한국잡월드 클라우드 이전 및 전환 용역
보안성검토 요청서

2022. 03.

한국잡월드

< 목 차 >

Ⅰ 사업 계획서

1. 사업 개요

○ 사업명 : 과 업 명: 한국잡월드 클라우드 이전 및 전환 용역

○ 사업기간 : 2022. 1. 1. ~ 2022. 7. 31(7개월)

○ 사업예산 : 금 131백만원

○ 구매방식 : 조달계약(디지털서비스 카달로그 계약)

2. 주요 사업 내용 및 산출물

가. 주요 사업 내용

○ 추진배경

- 홈페이지 및 전시운영시스템의 노후화로 장애 발생 시 홈페이지, 체험실 운영 등의 고객서비스에 문제 발생
- 상용SW의 EOS로 인한 업그레이드 필요 및 지속적인 유지보수비 절감을 위한 오픈소스 기반의 공개SW 개발환경 마련

○ 추진목적

- 디지털 수요에 탄력적으로 대응할 수 있도록 클라우드 기반 통합운영 환경을 구축하고 서비스 안정성 확보
- 체험관 시스템의 통합 및 확장에 유연한 정보자원체계 확충

○ 주요사업 범위

- 클라우드 운영 환경 구성을 위해 홈페이지 및 전시운영시스템 관련 응용프로그램, DBMS 전환
- 클라우드 서비스의 용량 변경, 추가 서비스 선택 및 모니터링을 위한 환경 제공
- 홈페이지 및 전시운영시스템 인프라 체계 재구성을 위한 서버, 네트워크, 보안, 관제, SW 등 클라우드 서비스 이관 및 일괄 임차 운영

나. 주요 산출물

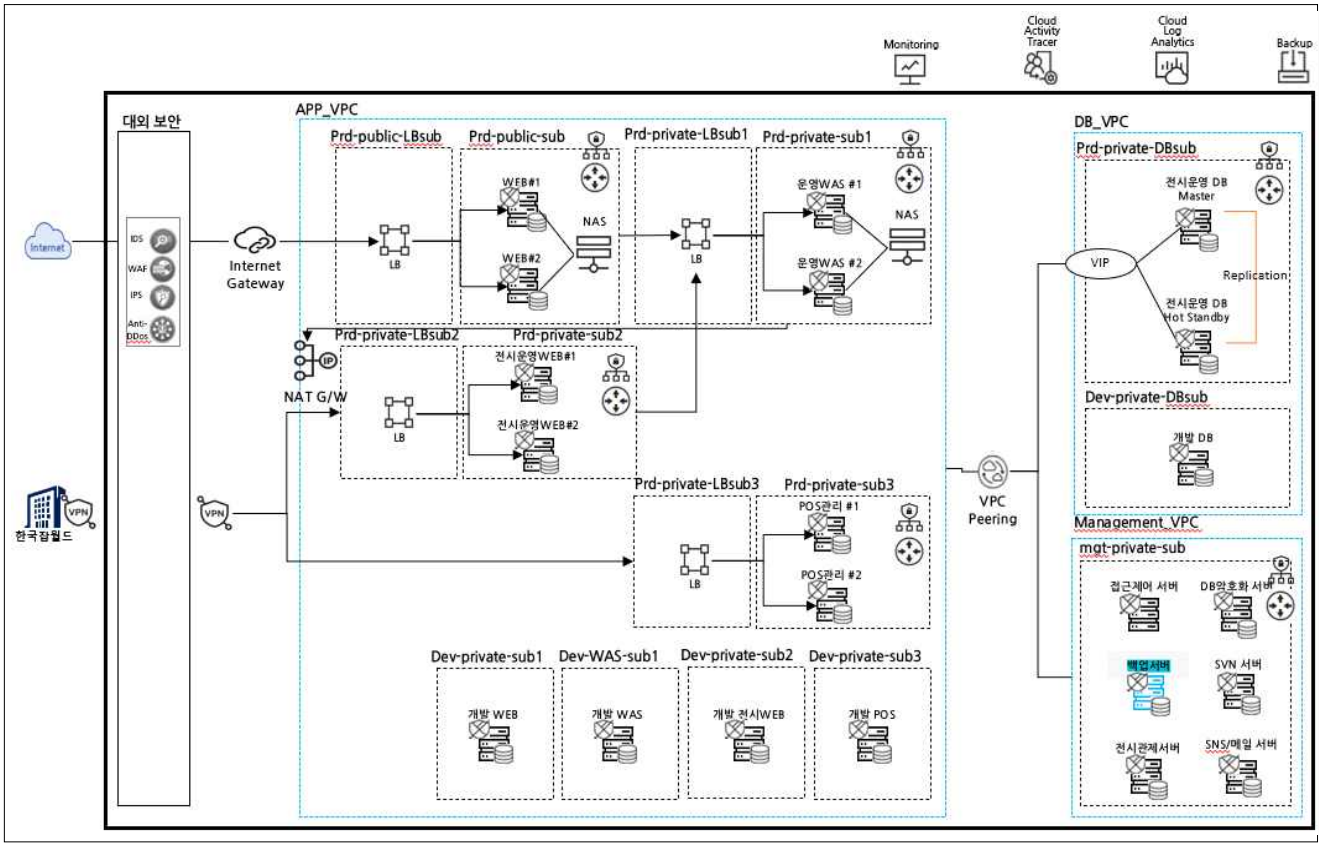
- 홈페이지 및 전시운영시스템의 노후화로 장애 발생 시 홈페이지, 체험실 운영 등

의 고객서비스에 문제 발생

사 업 범 위	세 부 사 항	산출물
H/W	홈페이지 및 전시운영시스템, POS 관련 서버 16식	클라우드 운영 구성도
보안	웹방화벽(WAF), 방화벽(F/W), 침입방지시스템(IPS) 등	클라우드 운영 구성도
S/W	WEB, WAS, DBMS 등 소프트웨어 18식	클라우드 운영 구성도 - 상세설계 SW

Ⅱ 정보통신망 구성도

1. 시스템 및 네트워크 구성도



가. 시스템간 연계 구성 현황

○ 시스템간 연계 구성 현황

시스템	연계 구성	설명
홈페이지 (인터넷망)	일반사용자 – WEB#1,2 – 운영WAS#1,2 – 전시운영 DB	3 Tier 구조 서브넷간 ACL통제
전시운영 (내부망)	한국잡월드 – 전시운영WEB – 운영WAS#1,2 – 전시운영 DB	전시운영관리 행정
POS관리 (내부망)	한국잡월드 – POS관리 – 운영WAS#1,2 – 전시운영 DB	POS관리 행정
개발서버 (내부망)	한국잡월드 – 개발WEB – 개발WAS – 개발DB 한국잡월드 – 개발전시운영WEB – 개발WAS – 개발DB 한국잡월드 – 개발POS – 개발WAS – 개발DB	홈페이지 개발, 전시운영 개발, POS개발
관리서버 (내부망)	접근제어, DB암호화, 백업, SVN, 전시관제, SNS/메일	서버관리, 형상관리, 접근제어, DB암호화, 백업, 문자/이메일

○ **공통 네트워크 연계 구성 설명 (VPC, VPC Peering, Subnet)**

구성	대상 설명	연계 방법
APP_VPC	WEB #1/2, 운영WAS #1/2, 전시운영WEB #1/2, POS관리 #1/2, 개발 WEB, 개발 WAS,개발 전시WEB, 개발 POS서버별로 Subnet으로 구성함	원칙적으로 VPC, Subnet간에 통신 불가
Management_VPC	접근제어 서버, DBN암호화 서버, 백업 서버, SVN 서버, 전시관제 서버, 눈/메일 서버별로 Subnet으로 구성함	원칙적으로 VPC, Subnet간에 통신 불가
DB_VPC	전시운영 DB(Master, Hot Standby), 개발 DB별로 Subnet으로 구성함	원칙적으로 VPC, Subnet간에 통신 불가
LB용 Subnet	Prd-Public-LBsub, Prd-Private-LBsub1, Prd-Private-LBsub2, Prd-Private-LBsub3으로 구성됨	ACG 규칙을 이용하여 부하 분산용 서버 Subnet 연결함
Prd-public-sub Subnet	WEB#1, WEB#2서버로 Subnet구성됨	운영WAS#1,2연결
Prd-private-sub1 Subnet	운영WAS#1, 운영WAS#2서버로 Subnet구성됨	DB연결시 VPC Peering 연결됨
Prd-private-sub2 Subnet	전시운영WEB#1, 전시운용WEB#2서버로 Subnet구성됨	DB연결시 VPC Peering 연결됨
Prd-private-sub3 Subnet	WEB#1, #2서버로 Subnet구성됨	DB연결시 VPC Peering 연결됨
Prd-public-DBsub Subnet	전시운영 DB Master, 전시운영 DB HotStandby	VIP(가상IP)기반의 HA구조로 VPC Peering 연결됨
Dev-public-DBsub Subnet	개발 DB	개발WEB, 개발 WAS,개발 전시WEB, 개발 POS를 VPC Peering 연결됨
Dev-private-sub1	개발 WEB	개발 DB를 VPC Peering 연결됨
Dev-WAS-sub1	개발 WAS	개발 DB를 VPC Peering 연결됨
Dev-private-sub2	개발 전시WEB	개발 DB를 VPC Peering 연결됨
Dev-private-sub3	개발 POS	개발 DB를 VPC Peering 연결됨
mgt-private-sub	접근 제어 서버, DB암호화 서버, 백업 서버, SVN 서버, 전시관제 서버, SNS/메일 서버	VPC Peering 연결됨
VPC Peering	전용 네트워크의 확장 효과와 함께 인터넷 통신을 거치지 않기에 안전한 통신을 지원	VPC간 통신 지원

○ **홈페이지 연계 구성 현황 설명 (일반사용자 – WEB#1,2 – 운영WAS#1,2 – 전시운영 DB)**

홈페이지 연계 (인터넷망)			
아키텍처 구조	3계층 구조	프로토콜	HTTPS(SSL/TLS)
가용성 보장	LB(Load Balancer) 이중화	DB 구조	Active - Hot standby
로그인	아이디 / 패스워드	패스워드 암호화	SHA-256
3계층 구분	VPC, Subnet	데이터 암호화	개인정보 대상
접근제어	서버 접근제어	백업	백업서버 운영

- 기관 홈페이지 서비스를 위해서 정보 보안 및 안전성에 적합한 구성을 목표로 사용자 폭증에 유연한 대응을 위해서 고가용성 및 호환성, 확장성, 효율성을 고려하여 3계층 구조인 WEB, WAS, DB서버 형태로 최적의 시스템 구축
- 홈페이지 서비스로 접속을 위해서 사용자 단말에서 웹 브라우저 이용한 HTTPS 소켓 통신으로 일반 텍스트를 암호화하여 안전한 웹서비스를 제공하고 있으며, 홈페이지 로그인시 아이디와 패스워드로 접근이 가능하고 패스워드는 SHA265으로 암호화해서 저장하고 있으며, 개인정보는 암호화솔루션을 이용하여 암호화처리하여 저장하고 있습니다.
- 홈페이지 서비스로 다량의 접속자 증가 시 부하 분산을 위해서 WEB, 운영 WAS는 LB(Load Balancer)로 수신 트래픽을 다수의 서버로 분산시키는 서비스 구성하였으며 전시운영 DB에서는 이중화 구성으로 Active-Hot Standby, Logical Replication기능을 지원하여 안정적인 서비스를 제공합니다.
- 전시운영DB는 가용성을 이중화 구성를 하였으며, 개인정보는 데이터 암호화 처리 및 접근제어 서버를 통해서만 접근이 가능합니다.

○ **전시운영 연계 구성 현황 설명 (한국잡월드 – 전시운영WEB – 운영WAS#1,2 – 전시운영 DB)**

전시운영 연계 (내부망 - IPSec VPN)			
아키텍처 구조	3계층 구조	프로토콜	HTTPS(SSL/TLS)
가용성 보장	LB(Load Balancer) 이중화	DB 구조	Active - Hot standby
로그인	아이디 / 패스워드	패스워드 암호화	SHA-256
3계층 구분	VPC, Subnet	데이터 암호화	개인정보 대상
접근제어	서버 접근제어	백업	백업서버 운영

- 전시운영 서비스는 내부망 연계를 위해서 IPSec VPN를 이용한 구간에 터널링을 이용하여 패킷 이동과 암호화를 가상 전용회선의 내부 서비스를 제공합니

다.

- 전시운영 서비스로 접속을 위해서 관리자 단말에서 웹 브라우저 이용한 HTTPS 소켓 통신으로 일반 텍스트를 암호화하여 안전한 전시운영를 제공하고 있으며, 전시운영 로그인시 아이디와 패스워드로 접근이 가능하고 패스워드는 SHA265으로 암호화해서 저장하고 있으며, 개인정보는 암호화 솔루션을 이용하여 암호화 처리하여 저장하고 있습니다.
- 전시운영 서비스는 인터넷망을 통해서 접근할 수가 없습니다.
- 전시운영 서비스로 다량의 접속자 증가 시 부하 분산을 위해서 전시운영 WEB는 LB(Load Balancer)로 수신 트래픽을 다수의 서버로 분산시키는 서비스 구성하였으며 전시운영 DB에서는 이중화 구성으로 Active-Hot Standby, Logical Replication기능을 지원하여 안정적인 서비스를 제공합니다.
- 전시운영DB는 가용성을 이중화 구성를 하였으며, 개인정보는 데이터 암호화 처리 및 접근제어 서버를 통해서만 접근이 가능합니다.

○ **POS관리 연계 구성 현황 설명 (한국잡월드 – POS관리 – 전시운영 DB)**

POS관리 연계 (내부망 - IPSec VPN)			
아키텍처 구조	2계층 구조	프로토콜	HTTPS(SSL/TLS)
가용성 보장	LB(Load Balancer) 이중화	DB 구조	Active - Hot standby
로그인	아이디 / 패스워드	패스워드 암호화	SHA-256
3계층 구분	VPC, Subnet	데이터 암호화	개인정보 대상
접근제어	서버 접근제어	백업	백업서버 운영

- POS관리 서비스는 내부망 연계를 위해서 IPSec VPN를 이용한 구간에 터널링을 이용하여 패킷 이동과 암호화를 가상 전용회선의 내부 서비스를 제공합니다.
- POS관리 서비스로 접속을 위해서 관리자 단말에서 웹 브라우저 이용한 HTTPS 소켓 통신으로 일반 텍스트를 암호화하여 안전한 POS관리를 제공하고 있으며, POS관리 로그인시 아이디와 패스워드로 접근이 가능하고 패스워드는 SHA265으로 암호화해서 저장하고 있으며, 개인정보는 암호화 솔루션을 이용하여 암호화 처리하여 저장하고 있습니다.
- POS관리 서비스는 인터넷망을 통해서 접근할 수가 없습니다.
- POS관리 서비스로 다량의 접속자 증가 시 부하 분산을 위해서 POS관리 WEB/WAS는 LB(Load Balancer)로 수신 트래픽을 다수의 서버로 분산시키는

서비스 구성하였으며 POS관리 DB에서는 이중화 구성으로 Active-Hot Standby, Logical Replication기능을 지원하여 안정적인 서비스를 제공합니다.

- 전시운영DB는 가용성을 이중화 구성를 하였으며, 개인정보는 데이터 암호화 처리 및 접근제어 서버를 통해서만 접근이 가능합니다.

○ **개발서버 연계 구성 현황 설명 (한국잡월드 – 개발WEB – 개발WAS – 개발DB, 한국잡월드 – 개발전시운영WEB – 개발WAS – 개발DB, 한국잡월드 – 개발POS – 개발DB)**

개발서버 연계 (내부망 - IPSec VPN)			
아키텍처 구조	3계층 구조	프로토콜	HTTPS(SSL/TLS)
가용성 보장	없음	DB 구조	단일 구조
로그인	아이디 / 패스워드	패스워드 암호화	SHA-256
3계층 구분	VPC, Subnet	데이터 암호화	개인정보 대상
접근제어	서버 접근제어	백업	백업서버 운영

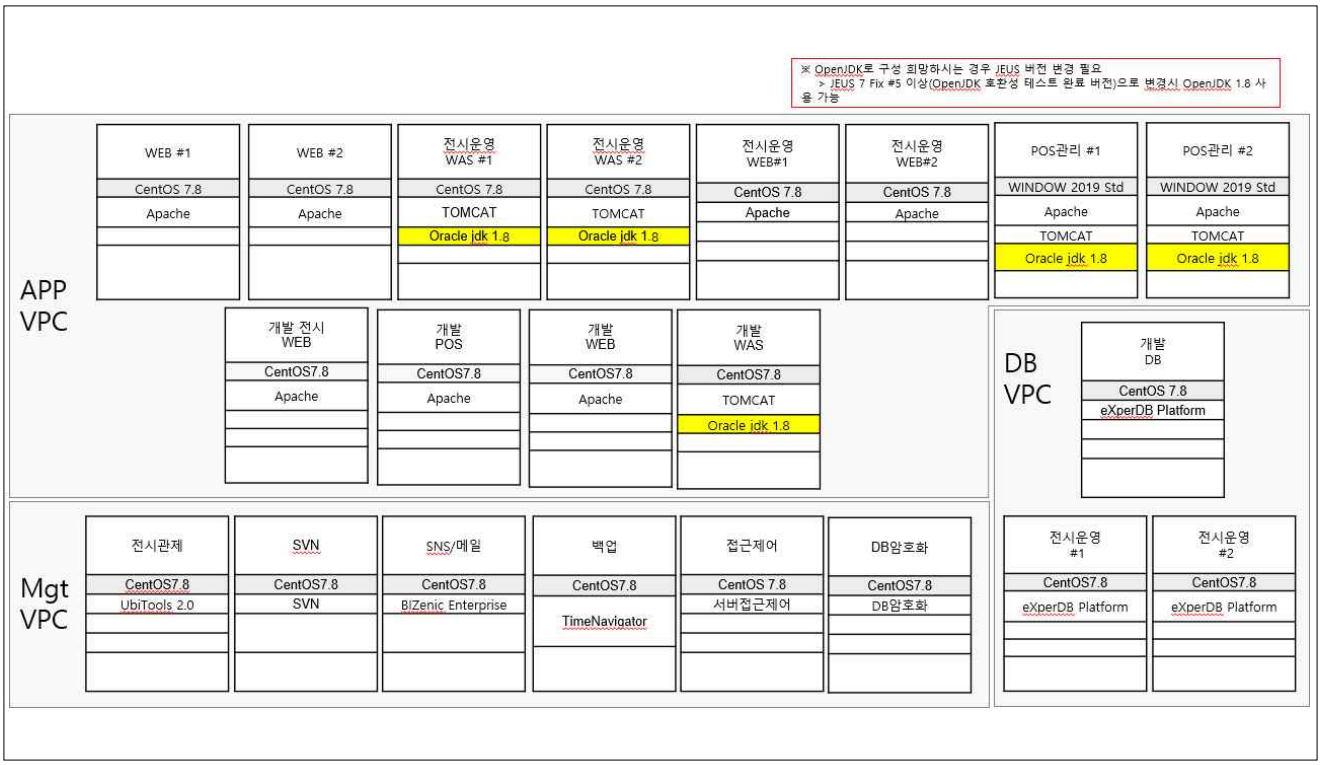
- 개발계(개발웹, 전시운영, POS관리) 서비스는 내부망 연계를 위해서 IPSec VPN를 이용한 구간에 터널링을 이용하여 패킷 이동과 암호화를 가상 전용회선의 내부 서비스를 제공합니다.
- 개발계(개발웹, 전시운영, POS관리) 서비스로 접속을 위해서 관리자 단말에서 웹 브라우저 이용한 HTTPS 소켓 통신으로 일반 텍스트를 암호화하여 안전한 개발계(개발웹, 전시운영, POS관리)를 제공하고 있으며, 개발계(개발웹, 전시운영, POS관리) 로그인시 아이디와 패스워드로 접근이 가능하고 패스워드는 SHA265으로 암호화해서 저장하고 있으며, 개인정보는 암호화 솔루션을 이용하여 암호화 처리하여 저장하고 있습니다.
  - 개발계(개발웹, 전시운영, POS관리) 서비스는 인터넷망을 통해서 접근할 수가 없습니다.
  - 개발DB는 데이터 비식별화처리 후 개발DB로, 개인정보는 데이터 암호화 처리 및 접근제어 서버를 통해서만 접근이 가능합니다.
  - 개발계(개발웹, 전시운영, POS관리)서버에는 운영서버들(WEB#1/#2, 전시운영 WEB#1/#2, POS관리#1/#2, 전시운영 DB) 접근이 불가능 합니다.

○ **관리서버 연계 구성 현황 설명(접근제어, DB암호화, 백업, SVN, 전시관제, SNS/메일)**

관리서버 연계 (내부통신)			
아키텍처 구조	중앙집중구조	프로토콜	솔루션별 상이함
가용성 보장	없음	DB 구조	미사용
계층 구분	VPC, Subnet	데이터 암호화	개인정보 대상
접근제어	서버 접근제어	백업	미대상

- 운영서버들(WEB#1/#2, 전시운영 WEB#1/#2, POS관리#1/#2, 전시운영 DB)서버의 접근제어, DB암호화, 백업, SVN, 전시관제, SNS/메일 서비스 제공하기 위해서 연계가 하였습니다.
- 개발서버들(개발 WEB, 개발WAS, 개발DB, 개발전시운영WEB, 개발POS)서버의 접근제어, DB암호화, SVN, SNS/메일 서비스 제공하기 위해서 연계가 하였습니다.
- ACL 방화벽 정책은 운영서버들과 개발서버들의 최소화의 권한만 설정하여 운영 하였습니다.

2. 소프트웨어 구성도



3. 클라우드 서비스

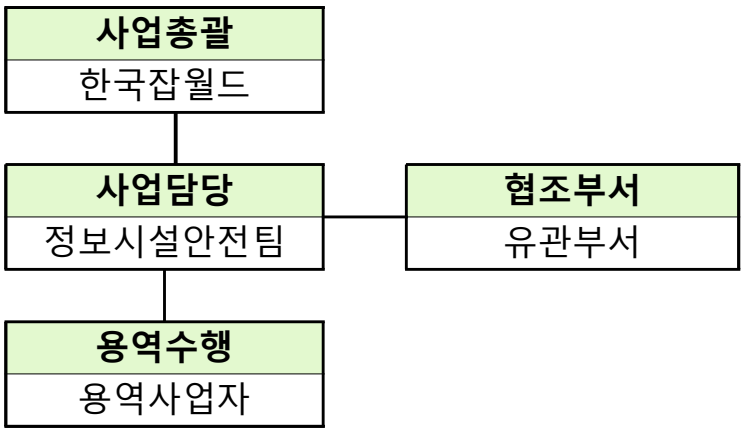
시스템	연계 구성	설명
Server	물리적인 서버 자원을 별도로 구매하지 않고, 클라우드 환경에서 빠르게 생성해 사용한 만큼만 비용을 지불하면 되는 효율적인 서비스	
NAS	서버 간 데이터 공유, 대용량 스토리지, 유연한 용량 확대/축소, 스냅샷 백업 등 NAS 서비스의 주요 기능을 활용해 사용자가 안전하고 편리하게 데이터를 관리	
Backup	검증된 백업 솔루션을 사용해 서버의 데이터를 정기적으로 백업하고 보관하는 서비스, 유사시 데이터 복구가 가능해 고객의 비즈니스 연속성을 보장	Managed Service
Load Balancer	고객의 서비스에 대한 네트워크 트래픽을 분산해 서버의 부하를 경감, 연결된 일부 서버에 장애가 발생하면 자동으로 다른 정상 서버로 부하를 배분	
ACG	서버 그룹에 대한 네트워크 접근을 제어, 관리할 수 있는 서비스입니다. 고객이 개별적으로 방화벽을 구축할 필요 없이 ACG에 서버 그룹별로 방화벽 규칙을 설정하면 인프라 보안 정책을 손쉽고 효율적으로 적용할 수 있는 서비스	
Security Monitoring	외부의 보안 위협을 실시간으로 감시하고 탐지된 이벤트에 효율적으로 대응할 수 있는 자동화된 보안 시스템으로 고객의 서비스를 안전하게 보호	Managed Service
Web Security Checker	Web Security Checker는 웹 서비스의 잠재적 취약점을 사전에 탐지하고 조치할 수 있도록 신속하고 상세한 검사를 진행하고, 발견된 취약점을 대응하기 위한 가이드가 포함된 리포트를 받아볼 수 있습니다.	
Cloud log Analytics	서버를 비롯하여 네이버 클라우드플랫폼이 제공하는 다양한 서비스에서 발생하는 다양한 로그들을 한 곳에 모아 저장하고 손쉽게 분석	
Cloud Activity Tracer	네이버 클라우드 플랫폼 서비스 상에서 발생한 계정 활동 로그를 자동으로 수집해주는 서비스입니다. 기본적으로 Console 및 API를 통한 계정 활동 로그가 수집되며, 수집된 계정 활동 이력은 Cloud Activity Tracer의 Console을 통해 간편하게 열람	
System Security Checker	고객 서버의 운영체제와 WAS의 보안 설정을 점검하여 취약점을 보완하기 위한 결과 리포트를 제공	
Cloud DB for MySQL	INZENT eXperDB가 지원하는 이 DBMS는 다른 데이터 소스와 통합되고 쉽게 관리 할 수 있는 엔터프라이즈 급 데이터베이스 솔루션을 제공합니다. 모든 기능을 갖춘 관계형 데이터베이스 인 PostgreSQL은 1996 년부터 오픈 소스 라이센스를 받고 있습니다.	㈜인젠트 제공
Petra	DB접근제어는 사용자가 DBMS에 로그인 하거나 SQL을 수행하려고 할 때 미리 정의된 보안규칙에 따라 권한 여부를 판단하여 통제하는 솔루션	마켓플레이스 제공

Ⅲ 자체 보안대책 강구사항

1. 관리적 보안대책

가. 사고 대응

○ 국가 정보보안 관련 규정 준수
○ 정보보안 정책 수립 및 변경 관리
○ 담당자 지정 및 역할 정의



구 분	핵심 역할	비고
사업담당 (정보시설안전팀)	▸ 정보보호관리체계 수립 및 운영관리와 감독 ▸ 사업자 선정 추진 및 사업투입 인력 관리 - 타 업무부서와의 업무협조 체제 정립 ▸ 사업수행업체 진도관리 및 검수	-
협조부서 (유관부서)	▸ 클라우드 이관 실무업무 분석·개발 지원	-
사업수행업체	▸ 한국잡월드 홈페이지 및 전시운영, POS시스템 주요 업무시스템 클라우드 이관 및 유지관리 주관	-

나. 사고 대응

○ 해킹사고 발생 시 대응 매뉴얼 개발
○ 보안사고 발생 시 로그정보 등을 제공 받기 위한 사전협조 체계 구축

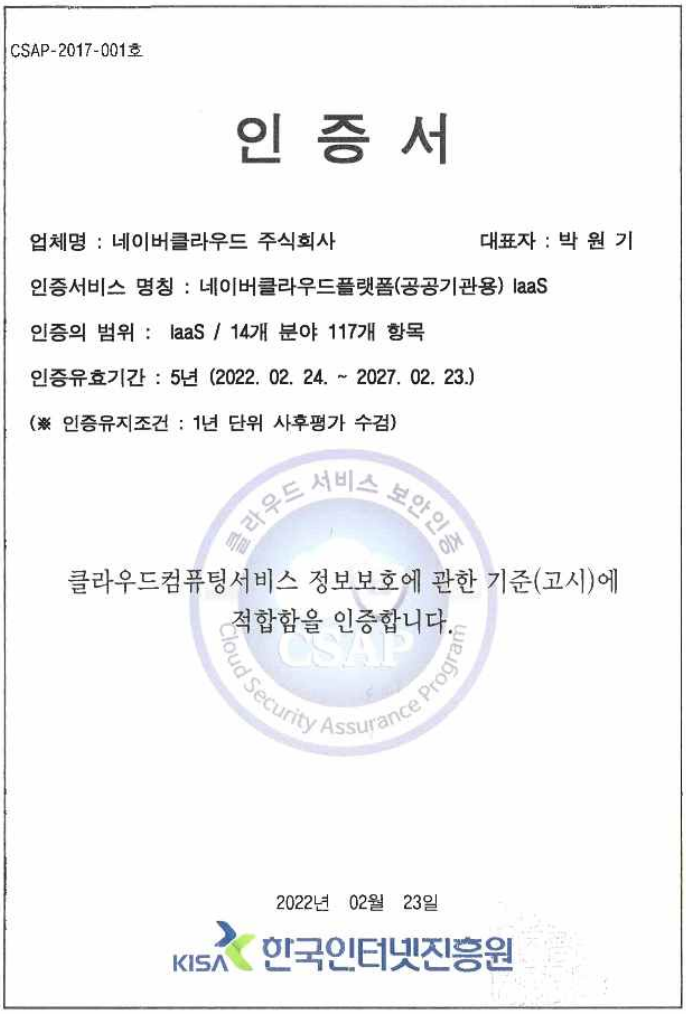
다. 보안 교육 및 점검

○ 사업 투입인력 전원 대상으로 보안 교육 실시 및 보안서약서 징구
○ 사업 투입인력의 보안준수 사항 확인 및 위반시 배상책임 명시
○ 사업 투입인력의 정보시스템 접근권한 및 제공자료 보안대책

○ 매월 용역사업 보안 점검 실시(용역 사업장 보안관리 실태 점검)
○ 개발PC 인터넷 전면 금지 및 USB 포트 봉인
○ 필요시 인터넷 전용 PC 설치 및 산출물 전용 PC 비치 운영 등

2. 물리적 보안

가. 클라우드 물리적 보안 대응 CASP IaaS인증



CSAP-2017-001호

인 증 서

업체명 : 네이버클라우드 주식회사 대표자 : 박 원 기

인증서비스 명칭 : 네이버클라우드플랫폼(공공기관용) IaaS

인증의 범위 : IaaS / 14개 분야 117개 항목

인증유효기간 : 5년 (2022. 02. 24. ~ 2027. 02. 23.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에
적합함을 인증합니다.

2022년 02월 23일

KISA 한국인터넷진흥원

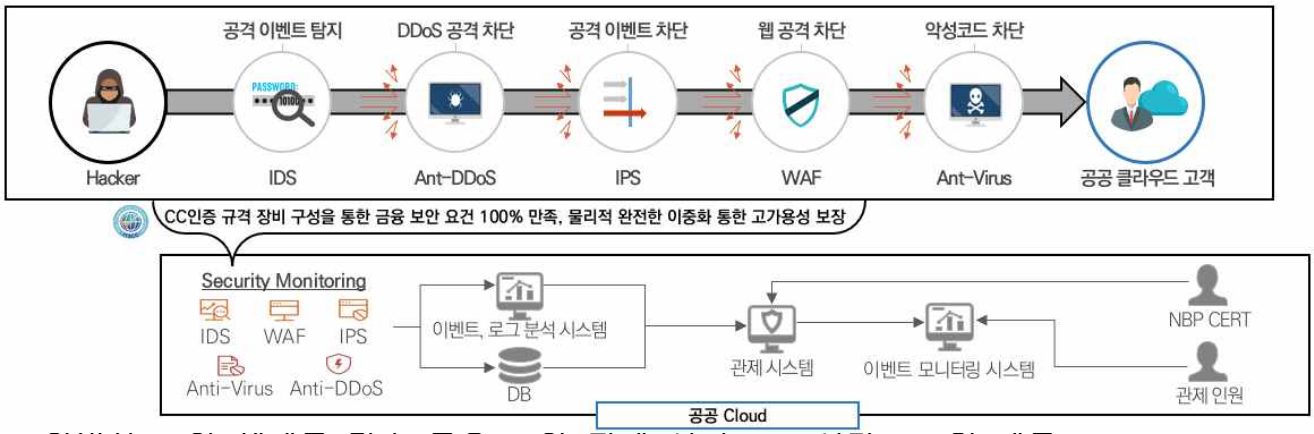
○ CASP IaaS인증에 8. 물리적보안 항목인 8.1 물리적 보호구역과 8.2 정보처리 시설 및 장보호 항목으로 대처함

3. 기술적 보안대책

가. 네트워크 보안

○ 공공 클라우드의 보안관제 서비스는 24*365 자체 보안관제를 제공하며 실시간으로 탐지·대응이 가능하여 전문보안관제 인력을 통해 보안분석을 지원

○ 탐지된 위협요소에 대해서는 재 침입 방지를 위한 취약점 점검 및 개선 사항을 리포트로 제공



○ 완벽한 보안 체계를 갖춘 금융 보안 관제 서비스 24시간 365일 제공

- 외부의 보안 위협을 실시간으로 감시하고 탐지된 이벤트에 효율적으로 대응할 수 있는 자동화된 보안시스템으로 고객 서비스를 안전하게 보호합니다.

○ 최적화된 보안 정책 제공

- 최고 수준의 보안 전문가 조직을 통하여 지능화, 조직화된 공격 기법을 정확히 탐지/

모니터링 하며, 서비스의 물리적 이중화를 통해 업무 연속성을 100% 보장합니다.

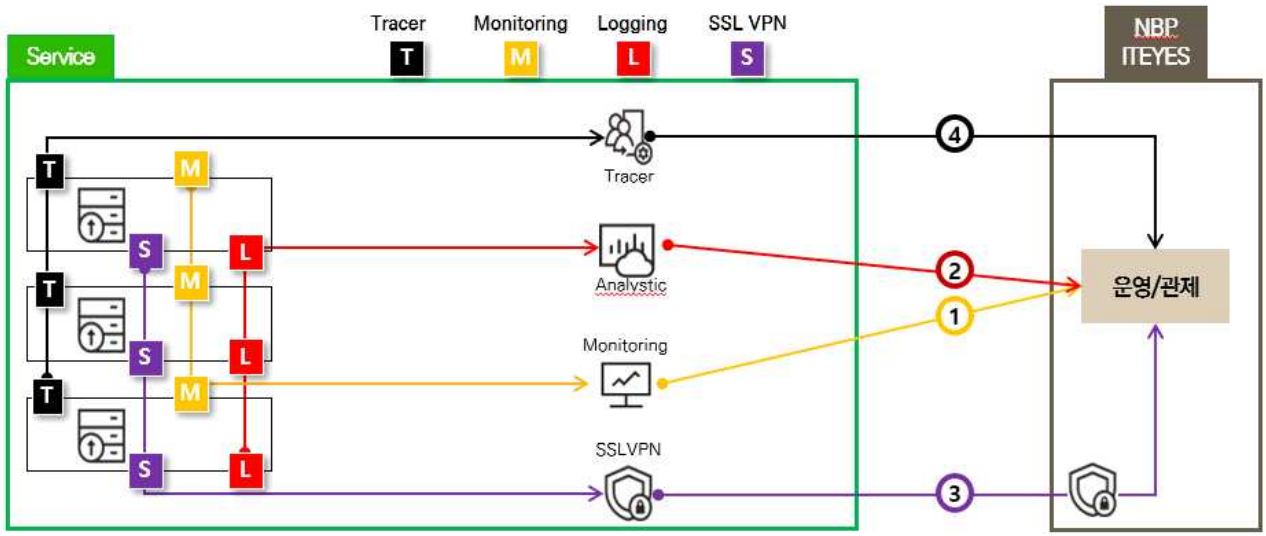
○ 모니터링부터 정기 보고서 까지 원스톱 서비스

- 공격 이벤트를 모니터링 하고 고객에게 통보함으로써 고객 서비스에 대한 보안위협을 원천 차단하며, 탐지된 보안위협에 대한 분석 리포트 및 대응 가이드를 제공합니다.

○ 네트워크 보안 시스템 주요 기능

- **WAF (웹방화벽서비스)** : Web기반(HTTP/HTTPS) 트래픽을 모니터링하여 고객의 웹서비스로 공격이 인입될 경우, WAF 전용 솔루션을 통해 탐지/방어함으로써 즉각적인 대응이 가능하도록 지원하는 서비스
- **침입방지 (IPS, Intrusion Prevention System)** : IP, 포트에 대한 패턴 분석으로 침입 탐지 및 차단
- **Anti-DDoS(Distributed Denial of Service, 분산 서비스 거부)** : 네트워크 트래픽의 외부에서 공격을 탐지하여 차단
- **IDS (침입탐지서비스)** : 실시간 공격을 탐지하여 고객의 서비스를 안전하게 보호
- **Anti-Virus(안티 바이러스)** : 네트워크를 통과하는 콘텐츠 중 바이러스나 웜 등 악성 프로그램을 검사하고 차단
- **침해 사고 기술 지원** : 고객의 서비스에 침해사고가 발생하면 대응 전문가가 침해사고에 대한 분석을 수행하고 원인을 파악해 이후에 똑같은 피해가 발생하지 않도록 지원하는 서비스

○ 네트워크 보안 관제 모니터링 구성



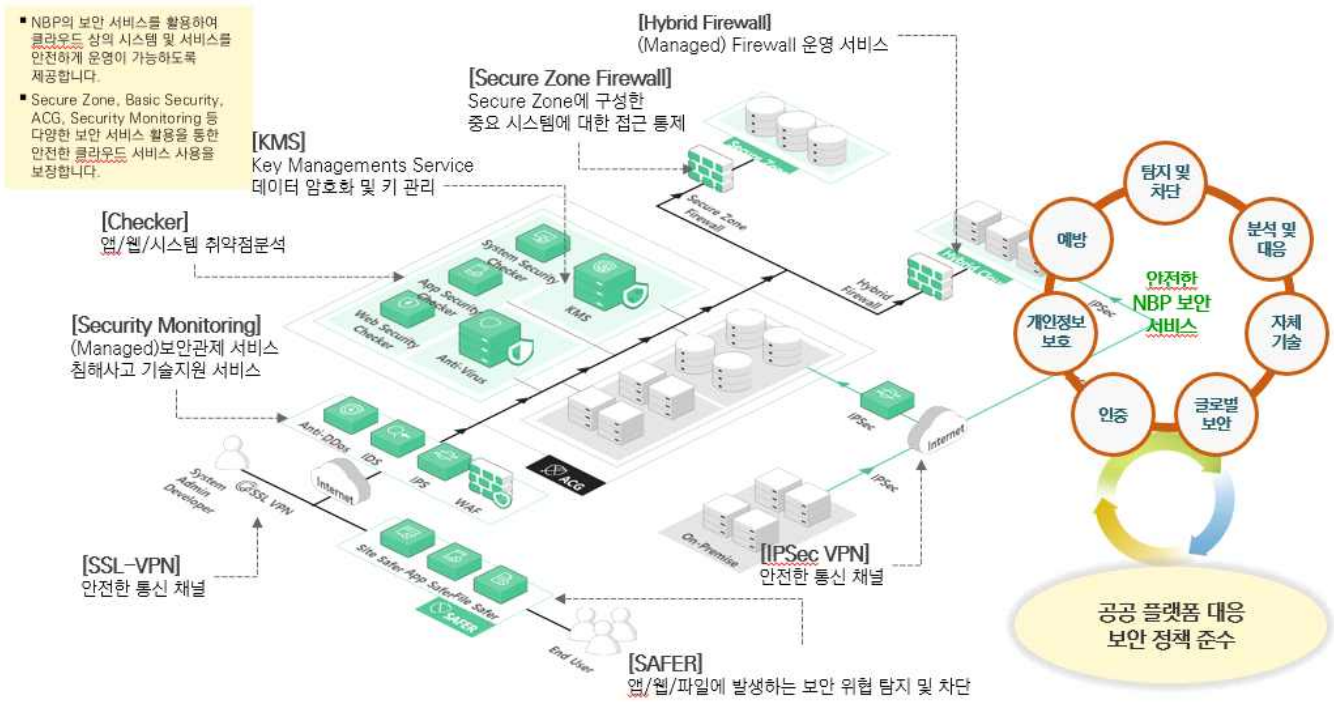
1. 시스템 모니터링: 네이버 클라우드의 Monitoring를 사용하여 경기도청, NBP, ITEYES 관제

2. Log 수집분석: Cloud Log Analytics를 이용하여 서비스의 Log를 수집/분석

3. 시스템 운영 접속: 클라우드 센터와 한국잡월드 사이에 연결된 SSL VPN을 이용하여 서버에 접속

4. Tracer: 서버 접속 이력 관리

나. 클라우드 센터 보안



○ 전산보안 정책을 준수하고 고객의 안전한 거래 보장 및 내부 전산자원의 보호가 가능한 센터

다. 소프트웨어 보안

○ 업무용 소프트웨어에 대해서 도입 전 취약점 및 보안조치 수행
○ 준공 전 개발 소스코드 취약점 진단 후 조치 완료한 운영서버 설치
○ 도입 시 全 개발PC 및 서버 장비 포맷 실시
○ 개발PC 내 산출물 정보 및 소스코드 보유 여부 수시 점검
○ 준공 후 도입된 全 개발PC 및 서버 장비 포맷 후 반출 처리
○ 장비 반입·반출 및 자료 무단반출 여부 점검

라. 전산자료 보안

○ 암호화된 인증체계(SSO)로만 접속가능하고 우회경로 사전차단
○ 백신 및 악성코드 치료프로그램 설치, 상시 업데이트
○ 사이버위협 탐지 시 사이버보안센터에 신고

Ⅳ 기타

1. 제안요청서/과업지시서

* 별도 사업계획서 존재시 작성 또는 붙임형태로 제출

2. 타기관 보안관리 협의사항

* 국가기관간 망 연동시 해당 기관간 보안관리 협의사항 존재시 작성 또는 붙임형태로 제출