NHN Cloud로 알아보는 클라우드 보안

박관규 / NHN Cloud

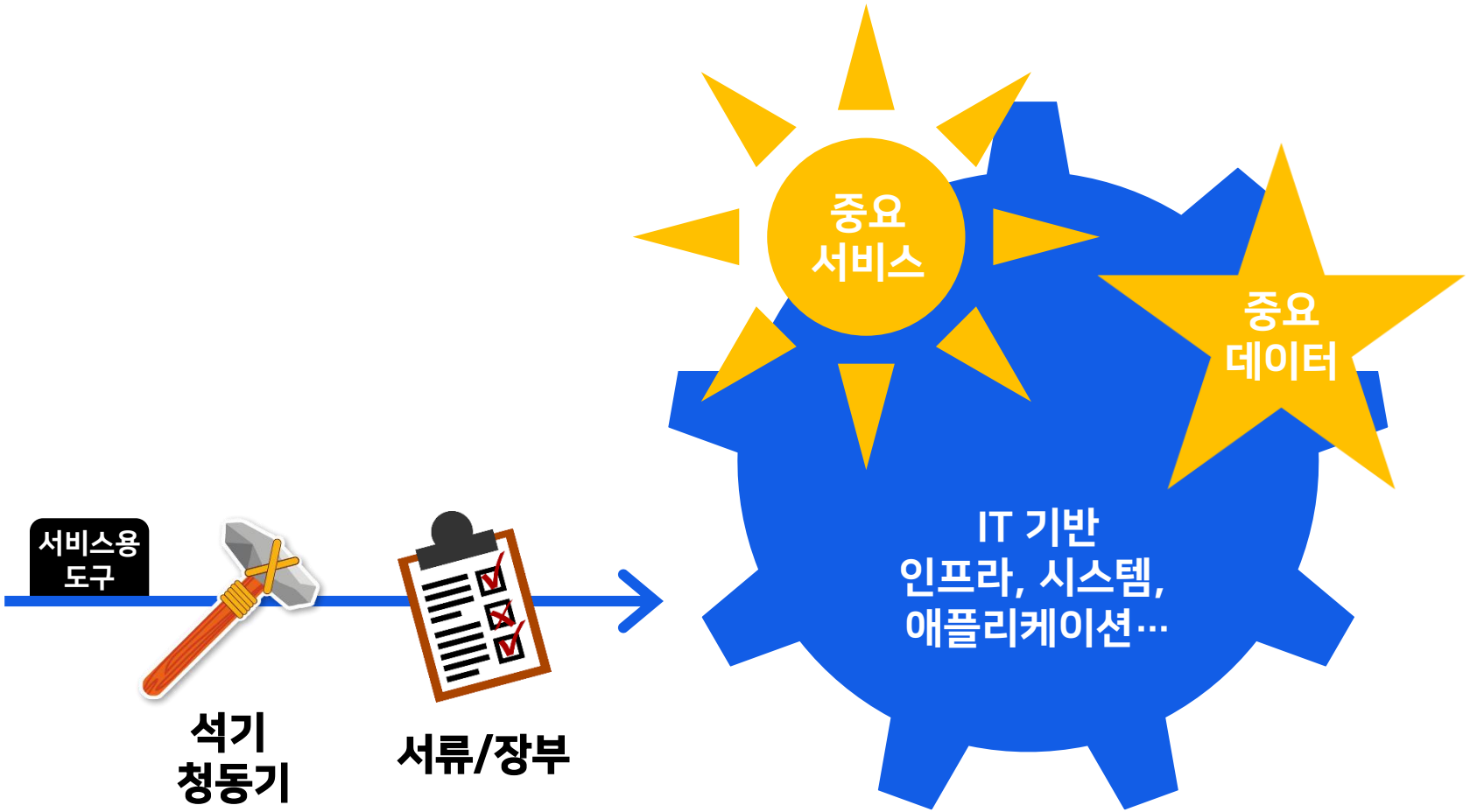
목차

클라우드 보안이란?

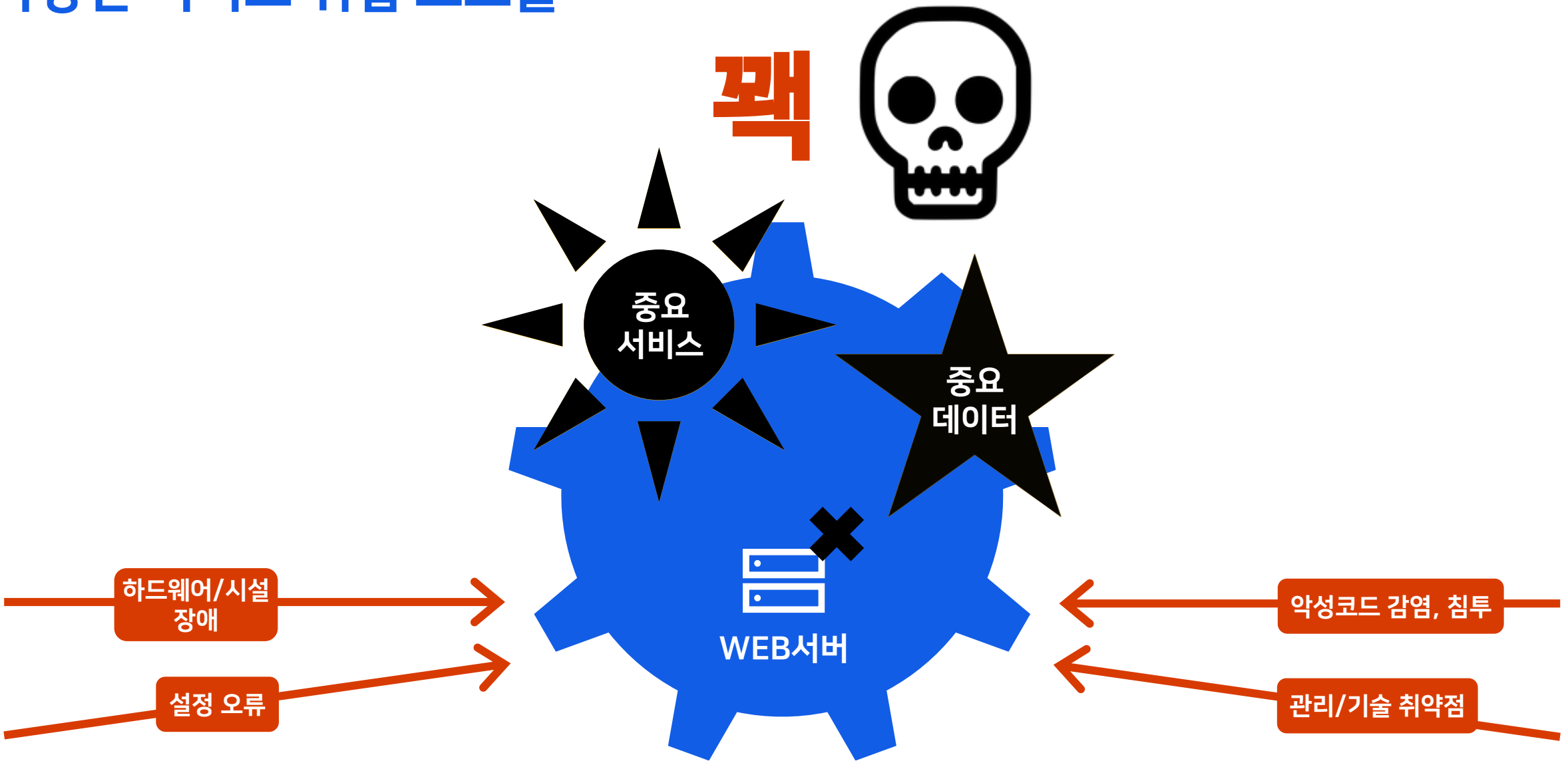
IT 서비스와 인프라

공익 또는 이익을 위한
우리 조직의 중요 서비스와 자료들

IT 서비스와 인프라



다양한 서비스 위협 요소들



서비스 중단과 파멸

대외 이미지 수락

ㅠㅠㅠ

감봉

영업 정지

과징금

직위 해제

감봉

서비스 중단과 파멸

파멸은...
막아야 하지
않겠나

-by 사장님-

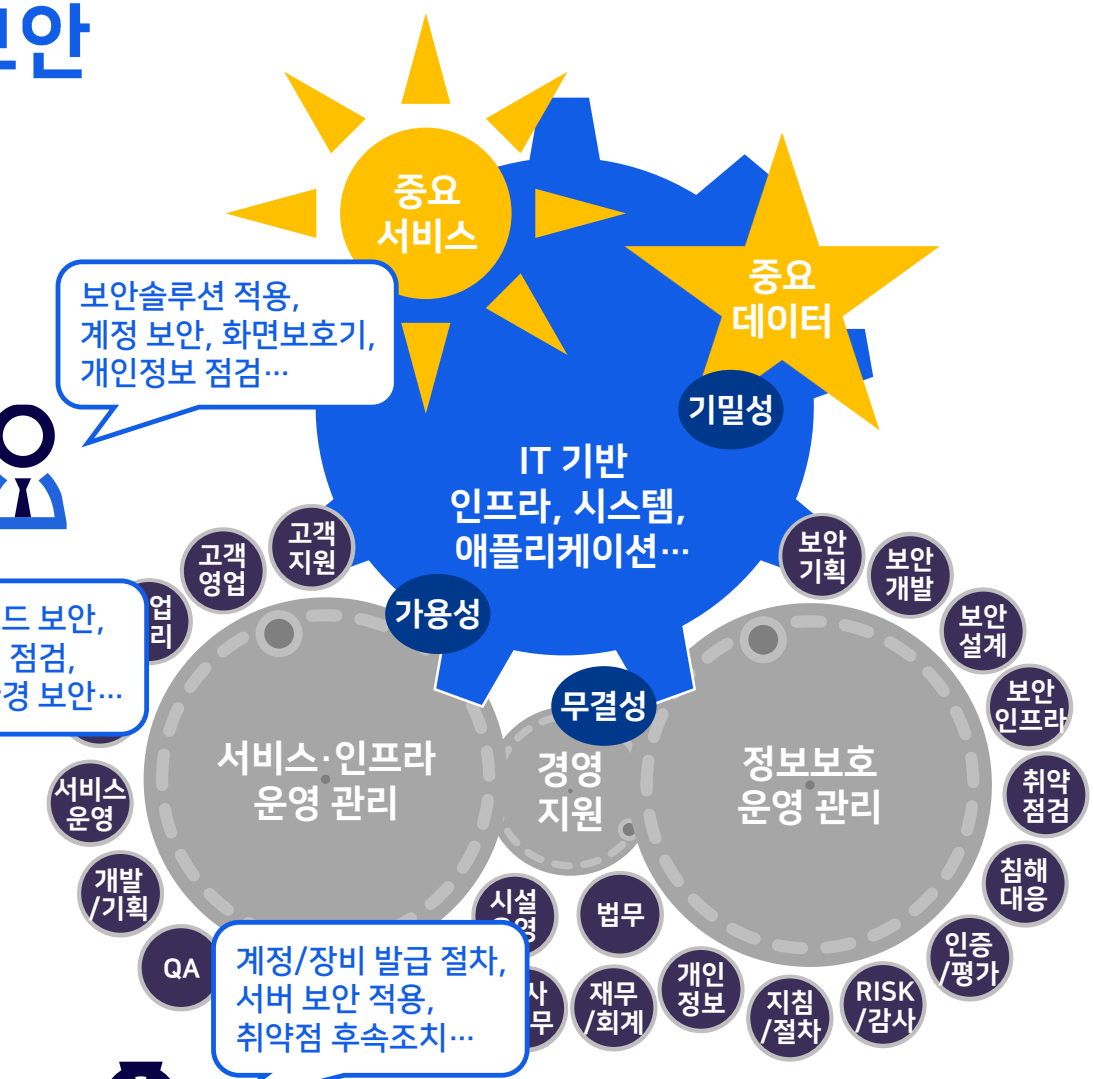
The
GodCEO

자네 월급을 깎고 싶지는 않네

쉽게 말해서 IT 보안이란

중요 서비스를 유지하고 데이터의 훼손을
방지하기 위한 모든 방법과 활동

우리 모두에 의한 보안



보안솔루션 적용,
계정 보안, 화면보호기,
개인정보 점검…

고객 담당자

소스코드 보안,
취약점 점검,
개발환경 보안…

개발자

계정/장비 발급 절차,
서버 보안 적용,
취약점 후속조치…

시스템/NW/DB 담당자

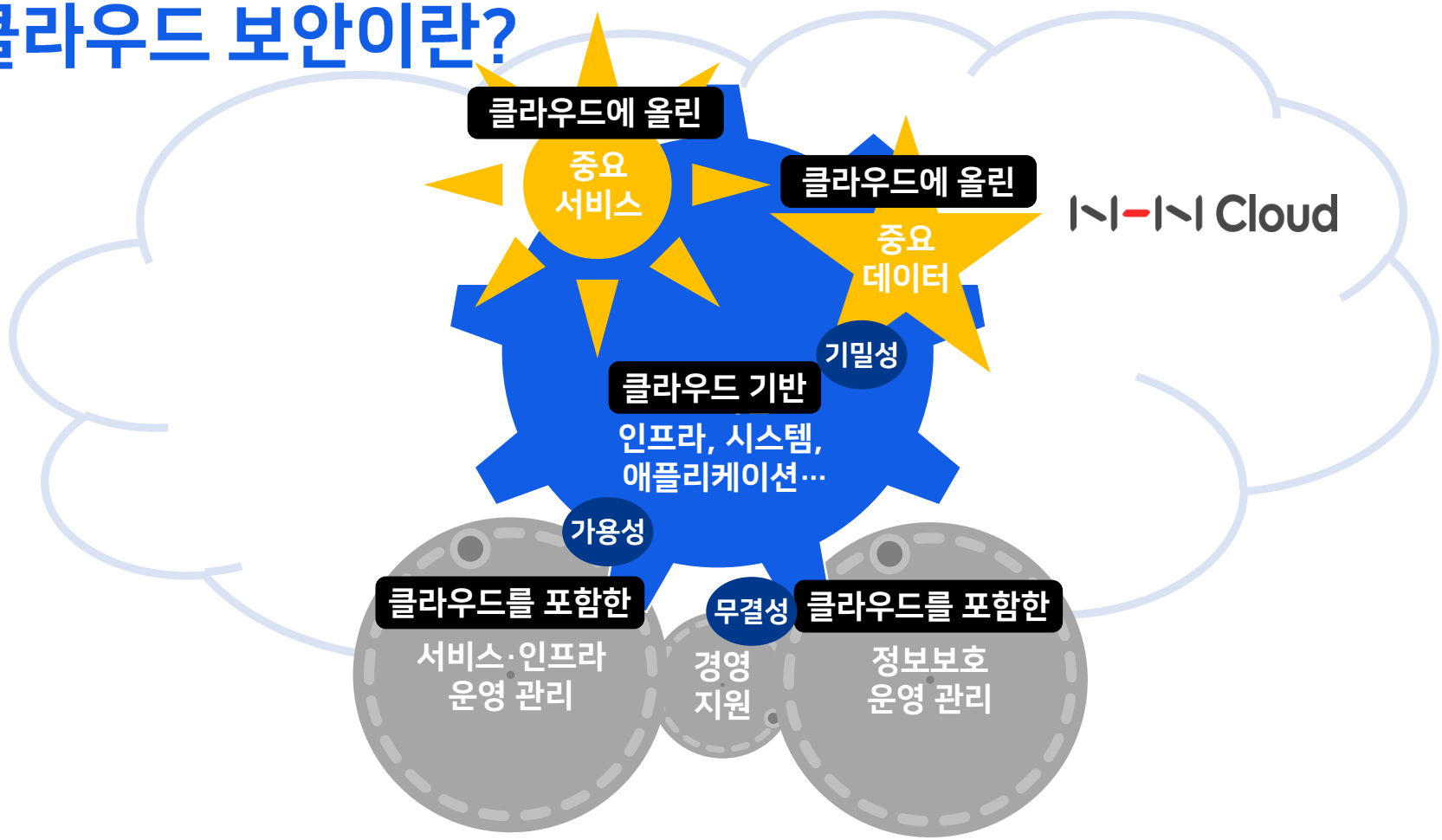
업무지원 담당자

기술 보안 담당자

관리 보안 담당자

아무도 해치지 않습니다. 친하게 지내요

그렇다면 클라우드 보안이란?



클라우드 기반 서비스가 안전하도록

클라우드 인프라에 가용성, 기밀성, 무결성 적용

그렇다면 클라우드 보안이란?

계정/권한/자산/정책
신청, 검토 및 승인

RISK 검토 요청

자산 관리

운영 절차/지침

고객지원/경영지원	개발	시스템/NW/DB
단말기 안전성 확보조치	소스코드/서비스 안전성 확보조치	시스템 안전성 확보조치
근무환경 보안 적용	개발환경 보안 적용	운영환경 보안 적용
개인정보 점검/후속조치	취약점 점검/후속조치	취약점 점검/후속조치

인프라 운영 및 지원 조직

계정/권한/자산/정책/RISK
검토 및 승인

보안 기획/현황분석

자산 관리

운영 절차/지침

위협 식별/관리

법무/관리보안	기술보안
법무/감사/전략/대외정책	앱/시스템 취약점 점검, 분석
보안 정책/절차/지침/교육	침해사고 감시/분석/대응/전파
개인정보/위수탁 관리, 점검	보안인프라 설계/검토/운영
정보보호 인증 관리	보안데이터 분석, 보안도구 개발

법무/정보보호 조직

정보보호 운영 관리 주요 활동

클라우드에서의 고민거리들

아직 클라우드 못 믿겠어요

마음을
열지 못한
고객

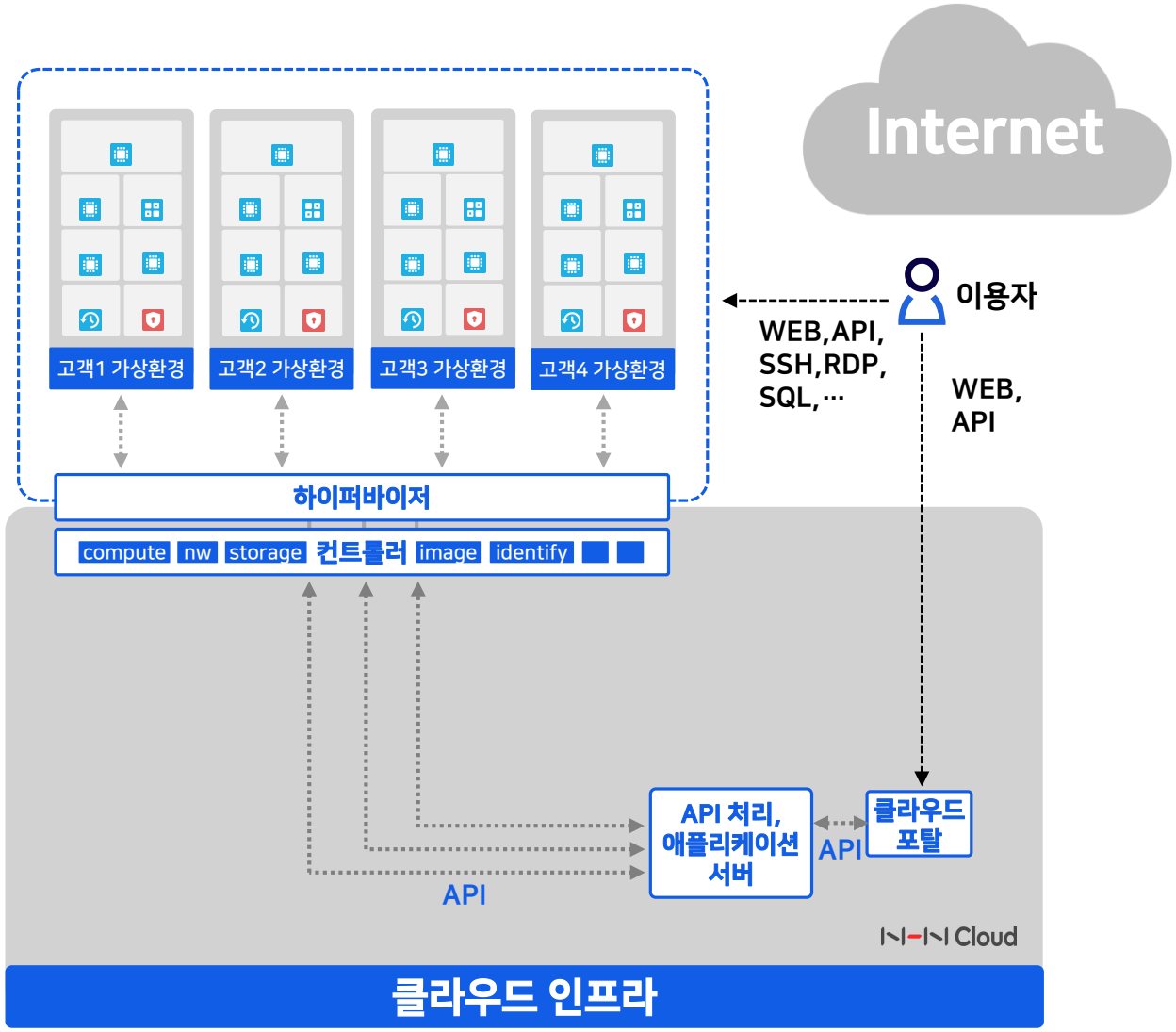
난 이 이용 반대일쎄

좀 더 안전성이
확보된 후에 찾아 오게나

정보보호
출신

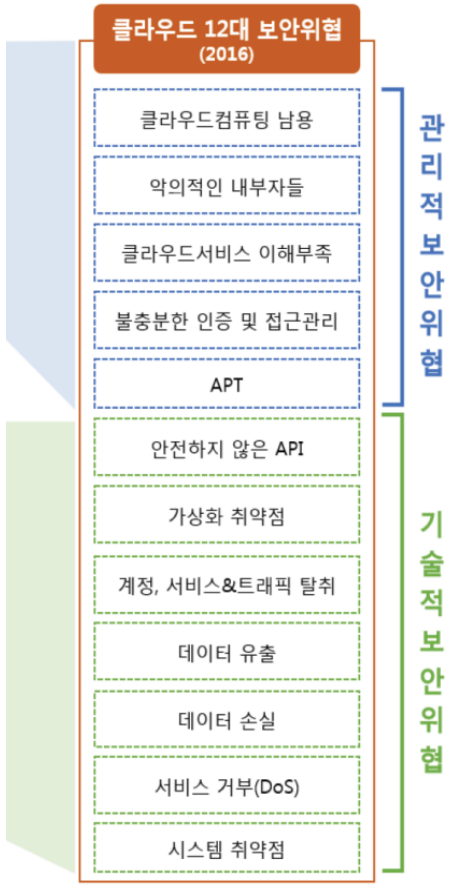
고객
아버님

클라우드 기본 구조

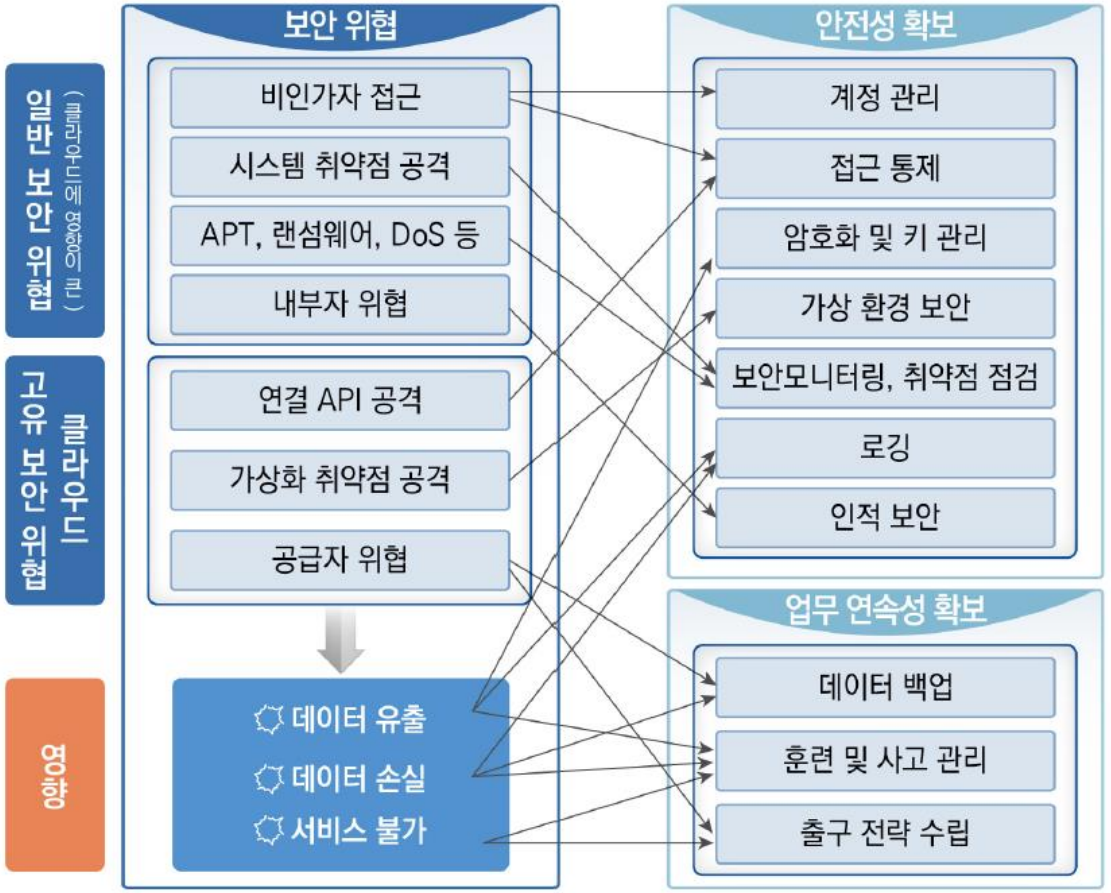

Internet
이용자
WEB,API,
SSH,RDP,
SQL,…
WEB,
API
고객1 가상환경
고객2 가상환경
고객3 가상환경
고객4 가상환경
하이퍼바이저
compute
nw
storage
컨트롤러
image
identify
API 처리,
애플리케이션
서버
API
클라우드
포탈
API
Cloud
클라우드 인프라

주로 겪는 공포와 환청

["CSA 클라우드 서비스의 보안위협 현황"
- 클라우드 정보보호 안내서 - KISA]



["클라우드 서비스 관련 보안위협"
- 금융분야 클라우드컴퓨팅서비스 이용 가이드 - 금융보안원]



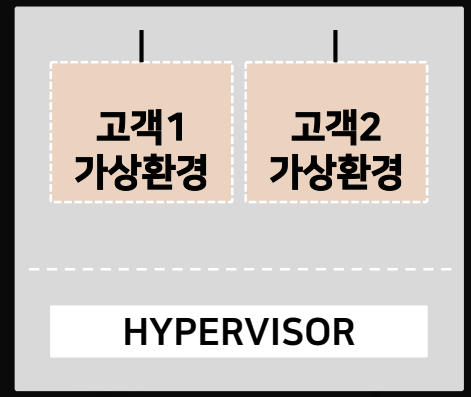
[국가 공공기관 클라우드 컴퓨팅
보안 가이드라인 - 국가정보원]

비밀..ㅋ

왼쪽 것들과 비슷함

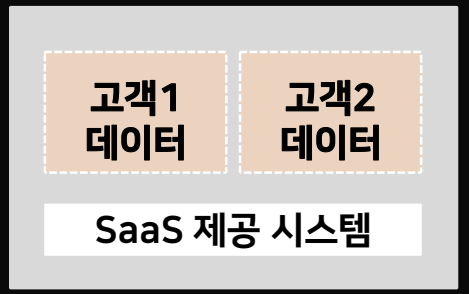
주로 겪는 공포와 환청

물리장비가
털리면 어쩌지?



클라우드
단골
취약점

장애 나면
책임지나?!



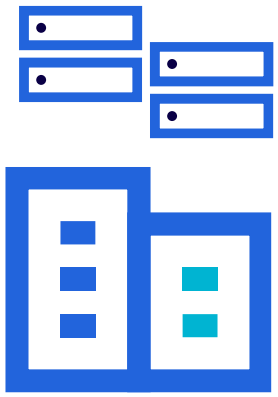
다른 고객과
내 데이터가
섞인다구?

우리 조직이 요구하는
보안기능 모두 제공하기 어려울 껄?

무엇보다 더

바빠 죽겠는데
배울 거는 많아졌고
사람은 부족해

LEGACY INFRA



대규모
레거시망
운영 중

클라우드
추가요

NEW! CLOUD PORTAL

NEW! K8S

NEW! RDS

NEW! OBS

NEW! IaC

NEW!

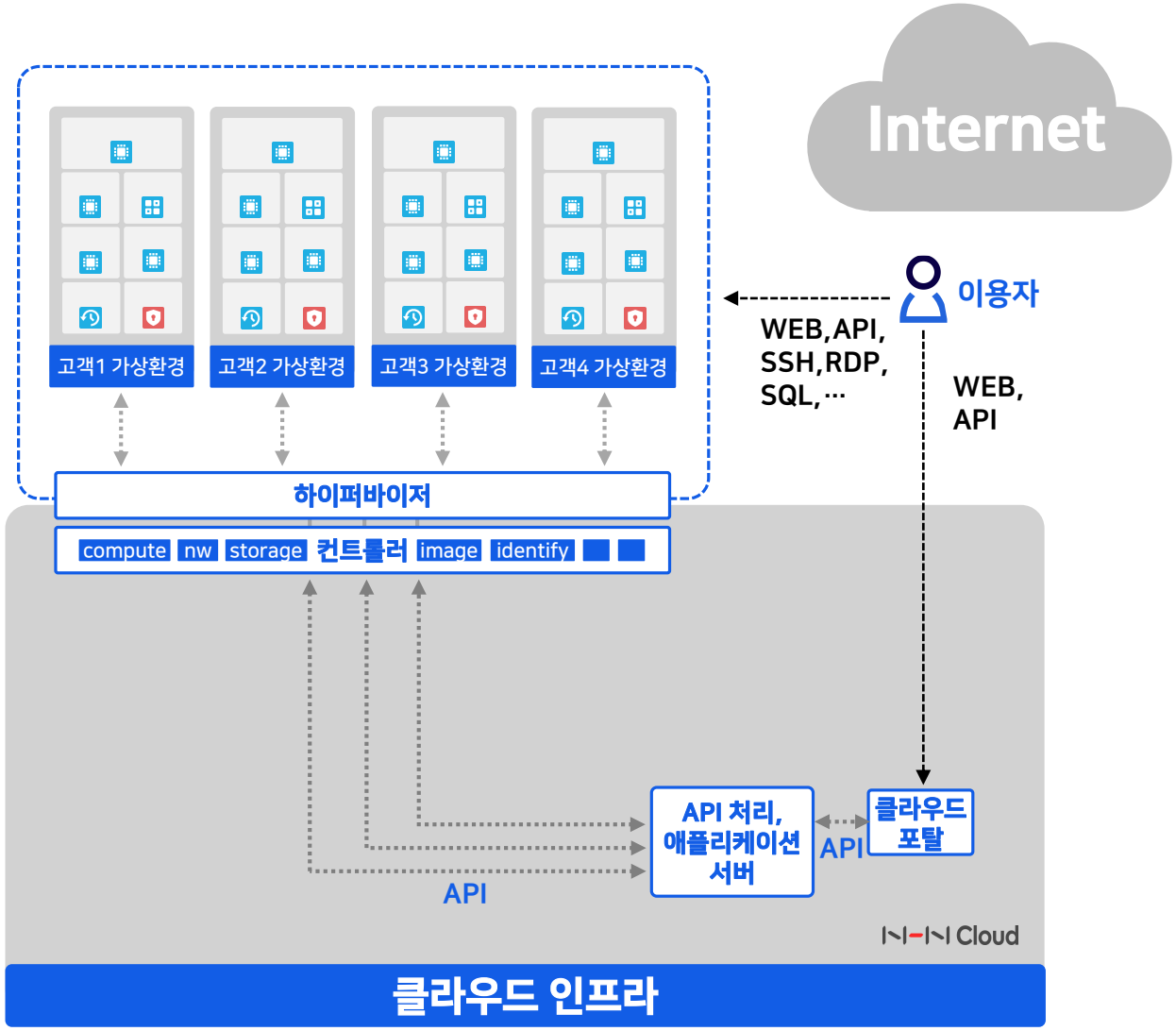
여기에 보안까지 고민해야 해?

공고 올릴테니
블라인드는 제발

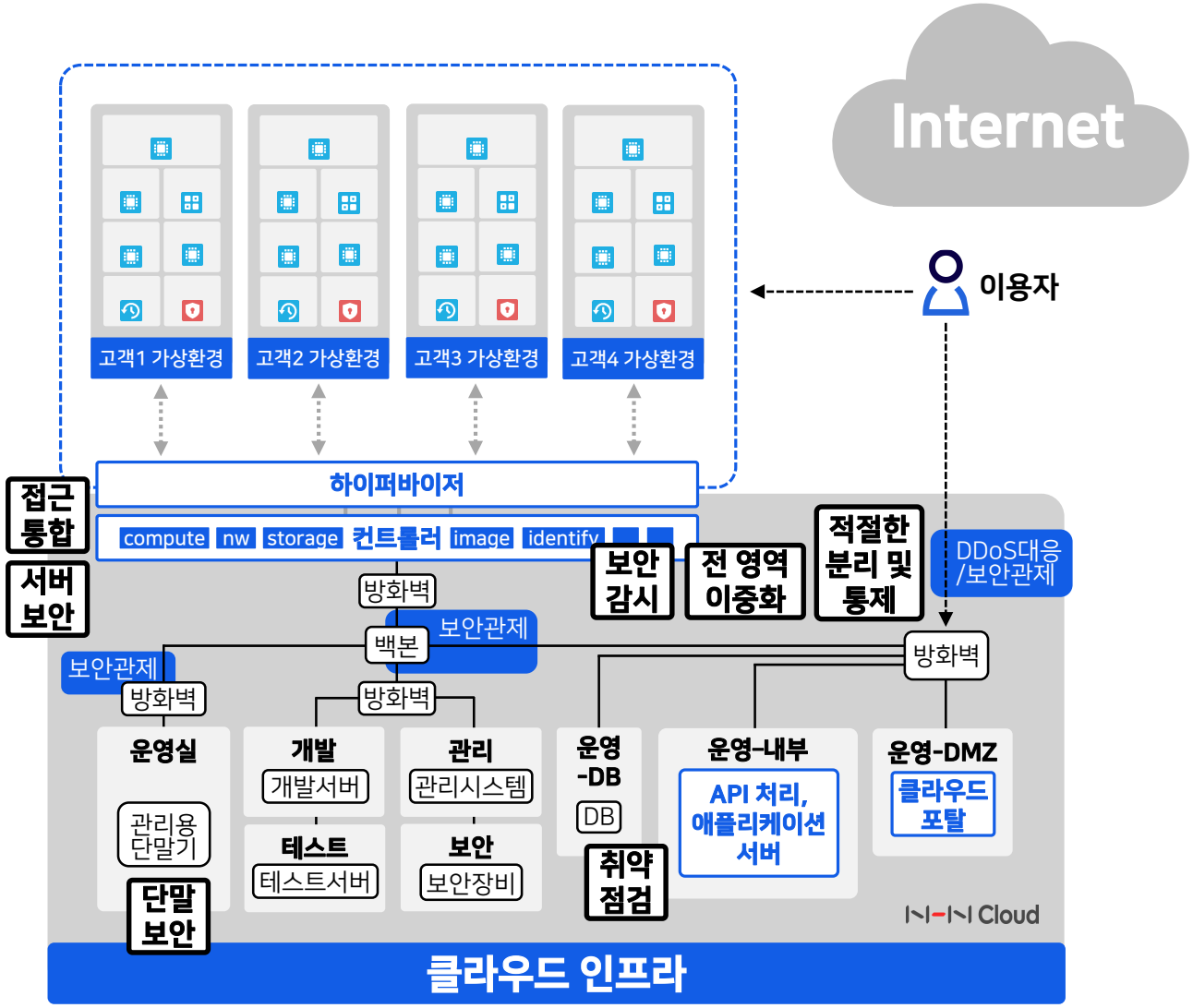
나도 알고보면 불쌍한 놈이야

CSP가 제공하는 보안

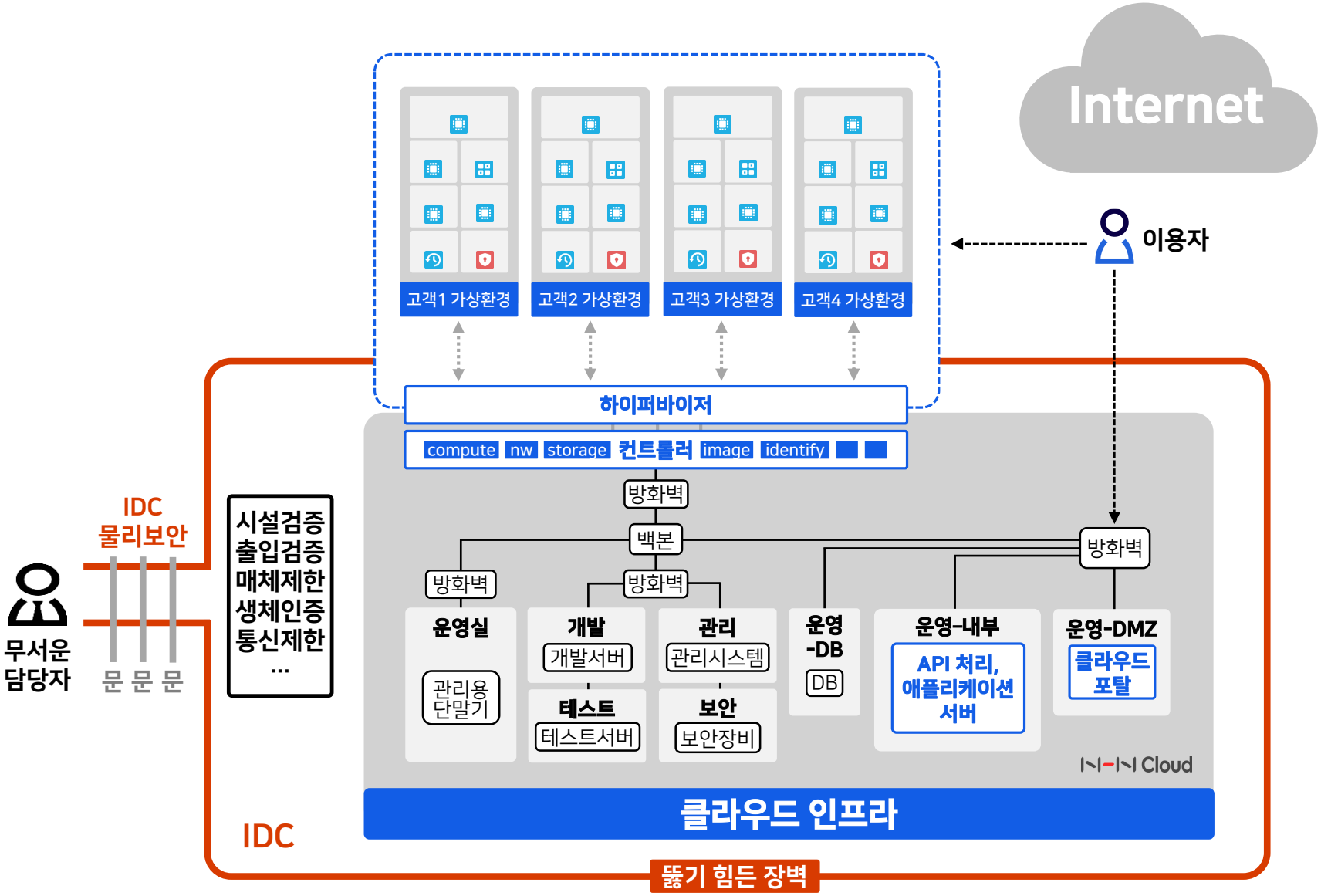
클라우드는 당신을 해치지 않는다 #1



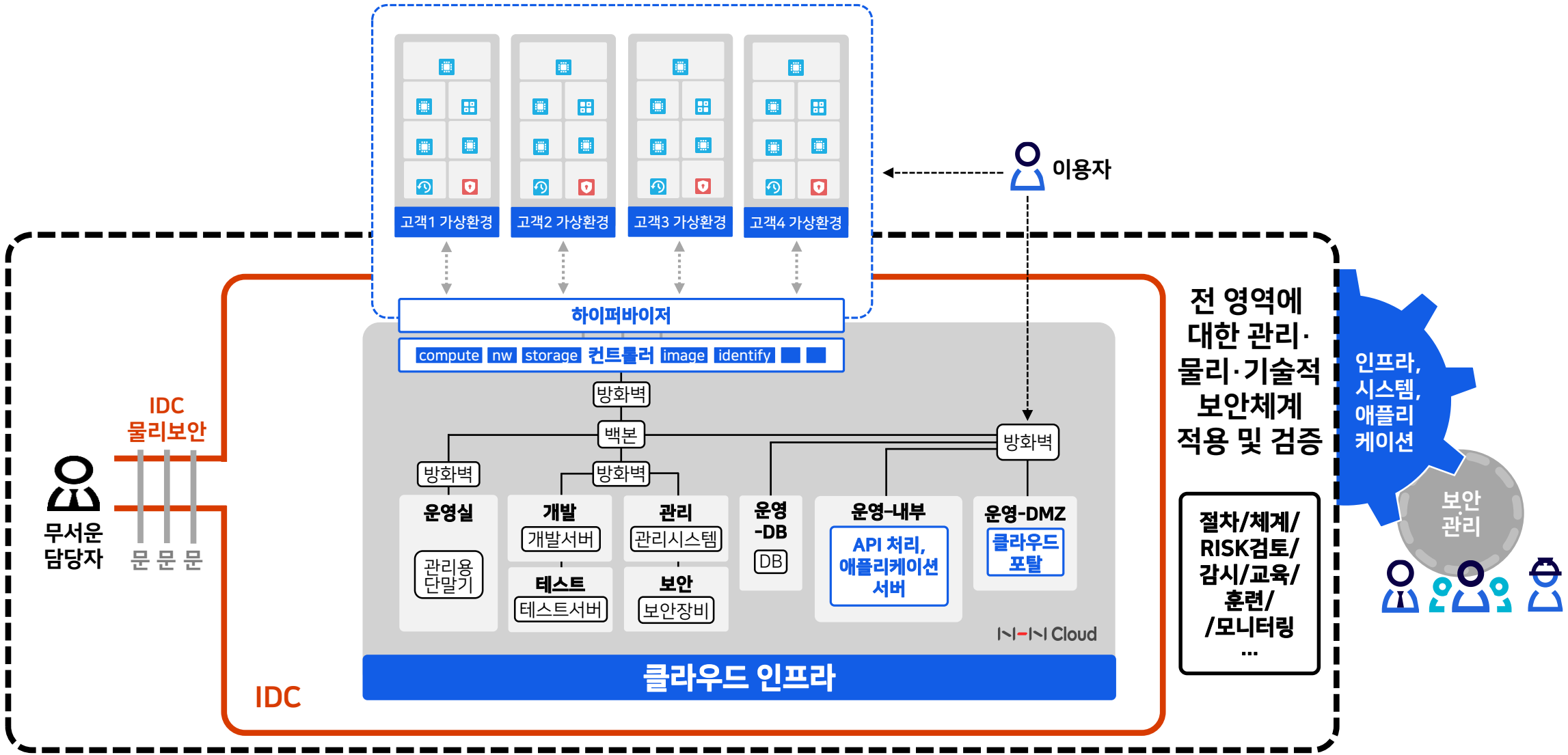
클라우드는 당신을 해치지 않는다 #1



클라우드는 당신을 해치지 않는다 #1



클라우드는 당신을 해치지 않는다 #1



클라우드는 당신을 해치지 않는다 #1

클라우드 제공 관련 주요 정보보호관리체계

ISO/IEC 27001 인증
정보보호 관리체계

ISMS-P 인증
정보보호 및 개인정보보호
관리체계

ISO/IEC 27017/27018 인증
클라우드 서비스 개인정보 관리체계

CSA STAR (GOLD)
국제 표준 인증기구인 BSI, CSA가
마련한 클라우드 정보보호 관리체계

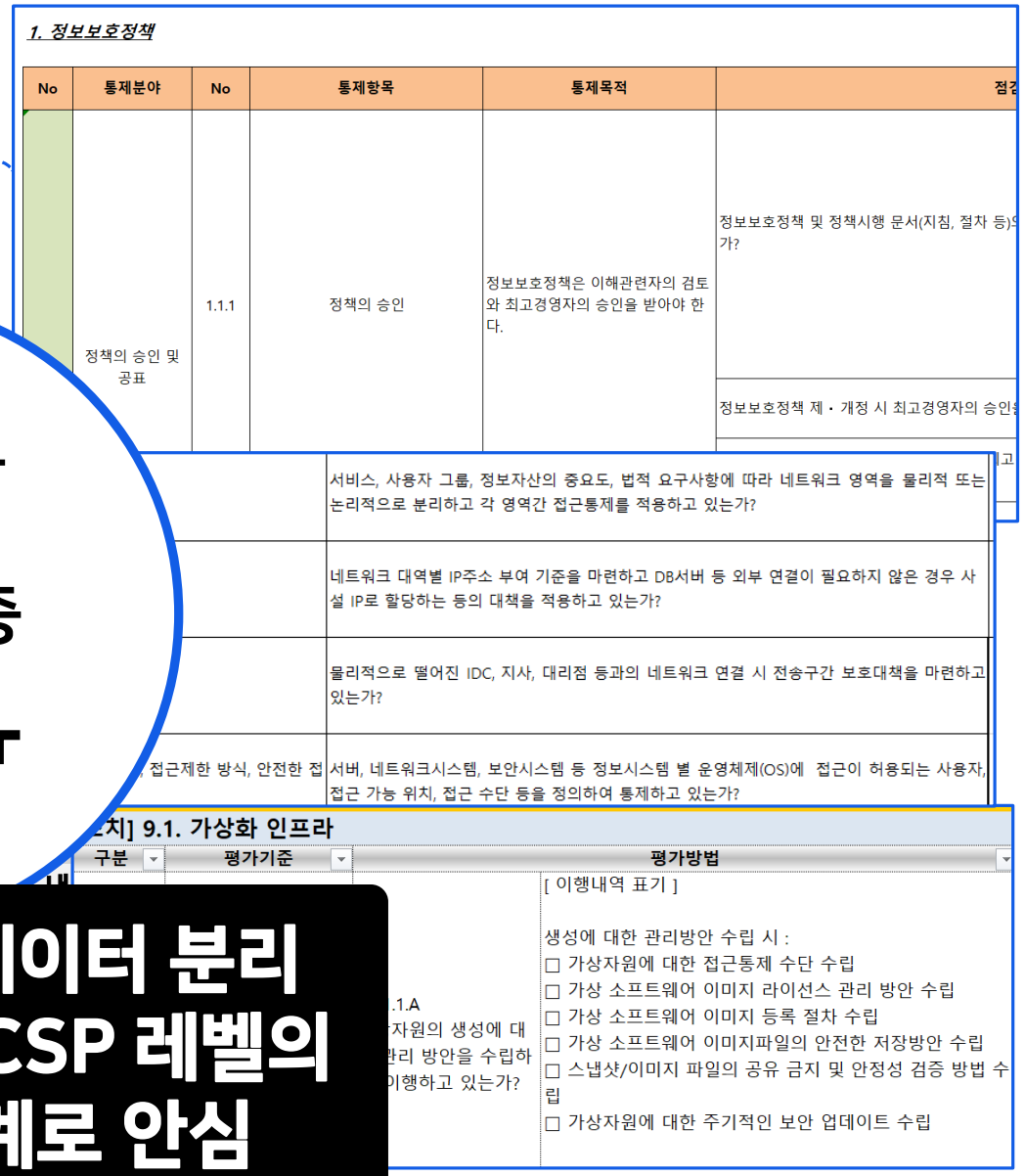
CSAP 인증 (KISA)
공공기관 제공을 위한
클라우드 정보보호 수준 평가

금융 CSP 평가 (금융보안원)
금융회사 제공을 위한
클라우드 정보보호 수준 평가

**구석구석을
철저하게
검증 받는 중**

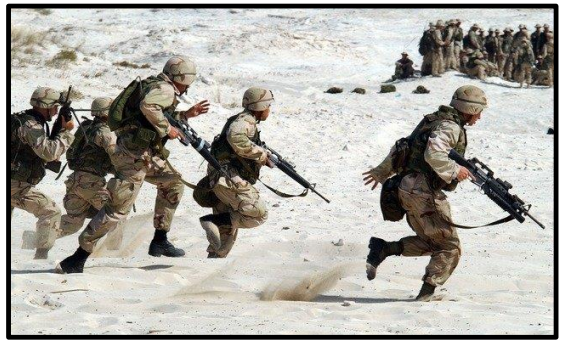
인증 담당

**가상화, API나 데이터 분리
등에 대한 우려는 CSP 레벨의
검증된 보안체계로 안심**



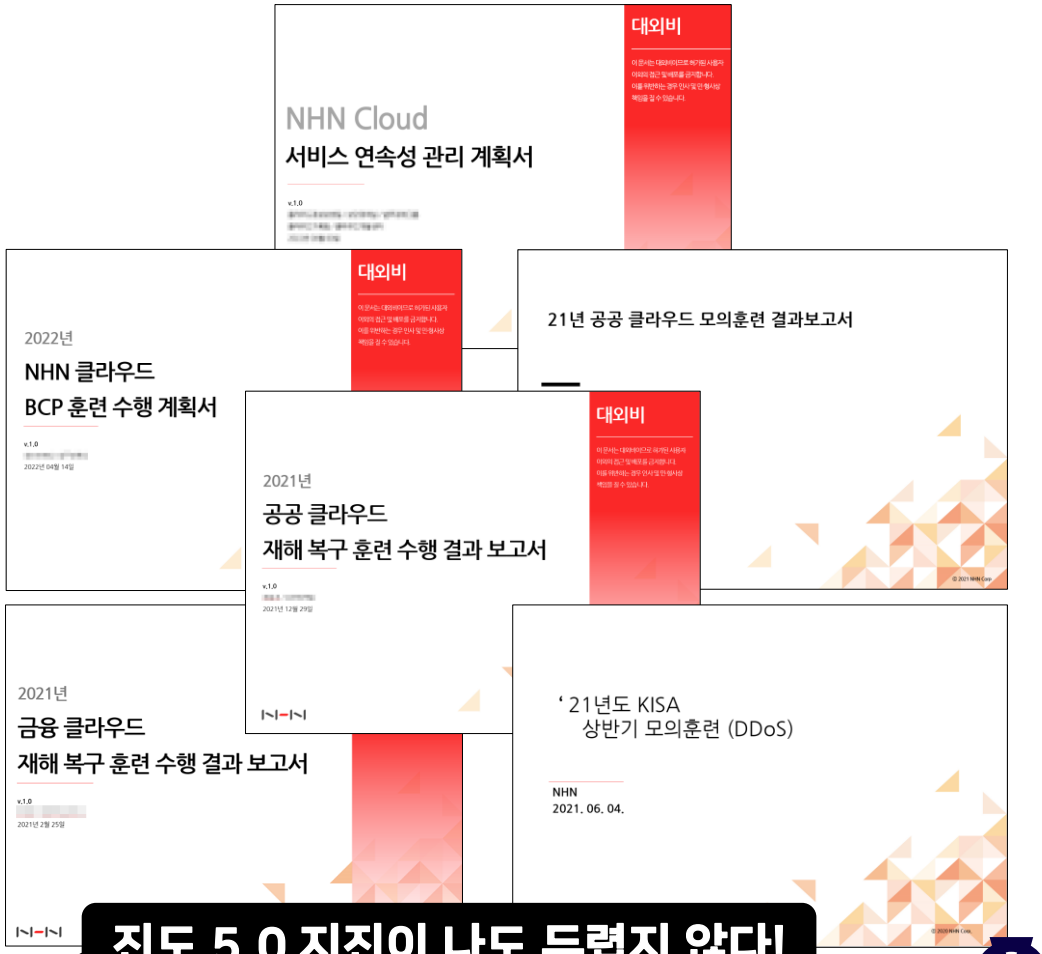
클라우드는 당신을 해치지 않는다 #1

재해복구!



APT!

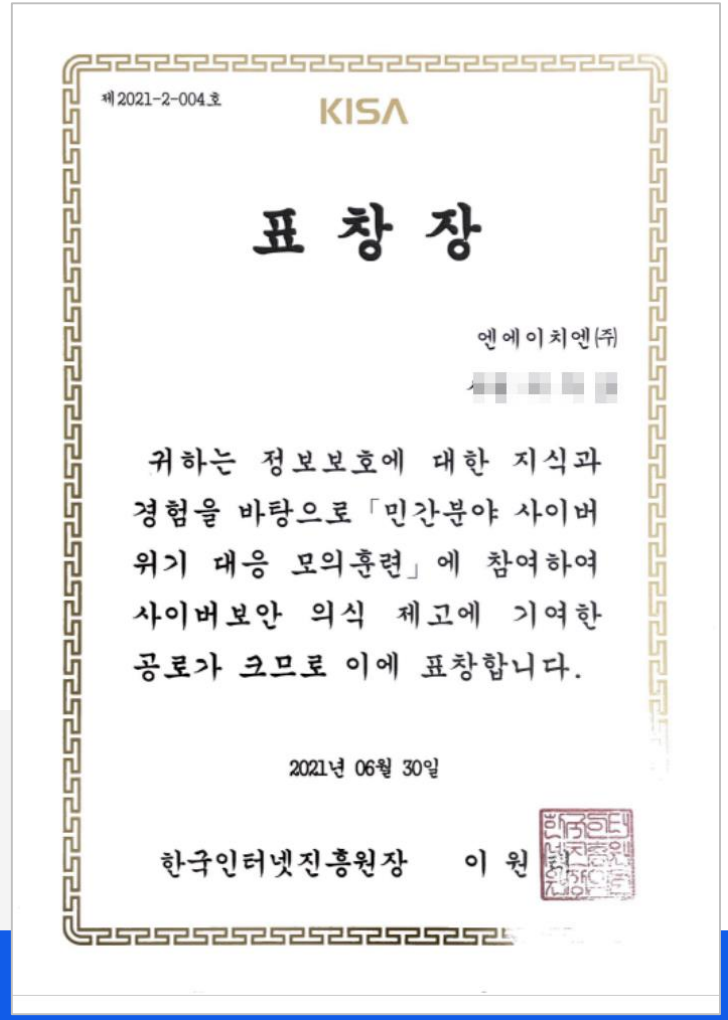
DDoS!



클라우드는 당신을 해치지 않는다 #1

침해사고대응팀

훈련 그것은 CSP의 숙명


제2021-2-004호

KISA

표 창 장

엔에이치엔(주)

귀하는 정보보호에 대한 지식과 경험을 바탕으로「민간분야 사이버 위기 대응 모의훈련」에 참여하여 사이버보안 의식 제고에 기여한 공로가 크므로 이에 표창합니다.

2021년 06월 30일

한국인터넷진흥원장 이 원

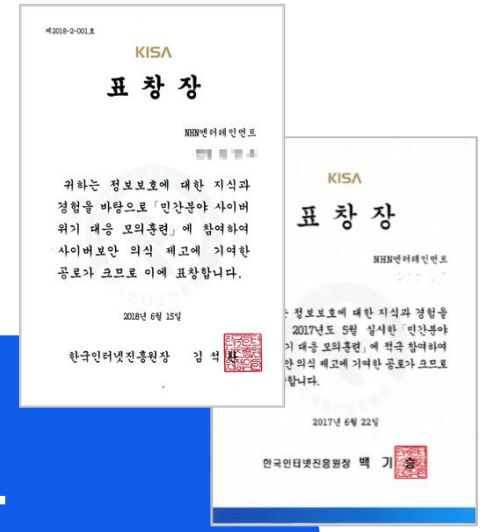

KISA

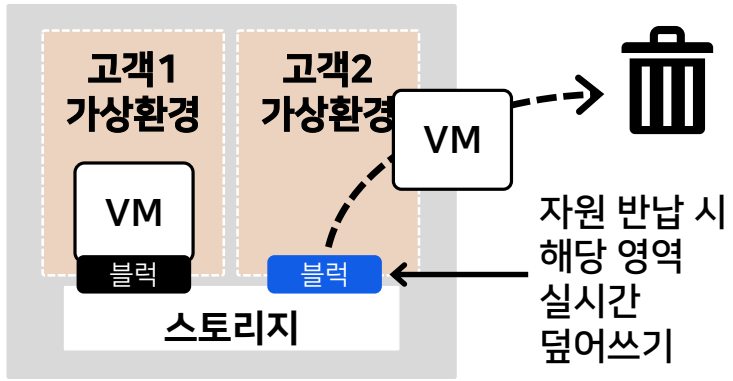
표 창 장

KISA

표 창 장

2021년 CSP 환경 침해사고 대응 모의훈련 우수 기업 선정

클라우드는 당신을 해치지 않는다 #1



CSP가 제공하는 완전삭제

KISA 曰

이용자와의 계약 종료 또는 이전 시, 이용자의 데이터를 재사용할 수 없도록 정보를 완전히 삭제하여야 한다.

- 시스템 설계 시 이용자 데이터 삭제 시 데이터 완전삭제 기능 적용
- 데이터 완전삭제
  - 표준화된 방법 적용(DoD 5220.22-M-ECE, DoD 5220.22-M, HMG IAS No.5 Higher Overwrite, Russian GOST, Canadian RCMP OPS, German VSITR, NIST 800-88 등)
  - 새로운(무의미한) 데이터를 여러 차례 덮어쓰기 적용

CSP 사용자 도우미 예시

Storage > Block Storage > 데이터 완전 삭제 가이드

인스턴스에 연결된 블록 스토리지 및 NAS의 데이터를 완전히 삭제하는 방법을 소개합니다.
KISA 데이터 완전 삭제 기준인 DoD 5220.22-M 패턴을 적용할 수 있는 scrub(Linux), Disk Wipe(Windows)를 이용해 데이터를 완전히 삭제할 수 있습니다.

Linux 인스턴스

1. scrub 패키지를 설치합니다.
   - Debian, Ubuntu 인스턴스

```
$ sudo apt-get install scrub
```

   - CentOS 인스턴스

고객이 수행할 수 있는 완전삭제

클라우드는 당신을 해치지 않는다 #2

클라우드 책임 모델 예시

고객 / NHN Cloud

보호 대상	보안 주체				
	레거시	IaaS	PaaS (관리형)	PaaS (서버리스)	SaaS
데이터	고객	고객	고객	고객	고객
애플리케이션	고객	고객	고객	고객	NHN Cloud
미들웨어	고객	고객	고객	NHN Cloud	NHN Cloud
운영체제	고객	고객	고객	NHN Cloud	NHN Cloud
가상 머신	고객	고객	고객	NHN Cloud	NHN Cloud
가상 네트워크	고객	고객	고객	NHN Cloud	NHN Cloud
클라우드 운영 S/W	고객	NHN Cloud	NHN Cloud	NHN Cloud	NHN Cloud
물리 인프라 (시스템, 네트워크, 스토리지…)	고객	NHN Cloud	NHN Cloud	NHN Cloud	NHN Cloud
물리 시설	고객	NHN Cloud	NHN Cloud	NHN Cloud	NHN Cloud

※ 서비스 세부 유형에 따라 변경될 수 있습니다.

기술적 가용성 + 정보보호관리체계로
장애는 최소화되고
약관과 SLA를 통해 보상 제공

이용약관, SLA 예시

제34조. 회사의 손해배상

1. “회사”는 “회사”의 책임 있는 사유로 “서비스”에 장애가 발생하여 “회원”이 손해를 입은 경우 “서비스”별 특성에 따라 “서비스”별로 정해진 서비스 수준 약정(이하 “SLA”)에서 정한 바에 따라 “회원”의 청구에 의해서 배상을 진행합니다.
2. 전항에도 불구하고, “SLA”가 정해져 있지는 않은 “서비스”의 경우에는 아래의 내용을 기준으로 하여 손해배상금액을 결정합니다.

월 가용성	손해배상금
99.0% 이상 ~ 99.9% 미만	3개월 월 평균 사용금액의 10%에 해당하는 금액
95.0% 이상 ~ 99.0% 미만	3개월 월 평균 사용금액의 25%에 해당하는 금액
95.0% 미만	3개월 월 평균 사용금액의 50%에 해당하는 금액

• 본 Kubernetes 서비스 수준 약정(“본 SLA”)은 Kubernetes(이하 “본 서비스”)를 사용하는 각 계정에 개별적으로 적용됩니다.

정의

• 장애: 1분 동안 본 서비스에 대한 모든 연결 요청이 실패함을 말합니다.
• 장애시간: 해당월 동안 장애가 발생한 시간의 총합을 말하며, 본 서비스를 이용하지 못한 사실을 회원이 회사에 통지한 때 (회원의 통지 전에 회사가 그 사실을 알 경우는 회사가 그 사실을 알게 된 때) 부터 측정됩니다. 단, 본 SLA의 적용이 배제되는 경우 그 해당 시간은 장애시간에 포함되지 않습니다.
• 월 가용성: 100 * [1-{본 서비스를 이용한 한달 동안 “회사”의 책임 있는 사유로 인한 장애로 본 서비스를 이용하지 못하는 장애시간(분)의 합/본 서비스를 이용할 수 있는 기간 한달(분)}] (“분”은 시간단위인 분(分)을 의미함)

서비스 책임

• 회사는 회사의 책임 있는 사유로 장애가 발생하여 아래와 같은 월 가용성 구간 미만을 제공하였고, 그로 인해 회원이 손해를 입은 경우 회원의 청구에 의해 손해를 배상합니다.

월 가용성	손해배상금
99% 이상 ~ 99.9% 미만	3개월 월 평균 사용 금액의 10%에 해당하는 금액
95% 이상 ~ 99% 미만	3개월 월 평균 사용 금액의 25%에 해당하는 금액
95.0% 미만	3개월 월 평균 사용 금액의 50%에 해당하는 금액

클라우드는 당신을 해치지 않는다 #3

국가 정보보안 기본지침 준수를 위한,
클라우드컴퓨팅 보안 가이드라인 준수를 위한,
네트워크 구축 가이드라인 준수를 위한,
업무전산망 분리 및 자료전송 가이드라인 준수를 위한,
행정기관 및 공공기관 정보시스템 구축·운영 지침 준수를 위한,
국정원 보안성 검토 기준 준수를 위한,
개인정보영향평가 기준 준수를 위한,

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률,
국가정보화기본법, 국가정보원법, 전자정부법,
정보통신기반보호법, 국가사이버안전관리규정 등등…

전자금융감독규정, 신용정보업감독규정 준수를 위한,
금융분야 클라우드컴퓨팅서비스 이용가이드 준수를 위한,
금융ISMS 기준 준수를 위한,
금융감독원 심사 기준 준수를 위한,
내부 보안성 심의 기준 준수를 위한,

전자금융감독규정, 신용정보업감독규정,
금융기관의 업무위탁 등에 관한 규정 등등…

ISMS, ISMS-P, ISO27001 기준 준수를 위한,
개인정보 안전성 확보조치 기준 준수를 위한,
정보통신기반시설 보호지침 준수를 위한,
의료정보보호 관리체계 (ISO27799) 기준 준수를 위한,
가상자산거래 관련 ISMS 기준 준수를 위한,

정보통신망법, 개인정보보호법, 정보통신기반보호법 등등…

까다롭고 다양한 고객 기준의 보안 요건

클라우드 포탈

Cloud

클라우드 인프라

클라우드는 당신을 해치지 않는다 #3

고객 기준 보안요건과 신규 서비스 보안 적용을 위한 다양한 상품 및 맞춤 지원 제공

국가 정보보안 기본지침 준수를 위한,
클라우드컴퓨팅 보안 가이드라인 준수를 위한,
네트워크 구축 가이드라인 준수를 위한,
업무전산망 분리 및 자료전송 가이드라인 준수를 위한,
행정기관 및 공공기관 정보시스템 구축·운영 지침 준수를 위한,
국정원 보안성 검토 기준 준수를 위한,
개인정보영향평가 기준 준수를 위한,

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률,
국가정보화기본법, 국가정보원법, 전자정부법,
정보통신기반보호법, 국가사이버안전관리규정 등등…

전자금융감독규정, 신용정보업감독규정 준수를 위한,
금융분야 클라우드컴퓨팅서비스 이용가이드 준수를 위한,
금융ISMS 기준 준수를 위한,
금융감독원 심사 기준 준수를 위한,
내부 보안성 심의 기준 준수를 위한,

전자금융감독규정, 신용정보업감독규정,
금융기관의 업무위탁 등에 관한 규정 등등…

ISMS, ISMS-P, ISO27001 기준 준수를 위한,
개인정보 안전성 확보조치 기준 준수를 위한,
정보통신기반시설 보호지침 준수를 위한,
의료정보보호 관리체계 (ISO27799) 기준 준수를 위한,
가상자산거래 관련 ISMS 기준 준수를 위한,

정보통신망법, 개인정보보호법, 정보통신기반보호법 등등…

보안 서비스와 상품 제공

- DDoS Guard
- Security Monitoring
- Basic Security
- Web Firewall
- Vaccine
- Security Compliance
- Secure Key Manager
- Server Security Check
- App Security Check
- NHN AppGuard
- CSAP SaaS Guidance
- SIEM
- 그 외 다양한 서비스 및 마켓플레이스 보안 상품들

DMZ
내부
DB
개발
테스트
관리
보안
K8S
OBS
RDS

고객 가상환경

Internet

이용자

보안 설계/기술 /요건 상담

전담 보안 아키텍트

포탈 보안 기능

클라우드 포탈

NHN Cloud

클라우드 인프라

클라우드 지원 조직

이제 남은 것은

제공자 영역 보안 관리

체계적 보안기능 제공

장애 책임 준수

OK

CSP
구성원
일동

물리/논리 환경

인프라

보안
관리

CSP

기술과 경험 지원

OK

엔지니어

보안
아키텍트

CSP + MSP

**고객 영역
클라우드 보안 적용**

GoGoGoGo!

곱게 키운
우리 시스템
잘 도와주게

논리 환경

인프라

보안
관리

고객

주로 챙겨야 할 것들

중점 보안요소들

1 계정 관리

2 접근통제

3 네트워크 분리 ,단말 연계

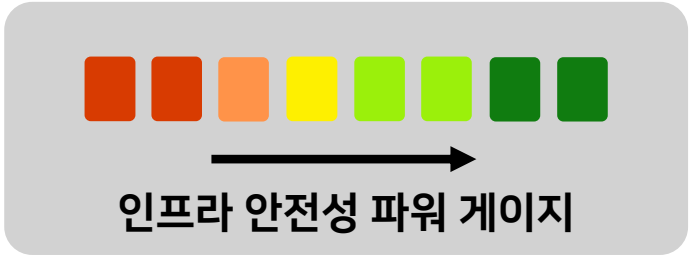
4 암호화, 개인정보 보호

5 로깅, 감사

6 보안 모니터링, 취약점 점검

7 가상서버영역 보안 강화

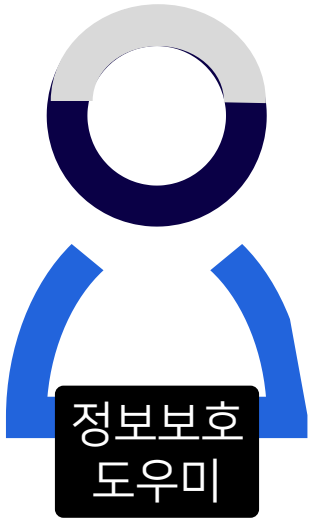
8 관리/운영 보안 적용



#1 계정 관리

계정? 중요한가요?

통제/분석/대응의 기본 단위



계정관리 주요 적용방안

부모님 /친구 | 책임자 /관리자 | 감사자 /점검자 | 운영자 | 개발자 | 협력 업체

접속 불가

클라우드포탈 관리 접속 (HTTPS/API)

가상요소 별 관리 접속 (SSH/RDP/HTTPS/ SQL/SFTP/API 외)

1인 1계정

잘 알려진 계정 = X

최소권한

클라우드 포탈

NHN Cloud 회원 계정

- 조직 관리자: RW (ORG+ PROJECT)
- 프로젝트 관리자: RW (PROJECT)
- 프로젝트 운영자: RW (PROJECT)
- 감사/점검: RO

IAM 계정 (PROJECT-Limited)

- 운영자: RW
- 개발자: RW (개발/ 테스트 only)
- 모니터링: RO
- 감사/점검: RO

Oauth2 SAML2.0

API

가상환경 주요 요소 별 계정체계 예시

	개발자	운영자	모니터링	감사/점검
애플리케이션	RW (개발/ 테스트 only)	RW	RO	RO
컨테이너	RW (개발/ 테스트 only)	RW	RO	RO
DB	RW (개발/ 테스트 only)	RW	RO	RO
가상머신		RW	RO	RO
보안시스템		RW	RO	RO

조직: 암호규칙, 감사기록, 세션관리

프로젝트: PEM키, MFA

암호규칙 | MFA | 감사기록 | 세션관리

'포탈' 계정 세분화 및 권한 적용

필요 시 계정 연동

API

SSO / AD/LDAP — 고객 영역 인증시스템

필요 시 통합 관리

'가상자원' 계정 세분화 및 권한 적용

특히 2차 인증

우리를 아껴 주시는 고객 하나 하나의 포탈이
광야의 해로운 무리들에게 털림으로써
몰래 생성된 인스턴스와 공인IP 연결을 통해
악한 이들의 주린 배를 불리는 잠행 채굴이
일어나지 않기를 오늘도 간곡히 기도 드리나이다

- CSP 일일 기도문

제발.. ㅠㅠ

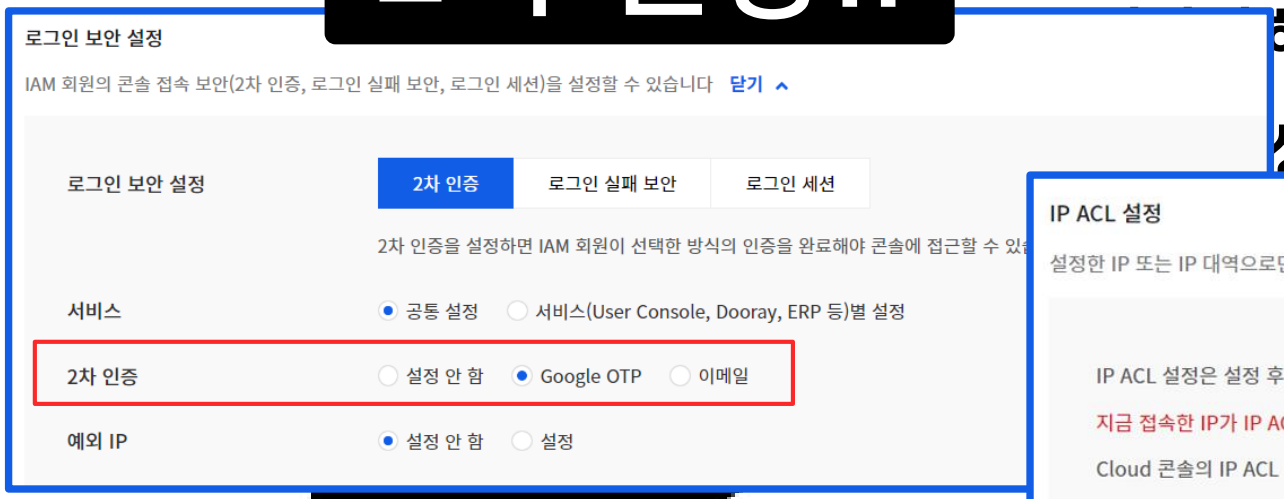
CEO 및 센터장 일동

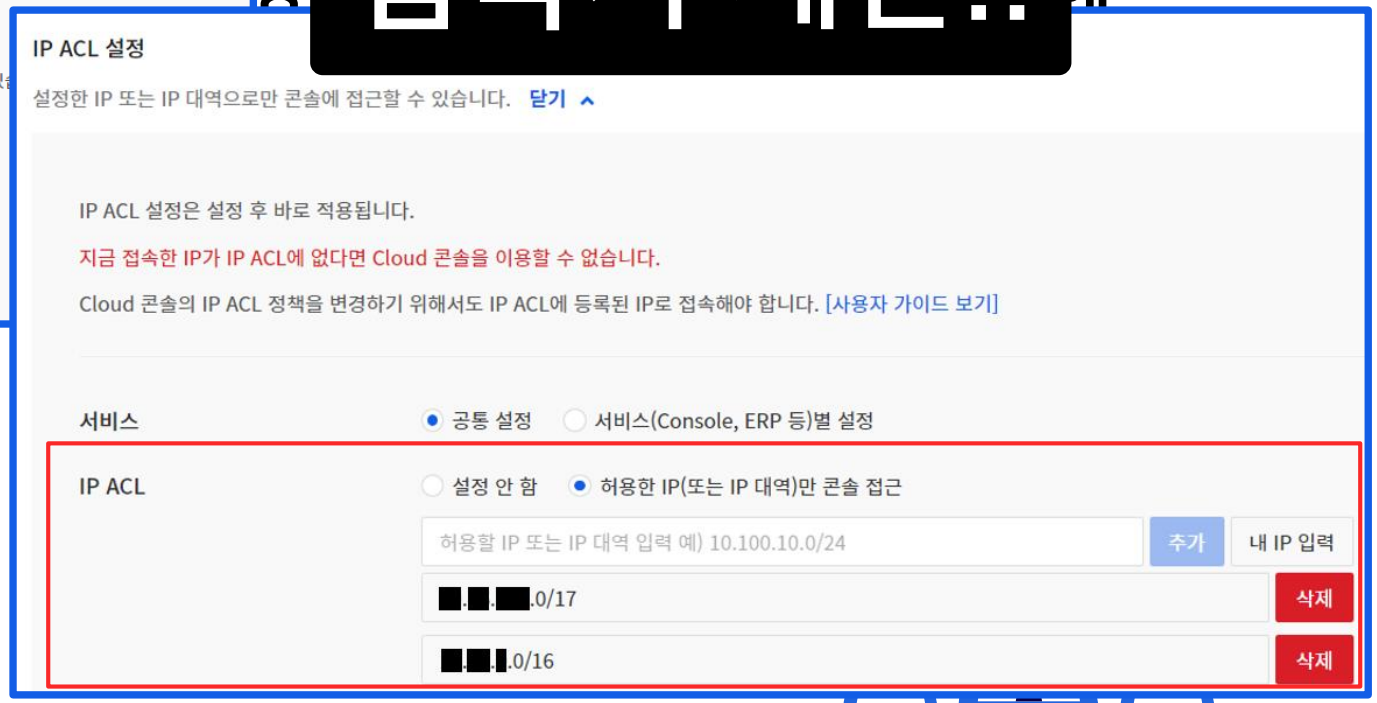
특히 2차 인증

2차 인증!!

우리를 아껴 주시는 고객 하나 하나의 포탈이

접속지 제한!!

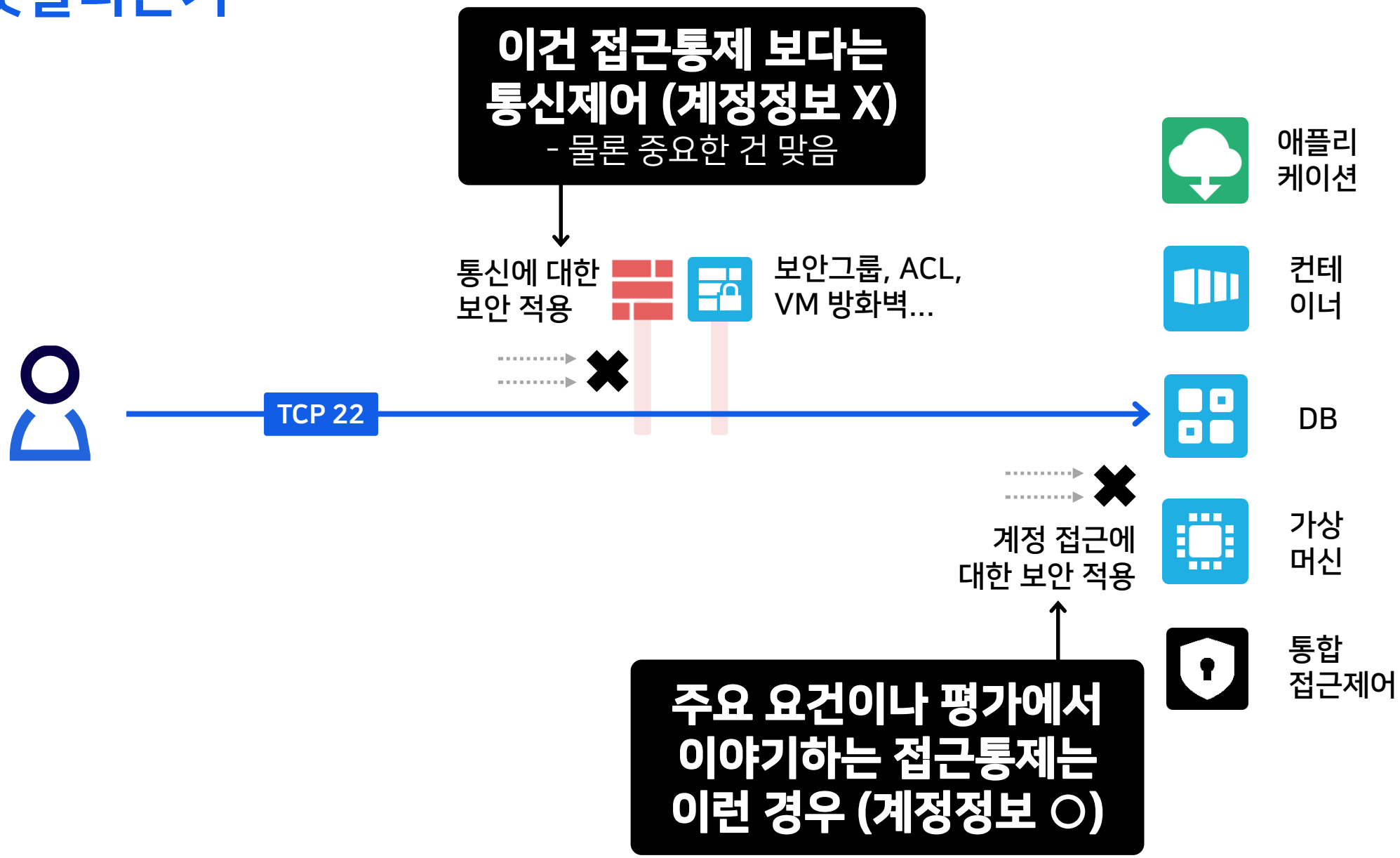




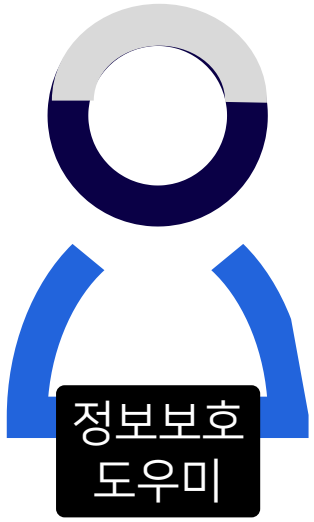
CEO 및 센터장 일동

#2 접근통제

좀 헷갈리는거


이건 접근통제 보다는
통신제어 (계정정보 X)
- 물론 중요한 건 맞음
통신에 대한
보안 적용
보안그룹, ACL,
VM 방화벽...
TCP 22
애플리
케이션
컨테
이너
DB
가상
머신
통합
접근제어
계정 접근에
대한 보안 적용
주요 요건이나 평가에서
이야기하는 접근통제는
이런 경우 (계정정보 O)

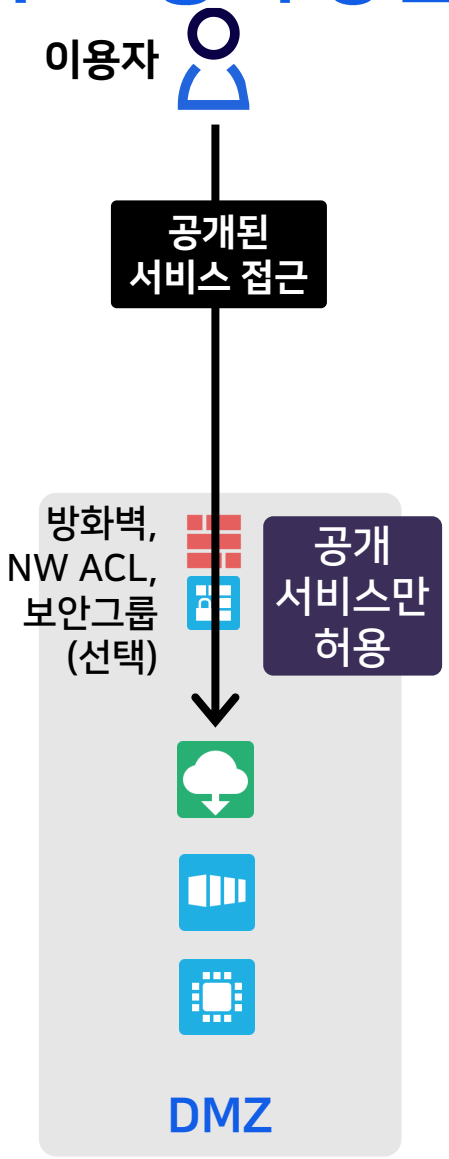
이것만 알면 무섭지 않다



1. 접근자
2. 접근지
3. 접근경로
4. 목적지
5. 수행업무 식별 후

→ 최소한의 통신과
최소한의 권한 적용

주요 통제 방안

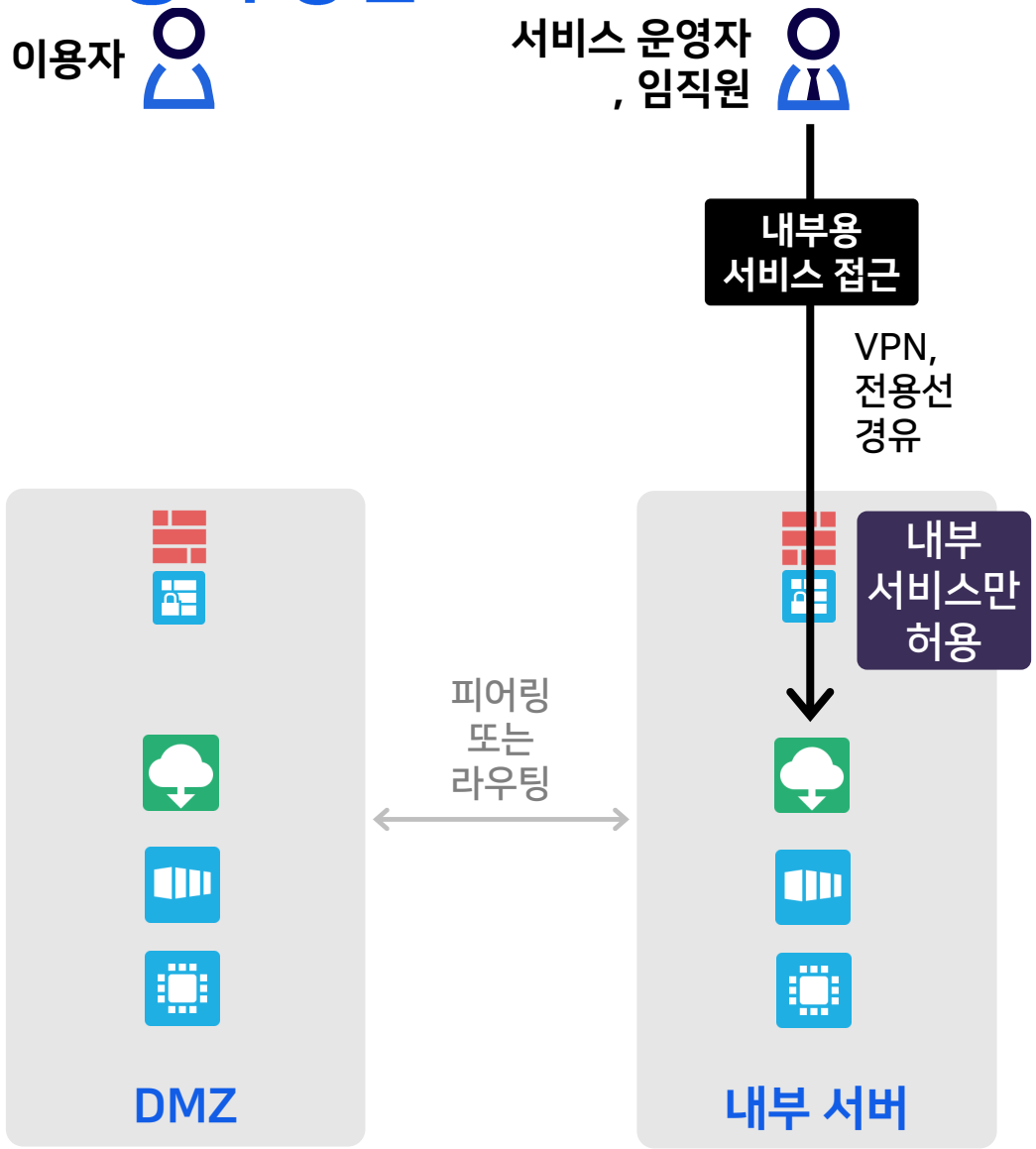


모든 접근자와 세부 경로 식별

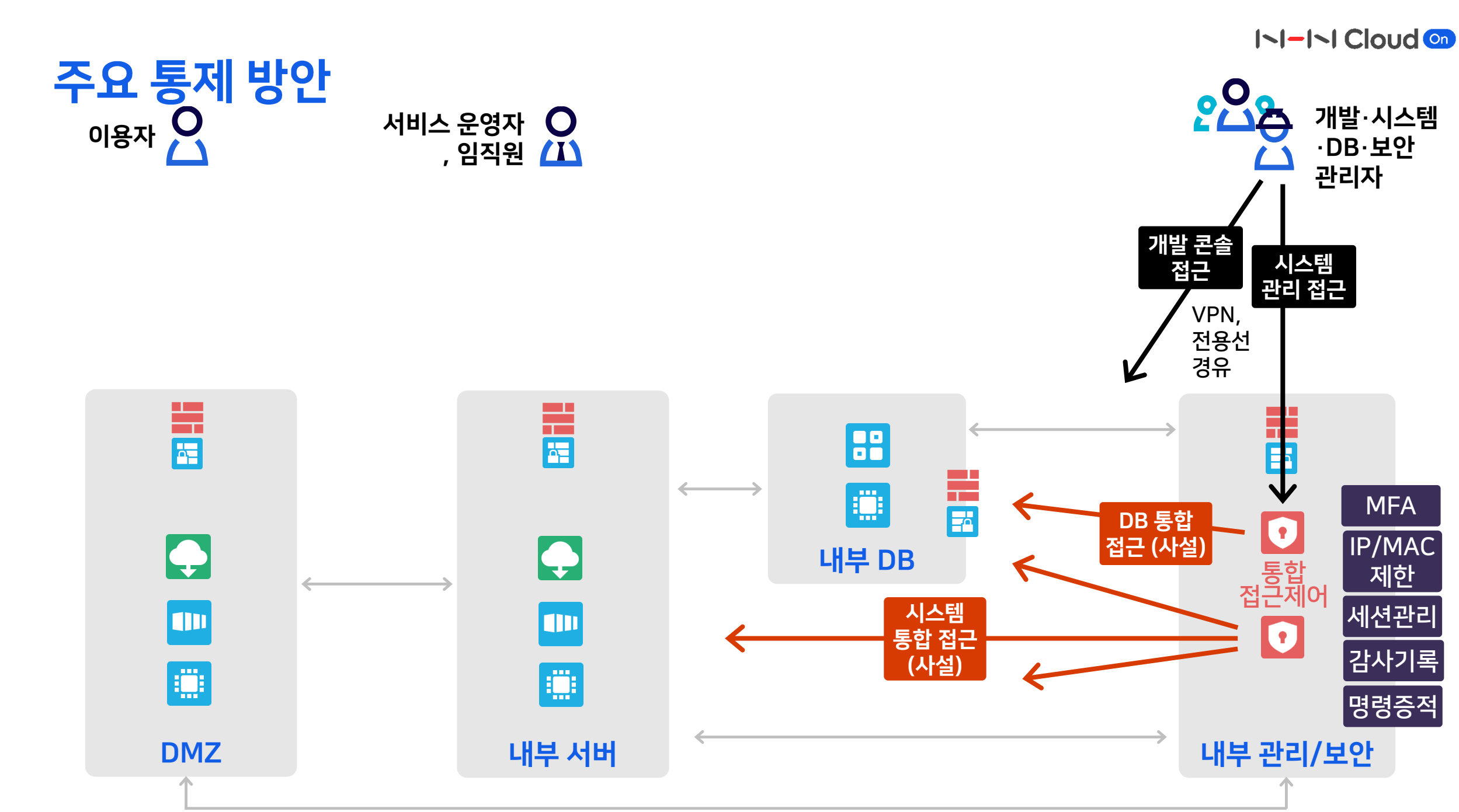
1. 접근자
2. 접근지
3. 접근경로
4. 목적지
5. 수행업무 식별 후

→ 최소한의 통신과
최소한의 권한 적용

주요 통제 방안


이용자
서비스 운영자
, 임직원
내부용
서비스 접근
VPN,
전용선
경유
내부
서비스만
허용
피어링
또는
라우팅
DMZ
내부 서버

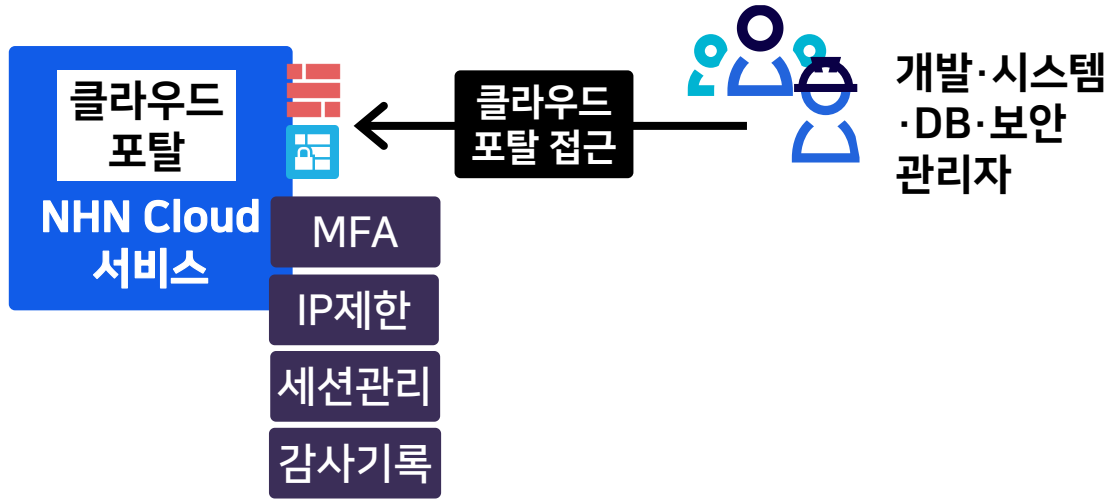
주요 통제 방안

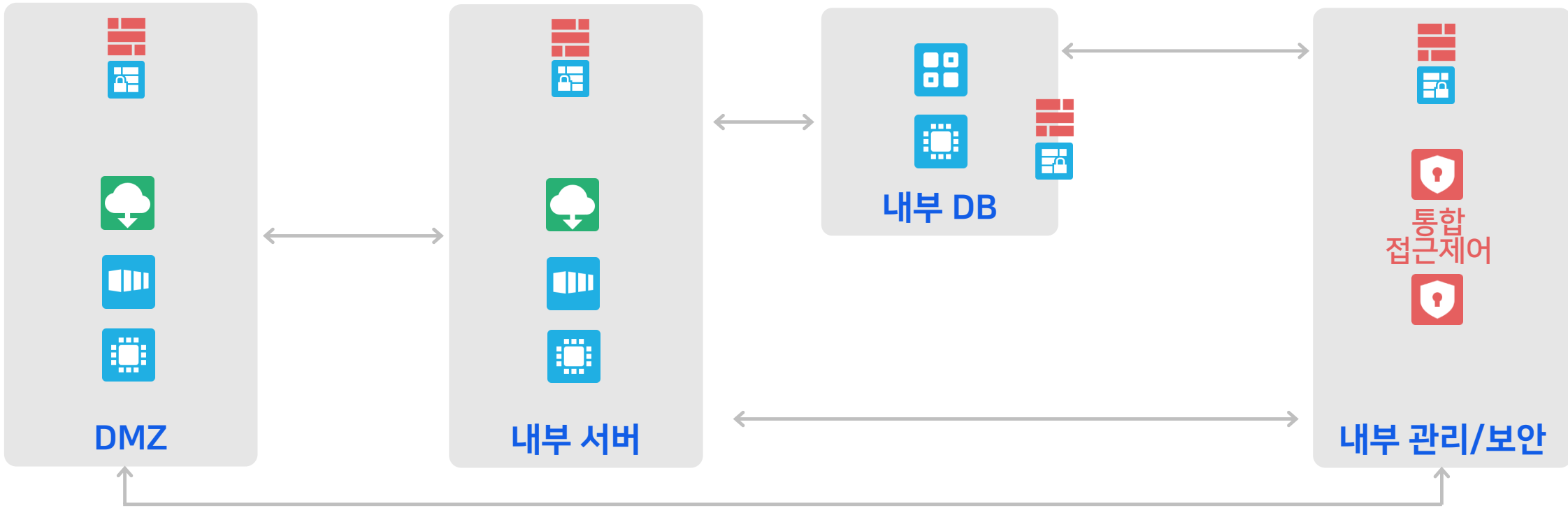

이용자
서비스 운영자
, 임직원
개발·시스템
·DB·보안
관리자
개발 콘솔
접근
시스템
관리 접근
VPN,
전용선
경유
DMZ
내부 서버
내부 DB
내부 관리/보안
DB 통합
접근 (사설)
시스템
통합 접근
(사설)
통합
접근제어
MFA
IP/MAC
제한
세션관리
감사기록
명령증적

주요 통제 방안

이용자

서비스 운영자
, 임직원



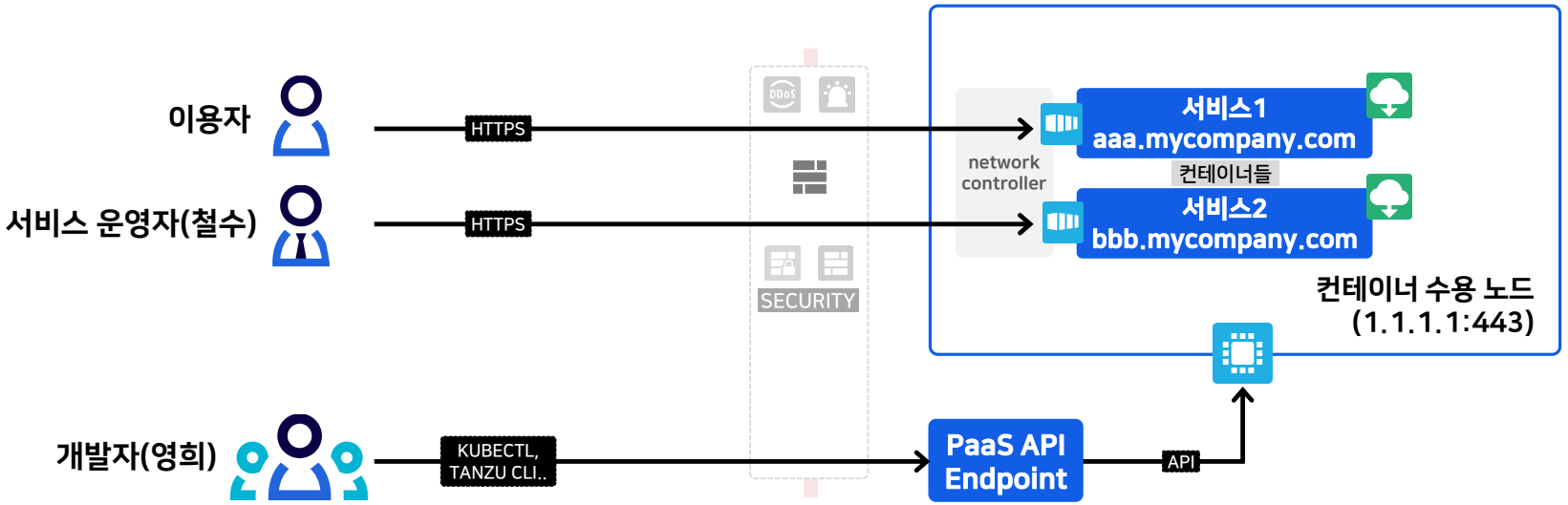


이런 접근통제도 고민 필요 (컨테이너 접근 관련)

이용자는 aaa로 웹 접속 허용한다
bbb에는 철수만 들어가게 해야 겠다
보안사고 분석을 위해 aaa만 잠깐 막아놔야 겠다
원격 CLI 명령은 아무데서나 하면 안되겠다
원격 CLI 작업한 거 추적할 수 있어야 겠다

보안담당자

알려진 보안가이드 내용 외에
관리 운영 상 노하우도 필요



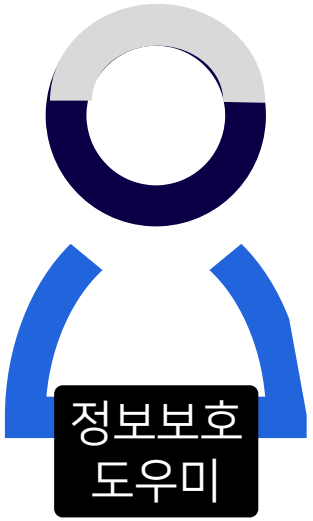
#3 네트워크 보안 구성 및 단말 연계

퀴즈탐험 분리의 세계

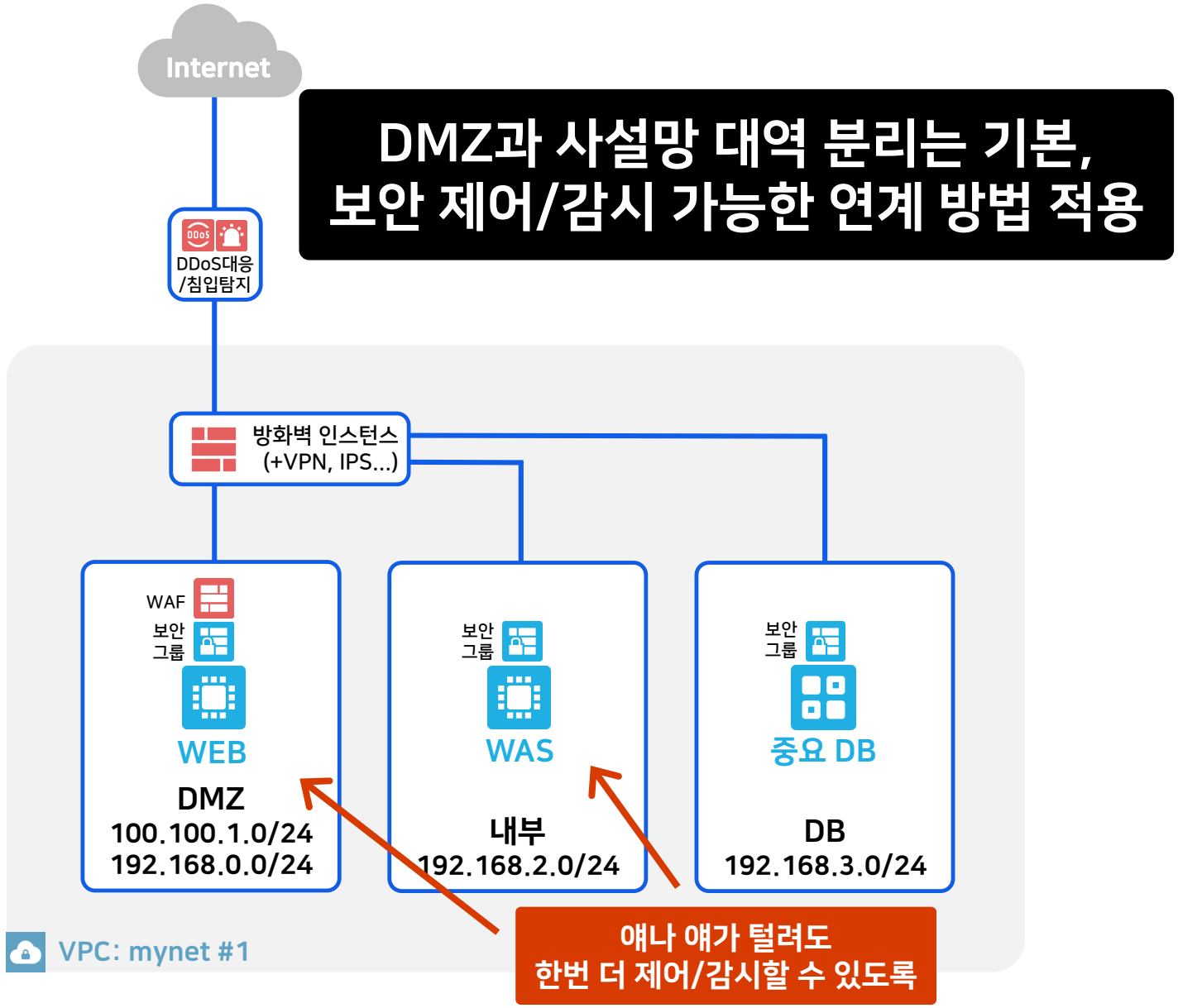
1. 대역 분리 = 서브넷 이상으로 나눈다

2. 영역/환경 분리 = 서브넷 이상으로 나누고
   서로 간 통신을 제한하되 그 안의 시스템과
   관리계정 체계를 나눈다

3. 망분리 = 서로 통신이 도달하지 않도록
   회선, 백본장비, 시스템과 관리계정 체계를 나눈다



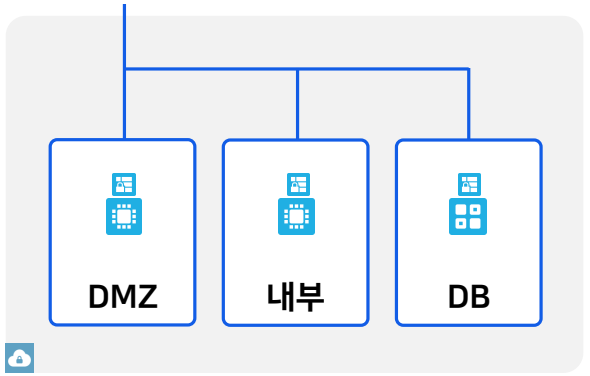
경계 네트워크 구성



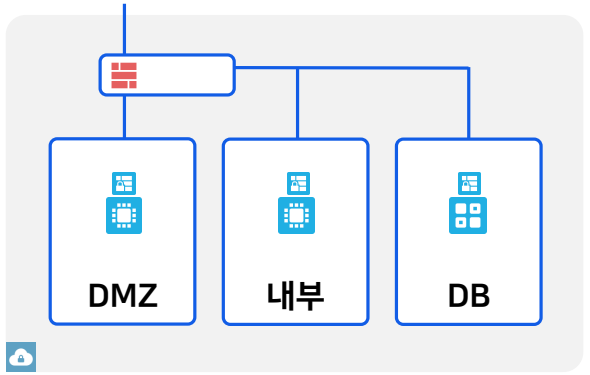
DMZ과 사설망 대역 분리는 기본,
보안 제어/감시 가능한 연계 방법 적용

(적절히
보안감시
된다면)

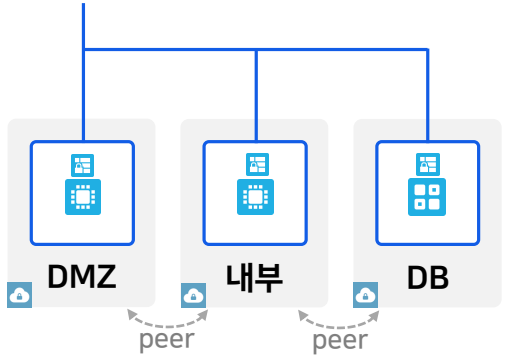
이것도
되고



이것도
되고

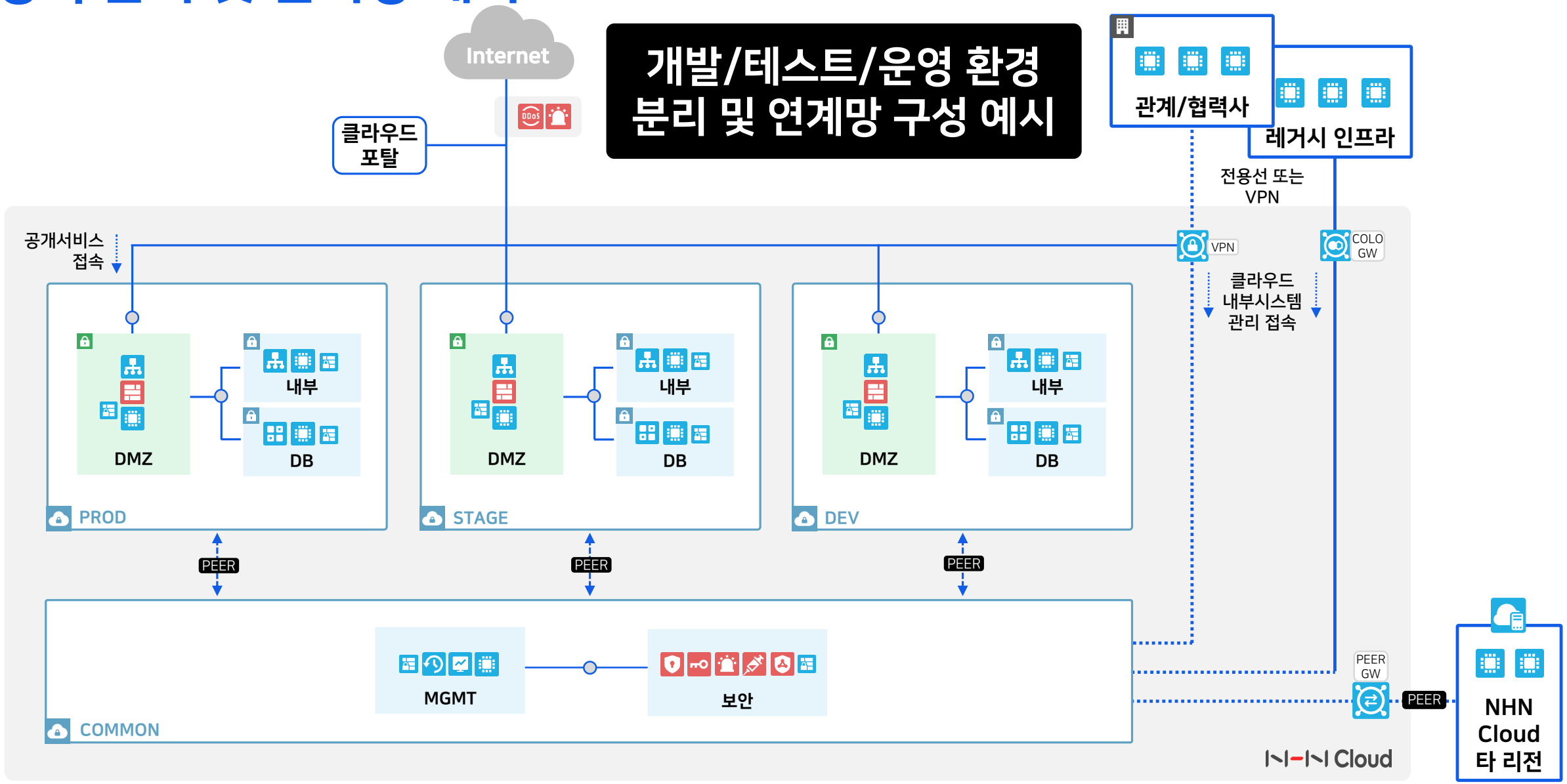


이것도
가능



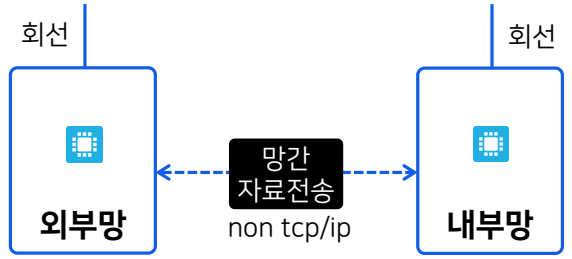
민간 기준

영역 분리 및 관리망 배치

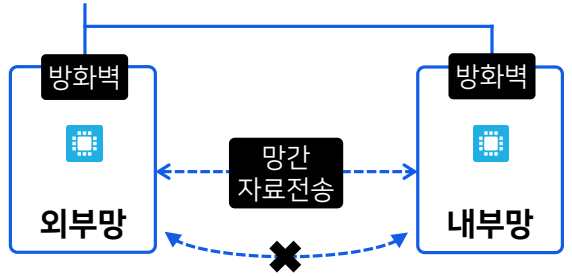

Internet
클라우드 포탈
개발/테스트/운영 환경
분리 및 연계망 구성 예시
관계/협력사
레거시 인프라
전용선 또는 VPN
공개서비스 접속
VPN
COLO GW
클라우드 내부시스템 관리 접속
DMZ
내부
DB
PROD
STAGE
DEV
PEER
MGMT
보안
COMMON
PEER GW
NHN Cloud 타 리전

망분리 적용

원칙 상 회선을 포함한 백본의 분리를 의미했으나



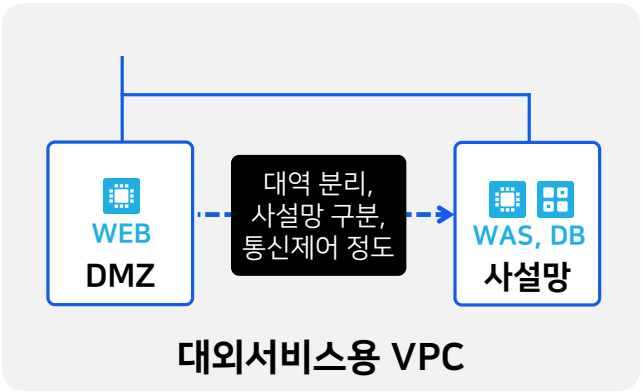
현실 상 통신이 도달되지 않으면서 적절한 보안장치를 각각 두면 인정



통신 불가 X
설정 바꿔도 도달 불가 ○

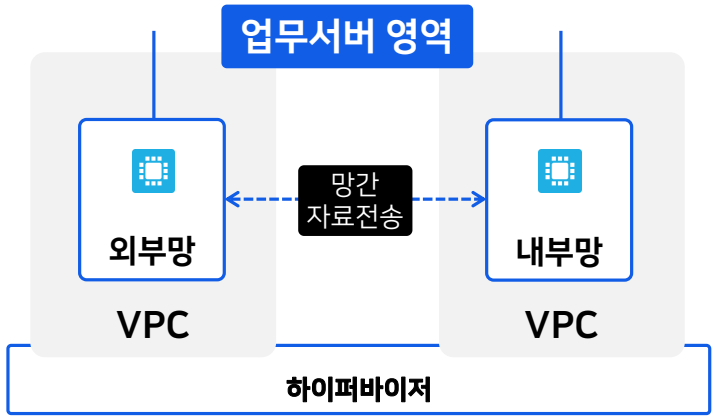
망분리 적용

대외서비스 내 시스템 간에는 '망분리'까지는 필요 없음



공공은
서비스에
따라 달라요

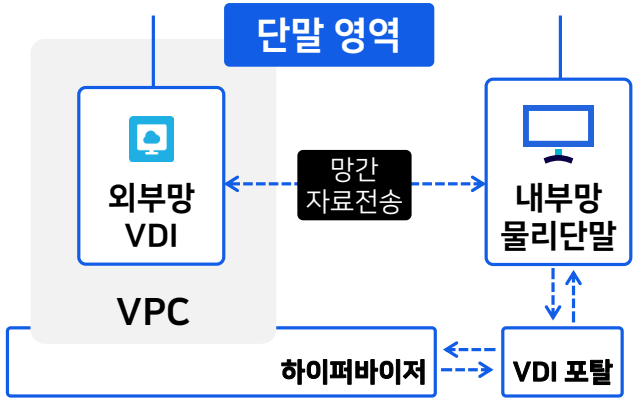
분야 별로 논리적 망분리는 인정 but 별도 연계 장치 필요



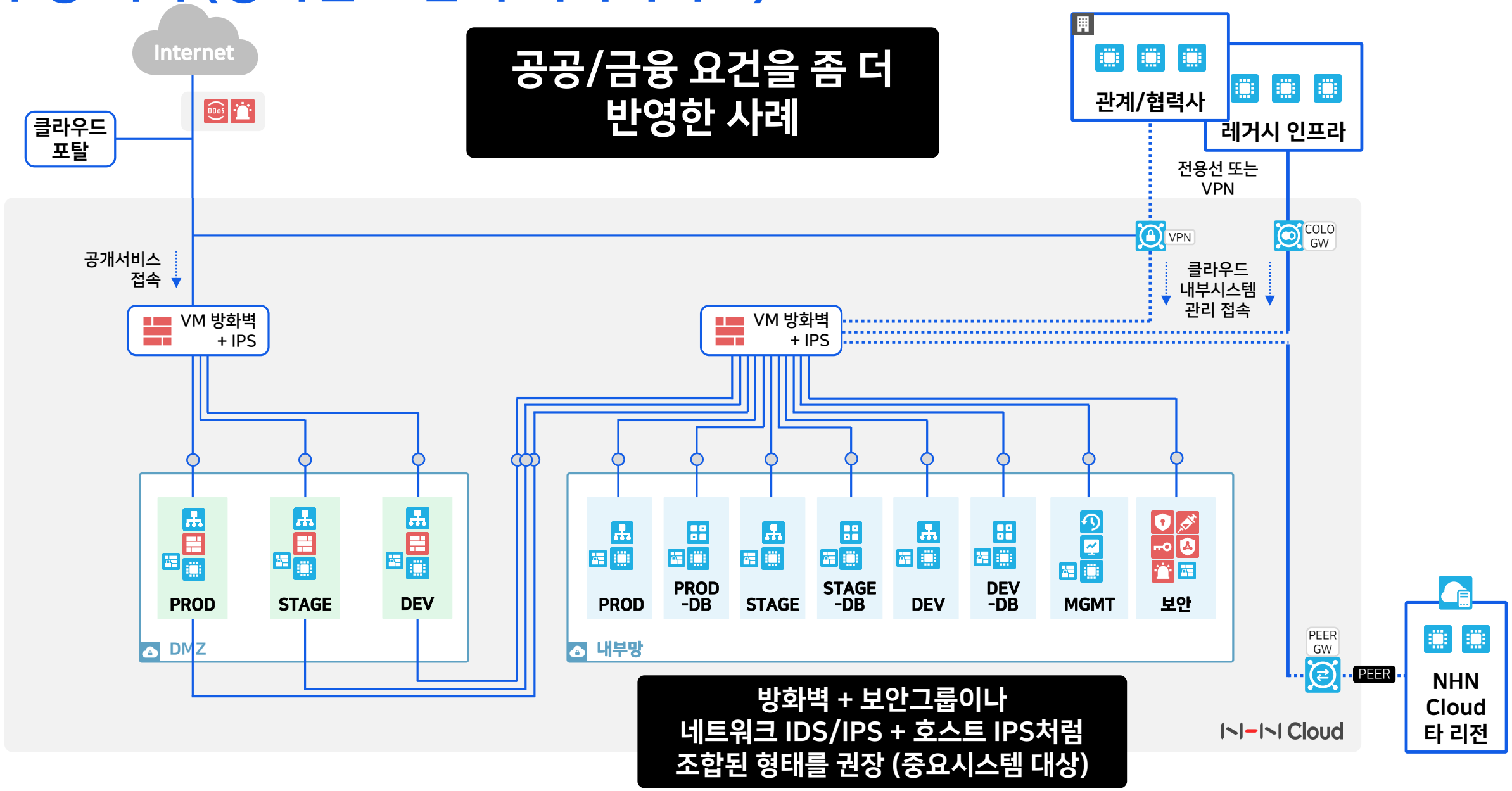
이것도
공공은
좀 달라요

보안USB는 클라우드에서 쓰기 어려움

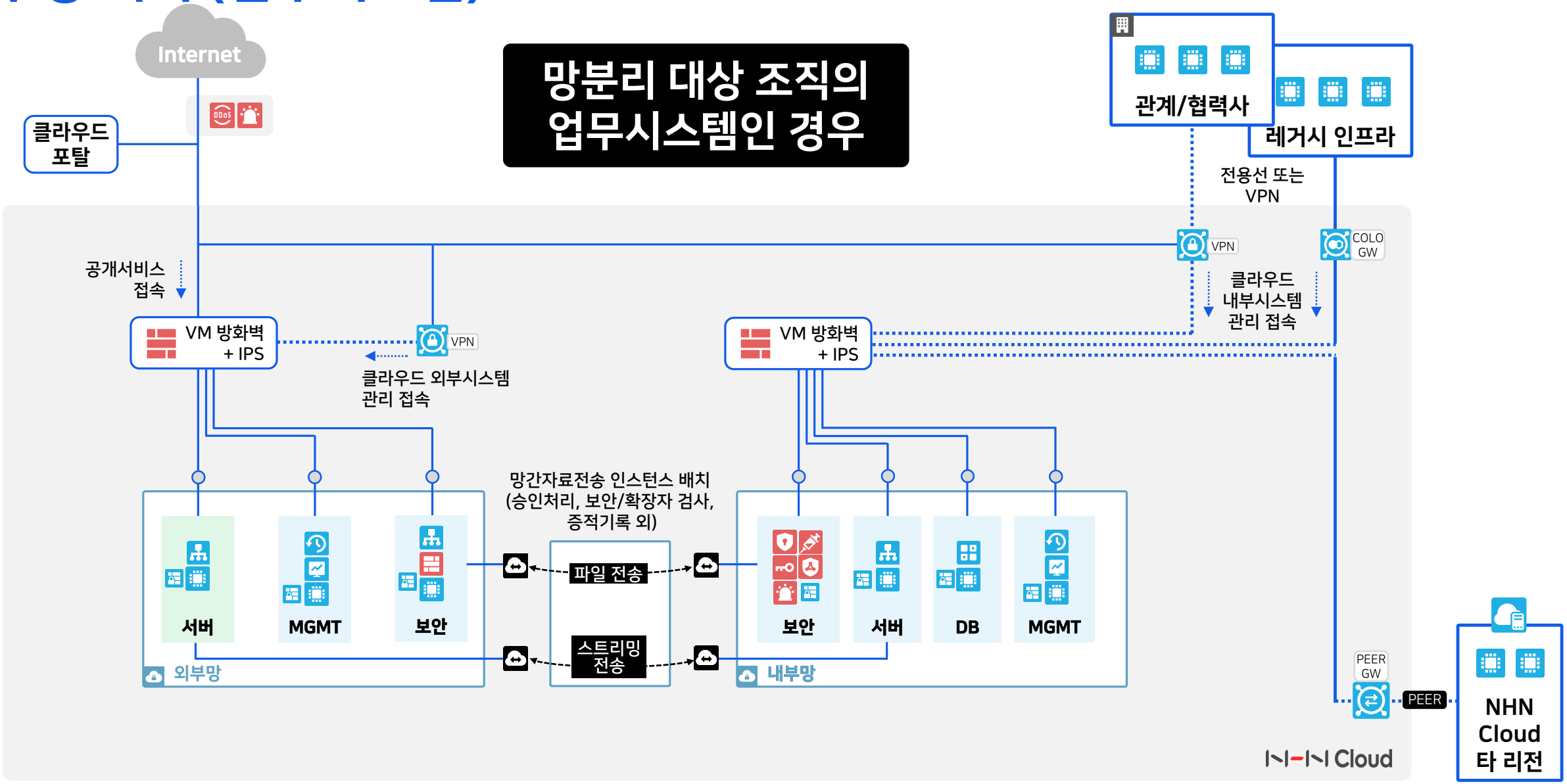
Subnet, VPC 나누는 것 만으로 '망분리'는 인정 안 되는 경우 많음



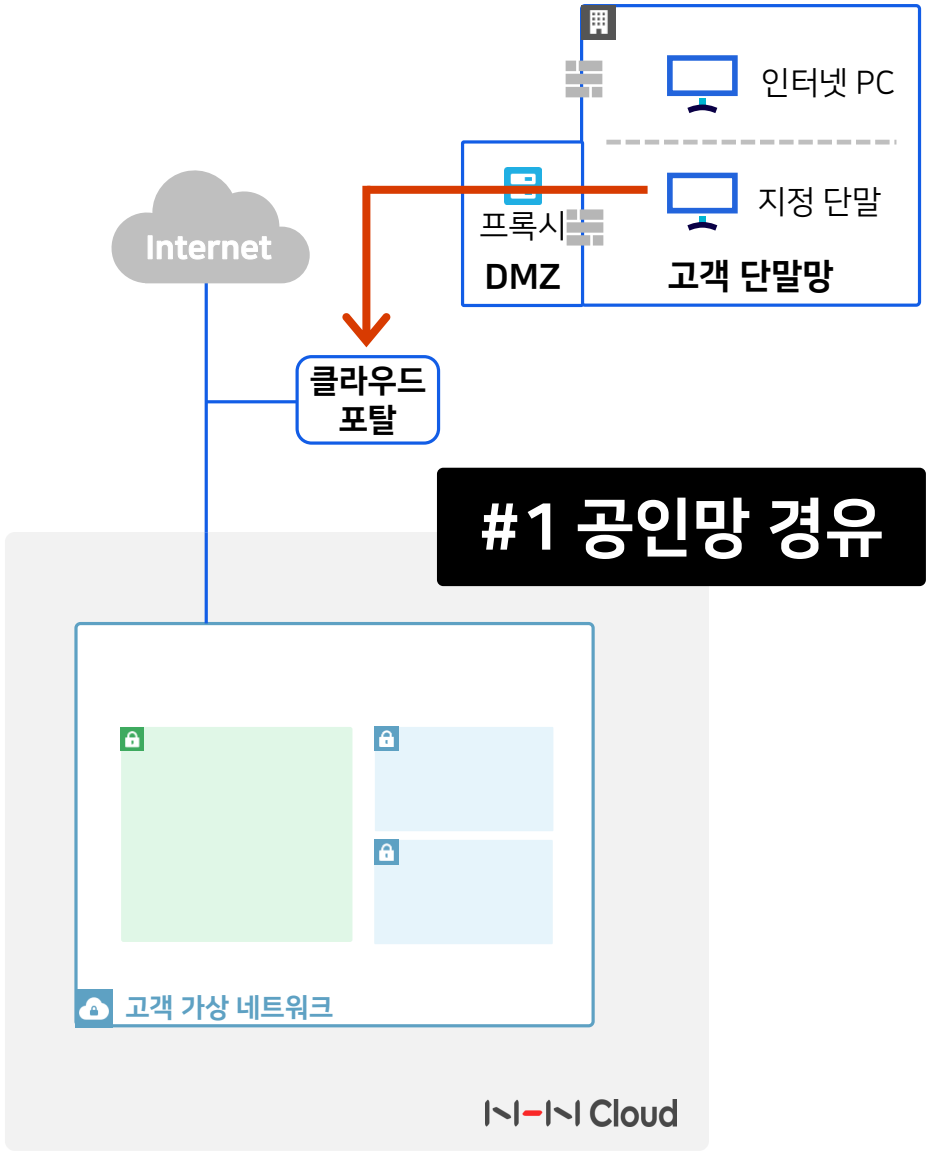
구성 예시 (강화된 보안의 대외서비스)

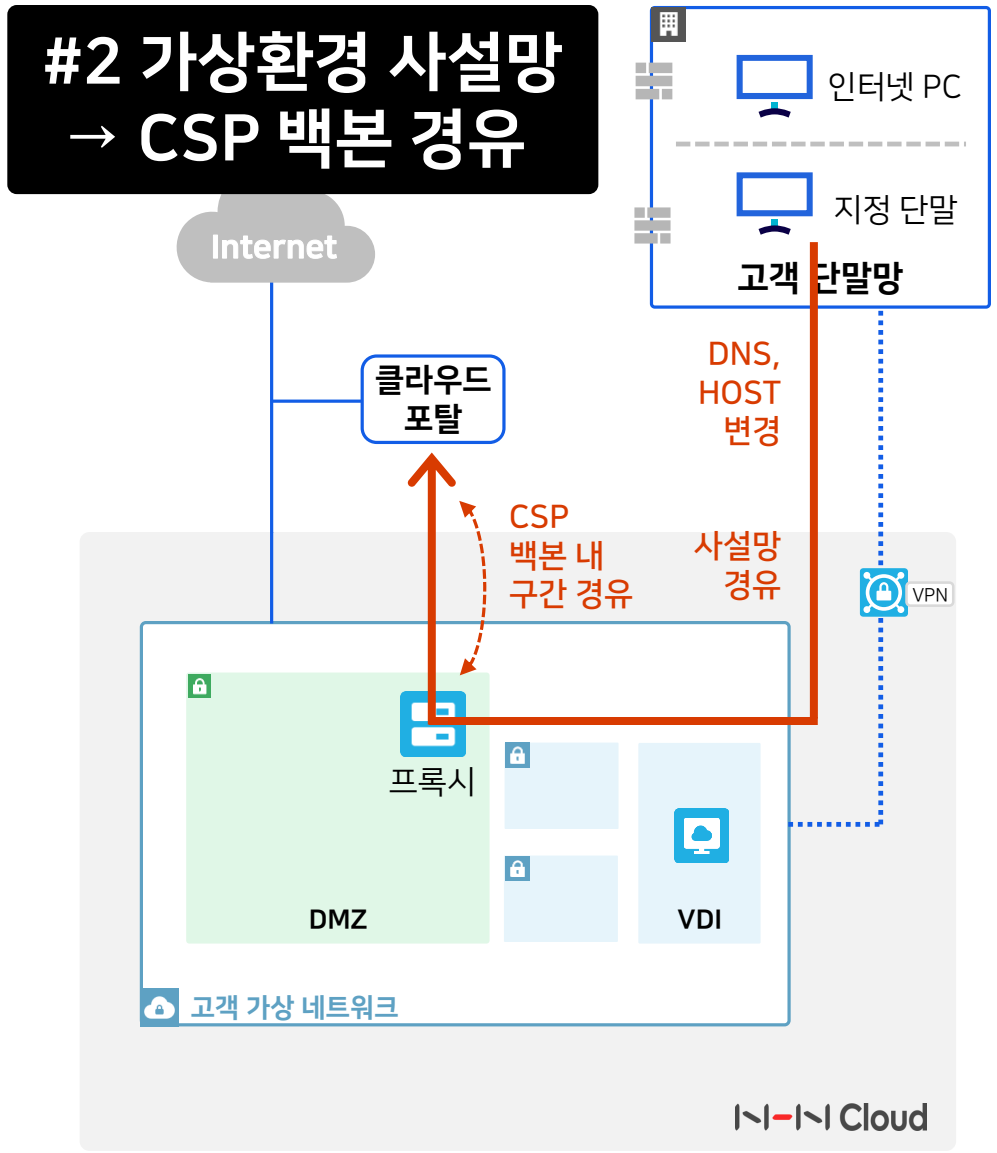


구성 예시 (업무시스템)


Internet
클라우드 포탈
망분리 대상 조직의 업무시스템인 경우
관계/협력사
레거시 인프라
전용선 또는 VPN
VPN
COLO GW
공개서비스 접속
클라우드 내부시스템 관리 접속
VM 방화벽 + IPS
VPN
클라우드 외부시스템 관리 접속
VM 방화벽 + IPS
망간자료전송 인스턴스 배치 (승인처리, 보안/확장자 검사, 증적기록 외)
서버
MGMT
보안
파일 전송
스트리밍 전송
보안
서버
DB
MGMT
외부망
내부망
PEER GW
PEER
NHN Cloud 타 리전

클라우드 포탈에 단말기 어떻게 붙이나요





보안그룹과 방화벽 뭐 써야 하나요

구분	Security Group	Network ACL	VM 방화벽
제어 대상	인스턴스	네트워크, 인스턴스	네트워크, 인스턴스
설정 대상	프로토콜, IP, 포트 설정	프로토콜, IP, 포트 설정	프로토콜, IP, 포트, APP, 도메인, URL, 사용자 설정
제어 트래픽	방향(송신/수신) 및 타겟(보안그룹/주소) 선택	출발지, 목적지 짝으로 선택	출발지, 목적지 짝으로 선택
접근 제어 타입	허용 규칙만 설정 (whitelist)	허용 또는 차단 규칙 선택 가능 (whitelist or blacklist)	허용 또는 차단 규칙 선택 가능 (whitelist or blacklist)
상태	상태 저장	상태 비저장	상태 저장

관리 기능이나 제어 대상에 대한 특성 확인하고 선택

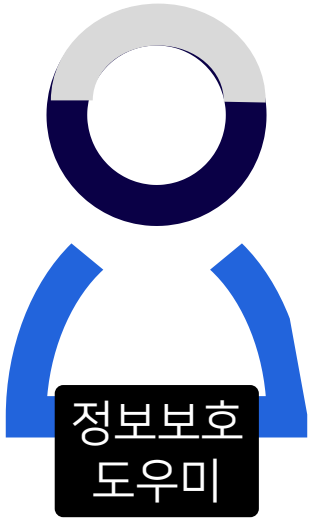
#4 암호화 및 개인정보 보호

암호화는 왜 하나요

중요 데이터 보호에 가장 효과적인 수단

→ 정보가 감청 또는 탈취되어도 식별·사용할 수 없게 함

→ 구간 암호화, 데이터 암호화 등을 주로 사용



암호화·키관리의 정석

개인정보의 안전성 확보조치 기준 해설서

금융부문 암호기술 활용 가이드

2019. 1.

2020. 12.

금융보안 FINANCIAL SECURITY INST

주요 내용

관리 계획 | 접근 권한 | 접근 통제 | 암호화 | 접속기록 관리 | 악성프로그램 방지 | 단말기 안전조치 | 물리적 안전조치 | 외 등등등

KISA

암호화 영역 주요 내용

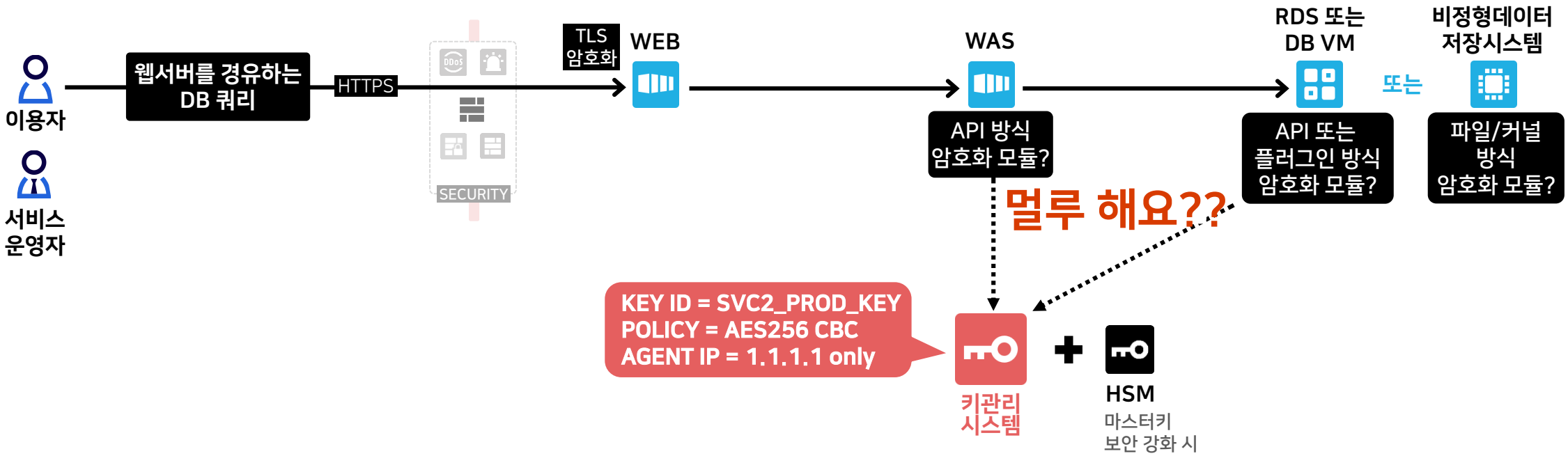
- ▣ 비밀번호 및 바이오 정보 암호화 (비밀번호는 일방향 암호화)
- ▣ 인터넷·DMZ 구간 고유식별정보 저장 시 암호화
- ▣ 안전한 암호알고리즘 사용
- ▣ 암호 키 생성/이용/보관/배포/파기 절차 수립 및 시행
- ▣ 고유식별정보 저장·관리 시 업무용 컴퓨터 및 모바일 기기 내 상용 암호화 S/W 또는 안전한 암호화 알고리즘 사용

■■■ 암호화 적용 기준 요약표 ■■■

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보 고유식별정보			암호화 송신
개인정보처리 시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인 등록번호, 운전면허 번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부·적용범위를 정하여 시행 ① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ② 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보			암호화 저장 ※ 비밀번호는 일방향 암호화 저장

관리, 기술적으로 레거시 대비 크게 바뀐 건 없으나

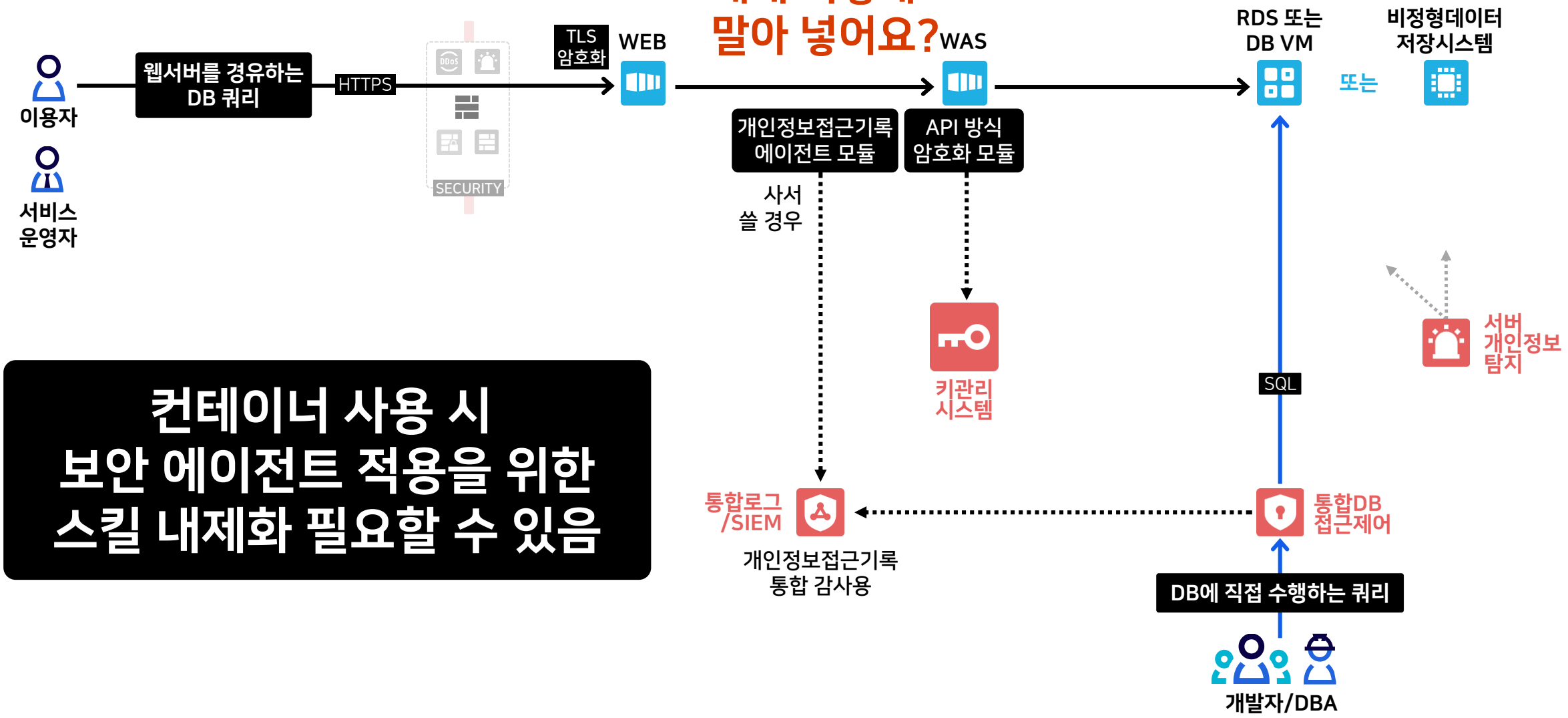
클라우드 DB 암호화 방식 특이점



RDS, 컨테이너 등의 사용 여부에 따라 DB 암호화 방식이 한정될 수 있고

RDS 환경 대응 + 구간 암호화 대용으로 활용되는 등 장점으로 API 방식이 많이 사용되는 추세

컨테이너 적용 특이점



컨테이너 사용 시 보안 에이전트 적용을 위한 스킬 내제화 필요할 수 있음

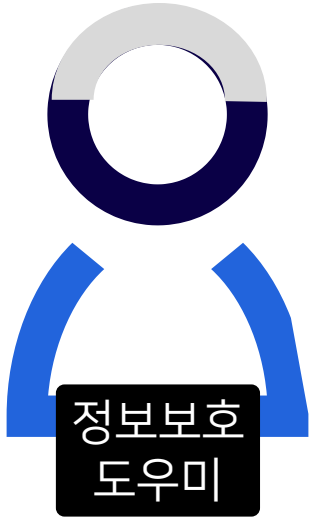
#5 로깅, 감사

로깅?

→ 분석, 모니터링의 유용한 도구

→ 사고나 이슈 추적 시 최우선 필요

→ 선량한 관리자로써의 의무를
가장 쉽게 증명할 수 있는 수단



소중한 로깅

소중하게 간직할거
하나 추가요

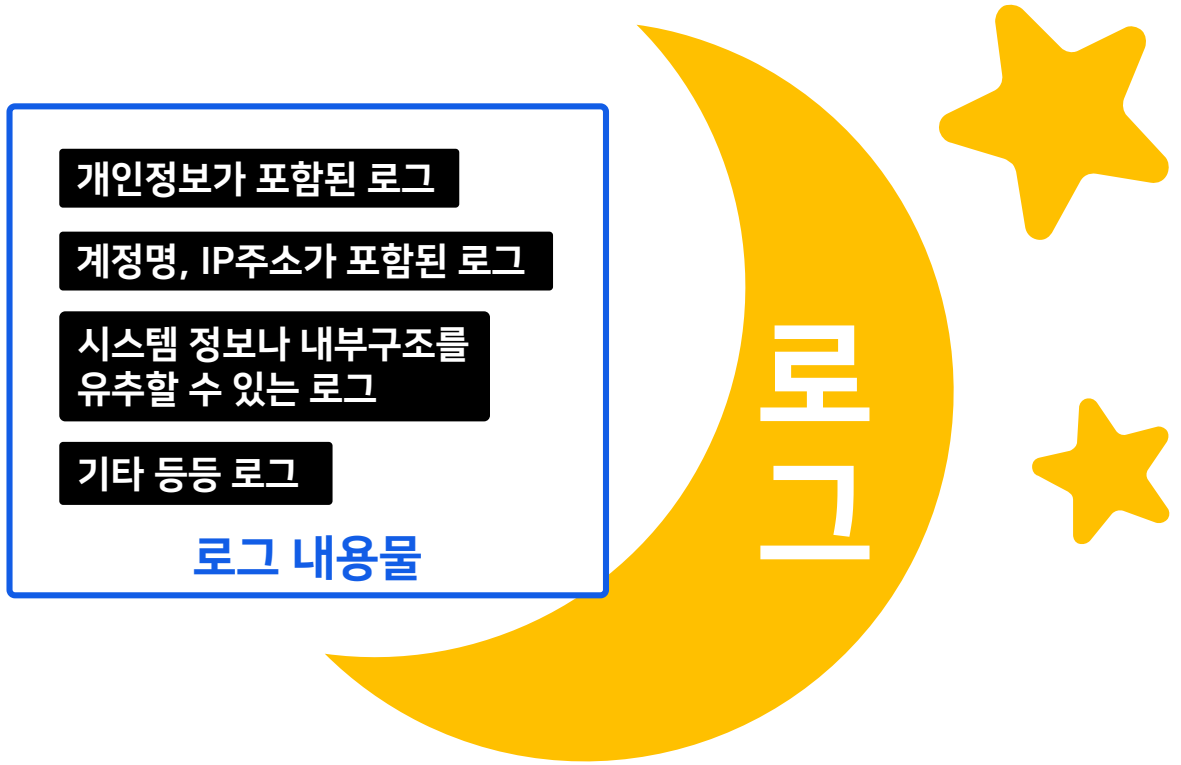
접근기록 가동기록

독립된 공간에 안전하게 보관

소중한 로깅

개인정보 포함된 로그가 유출이나 거래에 악용될 수 있는 점 외에,

개인정보가 없더라도 내부망 침입이나 포탈 계정 탈취 등에 매우 요긴하게 활용될 수 있음



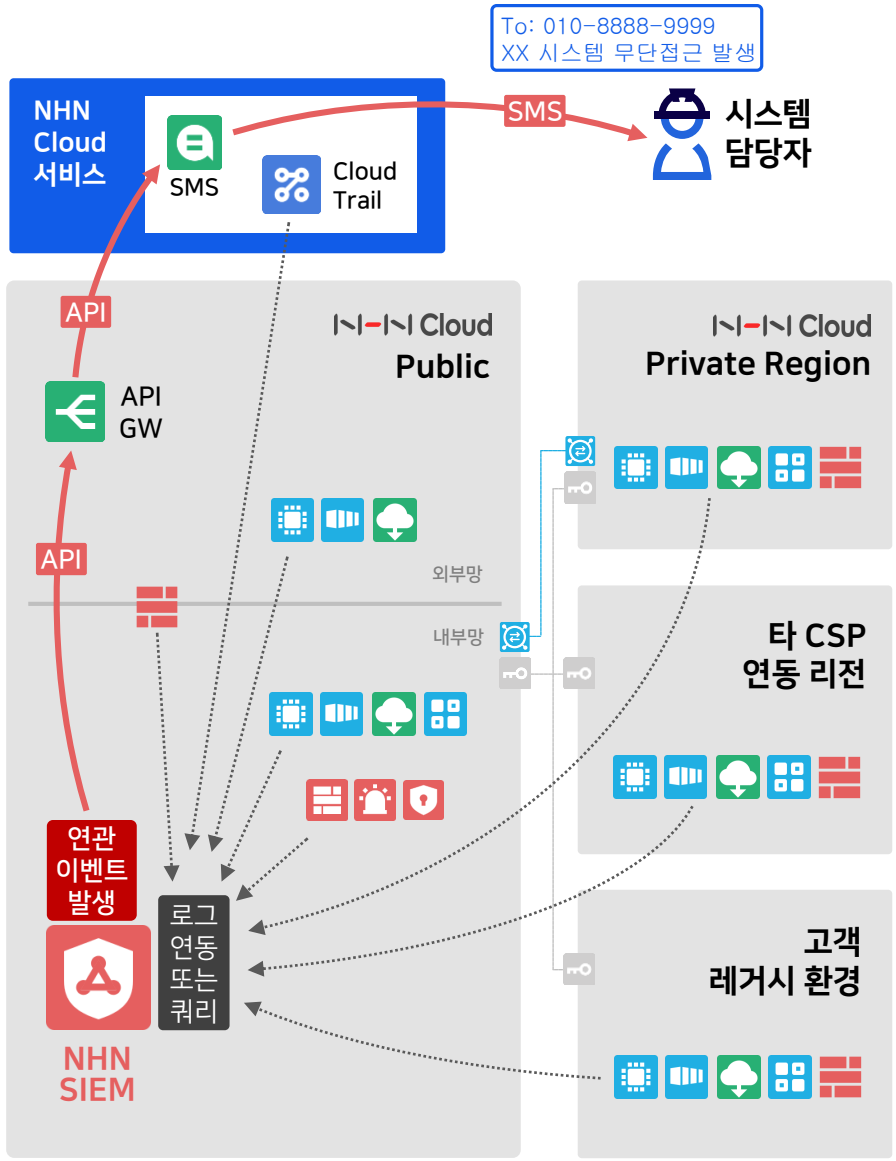
클라우드 로깅 체계 구성 예시

가상자산 별 로그 요건 식별하고 각 시스템에 우선 적용하되 (기간, 조회 권한, 백업, 암호화, 무결성 외)

클라우드 포탈이나 PaaS 관련 로그 관리 방안도 고려해야 하며

감사/모니터링 업무를 위한 통합관리도 고민하되

SIEM 연관분석 기능 등으로 추가 위협 식별이나 업무 자동화 적용 검토



기록 요건 분류 예시 (시스템 별)

유형	기록필요사항	적재 경로	보존기한
S/W 가동기록	S/W 가동 및 중지 시각		1년
	S/W 오류 및 에러		1년
S/W 접근기록	접속 기록 (일시, 접속IP, 접속자, 접근대상 등 포함)		1년
	이용자 로그인 및 로그아웃 (실패한 접근 시도 포함)		1년
	관리자 로그인 및 로그아웃 (실패한 접근 시도 포함)		1년
	웹콘솔/관리콘솔에 대한 접근통제 기록 (차단/허용)		1년
	웹콘솔 감사기록 (사용자/일시/변경내용/조회내용/수행내용 포함)		1년
	개인정보처리시스템 접근권한 부여/변경/말소		3년
	개인정보처리시스템 접속기록 (계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등 포함)		1년 또는 2년
	전자금융 관련 접속 및 거래기록		5년
	개인신용정보처리시스템의 접근권한 부여/말소 기록		3년

유형	기록필요사항	적재 경로	보존기한
보안시스템 추가 기록	보안시스템 위협 탐지/차단 기록 (방화벽)		1년
	보안시스템 위협 탐지/차단 기록 (백신)		1년

SIEM 연관분석 탐지 적용 예시

◎ 주요 서버에 접근제어시스템 경유 없이 직접 접근
◎ 심야 시간에 클라우드 포탈 내 프로젝트 진입
◎ 동일 수신자에게 제한된 크기 이상의 파일로 하루 10회 이상 파일을 첨부하여 발송
◎ 동일 소스 IP에서 동일 대역으로 지속적인 SSH 접속 시도 (10분에 5회 이상) 등등

#6 보안 모니터링 & 취약점 점검

보안관제와 취약점 점검

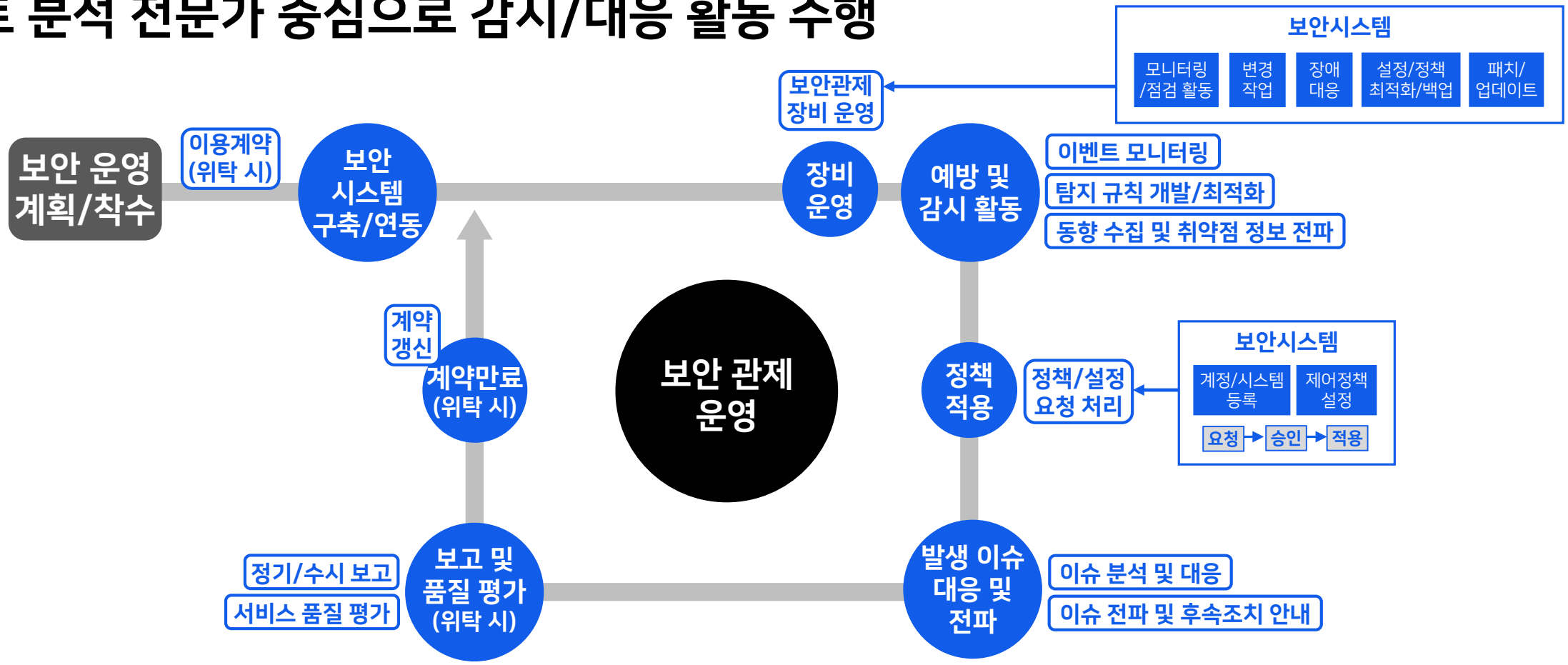
보안관제 : 실시간 취약점 감시/분석/전파/대응
취약점 점검 : 사전 취약점 점검 및 후속조치

사전 점검의
한계점 보완

침해대응의
가능성/빈도 감소

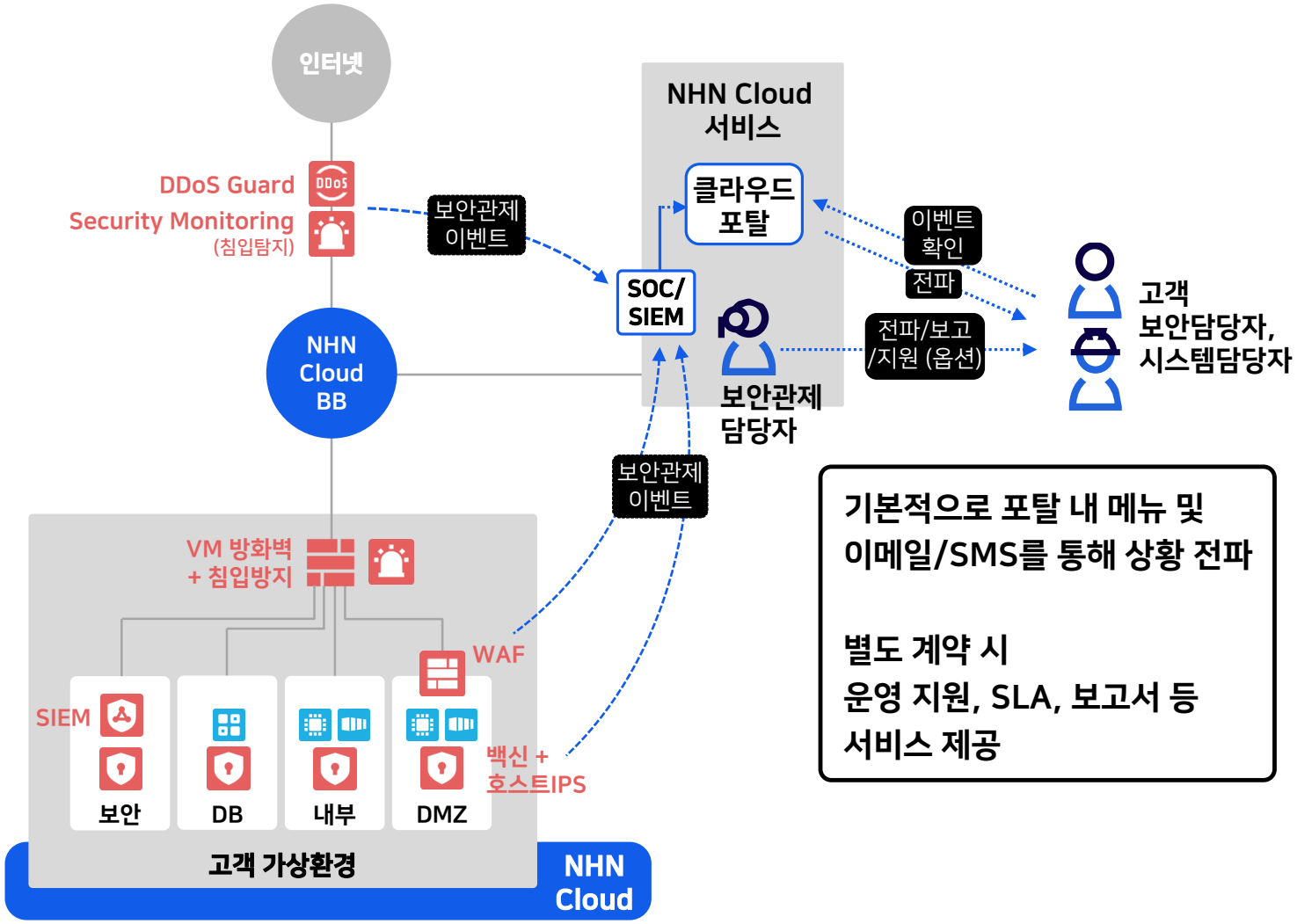
보안관제 주요 업무

보안관제용 장비 (침입탐지/방지, 웹방화벽, 백신 등)
이벤트 분석 전문가 중심으로 감시/대응 활동 수행



보안담당자 전파 후 대응할 시스템/NW/DB/서비스 담당자의 유기적 협조체계 필요

보안관제 모니터링 구조



기본적으로 포탈 내 메뉴 및
이메일/SMS를 통해 상황 전파

별도 계약 시
운영 지원, SLA, 보고서 등
서비스 제공

**고객이 직접 수행하거나
CSP 서비스 이용 가능**

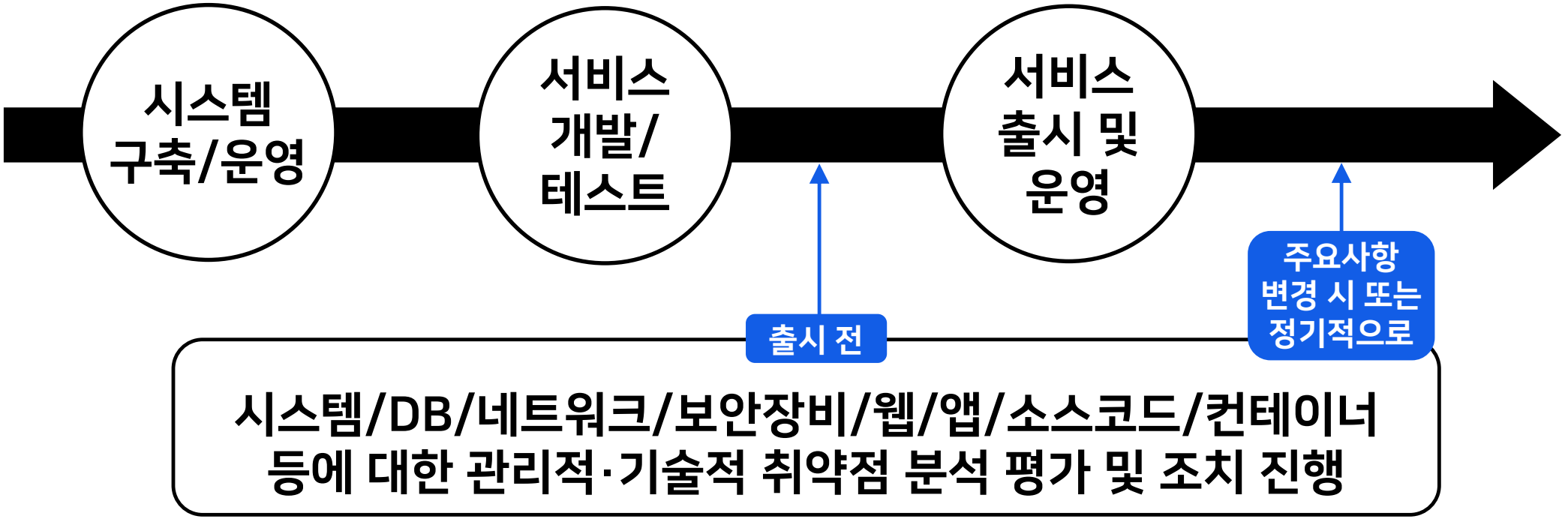
기술/관리적 감시 방법이 레거시 대비 크게 변화한 것은 없음

웹서버나 컨테이너 보호를 위한 WAF를 두고 암호화 트래픽을 복호화하여 위협 검사하되,

컨테이너 세부 보안관제를 위한 솔루션도 필요 시 검토 (CWPP, RASP 외)

컨테이너 이미지 취약점을 악용한 권한 상승, Escape 등의 보안위협을 무시할 수 없으며, 컨테이너 설정 점검, 권한 제어 등 외에 전용 보안장치로 보완 가능

고객 영역 취약점 점검



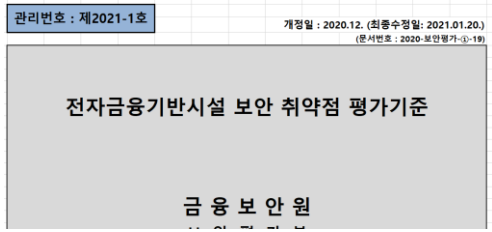
주로 이런 형태로 운영되며,
요건·제도화된 영역의 점검은
레거시와 유사 (시스템/웹/앱/소스코드 등)

고객 영역 취약점 점검

주요정보통신기반시설

기술적 취약점 분석·평가 방법 상세가이드

2021. 3.


관리번호 : 제2021-1호

개정일 : 2020.12. (최종수정일: 2021.01.20.)
(문서번호 : 2020-보안평가-①-19)

전자금융기반시설 보안 취약점 평가기준

금 융 보 안 원

과학기술정보통신부 KISA 한국인터넷진흥원

조직 내 기준 또는
기반시설 점검 기준 반영
(주요정보통신기반시설,
전자금융기반시설 등)

Kubernetes 보안 가이드

Kubernetes Security Guide

2.16. Docker

Host 설정(8개 항목), 도커 데몬 설정(4개 항목), 도커 데몬 설정 파일(12개 항목), 컨테이너 이미지 및 빌드 파일(2개 항목) 컨테이너 런타임(6개 항목) 총 5개 영역에서 32개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
	DO-01	도커 최신 패치 적용	상
	DO-02	도커 그룹에 불필요한 사용자 제거	중
	DO-03	Docker daemon audit 설정	상

컨테이너 사용 시
KISA/보안업체/CSP가 제공하는
점검 가이드라인이나,
오픈소스/상용 점검 도구 활용
(Trivy, Clair, Qualys, CWPP 외)

클라우드 포탈의 보안설정도
주기적으로 점검

1. 계정 및 권한 관리기준	관련 이슈 및 권장사항	
1.1 계정 및 권한 관리 기준	사용자의 직무에 따라 계정의 그룹과 정책을 최소 권한으로 생성하여 권한 남용으로 보안 사고가 발생하지 않도록 절차를 준수해야 하며, 리소스 접근에 대한 보안, 관리, 감사를 위해 그룹화 필요	[NHN Cloud 사용자 권한] NHN Cloud Console > 조직&프로젝트 > 멤버 관리 > [IAM사용자 권한] NHN Cloud Console > 조직&프로젝트 > 멤버 관리 > * 필요한 서비스를 기준으로 admin/member/viewer 등
1.2 계정 최초 패스워드 설정	신규 등록한 계정은 최초 사용 시 로그인한 사용자가 직접 패스워드를 변경하도록 하며, 관리자 및 다른 사용자가 패스워드를 알 수 없도록 즉시 변경 필요	IAM 회원의 경우 OWNER의 IAM 회원 등록 시 비밀번호

NHN Cloud Server Security Check

시스템 점검 관련 CSP 제공 도구 활용 가능

인스턴스 명	인스턴스 OS	점검 종류	시스템 버전	점검 기준	점검 버전	점검 일시	취약/전체	상	중	하	보고서
CentOS7.8	Linux	OS	CentOS 7.8	주요정보통신기반시설	G-1	2020-10-13T07:57:10+09:00	15/65	6	4	5	다운로드
CentOS7.8	Linux	OS	CentOS 7.8	전자금융기반시설	F-1	2020-10-13T07:57:07+09:00	17/80	7	5	5	다운로드

위험도 선택 ▾ 점검 결과 선택 ▾

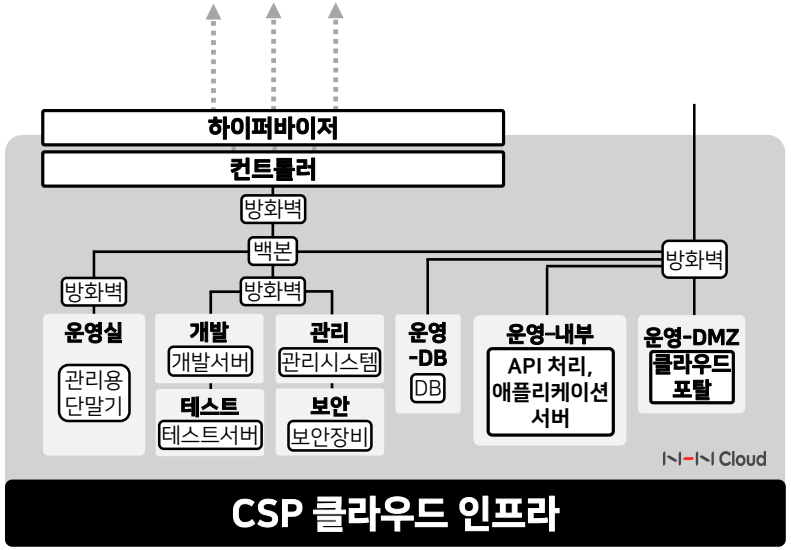
분류	번호	항목 명	위험도	점검 결과	대응 방안
1. 계정관리	U-01	root 계정 원격 접속 제한	상	취약	가이드
1. 계정관리	U-02	패스워드 복잡성 설정	상	취약	가이드

#7 가상서버 영역 보안 강화

가상 환경 및 서버에 대한 보안 강화

앞에 나왔던 내용들을 포함하여
가상서버 보안용 지침 내용을 추가 반영

이행 필요



이행 중
(CSP 인증과 평가에 포함)

서버 및 가상화 보안 정보보호 요구사항 KISA 클라우드 정보보호 안내서

공통	① 바이러스, 웜, 트로이목마 등의 악성코드 예방을 위해 서버 및 가상환경을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 적용한다. 특히, 가상환경의 경우 이상 징후 발견 시 사용 중지 및 격리 조치를 수행할 수 있는 체계를 갖추고 운영한다.
가상화 보안	① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립한다. ② 가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 한다. ③ 호스트 OS 및 하이퍼바이저를 모니터링 하고 악성코드 감염예방을 위해 주기적인 보안패치를 시행한다. ④ 가상화 실행 이력은 스냅샷 등 이미지 형태로 저장 · 관리하는 방안 등 안전한 저장 방법으로 관리한다. ⑤ 가상화 OS의 내 · 외부 데이터 이용에 대한 로그 정보를 관리 한다. ⑥ 가상머신별 자원 사용량 제한하여 특정 가상머신의 자원이 남용되지 않도록 한다. ⑦ 호스트와 가상영역 간의 경계를 명확히 구분하고 운영한다.
서버 보안	① 클라우드 서비스 운영 시 시스템에 대해 기술적 보호대책을 수립하고 적용한다. - 웹서버, DB서버, 클라우드 인프라 관리서버 등 운영 시 다음의 보호대책 적용 · 송 · 수신 시 SSL/TLS 통신 적용, 불필요한 서비스 및 포트 차단 · 접근권한 설정, 백신설치 및 OS 최신 패치 · 불필요한 소프트웨어, 스크립트, 실행파일 등 설치 금지 · 불필요한 페이지(테스트 페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지 · 주기적인 보안패치 및 취약점 점검 실시 등 ② 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호한다. ※ 보안솔루션 구축 시 고려사항 기존 IT 환경에서는 일반적으로 H/W 형태 보안솔루션(Firewall, IPS, IDS, Web Application firewall 등)을 구축하지만, 가상환경에서는 유연한 확장성을 고려하여 S/W 방식으로 구축하는 것이 일반적이다. 따라서, 확장성이 반드시 보장되어야 한다면 호스트 기반의 보안솔루션을 설치하는 것이 적합한 방법이다.

#8 관리·운영 보안 적용

관리 체계 변경점 도출

- 담당 조직 구성 및 역할 검토
- 자산 식별 및 관리
- 시스템 신청/승인/처리/증적
- 기록 감사와 모니터링
- 위협 식별 및 조치
- 교육 계획 및 수행
- 퇴사/전배자 변경 관리
- 지침과 가이드라인
- 외부 인력 보안 관리
- 기타 등등등 모든 관리사항

관리 체계 변경점 도출

- 클라우드 담당 조직 구성 및 역할 검토
- 클라우드 자산 식별 및 관리
- 클라우드 시스템 신청/승인/처리/증적
- 클라우드 기록 감사와 모니터링
- 클라우드 위협 식별 및 조치
- 클라우드 교육 계획 및 수행
- 클라우드 퇴사/전배자 변경 관리
- 클라우드 지침과 가이드라인
- 클라우드 외부 인력 보안 관리
- 클라우드 기타 등등등 모든 관리사항

기술의 변화는 관리적 변화를 수반

체크리스트 작성

정보보호 관리체계 체크리스트

주로 정보보호 담당자가
조직 별 요건 분배

		상세내용	클라우드 변동 유무	클라우드 적용 방안	주 검토 조직	추가 이슈	비고
	관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.	O	- 클라우드포탈, VM 등을 대상으로 한 특수 계정/권한 식별 및 관리 적용 - 클라우드포탈 내 멤버관리를 통해 인증 및 권한 부여 - 기존 레거시망 내 통합접근제어 시스템을 연동하여 VM 접근 계정 및 권한 적용 (VPN 연결)	보안정책팀 보안기술팀	- 클라우드에 추가된 새로운 유형의 시스템이 있을지 기술조직 인터뷰 필요	
2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다	O	- 클라우드포탈, VM 등의 사용자 계정 및 권한에 대해 이력 적용 방안 검토 - 클라우드포탈 계정에 대한 감사기록 도구 적용 (CloudTrail) - 기존 레거시망 내 통합접근제어 시스템을 연동하여 VM 접근 계정에 대한 감사기록 도구 적용	보안정책팀 IT시스템팀		
2.6.1	네트워크 접근	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.	O	- 클라우드 내 논리적 네트워크 구성을 파악하고 적절한 통제방안 적용 (보안그룹, ACL, VM방화벽 등)	보안기술팀 네트워크팀	- 세부 기능 비교 필요	

추가

CSP 상품 활용

NHN Cloud Security Compliance

CSP가 제공하는 도구를 활용하는 것도 유용

NHN Cloud On

Security Compliance > 가이드

URL & Appkey | 사용자 가이드

인증서 | 가이드

정보보호 인증 가이드

ISMS-P | 책임 선택 | 입력해주세요. | 검색 | 다운로드

대분류	소분류	항목 ID	항목	상세 내용	책임	대상 서비스	준수 방안
인증 및 권한 관리		2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.	공통	Console > 멤버 관리 마켓플레이스 > 시스템/DB 접근제어 및 계정관리 유형의 상품	(NHN Cloud) o NHN Cloud는 각 정보시스템의 관리자를 특수 권한자로 식별하여, 책임자의 승인을 득한 후 최소한의 인원에게만 권한을 부여하고 있으며, 특수 권한 관리자는 별도로 목록화 하여 관리하고 있습니다. (고객) o 고객은 정보시스템 및 중요 데이터의 특수 목적을 위하여 사용하는 계정 및 권한을 최소한으로 부여하고 식별할 수 있도록 관리하여야 합니다. [클라우드 활용방안] o 고객은 클라우드 콘솔 및 VM Instance에 대한 특수 계정 및 권한을 관리하여야 하며, NHN Cloud에서 제공하는 다음의 기능 및 서비스를 이용할 수 있습니다. - 클라우드 콘솔의 멤버관리를 통해 콘솔의 특수 계정에 대한 인증(로그인) 및 권한 부여를 통제 할 수 있습니다. 프로젝트와 조직에서 멤버 관리를 별도로 할 수 있으며, 멤버는 콘솔 회원과 IAM 회원으로 구분됩니다. - 또한 마켓플레이스에서 제공하는 접근제어 및 계정관리 상품을 통해서 VM Instance(시스템/DB)에 대한 사용자 계정 및 권한, 접근통제, 로그를 통합적으로 관리할 수 있습니다.
						Console > 멤	(NHN Cloud) o NHN Cloud는 정보시스템에 접근하는 사용자 계정 및 권한에 대한 부여/변경/삭제 로그를 기록하고 있으며, 접근권한 현황 및 권한의 적절성에 대하여 정기적으로 검토하고 있습니다.

NHN Cloud On

CSP 상품 활용

NHN Cloud
CSAP SaaS Guidance

CSAP SaaS 인증을 위한 가이드라인, 샘플 지원 + **방문 상담 지원**

보안 아키텍트

항목 ID	점검항목	점검항목 설명	ISMS-P 대체	대상 서비스	신청기관 준비사항 (관련증적)	참고사항 (샘플자료)	준수방안
7.2.2.1	보안감사 증적(로그)을 식별하고 로그유형 및 보존기간(1년 이상)을 정의하여 법적요건을 고려하여 기록(보관)하고 검토하고 있는가?	ㅇ 보안감사로그 유형 및 보존기간(최소 1년 이상)은 법적요건을 고려하여 정하고 안전하게 보관하여야 한다. - 로그유형 및 보존기간 정의 확인 - 로그기록 보존(백업) 방법 확인 ※ 보안감사 로그 : 사용자 접속기록(사용자식별정보 : ID, 접속일시, 접속지 : 단말기 IP, 수행업무 : 정보생성, 수정, 삭제, 검색 출력 등), 인증 성공/실패 로그, 파일 접근, 계정 및 권한 등록/변경/삭제 등 ※ 참고 ※ - 개인정보보호법 '개인정보의 기술적 · 관리적 보호조치(개인정보보호위원회 고시)' 기준 제4조(접근권한의 관리) 및 제5조(접속기록의 위·변조방지) - 개인정보보호법률 '개인정보의 안전성 확보조치(고시)' 제5조(접근 권한의 관리) 및 제8조(접속기록의 보관 및 점검) ㅇ 공공기관용 클라우드 서비스의 경우 공공기관이 감사 로그를 요청 시 제공하여야 한다.		서비스 > CloudTrail 마켓플레이스 > 시스템/DB 접근제어 및 계정관리 유형의 상품 서비스 > SIEM	• 로그 기록 • 로그 백업 대장 • 로그 기록 검토/보호 방법	• 정보보호 정책서	ㅇ SaaS 사업자는 클라우드 서비스를 위한 시스템의 보안감사 증적(로그)를 식별하여야 하며, 유형 및 보존간은 법적요건을 고려하여 정하고 안전하게 보관 및 검토하여야 합니다. 보안감사 증적(로그)은 식별할 수는 형태로 기록하고, 법률에 따라 최소 1년 이상 보관하여야 하며, 보관되고 있는 보안감사 증적을 모니터할 수 있는 수단을 제공해야 합니다. ※ 공공기관용 클라우드 서비스의 경우 공공기관이 감사 로그를 요청할 경우 제공하여야 합니다. [클라우드 활용방안] ㅇ SaaS 사업자는 클라우드 콘솔, VM Instance 및 애플리케이션에 대한 로그 및 접속기록 등 보안감사 증적을 관리하여야 하며, NHN 클라우드에서 제공하는 다음의 기능 및 서비스를 이용할 수 있습니다. - NHN 클라우드에서 제공하는 CloudTrail을 통해 콘솔의 신규 계정 생성, 삭제 등의 계정 활동 로그와 Instance 생성, 삭제 등의 서비스 활동 로그를 기록 및 확인할 수 있으며, 마켓플레이스에서 제공하는 접근제어 및 계정관리 상품을 통해서 VM Instance(시스템/DB)의 로그를 법적요건에 맞게 관리할 수 있습니다. - 또한 SIEM 서비스를 통해 VM Instance 및 애플리케이션의 로그를 통합적으로 관리할 수 있으며, 계정에 따른 로그 검색 권한 할당, 실시간 위협 탐지, 이기종 시스템 로그 연관 분석, 컴플라이언스 관리 및 이벤트 발생 시 알람 설정 기능을 적용할 수 있습니다.
7.2.2.2	로그기록을 별도 저장장치를 통해 백업하고 비인가된 접근 및 변조로부터 보호하고 있는가?	ㅇ 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한부여는 최소화하여 비인가자에 의한 로그기록 위변조 및 삭제 등이 발생하지 않도록 하여야 한다. ㅇ 주요 서버, 네트워크, 보안 장비의 로그는 최소 1년 이상 유지 및 관리하여야 한다.		서비스 > NAS (offline) 서비스 > Object Storage 서비스 > Backup	• 로그 기록 • 로그 백업 대장 • 로그 기록 검토/보호 방법	• 정보보호 정책서	ㅇ SaaS 사업자는 클라우드 서비스를 위한 보안감사 증적은 별도 저장장치에 백업하여야 하며, 비인가된 접근 및 변조로부터 보호하여야 합니다. 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한 부여를 최소화하여야 하며, 주요 서버, 네트워크, 보안 장비의 로그는 최소 1년 이상 유지 및 관리하여야 합니다. [클라우드 활용방안] ㅇ SaaS 사업자는 클라우드에 저장되는 로그 데이터에 대한 백업 및 복구 방안을 마련하여야 하며, NHN 클라우드에서 제공하는 다음의 기능 및 서비스를 이용할 수 있습니다. - NAS 및 Object Storage 서비스를 통해 이용자가 직접 데이터에 대한 백업을 수행할 수 있습니다. NAS는 여러 개의 인스턴스에서 네트워크를 통해 액세스할 수 있는 스토리지로써, 사용자 프로젝트 단위로 NAS 볼륨 접근을 제어해 높은 보안성을 제공하며, 스냅샷 기능으로 데이터를 복구할 수 있습니다. Object Storage는 REST API 기반의 확장 가능한 대용량 스토리지로써, 서로 다른 여러 하드웨어에 파일을 분산, 중복 저장하여 데이터의 안정성을 보장합니다. - NHN 클라우드는 고객 데이터의 안전한 백업을 위해 Backup 서비스를 제공합니다. Backup 서비스는 전체 백업 방식과 증분 백업 방식을 함께 사용함으로써 백업 시간이 단축되고 네트워크 사용량도 줄어드는 효과가 있습니다. 또한 간편한 백업 정책 등록 및 백업 이력 조회가 가능하고, 복구 요청을 할 수 있는 웹 콘솔 환경을 제공하며, 백업 결과는 매일 취합되어 사용자의 메일로 보고됩니다.

CSP 상품 활용

NHN Cloud

CSAP SaaS Guidance

프로모션 중!

Summary

WIN WIN

화 이 팅

체계적인 가상환경 인프라 운영 및 정보보호 관리

고객 가상 인프라 및 애플리케이션

클라우드 환경과 신기술에 대한 기술력 및 노하우 지원

체계적인 보안 기능과 상품 제공

CSP, MSP 지원 조직

엄격한 클라우드 인프라 운영 및 정보보호 관리

CSP 클라우드 인프라

WIN WIN

안전한 클라우드 서비스 체계 실현!

NHN Cloud On

NHN Cloud

유연하게, 안전하게
비즈니스에 힘이 되다.