



NHN Cloud 보안 백서

NHN Cloud Security White Paper



NHN Cloud 보안 백서

저작권

Copyright NHN Cloud Corp. All rights reserved.

이 문서는 NHN Cloud의 지적 자산이므로 NHN Cloud의 승인 없이 문서를 다른 용도로 임의 변경하여 사용할 수 없습니다.

이 문서는 정보 제공의 목적으로만 제공됩니다. NHN Cloud는 이 문서에 수록된 정보의 완전성과 정확성을 검증하기 위해 노력하였으나, 발생할 수 있는 내용상의 오류나 누락에 대해서는 책임지지 않습니다. 따라서 이 문서의 사용이나 사용 결과에 따른 책임은 전적으로 사용자에게 있으며, NHN Cloud는 이에 대해 명시적 혹은 묵시적으로 어떠한 보증도 하지 않습니다.

관련 URL 정보를 포함하여 이 문서에서 언급한 특정 소프트웨어 상품이나 제품은 해당 소유자의 저작권법을 따르며, 해당 저작권법을 준수하는 것은 사용자의 책임입니다.

NHN Cloud는 이 문서의 내용을 예고 없이 변경할 수 있습니다.

문서 이력

버전	일자	이력 사항
1.0 버전	2023. 6.	NHN Cloud 보안 백서 1.0 버전 출시

목차

NHN Cloud 보안 백서	2
저작권	2
문서 이력	2

1장. 클라우드의 이해와 개념

1 클라우드 컴퓨팅의 개념	7
1.1 클라우드의 개념	7
1.1.1 클라우드란?	7
1.1.2 클라우드 서비스의 장점	7
1.1.3 클라우드 서비스 제공 형태	8
1.1.4 클라우드 서비스 유형	9
1.1.5 NHN Cloud와 OpenStack	10
1.2 클라우드 보안 위협	11
1.3 보안 책임 공유 모델	13

2장. NHN Cloud의 보안

2 NHN Cloud 정보보호 체계	17
2.1 NHN Cloud 정보보호 목적	17
2.2 NHN Cloud 정보보호 관리 체계	17
2.2.1 정보보호 정책 및 조직	17
2.2.2 서비스 개발 및 운영 프로세스	18
2.3 규정 준수와 인증	19
2.3.1 법령과 규정 준수	19
2.3.2 정보보호 인증 현황	19
2.4 비즈니스 연속성 관리	23
3 NHN Cloud 물리보안	24
3.1 데이터 센터 보안 관리	24
3.1.1 환경 및 설비 보안	24
3.1.2 출입 통제	25
3.1.3 자료 및 설비 관리	25
4 NHN Cloud 클라우드 플랫폼 보안	26
4.1 클라우드 플랫폼 보안	26
4.1.1 호스트 보안	26
4.1.2 데이터 보안	27
4.1.3 네트워크 보안	27
4.1.4 가상화 보안	30

5 NHN Cloud 계정 보안	31
5.1 이용자 계정 보안	31
5.1.1 멤버(Member)	31
5.1.2 인증(Authentication)	32
5.1.3 권한 부여	34
5.1.4 감사(Audit)	37
6 NHN Cloud 보안 관제 및 예방	38
6.1 보안 모니터링 및 취약점 진단	38
6.1.1 위협 탐지 및 대응	38
6.1.2 취약점 점검과 모의 훈련	40
7 NHN Cloud 가상화 인프라 보안	41
7.1 클라우드 가상화 인프라 보안	41
7.1.1 Compute	41
7.1.2 컨테이너	43
7.1.3 스토리지	46
7.1.4 네트워크	51
7.1.5 데이터베이스	58
8 NHN Cloud 보안 서비스	62
8.1 클라우드 보안 서비스	62
8.1.1 취약점 점검	62
8.1.2 네트워크 보안	63
8.1.3 시스템 보안	65
8.1.4 보안 관리	67
8.1.5 암호 및 인증	67

1장. 클라우드의 이해와 개념

정보 통신 산업의 흐름이 하드웨어와 소프트웨어에서 클라우드 컴퓨팅과 인공 지능으로 끊임없이 변화하면서 점점 더 빠른 속도를 내고 있습니다. 4차 산업 혁명의 핵심 기술 중 하나인 클라우드 컴퓨팅은 인터넷을 기반으로 정보 기술 서비스를 언제 어디서나 이용할 수 있게 했습니다.

공공 및 민간 분야를 포함한 다양한 산업군의 요구가 증가하고, 신속한 서비스 제공과 기업의 이익 확대를 위해 비즈니스의 민첩성이 요구되고 있습니다. 이와 같은 상황에서 클라우드는 무한 확장과 빠른 서비스 구성을 가능하게 해 많은 기업들이 클라우드를 우선 고려하게 되었습니다.

클라우드 컴퓨팅의 확산으로 새로운 서비스와 기술이 등장하면서 데이터 분산과 증가가 심화되고 있습니다. 또한 그만큼 서비스의 연속성과 안전성에 영향을 주는 보안 위험도 함께 늘어나고 있습니다. 이에 대응하기 위해 많은 기업과 기관들이 전사적인 조직 체계를 구축해 다양한 영역에 대한 보안 관리 활동을 하고 있습니다. 차세대 인프라의 핵심인 클라우드 컴퓨팅 환경에서도 보안 관리는 중요한 요소가 되었습니다.

본 백서는 이러한 변화에 대응하고, 클라우드와 클라우드 환경의 보안을 이해하며, NHN Cloud 제품과 서비스를 이해할 수 있도록 돕기 위해 제작되었습니다. 본 백서는 크게 ‘1장. 클라우드의 이해와 개념’과 ‘2장. NHN Cloud의 보안’으로 구성되었습니다. ‘1절. 클라우드 컴퓨팅의 개념’으로 구성된 ‘1장. 클라우드의 이해와 개념’에서는 클라우드의 기본 개념과 제공 형태 및 서비스 유형을 비롯해 클라우드 오픈 소스 플랫폼인 OpenStack을 간략히 설명합니다. 또한 클라우드 환경에서의 보안 위협과 클라우드 서비스 공급자(cloud service provider, CSP)와 클라우드 서비스 이용자(cloud service customer, CSC)의 보안에 대한 책임과 역할을 정의한 보안 책임 공유 모델에 대해 설명합니다. 2절부터 8절로 구성된 2장의 내용은 ‘2장. NHN Cloud의 보안’에서 확인할 수 있습니다.

본 백서는 클라우드의 이해 및 NHN Cloud가 제공하는 보안 체계와 기술을 이해하기 위한 목적으로 작성되었습니다. 클라우드 또는 보안에 생소했던 이용자에게는 안전하고 연속성을 갖춘 클라우드 환경을 더욱 쉽게 구현하기 위한 자습서가 될 것이며, 이미 익숙한 이용자에게는 전문가로서 더욱더 능숙하고 빠르게 클라우드 환경을 구현해 비즈니스 목표를 더욱 빠르게 달성하는 것에 도움이 되고자 합니다.

본 백서를 NHN Cloud의 이해와 학습을 위한 도구로 활용하고, 이를 기반으로 서비스 아키텍처를 수립할 수 있습니다. 또한 클라우드 서비스 이용 시 적절한 기술적 보안 대책을 마련하는 데 참고할 수 있으며, 취약점 관리, 위협 탐지 및 대응, 인증, 컴플라이언스, 접근 통제, 데이터 보호 및 암호화 서비스를 이용한 안전한 서비스 인프라 구성 시에도 활용할 수 있습니다. NHN Cloud는 다양한 국내외 보안 인증을 획득하였기에 규제 준수 및 감독 기관의 증적 자료 제출을 위해 사용할 수 있습니다.

1 클라우드 컴퓨팅의 개념

1.1 클라우드의 개념

1.1.1 클라우드란?

클라우드 컴퓨팅(cloud computing)은 인터넷을 통해 가상 컴퓨팅 리소스(서버, 네트워크, 스토리지, 애플리케이션 등)에 언제 어디서나 접근하고 사용할 수 있는 주문형 서비스입니다. 클라우드 환경에서 이용자는 직접 리소스를 구축하거나 관리할 필요가 없으며, 필요한 만큼만 사용하고, 사용한 만큼만 비용을 지불합니다. 클라우드 컴퓨팅은 자원의 효율적인 사용과 유연한 IT 자원을 제공해 기업과 개인에게 많은 이점을 제공합니다.

1.1.2 클라우드 서비스의 장점

클라우드 환경은 기업이 서버, 스토리지 등 IT 인프라를 자체 데이터 센터나 전산실에 직접 구축하고 운영하는 온프레미스(On-premises) 환경에 비해 몇 가지 장점이 있습니다.

1. 신속한 인프라 도입

- 클라우드 컴퓨팅 환경은 IT 리소스를 신속하게 확보할 수 있습니다. 자체 인프라를 갖추지 않아도 될 뿐만 아니라, 애플리케이션의 설계와 개발에 소요되는 시간을 줄여 서비스를 빠르게 개발할 수 있습니다.

2. 합리적인 비용 관리

- 사용하는 시간이나 용량을 이용자가 합리적으로 선택할 수 있고, 사용한 만큼만 비용을 지불합니다.

3. 유연한 인프라 관리

- 클라우드 환경에서는 컴퓨팅 리소스를 자유롭게 증감할 수 있습니다. 서비스 변화에 따라 필요한 만큼 인프라를 빠르게 확장하거나 축소할 수 있기 때문에 인프라 부족이나 과도한 도입의 문제를 예방할 수 있습니다.

4. 강력한 보안과 서비스 연속성

- 데이터와 개인정보를 안전하게 보관하기 위한 보안 솔루션 및 보안 기술뿐만 아니라, 물리적으로 분리된 상호 보완용 데이터 센터(리전)를 운영합니다. 또한 장애로 인한 비즈니스 손실을 방지하기 위해 이중화 및 가상화 기술을 활용해 서비스 연속성을 보장합니다.

5. 글로벌 서비스 접근성

- 클라우드 서비스 공급자가 미리 구축한 글로벌 데이터 센터를 활용해 대기업뿐만 아니라 중소기업도 서비스를 손쉽게 전 세계 어디에나 빠르게 제공할 수 있습니다.

1.1.3 클라우드 서비스 제공 형태

클라우드 컴퓨팅은 서비스 제공 형태에 따라 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud), 하이브리드 클라우드(hybrid cloud)로 구분합니다.

1. 퍼블릭 클라우드

- 클라우드 서비스 공급자가 인터넷을 통해 이용자들에게 서버, 네트워크, 스토리지, 데이터베이스 및 애플리케이션 등의 컴퓨팅 리소스를 제공하는 형태입니다. 이용자별로 권한 관리와 격리를 할 수 있어 서비스 이용자 사이의 간섭은 없습니다.

2. 프라이빗 클라우드

- 특정 기업이나 조직의 전용 용도로 컴퓨팅 리소스를 제공하고 관리하는 형태입니다. 이용자가 직접 운영하고 관리하기 때문에 상황에 맞춰 유동적으로 서비스를 활용할 수 있고, 폐쇄적인 형태로 보안, 규제, 데이터 소유권 등에 대한 요구가 강한 기업에 적합합니다.

3. 하이브리드 클라우드

- 앞서 이야기한 퍼블릭 클라우드와 프라이빗 클라우드를 혼합해 사용하거나 클라우드와 온프레미스를 결합한 형태를 말합니다. 퍼블릭 클라우드의 신속성, 경제성 및 유연성과 프라이빗 클라우드의 보안성과 독립성을 함께 얻을 수 있다는 장점이 있습니다. 최근에는 주요 데이터나 데이터베이스는 온프레미스에 구성하고 웹 서버나 트래픽을 예상하기 어려운 서비스는 클라우드를 이용하는 형태가 증가하는 추세입니다.

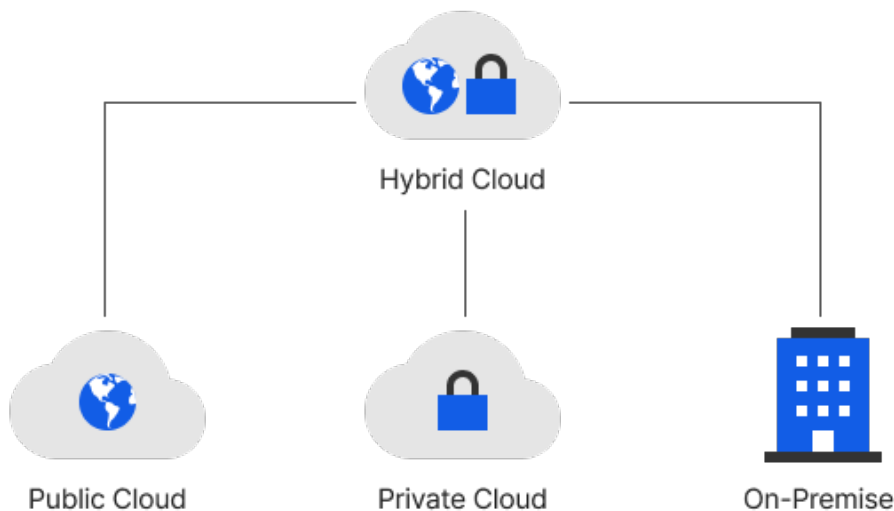


그림 1-1 클라우드 서비스 제공 형태

1.1.4 클라우드 서비스 유형

클라우드 서비스 관리 주체와 수준에 따라 서비스를 IaaS (infrastructure as a service), PaaS (platform as a service), SaaS (software as a service)로 구분할 수 있습니다.

1. IaaS

- 클라우드 서비스 공급자는 데이터 센터를 구축해 서버, 네트워크, 스토리지 등 서비스 운영에 필요한 인프라를 제공하고, 이용자는 가상화된 리소스를 이용해 OS, 미들웨어, 데이터 및 애플리케이션 등을 직접 구성하는 서비스로 이용자의 관리 범위가 가장 넓은 클라우드 컴퓨팅 서비스입니다.

2. PaaS

- 개발자나 애플리케이션 관리자가 애플리케이션을 개발, 배포, 관리할 수 있는 플랫폼을 미리 구성해 서비스 형태로 제공하는 것을 의미합니다. 개발자에게 필요한 인프라와 개발 도구, 플랫폼 서비스를 제공해 개발 및 배포 프로세스를 간소화할 수 있고, 인프라에 대한 자유도는 낮지만 운영체제, 소프트웨어 관리 등 유지 보수 비용을 줄이면서 개발에 집중할 수 있습니다.

3. SaaS

- 클라우드 인프라에 애플리케이션을 구성해 제공하는 형태로 IT 인프라 자원뿐만 아니라 소프트웨어, 애플리케이션의 업데이트나 버그도 서비스 공급자가 모두 책임지고 관리합니다. 별도의 인프라 구축, 애플리케이션 개발 및 관리를 하지 않고 구독 사용료를 지불하고 서비스를 이용하기만 하면 됩니다.

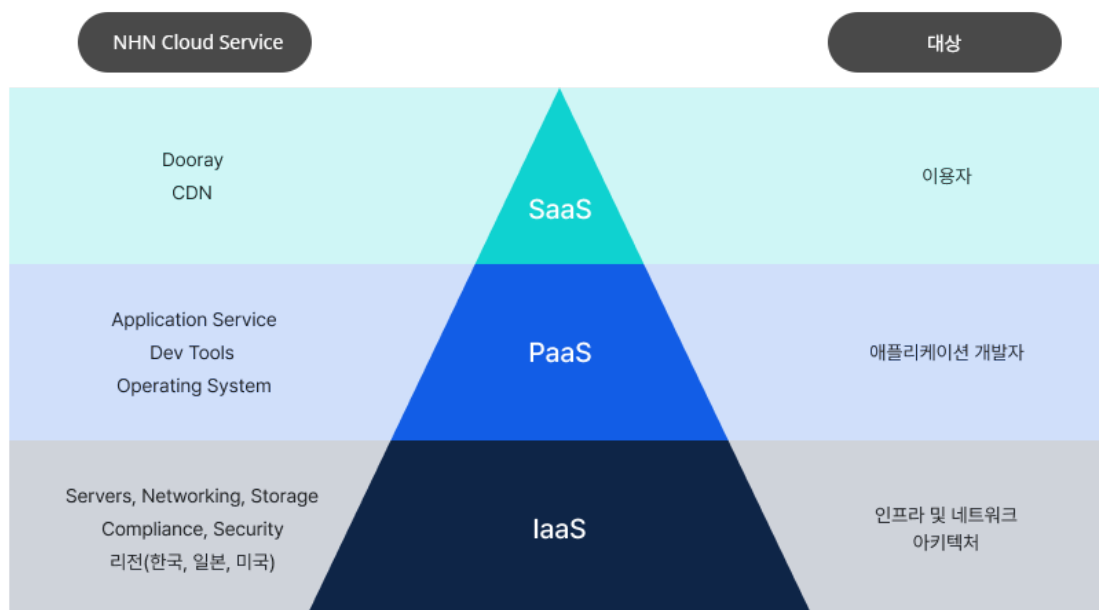


그림 1-2 클라우드 서비스 유형

1.1.5 NHN Cloud와 OpenStack

NHN Cloud는 OpenStack 클라우드 플랫폼을 활용해 클라우드 인프라와 서비스를 제공하고 있습니다.

OpenStack은 컴퓨트(Nova), 네트워킹(Neutron), 이미지(Glance), 블록 스토리지(Cinder), 오브젝트 스토리지(Swift), 인증 서비스(Keystone) 등 다양한 제어 모듈을 통해 클라우드 구성과 기능을 제공하는 통합 클라우드 플랫폼입니다.

OpenStack은 2012년 창설된 비영리 단체인 OpenStack Foundation에서 제공 및 유지 보수하고 있으며 Apache 라이선스 하에 배포됩니다. NHN Cloud는 OpenStack이 가진 장점 위에 기능과 성능 강화를 위한 다양한 요소를 추가 개발하고 커스터마이징하여 공공, 게임, 금융, 커머스를 포함해 다양한 영역의 특화된 요구 사항에 맞게 IT 서비스를 더 유연하고 안전하게 이용할 수 있는 클라우드 서비스를 제공하고 있습니다.

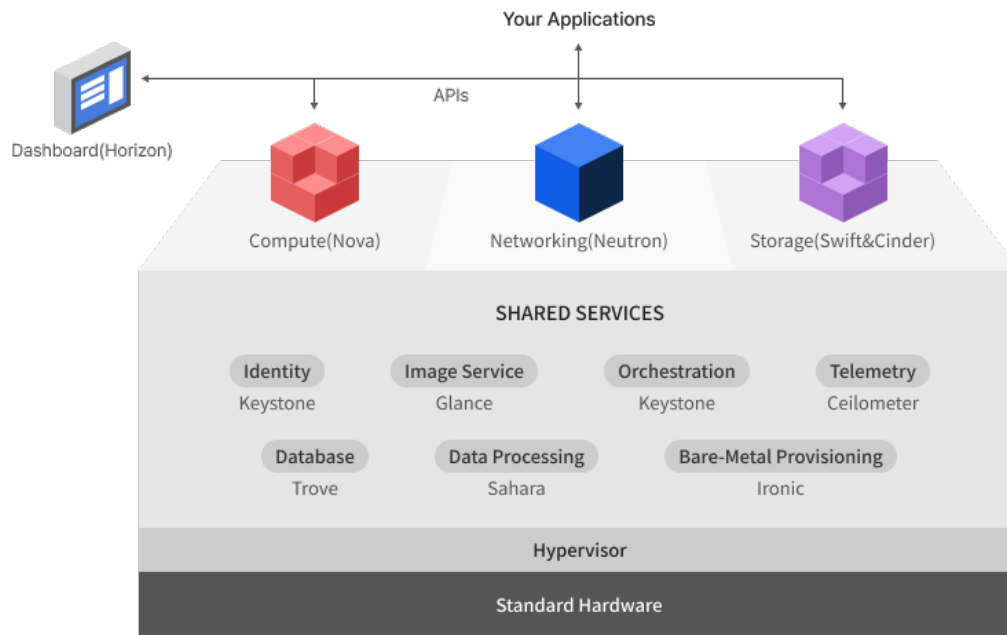


그림 1-3 OpenStack 기본 인프라 구조

1.2 클라우드 보안 위협

클라우드 컴퓨팅은 기존 정보 시스템 환경에서 나타날 수 있는 취약점 공격, 악성 코드 감염 및 DDoS와 같은 보안 위협과 더불어 가상화 기술, 자원의 공유 및 인터넷을 통한 접속이라는 특징으로 인해 가상화 취약점이나 레거시 인프라에 없었던 유형의 보안 위협도 다양하게 발생할 수 있습니다.

편리하고 유연한 클라우드를 안전하게 이용하기 위해서는 클라우드 이용자와 공급자가 각자의 영역에서 적극적인 정보보호 활동을 수행해야 하며 이를 위해 클라우드의 구조와 보안 관리 방안을 정확히 이해하고 가상 환경에 적용해 나가는 것이 필요합니다.

이를 위해, 클라우드 보안 위협을 관리적, 기술적 분류로 살펴보고 이러한 위협을 최소화할 수 있도록 해야 합니다.

표 1-1 클라우드 보안 위협

분류	보안 위협
관리적 보안 위협	클라우드 컴퓨팅 남용 및 악용
	내부자 위협
	클라우드 보안 아키텍처와 전략 미흡
	불충분한 ID, 자격 증명, 액세스 및 키 관리
기술적 보안 위협	잘못된 설정과 부적절한 변경 관리
	안전하지 않은 API
	가상화 취약점
	계정 하이재킹
	데이터 유출
	서비스 거부 공격(DDoS)
	시스템 취약점

1. 클라우드 컴퓨팅 관리적 보안 위협

클라우드 컴퓨팅은 수많은 이용자가 하나의 대용량 인프라를 공유하는 환경입니다. 따라서 관리적 측면에서도 보안에 대한 위험성을 최소화할 수 있도록 점검해야 합니다.

• 클라우드 컴퓨팅 남용 및 악용

악의적인 행위자는 클라우드 컴퓨팅 자원을 이용해 악의적인 행위를 정상 서비스처럼 활용할 수 있습니다. 클라우드 서비스 남용과 오용을 막기 위해서 기업은 클라우드 이용자의 신원을 철저하게 검증하는 절차를 도입하고, 이용자의 행위를 감시하고 데이터 손실 방지 기술을 사용해 무단 데이터 유출을 감시하고 차단해야 합니다.

• 내부자 위협

내부자는 재직 중이거나 퇴사한 임직원, 계약자 또는 그 외 신뢰할 수 있는 비즈니스 파트너일 수 있습니다. 내부자는 내부 중요 데이터에 직접 접근할 수 있어 그 위험성이 상당히 크기 때문에 사용자 계정과 권한에 대한 지속적인 관리와 감시가 이루어져야 하고, 특정 이용자에게 권한이 집중되지 않도록 최소한의 권한을 부여해야 합니다.

• 클라우드 보안 아키텍처와 전략 미흡

클라우드 구축 및 이전 시 기존 IT 스택과 보안을 그대로 이식하거나, 속도를 보안보다 우선시할 경우 클라우드 보안 아키텍처와 전략이 미흡해 공격에 취약해질 수 있습니다. 비즈니스 목적에 맞는 보안 아키텍처를 구현해 단단한 기반을 확보함으로써 안전한 서비스와 전반적인 보안 상태를 유지해야 합니다.

• 불충분한 ID, 자격 증명, 액세스 및 키 관리

ID, 자격 증명, 액세스 관리 시스템은 조직이 중요 자산에 안전하게 접근하고, 이를 관리·감시할 수 있는 도구와 정책을 포함하고 있습니다. 클라우드 서비스 이용 시 이용자 인증과 권한 관리는 매우 중요하며, 2단계 인증, 제한된 루트 계정 사용과 액세스 제어, 최소 권한 원칙 및 키 관리 등을 통해 치명적인 피해가 발생하지 않도록 주의해야 합니다.

- 잘못된 설정과 부적절한 변경 관리

잘못 설정된 클라우드 리소스는 데이터 유출 또는 리소스 삭제, 변경 등으로 서비스 중단을 야기할 수 있습니다. 이러한 잘못된 설정은 변경 관리의 부재로 발생합니다. 빠르고 유동적인 클라우드 환경에서 기업은 자동화를 도입하거나 잘못 설정된 자산이 있는지 지속적으로 검색하고 문제를 해결하기 위해 노력해야 합니다.

2. 클라우드 컴퓨팅 기술적 보안 위협

클라우드 서비스가 이용자에게 편리한 사용과 다양한 서비스를 제공하고 있지만, 그 이면에는 클라우드의 복잡한 인프라 구조와 다양한 최신 기술들이 포함되어 있습니다. 이러한 환경에서 클라우드 고유의 보안 위협이나 기존의 전통적인 보안 위협들이 존재합니다. 클라우드 서비스 공급자와 클라우드 서비스 이용자는 각자의 역할과 책임에 맞게 보안을 확립해 나가야 합니다.

- 안전하지 않은 API

클라우드 서비스 공급자는 이용자가 다수의 애플리케이션을 이용하거나 데이터에 접근할 수 있도록 다양한 API를 제공합니다. 하지만 안전하지 않은 API의 취약점을 통해 보안 사고가 발생할 수 있습니다. 인증, 접근 제어, 암호화 및 모니터링에 이르기까지 이러한 API는 악의적인 위협으로부터 보호할 수 있도록 설계되어야 합니다. 클라우드 서비스 공급자는 안전한 API 설계, 테스트, 검사 등 철저히 관리 감독을 수행해야 하며, 클라우드 서비스 이용자는 API 보안 솔루션 및 API 키와 재사용 여부 등을 확인해야 합니다.

- 가상화 취약점

클라우드의 기술로 구성되는 것이 아니라 네트워크, CPU, 메모리, 스토리지 등 수많은 요소 기술이 서로 연결되어 서비스를 구성하고 있습니다. 하이퍼바이저, 하드웨어 및 기반 기술의 취약점은 전체 클라우드 환경의 위험 요소로 확산될 수 있기 때문에 클라우드 제공 업체는 가상 환경에 대한 취약점 패치, 악성 코드 및 취약점 공격을 상시 모니터링하고 대응해야 합니다.

- 계정 하이재킹

클라우드 서비스를 이용할 때 가장 기본이 되는 것이 계정입니다. 계정 정보에 기반을 두고 인증과 권한을 부여하게 됩니다. 이러한 계정이 탈취되면 사용자 조직과 자산의 손실로 비즈니스 위험을 초래할 수 있습니다. 클라우드 리소스 보호를 위한 심층 방어 보안 전략과 IAM 제어를 통해 계정 하이재킹 차단을 위한 노력을 기울여야 합니다.

- 데이터 유출

클라우드 이용자가 가장 두려운 것 중 하나는 데이터의 유출일 것입니다. 데이터 유출의 주 원인은 공격 대상이 되는 것, 사람의 실수, 애플리케이션 취약점 또는 잘못 구성된 보안 등입니다. 이러한 데이터 유출은 고객과 파트너의 평판과 신뢰에 악영향을 초래할 수 있으며, 비즈니스와 금전적 손실을 발생시킬 수 있습니다. 데이터를 적절하게 보호하고 지속적으로 유출 가능성을 모니터링해 중요 정보가 유출될 위험을 최소화하는 것이 중요합니다.

- 서비스 거부 공격(DDoS)

서비스 거부 공격은 대량의 트래픽 또는 요청으로 네트워크나 서버의 자원을 소진함으로써 서비스의 가용성을 저해하는 형태의 공격입니다. 클라우드 서비스를 구성하는 인프라 자원의 가용성을 저해하고, 나아가 클라우드 서비스를 이용하는 기업의 서비스도 사용할 수 없도록 할 수 있습니다. 클라우드 서비스 공급자는 자체 DDoS 방어 체계를 통해 클라우드 자원 및 이용자의 서비스를 보호하고, 클라우드 서비스 이용자는 불필요한 서비스 오픈이 발생하지 않도록 주의해야 합니다.

- 시스템 취약점

클라우드 컴퓨팅 환경에서의 시스템 취약점은 새로운 유형의 위협은 아닙니다. 일반적인 시스템 취약점에는 시스템 자체 소프트웨어 취약점(common vulnerabilities and exposure, CVE)과 환경 설정 미흡의 취약점(common configuration enumeration, CCE)이 있으며 클라우드 환경 또한 동일한 취약점을 가지고 있습니다. 오픈 소스 플랫폼, 하이퍼바이저, OS 등의 취약점을 이용해 권한을 획득하거나 보안 정책, 환경 설정 미흡, 계정이나 권한의 오남용, 취약한 패스워드 및 클라우드 콘솔 보안 설정 미흡으로 인해 노출될 가능성이 있습니다. 클라우드 서비스 공급자와 이용자는 각자의 역할과 임무에 맞게 보안 강화 활동을 해야 합니다.

1.3 보안 책임 공유 모델

보안 책임 공유 모델(shared security responsibility model, SSRM)이란 안전한 클라우드 서비스를 위해 클라우드 서비스 공급자와 클라우드 서비스 이용자의 책임과 역할을 분류하는 것입니다. 보안 책임 공유 모델의 목표는 서비스 공급자와 서비스 이용자가 협력해 각자가 통제하는 요소를 보호하여 클라우드 전반의 안전하고 신뢰성 있는 보안을 확립하는 것입니다.

NHN Cloud는 클라우드 서비스의 물리 시설, 물리 시스템 및 클라우드 인프라와 소프트웨어 등을 책임지며, 서비스 이용자는 클라우드 포털 고객 영역, 데이터 등을 책임집니다. 그 외 일부 책임은 IaaS, PaaS, SaaS의 서비스 모델에 따라 NHN Cloud와 서비스 이용자가 함께 공유합니다.

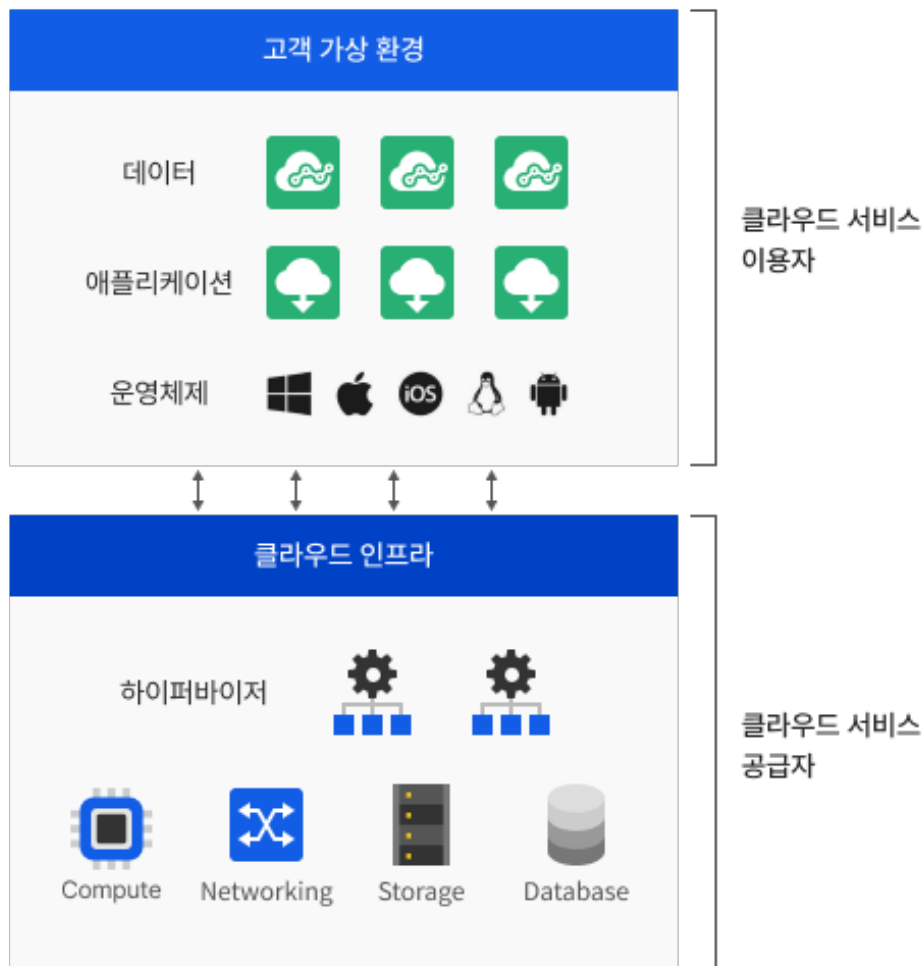


그림 1-4 클라우드 서비스 이용자와 공급자 영역

1. 클라우드 서비스 공급자의 책임 영역

NHN Cloud는 데이터 센터(IDC) 시설과 물리 시스템, 클라우드 인프라, 클라우드 제품 및 서비스의 보안을 책임지고, 고객에게 애플리케이션 및 데이터를 보호하는 데 필요한 기술과 기능을 제공합니다.

2. 클라우드 서비스 이용자의 책임 영역

서비스 이용자는 클라우드에서 가상 리소스와 데이터 보안을 위해 클라우드 제품 및 보안 서비스를 활용해 보안을 고려한 서비스를 구성하고 관리할 책임이 있습니다.

아래 매트릭스는 유형별 NHN Cloud의 보안 책임 공유 모델 영역입니다.

표 1-2 NHN Cloud의 보안 책임 공유 모델(SSRM)

분류	온프레미스	IaaS	PaaS	SaaS
클라우드 포털 고객 영역	●	●	●	●
데이터	●	●	●	●
애플리케이션	●	●	●	●
가상 네트워크	●	●	●	●
운영체제	●	●	● ●	●
하이퍼바이저, 클라우드 소프트웨어	●	●	●	●
물리 시스템 (시스템, 스토리지, DB, 네트워크)	●	●	●	●
물리 시설	●	●	●	●

● CSC(cloud service customer) ● CSP(cloud service provider)

• 클라우드 포털 고객 영역

클라우드 이용 고객의 서비스 영역으로 명확한 자산 식별과 보안 통제 적용은 서비스 이용자의 책임이 필요합니다.

• 데이터

서비스 이용자가 수집/생성하는 고객 데이터의 보안 통제 적용은 서비스 이용자의 책임이 필요합니다.

• 애플리케이션

애플리케이션에 대한 보안 책임은 서비스 공급자와 서비스 이용자가 공유합니다. IaaS와 PaaS 서비스는 서비스 이용자의 총괄적인 보안 관리 책임이 필요하며, SaaS 서비스는 서비스 공급자의 책임이 필요합니다.

• 가상 네트워크

클라우드 서비스를 구성하기 위한 네트워크 보안은 서비스 공급자와 서비스 이용자의 공동 책임이 필요합니다. IaaS와 PaaS 서비스는 서비스에 대한 네트워크 구성을 서비스 이용자가 수행하므로 서비스 이용자의 책임이 필요합니다. SaaS 서비스는 제공 서비스의 내부 네트워크는 서비스 공급자가 구성하여 제공하므로 서비스 공급자의 책임이 필요합니다. 네트워크 보안은 서비스 장애 및 침해 사고 등에 주요 이슈가 되므로 서비스 이용자는 클라우드 네트워크 서비스 스택에 대한 높은 이해가 필요합니다.

• 운영체제

운영체제에 대한 보안 책임은 서비스 공급자와 서비스 이용자가 공유합니다. IaaS와 일부 PaaS(예: NHN Kubernetes Service(NKS)) 서비스는 서비스 이용자의 운영체제 보안 관리 책임이 필요하며, 일부 PaaS(예: RDS for MySQL)와 SaaS 서비스는 서비스 공급자의 책임이 필요합니다.

• 하이퍼바이저, 클라우드 소프트웨어

클라우드 서비스의 근간인 하이퍼바이저와 클라우드 제공용 소프트웨어에 대한 보안은 서비스 공급자의 책임이 필요합니다. NHN Cloud는 OpenStack 기반의 클라우드 서비스 운영 노하우를 토대로 안전한 하이퍼바이저 보안을 책임지겠습니다.

• 물리 시스템(시스템, 스토리지, DB, 네트워크)

클라우드 서비스를 사용함으로써 생성되는 데이터에 대한 보안은 서비스 공급자의 책임이 필요합니다.

• 물리 시설

클라우드 서비스의 물리적 시설, 건물, 서버에 대한 관리 및 운영은 서비스 공급자의 책임이 필요합니다.

2장. NHN Cloud의 보안



그림 2 NHN Cloud 보안 프레임워크

NHN Cloud는 고객의 가상 환경이 안전하고 신뢰성 있게 운영될 수 있도록 클라우드 인프라와 서비스 보안에 최선을 다하고 있습니다. NHN Cloud는 정보보호 조직을 통해 관리적, 기술적, 물리적 보안을 위한 기준을 마련하고 정보보호 지침, 절차, 매뉴얼을 최신 상태로 유지·관리하고 있습니다.

클라우드에 대한 컴플라이언스 및 인증을 기반으로 클라우드 데이터 센터의 안전한 물리 시설과 클라우드 플랫폼, 이용자의 가상화 인프라, 클라우드 제품 및 서비스, 이용자 계정에 대한 보안 요소 기술을 적용하고 있습니다. 또한 다양한 클라우드 보안 위협에 대해 취약점 점검과 24시간 365일 실시간 위협에 대응함으로써 고객의 가상 인프라와 서비스를 안전하게 운영하고 있습니다.

이용자의 개인정보와 데이터 보호를 위한 다양한 보안 기능과 서비스를 제공하며, 다양한 영역과 시점에서 보안 위협에 적극 대응함으로써 안전한 클라우드 환경을 이용할 수 있도록 전략적인 보안 기능과 서비스를 지속적으로 마련하고 있습니다.

이러한 다양한 영역에서의 보안 활동은 ISMS-P, ISO27001, ISO27017, ISO22301, CSA STAR, CSAP 등 기업으로서뿐만 아니라 클라우드 서비스 공급자로서 필요한 인증을 획득하였습니다.

본 백서의 ‘2장. NHN Cloud의 보안’은 아래와 같이 2절~8절로 구성되었습니다.

2절 정보보호 체계는 NHN Cloud의 정보보호 조직, 정책, 프로세스, 규정 준수 및 정보보호 인증 현황과 비즈니스 연속성에 대해 설명합니다.

3절 물리 보안은 NHN Cloud의 클라우드 서비스 제공을 위한 데이터 센터와 물리적 환경 보안에 대한 규정, 절차 및 활동에 대해 설명합니다.

4절 클라우드 플랫폼 보안은 NHN Cloud의 클라우드 구성을 위해 필요한 물리 하드웨어, 저장 매체, 네트워크 및 가상화에 대해 설명합니다.

5절 계정 보안은 NHN Cloud를 이용하기 위해 필요한 회원, IAM 멤버의 인증과 권한 부여 및 감사에 대해 설명합니다.

6절 보안 관제 및 예방은 안전한 클라우드 서비스 제공을 위한 NHN Cloud의 보안 활동으로 24시간 365일 보안 관제를 통한 실시간 위협 탐지와 대응, 모의 해킹 및 취약점 점검의 예방 활동에 대해 설명합니다.

7절 NHN Cloud 가상화 인프라 보안은 이용자의 컴퓨트, 컨테이너, 스토리지, 네트워크 및 데이터베이스와 같은 주요 인프라 서비스와 접근 제어 및 데이터 보호를 위한 방법에 대해 설명합니다.

8절 NHN Cloud 보안 서비스는 추가적인 보안 제품과 서비스를 통한 시스템, 네트워크, 애플리케이션 보호 및 보안 컴플라이언스를 위한 보안 서비스에 대해 설명합니다.

2 NHN Cloud 정보보호 체계

2.1 NHN Cloud 정보보호 목적

NHN Cloud의 클라우드 컴퓨팅 서비스는 국내외 관련 법률 및 산업 표준을 준수합니다. 클라우드 서비스 제공을 위해 보안을 최우선으로 고려한 아키텍처 설계와 체계적인 운영을 통해 다양한 영역의 보안 시스템과 서비스로 클라우드 서비스 공급자의 관리망을 보호하고 안전성 확보를 위한 도구를 제공함으로써 이용자의 시스템과 데이터의 기밀성, 무결성 및 가용성을 안전하게 보호하는 데 있습니다.

2.2 NHN Cloud 정보보호 관리 체계

2.2.1 정보보호 정책 및 조직

NHN Cloud의 정보보호 정책 및 지침은 클라우드 제공, 정보통신망 이용이나 개인정보 처리 등 관련 법률을 준수하고 클라우드 서비스의 안전성과 신뢰성 확보를 위해 관리적, 물리적, 기술적 보호 조치의 기준을 명시하고 명확한 책임과 역할을 정하고 있습니다.

1. 정보보호 정책 체계

NHN Cloud의 정보보호 정책 및 지침은 정보보호 관련 법률 및 규정과 클라우드 컴퓨팅 서비스의 요구 사항을 고려해 정보보호 관리 체계를 운영하기 위한 세부적인 절차, 방법 등을 정의한 문서로 구성되어 있습니다. 정보보호 주관 부서는 최신 법률 및 보안 요구 사항 등을 고려해 지침의 제·개정 여부를 주기적으로 검토하고 최신으로 유지하며, 내부 시스템으로 운영 중인 정보보호 포털을 통해 전 임직원에게 공지하고 있습니다.

2. 정보보호 조직 구성

CEO 및 CISO, CPO를 지정하고 하위 실무 부서를 구성하고 있습니다. 정보보호 조직은 개인정보보호 주관 부서, 정보보호 주관 부서, 보안 인프라 영역을 담당하는 IT 보안 주관 부서로 구성되어 있습니다.

개인정보보호 주관 부서는 개인정보 관리적, 기술적 부문 및 관련 법률 검토 업무를 총괄합니다. 정보보호 주관 부서는 정보보호 및 규정 준수를 위한 관리적 보안 업무 및 개인정보보호 기술 부문을 수행합니다. IT 보안 주관 부서는 정보보호 시스템 구축 및 서비스 운영과 관련된 기술적 보안 업무를 수행합니다.

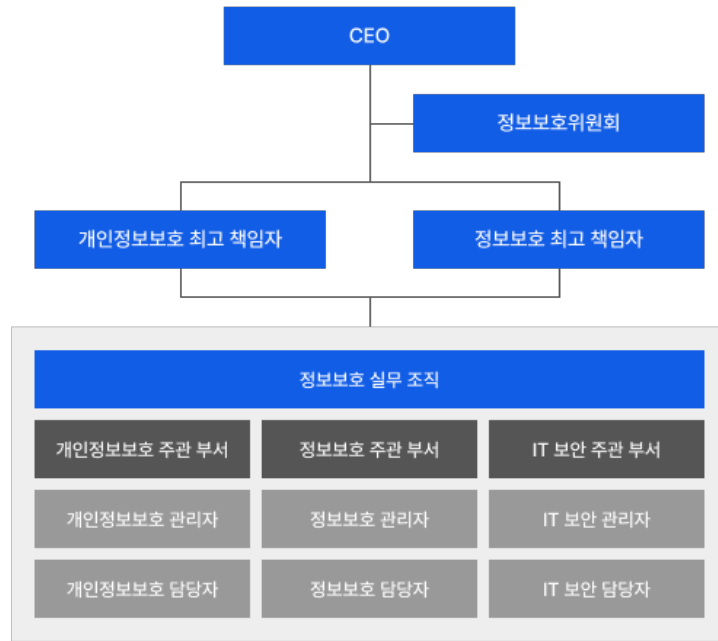


그림 2-1 NHN Cloud 정보보호 조직도

3. 역할과 책임

CEO(최고경영자)는 조직의 규모 및 서비스의 중요도에 따라 필요 인력, 예산 등을 고려하여 CISO, CPO, 정보보호 실무 조직을 지정합니다.

CISO(chief information security officer, 정보보호 최고 책임자)는 정보보호 정책 및 관리 체계를 수립하고, 정보보호 조직을 구성해 침해 사고 예방 및 대응, 취약점 분석, 평가 및 개선 등의 위험 관리 업무를 포함한 정보보호 활동을 총괄합니다. CPO(chief privacy officer, 개인정보보호 최고 책임자)는 개인정보보호에 대한 활동을 총괄하며, 개인정보보호 계획의 수립 및 관리, 관련 보안 시스템을 구축하고 교육 수행의 역할을 담당합니다. 정보보호 위원회는 정보보호 관련 주요 이슈 사항과 대응 방안을 마련하는 역할의 협의체이며 중요 이슈에 대한 의사 결정을 할 수 있는 책임자와 관리자로 구성됩니다.

그 외 각 역할 및 수행 사항에 대해서는 내부 정보보호 지침을 통해 관리되고 있습니다.

4. 정보보호 교육

전 임직원 및 계약직, 파견직 등을 대상으로 사내 보안, 개인정보보호, 정보보호 동향 등을 포함한 정보보호 교육 계획을 수립해 주기적인 교육을 수행하고 있으며, 클라우드 특성을 반영한 보안 교육을 별도로 연 1회 이상 시행하고 있습니다.

2.2.2 서비스 개발 및 운영 프로세스

클라우드 시스템 개발 및 운영을 위한 업무는 관련 법적 요구 사항, 정보보호 기본 요소, 최신 보안 취약점 등을 고려하여 수행합니다. 서비스 기획, 설계, 구현, 시험 및 출시에 이르는 각 단계의 다양한 보안 요소를 면밀히 검토하고 조치함으로써 클라우드 컴퓨팅 관련 보안 요구 사항을 충족시키고 클라우드 서비스 공급자와 이용자의 보안 사고를 예방합니다.

1. 개발 보안

기획, 설계, 개발 및 디자인, 테스트, 이관 및 출시의 각 단계에서 보안 사항을 반영합니다.

- 기획

서비스 기획 시 보안 요구 사항을 반영하고, 중요 정보보호를 위한 보안 요건의 정의와 관련된 활동을 문서화합니다.

- 설계

설계 담당자는 환경 보안, 개발 보안, 보안 관련 법적 요건이 준수되도록 설계합니다. 또한 설계 완료 단계에서 RISK 검토 절차에 따라 위험 평가(법무, 특허, 개인정보)를 받아야 합니다.

- 개발 및 디자인

보안 요건을 반영하고 중요 정보가 보호되도록 개발 및 디자인할 책임을 가지고 안전한 개발 환경을 위해 코딩, 소스 코드 및 데이터 보호를 위한 보안 관리 체계를 적용합니다.

- 테스트

실데이터가 아닌 가상의 데이터를 활용해 테스트를 수행하며, 보안 요건이 충족하였는지 검토 및 테스트합니다.

- 이관 및 출시

서비스를 운영으로 이관하기 위한 업무는 적절한 권한을 지닌 최소한의 담당자가 수행하며, 직무 분리와 권한 회수를 수행합니다.

2. 운영 보안

- 인프라 운영자를 위한 보안 지침은 서버, 네트워크, DB 등 인프라 자산의 취약점 및 위험 요소를 이용한 유출, 오·남용, 손상, 파괴 등 일련의 불법적 행위와 사고로부터 안전하게 관리될 수 있도록 관리 기준과 담당 역할을 정의하고 관리하고 있습니다.
- 적용 대상은 NHN Cloud 내 등록된 모든 인프라 및 인증, 접근 통제, 변경 관리, 모니터링, 백업, 파괴 등 모든 유형의 서비스를 대상으로 합니다.

3. 침해 사고 예방 및 대응

- 보안 관제 센터 및 위협 분석(CERT) 조직을 통해 보안 시스템 운영과 위협 대응 체계를 기반으로 불법적인 침입 시도에 대해 24시간 365일 상시 감시와 대응을 수행하고 있습니다.
- 침해 사고 발생 시 탐지, 전파, 접수, 분석, 대응, 복구를 담당하는 조직을 가동해 서비스 가용성 확보와 사고 확산을 방지하고, 세부 원인 분석을 통해 취약점 제거와 재발 방지 대책을 수립하고 이행합니다.
- 내부 모의 해킹 및 취약점 분석 조직을 운영하고 있으며, 정기/수시 모의 해킹 및 취약점 진단을 통해 위협을 제거하고 개선하는 활동을 수행합니다.

2.3 규정 준수와 인증

NHN Cloud는 산업의 발전과 변화에 따라 각 산업에서 준수해야 할 규정을 준수하고 있습니다.

NHN Cloud는 정기적으로 정보보호 관리 체계와 클라우드 컴퓨팅 산업에 필요한 규정을 준수하며 국내외 제3자의 공인된 인증 기관으로부터 인증을 획득하였습니다.

정보보호 관리 체계 및 클라우드 컴퓨팅 서비스 제공에 필요한 규정을 준수하며 국내외 제3자의 공인된 인증 기관으로부터 다양한 정보보호 관리 체계 인증을 획득하여 유지 관리하고 있습니다.

2.3.1 법령과 규정 준수




NHN Cloud는 정보통신 서비스 공급자, 클라우드 서비스 공급자 및 개인정보 처리자가 준수해야 하는 관계 법령 및 규정을 준수하며 이용자의 개인정보 및 데이터 보호를 위해 노력하고 있습니다. 제품과 서비스는 사전 위험 평가와 후속 조치 활동을 통해 안전하게 제공되며 이용자의 개인정보는 동의한 목적으로만 사용됩니다(세부 사항 하위 참조).

- [NHN Cloud 개인정보 처리 방침 바로 가기](#)




2.3.2 정보보호 인증 현황

NHN Cloud는 클라우드 정보보호 및 개인정보보호 관리 체계에 대한 규제와 표준을 준수하며 국내외 제3자의 공인된 인증 기관으로부터 관련 인증을 취득하여 유지 관리하고 있습니다. 또한 이용자의 정보보호 인증과 효과적인 컴플라이언스 대응을 위해 보안 인증서와 세부 보안 가이드라인을 제공합니다.

표 2-1 NHN Cloud 정보보호 인증 현황

인증	설명
<p>ISMS-P</p> 	<p>국내 최고 권위의 정보보호 및 개인정보보호 인증 제도</p> <p>ISMS-P(정보보호 및 개인정보보호 관리 체계) 인증은 기업이 정보보호 및 개인정보보호를 위한 일련의 조치와 활동을 체계적이고 지속적으로 수행하고 있는지 점검하여 일정 수준 이상의 기업에 국가 인증을 부여하는 제도입니다. NHN Cloud는 2022년 4월 이후 ISMS-P 인증을 취득하여 정보보호 및 개인정보보호 관리 체계를 검증 받았습니다.</p> <ul style="list-style-type: none"> • 인증 범위 • ISMS-P: NHN Cloud Service • ISMS: NHN Cloud Center (IDC)
<p>클라우드 서비스 보안인증 (CSAP)</p> 	<p>클라우드 컴퓨팅 서비스 정보보호 관리 체계에 대한 검증</p> <p>클라우드 서비스 보안인증은 클라우드 서비스 공급자가 제공하는 서비스에 대해 『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』 제23조 제2항에 따라 정보보호 기준의 준수 여부 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도입니다. NHN Cloud는 2022년 12월 NHN Cloud(공공기관)에 대한 CSAP 인증을 취득하였으며, NHN Dooray는 2019년 12월, NHN Cloud PaaS-TA는 2021년 6월 해당 인증을 취득하여 유지하고 있습니다.</p> <ul style="list-style-type: none"> • 인증 범위 • IaaS 인증 범위: NHN Cloud(공공기관용) • SaaS 인증 범위: Dooray! • PaaS 인증 범위: NHN Cloud PaaS-TA
<p>CSA STAR</p> 	<p>미국 CSA(Cloud Security Alliance) 주관 국제 클라우드 서비스 정보보호 인증</p> <p>CSA STAR 인증은 미국 CSA(Cloud Security Alliance)에서 주관하는 국제 클라우드 서비스 정보보호 인증으로 Cloud Controls Matrix를 통해 보안 통제의 효과와 성숙도를 평가해 STAR(Security, Trust & Assurance, Registry) 인증을 부여하는 제도입니다. NHN Cloud는 2022년 7월 NHN Cloud(IaaS, PaaS, SaaS) 서비스에 대해 CSA STAR Certification을 획득하였으며, Gold Level의 성숙도를 유지하고 있음을 평가받았습니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical IaaS services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning) service for public, financial, governmental, and medical SaaS services.

인증	설명
<p>ISO/IEC 27001</p> 	<p>정보보호 관리 체계에 대한 국제 표준 검증</p> <p>ISO/IEC 27001은 국제표준화 기구(ISO) 및 국제 전기기술 위원회(IEC)에서 제정한 정보보호 관리 체계 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaborations service, groupware, ERP(enterprise resource planning), and digital tax invoice services.
<p>ISO/IEC 27701</p> 	<p>개인정보 관리 체계에 대한 국제 표준 검증</p> <p>ISO/IEC 27701은 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 EU GDPR 등 전 세계의 개인정보보호 요구 사항을 충족하는 글로벌 개인정보 관리 체계 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning), and digital tax invoice services.
<p>ISO/IEC 29100</p> 	<p>개인정보 프레임워크에 대한 국제 표준 검증</p> <p>ISO/IEC 29100은 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 글로벌 개인정보 프레임워크 수립 및 운영에 필요한 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning), and digital tax invoice services.
<p>ISO/IEC 27017</p> 	<p>클라우드 서비스 개인정보 관리 체계에 대한 국제 표준 검증</p> <p>ISO/IEC 27017은 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 클라우드 서비스 개인정보 관리 체계 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning), and digital tax invoice services.

인증	설명
<p>ISO/IEC 27018</p> 	<p>클라우드 서비스 개인정보 관리 체계에 대한 국제 표준 검증</p> <p>ISO/IEC 27018은 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 클라우드 서비스 개인정보 관리 체계 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning), and digital tax invoice services.
<p>ISO/IEC 27799</p> 	<p>의료 정보보호 관리 체계에 대한 국제 표준 검증</p> <p>ISO/IEC 27799는 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)에서 제정한 의료 정보보호 관리 체계 국제 규격 인증입니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services. • NHN Dooray: The provision of collaboration service, groupware, ERP(enterprise resource planning), and digital tax invoice services.
<p>ISO/IEC 22301</p> 	<p>비즈니스 연속성 경영 시스템에 대한 국제 표준 검증</p> <p>ISO/IEC 22301은 비즈니스 연속성 경영(business continuity management, BCM)을 위한 국제 표준 인증입니다. NHN Cloud는 2022년 7월 IaaS 서비스에 대한 연속성 있는 서비스 제공 역량을 해당 국제 표준 기준으로 검증 받아 인증을 취득하였습니다.</p> <ul style="list-style-type: none"> • 인증 범위 • NHN Cloud: The provision of NHN Cloud service for public, finance, governmental, and medical business services.

2.4 비즈니스 연속성 관리

NHN Cloud는 재해, 재난으로 인한 업무 중단에 대비하여 서비스의 핵심 기능(critical business functions)을 복구하고 재개할 수 있도록 하는 대응 체계를 갖추고 있으며, 세부 수행 절차 및 훈련은 별도 문서로 관리합니다.

1. 범위

- NHN Cloud의 모든 클라우드 환경을 포함하고 있으며 서비스 중단 발생 시 각 핵심 서비스별 복구 전략을 포함합니다.

2. 목표

- 클라우드 서비스의 중요도가 높은 서비스 대상으로 RPO(Recovery Point Objective) 및 RTO(Recovery Time Objective)가 정해진 목표 시간으로 설정되어 있습니다.
- ※ 고객의 데이터는 BCP 범위에 포함되지 않습니다(클라우드 서비스 이용 시 고객 데이터는 자체 BCP 계획 수립 필요).

3. 서비스별 대응

- 클라우드 서비스는 KR1과 KR2 간의 이중화 구성을 통해 비즈니스 연속성을 제공하며, 리전 서비스의 경우 서비스 중단 된 리전을 제외하고 정상 리전에서 서비스를 이용할 수 있도록 구성해 각 상황에 맞는 프로세스와 대응 절차에 따라 서비스를 재개합니다.

4. 조직

- 서비스 연속성 계획(Business Continuity Plan: BCP)을 위한 조직은 크게 BCP 대응 위원회와 BCP 대응 팀으로 구성하며, 각 조직은 BCP 대응 책임자 및 각 분야별 책임자와 담당 구성원으로 인력이 배치되어 있습니다.
- BCP 대응 위원회: BCP 선포, 상황 총괄 지휘 및 중요 사항의 의사 결정을 하며, BCP 대응 조직별 역할과 책임을 할당하고 총괄합니다.
- BCP 대응 팀: 세부 업무 영역별 조직을 구성하고 재해 유형별 서비스 연속성 관련 실무를 수행합니다.



그림 2-2 NHN Cloud BCP 조직도

5. 커뮤니케이션

- 서비스 중단 시 BCP 대응 위원회는 BCP 대응 팀과 서비스별 담당자, 주요 기관, 고객, 파트너와 사전에 정해진 절차와 수단을 통해 신속히 소통합니다. 비상시 대응 체계가 정상 작동할 수 있도록 각 이해 관계자 정보와 비상 연락망을 상시 관리합니다.

3 NHN Cloud 물리보안

3.1 데이터 센터 보안 관리

NCC(NHN Cloud Center)는 NHN Cloud의 자체 기술력으로 설계·구축한 도심형 고집적 데이터 센터입니다. 오랜 기간 대규모 인프라 운영 경험을 바탕으로 미국 Uptime Institute의 Tier Standard와 미국 통신산업협회(telecommunications industry association, TIA)의 TIA-942 Tier-3 이상의 설계 등급을 충족하는 설비를 갖추고 있으며, 안정적인 IT 서비스 제공과 출입 인원 및 시설의 안전한 관리를 통해 물리 보안 환경을 유지하고 있습니다.

3.1.1 환경 및 설비 보안

1. 화재 감지 및 대응

- 서버실 출입구에는 화재에 대비한 방화문과 자동 개폐 장치를 설치하였고, 서버 및 기타 장비에 피해를 주지 않으면서 공기 중 산소의 농도를 낮추기 위해 청정소화 약재를 사용한 자동소화 설비를 운영 중입니다.
- 누수 및 화재 감지를 위한 조기 연기 감지 시스템(very early smoke detection apparatus, VESDA)을 통해 각종 알람 신호를 24시간 인지할 수 있는 중앙 상황실을 운영하고 있습니다.

2. 온도 습도

- 서버실 내부에는 적절한 온도, 습도를 유지할 수 있도록 자체 구축한 FMS(facility management system)를 통해 전력 및 온도, 습도를 모니터링하며, Cold zone과 Hot zone의 온도 센서를 통해 냉기가 원활히 순환하도록 운영하고 있습니다.

3. 전력

- 무중단 서비스를 위해 데이터 센터는 전력 공급원의 이중화 구성과 전용 선로를 사용하여 안정성을 향상하였으며, 무중단 전원 공급 장치(Dynamic UPS)를 도입해 배터리 및 연료 보충 없이도 발전이 가능한 자가 발전 설비로 데이터 센터에 전원을 공급할 수 있습니다.



그림 3-1 NHN Cloud Dynamic UPS

3.1.2 출입 통제

1. 출입 통제 기준

- 데이터 센터 전 구역은 총괄 보안 관리자에게 허가 받은 인원만 한해 출입할 수 있으며, 출입 권한 신청, 권한 변경, 삭제 등의 출입 권한 변동 내역을 관련 규정에 따라 보관합니다. 또한 출입 권한은 구역별로 구분해 업무 목적상 최소한의 범위로 부여합니다.

2. 출입 구역

- 출입 구역은 일반 구역, 제한 구역, 통제 구역으로 용도별로 구분해 각각의 보호 대책을 준수합니다.
- 클라우드 인프라 시스템은 통제 구역으로 정하고 있으며, 공공기관과 민간 클라우드 인프라는 물리적으로 구분하여 보호합니다.

3. 출입 보안 등급

- 데이터 센터 출입자는 6개의 출입 등급으로 구분되며, 각각의 세부 보안 등급 기준을 적용해 업무 목적상 필요한 최소한의 범위로 출입 권한을 부여합니다.

4. CCTV

- 데이터 센터 내 시설물 및 전산실 출입구의 사각지대가 없도록 CCTV를 설치하였으며, CCTV 네트워크 비디오 녹화기(network video recorder, NVR)에 대한 정기 점검과 오류 발생 시 부품을 교체해 데이터 저장에 문제없도록 관리하고 있습니다.

3.1.3 자료 및 설비 관리

1. 자료 관리

- 출입 통제 시스템에 저장된 정보는 임의 삭제 및 변경되지 않도록 관리하고 있으며, 정보 발생 이후 일정 기간 규정에 따라 보관합니다. 추가로 CCTV 영상 정보의 관리는 ‘영상 정보보호 가이드라인’을 준수합니다.
- 업무상 수집 또는 생성된 정보는 명시된 보관 기간 만료 후 파기하며, 추가 보존이 필요할 경우 총괄 보안 관리자의 승인을 득하여 연장합니다.

2. 설비 점검

- 소방 시설물, 보안 시설물 및 기타 내부 시설물의 이상 유무에 대해 육안 확인과 작동 상태를 점검합니다.

4 NHN Cloud 클라우드 플랫폼 보안

4.1 클라우드 플랫폼 보안

NHN Cloud는 클라우드 컴퓨팅 서비스 이용을 위한 기반이 되는 하드웨어 및 가상화의 보안을 구성하고 관리합니다. 해당 영역은 이용자에게 보이지 않는 영역으로 지속적인 보안 설정, 점검 및 관리를 통해 안전하게 유지되고 있습니다.

클라우드 이용자의 인프라 보안 기능과 요구 사항은 호스트 보안, 네트워크 보안 및 데이터 보안에 중점을 두고 있습니다. 네트워크 가상화 기술을 사용해 중요한 컴퓨팅 리소스를 서로 격리하고, 클라우드 인프라를 구성하는 여러 모듈을 통해 이용자의 애플리케이션과 서비스를 제공합니다. 이러한 클라우드 제품과 서비스는 플랫폼에서 제공하는 보안 기능이 포함되어 있으며 일부 보안 기능은 이용자가 활성화하고 구성하여 사용할 수 있습니다.

4.1.1 호스트 보안

1. 침입 탐지

- 클라우드 플랫폼 및 이용자 서비스 보호를 위해 NHN Cloud는 Anti-DDoS, IDS, 백신 등 보안 솔루션을 구성하였으며, 해당 보안 솔루션과 다양한 로그를 활용해 침입 시도와 비정상 행위에 대한 보안 모니터링을 수행합니다.
- 보안 관제 센터는 24시간 365일 침해 위협 및 비정상 행위 등을 모니터링하며, 이상 행위 발견 시 내부 유관 부서 및 고객에게 내용을 전파하고 화이트리스트에 해당되지 않는 경우 서비스 손상을 방지하기 위해 침입 차단을 진행합니다.

2. 바이러스 탐지

- 멀웨어, 코인 마이너, 랜섬웨어, 악성 코드 등 호스트 레벨에서 파일, 메모리 및 프로세스를 모니터링하고 분석해 결과에 따라 파일 삭제 및 격리 등의 대응을 조치합니다. 또한 분석팀과 운영팀을 통해 백신의 바이러스 탐지 정책 및 엔진을 최신으로 유지 및 관리하고 있습니다.

3. 취약점 관리

- 호스트 및 인스턴스 OS의 취약점 점검은 자동 스캐너 및 인증 기관 체크 리스트와 NHN Cloud의 다년간 축적한 점검 방법을 이용해 정기적으로 진행하고 있습니다. 점검 시 발견된 취약점은 내부 프로세스와 절차에 따라 담당자에게 전달되며 조치 결과를 지속적으로 관리합니다. 또한 애플리케이션 및 웹 서비스도 모의 해킹과 소스 코드 취약점 진단을 수행해 예방 활동을 합니다.

4. 보안 하드닝

- 취약점을 제거한 OS로 골든 이미지를 생성해 배포 및 관리하고 있으며, 주기적인 취약점 점검과 최신 패키지 배포와 관리를 위해 내부 리포지터리(repository)를 운영하고 있습니다.

5. 인스턴스 자동 복구

- 호스트 및 하드웨어 오작동 또는 기타 오류로 인해 컴퓨터 노드가 실패하는 경우 자동 호스트 evacuation을 실행해 인스턴스를 다시 사용할 수 있도록 합니다. 인스턴스를 정상 호스트로 자동 복구함으로써 인스턴스 및 애플리케이션이 정상 작동해 고가용성을 보장합니다.

4.1.2 데이터 보안

1. 저장 장치 관리

- 공공기관용 클라우드 시스템은 전용 잠금 장치를 장착한 кей지에 설치되어 있고, 스토리지는 저장 장치의 도난을 방지하기 위해 잠금 장치를 설치하여 보호하고 있습니다.

2. 데이터 관리

- 호스트, 하이퍼바이저, 컨테이너, DBMS, 네트워크, 스토리지 및 정보보호 시스템에서 발생하는 다양한 로그(운영자 접속 로그, 행위 로그, 명령어, 부팅, DB 접속, 기타 OS, 정보보호 시스템별 각종 로그)를 내부 저장 장치 및 별도의 시스템에 보관하고 해당 로그의 무결성을 검증하며, 각 로그의 유형과 특성에 따라 보관 기간을 준수합니다.
- 정보보호 시스템의 로그는 식별할 수 있는 형태로 기록 및 모니터링되어야 하며 비인가된 접근 및 변조로부터 보호되어야 합니다. 이를 위해 NHN Cloud는 정보보호 시스템 로그 백업 프로세스에 따라 내부 통합 로그 관리 솔루션 및 2차 로그 백업 시스템을 통해 데이터를 저장하고 무결성 검증과 변조 등이 발생하지 않도록 관리하고 있습니다.

3. 데이터 보호

- 데이터가 저장되는 시스템은 별도의 전용 게이트웨이 서버를 구성해 최소 권한 부여된 인원에게 접근 통제와 접근 및 운영에 대한 감사를 합니다.
- 장애로 인한 데이터 유실을 방지하기 위해 1일 1회 백업을 적용하며, 백업된 데이터는 7일간 유지하고 있습니다.
※ 단, 고객의 데이터는 별도 기준으로 백업을 해야 합니다.

4. 암호화 전송

- NHN Cloud 제품 및 서비스는 이용자 데이터 처리 시 SSL/TLS 프로토콜을 적용해 전송 구간 내 기밀성, 무결성을 보장합니다.
- 클라우드 콘솔의 접속과 클라우드 제품 및 서비스 API는 HTTPS 암호화를 통해 이용자 단말과 안전하게 통신합니다. 또한 네트워크 제품인 VPN Gateway는 IPsec VPN 설정으로 VPC와 온프레미스를 암호화된 구간으로 연결할 수 있습니다.

5. 데이터 폐기

- 정보 시스템 및 저장 매체에 대해서는 외부 전문 업체를 통해 데이터가 복구되지 않도록 디가우징(degaussing) 및 천공 파괴하고 있습니다.
- 이용자가 클라우드 서비스 이용 중 수집, 저장, 생성한 일체의 정보는 계약 종료 시 반환(요청 시) 또는 파기합니다.
- 고객 회원의 개인정보는 개인정보보호 법령의 최소 수집 원칙을 준수하고 있으며, 회원 탈퇴 시 즉시 회원 DB에서 분리 저장되며, 법령에 의한 보존 사유 만료 후 삭제됩니다.

4.1.3 네트워크 보안

1. 리전

- 리전은 독립적이고 지리적으로 격리된 클라우드 인프라의 물리적 위치를 의미합니다. 독립된 전원과 네트워크를 갖춘 다수의 가용성 영역으로 구성되며, 사용하려는 지역과 서비스에 맞춰 리전을 선택할 수 있습니다.
- NHN Cloud는 안정적인 글로벌 서비스 제공을 위해 4개의 리전을 운영하고 있으며, 고가용성을 지원하기 위해 여러 가용성 영역 및 복수의 리전에 애플리케이션을 배포합니다. 글로벌 서비스 및 AI, 스마트 제조, 공공 클라우드 등 특화 산업을 위한 데이터 센터를 확장하고 있습니다.

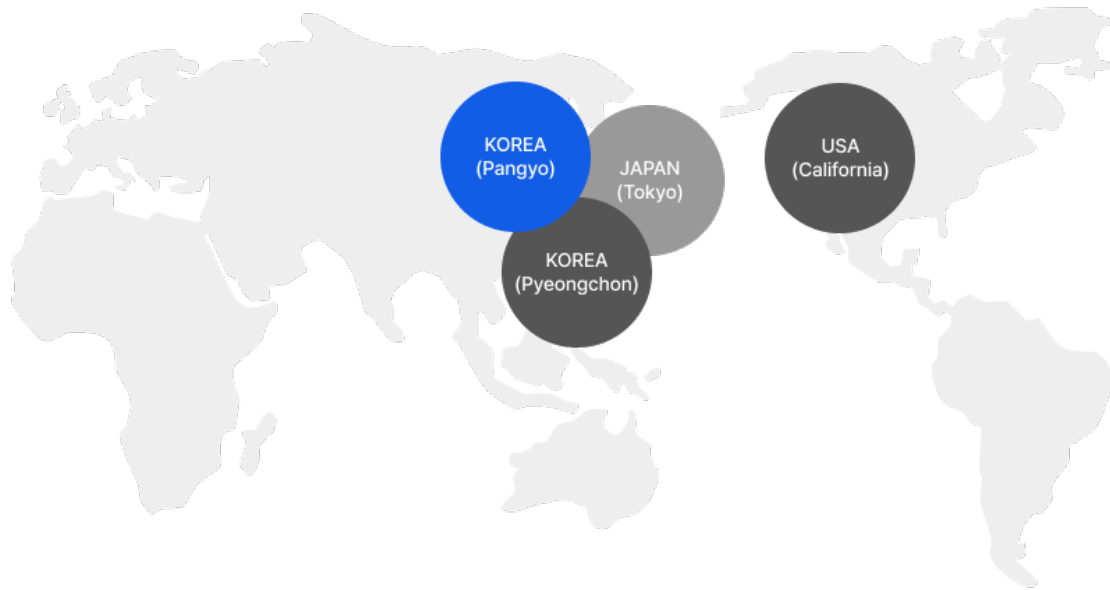


그림 4-1 NHN Cloud 글로벌 데이터 센터(리전)

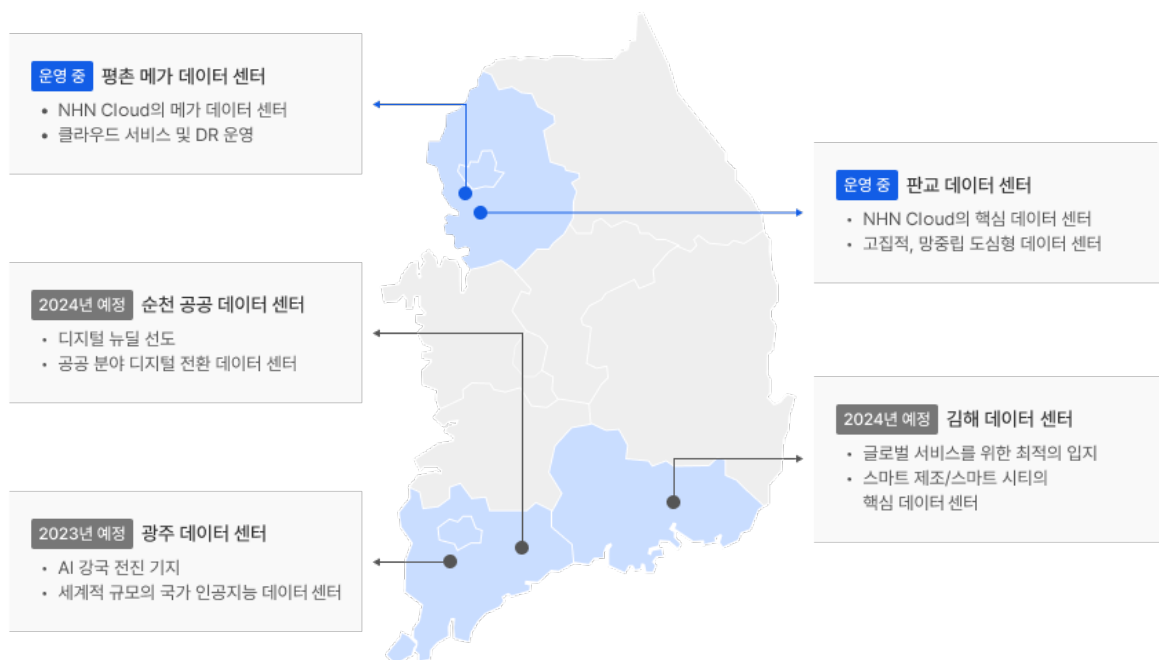


그림 4-2 NHN Cloud 국내 데이터 센터(리전)

2. 가용성 영역

- 클라우드 인프라의 하드웨어 문제로 발생하는 장애를 대비하기 위해 전체 시스템을 여러 가용성 영역으로 나누었습니다. 각 가용성 영역은 자체 네트워크, 전원 공급, 상면 및 인프라를 갖추고 있어서 하나의 영역에서 발생하는 문제가 다른 영역에 영향을 미치지 않습니다. 이러한 구조는 높은 가용성과 이용자의 애플리케이션이나 서비스를 복제하거나 각 가용성 영역에 배치해 시스템의 견고성을 강화할 수 있도록 하였습니다.

3. 클라우드 영역 분리

- NHN Cloud는 퍼블릭, 공공 인터넷망, 공공 업무망 클라우드 서비스를 구성하는 서버, 네트워크, 스토리지 및 하이퍼바이저 등의 하드웨어가 물리적으로 분리되어 있으며 서로 연결이 불가능한 독립된 구성으로 되어 있습니다. 각 서비스 목적과 용도에 맞춰 알맞은 클라우드 서비스를 이용할 수 있습니다.
- 국가·공공기관은 「국가 정보보안 기본지침」에 근거하여 중요 자료의 외부 유출을 방지하기 위해 업무망(내부망)과 인터넷망(외부망)을 분리하여 운영하고 있습니다. 이는 인터넷을 통한 업무 관련 정보에 대한 접근을 차단해 안전한 업무 환경을 구축하기 위한 것입니다. 각급 기관의 업무망과 연동된 클라우드는 각급기관의 업무망으로 보며, 인터넷망과 연동된 클라우드는 각급 기관의 인터넷망으로 보고 이에 따른 보안 대책을 마련해야 합니다(「국가 정보보안 기본지침」 제41조 참조).

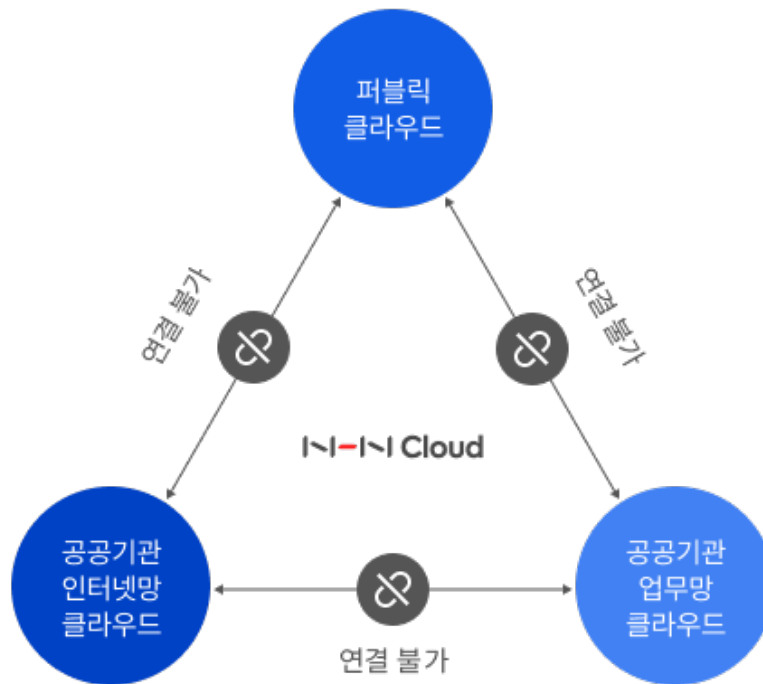


그림 4-3 NHN Cloud의 클라우드 영역 분류

4. 물리적 망분리(공공 업무망 영역)

- 공공기관이 내부 업무망과 연결하여 클라우드 서비스를 제공해야 할 경우 인터넷 접점이 없어야 하며, 공공 인터넷망 영역(대외 서비스 영역)과 물리적 망분리가 되어야 합니다. NHN Cloud는 공공 인터넷망 영역(대외 서비스 영역)과 공공 업무망 영역을 물리적으로 별도로 구성하여 제공하고 있습니다.
- 단, 공공 업무망 영역과 공공 인터넷망 영역 사이의 파일 전송 및 스트리밍은 망 연계 솔루션을 이용해 통신 제어를 수행하며, 추가적인 안전성 확보 조치를 통해 안전하게 구성하였습니다.

5. 물리적 영역 분리(공공 인터넷망 영역)

- 공공 인터넷망 영역은 각급 기관의 인터넷망과 연결하여 클라우드 서비스를 제공하며, Public 클라우드 영역과 물리적 영역이 분리되어 있으며, 공공 업무망 영역과는 물리적 망분리가 되어 있습니다.

6. 관리망 및 접근 통제

- NHN Cloud는 사용자 클라우드 서비스 네트워크와 내부 운영 및 관리 네트워크는 분리되어 있으며, 클라우드 플랫폼을 구성하는 서버 및 네트워크 장치로의 직접 액세스는 허용되지 않습니다.
- 서버 및 네트워크 장치의 접근을 위해서는 별도의 관리망이 있으며, 정보보호 관리 지침에 따라 각 영역별 담당자 지정과 엄격한 접근통제와 인증을 통해 관리하고 있습니다.

7. DDoS 공격 보호

- NHN Cloud는 클라우드 플랫폼 및 리소스를 다양한 유형의 DDoS 공격으로부터 보호하기 위해 Anti-DDoS 솔루션을 구성해 모든 데이터 센터를 보호합니다. 네트워크 및 서비스에 대한 보호 규칙을 적용하고 공격 행동을 정확히 식별해 네트워크의 안정성을 보장합니다. 보안 관제센터의 24시간 365일 모니터링으로 위협 상황을 인지해 내부 담당자 공유 및 DDoS 대응 절차를 수행합니다.

4.1.4 가상화 보안

1. 하이퍼바이저 보안

- NHN Cloud는 KVM 기반의 하이퍼바이저를 사용해 클라우드 컴퓨팅 리소스를 제공합니다. 하이퍼바이저 보안과 리소스의 격리를 강화하기 위해 SELinux(Security-Enhanced Linux)를 사용하며, 커널 취약점은 정기 점검을 통해 서비스 및 보안 영향도 파악 후 내부 절차에 따라 적용하고 있습니다.
- 하이퍼바이저 호스트의 보안성 강화를 위해 시스템 담당 부서는 접근 통제 정책을 적용해 시스템을 관리하고 있으며, 각 시스템은 백신을 설치해 악성 코드로부터 보호하고 있습니다.
- 하이퍼바이저의 버그 및 보안 패치는 서비스 및 보안 영향도 검토 후 적용하고 있으며, 제품 단종(end of life, EOL) 도래 시 업그레이드를 위해 주기적으로 내부 시스템을 파악하고 조치합니다.

2. 컴퓨팅 격리

- 애플리케이션 및 비즈니스 요구 사항을 충족하기 위해 자동 확장이 가능한 다양한 인스턴스를 제공합니다. 구성의 유연성과 네트워크 공격, 보안 위협 등을 방지하고 데이터 보호를 위해 관리 시스템과 가상 서버뿐만 아니라 가상 서버와 가상 서버 사이도 격리되어 있습니다. 이러한 격리는 하이퍼바이저에서 제공하며, 인스턴스가 독립형으로 실행되는 가상화 환경을 사용하면서 호스트 및 다른 인스턴스에 대한 이용자의 무단 액세스를 방지하기 위해 물리 프로세스의 권한 수준(Protection Ring)을 사용합니다.

3. 스토리지 격리

- NHN Cloud는 가상 서버 기반의 인스턴스와 스토리지를 분리합니다. 이러한 분리는 컴퓨팅 및 스토리지를 독립적으로 확장할 수 있고, 다중 테넌트 환경을 유연하게 제공합니다. 하이퍼바이저는 물리적으로 동등한 저장 장치를 가상 장치로 대체하며, 인스턴스의 I/O 작업은 하이퍼바이저가 인스턴스에 할당한 디스크 공간에만 액세스할 수 있도록 해 서로 다른 가상 서버의 디스크에 대한 격리를 구현합니다.

4. 네트워크 격리

- 인스턴스에 네트워크 연결을 위해 가상 네트워크를 제공합니다. 이러한 가상 네트워크는 물리적 네트워크 구조 위에서 구성된 논리적인 구조입니다. 논리적인 가상 네트워크는 서로 격리되어 있어 악성 인스턴스가 트래픽을 가로채는 것을 방지합니다.

5 NHN Cloud 계정 보안

5.1 이용자 계정 보안

클라우드 컴퓨팅 서비스의 이용자 계정 보안은 인증, 권한 부여, 계정 관리, 감사 관리가 매우 중요합니다. NHN Cloud의 이용자 계정은 NHN Cloud 회원과 IAM 멤버로 구분되며, 조직과 프로젝트로 멤버를 관리할 수 있습니다. 각각의 역할과 권한에 따라 안전하게 클라우드 콘솔 및 리소스를 이용할 수 있습니다.

5.1.1 멤버(Member)

1. 조직

- NHN Cloud 서비스를 효율적으로 이용하고 관리하기 위해 만들어진 그룹입니다.
- 동일한 서비스 정책을 이용자에게 공유하여 사용할 수 있습니다.
- 조직을 생성하는 회원은 자동으로 조직의 OWNER가 됩니다.

2. 프로젝트

- 프로젝트는 조직 생성 후 NHN Cloud 서비스를 이용하기 위해 만들어진 그룹입니다.
- 프로젝트를 생성하는 회원은 프로젝트의 ADMIN 권한을 가집니다.
- 프로젝트 서비스는 프로젝트 단위로 이용하며, 사용량에 따라 과금이 정해집니다.

3. NHN Cloud 회원과 IAM 멤버 정책

- NHN Cloud 회원과 IAM 멤버 정책은 표 5-1의 내용과 같이 구분됩니다.

표 5-1 NHN Cloud 회원 및 IAM 멤버 정책 비교

구분	NHN Cloud 회원	IAM 멤버
정의	<ul style="list-style-type: none"> • 조직 관리를 위한 멤버 • NHN Cloud 이용 약관에 동의한 NHN Cloud 회원으로 서비스 이용에 대한 책임과 의무를 가지는 멤버 • NHN Cloud 서비스 전체에서 유효한 멤버로 소속된 조직이 삭제되어도 NHN Cloud 회원으로 존재 	<ul style="list-style-type: none"> • 서비스 이용을 위한 멤버 • NHN Cloud 이용 약관에 동의하지 않은 멤버 • 조직 내에서만 유효한 멤버로 소속된 조직이 삭제되면 더 이상 사용할 수 없고 삭제되는 멤버
등록 방법	<ul style="list-style-type: none"> • 조직의 OWNER나 ADMIN이 NHN Cloud 회원 ID(E-mail)를 입력하여 등록 	<ul style="list-style-type: none"> • 조직의 OWNER나 ADMIN이 조직 내 유일한 ID를 입력하여 등록
역할	<ul style="list-style-type: none"> • 조직 관리(조직 생성/수정/조직 멤버 관리/조직 서비스 관리/결제 관리) • 프로젝트 생성/삭제 	<ul style="list-style-type: none"> • 조직 서비스 이용

구분	NHN Cloud 회원	IAM 멤버
콘솔 접근	<ul style="list-style-type: none"> NHN Cloud 콘솔(https://console.nhncloud.com) 접근 회원 ID/비밀번호로 로그인 회원 정보에서 설정한 로그인 보안(2차 인증(이메일, SMS)) 사용 	<ul style="list-style-type: none"> IAM 콘솔(https://조직도메인.console.nhncloud.com) 접근 조직의 OWNER 또는 ADMIN이 설정한 ID/비밀번호로 로그인 조직에서 설정한 로그인 보안(2차 인증(이메일, Google OTP)) 인증

5.1.2 인증(Authentication)

NHN Cloud의 신원 인증은 계정 자격 증명을 사용해 이용자의 실제 신원(Identity)을 확인하는 것입니다. 계정 자격 증명은 이용자의 ID/비밀번호 또는 User Access Key ID를 사용합니다.

계정 자격 증명은 인증 과정에서 가장 기본이 되는 요소 중 하나이며, 이를 안전하게 보호하는 것은 보안의 가장 기본입니다. 따라서, 비밀번호를 주기적으로 변경하거나 다중 요소 인증(multi-factor authentication, MFA)을 적용하는 것을 권장합니다. 또한 NHN Cloud는 로그인 및 개인정보 등 보안 컴플라이언스 준수를 위해 콘솔의 손쉬운 설정으로 조직의 공통된 정책을 수립하고 조직의 멤버가 정책을 준수할 수 있도록 보안 기능을 제공합니다.

1. 로그인 비밀번호 정책

- NHN Cloud 회원 및 IAM 멤버는 이용자 ID 및 비밀번호를 사용하여 NHN Cloud 콘솔에 로그인할 수 있으며, 클라우드 리소스에 대한 작업을 할 수 있습니다.
- 클라우드 콘솔의 안전한 사용을 위한 비밀번호 정책은 영문자, 숫자, 특수문자를 조합하여 최소 8자 이상으로 구성해야 합니다.

2. 로그인 보안 설정

- NHN Cloud 회원 및 IAM 멤버의 클라우드 콘솔 접속 보안 강화를 위한 2차 인증, 로그인 실패 보안, 로그인 세션을 설정할 수 있는 기능을 제공합니다.
- NHN Cloud 회원의 콘솔 접속 2차 인증은 회원 정보에서 설정할 수 있습니다.

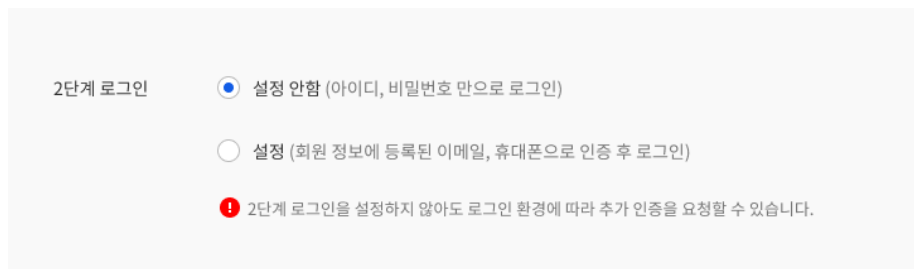


그림 5-1 NHN Cloud 회원 2단계 로그인

- IAM 멤버의 콘솔 접속 로그인 보안 설정은 조직 관리 > 거버넌스 설정 > IAM 거버넌스 설정에서 2차 인증, 로그인 실패 보안, 로그인 세션을 제공합니다.

로그인 보안 설정

IAM 회원의 콘솔 접속 보안(2차 인증, 로그인 실패 보안, 로그인 세션)을 설정할 수 있습니다.

그림 5-2 IAM 멤버 로그인 보안 설정

3. 클라우드 콘솔 접근 통제

- 클라우드 콘솔의 이용자 접근 보안 강화를 위해 복잡한 정책이나 권한 설정을 하지 않더라도 조직 거버넌스 설정의 IP ACL 설정을 이용해 간단하게 허용한 IP에서만 콘솔에 접근할 수 있도록 강화된 접근 통제를 할 수 있습니다.

IP ACL 설정

콘솔 접근의 IP 혹은 IP 대역을 설정하여, 허용한 IP로만 접근을 허용합니다.

그림 5-3 클라우드 콘솔 IP ACL 설정

4. 키 페어

- SSH Key Pair(키 페어)는 공개 키 기반 구조(public key infrastructure, PKI)를 바탕으로 개인 키(private key)와 공개 키(public key) 두 개의 암호화 키로 이루어집니다. 이용자는 키 페어의 개인 키를 이용해 로그인 정보를 인코딩하여 인스턴스로 전송해 접속 인증을 받은 후 안전하게 인스턴스에 접속할 수 있습니다. 키 페어 사용은 보안성이 높기 때문에 일반적으로 비밀번호를 사용하는 것보다 안전합니다.

5. API 보안 설정

- API 보안 설정은 User Access Key ID(NHN Cloud 서비스 이용 시 이용자 인증을 위해 필요한 이용자 설정 키)를 발급하는 기능입니다.
- Access Key는 클라우드 서비스 API 호출에 사용하는 보안 자격 증명으로 API를 통해 NHN Cloud 리소스에 접근하는 클라이언트의 ID를 인증하는 데 사용됩니다. API 통신은 SSL의 암호화된 HTTPS 통신을 통해 전송 구간의 데이터를 암호화하여 안전하게 전송합니다.

- 보안 및 사용성 강화를 위해 Access Key ID는 아래 두 가지 유형으로 발급합니다.
 - ① User Access Key ID-Secret Access Key 관리형: C(Create, 생성), U(Update, 갱신), D(Delete, 삭제) 기능의 API 이용 시 Secret Access Key까지 관리하여 보안성 강화
 - ② User Access Key ID 관리형: 단순 조회 기능의 API 이용 시 User Access Key ID 설정만으로 이용 가능
- Access Key는 장기간 API 요청에 사용할 수 있으므로 보안을 위해 생성된 키는 안전한 장소에 보관하고 주기적으로 변경하는 것을 권장합니다.

5.1.3 권한 부여

권한 부여(Authorization)는 이용자 또는 API 호출 시 NHN Cloud의 리소스나 기능에 특정 작업을 수행할 수 있는 권한을 부여하는 프로세스로 자격 증명을 사용해 인증 이후 계정 및 역할에 따라 수행 권한을 부여합니다.

권한 부여는 다양한 레벨에서 이루어질 수 있으며, 직무 또는 역할별로 각 담당자에 따라 차등 부여하고 업무 수행에 필요한 최소 권한만 할당해야 합니다. NHN Cloud는 멤버와 역할 관리를 통해 이용자별 권한을 부여합니다.

1. 조직 멤버

- 조직의 OWNER는 계정의 모든 역할을 부여하고 서비스를 신청할 수 있으며, 회원을 등록하고 조직별 관리 역할(ADMIN, MEMBER, BILLING VIEWER, LOG VIEWER)을 부여할 수 있습니다.

표 5-2 NHN Cloud 회원의 조직 역할

작업	역할	OWNER	ADMIN	MEMBER	BILLING VIEWER	LOG VIEWER
조직 관리	조직 생성	○				
	조직 수정	○	○			
	조직 삭제	○				
멤버 관리	조직 멤버 등록	○	○			
	조직 멤버 삭제	○	○			
서비스 관리	조직 서비스 활성화	○	○			
	조직 서비스 비활성화	○	○			
결제 관리	청구서 조회	○				
	이용 현황	○	○		○	
프로젝트 관리	프로젝트 생성	○	○	○		
	프로젝트 삭제	○	○			
이용자 Action 로그 관리	이용자 Action 로그 조회	○	○			○

- IAM 멤버는 MEMBER 역할을 부여하면 프로젝트를 직접 생성할 수 있으며, 미부여 시에는 역할을 할당해 서비스별 역할을 수행할 수 있습니다.

표 5-3 IAM 멤버의 조직 역할

작업	역할	MEMBER
프로젝트 관리	프로젝트 생성	○

2. 프로젝트 멤버

- 조직의 멤버가 아니더라도 프로젝트의 멤버가 될 수 있으며, 프로젝트 멤버에게 필요한 역할을 여러 개 또는 역할 그룹을 만들어 부여할 수 있습니다.

표 5-4 프로젝트 관리 역할

역할	설명
ADMIN	프로젝트 전체에 대한 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
MARKETPLACE_ADMIN	마켓플레이스 서비스 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
MARKETPLACE_VIEWER	마켓플레이스 서비스 Read(읽기)
MEMBER	프로젝트 내 모든 서비스 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
BILLING VIEWER	이용 현황 Read(읽기)
PROJECT MANAGEMENT ADMIN	<ul style="list-style-type: none"> • 프로젝트 기본 정보 Update(갱신) • 프로젝트 통합 Appkey Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제) • 프로젝트 역할 그룹 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제) • 프로젝트 서비스 활성화(Enable)/비활성화(Disable) • 프로젝트 Delete(삭제)
PROJECT MANAGEMENT VIEWER	<ul style="list-style-type: none"> • 프로젝트 기본 정보 Read(읽기) • 프로젝트 통합 Appkey Read(읽기) • 프로젝트 역할 그룹 Read(읽기)
PROJECT MEMBER ADMIN	프로젝트 멤버 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
PROJECT MEMBER VIEWER	프로젝트 멤버 Read(읽기)

표 5-5 프로젝트 서비스 이용 역할

서비스	역할	설명
Infrastructure	ADMIN	Infrastructure 서비스 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
Infrastructure	MEMBER	VPC, Subnet, Network Interface, Routing, Network ACL, Internet Gateway, Peering Gateway, Colocation Gateway, NAT Gateway, VPC Gateway(Site-to-Site VPN), Service Gateway, Security Group, Load Balancer 서비스 Read(읽기). 이외 서비스 Create(생성), Read(읽기), Update(갱신), Delete(삭제)
Virtual Desktop	ADMIN	Virtual Desktop 서비스 Create(생성)/Read(읽기)/Update(갱신)/Delete(삭제)
NHN Container Registry (NCR)	ADMIN	NHN Container Registry (NCR) 서비스 Create(생성), Read(읽기), Update(갱신), Delete(삭제)
NHN Container Registry (NCR)	VIEWER	NHN Container Registry (NCR) 서비스 Read(읽기)
Marketplace	ADMIN	marketplace 프로젝트 서비스 Read(읽기)

• 프로젝트 서비스 이용 역할 목록 바로 가기

표 5-6 프로젝트 서비스 활성화 역할

역할	설명
서비스명 PERMISSION	서비스 Enable(활성화), Disable(비활성화)

구분	조직	프로젝트
Owner	Owner NHN Cloud 회원	
사업 담당자(PM)	Admin, Billing Viewer NHN Cloud 회원	
시스템 관리자	Admin NHN Cloud 회원	Infrastructure Admin IAM 멤버
빌딩 관리자	Billing Viewer NHN Cloud 회원	Billing Viewer IAM 멤버
개발자		Infrastructure Member IAM 멤버

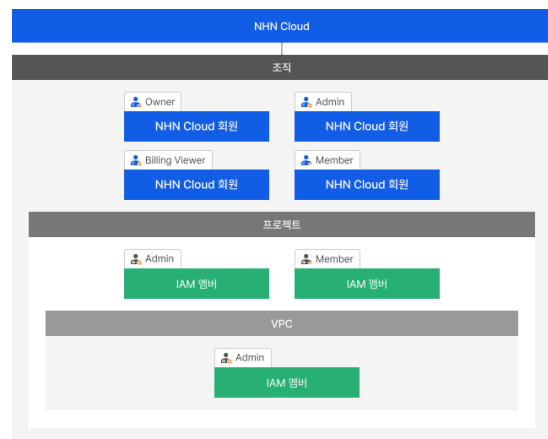


그림 5-4 NHN Cloud 회원 및 IAM 멤버의 역할(권한) 예시

5.1.4 감사(Audit)

이용자 인증 및 권한 부여에 대한 제어는 계정 보안의 중요한 요소입니다. 또한 운영 중 발생한 다양한 로그는 이용자가 보안 상황을 이해하고 판단하는 데 도움을 줄 수 있습니다.

CloudTrail은 계정에서 수행한 로그인 및 리소스의 접근과 작업 기록을 조직 단위로 제공합니다.

CloudTrail에 기록된 로그는 보안 분석, 리소스 변경 추적 및 규정 준수를 위한 감사 활동으로 활용할 수 있으며, NHN Cloud의 Resource Watcher 또는 통합 로그 관리 솔루션과 연동하여 승인되지 않은 리소스의 생성, 변경, 삭제 등의 위반 활동 및 오·남용에 대한 알람을 받을 수 있습니다.

- [CloudTrail 이벤트 목록 바로 가기](#)

6 NHN Cloud 보안 관제 및 예방

6.1 보안 모니터링 및 취약점 진단

NHN Cloud는 가상화, 호스트, 네트워크 및 저장 장치와 같은 클라우드 플랫폼뿐 아니라 리소스, 애플리케이션, 비즈니스 및 계정 등 안전하게 클라우드 서비스를 이용할 수 있도록 보안을 고려하여 설계되었으며 외부 위협으로부터 플랫폼과 이용자의 서비스를 보호하기 위해 보안 솔루션을 구성하여 운영하고 있습니다.

또한 상시 모니터링을 통해 보안 위협에 대응하고 있으며, 시스템 및 애플리케이션 점검을 통해 사전 취약점을 제거하고 있습니다.

6.1.1 위협 탐지 및 대응

1. 보안 위협 분석 센터

- 클라우드 플랫폼 및 이용자 서비스 보호를 위해 구축한 보안 솔루션의 이벤트 수집, 위협 탐지 및 분석, 대응 및 보고의 프로세스로 내부 플랫폼과 고객의 서비스를 안전하게 보호하고 있습니다.
- 각 프로세스 단계별 주요 역할 및 산출물에 대해서 내부 정책으로 관리하고 있습니다.
- 식별: 보안 장비 등 보안 관제 환경 분석
- 탐지/분석: 보안 관제 및 로그 연동 대상 파악, 보안 장비 로그 수집, 실시간 모니터링, 이벤트 분석, 탐지 정책 설정, 상황 전파, 보안 동향 수집 및 분석
- 대응: 위협 정보 상세 분석, 침해 사고 대응, 차단 정책 설정
- 보고/관리: 침입 대응 보고, 보안 관제 정기 보고, SLA 관리

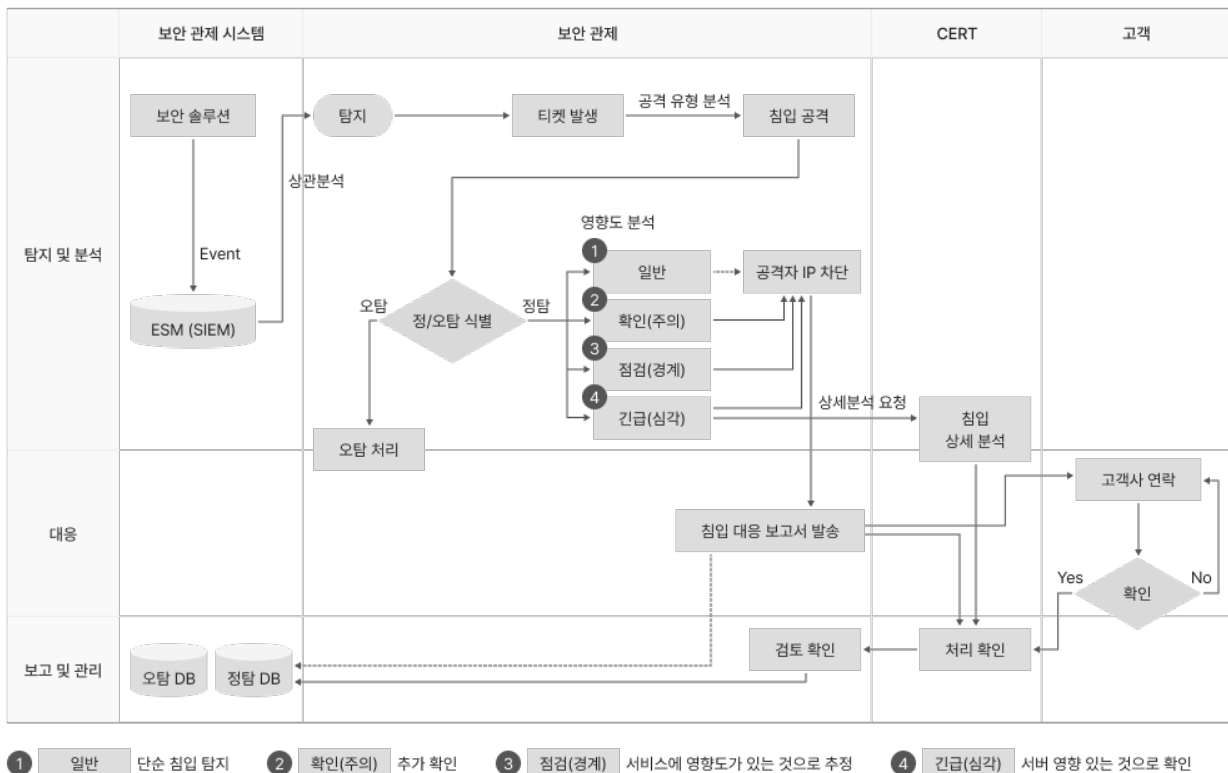


그림 6-1 이벤트 탐지 및 대응 프로세스(보안 관제 프로세스)

- 수년간 축적된 침입 탐지 패턴을 DDoS 방어 장비 및 침입 탐지 시스템에 적용하고, 탐지된 이벤트는 중앙의 통합 보안 관제 시스템으로 모두 수집해 24시간 365일 실시간으로 공격에 대한 탐지와 분석을 수행하고 있습니다. 또한 다수의 Threat Intelligence를 활용해 최신 위협 정보 수집과 신규 공격 탐지 패턴을 제작해 클라우드 플랫폼 및 사용자 서비스에 대한 위협 시도를 모니터링합니다.

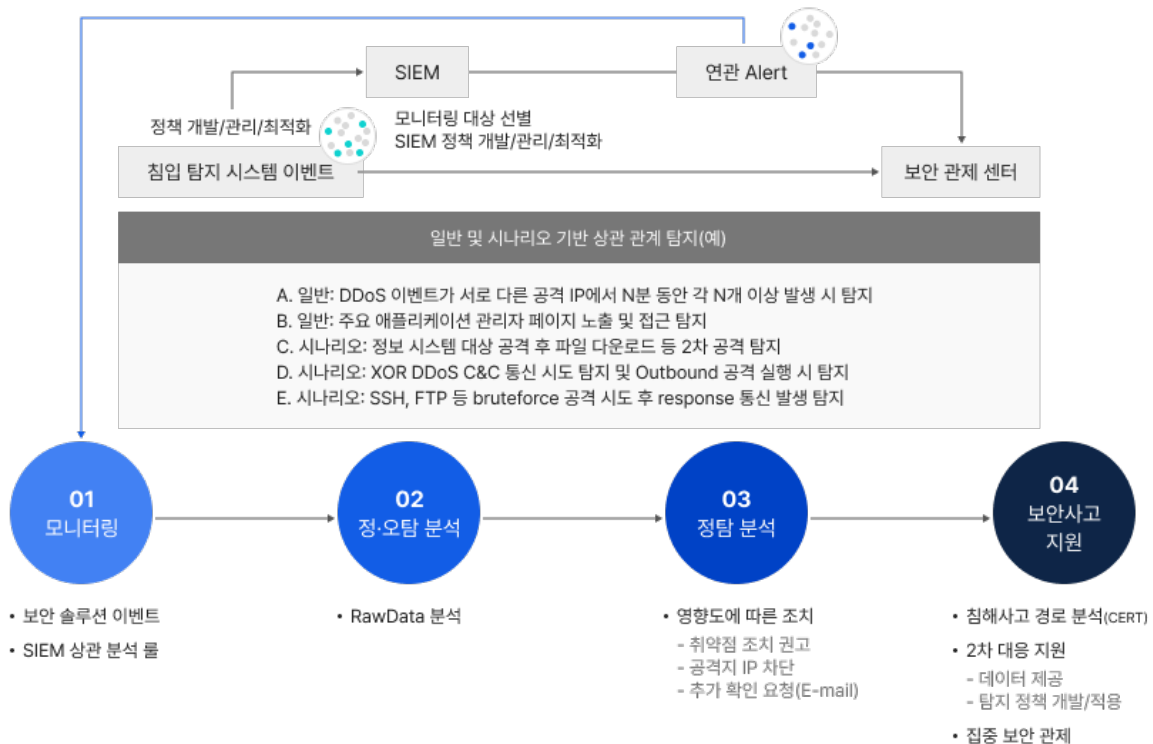


그림 6-2 이벤트 식별 및 탐지 방법

2. 침해 사고 대응

- NHN Cloud는 침해 사고 의심 상황이나 내·외부의 보안 사고 및 취약점 발견 즉시 대응합니다. 신고된 내용의 진위 여부를 확인하고, CERT(computer emergency response team)는 침해 사고 대응 프로세스에 따라 확산 방지와 사고 원인 분석을 수행합니다. 또한 외부 기관의 협력과 온라인 공지를 통해 보안 문제를 이용자에게 신속히 공지하고 추가 문제가 발생하지 않도록 조치합니다.
- 실시간 모니터링을 통한 침해 사고 의심 상황 인지 및 사내 사고 접수를 통한 인지
 - 보안 이벤트 연관 분석, Raw 데이터, 패킷 덤프 분석, 영향력 확인
 - 침해 의심 신고에 대한 1차 분석 수행
 - 침해 사고 확정 및 침해 등급 분류, 침입 IP 차단, 서비스 중지, 1차 상황 전파 등 선조치 수행
 - 침해 사고 확산 여부 확인 및 디지털 포렌식, 취약점 제거 및 서비스 복구
 - 포맷, 보안 패치 등 침해 사고에 악용된 취약점 제거 및 서비스 복구
 - 재발 방지 대책 수립 및 각 유관 부서의 재발 방지 이행 여부에 대한 지속 점검

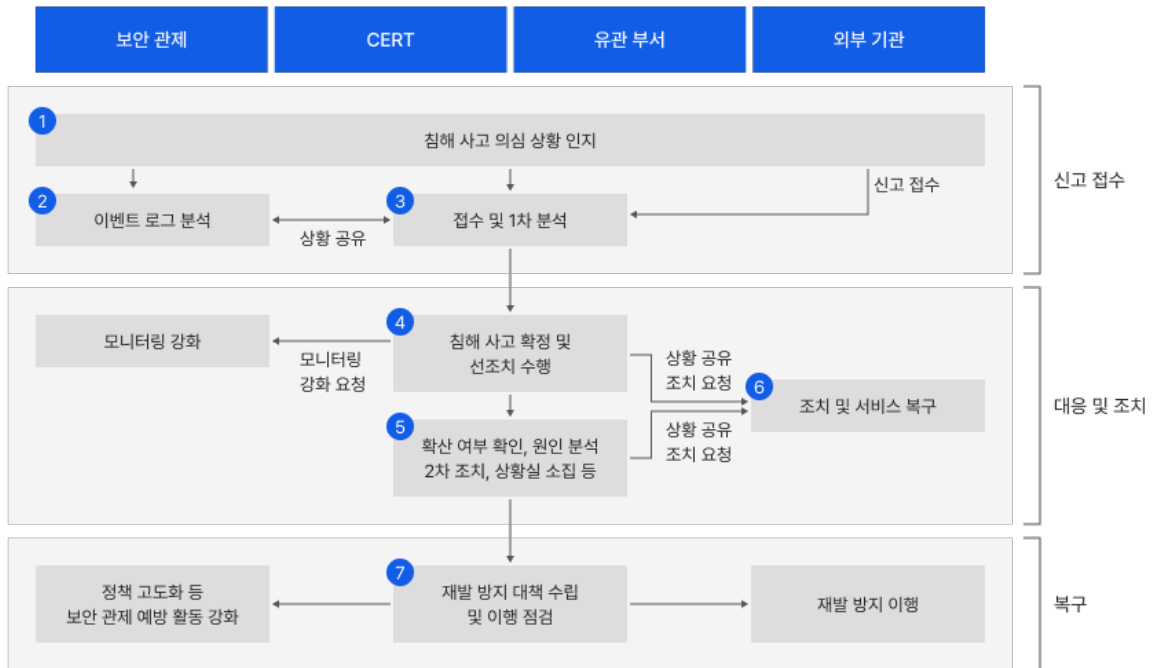


그림 6-3 침해 사고 대응 프로세스

6.1.2 취약점 점검과 모의 훈련

1. 모의 해킹 및 소스 코드 진단

- NHN Cloud 내부 분석 전담 조직을 통해 웹, 앱에 대한 정기/수시 모의 해킹을 진행하며, 취약점 발견 시 조치 후 안전성 검사 통과 후 서비스를 오픈합니다.
- 웹, 앱에 대한 개발 및 완료 후 소스 코드에 대한 자동, 수동 분석을 통한 오류 및 보안 취약 부분을 발견하고 조치합니다.

2. 취약점 점검

- 물리 시스템(서버, 네트워크, DB, 보안 장비)에 대해 자체 제작한 취약점 스캐너를 이용한 주기적인 스캐닝으로 취약점을 발견하고 개선하는 활동을 수행합니다.
- 물리 시스템(서버, 네트워크, DB, 보안 장비)에 보안 위험 요소를 대응하기 위해 내부 및 국·내외 인증 기준 및 자체 보안 기준 항목에 따라 보안 하드닝을 진행하여 취약 요소를 제거합니다.

3. 사이버 침해 모의 훈련

- 기관 및 자체 DDoS 공격, APT(advanced persistent threat) 공격, 악성 메일, 웹/앱 공격 등의 모의 훈련을 통해 클라우드 인증 사업자의 침해 사고 대응 역량을 확인하고, 클라우드의 보안성과 관련 법규에서 요구하는 침해 사고 대응 절차를 점검하여 미흡한 사항을 개선하기 위한 활동을 정기적으로 진행하고 있습니다.

7 NHN Cloud 가상화 인프라 보안

7.1 클라우드 가상화 인프라 보안

클라우드 가상화 인프라는 데이터 센터의 물리 서버, 네트워크, 스토리지 등으로 구성되어 있으며, 가상화 기술을 통해 가상 서버, 가상 네트워크, 가상 스토리지 등의 리소스를 생성해 클라우드 서비스를 제공합니다. 이를 통해 이용자는 컴퓨팅 리소스를 생성하고 필요에 따라 즉시 리소스를 확장하거나 축소하면서 서비스를 효율적으로 운영할 수 있습니다.

이러한 클라우드 가상화 인프라 자원을 보호하기 위한 접근 제어, 네트워크 보안, 데이터 보호 등의 기능으로 이용자 데이터의 안전을 보장하고, 인프라 자원의 안전성을 확보하여 클라우드 환경에서 안전하게 비즈니스를 수행할 수 있도록 합니다.

NHN Cloud 주요 인프라 서비스에서 제공하는 보안 기능을 통해 이용자의 서비스 환경을 안전하게 구성할 수 있습니다.

7.1.1 Compute

1. Instance

- 인스턴스는 클라우드 컴퓨팅 환경에서 사용되는 가상 서버입니다. 가상화 기술을 사용해 하나 이상의 물리적 서버에서 동작합니다. 가상의 CPU, 메모리, 스토리지, 네트워크를 할당 받아 이용자가 사용할 수 있도록 구성된 서버입니다. 이러한 가상 서버는 이용자 영역으로 NHN Cloud는 접근이 불가하며, 이용자는 가상의 서버에 운영체제, 애플리케이션 등을 설치하고 NHN Cloud에서 제공하는 다양한 서비스를 조합하여 서비스 환경을 만들 수 있습니다.

2. GPU Instance

- GPU 인스턴스는 GPU(graphics processing unit)를 추가 구성한 가상 서버입니다. GPGPU(general-purpose computing on graphics processing units) 기술을 사용해 대규모 병렬 계산을 수행할 수 있도록 설계되어 기계 학습, 딥 러닝, 데이터 처리 등의 고성능 컴퓨팅 작업에 적합합니다. NHN Cloud는 NVIDIA V100과 T4 GPU 모델을 제공합니다. 딥 러닝, 기계 학습, 비디오 인코딩, 게임 스트리밍 등 작업에 따라 최적의 GPU를 선택할 수 있습니다.

3. Image

- 이미지는 운영체제와 애플리케이션이 설치된 가상 디스크이며, 인스턴스의 기본 디스크로 사용합니다. NHN Cloud에서는 다양한 운영체제와 애플리케이션이 설치된 이미지를 기본으로 제공하며, 이용자의 환경에 맞게 이미지를 수정하여 사용할 수도 있습니다.
- 이미지는 가상 하드웨어에 최적으로 실행되도록 설정되어 있고, 보안 하드닝을 완료한 이미지를 제공합니다.

4. 보안 그룹(security groups)

- 보안 그룹은 인스턴스의 송수신 트래픽을 제어해 인스턴스를 보호할 목적으로 사용합니다. 규칙으로 지정한 트래픽은 허용하고 그 외 트래픽은 차단하는 포지티브 시큐리티 모델(positive security model)을 사용합니다.
- 보안 그룹은 인바운드 및 아웃바운드 정책에 대해 IP 주소, 포트 번호, 프로토콜을 기반으로 트래픽에 대한 패킷을 필터링합니다. 또한 stateful로 동작하기 때문에 규칙으로 연결된 세션은 반대 방향의 규칙이 없더라도 통신이 허용됩니다.

5. 키 페어(key pair)

- SSH Key Pair(키 페어)는 공개 키 기반 구조(public key infrastructure, PKI)를 바탕으로 개인 키(private key)와 공개 키(public key) 두 개의 암호화 키로 이루어집니다. 이용자는 키 페어의 개인 키를 이용해 로그인 정보를 인코딩하여 인스턴스로 전송해 접속 인증을 받은 후 안전하게 인스턴스에 접속할 수 있습니다. 키 페어 사용은 다수의 인스턴스 운영에 효율적이고 보안성이 높아 일반적인 아이디/패스워드를 사용하는 것보다 안전합니다.

- 키 페어는 NHN Cloud 콘솔에서 새로 만들 수도 있고, 이용자가 직접 만든 키 페어를 등록하여 사용할 수도 있습니다.
- 키 페어를 새로 생성하면 키 페어의 개인 키(.pem)를 다운로드하여 인스턴스에 접근할 수 있습니다. 개인 키는 두 번 발급되지 않으며, 외부 유출 시 해당 키로 인스턴스에 접근할 수 있으므로 안전하게 관리해야 합니다.

6. IP/MAC Spoofing 방어

- IP/MAC 스푸핑은 네트워크에서 심각한 문제이며 네트워크 환경을 교란하거나 데이터를 가로챌 수 있습니다. NHN Cloud에서는 OS 커널 파라미터 변경과 네트워크 인터페이스 생성 시 보안 기능을 사용해 해당 네트워크 인터페이스의 IP/MAC 주소가 출발지가 아닌 패킷이 나가는 것을 차단하여 스푸핑을 방지합니다.

7. Auto Scale

- 오토 스케일 서비스를 사용하면 인스턴스의 부하를 지속적으로 모니터링하여 필요한 경우 인스턴스를 추가로 생성하거나 삭제할 수 있습니다. 또한 개별 인스턴스에 네트워크 단절 등의 장애가 발생하면 자동으로 새로운 인스턴스를 생성해 장애가 발생한 인스턴스를 대체할 수도 있습니다. 오토 스케일을 통해 부하와 장애에 실시간으로 대응해 안정적이고 탄력적인 서비스를 제공할 수 있습니다.

8. Auto Scaling 그룹

- 스케일링 그룹은 인스턴스를 추가로 생성 또는 삭제하는 조건과, 조건이 만족하는 경우의 동작을 정의한 것입니다.
- Auto Scaling 그룹 설정 시 최소/최대 인스턴스 개수를 지정할 수 있습니다. 확장과 감축(scale out/scale in)이 발생하더라도 인스턴스의 수량이 무한정 증가하거나 감소하면 비용 및 운영에 영향을 줄 수 있기 때문에 최소/최대 인스턴스 수량을 사전 정의해 일정 범위에서 사용할 수 있도록 설정할 수 있습니다.



그림 7-1 Auto Scaling Group

9. Auto Scale 정책

- 인스턴스를 생성하거나 제거하는 기준을 정의한 것으로 한 개 이상의 조건이 충족했을 때 동작합니다. 정책의 조건은 인스턴스 성능 지표, 기준 값, 지속 시간으로 구성되며, 인스턴스 성능 지표는 CPU, Memory, Disk, Network의 사용률과 상태에 따라 정의할 수 있습니다.

표 7-1 Auto Scaling 구성 요소

구성 요소	설명
설정	<ul style="list-style-type: none"> • 인스턴스 템플릿을 등록하고 Auto Scaling 발생 시 구동되는 이미지 지정 • 최소/최대/구동 인스턴스 수량 정의

구성 요소	설명
정책	<ul style="list-style-type: none"> • Auto Scaling 시 사용할 자원 및 스케줄 정책 정의 • 자원 변화에 따른 증설/감축/자동 복구 정책과 스케줄에 따른 예약 작업을 통해 1회 또는 Cron 설정을 지원 • Auto Scale 구동되기 위한 인스턴스 성능 지표 조건 정의[(CPU(%), Memory(%), Disk(KB/m), Network(KB/m)]
로드 밸런서	<ul style="list-style-type: none"> • 확장 정책이 발동되었을 때 생성된 인스턴스는 지정된 로드 밸런서에 연결되며, 새로 추가된 인스턴스에 부하를 분배합니다.

7.1.2 컨테이너

1. NHN Kubernetes Service(NKS)

- NHN Kubernetes Service(NKS)는 클라우드에서 쿠버네티스를 올바르게 안전하게 구동할 수 있게 쿠버네티스 클러스터를 생성하고 관리할 수 있는 서비스입니다. 이용자는 웹 콘솔을 이용해 NHN Cloud에 맞는 쿠버네티스 클러스터를 만들고 관리할 수 있습니다. 클러스터의 컨트롤 플레인(마스터)은 NHN Cloud에서 관리하고 고가용성을 보장하며, 이용자는 노드와 서비스, 파드(Pod) 등을 관리하며 서비스를 이용할 수 있습니다. NHN Cloud의 클라우드 리소스와 연동해 Managed Kubernetes 제공을 통해 워커 노드(worker node)의 자동 증설 및 감축 등이 용이합니다.
- 클러스터 사용을 위한 권한
클러스터를 만들고자 하는 사용자는 대상 프로젝트에 대해 반드시 기본 인프라 서비스의 Infrastructure ADMIN 또는 Infrastructure Load Balancer ADMIN 권한이 있어야 기본 인프라 서비스를 기반으로 하는 클러스터를 정상적으로 생성하고 활용할 수 있습니다.
- 마스터
마스터는 클러스터 내에서 중앙 집중적인 제어를 담당하는 컴포넌트입니다. 여러 구성 요소로 구성되어 있으며, 대표적으로는 클러스터의 모든 리소스를 관리하는 중앙 집중적인 API 엔드 포인트인 API 서버, 새로운 파드를 어느 노드에 배치할지 결정하는 스케줄러, 클러스터 내의 리소스 상태를 감시하고 제어하는 컨트롤러 매니저가 있습니다.
- 노드
클러스터 내에서 애플리케이션 컨테이너를 실행하는 워커 머신입니다. 워크로드(workload)를 실행하기 위한 기본 단위이며, 각 노드는 컨테이너 런타임(예: Docker)과 쿠버네티스 에이전트 프로세스(Kubelet)를 포함합니다. 노드는 애플리케이션을 실행하는 데 필요한 모든 리소스(예: CPU, 메모리, 스토리지 등)를 제공하며, 클러스터의 규모를 확장할 수 있습니다. 노드는 마스터와 연결해야 동작하며, 애플리케이션 구동, 정지 등의 명령에 따라 수행합니다.

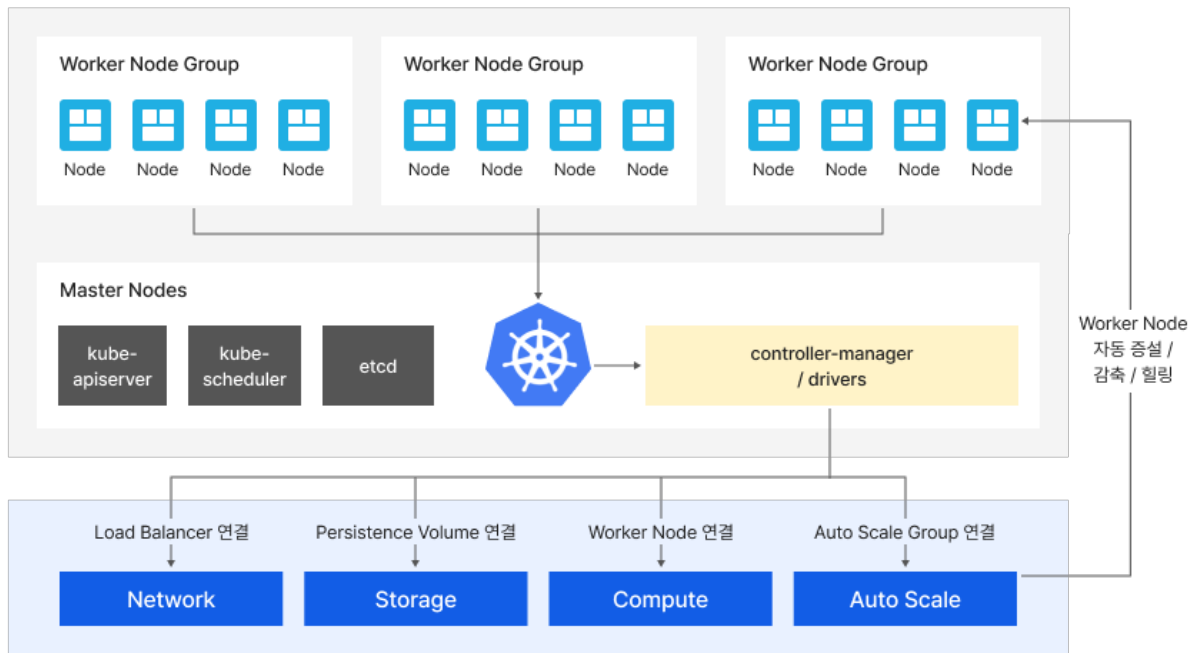


그림 7-2 NHN Kubernetes Service 특징

2. NHN Container Service(NCS)

- NHN Container Service(NCS)는 컨테이너를 구동하는 환경을 제공하는 서비스입니다. 인스턴스, 쿠버네티스와 같은 컨테이너 실행 환경을 구성하지 않아도 이 서비스를 이용하여 컨테이너를 실행할 수 있습니다.
- 퍼블릭/프라이빗 컨테이너 레지스트리에 보관된 컨테이너 이미지를 구동시킬 수 있습니다.
- 컨테이너는 이용자 VPC에 연결되므로 VPC를 통해 통신 가능한 인스턴스, 로드 밸런서, NAS 등 모든 IaaS 자원과 통신할 수 있고, VPC가 제공하는 네트워킹 기능을 활용할 수 있습니다.
- 컨테이너에 로드 밸런서를 연결해 플로팅 IP와 도메인을 통해 서비스를 외부에 노출시킬 수 있습니다.
- 컨테이너의 리소스 사용률(CPU, 메모리, 디스크, 네트워크) 확인이 가능하며, 수집된 데이터는 최대 1년간 보관됩니다. 또한 워크로드의 템플릿 변경 진행 상황 및 이력을 확인할 수 있는 실행 히스토리 기능도 제공합니다.

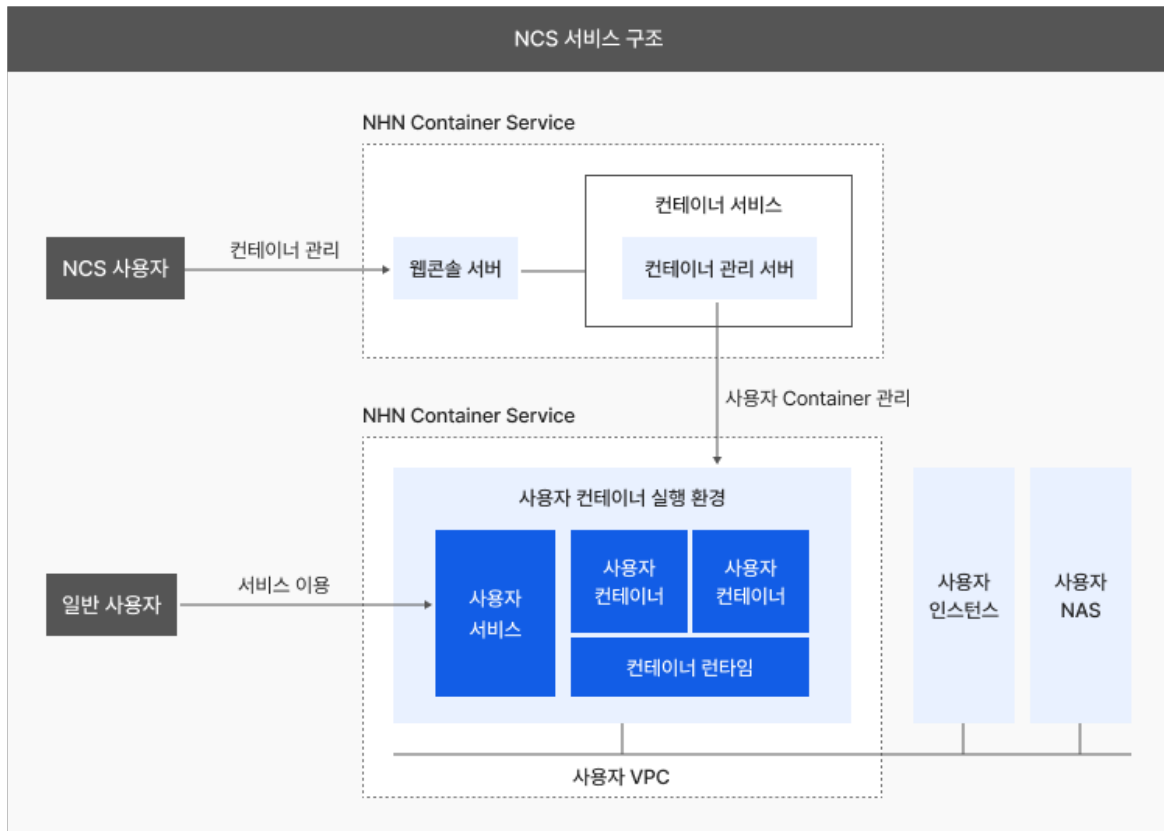


그림 7-3 NHN Container Service 구조

3. NHN Container Registry(NCR)

- NHN Cloud의 확장성 및 안전성이 보장된 오브젝트 스토리지 기반의 도커 컨테이너 이미지를 쉽고 안전하게 저장, 관리, 배포할 수 있는 컨테이너 레지스트리 서비스입니다. NHN Container Registry(NCR) 서비스는 NHN Kubernetes Service(NKS)와 연동해 이용자의 애플리케이션을 손쉽게 컨테이너 환경으로 구축할 수 있습니다.
- NHN Cloud 인증 및 권한 관리와 HTTPS 암호화 통신으로 보안성이 높습니다.
- 컨테이너 이미지 보호 기능으로 레지스트리에 저장된 이미지와 아티팩트가 삭제/변경되지 않도록 할 수 있습니다.
- 보안을 강화하기 위해 인터넷 게이트웨이에 연결하지 않고 외부 네트워크와 단절된 인스턴스에서 NCR을 사용하고자 할 때 서비스 게이트웨이와 연동해 Private URI(NHN Cloud의 VPC 네트워크 내에서 사용할 수 있는 NCR 주소) 기능을 활용할 수 있습니다.

- 이미지 취약점 스캐닝 기능을 사용해 아티팩트에 대한 수동 스캔을 할 수 있으며, 특정 간격으로 NCR 내 모든 아티팩트를 자동으로 스캔하도록 주기를 설정할 수도 있습니다. 스캔 결과에 대한 자세한 취약점 정보도 확인되며, 이미지에 포함된 CVE(common vulnerabilities and exposure)를 식별해 CVE의 심각도에 따라 이미지의 실행을 허용하지 않을 수 있습니다. 필요시 CVE 허용 목록을 만들어 특정 CVE는 무시할 수도 있습니다.

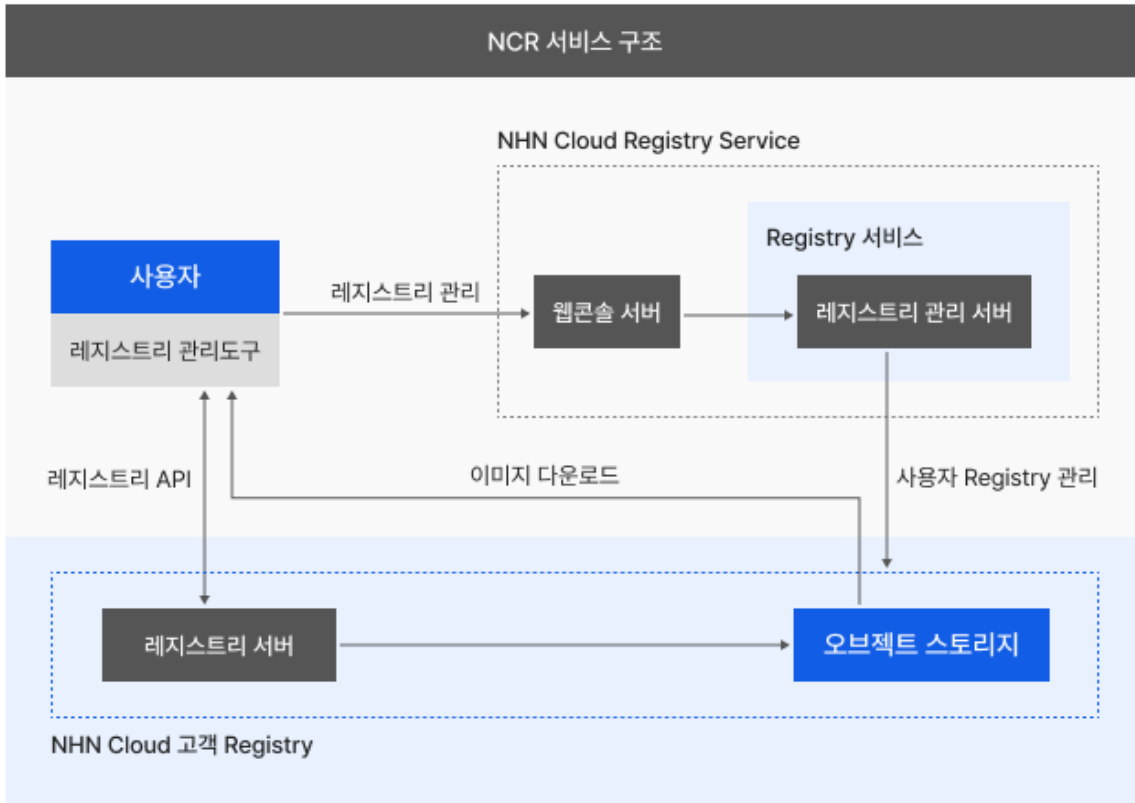


그림 7-4 NHN Container Registry 구조(오브젝트 스토리지 기반)

7.1.3 스토리지

1. Block Storage

인스턴스 기본 디스크 외에 추가로 연결하여 사용할 수 있는 블록 레벨 스토리지로 쉽게 복제하여 여러 인스턴스에 할당할 수 있습니다. 인스턴스에 마운트 시 블록 스토리지 생성, 파티션 생성, 포맷, 디스크 마운트 작업을 수행해야 하며, 스냅샷 서비스를 이용해 특정 시점의 블록 스토리지 상태를 저장 및 복구할 수 있습니다. 또한 디스크에 대한 암호화 적용을 통해 안전하게 보호하고 있습니다.

- 무결성 점검

스냅샷에서 블록 스토리지 생성 시 메타데이터 무결성 체크 기능을 제공해 데이터의 정합성과 안정성을 검증할 수 있습니다.

- 데이터 삭제

사용 중이던 인스턴스 및 스토리지의 해제 후 이용자는 데이터 보안을 위해 스토리지 공간을 표준화된 방법(DoD 5220.22-M-ECE, DoD 5220.22-M, HMG IAS No.5 Higher Overwrite, Russian GOST, Canadian RCMP OPS, German VSITR, NIST 800-88 등) 수준 이상으로 삭제해야 합니다. 추가로 DoD 5220.22-M 패턴을 적용할 수 있는 scrub(Linux), Disk Wipe(Windows)를 이용해 데이터 삭제 가이드를 제공하고 있으니 데이터 삭제 시 참고 바랍니다.

- [Block Storage 데이터 완전 삭제 가이드 바로 가기](#)

2. NAS(network attached storage)

NAS는 공유 액세스, 확장성, 고가용성 및 보안성을 제공하는 분산 파일 시스템으로 여러 인스턴스에서 네트워크를 통해 접근할 수 있는 스토리지입니다. 접근 권한 및 암호화를 통해 안전하게 사용할 수 있는 기능을 함께 제공하고 있습니다.

- 접근 제어(access control list, ACL)

접근 제어 설정을 통해 특정 IP 주소 및 서브넷으로 파일 시스템에 대한 읽기, 쓰기 권한을 제어할 수 있습니다.

- 고가용성

NAS에 저장된 데이터를 자동 또는 수동으로 복제(스냅샷)할 수 있으며, 이를 통해 단일 장애 지점의 위험을 방지하고 데이터의 손실 위험을 줄일 수 있습니다.

3. Object Storage

대용량 데이터를 저장하고 관리할 수 있는 안전하고 안정적인 스토리지 서비스입니다. REST API를 사용해 플랫폼 독립적인 방식으로 인터넷 연결이 되는 어느 곳에서나 접근할 수 있으며, 용량과 처리 능력을 탄력적으로 활용할 수 있습니다.

- 데이터 무결성

이용자가 오브젝트 스토리지를 이용해 업로드한 데이터의 무결성을 확인할 수 있도록 md5 hash 값을 제공하고 있습니다. 업로드 요청의 응답 헤더 또는 오브젝트 조회 요청의 응답 헤더에서 Etag 값을 확인할 수 있습니다. 업로드 후 오브젝트의 Etag 값과 로컬에서 계산한 md5 값을 비교해 데이터의 무결성을 확인할 수 있으며, 클라이언트는 업로드 응답 헤더에서 Etag를 얻어 확인이 가능하고, 추가로 클라우드 콘솔에서도 Etag 값을 쉽게 확인할 수 있습니다.

- 데이터 고가용성

오브젝트 스토리지의 데이터를 안전하게 저장하기 위해 오브젝트를 하나 업로드하면 서로 다른 디스크에 3개의 오브젝트가 저장됩니다. 데이터가 변경되려면 서로 다른 디스크에 저장된 3개의 오브젝트가 md5 값까지 동일하게 동시에 변경되어야 하며, 만약 일부만 변경되었다면 변경된 오브젝트는 삭제되고 다른 온전한 오브젝트의 복제본으로 복구됩니다. 또한 리전 간 복제 기능을 활용해 오브젝트를 소스 리전과 동일하게 복제하고 관리하여 재해 복구(disaster recovery, DR)를 위한 데이터를 관리할 수 있습니다.

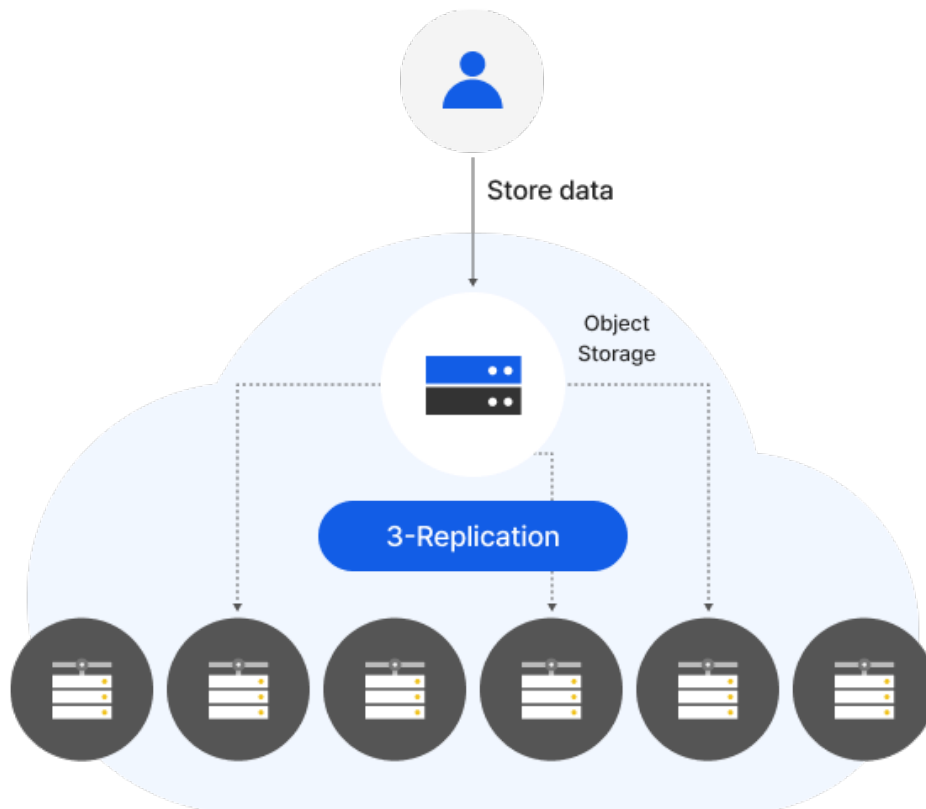
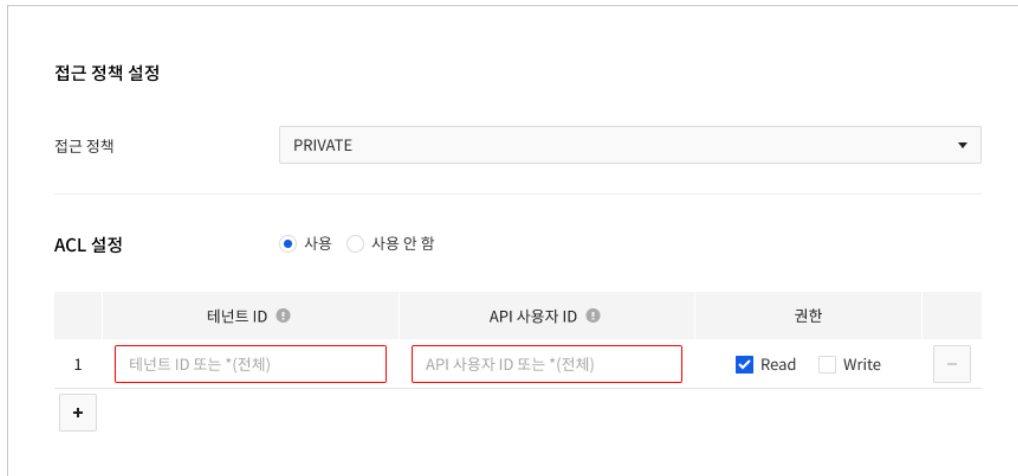


그림 7-5 오브젝트 스토리지 복제

- 접근 정책

컨테이너 접근 정책을 통해 허가된 사용자만 컨테이너 내부의 오브젝트에 접근할 수 있거나(PRIVATE) 또는 공개 URL을 통해서 누구나 컨테이너 내부의 오브젝트에 접근할 수 있게(PUBLIC) 구성할 수 있습니다. 추가로 각 컨테이너의 ACL 설정으로 테넌트 ID, API 사용자 ID 별로 읽기(Read), 쓰기(Write) 권한을 제어할 수 있습니다.



접근 정책 설정

접근 정책: PRIVATE

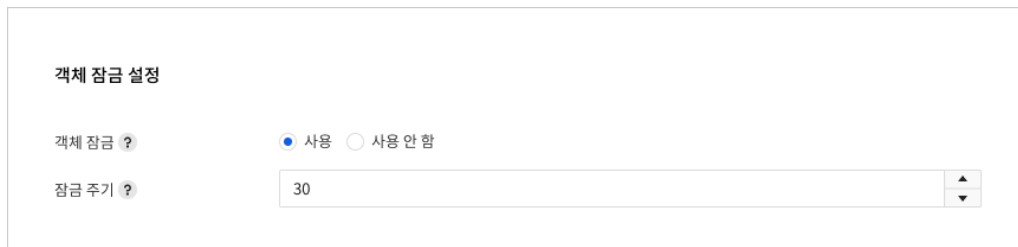
ACL 설정: ☒ 사용 ☐ 사용 안 함

	테넌트 ID ⓘ	API 사용자 ID ⓘ	권한	
1	테넌트 ID 또는 *(전체)	API 사용자 ID 또는 *(전체)	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write	-
+				

그림 7-6 접근 정책 설정

- 객체 잠금 설정

객체 잠금 컨테이너에 업로드한 오브젝트는 지정된 시간 동안 개체가 삭제되거나 덮어쓰지 않도록 보호합니다. WORM(write once, read many) 모델을 사용하여 저장되며, 오브젝트에 잠금 만료 날짜를 설정해 만료 날짜 이전에는 오브젝트를 덮어쓰거나 삭제할 수 없도록 보호할 수 있습니다. 이러한 WORM 기능은 금융, 보험, 의료 및 보안 산업에 유용하게 적용할 수 있습니다.



객체 잠금 설정

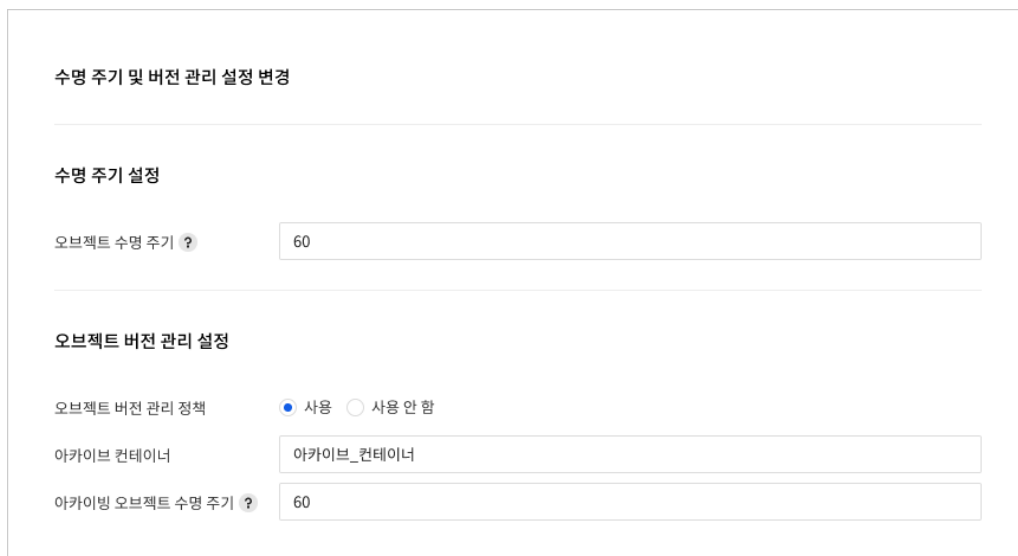
객체 잠금 ? ☒ 사용 ☐ 사용 안 함

잠금 주기 ? 30

그림 7-7 객체 잠금 설정

- 수명 주기 및 버전 관리

컨테이너에 저장되는 오브젝트의 수명 주기와 버전 관리 정책을 조회하고 변경할 수 있습니다. 수명 주기는 일 단위로 관리되며, 오브젝트 버전 관리를 통해 이전 버전의 오브젝트를 관리할 수 있으며 설정된 수명 주기로 과거 오브젝트는 자동 삭제됩니다.



수명 주기 및 버전 관리 설정 변경

수명 주기 설정

오브젝트 수명 주기 ? 60

오브젝트 버전 관리 설정

오브젝트 버전 관리 정책 ☒ 사용 ☐ 사용 안 함

아카이브 컨테이너 아카이브_컨테이너

아카이빙 오브젝트 수명 주기 ? 60

그림 7-8 수명 주기 및 버전 관리 설정

- 교차 출처 리소스 공유(cross-origin resource sharing, CORS)

브라우저에서 Object Storage API를 직접 호출하려면 교차 출처 리소스 공유 설정이 필요합니다. 컨테이너의 교차 출처 리소스 공유 항목의 변경 버튼을 클릭하면 허용할 출처 URL을 등록할 수 있습니다. URL에는 프로토콜(https:// 또는 http://)을 포함해 공백 ()으로 구분된 하나 이상의 출처를 입력하거나 *을 등록하면 모든 출처를 허용할 수 있습니다.

그림 7-9 교차 출처 리소스 공유(CORS) 설정

- 암호화

암호화 컨테이너에 업로드하는 오브젝트는 NHN Cloud의 Secure Key Manager 서비스에서 관리하는 대칭 키를 사용해 암호화됩니다. 따라서 암호화 컨테이너를 만들기 위해서는 미리 Secure Key Manager 서비스에서 대칭 키를 생성해야 합니다. 이 과정에서 Object Storage와 Secure Key Manager 사이의 내부 API 호출은 내부 접근 제어를 통해 제어하고 있습니다. 암호화 컨테이너의 오브젝트를 복사 또는 리전 간 복제를 통해 다른 컨테이너에 복사하면 대상 컨테이너의 암호화 설정에 따라 재암호화되거나 복호화되어 저장됩니다.

Secure Key Manager 서비스에서 암호화 컨테이너에 설정한 대칭 키를 회전한 다음 새로운 오브젝트를 업로드하면 이전 버전 키로 암호화된 오브젝트가 회전된 키로 재암호화 됩니다. 이 작업은 사용량에 따라 처리 시간이 길어질 수 있습니다. 재암호화가 완료되기 전에 이전 버전 키를 삭제하지 않도록 주의해야 합니다.

Secure Key Manager 서비스에서 암호화 컨테이너에 설정한 대칭 키를 삭제하면 암호화된 오브젝트를 복호화할 수 없습니다. 대칭 키를 실수로 삭제하지 않도록 주의하여 관리해야 합니다.

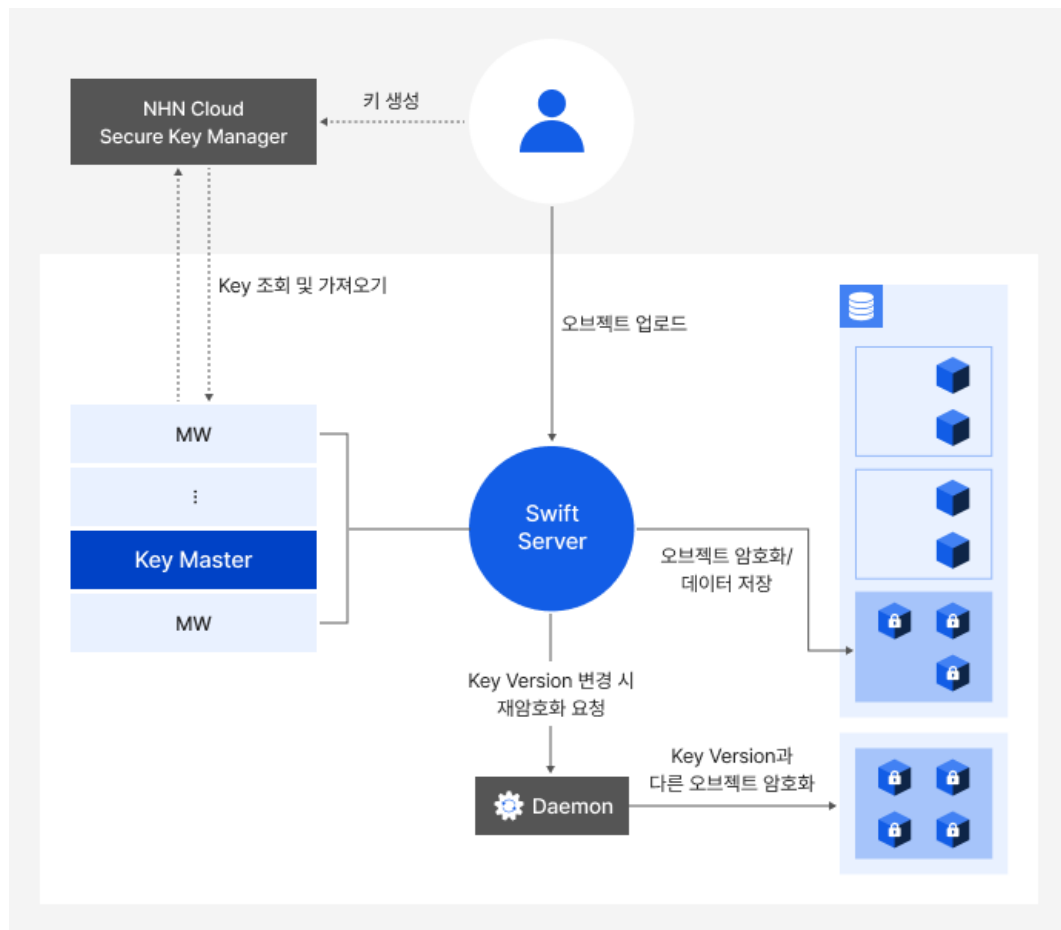


그림 7-10 Object Storage 암호화 과정

4. Backup

백업은 보안 위협, 이용자의 조작 실수, 저장 장치의 고장, 자연재해 등으로 인한 데이터 손실에 대비해 복제본을 만들고 안전하게 보관해 주는 서비스입니다. 또한 보관한 복제본을 이용해 데이터를 복구할 수 있습니다.

- 백업 방식

전체 백업과 증분 백업 방식을 함께 사용합니다. 최초 1회는 이용자가 등록한 경로의 데이터 전체를 백업하고, 이후 백업 주기에 따라 데이터의 중복을 제거하여 백업 데이터를 최소화할 수 있는 가변 길이 중복 제거(variable-length deduplication) 기술을 이용해 증분 데이터만 백업합니다. 이러한 방법은 백업 시간의 단축과 네트워크 사용량 감소로 효율적인 운영을 보장합니다. 또한 백업 대상과 스토리지 사이는 암호화 통신으로 안전하게 데이터를 보관합니다.

표 7-2 백업 서버 통신을 위한 보안 그룹(security groups)

방향	포트	리전	CIDR
Ingress/Egress	ALL TCP	한국(판교)	133.186.132.0/24
		한국(평촌)	133.186.207.4/32, 133.186.207.5/32
		일본(도쿄)	133.223.17.0/24
Egress	443	한국(판교)	103.243.202.188/32
		한국(평촌)	103.243.202.188/32
		일본(도쿄)	119.235.231.50/32

7.1.4 네트워크

1. VPC(virtual private cloud)

터널링 기술을 기반으로 하는 VPC는 논리적으로 격리된 가상 네트워크 환경을 구축하는 중요한 역할을 합니다. 이용자는 VPC를 이용해 논리적으로 격리된 가상 네트워크를 구축하고 완전히 독립된 IP 주소, 서브넷, 라우팅 테이블 및 게이트웨이를 구성하고 제어할 수 있습니다. 인터넷을 액세스할 수 있는 서비스를 연결하거나 폐쇄된 서브넷에서 데이터베이스나 애플리케이션을 구동할 수 있어 공유 인프라를 사용하는 것보다 높은 수준의 보안과 격리를 제공합니다.

VPC는 프라이빗 IPv4 CIDR 블록, 가상 라우터, 가상 스위치로 구성합니다. 가상 라우터는 VPC의 허브 역할을 하며 VPC 내의 가상 스위치를 연결하고 VPC를 서로 다른 네트워크에 연결하는 게이트웨이 역할을 합니다. 가상 스위치는 서로 다른 클라우드 리소스를 연결하는 VPC의 기본 네트워크 요소입니다. 이러한 가상 라우터와 가상 스위치는 클라우드의 VPC를 생성하게 되면 이용자가 직접 생성하지 않아도 클라우드 플랫폼에서 자동으로 구성됩니다.

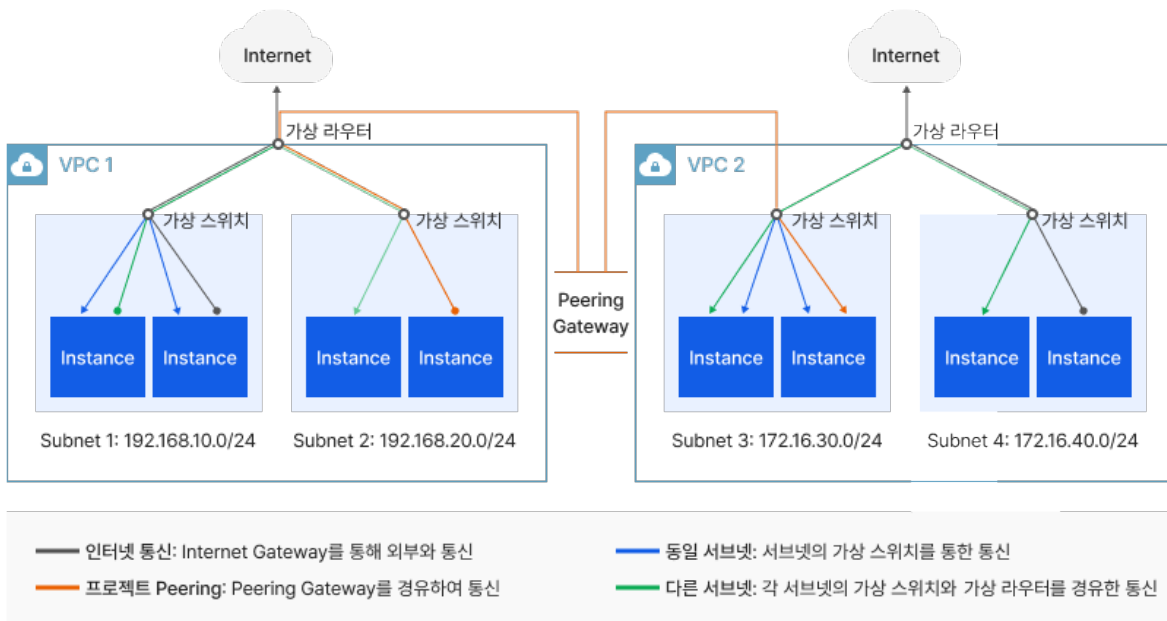


그림 7-11 VPC 네트워크 통신 플로우

- 프라이빗 네트워크

VPC의 IPv4 주소 범위는 아래와 같이 RFC 1918에 지정된 프라이빗(공개적으로 라우팅할 수 없는) IPv4 주소 영역에 있어야 하며, 링크 로컬 주소(169.254.0.0/16)에 포함되는 65,536개의 IP 주소는 사용할 수 없습니다.

표 7-3 커스텀 프라이빗 CIDR 블록

RFC 1918	IP 주소 범위	사용 가능한 주소 개수	가장 큰 CIDR 블록(서브넷 마스크)
24bit block	10.0.0.0~10.255.255.255	16,777,216	10.0.0.0/8(255.0.0.0)
20bit block	172.16.0.0~172.31.255.255	1,048,576	172.16.0.0/12(255.240.0.0)
16bit block	192.168.0.0~192.168.255.255	65,536	192.168.0.0/16(255.255.0.0)

- 서브넷

VPC는 서브넷으로 나누어 작은 네트워크 여러 개를 구성할 수 있습니다. 다만 서브넷의 경우는 VPC 주소 범위에 포함되어야 합니다. 서브넷이 생성되면 VPC에 포함된 기본 라우팅 테이블에 자동으로 연결되며 게이트웨이 IP는 자동으로 지정됩니다. 서브넷의 **정적 라우트** 설정을 이용해 라우팅할 패킷의 목적지 CIDR와 대상 패킷을 전달할 게이트웨이 정보를 구성할 수 있습니다. CIDR가 **0.0.0.0/0**인 정적 라우트를 생성하면 인스턴스의 기본 게이트웨이를 서브넷의 게이트웨이가 아닌 이용자가 설정한 다른 IP로 변경할 수 있습니다. 게이트웨이는 라우팅 테이블의 **라우트**와는 달리 텍스트로 입력해야 하며, 서브넷 내에

할당되지 않은 IP도 지정할 수 있습니다.

- 라우팅 테이블

라우팅 테이블은 VPC와 함께 생성되며 VPC가 삭제되면 함께 삭제됩니다. VPC의 라우팅 테이블은 시스템 라우팅 테이블과 사용자 지정 라우팅 테이블로 구성됩니다. 시스템 라우팅 테이블은 VPC 생성 시 VPC의 경로를 제어하기 위한 기본 라우팅 테이블입니다.

라우팅 테이블은 생성되는 위치에 따라 **분산형 라우팅(distributed virtual routing, DVR)** 방식과 **중앙 집중형 라우팅(centralized virtual routing, CVR)** 방식으로 생성할 수 있습니다.

- Network ACL

Network ACL은 VPC의 인바운드 및 아웃바운드 트래픽을 제어합니다. Network ACL은 상태 비저장(stateless) 방식으로 인바운드 트래픽을 허용하도록 구성하는 모든 규칙에 대해 해당 트래픽에 응답을 활성화하는 아웃바운드 규칙을 구성해야 합니다. 그렇지 않으면 요청에 대한 응답이 되지 않습니다. 유입/유출 트래픽에서 Network ACL 설정은 보안 그룹 설정보다 먼저 적용됩니다. Network ACL 설정에서 허용되었더라도 보안 그룹에서 차단될 수 있으므로 두 곳 모두 확인해야 합니다. 한 프로젝트에 최대 10개의 ACL을 생성할 수 있습니다.

표 7-4 보안 그룹과 Network ACL 기능 비교

구분	보안 그룹	Network ACL	비고
제어 대상	인스턴스	네트워크	
설정 대상	Protocol, IP, Port	Protocol, IP, Port	ACL은 blacklist, whitelist 선택적으로 운영 가능
제어 트래픽	유입/유출 트래픽 선택 가능	src, dst 주소 선택 가능	
접근 제어 타입	허용 정책만 설정	허용 또는 차단 정책 선택 가능	

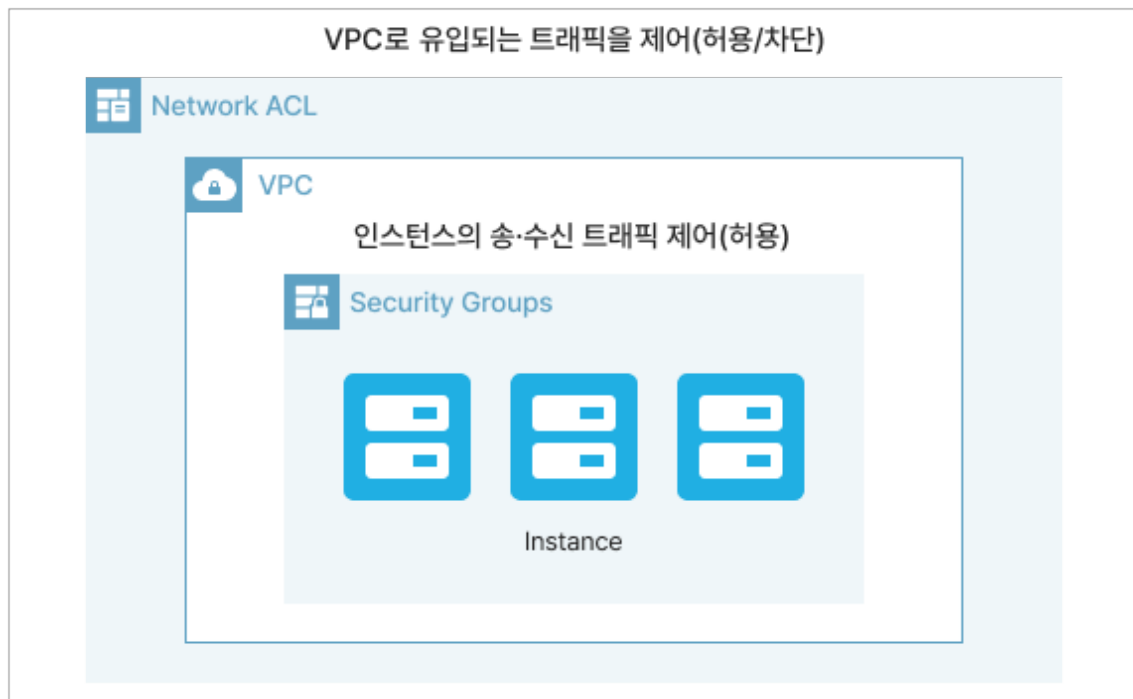


그림 7-12 Security Groups과 Network ACL 트래픽 제어 비교

2. Load Balancer

인스턴스 하나로 처리하기 힘든 부하를 여러 대의 인스턴스로 트래픽을 분산하는 서비스입니다. 로드 밸런서를 이용해 단일 장애 지점(single point of failure, SPOF)을 방지하고 응용 프로그램의 가용성을 향상시킬 수 있습니다. 로드 밸런서에 연결된 서버 중 일부 서버에 장애가 발생하면 자동으로 다른 서버로 부하를 배분해 서비스가 중단되는 상황을 막음으로써 높은 안정성을 보장하게 됩니다. 로드 밸런서만을 이용한 분산 처리는 정해진 서버 자원만 분산 처리하지만, Auto Scaling을 활용하면 더 탄력적인 운영이 가능합니다.

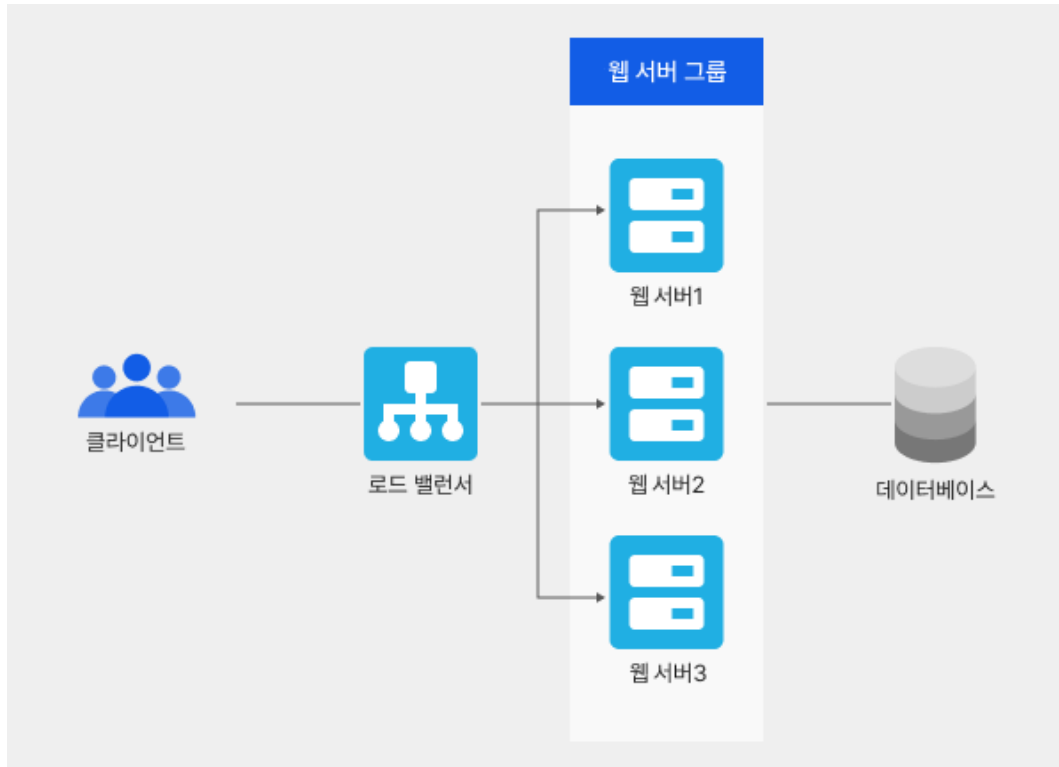


그림 7-13 로드 밸런서 구성

- 고가용성

로드 밸런서는 단일 장애 지점을 피하기 위해 이중화로 구성되어 있으며, LBaaS(load balance as a service) Node의 장애 발생 시 evacuation을 실행해 서비스 복구를 진행합니다. 장애가 발생했거나 점검 중인 인스턴스는 자동으로 서비스에서 제외해 가용성을 높일 수 있습니다. 또한 인스턴스의 Auto Scaling에 따른 시스템 및 트래픽 변동 시에도 지속적인 서비스를 제공합니다.

- 로드 밸런싱 방식

Round Robin(순차 선택): 트래픽을 전달할 인스턴스를 순차적으로 선택하는 방식입니다. 모든 멤버 인스턴스들이 같은 요청에 대해서 동일한 응답을 하는 경우에 사용할 수 있습니다.

Least Connections(최소 연결 우선 선택): 현재 TCP 연결 수가 가장 작은 인스턴스를 선택하는 방식입니다. 즉, TCP 연결 수를 기준으로 인스턴스들의 부하 상태를 파악하고 멤버 중 가장 부하가 적은 인스턴스로 요청을 보내 가능한 한 균등하게 처리될 수 있도록 합니다. 요청에 따른 처리 부하가 변동이 심할 때 적용한다면 특정 인스턴스에 부하가 집중되는 상황을 방지할 수 있습니다.

Source IP(원본 IP 기준 선택): 요청자의 원본 IP를 Hashing Key를 가지고 처리할 인스턴스를 선택하는 방식입니다. 이 방식을 사용하는 경우, 동일한 IP에서 들어오는 요청은 항상 같은 인스턴스로 전달됩니다. 한 이용자의 요청을 매번 동일한 인스턴스에서 처리하고자 할 때 사용하면 유용합니다.

- IP 접근 제어

로드 밸런서는 연결된 내부 서버의 IP 주소는 숨기고 대신 가상 IP 주소만 노출할 수 있습니다. 로드 밸런서로 유입되는 패킷을 제어하기 위해 IP 접근 제어 기능을 이용할 수 있으며 보안 그룹과는 구분되는 기능입니다.

표 7-5 보안 그룹과 로드 밸런서 IP 접근 제어 기능 비교

구분	보안 그룹	로드 밸런서 IP 접근 제어	비고
제어 대상	인스턴스	로드 밸런서	
설정 대상	Protocol, IP, Port	IP	로드 밸런서에 설정된 포트 이외의 트래픽은 기본적으로 차단
제어 트래픽	유입/유출 트래픽 선택 가능	유입 트래픽만 제어 대상	
접근 제어 타입	허용 정책만 설정	허용 또는 차단 정책 선택 가능	

- HTTPS 복호화(TERMINATED_HTTPS)

TERMINATED_HTTPS 프로토콜을 사용하는 로드 밸런서를 생성할 때 클라이언트와 로드 밸런서 간 통신에 사용하는 SSL/TLS(secure socket layer/transport layer security) 버전을 선택할 수 있습니다.

SSL/TLS 프로토콜 버전이 낮으면 보안 결함이 있을 수 있고 암호화 스위트(cipher suite)를 구성하는 암호 알고리즘의 보안 성도 낮기 때문에 클라이언트가 지원하는 SSL/TLS 버전 중 가장 높은 버전을 선택할 것을 권장합니다.

표 7-6 SSL/TLS 버전

SSL/TLS 버전 설정	로드 밸런서가 사용하는 SSL/TLS 버전
SSLv3	SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
TLSv1.0	TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
TLSv1.0_2016	TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3
TLSv1.1	TLSv1.1, TLSv1.2, TLSv1.3
TLSv1.2	TLSv1.2, TLSv1.3
TLSv1.3	TLSv1.3

※ SSL/TLS 버전별 암호화 스위트는 NHN Cloud 로드 밸런서 사용자 가이드를 참고 바랍니다.

- [NHN Cloud 로드 밸런서 사용자 가이드 바로 가기](#)

- SSL 인증서 등록

Certificate Manager를 이용한 연동과 직접 등록하는 방법 두 가지를 사용할 수 있습니다. Certificate Manager 서비스에 인증서를 등록하고 리스너에 해당 인증서를 연결하면 이메일로 인증서 만료일 알람을 받을 수 있습니다. Certificate Manager 서비스에서 인증서를 갱신한 경우는 영향을 받는 리스너의 인증서도 함께 갱신해야 합니다.

리스너에 직접 인증서를 등록한 경우에는 인증서 만료일 알람이 없습니다. 다만 콘솔의 리스너 화면에서 만료일을 확인할 수는 있습니다.

특히 공공기관의 경우 상위 기관과 국정원 룰 연동에 대한 구성이 가능하도록 고객의 내부 VPC에서 NHN Cloud 서비스와 마켓플레이스 솔루션(국내 솔루션)을 활용해 요구 사항에 충족한 서비스 구성이 가능합니다. 암호화된 TERMINATED_HTTPS 기능으로 복호화 후 IDS/IPS에서 패킷을 확인할 수 있습니다.

또한 구성 방식에 따라 IDS/IPS 단독으로 구성하거나 웹 방화벽, 방화벽과 같이 조합하여 이중화 구성도 가능합니다.

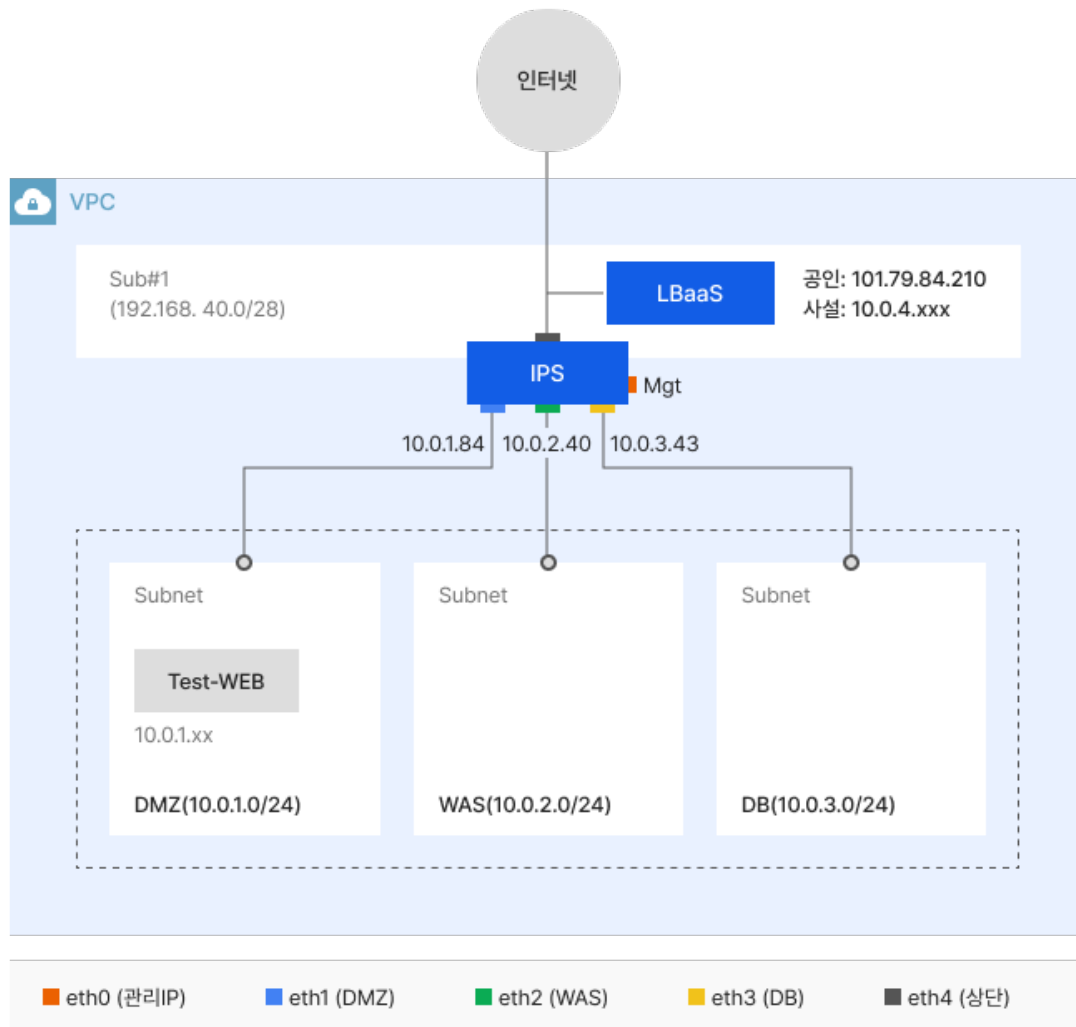


그림 7-14 고객 VPC 내부에서 VM IDS/IPS 구성(예)

- 유효하지 않은 요청 차단

HTTP 요청 헤더에 유효하지 않은 문자가 포함된 경우 이를 차단하는 기능입니다. 서버의 취약점을 노린 해커의 공격이나, 버그가 있는 브라우저를 통해서 유효하지 않은 문자가 포함된 HTTP 요청 헤더가 유입될 수 있습니다. 기능이 활성화되면 로드 밸런서는 유효하지 않은 문자가 포함된 HTTP 요청을 차단해 인스턴스에 전달되는 것을 막으며, 400 Bad Request를 클라이언트에 전송합니다

- 로깅

작업 로그는 CloudTrail에 기록되며 이용자는 콘솔을 사용해 작업 로그를 확인할 수 있고 추가로 CloudTrail을 통합 로그 관리 솔루션과 연동해 실시간 경보 체계를 수립할 수 있습니다.

- [CloudTrail 이벤트 목록 바로 가기](#)

3. X Gateway

- Internet Gateway

프라이빗 네트워크로 생성된 VPC는 인터넷 게이트웨이를 이용하여 VPC의 리소스를 인터넷에 연결할 수 있습니다. 인스턴스, 로드 밸런서에 플로팅 IP를 연결하여 외부에 서비스를 제공할 수 있습니다. 인터넷 게이트웨이를 생성하면 자동으로 인터넷 연결에 필요한 라우팅 설정과 퍼블릭 IP를 할당하며, 외부에서 인터넷 게이트웨이의 퍼블릭 IP 주소로 유입되는 트래픽을 차단하여 VPC 내부 인스턴스나 로드 밸런서에 직접 접근하는 것을 방지합니다.

- NAT Gateway

인터넷 게이트웨이에 연결되지 않은 프라이빗 서브넷의 인스턴스들이 NAT 게이트웨이의 플로팅 IP로 인터넷에 액세스할 수 있습니다. 하지만 인터넷에서 이 인스턴스들로 연결할 수는 없습니다. 외부에서 NAT 게이트웨이 주소로 연결하려는 트래픽은 차단됩니다.

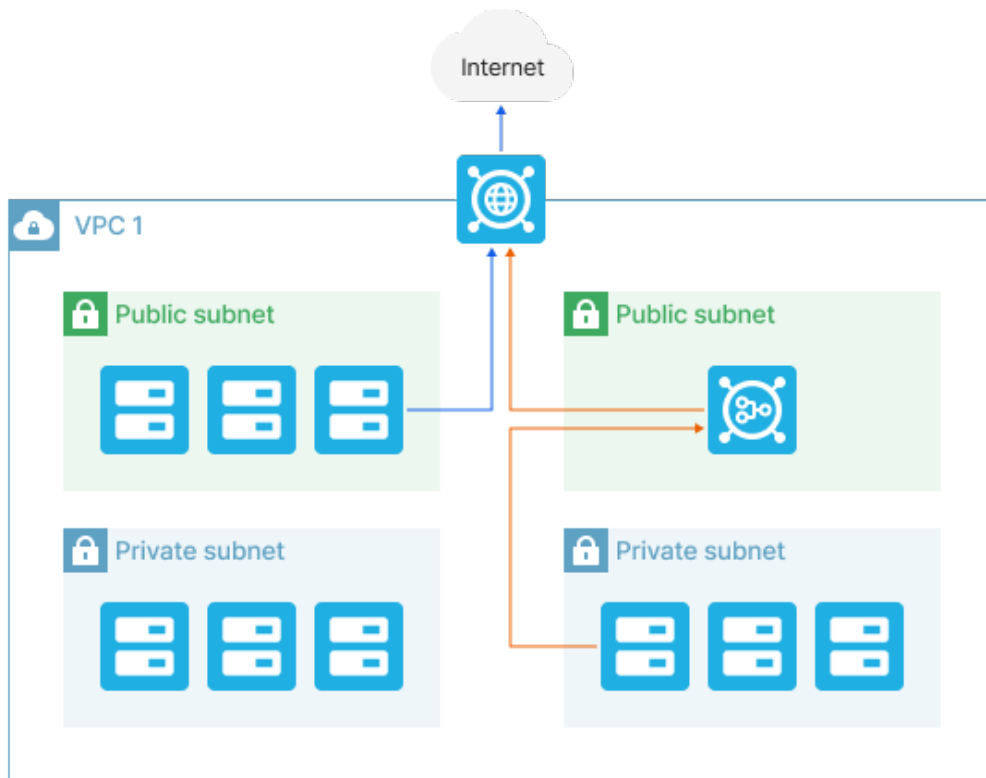


그림 7-15 Internet Gateway, NAT Gateway 연결(예)

표 7-7 Internet Gateway, NAT Gateway, NAT Instance 비교

구분	Internet Gateway	NAT Gateway	NAT Instance
가용성	이중화 지원	이중화 지원	이중화 지원 안 함
유지 관리	NHN Cloud에서 관리	NHN Cloud에서 관리	이용자가 직접 관리
고정된 소스 IP	사용 불가	사용 가능	사용 가능
보안 그룹	설정 불가	설정 불가	설정 가능
네트워크 ACL	설정 불가	설정 불가	설정 가능
SSH	설정 불가	설정 불가	설정 가능
Port Forward	설정 불가	설정 불가	수동 설정 가능

- Peering Gateway

서로 다른 두 개의 가상 사설 네트워크를 연결할 수 있습니다. 서로 다른 두 VPC를 연결하여 VPC에 할당된 사설 IP를 기반으로 상대 VPC 내의 리소스에 직접 액세스할 수 있습니다. 피어링(동일 리전, 동일 프로젝트), 프로젝트 피어링(동일 리전, 다른 프로젝트), 리전 피어링(다른 리전, 동일 프로젝트)을 제공합니다.

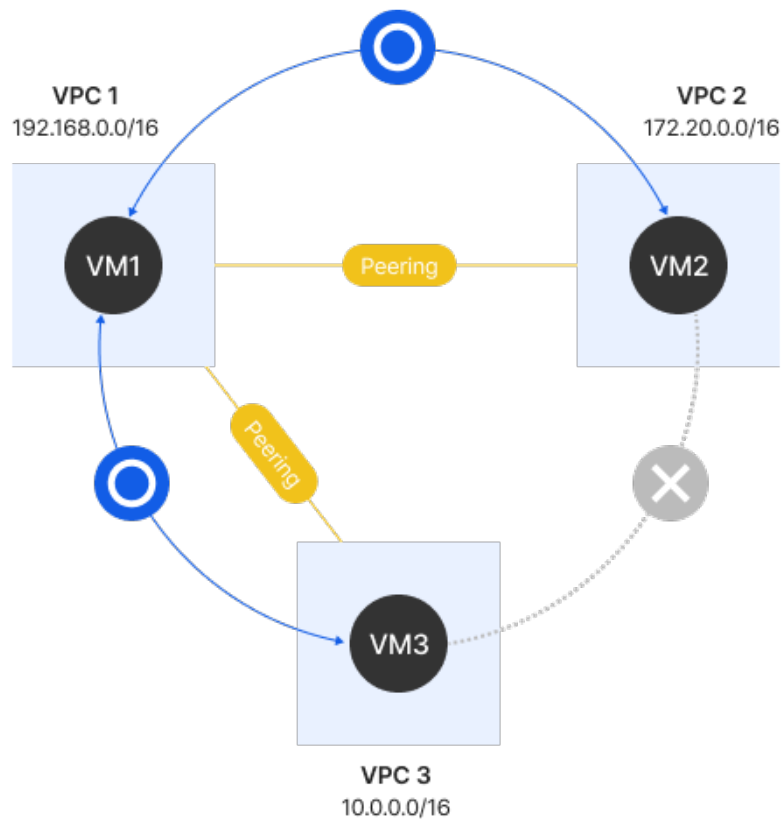


그림 7-16 VPC Peering

- VPN Gateway

Site-to-Site VPN 연결을 생성해 VPC와 고객의 온프레미스 네트워크 사이에 암호화된 연결을 할 수 있습니다. 암호화 알고리즘은 AES192, AES256, DES, 3DES를 제공하고 있으며, 무결성 알고리즘은 MD5, SHA1 중에 선택할 수 있습니다.



그림 7-17 VPN Gateway와 온프레미스 VPN 장비 연결 구성(예)

표 7-8 IKE 1, IKE 2단계 옵션 구성

정책	IKE 1	IKE 2
인증 방식	Pre-Shared Key	
IPSec Protocol		AH, ESP
암호화 방식	AES192, AES256, DES, 3DES	AES192, AES256, DES, 3DES
키 교환 방식	Diffie-Hellman Group(1,2,5)	Diffie-Hellman Group(1,2,5)
무결성 확인 방식	MD5, SHA1	MD5, SHA1
인증 수명 시간	900~28,800초	900~28,800초

- Service Gateway

서비스 게이트웨이를 이용하면 플로팅 IP를 사용해 트래픽이 인터넷을 경유하지 않고 VPC 외부에 위치한 NHN Cloud의 서비스를 이용할 수 있습니다. 서비스 게이트웨이 생성 시 선택된 서비스와 자동으로 할당된 IP는 1:1 연결 관계를 유지하며, VPC에서는 서비스 게이트웨이의 IP를 이용하여 인터넷을 경유하지 않고 NHN Cloud의 내부 네트워크 통신만으로 보안성을 강화하면서 선택한 서비스를 안전하게 이용할 수 있습니다. 현재 제공되는 서비스는 Server Security Check, IaaS API Identify, CloudTrail, Object Storage, NHN Container Registry(NCR)이며 점차 확대해 나갈 예정입니다.

- Direct Connect

다이렉트 커넥트 서비스는 NHN Cloud의 IaaS 자원과 외부 네트워크(예: 고객사 온프레미스) 구간을 통신사에서 제공하는 전용 회선으로 연결하기 위한 서비스입니다. 이중화 및 독립적 데이터 센터로 고객이 선호하는 통신사 전용 회선 인입이 가능하며, 연결 방식은 전용 연결(전용 회선 사업자)과 호스팅 연결(파트너의 네트워크 환경 이용)을 제공합니다. 외부 간섭 없이 보다 안전한 내부 연결이 필요한 상황에서 사용합니다.

- Colocation Gateway

NHN Cloud와 온프레미스 환경의 네트워크를 하이브리드로 연결할 수 있습니다. 하이브리드 서비스를 이용하는 경우 NHN Cloud Zone이 제공되며, 코로케이션 게이트웨이를 이용하여 구성된 VPC에 NHN Cloud Zone을 연결하여 서비스를 이용할 수 있습니다.

- DNS Plus

DNS Plus는 전 세계 이용자들이 안정적이고 빠르게 접속할 수 있는 DNS 서비스입니다. 애니캐스트 네트워크를 지원해 국내외 어디서든 안정적이고 빠르게 DNS에 접속할 수 있으며, 별도의 DNS 솔루션이나 서버 없이 웹 콘솔에서 바로 DNS 서비스를 할 수 있습니다. 또한 대규모 DNS 질의를 받을 수 있도록 설계되었기 때문에, 대규모 DNS 질의 처리와 DNS를 대상으로 한 DDoS 공격도 대비할 수 있습니다.

GSLB(global server load balancing)는 DNS 서비스 기반으로 엔드 포인트에 안정적으로 트래픽을 로드 밸런싱해 주는 서비스로 Failover, Random, Geolocation의 다양한 라우팅 규칙을 제공합니다.

- Traffic Mirroring

트래픽 미러링은 VPC의 네트워크 패킷을 캡처하여 콘텐츠 보안, 위협 분석, 트러블 슈팅 등의 목적을 가진 애플리케이션(인스턴스)으로 전송할 수 있는 서비스입니다. 미러 소스와 대상을 미러 세션 단위로 연결할 수 있습니다. 미러링할 패킷의 방향은 인바운드, 아웃바운드 모두 설정할 수 있으며, 필터 설정을 통한 특정 네트워크 패킷을 미러링 할 수 있습니다. 필터는 프로토콜(TCP/UDP/ICMP), IP, Port를 적용할 수 있으며 필터가 적용되지 않는 경우는 기본 Drop 정책이 적용됩니다.

7.1.5 데이터베이스

NHN Cloud의 데이터베이스는 이용자가 복잡한 설치 및 설정 없이 손쉽게 구성할 수 있습니다. 인스턴스 유형은 DBMS 설치 과정에 대한 고민 없이 간단하게 인스턴스 생성으로 데이터베이스를 사용할 수 있으며, RDS for Database는 복잡한 설치 및 설정 과정 없이 NHN Cloud 환경에서 관계형 데이터베이스를 사용할 수 있습니다. 해당 서비스 이용으로 백업 및 복원, 파라미터 그룹, DB 보안 그룹, 모니터링을 포함해 고가용성의 데이터베이스를 사용할 수 있으며, 보안 취약점 및 버그가 발생하면 개선된 소프트웨어를 통해 보안성이 강화된 안정적인 서비스를 제공합니다.

1. 테넌트 분리

- RDS용 데이터베이스는 가상화 기술을 사용해 이용자와 NHN Cloud의 테넌트를 분리하고 서로 격리되어 있습니다. 동일 클라우드 타입의 NHN Cloud 내부 계정과 이용자의 프로젝트와 1:1 매핑으로 연결되어 있고, 이용자는 서로 연결이 불가능합니다.

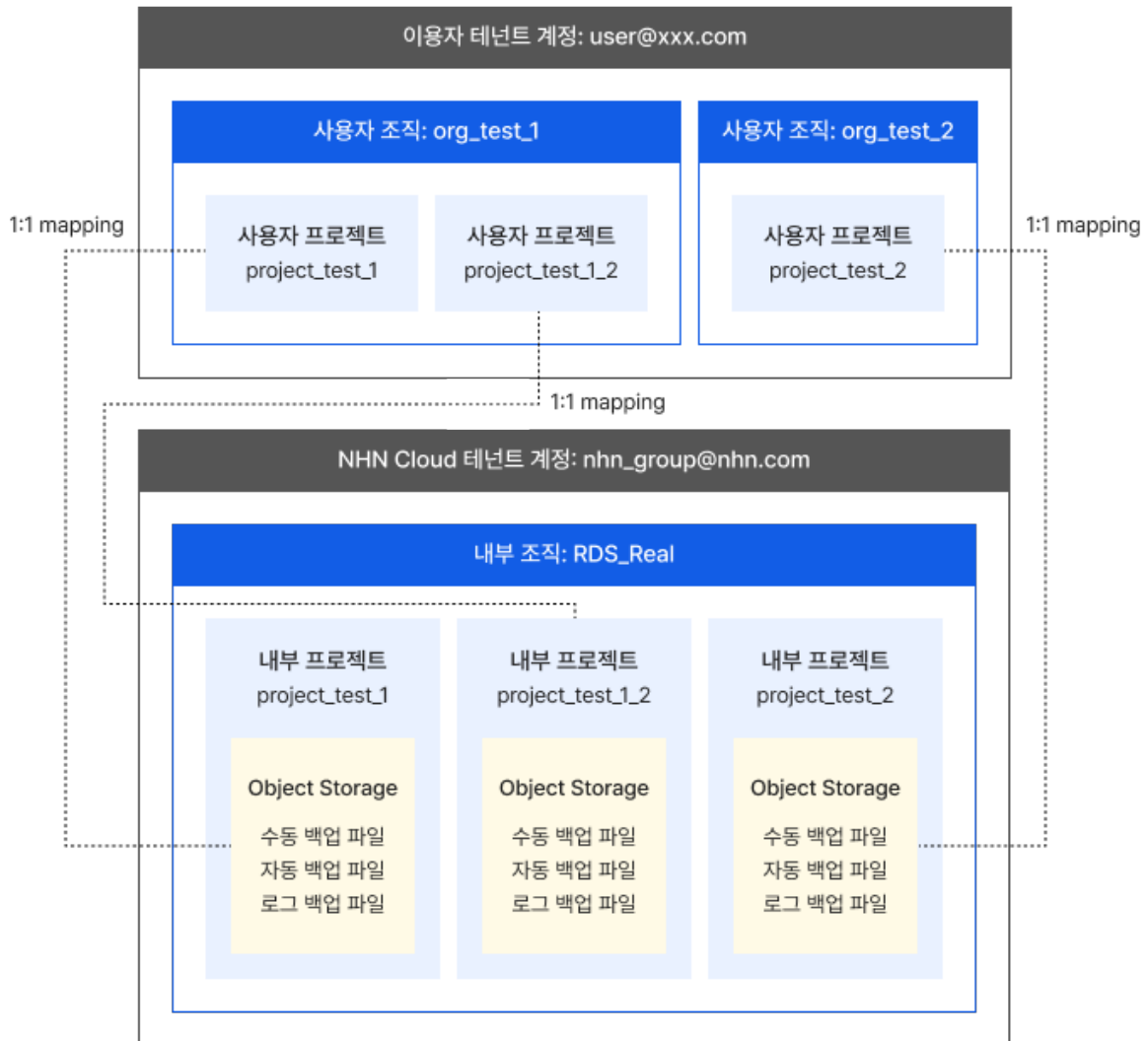


그림 7-18 RDS 프로젝트 연결 관계

2. 고가용성

- 고가용성은 예측할 수 없는 장애 상황에서 데이터베이스 중단으로 인한 서비스 장애 상황을 최소화하기 위한 기능입니다. 고가용성 기능을 사용하기 위해서는 마스터(master) DB 인스턴스와 다른 가용성 영역(availability zone)에 예비 마스터(candidate master)를 준비합니다. 마스터와 예비 마스터는 복제 관계를 맺고 있으며, 현재 사용 중인 마스터 DB 인스턴스 또는 가용성 영역에 문제가 발생할 경우 예비 마스터가 새로운 마스터의 역할을 수행하여 서비스 가용성을 최대한 유지할 수 있습니다.

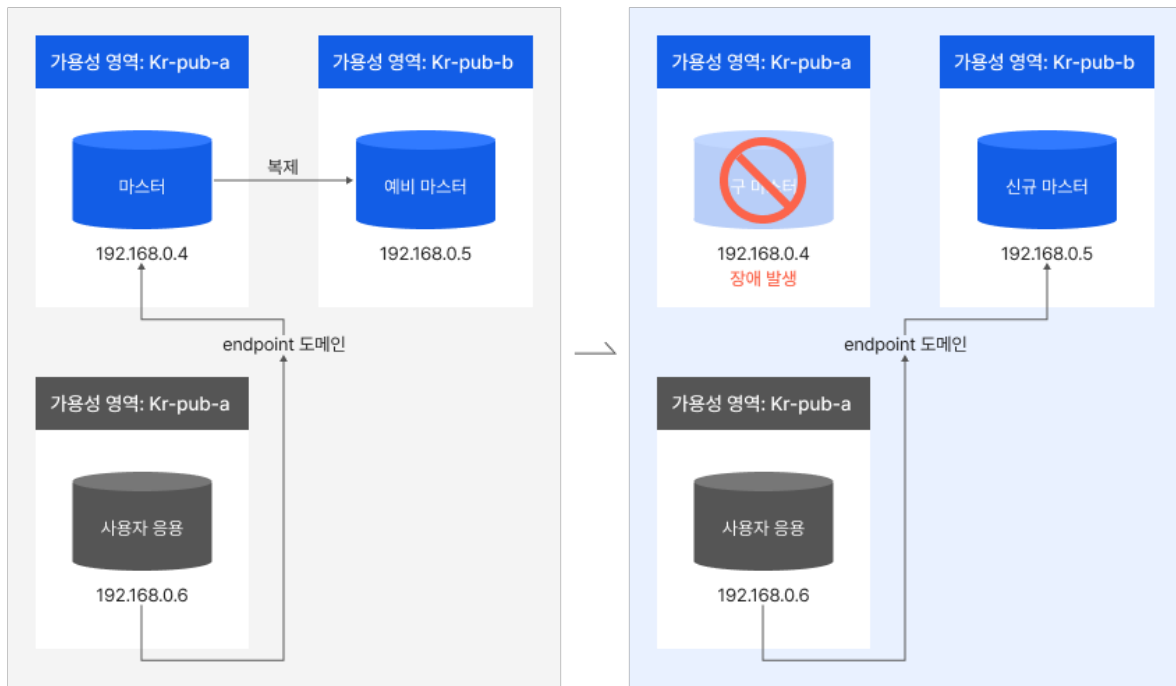


그림 7-19 RDS Failover

3. 접근 제어

- 데이터베이스 이용자 계정

RDS 인스턴스는 초기 데이터베이스 기본 계정을 제공하지 않고 콘솔에서 DB 인스턴스 생성 시 계정을 만들고 Read, CRUD, DDL 권한을 부여할 수 있습니다.

- 이용자 접근 제어(RDS for MySQL, RDS for MariaDB)

DB 인스턴스에 접근 가능한 이용자를 CIDR 형식으로 송수신을 제어할 수 있으며, 등록되지 않은 IP 접속이 불가능합니다.

이용자 접근 제어

방향	원격	동작
수신	0.0.0.0/0	삭제
수신	10.10.10.10/32	삭제
수신 ▼	<input type="text" value="10.10.10.10/32"/>	추가

! CIDR 형식에 맞게 입력해 주세요.

그림 7-20 RDS 이용자 접근 제어

- 보안 그룹(RDS for MS-SQL)

DB 보안 그룹은 DB 인스턴스를 다른 트래픽으로부터 보호할 목적으로 사용합니다. 지정한 트래픽은 허용하고 나머지 트래픽은 차단하는 포지티브 시큐리티 모델(positive security model)을 사용합니다. 플로팅 IP를 할당하더라도 바로 접속할 수 없으며, 필요한 정책을 설정해야만 접속할 수 있습니다. 이는 외부 접근과 사실 IP를 사용한 내부 접근 모두 동일하게 적용됩니다.

DB 보안 그룹 생성

이름

DB 운영자 정책

설명

운영자 접근 정책

보안 정책 추가

방향	Ether 타입	포트 범위	원격	설명	
수신 ▼	IPv4 ▼	DB 포트 ▼	192.168.10.10/32	mgt	-
수신 ▼	IPv4 ▼	포트 ▼ 22	192.168.10.10/32	mgt	-

+

• 보안 정책은 DB 보안 그룹이 할당된 인스턴스에 어떤 트래픽을 허용할지 정의합니다.

그림 7-21 DB 보안 그룹

4. 백업 및 복구

- 백업 및 복구

데이터 무결성과 안정성을 보장하기 위해 데이터베이스 백업 및 복구 기능을 제공하며 데이터 백업과 로그 백업을 제공합니다. 생성된 백업 파일은 이용자의 Object Storage로 업로드하여 보관할 수 있으며, 백업 파일을 이용해 백업된 순간으로 복원을 하거나, 특정 시점을 선택해 복원할 수 있습니다.

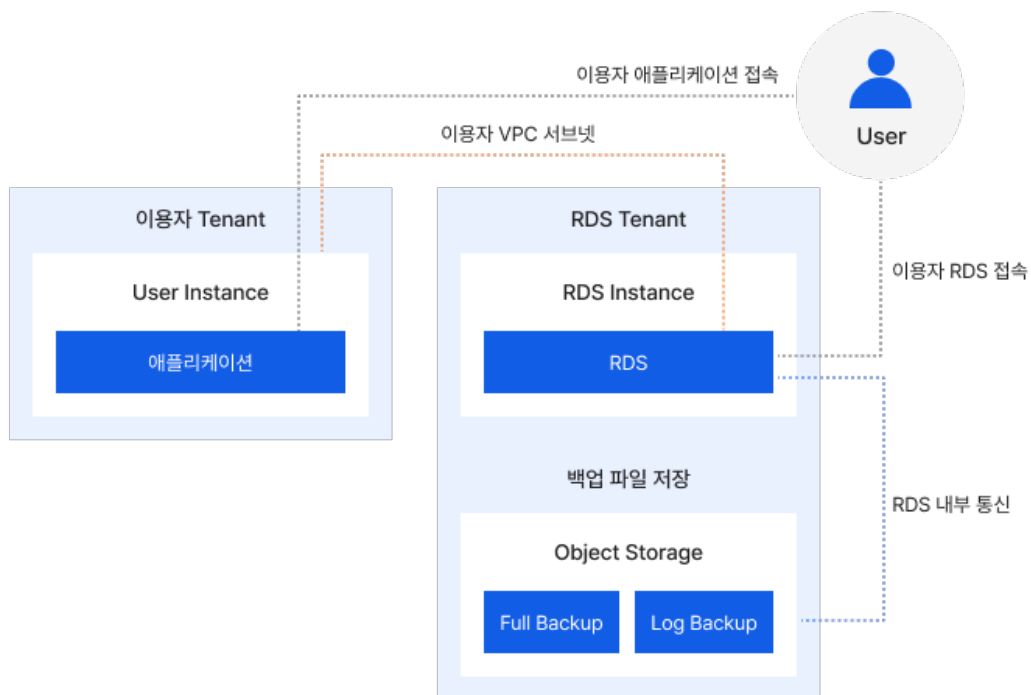


그림 7-22 RDS 백업 및 복구

8 NHN Cloud 보안 서비스

8.1 클라우드 보안 서비스

NHN Cloud는 클라우드 컴퓨팅 서비스의 플랫폼을 보호하기 위해 시스템 보호 조치와 외부 공격에 대한 모니터링을 수행하고 있습니다. 또한 이용자의 가상화 인프라 및 서비스를 보호하기 위한 시스템, 네트워크, 애플리케이션 보호 조치 및 산업별 컴플라이언스 요건 충족을 위한 다양한 보안 서비스를 제공하고 있습니다. 그 외에도 마켓플레이스 파트너의 다양한 보안 상품을 통해 추가적인 보호 조치를 수행하여 안전한 클라우드 서비스 환경을 구성할 수 있습니다.

8.1.1 취약점 점검

1. Server Security Check

- 신규 또는 운영 중인 시스템의 주요 보안 설정을 점검하고 조치해 시스템 안전성을 확보하고 잠재적 취약점을 제거할 수 있는 서비스입니다. 에이전트를 이용한 점검이며, 에이전트 설치 및 실행은 콘솔 화면에서 제공되는 스크립트를 이용해 간편하게 복사한 뒤 인스턴스 접속하여 실행하면 됩니다.
- 주요정보통신기반시설, 전자금융기반시설 보안 기준을 바탕으로 점검 항목을 분류하여 점검을 수행합니다.
- Service Gateway 서비스와 연동하여 플로팅 IP를 사용하지 않고 NHN Cloud 내부 네트워크를 통한 점검과 결과를 확인할 수 있습니다.

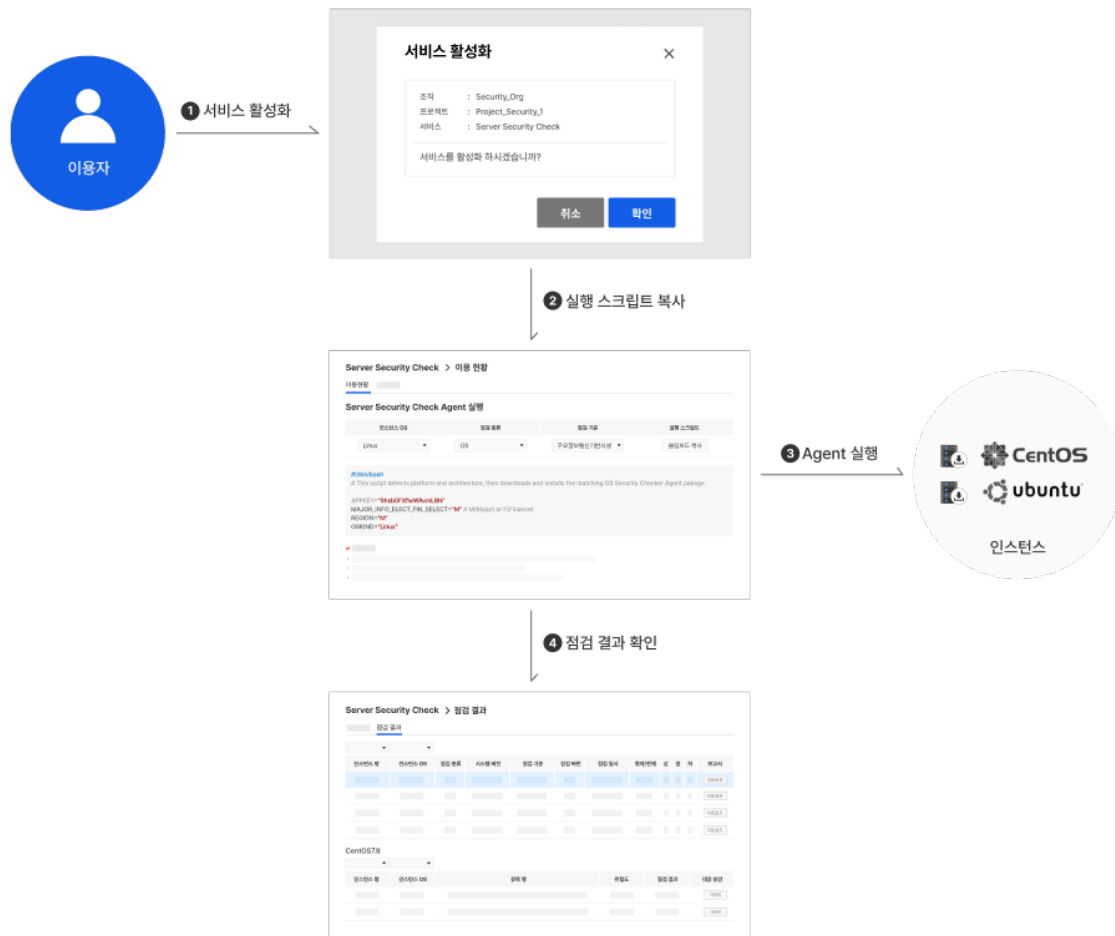


그림 8-1 Server Security Check 서비스 절차

2. APP Security Check

- 수년간 축적된 실무 경험과 전문 기술을 바탕으로 신규 또는 운영 중인 웹 애플리케이션 및 모바일 앱의 보안 취약점을 수동 및 자동으로 점검하고 발견된 취약점에 대한 대응 방법을 제공합니다. 웹, 모바일, 게임 서비스 등 사전 질의서(샘플 제공)를 통해 서비스 특성을 고려한 점검을 수행합니다.

8.1.2 네트워크 보안

1. Basic Security

- 한국 리전을 이용하는 모든 고객에게 제공하는 무료 보안 서비스로 심각한 보안 침해 사고가 발생하면 식별된 취약점을 고객에게 통보하여 즉각 조치할 수 있도록 지원하고 있습니다. 또한 자체 수집한 보안 취약점 및 범용 애플리케이션의 주요 보안 취약점과 조치 방안을 공지해 보안 사고를 예방할 수 있도록 합니다.

2. Security Monitoring

- NHN Cloud는 수년간 축적되고 검증된 IDS(intrusion detection system)/SIEM(security information and event management) 패턴 및 위협 대응 체계를 바탕으로 클라우드 플랫폼 및 고객의 서비스를 보호하기 위해 보안 전문 인력이 24시간 365일 실시간으로 침입 시도에 대한 보안 관제 서비스를 제공합니다.
- 침입 탐지
24시간 365일 실시간 고도화된 IDS/SIEM 연관성 탐지 패턴을 적용해 침입 시도에 대한 모니터링을 수행합니다.
- 침입 분석
이벤트(raw data)와 패킷 덤프 데이터를 자체 보안 관제 방법론으로 위협의 정/오탐 확인과 영향도 분석을 수행해 공격 정보를 제공함으로써 고객이 서비스 이상에 대한 의사 결정을 할 수 있도록 합니다.
- 침입 대응
식별된 취약점에 대한 정보를 제공하고 침해 사고 발생 시 사고 분석 지원을 통해 침해 경로, 취약점 정보, 취약점 조치 방안 및 재발 방지 방안을 제공해 추가적인 위험이 발생하지 않도록 지원합니다.
- 침입 예방
보안 동향을 지속적으로 확인해 신규 위협에 대한 탐지 패턴 제작 및 내부 적용한 패턴 최적화를 통해 지속적인 위협 관리를 수행합니다.
- 정보 제공
실시간 탐지 이벤트의 상세 현황과 보안 관제 워크플로우 시스템을 이용해 클라우드 콘솔에서 관제 업무 현황을 확인할 수 있습니다.

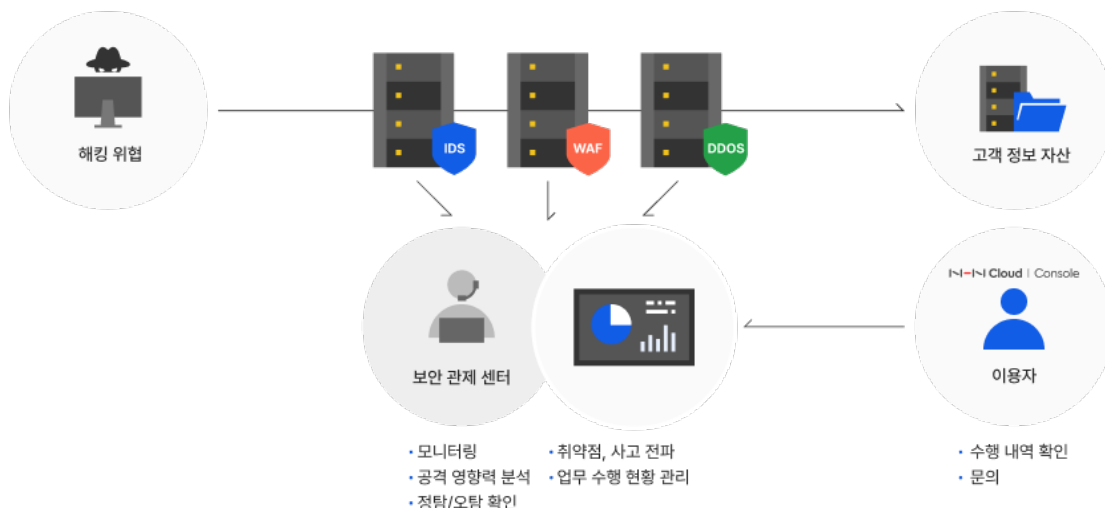


그림 8-2 Security Monitoring 서비스

3. DDoS Guard

- 외부 DoS/DDoS 공격을 실시간으로 탐지하고 차단해 고객의 서비스를 보호하는 서비스로 2개 유형을 제공합니다.

- Basic

일반적인 네트워크 레벨의 DoS/DDoS 공격으로부터 클라우드의 서비스를 보호하며, NHN Cloud의 모든 고객에게 무료로 제공되는 서비스입니다.

- Managed

고객 맞춤형 구독 서비스로 보다 향상된 보호 기능을 제공합니다. 서비스 특성에 따라 트래픽을 학습하고 임계치를 수정하며, 정교한 정책 관리와 유효성 검증을 통해 애플리케이션 형태의 DDoS 공격에 대응합니다. 또한 보안 관제팀의 24시간 365일 모니터링과 상황 전파를 통해 DDoS 공격을 빠르게 파악하고 대응합니다.

4. WEB Firewall

- 웹 서비스의 증가와 함께 공격의 형태가 다양해지고 지능화되면서 SQL Injection, Cross-Site Scripting(XSS) 등과 같은 웹 애플리케이션에 특화된 공격을 탐지하고 차단하는 서비스로 Self 서비스와 Managed 서비스의 두 가지 유형을 제공하며, 고객 클라우드 영역에 웹 방화벽을 구성하여 독립적인 운영 환경과 보안성을 보장합니다.
- OWASP Top 10, 국정원 8대 취약점에 대응해 다양한 유형의 위협을 대응하고, GS 인증, PCI-DSS 인증, CC 인증을 획득하였습니다.
- 로드 밸런서 서비스 또는 웹 방화벽 자체 기능으로 HTTPS 복호화 후 트래픽을 분석할 수 있으며, 별도의 로드 밸런서가 없어 도 웹 방화벽 자체 L7 기반 부하 분산 모드로 서비스를 구성할 수 있습니다.

- Self 서비스

고객이 직접 웹 방화벽을 구축하고 운영할 수 있도록 웹 방화벽 이미지 및 운영 가이드를 제공합니다.

- Managed 서비스

전문 엔지니어의 컨설팅을 통한 웹 방화벽 설치와 트래픽 분석을 통한 정책 최적화 및 운영 대행 서비스를 제공하며, 24시간 365일 보안 관제 서비스를 통해 보안 사고 발생 시 신속하게 대응할 수 있습니다.

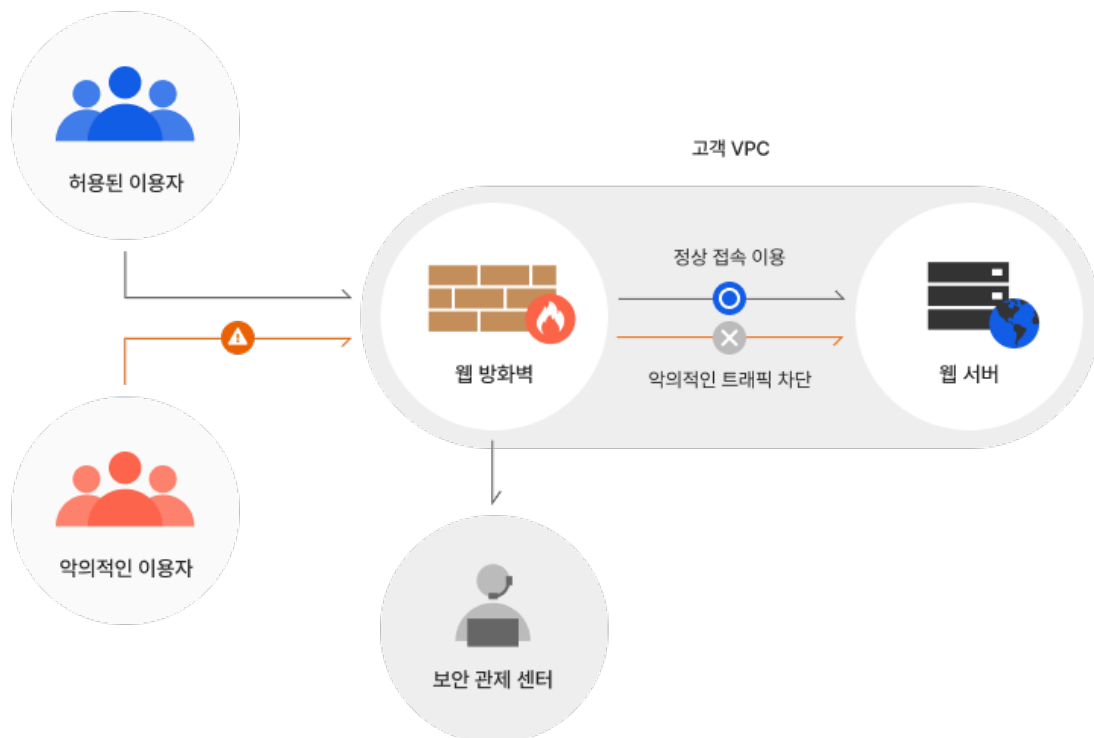


그림 8-3 WEB Firewall 공격 차단

8.1.3 시스템 보안

1. Vaccine

- 컴퓨터의 바이러스, 스파이웨어, 애드웨어 등의 악성 코드를 탐지하고 방어하기 위한 소프트웨어로 이용자의 시스템을 안전하게 보호합니다. 이용자는 백신 매니저와 에이전트를 별도 구매 없이 Vaccine 서비스를 이용함으로써 백신 사용 시 필요한 관리 서버 운영, 정책 설정 등의 업무 부담을 덜어줍니다. 또한 악성 코드 탐지 현황을 클라우드 콘솔과 이메일을 통해 확인할 수 있습니다.

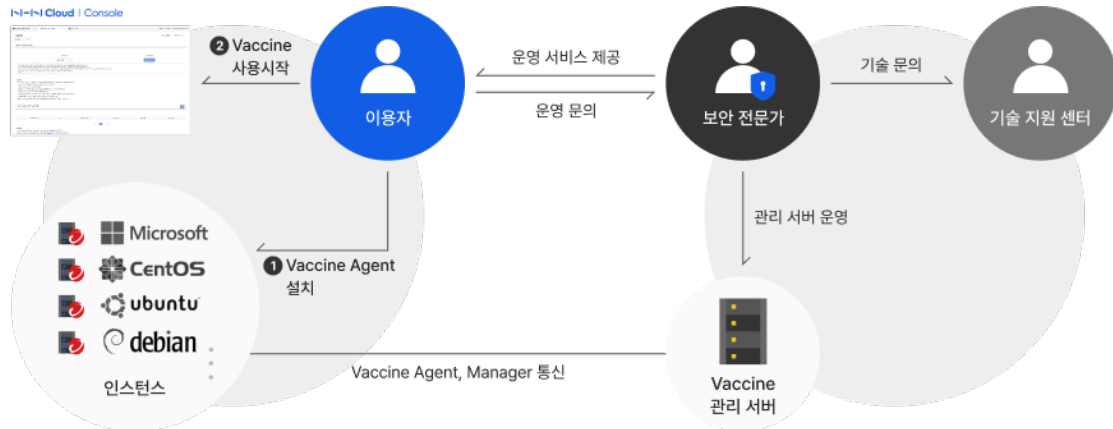


그림 8-4 Vaccine 서비스 구성

2. Webshell Threat Detector

- 웹 셸(web shell)은 해커가 악의적인 목적으로 웹 서버에서 임의의 명령어를 수행하게 하는 프로그램으로서 개인정보 및 주요 정보 유출, 소스 코드 열람, 홈페이지 위변조 및 악성 코드 유포지로 악용하는 등 치명적인 공격이 가능한 해킹 도구입니다. 해킹 당한 웹 서버의 80~90%에서 웹 셸의 흔적이 발견되는 만큼 웹 서버 보안을 위해 웹 셸에 대한 빠른 탐지와 대응을 통해 보안을 강화해야 합니다.
- Webshell Threat Detector는 파일(웹 셸 코드에서 식별 가능한 패턴 탐지)과 행위(프로세스 호출 행위에 대한 탐지)를 점검하고, 의심 행위 발생 시 실시간으로 탐지하고 설정된 이메일 주소로 알림을 전송해 서버에 접속하지 않고도 클라우드 콘솔 화면에서 탐지 결과를 확인 후 대응할 수 있습니다.

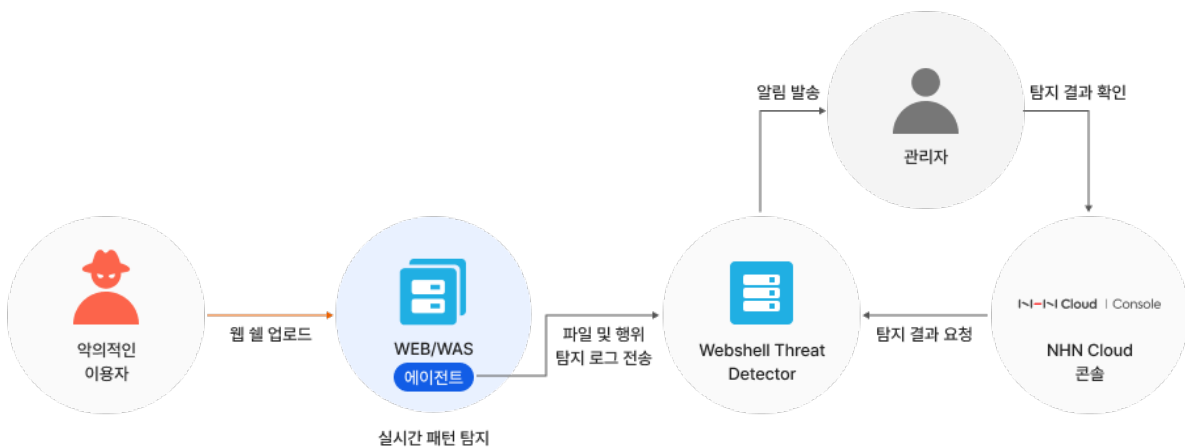


그림 8-5 Webshell Threat Detector 동작 방식

3. NHN AppGuard

- NHN AppGuard는 Android와 iOS 모바일 앱을 다양한 보안 위협으로부터 안전한 실행 환경을 유지하도록 도와주는 모바일 앱 보호 서비스입니다. 악의적인 공격을 통해 서비스에 영향을 줄 수 있는 상황에서 소스 코드 보호, 메모리 변조 및 후킹, 해킹 툴 차단, 안티 디버깅, 위변조 방지 등의 다양한 기능으로 보호하여 안정적인 서비스를 제공할 수 있도록 합니다.
- NHN AppGuard의 SDK를 통해 앱에 코드 연동(선택 사항) 후, 콘솔 또는 CLI(command line interface)를 이용해 앱 보호(필수 사항) 작업을 완료하고 배포합니다.

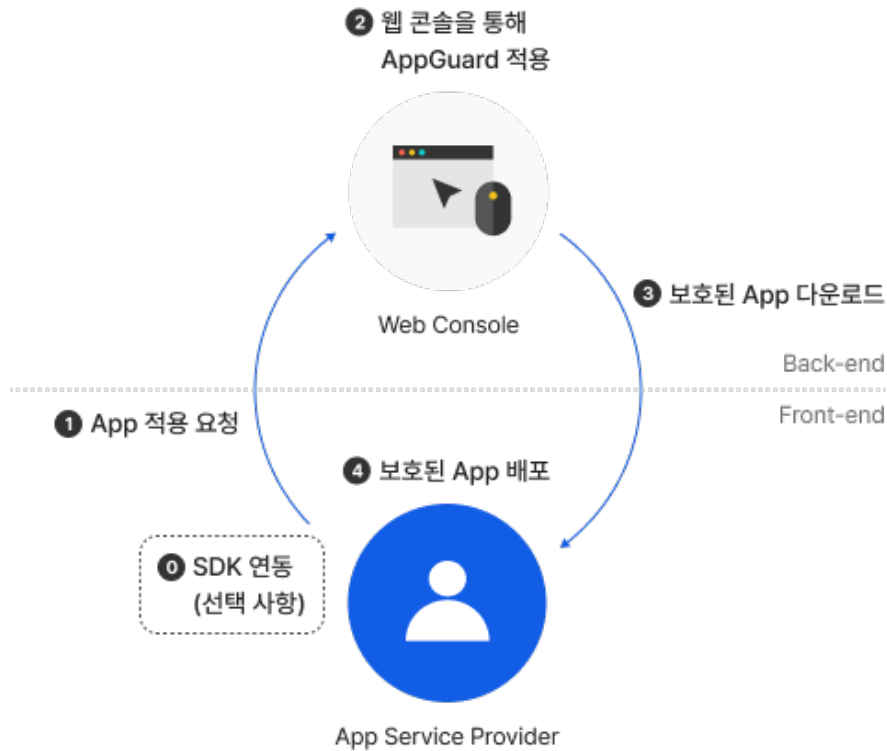


그림 8-6 NHN AppGuard 적용 절차

- NHN AppGuard Engine은 어뷰징을 탐지해 차단하거나 제재할 수 있는 로그를 서버로 전송합니다. 보안 관리자는 NHN Cloud의 콘솔을 이용해 탐지 로그를 확인할 수 있으며, 차단 조건 설정을 통해 안전한 서비스를 운영할 수 있습니다.

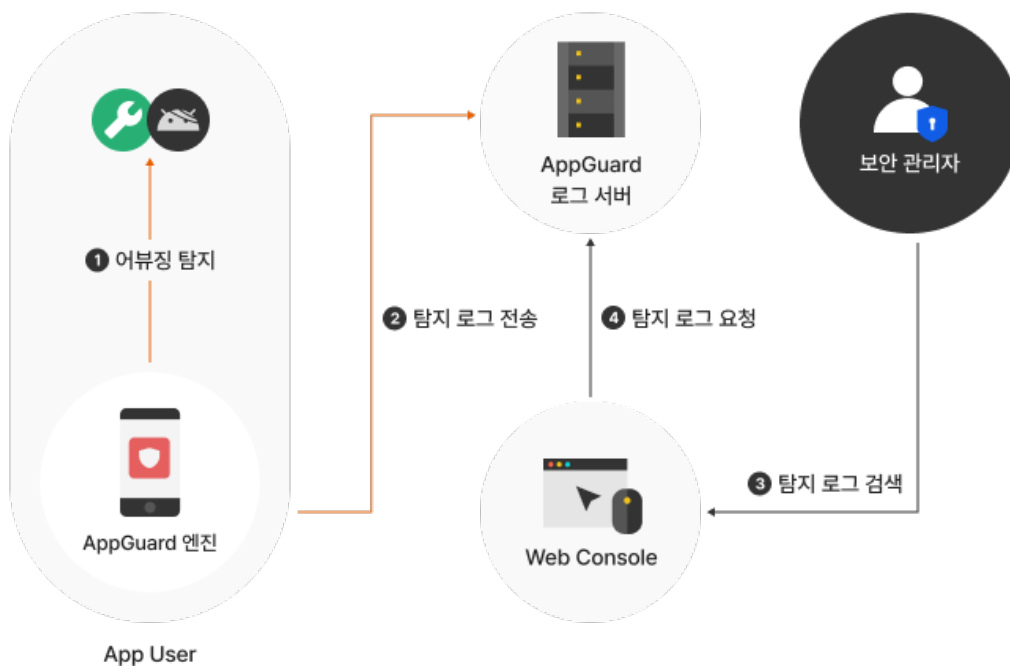


그림 8-7 NHN AppGuard 운영

8.1.4 보안 관리

1. SIEM

- SIEM(security information and event management)는 보안 정보 관리(security information management, SIM)와 통합 보안 관리(enterprise security management)를 결합하여 실시간 모니터링과 이벤트 분석 기능을 제공할 뿐 아니라, 규정 준수 및 감사 목적으로 보안 데이터를 저장 및 분석할 수 있는 솔루션입니다.
- 보안 솔루션 및 CloudTrail 이벤트를 수집해 이벤트에 대한 종합적인 연관 분석으로 신속하게 보안 위협을 식별할 수 있으며 관련 정보는 클라우드 콘솔을 통해 확인할 수 있습니다.

2. Security Compliance

- NHN Cloud가 보유한 정보보호 인증과 컴플라이언스에 효과적으로 대응할 수 있도록 인증 범위, 유효 기간을 포함한 보안 인증서와 정보보호 통제 항목에 대한 상세 내용과 준수 방안을 제공하는 서비스입니다.

3. Certificate Manager

- 서비스를 운영하면서 잊고 지내다 놓치기 쉬운 만료일이 존재하는 TLS 인증서, 도메인, 사용자 데이터(예: 라이선스)를 관리 해줌으로써 알림 발송 규칙과 등록된 이용자에게 만료 예정 알림(SMS/이메일)을 발송하는 서비스입니다.

8.1.5 암호 및 인증

1. Secure Key Manager

- Secure Key Manager는 이용자의 중요 데이터를 안전하게 보관하고 접근 권한을 제어하는 서비스입니다. 이용자는 Secure Key Manager를 이용해 기밀 데이터, 대칭 키, 비대칭 키를 저장할 수 있고, 저장한 데이터는 접근 제어를 통해 이용자가 설정한 인증 방법을 통과한 클라이언트만 접근할 수 있습니다. 또한 정보보호 및 개인정보보호 관리체계(ISMS-P) 2.7.2 암호 키 관리와 클라우드 보안인증제도(iaaS) 평가 기준 12.3.2 암호 키 관리 요구 사항(암호 키 생성 후 암호 키는 별도의 안전한 장소에 소산 보관하고, 암호 키 사용에 관한 접근 권한 부여를 최소화하고 있는가)을 만족해 인증 심사 대응으로 사용할 수 있습니다.

• 접근 제어

Secure Key Manager는 이용자의 데이터를 보호하기 위한 다양한 인증 방법을 제공하며, 인증을 통과한 클라이언트만 Secure Key Manager에 저장한 데이터를 사용할 수 있습니다. 인증 방법은 IPv4 주소를 확인하는 'IPv4 주소 인증', 클라이언트의 MAC 주소를 확인하는 'MAC 주소 인증', 클라이언트가 통신에 사용하는 인증서를 확인하는 '클라이언트 인증서 인증'으로 구분합니다. 이용자는 최소 한 개 이상의 인증 방법을 선택해야 하며, 두 개 이상을 선택한 경우 클라이언트는 모든 인증을 통과해야 합니다.



그림 8-8 Secure Key Manager 데이터 접근 제어

- 승인 기능

국내 ·외 보안 인증 심사(ISMS-P, ISO 등)에서 요구하는 안전한 암호화 키 관리 요구 사항을 충족하기 위해 조직 거버넌스 설정의 승인 프로세스 관리 설정을 이용해 키 생성, 수정, 삭제 및 접근 통제에 대한 책임자의 승인 절차를 추가할 수 있습니다.

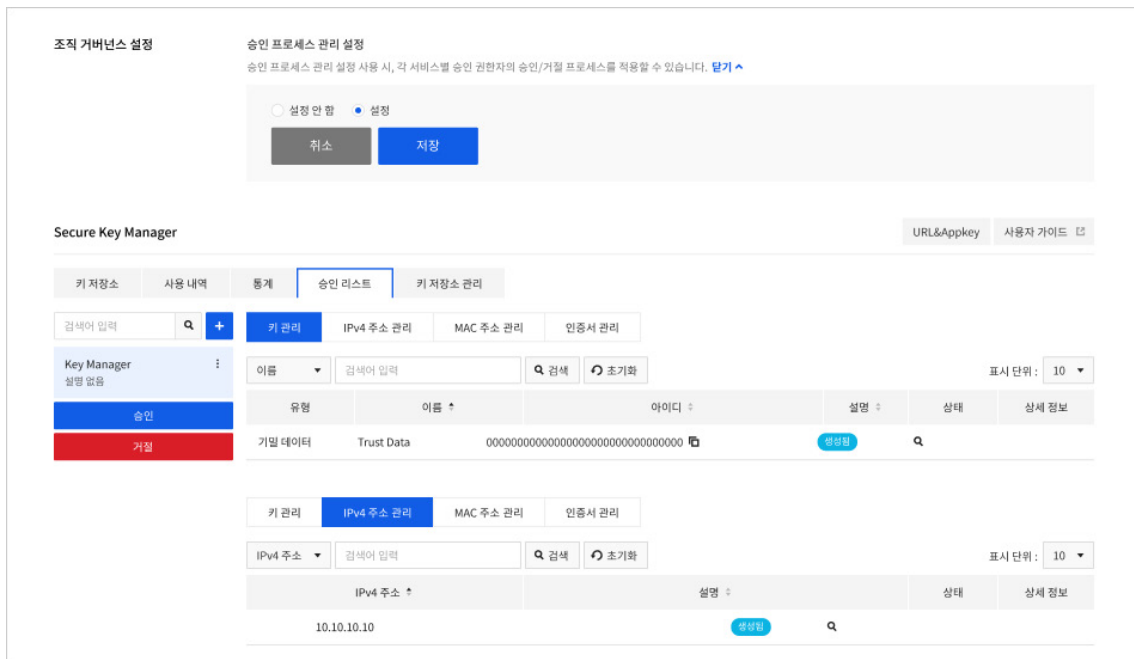


그림 8-9 Secure Key Manager 승인 설정

- 키 버전 관리

보안을 위해 데이터 암호 키의 생명 주기 관리가 필요합니다. 다양한 보안 위협에 대비하기 위해 사용 기한을 정하고 만료되기 전 새로운 키로 갱신하는 것이 좋습니다. Secure Key Manager에서 암호/복호화에 이용되는 실제 키 값은 버전을 기준으로 구분되며, 키 회전을 통해 새로운 버전의 키를 생성할 수 있습니다.

대칭 키와 비대칭 키는 키 회전 기능을 이용해 키 버전을 관리할 수 있으며, 최초 생성된 키의 버전은 0이며 이후 회전할 때마다 1씩 증가하면서 버전이 생성됩니다. 삭제된 키는 버전에서 제외됩니다.

키 회전 주기는 최소 30일 이상을 입력해야 하며 정해진 회전 주기에 따라 수행하는 자동 회전과 이용자가 필요에 의해 수동으로 즉시 회전하는 수동 회전이 있습니다. 수동 회전을 하더라도 회전 주기에 등록된 스케줄(다음 회전일)에는 영향을 주지 않습니다.

키 상세 정보

유형

대칭키

아이디

00000000000000000000000000000000

이름

Key Rotation

설명

Rotation

회전 주기(일)

30

다음 회전일 : 2023-04-21 (UTC +09)

즉시 회전 ?

상태

사용 중

삭제 요청 ?

마지막 사용 일시

-

키 버전 목록	버전	상태	삭제 요청 ?
	6	사용 중	삭제할 수 없음
	5	사용 중	삭제 요청
	3	사용 중	삭제 요청

이력

생성

2023-03-22 09:42:14 (UTC+09) (so*****@nhn.com)

수정

2023-03-22 11:44:10 (UTC+09) (so*****@nhn.com)

취소

수정

그림 8-10 키 회전 및 버전 관리

• 서비스 구조

Secure Key Manager는 이용자 데이터를 안전하게 보관하기 위해 루트 키와 시스템 키 두 개의 암호 키를 내부적으로 사용합니다. 루트 키는 시스템 키를 보호하기 위해 사용하며 시스템 키는 이용자 데이터를 보호하기 위해 사용합니다. 시스템 키는 루트 키로 암호화해서 Secure Key Manager 시스템 키 관리 서버에 저장합니다. Secure Key Manager 서버는 서비스를 시작할 때 인증 과정을 거쳐 Secure Key Manager 시스템 키 관리 서버로부터 암호화된 시스템 키를 가져옵니다. 루트 키를 사용해 보호하면 시스템 키 처리 모듈이 시스템 키를 사용할 수 있는 상태가 됩니다. Secure Key Manager에 저장한 사용자 데이터를 비정상적인 방법으로 접근하려면 물리적으로 분리된 세 개의 시스템에서 루트 키, 시스템 키, 사용자 데이터를 모두 획득해야 합니다.

이용자는 NHN Cloud 웹 콘솔에서 Secure Key Manager를 관리할 수 있습니다. 웹 콘솔은 이용자 데이터 생성/관리, 클라이언트 인증 데이터 생성/관리 등의 기능을 제공합니다. Secure Key Manager에서 생성한 모든 이용자 데이터는 시스템 키로 암호화해서 이용자 데이터 저장소에 저장합니다. 클라이언트 인증 데이터는 일부 중요 정보를 시스템 키로 암호화해서 클라이언트 인증 데이터 저장소에 저장합니다.

Secure Key Manager는 클라이언트 서버에서 사용할 수 있는 다양한 API를 제공합니다. 클라이언트 서버는 기밀 데이터 조회, 대칭 키를 사용한 암호/복호화, 비대칭 키를 사용한 서명/검증을 요청할 수 있습니다. 클라이언트 인증 모듈은 클라이언트 인증 데이터를 사용해서 클라이언트의 요청을 허가할지 결정합니다. 클라이언트의 요청이 허가되면 사용자 데이터 처리 모듈은 시스템 키 처리 모듈을 사용해서 암호화된 사용자 데이터를 복호화한 후 서비스를 제공합니다.



엔에이치엔클라우드

13487 경기도 성남시 분당구 대왕판교로645번길 16 NHN 플레이뮤지엄

고객 센터: 1588-7967 | 이메일: support@nhncloud.com

©NHN Cloud Corp. All rights reserved.