NHN Cloud
개인정보보호 준수 가이드

NHN Cloud
Personal Information Compliance Guide

NHN CLOUD

NHN Cloud 개인정보보호 준수 가이드

저작권

문서 이력

버전	일자	이력 사항
1.0 버전	2024. 8.	NHN Cloud 개인정보보호 준수 가이드 1.0 버전 출시

목차

1 개요

클라우드 환경은 이용자의 데이터를 인터넷상의 서버에 저장하고 이를 다양한 기기를 통해 언제 어디서든 접근할 수 있는 편리함을 제공합니다. 그러나 이러한 장점에도 불구하고 서버 해킹으로 인한 정보 유출, 데이터 통제권 약화, 국제적 정보보호법규 적용의 혼란 등의 문제점이 존재합니다.

더불어 개인정보보호는 점점 더 중요한 이슈로 부각되고 있으며, 최근 발생한 대규모 데이터 유출 사건들은 그 심각성을 다시 한번 일깨워 주고 있습니다. 따라서 안전한 클라우드 환경을 구축하기 위해서는 고도화된 보안 조치와 모범 사례를 준수하는 것이 필수적입니다.

본 가이드는 클라우드 환경에서의 개인정보의 안전성 확보조치 기준 준수를 위한 기술적 방안을 살펴보고, NHN Cloud에서 구현할 수 있는 서비스를 제시함으로써 안전하고 신뢰할 수 있는 클라우드 서비스를 구축하는 데 기여하고자 합니다.

1.1 개인정보의 이해

1.1.1 개인정보의 정의

개인정보란 살아 있는 개인에 대한 정보로 성명, 주민등록번호 및 영상 등을 통해 개인을 식별할 수 있는 정보를 의미합니다. 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있다면 개인정보로 간주합니다. 예를 들어, 전화번호나 이메일 주소도 이에 해당될 수 있습니다. 또한, 적절한 처리를 통해 개인을 특정할 수 없도록 처리한 가명정보도 개인정보의 일종입니다.

※ 가명정보란 특정 개인을 식별할 수 없도록 개인정보의 일부를 대체하거나 삭제하여 처리한 정보를 말합니다. 이는 원래의 정보만으로 개인을 직접 식별할 수는 없지만, 다른 정보와 결합하면 식별 가능성이 있는 정보를 의미합니다. 가명정보는 데이터의 활용 가치를 높이면서도 개인정보보호를 강화하기 위해 사용됩니다. 예를 들어, 이름이나 주민등록번호 대신 임의의 식별자를 사용하여 개인을 특정하지 않고 데이터를 분석하거나 연구하는 데 사용될 수 있습니다. 개인을 알아볼 수 없는 정보이지만 추가 정보를 사용하거나 결합하면 개인을 식별할 수 있기 때문에 가명정보도 개인정보로 규정할 수 있습니다.

1.1.2 개인정보의 특징

- **식별 가능성**
  개인정보는 해당 정보로 특정 개인을 식별할 수 있어야 합니다. 예를 들어 이름이나 주민등록번호는 직접적으로 특정 개인을 식별할 수 있습니다. 식별 가능성은 정보의 단독 사용뿐 아니라 다른 정보와의 결합을 통해서도 고려됩니다.
- **민감성**
  개인정보에는 건강 상태, 신용 정보, 비밀번호 등 타인에게 노출되면 개인의 사생활이 침해되거나 금전적 피해를 입을 수 있는 민감한 정보가 포함됩니다. 이러한 정보는 더욱 보호 필요성이 높습니다.
- **보호 필요성**
  개인정보는 개인의 사생활과 직결되므로 정보 유출 시 개인의 사생활 침해, 경제적 손실, 명예 훼손 등 다양한 피해가 발생할 수 있어 더욱 보호가 필요합니다.
- **변경 가능성**
  개인정보는 시간이 지남에 따라 변경될 수 있습니다. 예를 들어, 주소나 전화번호는 시간이 지나면서 변경될 수 있으므로 개인정보 관리 시 이러한 변경 사항을 반영해야 합니다.
- **법적 규제**
  개인정보는 다양한 법적 규제를 받습니다. 한국에서는 개인정보보호법, 유럽 연합에서는 GDPR(general data protection regulation) 등이 개인정보의 수집, 이용, 보관, 파기에 대해 엄격하게 규제하고 있습니다.
- **적용 범위**
  개인정보는 전자적 형태뿐 아니라 종이 문서 등 비전자적 형태로도 존재할 수 있습니다. 따라서 모든 형태의 개인정보는 보호의 대상이 됩니다.

1.1.3 개인정보의 중요성

개인정보는 마케팅, 빅데이터, 인공 지능 등 다양한 분야에서 중요한 데이터로 활용되고 있습니다. 전자 상거래, 고객 관리, 금융 거래 등 사회의 구성과 발전을 위한 필수적인 요소로 작용하며, 데이터 경제 시대를 맞이하여 기업 및 기관에서는 이를 중요한 자산으로 평가합니다. 그러나 인터넷의 발달로 개인정보 유출의 위험이 증가하고 있으며, 유출된 개인정보는 스팸 메일, 불법 텔레마케팅, 보이스 피싱 등 다양한 범죄에 악용될 수 있습니다. 이로 인해 개인의 사생활과 안전, 재산에 큰 피해를 주며, 한번 유출된 개인정보는 회수가 사실상 불가능합니다. 이러한 이유로 개인정보보호는 선택이 아닌 필수적인 과제입니다.

1.1.4 개인정보의 종류

개인정보의 범주는 이름, 주민등록번호, 생년월일과 같은 인적 신상 정보뿐만 아니라, 사회·경제적 지위와 상태, 교육 정보, 신용 정보, 건강·의료 정보, 신체적 특징, 재산 소유 정보, 문화 활동 및 정치적 성향 등의 내면적인 비밀까지 다양합니다. 또한, 이용자가 사업자의 서비스를 이용하는 과정에서 발생하는 통화 내역, 로그 기록, 구매 내역과 같은 정보도 개인정보로 간주됩니다.

표 1 개인정보 종류

구분		내용
인적 사항	**일반 정보**	성명, 주민등록번호, 주소, 연락처, 생년월일, 출생지, 성별 등
	가족 정보	가족 관계 및 가족 구성원 정보 등
신체적 정보	**신체 정보**	얼굴, 홍채, 음성, 유전자 정보, 지문, 키, 몸무게 등
	의료·건강 정보	건강 상태, 진료 기록, 신체 장애, 장애 등급, 병력, 혈액형, IQ, 약물 테스트 등의 신체검사 정보 등
정신적 정보	**기호·성향 정보**	도서·비디오 등 대여 기록, 잡지 구독 정보, 물품 구매 내역, 웹사이트 검색 내역 등
	내면의 비밀 정보	사상, 신조, 종교, 가치관, 정당·노조 가입 여부 및 활동 내역 등
사회적 정보	**교육 정보**	학력, 성적, 출석 상황, 기술 자격증 및 전문 면허증 보유 내역, 상벌 기록, 생활기록부, 건강기록부 등
	병역 정보	병역 여부, 군번 및 계급, 제대 유형, 근무 부대, 주특기 등
	근로 정보	직장, 고용주, 근무처, 근로 경력, 상벌 기록, 직무 평가 기록 등
	법적 정보	전과·범죄 기록, 재판 기록, 과태료 납부 내역 등
재산적 정보	**소득 정보**	봉급액, 보너스 및 수수료, 이자 소득, 사업 소득 등
	신용 정보	대출 및 담보 설정 내역, 신용카드 번호, 통장 계좌 번호, 신용 평가 정보 등
	부동산 정보	소유 주택, 토지, 자동차, 기타 소유 차량, 상점 및 건물 등
	기타 수익 정보	보험(건강, 생명 등) 가입 현황, 휴가, 병가 등
기타 정보	**통신 정보**	이메일 주소, 통화 내역, 로그 파일, 쿠키 등
	위치 정보	GPS 및 휴대폰에 의한 개인의 위치 정보
	습관 및 취미 정보	흡연 여부, 음주량, 선호하는 스포츠 및 오락, 여가 활동, 도박성 성향 등

1.2 개인정보보호법

1.2.1 개인정보보호법의 정의

중요한 개인정보를 만약 누군가 악의적인 목적으로 이용하거나 불법으로 유출한다면 개인의 안전과 재산에 큰 피해를 줄 수 있습니다. 따라서 이러한 피해를 근절하여 안전하고 신뢰할 수 있는 정보화 사회를 구현하기 위하여 마련된 법이 바로 개인정보보호법입니다.

개인정보보호법은 개인정보보호에 관해 규정한 일반법으로, 개인정보의 유출, 오용, 남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고 개인의 존엄과 가치를 구현하기 위하여 개인정보의 처리에 관한 사항을 규정하고 있습니다.

개인정보보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따르며, 2011년 3월 29일 공포되어 같은 날부터 시행되고 있습니다.

1.2.2 개인정보보호법의 제정 배경

개인정보의 중요성이 증가하고 정보화 사회로 변화하면서 데이터 활용이 더욱 증가함에 따라, 개인정보의 안전한 처리와 보호가 절실해졌습니다. 이에 따라 중복된 법령을 통합하여 일원화되지 않은 개별적인 법을 개인정보보호법으로 통합하고, 개인정보 감독 기구의 역할을 강화하여 보다 효과적인 개인정보보호를 실현하고자 하였습니다. 개인정보보호법은 개인정보의 수집, 처리, 이용, 보호 등을 체계적으로 규정하여 개인의 자기 정보 보호와 권익 보호를 강화하고, 정보 사회의 안전하고 신뢰할 수 있는 발전을 촉진하기 위해 제정되었습니다.

1.2.3 개인정보보호법의 구성

개인정보보호법은 2011년 3월 29일 제정되어 여러 차례 개정을 통해 현재는 총 10장 76조, 11개의 부칙으로 이루어져 있으며, 명령으로는 대통령령(개인정보보호법 시행령 8장 63조)이 있습니다. 행정 규칙으로는 개인정보의 안전성 확보조치 기준이 있으며 행정안전부에서 해설서를 배포하여 실무에서 활용할 수 있도록 상세한 규칙을 안내하고 있습니다. 그 외에도 다수의 행정 규칙이 있습니다.

그림 1 국내 개인정보보호 체계 일원화

1.3 개인정보의 안전성 확보조치기준

1.3.1 개인정보의 안전성 확보조치 기준이란

개인정보의 안전성 확보조치 기준은 개인정보처리자가 개인정보를 처리하는 과정에서 개인정보의 분실, 도난, 유출, 변조, 훼손을 방지하기 위해 필요한 세부적인 기준을 제시하는 것을 목적으로 합니다. 여기에는 개인정보보호 정책의 수립 및 운영과 같은 관리적 조치, 암호화 및 접근 통제와 같은 기술적 보안 요구 사항, 전산실과 자료 보관실 등의 물리적 장소에 대한 잠금장치와 반출·입 통제 절차 등의 물리적 안전 조치가 포함됩니다. 또한, 개인정보보호법 시행령의 정보통신서비스 특례규정(영 제48조의 2)이 일반규정(영 제30조)으로 통합됨에 따라 '개인정보의 안전성 확보조치 기준'과 '개인정보의 기술적·관리적 보호조치 기준'이 통합되었고, 공공시스템 운영기관 등에 대한 특례 규정(영 제30조의 2)이 신설됨에 따라 고시 위임 사항인 공공시스템 지정 기준 및 공공시스템 운영기관의 안전조치 기준이 신설되어 공공시스템 운영기관의 개인정보보호를 강화하기 위한 조치가 이루어졌습니다. 이 기준은 법적 효력을 가지며, 이를 위반할 시 과태료 및 과징금이 부과될 수 있습니다.

1.3.2 개인정보의 안전성 확보조치 기준 구성

해당 기준은 제1장 총칙, 제2장 개인정보의 안전성 확보조치, 제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치로 총 3장 제18조로 구성되어 있으며 각 내용은 아래와 같이 세부 구성되어 있습니다.

표 2 개인정보의 안전성 확보조치 기준

구분	항목
제1장 총칙	제1조 목적
	제2조 정의
제2조 개인정보의 안전성 확보조치	제3조(안전 조치의 적용 원칙)
	제4조(내부 관리 계획의 수립 · 시행 및 점검)
	제5조(접근 권한의 관리)
	제6조(접근 통제)
	제7조(개인정보의 암호화)
	제8조(접속 기록의 보관 및 점검)
	제9조(악성 프로그램 등 방지)
	제10조(물리적 안전 조치)
	제11조(재해 · 재난 대비 안전 조치)
	제12조(출력 · 복사 시 안전 조치)
	제13조(개인정보의 파기)
제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치	제14조(공공시스템 운영기관의 안전 조치 기준 적용)

제3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치	제15조(공공시스템 운영기관의 내부 관리 계획의 수립 · 시행)
	제16조(공공시스템 운영기관의 접근 권한의 관리)
	제17조(공공시스템 운영기관의 접속 기록의 보관 및 점검)
	제18조(재검토 기한)

※ 개인정보의 안전성 확보조치 기준

2 개인정보의 안전성 확보 방안

2.1 NHN Cloud를 이용한 개인정보보호 방안

NHN Cloud는 개인정보 및 데이터 보호를 위해 다양한 보안 서비스와 기능을 제공하고 있습니다.
본 가이드는 개인정보의 안전성 확보조치 기준을 준수하기 위해 NHN Cloud의 다양한 서비스와 기능을 활용하여 기술적으로 구현할 수 있는 방법을 제시합니다. 정책, 절차 등 관리적 부분과 물리적 안전 조치에 대한 내용은 본 가이드에 포함되지 않으므로, 별도의 보호 대책 수립이 필요합니다.

2.1.1 접근 권한의 관리

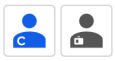
접근 권한 관리는 개인정보에 접근할 수 있는 권한을 부여하고, 이를 관리하는 절차를 의미합니다. 권한이 없는 자의 접근을 차단하고, 접근 권한이 있는 자의 경우에도 최소한의 범위 내에서만 접근할 수 있도록 제한합니다.

표 3 NHN Cloud의 접근 권한 관리 서비스

구분	NHN Cloud 서비스 활용
접근 권한을 최소한의 범위로 차등 부여 **접근 권한 변경 또는 말소 관리** **접근 권한 부여, 변경 또는 말소에 대한 내역 기록 및 보관(최소 3년)** **개인정보 취급자별 개별 계정 발급**	• **조직 멤버 관리**로 역할(OWNER/ADMIN/MEMBER/Billing Viewer/Log Viewer)에 따른 권한 부여 • **프로젝트 관리**로 서비스별 권한(생성/읽기/갱신/삭제) 차등 부여 • 기본(무료)으로 제공되는 **CloudTrail** 서비스로 접근 권한 내역 기록 및 관리 • CloudTrail과 **Object Storage** 연동을 통해 접근 권한 기록 3년 이상 보관
안전한 인증 수단 적용 **인증에 실패한 경우 접근 제한**	• 조직 거버넌스 설정을 통해 **IP 접근 통제 설정** • **IAM 거버넌스 설정 > 로그인 보안 설정**으로 2차 인증(OTP, 이메일/휴대폰), 로그인 실패 횟수 제한, 로그인 세션 시간, 비밀번호 정책 설정(최소 길이, 강도, 만료 기간, 재사용 제한)

계정 및 서비스 활동 로깅


Object Storage
확장 가능한 대용량 스토리지

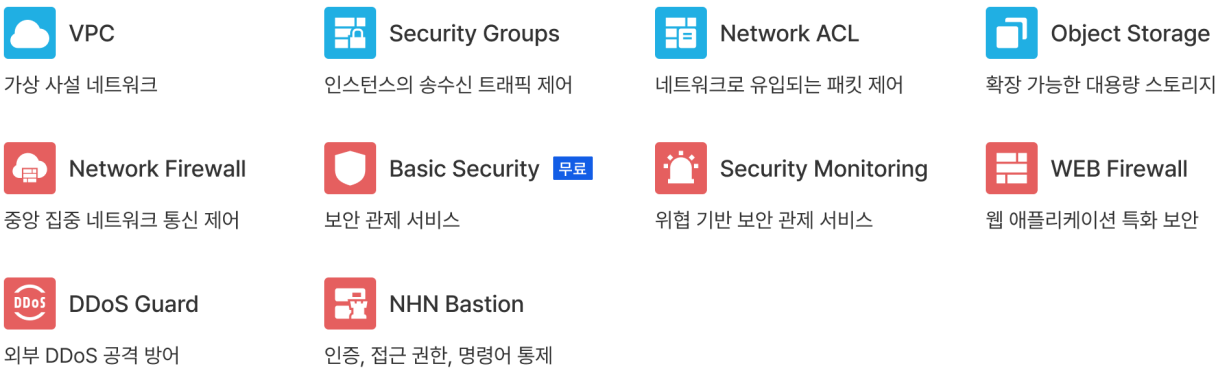

NHN Cloud·IAM Member
역할 및 권한 세분화

2.1.2 접근 통제

접근 통제는 개인정보의 무단 접근을 방지하기 위한 다양한 기술적 조치를 의미합니다. IP, MAC, 방화벽 등의 방법으로 접속 권한을 제한해야 하며, 불법적인 개인정보 유출 시도를 탐지하고 대응해야 합니다.

표 4 NHN Cloud의 접근 통제 서비스

구분	NHN Cloud 서비스 활용
정보통신망을 통한 불법적인 접근 및 침해 사고 방지 • IP 접근 통제 • 개인정보 유출 시도 탐지 및 대응	• **VPC**(virtual private cloud)로 논리적으로 격리된 가상의 네트워크 구성 • 조직 거버넌스 설정을 통해 **IP 접근 통제 설정** • **Security Groups**으로 인스턴스의 송수신 트래픽 제어 • **Network ACL**을 사용한 네트워크로 유입되는 트래픽 제어 • **Network Firewall**을 사용한 허브 앤 스포크(hub-spoke) 구조의 트래픽 제어 및 외부 공격 방어 • **Object Storage**의 테넌트 또는 개별 사용자 역할 기반 및 IP ACL을 통한 접근 정책 관리 • 무료 보안 서비스인 **Basic Security**로 기본적인 위협 보안 모니터링 대응 • **Security Monitoring**으로 전문적인 침해 위협 모니터링 대응(보안 관제) • 웹 애플리케이션 공격에 대한 탐지와 대응을 위해 **WEB Firewall**로 보안성 강화 • 외부로부터의 DDoS 공격을 신속하게 탐지하고 차단하기 위한 **DDoS Guard** • 인스턴스 SSH 접근 시 **NHN Bastion**을 사용하여 인증, 접근 권한, 명령어 통제를 통해 보안성을 강화
정보통신망을 통한 외부에서의 접속 시 안전한 인증 수단 적용	• NHN Cloud 사용자 관리 체계에 따라 영문 대소문자, 숫자, 특수 문자를 조합하여 최소 8자리 이상의 안전한 **비밀번호 정책** 준수 • **IAM 거버넌스 설정 > 로그인 보안 설정**으로 2차 인증(OTP, 이메일/휴대폰), 로그인 실패 횟수 제한, 로그인 세션 시간, 비밀번호 정책 설정(최소 길이, 강도, 만료 기간, 재사용 제한) • NHN Cloud 회원 및 IAM 멤버 모두 이용자가 직접 주기적으로 비밀번호를 변경하여 관리
일정 시간 업무를 처리하지 않는 경우 자동 접속 차단(시스템 접속 시간 제한/ 로그인 세션 시간 설정)	• **IAM 거버넌스 설정 > 로그인 보안 설정**으로 2차 인증(OTP, 이메일/휴대폰), 로그인 실패 횟수 제한, 로그인 세션 시간, 비밀번호 정책 설정(최소 길이, 강도, 만료 기간, 재사용 제한) • 시스템(인스턴스/DB)의 세션 시간 초과 설정
개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치	• **VPC**(virtual private cloud)로 논리적으로 격리된 가상의 네트워크 분리 구성 및 운영 • **Virtual Desktop**을 이용해 사용자 업무 특성에 맞는 독립적인 가상 PC 관리 • 망 연계 솔루션을 이용한 논리적 망 분리 클라우드 서비스 환경 구성

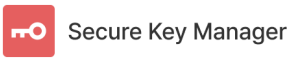


2.1.3 개인정보의 암호화

개인정보의 암호화는 개인정보를 안전하게 보호하기 위해 암호화 알고리즘을 적용하는 것을 의미합니다. NHN Cloud는 강력한 암호화 기술을 사용하여 개인정보를 안전하게 보호합니다.

표 5 NHN Cloud의 개인정보 암호화 서비스

구분	NHN Cloud 서비스 활용
인증 정보 저장 및 송·수신 시 안전한 암호 알고리즘 적용 (비밀번호 일방향 암호화)	• NHN Cloud 이용자가 접속하는 NHN Cloud 콘솔은 SSL 기반의 암호화된 통신 환경 • 비밀번호와 같은 인증 정보에 대하여 SHA-256 이상의 해시 함수를 사용하여 최소 128bit 이상의 보안 강도 유지
이용자의 개인정보 저장 시 안전한 암호 알고리즘 적용	• **Secure Key Manager** 서비스를 이용한 개인정보 및 중요 데이터의 암·복호화
개인정보 송·수신 시 암호화 적용	• NHN Cloud 이용자가 접속하는 NHN Cloud 콘솔은 SSL 기반의 암호화된 통신 환경 • 공공기관용 클라우드 시스템 접속 시 암호화 접속 수단(SSH) 이용, 외부 접속 시 IPSec VPN 또는 SSL VPN 적용하여 2차 인증 후 접속 • 고객이 구성한 애플리케이션의 송·수신 암호화 적용은 별도 구성 필요
개인정보 저장 시 암호화	
안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차 수립 및 시행	• Secure Key Manager의 Life-Cycle 기능으로 암호 키 관리 • 조직 거버넌스의 **승인 기능**을 통해 키 생성, 수정, 삭제 시 관리자의 승인 프로세스 수립



중요 정보 암호화 저장 관리 서비스

IPSec 암호화 터널링 통신

SSL 프로토콜, 인증, 암호화 터널링

VPC와 온프레미스 네트워크 IPSec VPN 연결

2.1.4 접속 기록의 보관 및 점검

접속 기록의 보관 및 점검은 개인정보에 대한 접근 내역을 기록하고, 이를 주기적으로 점검하여 이상 징후를 조기에 발견하고 대응하는 절차를 의미합니다. NHN Cloud는 접속 기록을 안전하게 보관하며, 정기적인 점검을 통해 보안 위협을 최소화합니다.

표 6 NHN Cloud의 접속 기록 보관 및 점검 서비스

구분	NHN Cloud 서비스 활용
접속 기록 1년 이상 보관·관리 • 5만 명 이상의 정보 주체, 고유 식별 정보 또는 민감정보 처리 시스템 (2년 이상 보관)	• **CloudTrail** 서비스로 조직/프로젝트/멤버별 계정 및 서비스 활동 로그 확인 (3개월 무료 제공) • CloudTrail과 **Object Storage** 연동을 통해 접근 권한 기록 1년 이상 보관 및 백업 • **Log & Crash Search** 서비스로 개인정보 처리 시스템의 로그 조회, 분석 및 외부 로그 보관(Object Storage) 설정 시 로그 변조 알림 사용 • **SIEM** 서비스로 개인정보 처리 시스템 및 보안 솔루션 로그, 이벤트 분석으로 보안 위협 식별 및 대응 • **Backup** 서비스로 중요 데이터 및 접속 기록을 안전하게 보관 • **Network Firewall** 로그 원격 전송 설정을 통해 허용·차단 로그 전송 및 저장
개인정보 처리 시스템의 접속 기록 월 1회 이상 점검	
접속 기록의 안전한 보관 (접속 기록 백업)	

CloudTrail 무료
계정 및 서비스 활동 로깅

Object Storage
확장 가능한 대용량 스토리지

Log & Crash search
로그 수집 및 분석 서비스

SIEM
로그 분석 및 가시성 확보

Backup
중요 데이터 보관

Network Firewall
중앙 집중 네트워크 통신 제어

2.1.5 악성 프로그램 등 방지

악성 프로그램 등의 방지는 바이러스, 스파이웨어, 랜섬웨어 등 악성 프로그램으로부터 개인정보를 보호하기 위한 기술적 조치를 의미합니다. NHN Cloud는 최신 백신 프로그램을 사용하여 악성 프로그램의 침투를 방지합니다.

표 7 NHN Cloud의 악성 프로그램 방지 서비스

구분	NHN Cloud 서비스 활용
보안 프로그램 설치 및 운영 • 자동 또는 일 1회 이상 업데이트 • 악성 프로그램 삭제 등 조치(신규 보안 업데이트 즉시 실시)	• **Vaccine** 서비스로 인스턴스에 백신을 설치하여 실시간 및 수동 스캔, 최신 탐지 패턴 업데이트, 멀웨어 차단, 이벤트 탐지 현황 모니터링

Vaccine
악성 프로그램 방지를 위한 보안 프로그램

2.1.6 재해·재난 대비 안전 조치

재해 및 재난 대비 안전 조치는 자연재해나 인재로 인한 데이터 손실을 예방하기 위한 조치를 의미합니다. NHN Cloud는 리전 이중화와 데이터 백업 및 복구 시스템을 통해 재해 발생 시에도 개인정보를 안전하게 보호합니다.

표 8 NHN Cloud의 재해·재난 대비 안전 조치

구분	NHN Cloud 서비스 활용
위기 대응 매뉴얼 등 대응 절차 수립 및 점검	• NHN Cloud 리전, 가용성 영역을 이용한 서비스 이중화 및 DR 환경 구성 • **DNS Plus** GSLB(global server load balancing)의 DNS 기반으로 서비스 DR 구성
개인정보 처리 시스템 백업 및 복구 계획	• **Backup** 서비스로 중요 데이터 백업 및 복구를 위한 환경 구성

DNS Plus
DNS 기반 로드밸런싱

Backup
중요 데이터 보관

2.1.7 개인정보의 파기

개인정보처리자는 개인정보를 파기할 경우 데이터가 복원되지 않도록 완전 파괴, 삭제, 초기화 등을 수행해야 합니다.

표 8 NHN Cloud 서비스의 개인정보 파기 기능

구분	NHN Cloud 서비스 활용
개인정보 완전 파괴, 삭제 및 초기화 또는 덮어쓰기	• NHN Cloud 데이터 완전 삭제 가이드를 이용해 인스턴스 및 스토리지 해제 후 데이터 삭제(DoD 52202.22-M) • **Block Storage 데이터 완전 삭제 가이드** • **Virtual Desktop**을 이용해 독립적인 가상 PC 이용, 높은 보안 기준 적용, 사용 완료 후 가상 PC 삭제
개인정보 복구 및 복원 불가능하도록 조치	※ 이용자의 서비스 종료 시 NHN Cloud는 데이터 삭제 프로세스에 따라 자동으로 데이터 삭제를 진행하며, 사용 기한이 지난 디스크는 완전 파괴 절차를 수행하고 있습니다.

Virtual Desktop
독립적인 개인 업무 환경 접속

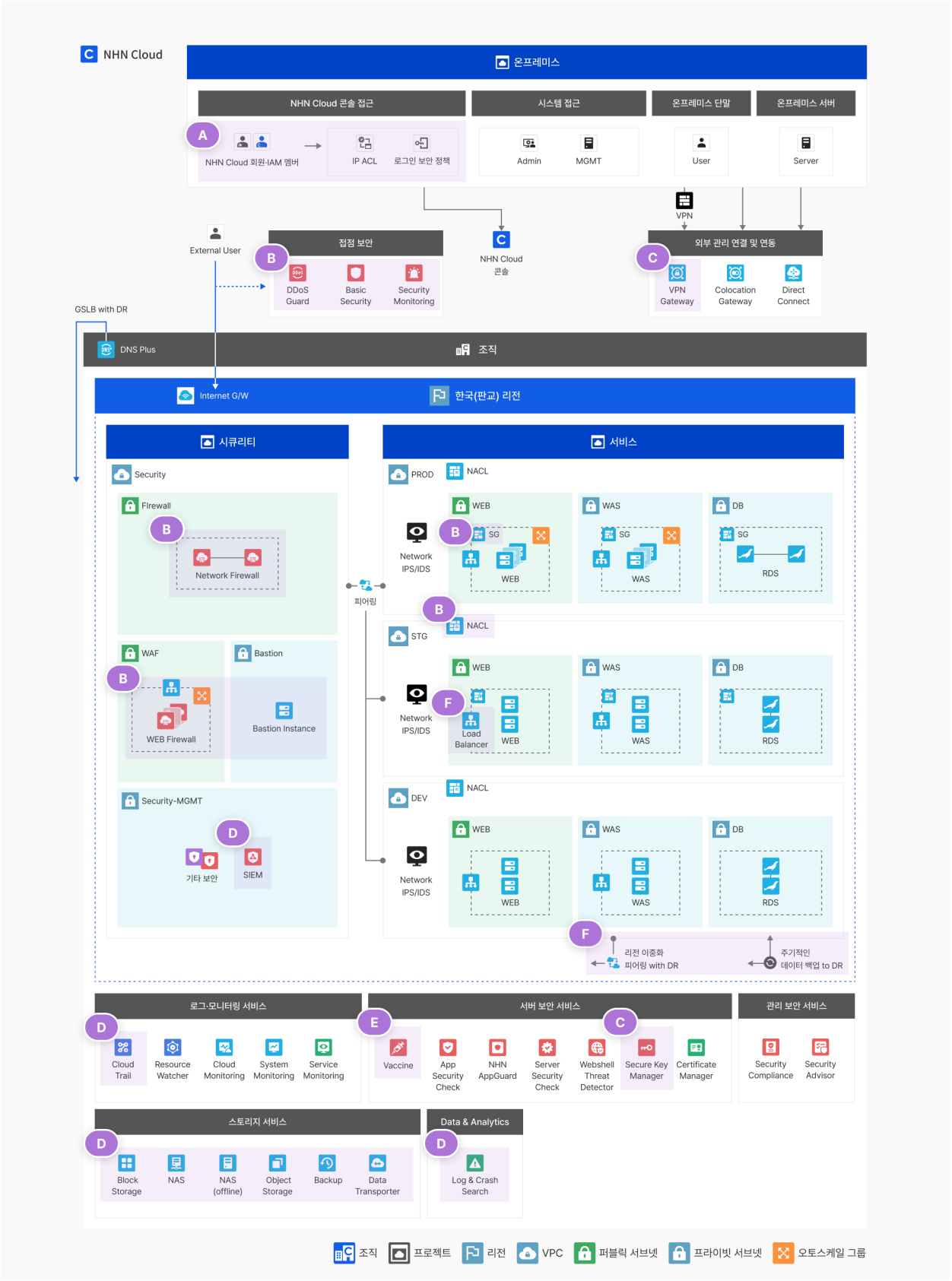
3 마무리

개인정보보호는 오늘날 클라우드 서비스 공급자에게 있어 필수적인 요소입니다. NHN Cloud는 최신 보안 기술과 엄격한 보안 정책을 통해 고객의 개인정보를 안전하게 보호하며, 지속적인 보안 강화를 통해 신뢰할 수 있는 클라우드 서비스를 제공하고자 최선을 다하고 있습니다. 이 가이드가 NHN Cloud를 이용하는 모든 고객에게 개인정보보호에 대한 신뢰와 안정적인 서비스를 제공하는 데 기여하길 바랍니다.

NHN Cloud의 보안 서비스 및 가이드

- **NHN Cloud 보안 서비스**
- **NHN Cloud 보안 가이드**

개인정보 안전성 확보조치 기준 적용 구성안



A 접근 권한의 관리 B 접근 통제 C 개인정보의 암호화 D 접속 기록의 보관 및 점검 E 악성프로그램 방지
F 재해·재난 대비 안전 조치

그림 2 NHN Cloud 개인정보 안전성 확보조치 구성안

엔에이치엔클라우드

13487 경기도 성남시 분당구 대왕판교로645번길 16 NHN 플레이뮤지엄

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