네이버 클라우드 플랫폼 보안 모범 사례

NAVER Cloud Platform

Security Best Practices

NAVER Cloud

목차

Section1. 네이버 클라우드 플랫폼 보안 개요

1. 클라우드 책임 공유 모델의 이해
2. 네이버 클라우드 플랫폼 보안 상품 현황
3. 온 프레미스 환경의 보안 서비스와 네이버 클라우드 플랫폼의 보안 서비스
4. 정보보호 인증 획득 현황

Section2. 클라우드 계정 관리

1. 클라우드 계정 관리의 이해
2. Account 구성
3. Sub Account 를 통한 직무 분리
4. Account 보안 설정

Section3. 클라우드 인프라 보호

1. 클라우드 인프라 보호의 이해
2. 네이버 클라우드 플랫폼의 VPC
3. Security Monitoring
4. 인프라 보안 아키텍처

Section4. 클라우드 리소스 보호

1. 클라우드 환경의 IT 자원
2. 데이터 보호를 위한 클라우드 서비스
3. 취약점 관리를 위한 클라우드 서비스
4. 전송 구간 암호화를 위한 클라우드 서비스
5. 보안 위협 탐지 및 대응을 위한 클라우드 서비스

Section5. 클라우드 환경 보안 감사

1. 클라우드 환경의 보안 규제
2. 네이버 클라우드 플랫폼 보안 감사
3. Cloud Activity Tracer 보안 감사 시나리오

그림 목차

Section1. 네이버 클라우드 플랫폼 보안 개요

그림 1-1. NAVER Cloud Platform의 책임 공유 모델
그림 1-2. NAVER Cloud Platform Security Map
그림 1-3. NAVER Cloud Platform의 정보보호 인증 획득 현황

Section2. 클라우드 계정 관리

그림 2-1. 클라우드 환경의 Account 종류
그림 2-2. 클라우드 환경의 Account 구성 요소별 상관 관계
그림 2-3. Sub Account를 통한 직무 분리 예제

Section3. 클라우드 인프라 보호

그림 3-1. 다중 VPC 구성 예제
그림 3-2. 서브넷 구분 예제
그림 3-3. VPC Flow Log 항목
그림 3-4. Security Monitoring 대응 프로세스
그림 3-5. 클라우드 인프라 보안 아키텍처 예제

Section4. 클라우드 리소스 보호

그림 4-1. NAVER Cloud Platform의 리소스 보호 서비스
그림 4-2. KMS를 이용한 데이터 암·복호화
그림 4-3. KMS 키 관리 정책
그림 4-4. KMS 사용자 콘솔 화면
그림 4-5. HSM 서비스 구성
그림 4-6. Certificate Manager 서비스 구성
그림 4-7. Cloud Advisor 콘솔 화면
그림 4-8. Cloud Advisor 점검 항목
그림 4-9. App Security Checker 사용 프로세스
그림 4-10. Web Security Checker 서비스 구성
그림 4-11. SSL VPN 서비스 구성
그림 4-12. Cloud Connect 서비스 구성
그림 4-13. Ipsec VPN 서비스 구성
그림 4-14. File Safer 이용 프로세스
그림 4-15. App Safer 이용 프로세스
그림 4-16. Site Safer 이용 프로세스
그림 4-17. 악성 웹 사이트를 통한 사용자 공격 프로세스
그림 4-18. Webshell 공격 프로세스
그림 4-19. Webshell Behavior Detector 서비스 구성

Section5. 클라우드 환경 보안 감사

그림 5-1. Cloud Activity Tracer를 이용한 보안 감사

표 목차

Section1. 네이버 클라우드 플랫폼 보안 개요

표 1-1. On-Premises의 Security와 NAVER Cloud Platform의 Security

Section2. 클라우드 계정 관리

Section3. 클라우드 인프라 보호

표 3-1. ACG와 Network ACL 비교

Section4. 클라우드 리소스 보호

표 4-1. KMS 활용을 통한 인증 및 법률 준수

표 4-2. HSM 활용을 통한 인증 및 법률 준수

표 4-3. Certificate Manager 활용을 통한 인증 및 법률 준수

표 4-4. Cloud Advisor 활용을 통한 인증 및 법률 준수

표 4-5. System Security Checker의 지원 운영체제 및 WAS

표 4-6. Web Security Checker 활용을 통한 인증 및 법률 준수

표 4-7. SSL VPN 활용을 통한 인증 및 법률 준수

표 4-8. Cloud Connect 활용을 통한 인증 및 법률 준수

표 4-9. SSL VPN, IPsec VPN, Cloud Connect 비교

표 4-10. Safer 시리즈 활용을 통한 인증 및 법률 준수

표 4-11. Webshell Behavior Detector 활용을 통한 인증 및 법률 준수

Section5. 클라우드 환경 보안 감사

서론

글로벌 IT 자문기관인 가트너는 국내 퍼블릭 클라우드 서비스 시장 규모가 2019년 2조 3427억 원, 2020년 2조 7818억 원에서 2021년 3조 2400억 원, 2022년 3조 7238억 원까지 급성장할 것이라고 전망했습니다. 향후 클라우드 서비스 시장의 성장세에 대해서는 "2022년까지 전체 IT 서비스 성장세의 약 3배에 이를 것"이라고 덧붙였습니다.
또한 코로나19로 인해 확산된 언택트(Untact) 문화가 클라우드 시장 확대에 모멘텀으로 작용하며 클라우드 전환은 더욱 가속화될 것으로 예상했습니다.

하지만 이러한 전망에도 불구하고 기업(또는 개인)에서는 보안 문제에 대한 우려로 클라우드 도입을 어렵게 인식하고 있습니다.

분명 클라우드 환경의 보안은 기존 온 프레미스(On-premis) 환경의 보안과 달라진 점이 있습니다. 하지만 신뢰할 만한 기술과 노하우를 가진 검증된 클라우드 서비스 제공자가 이를 체계적으로 구축한다면 보안은 클라우드 도입에 있어 유의미한 허들로 작용하지 않습니다.

네이버 클라우드 플랫폼(NAVER Cloud Platform)은 공인된 인증 기관을 통해 다수의 보안 관련 인증을 획득했습니다. 인증된 기술을 토대로 온·오프라인을 아우르는 클라우드 보안 인프라와 서비스를 제공합니다. 네이버 클라우드 플랫폼의 보안 서비스를 사용한다면 클라우드 환경에서도 안전하게 서비스를 구성하고 운영할 수 있습니다.

이 백서에서는 지금 이 순간에도 수많은 고객들의 경험을 통해 지속적으로 안정성이 입증되고 있는 네이버 클라우드 플랫폼의 보안 서비스를 설명하고 이용 사례를 소개합니다.

Section 1. 네이버 클라우드 플랫폼 보안 개요

1 클라우드 책임 공유 모델의 이해

네이버 클라우드 플랫폼이 제공하는 글로벌 수준의 클라우드 보안 서비스는 네이버 클라우드 플랫폼의 클라우드 책임 공유 모델을 이해하는 것에서 시작합니다.
클라우드 책임 공유 모델이란, 클라우드에 구성한 고객의 리소스를 안전하게 보호할 수 있도록 클라우드 서비스 제공자와 고객이 각각 역할을 나누어 함께 책임을 다하는 것입니다. 이를 위해 고객의 책임 영역과 클라우드 서비스 제공자인 네이버 클라우드 플랫폼의 책임 영역을 명확하게 구분하고 있습니다.
우선 클라우드 서비스 제공자인 네이버 클라우드 플랫폼은 보안 인프라를 제공합니다. 네이버 클라우드 플랫폼의 클라우드 인프라 스트럭처에 대한 보안을 책임지는 일입니다. 인프라란, 네이버 클라우드 서비스 구성의 근간이 되는 하드웨어, 네트워크 및 시설 등을 의미합니다.
고객은 고객의 책임 영역에 협력합니다. IaaS, PaaS, SaaS 등 서비스 모델에 따른 운영체제, 애플리케이션, 데이터 보안을 고객 정책에 맞게 직접 설정하고 보호하는 일입니다. 고객이 효과적인 보안 환경을 구성할 수 있도록 네이버 클라우드 플랫폼은 다양한 보안 서비스도 제공하고 있습니다.

Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data	Tenant	Tenant	Tenant
Interfaces(APIs, GUIs)	Tenant	Tenant	Tenant / NAVER Cloud Platform
Applications	Tenant	Tenant	NAVER Cloud Platform
Solution Stack(Programming languages)	Tenant	Tenant	NAVER Cloud Platform
Operation Systems(OS)	Tenant	NAVER Cloud Platform	NAVER Cloud Platform
Virtual Machines	Tenant	NAVER Cloud Platform	NAVER Cloud Platform
Hypervisors	NAVER Cloud Platform	NAVER Cloud Platform	NAVER Cloud Platform
Processing and Memory	NAVER Cloud Platform	NAVER Cloud Platform	NAVER Cloud Platform
Data Storage(hard drivers, removable disks, backups, etc.)	NAVER Cloud Platform	NAVER Cloud Platform	NAVER Cloud Platform
Network(Interfaces and devices, communications infrastructure)	NAVER Cloud Platform	NAVER Cloud Platform	NAVER Cloud Platform
Physical facilities / data centers	NAVER Cloud Platform	NAVER Cloud Platform	NAVER Cloud Platform

[그림 1-1 : NAVER Cloud Platform의 책임 공유 모델]

2

네이버 클라우드 플랫폼 보안 상품 현황

네이버 클라우드 플랫폼은 고객이 책임 영역에 대한 보안 시스템을 효과적으로 구성할 수 있도록 다양한 보안 서비스를 지원합니다. 다음에 소개될 NAVER Cloud Platform Security Map을 통해 각 서비스 상품이 어떤 카테고리의 영역을 보호할 수 있는지 설명합니다.

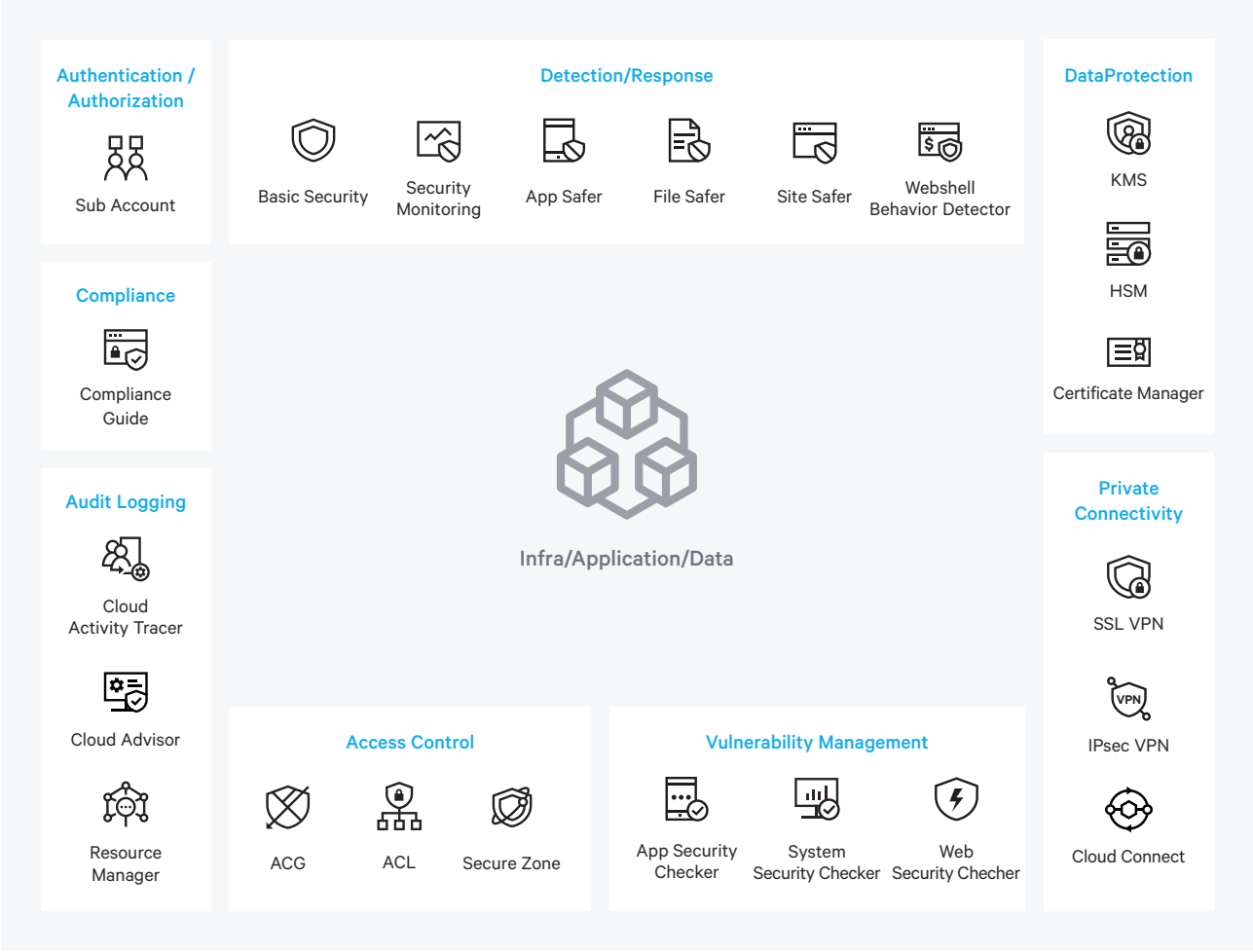
네이버 클라우드 플랫폼은 위협 탐지 대응, 사용자 인증, 접근 통제, 데이터 보호, 감사 추적, 취약점 관리, 컴플라이언스, 전송 구간 암호화의 총 8개 영역에 대한 보안 서비스를 제공합니다.

위협 탐지 대응 (Detection/Response)

위협 탐지 대응 영역의 Security Monitoring 상품은 Anti-DDoS, IDS, IPS, WAF, Anti-Virus와 같은 다양한 기능을 제공하며, 전문 인력을 통해 365일 24시간 실시간으로 서비스를 안전하게 보호하는 Managed 서비스입니다. 이외에도 모바일 애플리케이션, 웹 사이트, 파일 등에 대한 보안 위협을 탐지하여 대응합니다.

사용자 인증 (Authentication/Authorization)

사용자 인증 영역의 Sub Account 상품은 역할 기반의 권한 관리 서비스입니다. 내부 사용자를 서브 계정으로 등록한 다음 특정 서비스에 대한 권한을 부여할 수 있습니다.



[그림 1-2 : NAVER Cloud Platform Security Map]

접근 통제 (Access Control)

접근 통제 영역의 상품들은 레거시 환경의 방화벽과 동일한 역할을 제공하는 서비스입니다.

데이터 보호 (Data Protection)

데이터 보호 영역의 상품들은 암·복호화 키와 연동 서비스에서 사용할 인증서를 안전하게 보호하는 역할을 제공하는 서비스입니다.

감사 추적(Audit Logging)

감사 추적 영역의 상품들은 클라우드 환경 리소스의 통합 관리 및 리소스 수정, 삭제 로그를 제공하거나 안전한 이용 권장 지침을 제공하는 서비스입니다.

취약점 관리(Vulnerability Management)

취약점 영역의 상품들은 웹, 앱, 서버 운영체제 및 WAS 시스템에 대한 취약점을 간편하게 진단하고 보안 가이드를 제공하는 서비스입니다.

컴플라이언스(Compliance)

컴플라이언스 영역의 상품은 고객이 보안 인증이나 규제에 대응하는 데에 필요한 사항을 알기 쉽게 정리한 가이드를 제공하는 서비스입니다.

전송 구간 암호화(Private Connectivity)

전송 구간 암호화 영역의 상품은 네이버 클라우드 플랫폼에 생성된 리소스에 안전하게 접근할 수 있도록 도와주는 서비스입니다.

3 온 프레미스 환경의 보안 서비스와 네이버 클라우드 플랫폼의 보안 서비스

온 프레미스 환경의 보안 서비스 라인 업과 대조하여 살펴 본다면 네이버 클라우드 플랫폼의 보안 서비스 구성을 좀 더 쉽고 효과적으로 이해할 수 있습니다.
온 프레미스 환경에서 사용하던 보안 서비스를 클라우드 환경에서도 동일하게 사용할 수 있도록 네이버 클라우드 플랫폼에서는 지원하고 있습니다. 네이버 클라우드 플랫폼이 기본적으로 제공하는 보안 서비스 외에도 마켓플레이스(Marketplace)에 등록되어 있는 다양하게 특화된 보안 솔루션을 통해 안전한 클라우드 환경을 섬세하게 구축할 수 있습니다.

구분	On-premises Security	NAVER Cloud Platform Security
Network	DDoS	Security Monitoring
	방화벽	ACG(Access Control Group)
	IDS/IPS	Security Monitoring
	전송 구간 암호화	IPsec/SSL VPN, Cloud Connect
DB	DB 접근 통제	NAVER Cloud Platform Marketplace
	DB 암호화	NAVER Cloud Platform Marketplace
Server	서버 접근 통제	SSL VPN, NAVER Cloud Platform Marketplace
	서버 보안 (SecureOS)	NAVER Cloud Platform Marketplace
	Anti-Virus	Security Monitoring
Application	웹 방화벽	Security Monitoring
	Anti-Webshell	Webshell Behavior Detector
User Access	사용자 접근 통제	Sub Account
Audit	-	Cloud Activity Tracer, Resource Manager

[표 1-1 : On-Premises의 Security와 NAVER Cloud Platform의 Security]

4 정보보호 인증 획득 현황

네이버 클라우드 플랫폼은 국내　외 다양한 보안 인증을 획득하여 규제, 표준, 모범 사례를 준수하고 있습니다.
국제 클라우드 보안 협회(CSA)의 클라우드 서비스 역량 수준을 정량적으로 측정하는 CSA Star 인증의 최고 등급인 Gold 등급을 획득했으며, 클라우드 보안 인증제 CSAP(Cloud Security Assurance Program), ISMS-P, ISO27001 등 다수의 인증도 획득했습니다.
네이버 클라우드 플랫폼은 인증, 규제 준수를 바탕으로 다양한 분야의 인터넷 기업과 스타트 업, 대기업 뿐만 아니라 공공, 금융, 의료 고객들이 클라우드 서비스를 안전하게 이용할 수 있도록 보안 환경 조성에 힘쓰고 있습니다.

클라우드컴퓨팅서비스 보안인증[IaaS, SaaS]

공공기관에게 안전성 및 신뢰성이 검증된 클라우드 서비스를 공급할 수 있는지 판단할 수 있는 기준이며, 국내 유일의 SaaS 인증 보유 사업자

글로벌 서비스 통제수준 표준인증 SOC 1,2,3 인증

글로벌 수준의 내부통제가 구현 운영되고 있다는 것을 독립적인 감사인을 통해 증명

글로벌 클라우드 통제수준 표준인증 CSA STAR 인증

국제 클라우드 보안협회(CSA)의 클라우드 서비스 역량 수준을 정량적으로 측정하는 CSA Star 인증의 최고 등급 (Gold)을 획득한 국내 유일의 클라우드 사업자

정보보호관리체계 인증 ISMS/ISMS-P 인증

기업이 전사 정보보호 및 개인정보보호를 위해 지속적 보호 활동을 수행하고 있는지, 해당 보호활동을 통해 적절한 정보보호 수준을 유지하고 있는지 점검하여 일정수준 이상의 기업에 대해 인증을 부여하는 제도

지불카드 산업 정보 보호 표준인증 PCI DSS 인증

네이버 클라우드 플랫폼의 Application, Hardware, Infrastructure 등 11가지 영역이 결제 정보를 안전하게 보호할 수 있음을 검증

글로벌 클라우드 개인정보보호 표준인증 ISO 27018

의료정보보호 시스템 인증 ISO 27799

글로벌 정보보호 관리체계 인증 ISO 27001

글로벌 클라우드 보안 표준인증 ISO 27017

비즈니스 연속성 국제 표준인증 ISO 22301

정보보호관리체계, 클라우드서비스 관리체계, 클라우드 서비스 개인정보보호, 개인의료정보보호, 비즈니스 연속성 국제 표준 인증을 모두 획득한 클라우드 사업자

[그림 1-3 : NAVER Cloud Platform의 정보보호 인증 획득 현황]

Section 2. 클라우드 계정 관리

1 클라우드 계정 관리의 이해

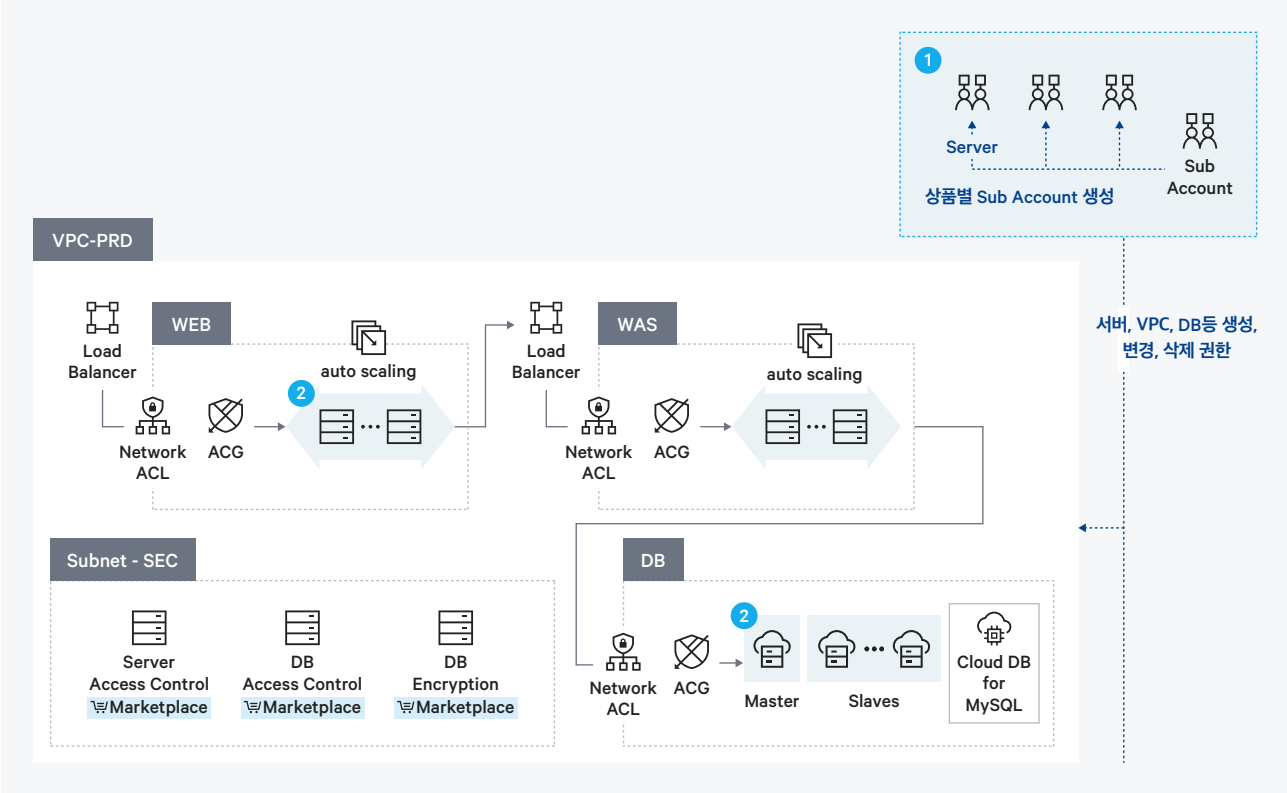
클라우드 환경에서 Account(계정)는 크게 두 가지 종류로 구분합니다. 첫 번째 종류는 리소스를 생성, 변경, 삭제, 관리할 수 있는 클라우드 콘솔 계정입니다. 두 번째 종류는 생성한 리소스에 접속하여 개발이나 운영을 수행할 수 있는 리소스 계정입니다.

클라우드 콘솔 계정

리소스(서버, 데이터베이스 등)를 생성/변경/삭제 관리를 위한 계정

리소스 계정

리소스(서버, 데이터베이스 등)에 접속하여 개발/운영 수행을 위한 계정



[그림 2-1 : 클라우드 환경의 Account 종류]

네이버 클라우드 플랫폼에서 콘솔 계정 관리를 위해 사용하는 상품은 Main Account, Sub Account입니다.

Main Account은 네이버 클라우드 플랫폼 포털에 회원 가입 시 사용한 메일 주소입니다. Main Account 상품의 사용자는 모든 상품을 관리할 수 있는 권한을 가집니다. 또한 Sub Account 상품을 통해 콘솔에 접속할 수 있는 계정을 생성할 수 있고, Sub Account 각 계정별로 역할에 맞게 권한을 부여함으로써 체계적인 접근 제어를 할 수 있습니다.

Main Account 사용자를 통해 권한을 부여 받은 Sub Account 사용자는 부여 받은 권한에 따라 상품을 관리합니다.

2

Account 구성

클라우드 환경의 Account는 앞서 살펴 본 Main Account, Sub Account로 구분되며, 여기에 Group(그룹), Polices(정책) 개념과 더불어 완전한 구성을 이룹니다.
Main Account는 Sub Account를 통해 생성된 계정이 접속할 수 있는 전용 도메인을 생성할 수 있으며, 그룹과 정책도 생성할 수 있습니다. 그룹의 반영과 정책의 반영 또한 Main Account를 통해서만 가능합니다. 클라우드 환경의 Account를 구성하는 각 요소에 대한 자세한 설명은 다음과 같습니다.

Main Account

기본적으로 네이버 클라우드 플랫폼의 전체 리소스를 관리합니다. Sub Account 사용자를 생성할 수 있으며, Tennant가 독립적으로 접근 가능한 콘솔 도메인을 생성할 수 있습니다.

Sub Account

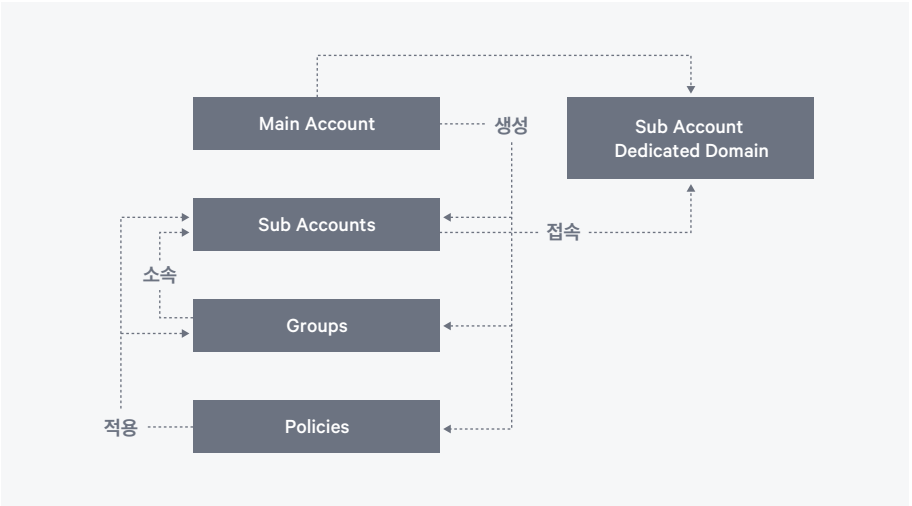
Main Account는 RBAC(Role-Based Access Control) 기능을 통한 권한 관리를 Sub Account를 통해 구현합니다. 주요 직무자를 식별할 수 있도록 네이밍 규칙을 통해 사용자를 생성하고, 권한을 부여하여 관리할 수 있습니다.

Group

동일한 역할을 수행하는 사용자를 하나의 그룹으로 묶어 관리합니다.

Policies

Sub Accounts 사용자와 Group별로 권한을 부여합니다.



[그림 2-2 : 클라우드 환경의 Account 구성 요소별 상관 관계]

3

Sub Account를 통한 직무 분리

회사의 내부 규정에 따라 직무를 분리하고 권한을 부여하는 것을 Sub Account를 통해 구현할 수 있습니다. 단, 권한은 직무에 따라 최소한으로 부여해야 합니다.
다음 이용 사례에서는 보안 관점에서 Sub Account를 통해 클라우드 전체 관리자(Main Account), 보안 담당자(Security Manager), 인프라 담당자(Infra Manager), 데이터베이스 담당자(DB Manager)로 직무 분리하여 효과적으로 계정을 관리하는 모델을 확인할 수 있습니다.

Main Account

Sub Account 사용자를 생성하고 권한 부여와 회수를 수행하며 미접속 계정과 미사용 리소스를 지속적으로 관리합니다.

Security Manager

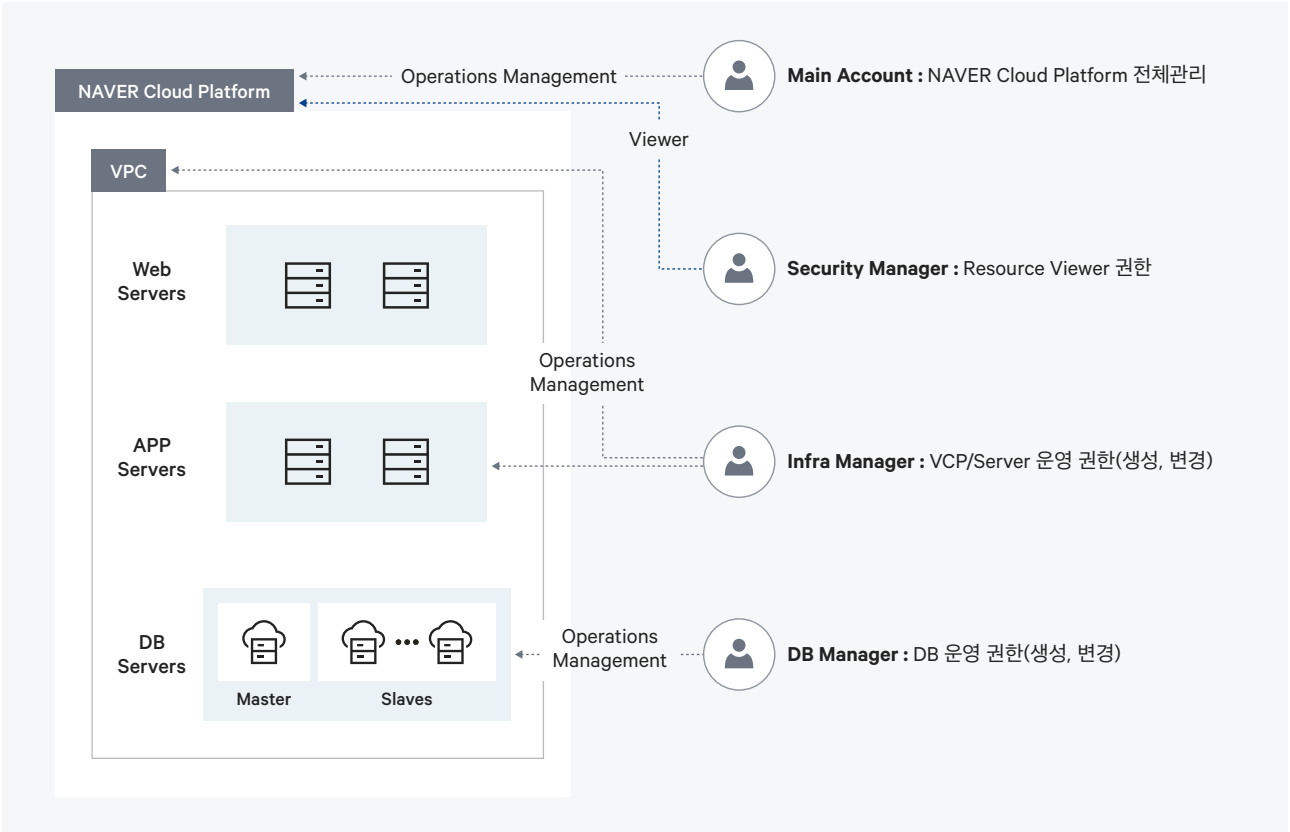
모든 리소스에 대한 Viewer 권한을 할당 받은 후 비인가된 사용자나 리소스 여부를 검토하여 적절한 보안 서비스를 적용하고 운영합니다.

Infra Manager

서버, VPC의 운영 권한을 할당 받은 후 인프라 관련 서비스를 관리하며 ACG, NACL의 허용 및 삭제를 수행합니다.

DB Manager

DB의 운영 권한을 할당 받은 후 데이터베이스를 생성하고 운영합니다.



[그림 2-3 : Sub Account를 통한 직무 분리 예제]

4

Account 보안 설정

4.1 사용자 계정에 대한 강력한 암호 정책 구성

네이버 클라우드 플랫폼 포털의 강력한 비밀번호 정책에 따라 계정 비밀번호는 영문자, 숫자, 특수문자를 조합하여 8자 이상 16자 이하로 설정해야 합니다. 5회 이상 비밀번호를 잘못 입력한 경우 보안을 위해 계정이 잠기며, 잠긴 계정은 관리자를 통해서만 해제할 수 있습니다.

4.2 Multi-Factor 인증

네이버 클라우드 플랫폼 포털의 **마이 페이지 > 계정 관리**에서 2차 인증을 설정할 수 있습니다. 2차 인증 수단은 계정 관리 화면에서 인증번호나 OTP 가운데 선택합니다. 인증번호(휴대폰, 메일 주소) 기반 2차 인증의 경우 Main Account와 Sub Account 모두 설정이 가능합니다.

4.3 Sub Account 접근 관리

Sub Account를 통해 콘솔 접근 시 접근이 가능한 IP 주소 대역을 제한할 수 있습니다.

4.4 API 인증키 관리

네이버 클라우드 플랫폼은 제공 중인 상품을 API로 제어할 수 있도록 지원합니다. 액션에 따라 파라미터 값을 입력하고 리소스를 등록, 수정, 삭제, 조회할 수 있으며 서비스 및 운영 도구 자동화에도 활용할 수 있습니다. 따라서 보안을 위해 타인과 공유를 금지하며 주기적인 교체를 권장하고 있습니다. API 인증키는 Main Account, Sub Account 모두 발급이 가능합니다.

4.5 불필요한 계정 제거

Sub Account 사용자 계정 및 접근 권한의 적정성 검토 기준, 검토 주체, 검토 방법, 주기 등을 수립하여 정기적 검토를 이행해야 합니다. 미사용 계정, 직무 변경 사용자 계정에 대해 정기적으로 검토하여 계정 사용 중지, 계정 삭제 처리를 합니다.

4.6 계정 활동 모니터링

네이버 클라우드 플랫폼 계정의 활동 로그를 제공하는 상품인 Cloud Activity Tracer를 이용하여 사용자가 계정에서 수행한 작업과 사용한 리소스를 확인할 수 있습니다. 승인되지 않은 리소스의 생성, 변경, 삭제 등 고객의 클라우드 환경이 오·남용되지 않도록 정기적으로 점검합니다.

Section 3. 클라우드 인프라 보호

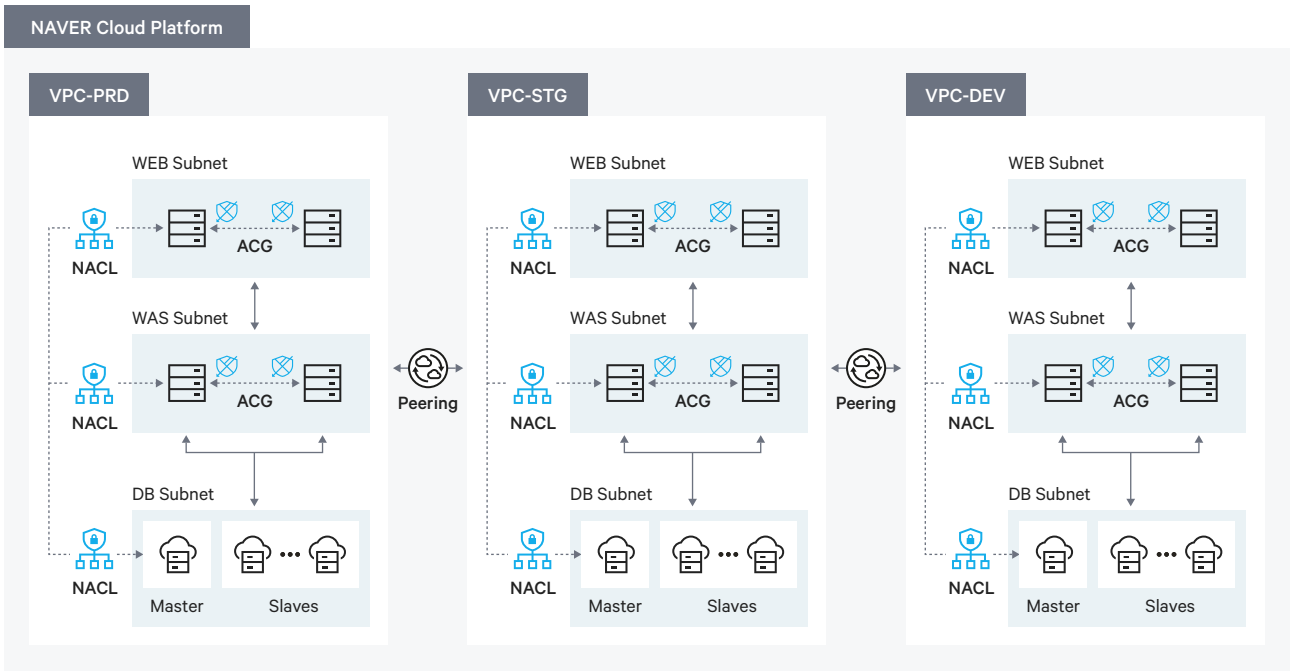
1 클라우드 인프라 보호의 이해

클라우드 환경에서 성공적인 비즈니스를 지속하기 위해서는 모범 사례와 규정 및 컴플라이언스를 준수해야 하며, 기존 온 프레미스와의 IT 거버넌스 연결성 확보와 다양한 보안 위협에 대한 보호가 필요합니다. 이를 위해 클라우드 환경에서 인프라 보안은 필수적이며 핵심적인 요소입니다. 책임 공유 모델에 따라 네이버 클라우드 플랫폼과 고객은 구축한 인프라 자산(리소스) 보호를 위해 협력하여 각자의 역할을 수행해야 합니다. 네이버 클라우드 플랫폼은 고객의 인프라 보호를 돕기 위해 VPC(Virtual Private Cloud)와 Security Monitoring 서비스를 제공합니다.

2 네이버 클라우드 플랫폼의 VPC

2.1 VPC의 이해 및 구성 요소

클라우드 환경에 구성한 인프라 보호를 위해서는 기본적으로 네트워크 설계를 철저하게 계획하고 관리해야 합니다. 네이버 클라우드 플랫폼은 고객의 기존 온 프레미스 환경 네트워크와 유사하게 구현 가능하면서도 다양한 네트워크 설계가 가능하도록 VPC를 제공합니다. VPC는 네이버 클라우드 플랫폼 상에서 제공되는 고객 전용 사설 네트워크를 의미하며, 각각의 VPC는 논리적으로 완벽하게 분리되어 있어 다른 사용자의 네트워크와 상호 간섭이 발생하는 영역 없이 사용할 수 있습니다. 계정마다 최대 3개의 VPC를 생성할 수 있으며, 각 VPC는 최대 /16의 IP 네트워크 공간을 제공합니다. (IP 대역: RFC 1918) VPC Peering 기능을 이용하면 서로 다른 VPC간 내부 네트워크 통신 환경도 구성이 가능합니다.



[그림 3-1 : 다중 VPC 구성 예제]

VPC는 Subnet(서브넷), Network ACL, ACG, NAT Gateway, Virtual Private Gateway, Route Table, VPC Peering으로 구성됩니다. VPC의 다양한 구성 요소를 활용하여 가상 네트워크 환경을 효과적으로 제어할 수 있습니다. 또한 VPC의 기능으로 계층적인 네트워크를 구성함으로써 VPC 안에서 동작하는 다양한 네이버 클라우드 플랫폼의 리소스를 보호할 수 있습니다. VPC의 다양한 구성 요소별 설명은 다음과 같습니다.

Subnet

할당된 VPC를 용도에 맞게 네트워크 공간을 세분화하여 사용할 수 있는 기능을 제공합니다. Subnet은 /16 ~ /28의 네트워크 주소 할당이 가능합니다.

NAT Gateway

인터넷 접속이 제한된 네트워크에서 외부 통신을 위해 사용하는 게이트웨이입니다. IP 노출을 최소화하는 효과를 얻을 수 있습니다.

Route Table

네트워크 경로를 설정할 수 있는 기능을 제공합니다. VPC 내부 통신을 위한 Local은 기본적으로 설정되어 있으며, Destination과 Target으로 구성됩니다. 공인 Route Table 생성 시 인터넷 통신을 위한 규칙이 자동 추가됩니다.

Network ACL

Subnet에서 Inbound/Outbound의 네트워크 접근을 제어하는 기능을 제공합니다. Stateless 기반으로 동작합니다.

ACG

서버에서 Inbound/Outbound(Inbound/Outbound)의 네트워크 접근을 제어하는 기능을 제공합니다. Stateful 기반으로 동작합니다.

Virtual Private Gateway(VGW)

VPC와 외부 연결 네트워크 장치 간 연결 접점의 역할을 수행하는 기능을 제공합니다. 외부 연결을 위해서 반드시 생성해야 합니다.

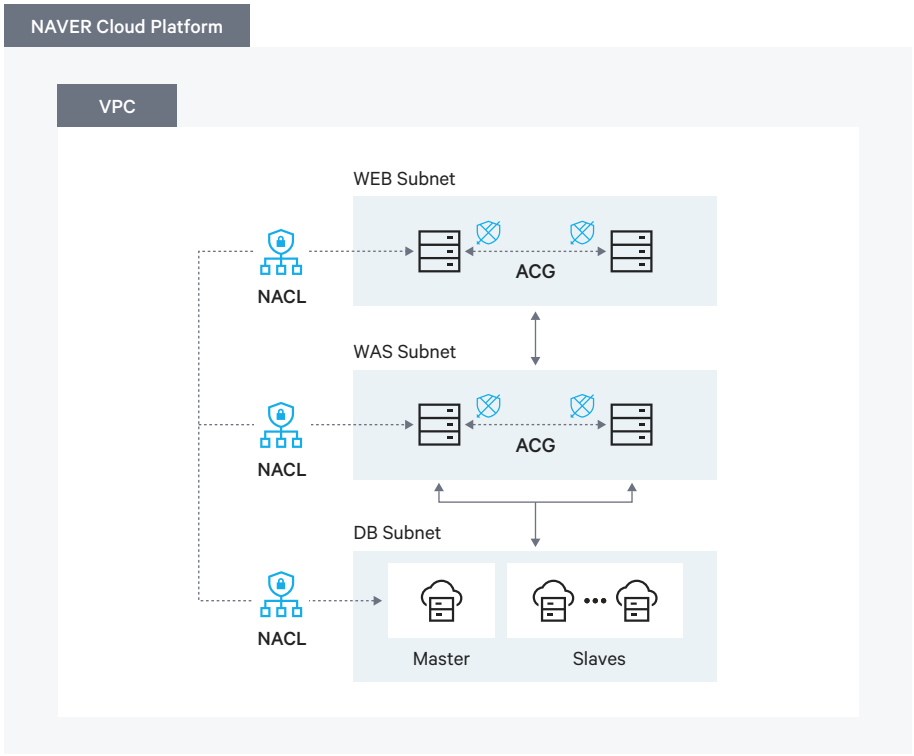
VPC Peering

VPC간 사설 연결을 보장하는 기능을 제공합니다. 단방향 통신을 제공하므로 양방향 통신 시 Source와 Destination이 뒤바뀐 2개의 VPC Peering을 생성해야 합니다.

2.2 Subnet

VPC가 구성되면, 용도 및 서비스 목적에 따라 서브넷을 생성하여 네트워크를 분리 구성할 수 있습니다. 서브넷은 할당된 VPC에 대한 공간을 세분화하여 사용할 수 있는 기능입니다. 네이버 클라우드 플랫폼에서 서브넷은 Public Subnet과 Private Subnet 두 가지 형태로 제공됩니다. 인터넷 접근이 필요한 서버의 경우 공인 IP를 할당하여 Public Subnet 내에 배치합니다. 인터넷 연결이 필요 없는 서버의 경우 기본적으로 내부 통신만 지원하는 Private Subnet에 배치하여 사용합니다.

그림 3-2.와 같이 WEB, WAS, DB 서브넷을 구분하여 비슷한 연결성을 가지고 있는 서버들을 적절한 서브넷 공간에 배치하면 서브넷 레벨에서의 계층적인 네트워크를 구성할 수 있어 의도하지 않은 네트워크 접근을 허용할 수 있는 단일 계층 구성의 위험도를 낮출 수 있습니다.



[그림 3-2 : 서브넷 구분 예제]

2.3 Network ACL과 ACG(Access Control Group)

VPC와 서브넷을 통해 네트워크를 분리했다면 업무 목적 및 중요도에 따라 네트워크에 대한 접근 통제를 적용해야 합니다. 네이버 클라우드 플랫폼은 네트워크에 대한 비인가 접근을 통제하기 위한 Network ACL과 ACG를 제공하고 있습니다.
이해를 돕기 위해 Network ACL과 ACG를 비교하여 설명하면 다음과 같습니다.

ACG	Network ACL
서버 레벨에서 운영	서브넷 레벨에서 운영
허용 규칙만 지원	허용 및 거부 규칙을 지원
Stateful (규칙에 관계없이 반환 트래픽 자동 허용)	Stateless (규칙에 의해 반환 트래픽 명시적 허용)
트래픽 허용 여부 결정 전 모든 규칙 평가	트래픽 허용 여부 결정 시 규칙 우선순위 처리
서버 시작 시 보안 그룹을 지정하거나 나중에 보안 그룹을 인스턴스와 연결하는 경우에만 서버에 적용	연결된 Subnet에서 모든 서버에 자동으로 적용 (ACG를 지정하는 사용자에게 의존할 필요 없음)

[표 3-1 : ACG와 Network ACL 비교]

예를 들어 애플리케이션 서버와 데이터베이스 서버가 서브넷을 통해 분리되어 있는 경우 데이터베이스 서브넷 내 DB 서버들은 Network ACL과 ACG를 이용하여 애플리케이션 서브넷 내 WAS 서버에서 전송하는 트래픽만 허용하도록 접근 통제를 설정할 수 있습니다.
Network ACL을 이용하여 각 서브넷을 독립적인 네트워크로 구분하고, 서브넷 내 통신의 보안은 ACG로 제어함으로써 강력한 네트워크 보안체계를 구성할 수 있습니다. 또한 Network ACL은 허용(Allow) 및 거부(Deny) 정책을 모두 설정할 수 있기 때문에 사용자가 직접 외부에서 접근하는 비인가 IP를 차단하여 보안 위협에 빠르게 대응이 가능합니다.

2.4 Flow Log

계층적인 네트워크 구성과 효과적인 접근 통제를 구현했더라도 네트워크 트래픽 모니터링은 간과할 수 없는 중요한 요소입니다. 네이버 클라우드 플랫폼은 비인가된 통신이 있는지 검토하고 의심되는 네트워크 통신을 확인하여 보안 위협을 예방할 수 있도록 Flow Log 기능을 제공합니다.
Flow Log를 통해 ACG, NACL에서 허용 및 차단 로그를 확인할 수 있습니다. Flow Log를 사용하기 위해서는 인터페이스에서 Flow Log를 활성화한 다음 미리 생성해 놓은 Object Storage에 저장해야 합니다. Flow Log를 통해 시간, 통신 방향, 리전, 출발지 IP와 포트, 목적지 IP와 포트, 허용/차단 정보, 프로토콜 등을 확인할 수 있습니다.

LOG_TIME	DIRECTION	REGION	VPC_NM	VPC _NO	SBNET _NO	INSTC _NO	NIC_ID	SRC_ADDR	SRC _PORT	DST_ADDR	DST _PORT	ACTION	PRO TOCOL	TP _CD
159643320	inbound	1	flowlog-security	592	871	1318810	11439	101.xxx.xxx.3	36550	172.xx.xx.4	80	allow	tcp	SVR
159643320	outbound	1	flowlog-security	592	871	1318810	11439	172.xx.xx.0	44900	169.xx.xx.9	9973	allow	tcp	SVR
159643322	inbound	1	flowlog-security	592	871	1318810	11439	79.xx.xx.34	57695	172.xx.xx.0	54321	deny	tcp	SVR
159643322	inbound	1	flowlog-security	592	871	1318810	11439	45.xx.xx.22	55588	172.xx.xx.0	3303	deny	tcp	SVR
159643323	inbound	1	flowlog-security	592	871	1318810	11439	45.xx.xx.151	42968	172.xx.xx.0	21076	deny	tcp	SVR
159643324	inbound	1	flowlog-security	592	871	1318810	11439	169.xx.xx.16	0	172.xx.xx.0	0	allow	icmp	SVR
159643324	inbound	1	flowlog-security	592	871	1318810	11439	198.xx.xx.242	23053	172.xx.xx.0	993	deny	tcp	SVR

[그림 3-3. VPC Flow Log 항목]

2.5 네트워크 보안 모범 사례 및 지침

네이버 클라우드 플랫폼의 네트워크 보안 모범 사례 및 VPC 환경 구축 지침을 소개합니다. 서비스 구성 시 이 지침을 참고한다면 안전한 네트워크 환경 구현에 도움이 되는 유용한 인사이트를 얻을 수 있습니다.

✓ 서버 간 네트워크 접근 제어 및 관리할 수 있는 ACG를 사용합니다. 서비스에 필요한 IP, 포트만 허용한 다음 정기적으로 사용하지 않는 IP, 포트가 허용되어 있는지 점검하여 보안 사고를 사전에 예방할 수 있습니다.

- ✓ Network ACL을 사용합니다. Network ACL은 서브넷 간 네크워크 접근 제어 기능을 제공하기 때문에 ACG 외에 추가적인 접근 제어를 적용할 수 있습니다.
- ✓ 외부에 있는 다른 네트워크와 연결이 필요한 경우 IPsec VPN이나 Cloud Connect를 사용하여 네트워크 보안 수준을 고도화합니다.
- ✓ 전송 중인 데이터를 보호하여 데이터의 기밀성과 무결성을 확보합니다.
- ✓ 네트워크 보안을 계층적으로 설계합니다. 단일 네트워크 보호 계층을 만들지 않고 외부, DMZ 및 내부 계층에 네트워크 보안을 적용합니다.
- ✓ Flow Log를 사용하여 ACG, NACL에서 전송되고 수신되는 IP 트래픽에 대한 정보를 확인합니다. 네트워크 트래픽에 대한 가시성이 향상됩니다.

3 Security Monitoring

네이버 클라우드 플랫폼은 네이버 클라우드 환경에 구성한 고객의 인프라 자산(리소스)을 안전하게 보호할 수 있는 Security Monitoring 서비스를 제공합니다. Security Monitoring 서비스의 특징은 다음과 같습니다.

- ✓ **One-stop 서비스**

  사용 신청만 하면 네이버클라우드의 전문 보안 조직 인력이 고객의 인프라 구성과 서비스를 신속히 분석하여 구축에서부터 운영 및 관제 서비스까지 최적화된 보안 서비스를 제공합니다.

- ✓ **고도화된 보안 정책**

  최신 공격 기법을 정확히 탐지하고 모니터링할 수 있는 고도화된 보안 정책을 제공합니다. 필요한 경우 고객 서비스에 특화된 보안 정책을 제공하여 고객의 서비스를 강력하게 보호합니다.

- ✓ **보안 위협에 대한 가시성 제공**

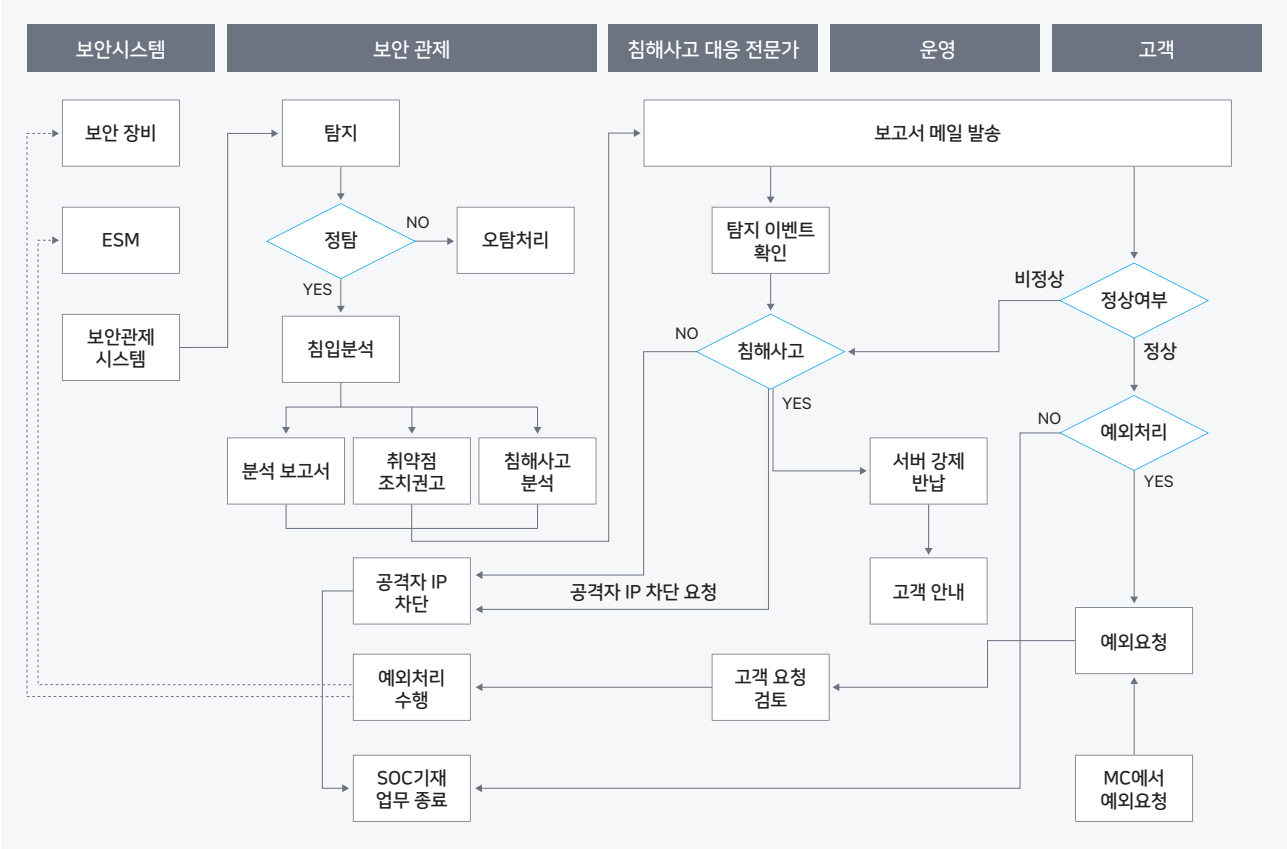
  콘솔을 통해 다양한 보안 이벤트에 대한 대응(탐지/차단) 현황을 대시보드 형태로 제공합니다. 고객의 서비스를 더욱 안전하게 보호할 수 있도록 탐지된 보안 위협에 대한 분석 리포트 및 대응 가이드를 제공합니다.

- ✓ **보안 전문가(네이버 CERT)**

  고객이 별도 보안관제팀을 구성하지 않더라도 최고 수준의 전문 보안 인력이 다양한 공격 이벤트를 365일 24시간 실시간으로 모니터링하여 고객에게 통보함으로써 최적의 보안 관제 서비스를 제공 받을 수 있습니다.

Security Monitoring 상품은 보안 솔루션 구축부터 운영, 실시간 보안 관제 서비스까지 통합으로 제공해주는 Security managed 서비스이며 DDoS, WAF, IDS, IPS, Anti-Virus 솔루션을 통해 외부에서 유입되는 다양한 위협에 대응할 수 있도록 도와줍니다. 콘솔 및 분석 리포트를 통해 다양한 보안 이벤트에 대한 높은 가시성을 제공하며, 침해 사고 발생 시, 네이버클라우드 보안 전문가가 침해사고에 대한 분석을 수행하고 원인을 파악하여 차후 동일한 피해가 발생하지 않도록 지원합니다. 따라서 고객은 별도의 전문 보안 인력을 구성하지 않아도 최적의 인프라 보호 서비스를 제공받을 수 있습니다.

Security Monitoring의 구체적인 대응 프로세스는 그림 3-4.와 같습니다.



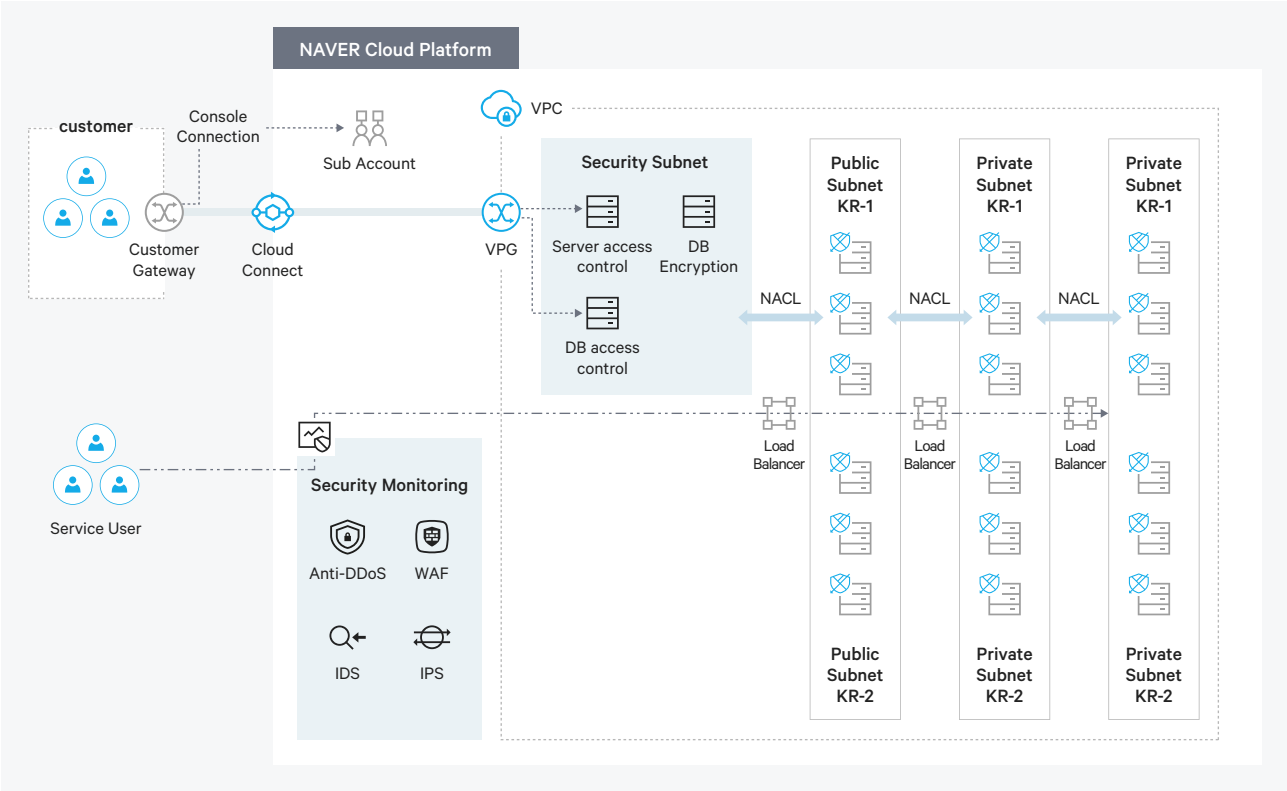
[그림 3-4 : Security Monitoring 대응 프로세스]

클라우드 환경에 구축되어 있는 보안 시스템의 이벤트를 ESM에 전송하여 네이버클라우드 전문 보안 관제 요원들이 모니터링을 수행합니다. 탐지된 이벤트를 분석하여 정탐과 오탐으로 구분하고, 정탐 이벤트에 대해서는 세부적인 분석을 진행합니다. 분석된 이벤트는 상세 분석 내용과 취약점 조치 권고가 담긴 보고서로 고객에게 제공되며, 고객은 추가적인 확인 과정을 거칠 수 있습니다. 이후 실제 침해로 판단된 이벤트에 대해서는 공격자 IP를 차단하고 후속 조치를 진행하게 됩니다.

4

인프라 보안 아키텍처

네이버 클라우드 플랫폼은 고객의 인프라 자산(리소스)을 보호할 수 있는 다양한 보안 솔루션을 마켓플레이스를 통해 추가 제공하고 있습니다. 앞에서 설명한 네이버 클라우드 플랫폼 보안 서비스와 마켓플레이스에서 제공하는 보안 솔루션을 활용하여 구성한 클라우드 보안 아키텍처 예제는 다음과 같습니다.



[그림 3-5 : 클라우드 인프라 보안 아키텍처 예제]

우선 온 프레미스와 네이버 클라우드 플랫폼은 전용선 서비스인 Cloud Connect를 이용하여 연결합니다. VPC 안에 Security 서브넷을 분리하여 마켓플레이스에서 제공하는 DB/시스템 접근 제어, DB 암호화를 구성합니다. Public Subnet과 Private Subnet은 Network ACL을 통해 서브넷 간 통신을 제어하고, ACG를 이용하여 서버 간 접근 통제를 수행합니다. 마지막으로 Security Monitoring의 DDoS, WAF, IPS, IDS, Anti-Virus 관련 다양한 서비스를 활용하여 네이버 클라우드 플랫폼에 구축한 리소스를 보호하도록 구성합니다.

이처럼 서비스 중요도 및 목적에 맞게 네이버 클라우드 플랫폼의 다양한 보안 서비스와 마켓플레이스에서 제공하는 보안 솔루션을 활용한다면 좀 더 심층적이고 섬세한 인프라 보호 대책을 구현할 수 있습니다.

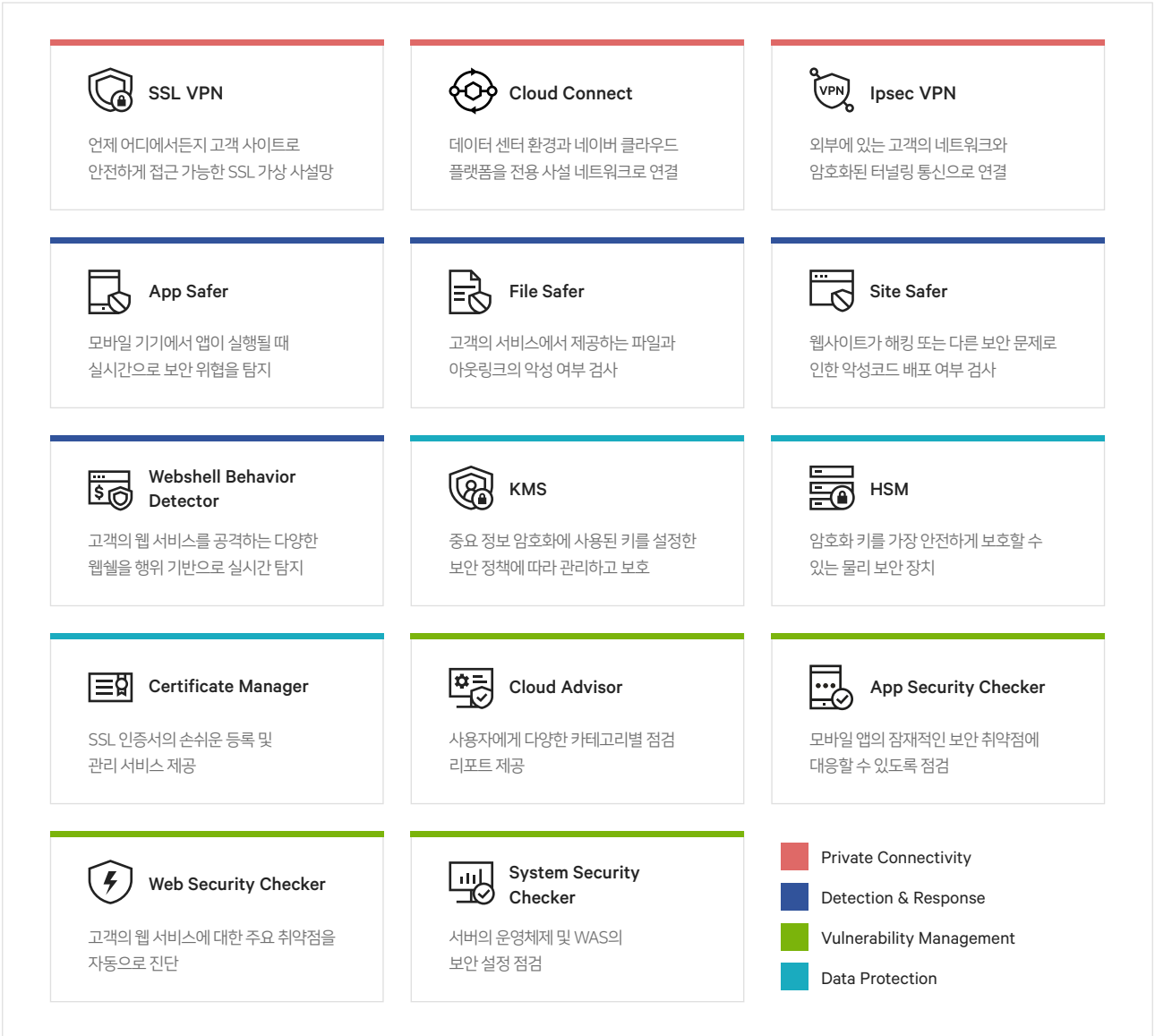
Section 4. 클라우드 리소스 보호

1 클라우드 환경의 IT 자원

네이버 클라우드 플랫폼에서는 IT 자원을 '리소스'라고 명명하고 있으며, 리소스는 사용자가 네이버 클라우드 플랫폼 환경에서 생성한 모든 가상 자원을 의미합니다. 리소스는 동시에 가상 자원의 단위로도 사용됩니다.

예를 들어 서버 상품 내 Instance, Public IP, Snapshot과 Object Storage 상품 내 Bucket 등이 리소스가 될 수 있습니다. 그리고 리소스는 네이버 클라우드 플랫폼 내에서 명확한 구분을 위해 리소스마다 고유 이름을 사용하고 있으며 NRN(Ncloud Resource Name)으로 표현하고 관리되고 있습니다.

네이버 클라우드 플랫폼은 고객의 리소스를 안전하게 관리하여 보안 위협으로부터 보호할 수 있는 다양한 보안 서비스를 제공합니다. 모든 보호 서비스는 콘솔을 통해 쉽고 간편하게 사용이 가능합니다. 이를 활용하면 다양한 보안 인증 및 법률의 세부 규정을 준수함과 동시에 서비스 목적 및 중요도에 따른 리소스 보호를 구현할 수 있습니다.



[그림 4-1 : NAVER Cloud Platform의 리소스 보호 서비스]

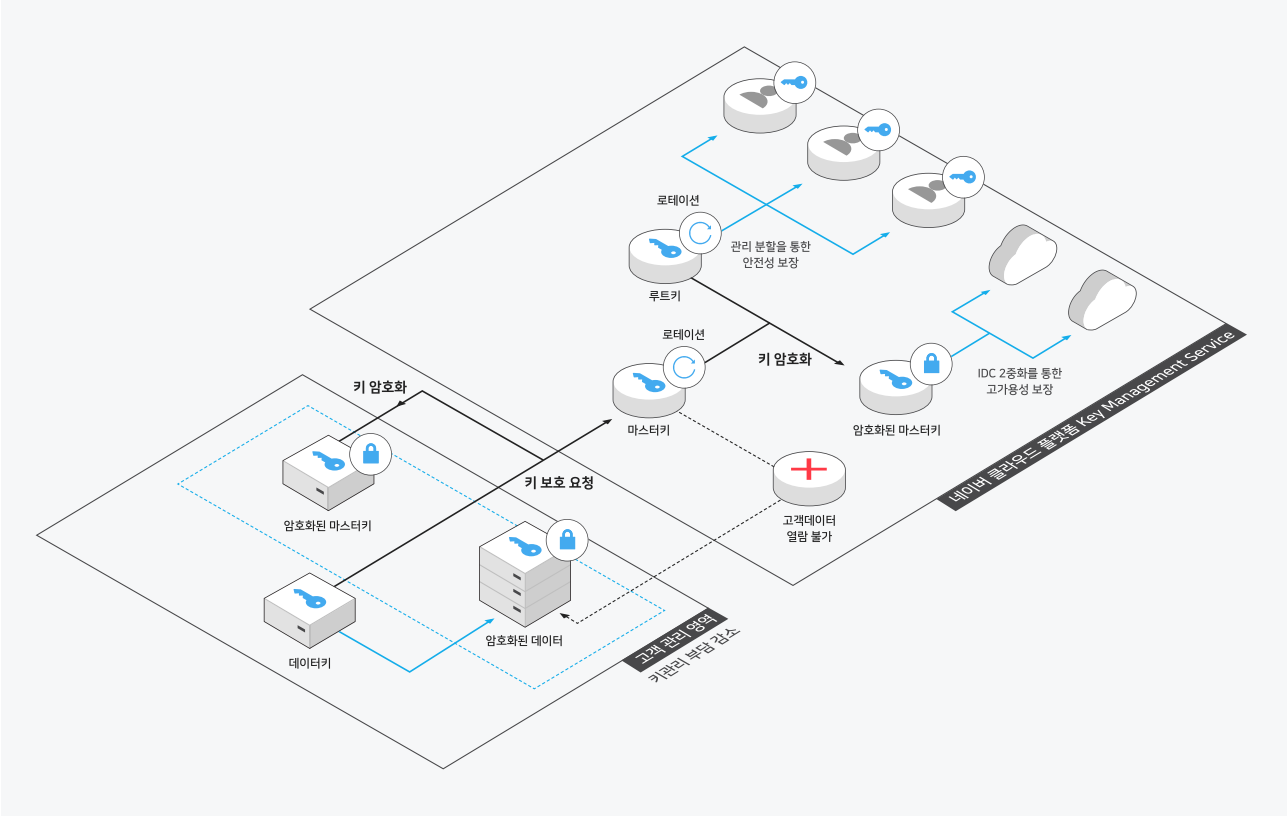
2

데이터 보호를 위한 클라우드 서비스

데이터 보호를 위한 네이버 클라우드 플랫폼의 클라우드 서비스를 소개합니다.

2.1 KMS (Key Management Service)

네이버 클라우드 플랫폼의 KMS는 고객의 중요 정보 암호화에 사용된 키를 고객이 설정한 보안 정책에 따라 안전하게 보호할 수 있는 서비스입니다. KMS는 암호화 키 보호에 필요한 모든 조건을 손쉽게 충족시킬 수 있는 다양한 기능을 제공합니다. 키의 생성, 회전, 상태 관리, 폐기 등 모든 키 관리 요건을 편리하게 관리할 수 있으며, 엄격한 관리 절차에 따라 암호화 키 혹은 최대 32KB 기밀 데이터를 안전하게 보호할 수 있습니다.
네이버 클라우드 플랫폼의 Sub Account에서 키에 대한 사용자별 역할을 할당하여 키 접근 제어를 설정할 수도 있습니다. 키의 모든 사용 이력은 즉시 기록되며, 키 감사 권한을 가진 사용자는 언제든지 사용 이력을 모니터링하고 감사할 수 있습니다.



[그림 4-2 : KMS를 이용한 데이터 암·복호화]

KMS는 데이터를 암호화한 키를 보호하는 봉투 암호화 방법과 REST API를 사용하여 기밀 데이터를 직접 암·복호화하는 방법으로 활용이 가능합니다.
봉투 암호화 방법은 계층적 키 관리 솔루션입니다. 데이터를 암호화한 암호 방식을 보호함으로써 데이터 기밀성과 통제권을 모두 만족시킬 수 있습니다. 솔루션과 관련된 키는 데이터 키, 마스터 키, 루트 키이며, 네이버 클라우드 플랫폼에서는 마스터 키와 루트 키를 관리합니다.

데이터 키

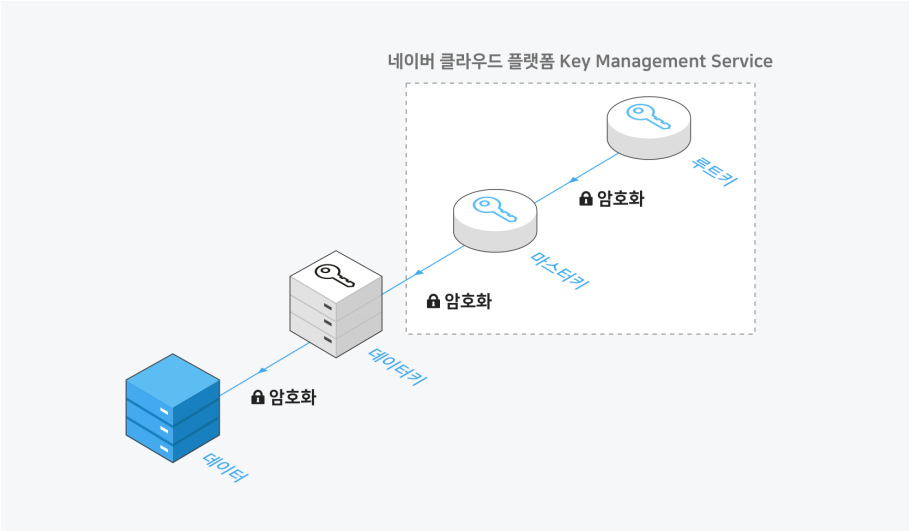
데이터 암·복호화에 사용되며 고객이 직접 관리해야 합니다. KMS를 이용한다면 마스터 키 사용으로 안전하게 보호가 가능하기 때문에 관리 부담을 줄일 수 있습니다.

마스터 키

KMS에서 생성한 키입니다. 생성 및 회전, 삭제까지 고객이 관리합니다. 관리자 권한이나 접근 권한을 가진 경우 사용자 콘솔을 통해 키와 관련된 다양한 설정 사항을 관리할 수 있습니다.

루트 키

마스터 키를 암호화하는 데에 사용됩니다. 암호화된 마스터 키는 KMS 내부 스토리지에 저장됩니다. 고객의 키와 동일한 관리 정책으로 운영되어 정해진 기간 내에 회전, 갱신되며 접근 권한을 가진 사용자만 관리 목적 하에 접근할 수 있습니다. 다수의 조각으로 분할되어 물리적 보안 매체에 각각 저장됩니다.



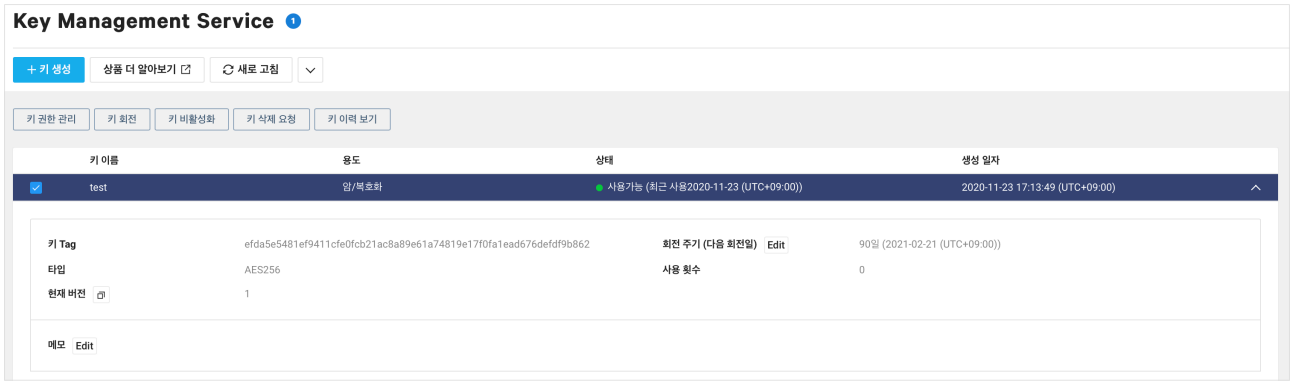
[그림 4-3 : KMS 키 관리 정책]

KMS에서 생성된 키를 이용하여 직접 데이터를 암·복호화하는 기능은 REST API 호출을 통해 구현이 가능합니다. REST API를 호출하려면 API Gateway와 Sub Account 인증이 필요합니다. 네이버 클라우드 플랫폼에서는 KMS 사용 방법을 좀 더 상세하게 안내하고 다양한 활용을 돕기 위해 **KMS API 참조서**와 **샘플 코드:Best Practice**를 제공합니다.
KMS의 키 회전, 삭제, 사용자별 권한 설정 등 기능을 사용하여 ISMS-P 관련 항목을 만족할 수 있으며 금융권의 경우 전자금융감독규정, 공공 기관의 경우 클라우드 컴퓨팅 서비스 정보보호에 관한 기준 내 세부 항목을 준수할 수 있습니다.

인증 및 법률	전자금융감독규정	ISMS-P	클라우드컴퓨팅서비스 정보보호에 관한 기준
항목	제 33조 (암호프로그램 및 키 관리 통제)	2.7.2 암호키 관리	기술적 보호조치 중 12.3.2 암호키 관리
세부 내용	금융회사 또는 전자 금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다.	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고 암호키는 별도의 안전한 장소에 보관하여야 한다.

[표 4-1 : KMS 활용을 통한 인증 및 법률 준수]

접근 권한을 가진 사용자나 관리자라면 누구나 쉽게 네이버 클라우드 플랫폼의 사용자 콘솔을 통해 키 권한 관리, 회전 등의 기능을 용도에 알맞게 직접 설정할 수 있으며, 생성된 키의 상태, 생성 일자, 버전 등을 한 눈에 확인할 수 있습니다.

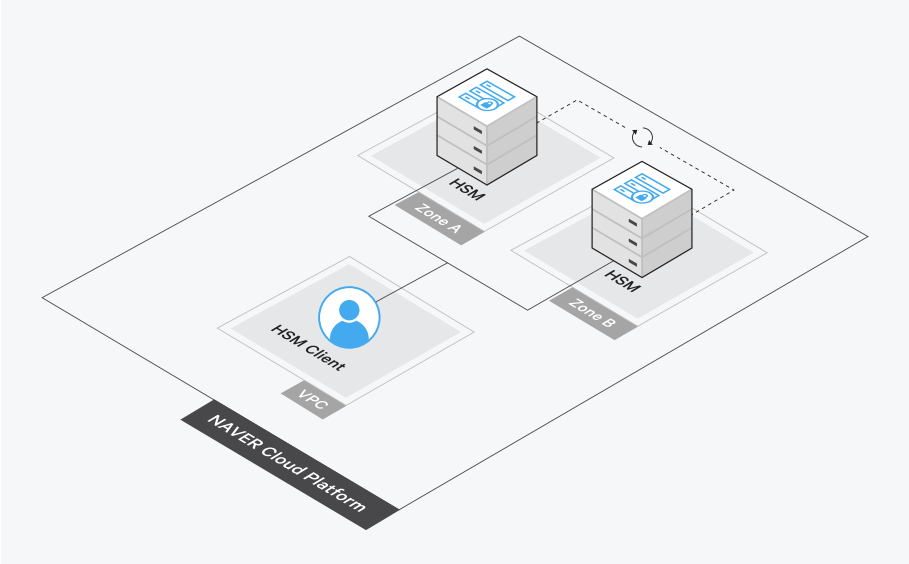


[그림 4-4 : KMS 사용자 콘솔 화면]

2.2 HSM(Hardware Security Module)

네이버 클라우드 플랫폼의 금융 전문 퍼블릭 클라우드 서비스에서는 데이터 암호화 키를 안전하게 보호하기 위한 물리 보안 장치인 HSM 서비스를 제공하고 있습니다. 이를 자체 구성하여 운영 시 높은 초기 비용과 복잡한 구성 및 설정 등 다양한 문제가 존재하여 어려움을 겪는 경우가 많습니다. 네이버 클라우드 플랫폼의 HSM은 이러한 어려움을 최소화하여 별다른 초기 비용 없이 간편하게 이용할 수 있는 기능과 구성을 제공합니다. 고가용성 및 백업 등을 필요에 따라 구성할 수도 있습니다.

HSM은 고객으로부터의 접근을 제외한 다른 모든 접근으로부터 안전하게 격리되며, HSM에 저장되는 키에 대해 완전한 제어권을 보장합니다. 전용 VPC에서 독립적으로 접속 가능한 HSM 액세스를 통해 암호화 키에 대한 완전 제어가 가능합니다. HSM을 사용하여 엄격한 기준이 적용되는 일부 산업, 기업 및 애플리케이션의 기준을 충족할 수 있으며 암호화 키 보호에 대한 대부분의 보안 규정도 준수할 수 있습니다.



[그림 4-5 : HSM 서비스 구성]

HSM Pool

모든 HSM 어플라이언스는 외부로부터 접근이 철저하게 차단되어 격리 운영됩니다. HSM Pool은 지역적으로 떨어진 두 Zone에 구성되어 있으며, HSM은 각 Zone별 HSM Pool에서 독립적인 파티션 영역 형태로 생성되어 할당됩니다.

HSM

HSM Pool에서 고객에게 할당된 독립적인 HSM 파티션입니다. 280KB의 용량을 가지기 때문에 1,024비트 기준으로 약 2,100개의 키를 저장할 수 있습니다. HSM은 전용 클라이언트를 통해 고객이 직접 관리하고 사용합니다.

연결

고객의 HSM에 접근할 수 있도록 설정된 유일한 통신 경로입니다. 전용 VPC에 생성된 서버 인스턴스로부터 시작되며, 직접 생성한 개인 키로 보호됩니다.

HSM Client

초기 구성이 완료된 전용 클라이언트인 SafeNet Luna Client에는 고객에게 할당된 HSM Pool 정보 및 HSM 영역에 대한 정보가 설정되어 있습니다. 라이선스가 적용되어 무단 복제 및 허가 받지 않은 사용은 금지합니다.

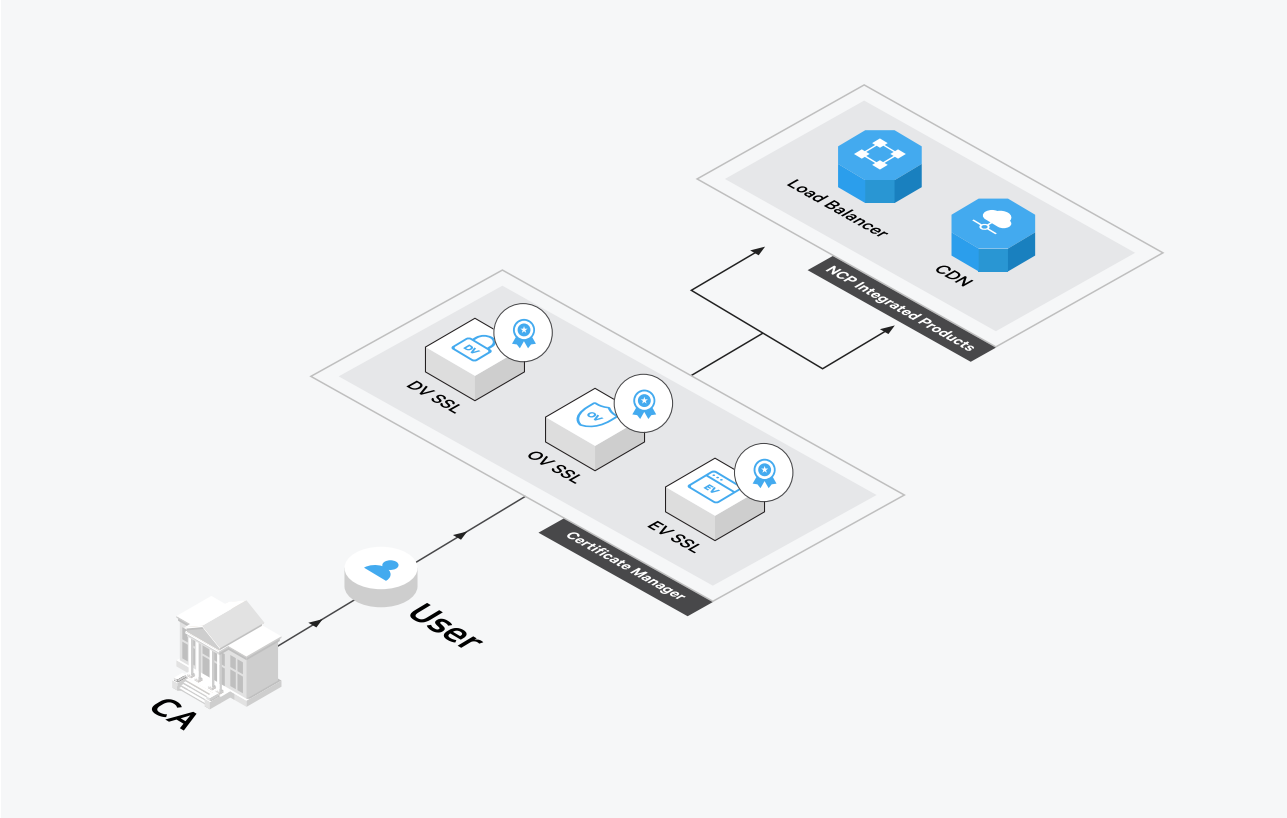
데이터 보호 및 전송에 사용하는 암호화 키를 네이버 클라우드 플랫폼의 HSM 서비스를 활용하여 물리적으로 분리하여 관리한다면 정보통신망법이나 개인정보보호법 등과 같은 법률 및 보안 인증 속 암호화 키 관리 관련 요구사항을 만족할 수 있습니다.

인증 및 법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률	개인정보에 대한 안전성을 확보 조치 의무	PCI-DSS
항목	제28조 (개인정보의 보호조치) 제1항 제4호	제7조(개인정보의 암호화) 제6항	3.5.3
세부 내용	개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치	개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.	카드소유자 데이터를 암호화/복호화하기 위한 비밀키와 사설키를 언제나 다음의 형태중 하나로 저장하여야 한다. • 키 암호화 키로 암호화되며 이는 적어도 데이터 암호화 키 보다는 강력해야 하며, 데이터 암호화 키로부터 분리되어 저장되어야 함 • 안전한 암호화 디바이스 안에 저장 (HSM 또는 PTS-approved point-of-interaction device 등)

[표 4-2 : HSM 활용을 통한 인증 및 법률 준수]

2.3 Certificate Manager

Certificate Manager(CM)는 네이버 클라우드 플랫폼 연계 서비스인 Load Balancer, CDN(Content Delivery Network)에서 사용할 공인 SSL 인증서를 등록하고 통합하여 관리하는 서비스입니다. SSL 인증서는 Certificate Manager 서비스를 통해서만 등록 및 삭제가 가능합니다. 인증서 등록 시 인증서의 유효성을 체크하며 발급 기관, 대상 도메인 및 유효 기간 등의 다양한 정보를 제공합니다. 또한 인증서 만료 예정일 한 달 전부터 정기적인 알람으로 인증서의 효율적인 관리가 가능하도록 도와줍니다.



[그림 4-6 : Certificate Manager 서비스 구성]

네이버 클라우드 플랫폼 Security Monitoring 이용 시 Security Monitoring에서 제공하는 IDS, IPS, WAF, Anti-DDoS 서비스는 기본적으로 암호화된 패킷을 탐지 분석할 수 없습니다. 그러나 Certificate Manager 상품을 통해 SSL 인증서를 Load Balancer 연계 서비스에 설정하면 IPS, WAF 서비스에 한해 네이버 클라우드 플랫폼 Load Balancer의 SSL Offloading 기능(HTTPS 프로토콜 사용)을 사용하여 암호화된 패킷에 대해서도 모니터링할 수 있습니다.

Certificate Manager 상품을 사용하여 SSL 인증서 등록 및 관리를 효율적으로 수행한다면 네트워크 암호화 통신 요건을 만족할 수 있을 뿐 아니라 관련 인증 및 법률도 준수할 수 있습니다.

인증 및 법률	개인정보의 기술적·관리적 보호조치 기준	ISMS-P	클라우드컴퓨팅서비스 정보보호에 관한 기준
항목	제6조(개인정보의 암호화) 제3항 제1호	2.7.1.암호정책 적용	기술적 보호조치 중 11.1.4 네트워크 암호화
세부 내용	정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다. 1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.

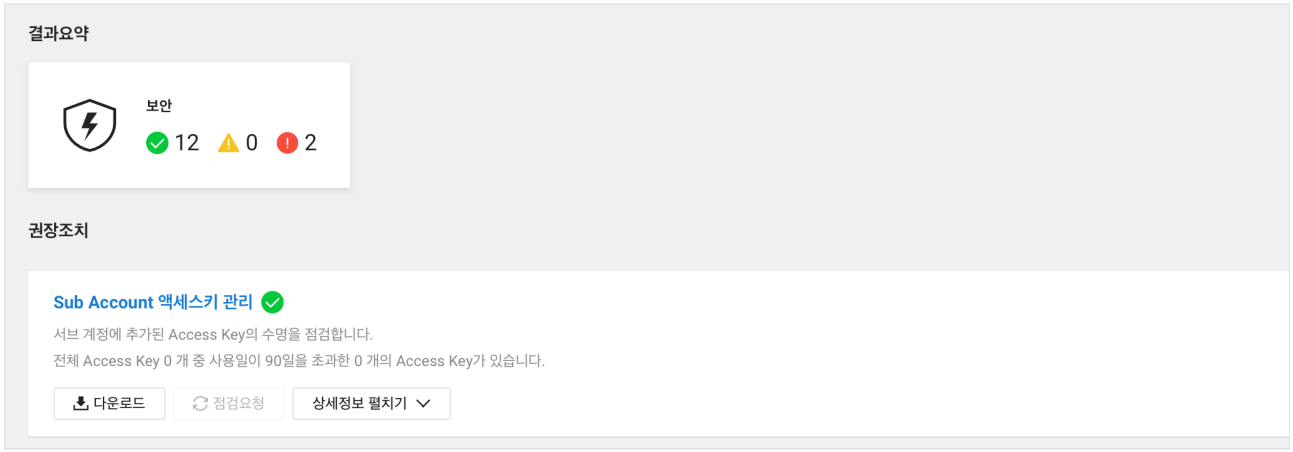
[표 4-3 : Certificate Manager 활용을 통한 인증 및 법률 준수]

3 취약점 관리를 위한 클라우드 서비스

취약점 관리를 위한 네이버 클라우드 플랫폼의 클라우드 서비스를 소개합니다.

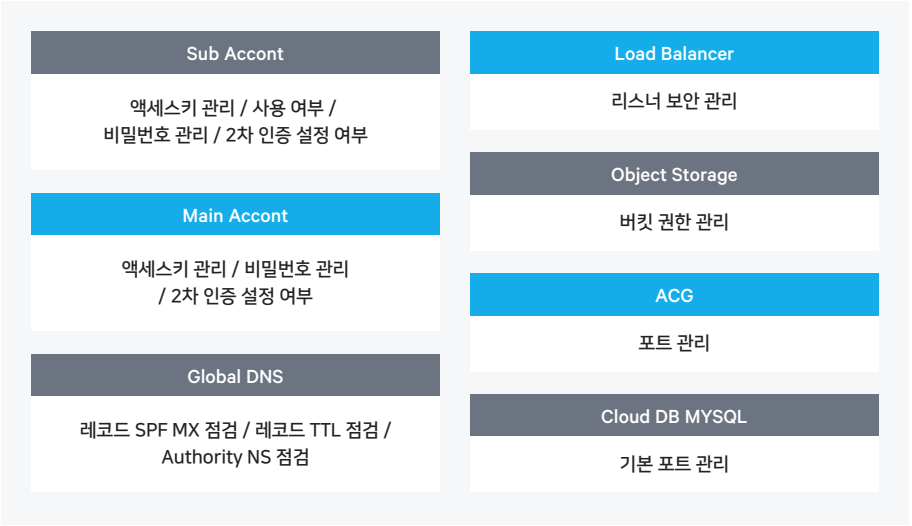
3.1 Cloud Advisor

Cloud Advisor는 사용자의 리소스를 점검하여 리소스가 안정적인 상태에서 운영될 수 있도록 도와주는 VPC 전용 상품입니다. 네이버 클라우드 플랫폼 운영 노하우를 바탕으로 도출한 자체 모범 사례와 사용자의 이용 내용을 비교 분석하여 좀 더 안전하고 효율적으로 서비스를 이용할 수 있도록 사용자에게 권장 지침을 제공합니다.
대시보드 메뉴에서 사용자의 리소스 점검 현황을 한 눈에 확인할 수 있고, Cloud Advisor에서 제공하는 리소스 점검 및 리포트 다운로드 기능을 수행할 수 있습니다. 점검 리포트를 파일 및 메일 등의 방법으로 확인이 가능하며 권장 조치 사항을 확인하고 이를 반영하면 높은 수준의 리소스 보호를 실현할 수 있습니다.



[그림 4-7 : Cloud Advisor 콘솔 화면]

현재 보안 카테고리에 한해 15개 점검 항목을 제공하고 있습니다.



[그림 4-8 : Cloud Advisor 점검 항목]

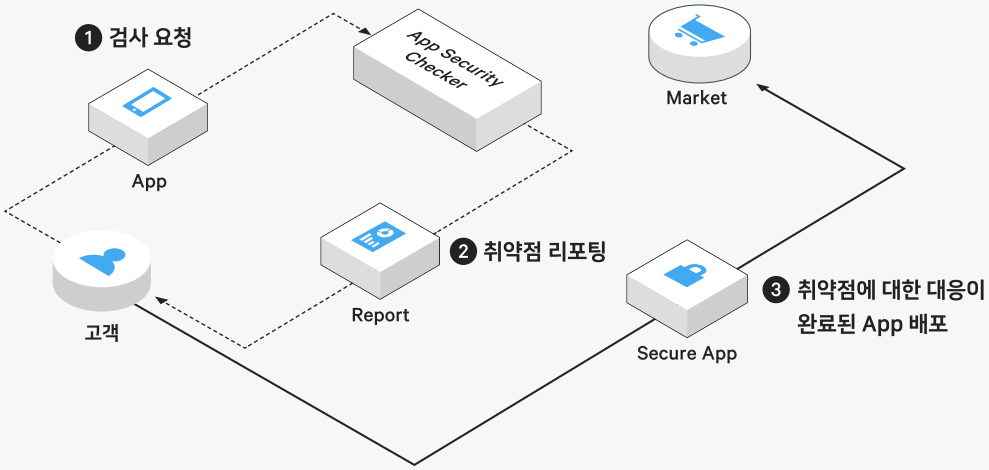
Cloud Advisor를 활용하여 주기적인 점검을 진행하여 Sub Account, Main Account 등에 관한 권장 요구사항을 충족한다면 사용자 계정, 스토리지 권한, 포트 규칙 관련 보안 인증 및 법률을 준수할 수 있습니다.

인증 및 법률	개인정보의 기술적·관리적 보호조치 기준	클라우드컴퓨팅서비스 정보보호에 관한 기준	
항목	제4조(접근통제) 제8항 제3호	10.3.3 강화된 인증 수단 제공	10.3.4 사용자 패드워드 관리
세부 내용	비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립, 이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다.

[표 4-4 : Cloud Advisor 활용을 통한 인증 및 법률 준수]

3.2 App Security Checker

App Security Checker는 모바일 서비스의 정보 유출 위험을 비롯하여 잠재적인 취약점을 사전에 탐지하고 조치할 수 있도록 점검하는 서비스입니다. 모바일 앱 출시 전 사용하여 앱 취약점 존재 여부를 확인할 수 있습니다. 마켓 스토어 등록 결격 사유, 잘못된 프레임 사용, 개인정보 유출 취약점에 대한 다양한 진단을 수행하며 네이버 모바일 앱 보안 노하우를 기반으로 개발된 자체 진단 엔진을 통해 위험도가 높은 취약점 항목에 대해 상세하게 검사합니다.



[그림 4-9 : App Security Checker 사용 프로세스]

사용자 콘솔을 통해 진단 상태, 시작 및 종료 시각, 앱 버전 등을 확인할 수 있습니다. 진단이 완료되면 Web과 PDF로 취약점 대응 방안이 담긴 상세 리포트를 제공합니다. 진단 결과 리포트를 통해 공격 시나리오는 물론 보완이 필요한 코드의 위치 및 수정 방법에 대한 자세한 설명을 확인할 수 있습니다.

3.3 System Security Checker

System Security Checker는 고객 서버의 운영체제 및 WAS의 보안 설정을 점검하여 서버의 보안성을 향상하는 서비스입니다. 에이전트를 설치하여 간편하게 점검할 수 있으며, KISA 가이드와 함께 네이버의 다양한 서비스를 운영하며 축적된 경험을 바탕으로 철저한 보안 정책기준으로 점검합니다. '계정 관리', '중요 시스템에 대한 권한 관리', '보안 config 값'을 주요 점검 항목으로 분류하여 진행합니다. 리눅스, 윈도우 운영체제를 지원하며 WAS는 Apache, Tomcat, Nginx를 지원합니다.

분류	설명
OS	Linux - CentOS 6.3 - CentOS 6.6 - CentOS 7.2 - CentOS 7.3 - Ubuntu 16.04 - Ubuntu 18.04 Windows - Windows Server 2008 R2 with SP1 (64-bit) - Windows Server 2012 R2 (64-bit) - Windows Server 2016 (64-bit)
WAS	Apache(httpd) Tomcat Nginx

[표 4-5 : System Security Checker의 지원 운영체제 및 WAS]

점검 항목에 대한 원활한 이해를 위해 운영체제 및 WAS의 보안 점검 항목에 대한 상세 설명을 제공합니다. 또한 콘솔을 통해 수정 가이드가 포함된 점검 결과 상세 리포트를 제공하므로 취약점이 발견된 부분에 대한 보완 조치를 쉽게 이행할 수 있습니다. 이러한 기능을 바탕으로 System Security Checker를 대부분의 보안 인증에서 요구하는 시스템 취약점 점검 중 CCE(Common Configuration Enumeration)의 용도로 사용할 수 있습니다.

3.4 Web Security Checker

Web Security Checker는 고객 웹 서비스의 잠재적 취약점을 사전에 탐지하고 조치할 수 있도록 취약점을 자동으로 진단하는 서비스입니다. SQL Injection, XSS 등과 같이 실제로 해커가 가장 많이 이용하는 취약점과 공격이 성공할 경우 피해가 큰 취약점을 중점적으로 진단합니다.

[그림 4-10 : Web Security Checker 서비스 구성]

웹 서비스에 과도한 영향을 주지 않고 진단이 가능하도록 개발된 알고리즘을 통해 서비스 중인 웹 사이트도 안정적으로 진단할 수 있습니다. 모든 과정이 자동화되어 있고 콘솔을 통해 진단 대상 URL 정보 및 진단에 필요한 간략한 정보만을 입력 받아 점검을 수행하므로 쉽고 편리한 사용성을 제공합니다. 또한 REST API를 통한 진단 리스트 출력 및 검색, 진단 취소 및 중지와 리포트 기능을 제공하고 있습니다. API Gateway를 통해 Web Security Checker API도 제공합니다. Web Security Checker 이용 시 네이버 클라우드 플랫폼 Sub Account를 이용하여 서브 계정을 생성하고 사용 권한을 할당할 필요가 있습니다. 네이버 클라우드 플랫폼에서는 API 활용법을 안내하고자 Web Security Checker API 참조서를 제공합니다.

세 종류의 Checker 상품 모두 동일한 대상을 다시 진단하여 취약점 조치 여부를 확인하는 용도로 활용할 수 있습니다. 첫 진단 후 상세 결과 리포트를 통해 보완 조치를 실행했지만 실제 정상 적용 여부를 파악하려면 동일한 조건에서의 동일한 공격 시행이 필요합니다. 따라서 사용하는 서비스의 취약점 존재 여부 뿐만 아니라 사후 보완 조치까지 확인하는 데에 Checker 시리즈를 사용하면 효과적으로 취약점을 점검한 후 보완 및 관리까지 가능합니다.
컴플라이언스 측면에서도 Checker 시리즈를 활용할 수도 있습니다. 다양한 점검 항목을 지원하므로 보안 인증이나 법률에서 요구하는 취약점 진단의 도구로 활용이 가능합니다. 상품을 이용한 취약점 점검 및 문제점 개선 프로세스 수립을 통해 다양한 보안 인증의 세부 항목을 준수할 수 있습니다.

인증 및 법률	PCI DSS	ISMS-P	
항목	6.6	2.8.2 보안 요구사항 검토 및 시험	2.10.3 공개서버 보안
세부 내용	일반인들이 접촉하는 웹 어플리케이션의 경우, 새로운 위협과 취약성을 지속적으로 다루고, 이러한 어플리케이션이 다음 방법들 중 하나를 이용해 알려진 공격으로부터 보호될 수 있게 한다.	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현 되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.

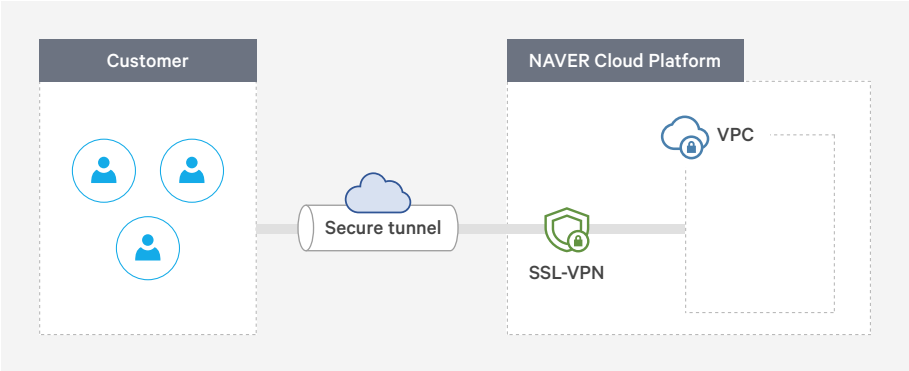
[표 4-6 : Web Security Checker 활용을 통한 인증 및 법률 준수]

4 전송 구간 암호화를 위한 클라우드 서비스

전송 구간 암호화를 위한 네이버 클라우드 플랫폼의 다양한 클라우드 서비스를 소개합니다.

4.1 SSL VPN

SSL VPN은 외부에서 인가된 사용자가 네이버 클라우드 플랫폼 리소스에 접속 시 암호화된 터널링 통신과 1차, 2차 인증을 통해 언제 어디서든 안전하게 접속할 수 있는 Secure 통신을 제공하는 서비스입니다. SSL VPN의 2차 인증은 Email과 SMS 방식을 지원하고 있으며, 최대 10개까지 외부 접속 ID를 콘솔에 등록하여 사용할 수 있습니다. 외부 접속을 허용할 최대 ID 수, 인증 방식, VPN 아이디 정보를 콘솔에 등록하고 SSL VPN 에이전트를 다운받으면 좀 더 쉽게 SSL VPN을 사용하여 접속할 수 있습니다.



[그림 4-11 : SSL VPN 서비스 구성]

외부에서 네이버 클라우드 플랫폼 주요 서비스에 접속할 때 SSL VPN을 활용할 수 있습니다. 대표적으로 DB 서버에 접근하기 위해 SSL VPN을 사용할 수 있습니다. 네이버 클라우드 플랫폼 ACG 상품을 통해 외부로부터의 접근을 차단하고 할당된 SSL VPN의 IP 주소 대역에서의 접근을 허용하여 SSL VPN 접속으로 인가된 사용자라면 어디서나 안전하게 접속할 수 있도록 구현할 수 있습니다. 네이버 클라우드 플랫폼에서는 상품 활용 방법을 안내하기 위해 **SSL VPN을 이용한 DB 서버 외부 접근 가이드**를 제공하고 있습니다. 이를 통해 일반 서버 뿐만 아니라 Cloud DB 관련 상품에 대한 접근을 손쉽게 구현할 수 있습니다.

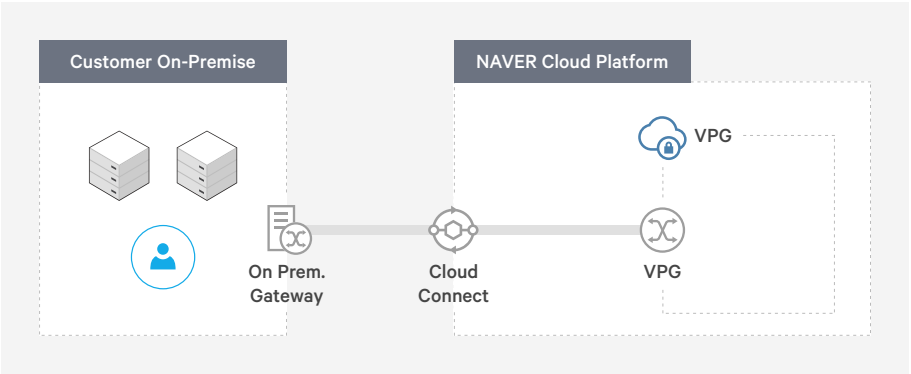
컴플라이언스 측면에서도 SSL VPN을 활용하여 안전한 사용자 2차 인증 설정 및 원격 접근 프로세스를 수립하여 일반적으로 관련 보안 인증 및 법률의 세부 규정 사항을 준수할 수 있습니다. 공공 기관은 SSL VPN 상품을 사용하여 클라우드 컴퓨팅 서비스 정보보호에 관한 기준의 기술적 보호 조치 중 네트워크 관련 세부 항목까지 만족시킬 수 있습니다.

인증 및 법률	ISMS-P	클라우드컴퓨팅서비스 정보보호에 관한 기준	개인정보의 기술적·관리적 보호조치 기준
항목	2.6.6 원격접근 통제	기술적 보호조치 중 11.1.3 네트워크 정보보호시스템 운영	제4조(접근통제) 제4항
세부 내용	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.	정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

[표 4-7 : SSL VPN 활용을 통한 인증 및 법률 준수]

4.2 Cloud Connect

Cloud Connect는 인터넷이 아닌 전용 회선을 이용하여 사용자의 온 프레미스 환경과 네이버 클라우드 플랫폼 간 네트워크 연결을 지원하는 서비스입니다. 대역폭은 최대 10Gbps까지 지원합니다. 전용 회선으로 통신하기 때문에 빠르고 안정적인 프라이빗 연결을 제공하여 고객 서비스 자원과 네이버 클라우드 플랫폼 간의 대용량 데이터 전송, 정기 백업 및 복구 등과 같이 고가용성이 필요한 경우 효과적으로 사용할 수 있습니다.
전용 회선 통신으로 인해 안정적이며 데이터 통신 보안성과 속도를 높일 수 있기 때문에 데이터 센터 확장을 위한 최적의 솔루션으로 활용할 수 있습니다.



[그림 4-12 : Cloud Connect 서비스 구성]

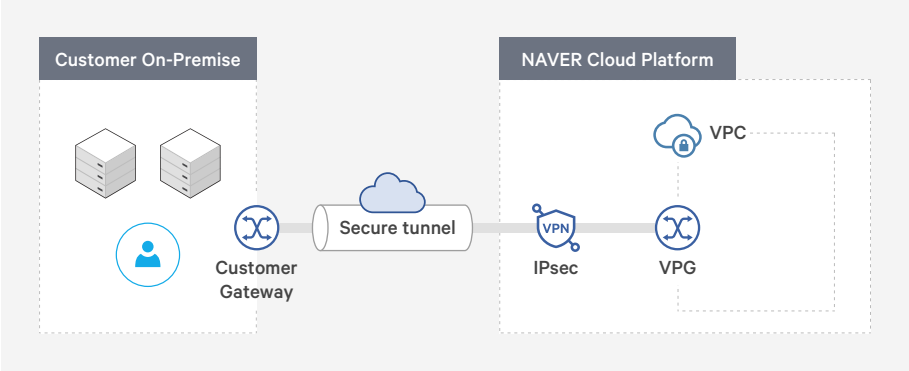
이러한 기능을 바탕으로 다양한 보안 인증 및 법률을 준수하는 데에 Cloud Connect 상품을 활용할 수 있습니다. 인터넷이 아닌 전용 회선 연결을 통해 데이터 센터 수준의 보안성을 보장하기 때문에 일반적으로 보안 인증 뿐 아니라 의료 기관의 경우 전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준을, 금융회사의 경우 전자금융감독규정 등의 법률을 준수할 수 있습니다. 또한 빠르고 안정적인 연결을 제공하여 재해 복구 및 기타 고가용성 전략과 같은 시나리오에 대한 유연한 대처가 가능하므로 이를 바탕으로 재해 복구 프로세스를 수립한다면 재해 복구 관련 세부 인증 및 법률의 요구 사항도 준수할 수 있습니다.

인증 및 법률	ISMS-P	전자의무기록의 관리·보존에 필요한 시설과 장비에 관한 기준	전자금융감독규정
항목	2.6.1 네트워크 접근	제2장 제5조 (전자의무기록의 백업 저장장비)	제13조(전산자료 보호대책) 제1항 제8호
세부 내용	네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.	전자의무기록 관리자는 전자의무기록의 분실·도난·유출·위조·변조 또는 훼손 등의 사고를 대비할 수 있도록 다음 각 호의 구분에 따른 장비와 장소를 확보하여야 한다. 1. 전자의무기록을 주기적으로 안전하게 백업할 수 있는 기능을 갖춘 백업 저장장비 2. 백업 저장장비에 대한 잠금장치가 구비된 보관장소	중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것

[표 4-8. Cloud Connect 활용을 통한 인증 및 법률 준수]

4.3 IPsec VPN

IPsec VPN은 외부에 있는 사용자의 네트워크와 네이버 클라우드 플랫폼에 있는 네트워크를 암호화된 터널링 통신, 즉 사설 통신으로 연결할 수 있는 서비스입니다. 다양한 벤더 제품과의 호환성을 제공하며 10~30Mbps의 서비스 규모에 맞는 대역폭을 선택할 수 있어 효율적인 이용이 가능합니다. 안전성이 검증된 IPsec VPN 전용 하드웨어 어플라이언스 기반으로 안정적인 고품질의 보안 통신을 제공합니다.



[그림 4-13 : IPsec VPN 서비스 구성]

4.4 SSL VPN, IPsec VPN, Cloud Connect 비교

네이버 클라우드 플랫폼에서 전송 구간 암호화를 위해 제공하고 있는 SSL VPN과 IPsec VPN, Cloud Connect의 이해를 돕기 위해 각 서비스를 비교하여 설명하면 다음과 같습니다.

구분	SSL VPN	IPsec VPN	Cloud Connect
암호화 방식	SSL (Secure Sockets Layer)	IPsec (IP Security Protocol)	전용 물리 회선
적용 모델	Site to Client	Site to site	Site to site
활용 방안	인가된 사용자와 네이버 클라우드 플랫폼 리소스 연결	온 프레미스와 네이버 클라우드 플랫폼 리소스 연결	온 프레미스와 네이버 클라우드 플랫폼 리소스 연결
추가 기능	2차 인증 제공	다양한 벤더 제품과의 호환성 제공	고객 서비스 자원과 네이버 클라우드 플랫폼 간 대용량 데이터 전송, 정기 백업 및 복구 등과 같이 고가용성이 필요한 경우
대역폭	3~10개 ID 지원	10~30 Mbps	56k~10Gbps
가용성	필요 시 인증을 통한 연결	Active-Standby 방식의 이중화 구성	고가용성 (일관된 성능 제공)
구축 시간	없음	없음	3~4주

[표 4-9 : SSL VPN, IPsec VPN, Cloud Connect 비교]

5

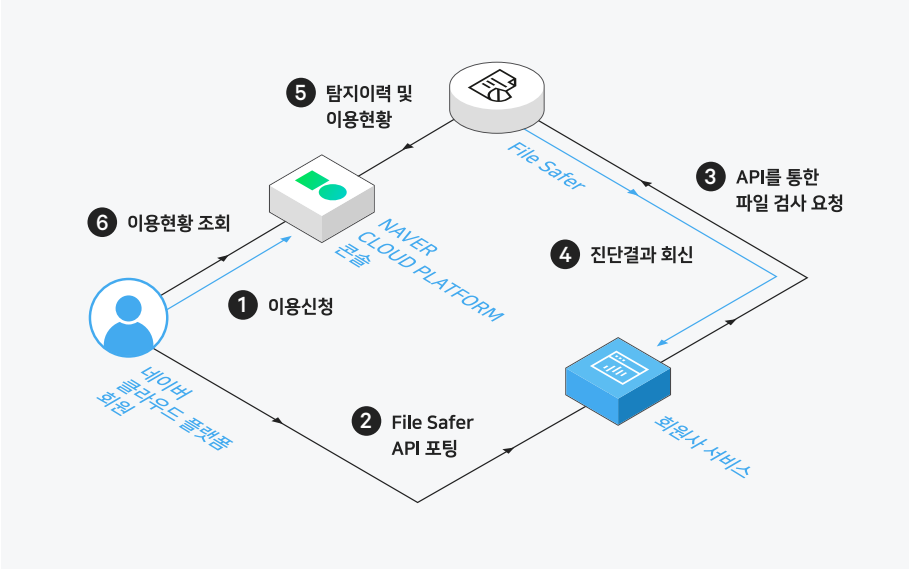
보안 위협 탐지 및 대응을 위한 클라우드 서비스

보안 위협 탐지 및 대응을 위한 네이버 클라우드 플랫폼의 다양한 클라우드 서비스를 소개합니다.

5.1 File Safer

File Safer는 웹 사이트에 업·다운로드 되는 파일의 악성코드 여부를 손쉽게 탐지하여 차단할 수 있는 서비스입니다. 네이버 메일과 블로그, 카페를 포함한 여러 서비스에서 활용하고 검증된 악성코드 필터링 시스템으로, 서비스의 성능을 유지하면서 효과적으로 악성코드를 차단하기 위해 Hash 필터와 File 필터를 REST API로 제공합니다.
Hash 필터는 악성으로 의심되는 파일이나 URL의 스트링에서 추출한 해시값을 이용하여 악성 여부를 확인할 수 있는 기능을 제공합니다. File 필터는 Hash 필터에서 확인되지 않은 파일을 업로드하여 악성 여부를 분석할 수 있는 기능을 제공합니다. 사용자 인터페이스와 연관되어 속도가 중요한 부분에는 더욱 속도가 빠른 Hash 필터를 사용하여 악성코드를 필터링하고, 시스템상에 인입되어 사용자에게 불편을 초래하지 않아야 하는 부분에는 좀 더 민감한 File 필터를 적용하여 서비스 성능을 유지하는 동시에 악성코드를 차단합니다.

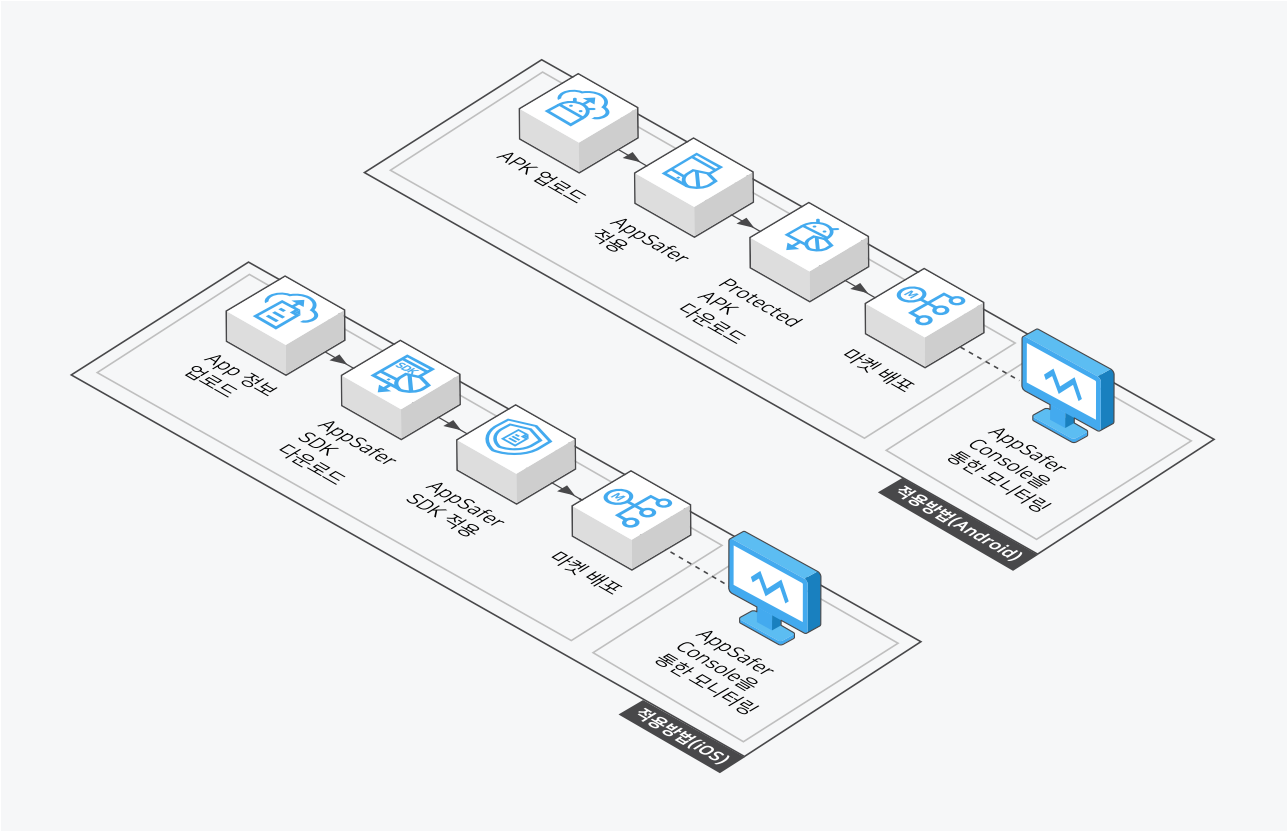
서비스를 운영하다 보면 게시판 등을 통해 파일이 업로드되거나 파일을 전달하는 경우가 빈번히 발생합니다. 이 과정에서 취약점을 악용한 악성코드가 업로드되거나 의도하지 않게 악성코드에 감염된 파일이 배포될 수 있습니다. File Safer는 업·다운로드되는 파일의 악성 여부를 확인하고 필요에 따라 허용하거나 차단하도록 설정하여 서비스 신뢰도를 향상시킬 수 있습니다.



[그림 4-14 : File Safer 이용 프로세스]

5.2 App Safer

App Safer는 모바일 기기에서 앱이 실행될 때 실시간으로 보안 위협을 탐지하고 보호하는 서비스입니다. 바이너리 위·변조, 메모리 변조, 해킹 등 다양한 보안 위협으로부터 모바일 애플리케이션의 안전한 실행 환경을 유지하기 위한 정책 설정 기능을 제공합니다.

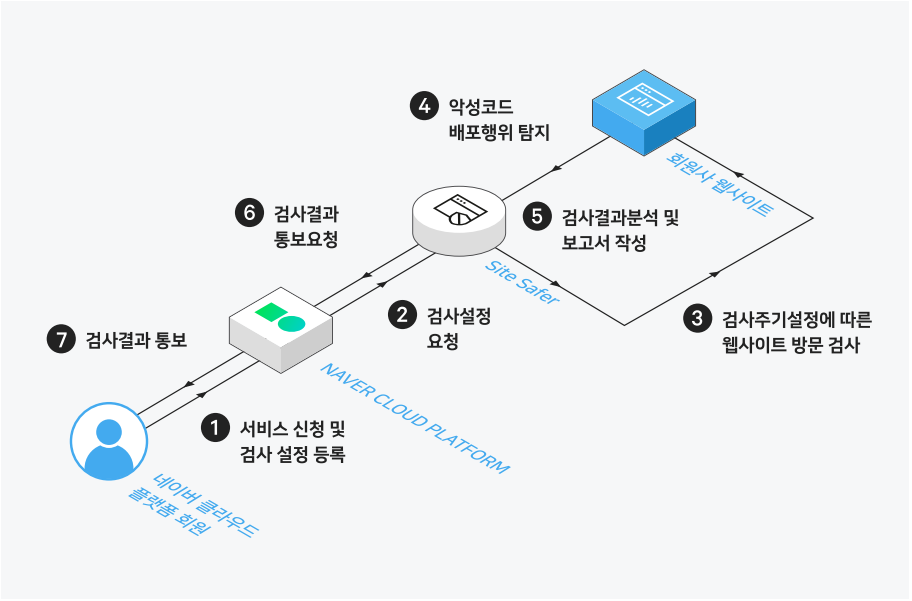


[그림 4-15 : App Safer 이용 프로세스]

APK 파일을 업로드하면 자동으로 App Safer의 보안 서비스가 적용되므로 쉽고 편리한 서비스 이용이 가능합니다. 콘솔에서 애플리케이션 등록, 설정 관리, 탐지 관리 조회를 한번에 진행할 수 있습니다. Android, iOS 애플리케이션에 특화된 보호 기능을 제공하기 때문에 보안 위협으로부터의 신속하고 정확한 대응이 가능합니다.

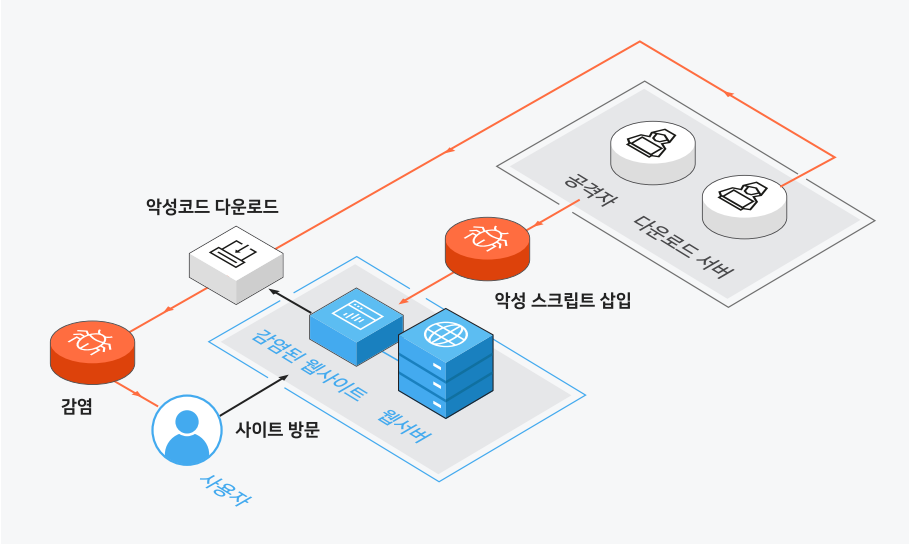
5.3 Site Safer

Site Safer는 웹 사이트에서 악성코드나 랜섬웨어와 같은 악성 파일의 배포 여부를 주기적으로 검사하는 서비스입니다. 악성 파일 배포를 패턴 기반이 아닌 행위 기반으로 탐지하여 다양한 케이스의 탐지가 가능하여 쉽고 편리하게 웹 사이트를 검사가 가능합니다.
한번 설정한 URL에 대한 주기적인 검사를 진행할 수 있고 알림 기능을 통해 검사 안내를 받을 수 있기 때문에 웹 사이트를 지속적으로 안전하게 관리하기에 유용합니다. Site Safer는 오랜 기간 네이버의 뉴스, 쇼핑 광고 등에 활용되고 있으며, 다수의 웹 사이트에서도 사용하고 있는 검증된 서비스입니다. 고객의 도메인 뿐만 아니라 웹 페이지에 추가된 외부 콘텐츠 및 URL에 대한 점검도 가능합니다.



[그림 4-16 : Site Safer 이용 프로세스]

최근 악의적인 목적을 가진 해커가 그림 4-17.과 같이 웹 사이트나 서버의 취약점을 이용하여 서비스를 조작하고 악성 파일을 배포하는 문제가 자주 발생하고 있습니다. 웹 사이트에 접근한 사용자는 사이트에 접속하는 행위만으로도 자신의 PC에 악성 파일이 설치될 수 있습니다. 악성 파일 설치 여부를 사용자가 인지할 수 없는 상태에서 사용자의 PC가 좀비 PC가 되어 다른 공격에 악용되기도 합니다. 특히 랜섬웨어와 같은 보안 위협의 경우 사용자에게 직접적인 피해를 주기 때문에 웹 사이트를 운영하는 서비스 제공자는 다양한 보안 위협에 대비하는 시스템을 주의 깊게 고민할 필요가 있습니다. 만약 기업이나 고객이 이러한 고민이 부족하여 악의적인 공격에 대한 자체 대응 시스템을 갖추지 못했다면 해킹과 악성코드 탐지의 어려움에서 결코 자유로울 수 없습니다. 이러한 경우 Site Safer를 도입한다면 별도 시스템 구축 없이도 보안 위협에 효과적인 대응이 충분히 가능합니다.



[그림 4-17 : 악성 웹 사이트를 통한 사용자 공격 프로세스]

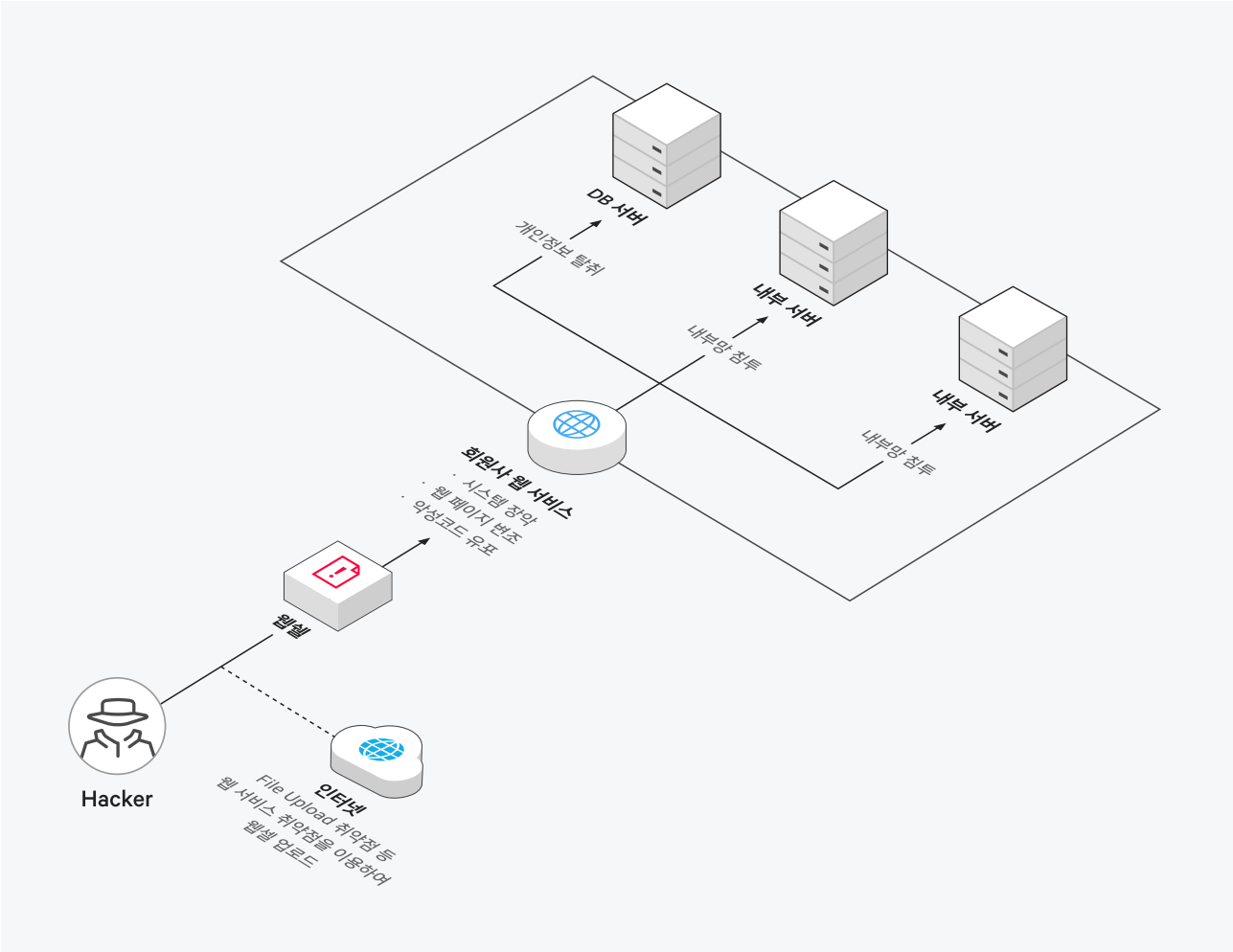
Safer 시리즈를 통해 모바일 애플리케이션, 파일, 웹 사이트 등에 대한 보안 위협을 사전에 대응할 수 있는 프로세스를 수립하여 공격자의 공격 통로가 되는 서비스 취약점을 제거할 수 있습니다. 이로 인해 다수의 사용자에게 안전한 서비스를 제공할 수 있게 되며, 각종 보안 인증 및 금융, 공공 관련 법률도 준수할 수 있습니다.

인증 및 법률	클라우드컴퓨팅서비스 정보보호에 관한 기준	전자금융감독규정	ISMS-P
항목	기술적 보호조치 중 9.2.1 악성코드 통제	제16조(악성코드 감염 방지대책) 제1항	2.10.9 악성코드 통제
세부 내용	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상 PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한, 이상 징후 발견 시 이용자에게 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.	금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다. 1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것 2. 악성코드 검색 및 치료프로그램은 최신 상태로 유지할 것 3. 악성코드 감염에 대비하여 복구 절차를 마련할 것 4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.

[표 4-10 : Safer 시리즈 활용을 통한 인증 및 법률 준수]

5.4 Webshell Behavior Detector

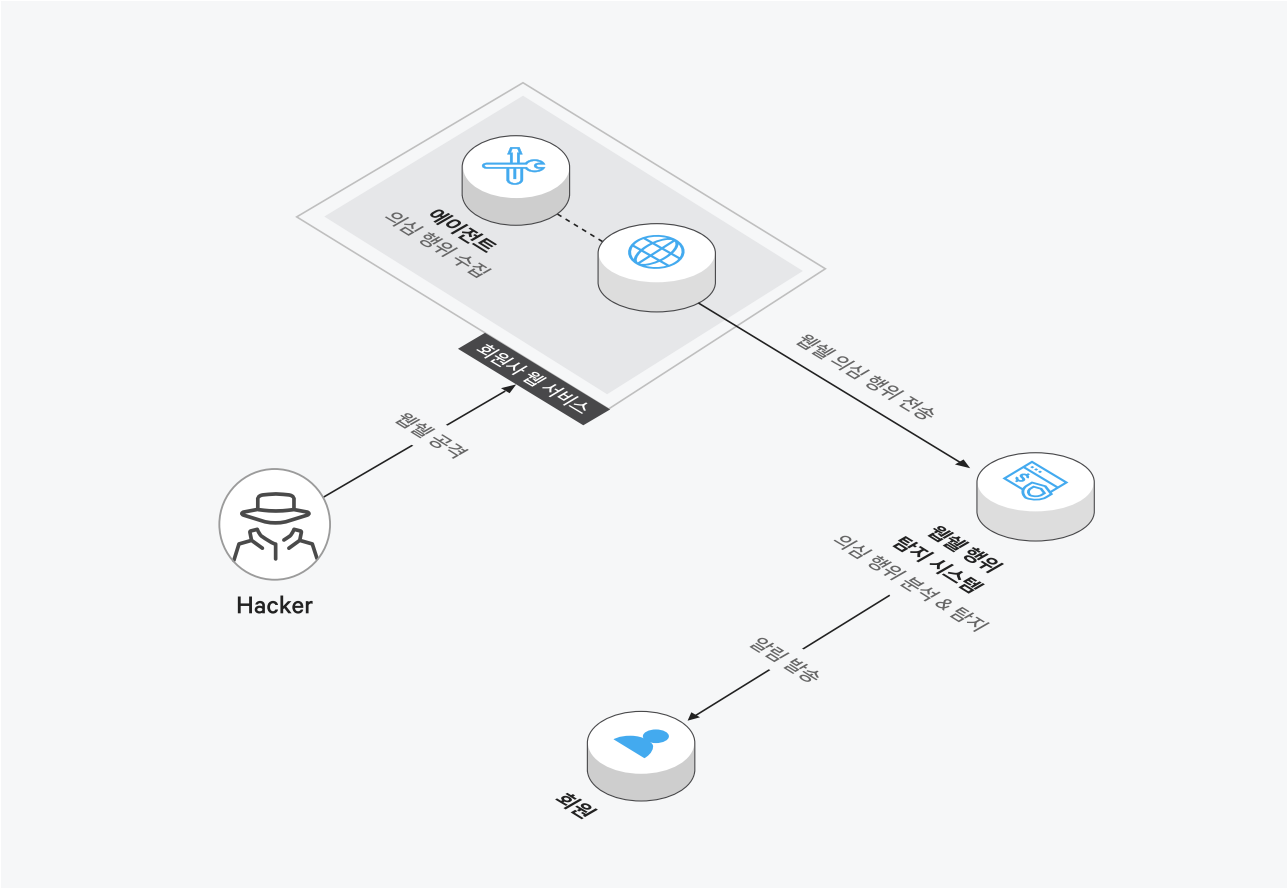
Webshell Behavior Detector는 웹 서비스를 안전하게 보호하기 위해 Webshell 공격을 실시간으로 탐지하고 알림을 발송하는 서비스입니다. Webshell 공격은 탐지를 회피하기 위한 다양한 은폐 기술이 존재하여 탐지가 매우 어렵습니다. 하지만 Webshell Behavior Detector는 이러한 은폐 기술을 무력화하여 기존 유형은 물론 새로운 유형의 Webshell 공격도 문제 없이 실시간 탐지가 가능합니다.



[그림 4-18 : Webshell 공격 프로세스]

Webshell Behavior Detector 서비스는 고객 서버 내 설치된 에이전트를 통해 정보를 실시간으로 수집하여 분석 서버로 전송합니다. 수집된 정보를 바탕으로 Webshell 행위로 판단될 경우 빠르게 대응할 수 있도록 알림을 발송합니다. 또한 콘솔에서 Webshell 분석 및 대응 시 참고할 수 있는 Webshell 의심 행위, Webshell 의심 파일, 공격자 의심 IP 주소를 제공합니다.

따라서 Webshell Behavior Detector를 활용한다면 실시간 탐지 및 대응이 가능합니다. Webshell 의심 행위 알림을 받은 경우 즉시 분석 및 대응을 할 수 없는 상황일지라도 네이버 클라우드 플랫폼 콘솔에 접속한 다음 파일 격리 기능으로 의심 파일을 격리 조치하여 공격을 일시적으로 차단한다면 사용자의 피해를 최소화할 수 있습니다.



[그림 4-19 : Webshell Behavior Detector 서비스 구성]

Webshell Behavior Detector 서비스를 활용하여 Webshell 공격으로부터 웹 서비스를 안전하게 보호하고 관리한다면 웹 서비스 보안 관련 인증 및 법률에서 요구하는 기준을 충분히 충족할 수 있습니다.

인증 및 법률	ISMS-P	PCI-DSS	정보통신기반 보호법
항목	2.8.2 보안 요구사항 검토 및 시험	6.6	제9조(취약점의 분석·평가) 제1항
세부 내용	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현 되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선조치를 수행하여야 한다.	일반인들이 접촉하는 웹 어플리케이션의 경우, 새로운 위협과 취약성을 지속적으로 다루고, 이러한 어플리케이션이 다음 방법들 중 하나를 이용해 알려진 공격으로부터 보호될 수 있게 한다. 수동 혹은 자동 어플리케이션 취약성 보안 평가 도구나 방법을 이용해 변경 이후 최소 일년 단위로 일반인들이 접촉하는 웹 어플리케이션을 검토한다.	관리기관의 장은 대통령령으로 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

[표 4-11 : Webshell Behavior Detector 활용을 통한 인증 및 법률 준수]

Section 5. 클라우드 환경 보안 감사

1 클라우드 환경의 보안 규제

클라우드 산업의 발전에 따라 각 산업에서 준수해야 할 클라우드 관련 규제가 규격화됐습니다. 금융권에서 퍼블릭 클라우드를 도입하기 위해서는 CSP 안전성 평가를 받아야 합니다. 클라우드 서비스 제공자가 공공 기관에 클라우드를 도입하려면 클라우드 서비스 보안 인증을 획득해야 합니다. ISMS-P 인증 대상 기업 중 클라우드를 사용하려는 기업은 ISMS-P 인증 항목 중 클라우드 보안 항목에 대한 기준을 준수해야 합니다.

클라우드 이용 시 보안 감사에 해당하는 항목은 금융 분야 클라우드 컴퓨팅 서비스 이용 가이드의 안전성 확보 조치 방안 수립 중 로깅 부분에 해당하며, 공공 기관이 준수해야 하는 클라우드 컴퓨팅 서비스 정보보호에 관한 기준의 기술적 보호 조치에 세부 내용을 명시하고 있습니다.
또한 ISMS-P 인증 대상 기업 중 클라우드를 사용하는 기업은 클라우드 서비스 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하도록 명시하고 있습니다.

클라우드 환경의 보안 감사는 위협 대응 뿐만 아니라 규제를 준수하기 위해서도 반드시 이행해야 하는 중요한 활동입니다.

보안 감사에는 다양한 항목이 존재하지만, 좀 더 쉬운 이해를 돕기 위해 사용자 변경 작업을 바탕으로 레거시 환경과 클라우드 환경을 비교해보도록 하겠습니다.

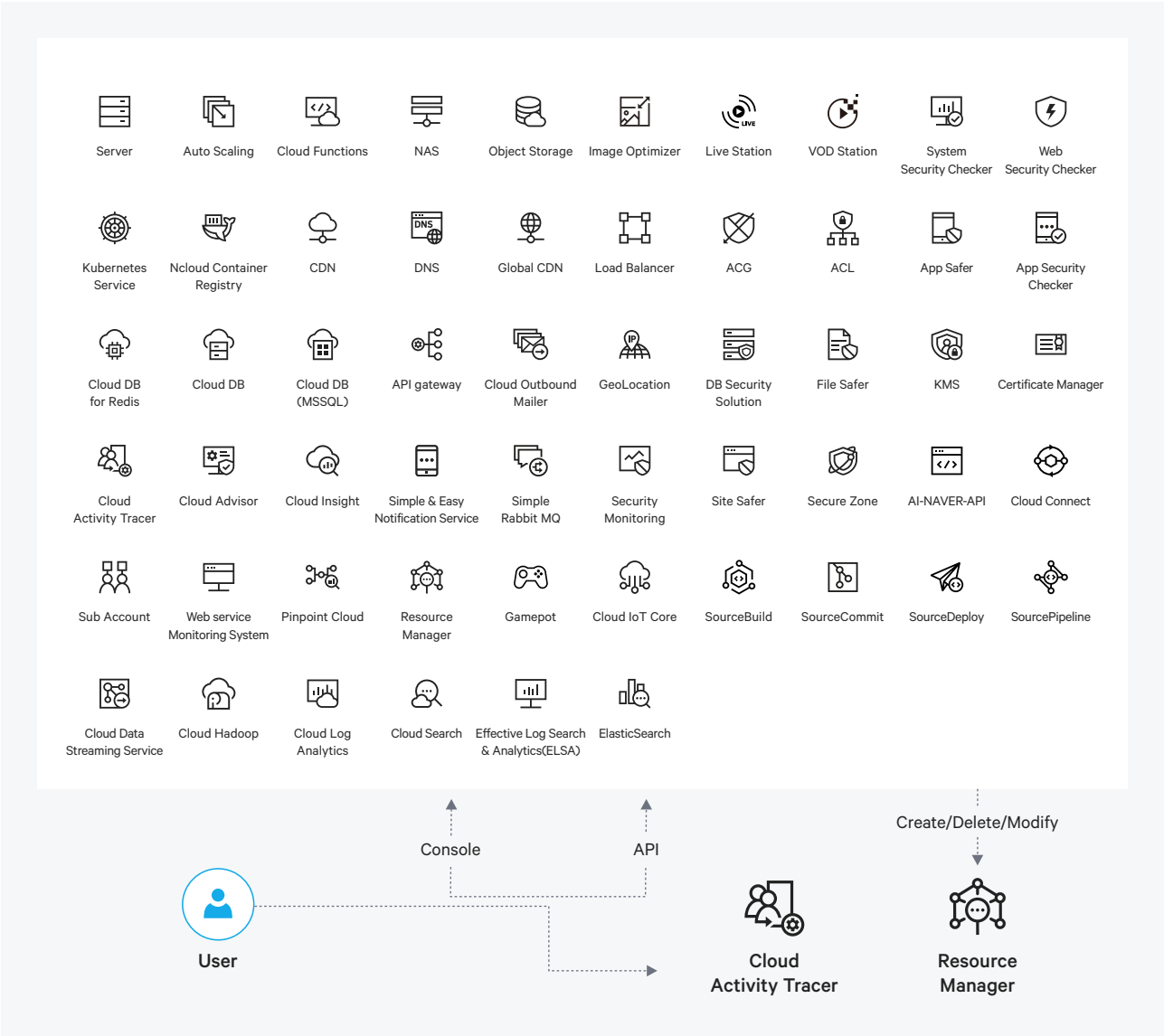
레거시 환경에서는 특정 사용자가 IDC에 출입하여 장비를 설치하고 Config를 설정하는 행위를 하는 경우 해당 사용자가 출입 인가된 사용자인지, 장비는 반·출입 허용이 된 장비인지, Config 설정은 승인된 작업인지 여부를 검토할 것입니다.
또한 그에 대한 증적으로 출입통제 시스템, 반출입대장, 변경 작업 요청서를 검토할 것입니다.
그리고 주기적으로 증적을 검토하여 비인가 행위, 승인 없는 변경 작업 등을 검토해야 합니다.

그렇다면 클라우드 환경에서는 어떻게 진행될까요?
작업자의 물리적 출입, 물리적 작업 공간이 없어 졌을 뿐 큰 차이는 없습니다. 어떤 사용자가 클라우드 환경에 접속하여 어떠한 작업을 수행했는지에 대한 내용을 검토하면 되는 것입니다.
다만 클라우드 특성상 언제 어디서든 접속할 수 있고, 작업을 수행할 수 있기 때문에 사용자의 접근 통제 절차, 변경 작업 승인 절차에 대한 내부 규정이 필요할 것이며, 그 행위를 주기적으로 감사하고 모니터링하는 행위가 반드시 수반되어야 할 것입니다.

2 네이버 클라우드 플랫폼 보안 감사

네이버 클라우드 플랫폼에서는 Cloud Activity Tracer 상품을 통해 보안 감사를 수행할 수 있습니다.
Cloud Activity Tracer는 리소스와 관련된 계정 내 모든 활동을 기록하며 특정 활동에 대한 접근 시간, 접근 ID, 작업 내용 등에 대한 로그를 제공합니다. 계정 활동 기록은 90일간 보관하기 때문에 언제든지 콘솔에서 확인이 가능하며 감사 로그로도 활용할 수 있습니다. Object Storage 서비스와 연동한다면 계정 활동 기록을 원하는 기간만큼 장기간 보관할 수도 있습니다.

콘솔과 API를 통해 수행한 활동을 기록하는데, 이 기록은 상품, 리전, 계정, 작업 내역에 따라 검색하여 확인이 가능합니다.



[그림 5-1 : Cloud Activity Tracer를 이용한 보안 감사]

Cloud Activity Tracer는 Activities, Tracer로 구분할 수 있습니다.

Activities에서는 계정 내 활동 기록에 대한 이력을 확인할 수 있습니다.
작업 일시, 작업 내역, 작업 결과, 상품명, 리소스 유형, 리전, 플랫폼, 계정 구분, 요청 구분, 작업 상세 탭으로 구분되어 있으며 특정 작업을 확인하고 싶은 경우 필터를 설정하여 검색이 가능합니다. 단, Cloud Activity Tracer 콘솔은 90일 간의 활동 기록만 보관된다는 점을 유의하여 사용해야 합니다. Cloud Activity Tracer 로그를 90일 이상 보관하려는 경우 Tracer를 설정하여 앞서 언급한Object Storage에 보관해야 합니다.

Tracer에서는 Cloud Activity Tracer 로그를 보관하기 위한 설정을 할 수 있습니다. Tracer에는 Default 타입과 Custom 타입이 존재합니다.
Default 타입은 Tracer 이름 및 상세 조건을 임의로 설정할 수 없으며, 계정당 1개만 생성 가능하며 무료로 이용할 수 있습니다. Custom 타입은 Tracer 상세 조건을 임의로 설정할 수 있으며 계정당 여러 개의 Tracer를 생성할 수 있습니다. 단, 내보내는 이벤트 데이터 건 수를 합산하여 요금이 별도로 발생합니다.

전송 데이터 형식은 JSON, CSV 두 가지 중 선택하여 내보내기할 수 있습니다. CSV로 내보내기하는 경우 cell 표현 가능 범위(32767)가 넘는 데이터를 포함하게 되면 해당 데이터 필드는 내보내기가 수행되지 않습니다. 이러한 경우 JSON으로 내보내기를 수행해야 합니다.

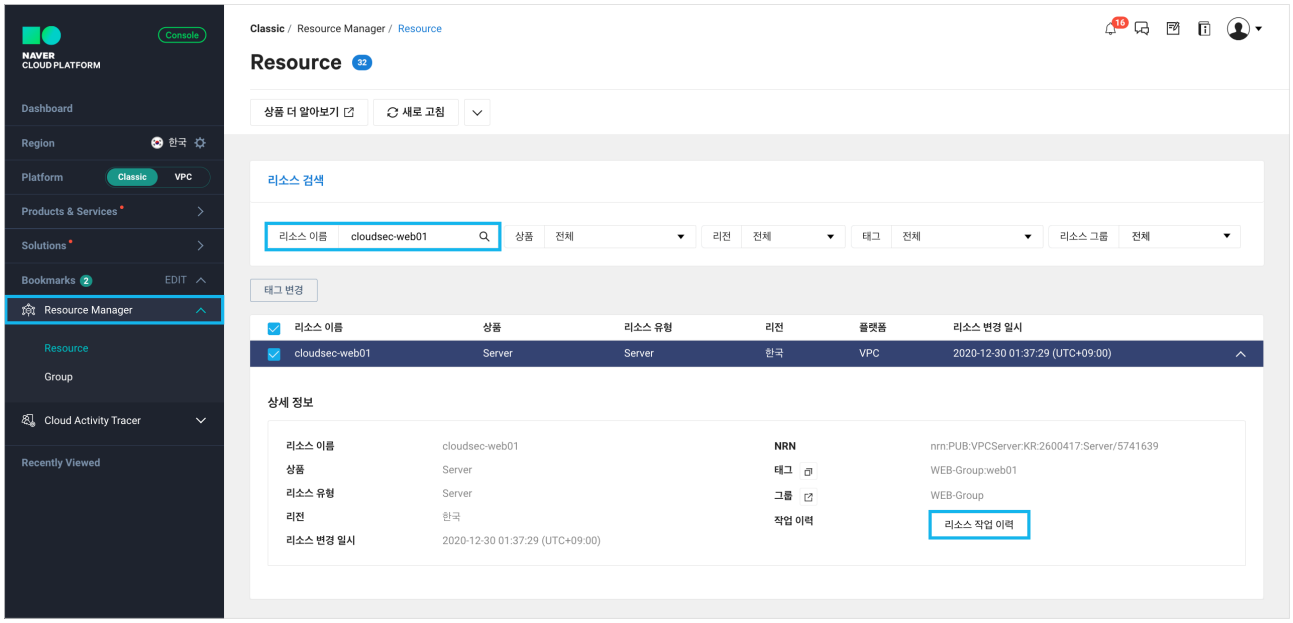
Tracer 이름, 대상 Bucket, Object Storage 전송 시점 확인이 모두 선택되면 생성 버튼이 활성화 됩니다. 생성을 완료하게 되면 Tracer 조건에 해당하는 사용자의 활동 이력을 15일 이후 하루 단위로 Bucket에 전송합니다. 단, Tracer 신규 생성 시에는 90일 이전 활동 이력부터 15일 전까지의 활동 이력을 Object Storage로 일괄 내보냅니다.

3 Cloud Activity Tracer 보안 감사 시나리오

특정 웹 서버가 승인 없이 중지되어 장애가 발생됐다고 가정하고 원인을 추적하기 위해 Resource Manager와 Cloud Activity Tracer를 이용하여 원인을 파악하는 보안 감사 시나리오를 소개합니다. 시나리오 순서는 다음과 같습니다.

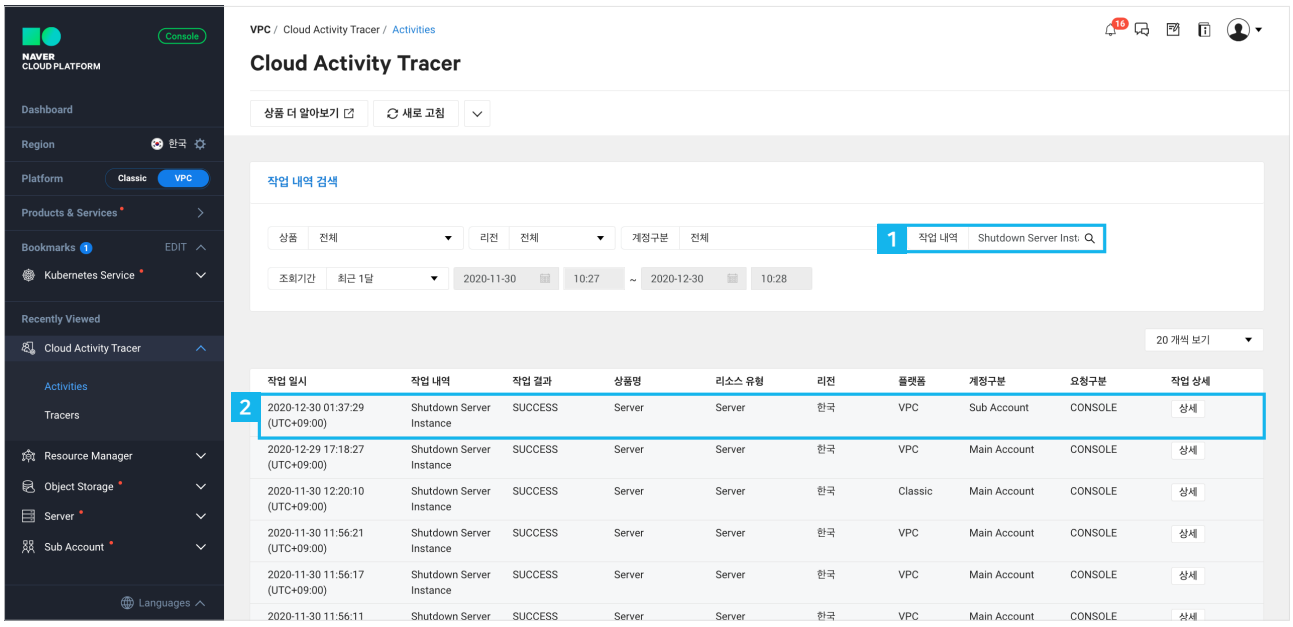
1. 콘솔에 접속하여 서버 목록 중 중지 상태의 서버를 확인합니다. 이 시나리오에서는 cloudsec-web01 서버가 중지되어 있는 것을 확인했습니다.

2 Resource Manager로 이동하여 서버 콘솔에서 확인한 서버명 cloudsec-web01을 리소스 이름 검색 필터에 입력합니다. 검색된 리소스의 내용을 펼친 다음 리소스 작업 이력을 클릭합니다.



3 서버가 마지막으로 중지된 시점을 확인합니다. 이 시나리오에서는 2020년 12월 30일 01시 37분 29초에 콘솔에서 서버 중지가 실행됐습니다.

4 Cloud Activity Tracer로 이동하여 작업 내역과 기간을 선택한 다음 서버 중지 이력을 검색합니다. 이 시나리오에서는 중지된 시간을 알고 있기 때문에 Shutdown Server Instance 작업 내역으로 검색하여 Resource Manager에서 확인한 중지 시간과 일치하는 작업 내용을 검색합니다.



5 작업 상세를 클릭하여 서버를 중지한 계정, IP 정보 등을 확인합니다. 알 수 없는 작업의 경우 특정 작업자의 실수일 수도 있고, 계정 정보의 유출로 인한 비인가 행위일 수도 있습니다. 따라서 해당 계정 활동 기록을 확인할 필요가 있습니다.

6 계정 활동에 대한 추적을 위해서 Tracer에 저장된 CSV, JSON 파일을 다운로드하여 확인합니다. Cloud Activity Tracer에서 확인할 수도 있지만 잘 사용하지 않았던 계정인 경우 계정의 생성 시점, 접속 시점 등을 확인하기 위해 90일 이상의 데이터가 필요할 수 있습니다. 따라서 Object Storage에 별도로 저장한 데이터를 확인할 필요가 있습니다.

7 계정 소유자를 통해 작업에 대한 내용을 파악하고 작업 실수, 계정 정보 유출에 대한 내역을 함께 검토합니다. 주기적으로 관련 기록을 검토하여 비인가 계정의 활동, 승인되지 않은 리소스의 변경을 모니터링해야 합니다.

네이버 클라우드 플랫폼에서는 Object Storage에 저장된 오브젝트를 수집할 수 있도록 API를 제공하고 있습니다. 따라서 Cloud Activity Tracer의 데이터를 SIEM이나 모니터링 도구로 전송하여 감사를 자동화하는 방안도 구상할 수 있습니다.

결론

전세계적으로 퍼블릭 클라우드 서비스 시장 규모가 급성장하고 있으며 국내 역시 동일한 성장세를 보이고 있는 가운데 기업(또는 고객)에게 클라우드 도입에 있어 보안 환경 구축은 가장 중요한 화두입니다.

네이버 클라우드 플랫폼은 이러한 고객의 고민을 인지하여 다수의 보안 인증을 획득한 기술과 경험을 토대로 보안 인프라 지원 뿐 아니라 다양한 클라우드 보안 서비스를 제공하여 안전한 보안 환경 구축을 지원하고 있습니다.

네이버 클라우드 플랫폼의 보안 서비스는 위협 탐지 대응(Detection/Response), 사용자 인증(Authentication/Authorization), 접근 통제(Access Control), 데이터 보호(Data Protection), 감사 추적(Audit Logging), 취약점 관리(Vulnerability Management), 컴플라이언스(Compliance), 전송 구간 암호화(Private Connectivity)의 총 8개 영역으로 세분화하여 제공합니다.
뿐만 아니라 네이버 클라우드 플랫폼의 보안 서비스는 위협 대응 및 규제 준수 목적으로 반드시 이행해야 하는 클라우드 환경 보안 감사에도 활용할 수 있습니다.

이 백서에서 설명한 네이버 클라우드 플랫폼의 보안 서비스와 이용 사례를 참고한다면 좀 더 쉽고 안전하게 클라우드 보안 환경 구축이 가능합니다.

NAVER Cloud