『디지털서비스 심사신청 자가 점검 체크리스트』 이용 안내사항

1. 본 "디지털서비스 심사신청 자가 점검 체크리스트"는 「디지털서비스 심사·선정 등에 관한 고시」에 따라 신청인이 디지털서비스 심사신청 시 제출할 서류(별표4에 따른 디지털서비스 제공역량 증명자료)에 포함해야 할 사항을 안내하고 있습니다.
   - 본 자료는 디지털서비스 검토반 상정 시 검토 위원의 검토자료로 사용될 수 있으며, 실제 서비스의 자가 점검 체크리스트입니다. 해당 내용 참고하시기 바랍니다.

2. 디지털서비스 심사선정 여부는 "디지털서비스 심사위원회"에서 최종 판단할 사항으로 본 "자가 점검 체크리스트"와는 무관함을 알려드립니다.

※ 파란색으로 표기된 부문은 구체적인 설명 및 예시를 기술한 것으로 해당 내용을 참고

디지털서비스 심사신청 자가 점검 체크리스트

기업명/서비스명/서비스유형	㈜아이티아이즈/아이티아이즈 지원서비스/클라우드지원서비스
검토자	수석 / 임철현 / 010-5653-9986 / 56539986@iteyes.co.kr

I. 디지털서비스 해당여부

검토 항목	세부 내용
클라우드 컴퓨팅 서비스	▪ 클라우드컴퓨팅*을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스 * 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계 ☐ 클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스에 해당함 ☐ 클라우드컴퓨팅을 활용하여 상용으로 타인에게 정보통신자원을 제공하는 서비스에 해당하지 않음 ▪ 제조사의 클라우드컴퓨팅기술을 이용해 수요기관에게 재판매하는 서비스 ☐ 지원체계 또는 기술지원을 추가로 제공하는 공급사
클라우드 컴퓨팅 서비스를 지원하는 서비스 (이하 "지원서비스")	▪ 클라우드컴퓨팅서비스를 지원하는 서비스(다만, 클라우드컴퓨팅서비스에 해당되는 서비스는 클라우드컴퓨팅서비스로 분류하여 검토) ☑ 매니지드서비스에 해당함(클라우드컴퓨팅서비스 도입·전환에 필요한 컨설팅, 운영관리, 마이그레이션 등을 조합하여 지원하는 서비스) ☐ 컨설팅서비스에 해당함(클라우드컴퓨팅서비스 도입 및 전환에 필요한 요구사항 분석, 현황 분석, 타당성 검토, 도입전략 수립 등을 지원하는 서비스) ☐ 운영관리서비스에 해당함(클라우드 인프라 시스템을 안정적으로 운영하기 위한 기술지원, 모니터링, 장애처리, 백업 및 복구, 보안관리 등의 서비스) ☐ 마이그레이션서비스에 해당함(기존 시스템 운영환경의 일부 또는 전부를 클라우드컴퓨팅서비스 운영환경으로 전환하는 것을 지원하는 서비스) ☐ 기타 클라우드컴퓨팅서비스를 지원하는 서비스에 해당함 ☐ 위 어느 서비스에도 해당하지 않음
다른 기술·서비스와 클라우드컴퓨팅 기술을 융합한 서비스 (이하 "융합서비스")	▪ 클라우드컴퓨팅기술*및 다른 기술·서비스가 융합된 서비스(다만, 클라우드컴퓨팅서비스에 해당되는 서비스는 클라우드컴퓨팅서비스로 분류하여 검토) * 클라우드컴퓨팅의 구축·이용에 관한 정보통신기술로서, 가상화 기술, 분산처리기술, 그 밖에 정보통신자원의 배치와 관리 등을 자동화하는 기술 등 ☐ 클라우드컴퓨팅기술 및 다른 기술·서비스가 융합된 서비스에 해당함 - 활용된 클라우드컴퓨팅기술 : - 융합된 다른 기술·서비스 : ☐ 클라우드컴퓨팅기술이 활용되지 않았거나, 다른 기술·서비스가 융합되지 않음 ☐ 아래 기준에 부합하면 클라우드컴퓨팅서비스에 해당함 - 기관이 직접 운영하는 전형적인 업무용 응용프로그램과 시스템, 중요 데이터들을 처리·관리하는 분야의 서비스 · (예시) ERP, 그룹웨어, 협업툴, HRMS, 회계, 전자결제, 메일, 문서저작도구, 보안프로그램, 콘텐츠관리시스템(CMS), 지식관리서비스(KMS), 문서관리프로그램 ☐ 아래 기준을 모두 부합하면 클라우드컴퓨팅서비스에 해당함 - (셀프서비스) 사용자 중심의 요청기반 셀프서비스를 제공 - (범용네트워크) 단말기에 관계없이 네트워크를 통해 접속 가능 - (신속한 탄력성) 사용자의 요청에 의해 자원을 확장 가능한 구조를 제공 - (공동이용) 멀티테넌트 구조로서 이용자 요청에 따라 동적 할당 및 회수 - (서비스 측정) 사용량 모니터링이 가능하며 이에 따라 과금

II. 제공역량

1. 보안성(* 보안인증서 제출서비스는 1.2~1.5 제외)

검토 항목	1.2 침해사고 대응 절차 및 사후관리 대책
검토 내용	□ **클라우드컴퓨팅법, 정보통신망법 등 관련 법률에서 침해사고와 관련하여 요구하는 준수사항으로** 1) 침해사고 발생시 이용자에게 "통지의 내용 및 방법"을 명시하여 제시하고 있는가? 2) 침해사고에 효과적으로 대응하고 재발을 방지하기 위한 절차가 있는가?
검토 기준	▪ "침해사고 통지내용 및 방법"의 적정성 - 침해사고 통지방법, 침해사고 발생내용, 발생원인, 서비스 제공자의 피해확산 방지 조치 현황, 서비스 이용자의 피해 예방 또는 확산방지 방법, 담당부서 및 연락처 등을 포함하여 필수 제시 ▪ "침해사고 대응절차 및 사후관리 대책"의 적정성 - 침해사고 원인분석 및 대응절차, 재발 및 확산방지 대책, 주기적인 훈련 및 점검실시 계획 등을 포함하여 필수 제시 * 재발 및 확산방지 대책으로는 시스템 개선사항 및 보안교육 실시계획 등을 포함할 수 있음
증빙 문서명	▪ 침해사고 대응절차서(지침, 매뉴얼, 결재문서, 정보보호정책서 등) 등 해당내용을 증빙하는 공식문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 정보보호정책서 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 침해사고대응절차서)별로 제출도 가능**(단, 해당 검토영역의 풀본을 필수 제출)**
증빙 내용	**1. 침해사고시 통지의 내용 및 방법** - [참조 자료] 02. 침해사고관리지침_Ver 1.1 ③ 침해사고 발생 시 법률이나 규정 등에 따라 관계기관에 신고하여야 하며 개인정보와 관련한 침해사고는 이용자(정보주체)에게 신속하게 통지하여야 한다. 1. 통지방법 : 전화, 휴대전화, 전자우편, 서비스접속화면등 방법으로 제시함 2. 발생내용 3. 발생원인 4. 서비스 제공자의 피해확산 방지 조치 현황 5. 서비스 이용자의 피해예방 또는 확산방지 방법 6. 담당부서 및 연락처 **2. 침해사고 대응절차 및 사후관리 대책** - [참조 자료] 02. 침해사고관리지침_Ver 1.1 **제 8 조(침해사고 대응)** ① 정보보호 침해사고 접수 후 정보시스템별 담당자는 침해사고 유형별로 다음 각 호의 절차에 따라 대응한다. 1. 침해사고가 확대되지 않도록 침해당한 서버의 네트워크 분리, 공격 포트의 차단 등 필요한 응급조치를 먼저 취한다. 2. 침해사고의 확산을 막기 위해 해당 정보시스템의 중단이 통계청 전체 업무에 영향을 미치는 경우 업무시간 종료 후에 서비스를 중단하며, 해당 정보시스템의 중단이 일부 업무에 영향을 미치는 경우에는 해당 업무

부서와 협의 후 즉시 해당 정보시스템을 중단시킨다.

3. 응급조치 후 정보보호 침해사고의 원인 분석 및 증거확보를 위하여 해당 침해사고 관련 로그 및 제반 증거자료를 수집 및 확보해야 한다.

4. 국가정보원 등에서 권고하는 유형별 대응 조치를 취하고, 추후 재발방지를 위한 교육 등 대응책을 마련해야 한다.

② 정보보호 침해사고 유형에 따라 다음과 같이 구분한다.

1. 악성코드 공격
2. 서비스거부 공격
3. 비인가접근 공격
4. 복합구성 공격

제 13 조(사후관리)

① 정보보호 관리자는 유사한 사고의 재발 방지를 위하여 관련 정책 및 지침의 개정, 정보보호시스템 도입, 유관기관 협조체계 구축 등 효과적인 재발방지 대책을 수립하여야 하고, 필요 시 보안사고 대응절차에 대한 내용을 변경하여야 한다.

② 정보보호 관리자는 수립된 재발방지 대책을 보고하여 동일 또는 유사 사고의 재발에 대비하여야 하며 보안사고의 대응 및 복구가 완료되었음을 확인하여야 한다.

③ 정보보호 담당자는 1, 2 등급의 보안사고 관련된 기록을 대외비 이상 등급으로 분류하고, 이를 보존·관리하여야 한다.

④ 법적 또는 규정상 보안사고 관련하여 대외기관의 요청이 있는 경우 대외협력 관련부서는 정보보호 관리자와 협의 후 대응하여야 한다.

⑤ 정보보호 관리자는 보안사고에 대한 정보와 발견된 취약점들을 관련 부서 및 임직원들에게 공유 및 전파하여야 한다.

3. 관련업체 연락망

부서명	담당자	담당업무	연락처
NaverCloud(IT Security)	정보보호담당	정보보호 업무	1544-5876
NaverCloud	고객지원	고객지원	1833-5055
KT G-cloud	고객센터	고객센터 및 정보보호	080-2580-005

4. 관계기관 연락망

부서명	담당자	담당업무	연락처
KISA 해킹신고센터	해킹침해센터	해킹·스팸 개인정보 침해	118
대검찰청 사이버수사과	사이버수사과	해킹 및 개인정보 침해	02-3480-3570
경찰청 사이버안전국	사이버안전국	해킹 및 개인정보 침해	182

5. 담당부서 및 연락처

- 담당부서 : 클라우드팀

- 연락처

(정보보호 최고책임자) 조왕래 010-9655-5668

(정보보호 관리자) 김종룡 010-9162-8205

(정보보호 담당자) 김대회 010-5491-4744

6. 주기적인 훈련 및 점검실시 계획

- CSP사에서 아래와 같이 시행된 내역에 대한 보고서 전달받아 취약점 조치 및 상황전파

구분	주요 내용
훈련 대상	o 개인 정보를 대량으로 보유하고 있는 사이트 o 외부에서 접속 가능한 사이트
훈련 시기	o 연중 2회 이상
훈련 항목	o DDoS 공격 o SQL Injeciton 공격 o XSS 공격 o 포트, 웹스캔 공격 o 파일 업로드/다운로드 공격 o ID/PW 무작위 대입 공격 등

7. 물적보안 및 인적보안

- **물적보안 : OP관제실, CSP사의 침입탐지 장비 및 솔루션 서비스**

실

- **인적보안 : OP관제, 침해사고 발생으로 인한 비상연락망 및 운영팀 24시간 대기**

참조 자료	02. 침해사고관리지침_Ver 1.1

검토 항목	**1.3 개인정보·데이터 관리정책**
검토 내용	□ 개인정보의 암호화 등 안전한 전송·저장 여부 및 데이터보관, 반환 폐기 절차·정책, 국외이전 여부를 구체적으로 제시하고 있는가?
검토 기준	▪ "개인정보 암호화 조치"의 적정성을 제시 - 암호화대상 개인정보 종류 필수 제시 * 비밀번호·바이오정보·고유식별정보를 처리할 경우 암호화 대상으로 필수 포함하여야 함

	- 비밀번호는 단방향 암호화 조치함을 필수 제시 - 전송구간에 있어서 암호화(SSL)를 적용함을 필수 제시 - 암호화 대상별(비밀번호, 고유식별번호 등) 안전한 암호화 알고리즘을 적용함을 필수 제시(SEED, SHA224 이상 등) * 개인정보보호법 해설서(국내외 권고 알고리즘 적용) 참조 ※ 개인정보를 처리하지 않거나 암호화 대상이 없을 경우는 개인정보 처리하지 않고 있음과 암호화 대상여부가 없음을 반드시 명시 ※ "처리"란 개인정보 및 데이타의수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 의미 ▪ "데이터 반환 및 폐기 절차"의 적정성 - 데이터 반환 및 폐기 절차, 데이터 국외이전 여부, 데이터·서비스 처리 위치(국내/국외) 포함하여 필수 제시
증빙 문서명	▪ 개인정보처리방침, 개인정보관리정책, 개인정보보호계획서 등 해당내용을 증빙하는 공식문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 정보보호정책서 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 개인정보관리정책)별로 제출도 가능**(단, 해당 검토영역의 풀본을 필수 제출)**
증빙 내용	**1. 개인정보 암호화 조치** - [참조 자료] 03. 개인정보관리정책서_Ver 1.2 **4. 개인정보의 암호화** 개인정보는 암호화 등을 통해 안전하게 저장 및 관리되고 있습니다. 또한, 중요한 데이터는 저장 및 전송 시 암호화하여 사용하는 등의 별도 보안기능을 사용하고 있습니다. 1) 개인정보의 암호화 대상 - ㈜아이티아이즈는 업무상 개인정보를 인터넷을 통하여 외부로 송수신 할 경우 암호화(SSL)나 파일 패스워드 지정 등의 암호를 적용해야 한다. - 개인정보를 다루는 개인정보취급자는 시스템 또는 정보통신망 접속에 사용되는 비밀번호를 일방향 암호화하여 저장한다. - 개인정보취급자는 개인정보를 개인용컴퓨터(PC)에 저장 할 때 암호화 한다. - 시스템 개발 시 개발담당자는 암호 및 인증시스템에 적용되는 키에 대하여 주입, 운용, 갱신, 폐기에 대한 절차 및 방법에 따라 안전하게 관리한다. - 운영 시스템의 암호 및 인증시스템에서 이용하고 있는 키와 테스트 시스템에서 테스트용으로 사용되고 있는 키는 동일한 키를 사용하지 않아야 한다. - 모든 개인정보에 대하여 안전하게 보호하기 위한 암호 알고리즘을 선정해야 한다. 2) 암호화 범위 및 안전한 암호화 알고리즘 사용 - ㈜아이티아이즈가 보유하고 있는 고객의 고유식별정보(주민등록번호, 계좌번호, 신용카드 번호등)는 AES-128 또는 SEED-128 이상 암호화 알고리즘을 이용한다. - 개인정보 및 인증정보를 송수신 할 경우 보안서버 구축(SSL) 등의 조치를 통한 암호화 하여야 한다. - 서비스 이용자 및 내부 임직원 비밀번호 저장 시 단방향(해쉬) 방식의 암호화 알고리즘을 이용하며 SHA-256 이상 암호화 알고리즘을 이용한다. **2. 데이터 반환 및 폐기 절차**

- [참조 자료] 03. 개인정보관리정책서_Ver 1.2

제 11 조(개인정보 파기)

① 보유기간의 경과, 개인정보의 처리 목적 달성 시 지체없이 파기하여야 한다.

② 개인정보를 파기할 때에는 복원이 불가능한 방법으로 개인정보를 파기하여야 한다.

③ 개인정보를 파기한 경우에는 개인정보 파기에 관한 사항을 기록하여 관리하고 개인정보 보호관리자는 파기 결과를 확인하여야 한다.

제 7 조(개인정보 파기 절차 및 방법)

① ㈜아이티아이즈는 원칙적으로 개인정보 처리목적이 달성된 개인정보는 지체없이 파기합니다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 않을 수 있습니다. 파기의 절차, 기한 및 방법은 다음과 같습니다.

가. 파기절차

불필요한 개인정보 및 개인정보파일은 개인정보 보호관리자의 책임하에 내부절차에 따라 다음과 같이 처리하고 있습니다.

- 개인정보의 파기

보유기간이 경과한 개인정보는 종료일로부터 지체없이 파기합니다.

- 개인정보파일의 파기 개인정보파일의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보파일이 불필요하게 되었을 때에는 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 지체없이 그 개인정보파일을 파기합니다.

나. 파기방법

1) 전자적 형태의 정보는 기록을 재생할 수 없는 기술적 방법을 사용합니다.

2) 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기합니다.

3. 데이터 처리 위치 및 국외이전 여부

- [참조 자료] 03. 개인정보관리정책서_Ver 1.2

제 2 조(수집하는 개인정보항목)

① ㈜아이티아이즈에서 개인정보를 수집하여 처리하고 있습니다. 이용자의 개인정보를 수집하는 경우에는 반드시 사전에 이용자에게 해당 사실을 알리고 동의를 구하도록 하겠습니다.

1. 고객지원

구분	수집항목	수집시점
고객지원	[필수] 이름, 이메일, 휴대폰	고객지원 서비스 제공시

2. 네이버클라우드 서비스제공

구분	수집항목	수집시점
NAVER Cloud	[필수] LoginID, 대표자명, 대표전화, 담당자명, 이메일, 휴대폰, 주소, 담당자이메일, 청구서이메일	네이버 클라우드 서비스 가입시

3. KT Cloud 서비스제공

구분	수집항목	수집시점
KT Cloud	(필수) 성명, 아이디, 이메일 주소, 연락처, 업종 (선택) 이메일 주소, 휴대전화 번호	회원가입
	[기본정보] - 이름, 생년월일 [청구정보] 이메일주소(이메일로 청구를 받을 경우), 청구지주소,	결제 정보
	지번주소, 도로명 주소, 휴대전화번호, 유선전화번호 [결제 방법] 신용카드의 경우 : 생년월일, 카드소유자명, 카드번호, 카드만료일 자동이체의 경우 : 생년월일, 계좌번호, 예금주명	
	회신 이메일, 휴대전화번호, 첨부파일	문의
	휴대전화번호, 이메일	정보 추가
	(필수) 이름, 이메일, 전화번호 (선택) 첨부파일	교육 및 지원 프로그램
	(필수) 신청인의 업체명, 담당자명, 휴대전화번호, 일반전화번호, e-mail 주소, 소재지 (선택) 사업자 등록번호	컨설팅 신청
	아이디(이메일 주소), 사용자 이름, 휴대전화번호, 마케팅 담당자명, 마케팅 담당자 휴대전화번호, 마케팅 담당자 이메일, 영업 담당자명, 영업 담당자 휴대전화번호, 영업 담당자 이메일	제휴사 회원가입

제 4 조(개인정보의 위탁 및 국외이전)

① ㈜아이티아이즈는 이용자 동의 없이 개인정보를 위탁 및 국외이전하지 않습니다. 향후, 필요 시 위탁 및 국외이전 내용에 대해 이용자에게 통지하고 사전 동의를 받도록 하겠습니다.

② 개인정보의 처리를 위탁하는 경우에는 개인정보 보호의 안전을 기하기 위하여 개인정보보호 관련 지시엄수, 개인정보에 대한 비밀유지, 제3자 제공의 금지 및 사고시의 책임부담, 위탁기간, 처리 종료 후의 개인정보의 반환 또는 파기 등을 명확히 규정하고, 위탁업체가 개인정보를 안전하게 처리하도록 감독합니다.

③ 업체, 위탁하는 업무의 내용이 변경될 경우, 웹사이트 공지사항(또는 서면·이메일·전화·SMS 등의 방법으로 개별공지)을 통하여 알려드리겠습니다.

1. 개인정보 위탁업무 내용

수탁업체	제공목적(위탁업무 내용)	보유 및 이용 기간
NAVER Cloud	네이버 클라우드 서비스 제공목적	회원탈퇴 또는 위탁계약 종료시 까지
KT Cloud	KT Cloud 서비스 제공목적	회원탈퇴 또는 위탁계약 종료시 까지
NHN Cloud	NHN Cloud 서비스 제공목적	회원탈퇴 또는 위탁계약 종료시 까지

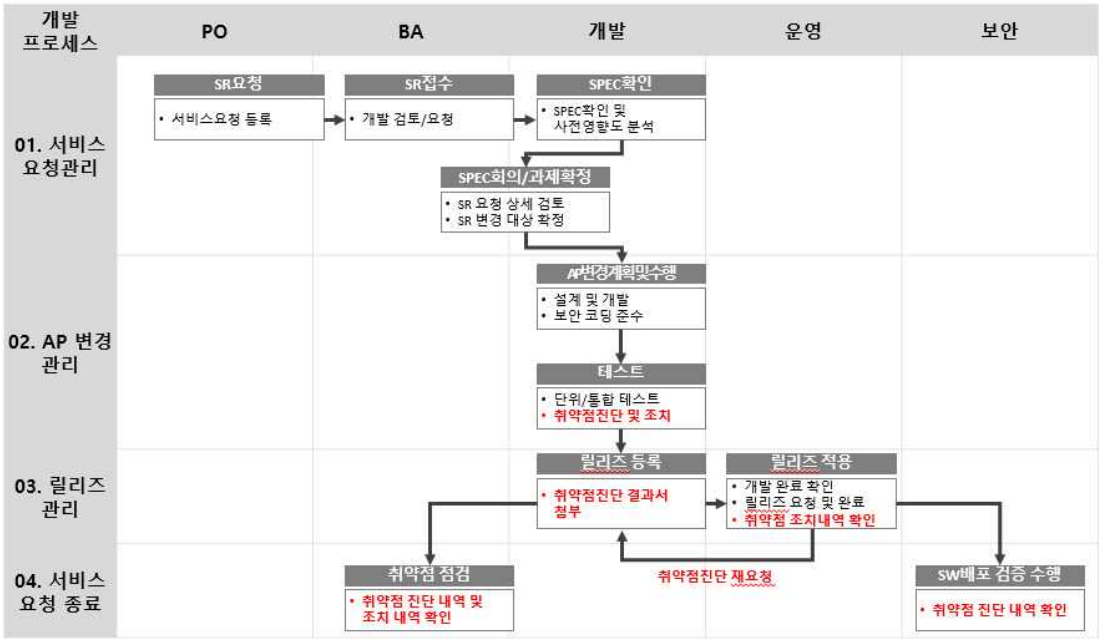
참조 자료	클라우드법 시행령 제17조(통지의 내용 및 방법), 정보통신망법 제48조의3(침해사고의 신고), 제48조의4(침해사고원인분석)

.검토 항목	**1.4 안전한 코딩방법**
검토 내용	□ 안전한 코딩방법에 따라 구현될 수 있는지 확인할 수 있는 점검방법과 점검절차 등 점검체계를 제시하고 있는가?
검토 기준	▪ "시큐어코딩" 점검계획 수립 여부 및 그 내용의 적정성 확인 - 점검방법(수행주체, 점검 툴 등 포함), 점검시기, 점검결과에 따른 조치사항 등을 포함하여 필수 제시 * 별도의 점검 툴 없이 전문인력을 활용할 경우에는 해당 내용을 명기 * 다만, 기술적 보안 취약점 점검에 있어서 신청한 서비스 특성 및 운영 상황을 고려하여 적합한 점검방법 및 점검기준을 적용
증빙 문서명	▪ 정보보호정책서, SW개발보안지침, 시큐어코딩 점검계획서 및 조치 결과보고서 등 해당 내용을 증빙하는 공식 문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 정보보호정책서 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 시큐어코딩 정책)별로 제출도 가능**(단, 해당 검토영역의 풀본을 제출)**
증빙 내용	- 진단 Rule - 점검 도구 : Sparrow

구분	취약점	내용
보안	Path Manipulation	시스템 중요파일(password, 소스코드 등)에 접근하여 시스템 침탈 가능
	SQL Injection	DB 공격하여 비인가 정보 획득, 데이터 변조 가능
	Cross-Site Scripting	페이지 가로채기, 바이러스 설치, 백도어 등의 스크립트 공격 가능
	HTTP Response Splitting	
	Trust Boundary Violation	프로그램 내부 데이터 조작 공격
	Unchecked Return Value : Missing Check against Null	시스템 간접정보 획득 및 프로그램 오동작 가능
	J2EE Misconfiguration : Missing Error Handling	시스템 간접정보 획득 가능성
품질	Poor Style : Redundant Initialization	이 변수 값은 할당되어 있지만 사용하지 않으므로 불필요한 저장 공간을 차지합니다
	Poor Style : Value Never Read	
	Redundant Null Check	프로그램이 null 포인터를 역 참조할 가능성이 있기 때문에 null 포인터 예외가 발생합니다
	Unreleased Resource : Database	프로그램이 시스템 리소스를 해제하지 못할 수도 있습니다
	Unreleased Resource : Stream	
	Dead Code : Expression is Always True	이 식은 항상 true 가 됩니다
	Dead Code : Unused Field	이 필드는 사용되지 않습니다

- 점검 시기 : 서비스 오픈, SR/릴리즈 등 보안검토 필요한 경우 수시 점검 진행

- Secure coding : SW개발 보안 프로세스



- [참조 자료] 1-4. 안전한 코딩지침_Ver 1.0

제2장 웹 시큐어코딩 점검

제 4조 웹 시큐어코딩의 개요

웹 소프트웨어 개발시 소프트웨어의 보안약점을 최소화하기 위해 웹 시큐어코딩 점검 지침을 제시한다.

제 5조 대상 점검 범위 및 점검 시기

① 대상 점검 범위는 웹애플리케이션 서비스를 제공하기 위한 소프트웨어 소스를 말하며, 해당소스는 Java 또는 C언어로 이루어진 점검기준을 제공한다.

② 해당 소프트웨어의 단위 테스트, 통합 테스트 시기에 점검 도구를 이용하여 점검을 진행한다.

제6조 Java기반 시큐어코딩 점검 기준

① Java언어로 개발된 웹은 아래의 보안 약점 항목들을 기준으로 검사를 실시한다.

1. 입력데이터 검증 및 표현은 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점(총 26 개)을 말한다.
2. 보안기능은 보안기능(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 적절하지 않게 구현시 발생할 수 있는 보안약점(총24개)을 말한다.
3. 시간 및 상태는 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안약점(총 7개)을 말한다.
4. 에러처리는 에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점(총4개)을 말한다.
5. 코드오류는 타입변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점(총 7개)을 말한다.

6. 캡슐화는 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않는 사용자에게 데이터 누출이 가능해지는 보안약점(총8개)을 말한다.

7. API오용은 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점(총7개)을 말한다.

제7조C기반 시큐어코딩 점검 기준

① C 언어로 개발된 웹은 아래의 보안 약점 항목들을 기준으로 검사를 실시한다.

1. 입력데이터 검증 및 표현은 프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점(총 19 개)을 말한다.

2. 보안기능은 보안기능(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 적절하지 않게 구현시 발생할 수 있는 보안약점(총17개)을 말한다.

3. 시간 및 상태는 동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 잇는 보안약점(총 3개)을 말한다.

4. 에러처리는 에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점(총 3개)을 말한다.

5. 코드오류는 타입변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점(총 2개)을 말한다.

6. 캡슐화는 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않는 사용자에게 데이터 누출이 가능해지는 보안약점(총 2개)을 말한다.

7. API 오용은 의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점(총 5개)을 말한다.

제 8조 웹 시큐어 코딩 점검 도구

웹 시큐어 코딩 점검에 사용할 점검 도구를 제시한다. 각 도구의 점검 유형은 [첨부 1]을 참조하여 점검도구 선정한다.

① Spotbugs(SpotBugs Team, LGPL라이센스, 정적 분석을 통해 코드에서 버그를 찾는 툴)

② FindSecurityBugs(SpotBugs Team, LGPL라이센스, Spotbugs의 기능 확장용 소프트웨어)

③ PMD(PMD,BSD 라이선스, 정적 분석을 통해 코드에서 버그를 찾는 툴)

④ Jenkins(키와쿠지 코스케 제작, 진단결과를 보고하는 오픈 소스 Continuous Integration 툴)

제 9조 웹 시큐어 코딩 점검절차

① 요구사항(보안 요구사항)는 오용사례와 위험분석으로 설계보안항목에 대한 정의와 명세를 작성하고, 오용사례에 대한 정의 및 케이스 예시를 작성한다.

② 구조 설계(위험 분석)절차는 공격저항 분석(attack resistance analysis), 모호성 분석, 허점 분석 등으로 위험요소를 분석한다.

③ 테스트 계획는 공격 패턴, 위험 분석 결과, 악용 사례를 기반으로 위험기반 보안테스트를 수행한다.

④ 코드 검토 절차는 구현 오류(implementation bug)에 중점을 두며 특히 소스코드에 존재하는 취약성을

발견할 목적으로 수행되는 코드 정적분석에 중심을 둔다.

⑤ 테스트/테스트 결과(위험분석)는 위험 분석 및 침투 테스트를 수행한다. 침투테스트로 실제 작동 환경에서의 필드 소프트웨어에 대한 좋은 이해를 제공한다.

⑥ 현장과의 피드백절차에서는 보안 운영으로 얻은 공격자와 공격 도구에 대한 경험과 지식은 개발자에게 다시 피드백한다.

제 10 조 웹 시큐어 코딩 조치 후 사후점검

① 현장의 담당자는 점검 체크리스트[첨부 2]를 근거하여 조치 후 관리자에게 다시 보고한다

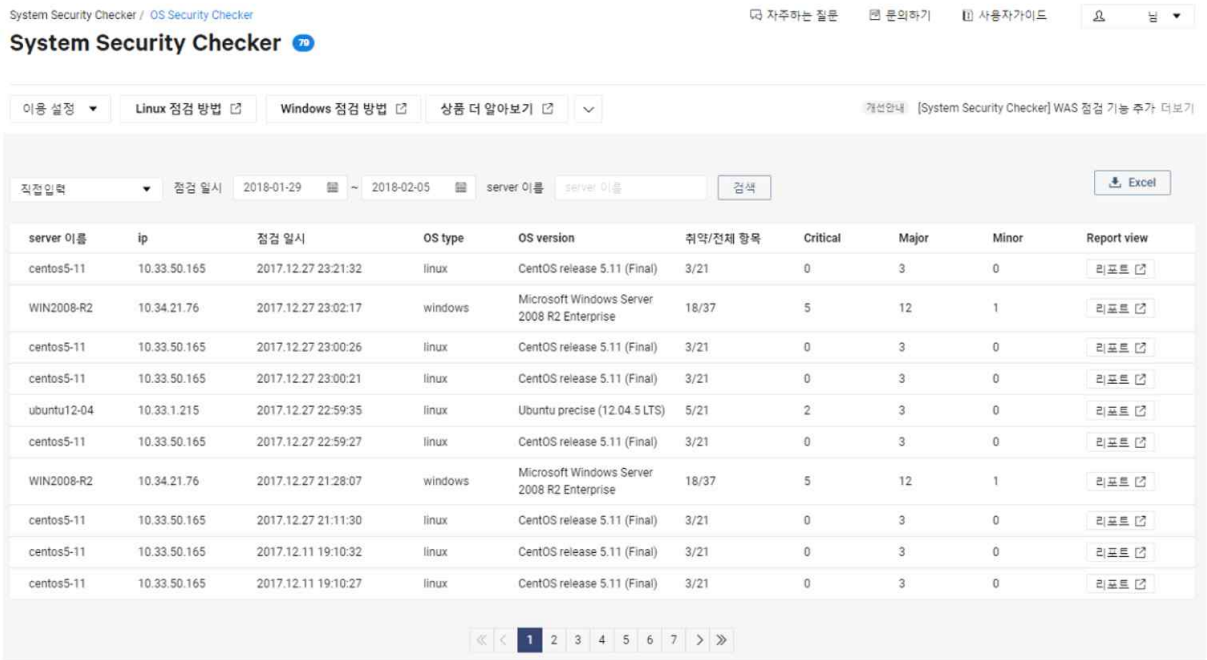
[첨부 2] 웹 시큐어코딩 체크리스트

① Java

유형	체크사항	체크 여부
입력 데이터 검증 및 표현	데이터베이스와 연동된 웹 어플리케이션에서 입력된 데이터에 대한 유효성 검증 절차가 있는가	
	시스템 자원에 대한 식별자로 사용하는 경우 외부 입력값을 검증 절차가 있는가	
	외부 입력 내용이 동적 웹 페이지 생성에 사용될 경우 입력 내용에 검증 절차가 있는가	
	사용자 입력값이 운영체제 명령어의 일부 또는 전부로 구성되어 실행될 때 검증절차가 있는가	
	위험한 형식의 파일이 업로드가 실행되지 않도록 업로드에 제한이 있는가	
	신뢰되지 않는 url 주소 접속을 제한하는 절차가 있는가	
	XQuery 를 사용하여 xml 데이터에 대한 동적 쿼리문을 생성할 때 사용자의 외부 입력값에 대한 검증절차가 있는가	
	XPath 쿼리문 생성할 때 사용자의 외부 입력값에 대한 검증절차가 있는가	
	LDAP 명령어를 수행할 때 외부 입력값에 대한 검증절차가 있는가	
	사용자로부터 받은 요청에 대해서 사용자가 의도한 대로 작성되고 전송된 것인지 확인하는 절차가 있는가	
	외부 입력값에 대하여 디렉터리 경로 조작 문자열 검증절차가 있는가	
	HTTP 요청에 들어 있는 인자값을 검증하는 절차가 있는가	
	사용자의 입력값(정수)이 변수의 값 범위에 포함되는지 검증하는 절차가 있는가	
	보호 메커니즘을 우회하는 입력값 변조를 막는 절차가 있는가	
	Java Data Objects API 를 이용한 검사과정을 거치지 않는 문자열을 검증하는 절차가 있는가	
	J2EE Persistence API 를 이용한 검사과정을 거치지 않는 질의문을 검증하는 절차가 있는가	
	외부에서 입력된 값이 질의 명령어에 연결되는 문자열로 사용되지 않게 검증하는 절차가 있는가	
	외부에서 입력된 값이 LDAP 질의문의 내용을 변경되지 않게 검증하는 절차가 있는가	
	외부에서 시스템 설정이나 구성요소를 제어 할 수 없게 막아져 있는가	
	외부에서 입력되는 스크립트 문자열이 웹 페이지 생성에 사용되지 않게 검증하는 절차가 있는가	
	외부에서 입력되는 내용이 스크립트 또는 프로그램 명령어 문자열 생성에 사용되지 않게 검증하는 절차가 있는가	
	프로그램 내에서 라이브러리를 적재할 때 절대 경로를 사용하는가	
	외부의 입력되는 내용에서 의도하지 않은 클래스가 적재되지 않게 검증하는 절차가 있는가	
	원격으로 소스 코드 또는 실행파일을 다운로드 했을 때 무결성 검사를 하는 절차가	

참조 자료

- 소프트웨어 개발보안 가이드(행정안전부, 2019.11.)
- 소프트웨어 보안약점 진단가이드(행정안전부, 2019.6.)
- 공개소프트웨어를 활용한 소프트웨어 개발보안 진단 가이드(행정안전부, 2019.6.)
- https://www.kisa.or.kr/public/laws/laws3.jsp 참조

검토 항목	**1.5 취약점 점검 및 조치**
검토 내용	☐ 서비스 SW 및 개발·운영환경 보안 취약점 점검방법을 제시하고 있는가?
검토 기준	▪ 취약점 점검 및 조치계획의 적정성 확인 - 취약점 점검시기, 점검결과에 따른 조치사항, 주기적인 점검계획 등을 포함하여 필수 제시 * 취약점 제거 등 보안조치 수행에 있어서도, 예를 들어 취약판단을 받아도 그 위험을 최소화할 수 있는 합당한 조치와 근거를 제시할 수 있음
증빙 문서명	▪ 정보보호정책서, 보안취약점 점검계획서 등 해당 정책 내용을 증빙하는 공식 문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 정보보호정책서 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 취약점 점검계획서)별로 제출도 가능**(단, 해당 검토영역의 풀본을 제출)**
증빙 내용	- 취약점 점검 : KISA 보안가이드 기준 취약점 점검 및 조치를 수행하고있으며, CSP 점검툴을 이용하여 담당 엔지니어가 점검 진행 - 취약점 조치 : 점검 결과 리포트를 고객사 및 대상 시스템 담당자에게 공유하고 영향도 파악 후 담당 엔지니어가 조치 진행 - NCP 취약점 점검 기록 

System Security Checker / OS Security Checker

자주하는 질문 문의하기 사용자가이드 님

System Security Checker 70

이용 설정 Linux 점검 방법 Windows 점검 방법 상품 더 알아보기 개선안내 [System Security Checker] WAS 점검 기능 추가 더보기

직접입력 점검 일시 2018-01-29 ~ 2018-02-05 server 이름 server 이름 검색 Excel

server 이름	ip	점검 일시	OS type	OS version	취약/전체 항목	Critical	Major	Minor	Report view
centos5-11	10.33.50.165	2017.12.27 23:21:32	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
WIN2008-R2	10.34.21.76	2017.12.27 23:02:17	windows	Microsoft Windows Server 2008 R2 Enterprise	18/37	5	12	1	리포트
centos5-11	10.33.50.165	2017.12.27 23:00:26	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
centos5-11	10.33.50.165	2017.12.27 23:00:21	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
ubuntu12-04	10.33.1.215	2017.12.27 22:59:35	linux	Ubuntu precise (12.04.5 LTS)	5/21	2	3	0	리포트
centos5-11	10.33.50.165	2017.12.27 22:59:27	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
WIN2008-R2	10.34.21.76	2017.12.27 21:28:07	windows	Microsoft Windows Server 2008 R2 Enterprise	18/37	5	12	1	리포트
centos5-11	10.33.50.165	2017.12.27 21:11:30	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
centos5-11	10.33.50.165	2017.12.11 19:10:32	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트
centos5-11	10.33.50.165	2017.12.11 19:10:27	linux	CentOS release 5.11 (Final)	3/21	0	3	0	리포트

« ‹ 1 2 3 4 5 6 7 › »

- NCP 취약점 점검 결과 리포트

Summary

Server Information

Server	
Region	KR
Hostname	centos5-11
IP	10.33.50.165
OS	linux
OS Version	CentOS release 5.11 (Final)
Security Checker	
Project name	linux
Script version	2.0.0
Checked date	2017.12.27 23:21:32

Check Result

Summary

Total	Good	Critical	Major	Minor
21	18	0	3	0

Details

LAC-01

Title	root 계정 원격 접속 제한
Risk level	Major
Mitigation level	High
Description	root 계정은 시스템을 관리하는 매우 중요한 계정입니다. 직접 로그인하도록 허용하면 불법적인 침입자의 목표가 될 수 있습니다. root 계정을 탈취하려는 무작위 대입 공격이 빈번히 발생하고 있습니다. root 계정의 원격 접속을 제한하고, 사용자가 생성한 별도의 사용자 계정으로 로그인한 뒤 su 명령을 이용하여 root 권한으로 변경하여 작업하는 것이 안전합니다.
Recommended setting and judgment judgment criteria	/etc/securetty 파일 내에 console, tty1, tty2 vc/1, vc/2만 존재하는 경우 점수 부여
Current setting	
Mitigation method	"/etc/securetty" 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리

BAD

LAC-05

Title	Password 최장 사용기간 설정
Risk level	Major
Mitigation level	Medium
Description	사용자의 비밀번호는 자주 변경하는 것이 중요합니다. 동일한 비밀번호를 오래 사용하면, 이전에 발생한 외부 침입으로 인해 노출된 비밀번호로 지속적인 공격에 노출됩니다. 사용자가 비밀번호를 주기적으로 변경할 수 있도록 정책적으로 유도하는 것이 바람직합니다.
Recommended setting and judgment judgment criteria	/etc/login.def 파일 내에 "PASS_MAX_DAYS"의 값이 100 이하로 설정된 경우 점수 부여
Current setting	PASS_MAX_DAYS 120
Mitigation method	1. vi 편집기를 이용하여 "/etc/login.defs" 파일을 연 후 2. 아래와 같이 수정 또는, 신규 삽입 (수정 전) PASS_MAX_DAYS 99999 (수정 후) PASS_MAX_DAYS 100 (단위: 일)

BAD

LAC-09

Title	Session Timeout 설정
Risk level	Major
Mitigation level	Medium
Description	계정이 접속된 상태로 방치될 경우 권한이 없는 사용자에게 중요시스템이 노출되어 악의적인 목적으로 사용될 수 있습니다. 일정 시간동안 어떠한 이벤트도 발생하지 않으면, 연결을 강제 종료하는 Session Timeout 설정이 필요합니다.
Recommended setting and judgment judgment criteria	/etc/profile 파일 내에 "TMOUT = 32400" 설정이 존재하는 경우 점수 부여(32400 이하 값도 인정)
Current setting	TMOUT=324000
Mitigation method	1. vi 편집기를 이용하여 "/etc/profile(.profile)" 파일을 연 후 2. 아래와 같이 수정 또는, 추가 TMOUT=600 (단위: 초) export TMOUT

BAD

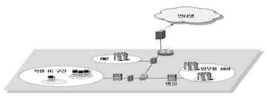
- KTDS 취약점 진단 및 조치 계획

- **점검 주체 : KT DS 정보보안센터 보안정책팀**
- **담 당 자 : 조명기 차장 010-8884-7240**
- **점검 시기 : 연 1회 정기점검. 서비스 오픈, ITO전환 등 필요한 경우 수시 점검 진행**
- **점검 도구 : Solidstep**
- **소스 진단결과**
- **인증 내역 : GS인증서 / 정보보호 전문서비스 기업 지정서**

분류	코드	항목	위험도
서비스관리	TOM-101	관리자 콘솔 접근 제한 설정	중
계정관리	TOM-201	관리자 콘솔 계정명 변경	중
계정관리	TOM-202	관리자 콘솔 패스워드 관리	상
권한관리	TOM-203	관리자 콘솔 패스워드 파일 권한 설정	중
권한관리	TOM-204	프로세스 권한 제한	중
권한관리	TOM-301	설정 파일 쓰기 권한 제거	중
권한관리	TOM-302	소스 파일 쓰기 권한 제거	중
시스템보안설정	TOM-401	사용자 오류 페이지 설정	중
시스템보안설정	TOM-402	디렉토리 검색 기능 제거	상
파일및디렉토리관리	TOM-403	불필요한 파일 제거	하
시스템보안설정	TOM-404	불필요한 프로세스 관리 디렉토리 삭제	중
로그관리	TOM-405	접근로그 설정 관리	하
권한관리	TOM-406	로그 디렉토리 및 파일의 권한 제한	하
패치관리	TOM-501	아파치 스트럿츠(Apache Struts) 최신 보안 패치 및 벤더 권고사항 적용	상
패치관리	TOM-502	최신 보안 패치 및 벤더 권고사항 적용	상
시스템보안설정	TOM-503	SSL v3.0 POODLE 취약점	상

진단 계획 수립

구축 시스템의 진행 현황을 고려하여 진단대상, 일정 수립



점검 방안 확정

스크립트, 체크리스트를 기반으로 점검 방안 확정

진단 수행

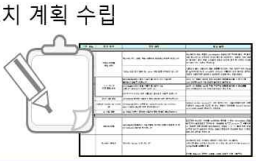
진단대상 특징 및 수량에 따라 수동진단 또는 자동진단 수행

점검결과 정리 및 보고

진단 결과를 정리, 분석하여 오탐 분류 및 조치 대상 보고

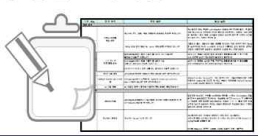
조치계획 수립

진단 결과의 취약점에 대한 조치 방안 및 조치 계획 수립



조치 이행

조치 계획에 따라 이행 점검하여 미흡사항 완전 조치 확인



- KTDS CSAP 인증서

CSAP-2016-001호

인 증 서

업체명 : ㈜케이티클라우드 대표자 : 윤 동 식

인증서비스 명칭 : KT G-Cloud (IaaS)

인증의 범위 : IaaS / 14개 분야 117개 항목

인증유효기간 : 5년 (2021. 10. 20. ~ 2026. 10. 19.)

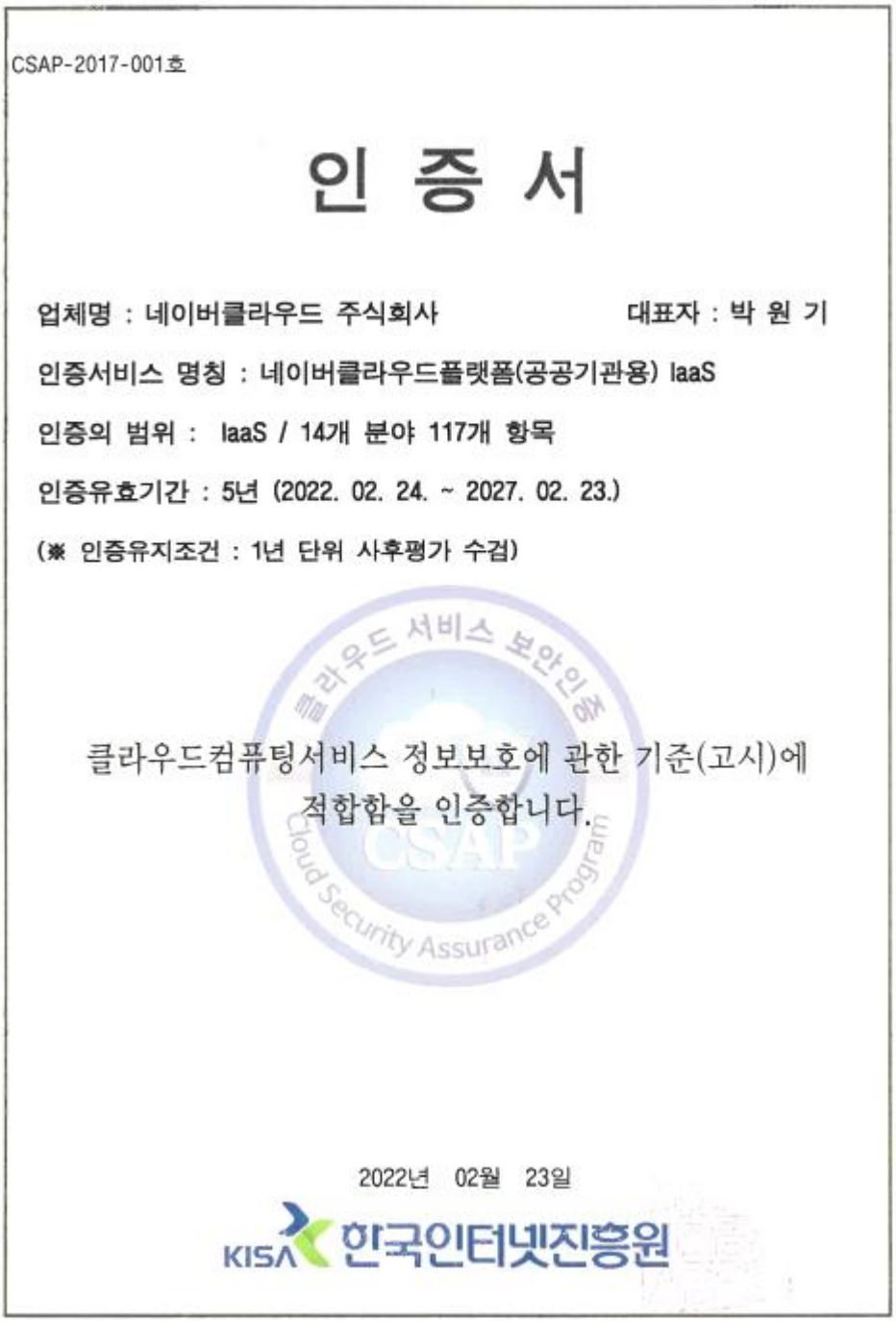
(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에
적합함을 인증합니다.

2022년 4월 5일

KISA 한국인터넷진흥원

- NCP CSAP 인증서



CSAP-2017-001호

인 증 서

업체명 : 네이버클라우드 주식회사 대표자 : 박 원 기

인증서비스 명칭 : 네이버클라우드플랫폼(공공기관용) IaaS

인증의 범위 : IaaS / 14개 분야 117개 항목

인증유효기간 : 5년 (2022. 02. 24. ~ 2027. 02. 23.)

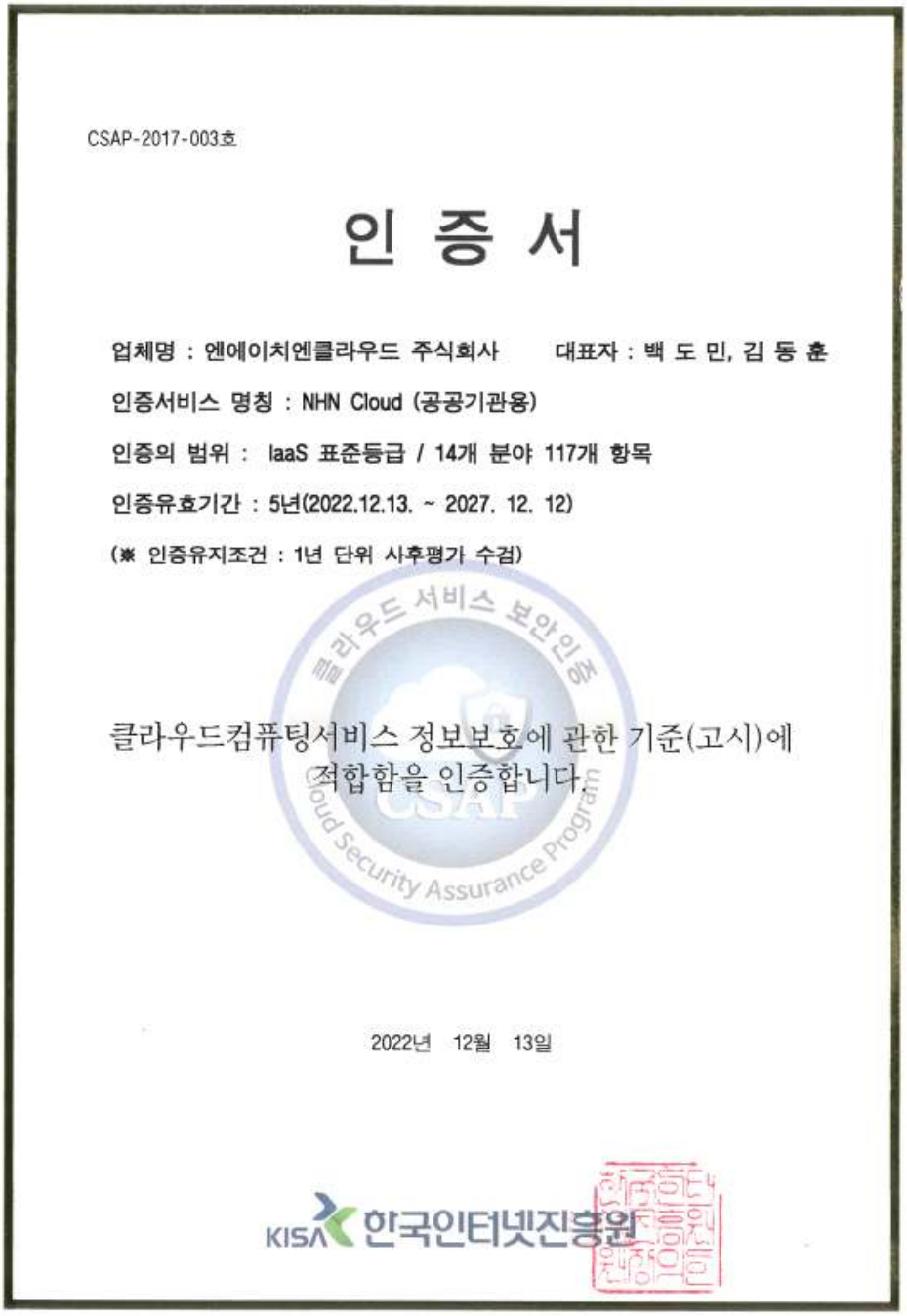
(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에
적합함을 인증합니다.

2022년 02월 23일

KISA 한국인터넷진흥원

- NHN 취약점 진단 및 조치 계획은 CSAP 인증서로 대체



CSAP-2017-003호

인 증 서

업체명 : 엔에이치엔클라우드 주식회사 대표자 : 백 도 민, 김 동 훈

인증서비스 명칭 : NHN Cloud (공공기관용)

인증의 범위 : IaaS 표준등급 / 14개 분야 117개 항목

인증유효기간 : 5년(2022.12.13. ~ 2027. 12. 12)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드 서비스 보안인증 CSAP Cloud Security Assurance Program

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에
적합함을 인증합니다.

2022년 12월 13일

KISA 한국인터넷진흥원

[첨부 1] 웹 취약점 사후 조치보고서

점검사항	점검결과	조치여부	조치확인	비고
크로스 사이트 스크립팅				
삽입 취약점				
악성 파일 실행				
불안전한 직접객체 참조				
크로스 사이트 요청 참조				
정보유출 및 부적절한 오류처리				
취약한 인증 및 세션 관리				
불안전한 암호화 저장				
불안전한 통신				
URL 접근제한 실패				
디렉토리 리스팅				
부적절한 환경 설정				
파일 다운로드				
파일 업로드				
백업파일 노출				
입력값 검증 부재				
쿠키(Cookie) 암호화				
취약한 접근 통제				
서비스 거부 공격				
버퍼 오버플로우				
가짜 액티브(Active) X 확인하기				
티맥스 WAS(JEUS) 취약점				

참조 자료

- 소프트웨어 보안약점 진단가이드(행정안전부, 2019.6.)
- 모바일 대민서비스 보안취약점 점검 가이드(행정자치부, 2015.12.)
- 기술적 취약점 분석평가 방법 상세가이드(과학기술정보통신부, 2017.12)
- OWASP "OWASP Top 10", https://www.kisa.or.kr/public/laws/laws3.jsp 참조

II. 제공역량

2. 운영 안정성

검토 항목	**2.1 가용률**
검토 내용	□ 가용률 보장정책(보상조건, 산정방식)을 제시하고 있는가?
검토 기준	▪ IaaS, PaaS : 99.9% 이상 가용률 목표수준 및 보장정책 필수 제시(보상조건 및 산정방식 포함) ▪ SaaS : 99.5% 이상 가용률 목표수준 및 보장정책 필수 제시(보상조건 및 산정방식 포함) ▪ 그 외 서비스 : 가용률 목표 수준 및 보장정책 필수 제시(보상조건 및 산정방식 포함) * 가용률이란 정해진 서비스 운영 시간(예정된 가동시간) 대비 클라우드컴퓨팅서비스에 접속 가능한 시간의 비율
증빙 문서명	▪ SLA 정책서, 서비스 이용약관 등 해당 내용을 증빙하는 공식 문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 이용약관 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : SLA정책서)별로 제출도 가능**(단, 해당 검토영역의 풀본을 제출)**
증빙 내용	제 1장 총칙 제1조 목적 이 서비스수준협약(Service Level Agreement, 이하 SLA)은 "고객"의 운영관리(매니지드) 서비스 대상에 대한 모니터링, 장애 접수/처리, 예방 점검 활동을 통한 시스템 가동률 및 서비스 향상을 목적으로 한다. 제2조 목표수준 목표수준은 클라우드센터와 협의하여 결정한다. 제3조 용어의 정의 ① "장애"란 가동 중인 고객의 인스턴스 또는 태스크가 모두 외부 연결을 확보하지 못하는 경우를 말한다. ② "장애 시간"이란 해당 월 동안 장애가 발생한 시간의 총합을 말한다. 단, 본 SLA의 적용이 배제되는 경 우에 그 해당 시간은 장애 시간에 포함되지 않는다. ③ "월 가용률"이란 다음과 같다. 장애 시간의 합(분 단위) 월 가용률(%) = 100x{1 −} 해당 월의 총 시간(분 단위) ④ "월 이용요금"이란 장애가 발생한 해당 월의 본 서비스에 대하여 고객이 회사에 실제 지급하는 금액을 의미한다. ⑤ "운영관리(매니지드) 서비스"란 고객의 클라우드 인프라 시스템을 운영 및 관리하는 IT 운영 서비스를 의미한다 제 5 장 운영관리(매니지드) 서비스 제 19 조 용어의 정의 ① "운영관리(매니지드) 서비스(Managed Service)"라 함은 회원이 인터넷 서비스를 하기 위해 클라우드 컴퓨팅 서비스 내에서 운영하는 서버 및 네트워크 장비의 시스템을 운영/관리해주는 서비스를 의미

	한다. 제 20 조 서비스의 종류 및 범위 회사가 제공하는 기술 지원 서비스는 Linux 및 Windows Server, 기타 IT 기기들을 대상으로 24 시간 365 일 시스템 모니터링 및 상태 체크 서비스가 제공된다. 단, 회원의 웹사이트 운영 및 프로그램, HTML 과 관계 있는 DB/CGI/Script 파일 내용은 서비스 대상이 아니며 시스템 운영 및 관리와 직접 관련이 없는 홈페이지 콘텐츠 및 프로그램 오류에 관한 사항 역시 서비스 대상이 아니다. ① 서비스의 종류 및 범위 1. 운영관리(매니지드) 서비스의 종류에 따른 서비스 범위는 각 종류별(등급별) 개별 부가 서비스의 범위는 각 종류별(등급별) 개별 부가 서비스의 서비스 내용을 따르며 그 내용은 해당 부가 서비스의 약관에 준한다. 2. 운영관리(매니지드) 서비스는 각 부가 서비스를 서비스의 종류(등급)에 따라 통합시킨 패키지 형태의 서비스이다. ② 이 약관에서 사용하는 용어 중 제 15조에서 정하지 아니한 것은 관계 법령 및 서비스별 안내에서 정하 는 바에 따르며, 그 외에는 일반 관례를 따른다. 제 21 조 이용 계약의 단위 회사의 모든 서비스에서 제공되는 시스템(서버 또는 하드웨어)이 기본 단위이며, 기본 단위별(VM 가상 머신 1 대당)로 운영관리(매니지드) 서비스 요금이 각각 합산된다. 제 22 조 서비스 이용요금 ① 서비스 종류별로 서비스 요금이 달리 부과될 수 있다. ② 운영관리(매니지드) 서비스에 포함되지 않은 별도 추가지원 사항에 대해서는 기타 지원 서비스의 가격에 따라 개별 요금 부과된다. ③ 회사는 이용요금 납입 위한 청구서를 서비스 이용요금 청구와 함께 회원에게 발송하며, 회원은 청구일 (공휴일인 경우 익일)까지 요금을 납입하여야 한다. ④ 체납한 이용 요금이 있는 경우 익월 이용 요금에 합산하여 청구하고, 이용약관에 따른 가산금을 부과할 수 있다. 제 23 조 면책사항 회사는 다음 각호의 사유에 의해 회원에게 손해가 발생한 경우 회원에게 손해배상 책임을 부담하지 않는다. 1. 회원이 직접 구입한 단말장치의 불량으로 서비스 장애가 발생한 경우 2. 전시, 사변, 화재, 천재지변 또는 이에 준하는 국가비상사태 등 불가항력적인 경우 3. 회원의 고의나 과실로 인해 발생한 경우 4. 전기통신서비스의 특성상 불가피한 사유가 있는 경우 5. 회원의 정보시스템에 발생한 사고의 확산을 방지하기 위한 서비스 중단 6. 서비스의 장애가 타 사업자가 제공하는 서비스에 의한 경우

7. 서비스 점검이 불가피하여 사전에 공지한 경우로 회사의 고의, 중과실이 없는 경우

8. 사전 공지된 정기점검으로 서비스를 중지했을 경우

9. 기타 회사의 고의 또는 과실이 아닌 사유로 서비스 장애가 발생하거나 파일 손상이 있는 경우

제 24 조 손해배상

① 데이터 손실로 인해 서비스가 중단된 경우 데이터 내재 가치 및 그로 인한 영업 손실에 대해서는 보상 하지 않는다.

② 회사는 서비스의 이용과 관련하여 회사에게 책임이 없는 사유로 회원에게 발생한 손해에 어떠한 책임도 지지 않는다.

③ 회원이 서비스를 이용함에 있어 행한 불법행위나 본 약관 위반행위로 인하여 회사가 당해 회원 이외의 제3자로부터 손해배상 청구 또는 소송을 비롯한 각종 이의제기를 받는 경우 당해 회원은 자신의 책임과 비 용으로 회사를 면책시켜야 하며, 회사가 면책되지 못한 경우 당해 회원은 그로 인하여 회사에 발생한 모든 손해를 배상하여야 한다.

④ 회사는 회사에게 책임 있는 사유로 장애가 발생하여 회원이 손해를 입은 경우에도 서비스 약관의 개별 서비스 수준 약관(SLA)이 존재할 경우, 그에 따른 Credit 제공으로 손해배상을 갈음하며, 그 외에 추가 손 해배상은 없다.

⑤ 회사는 회원의 서비스와 관련하여 타인의 지식재산권 위반 등의 범죄행위로 인한 민형사상의 책임을 부 담하지 않는다. 만약 이로 인하여 회사가 타인으로부터 손해배상청구 등 이의 제기를 받은 경우 회원은 회 사를 면책하고 자신의 비용과 책임으로 처리하여야 하며, 회원은 그로 인해 회사에 발생한 모든 손해를 배 상하여야 한다.

⑥ SLA 보상 방안은 다음과 같다.

항목	기준	할인율
서비스 가용성	99.0% 이상 ~ 99.9% 미만	최근 3개월 월 평균 이용요금의 10%
	95.0% 이상 ~ 99.0% 미만	최근 3개월 월 평균 이용요금의 25%
	95.0% 미만	최근 3개월 월 평균 이용요금의 50%
백업	99.0% 미만	최근 3개월 월 평균 이용요금의 1.5배

제25조 운영관리(매니지드) 서비스의 SLA

구분	기준	운영 시간	문의 채널	응답시간
일반문의	업무 시간 내의 일반적인 문의	업무시간 내 (평일 9:00~17:00)	이메일, 전화	4시간 이내
작업요청	별도의 작업 시간을 투입해야 하는 작업	24*7*365	이메일, 전화	4시간 이내 (업무시간 외 요청은 별도 협의)
장애	서비스 운영에는 지장이 없으나 애플리케이션이 비정상적으로 작동하거나 오류가 발생한 상태	24*7*365	전화	1시간 이내

- NHN 서비스 책임

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

- 네이버클라우드플랫폼 SLA 적용기준

- 장애 : 가동 중인 고객의 인스턴스 또는 태스크가 모두 외부 연결을 확보하지 못하는 경우
- 장애 시간 : 해당월 동안 장애가 발생한 시간의 총합. 단, 본 SLA 의 적용이 배제되는 경우에 그 해당 시간은 장애 시간에 포함되지 않음
- 월 가용률(%) = 100 x [1-{장애 시간의 합(분 단위)/해당월의 총 시간(분 단위)}]
- 월 이용요금 : 장애가 발생한 해당월의 본 서비스에 대하여 고객이 회사에 실제 지급하는 금액을 의미. 단, 인스턴스 또는 태스크 별로 이용요금이 별도로 산정되어 청구되는 경우에는 해당 인스턴스 또는 태스크에 대하여 고객이 실제로 지급하는 금액을 의미

월 가용률	서비스 크레딧
99.0% 이상 ~ 99.9% 미만	월 이용요금의 10%
95.0% 이상 ~ 99.0% 미만	월 이용요금의 25%
95.0% 미만	월 이용요금의 100%

	- KT 가용률 정책

1. 목표 수준 : 99.99%의 가용률을 보장.

1) 구분 : Cloud Server.

2) 정의 : 서버의 가용성 (월 가용률의 99.9% 이상).

3) 장애의 정의 : 2개 이상의 서버로 이중화 구성시 서버/네트워크 고장으로 인한 서비스 접속 불가.

4) 손해배상 방법 : 아래 3) 항목 표들을 참조.

2. 가용률 산정방식.

1) 월 가용률(%)=100x{1-{서비스를 이용한 한 달 동안 회사의 귀책사유로 인한 장애로 서비스를 이용하지 못하는 장애시간(분)의 합/서비스를 이용한 한 달(분)}} ("분" 은 시간단위인 분(分)을 의미함).
2) 장애시간: 서비스를 이용하지 못한 사실을 고객이 회사에 통지한 때(고객의 통지 전에 회사가 그러한 사실을 알게 된 경우는 회사가 그러한 사실을 알게 된 때)로부터 측정됨.

3) 가용률 보장정책.

1) server.

가. 멀티가용성존(Multi-Availability Zone) 구성시.

월 가용률.	할인률(%).
99.9% 이상 ~ 99.95% 미만.	10.
99.5% 이상 ~ 99.9% 미만.	20.
99.5% 미만.	30.

= 월 가용성 99.95%를 만족하지 못하는 시점부터 99.9%까지 : 월 이용요금의 10%.
= 월 가용성 99.9%를 만족하지 못하는 시점부터 99.5%까지 : 월 이용요금의 20%.
= 월 가용성 99.5% 미만까지: 월 이용요금의 30%.
* 단일 존에서도 DB 등 주요 server 의 이중화 구성 필요.

나. 멀티가용성존(Multi-Availability Zone) 미구성시.

월 가용률.	할인률(%).
99.9% 이상 ~ 99.95% 미만.	10.
99.0% 이상 ~ 99.5% 미만.	20.
99.0% 미만.	30.

= 월 가용성 99.9%를 만족하지 못하는 시점부터 99.5%까지 : 월 이용요금의 10%.
= 월 가용성 99.5%를 만족하지 못하는 시점부터 99%까지: 월 이용요금의 20%.
= 월 가용성 99%미만까지: 월 이용요금의 30%.

2) CDN/storage/backup 서비스.

월 가용률.	할인률(%).
99.0% 이상 ~ 99.9% 미만.	10.
99% 미만.	25.

가. 월 가용성 99.0%를 만족하지 못하는 시점부터 99.9%까지: 월 이용요금의 10%.
나. 월 가용성 99% 미만: 월 이용요금의 25%.

참조 자료	클라우드컴퓨팅서비스 품질・성능에 관한 기준(과학기술정통부, 2018.8) https://www.cloudqos.or.kr/page/availability

<table>
<tr><td>검토 항목</td><td>2.2 모니터링 정보</td></tr>
<tr><td>검토 내용</td><td>□ 리소스 모니터링 및 장애 정보를 제공하고 있는가?</td></tr>
<tr><td>검토 기준</td><td>▪ IaaS: 리소스 사용량(CPU, Memory, Disk, 트래픽 필수 포함), 장애정보 및 장애정보 알림기능(이메일, SMS 등), API 제공 등을 필수 포함하여 모니터링 정보 필수 제시
▪ PaaS, SaaS: 서비스 모니터링 제공 정보, 제공절차(제공주기, 제공방법) 등을 포함하여 필수 제시
▪ 그 외 서비스: 리소스 사용량, 장애정보 및 장애정보 알림기능 등 모니터링 정보제공 절차(제공주기, 제공방법) 등을 포함하여 필수 제시
* 이용자에게 제공 가능한 모니터링 및 장애 정보를 제시하여야 함
* 모니터링 정보제공 절차 중 모니터링 정보의 제공주기(상시, 일/주/월 등) 및 제공방법 등 제공절차를 필수 포함하여야 함</td></tr>
<tr><td>증빙 문서명</td><td>▪ 모니터링 매뉴얼, 관리자 매뉴얼, 이용자 매뉴얼 등 해당 내용을 증빙하는 공식 문서명 기입
* 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의
* 증빙 문서 제출시 모니터링 매뉴얼 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 모니터링 매뉴얼)별로 제출도 가능(단, 해당 검토영역의 풀본을 제출)</td></tr>
<tr><td>증빙 내용</td><td>제 5 장 운영관리(매니지드)
제 19 조 리소스 사용량
① 모니터링 서비스 신청한 고객에게는 통계 그래프를 활용하여 기본적인 서버 사용 추이나 패턴을 손 쉽게 파 악할 수 있다. 자신이 생성한 모든 Cloud Server들의 평균 리소스 사용량(CPU, Memory, Disk, Traffic 등)을 조 회할 수 있다.
제 20 조 지표 수집 주기 및 보관 기간
① 모니터링 지표는 1분 단위로 수집되며, 최대 3년간 보관된다. ② 지표 데이터는 5분, 30분, 2시간, 1일 단위로 집계된다. ③ 집계 단위별로 보장하는 기간은 아래와 같다.
<table><tr><th>집계 단위</th><th>보관 기간</th></tr><tr><td>1분</td><td>7일</td></tr><tr><td>5분</td><td>1개월</td></tr><tr><td>30분</td><td>6개월</td></tr><tr><td>2시간</td><td>1년</td></tr><tr><td>1일</td><td>3년</td></tr></table>
제21조 제공방법 및 제공주기
① 설정한 감시 조건을 충족하는 상황이 발생했을 때 알림을 제공한다. ② 알림 방법은 이메일이나 SMS로 받을 수 있다.
제22조 장애정보 및 장애정보 알림
수집된 지표의 임계치를 설정해 서버를 항상 감시할 수 있으며 이상 징후를 파악할 수 있다. 서버의 상태를 파악 할 수 있는 다양한 감시 항목을 제공하며 통보 방법은 이메일이나 SMS로 알림을 받을 수 있다</td></tr>
</table>

◇ 원사업자 업체별 모니터링 정보

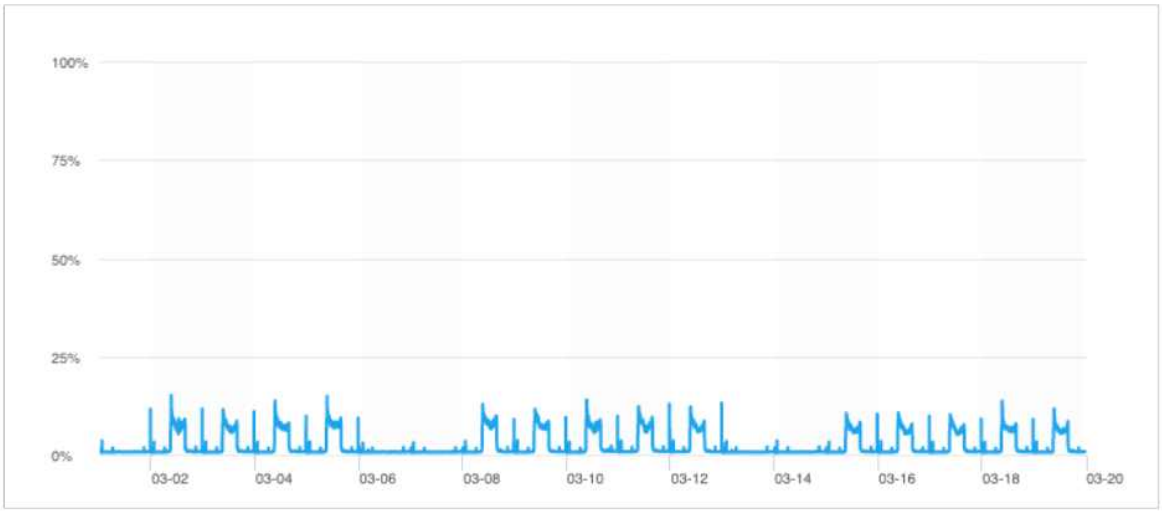
(1) KT 모니터링 정보

- KT 리소스 사용량 모니터링

운영 시스템 실시간 성능 요약정보 대시보드

서버명	IP	상태	운영상태	서비스상태	CPU Used	MEM Used	Swap Used	파일시스템 평균	파일시스템 최대	최대 파티션	bps		프로세스수 (전)	OS 가동시간
											In	Out		
			정상	서비스수집	0.66 %	40.21 %	0.28 %	4.96 %	14.48 %	/boot	64.15 k	119.33 k	137	143일 06:36:17
			정상	서비스수집	0.85 %	18.81 %	1.03 %	69.23 %	72.35 %	/	1.66 M	181.53 k	116	150일 12:37:47
			정상	서비스수집	0.28 %	6.80 %	0.03 %	11.20 %	14.48 %	/boot	12.34 k	205.76 k	157	135일 04:33:34
			정상	서비스수집	0.28 %	6.91 %	0.00 %	8.58 %	14.48 %	/boot	12.16 k	70.17 k	156	135일 04:33:32
			정상	서비스수집	0.17 %	4.43 %	0.00 %	9.18 %	10.33 %	/boot	16.84 k	103.43 k	193	142일 05:33:06
			정상	서비스수집	0.21 %	5.55 %	0.00 %	9.67 %	10.33 %	/boot	22.57 k	131.77 k	193	134일 05:02:54
			정상	서비스수집	0.80 %	15.11 %	0.00 %	11.19 %	11.19 %	/	29.10 k	270.02 k	363	25일 03:53:03
			정상	서비스수집	0.76 %	13.58 %	0.00 %	7.54 %	10.33 %	/boot	23.85 k	227.16 k	365	17일 04:52:24
			정상	서비스수집	0.81 %	14.41 %	0.00 %	9.20 %	10.33 %	/boot	35.90 k	238.45 k	364	25일 03:52:55
			정상	서비스수집	0.82 %	10.36 %	0.00 %	7.62 %	10.33 %	/boot	63.12 k	8.82 M	365	04일 13:00:33
			정상	서비스수집	0.71 %	10.72 %	0.00 %	7.52 %	10.33 %	/boot	40.92 k	238.60 k	364	04일 13:01:29
			정상	서비스수집	0.78 %	10.79 %	0.00 %	12.74 %	12.75 %	/	24.26 k	233.88 k	363	25일 10:00:09
			정상	서비스수집	0.77 %	10.18 %	0.18 %	14.16 %	14.18 %	/	86.34 k	292.75 k	363	29일 05:30:14
			정상	서비스수집	0.79 %	13.52 %	0.02 %	11.77 %	11.77 %	/	37.52 k	244.68 k	362	28일 05:52:33
			정상	서비스수집	0.73 %	9.73 %	0.00 %	14.13 %	14.14 %	/	24.63 k	226.82 k	362	28일 05:52:21
			정상	서비스수집	0.45 %	8.72 %	0.03 %	3.72 %	10.33 %	/boot	19.03 k	86.97 k	130	150일 08:47:00
			정상	서비스수집	1.77 %	33.01 %	13.23 %	30.08 %	30.08 %	C:/	90.79 k	105.57 k	91	72일 12:25:33

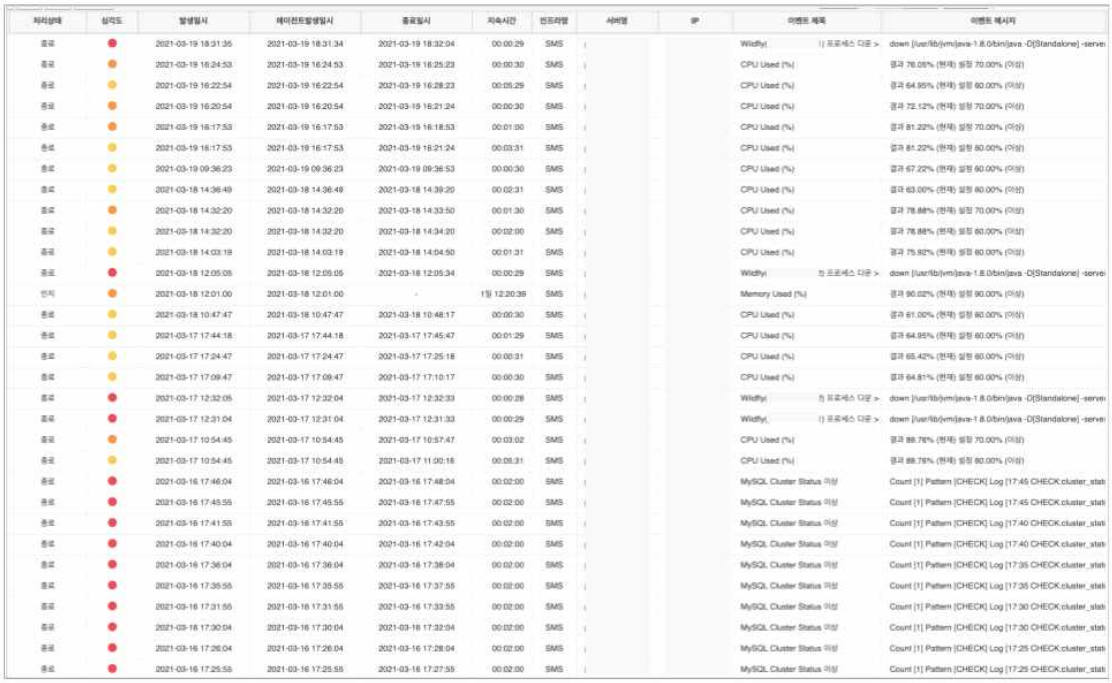
CPU 사용량 (%) 정보



- VM별 CPU 5분, 1시간당 평균 CPU 사용량 데이터 제공(그래프, raw데이터)
- 필요한 기간 동안 성능 데이터 추출, 제공 가능

- KT 장애 정보 및 알림 기능

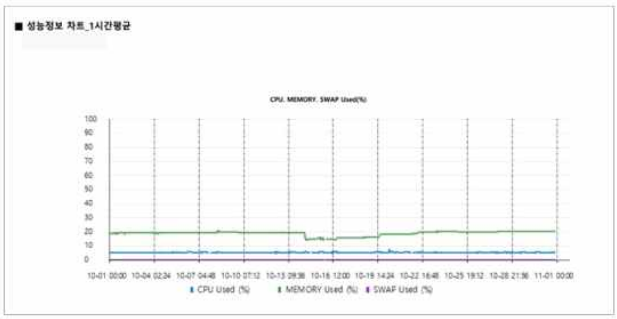
이상징후, 장애 이벤트 대시보드

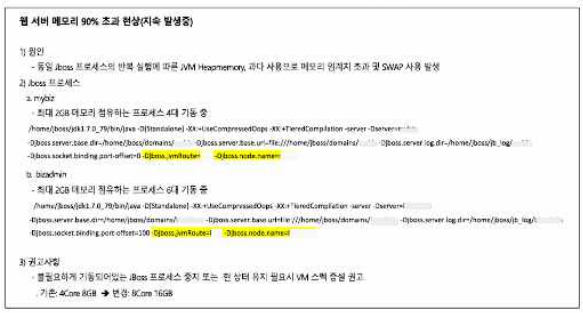


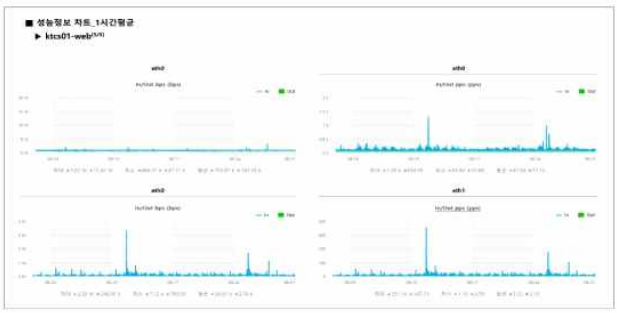
처리상태	심각도	발생일시	에이전트발생일시	종료일시	지속시간	전조라업	서버명	IP	이벤트 제목	이벤트 메시지
종료		2021-03-19 18:31:35	2021-03-19 18:31:34	2021-03-19 18:32:04	00:00:29	SMS			Wildfyl	1) 프로세스 다운 > down [/usr/lib/jvm/java-1.8.0/bin/java -D[Standalone] -server
종료		2021-03-19 16:24:53	2021-03-19 16:24:53	2021-03-19 16:25:23	00:00:30	SMS			CPU Used (%)	경과 76.05% (현재) 설정 70.00% (이상)
종료		2021-03-19 16:22:54	2021-03-19 16:22:54	2021-03-19 16:28:23	00:05:29	SMS			CPU Used (%)	경과 64.95% (현재) 설정 60.00% (이상)
종료		2021-03-19 16:20:54	2021-03-19 16:20:54	2021-03-19 16:21:24	00:00:30	SMS			CPU Used (%)	경과 72.12% (현재) 설정 70.00% (이상)
종료		2021-03-19 16:17:53	2021-03-19 16:17:53	2021-03-19 16:18:53	00:01:00	SMS			CPU Used (%)	경과 81.22% (현재) 설정 70.00% (이상)
종료		2021-03-19 16:17:53	2021-03-19 16:17:53	2021-03-19 16:21:24	00:03:31	SMS			CPU Used (%)	경과 81.22% (현재) 설정 60.00% (이상)
종료		2021-03-19 09:36:23	2021-03-19 09:36:23	2021-03-19 09:36:53	00:00:30	SMS			CPU Used (%)	경과 67.22% (현재) 설정 60.00% (이상)
종료		2021-03-18 14:36:49	2021-03-18 14:36:49	2021-03-18 14:39:20	00:02:31	SMS			CPU Used (%)	경과 63.00% (현재) 설정 60.00% (이상)
종료		2021-03-18 14:32:20	2021-03-18 14:32:20	2021-03-18 14:33:50	00:01:30	SMS			CPU Used (%)	경과 78.88% (현재) 설정 70.00% (이상)
종료		2021-03-18 14:32:20	2021-03-18 14:32:20	2021-03-18 14:34:20	00:02:00	SMS			CPU Used (%)	경과 78.88% (현재) 설정 60.00% (이상)
종료		2021-03-18 14:03:19	2021-03-18 14:03:19	2021-03-18 14:04:50	00:01:31	SMS			CPU Used (%)	경과 75.92% (현재) 설정 60.00% (이상)
종료		2021-03-18 12:05:05	2021-03-18 12:05:05	2021-03-18 12:05:34	00:00:29	SMS			Wildfyl	1) 프로세스 다운 > down [/usr/lib/jvm/java-1.8.0/bin/java -D[Standalone] -server
인지		2021-03-18 12:01:00	2021-03-18 12:01:00	-	1일 12:20:39	SMS			Memory Used (%)	경과 90.02% (현재) 설정 90.00% (이상)
종료		2021-03-18 10:47:47	2021-03-18 10:47:47	2021-03-18 10:48:17	00:00:30	SMS			CPU Used (%)	경과 61.00% (현재) 설정 60.00% (이상)
종료		2021-03-17 17:44:18	2021-03-17 17:44:18	2021-03-17 17:45:47	00:01:29	SMS			CPU Used (%)	경과 64.95% (현재) 설정 60.00% (이상)
종료		2021-03-17 17:24:47	2021-03-17 17:24:47	2021-03-17 17:25:18	00:00:31	SMS			CPU Used (%)	경과 65.42% (현재) 설정 60.00% (이상)
종료		2021-03-17 17:09:47	2021-03-17 17:09:47	2021-03-17 17:10:17	00:00:30	SMS			CPU Used (%)	경과 64.81% (현재) 설정 60.00% (이상)
종료		2021-03-17 12:32:05	2021-03-17 12:32:04	2021-03-17 12:32:33	00:00:28	SMS			Wildfyl	1) 프로세스 다운 > down [/usr/lib/jvm/java-1.8.0/bin/java -D[Standalone] -server
종료		2021-03-17 12:31:04	2021-03-17 12:31:04	2021-03-17 12:31:33	00:00:29	SMS			Wildfyl	1) 프로세스 다운 > down [/usr/lib/jvm/java-1.8.0/bin/java -D[Standalone] -server
종료		2021-03-17 10:54:45	2021-03-17 10:54:45	2021-03-17 10:57:47	00:03:02	SMS			CPU Used (%)	경과 88.76% (현재) 설정 70.00% (이상)
종료		2021-03-17 10:54:45	2021-03-17 10:54:45	2021-03-17 11:00:16	00:05:31	SMS			CPU Used (%)	경과 88.76% (현재) 설정 60.00% (이상)
종료		2021-03-16 17:46:04	2021-03-16 17:46:04	2021-03-16 17:48:04	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:45 CHECK:cluster_stat
종료		2021-03-16 17:45:55	2021-03-16 17:45:55	2021-03-16 17:47:55	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:45 CHECK:cluster_stat
종료		2021-03-16 17:41:55	2021-03-16 17:41:55	2021-03-16 17:43:55	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:40 CHECK:cluster_stat
종료		2021-03-16 17:40:04	2021-03-16 17:40:04	2021-03-16 17:42:04	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:40 CHECK:cluster_stat
종료		2021-03-16 17:36:04	2021-03-16 17:36:04	2021-03-16 17:38:04	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:35 CHECK:cluster_stat
종료		2021-03-16 17:35:55	2021-03-16 17:35:55	2021-03-16 17:37:55	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:35 CHECK:cluster_stat
종료		2021-03-16 17:31:55	2021-03-16 17:31:55	2021-03-16 17:33:55	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:30 CHECK:cluster_stat
종료		2021-03-16 17:30:04	2021-03-16 17:30:04	2021-03-16 17:32:04	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:30 CHECK:cluster_stat
종료		2021-03-16 17:26:04	2021-03-16 17:26:04	2021-03-16 17:28:04	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:25 CHECK:cluster_stat
종료		2021-03-16 17:25:55	2021-03-16 17:25:55	2021-03-16 17:27:55	00:02:00	SMS			MySQL Cluster Status 이상	Count [1] Pattern [CHECK] Log [17:25 CHECK:cluster_stat

- 장애 내용, 발생시각, 진행상황 현황 관리 대시보드

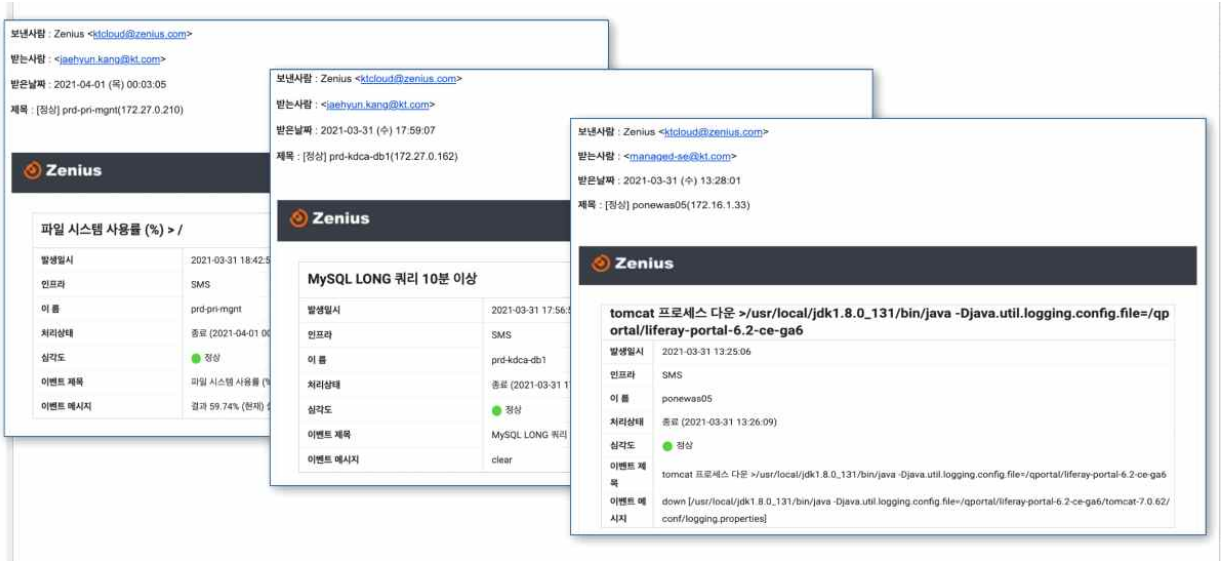
- KT 모니터링 정보 제공 주기 및 제공 방법







- KT 모니터링 알람기능



(2) NHN 모니터링 정보

1.1 Compute > System Monitoring > 개요

Compute > System Monitoring 서비스에서는 **Instance**에서 사용자가 생성한 인스턴스에 대한 모니터링 기능을 제공합니다. 인스턴스의 시스템 리소스 상태를 차트 형태로 시각화해서 볼 수 있으며, 사용량 임계치를 설정해 특정 상태의 알림을 이메일 또는 SMS로 받을 수 있습니다.

System Monitoring은 각 인스턴스 서버에 설치된 System Monitoring Agent로 시스템 지표를 수집합니다. 기본적으로 Agent는 인스턴스의 이미지에 포함되어있기 때문에 인스턴스 구동시 자동으로 수집을 시작합니다. 하지만 System Monitoring 서비스가 출시된 2019년 7월 23일 이전에 생성되어 동작 중인 인스턴스의 경우 별도의 Agent 설치가 필요합니다. Agent 설치 방법은 **Compute > System Monitoring > 콘솔 가이드 > Agent 설치 방법**을 참고하시기 바랍니다.

1.2 제공 기능

1.2.1 시스템 지표 대시보드 제공

Compute > Instance에서 생성한 서버 인스턴스의 각종 시스템 지표를 차트로 제공해 각 서버의 상태를 파악할 수 있습니다. 시스템 지표 차트를 선택하여 원하는 레이아웃으로 배치할 수 있으며, 레이아웃을 여러 개 생성해 목적에 따라 관리할 수 있습니다.
시스템 지표는 1분 단위로 수집되며 최대 5년간 보관됩니다. 지표 데이터는 5분, 30분, 2시간, 1일 단위로 집계됩니다. 집계 단위별 보관 기간은 아래와 같습니다.

집계 단위	보관 기간
1분	7일
5분	1개월
30분	6개월
2시간	2년
1일	5년

1.2.2 지표 감시 설정 및 알림

수집된 지표의 임계치를 설정해 서버를 항상 감시할 수 있으며 이상 징후를 파악할 수 있습니다. 예를 들어, CPU 사용률이 90%를 넘는 경우, 특정 NIC의 사용량이 1000pps를 넘은 경우, 특정 프로세스가 중단된 경우 등 서버의 상태를 파악할 수 있는 다양한 감시 항목을 제공합니다.

1.2.3 통보 방법 선택: 이메일, SMS

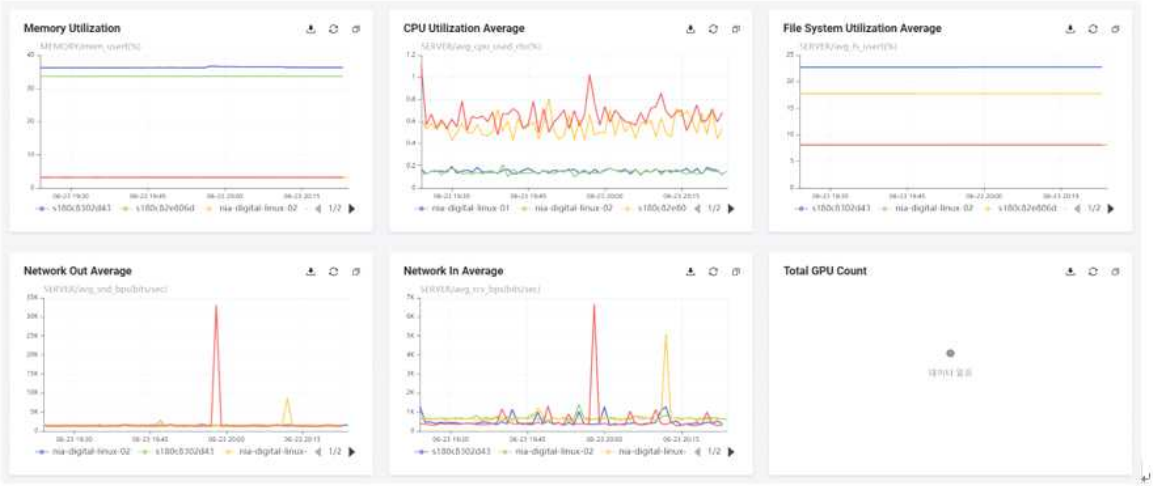
설정한 감시 조건을 충족하는 상황이 발생했을 때 어떤 방법으로 알림을 받을지 선택할 수 있습니다. 이메일이나 SMS로 알림을 받을 수 있습니다.

(3) 네이버클라우드플랫폼 모니터링 정보

1. 모니터링

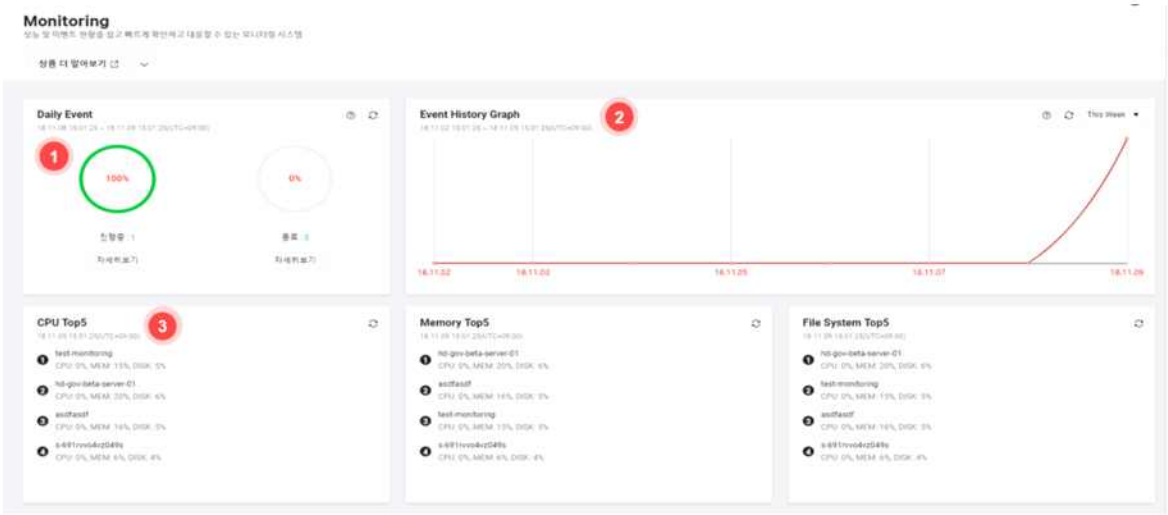
1.1. 리소스 사용량 등 모니터링 정보 확인

- Cloud Insight를 통해 제공하는 서비스의 성능 지표를 통합 관리하고, 장애 발생 시 담당자에게 장애 정보를 신속히 전달합니다.
- Cloud Insight의 대시보드를 통해 리소스의 사용량을 한눈에 확인할 수 있으며, 사전에 설정된 Memory, CPU, File System Utilization, Network In/Out 등의 다양한 지표 선택이 가능합니다.



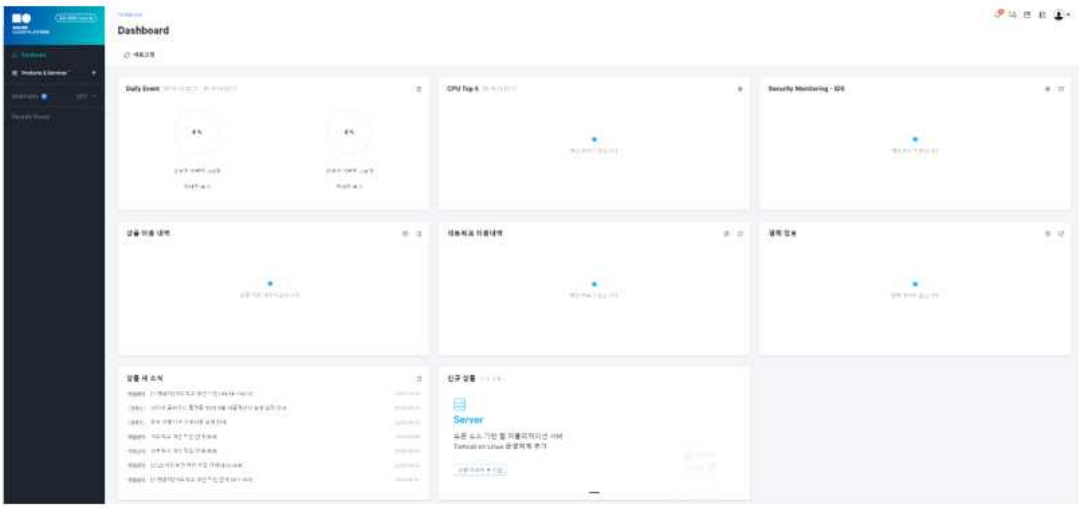
1.2. 장애 정보 및 장애정보 알림 기능

- 장애(이벤트) 정보에 대해 콘솔의 대시보드에서 확인합니다.



1.3. 모니터링 정보 제공 절차

- 대시보드를 통해 1분 주기로 수집된 모니터링 정보에 대한 리소스 사용량(CPU, Memory, Disk, 트래픽 필수 포함), 장애정보 및 장애정보 알림기능(이메일, SMS 등), API 제공 등을 포함한 정보 확인이 가능



- 모니터링은 다음과 같은 통보 대상 설정을 통해 대상 관리가 가능하며, 통보는 Email과 SMS를 통해 가능합니다.

1.4. 이용자에게 제공 가능한 모니터링 및 장애 정보

▪ 이용자에게 제공하기 위해 수집하는 모니터링 정보와 장애 정보 제공을 위해 이벤트 통보 설정을 수행하는 항목은 다음과 같습니다.

수집하는 모니터링 정보		이벤트 통보 설정 항목	
항목	세부항목	항목	세부항목
CPU	Used(%), System(%), User(%), iowait(%)	CPU	Used(%), System(%), User(%), Idle(%), iowait(%), nice(%), irq(%), softirq(%), privileged time(%), dpc time(%), interrupt time(%), processor time(%)
Memory	Used(%), Total/Used/Free/Buffer/Cached(Bytes)	Memory	Used(%), Total/Used/Free/Buffer/Cached/Shared(Bytes), pgin/sec(MB), pgout/sec(MB)
File System	FimeSystem 명칭, Size(MB), Used(MB/%), Avail(MB), Mount	File System	Used/iuse(%), 가용량/사용량(MB), 마운트 상태
NIC	Output(bps/pps/error), Input(bps/pps)	NIC	Output(bps/pps/error), Input(bps/pps/error), collision
Disk I/O	Read Bytes, Write Bytes	Disk I/O	Read Bytes/Count, Write Bytes/Count
Swap	Used(%), Total/Used/Free(Bytes)	Swap	Used(%), Total/Used(Bytes)
Load Average	1분, 5분, 15분	Load Average	1분, 5분, 15분
		파일 감시	변경, 크기, 존재 여부, 무변경
		사용자수	사용자수
		로그 감시	파일로그
		Ping Fail	Ping Fail
프로세스	상위 TOP10에 대하여	프로세스	프로세스 다운, CPU(%), 메모리(%/KB), Thread 수, 전체 프로세스 수, 프로세스 재시작
	Process 명칭, PID, CPU(%), 메모리(%/KB), Prior, Thread, CPU Time		

참조 자료 -

검토 항목	**2.3 백업 및 복구**
검토 내용	□ 서비스의 신속한 복구를 위한 장애 대응체계 및 백업·복구 정책을 제시하고 있는가?
검토 기준	▪ "장애대응체계"를 필수 제시 ▪ IaaS, PaaS: 평균 서비스 회복시간(일반 및 고가용성 환경), 데이터 백업 및 복구정책(백업주기, 백업 준수율, 데이터복구시간 및 복구시점, 백업데이터 보관기간, 데이터반환 및 폐기) 등을 포함하여 필수 제시 * 일반 및 고가용성(HA, DR 등) 환경에서의 평균 서비스 회복시간을 구분하여 필수 제시 ▪ SaaS : 백업주기, 백업시간, 백업방법(유형), 백업대상 및 범위, 보관장소, 보관기간 등를 포함한 백업 정책 및 백업기능(서비스) 제공에 따른 유·무상 여부, 유상의 경우 가격정책 등을 포함하여 필수 제시 ▪ 그 외 서비스 : 백업주기, 백업시간, 백업방법(유형), 백업대상 및 범위, 보관장소, 보관기간 등을 포함하여 백업정책을 필수 제시
증빙 문서명	▪ 장애대응절차서, 백업 및 복구 정책서, 지침 등 해당 내용을 증빙하는 공식 문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 장애대응지침 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 장애대응절차서)별로 제출도 가능**(단, 해당 검토영역의 풀본을 제출)**
증빙 내용	◇ 원사업자 백업 및 복구 정보 (1) KT 백업 및 복구

[지원 체계] 백업 정책

□ 백업 구성 절차

1. 백업 Agent 설치

1) kt cloud Backup 서비스 Agent 설치 (HPDP Client Agent)

2) 백업 연동 방화벽 오픈

- 양방향 TCP 5500 ~ 6000

2. 백업 정책 작성

1) 전체, 증분 백업 선택

2) 백업 용량 산정, 백업 대상 선정

3) 백업 보관주기 설정

4) 백업신청서 작성

3. 백업 정책 등록

1) Backup 메뉴에서 백업신청서 등록 신청

2) 백업 적용 확인

4. 백업 결과 확인

1) 전체, 증분 백업 별 결과 리포트 메일 확인

2) 백업 오류 발생시 원인파악 및 백업 재 수행 진행

□ 백업정책 및 보관주기 설정 (예시)

구분	백업 대상	손실 위험도	전체 백업	증분 백업	보관기간
파일시스템	AP 실행파일, 설정파일, 로그파일, 프로그램 소스	중간	Weekly	Daily	4주
데이터베이스	오라클DB 실행/설정파일, 데이터파일, Archive Log Redo Log , MSSQL 등	높음	Daily (Online)	Archive Log	2주
DEV, TB[1]	개발소스, 요청파일	낮음	Monthly	Weekly	8주

1) TB: Test Bed

(2) NHN 백업 및 복구

□ OS, 파일시스템 백업 복구 절차

1. O/S 시스템 전체 복구

1) 생성해둔 기본 OS 이미지나 Cloud 에서 제공되는 이미지로 신규 VM 생성
   - 디스크 구성 및 네트워크 정보 기존 시스템과 동일하게 설정
2) 기본 OS 설치 후 HP DP Agent 설치 (HP DP: kt cloud 백업 솔루션)
3) HP DP 를 통하여 시스템 구성에 필요한 백업 항목 복구 시행
   - 예: 특정 날짜, 복구 위치 지정

2. O/S 부분 복구 및 파일 시스템 부분/전체 복구

1) HP DP 에서 복구 대상 지정 (파일시스템, 디렉토리 또는 개별 파일)
2) 대상 서버 선택, 복구 위치 지정 후 복구

□ DB 백업 복구 절차

1. Oracle 데이터베이스 복구

1) 대상 서버 데이터베이스 인스턴스 종료 확인
2) 컨트롤 파일 소실시 컨트롤 파일 복구 후 mount 상태로 기동
3) 복구 대상 파일 복구 (Restore Database)
4) 목표 시점까지 데이터베이스 복구 (Recover Database)
5) 대상 서버 데이터베이스 인스턴스 오픈

2. 기타 데이터베이스 복구

기타 DB 의 경우 HP 예를 이용하여 DB 백업 파일을 Restore 후
DB 자체에서 복구작업 진행

□ 이용 약관 명시


서비스 이용약관

Cloud Service
클라우드 서비스

• Home • 이용약관 • 서비스 이용약관

이용약관 - 시행일: 2018년 4월 23일 보기

제 8 장 cloudpack backup

제21조 서비스의 종류

① 회사가 제공하는 cloudpack backup 서비스의 종류는 아래와 같고, 향후 추가하거나 변경할 수 있습니다.
1. 로컬백업 : cloudpack server와 파일시스템 및 데이터베이스를 1~4주 주기로 백업시스템에 백업(backup)하고, 변경 분에 대해 사전정한 주기로 증분 백업(incremental backup)하여 필요 시 복구하는 서비스
2. 소산백업 : 회사의 클라우드 데이터센터(IDC)간 로컬백업된 데이터의 원격지 백업을 제공하는 서비스로 로컬백업과 부가서비스 업종입니(소산백업을 수행하기 위해서는 로컬백업이 반드시 사전 수행되어야 함)

② 백업된 데이터는 다음과 같은 절차를 통해 검증할 수 있습니다.
1. 고객이 요청한 백업대상의 백업성공 확인은 고객이 사이트의 cloudpack backup 서비스 백업 & 복구이력 조회를 통해 확인할 수 있습니다.
2. 백업 완료가 고객이 요청한 내용과 다를 경우 고객은 즉시 회사에 수정을 서면으로 요청하여야 하며, 그렇지 않은 백업 & 복구이력 조회 상의 모든 정보에 동의하는 것으로 간주됩니다.
3. 백업된 데이터의 검증을 위해 고객은 월 1회에 한하여 데이터 복구를 요청할 수 있으며, 백업 데이터의 검증은 복구 요청이 없을 경우 백업되어 보관 중인 데이터가 고객이 요청한 데이터와 일치하는 것으로 간주됩니다.

제22조 서비스의 이용요금

월 이용요금은 서비스 이용 시 매월 고객이 납입해야 하는 요금으로서, 월 이용요금의 구체적인 사항에 대해서는 서비스 제공을위한 웹사이트(https://www.cloudpack.co.kr)에 게시합니다.

(3) 네이버클라우드플랫폼 백업 및 복구

- 데이터 백업 정책

종류	백업 주기	백업 시간	백업 준수율	백업 방법	백업 대상 및 범위	보관 장소	보관 기간
DB	1일	04:00	99%	dump	모든 사용자 정보	NAS, DR(avamar)	1년
스토리지	1일	05:00	99%	데이터 동기화	모든 폴더와 파일	object storage, NAS, DR(avamar)	1년

- 데이터 복구 정책

구분	복구 방법	복구 방안	복구시간	복구시점
고객 실수로 인한 단순 데이터 유실	NHN Cloud 서비스 (유상 솔루션)	NHN Cloud에서 제공하는 Backup 서비스를 통한 데이터 복구	사용자 백업 설정시간에 따름	사용자 설정에 따름
CSP사업자의 장애로 인한 데이터 유실	클라우드서비스 자체 백업	주기적인 데이터 백업을 통한 데이터 복구	1시간 이내 (이중화 시 30분 이내)	장애 확인 시
재난재해로 인한 데이터 유실	DR센터 백업	DR센터로의 주기적인 데이터 동기화를 통한 데이터 복구	1시간 이내	장애 확인 시

- 평균 서비스 회복시간

구 분	환경 설명	평균복구시간 (MTTR, Mean Time To Repair) (MTTR = 총 고장시간/고장횟수)	비고
일반 환경	서비스 단중화 환경	1시간 이내	
고가용성 환경	Infra부터 Application Level 까지의 전체 이중화 환경 (ex. WEB, WAS, DBMS 이중화)	30분 이내	

- 데이터 반환 및 폐기 정책

구분	설명	지원업무	보관 기간
데이터 반환	고객 요청에 따른 데이터 반환	방화벽 오픈 지원, 접속 정보 안내 등	1년
데이터 폐기	고객 요청에 따른 데이터 폐기 (ex. 가상서버 삭제, 스토리지 삭제 등)	요청 시 데이터 즉시 폐기	요청 시 데이터 즉시 폐기

◇ 장애 대응 관련 내용

▪(백업 및 복구)

1. 성능 및 용량관리

클라우드 컴퓨팅 서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.

▶ 매일 오전 9 시 기준으로 인프라(메모리, 스토리지, 공인 IP 등) 용량을 주기적으로 점검하며, 메일로 운영그룹에 공유한다.

물리용량 대비 70% 수준으로 내부 임계치를 정하고, 사용량이 이를 초과할 경우 조직장 승인을 받아 증설을 진행한다.

2. 이중화 및 백업

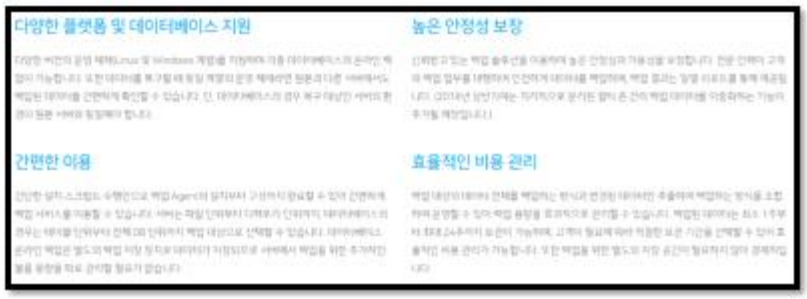
정보 처리설비의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.

▶ 백업대상 선정기준 수립 : 공공클라우드 서비스 운영/관리를 위한 중요데이터.

▶ 백업담당자 및 책임자 지정 : 백업담당자 IT 엔지니어링실 김영훈, 책임자 클라우드실 한상영

▶ 백업 주기 및 보존기한 정의

- NCP 의 부가서비스로 고객은 운영정책에 따라 자유롭게 백업 정책을 설정 및 운영 할 수 있음.
- 최소 1 일 1 회~4 주 1 회 까지, 백업주기 선정.



※ 백업매체 관리 : 스토리지(VTL)이므로 별도 라벨링, 관리대장등은 존재하지 않음.

▶ 백업방법 및 복구 절차

정책/기준 및 가이드	업무 처리 기준
백업 대상	DB • DB의 경우 Naver에서 사용되는 Oracle, My-sql, MS-sql, Cubrid를 지칭함. • DB백업은 매일 전체 백업 방식을 사용하여 일주일 보관 • 5G의 경우 업무일에 한번 전체백업 방식을 사용하여 1개월 보관 그룹웨어 • 그룹웨어의 경우 Naver에서 사용되는 Domino, exchange를 지칭함. • 그룹웨어 백업은 백업솔루션에서 제공하는 APM을 사용하여 online백업 • 매일 증분백업/매주 한번 전체 백업 방식을 사용하여 1개월 보관 일반 • 일반의 경우 서비스중인 소스, 이미지등 일반 파일백업을 지칭함. • 일반 파일의 경우는 보관주기에 따라 백업 방식 차등 • 기본적으로 매일 증분백업/매주 한번 전체 백업 방식을 사용하여 1개월 보관
백업 미디어	• 보관주기가 1개월 미만의 데이터백업은 VTL적용 • 보관기간이 1개월 이상의 데이터백업은 Tape적용
데이터 보관	• 일 단위 백업(Daily Backup)은 전체 백업을 사용하여 1주일간 보관 • 주 단위 백업(Weekly Backup)은 전체 백업 방식을 사용하여 1달간 보관 • 월 단위 백업(Monthly Backup) 은 전체 백업 방식을 사용하여 1분기간 보관 • 분기 단위 백업(Quaterly Backup)은 전체 백업 방식을 사용하여 1년간 보관 • 1년 이상단위 백업은 2개본을 생성하여 그 중 한 개는 소산보관 (단, 법적보관기간 혹은 비즈니스상 중요데이터에 한해 1년이상 장기보관)

제 2장 장애대응

제 4조(장애대응 체계)

① MSP(Managed Service Provider)는 최초 장애 접수, 장애 확인 및 장애 정도의 판단을 한다.

② CSP(Cloud Service Provider)는 장애 처리 과정에서 MSP에게 기술지원 및 2차 장애 조치를 한다.

③ MSP가 장애조치가 완료되고 서비스의 정상확인, 장애 종료 및 전파를 한다.

제 5조(장애 처리 절차)

① 장애가 발생하면 MSP사의 운영관리팀은 장애 인지 또는 고객의 장애를 접수하고 업무시간에는 상주 인력을 통한 대응을 하며 업무외 시간에 중요 장애 발생 시 비상체계를 가동한다.

② 장애 처리시 긴급 장애와 단순 장애를 구분하여 처리한다.

1. 긴급 장애 발생시에는 상주 및 비상주 인력을 총동한 복구 체계로 기술지원을 구성한다.

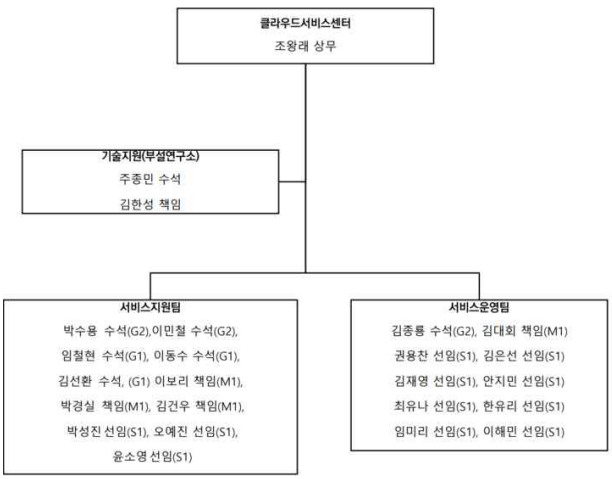
	2. 단순 장애 발생시에는 원격 복구 지원 및 원인 복잡 장애시에는 4시간 이내의 복구시간을 가진다. ③ 장애 분석 및 보고 시 복잡한 장애 또는 CSP 장애는 Log File 벤더 기술 지원 분석을 요청하고 장애원인 분석 보고서를 작성한다. ④ 장애 이력 관리시 장애 내역과 이슈를 관리하며 유사장애처리 내역을 정보화 한다. 제 6조(장애 등급 분류) ① 장애등급은 고객의 서비스 정지 시간 및 CSP사의 IDC(Internet Data Center)시설 장애 수준을 기준으로 분류한다. ② 고객의 서비스 정지 시간은 서비스장애 지속시간을 기준으로 1~4등급으로 구분한다. 1. 1등급은 주요 서비스 장애가 2시간이 초과된 경우 2. 2등급은 주요 서비스 장애가 1시간이 초과된 경우 3. 3등급은 주요 서비스 장애가 1시간 이내인 경우 4. 4등급은 주요 서비스 장애가 30분 이내인 경우 ③ CSP사의 IDC시설 장애 수준은 다음과 같이 장애범위를 기준으로 구분한다. 1. 1등급은 CSP의 IDC 전체 장애인 경우 2. 2등급은 CSP IDC의 Zone급 장애인 경우 3. 3등급은 CSP IDC의 POD급 장애인 경우 4. 4등급은 CSP IDC의 Cluster 장애인 경우 ④ 장애 보고서 관리를 통한 재발 방지 및 선제 대응 관리 및 침해사고 대응 등의 장애 대응을 제공한다. 제 7조(역할 및 책임) ① MSP사의 운영관리팀은 다음 각 호의 사항을 수행한다. 1. 영업일 기준 주간에 운영 관리 업무 2. VOC(Voice of Customer) 대응, 기록, 관리 등 운영 관리업무 3. 클라우드 시스템 매니지드 서비스 제공. 4. 장애 발생 시 1선 처리 담당 (야간, 공휴일은 2선 처리 담당) 5. 대응 제한 시 기술지원팀에 문의 및 협업 ② MSP사의 통합관제센터는 다음 각 호의 사항을 수행한다. 제 3장 운영관리(매니지드)서비스 제 8조(평균 서비스 회복시간) 아이티아이즈는 SLA기준에 준용하여 1시간 이내의 평균 서비스 회복시간을 가진다. 제 9조(백업 및 복구 정책) ① 자사의 운영정책에 따라 백업주기를 가진다. ② 백업준수율은 99.9%로 한다. ③ 데이터복구시간은 최대 1시간 이내 복구를 원칙으로 한다. (클라우드 인프라 장애를 제외한 데이터 유실의 경 우, 데이터백업 서비스를 활용할 수 있지만 데이터의 양에 따라 고객과 협의하여 작업 일정 확정)

	④ 백업 단위에 따라 1주일에서 1년간의 보관기간을 가진다. 제 10조(데이터 반환 및 폐기) ① 백업 데이터의 보관 계약에 따라 보관 기간이 초과된 데이터에 대해서는 고객에게 반환 또는 자체 폐기의 절차를 진행한다. ② 데이터 폐기는 내부 지침에 따라 복원 불가능한 방법으로 시행한다. ③ 데이터 반환을 위해 임시 저장된 데이터는 완전 삭제를 위해 공백으로 저장 후, 삭제한다. ④ 고객이 파기 확인서를 요청 시 이를 제출한다.
참조 자료	https://www.cloudqos.or.kr/page/responsibility

II. 제공역량

3. 지원 체계

검토 항목	**3.1 조직·인력 구성 현황 및 이용자 지원 체계**
검토 내용	□ 디지털 서비스의 유지 및 지원을 위한 이용자 지원체계를 제시하고 있는가?
검토 기준	▪ 조직인력 구성현황(디지털 서비스를 유지하기 위한 담당조직 및 역할 등) - 고객 서비스 유지 및 요구사항을 원활히 지원하기 위한 담당조직, 담당인력, 담당업무 등을 포함하여 필수 제시 ▪ 이용자 지원체계(이용자 매뉴얼, 교육자료, 기술자료 등) - 이용자 매뉴얼, 교육자료, 온라인 교육, 기술지원 등 제공 가능한 범위의 이용자 지원 방안을 필수 제시 ▪ 클라우드 지원 서비스 조직 역량(* 클라우드 지원서비스 유형에만 해당되는 사항) - 클라우드 지원서비스는 클라우드 컴퓨팅서비스 도입·전환에 필요한 업무수행(컨설팅, 운영관리, 마이그레이션 등)을 위해 관련 자격보유, 교육이수, 수행경험 등을 포함한 조직 및 수행 인력의 역량을 필수 제시
증빙 문서명	▪ 조직도, 직제규정, 이용자 매뉴얼, (지원서비스의 경우, 자격증명서, 교육수료증, 사업실적증명서 포함) 등 해당 내용을 증빙하는 공식 문서명 기입 * 증빙 문서는 이용지원시스템 심사신청시 등록, 대용량의 경우는 별도 문의 * 증빙 문서 제출시 정보보호정책서 등 다수의 검토항목에 대하여 증빙하는 경우 1개 파일로 제출 가능 또는 별도로 해당파트(예 : 침해사고대응절차서)별로 제출도 가능(단, 해당 검토영역의 풀본을 제출)
증빙 내용	○ 클라우드 센터 조직도 및 업무분장



팀명	역할	담당자
서비스 센터	- 클라우드 서비스 센터장으로 총괄 최고책임자	조왕래 상무
서비스 지원팀	- 클라우드 사업 지원 지원 및 컨설팅 - 클라우드 마이그레이션 사업	박수용 수석(G2) 이민철 수석(G2) 임철현 수석(G1) 이동수 수석(G1) 김선환 수석(G1) 이보리 책임(M1) 박경실 책임(M1) 김건우 책임(M1) 박성진 선임(S1) 이연호 선임(S1) 오예진 선임(S1) 윤소영 선임(S1)
서비스 운영팀	- 클라우드 서비스 고객 대응 및 24시 365일 관제 - 클라우드 사업 인력지원 및 구축 지원	김종룡 수석(G2) 김대회 책임(M1) 권용찬 선임(S1) 김은선 선임(S1) 김재영 선임(S1) 안지민 선임(S1) 최유나 선임(S1) 한유리 선임(S1) 임미리 선임(S1) 이해민 선임(S1)
기술지원 (부설연구소)	- 클라우드 애플리케이션 기술연구	주종민 수석 김한성 책임

	 eyes NAVER CLOUD PLATFORM 네이버 클라우드 이용자 교육자료  eyes NAVER CLOUD PLATFORM 네이버 클라우드 운영자 가이드
참조 자료	-