NHN Cloud 공공기관을 위한 클라우드 보안 가이드

NHN Cloud's
Cloud Security Guide
for Public Institutions



NHN CLOUD

NHN Cloud 공공기관을 위한 클라우드 보안 가이드

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	2025. 12.	NHN Cloud 공공기관을 위한 클라우드 보안 가이드 1.0 버전 출시

목차

NHN Cloud 공공기관을 위한 클라우드 보안 가이드 ····· 2

저작권 ····· 2

문서 이력 ····· 2

1 개요 ····· 7

1.1 가이드 소개 ····· 7

2 보안 위협 ····· 8

2.1 보안 위협이란 ····· 8

2.2 보안 대응 방안 ····· 9

3 컴플라이언스 ····· 10

3.1 컴플라이언스란 ····· 10

3.2 공공 부문 컴플라이언스 ····· 11

3.2.1 법률과 지침, 가이드 ····· 11

3.2.2 클라우드 및 정보보호 관련 인증 제도 ····· 12

3.2.3 NHN Cloud의 인증 현황 ····· 14

4 민간 클라우드 도입을 위한 고려 사항 ····· 15

4.1 보안 책임 공유 모델(SSRM)의 이해 ····· 15
4.2 공공기관의 클라우드 도입 전 고려 사항 ····· 16
4.2.1 민간 클라우드 영역 선택 고려 사항 ····· 16
4.2.2 민간 클라우드 도입 시 망별 보안 요구 사항 ····· 18
4.2.3 민간 클라우드 도입 시 고려할 기술적 보안 요구 사항 ····· 19
4.2.4 공공기관 보안 솔루션 도입 시 고려 요건 ····· 22

5 보안 인프라 구성 방안 ····· 25

5.1 NHN Cloud 영역 선택 및 망 분리 ····· 25
5.1.1 NHN Cloud 영역 선택 ····· 25
5.1.2 망 분리 및 망 간 연계 ····· 26
5.2 클라우드 콘솔 보안 ····· 27
5.2.1 콘솔 접근제어 ····· 27
5.2.2 콘솔 계정 관리 ····· 29
5.2.3 클라우드 콘솔 로깅 ····· 32
5.3 네트워크 보안 ····· 33
5.3.1 네트워크 접근제어 ····· 33
5.3.2 가상 사설망 연결(구간 보안) ····· 35
5.3.3 DDoS 공격 대응 ····· 36
5.3.4 침입 탐지 및 차단 ····· 36
5.3.5 웹 서버 위협 방어 ····· 37
5.3.6 SSL 가시화 ····· 38

5.4 시스템 및 데이터 보안 ····· 39
5.4.1 서버 접근제어 및 계정 관리 ····· 39
5.4.2 DB 접근제어/계정 관리 ····· 40
5.4.3 스토리지 접근 관리 ····· 41
5.4.4 백신 ····· 43
5.4.5 암호화 ····· 44
5.4.6 취약점 관리 ····· 45
5.4.7 API 보안 ····· 46
5.5 관제, 모니터링 및 로그 관리 ····· 48
5.5.1 로그 관리 ····· 48
5.5.2 관제 및 모니터링 ····· 49
5.6 컨테이너 보안 ····· 51

6 국가 보안 기준 준수 방안 ····· 52

6.1 보안 기본 원칙 ····· 52
6.1.1 정책적 측면에서의 기본 원칙 ····· 52
6.1.2 기술적 측면에서의 기본 원칙 ····· 53
6.2 세부 보안 기준 ····· 54
6.2.1 정책 ····· 54
6.2.2 클라우드 인프라 ····· 55
6.2.3 가상 환경 보안 ····· 56
6.2.4 데이터 ····· 57
6.2.5 인증 및 권한 ····· 58
6.2.6 사고 및 장애 대응 ····· 59

7 별첨 ····· 61

7.1 법, 지침 등의 요구 사항 ····· 61

7.1.1 법 주요 요구 사항 ····· 61

7.1.2 국가정보보안기본지침 ····· 66

7.1.3 국가 클라우드 컴퓨팅 보안 가이드라인 4장 제2절 요약 ····· 68

7.1.4 컨테이너 보안(국가 클라우드 컴퓨팅 보안 가이드라인 부록 6) ····· 69

1 개요

1.1 가이드 소개

본 문서는 공공기관의 민간 클라우드 도입 시 고려해야 할 컴플라이언스 사항과 NHN Cloud 보안 구성 방법을 정리하여 안전하고 효율적인 클라우드 도입을 지원하는 것을 목적으로 합니다.
인증 제도 및 컴플라이언스 관련 내용은「국가 클라우드 컴퓨팅 보안 가이드라인」,「국가정보보안기본지침」과 관련 법령 등을 참고하여 발췌 및 정리하였습니다. 본 문서 작성 시점에 참고한 법령, 지침, 가이드는 향후 변경될 수 있으며, 일부는 유예 중이거나 확정되지 않은 사항일 수 있습니다.

본 문서는 공공기관이 NHN Cloud 도입 시 보안 구성을 위한 참고 가이드이며 더 많은 전문적인 내용은 **NHN Cloud 보안 센터**에서 제공하는 별도의 세부 가이드와 관련 문서를 참조하세요.

표 1-1 NHN Cloud 보안 센터에서 제공하는 보안 가이드

가이드명	설명
클라우드 보안 백서	NHN Cloud는 클라우드에 대한 이해를 돕고 안전하게 클라우드 보안 설계와 운영을 할 수 있도록 보안 백서를 제공하고 있습니다.
개인정보보호 준수 가이드	NHN Cloud는 개인정보 보호법을 준수하실 수 있도록 고객에게 다양한 상품 및 기능을 제공하고 있습니다.
콘솔 보안 가이드	NHN Cloud에서 제공하는 다양한 보안 기능을 이용하여 클라우드 환경에서 애플리케이션 및 서비스를 안전하게 구성할 수 있도록 권장되는 보안 설정에 대해 안내합니다.
네트워크 아키텍처 보안 가이드	NHN Cloud에서 제공하는 다양한 네트워크 기능과 네트워크 보안 서비스를 이용하여 클라우드 환경에서 가상 인프라 및 서비스를 안전하게 제공할 수 있는 네트워크 아키텍처 보안 방법에 대해 안내합니다.
컨테이너 보안 가이드	안전한 컨테이너 환경을 구축하는 데 필요한 구성 설계 및 보안 적용 방법을 안내합니다.
데이터 이전 보안 가이드	데이터 이전 과정에서 발생할 수 있는 보안 위험을 방지하고 안전하게 데이터를 옮기기 위한 내용을 안내합니다.
랜섬웨어 대응 가이드	조직의 데이터와 시스템을 안전하게 보호하기 위해 랜섬웨어 공격에 대비하고 효과적으로 대응할 수 있도록 체계적인 방안을 소개합니다.

2 보안 위협

2.1 보안 위협이란

공공기관은 민감한 데이터를 다루며, 이에 대한 위협은 점점 더 지능화되고 복잡해지고 있습니다. 특히 클라우드 전환 과정에서는 기존 레거시 환경에서 고려하지 않았던 새로운 보안 위협과 요구 사항이 등장합니다.

표 2-1 레거시 환경과 클라우드 환경의 보안 위협 비교

항목	레거시 환경의 보안 위협	클라우드 환경의 보안 위협
물리적 접근	내부자 위협, 물리적 침입	하이퍼바이저 공격, 데이터 센터 공유, 글로벌 리전
자산 관리	고정 인프라, 자산 파악 쉬움	탄력적 자산 증가로 가시성 저하
접근제어	관리자 중심의 비교적 단순한 권한 모델	다양한 형태의 가상 자산 접근제어, IAM 구성 오류
취약점 관리	OS/미들웨어 취약점 위주	컨테이너, 서버리스 등 신규 공격 대상 확대
운영 주체	단일 조직이 통제	클라우드 서비스 사업자(CSP)와 책임 공유

클라우드 특화 보안 위협

- 과도한 IAM 권한, 오픈된 포트, 잘못된 설정 등으로 인한 데이터 유출
- 계정 탈취 및 API 키, Access Token 유출 시 외부 공격자가 클라우드 리소스 조작 가능
- SaaS, 오픈소스 소프트웨어에 악성코드가 삽입될 경우 광범위한 피해 발생
- 클라우드 서비스의 API를 노린 공격으로 인증 우회, 데이터 조작 등의 위협이 존재
- 클라우드의 분리 정책 실패 시 다른 테넌트 간 데이터 접근 위협 존재

2.2 보안 대응 방안

제로 트러스트 기반 클라우드 보안 설계

기존의 '신뢰하고 검증한다'는 방식이 아니라, '절대 신뢰하지 않고 항상 검증한다(never trust, always verify)'는 방식인 제로 트러스트(zero trust) 모델은 클라우드 환경에 더욱 적합합니다.
이 모델은 신원 중심의 접근제어를 기반으로 하며, 사용자의 ID, 기기 상태, 위치 등을 종합적으로 평가하여 접근을 허용합니다. 또한 마이크로 세그먼테이션(micro segmentation)을 통해 네트워크, 워크로드, 서비스 수준까지 세분화된 접근 정책을 적용합니다. 최소 권한 원칙에 따라 모든 권한은 기본적으로 최소화하고, 필요한 경우에만 일시적으로 부여해야 합니다. 아울러, 단발성 인증에 그치지 않고 지속적으로 상태를 평가하고 접근을 제어하는 지속적 인증 및 모니터링이 필요합니다.

설계 및 운영 단계에서의 보안 고려 사항

클라우드 보안은 설계 단계와 운영 단계 모두에서 체계적인 접근이 필요합니다.
설계 단계에서는 먼저 CSP와의 책임 보안 모델을 명확히 이해하고, CSAP(cloud security assurance program, 클라우드 보안 인증)나 보안적합성, 개인정보 보호법과 같은 컴플라이언스 요건을 사전에 반영해야 합니다. 또한 로깅, 모니터링, 감사 로그를 포함한 체계를 설계하고, 네트워크 분리, 데이터 암호화, 키 관리 구조를 포함한 보안 아키텍처를 설계하고 검토해야 합니다.
운영 단계에서는 자동화된 취약점 스캔과 패치 관리를 지속적으로 수행하고, 계정과 권한에 대한 정기적인 리뷰를 실시해야 합니다. 모니터링 도구를 활용하여 이상 징후를 탐지하며, 안정적인 백업 및 재해 복구 계획을 마련해 두는 것이 중요합니다.

컴플라이언스 및 감사 대응

공공 클라우드 보안은 단순히 기술적 보안 조치에 그치지 않고, 관련 법적·제도적 준수 요건을 충족해야 합니다.
대표적인 관련 법령으로는 「전자정부법」, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」, 「개인정보 보호법」 및 「정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 기준」 등이 있습니다. 또한, 클라우드를 이용할 때는 데이터 주권(data sovereignty) 확보 방안도 함께 고려해야 합니다.
클라우드는 높은 유연성과 효율성을 제공하지만, 이에 수반되는 새로운 보안 위협과 책임 구조의 변화에 대한 명확한 이해와 대응이 필요합니다. 제로 트러스트 보안 모델의 도입, 설계 초기부터 보안을 고려한 아키텍처, 지속적인 모니터링과 감사 대응을 통해 공공기관의 클라우드 전환을 안전하게 추진할 수 있습니다.

3 컴플라이언스

3.1 컴플라이언스란

컴플라이언스(compliance)는 준수를 의미하는 용어로, 조직이 관련 법령, 규정, 가이드 등을 충실히 이행하는 것을 말합니다. 공공기관의 컴플라이언스는 단순히 법적 의무를 지키는 것을 넘어서, 안전하고 책임감 있는 서비스를 제공하기 위해 필수적으로 고려해야 하는 체계입니다.

클라우드 서비스 도입 시 컴플라이언스는 더욱 중요합니다. 데이터가 외부 인프라에 저장되고 처리되는 환경에서는 기존보다 복잡하고 다양한 법적, 기술적 요구 사항을 충족해야 하기 때문입니다. 이에 따라 공공기관은 클라우드 환경에 특화된 컴플라이언스 관리체계를 구축하고, 지속적으로 준수 상태를 점검·개선해 나가야 합니다.

3.2 공공 부문 컴플라이언스

3.2.1 법률과 지침, 가이드

공공기관이 클라우드 서비스를 안전하고 효과적으로 도입, 운영하기 위해서는 관련 법령과 각종 지침, 가이드라인을 체계적으로 준수해야 합니다. 이러한 규정들은 법적 구속력의 정도에 따라 차이가 있지만, 공공기관의 안전한 클라우드 환경 구축을 위해 반드시 고려해야 할 핵심 요건입니다.

법률은 가장 강력한 법적 구속력을 가지며, 이를 위반할 경우 직접적인 법적 제재를 받을 수 있습니다. 가이드라인은 법적 강제력은 없지만, 실무적으로는 표준이자 모범 사례로 인식되어 사실상 준수가 요구되는 기준으로 활용되고 있습니다.

따라서 공공기관은 클라우드 서비스 도입 과정에서 이러한 다층적 규제 체계를 종합적으로 검토하고 준수함으로써, 법적 리스크를 최소화하고 안전한 클라우드 환경을 구축할 수 있습니다.

표 3-1 주요 법과 지침 및 가이드

분류	컴플라이언스	설명
법	국가정보원법	국가정보원의 조직 및 직무 범위와 국가안전보장 업무의 효율적인 수행을 위하여 필요한 사항을 규정
법	사이버안보 업무규정	사이버안보 업무의 수행에 필요한 사항을 규정
법	보안업무규정	국가정보원의 직무 중 보안 업무 수행에 필요한 사항을 규정
지침	국가 정보보안 기본지침	정보보안 기본 업무에 대한 규정
법	전자정부법	행정업무의 전자적 처리를 위한 기본 원칙, 절차 및 추진 방법 등을 규정
행정 규칙	행정기관 및 공공기관 정보 시스템 구축·운영 지침	행정기관등의 장이 정보 시스템을 구축, 운영함에 있어서 준수해야 할 기준, 표준 등에 관한 지침
법	클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률	클라우드 컴퓨팅의 발전 및 이용을 촉진하고 클라우드 컴퓨팅 서비스를 안전하게 이용할 수 있도록 보호하는 법
행정 규칙	행정기관 및 공공기관의 클라우드 컴퓨팅 서비스 이용 기준 및 안전성 확보 등에 관한 고시	클라우드 컴퓨팅 서비스 이용 기준 및 안전성 확보 등에 필요한 사항 등에 관한 고시
법	국가사이버안전관리규정	국가 안보를 위협하는 사이버 공격으로부터 국가정보통신망을 보호함을 목적으로 하는 규정
법	개인정보 보호법	개인정보의 처리 및 보호에 관한 사항 규정
가이드라인	국가 클라우드 컴퓨팅 보안 가이드라인	국가/공공기관이 클라우드 컴퓨팅 서비스를 사용함에 있어 발생 가능한 보안 위협을 최소화하기 위한 보안 기준과 가이드
가이드라인	국가 망 보안체계 보안 가이드라인 1.0	각급 기관의 업무를 식별하고 중요도별(C: 기밀/S: 민감/O: 공개)로 등급을 구분한 후, 해당 등급에 맞추어 보안 대책을 차등 적용하는 사이버 보안 프레임워크인 N2SF 관련 가이드라인
가이드라인	국가 클라우드 컴퓨팅 보안관제 가이드라인(비공개)	클라우드 관제 관련 필요 사항을 가이드(비공개 문서로 공공 기관에만 공개)

컴플라이언스의 보안 주요 요구 사항

- 데이터 보안 및 시스템 보호: 암호화, 접근통제, 물리적 보호
- 거버넌스 및 관리체계 수립: 책임자 지정, 정책 수립, 위험 관리체계
- 감사 및 기록: 로그 관리, 보존 주기, 추적 가능성
- 서비스 제공자 보안 검토: CSAP 인증 여부, SLA(service level agreement, 서비스 수준 계약)상 보안 기준

※ 규제와 가이드 등은 본 문서 제작 시점 이후 변경될 수 있으므로, 정확한 확인을 위해서는 관련 법령 사이트나 국가사이버안보센터, 국정원, KISA 등의 최신 원문을 참고할 것을 권장합니다.

3.2.2 클라우드 및 정보보호 관련 인증 제도

공공기관이 클라우드 서비스를 도입하거나 이용할 때에는 국가 차원의 정보보호 및 신뢰성 확보를 위한 일정한 기준과 절차를 충족해야 합니다. 주요 제도로는 클라우드 서비스 보안 인증(CSAP) 및 보안성 검토, 보안 솔루션 인증 제도 등이 있으며, 이는 공공 부문에서의 안전한 클라우드 이용을 위한 제도입니다.

3.2.2.1 클라우드 서비스 보안 인증(CSAP)

클라우드 서비스 보안 인증(CSAP)은 공공기관이 클라우드 서비스를 도입하기 전, 해당 서비스가 일정 수준 이상의 보안성을 갖추었는지를 검증하기 위해 마련된 인증 제도입니다.

- 인증 대상: IaaS, SaaS, DaaS 등 클라우드 서비스 제공 사업자
- 인증서 발급 현황 확인: **KISA 한국인터넷진흥원 클라우드 보안인증제**에서 확인
- 참고: **인증의 유형 및 등급**

표 3-2 유형에 따른 통제 항목

유형	통제 항목
IaaS	관리적·물리적·기술적 보호 조치 및 공공기관용 추가 보호 조치 14개 분야 116개 통제 항목
SaaS 표준	관리적·기술적 및 공공기관용 추가 보호 조치(보안 인증 IaaS 환경에 구축 필요) 13개 분야 79개 통제 항목
SaaS 간편	관리적·기술적 및 공공기관용 추가 보호 조치(보안 인증 IaaS 환경에 구축 필요) 11개 분야 31개 통제 항목
DaaS	관리적·물리적·기술적 및 공공기관용 추가 보호 조치 14개 분야 110개 통제 항목

표 3-3 등급에 따른 통제 항목

유형	통제 항목
하등급	관리적·기술적 및 공공기관용 추가 보호 조치 14개 분야 64개 통제 항목
하등급 SaaS	관리적·기술적 및 공공기관용 추가 보호 조치 11개 분야 30개 통제 항목

※ 클라우드 서비스 보안 인증 등급은 '상/중/하'로 구분됩니다. '하' 등급은 **클라우드컴퓨팅서비스 보안인증에 관한 고시**에 반영되어 있으며, '상/중' 등급은 추후 반영 예정(**KISA** 발췌)입니다. '상/중' 등급에 대한 고시 변경 사항은 **입법행정예고** 중이며 고시의 제14조 제2항 후단에 신설될 예정입니다.

3.2.2.2 보안 관련 제도

표 3-4 보안 관련 제도

제도명	설명
보안적합성 검증	국가/공공기관이 도입하는 정보보호시스템/네트워크 장비 및 양자 암호통신장비 등 보안기능이 탑재된 IT 제품 및 저장 자료, 완전 삭제 제품의 안전성을 검증하는 제도. 정보보호시스템·네트워크 장비 및 양자 암호통신장비 등 보안 기능이 탑재된 IT 제품 및 저장 자료, 완전 삭제 제품 등이 대상. 단, 검증필 제품 목록 등재 제품 도입 시 보안적합성 검증 생략 가능 ※ 상세 내용은 **국가사이버안보센터**의 **보안적합성검증**에서 확인 가능
안전성 검증필 제품	국가정보원법 제4조, 사이버 안보 업무규정 제9조 및 전자정부법 제56조, 동법 시행령 제 69조에 의거, 국가정보원장이 정한 보안 기준을 만족한 제품 • 「보안기능 확인서」가 발급된 제품 • 「국내용 CC인증서」가 발급된 제품 • 국가용 보호프로파일 등 국가정보원장이 인정한 보호프로파일(PP)을 준수하여 CC인증을 받은 제품 • 그 외 국가정보원장이 안전성을 확인한 제품 ※ 상세 내용은 **국가사이버안보센터**의 **보안적합성검증 > 안전성 검증필 제품목록**에서 확인 가능
암호모듈 검증제도	「사이버안보 업무규정」 제9조와 「전자정부 시행령」 제69조 등에 따라 비밀로 분류되지 않은 중요 자료를 보호하기 위해 국가·공공기관에서 도입하는 암호 모듈의 안전성과 구현 적합성을 검증하는 제도 ※ 상세 내용은 **국가사이버안보센터**의 **암호모듈검증**에서 확인 가능
CC인증	정보 보호 제품이 국제, 국내 기준의 보안 요건에 따라 정보 보호 수준을 갖추었는지 평가하고 인증하는 제도 ※ 인증 제품 목록 및 상세 내용은 **IT보안인증사무국**에서 확인 가능 ※ **국가사이버안보센터** > 보안적합성검증 자료실의 「(1, 2편) 국가용 보안요구사항 V3.0 - 해설 및 공통보안요구사항」 자료에서 국가·공공기관이 도입하는 IT 보안제품의 보안 기능 상세 내용 확인 가능
ISMS-P	기업이나 기관이 정보보호와 개인정보보호를 체계적으로 관리하고 있는지 종합적으로 인증하는 제도 ※ 상세 내용은 **한국인터넷진흥원**에서 확인 가능

※ 국가·공공기관이 도입하는 정보보호시스템, 네트워크 장비 등에 대한 보안적합성, 안전성 검증필, CC인증에 대한 상세 내용은 **국가정보원**이나 **국가사이버안보센터**의 내용을 참고하세요.

3.2.3 NHN Cloud의 인증 현황

NHN Cloud는 CSAP(클라우드 보안인증)를 비롯하여 ISMS, CSA STAR등 다양한 보안 인증을 획득함으로써, 공공기관이 요구하는 보안 요건을 충족할 수 있는 서비스 체계를 갖추고 있습니다.
이러한 인증을 기반으로 공공기관은 NHN Cloud를 안전하고 신뢰성 있게 활용할 수 있으며, 보안성과 안정성이 검증된 환경에서 서비스를 운영할 수 있습니다. 또한, NHN Cloud는 '국가·공공기관 민간클라우드 컴퓨팅서비스 도입 가능 목록'에 등재되어, 공공 부문에서 공식적으로 활용 가능한 민간 클라우드 서비스로 인정 받고 있습니다.



그림 1 NHN Cloud CSAP 인증 현황

표 3-5 국가공공기관 민간 클라우드 컴퓨팅서비스 도입 목록

인증 번호	업체(기관)명	인증 범위	유효 기간
CSAP-2017-003호	엔에이치엔 클라우드	NHN Cloud(IaaS)	2022-12-13 ~ 2027-12-12
CSAP-2025-006호	엔에이치엔 클라우드	NHN Cloud (NCGN)(IaaS)	2025-02-27 ~ 2030-02-26
국가 클라우드 보안기준 적합 확인	엔에이치엔 클라우드	[NHNCloud] 클라우드 컴퓨팅 서비스 (IaaS '상' 등급: 인터넷·행정·공공영역) (나라클라우드)	2025-09-26 ~ 2030-09-25

NHN Cloud 정보 보호 인증 현황은 NHN Cloud 보안 센터의 **정보 보호 인증 현황**에서 보다 자세히 확인하실 수 있습니다.

4 민간 클라우드 도입을 위한 고려 사항

4.1 보안 책임 공유 모델(SSRM)의 이해

보안 책임 공유 모델(shared security responsibility model, SSRM)이란 안전한 클라우드 서비스를 위해 클라우드 서비스 공급자(cloud service provider, CSP)와 클라우드 서비스 사용자(cloud service customer, CSC)의 책임과 역할에 대해 구분하는 것입니다. 보안 책임 공유 모델의 목표는 서비스 공급자와 서비스 사용자가 협력해 각자가 통제하는 요소를 보호하여 클라우드 전반의 안전하고 신뢰성 있는 보안을 확립하는 것입니다.

표 4-1 NHN Cloud SSRM 매트릭스

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)

보안 책임 공유 모델은 클라우드 서비스 유형인 IaaS, PaaS, SaaS에 따라 다릅니다.
IaaS 모델에서는 서비스 제공자가 서버, 스토리지, 네트워크 등 물리적 인프라와 가상화 계층을 관리하고 보안 책임을 집니다. 하지만 운영체제, 애플리케이션, 데이터, 계정 및 접근 권한 등 상위 계층은 이용자가 직접 설정하고 보호해야 하며, 그에 따른 보안 책임 역시 고객에게 있습니다.

PaaS 모델은 IaaS보다 고객의 책임 범위가 줄어듭니다. 클라우드 제공자가 인프라는 물론 운영체제, 미들웨어, 런타임 환경까지 제공하고 관리하므로, 고객은 자신이 배포하는 애플리케이션과 그 안의 데이터에 대한 보안만을 책임집니다. 즉, 애플리케이션 취약점 관리, 데이터 암호화, 접근제어 등의 영역이 고객의 주요 관리 대상입니다.

SaaS 모델은 대부분의 보안 책임이 클라우드 서비스 제공자에게 있습니다. 애플리케이션부터 인프라, 플랫폼 전반을 CSP가 운영하므로, 고객은 사용자 계정 관리나 데이터 접근 설정 등 제한된 범위만을 책임집니다. 그러나 사용자의 부주의나 계정 도용, 잘못된 접근 권한 설정 등은 여전히 보안 사고로 이어질 수 있으므로, 최소한의 보안 조치는 고객이 수행해야 합니다.

클라우드 서비스 유형에 따라 보안 책임 범위가 달라지므로, 각자의 역할과 책임을 명확히 이해하고 이에 따라 보안 관리와 운영을 수행해야 합니다.

4.2 공공기관의 클라우드 도입 전 고려 사항

공공기관은 민간 클라우드 도입 시 단계별 보안 요건을 고려하여 클라우드를 선택하고 보안 적용 후 운영해야 합니다.
아래 그림은 국가 클라우드 컴퓨팅 이용 가이드의 내용을 발췌하여 도입 절차를 나타낸 것입니다. 절차별 주요 보안 요구 사항은 본 가이드의 4.2.1, 4.2.2, 4.2.3절을 참고하세요.

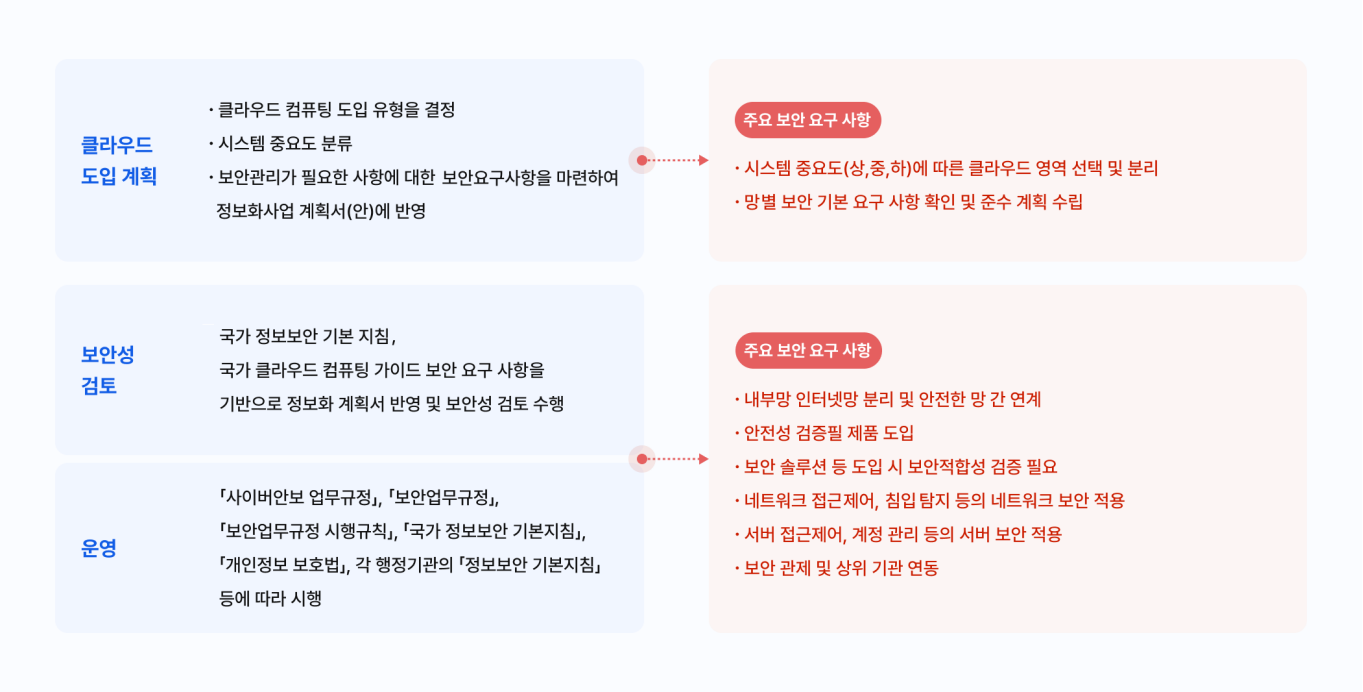


그림 2 클라우드 도입 절차

4.2.1 민간 클라우드 영역 선택 고려 사항

국가·공공기관은 민간 클라우드 도입 시 클라우드 서비스 보안인증(CSAP) 또는 국가기준보안적합확인을 받은 클라우드를 도입해야 합니다.[1] 그리고 클라우드에 시스템 구축 시 시스템의 중요도 등급에 따라 클라우드를 선택해야 합니다.

표 4-2 국가 클라우드 컴퓨팅 보안 가이드라인 표 8 발췌

분류 등급	세부 사항		영역 분리
상	파급 영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적 악영향을 미칠 수 있음.	물리적 분리
	분류 기준	국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감 정보를 포함하거나 행정 내부 업무 등을 운영하는 시스템	
중	파급 영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음.	물리적 분리
	분류 기준	비공개 업무 자료를 포함 또는 운영하는 시스템	
하	파급 영향	해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음.	물리적 또는 논리적 분리
	분류 기준	개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템	

1 '국가·공공기관은 민간 클라우드컴퓨팅서비스 **국가정보원 국가사이버안보센터 홈페이지**에 게시된 도입 요건 확인을 완료한 민간 사업자 클라우드 컴퓨팅 서비스를 이용한다.' - 국가 클라우드 컴퓨팅 보안 가이드라인 발췌

「국가 클라우드 컴퓨팅 보안 가이드라인」에서는 시스템 등급에 따라 물리적 또는 논리적 분리 방식을 선택하여 적용할 수 있도록 안내하고 있습니다.

- 민간 클라우드와 공공 클라우드가 동일한 콘솔, 하이퍼바이저 등을 사용하고 논리적으로 분리되어 시스템 등급 '하'인 경우 해당 클라우드를 도입할 수 있습니다.
- 하이퍼바이저, 콘솔 등이 민간용과 공공용이 물리적으로 분리되어 운영되는 클라우드로 시스템 등급 '중, 상'인 경우 해당 클라우드에 시스템을 구성할 수 있습니다.

NHN Cloud는 민간, 공공기관용 뿐만 아니라 행정기관용 등으로 클라우드 서비스가 물리적으로 분리되어 있습니다.

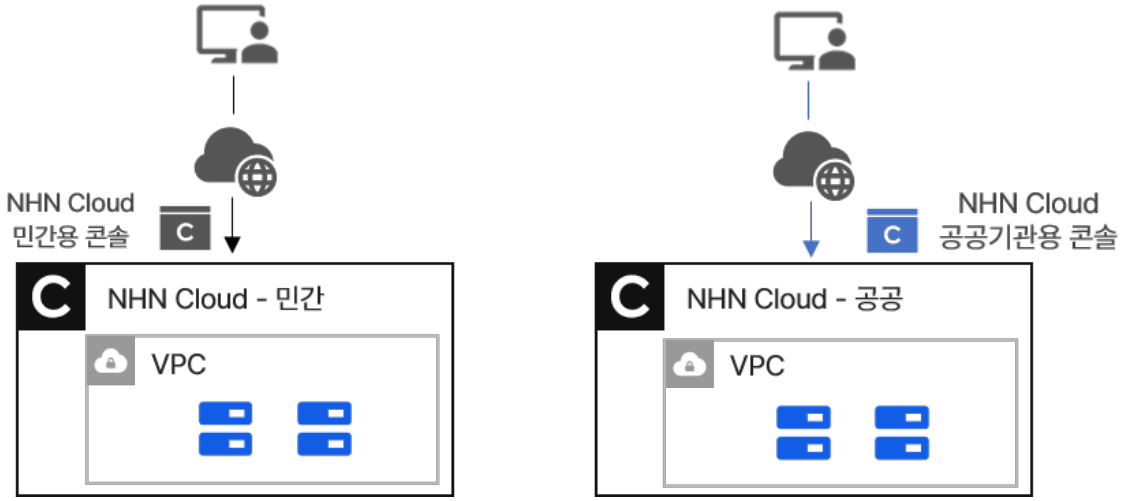


그림 3 물리적으로 분리된 NHN Cloud 서비스 제공

표 4-3 국가/공공기관을 위한 NHN Cloud 영역

NHN Cloud 분류	분리 수준	용도	중요도[2]
NHN Cloud 공공	민간과 물리 분리	공공/행정기관 인터넷 서비스	중 등급 가능
행정망 NHN Cloud 업무	민간 및 공공 업무망/인터넷망과 물리 분리	행정기관 업무용 시스템	상 등급 가능
공공망 NHN Cloud 업무	민간, 공공 인터넷, 행정망과 물리 분리	공공기관 업무용 시스템	상 등급 가능
행정망 NHN Cloud 인터넷	민간, 공공, 행정 업무망과 물리 분리	행정기관 대민 시스템	상 등급 가능
공공망 NHN Cloud 인터넷	민강, 행정, 공공 업무망과 물리 분리	공공기관 대민 시스템	상 등급 가능
NHN Cloud 퍼블릭	공공, 행정 클라우드와 물리 분리	민간 기업 등	이용 불가

※ 영역 분리는 국가기관용 클라우드 컴퓨팅 서비스가 일반 이용자용 클라우드 컴퓨팅 서비스와 데이터 및 프로세스 등의 간섭 없이 국가정보원 및 이용기관의 보안 관제, 사고 조사, 예방 보안 활동 유지를 위한 제반 환경을 만족시킬 수 있는 보호 조치를 말한다.[3]

2 시스템 중요도는 「국가 클라우드 컴퓨팅 보안 가이드라인」의 제3절 시스템 중요도 분류 기준 및 절차의 기준을 참고하세요. 또한 시스템 중요도에 따른 클라우드 사용 정책은 변경될 수 있으므로 국가정보원 또는 국가사이버안보센터 정책 공지의 수시 확인이 필요합니다.

3 「국가 클라우드 컴퓨팅 보안 가이드라인」 발췌

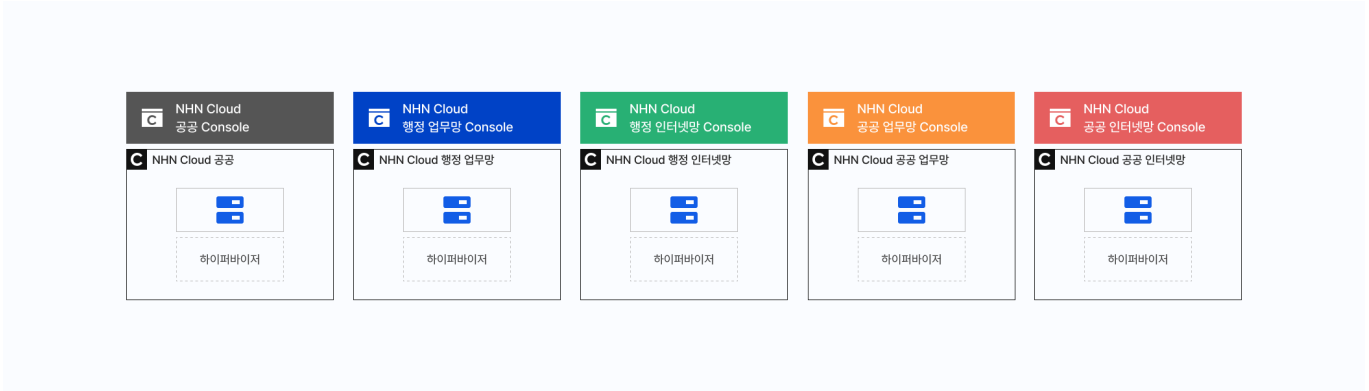


그림 4 공공 · 행정기관을 위한 NHN Cloud

NHN Cloud 국가·공공기관 민간 클라우드 컴퓨팅서비스 도입 가능 목록

국가사이버안보센터 **자료실**> **지침·가이드·공시**에서 도입 가능한 민간 클라우드 목록을 확인할 수 있습니다. 아래 발췌한 자료 목록과 같이 NHN Cloud가 제공하는 클라우드 서비스가 국가공공기관에서 도입할 수 있도록 인증되었음을 확인할 수 있습니다.

표 4-4 국가공공기관 민간 클라우드 컴퓨팅서비스 도입 목록

인증 번호	업체(기관)명	인증 범위	유효 기간
CSAP-2017-003호	엔에이치엔 클라우드	NHN Cloud(IaaS)	2022-12-13 ~ 2027-12-12
CSAP-2025-006호	엔에이치엔 클라우드	NHN Cloud (NCGN)(IaaS)	2025-02-27 ~ 2030-02-26
국가 클라우드 보안기준 적합 확인	엔에이치엔 클라우드	[NHNCloud] 클라우드 컴퓨팅 서비스 (IaaS '상' 등급: 인터넷·행정·공공영역) (나라클라우드)	2025-09-26 ~ 2030-09-25

4.2.2 민간 클라우드 도입 시 망별 보안 요구 사항

표 4-5 국가 클라우드 컴퓨팅 보안 가이드라인의 망별 보안 주요 요구 사항

구분	주요 기준	상세 내용
공통 기본 원칙	데이터 위치	데이터 센터는 국내 위치
	암호화 기술	검증필 암호 모듈 사용
	통신 보안	전용선 또는 VPN 기반 암호화 통신
	사용자 인증	다중 요소 인증(MFA) 방식 적용
	논리적 분리	기관/서비스별 분리 구성
	보안 관제	국가정보원·이용기관의 사이버 위협 대응 환경 유지
	운영 절차	백업, DR, 변경 관리, 사고 대응 등 SOP 수립

공공 업무망 영역	물리 위치	공공 업무망 전용 민간 클라우드 센터
	망 분리 기준	내부망으로 간주, 국가정보보안 기본 지침의 제40조(내부망·인터넷망 분리) 준수
	외부 접속 차단	외부 인터넷과 접점 없음
	보안 관제 연동	기관 자체 보안관제체계와 연동
	자료 연계	망연계 및 일방향 전송 기능 지원
	시스템 위치 등급	상/중/하 등급 위치 가능
물리 분리 인터넷망 영역	물리 위치	공공 인터넷망 전용 민간 클라우드 센터
	인터넷 접속	인터넷 접속 환경 구성
	보안 관제 연동	정부 보안관제체계(사이버안보 업무규정 제14조) 연계
	시스템 위치 등급	중/하 등급 위치 가능
논리 분리 인터넷망 영역	물리 위치	공공 인터넷망 전용 민간 클라우드 센터
	영역 분리 방식	국가·공공기관용 vs 민간용 논리적 분리 수행
	분리 안전성	논리 분리 훼손 위험 방지/완화/모니터링 수행
	보안 관제 연동	기관 보안 관제 → 정부 보안 관제 체계 연계 운영
	시스템 위치 등	하 등급 위치 가능

4.2.3 민간 클라우드 도입 시 고려할 기술적 보안 요구 사항

「국가정보보안기본지침」과 「국가 클라우드 컴퓨팅 보안 가이드라인」을 기반으로 주요 기술적 요구 사항을 정리·요약하였습니다. 해당 지침과 가이드라인은 법률의 세부 요건 등을 포함하고 있으므로, 민간 클라우드에 국가·공공기관의 정보시스템을 구축할 경우 기존 법률에서 요구하는 사항을 준수해야 합니다. 또한, 필요에 따라 보안성 검토(「국가정보보안기본지침」 제14조 등 참조)를 수행해야 합니다.

아래 내용은 「국가정보보안기본지침」 중 클라우드에 구축하는 정보시스템에 적용되는 주요 보안 요구 사항을 발췌·요약한 것이며, 보다 구체적인 사항은 「국가정보보안기본지침」 원문을 참고하세요.

표 4-6 국가정보보안기본지침의 보안 요구 사항 요약(상세 내용은 별첨 확인)

분류	키워드
제3절 제품 도입 정보통신제품(보안 솔루션) 등 도입 기준	보안적합성 안전성 검증필 등
내부망, 인터넷망 분리(40조)	망 분리 및 망간 연계
보안/네트워크장비 보안(42조)	보안 설정
	솔루션 버전 관리
	로그 보관
	탐지/차단 규칙 최신화

서버 보안(53조)	서버 접근제어
	서버 설정
	서버 백업
	DB 접근제어
공개 서버 보안(54조)	네트워크 분리(방화벽 등)
	IDS/IPS
	DDoS 차단
	서버 접근제어
로그 기록(55조)	로그 저장/관리(1년 이상 보관)
	로그 위·변조 방지
저장매체 폐기(61)	클라우드 업무 협조
계정 관리(75조)	계정 관리
비밀번호 관리(76조)	비밀번호 관리
사이버 공격 대응 훈련(96조)	DDoS 모의 훈련
암호 사용 원칙(102조)	검증필 암호 모듈
보안관제센터 설치·운영(131조)	보안 관제 연계
탐지규칙정보 개발 및 배포(133조)	탐지규칙정보 연동
공격정보 탐지·처리(134조)	SSL 가시화

표 4-7 국가 클라우드 컴퓨팅 보안 가이드라인(4장 제2절)의 보안 요구 사항 요약(상세 내용은 별첨 확인)

분류	키워드
정책적 측면(공통 기본 원칙)	중요도 분류, 영역 분류
	국내 클라우드 사용
	CSAP 인증
	보안적합성
	망 분리 보안
	보안 책임 영역
정책적 측면(SaaS 환경 추가 기본 원칙)	SaaS 보안
	국내 클라우드
	SaaS 보안성 평가
기술적 측면(공통 기본 원칙)	망 분리
	시스템 접근제어
	암호화
	보안 관제

기술적 측면(SaaS 환경 추가 기본 원칙)	SaaS 보안성 평가
	API 취약점 관리
	취약점 관리
	SSL 적용
	암호화
	접근제어

표 4-8 컨테이너 보안(국가 클라우드 컴퓨팅 보안 가이드라인 부록 6 발췌)

분류	내용
[관리 노드]	오케스트레이터 등 가상화 관리 솔루션이 실행되는 호스트 시스템
오케스트레이터(orchestrator)	컨테이너 런타임으로 컨테이너를 지정된 컨테이너 노드에 배치하거나 문제가 발생한 컨테이너를 교체하거나 컨테이너 환경 정보를 설정하는 등 스케줄링, 클러스터링 및 네트워킹을 관리하는 오케스트레이션 수행(Kubernetes 등)
[컨테이너 노드]	컨테이너 가상화 환경이 운영되는 호스트 시스템
컨테이너	애플리케이션과 환경 정보가 포함된 독립적인 격리 실행 가상 환경·컨테이너 이미지는 메타데이터, 애플리케이션 바이너리 및 공유 라이브러리를 패키징하고 있는 .tar 형식 파일
컨테이너 런타임	컨테이너를 쉽게 가져오거나 공유하고 구동할 수 있도록 지원하는 도구(Docker 등)
호스트 운영체제	컨테이너를 실행하는 기반 시스템·운영체제 네임스페이스(namespace), 컨트롤 그룹(cgroups) 기능으로 컨테이너 런타임은 컨테이너 격리(isolation)를 수행
[가상 머신 레지스트리]	컨테이너 이미지가 저장되는 저장소
이미지 저장소	컨테이너 이미지를 관리하고 공유하기 위한 애플리케이션·OCI는 이미지 저장소(레지스트리)에 대한 규격을 제시
[관련 보안 정책 및 규정]	• 「국가정보보안기본지침」, 국가정보원 • 「국가 클라우드 컴퓨팅 보안 가이드라인」, 국가정보원 • 컨테이너 런타임은 가상 환경을 구현해 주는 '가상화 제품'에 해당, CC인증 대상이지만 도입 요건을 필수가 아닌 권고로 제시(2021.4.14.부터 적용, 국가정보원 홈페이지 참조)

※ 컨테이너 관련 보안 설계, 구성에 대한 내용은 NHN Cloud 보안 센터의 「**컨테이너 보안 가이드**」에서 상세하게 확인하실 수 있습니다.

위의 표에서 정리한 것은 가이드나 지침에서 발췌한 것으로 상세 내용은 전체 원문 확인이 필요하며 추가로 공공기관은 위 사항 외에도 개인정보 보호법 등에서 규정하는 다양한 컴플라이언스 요구 사항을 준수해야 합니다. 따라서 위의 표에서 기술된 사항 외 시스템 구축 전 관련 법규 및 시행령의 상세 내용을 면밀히 검토하여 법적 요구 사항을 파악하고, 이를 바탕으로 시스템에 적절한 보안 조치를 적용해야 합니다.

4.2.4 공공기관 보안 솔루션 도입 시 고려 요건

공공기관이 보안 솔루션 등의 도입 시 다음과 같은 검토, 절차가 필요합니다.

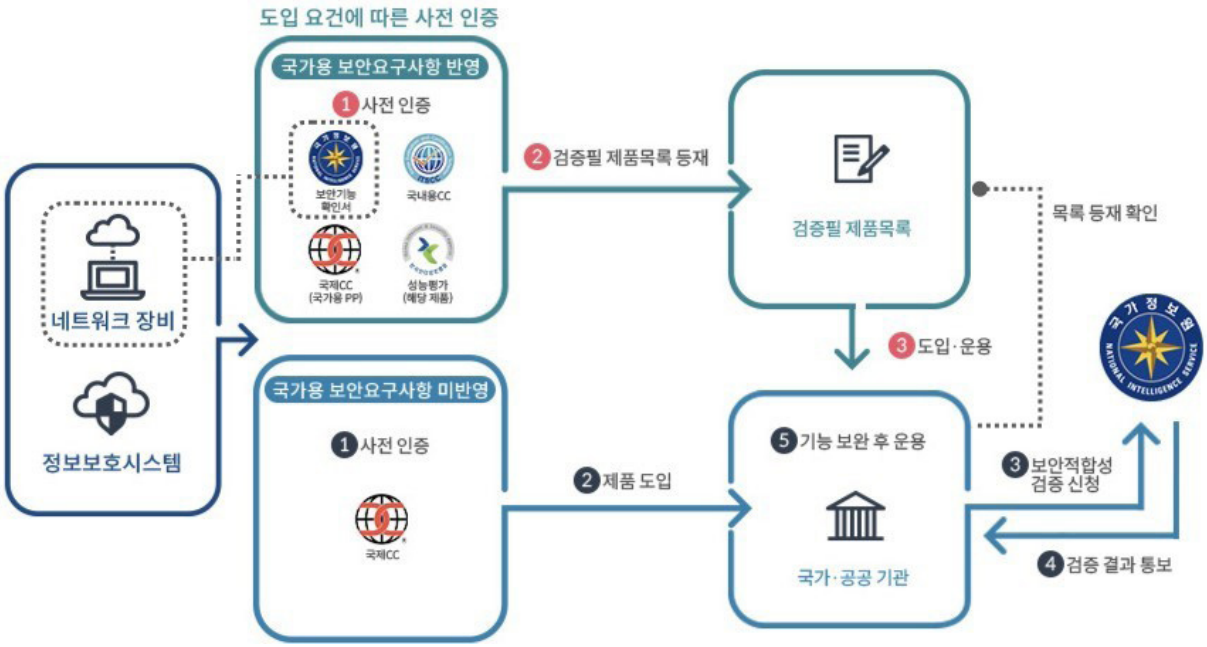


그림 5 정보보호시스템/네트워크 장비 도입 절차[4]



그림 6 암호 모듈 시험/검증[5]

4, 5 국가사이버안보센터 발췌

아래 그림은 국가사이버안보센터의 '정보보호시스템·네트워크 장비 도입 절차'와 '암호모듈 시험·검증' 등을 참고하여 간략히 재구성한 것입니다.

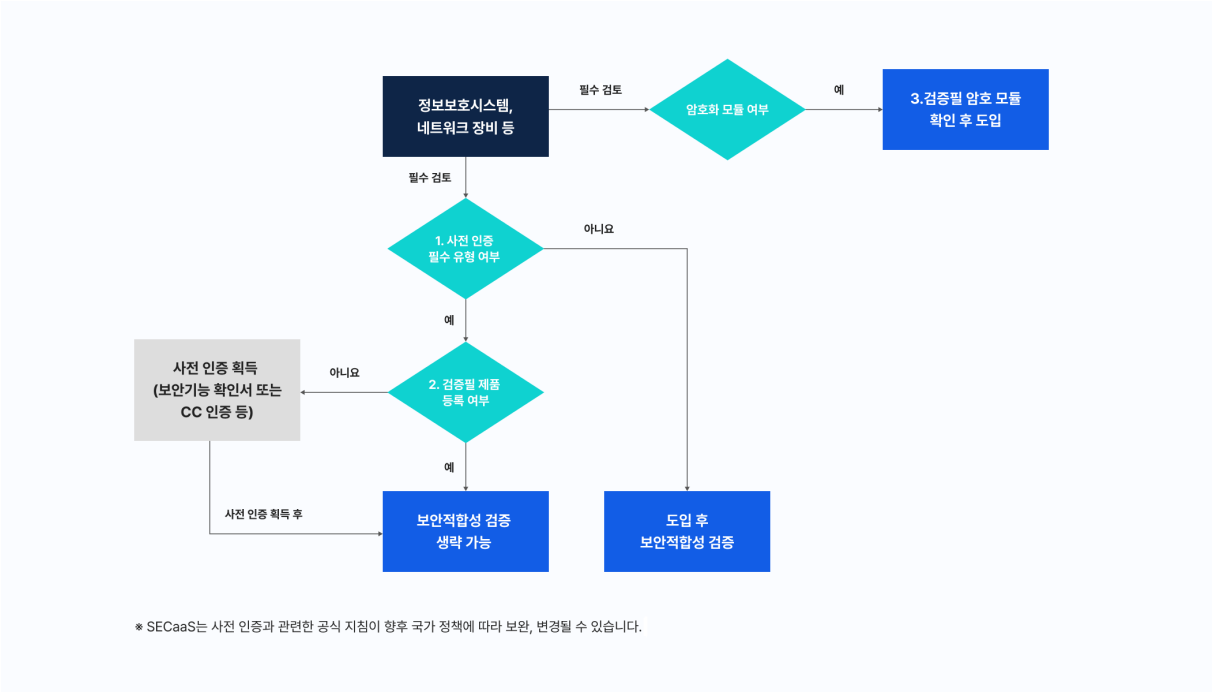


그림 7 보안 솔루션 도입을 위한 절차 참고

※ 참고[6]

사전 인증

- 보안기능 확인서[7] 또는 CC인증(CCRA 회원국이 발행한 CC인증)[8]을 보안적합성 심사 전 취득을 하는 것(특정 제품 유형에 대해 사전 인증이 필요)
- 보안기능 확인서 또는 CC인증 필수 여부는 제품군마다 상이하여 정확한 내용은 사이버안보센터에서 확인 필수

안전성 검증필 제품

국가정보원장이 정한 보안 기준을 만족한 '안전성 검증필 제품', 국가사이버안보센터에서 목록 확인 가능

- '보안기능 확인서'가 발급된 제품
- '국내용 CC인증서'가 발급된 제품
- 국가용 보호프로파일 등 국가정보원장이 인정한 보호프로파일(PP)을 준수하여 CC인증을 받은 제품
- 그 외 국가정보원장이 안전성을 확인한 제품

검증필 암호 모듈

국가·공공기관에서 도입하는 암호 모듈의 안전성과 구현 적합성을 검증하는 제도

6 **국가사이버안보센터**에 게시된 내용을 발췌, 인용하여 작성된 내용으로 정확한 내용은 국가사이버안보센터 홈페이지에서 확인하세요.

7 보안적합성 검증 절차 간소화를 위해 정보보호시스템·네트워크 장비 및 양자암호통신장비 등 IT 제품에 대해 공인 시험 기관이 '국가용 보안요구사항' 만족 여부를 시험하여 안전성을 확인해 주는 제도

8 CC인증에 대한 자세한 내용은 3.2.2장을 참고하세요.

표 4-9 NHN Cloud 보안 서비스 인증

분류	NHN Cloud 서비스	사전 인증 현황
침입 차단 제품군	DDoS Guard	CC인증서 보유
침입 차단 제품군	WEB Firewall	CC인증서 보유
침입 차단 제품군	Security Monitoring	CC인증서 보유
보안 관리 제품군	SIEM	CC인증서 보유
엔드포인트 보안 제품군(안티-바이러스 제품)	Vaccine	CC인증서 보유
구간 보안 제품군	SSL VPN	CC인증서 보유

※ 클라우드 보안 서비스 도입 기준은 현재 정책이 변경·보완되고 있으며, 참고 자료로는 국가사이버보안센너 자료실의 「클라우드 보안요구사항 V1.0 - 클라우드 운영환경 공통보안요구사항」을 확인하세요. 그 외 「국가용 보안요구사항 V3.0 - 해설 및 공통보안요구사항」 등에서 국가·공공기관에 도입되는 보안 기능이 탑재된 보안 솔루션에 대한 요구 사항을 확인할 수 있습니다(보안 요구 사항 관련 문서는 국가사이버안보센터 보안적합성검증 자료실에서 확인할 수 있습니다.).

※ NHN Cloud 보안 서비스의 보안 인증 관련 자료가 필요한 경우 **NHN Cloud 고객 센터 > 1:1 문의**를 통해 요청하세요.

5 보안 인프라 구성 방안

※ NHN Cloud 및 마켓플레이스에서 제공되는 서비스는 리전별로 구성이나 제공 범위가 다를 수 있으며, 정기적인 업데이트와 새로운 서비스 출시를 통해 지속적으로 개선되고 있습니다.

5.1 NHN Cloud 영역 선택 및 망 분리

5.1.1 NHN Cloud 영역 선택

NHN Cloud는 공공·행정기관을 위한 클라우드를 업무망용과 인터넷망용으로 구분하여 제공하고 있습니다. 4.2.1장에서 설명한 내용에 따라 민간 클라우드 선택 전 시스템의 등급을 식별하고 NHN Cloud의 영역을 적절하게 선택합니다.

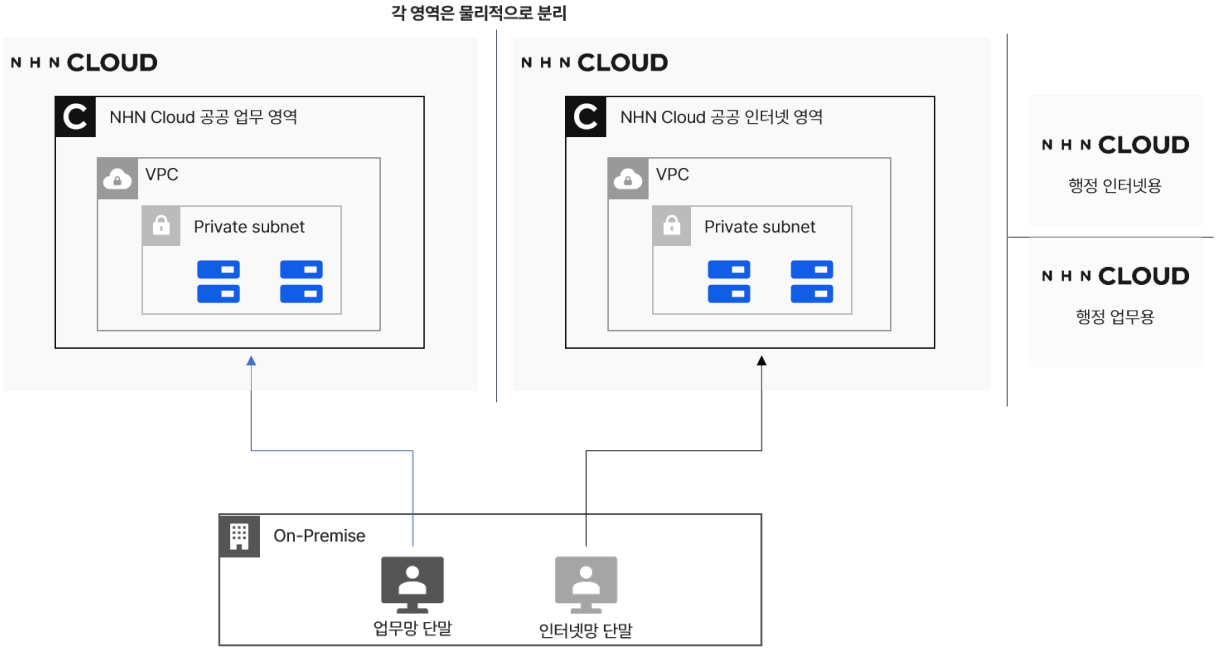


그림 8 공공기관 사용자인 경우 예시

5.1.2 망 분리 및 망 간 연계

NHN Cloud는 컴플라이언스 요건에 맞추어 클라우드 영역을 제공하고 있습니다. 물리적으로 독립된 NHN Cloud 환경에 업무망과 인터넷망 자원을 배치하여 구성할 수 있습니다. 네트워크의 분리나 관리적인 목적 등으로 자원을 분리하여 구성이 필요할 때는 조직, 프로젝트 및 VPC 등을 활용하여 분리하여 구성이 가능합니다.

물리적 망 분리 구성

NHN Cloud는 공공, 행정기관이 사용할 수 있는 업무용, 인터넷용 클라우드를 물리적으로 분리하여 제공합니다.

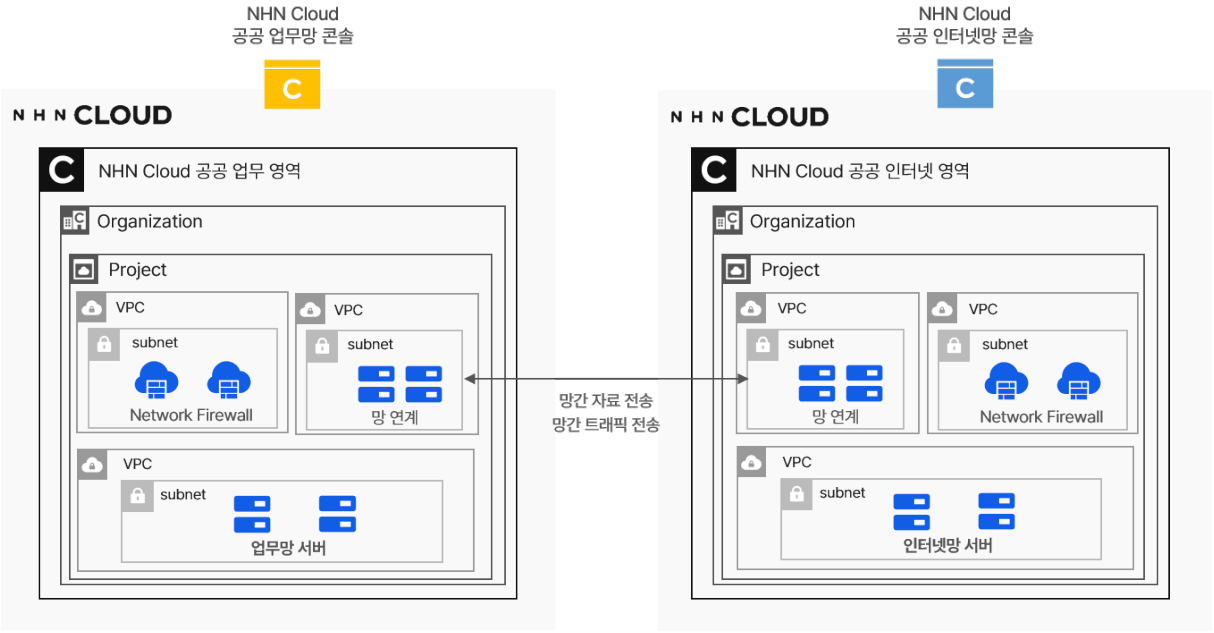


그림 9 물리적 방 분리와 망 간 연계 구성

5.2 클라우드 콘솔 보안

NHN Cloud 콘솔은 클라우드 자원의 생성, 설정 변경, 삭제 등 모든 관리 작업의 출발점이므로, 그 보안은 클라우드 환경 전반의 안정성과 직결됩니다. 만약 콘솔에 부적절한 접근이 발생한다면 심각한 보안 사고로 이어질 수 있습니다. 따라서 콘솔 보안을 강화하기 위해서는 먼저 체계적인 접근 정책을 수립하고, 계정과 권한을 최소 권한 원칙에 따라 관리해야 합니다. 아울러, 기술적으로 구현 가능한 부분은 솔루션이나 서비스를 활용해 자동화하거나 수동 적용하고, 관리자의 확인 등이 필요한 부분은 명확한 절차를 마련해 지속적으로 준수할 수 있도록 합니다.

5.2.1 콘솔 접근제어

도메인 설정

관리자는 IAM 계정 전용 콘솔 도메인을 설정할 수 있으며, 사용자는 설정된 도메인을 통해 콘솔에 접속하여 IAM 계정으로 로그인할 수 있습니다. IAM 계정 전용 로그인 도메인과 함께 로그인 보안 설정 등을 사용하면 인증 강도를 강화할 수 있습니다.

- **조직 > 조직 기본 설정 > 도메인 설정**

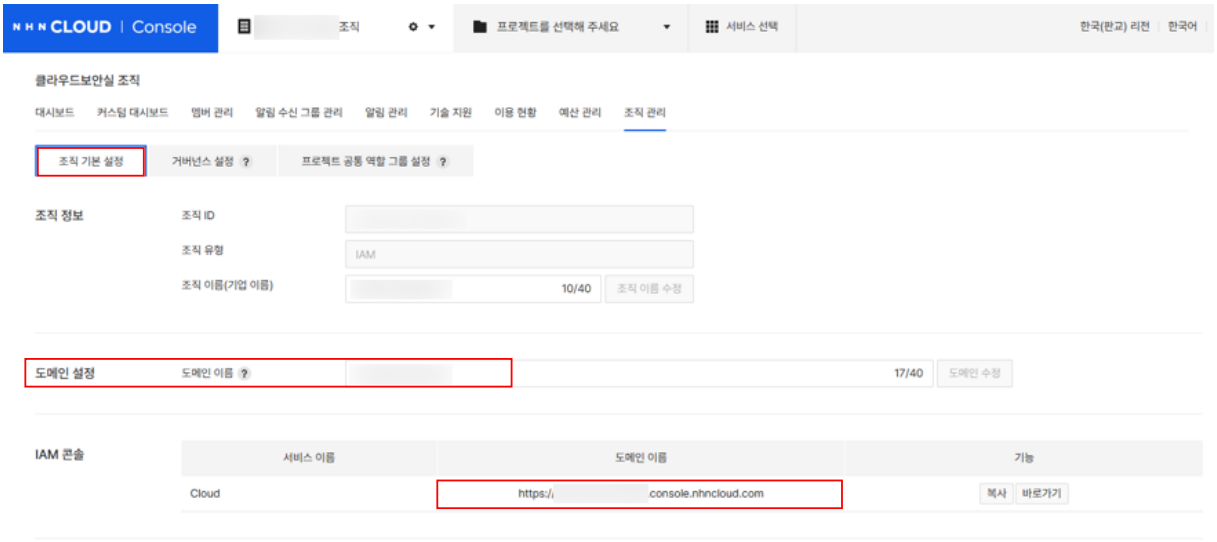


그림 10 IAM 콘솔 도메인 설정

IP ACL 설정

IP 기반 접근제어를 통해 NHN Cloud 콘솔과 프레임워크 API 등에 대한 접속을 관리할 수 있습니다. 관리자가 허용한 IP에서만 접근이 가능하도록 설정함으로써 불필요한 접근 시도를 방어할 수 있습니다.

- **조직 > 거버넌스 설정 > IP ACL 설정**

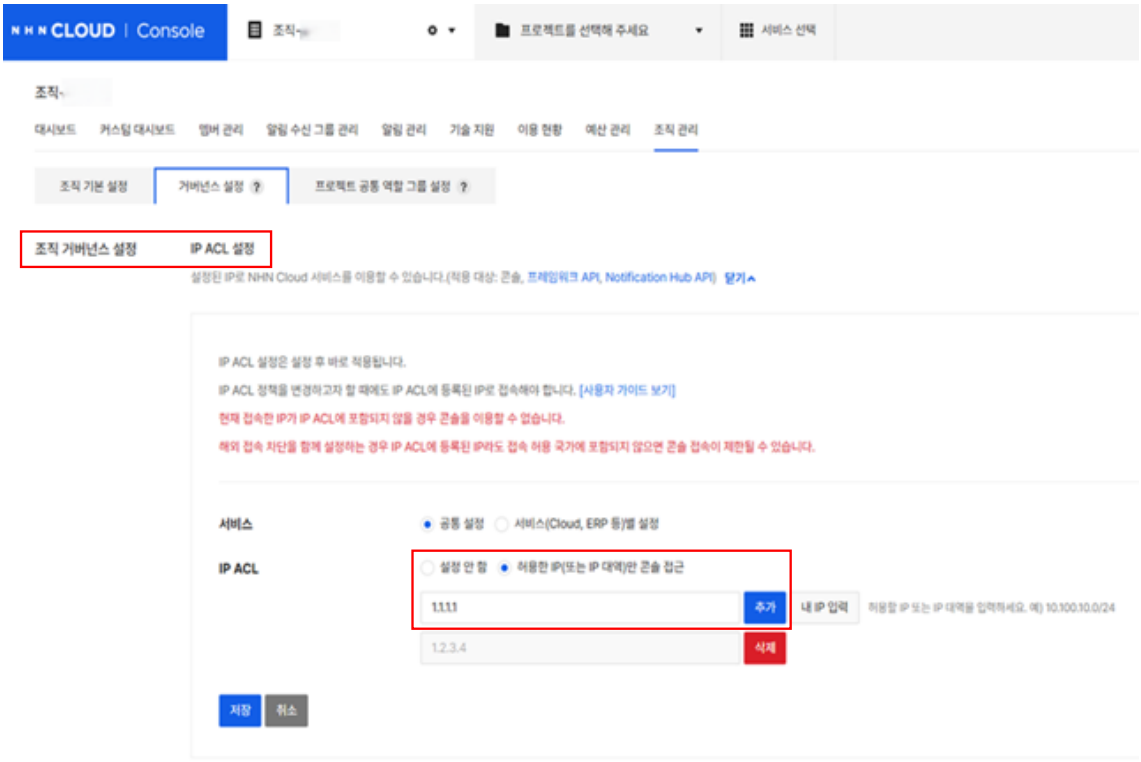


그림 11 IP ACL 설정

해외 접속 차단 설정

접속이 허용된 국가에서만 콘솔에 접속할 수 있도록 설정할 수 있습니다. 이를 통해 지정되지 않은 지역에서의 비정상적 접속 시도를 사전에 차단하여 계정 탈취, 무단 접근과 같은 보안 위협을 줄일 수 있습니다.

- **조직 > 거버넌스 설정 > 해외 접속 차단 설정**

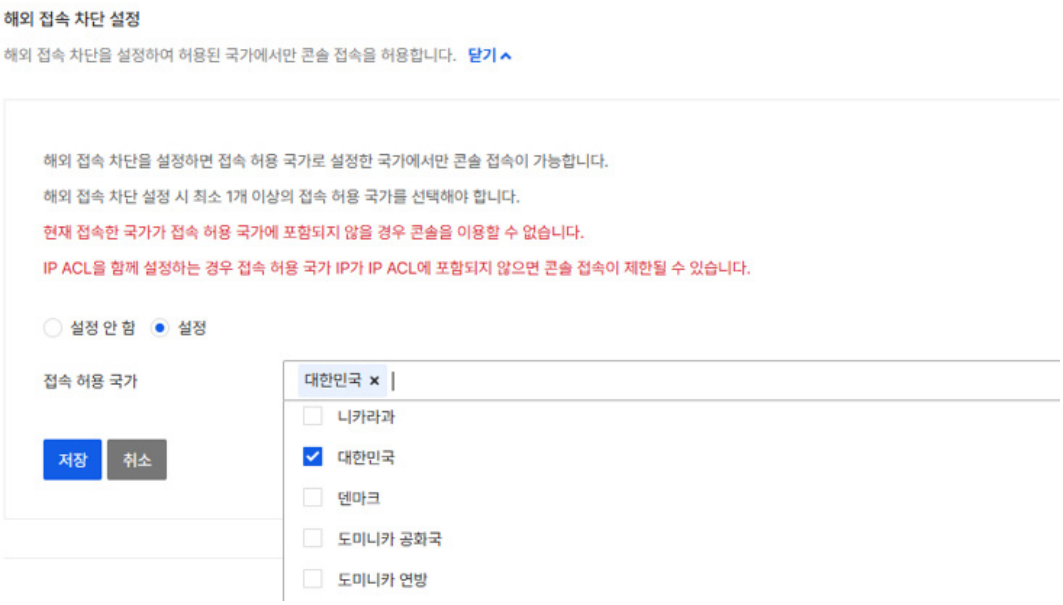


그림 12 해외 접속 차단 설정

NHN Cloud Security Advisor 점검

Security Advisor의 점검 항목으로 IAM 콘솔 도메인 설정 상태와 IP ACL 설정 상태를 점검할 수 있습니다.
Security Advisor를 이용하여 보안 설정에 미흡한 부분이 발생하지 않도록 주기적인 점검을 할 수 있습니다.

- **Security > Security Advisor**

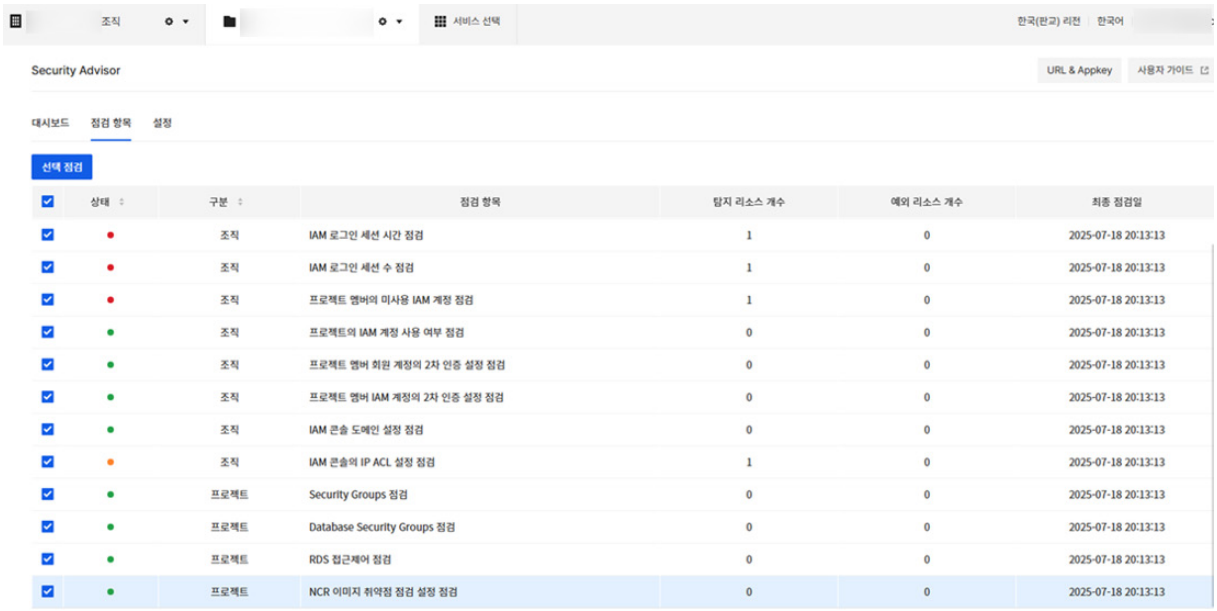


그림 13 Security Advisor 점검 항목

5.2.2 콘솔 계정 관리

콘솔 계정은 클라우드 자원을 생성, 관리, 삭제할 수 있는 강력한 권한을 가지므로 철저한 관리가 필요합니다. OWNER 계정 사용은 최소화하고, 역할과 권한이 적절히 부여된 IAM 계정을 활용하는 것이 바람직합니다.
사용자별 개별 IAM 계정을 발급하고, 계정 공유는 금지하며 2차 인증 설정 등의 로그인 보안 설정을 통해 안전하게 계정을 관리해야 합니다.

콘솔 계정과 역할

NHN Cloud에는 NHN Cloud 계정과 IAM 계정이 있습니다. NHN Cloud 계정은 이용 약관에 동의하여 가입한 회원으로, 서비스 이용에 대한 책임과 의무를 가지는 멤버로 소속된 조직이 삭제되어도 계정은 유지됩니다. IAM 계정은 NHN Cloud 이용 약관에 동의하지 않은 멤버로 조직 내에서만 유효하고 소속된 조직이 삭제되면 함께 삭제됩니다. NHN Cloud 계정과 IAM 계정에 대한 자세한 내용은 **NHN Cloud 사용자 가이드**를 참고하세요.
NHN Cloud 계정에는 역할을 부여할 수 있습니다. 계정 관리의 기본 원칙에 따라 계정은 1인 1계정으로 발급하고 최소 권한 원칙으로 역할 부여하는 것을 권장합니다.

역할(role)이란 NHN Cloud에서 계정이 특정 조직, 프로젝트, 또는 서비스를 이용할 수 있도록 부여되는 권한 집합입니다.
예를 들어 특정 계정에 조직 관리 역할 'BILLING_VIEWER'를 부여하면 결제 관리 이용 현황 및 예산 관리에 대한 읽기 등이 가능하게 됩니다. 역할에 대한 자세한 내용은 **NHN Cloud 사용자 가이드**를 참고하세요.
이처럼 콘솔 계정에 알맞은 역할을 부여해 권한 남용이나 실수로 인한 사고 방지 및 책임 추적성을 확보함으로써 보안을 더욱 강화할 수 있습니다.

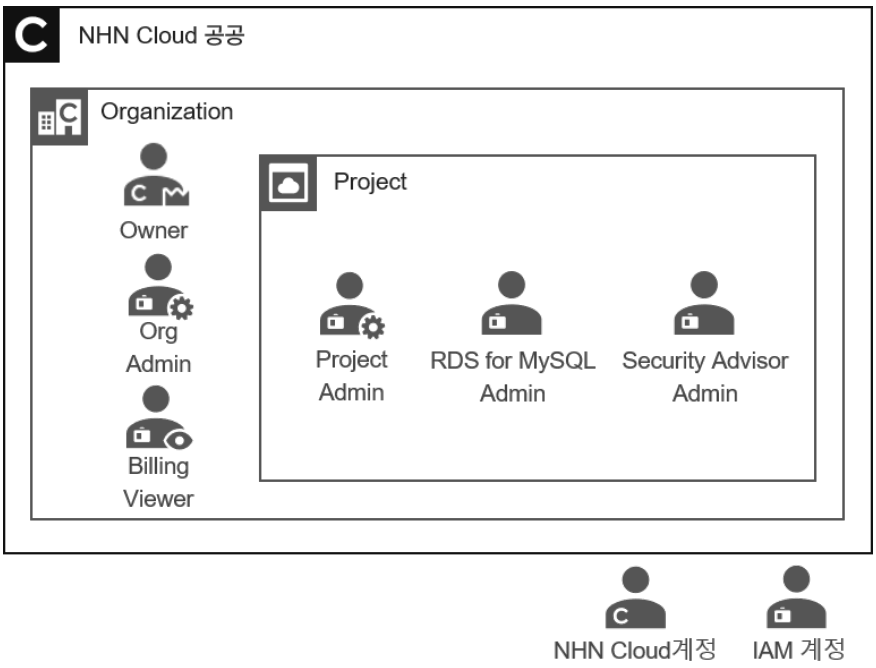


그림 14 계정별 역할 부여 예시

로그인 보안 설정

로그인 보안 설정은 IAM 계정에 대해 2차 인증, 세션 시간 제한, 로그인 시도 횟수 제한 등을 적용하여 계정을 각종 보안 위협으로부터 안전하게 보호할 수 있도록 하는 기능입니다. 2차 인증 설정을 포함하여 IAM 계정 보안을 위해 반드시 보안 설정 후 계정 관리하는 것을 권고합니다.

- **조직 관리 > 거버넌스 설정 > IAM 거버넌스 설정 > 로그인 보안 설정(2차 인증, 최대 로그인 시도, 로그인 세션)**



그림 15 로그인 보안 설정

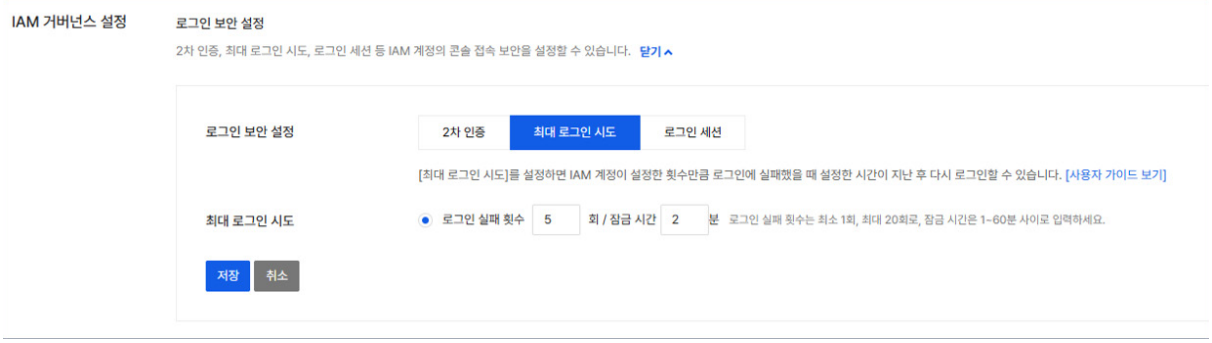


그림 16 최대 로그인 시도

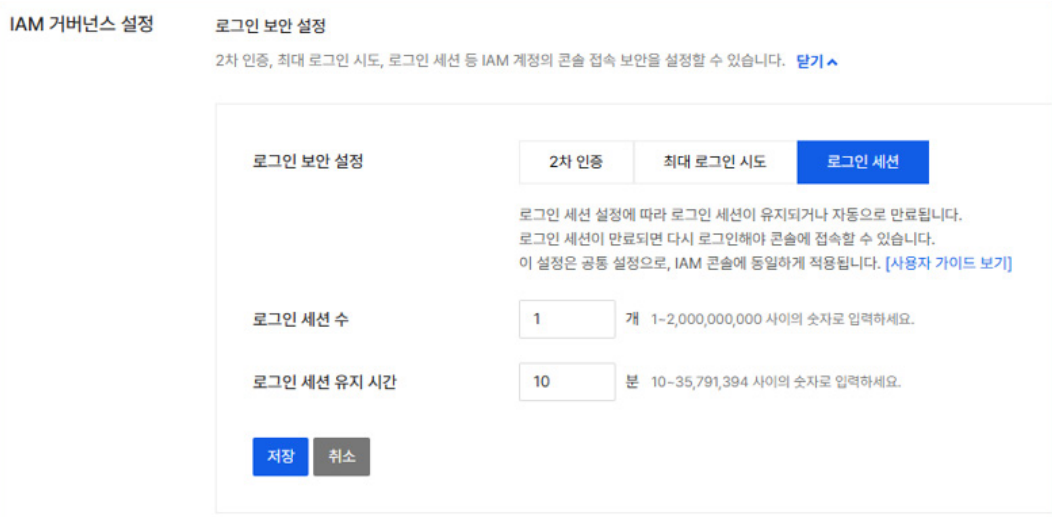


그림 17 로그인 세션

비밀번호 정책 설정

계정의 패스워드 최소 길이, 복잡성(강도), 만료 기간 등을 적절히 설정하는 것은 계정 탈취를 예방하기 위한 기본적인 보안 조치입니다. 약하거나 오래된 패스워드는 무차별 대입 공격(brute force)이나 사전 대입 공격(dictionary attack)에 쉽게 노출될 수 있으므로, 강력한 정책 수립과 지속적인 관리가 필수적입니다.

- **조직 관리 > 거버넌스 설정 > IAM 거버넌스 설정 > 비밀번호 정책 설정**

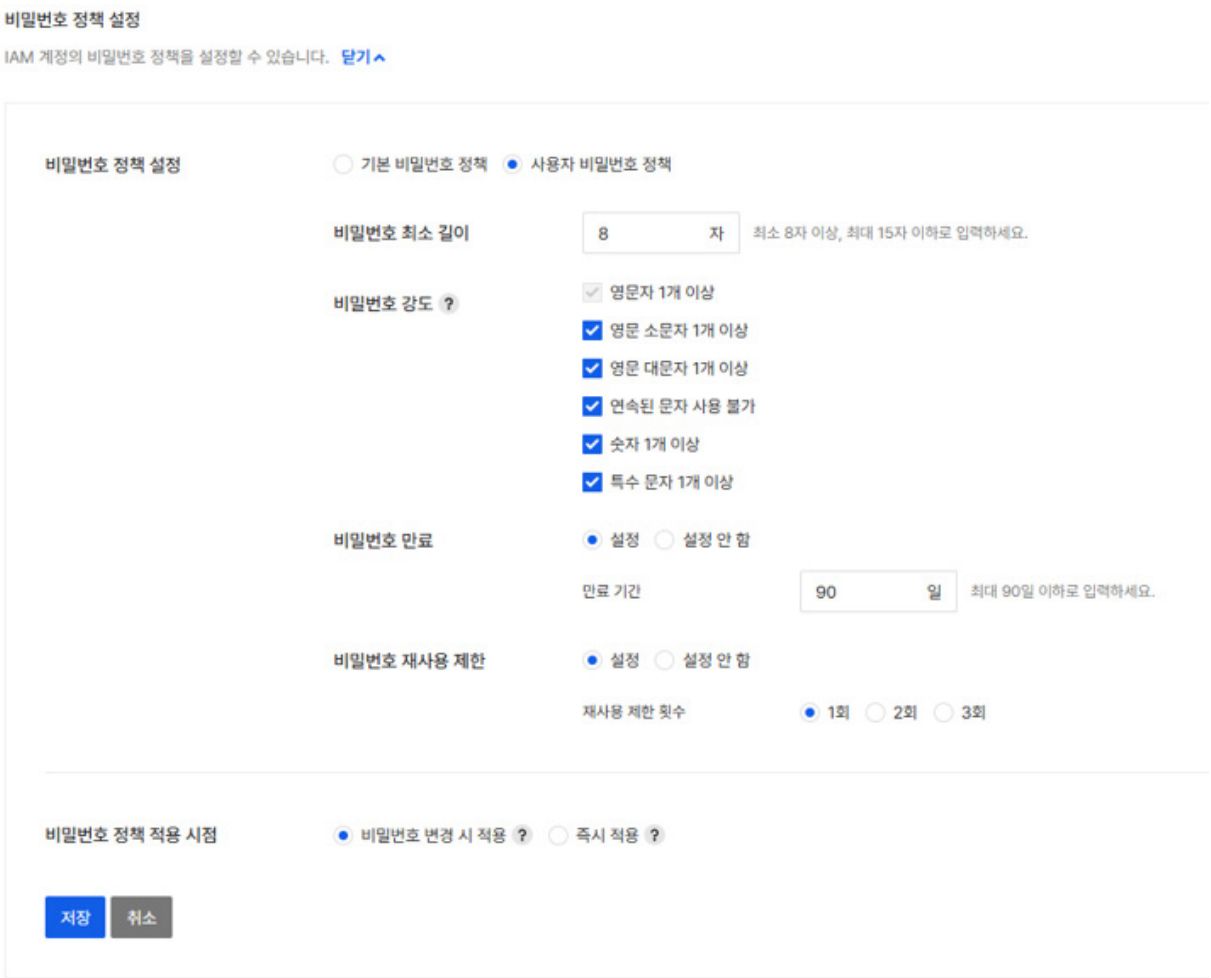


그림 18 비밀번호 정책 설정

NHN Cloud Security Advisor 점검

Security Advisor를 활용하여 로그인 보안 설정이나 IAM 계정 사용 유무, 미사용 계정 체크 등을 할 수 있습니다.

- **Security > Security Advisor**

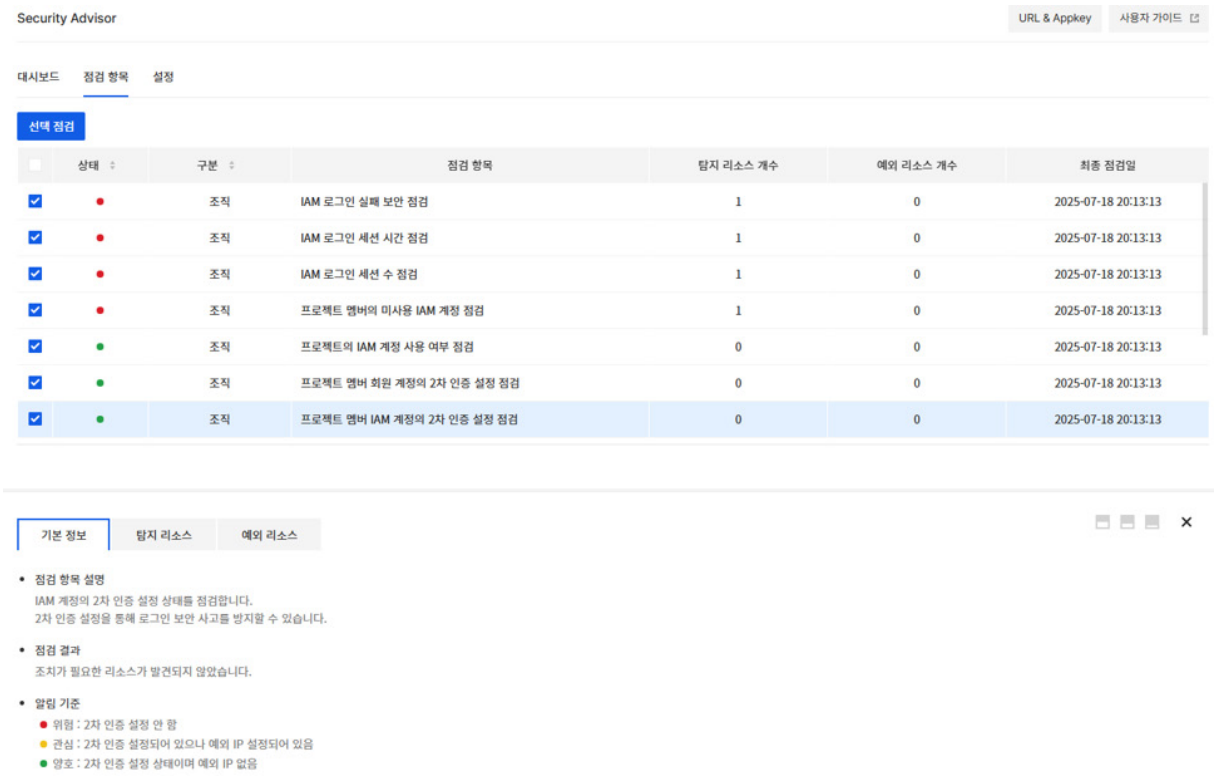


그림 19 Security Advisor 점검

5.2.3 클라우드 콘솔 로깅

NHN Cloud CloudTrail

사용자의 NHN Cloud 사용 이력을 확인할 수 있는 서비스로 조직 단위로 제공되며, 별도의 활성화 과정 없이 바로 사용 가능합니다. 기본 인프라 서비스와 콘솔 사용 이력 기록을 확인할 수 있으며 3개월 이상 로그 보관 필요시 Object Storage를 통해 별도 백업 보관이 가능합니다.

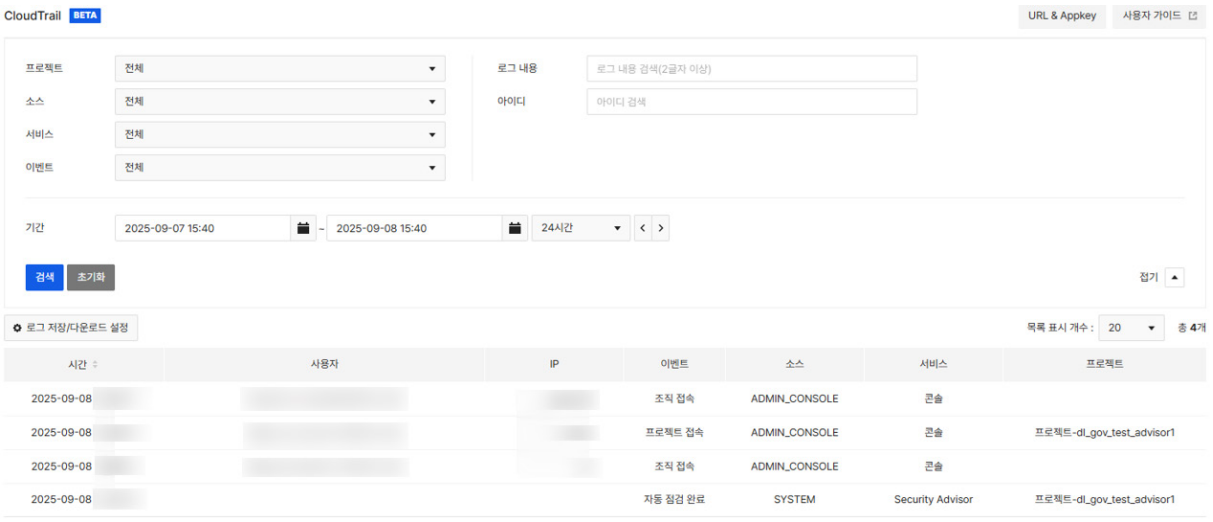


그림 20 CloudTrail

5.3 네트워크 보안

네트워크 보안은 조직의 정보 자산을 보호하기 위한 핵심 요소로, 외부 위협과 내부 위협으로부터 안전한 통신 환경을 보장하는 데 목적이 있습니다. 방화벽, 침입 탐지·방지 시스템, 네트워크 분리와 같은 기술적 통제뿐만 아니라, 접근제어와 모니터링 체계를 통해 위협을 조기에 탐지하고 대응하는 것이 중요합니다. 본 장에서는 안전한 네트워크 아키텍처 구축과 운영을 위한 주요 보안 서비스와 권장 사항을 제시합니다.
5장에서 소개하는 서비스의 내용과 구성 등은 NHN Cloud 보안 센터에서 제공하는 「**네트워크 아키텍처 보안 가이드**」에서 보다 더 상세히 확인하실 수 있습니다.

5.3.1 네트워크 접근제어

네트워크 제어는 IP, 포트 등을 기반으로 내/외부의 불법적인 접근을 차단하여 네트워크를 보호할 수 있습니다.

NHN Cloud Security Groups

Security Groups로 인스턴스의 송/수신 트래픽을 프로토콜, IP, 포트 기준으로 제어할 수 있습니다. 보안 그룹은 개별 인스턴스에 적용할 수 있습니다.

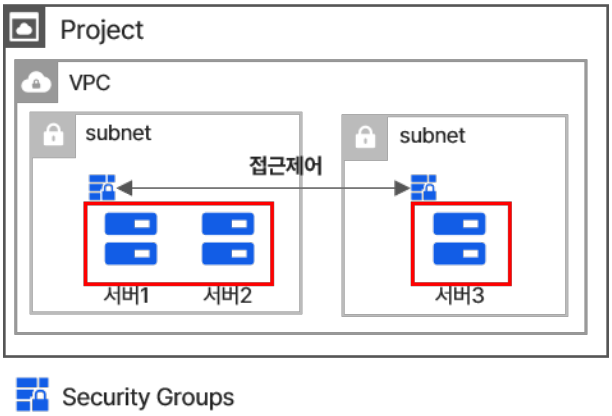


그림 21 Security Groups

Security Groups의 보안 규칙은 Security Advisor를 통해 보안 점검을 할 수 있습니다. Security Advisor는 그 외 여러 가지의 점검 항목을 제공하고 있으며 상세 내용은 **사용자 가이드**를 참고하세요.

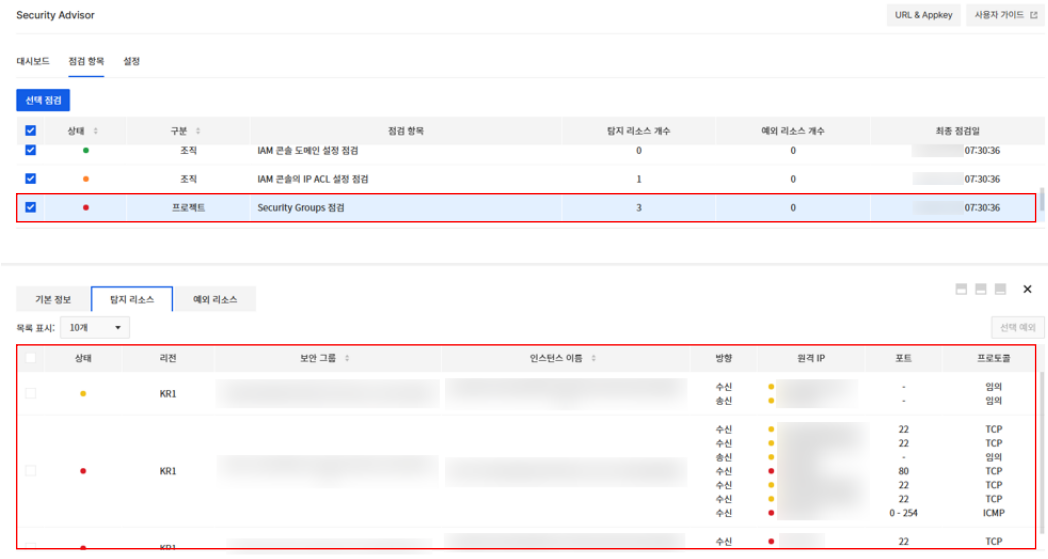


그림 22 Security Advisor의 Security Groups 점검 결과 예시

NHN Cloud Network ACL

IP, 프로토콜, 포트 기준으로 네트워크 접근을 통제할 수 있는 기능은 Security Groups와 유사합니다. 단 Network ACL은 VPC에 바인딩하여 접근통제 정책을 적용할 수 있습니다.

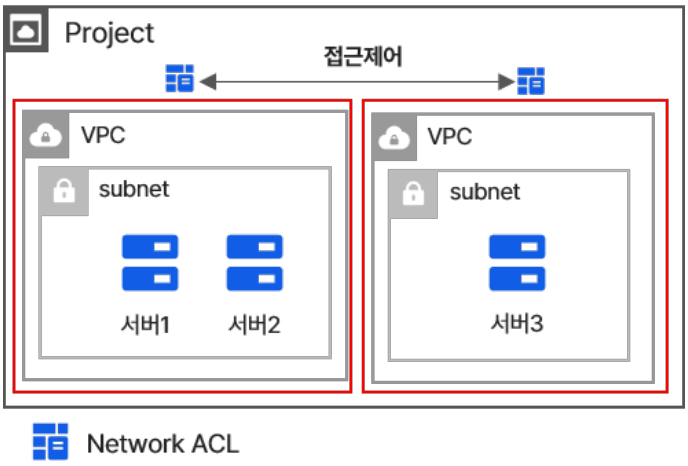


그림 23 Network ACL

NHN Cloud Network Firewall

Network Firewall은 VPC 등을 통해 목적에 맞는 네트워크 분리를 통해 접근통제를 적용할 수 있으며, 정책 및 로그 관리 측면에서 높은 편의성과 효율성을 제공합니다. 또한 Security Groups이나 Network ACL에 비해 관리성이 우수합니다. 아울러 인터넷 환경에서는 사이트 간 암호화된 터널을 통해 안전한 가상 사설 네트워크(VPN)를 제공할 수 있습니다.

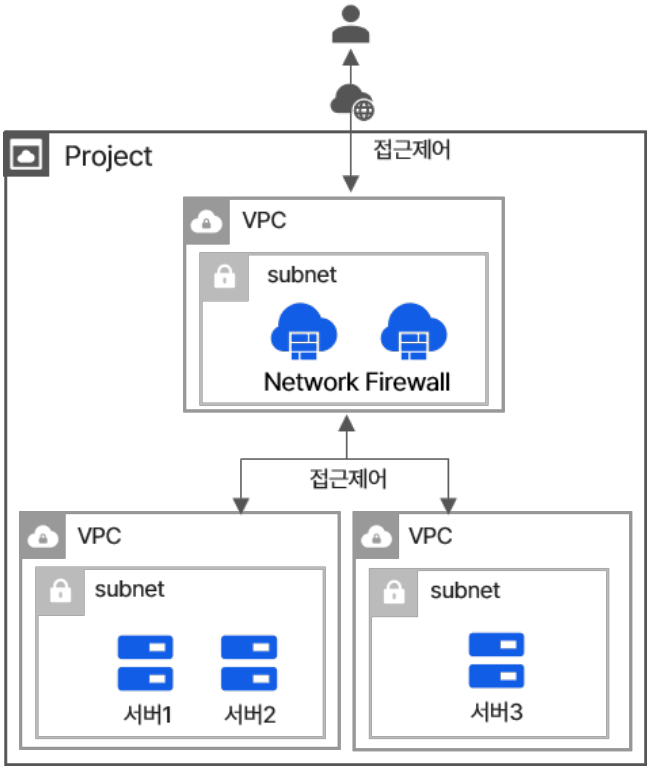


그림 24 Network Firewall

5.3.2 가상 사설망 연결(구간 보안)

NHN Cloud Network Firewall

Network Firewall은 방화벽 기능뿐만 아니라 인터넷 환경에서 사이트 간 암호화된 터널을 통해 안전한 가상 사설 네트워크(VPN) 기능을 제공합니다.

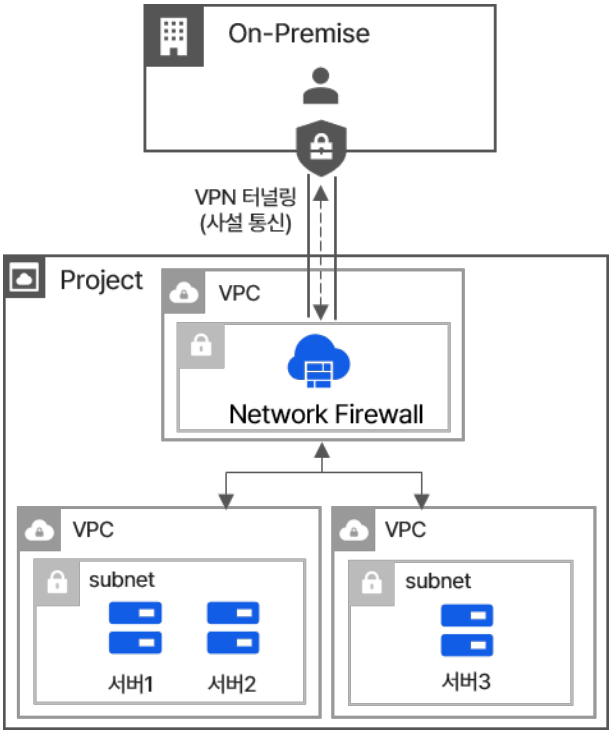


그림 25 Network Firewall - 가상 사설 네트워크(VPN) 기능

NHN Cloud Cloud Access

제로 트러스트 보안 모델에 기반한 전용 에이전트는 사용자 디바이스(IP 주소, MAC 주소, OS, 프로세스, 레지스트리, 백신 등)를 지속적으로 검증하여 보안을 강화합니다. 아울러 사용자가 별도의 복잡한 설정 없이도 리소스에 안전하게 접근할 수 있도록 편의성을 제공합니다.

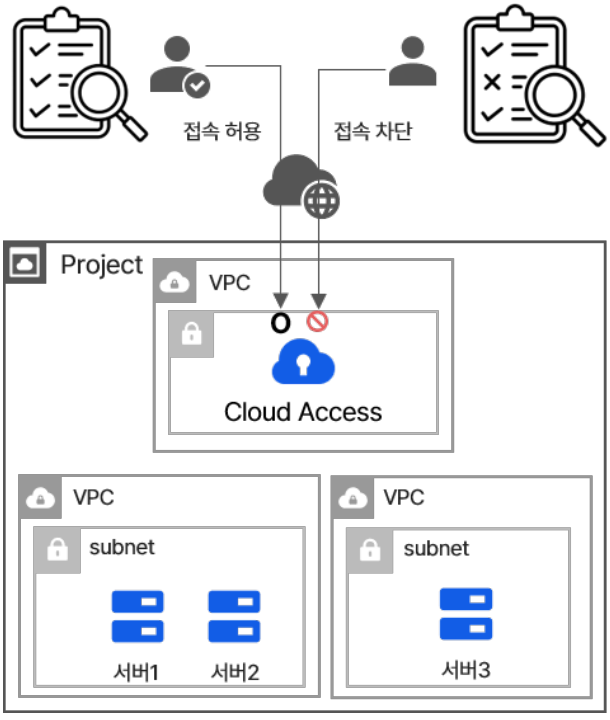


그림 26 Cloud Access

IPSec VPN

국정원 CC인증을 받은 IPSec VPN 어플라이언스를 기반으로, IPSec 방식의 암호화된 터널링 VPN 서비스를 제공합니다.

5.3.3 DDoS 공격 대응

NHN Cloud DDoS Guard

DDoS Guard 서비스는 NHN Cloud의 관문에 구성되어 DDoS 공격에 대응하는 서비스입니다. 유료 서비스에는 모니터링, DDoS 공격 시 초동 대응이 포함되며 DDoS 모의 훈련 지원과 일간/월간 트래픽 현황과 분석, 이벤트 탐지 현황, 대응 내 용에 대한 리포트를 받을 수 있습니다.

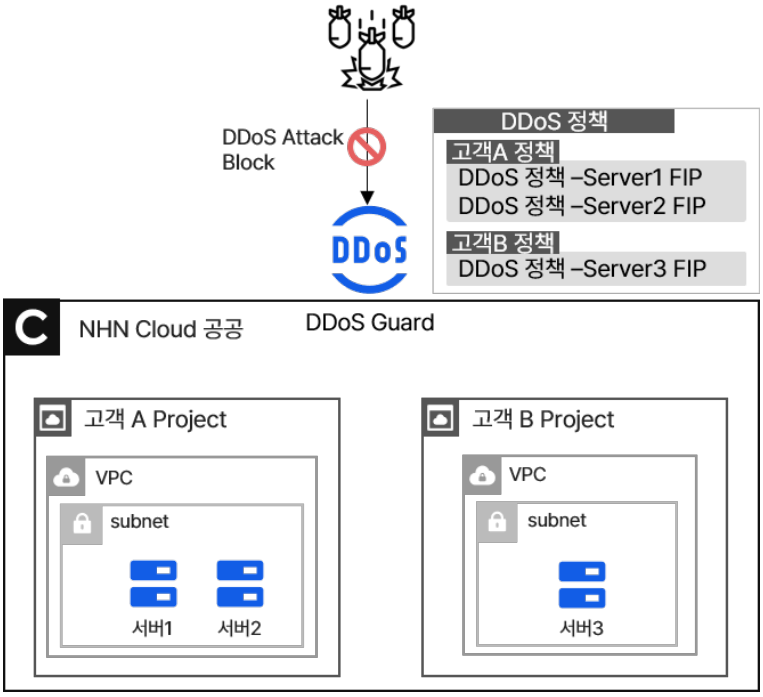


그림 27 DDoS Guard

5.3.4 침입 탐지 및 차단

NHN Cloud Security Monitoring

고객의 테넌트에 별도의 프로그램 설치 없이 NHN Cloud에서 수년간 축적 및 검증된 IDS/SIEM 패턴 및 위협 관리 대응 체계를 기반으로 위협을 탐지합니다. 침해 사고 발생 위험도에 따라 이벤트 수신 설정이 되어 있는 경우 긴급 유선 연락이나 업무 처리 내역 메일을 수신할 수 있습니다.

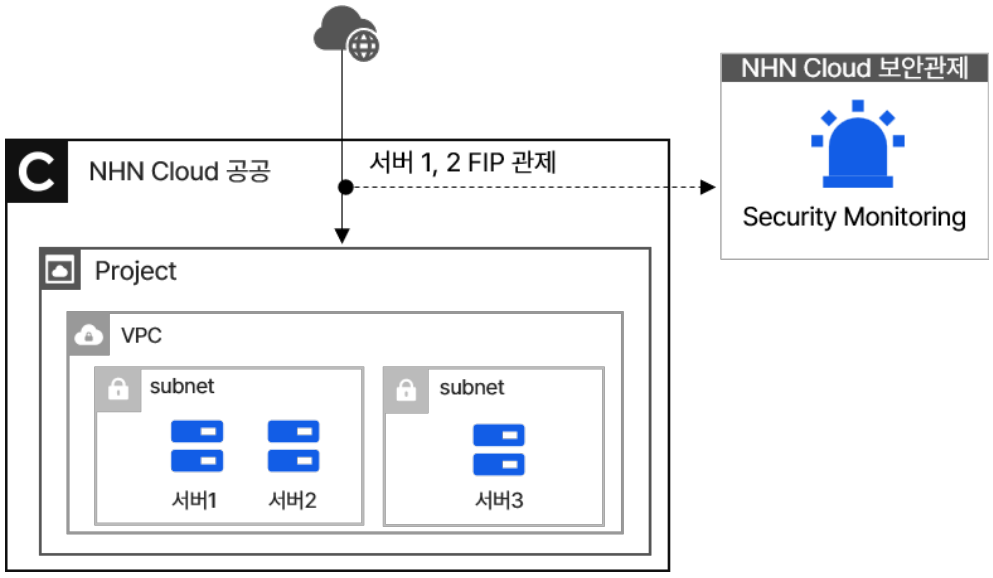


그림 28 Security Monitoring

마켓플레이스

마켓플레이스에서 제공되는 보안 솔루션을 활용해 고객 테넌트 환경에서 위협을 탐지하거나 차단할 수 있습니다. 호스트 레벨에서는 에이전트를 서버 인스턴스에 설치하여 침입을 탐지할 수 있으며, 가상 어플라이언스 형태의 솔루션을 통해서도 위협 대응이 가능합니다. 또한 NHN Cloud의 Traffic Mirroring 기능을 이용하면 인스턴스 네트워크 인터페이스의 트래픽을 모니터링하여 위협 탐지 구성을 할 수 있습니다.

5.3.5 웹 서버 위협 방어

NHN Cloud WEB Firewall

WEB Firewall 서비스를 이용하여 웹 서버를 보호할 수 있습니다. 웹 서버(인스턴스 또는 컨테이너)의 앞 단에 구성되며 HTTP, HTTPS 트래픽을 필터링하고 정책에 따라 악의적인 웹 공격을 탐지 또는 차단합니다.

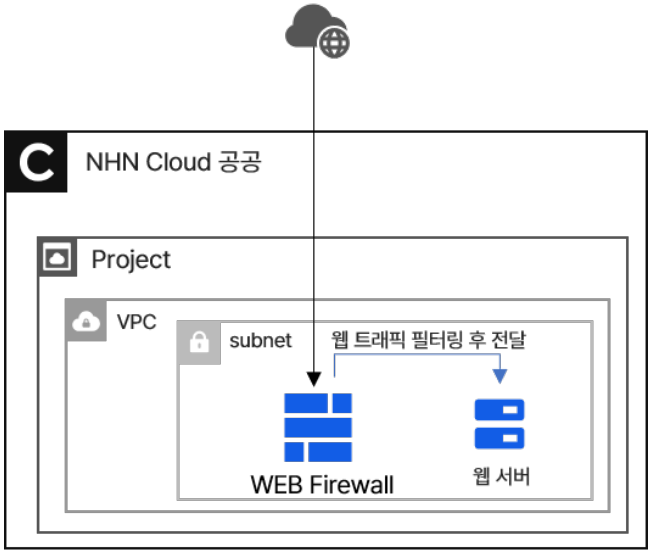


그림 29 프락시 방식의 WEB Firewall 구성 예시

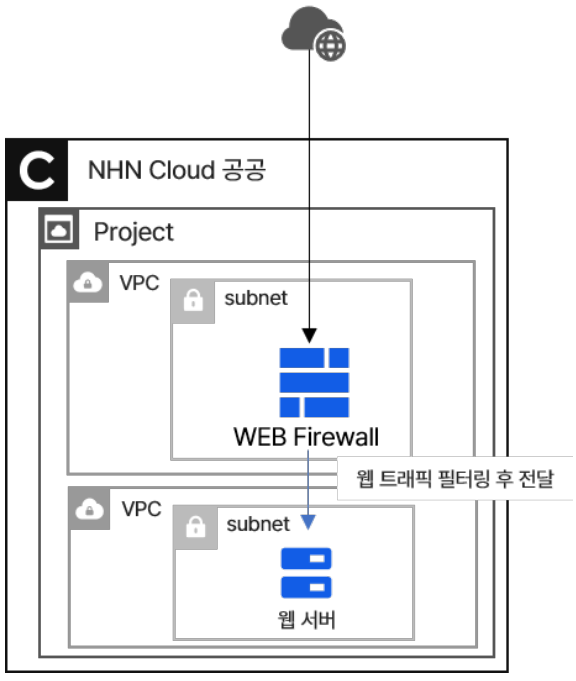


그림 30 인라인 방식의 WEB Firewall 구성 예시

5.3.6 SSL 가시화

마켓플레이스

3rd party 솔루션을 고객의 테넌트에 가상 인스턴스 형태로 설치하여 암호화된 패킷을 복호화할 수 있습니다. SSL로 암호화된 패킷을 복호화하여 고객 테넌트에 설치된 네트워크 위협 분석 센서로 전달하거나 동시에 다른 조직(프로젝트)에 구성되 어 있는 분석 센서로도 복호화된 패킷을 전달할 수 있습니다.

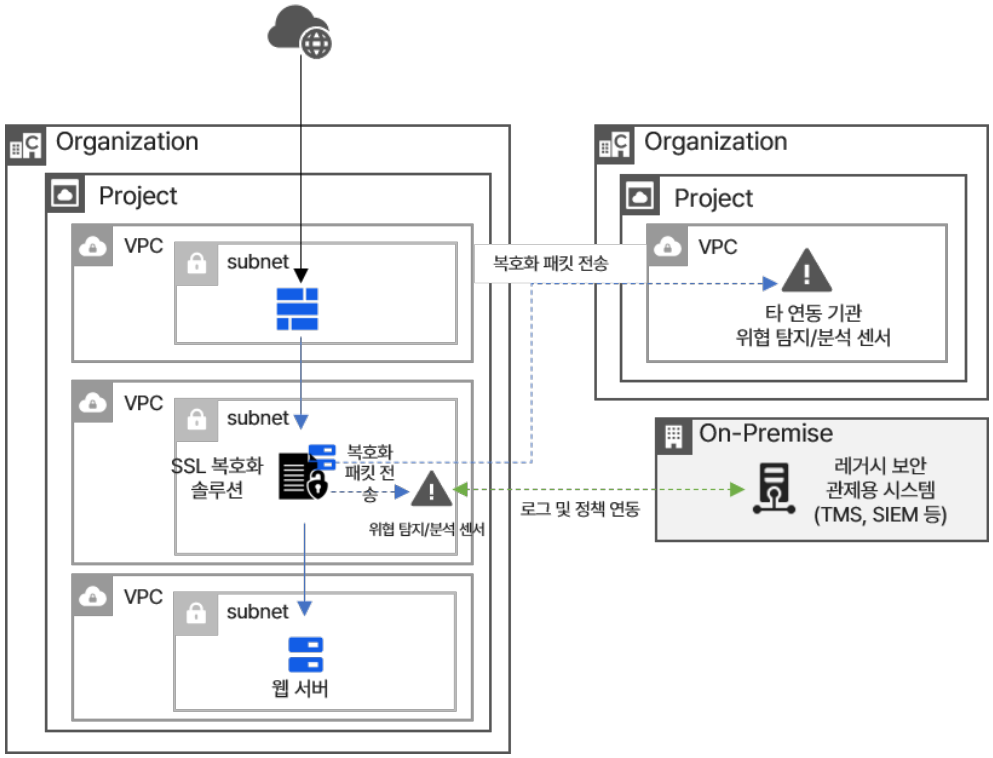


그림 31 암호화된 패킷 복호화

5.4 시스템 및 데이터 보안

5.4.1 서버 접근제어 및 계정 관리

클라우드 환경에서는 다중 인증(MFA)과 안전한 인증 프로토콜을 사용하여 계정 도용 위험을 최소화해야 합니다. 이러한 원칙은 콘솔 접속뿐만 아니라 OS 계정 인증에도 동일하게 적용되며, 계정과 인증 수단은 개인별로 발급, 관리하고 공유를 금지해야 합니다. 권한은 최소한으로 부여하고 주기적으로 점검하여 불필요한 권한은 회수해야 합니다.

또한 클라우드 서버 접근 시 사용하는 PEM 키는 안전한 저장소에 보관하고, 파일 접근 권한을 소유자만 읽기가 가능하도록 제한해야 합니다. PEM 키는 개인별로 관리하며 공유를 금지하고, 안전하지 않은 채널을 통한 전송은 피해야 합니다. 더불어 주기적인 교체와 로그 관리로 보안성을 강화해야 합니다.

NHN Cloud NHN Bastion

NHN Bastion은 시스템 접근통제와 실시간 세션 관리 기능을 제공하며, IP 기반으로 접근 대상 자원을 등록할 수 있습니다. 또한 별도의 터미널 프로그램 없이 웹 브라우저를 통해 원격 접속할 수 있어 별도의 터미널 프로그램을 관리하지 않아도 되어 편리합니다. 접근 대상 인스턴스의 생성, 삭제 및 오토스케일링 인/아웃에도 민첩하게 대응할 수 있습니다. 일회성으로 발급되는 임시 SSH 키를 통해 인증이 되어 별도의 키 관리가 불필요하고, 기록된 모든 접근 로그와 명령어 로그는 암호화되어 안전하게 관리됩니다.

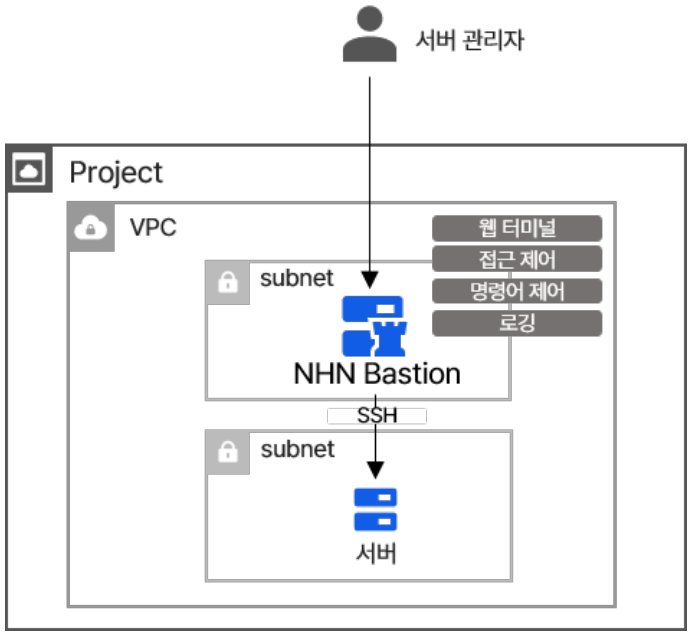
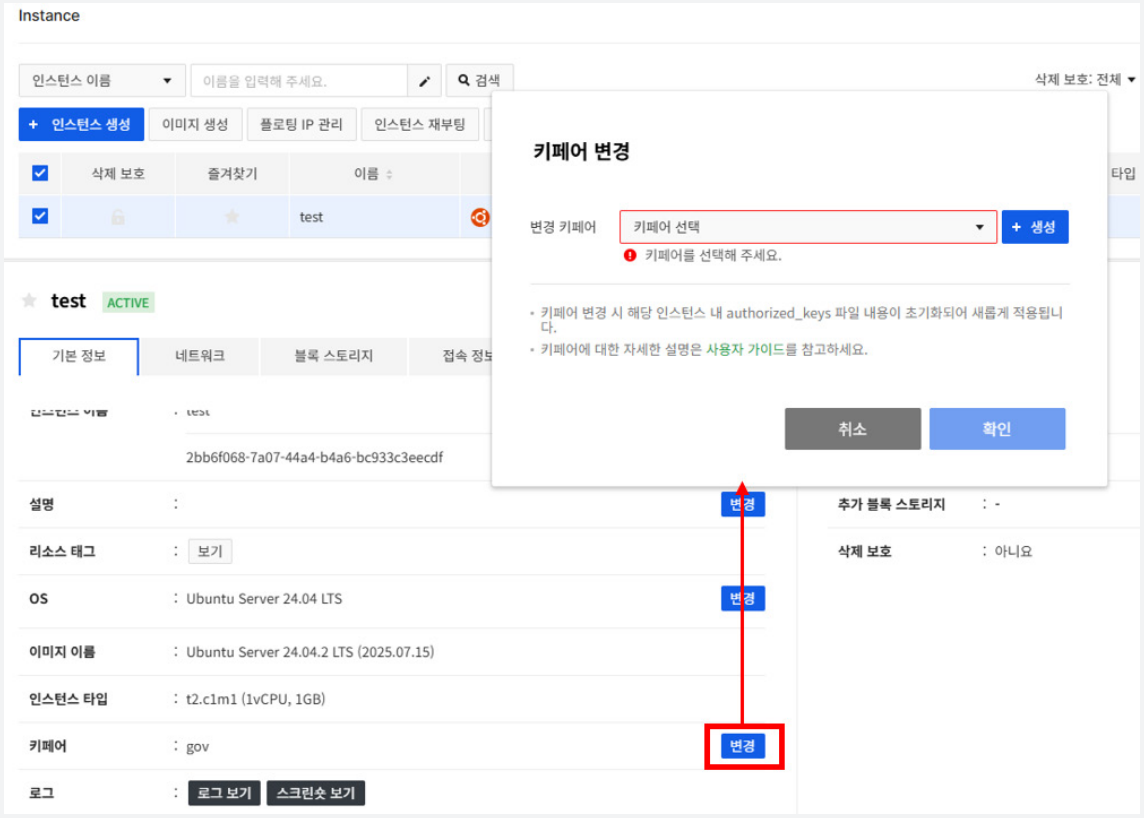


그림 32 NHN Bastion

※ PEM키 교체 방법

PEM가 분실 또는 유출되었을 경우 즉시 변경합니다. 생성된 인스턴스를 클릭하면 아래 그림과 같이 **키페어 변경** 메뉴를 통해 인스턴스 로그인할 수 있는 키를 변경할 수 있습니다.



5.4.2 DB 접근제어/계정 관리

클라우드 환경에서는 다중 인증(MFA)과 안전한 인증 프로토콜을 사용하여 계정 도용 위험을 최소화해야 합니다. 이러한 원칙은 콘솔 접속뿐만 아니라 OS 계정 인증에도 동일하게 적용되며, 계정과 인증 수단은 개인별로 발급, 관리하고 공유를 금지해야 합니다. 권한은 최소한으로 부여하고 주기적으로 점검하여 불필요한 권한은 회수해야 합니다.

NHN Cloud

RDS에서 제공하는 DB 보안 그룹을 활용하여 DB 인스턴스의 송수신 트래픽을 제어하여 DB 인스턴스를 보호할 수 있습니다. DB 보안 그룹은 RDS별로 DB 보안 그룹 기능을 개별로 제공하고 있으며 서비스 내 메뉴를 통해 기능을 적용할 수 있습니다. 인스턴스 형태로 생성한 DB인 경우 인스턴스에 적용되는 Security Groups(보안 그룹)을 통해 접근제어가 가능합니다.

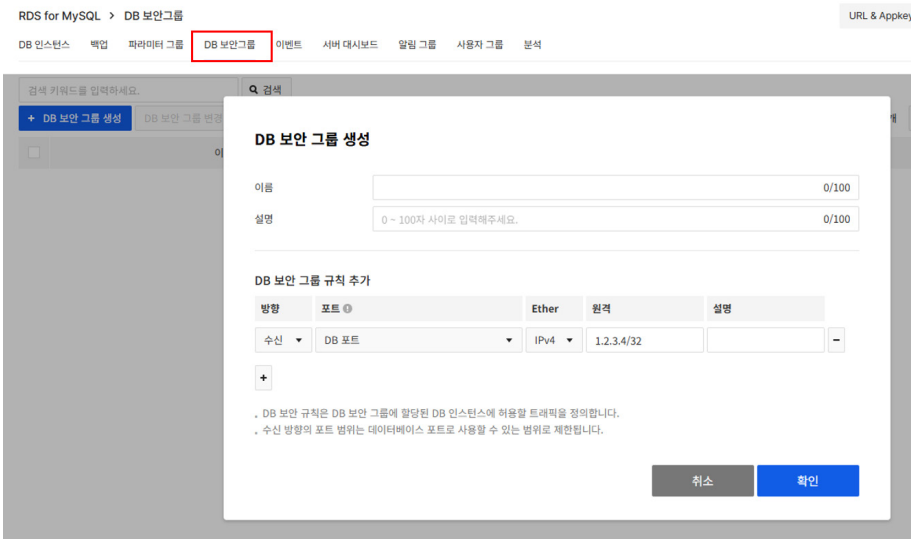


그림 33 RDS for MySQL DB 보안 그룹 화면 예시

마켓플레이스

마켓플레이스 상품 중 DB 접근제어 솔루션은 DB로의 접근을 게이트웨이 방식 등으로 통제하여, 적절한 권한을 부여함으로써 비인가자의 불법 접근을 차단합니다. 구축 전에 DB 종류, 계정 프로비저닝 등 사전 설계를 수행하고, 저장된 데이터의 성격에 맞는 권한을 부여하도록 합니다. 또한 솔루션을 통해 접근 로그, 권한 부여 로그, 명령어 실행 로그 등을 기록하고 관리할 수 있습니다.

5.4.3 스토리지 접근 관리

클라우드 스토리지는 중요한 데이터가 저장되는 핵심 자원이므로 접근 관리가 필수적입니다. 권한이 없는 사용자가 데이터를 열람, 수정, 삭제하는 것을 방지하기 위해 접근제어를 적용해야 합니다. 스토리지별로 역할 기반 권한을 부여하고 최소 권한 원칙을 준수해야 합니다. 또한 접근 기록을 로깅하고 주기적으로 점검하여 비정상적인 접근 시 신속히 대응할 수 있어야 합니다. 이를 통해 데이터 유출 및 무단 변경 위험을 효과적으로 감소시킬 수 있습니다.

NHN Cloud Object Storage 접근 정책

외부 공개가 불필요한 오브젝트 스토리지는 Private 설정을 통해 외부 접근을 차단할 수 있습니다. Private 설정은 컨테이너가 속한 프로젝트의 사용자에게만 접근 권한을 부여하는 기본 접근 정책입니다.

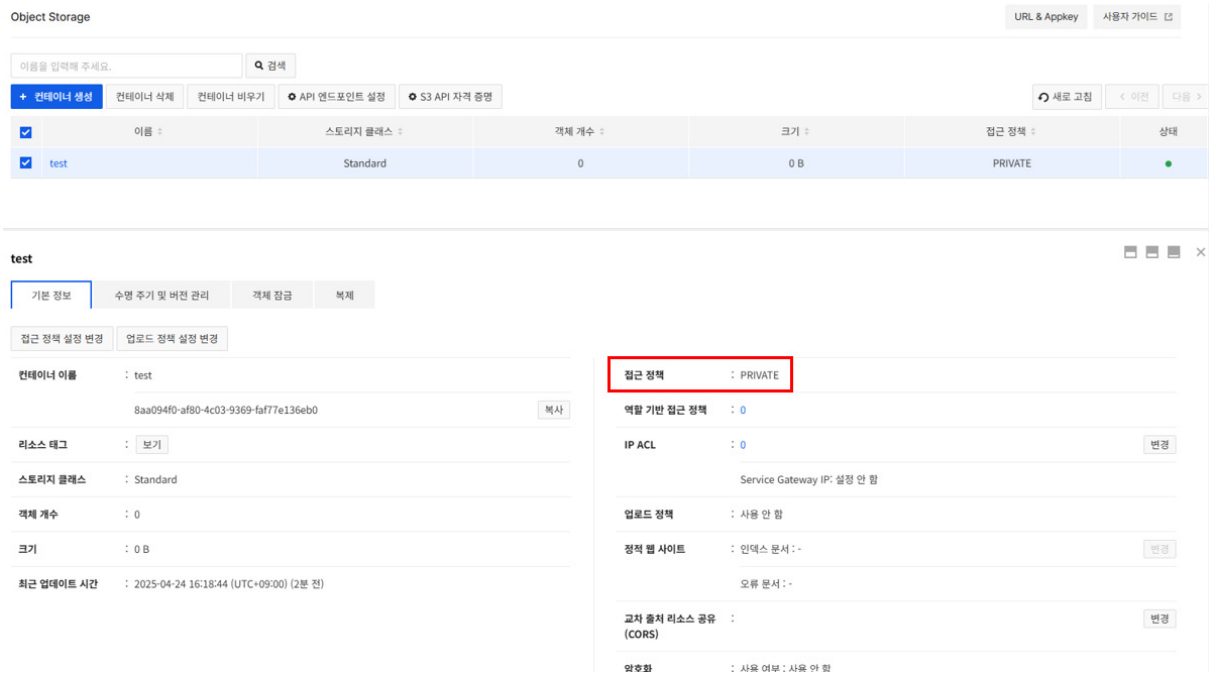


그림 34 Object Storage 접근 정책 화면 예시

화이트리스트 또는 블랙리스트 기반의 세부적인 IP 접근제어와 권한 설정이 가능하며 Service Gateway를 통해 접근하는 것에 대해 Read/Write 권한 설정이 가능합니다.

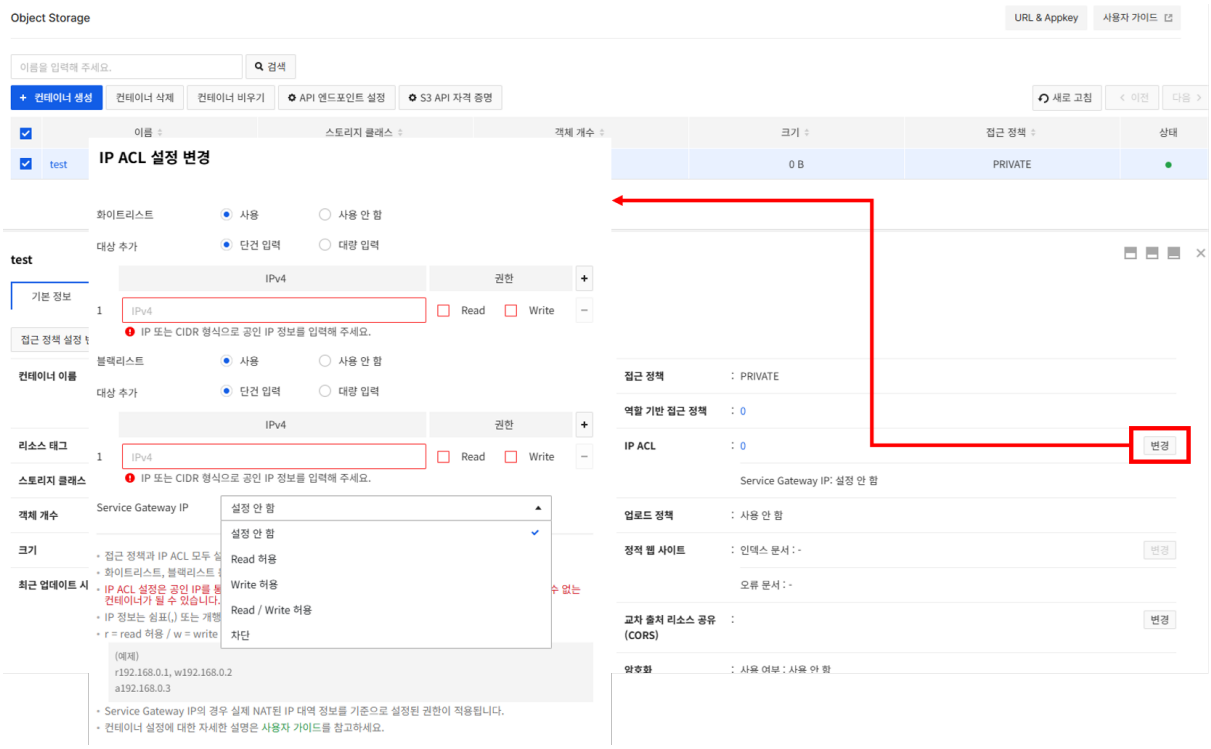


그림 35 Object Storage 접근 정책 화면 예시

클라우드 콘솔에서 역할 기반 접근 정책 설정을 통해 접근을 허용할 테넌트 및 API 사용자 ID를 설정하여 접근 권한을 설정할 수 있습니다.

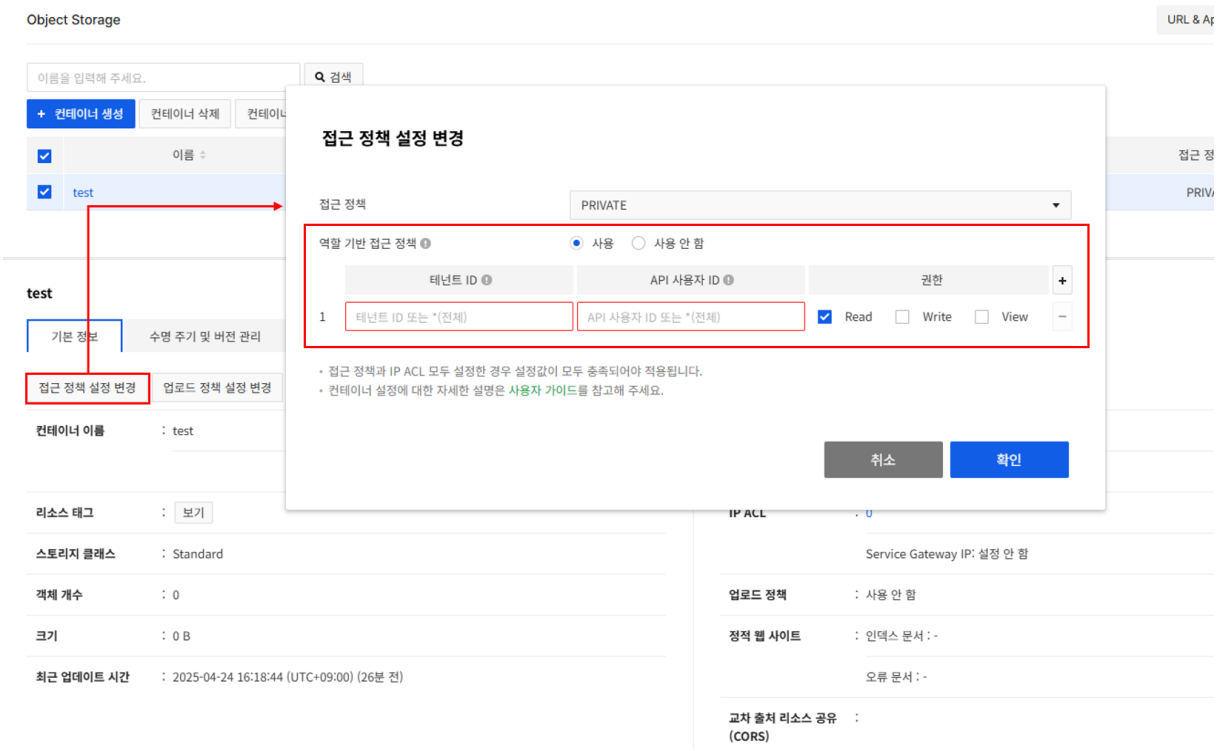


그림 36 Object Storage 접근 정책 화면 예시

5.4.4 백신

NHN Cloud Vaccine

인스턴스에 설치된 백신은 실시간으로 파일과 프로세스를 모니터링하며, 의심스러운 활동이 감지되면 자동으로 격리하거나 차단합니다. 또한 정기적인 시그니처 업데이트를 통해 최신 악성코드로부터 서버를 보호합니다.

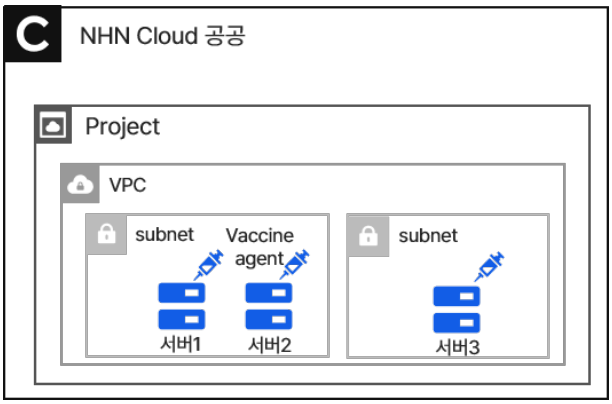


그림 37 Vaccine

5.4.5 암호화

중요 데이터는 암호화를 통해 안전하게 보관해야 합니다. 암호화 알고리즘 선택, 키 관리 등 암호화를 적용하기 위한 절차 및 관리 또한 중요합니다. 특히 암호화 키는 생성부터 폐기까지 전 주기(lifecycle)에 걸쳐 관리되어야 하며, 무단 접근·변조·유출을 방지하기 위해 승인된 보안 절차와 도구를 사용해야 합니다.
아래는 키 보안 절차의 예시입니다.

표 5-1 암호화 키 보안 절차 예시

단계	주요 내용

키 생성	• 안전한 암호 키 생성 방안 마련 및 절차 수립과 생성
	  • 키 길이 및 알고리즘 정보, 생성 일자 등의 절차 수립
	  • 중요도 및 사용 목적에 따라 다음과 같이 구분

키 저장 및 백업	• 마스터 키 등은 물리적으로 분리된 별도 서버에 백업 및 보관 • 암호 키 접근에 최소 접근 권한을 부여
키 배포	안전한 채널을 통해서만 배포
키 사용	키는 지정된 목적으로만 사용하고 애플리케이션 또는 사용자 계정별로 권한 분리 적용
키 교체 및 폐기	• 정기적인 키 교체 • 불필요하거나 유효기간 만료된 키는 폐기
모니터링 및 감사	• 키 접근, 교체, 폐기 등 모든 활동을 로그로 기록하고 정기적으로 점검

NHN Cloud Secure Key Manager

기밀 데이터(데이터베이스 접속 정보, 앱키, 비밀번호 등), 대칭 키, 비대칭 키와 같이 애플리케이션 서버에 저장할 경우 보안 위험에 노출될 수 있는 데이터를 중앙 집중적으로 안전하게 관리하고, 인증을 통과한 클라이언트만 접근할 수 있게 제어하는 서비스입니다. 대칭 키를 생성하고 관리할 수 있으며 API를 사용해서 대칭 키로 데이터를 암/복호화할 수 있습니다.

마켓플레이스

암호화 방식에는 여러 가지가 있으며, 각각 장단점이 있습니다. API 방식은 애플리케이션 수준에서 유연하게 적용할 수 있지만 개발과 운영 부담이 있고, 커널 방식은 운영체제 수준에서 성능 저하 없이 투명하게 암호화할 수 있으나 특정 OS에 종속될 수 있습니다. 플러그인 방식은 DB나 스토리지에 직접 통합되어 쉽게 적용되지만, 지원되는 시스템이 제한적입니다.
마켓플레이스에서 제공되는 암호화 솔루션을 활용하면 이러한 방식 중 환경과 목적에 맞는 암호화를 선택하여 데이터를 안전하게 보관할 수 있습니다. 구축 전에는 데이터의 특성과 운영 환경을 고려하여 최적의 암호화 방식을 적용하는 것이 중요합니다.

5.4.6 취약점 관리

취약점 관리는 시스템, 애플리케이션, 네트워크 등 IT 자산에 존재하는 보안 약점을 식별, 평가, 우선순위 지정, 조치하는 일련의 과정을 의미합니다. 클라우드 환경과 온프레미스를 포함한 모든 IT 인프라에서 취약점 관리는 보안 사고 예방과 규제 준수를 위해 필수적인 보안 활동입니다. 효과적인 취약점 관리를 위해 조직은 정기적인 취약점 스캐닝과 평가를 수행해야 하며, 발견된 취약점에 대해 심각도 수준(critical, high, medium, low)에 따라 우선순위를 정하고 신속하게 대응해야 합니다.

표 5-2 취약점 관리 대상 예시

관리 대상	관리 항목	관리 방법
가상 서버(인스턴스)	OS, 미들웨어 등	• 정기적인 패치 적용 • 불필요 서비스 제거 • 보안 설정 점검 • 최신 버전 적용, 계정 점검 등
네트워크	VPC, 서브넷, 보안 그룹, 라우팅	• 포트 및 접근제어 점검 • 보안 그룹/방화벽 규칙 확인
애플리케이션	웹, 모바일 앱 등	• 코드 취약점 점검 • 정기 보안 테스트 • 애플리케이션 패치 적용
데이터베이스(DB)	클라우드 DB 인스턴스, 계정 및 권한 등	• 계정·권한 점검 • 접근제어 강화 • 보안 패치 적용
컨테이너	컨테이너 노드, 이미지 등	• 컨테이너 노드 취약점 점건 • 이미지 취약점 스캔 및 레지스트리 관리 등

표 5-3 취약점 분류 체계 및 조치를 위한 참고 기관

구분	항목	내용
취약점 분류	CVE	공개된 소프트웨어/하드웨어에서 발견된 취약점에 고유 번호를 부여하는 체계
	NVD	CVE를 기반으로 심각도(CVSS 점수), 영향도, 패치 정보 등을 추가해 제공하는 공식 취약점 데이터베이스
	CWE	보안 취약점의 원인이 되는 약점을 분류 및 정리한 목록
	CCE	시스템 보안 설정의 취약점을 식별하는 체계
	CVSS	취약점의 심각도를 0~10점 사이의 점수로 정량화 하는 체계. 공격 용이성, 영향 등을 고려해 취약점 패치의 우선순위를 결정하는 데 사용
	OWASP Top 10	웹 애플리케이션 보안 위험 10가지를 정리한 목록. 실제 공격에 자주 악용되는 취약점 유형을 우선순위로 제시하여 개발자에게 가이드라인을 제공

조치/진단 가이드 등	한국인터넷진흥원(KISA)	인터넷 침해 사고 경보 발령, 보안 취약점 정보 및 패치 권고, 주요 정보통신 기반 시설에 대한 기술 가이드 제공
	NIST (미국 국립표준기술연구소)	NVD(국가 취약점 데이터베이스)를 통해 CVE 취약점 상세 정보 및 조치 권고 제공
	MITRE Corporation	CVE, CWE, ATT&CK 등 보안 표준을 개발하고 관리하며, 이를 통해 위협 분석 및 대응 전략 수립을 위한 기반 정보 제공
	OWASP (open worldwide application security project)	OWASP Top 10을 비롯해 웹 애플리케이션 취약점에 대한 상세 분석 자료와 안전한 코딩 가이드를 제공
	CIS Benchmark	CIS 벤치마크를 통해 운영체제, 서버, 클라우드, 컨테이너 등 다양한 시스템에 대한 구체적인 보안 설정 가이드 제공

NHN Cloud Server Security Check

인스턴스 OS의 취약점을 점검하고 발견된 취약점에 대한 대응 방법을 제공합니다. 점검 가능한 OS는 Rocky Linux와 Ubuntu Linux 이며 주요정보통신기반시설, 전자금융기반시설 보안 기준의 점검 항목을 선택하여 점검할 수 있습니다.

5.4.7 API 보안

클라우드 환경에서는 다양한 서비스와 애플리케이션이 API(Application programming interface)를 통해 상호 연동되므로, API는 중요한 보안 경계가 됩니다. 따라서 API 보안은 데이터 유출, 무단 접근, 서비스 오용 등 다양한 위협으로부터 시스템을 보호하기 위해 필수적으로 관리되어야 합니다. API 접근 시 사용자와 시스템을 식별할 수 있는 인증 체계를 적용하고 API 요청과 응답에 포함된 민감 데이터는 전송 중 암호화(TLS/HTTPS)를 적용하여 네트워크 상에서 유출되지 않도록 보호해야 합니다.

NHN Cloud 퍼블릭 API 보안

NHN Cloud API는 기본적으로 SSL을 적용하여 안전한 통신을 보장합니다.
모든 API 호출 시에는 인증 절차가 필요합니다. 해당 토큰은 일정 기간 동안만 유효하며, 보안 강화를 위해 주기적인 갱신 및 안전한 보관이 권장됩니다. 토큰 발급을 위해서는 User Access Key ID와 Secret Access Key 등이 필요하며 NHN Cloud 계정의 **API 보안 설정** 메뉴를 통해 발급할 수 있습니다. 서비스마다 API 호출 및 인증 방식이 다르므로 개별 서비스의 API 사용 방식은 NHN Cloud 사용자 가이드를 참고하세요.
API 인증 시 사용되는 User Access Key 생성 시 토큰 유효 시간을 설정하여 보안성을 강화할 수 있습니다.



그림 38 User Access Key 생성 화면

그리고 콘솔 접근제어에서 안내한 조직 거버넌스 설정의 IP ACL은 API 접근에도 적용됩니다.

마켓플레이스

API 기반 서비스 연동이 활발해짐에 따라, 요청 형식 검증 및 정책 기반 제어를 통해 API를 악용한 위협을 방지 및 차단할 필요가 있습니다. 이를 위해 API Gateway나 WAF와 같은 보안 솔루션을 도입하여 API 요청 무결성 검증, 인증·인가 강화, 비정상 트래픽 차단 기능을 활용함으로써 다양한 API 공격에 효과적으로 대응할 수 있습니다.
상품을 제공하는 벤더사의 제품마다 기능, 구성 방법이 상이할 수 있으므로 아래 구성은 참고로만 활용하세요.

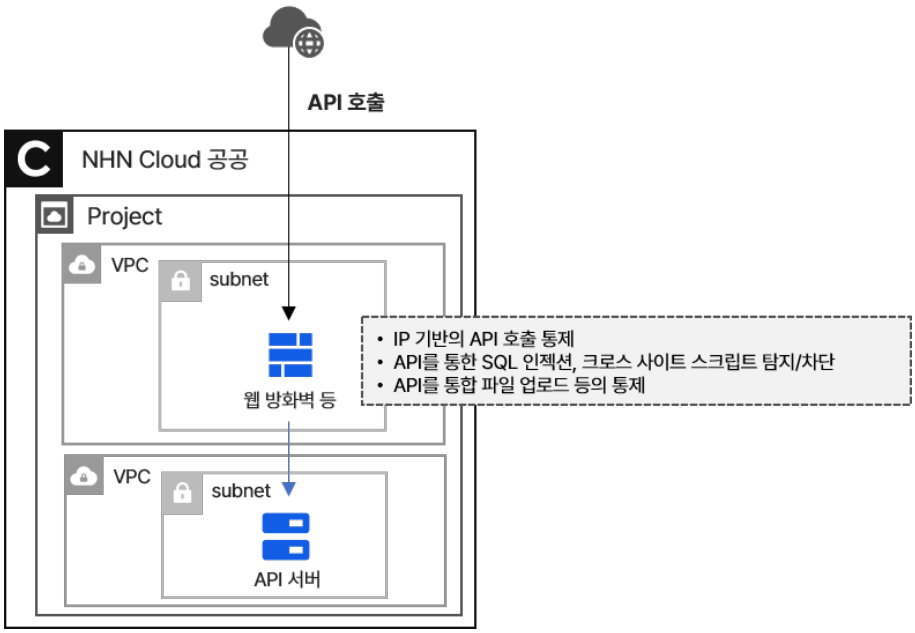


그림 39 API 통제 구성 예시

5.5 관제, 모니터링 및 로그 관리

5.5.1 로그 관리

NHN Cloud CloudTrail

콘솔과 API에서 발생하는 다양한 활동 로그와 이벤트를 수집하는 서비스입니다. 리소스 정보와 작업 요청 출처 등 상세한 정보를 확인할 수 있으며, 계정 활동(IAM 계정 포함)과 관련된 주요 내역을 기록하여 최근 90일간의 로그를 조회할 수 있습니다. 90일을 초과하는 로그를 보관 및 관리하려면 Object Storage를 활용해 로그를 다운로드하여 장기 보관할 수 있습니다.
로그의 무결성 관리를 위해 Object Storage 내 로그들이 임의로 수정 또는 삭제될 때 알림 기능을 통해 이메일로 알림을 받도록 설정할 수 있습니다. 외부 로그 변조 알림은 NHN Cloud Object Storage를 사용하는 경우 제공되는 기능이며 메일은 0분/30분 단위로 발송됩니다.

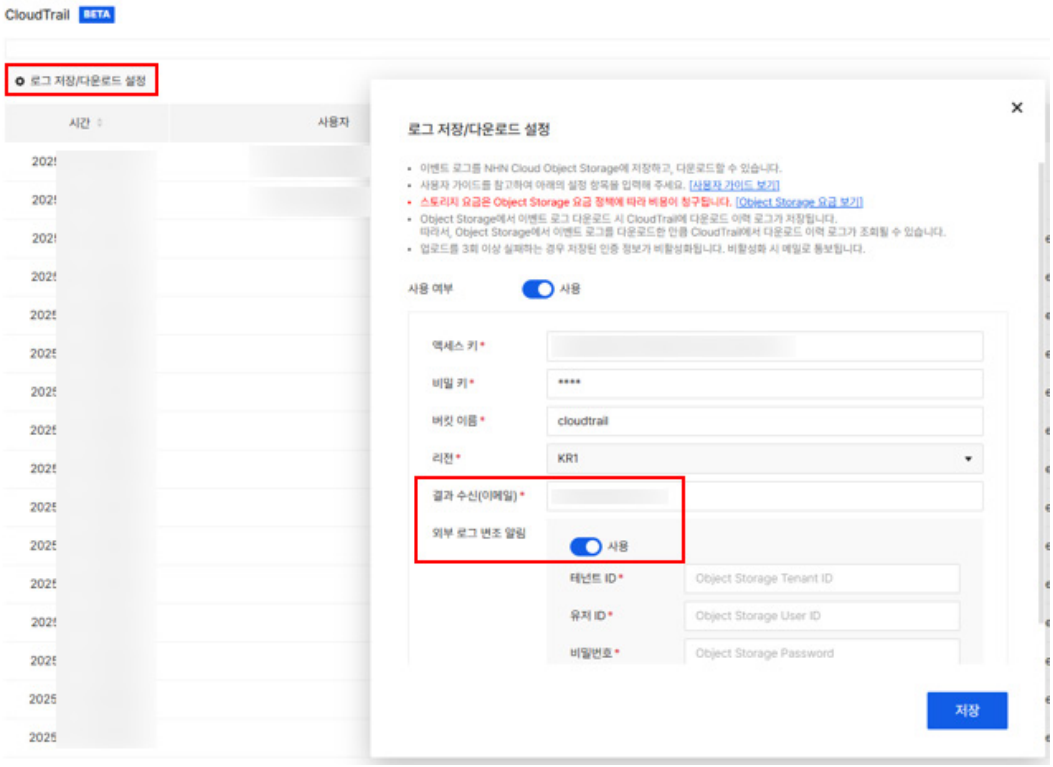


그림 40 CloudTrail 외부 로그 변조 기능

NHN Cloud SIEM

다양한 IT 시스템과 보안 장비에서 발생하는 로그를 통합 관리하고, 이를 기반으로 보안 이벤트 및 페이로드 분석을 수행하여 위협을 식별 및 대응하는 서비스입니다. 로그 통합 관리를 통해 이기종 시스템에서 발생하는 정보를 일원화하여 관리할 수 있으며, 보안 이벤트 및 페이로드 분석을 통해 단순한 알림을 넘어 위협의 맥락과 심각성을 파악할 수 있습니다. 또한 실시간 상관 분석 기능을 통해 개별적으로는 정상으로 보일 수 있는 행위들을 연계 분석함으로써 잠재적인 공격 시나리오를 신속히 탐지할 수 있습니다.

마켓플레이스

로그의 보관과 관리체계는 모든 보안 솔루션 운영에서 기본적이면서도 매우 중요한 요소입니다. 특히 로그 무결성이 보장되도록 안전하게 저장하고 관리하는 것이 필수적입니다. 가능하다면 개별 솔루션에서 발생하는 로그를 통합 관리할 수 있는 환경이 마련되면 더욱 효율적이며, 여건상 어려운 경우 각 솔루션이 제공하는 로그 관리 및 저장 기능을 적극 활용해야 합니다. 로그 관리 활동은 컴플라이언스 준수 요구 사항일 뿐 아니라, 사고 발생 시 책임 추적성과 원인 분석을 가능하게 하는 핵심 수

단입니다. 따라서 로그는 단순 기록이 아닌 보안 운영의 근간으로 인식하고 체계적으로 관리해야 합니다.

5.5.2 관제 및 모니터링

모니터링 및 관제는 보안 위협을 조기에 탐지하고 신속히 대응하기 위한 핵심 활동입니다. 로그와 이벤트를 지속적으로 수집·분석하여 이상 징후를 식별하고, 보안 사고 발생 시 신속한 경보와 대응 체계를 마련해야 합니다. 또한 관제 활동은 단순 탐지에 그치지 않고, 위협 분석과 사후 개선으로 이어져야 합니다.

공공기관은 국정원 보안 관제 요건(고객별 패턴 운영, 탐지 이벤트 센터 전송, SSL 가시화 등)을 충족하기 위해서는 기관별 특성을 반영한 맞춤형 보안 관제가 필요합니다.
특히 기관 간 가상 영역에서 발생할 수 있는 위협 확산과 전이 가능성을 최소화하기 위해서는 네트워크 기반 보안 관제 체계가 효과적입니다. NHN Cloud는 다양한 벤더의 네트워크 보안 장비를 유연하게 배치할 수 있는 가상화 네트워크 환경을 제공하여 이러한 요구를 지원합니다.
아울러 호스트 기반 보안 관제만으로는 최신 위협 대응에 한계가 있으므로, EDR 등 차세대 보안 도구와의 연계를 통해 고도화된 보안 관제 아키텍처를 구축하는 것이 고객 보안 수준을 한층 강화하는 핵심 전략이 될 수 있습니다.

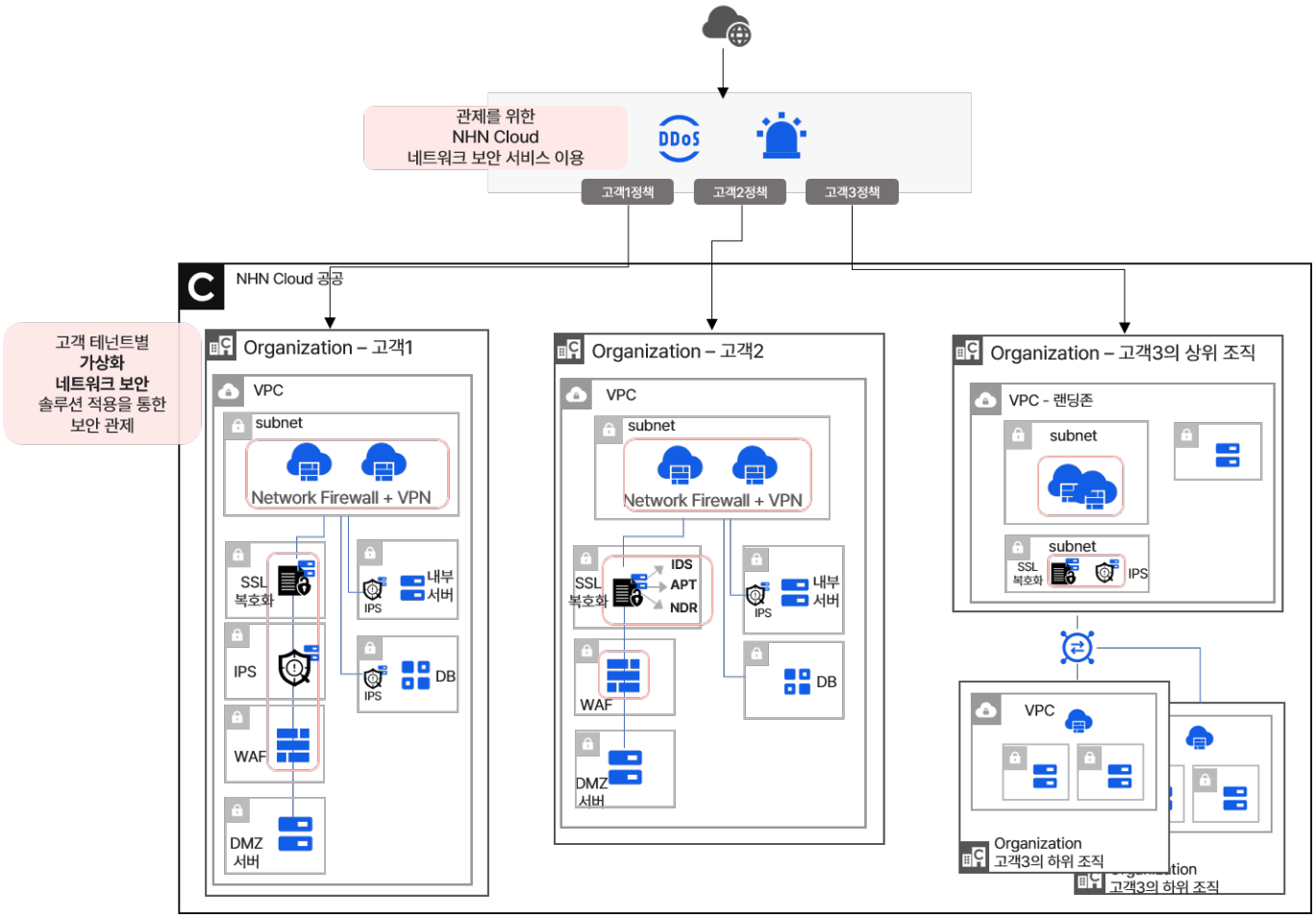


그림 41 관제를 위한 네트워크 보안 서비스 배치 예시

NHN Cloud Security Monitoring

5.3.4에서 소개한 것과 같이 Security Monitoring 서비스는 24시간, 365일 보안 관제 지원 및 고도화된 IDS/SIEM 연관성 탐지 패턴을 운용하고 이벤트 데이터와 패킷 덤프를 확인해 깊이 있는 분석 업무를 수행하여 침입을 분석합니다. 침해 사고 발생 시 전파 및 네트워크 수준의 침해 경로, 취약점 정보를 제공하고 후속 대응 업무를 통해 사고 분석을 지원합니다.
콘솔을 통해 상세 이벤트 및 보안 관제 대응 현황도 확인할 수 있습니다.

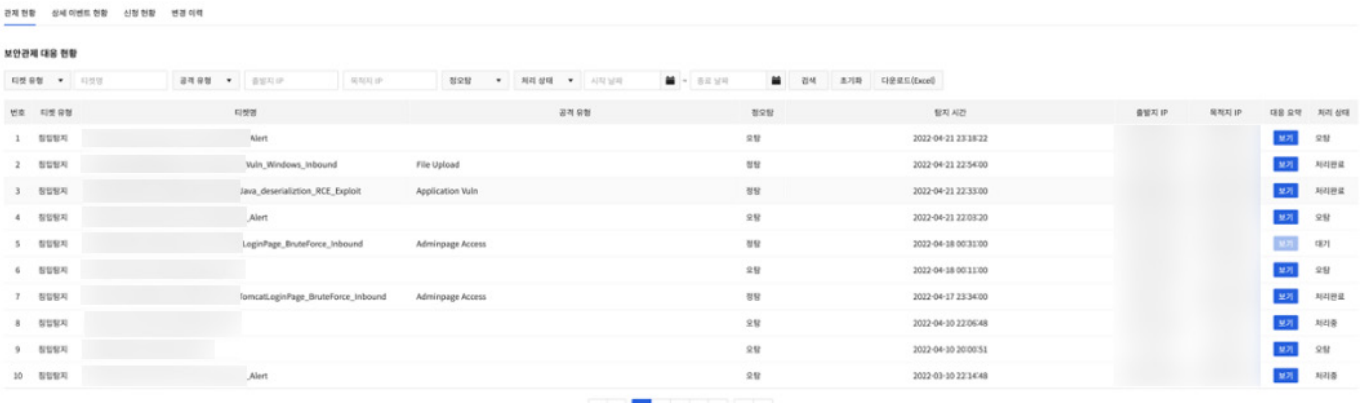


그림 42 관제 현황 콘솔 화면 예시

NHN Cloud 보안 관제 서비스

NHN Cloud **보안 관제 서비스**는 사이버 공격으로부터 고객사의 정보 자산을 보호하기 위해 보안 이벤트와 로그를 비롯한 다양한 데이터를 분석하여, 연중무휴(24x365) 실시간으로 위협을 탐지하고 대응합니다. 이를 통해 관제 대상 기관은 보안 운영 부담을 줄이고 핵심 업무에 집중할 수 있으며, NHN Cloud의 축적된 운영 경험과 전문 역량을 바탕으로 안정적인 보안 관제 서비스를 제공받을 수 있습니다. 또한 고객사의 환경과 요구 사항에 따라 원격, 하이브리드, 파견 형태 등 다양한 보안 관제 방식을 유연하게 지원합니다.

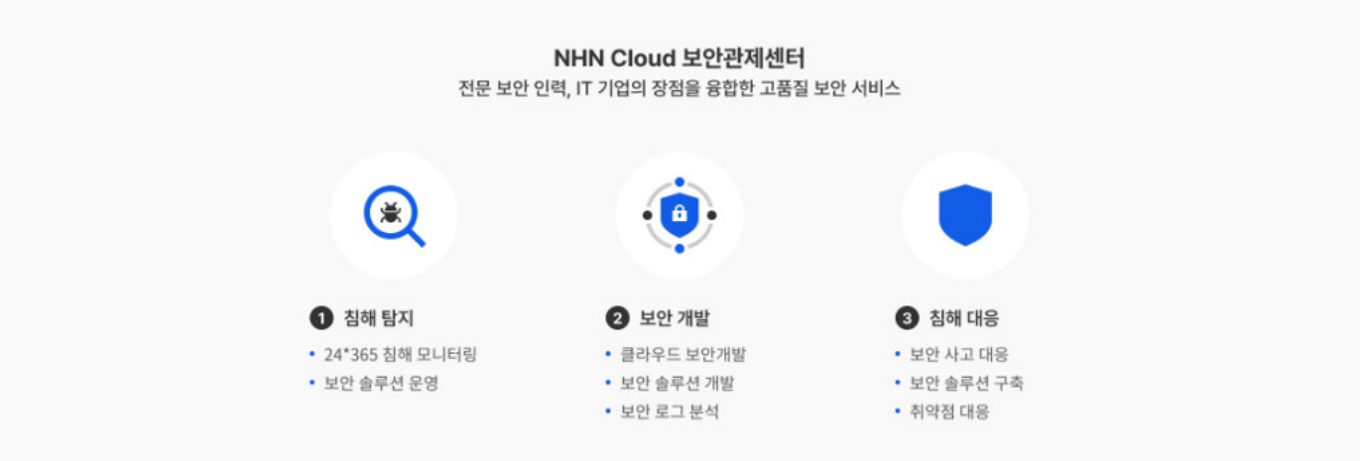


그림 43 NHN Cloud 보안 관제 센터

5.6 컨테이너 보안

컨테이너 기술은 클라우드 환경에서 애플리케이션을 신속하고 유연하게 배포할 수 있도록 지원하는 핵심 요소로 자리 잡고 있습니다. 그러나 컨테이너는 기존 가상머신과 달리 커널 자원을 공유하는 구조적 특성 때문에 새로운 보안 위협에 노출될 수 있습니다. 대표적으로 이미지 내부의 악성코드 삽입, 취약한 3rd party 라이브러리 사용, 컨테이너 간 격리 우회, 런타임 환경에서의 권한 오남용 등이 발생할 수 있으며, 이는 전체 클라우드 서비스의 안전성과 기밀성을 위협할 수 있습니다. 또한 컨테이너 오케스트레이션 도구(Kubernetes 등)에 대한 잘못된 설정이나 접근 권한 관리 미흡은 대규모 보안 사고로 이어질 수 있습니다. 따라서 보안 이미지를 통한 배포, 취약점 스캐닝 및 무결성 검증, 네트워크 세분화, 최소 권한 원칙 적용, 로그 및 모니터링을 통한 이상 행위 탐지 등이 필수적으로 수행되어야 합니다.

컨테이너 보안 관련 세부 지침은 NHN Cloud 보안 센터 「**컨테이너 보안 가이드**」에서 확인하실 수 있습니다.

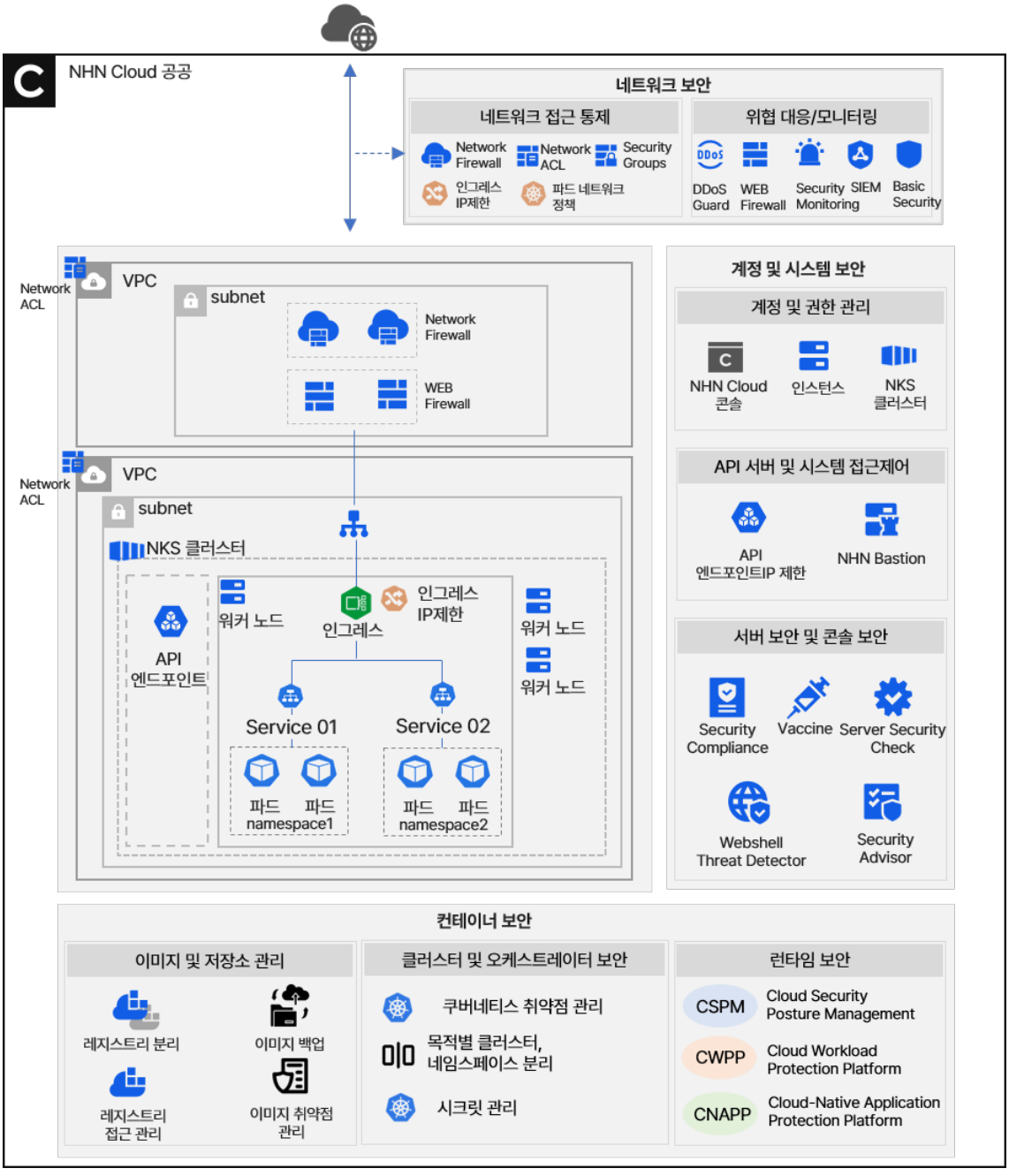


그림 44 컨테이너 보안 아키텍처

6 국가 보안 기준 준수 방안

6장은 「국가 클라우드 컴퓨팅 보안 가이드라인」 4장 2절 '민간 클라우드 컴퓨팅 서비스 이용 보안기준'의 목차를 기반으로, NHN Cloud 등이 제공하는 서비스의 적용 및 활용 방안을 설명하였습니다.
가이드라인의 주요 내용 중 NHN Cloud 역할, 서비스 등과 관련된 내용을 발췌 및 요약하여 구성된 것으로 일부 생략된 내용이 있으니 세부 사항은 반드시 원문을 참고하세요.
또한 「국가 클라우드 컴퓨팅 보안 가이드라인」의 내용 중 SaaS 개발 시 준수해야 하는 일부 요건은 SaaS를 개발하는 주체가 준수하고 적용해야 하는 것으로 해당 내용은 제외하고 작성되었습니다.

6.1 보안 기본 원칙

6.1.1 정책적 측면에서의 기본 원칙

표 6-1 정책적 측면에서의 기본 원칙

지침 요건	NHN Cloud 준수 방안	참고 장표
시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행	행정/공공기관의 인터넷, 업무 영역에 따라 시스템을 구축할 수 있는 분리된 환경을 제공하고 있습니다.	4.2.1 5.2.1
클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정	국내 위치에 공공/행정망용 클라우드 환경을 제공하고 있습니다.	-
민간 이용자용 클라우드 컴퓨팅 서비스 영역과 분리 운영	공공/행정 기관을 위한 컴퓨팅 서비스 영역을 제공하고 있습니다.	4.2.1
민간 이용자용 클라우드 컴퓨팅 서비스 영역과 물리적/논리적으로 분리 운영할 수 있음	물리적으로 분리된 영역을 제공하고 있습니다.	4.2.1
국가정보원이 도입 요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스를 이용	국가정보원의 도입 요건 확인이 완료된 환경을 제공하고 있습니다.	4.2.1
도입 정보보호 시스템 안전성을 확인	안정성 확인 후 보안 솔루션 등을 도입해야 합니다. 국가사이버안보센터 등을 통해 추가 자세한 내용을 확인할 수 있습니다.	4.2.4
	SaaS 환경 추가 기본 원칙	
SaaS 클라우드 인프라, 개발·운영 환경의 물리적 위치는 국내로 한정	국내 리전, 공공/행정망용 클라우드 환경을 제공하고 있습니다.	-
SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인	국가정보원의 도입 요건 확인이 완료된 환경을 제공하고 있습니다.	4.2.1

6.1.2 기술적 측면에서의 기본 원칙

표 6-2 기술적 측면에서의 기본 원칙

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 기본 원칙		
내부 업무와 인터넷 서비스 업무의 클라우드 컴퓨팅 혼용을 금지	물리적으로 분리된 업무망과 인터넷망 클라우드 환경을 제공하고 있습니다.	4.2.1 5.2.1
중요 장비 이중화 및 백업 체계 구축하고 표준 운영 절차를 수립	클라우드에서는 동일 자원을 복수로 생성하고, Load Balancer를 이용하거나 고가용성 DB 생성 등을 통해 이중화 구조를 손쉽게 구현할 수 있습니다. Load Balancer 및 고가용성 DB 생성은 해당 서비스의 사용자 가이드 내용을 참고하여 이용자의 환경에 맞게 구성할 수 있습니다.	-
관리자 및 이용자에 대한 접근통제 및 격리 수단을 확보	접근통제 대상에 따라 접근통제 수단, 격리 수단 등이 달라질 수 있습니다. NHN Cloud는 콘솔 접근제어, 계정 관리 등의 기능을 제공하고 있으며 NHN Bastion 등의 보안 서비스를 통해 인스턴스 OS 접근제어가 가능합니다. 인스턴스형 DB나 RDS의 경우 Security Groups, DB 보안 그룹으로 접근통제 등이 가능합니다.	5.2 5.4.1 5.4.2
클라우드에 저장 및 송수신되는 중요 업무 자료를 암호화(검증필 암호 모듈 탑재 제품을 이용)	암호화는 대상과 저장 방법에 따라 여러 가지 암호화 서비스, 솔루션을 이용하여 적용할 수 있습니다. NHN Cloud에서 제공되는 암호화 서비스 또는 NHN Cloud 마켓플레이스 등을 통해서 고객의 테넌트에 별도 구축하여 암호화를 적용할 수 있습니다.	5.4.5
민간 클라우드 컴퓨팅 서비스에 대한 보안 관제를 수행	전문 보안 인력을 통한 클라우드 관제 서비스를 제공하고 있으며 고객이 직접 관제할 수 있는 클라우드 환경과 인프라 노하우를 갖추고 있습니다.	5.5

6.2 세부 보안 기준

6.2.1 정책

6.2.1.1 시스템 보호

표 6-3 시스템 보호 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링(사용자 접근, 보안 정책 이벤트, 비정상 행위, 네트워크 등)	관제, 네트워크 접근 통제, 로그 관리 등과 같은 다양한 보안 관련 서비스를 제공하고 있습니다. 용도와 목적에 따라 NHN Cloud에서 제공하는 서비스 또는 마켓플레이스에서 제공하는 서비스 등을 활용하여 시스템 운영 상황이나 장애 모니터링을 할 수 있습니다.	5

6.2.1.2 보안 감사

표 6-4 보안 감사 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
IaaS 환경 보안 기준		
이용기관은 정보보안 감사에 필요한 관련 자료에 대한 종류를 정의하고, 필요시에 민간 사업자에게 해당 감사 로그를 요청하고 열람	감사 로그는 고객의 관리 영역과 NHN Cloud 관리 영역으로 구분됩니다. 고객이 직접 접근 가능한 로그는 자율적으로 확인/보관할 수 있으며, NHN Cloud 관리 영역의 로그는 고객지원 또는 사업 담당자 요청을 통해 신속히 지원 받을 수 있습니다.	-
로그 자료는 사후 추적 대상을 식별할 수 있는 형태로 기록되고 1년 이상 보호	이용하는 가상 자원, 서비스 및 솔루션 등에서 발생하는 로그는 해당 자원에서 제공하는 기능이나 별도 백업 등을 통해 관리할 수 있습니다. 클라우드 콘솔 로그는 CloudTrail 서비스를 통해 확인 및 관리할 수 있습니다.	5

표 6-5 로그 관리 책임 영역 예시

책임 영역	내용
이용자 관리 영역	이용자가 생성한 가상 자원 및 데이터, 이용자 콘솔에서 발생하는 로그 등
클라우드 사업자 협업 영역	보안 사고나 감사 등으로 CSP 관리 영역의 로그가 필요한 경우 별도 요청. 단, 내부 보안 정책 및 계약 범위 등에 따라 제공 가능한 로그 지원

6.2.2 클라우드 인프라

6.2.2.1 하드웨어

표 6-6 하드웨어 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
하드웨어 자원은 국가·공공기관 클라우드 컴퓨팅 서비스 제공을 위한 시스템에서만 사용	국가, 행정기관용 클라우드 서비스를 위한 별도 인프라(하드웨어 등)를 민간과 분리하여 제공하고 있습니다.	4.2.1
민간 클라우드 컴퓨팅 서비스 외부로부터 발생하는 DDoS, 비인가접속 등의 위협을 막기 위한 보안 대비책을 마련	NHN Cloud에서 제공하되는 보안 서비스 또는 마켓플레이스 상품 등을 활용하여 DDoS 위협 대응, 비인가 접속 차단 등의 대비책을 마련할 수 있습니다.	5.2 5.3 5.4.1 5.4.2 5.5

6.2.2.2 가상화 인프라

표 6-7 가상화 인프라 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
	공통 보안 기준	
가상 자원 회수 시 가상 자원 내에 존재하는 사용자 관련 데이터는 복구할 수 없는 형태로 삭제	DoD 5220.22-M 패턴을 적용할 수 있는 scrub(Linux), Disk Wipe(Windows)를 이용해 데이터 삭제 가이드를 제공하고 있습니다. 상세 내용은 사용자 가이드의 **데이터 완전 삭제 가이드**를 참고하세요. 데이터 완전 삭제에 대한 추가 문의가 있으신 경우 고객지원 등을 통해 문의하세요.	-
가상 자원에 대한 모니터링을 주기적으로 수행	가상 자원의 모니터링은 목적에 따라 여러 가지 서비스, 도구 등을 활용하여 주기적으로 수행할 수 있습니다. 인스턴스 서버 모니터링의 경우 NHN Cloud의 Cloud Monitoring 서비스를 활용하여 자원 모니터링이 가능합니다. 상세 내용을 사용자 가이드의 **Monitoring > Cloud Monitoring** 내용을 참고하세요. 또한 NHN Cloud 서비스와 마켓플레이스 상품을 활용하여 다양한 위협에 대해 효과적으로 모니터링 환경을 구성하고 적용할 수 있습니다.	5.5
기존 정보시스템 환경에서 클라우드 가상 환경으로 이전 시 자산 보호를 위한 암호화 등 안전한 이전 수단을 이용	레거시 환경에서 클라우드 환경으로 데이터를 이전할 때는 전송 구간의 기밀성과 무결성을 보장하기 위해 VPN, 전용 회선 등을 활용하여 데이터를 안전하게 전송할 수 있습니다. 데이터 마이그레이션 등 이전에 관한 상세 내용은 NHN Cloud 보안 센터의 「**데이터 이전 보안 가이드**」에서 확인할 수 있습니다.	5.3.2

IaaS 환경 추가 보안 기준		
2단계 인증, IP 기반 필터링 등 하이퍼바이저 관리 기능 및 관리자에 대한 접근통제 방안을 마련하고 하이퍼바이저에 대한 업데이트 및 보안 패치를 최신으로 유지	하이퍼바이저 관리는 클라우드 사업자의 책임 영역으로 NHN Cloud는 공공, 행정기관 등에 제공되는 클라우드 서비스의 인프라(하이퍼바이저 등)는 접근 통제, 취약점 관리, 사용자 계정 통제, 물리 보안 등을 하고 있으며 국가 기준 보안 적합 확인 등을 통해 인증을 받았습니다.	-

6.2.3 가상 환경 보안

6.2.3.1 보안 관리

표 6-8 가상 환경 보안 관리

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
개발 및 테스트를 위한 가상 개발 환경을 클라우드 서비스 운영 환경과 분리	목적에 따라 조직, 프로젝트, VPC 등으로 네트워크 환경을 구분하여 구성할 수 있습니다. NHN Cloud의 조직과 프로젝트 개념 및 사용 방법은 사용자 가이드의 **콘솔 정책 가이드**를 참고하여 적절히 설정할 수 있습니다. VPN 또는 서브넷 환경 구성은 IP 대역을 기준으로 네트워크를 분리할 수 있으며 분리된 네트워크는 Security Groups 또는 네트워크 방화벽 등을 통해 접근통제를 할 수 있습니다.	4.2.1
가상 개발 환경에 대한 비인가 접근 통제	본 가이드 및 NHN Cloud 보안 센터의 「**네트워크 아키텍처 보안 가이드**」를 참고하여 개발 환경에 대한 비인가 접근통제 정책 등을 적용할 수 있습니다.	5.3.1
IaaS 환경 추가 보안 기준		
웹 서버 등 공개용 가상 서버 보안 관리 (DDoS 대응, 계정 관리 등)	공개용 가상 서버는 외부에 노출되므로 위협 관리가 특히 중요합니다. DDoS 대응 서비스, 웹 방화벽, 서버 계정 관리 등이 필요하며, NHN Cloud의 보안 서비스와 마켓플레이스 상품 등을 활용하여 안전하게 구성할 수 있습니다.	5.3.3 5.3.5 5.4.1

6.2.3.2 악성코드 방지

표 6-9 악성코드 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
악성코드 감염 방지 및 탐지 조치(주기적인 보안 패치, 백신 설치 및 관리, 소프트웨어 설치 통제 등)	백신 설치와 주기적인 백신 업데이트, 실시간 감시를 통해 악성코드 탐지 및 예방이 가능합니다. 이와 함께 중앙 관리 정책을 적용하면, 전사적 위협 대응 및 보안 통제가 효율적으로 이루어질 수 있습니다. 백신 적용은 NHN Cloud 서비스 또는 마켓플레이스 상품 등을 이용하여 구성할 수 있습니다.	5.4.4

6.2.3.3 접근통제

표 6-10 접근통제 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
접근 제한(다중 인증, 동시 세션 제한 등)	클라우드 콘솔 계정, 인스턴스 OS 또는 DB의 계정의 접근 관리가 필요합니다. 대상 시스템에 따라 NHN Cloud 보안 서비스 또는 마켓플레이스 보안 상품 적용 등을 통해서 접근 정책을 적용할 수 있습니다.	5.2.1 5.4.1 5.4.2
식별 정보 등의 관리(고유 식별자 사용, 임시 식별자 관리, 유효 기관 관리, 권한 관리 등)	계정 식별자(아이디)는 고유한 값을 사용하여 발급 및 관리하고, 미사용 계정 및 비밀번호의 유효 기간을 체계적으로 관리해야 합니다. 아울러 최소 권한 원칙을 적용하여 계정으로 인한 보안 위협을 최소화해야 합니다. NHN Cloud에서 제공하고 있는 콘솔의 권한 관리는 **사용자 가이드의 멤버 정책**을 참고하시면 상세 내용을 확인하실 수 있습니다.	5.2.2 5.2.3 5.4.1 5.4.2

6.2.4 데이터

6.2.4.1 관리

표 6-11 데이터 관리 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
중요 데이터의 입·출력, 전송 또는 교환 및 저장에 대한 민간 사업자의 데이터 무결성 확인 방안을 마련	NHN Cloud 서비스와 마켓플레이스에서 제공하는 다양한 도구나 기능을 활용하여, 데이터 저장 및 전송 과정에서 암호화 기술과 암호화된 세션을 적용함으로써 데이터의 무결성을 확보할 수 있습니다. 이용자는 사용하는 서비스와 마켓플레이스 상품이 무결성 검증 기능을 제공하는지를 확인하기 위해, 데이터 전송 시 SSL 적용이나 암호화된 전송 프로토콜을 사용하는지 점검해야 합니다.	5.3.2 5.4.5
민간 사업자는 데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 하며 이용기관은 이를 확인	보안 서비스 및 마켓플레이스 상품 등을 통해 VPN 서비스 및 암호화 저장, 스토리지 접근 관리 기능 등을 적용할 수 있습니다.	5.4.3 5.4.5
데이터 폐기 조치 시 이용 기관은 민간 사업자에게 관련된 모든 데이터 폐기를 요청하여야 하며 폐기된 데이터가 복구할 수 없도록 삭제되었는지 확인	DoD 5220.22-M 등의 표준화된 완전 삭제를 적용하고 있으며 추가로 필요한 서류 등이 있을 경우 사업 담당자나 고객지원으로 언제든지 문의하세요.	-

6.2.4.2 암호화

표 6-12 데이터 암호화 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
이용 기관은 중요 업무 자료에 대한 암호화 수준 등에 대한 보안 요구 사항을 도출하여 계약 시 반영하여야 하며, 중요 업무 자료에 대한 생성·보관·처리·수신을 위한 정책적·기술적 방안을 민간 사업자로부터 제공 받아야 함		
민간 사업자와 협의하여 암호화 대상, 암호 강도(복잡도), 키 관리, 암호 사용에 대한 정책을 마련. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구 사항을 반드시 반영	이용자가 생성한 데이터는 암호화 서비스 및 솔루션 등을 이용하여 이용자가 암호화를 적용하고 키 관리를 할 수 있습니다. 그 외 클라우드 사업자와 협의가 필요한 암호화 대상에 대한 암호화 키 관리 절차 등관련은 클라우드 이용 시 고객지원로으로 언제든지 문의하세요.	5.4.5
민간 사업자와 협의하여 암호 키 생성, 이용, 보관, 배포, 파기에 대한 내용을 담은 암호 키 관리 절차를 수립하여야 하며 안전한 암호 키 관리 여부를 확인		

6.2.5 인증 및 권한

6.2.5.1 인증

표 6-13 인증 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
민간 클라우드 컴퓨팅 서비스에 대한 접근을 사용자 인증, 접근 주체별 권한 부여, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제	정책을 적용할 대상을 식별하고 적절한 접근 정책을 적용해야 합니다. 클라우드 콘솔 및 인스턴스, 데이터베이스 계정 등 모든 계정은 적절한 접근 정책과 최소 권한 원칙에 따라 설정 및 관리가 필요합니다.	5.2.1 5.2.2 5.4.1 5.4.2
민간 클라우드 컴퓨팅 서비스를 이용할 때 인증서(PKI) 기반, OTP, 지문 등 다중 요소(mMulti-factor) 인증을 통한 강화된 인증 수단 사용을 권고	민간 클라우드 컴퓨팅 서비스 이용을 위해 NHN Cloud 콘솔 로그인 시, 계정은 다중 요소 인증을 통해 보다 안전하게 로그인할 수 있습니다.	5.2.2
기관 필요에 따라 클라우드 접근 대상별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축	콘솔 인증 연동을 지원하고 있습니다. 단, 인증 체계 연동 대상 시스템에 따라 연동 방법이 다를 수 있어 협의가 필요합니다. 연동 관련 문의가 있을 시 고객지원으로 언제든지 연락하세요.	-

6.2.5.2 권한

표 6-14 권한 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
민간 클라우드 컴퓨팅 서비스 및 중요 정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근 권한을 최소한으로 부여	이용자가 수립한 클라우드 서비스 접근용 사용자 관리 정책에 따라, NHN Cloud 서비스 또는 마켓플레이스 상품에서 제공하는 기능을 활용하여 계정의 최소 권한 원칙을 적용하고 체계적으로 관리할 수 있습니다.	5.2 5.4.1 5.4.2
민간 클라우드 컴퓨팅 서비스 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제		
민간 클라우드 컴퓨팅 서비스 및 중요정보에 대한 접근을 관리하기 위하여 접근 권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무 변경, 부서 변경)의 적정성 여부를 정기적으로 점검	불필요하거나 미사용 중인 계정에 대해서는 주기적인 점검 및 삭제 정책을 수립하여 관리할 필요가 있습니다. 관리자는 클라우드 콘솔 계정을 NHN Cloud 서비스 등을 이용하여 주기적으로 점검할 수 있습니다. 인스턴스 OS 계정이나 DB 계정 등의 사용 여부를 정기적으로 점검하거나, 계정 관리 보안 솔루션이 적용되어 있다면 솔루션에서 제공하는 기능 등을 활용하여 효율적으로 관리할 수 있습니다.	5.2.2

6.2.6 사고 및 장애 대응

6.2.6.1 사고

표 6-15 사고 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
민간 사업자는 침해 사고 발생 시 침해 사고 대응 절차에 따라 법적 통지 및 신고 의무를 준수하여야 하며 이용자에게 발생 내용, 원인, 조치 사항 등을 신속하게 알려야 할 의무가 있음	NHN Cloud는 사업자의 책임 범위에 대해 침해 사고 발생 시 정해진 대응 절차에 따라 의무 사항을 이행하며, 이용자의 협조 요청에도 적극적으로 대응하고 있습니다. 추가 문의 사항이 있을 경우 언제든지 고객지원으로 문의하세요. 이용자가 생성한 자산의 침해 사고 모니터링은 관제 서비스 등을 이용할 수 있습니다.	5.5

6.2.6.2 장애

표 6-16 장애 세부 보안 기준

지침 요건	NHN Cloud 준수 방안	참고 장표
공통 보안 기준		
민간 사업자는 관련 법률에서 규정한 클라우드 컴퓨팅 서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 하며 이용 기관은 장애 대응 요구 사항, 담당자 정의 및 연락처 등을 담은 장애 대응 절차를 마련	클라우드 컴퓨팅 서비스 중단으로부터 업무 연속성을 보장하기 위해 NHN Cloud는 이중화, 백업, 복구 등의 절차와 함께 다양한 기술적 대책을 적용하고 있습니다. 또한 국가, 공공기관에 제공하는 클라우드 서비스는 **국가사이버안보센터 자료실 > 지침·가이드·공시**에 게시된 민간 클라우드 도입 가능 목록에 등록된 서비스로서, 국가 및 공공기관이 요구하는 서비스 수준을 충족하고 있음을 확인할 수 있습니다. 아울러 NHN Cloud는 국내외 공인 인증 기관으로부터 클라우드 정보보호 및 개인정보보호 관리체계 인증을 획득하여, 관련 활동을 체계적이고 지속적으로 수행하고 있음을 정기적으로 점검 받고 있습니다. NHN Cloud 인증 현황은 보안 센터 **정보보호 인증 현황**에서 확인할 수 있습니다. 이용자의 요구 사항에 대해서는 항상 적극적으로 대응하고 반영하고 있으며 추가 필요 사항에 대해서는 언제든지 **고객 센터**로 문의하세요.	-

7 별첨

7.1 법, 지침 등의 요구 사항

주요 법률, 지침 등의 내용을 발췌하여 작성되었습니다. 요약 및 축약 과정에서 의미가 일부 달라질 수 있으므로, 정확한 이해를 위해서는 원문을 함께 확인하세요.

7.1.1 법 주요 요구 사항

표 7-1 법 주요 요구 사항

분류	구분	조항	주요 내용 요약
법령	국가정보원법	제1조(목적)	국가정보원의 조직 및 직무 범위와 국가안전보장 업무의 효율적인 수행을 위하여 필요한 사항을 규정함을 목적으로 함.
법령	사이버안보 업무 규정	제1조(목적)	국가정보원의 직무 중 사이버안보 업무의 수행에 필요한 사항을 규정함을 목적으로 함.
		제4조(국가사이버안보센터)	국가정보원장은 사이버안보 업무를 효율적으로 수행하기 위하여 국가사이버안보센터를 둘 수 있음.
		제7조(사이버보안 업무 대상 공공기관의 범위)	대통령령으로 정하는 공공기관
		제9조(사이버보안 예방 조치 등)	국가정보원장은 정보화 사업 보안성 검토를 실시하고, 그 보안성 검토 결과의 이행 여부를 확인할 수 있음.
			암호 장치, 모듈 정보통신기기나 클라우드 서비스의 보안 대책을 수립할 수 있음.
			정보보호시스템 및 클라우드컴퓨팅서비스 보안 대책에 적합한지 검증할 수 있음. 보안 관리 수준을 측정할 수 있음.
		제10조(사이버보안 교육)	보안 교육 실시
		제11조(사이버보안 훈련)	사이버공격·위협에 대응하기 위한 훈련을 실시
		제12조(사이버보안 자체 진단·점검)	사이버공격·위협에 대한 예방 및 대응에 필요한 자체 진단·점검을 연 1회 이상 실시 및 조치 필요
		제13조(사이버보안 실태 평가)	조직, 인력, 예산, 직무 교육 및 사이버보안에 대한 자체 진단·점검 등 사이버보안 실태를 평가할 수 있음.

법령	사이버안보 업무 규정	제14조(통합보안관제)	통합보안관제체계를 구축·운영해야 함.
			통합보안관제체계와 연계된 보안관제센터를 설치·운영해야 함(다른 기관의 보안관제센터를 활용할 수 있음.).
			클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있음.
		제16조(사고 조사)	사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있음.
법령	보안업무규정	제1조(목적)	국가정보원의 직무 중 보안 업무 수행에 필요한 사항을 규정함을 목적으로 함.
		제7조(암호자재 제작 · 공급 및 반납)	국가정보원장은 암호자재를 제작하여 필요한 기관에 공급함.
법령	전자정부법	제1조(목적)	행정업무의 전자적 처리를 위한 기본 원칙, 절차 및 추진 방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민의 삶의 질을 향상시키는 것을 목적으로 함.
		제24조(전자적 대민서비스 보안 대책)	전자적 대민 서비스와 관련된 보안 대책을 국가정보원장과 사전 협의를 거쳐 마련하여야 함.
		제56조(정보통신망 등의 보안대책 수립·시행)	정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 보안 대책을 마련하여야 함.
			전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 보안 조치 필요
		제56조의2(정보시스템 장애 예방·대응 및 복구 등)	정보시스템 장애관리계획 수립지침(이하 '수립지침'이라 한다.)을 작성 필요
		제56조의3(정보시스템의 등급 관리)	정보시스템의 중요도·영향도 등에 따라 체계적으로 소관 정보시스템을 관리할 수 있도록 정보시스템의 등급 산정 기준을 정하고, 등급에 따른 관리 방안 마련 필요
		제56조의5(정보시스템 장애상황 및 사후관리)	주요 정보시스템의 장애상황 통합관제, 장애 대응 및 복구 관련 상황 관리 등의 업무를 수행하기 위하여 정보시스템종합상황실을 설치·운영할 수 있고 장애 관리, 대응 관련 절차, 의무를 실행해야 함.

법령	전자정부법 시행령	제20조(전자적 대민서비스 보안 대책의 범위)	전자적 대민 서비스 보안 관련 기본 계획의 수립, 보안관리, 정보보안시스템의 도입 및 운영, 사이버 침해 대응 지원 체계의 구축 필요
		제34조(행정전자서명의 관리)	행정 전자서명 생성 키를 안전하게 보관·관리하여야 하며, 그 행정 전자서명 생성 키가 분실·도난·유출 또는 훼손된 경우에는 소관 인증 기관에 지체 없이 통보 필요
		제69조(전자문서의 보관·유통 관련 보안조치)	전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 함.
		제70조의2(정보시스템 장애관리 계획의 수립 등)	정보시스템(정보시스템 운영시설을 포함한다.) 장애관리를 위한 계획(이하 '정보시스템 장애관리계획'이라 한다.)의 수립지침을 3년마다 작성하여 중앙행정기관등의 장에게 통보해야 함.
		제70조의3(정보시스템의 등급 관리)	전자정부서비스의 특성 및 중요도를 고려하여 등급 산정을 함.
행정규칙	행정기관 및 공공기관 정보시스템 구축·운영 지침	제1조(목적)	「전자정부법」(이하 '법'이라 한다) 제45조제3항에 따라 행정기관등의 장이 정보시스템을 구축·운영함에 있어서 준수해야 할 기준, 표준 및 절차와 법 제49조제1항에 따른 상호운용성 기술평가에 관한 사항을 정함을 목적으로 함.
		제8조(보안성 검토 및 보안관리)	정보시스템 「국가 정보보안 기본지침」 제14조부터 제19조까지에서 규정한 보안성 검토를 이행 필요
			용역사업 수행업체에 대한 보안관리 수행 필요
			개인정보 안전성 확보에 필요한 조치를 강구
			개인정보처리시스템을 신규 구축·운용 또는 변경하려고 하는 경우, 「개인정보 영향평가에 관한 고시」 제9조의2에 따라 개인정보 영향평가 필요
		제50조(소프트웨어 개발보안 원칙)	소프트웨어 보안 약점이 없도록 소프트웨어를 개발 또는 변경(이하 '소프트웨어 개발 보안'이라 한다.)하여야 함
		제51조(소프트웨어 개발보안 활동)	「소프트웨어 개발 보안 가이드」 참고
		제52조(보안 약점 진단 기준)	별표 3의 소프트웨어 보안 약점을 필수 진단 항목으로 포함
법령	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률	제1조(목적)	클라우드컴퓨팅의 발전 및 이용을 촉진하고 클라우드컴퓨팅서비스를 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 국민경제의 발전에 이바지함을 목적으로 함.

법령	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률	제23조(신뢰성 향상)	클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질·성능 및 정보보호 수준을 향상시키기 위하여 노력해야 함.
		제23조의2(클라우드컴퓨팅서비스의 보안인증)	과학기술정보통신부장관은 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 '보안인증'이라 한다.)을 할 수 있음.
			보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령으로 정하는 5년 내의 범위임.
		제25조(침해 사고 등의 통지 등)	클라우드컴퓨팅서비스 제공자는 다음 각 호(침해사고 관련)의 어느 하나에 해당하는 경우에는 지체 없이 그 사실을 해당 이용자에게 알려야 함.
		제26조(이용자 보호 등을 위한 정보 공개)	클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있음.
		제27조(이용자 정보의 보호)	클라우드컴퓨팅서비스 제공자는 법원의 제출 명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 동일함.
법령	클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령	제15조의6(클라우드컴퓨팅서비스의 보안인증 절차 등)	클라우드컴퓨팅서비스 보안인증 절차에 대한 내용
		제15조의7(보안인증의 유효기간 등)	유효기간은 5년
			유효기간이 만료되기 6개월 전까지 보안인증의 유효기간 연장을 신청
		제16조(통지가 필요한 클라우드컴퓨팅서비스의 중단 기간)	법 제25조제1항제3호에서 '대통령령으로 정하는 기간'은 서비스의 중단 기간이 연속해서 10분 이상인 경우
			법 제25조제1항제3호에서 '대통령령으로 정하는 기간'은 중단 사고가 발생한 때부터 24시간 이내에 클라우드컴퓨팅서비스가 2회 이상 중단된 경우로서 그 중단된 기간을 합하여 15분 이상인 경우
		제18조(피해 확산 방지 등을 위한 조치)	과학기술정보통신부장관은 피해확산 방지 등을 위한 조치를 할 수 있음.
		제19조(계약 종료 또는 사업 종료 사실의 통지 등)	이용자와의 계약이 종료되기 30일 전까지 종료 일시싱 등 관련 사항을 이용자에게 알려야 함.

행정규칙	행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시	제1조(목적)	클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 필요한 사항과 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제19조제6항에 따라 계약 및 사업 종료 사실의 통지 방법·시기, 이용자 정보의 반환 및 파기 방법·시기 등에 대한 기준을 정함을 목적으로 함.
		제7조(이용계약 종료 사실의 통지 방법 및 시기)	이용계약이 종료되기 30일 전까지 서비스 제공자로부터 다음 각 호의 사항을 통지 받을 수 있도록 조치해야 함.
		제8조(사업 변경 및 종료 사실의 통지 방법 및 시기)	서비스 제공자가 해당 이용계약과 관련된 사업을 변경하거나 종료하기 30일 전까지 서비스 제공자로부터 다음 각 호의 사항을 통지 받을 수 있도록 조치해야 함.
		제10조(안전성 검토)	서비스 제공자를 선정하는 경우에는 별표 2의 안전성 검토 항목에 따른 검토 결과를 고려함.
		제11조(보안성 기준)	「국가 정보보안 기본지침」을 준수
			인증(이하 '보안인증'이라 한다.)된 클라우드컴퓨팅서비스를 우선 고려함.
			정보시스템의 '시스템 중요도' 등급을 식별
			식별된 등급에 해당하는 보안인증된 클라우드컴퓨팅서비스로서 국가정보원장이 게시하거나 게시 예정인 클라우드컴퓨팅서비스를 이용
		제12조(운영실태 점검 등)	해당 클라우드컴퓨팅서비스에 대해 실태를 점검할 수 있도록 조치해야 함.
		제13조(저장정보의 보호와 관리)	저장정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 조치해야 함.
		제14조(저장정보의 반환 및 파기 등)	저장정보를 복구가 불가능한 방법으로 지체 없이 파기 필요
			복구가 불가능한 방법으로 파기한 것을 증명할 수 있는 근거자료를 확보해야 함.
		제15조(클라우드컴퓨팅서비스의 연속성 확보)	클라우드컴퓨팅서비스가 중단되지 않도록 필요한 조치를 해야 함.
행정규칙	클라우드컴퓨팅서비스 보안인증에 관한 고시	제1조(목적)	클라우드컴퓨팅서비스의 보안인증에 필요한 사항을 정하는 것을 목적
		제14조(보안인증 유형 및 등급)	IaaS, SaaS 등의 인증 기준과 유형
		제15조(보안인증기준)	보안인증기준

행정규칙	국가사이버안전관리규정	제1조(목적)	국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적
		제3조(적용범위)	이 훈령은 중앙행정기관(대통령 소속 기관, 국무총리 소속 기관 및 국가인권위원회를 포함한다. 이하 같다.), 지방자치단체 및 공공기관의 정보통신망에 적용함. 주요정보통신기반시설에 대해서는 「정보통신기반보호법」을 우선 적용함.
		제8조(국가사이버안전센터)	사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속 하에 국가사이버안전센터(이하 '사이버안전센터'라 한다.)를 둔다.
		제9조의2(사이버위기 대응 훈련)	매년 정기적으로 사이버위기 대응 훈련을 실시함.
		제10조의2(보안관제센터의 설치·운영)	사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 '보안관제센터'라 한다.)를 설치·운영 필요
			다른 중앙행정기관(국가정보원을 포함한다.)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있음.
			보안관제전문업체의 인원을 파견 받아 보안관제 업무를 수행하도록 할 수 있음.
			보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계기관의 장에게 제공하여야 함.
		제12조(사고통보 및 복구)	사고 발생 또는 징후 발견 시 지체 없이 보고해야 함.
		제13조(사고조사 및 처리)	국가정보원장은 사고 원인 분석, 조사를 실시할 수 있음
		제14조(전문기관간 협력)	전문기구를 운영하는 기관 간 관계전문가 회의를 소집하고 긴밀히 협력할 수 있음.

7.1.2 국가정보보안기본지침

표 7-2 국가정보보안기본지침 내용 요약

분류	내용 요약	대응 키워드
제3절 제품 도입 정보통신제품(보안솔루션) 등 도입 기준	• 보안적합성 검증 • 안전성 검증필 제품 도입 • 국가정보원장이 별도로 공지하는 도입 요건을 만족하는 제품 도입 • 암호화 제품은 검증필 암호 모듈 적용	• 보안적합성 • 안전성 검증필 등

내부망, 인터넷망 분리(40조)	• 내부망과 기관 인터넷망을 분리·운영 • 침입차단·탐지시스템 설치 등 비(非)인가자 침입 차단 대책 • 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단 대책 • 내부망 정보시스템의 인터넷 접속 차단 대책 • 내부망과 기관 인터넷망 간 일방향 전송 장비 등을 이용한 자료 전송 체계를 구축·운영하고 원본 파일은 3개월 이상, 전송 기록은 6개월 이상 유지	망 분리 및 망간 연계
보안/네트워크장비 보안(42조)	• 지정 단말기로부터의 접속·관리 허용 • 최초 설치할 경우 디폴트(default) 계정은 삭제하거나 변경해 사용하고 장비 관리를 위한 관리자 계정을 별도로 생성·운영 • 불필요한 서비스 포트와 개별사용자 계정은 차단 및 삭제	보안 설정
	펌웨어 무결성과 컴퓨터 운영체제·소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 유지	솔루션 버전 관리
	로그 기록을 1년 이상 유지, 비(非)인가자의 접속 여부를 정기적으로 점검	로그 보관
	침입차단·탐지 시스템의 침입차단·탐지규칙(rule)의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검·갱신	탐지/차단 규칙 최신화
서버 보안(53조)	• 서버 내 저장 자료에 대하여 업무별·자료별 중요도에 따라 개별사용자의 접근권한 차등 부여 • 개별 사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외 자료 접근통제 • 관리자용 서비스 접속 시 특정 IP 주소가 부여된 관리용 단말기 지정·운용	서버 접근제어
	서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별 사용자용 서비스 분리·운용	서버 설정
	서버 설정 정보 및 저장 자료에 대한 정기적 백업 실시	서버 백업
	데이터베이스에 대하여는 개별 사용자의 직접 접속 차단, 개인정보 등 중요 정보 암호화 등 데이터베이스별 보안조치 실시	DB 접근제어
공개서버 보안(54조)	내부망과 분리된 영역(DMZ)에 설치	네트워크 분리(방화벽 등)
	침입차단·탐지시스템 및 DDoS 대응장비 설치 등 보안 대책을 수립·시행	• IDS/IPS • DDoS 차단
	서버에 접근할 수 있는 개별 사용자를 제한하고 불필요한 계정은 삭제	서버 접근제어
로그기록(55조)	• 접속자, 정보시스템·응용프로그램 등 접속 대상 • 로그온·오프, 자료의 열람·출력 등 작업 종류 및 시간 • 접속 성공·실패 등 작업 결과 • 전자우편 사용 등 외부 발송 정보 등 • 로그기록을 1년 이상 보관, 로그기록의 위·변조 및 외부 유출 방지 대책을 수립·시행	• 로그 저장/관리 • 1년 이상 보관 • 로그 위변조 방지
저장매체 폐기(61)	비밀·대외비를 저장하거나 암호화 키를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전 파괴	클라우드 업무 협조 또는 베어메탈

계정관리(75조)	• 개별 사용자별 또는 그룹별 접근 권한 부여 • 외부인에게 계정을 부여하지 아니하되 업무상 불가피한 경우 기관의 장 책임하에 보안 조치 후 필요한 업무에 한하여 일정기간 동안 접속 허용 • 특별한 사유가 없는 한 용역업체 인원에게 관리자 계정 부여 금지 • 비밀번호 등 식별 및 인증 수단이 없는 사용자 계정은 사용 금지 • 시스템 접속(로그온)에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입여부를 점검 • 공용(公用) 정보시스템 관리자는 개별 사용자의 보직 변경, 퇴직, 계약 종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수 • 공용(公用) 정보시스템 관리자는 사용자 계정 부여 및 관리의 적절성을 연 2회 이상 점검하고 그 결과를 정보보안담당관에게 통보 • 공용(公用) 정보시스템 관리자는 제1항 및 제3항에 의한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관	계정관리
비밀번호 관리(76조)	• 사용자 계정(아이디)과 동일하지 않은 것 • 개인 신상 및 부서 명칭 등과 관계가 없는 것 • 일반 사전에 등록된 단어의 사용을 피할 것 • 동일한 단어 또는 숫자를 반복하여 사용하지 말 것 • 사용된 비밀번호는 재사용하지 말 것 • 동일한 비밀번호를 여러 사람이 공유하여 사용하지 말 것 • 응용 프로그램 등을 이용한 자동 비밀번호 입력 기능을 사용하지 말 것	비밀번호 관리
사이버공격 대응훈련(96조)	국가정보원장은 「사이버안보 업무규정」 제11조제2항에 따른 통합훈련을 「비상대비자원 관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.	DDoS 모의훈련
암호 사용 원칙	국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용	검증필 암호모듈
보안관제센터 설치·운영(131조)	보안관제센터를 국가보안관제체계와 연계 운영	보안관제 연계
탐지규칙정보 개발 및 배포(133조)	보안관제센터를 운영하는 기관의 장과 국가정보원장은 사이버공격을 탐지할 수 있는 기술정보(이하 '탐지규칙정보'라 한다.)를 개발하여 보안관제업무에 활용할 수 있다.	탐지 규칙정보 연동
공격정보 탐지·처리(134조)	사이버공격에 관한 정보를 실시간 탐지하는 장비(암호화된 사이버공격 패킷을 가시화(可視化)하는 장비를 포함한다.)를 보안관제 대상기관의 정보통신망에 설치·운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 처리할 수 있다.	SSL 가시화

7.1.3 국가 클라우드 컴퓨팅 보안 가이드라인 4장 제2절 요약

표 7-3 국가 클라우드 컴퓨팅 보안 가이드라인 내용 요약

분류	내용 요약	대응 키워드
정책적 측면 [공통 기본 원칙]	시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안 기준을 사전 확인	• 중요도 분류 • 영역 분류
	클라우드 시스템 및 데이터의 물리적 위치는 국내로 함	• 국내 클라우드

정책적 측면 [공통 기본 원칙]	국가정보원이 도입요건 확인을 완료한 민간 클라우드 컴퓨팅 서비스를 이용	CSAP 등
	도입 정보보호시스템 안전성을 확인	보안적합성
	각급 기관의 내부망과 연동된 공공 전용 민간 클라우드는 각급 기관의 내부망으로 간주하며, 각급 기관의 인터넷망과 연동된 공공 전용 민간 클라우드는 각급 기관의 인터넷망으로 간주하여 「국가 정보보안 기본 지침」에 따라 보안 관리	망 분리 보안
	보안 서비스수준협약(SLA)	보안책임영역
	공급망 관리 정책을 수립하고 관련 보안 요구사항을 계약상 반영	보안책임영역
정책적 측면 [SaaS 환경 추가 기본 원칙]	망 미분리 기관은 SaaS를 사용하는 단말에서 인터넷과 업무 영역 간 자료 교환이 되지 않도록 기술적 통제대책을 구현하여 SaaS를 사용	SaaS 보안
	SaaS 클라우드 인프라, 개발·운영 환경의 물리적 위치는 국내로 한정	국내 클라우드
	SaaS를 제공하기 위한 SaaS 개발·운영 환경, 클라우드 인프라 환경에 대한 보안성을 확인	SaaS 보안성 평가
	SaaS 개발·운영 환경은 SaaS 서비스 가용성을 보장할 수 있어야 하며, 사고 및 장애에 대응할 수 있는 체계가 마련	SaaS 보안성 평가
	SaaS는 허가 받은 외부 연동 서비스(스토리지, 데이터베이스, 빅데이터 처리 등)와 연계	SaaS 보안성 평가
기술적 측면 [공통 기본 원칙]	내부 업무와 인터넷 서비스 업무의 클라우드 컴퓨팅 혼용을 금지	망 분리
	관리자 및 이용자에 대한 접근통제 및 격리 수단을 확보	시스템접근제어
	클라우드에 저장 및 송수신되는 중요 업무자료를 암호화	암호화
	민간 클라우드 컴퓨팅 서비스에 대한 보안관제를 수행	보안관제
	클라우드 가상화 보안 모니터링 및 관리를 강화	보안관제
기술적 측면 [SaaS 환경 추가 기본 원칙]	SaaS 애플리케이션을 공유하는 다수의 사용자 간 자원 격리 방안 마련	SaaS 보안성 평가
	SaaS 애플리케이션 개발 및 운영 시 인터페이스 및 API의 취약점에 대한 주기적인 검증 수행	API 취약점 관리
	SaaS 애플리케이션 설계 및 개발 단계에서 취약점을 제거하고 SaaS 운영 중에도 주기적으로 취약점 제거를 수행	취약점 관리
	SaaS 애플리케이션 접근을 위한 네트워크 프로토콜 보호 방안 마련	SSL 적용
	SaaS 애플리케이션 관련 데이터(소스코드, 설정 파일, 로그 정보 등)에 대한 보호방안 마련	• 암호화 • 접근제어

7.1.4 컨테이너 보안(국가 클라우드 컴퓨팅 보안 가이드라인 부록 6)

표 7-4 컨테이너 보안

분류	내용
[관리 노드]	오케스트레이터 등 가상화 관리 솔루션이 실행되는 호스트 시스템
오케스트레이터(orchestrator)	컨테이너 런타임으로 컨테이너를 지정된 컨테이너 노드에 배치하거나 문제가 발생한 컨테이너를 교체하거나 컨테이너 환경 정보를 설정하는 등 스케줄링, 클러스터링 및 네트워킹을 관리하는 오케스트레이션 수행(Kubernetes 등)

[컨테이너 노드]	컨테이너 가상화 환경이 운영되는 호스트 시스템
컨테이너	애플리케이션과 환경정보가 포함된 독립적인 격리실행 가상 환경·컨테이너 이미지는 메타데이터, 애플리케이션 바이너리 및 공유 라이브러리를 패키징하고 있는 TAR 형식 파일
컨테이너 런타임	컨테이너를 쉽게 가져오거나 공유하고 구동할 수 있도록 지원하는 도구(Docker 등)
호스트 운영체제	컨테이너를 실행하는 기반 시스템·운영체제 네임스페이스(namespace), 컨트롤 그룹(cgroups) 기능으로 컨테이너 런타임은 컨테이너 격리(isolation)를 수행
[가상머신 레지스트리]	컨테이너 이미지가 저장되는 저장소
이미지 저장소	컨테이너 이미지를 관리하고 공유하기 위한 애플리케이션·OCI는 이미지 장소(레지스트리)에 대한 규격을 제시
[관련 보안정책 및 규정]	• 「국가 정보보안 기본지침」, 국가정보원 • 「국가 클라우드 컴퓨팅 보안 가이드라인」, 국가정보원 • 컨테이너 런타임은 가상 환경을 구현해주는 '가상화 제품'에 해당, CC인증 대상이지만 도입 요건을 필수가 아닌 권고로 제시(2021. 4. 14.부터 적용, 국가정보원 홈페이지 참조)



엔에이치엔클라우드

13487 경기도 성남시 분당구 대왕판교로645번길 16 NHN 플레이뮤지엄

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

©NHN Cloud Corp. All rights reserved.