Version:    1.8.0_392-b08
JVM Vendor:     Red Hat, Inc.
```

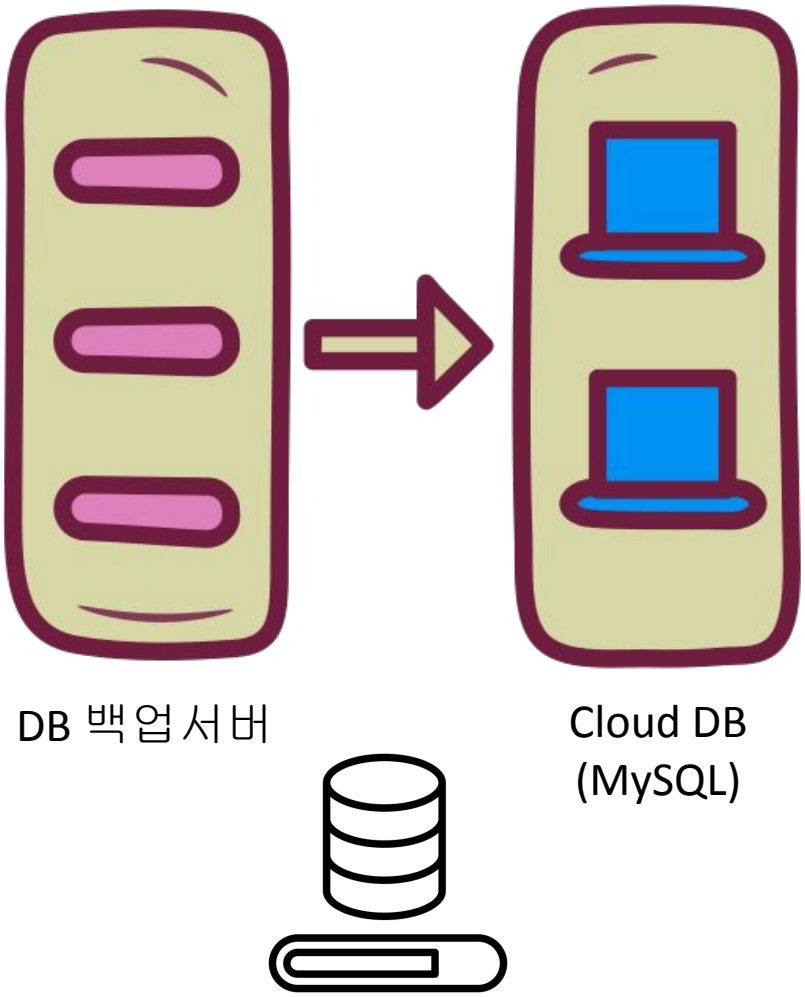
# 프로젝트 평가

5

1. 프로젝트 애로사항
2. 팀 구성원 피드백

NAVER CLOUD PLATFORM

# 1. 프로젝트 애로사항




75GB 이상으로 모든 데이터가 옮겨지는데
1일 이상 소요될 것으로 예상됨

- 기존 DB를 클라우드 내로 옮기는 과정에서 많은 시간이 소요될 것으로 예상되며, 데이터 옮기는 과정 내에서 오류 발생 시 불필요한 반복작업 가능성도 있음

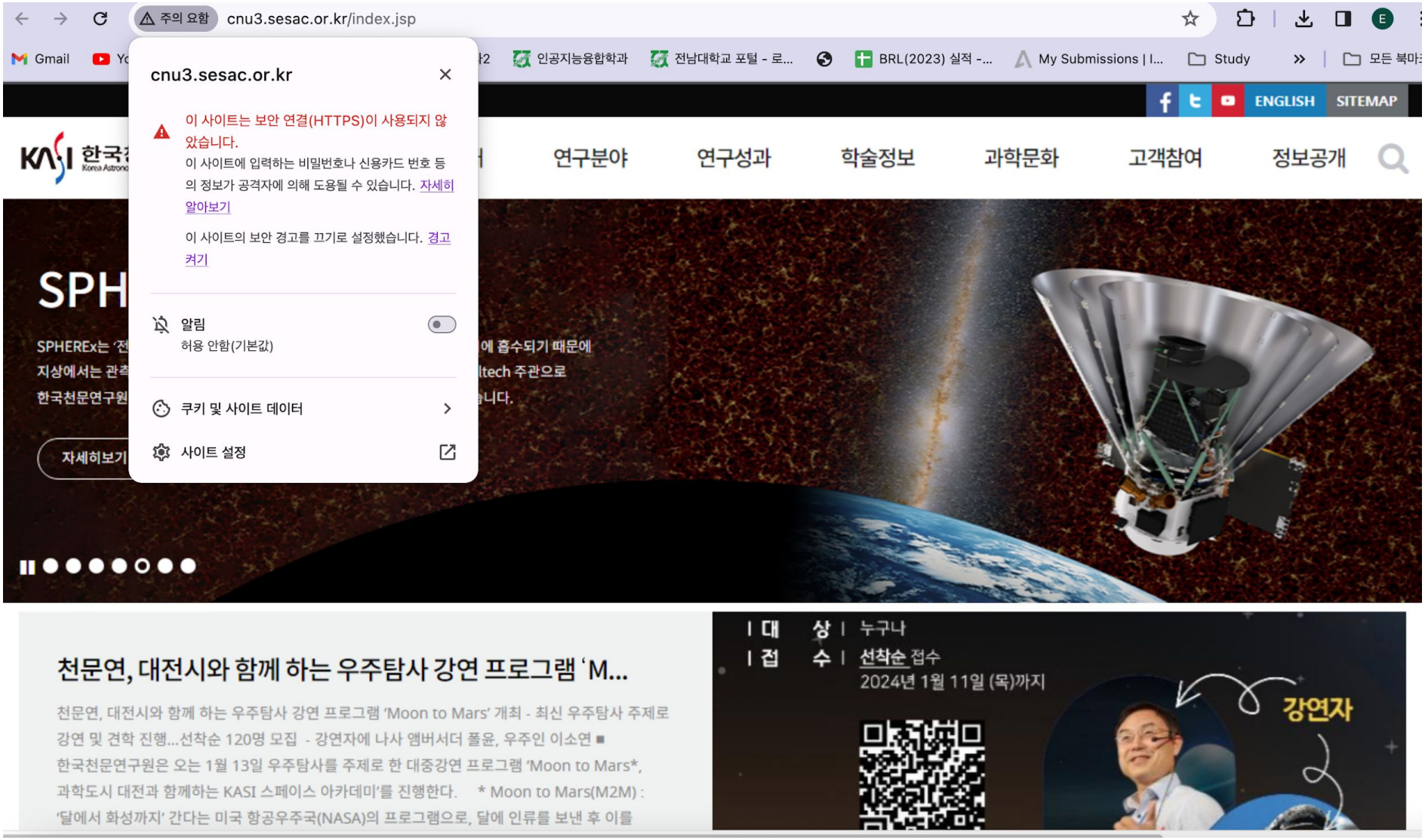
- 추후 빅데이터 관리방안 수립 필요
  (기존 데이터 + 새로 수집될 데이터)
  ➡️ 반정형, 비정형 데이터 관리방안, 데이터 통합 등

- 추후 세부적인 데이터 보안 방안 수립
  (개인정보보호, 암호화, 복호화 등)

NAVER CLOUD PLATFORM

# 1. 프로젝트 애로사항

- http 사용으로 보안에 취약함 (암호화가 안되서 공격자의 공격에 매우 취약)
  ➡️ https 사용으로 보안성 강화



# 1. 프로젝트 애로사항

• 인바운드 정책 설정 추가 필요

현재: 모든 대역에서 80번 포트로 웹 접속이 가능함

| nia3-vpc-auto-nacl | 83261 | nia-3 | 2 |
|---|---|---|---|

상세 정보 | Inbound 규칙 | Outbound 규칙

| 우선순위 | 프로토콜 | 접근 소스 | 포트 | 허용여부 |
|---|---|---|---|---|
| 0 | TCP | 0.0.0.0/0 (전체) | 80 | 허용 |
| 1 | TCP | 0.0.0.0/0 (전체) | 22 | 허용 |
| 100 | TCP | 168.131.0.0/16 | 22 | 허용 |
| 101 | ICMP | 168.131.0.0/16 | | 허용 |
| 198 | ICMP | 0.0.0.0/0 (전체) | | 차단 |

1. 북한 ip, 공격자 ip 대역 설정 후, 접속 못하게 차단해야함
(공격자 ip 확인: 국정원 국가사이버안전센터에서 가능)

2. 80, 22 포트들은 well known 포트로 공격자들이 다 아는 포트들이므로, 서버 담당자가 포트를 5자리로 변경해서 사용해야 외부 공격을 막을 수 있음 (예: 22 -> 32002)

NAVER CLOUD PLATFORM

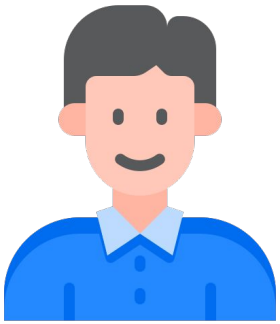
# 2. 팀 구성원 피드백 (3팀)

임은채

"기존에 기관에서 사용하던 시스템을 클라우드 환경으로 옮긴 후, 사용자가 시스템 속도를 기존과 비교했을 때 느려졌다고 생각하고 불편함을 느껴 원복하는 경우가 종종 있는 것 같습니다. 이러한 부분을 방지하기 위해 구축완료 후, 시범운영기간을 거치면서 사용자 피드백을 수용하고 보완하는 절차가 원활하게 진행되어야 할 것 같습니다. 또한 각 파트별로 담당자가 빠르고 정확한 의사소통을 진행하고 안정화 기간에는 꾸준한 모니터링이 필요합니다."

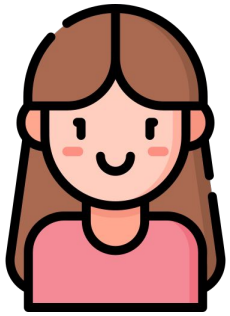
정수호

"실무 실습에서 네트워크 구성을 진행하며, 구체적인 설정 부분에 대한 이해 부족으로 어려움을 겪었습니다. 특히, 네트워크 장비 및 프로토콜 설정에 대한 상세 지침이 필요했으며, 이 과정에서의 지원과 안내가 더 강화되면 학습 효과가 향상될 것 같습니다. 실습 과정에서 네트워크 구성의 전반적인 흐름을 이해하는 데 추가적인 설명이나 예시가 제공되면 더욱 도움이 될 것입니다."



구동한

"실습과 프로젝트를 진행하면서 네트워크 단을 구성할 때에 이론적인 부분에 대한 이해가 많이 부족하다고 느껴졌습니다. 실제로 엔지니어로서 아키텍처를 구축할 때 어떤 정책과 설정을 적용하고 각 영역 간의 통신은 어떻게 구성되어야 하는지 자세하게 알고 있어야 클라우드로 이전하기에 더 효율적으로 작업할 수 있을 것 같습니다."



문지은

"공공기관 클라우드 전환 사업은 업무 효율성 향상과 유지 보수 비용을 감면시킨다는 점에서 꼭 필요합니다. 하지만 기존 시스템에서 클라우드로의 데이터 이전은 예상치 못한 문제를 발생시킬 수 있습니다. 데이터 이전 전에 충분한 테스트를 수행하여 호환성 문제를 사전에 해결하고, 데이터의 무결성을 보장할 필요가 있습니다."

감사합니다