요 약 문

1. 제목

클라우드 서비스 활성화를 위한 인증제도 도입방안 연구

2. 연구의 목적 및 중요성

가. 연구의 목적

o 클라우드 서비스에 특화된 인증영역을 정립하고 체계적인 인증프로세스 구축 연구를 통해 서비스 제공자 및 이용자 간 신뢰기반을 구축하여 클라우드 서비스 도입 및 활성화 촉진에 기여

→ 클라우드 서비스 활성화를 위한 중장기 정책 마련을 위한 정책자료 활용 및 클라우드 서비스의 표준화 및 품질 경쟁력 향상을 유도

o 클라우드 서비스에 대한 엄격한 품질 인증 및 사후관리 체계 구축을 위한 서비스 제공자의 품질인증 가이드라인 제시

→ 신뢰성 및 공신력을 확보한 인증체계 정립을 통해 클라우드 서비스 산업의 활성화와 그린 IT산업 성장의 견인차적 역할을 수행

나. 중요성

o 클라우드 서비스는 서버, 스토리지, S/W 등을 기술적으로 통합·제공하고 이용자가 인터넷을 통하여 IT 자원을 나누어 쓸 수 있는 차세대 인터넷 서비스로서, IT 기술의 비약적 발전과 고성능·고효율 IT 자원에 대한 수요 증가 및 녹색성장에 대한 사회적 요구 등에 힘입어 차세대 인터넷 비즈니스 모델로 각광받고 있음

o 그러나 보안, 성능, 가용성 및 상호운용성 등에 대한 시장의 우려가 클라우드 서비스의 활성화에 장애요인으로 작용하고 있어 이에 대한 정책대응마련이 시급한 실정임

※ 클라우드 컴퓨팅 활성화 장애요소로 보안(1위), 성능(2위), 가용성(3위) 등이 차지함, IDC 2008

o 따라서 위와 같은 장애요소를 해소하고 클라우드 서비스 제공자와 사용자 간 신뢰 기반을 구축함으로써 클라우드 서비스 활성화를 촉진하기 위하여 국내외 유사 인증제도에 대한 심층조사 및 분석과 연관 전문가와의 협업을 통해 클라우드 서비스에 특화된 인증체계 구축에 대한 연구가 절실히 요구됨

3. 연구의 구성 및 범위

o 조사 및 분석
- 클라우드 서비스 관련 국내외 유사인증 및 SLA 조사 및 분석
- 클라우드 서비스 관련 국내외 사례 분석

o 클라우드 서비스 인증 체계 마련
- 심사영역 정립 및 심사기준 마련
- SLA 가이드라인 마련

o 클라우드 서비스 관련 전문가 활용
- 전문가 자문을 통한 심사기준 항목 및 SLA 항목 도출
- 심사기준 및 SLA 전문가 의견수렴을 통한 수정 및 보완

4. 연구내용 및 결과

o 연구내용
- 국내외 유사 인증체계에 대한 심층 조사 및 분석 연구
- 클라우드 서비스 인증영역 정립 및 인증체계 연구

· 클라우드 서비스의 구성요소 및 인증영역 정립
· 인증 심사원칙, 심사기준 및 해설서 수립
· 클라우드 서비스 SLA 가이드라인 마련

- 민·관 협력 기반의 범정부 클라우드 서비스 테스트베드와 연계한 인증체계 구축 연구
- 관련 기업 및 이용자(기관) 등의 전문가 의견 수렴을 통한 실효성 있는 인증체계 구축 연구

o 연구결과

- 클라우드 서비스 인증영역 정립 및 인증체계 연구
· 클라우드 서비스의 구성요소 및 인증영역 정립
· 인증 심사원칙, 심사기준(IaaS, SaaS) 마련
· 클라우드 서비스 SLA 가이드라인 마련

5. 정책적 활용내용

o 이용자 신뢰기반 구축을 통해 클라우드 서비스 활성화를 위한 중장기 정책 수립의 정책자료로 활용

o 클라우드 서비스 인증 도입 및 보급을 위한 인증체계 추진을 위한 자료로 활용

o 클라우드 서비스 활성화 및 비즈니스 모델 발굴에 효과적인 자료로 활용

6. 기대효과

o 이용자 신뢰기반 구축을 통해 클라우드 서비스 활성화 유도 및 국내 서비스 제공 기업체의 서비스 품질 향상을 통한 글로벌 경쟁력 강화

o 클라우드 서비스 활성화를 통한 다양한 서비스 모델 발굴 및 그린 IT 정책의 견인차 역할 수행

o 세계 클라우드 시장의 우위선점과 클라우드 서비스 개발 전문인력 양성 및 일자리 창출 기여

SUMMARY

1. Title

A Study on the introduction of the Certificate system to activate the Cloud Service

2. Objective and Importance of Research

o Establishment of the Certification area of Cloud Services, the screening criteria, SLA guidelines established

o Construction and activation of cloud services, based on trust, promoting

3. Contents and Scope of the Research

o Research and Analysis
- Similar to that of international certification, and SLA research and analysis
- A Case Study from home and abroad

o The certification scheme established Cloud Service
- Formulation and assessment criteria of assessment area
- SLA guidelines established

o Use of experts
- Advisory
- Opinions

4. Research Results

o Establishment of the Certification area of cloud services

- Component of cloud services and establish an authentication realm
- Assessment principles, criteria of assessment
- SLA guidelines established

5. Policy Suggestions for Practical Use

o Cloud Services Related government policy document

o Authentication data dissemination policy for promoting

o Enabling services and business models Cloud Base

6. Expectations

o Users to build and strengthen global competitiveness based on trust

o Identification of various cloud services model and the driving force of Green IT policies

o Preemption and job creation, market leadership

목 차

표 목 차

그 림 목 차

Contents

제 1 장 서 론

인터넷을 통해 IT 자원을 온디맨드로 빌려 사용하는 클라우드 서비스가 세계적인 차세대 IT서비스로 각광 받으면서 성장단계로 진입하기 위해 기술적 발전과 다양한 서비스 모델 등이 빠르게 개발되고 있다. 또한, 미국, 영국, 일본 등 선진국에서 클라우드 서비스의 우위 선점을 위한 경쟁이 치열해 지고 있으며, 국가 차원의 정책지원 등 많은 투자와 연구가 활발히 진행되고 있다. 그러나 이용자들의 클라우드 서비스 인식 및 신뢰기반 구축이 미흡하여, 본격적인 성장단계로 진입하기 위한 걸림돌로 작용하고 있는 것이 사실이며, 이러한 걸림돌을 선결하기 위한 연구가 반드시 필요하다.

본 보고서에서는 클라우드 서비스 이용자 신뢰기반 구축을 위한 클라우드 서비스 인증을 위한 심사기준과 클라우드 서비스 제공을 위한 SLA 가이드라인 대해 언급하였다.

제 2 장 본 론

제 1 절 국외 SLA(Service Level Agreement) 사례

국외 SLA의 사례는 IaaS 서비스의 SLA 사례를 찾아볼 수 있고, 일본의 공공부분에 ASP/SaaS를 도입하는 경우의 SLA 도입사례를 찾아볼 수 있는데 본 항에서는 이 내용을 중심으로 기술하기로 한다.

1. 랙스페이스(rackspace)의 클라우드 서버와 클라우드 파일의 SLA 사례

미국 주요 호스팅 업체 중 하나인 랙스페이스(Rackspace)가 사용한 만큼 지불하는 방식의 서버 인스턴스(Instance)와 온라인 스토리지 서비스를 개시하면서 클라우드 컴퓨팅 시장에 본격 진입

2008년 5월 베타모드의 클라우드 스토리지 서비스인 클라우드 파일(Cloud Files)을 공개한 바 있는 랙스페이스는 베타 서비스를 종료하고 2009년 3월 정식 온라인 스토리지 서비스를 개시하는 것과 동시에 아마존의 EC2 서비스와 유사한 온디맨드 방식의 스토리지와 컴퓨팅 서비스 스위트인 클라우드 서버(Cloud Servers)를 새로이 발표했다.

1) 클라우드 서버 서비스

클라우드 서버 서비스는 2009년 3월 16일부터 이용할 수 있으며, 비용은 시간당 1.5센트, 또는 월 10.95달러부터 시작한다. 하지만 아직 서비스가 초기 단계라 클라우드 서버 API가 아직 준비되지 않은 상태이다. 또한 현재 클라우드 서버를 다양한 리눅스 플랫폼을 기반으로 애플리케이션을 실행할 수 있지만, 아직 윈도우 운영체제는 지원하지 않는다.

클라우드 서버 서비스는 사용자가 호스팅 할 인프라스트럭처에 관한 모든 제어권을 사용자에게 부여한다. 각 클라우드 서버는 전체적으로 사용자의 요청에 맞추어 자원을 할당하고, 사용 시간당 요금청구, 그리고 가상화된 개인의 컴퓨터 프로파일을 완벽히

접근하고 제어할 수 있다.

Xen 가상화 기술을 바탕으로 한 클라우드 서버는 일반적인 서버와 같이 자바 웹사이트부터 Ruby on Rails의 어플리케이션까지 사용할 수 있는 유연성을 가지고 있다.

(1) SLA(Service Level Agreement) 정책

SLA 정책은 <표 2-1>과 같은데, Network, Data Center, Infrastructure, Cloud Server Hosts, Migration별로 각각의 정책을 제시하고 있다.

<표 2-1> 클라우드 서버 서비스의 SLA 정책

분 류	내 용
Network	We guaranty that our data center network will be available 100% of the time in any given monthly billing period, excluding scheduled maintenance.
Data Center Infrastructure	We guaranty that data center HVAC and power will be functioning 100% of the time in any given monthly billing period, excluding scheduled maintenance. Infrastructure downtime exists when Cloud Servers downtime occurs as a result of power or heat problems.
Cloud Server Hosts	We guaranty the functioning of all cloud server hosts including compute, storage, and hypervisor. If a cloud server host fails, we guaranty that restoration or repair will be complete within one hour of problem identification.
Migration	If a cloud server migration is required because of cloud server host degradation, we will notify you at least 24 hours in advance of beginning the migration, unless we determine in our reasonable judgment, that we must begin the migration sooner to protect your cloud server data. Either way, we guaranty that the migration will be complete within three hours of the time that we begin the migration.

(2) 클라우드 파일 서비스

클라우드 파일 서비스는 온라인으로 무제한적으로 스토리지를 제공한다. 또한

Limelight Network의 CDN(Content Delivery Network) 서비스를 통해 매우 빠른 전송 속도를 보장한다.

클라우드 파일 서비스에는 사용자의 스토리지 공간을 사설용 컨테이너(Private Containers)와 공공용 컨테이너(Public Containers) 두 가지 타입을 제공한다. 사설용 컨테이너는 사용자와 클라우드 파일 서버 간에 SSL로 암호화된 채널을 통해 전송된다. 공공용 컨테이너는 웹 URL을 통해 받을 수 있으며, 다른 사람과의 공유도 가능하다.

(가) SLA(Service Level Agreement) 정책

SLA 정책은 <표 2-2>와 같은데, Guaranty, Unavailability별로 각각의 정책을 제시하고 있다.

<표 2-2> 클라우드 파일 서비스의 SLA 정책

분 류	내 용
Guaranty	We guaranty that Cloud Files service will be available 99.9% of the time in a given billing cycle. If we fail to meet this guaranty, you will be eligible to receive a credit to your account. The credit will be calculated as a percentage of your last billed fee for the Cloud Files service, or at your option, your fee for the current billing cycle (to be applied at the end of the billing cycle). Credits will be based on the duration of the unavailability that exceeds the 99.9% threshold as defined below.
Unavailability	Unavailability means: (i) The Rackspace Cloud network is down, or (ii) the Cloud Files service returns a server error response to a valid user request during two or more consecutive 90 second intervals, or (iii) the Content Delivery Network fails to deliver an average download time for a 1-byte reference document of 0.3 seconds or less, as measured by The Rackspace Cloud's third party measuring service. Unavailability due to scheduled maintenance is excluded from these conditions and does not contribute towards unavailability calculations.

2. Amazon Elastic Compute Cloud(EC2)의 SLA 사례

아마존의 EC2 서비스는 웹 기반 서비스로서 클라우드에서의 컴퓨팅 자원의 크기를 자유롭게 재조정할 수 있는 서비스를 제공하고 있으며, 또한 EC2는 사용자가 지정한 모든 컴퓨팅 자원의 제어권 부여 및, 아마존이 검증한 컴퓨팅 환경을 사용할 수 있도록 하고 있다.

아마존 EC2는 새로운 서버 인스턴스를 만들고 부팅하는 시간을 단축시킬 뿐만 아니라 사용자로 하여금 쉽고 빠르게 원하는 컴퓨팅 자원에 따라 증가시키거나 감소시킬 수 있다. 그리고 아마존 EC2는 가상 컴퓨팅 환경을 제공하며 그것은 웹 서비스 기반 인터페이스로 다양한 OS의 인스턴스들을 시작할 수 있게 해준다. 또한, 사용자가 만든 어플리케이션 환경을 로드할 수 있게 해주고, 네트워크 접근 권한 관리, 마지막으로 사용자가 원하는 만큼의 인스턴스들을 사용할 수 있도록 서비스한다.

EC2를 사용하기 위해선 단순히 사용자의 어플리케이션, 라이브러리, 데이터, 관련된 설정을 포함한 아마존 머신 이미지(AMI)를 만들고 그 AMI를 아마존 S3에 업로딩한다. 여기서 EC2는 이미지를 보관하는데 있어 쉽고 간단하게 할 수 있는 툴을 제공한다. 사용자는 제공되는 아무 타입의 인스턴스나 OS를 선택하여, 원하는 만큼의 AMI를 제공되는 웹 서비스 API나 많은 관리 도구를 사용하여 시작, 종료, 관리할 수 있다.

EC2는 사용자로 하여금 IaaS와 같이 인프라스트럭처를 골라 AMI를 만들고 로드하여 부팅할 수 있는 서비스를 제공한다. 그렇기 때문에 사용자는 사용자가 원하는 infrastructure를 고를 수 있으며, 또한 PHP, Perl, VB.NET, C#, JAVA, RUBY과 같은 웹 개발언어로 사용가능 자원, 관리는 사용자가 관리할 필요 없이 웹 프로그램, 도메인을 사용합니다. 요금에 따른 제한이 있지만 무한적인 자원을 제공해 개발할 수 있는 플랫폼도 제공한다.

1) SLA(Service Level Agreement) 정책

아마존 (EC2)의 SLA 정책은 <표 2-3>과 같은데, Credit Request and Payment Procedures와 SLA의 예외 내용을 각각 제시하고 있다.

<표 2-3> 아마존 EC2의 SLA

분 류	내 용
Definitions	"Service Year" is the preceding 365 days from the date of an SLA claim. "Annual Uptime Percentage" is calculated by subtracting from 100% the percentage of 5 minute periods during the Service Year in which Amazon EC2 was in the state of "Region Unavailable." If you have been using Amazon EC2 for less than 365 days, your Service Year is still the preceding 365 days but any days prior to your use of the service will be deemed to have had 100% Region Availability. Any downtime occurring prior to a successful Service Credit claim cannot be used for future claims. Annual Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon EC2 SLA Exclusion (defined below). "Region Unavailable" and "Region Unavailability" means that more than one Availability Zone in which you are running an instance, within the same Region, is "Unavailable" to you. "Unavailable" means that all of your running instances have no external connectivity during a five minute period and you are unable to launch replacement instances. The "Eligible Credit Period" is a single month, and refers to the monthly billing cycle in which the most recent Region Unavailable event included in the SLA claim occurred. A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon EC2 account. Service Commitments and Service Credits If the Annual Uptime Percentage for a customer drops below 99.95% for the Service Year, that customer is eligible to receive a Service Credit equal to 10% of their bill (excluding one-time payments made for Reserved Instances) for the Eligible Credit Period. To file a claim, a customer does not have to have wait 365 days from the day they started using the service or 365 days from their last successful claim. A customer can file a claim any time their Annual Uptime Percentage over the trailing 365 days drops below 99.95%.

분 류	내 용
Credit Request and Payment Procedures	To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request @ amazon.com. To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of Region Unavailable that you claim to have experienced including instance ids of the instances that were running and affected during the time of each incident; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within thirty (30) business days of the last reported incident in the SLA claim. If the Annual Uptime Percentage of such request is confirmed by us and is less than 99.95% for the Service Year, then we will issue the Service Credit to you within one billing cycle following the month in which the request occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.
Amazon EC2 SLA Exclusions	The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2, or any other Amazon EC2 performance issues: (i) that result from Service Suspensions described in Section 7.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances not attributable to Region Unavailability; or (vi) arising from our suspension and termination of your right to use Amazon EC2 in accordance with the AWS Agreement (collectively, the “Amazon EC2 SLA Exclusions”). If availability is impacted by factors other than those explicitly listed in this agreement, we may issue a Service Credit considering such factors in our sole discretion.

3. 일본의 공공부분의 ASP/SaaS 도입시 SLA 적용 사례

본 항에서는 일본 총무성이 발행한 「공공 IT에서 아웃소싱에 관한 가이드라인」에 근거하여 각 지자체가 작성한 사례이다. 이 SLA는 IDC에 관련된 것으로, 표 안에 설정치가 없는 경우에도, 어플리케이션 구축시마다 추가 검토할 수 있다. 또, 발주자 측이 정기적으로 감사를 실시할 때, 아래의 SLA에서 요구된 자료를 제출하도록 한다.

가. 호스팅

SLA 평가항목과 설정치는 <표 2-4>와 같다.

<표 2-4> 호스팅에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
기기제공 서비스	기기종별	퍼포먼스요건, 가동요건에 합치되는 서버 워크스테이션, 네트워크기기를 선택・구성한다. 시스템의 필요에 따라, 고가용성, 고퍼포먼스, 부하분산환경 등을 선택한다.	-	-
	가용성감시	제공하는 기기에 대해, 일정간격으로 가동감시를 실시한다. 감시 항목으로는, 네트워크 인터페이스와 URL응답을 감시서버로부터 감시한다.	・감시간격 ・감시시간 ・통지시간	경쟁 입찰에 의한다.
	퍼포먼스감시	제공된 기기에 대해, 일정간격으로 퍼포먼스 감시를 실시한다. 감시항목으로서 하드웨어와 OS(CPU사용률, 메모리, 스와프 점유율, 디스크 부하율 등), 미들웨어(어플리케이션의 감시가 아니라, 미들웨어가 어플리케이션의 서비스 제공에 충분한 성능을 발휘하고 있는가를 감시한다.)의 퍼포먼스를 감시한다. 또한, 이 감시는 수용능력(capacity)을 위한 것이 아니며, 어플리케이션의 감시는 포함하지 않는다.	・감시간격 ・감시시간 ・통지시간	경쟁 입찰에 의한다.
	장해감시	핑(Ping)의 응답, 감시툴에 의해 장해감시를 행한다.	사활(死活) 감시	1회/5분
	서비스시간	기기의 서비스시간을 규정한다. 설비, 네트워크 등의 점검, 보수를 위한 계획정지시간, 계획정지 통고기간・방법, 가동률을 규정한다. ※ 설정치 작성 시, 99% 이상(어플리케이션 규정 이상의 수치로 설정할 것)	・인프라 보수시간 ・가동률	경쟁 입찰에 의한다.

	시각동기	시스템의 시각동기(時刻同期) 방법을 규정한다.	-	-
	보고	가용성, 퍼포먼스감시의 결과를 보고한다. 또, 발생한 장해에 대한 대응상황(인프라, 서버에 발생한 장해의 내용, 발생이유, 대응경위, 실시작업 등)을 보고한다. 또 문제상황 보고는 사전에 설정한 중요도, 긴급도가 높은 것에 따라 적용한다.	보고 타이밍	대응 후 1일 이내 준수율 99.9%
소프트웨어 제공서비스	소프트웨어종별	요건에 합치되는 OS나 미들웨어를 선택·구성한다. 시스템의 필요성에 따라서, 고가용성, 고퍼포먼스, 부하분산환경을 선택한다.	-	-
소프트웨어 제공서비스	퍼포먼스감시	소포트웨어제공서비스로서 제공된 소프트웨어에 대해, 일정간격으로 퍼포먼스 감시를 실시한다. 감시항목으로서 하드웨어와 OS(CPU 사용률, 메모리, 스와프점유율, 데스크 부하율 등), 미들웨어(어플리케이션의 감시가 아니라, 미들웨어가 어클리케이션의 서비스 제공에 충분한 성능을 발휘하고 있는가를 감시한다.)의 퍼포먼스를 감시한다. 또, 이 감시는 수용능력을 위한 것이 아니며, 어플리케이션의 감시는 포함하지 않는다.	·감시간격 ·감시시간 ·통지시간	경쟁 입찰에 의한다.
	장해감시	감시툴을 이용하여 장해감시를 행한다	사활감시	1회/도5분
	서비스시간	소프트웨어의 서비스시간을 규정한다. 설비, 네트워크 등의 점검, 보수를 위한 계획정지시간, 계획정지통고기간·방법, 가동률을 규정한다. ※ 설정치 작성 시, 99% 이상(어플리케이션 규정 이상의 수치로 설정할 것)	·인프라보수시간 ·가동률	경쟁 입찰에 의한다
	시각동기	시스템의 시각동기의 방법을 규정한다.	-	-
	보고	퍼포먼스 감시결과를 보고한다. 또, 장해 시에 발생한 장해에 대한 대응상황(인프라, 서버에 발생한 상해의 내용, 발생이유, 대응경위, 실시작업 등)을 보고한다. 또한 문제상황보고는 사전에 호스팅업자와 살정한 중요도 긴급도가 높은 것에 적용한다.	보고 타이밍	대응후 일일 이내 준수율 99.9%
오퍼레이션 서비스	정기작업 대행	호스팅 업자가 제출한 작업절차서를 토대로, 정기적인 작업을 실시한다.	-	-
	부정기작업 대행	문제에 대응하기 위해 서비스 이용자의 지시에 근거, 부정기적인 작업을 실시한다.	오퍼레이터 스킬	경쟁 입찰에 의한다.
	기기교환	기기고장, 트러블슈팅의 일환으로서, 예비기로 교환을 행한다. 기기교환 시에는 하드웨어, OS까지의 복구를 서비스 범위로서 실시한다.	-	-

	기기가동 감시	서비스대상기기에 대해, Ping에 따라 활성/비활성감시를 실시한다.	-	-
		서버 운용 감시 절차서를 명시한다.	-	-
백업/복구 서비스	백업	서비스이용자가 기기제공을 받는 서버에서 저장영역(storage area)을 제공받는 경우, 사전에 조정한 주기, 시간에 정기 백업을 실시한다. 업무시스템마다 SLA가 있어서, 여기서는 규정하지 않는다.	-	-
	복구	서비스이용자로부터의 지시에 근거해서, 지정된 영역에 복구 작업을 실시한다.	-	-

나. 보안

SLA 평가항목과 설정치는 <표 2-5>와 같다.

<표 2-5> 보안에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
네트워크 보안	방화벽	방화벽에 의해 모든 통과 패킷(packet)을 체크한다.	-	-
	네트워크 부정침입 탐지(IDS)	부정침입탐지시스템을 도입하고, 정상적으로 가동시킨다. 침입탐지를 위해, 통과하는 모든 패킷의 패턴을 해석하고, 부정으로 보이는 패킷의 보고를 행한다.	서명 (패턴파일)의 갱신간격	판매자의 배포로부터 24시간 이내/24시간부터 3일 이내, 등
	리버스 프록시	외부로부터의 공격목표가 될 수 있는 정보가 누출되지 않도록 대책을 취한다.		
메일보안	바이러스 체크	메일에 첨부된 모든 비암호화 파일에 대해 파일체크를 실시한다.	패턴파일의 갱신간격	판매자의 배포로부터 24시간 이내/24시간부터 3일
웹보안	바이러스 체크 (웹서버)	다운로드된 모든 비암호화 파일에 대해 바이러스체크를 실시한다.	패턴파일의 갱신간격	판매자의 배포로부터 24일 이내/24시간에서 3일 이내

	인증 (웹서버)	인증기반을 통한 엄밀개인인증(단, 어플리케이션서비스로서 규정되어야 한다.)	인증방법	인증기반을 이용한 인증/ ID 패스워드 등
웹보안	부정침입 탐지 (웹서버)	비권한자에 의한 부정한 서버침입에 대한 탐지를 실시한다.	서명 (패턴파일)의 갱신간격	판매자의 배포로부터 24시간 이내24시간 부터 3일
서버보안	파일체크 (서버)	파일액세스 시에 모든 비암호화파일에 대해 바이러스체크를 실시한다.	패턴파일의 갱신간격	판매자의 배포로부터 24시간 이내24시간 부터 3일
	인증(서버)	본인이 접속하고 있는 것의 인증을 행한다.	인증방법	인증기반을 이용한 인증/ ID 패스워드 등
	부정침입 탐지 (서버IDS)	비권한자에 의한 부정한 서버침입에 대한 탐지를 실시한다.	서명(패턴파일)의 갱신기간	판매자의 배포로부터 24시간 이내24시간 부터 3일
	OS, 미들웨어의 보안패치 관리	OS, 미들웨어의 보안패치관리를 실시한다.	-	판매자의 배포로부터 24시간 이내에 패치실험 개시/ 24시간에서 3일이내 패치실험 개시 등.
	원본성 (原本性) 확보(데이터)	데이터(전자문서)의 원본성 확보를 행한다.	원본성 확보법	-
	원본성 확보(종이 출력문서)	출력한 종이서류의 원본성 확보를 행한다.	-	-
	타임스탬프 인증서비스	타임스탬프(일,시각의 同期・인증) 기능을 갖춘다.	-	-

	데이터 암호화	데이터의 암호화와, 키의 발행 및 관리를 행할 수 있다.	-	-
디렉터리 서비스	유저정보의 보호・관리	보안의 각서비스요건을 채우기 위한, 유저정보(주민, 기업, 직원)의 운용・관리를 행한다.	-	-
	인증	본인이 접속하고 있는 것의 인증을 행한다.	인증방법	인증기반을 이용한 인증/ ID 패스워드 등
	데이터암호화	데이터의 암호화와 키의 발행 및 관리를 행한다.	-	-
단말보안	바이러스 체크	모든 비암호화 파일에 대해, 바이러스체크를 실시한다.	패턴파일의 갱신간격	판매자의 배포로부터 24시간 이내24시간부터 3일
	인증	본인이 사용하고 있는 것의 인증을 행한다.	인증방법	인증기반을 이용한 인증/ ID 패스워드 등
	데이터 암호화	데이터의 암호화와 키의 발행 및 관리를 행한다.	-	-
운용관리	보고	정기적 혹은 수시로 보안 서비스 운용상황에 대해 보고를 행한다.	-	-
		부정침입, 바이러스 침입 등 문제가 발생한 경우, 수시연락을 행한다.	보고	보고30분 이내/대처시간은 협의해서 결정한다.
	매체나 종이에 출력한 정보 등의 적정한 관리	도난분실이나 정보누출 등을 박기 위해, 관리운용방법에 대해, 사전에 규정하여, 제출한다.		
	서버룸의 보안 운영 관리절차서	미야자키현(宮崎懸)에서 정한 보안정책에 따라, 운용에 관한 상세한 규칙을 정리하여 제출한다.		
	관리절차서의 갱신	환경 등의 변화를 포함해서, 항상 갱신을 한다.	수정기간	1년
감사	감사체제의 검토	발주자가 실시하는 감사에 따라, SLA의 준수상황을 필요시에 제출한다.	-	-

다. 네트워크

네트워크에서 SLA 평가항목과 설정치는 <표 2-6>와 같다.

<표 2-6> 네트워크에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
인터넷 접속서비스	백본접속 회선의 대역	ISP가 소유하는 백본네트워크에 접속하는 회선의 대역	대역보증	경쟁입찰
	백본대역	ISP가 소유하는 백본네트워크의 대역	네트워크 내의 지연시간	경쟁입찰
	부여 어드레스 수	서비스 이용자가 소유한 기기에, ISP가 소유한 IP 어드레스를 부여해서 사용하는 경우, 부여하는 IP 어드레스 수	장해복구 시간	경쟁입찰
	확장성	회선의 대역을 늘리고 싶은 경우 등에, ISP가 대응 가능한 기간	보수응답 시간 ※장해복구 시간	탐지 후 60분 이내 연락 준수률: 99.9%
	감시 · 통보	ISP가 소유하는 네트워크를 감시하고, 장해를 통보하는 시간대		
	보고 ※단체계약 시만	ISP가 소유하는 설비의 상황에 관해, 문서나 웹으로 트래픽 상황의 열람을 통해 보고를 행한다. ※내용으로서는 서비스를 총괄하는 네트워크 관리자를 대상으로 한다.		
IDC로 부터의 청사간(廳舍間)네트워크 접속	대역	대역을 보증하는(평균치에서 보증하는 타입, 최고치에서 보증하는 타입 등) 타입의 회선 접속서비스에서 접속회선의 대역	대역보증	경쟁입찰 1Gbps 이상
	감시 · 통보	네트워크를 감시하고, 장해를 통보하는 시간대	통보시간	감지 후 60분

서비스	확장성	접속하는 회선의 대역을 늘리고 싶은 경우에, 서비스 제공사업자가 대응 가능한 기간		이내의 연락 준수율: 99.9%
백업회선 접속서비스	대역	대역을 보증하는(평균치에서 보증하는 타입, 최고치에서 보증하는 타입 등) 타입의 회선 접속 서비스에서 접속회선의 대역	대역보증	경쟁입찰 50-100Mbps
	감시·통보	네트워크를 감시하고, 장해를 통보하는 시간대	통보시간	탐지 후 60분 이내의 연락 준수율: 99.9%
	확장성	접속하는 회선의 대역을 늘리고 싶은 경우에, 서비스제공사업자가 대응 가능한 시간		

라. 하우징

하우징에서 SLA 평가항목과 설정치는 <표 2-7>과 같다

<표 2-7> 하우징에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
건축물	주소	설치장소는 현내(시내에 있는 것이 보다 바람직하다)에 있을 것.	주소	현내
	빌딩내지니구조	건축기준법에 적합한 내진설계를 행한다. 진도 7급의 지진에 견딜 수 있을 것을 필수항목으로 한다.	적용건축시행기준 내진수치	있음 진도 7
	면진(免震)구조	지진의 흔들림을 흡수하고 건물내에 수용하는 장치등에 치명적인 손해를 입히지 않는 내진성능을 보유하는 방법으로서 면진구조·제진구조인 것이 바람직하다.	면진구조 제진(制震)구조	있음 있음
	수해대책	컴퓨터실 및 그와 관련된 시설이 저지에 위치할 경우에는 수해를 고려하고, 건물에 영향을 미치지 않도록 배수설비를 완비하는 것이 바람직하다.	배수대책의 완비 등	있음
	바닥면	저장고 등의 설치를 고려한 하중에 견딜 수 있는 구조로 한다.	최대 바닥하중	래크에어리아(rack area) 500kgf/㎡이상
공간제공 서비스	내장재	플로어의 내장재는 불연재를 사용한다.	불연재	사용

	주차장	컴퓨터실의 입관자의 교통수단이 주로 자동차임을 상정하고, 자차공간의 확보가 되어 있는 것이 바람직하다.	-	-
	IT기기설치공간	구획된 독립공간을 제공한다.	구획된 독립공간	-
	수용래크(rack)의 확장성	어플리케이션의 증가에 대응 가능한 것	증설가능한 설치공간	-
	조명 및 비상등	작업에 필요한 조명, 비상시의 비상등을 제공한다.	-	-
	방진	실내의 방진대책(방진도장, 에어컨디셔닝)을 실시하고 제공한다.	-	-
	피난경로	건축기준・소방법준거의 피난경로를 확보하고 제공한다.	-	-
	위스커(whisker)방책	바닥하부재의 아연으로부터 생기는 위스커의 발생대책이 서 있을 것.	위스커방책	있음
전원제공서비스	수전방법	장해시의 전원확보를 위해, 두 선의 수전 루트를 보유할 것.	수전방법	이회선 숫전방식 이상
	변전소 루트	동일발전소에서 장해를 피하기 위해 별도의 급전루트를 선택 할 수 있도록 한다.	별도의 급전 루트	-
	수전용량	수전용량은 장래의 수용계획에 근거해서 결정할 것. (서버 에어리어의 전원용량, 운용기기전원용량, 시설설비전원용량). 예를 들어 750W/㎡ 이상(역률0.8로 견적을 가진 경우)	수전용량	750W/㎡ 이상(역량 0.8의견적을가진 경우)
	지속성	법정점검이나 공사 시에도 전력 공급을 멈추는 일 없이, 컴퓨터실 내에 전력을 공급할 수 있는 지속구성일 것.	-	-
	무정전 전원장치(밧데리)	설치시스템이 동작하기 위해 필요한 전력용량을 10분이상 공급 가능한 능력을 확보할 것.	전력공급 시간	10분이상
	비상용 전원 (발전기)	비상용으로 자가발전설비를 설치해서, 서버 에어리어의 전원용량, 운용기기 전원용량, 시설설비 전원용량에 이상이 생겼을 때, 24시간 이상의 가동이 가능한 연료를 확보할 것.	연속가동 시간	10분이상

	전력설비 감시	전력설비의 집중감시가 가능할 것.	집중감시	있음
에어컨디셔닝서비스	에어 컨디셔닝 용량	설치되어 있는 IT기기에 의한 발열을 억지할 만큼 충분한 용량의 에어컨디셔닝을 제공한다.	에어 컨디셔닝 용량	총발열량의 115% 이상
	에어 컨디셔닝 가동시간	24시간 연속애서 에어컨디셔닝을 제공한다.	가동시간	24시간 연속운전
	습도 · 습도조절	래크 주위의 온도를 적정하게 유지하고, 오작동 하지 않으며, 사계절을 불문하고 이슬이 발생하지 않게 설정한 온도, 정정 습도의 유지가 가능하다.	-	-
	에어커디셔닝타입(송풍방법)	래크 아래로 송풍하는 형과 래크 위로 송풍하는 형	래크 위/아래 송풍	있음
	에어컨디셔닝 감시	공조설비의 집중감시가 가능할 것.	집중감시	있음
	예비 에어컨디셔닝(지속성)	에어컨디션설비 한 대가 고장나도 전체에 영향을 끼치지 않는 시스템을 구성할 것. (필요수 + 1이상의 구성)	예비에어 컨디셔닝	1대이상
	누수탐지 시스템	에어컨디셔너로부터 IT기기설치공간의 누수가 없도록, 에어컨디셔너 및 배수관 주위에 누수탐지시스템을 설치한다.	누수탐지 시스템	있음
소화설비제공서비스	컴퓨터실 내부 소화설비	스프링클러로 손실을 방지하고, 통전시의 화재방지를 위해 가스선 소화설비를 설치할 것.	소화설비	가스선 소화설비
	사무소 지역 소화설비	스프링클러, 소화기기 등 소화설비를 설치	소화설비	있음
	화재감지 · 보고시스템	화재를 자동적으로 탐지하는 방법으로, 열감지기, 연기감지기, 재감지기가 있다. 우선 사람이 발견해서 통보하는 수동보고를 갖출 것. 또 비상방송설비, 방화방배연설비, 각종소화설비와 연동하고 있을 것.	화재탐지 시스템	있음.
	소화설비 감시	소화설비의 집중감시가 가능할 것.	집중감시	있음.
피뢰 · 정전기대책설비제공서비스	직격뢰 대책	국내의 건축설비설계기준상, 빌딩 구조 상 옥상에 피뢰침을 의무적으로 설치하도록 되었다. 피뢰침과 대지와의 접지, 또는 보호하고 싶은 설비기기에 뢰대책장치를 부착해서, 대지와 접지를 충분히 고려한 대책을 강구 할 것.	직격뢰대책	있음

	유도뢰대책	전기설비기술기준에 의거, 이하의 대책을 강구할 것. 1. 고압전원계통대책으로서, 전원계통은 모두 유도뢰의 영향을 받지 않는 시공방법을 채용할 것. 혹은 가공(架空)선을 끌어들일 경우 전력회사로부터 수전하는 포인트(수전점)에 피뢰기를 설치 할 것. 2. 컴퓨터실의 설비기기대책으로서, 유도뢰의 영향을 받지 않는 시공방법을 채용할 것. 혹은 컴퓨터실의 분전반에 피뢰기를 설치할 것. 3. 근린에 낙뢰가 발생하면 대지전압이 상승하고 건물로 흘러들어갈 것으로 상정하고, 접지계통에서의 뢰노이즈(noise)침입대책으로 접지선용 피뢰기를 설치한다. 또 뢰노이즈침입 시에 접지극간의 전위차를 없애는 대책이 취해 져야 한다.	1. 유도뢰의 영향을 받지 않는 시공 방법(지중선을 끌어들이는 등)의 유무, 혹은 가공선을 끌어들이는 경우, 피뢰기의 최대방전 서지(serge) 전류 규격치 2. 유도뢰의 영향을 받지 않는 시공방법(지중선을 끌어들이는 등)의 유무, 혹은 분전반에 설치하는 피뢰기의 최대방전 서지전류규격치 3. 접지계통으로부터의 뢰노이즈대책의 유무 4. 약전설비의 뢰노이즈대책의 유뮤	1. 유도뢰의 영향을 받지 않는 시공방법... 만약 가공선을 끌어들이는 경우, 피뢰기의 최대방전 서지전류 규격치 40kA 이상 2. dv도뢰의 영향을 받지 않는 시공방법 만약 가공선을 끌어들이는 경우, 피뢰기의 최대방전 서지전류 규격치 40kA 이상 3. 약전설비의 뢰노이즈대책의 유무

	정전기 대책	정전기대책 리스트바인드의 착용, 에어컨디셔닝 기기에 의한 정전기 방지대책, 정전기 바닥대책, 정전기 방지 슈즈를 사용하는 등의 대책을 취한다. 또 작업자의 정전기 대책에 관한 작업절차서를 명시한다.	-	-
래크(rack) 제공서비스	내역	래크 탑재형의 IT기기의 탑재가 가능한 것으로 제공한다.	-	-
	규격	EIA규격준거 19인치래크를 제공한다.	-	-
	탑재중량	IT기기의 총중량의 탑재가 가능한 것을 제공한다.	탑재중량	300Kg정도
	선반	래크탑재형이 아닌 IT기기를 래크에 탑재할 수 있는 선반을 제공한다.	-	-
	콘센트・형상	NEMA5-15 상당의 콘센트 형상으로 제공한다. (접지형 2극 115A/125V)	형상	설치형 2극 15A/125V
	래크잠금	래크는 잠글 수 있고, 서비스 이용자 또는 허가에 의하지 않는 한 열릴 수 없도록 관리할 것. 또 관리방법을 명확히 해서, 열쇠를 두는 상소, 이용자의 제한 등을 열쇠관리절차서에 명시한다.	-	-
빌딩에서의 보안 서비스	입퇴관・입퇴실 관리	입퇴실기록과 감시카메라, IC카드나 바이오메트릭스등 개인인증시스템에 의해, 입퇴실이 허가된 사람으로 제한된다.	입퇴실기록 감시카메라 개인인증 시스템	있음 있음 있음
		오퍼레이터・청소 등을 담당한 위탁업자에 대해서는 성명관리를 시행할 것. 성명의 명부는 발주자 측에 제공할 것. 담당자의 변경이 있는 경우, 즉시 보고할 것.	위탁업자의 성명관리	있음
		컴퓨터실 입퇴관・입퇴실관리에 관한 절차서를 명시할 것.	컴퓨터실 입퇴관・입퇴실 관리절차서	있음
		입퇴실의 기록에 대해서는, 2년간 데이터로서 보존할 것. 또한, 발주자 측으로부터 요구된 경우는, 항상 제출 가능하도록 할 것.	입퇴실기록	2년간
	열쇠관리	컴퓨터실의 열쇠(긴급시 사용), 래크의 열쇠, 정보매체관리고의 열쇠 운용관리절차서를 작성한다. 서비스이용자 또는 허가된 자로부터의 요청이 없는 한은 개방 되지 않도록 관리할 것. 또 관리방법을 명확히 하고, 열쇠를 두는 장소,	-	-

		이용자의 제한 등을 열쇠관리절차서에 명시한다. 또한, 열쇠담당자의 성명을 발주자에 제출하고 담당이 변경되었을 때는 반드시 서류로 보고할 것.		
	입관가능 시간	24시간 365일로 한다.	입관가능 시간	24시간 365일
	모니터 감시	감시카메라 등의 감시에 의해, 24시간 365일의 감시를 행한다.	가동시간	24시간 365일
	감시영상 기록(보존 기간)	1개월 이상의 보존이 가능할 것.	보존기간	1개월 이상
빌딩에서의 보안서비스	감시 카메라의 감시 범위율	추적식 감시카메라나 고정식 카메라를 활용하고 입구부터 사무실, 컴퓨터실까지의 감시범위가 거의 100%의 비율일 것.	감시범위	거의 100%
	입실 도어	입실 도어 그 자체가 파괴되지 않도록 방책하고, 창문이 없도록 하는 등 외부로부터 보이지 않도록 대책을 세운다.	파괴대책 도어	있음
	오퍼 레이터 상주시간	오퍼레이터의 상주시간을 24시간 365일로 한다.	상주시간	24시간 365일
	오퍼 레이터 상주대응	상주 오퍼레이터용 휴게실, 취침실	휴게실, 취침실	있음
	전실	바이오메트릭스 인증을 통해 체크한다.	전실	있음

	매체보관	자기테이프나 광디스크 등 데이터미디어류의 보관장소의 구조는, 에어컨디셔닝 설비, 가스소화설비를 갖춘 보관고를 이용할 것.	에어컨디셔닝 설비, 가스소화 설비	있음 있음
		입퇴실에 관해서는 IC가드나 바이오메트릭스 등 개인인증시스템을 사용하는 등 철저한 보안을 도모할 것.	개인인증 시스템	있음
		데이터미디어류 그 자체의 보관에 대해서는, 보관고 내에 시건장치가 되어 있는 방화금고를 설치해서 보관할 것.	방화금고	있음.
		매체 및 매체 보관에 관한 관리절차를 명시할 것.	관리절차	있음.

마. 서비스 서포트

서비스 서포트에서 SLA 평가항목과 설정치는 <표 2-8>와 같다.

<표 2-8> 서비스 서포트에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
· 고장대응 · 업무문의 · 작성의뢰	· 서비스창구 (전화/팩스/웹/메일 등) · 서비스 시간대 (영업시간, 휴업일 등) · 동시접속 건수 · 긴급시 콜 건수	좌측의 요건들을 토대로, 콜센터에서 올라온 고장대응, 업무문의, 작업의뢰를 접수한다.	가동률	99.5%
			방기율	모든 문의전화의 5%미만
			문의전화 반복 비율	전요구 건수의 5%미만
			백로그율	전요구 건수의 5%미만
			응답시간 준수율	30초이내 90%이상
			기준시간 완료율	전요구 건수의 90%이상
	고객정보의 보호	문의 등에 관련될 수 있는 고객정보에 대한 관리방법을 명시한다.	고객정보관리방법	있음.

사. 어플리케이션

어플리케이션에서 SLA 평가항목과 설정치는 <표 2-9>와 같다.

<표 2-9> 어플리케이션에서 SLA 평가항목과 설정치

서비스 메 뉴	서비스 요 건	설명	SLA 평가항목	SLA 설정치
업무제공 서비스	업무요건	제공된 업무의 구체적인 범위, 내용	어플리케이션 단체에서는 SLA가 정해져 있지 않기 때문에 어플리케이션만 단독으로 계약하는 경우는 없다. (전술한 바처럼, 타서비스와의 조합을 이룬 SLA에 대해서는 총무성 가이드라인 5.10토탈 SLA를 참조할 것)	
		제공된 화면의 구체적인 내용(레이아웃, 표시·입력항목의 설명, 입력방법 등)		
		제공된 장표의 구체적인 내용, 센터 출력의 경우는 그 출력방법(레이아웃, 대상, 인쇄항목의 정의, 페이지브레이크의 타이밍, 특수용지의 사용 등.		
		이용자 측에서 설정가능 한 파라미터의 내용 등		

		제공된 타시스템과의 접속인터페이스의 종류 등(예: 외부와의 주고받는 인터페이스 등)		
	동작요건	지원된 하드웨어 종류·사양(예: PC/PD/FAX 등, 제공되는 단말기 성능, 메모리용량, 하드웨어 용량, 필요한 화면해상도, IC카드리더 등 특정한 주변기기가 요구되는 경우에는 그 종류와 성능 등)	상기와 같다.	상기와 같다.
		지원된 OS의 종류, 버전, 패치 등을 요구하는 경우는 그 패치의 버전(예: SP1이하 등)		
		지원된 RDBMS의 종류, 버전, 패치 등을 요구하는 경우는 그 패치의 버전		
		지원된 브라우저 등의 버전, 패치 등을 요구하는 경우는 그 패치의 버전		
		지원된 조작 인터페이스 종류		
업무제공 서비스	서비스량의 요건	어플리케이션의 이용가능시간(예: 평일 8시부터 20시, 24시간 365일)	상기와 같다.	상기와 같다.
		정기보수 등의 기능정지예상시간 및 횟수(예:연말연시 12/28부터 1/3은 휴지 등)		
		동시접속가능단말수(예: 동시접속 20대, 20섹션 등)		
		최대데이터량(예: 최대바이트수, 마스터의 최대리코더수, 트렌젝션량 등, 보존기간)		
		최대이용자등록수(예: 어플리케이션에 등록하는 최대 어카운트 수)		
		장해시의 연락방법, 대응방법 등		
		어플리케이션 유지이 내용, 빈도(예: 정상적 법개정에 대한 대응, 별도요금의 유무, 표준적 대응기간)		
		미들웨어 패치의 대응방법		
		데이터 백업의 대상, 빈도, 백업 방법, 보관방법, 원격지 백업의 유무 등(※매체보관의 방법 등 호스팅에서 규정된 경우)		
업무제공 서비스	보안요건	어플리케이션서비스이용에 관한 로깅어카운트의 관리방식(예: ID/패스워드, 증명서인증, 생체인증 등)	상기와 같다.	상기와 같다.
		어플리케이션서비스이용에 관한 이용권한 부여의 방식(예: 이용자 단위에 취급되는 업무를 설정할 수 있다. 사용하지 않는 업무 메뉴는 표시하지 않는다. 이용자단위에 최급되는 데이터범위를 설정할 수 있다. 이용자단위에		

		참조할 수 있는 데이터범위로 조작할 수 있는 데이터범위를 설정할 수 있다 등)		
		로그의 취득범위, 그 해석유무(예: 온라인 조작 로그, 설정변경 로그의 취득과 그 해석 서비스가 부속되는지, 부속되지 않는 것만 제공하는지, 해석은 계약 외인지)		
		인쇄장표에 대한 보안대응의 유무, 대상, 방법(예: 보안프린트, 특정 장표에 대한 복사방지 문양을 포함한 출력/문양용지로 인쇄 등)		
		웹서버에 대한 서버증명서의 설정 등		
		보관 데이터의 암호의 유무		
		어플리케이션에 공격에 대한 강도(예: 크로스스크립팅 대응 등)		
업무제공 서비스	요구성능 요건	서비스의 가동률(서비스의 제공시간 내에, 실제로 이용 가능한 시간)		
		처리성능(어플리케이션의 특성에 대해, 특히, 성능이 요구되는 화면, 온라인 응답시간, 패치처리시간, 단위시간의 최대처리 수 등).(※온라인 처리에서, 인터넷이나, 기관 내부의 랜 등 외부의 보증이 없는 환경의 영향이 있기 때문에, 측정환경, 방법을 명확히 규정할 필요가 있다.)		
		장해시의 대응시간(예: 이용자로부터 장해보고를 받은 후부터 지자체의 담당자로의 보고시간, 온라인 즉시대응책의 이용자로의 제시시간, 장해의 일차수정까지의 시간 등).(※즉시대응은 이용자의 접속으로부터의 해방을 가리킨다 등, 대응내용의 레벨에 대한 규정이 필요)		
도입 서비스	운용조작 지도	초기도입시의 운용・조작지도(운용관리자에게/현장조작자에게)(예: 대응자, 인원수, 방법, 회수, 기간)		
		단체에서 연수를 실시할 경우 지원 유무		
		어플리케이션 가동 후의 운용・조작지도(가동 후의 연간 운용・조작지도의 대상자, 인원수, 방법, 회수, 기간 등)		

	이행계획 입안과 지원	어플리케이션 이행계획의 입안과 이행지원		
		데이터 이행계획의 입안과 데이터 이행지원		
	어플리케이션의 초기설정	데이터센트업(위뢰가능한 데이터센트업 량)		
		운용환경 파라미터의 유무와 설정지원		
		초기이용자의 등록(초기이용자수의 등록 등)		

제 2 절 국내 SLA 사례

국내의 SLA의 사례는 김승윤, 김세한,김진화, 남기찬의 "아웃소싱의 서비스 수준 협약서에 관한 사례연구(2004)"와 정보통신부에서 발간한 ASP를 위한 서비스수준 협약서 작성 가이드라인(2006)이 대표적이다. 그리고 최근에는 TTA에서 클라우드 컴퓨팅 SLA 수립을 위한 품질요소에 관한 표준안(2010)이 연구되었는데, 본 절에서는 이를 간략하게 소개하기로 한다.

1, 김승윤 외 아웃소싱의 서비스 수준협약서에 관한 사례연구(2004)

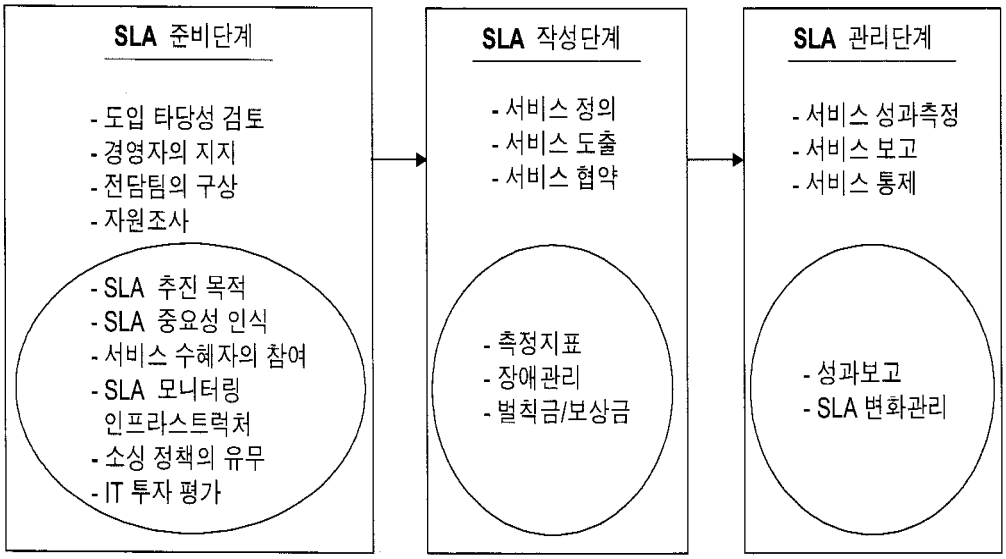
김승윤 외의 연구에서는 아웃소싱의 서비스 수준협약서에 관한 사례연구를 수행하였는데, 이를 위하여 국내·외 문헌조사를 통하여 <그림 2-1>에서 보는 바와 같이 SLA 구성요소를 기술하였다.

SLA의 구성요소를 보면 SLA 목적, 기산, 어플리케이션/서비스, 예측 가능한 고장시간, 지원시간, 비용청구협상, 변화고나리, 서비스측정 기준, 시리시간 서비스 모니터링, 서비스수준 보고, 실패에 대한 벌칙조항, 서비스 수혜자와 제공자간 검토회의 개최, 커뮤니케이션 계획, 협정과 재협정사이의 기간협의 등의 내용을 포함하고 있다.

- SLA의 목적
- SLA의 기간
- 어플리케이션/서비스
  - 시스템개관, 의존성, 우선 순위
  - 주요 사용기간, 최고 사용기간
  - 가용성(정의 및 목표)
  - 거래비율(표준일, 최고 사용기간)
  - 시스템 응답성(거래유형별, 정의)
  - 시스템 사용 예측기간
  - 일괄처리사항
  - 자료입력, 마감시기
  - 처리, 보고, 회람의 기간
  - 산출물협정내용
  - 저장 요구사항
  - 정확성(입력, 데이터베이스, 산출물)
  - 보안(복사, 접근, 백업, 재해복구 상황계획)
  - 서비스시간
- 예측 가능한 고장시간
  - 하드웨어, 소프트웨어 유지보수 설치/변환
- 지원시간
  - 헬프 데스크
  - 기술지원
  - 고객관리 방안
  - 단계적 해결절차
- 비용청구협상
- 변화관리
- 서비스측정 기준
- 실시간 서비스 모니터링
- 서비스수준 보고
- 실패에 대한 벌칙조항
- 서비스 수혜자와 제공자간 검토회의 개최
- 커뮤니케이션 계획
- 협정과 재협상의 기간 협의

<그림 2-1> SLA 구성요소

추가적으로 김승윤 외의 연구에서는 <그림 2-2>에서 보는 바와 같이 SLA의 단계적 모델을 제시하였는데, 이를 모델을 실현하기 위한 구체적인 설명과 그 내용을 기술하였다.



<그림 2-2> SLA의 단계적 모델

2. 정보통신부: ASP를 위한 서비스수준 협약서 작성 가이드라인

본 항에서는 정보통신부에서 발간한 ASP를 위한 서비스수준 협약서 작성 가이드라인이 주요 내용을 간략하게 소개하는데, 그 중에서도 가이드라인에 소개되어 있는 SLA 구성요소와 각 구성요소에 포함하고 있는 내용을 소개한다.

가. SLA 구성요소

일반적으로 SLA의 주요내용은 도입부, 서비스시간, 가용성(Availability), 신뢰성(Reliability), 지원력, 성능, 비용부담내용, 서비스보고서 및 검토 등으로 구성된다.

도입부의 내용은 계약의 주체, 서비스수준협약에 대한 제목 및 간략한 설명, 서명인, 포함될 내용의 범위, 양자의 책임 및 역할, 계약에 포함될 서비스에 대한 설명 등이 포함되며, 서비스 시간 정의 부분에는 서비스 시간(예: 월-금 09:00-18:00), 특정일(공휴일), 서비스 연장정의 등에 관한 내용이 기술된다.

가용성(Availability)부분은 계약시간 내 가용성 목표치는 일반적으로 Percentage로 표현되며, 이 경우 반드시 측정기간 및 방법이 정의되어야 한다. 가용성은 전체 서비스, 외부파트너 서비스, 중요 IT구성요소 또는 3가지 모두에 대해 표현될 수 있지만 서비스품질을 단순한 세 가지 수치로 연관시키는 것은 쉽지가 않다. 따라서 서비스 비가용성(Unavailability)을 측정하는 것이 더 좋은 방법일 수 있다.

신뢰성(Reliability)은 일반적으로 서비스장애 횟수로 표현하거나 Mean Time Between Failure (MTBF), Mean Time Between System Incidents(MTBSI)로 표현한다. 또한 지원력에 대한 부분에서는 지원시간(서비스 시간과는 다름), 특정시간(공휴일), 지원연장에 대한 부분, 응답목표시간 (예, Incident에 대한 전화응답, E-Mail응답 등)의 내용이 포함된다. 성능(Throughput)부분에서는 예상 트래픽 볼륨 및 성능(Throughput)지표 (예: 처리되는 트랜잭션 수, 동시사용자 수, 네트워크를 통해 전송되는 데이터 량), 트랜잭션 응답시간(Transaction Response Time),(예: 평균 또는 최대 응답시간에 대한 목표치), 배치작업 처리성능(배치작업의 성공적인 처리율) 등이 기술된다.

변경에 대한 부분에서는 변경요청(RFC ; Request For Change)를 승인, 처리, 구축할 때의 목표치, 일반적으로 변경유형 또는 변경 우선순위에 정의된다. IT서비스 연속성 및 보안(IT Service Continuity & Security)부분에서는 IT 서비스 연속성 계획에 대한 간략한 정의 및 계획을 실행에 옮기기 위한 방법과 보안항목에 대한 정의가 포함된다.

비용부담(Charging)부분에는 상세한 비용부과 및 기간 등이 기술되며, 서비스

레포트 및 검토에서는 서비스 레포트의 주기 및 분배, 내용, 서비스 검토회의 계획 주기 등이 작성된다. 마지막으로 성능에 따른 인센티브 및 페널티(Performance Incentive / Penalties)에서는 서비스 수준에 대한 성과에 따른 금전적 인센티브 및 페널티에 대한 상세한 내용 등이 기술된다.

1) ASP SLA 도입부

SLA 도입부에는 SLA 작성의 기본취지, 사용지침 등 전반적인 SLA의 개요와 계약 대상자, 계약 일시, 승인 및 변경 절차에 대해 기술한다.

o 계약 대상자
- 공급자와 이용자의 상호를 기입하고 서명을 한다.

o 개정 이력표
- SLA의 재・개정 여부와 내용, 일시를 기술한다.

2) ASP SLA 본문

SLA 본문에서는 ASP 서비스 관리를 위해 도출된 항목에 대한 기본 사항들과 적용범위, 그리고 서비스 항목을 평가하기 위한 기준 및 평가 방법에 대해 기술한다. 크게 4가지 부분으로 나누어 볼 수 있다.

o 목적, 서비스 내용, 조건
- SLA 체결의 목적, 서비스에 대한 구체적인 제공 기능, 계약기간, 서비스개시 및 종료, 요금에 대한 내용을 기술

o 성능 메트릭스, 서비스제공 플랫폼 및 구조, 확장성, 데이터 백업 및 복구, 보안
- 서비스의 성능에 대한 측정기준, 항목 및 서비스가 제공되고 있는 시스템적

환경, 시스템에 대한 기술적 대응책에 대한 내용을 기술

o 고객지원, 장애, 위약금, 서비스 향상 및 개선, 서비스 보고 및 처리

- 이용자를 위하여 서비스에 대한 개선 노력, 장애시 처리문제, 서비스 수준에 대한 주기적 보고에 대한 내용으로서 전반적인 고객 지원에 대한 내용을 기술

o 계약의 변경, 서비스의 해지, 분쟁의 해결

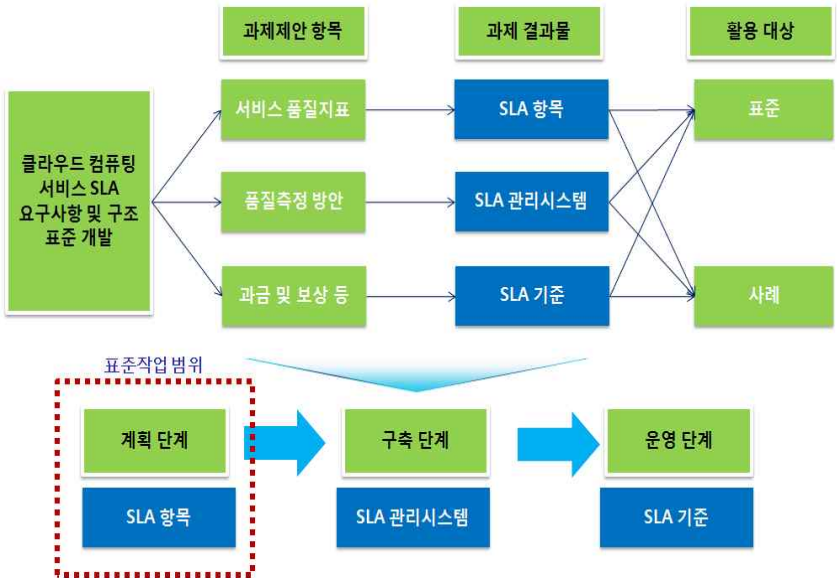
- SLA 계약내용의 변경, 해지, 분쟁해결 방법에 대한 내용을 기술

3. TTA Standard: 클라우드 컴퓨팅 SLA수립을 위한 품질요소

본 항에서는 클라우드 컴퓨팅 SLA 수립을 위한 품질요소의 주요 내용을 소개하는데 그 내용은 다음과 같다.

가. 표준의 범위 및 구성

TTA 표준안에서는 클라우드 컴퓨팅 SLA수립을 위한 품질요소에서의 표준의 범위와 구성을 **그림 2 와** 같이 설정하였다.



<그림 2-3> 클라우드 컴퓨팅 SLA 품질요소를 수립을 위한표준의 범위와 구성

나. 클라우드 컴퓨팅 SLA 정의

본 연구에서는 클라우드 컴퓨팅의 SLA에 대한 정의를 포함하고 있는데 그 내용은 다음과 같다.

클라우드 컴퓨팅 모델은 서비스로 정립되고 제공되며 사용자에게 제공되는 서비스는 평가되고 일정 수준이 보증되어야 한다. 클라우드 컴퓨팅 환경에서 SLA를 정의하면 다음과 같다.

“고객에게 제공하는 클라우드 컴퓨팅 서비스의 수준을 정량적으로 측정하고, 서비스 성과를 평가/보상하여 서비스를 주고받는 양 당사자 간의 서비스를 보증하기 위한 품질 상세 약정”

클라우드 컴퓨팅 SLA 정의에서 표현되었듯 SLA는 서비스 제공자와 서비스를

사용하는 사용자간의 서비스 보증을 기반으로 구성되며 서비스 보증을 위해 정량적인 측정이 가능한 지표를 기반으로 서비스 성과가 평가되어야 한다.

다. 클라우드 컴퓨팅 SLA 구조

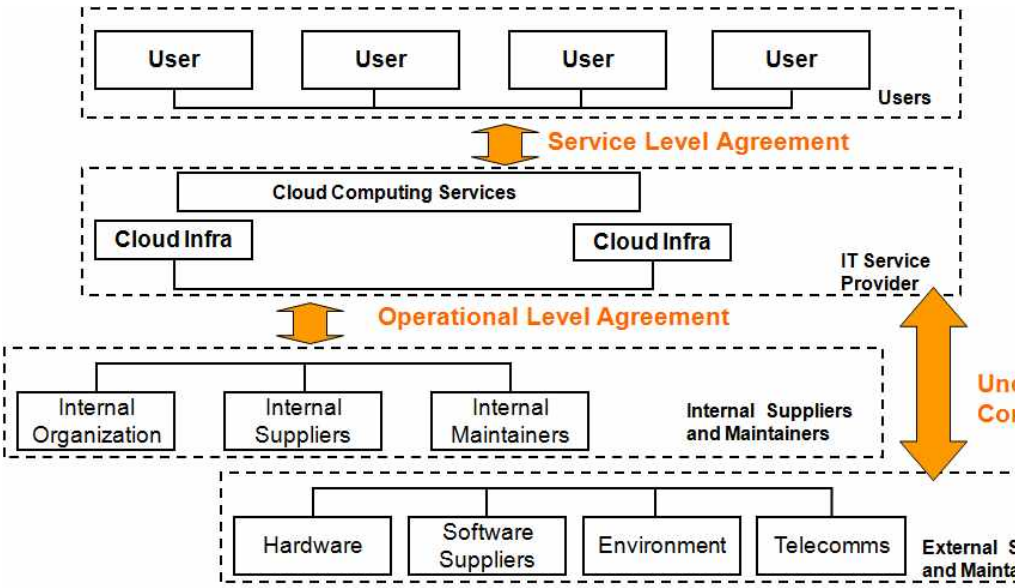
본 연구에서는 클라우드 컴퓨팅의 SLA 구조를 설명하고 있는데 그 내용은 다음과 같다.

클라우드 컴퓨팅의 SLA 구조는 사용자에게는 "SLA(Service Level Agreement)"를 제공하며 내부 조직 간에는 "OLA(Operation Level Agreement)", 외부 유지보수업체와는 "UC(Underpinning Contract)" 구조로 구성되어 진다.

클라우드 컴퓨팅 SLA 구조화를 위해서는 최종 사용자에게 제공되는 SLA 서비스 수준 이상으로 내부 OLA 운영 수준과 외부 유지보수 UC 계약 수준이 반영될 수 있도록 관리되어야 한다.

SLA-OLA-UC의 구조는 하위 구조의 지표 수준이 상위 구조의 지표 수준보다 같거나 높아야 하며 상위 구조의 수준을 하위 수준에서 보증해 주어야 한다.

만약 SLA 지표를 지원할 수 있는 하위 OLA 또는 UC 계약 수준이 존재 할 경우 최종 사용자에게 제공되는 SLA 서비스 수준은 보증될 수 없는 구조적 모순에 빠지게 된다.



<그림 2-4> 클라우드 컴퓨팅 SLA 구조

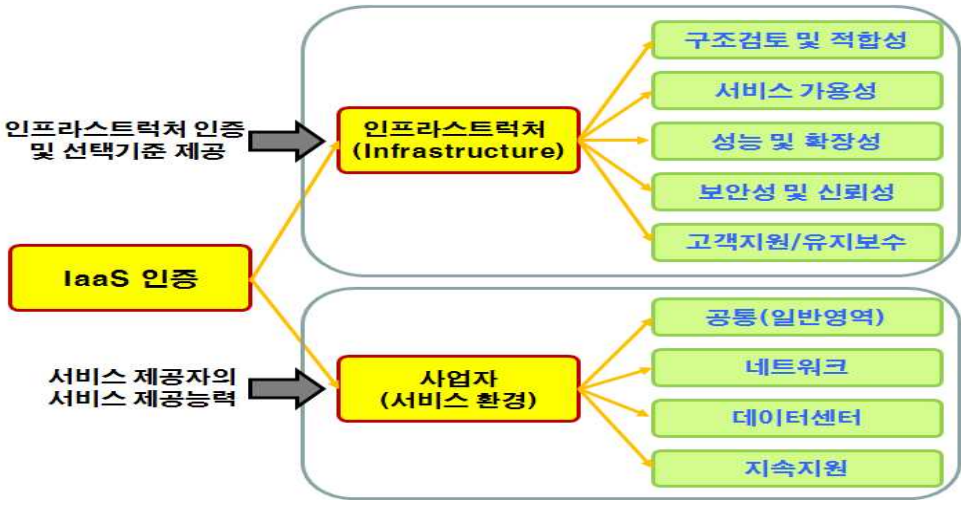
제 3 절 클라우드 서비스 인증

1. IaaS 인증제도

가. IaaS 인증영역

IaaS 인증영역은 크게 인프라스트럭처 인증과 사업자(서비스 환경) 인증으로 구분하여 개발하기로 하는데, IaaS의 기능, 특징 및 세부 기술적인 요소 등을 심사영역 및 항목으로 포함하여 인프라스트럭처 영역의 인증을 위한 심사영역과 세부 심사항목을 개발하기로 하고 SaaS 사업자(서비스 환경) 영역의 인증을 위한 심사영역과 세부 심사항목도 동시에 개발하기로 한다.

본 보고서에서 개발한 IaaS 인증영역은 아래 <그림 1>과 같다.



<그림 2-5> IaaS 인증범위

나. 인프라스트럭처(Infrastructure) 인증

본 항에서는 IaaS의 인프라스트럭처 인증을 위한 인증심사기준과 이에 대한 설명을

기술하기로 한다. IaaS의 인프라스트럭처 인증을 위하여 총 5개의 심사영역에 31개 심사항목이 개발되었는데, 이에 대하여 차례대로 기술하기로 한다.

1) 구조검토 및 적합성

<표 2-10> 구조검토 및 적합성 영역 인증심사기준

심사항목			심사방법	심사내용	근거
1.1	인프라스트럭처의 기능에 대한 명확하고 상세한 설명서 존재 유무		관련문서 점검 -인프라스트럭처 상세설명서 -인프라스트럭처 백서	이용자가 쉽게 이해하고 사용할 수 있는 문서관리 점검	-
1.2	인프라스트럭처의 논리적 구조에 대한 다이어그램, 설명서 존재 유무		관련문서 점검 -인프라스트럭처의 논리적 구성도	사용자의 인프라스트럭처의 이해도 증진 및 문제발생시 기본자료 제공 점검 - 데이터베이스, OS, 플랫폼, 하드웨어, 네트워크 등의 논리적인 구성 점검	-
1.3	인프라스트럭처의 물리적 구조에 대한 다이어그램, 설명서 존재 유무		관련문서 점검 -인프라스트럭처의 물리적 구성도	사용자의 인프라스트럭처의 이해도 증진 및 문제발생시 기본자료 제공 점검 -서버, 스토리지, 네트워크 등의 서비스의 물리적 구조 점검	-
1.4	인프라스트럭처의 윈도우, 리눅스, 유닉스 시스템 지원 여부		관련문서 점검 및 실사 -인프라스트럭처 운용검증	인프라스트럭처 데이터전송의 호환성 점검	
1.4	IaaS 서비스 제공을 위한 핵심기술 점검				-
	1.4.1	가상화기술	관련기술문서 점검 - 가상화기술문서	원활한 IaaS 서비스 제공을 위한 가상화 기술 점검 - 서버가상화, 스토리지가상화, 네트워크 가상화 기술문서 점검	-
	1.4.2	분산컴퓨팅 기술	관련기술문서 점검 - 분산컴퓨팅 기술 문서	원활한 IaaS 서비스 제공을 위한 분산컴퓨팅 기술 점검 - 분산파일 시스템기술, 분산병렬처리기술, 분산데이터 저장기술, 분산시스템간 데이터 스트리밍 처리기술 점검	-
	1.4.3	시스템관리 기술	관련기술문서 점검 - 시스템관리 기술 문서	원활한 IaaS 서비스 제공을 위한 시스템관리 기술 점검 - 가상인프라(서버가상화, 스토리지가상화, 네트워크 가상화) 관리기술, 물리적 인프라 관리기술 문서 점검	-
	1.4.4	서비스플랫폼 기술	관련기술문서 점검 - 서비스플랫폼 기술 문서	원활한 IaaS 서비스 제공을 위한 서비스 플랫폼 기술 점검 - 서비스 데이터 인터페이스 기술, 협업을 위한 인터페이스, 데이터베이스 인터페이스 기술문서 점검	-
	1.4.5	기타	관련기술문서 점검 - 기타핵심기술문서	원활한 IaaS 서비스 제공을 위한 기타 핵심기술 점검 - 기타기술(SLA, Trustworty, 프로비저닝 등)문서 점검	

이 영역은 인프라스트럭처의 기본적인 구조를 검토하여 IaaS 서비스로서의 유용성 및 적합성을 심사하는 영역으로서 인프라스트럭처의 기능, 논리적 구조, 물리적 구조 및 핵심기술 요소들을 점검함으로써 IaaS 서비스를 위한 인프라스트럭처 구조의 적합성 여부를 평가하는 영역이다.

1.1 기능에 대한 평가는 물론 이용자가 쉽게 이해하고 사용할 수 있도록 인프라스트럭처의 기능을 명확하고 상세하게 기술해 놓은 문서가 존재하고 그 유지관리를 시행하는지를 심사

1.2 인프라스트럭처에 대한 문제발생시(버그 등) 기본 자료로 제공가능한 문서의 존재 및 유지관리를 심사

1.3 인프라스트럭처에 대한 문제발생시(버그 등) 기본 자료로 제공가능한 문서의 존재 및 유지관리를 심사

1.4 원활한 IaaS 서비스 제공을 위한 핵심기술인 가상화, 분산컴퓨팅, 시스템관리, 서비스플랫폼 기술 등의 점검을 위한 기술 문서의 존재 심사

2) 서비스 가용성(Service Availability)

<표 2-11> 서비스 가용성영역 인증심사기준

심사항목		심사방법	심사내용	근거
2.1	다수의 사용자의 인프라스트럭처에 동시접속 사용가능 여부	관련문서 점검 및 실사 -기술구현 증빙자료 -인프라스트럭처 운용검증	동시접속 기술구현 점검 접근제어 및 인증기술 점검	ASPIC USA
2.2	인프라스트럭처의 모든 기능 및 관리를 웹브라우저를 통하여 접근 및 운용가능여부	인프라스트럭처 운용검증 -지원하는 웹브라우저 : 버전/제작사	다양한 웹접속기반에서의 안정성 검증	ASPIC USA
2.3	인프라스트럭처의 서비스가용성 점검	관련문서 점검 및 실사 -인프라스트럭처의 가용성 테스트보고서 -주기적 가용성테스트 보고서	인프라스트럭처의 서비스 가용성 점검 - 인프라스트럭처의 서비스가 중단되지 않고 사용가능한 정보를 나타내는 정량적 지표 체크 (예: 전체시간중 실제로 서비스를 사용할 수 있는 기간 비율)	관련표준

이 영역은 인프라스트럭처가 웹을 통하여 다수의 사용자의 접속이 가능하고 관리가 가능한지를 심사하는 영역으로서 다수 사용자의 동시접속 가능여부, 웹을 통한 접속 가능성 및 서비스 가용성을 평가하는 영역이다.

2.1 IaaS 서비스의 기본기술인 다수 사용자의 동시접속 가능여부 점검 및 인프라스트럭처의 동시접속 가능여부를 심사

2.2 인프라스트럭처의 웹브라우저를 통하여 접근 및 운용 가능여부를 심사

2.3 인프라스트럭처 서비스의 가용성 심사

3) 성능(Performance) 및 확장성(Scalability)\

<표 2-12> 성능 및 확장성 영역 인증심사기준

심사항목		심사방법	심사내용	근거
3.1	주기적인 인프라스트럭처 성능(Performance) 테스트실시 점검	관련문서 점검 -성능테스트 보고서(1. 네트워크 대역폭과 스위치의 지연시간, 서버의 프로세싱 파워 2. 처리시간과 전달시간의합인 응답시간 및 최대 처리량 테스트 결과 필수)	인프라스트럭처 성능유지를 위한 서비스 활동 점검 - 네트워크 회선 서비스의 경우 대역폭과 스위치의 지연시간으로 평가 - 서버의 경우 프로세싱(processing) 파워로 평가 - 주요 기능 구동의 응답시간에 대한 최소, 최대, 평균시간, 최대처리량, 장애복구 시간 등	SW품질인증기준(제10조)
3.2	주기적인 인프라스트럭처 안정성 테스트실시 점검	관련문서 점검 -안정성테스트 보고서(접근성, 신뢰성 테스트결과 필수)	인프라스트럭처의 안정성 유지를 위한 활동 점검 -제공되는 서비스의 접근성, 신뢰성 등	SW품질인증기준(제10조)
3.3	고객(사업)수의 증가에 대비한 성능유지가능 여부	관련문서 점검 -인프라스트럭처 기술지침서	인프라스트럭처의 사용자수 증가에 따른 인프라스트럭처 자원할당방법 및 서비스 성능 유지관리 점검	ASPIC USA
3.4	고객(사업)수의 증가에 대비한 확장성(scalability) 확보 여부	관련문서 점검 -인프라스트럭처 기술지침서	인프라스트럭처의 사용자수 증가에 따른 확장성 기술 점검 - 사용자에 대한 모니터일 및 확장을 동적으로 해줄 스케쥴러 및 푸로비저닝 기능 점검 - 운영중 다운타임없이 사용자, 서버 등 확장성 점검	ASPIC USA

이 영역은 해당 어플리케이션의 성능, 안정성 및 확장성 유지를 위한 점검활동 및 향후 사업 확장에 대한 계획 등 제반 활동사항을 평가하는 영역이다.

3.1 인프라스트럭처 성능유지를 위한 서비스 활동 점검하는 항목으로 네트워크 회선 서비스의 경우 대역폭과 스위치의 지연시간으로 평가할 수 있고, 서버의 경우 프로세싱(processing) 파워로 평가할 수 있는데, 주요 기능 구동의 응답시간에 대한 최소, 최대, 평균시간, 최대처리량, 장애복구 시간 등의 평가를 통해 서비스 성능을 주기적으로 테스트하고 유지관리하는가를 심사

3.2 인프라스트럭처 안정성 유지를 위한 활동 점검하는 항목으로 IaaS 서비스가 어느 정도 안정하게 서비스를 제공하는지를 점검. 즉, 처리량의 증가, 폭주, 시스템의 고장, 자연 재해 그리고 사람에 의한 고의적 공격에도 지속적이고 일관성 있으며 원래의 상태로 회복 가능한 서비스를 제공할 수 있는 능력을 점검하는 항목으로 서비스의 접근성, 신뢰성 등을 주기적으로 테스트하고 유지관리하는가를 심사

3.3 인프라스트럭처의 사용자수 증가에 따른 성능(performance) 유지관리 능력 심사

3.4 인프라스트럭처의 사용자수 증가에 따른 확장성 능력 심사하는 항목으로써 IaaS의 핵심기술인 분산된 데이터처리, 컴퓨팅 자원을 제어가능성, 가상화, 분산/병렬 처리 프레임워크 등은 확장성 있는 서비스를 제공하는 핵심 기술 능력 심사

4) **보안성 및 신뢰성**

<표 2-13> 보안성 및 신뢰성 영역 인증심사기준

심사항목		심사방법	심사내용	근거
4.1	보안정책 및 보안 채널 유무	보안정책 문서 점검 및 실사 -전체 보안정책 문서 -보안채널 관려 문서	인프라스트럭처 서비스 전체 보안정책 및 보안 채널 점검	관련 표준
4.2	접속 권한에 따른 접근 제어 유무	관련문서 점검 및 실사 -접근제어 기술문서 -어플리케이션 기술지침서 -ACL	비인가된 이용자로부터의 인프라스트럭처의 데이터 보호 장치 점검	관련 표준
4.3	검증을 통한 사용자의 인증 절차 유무	관련문서 점검 -인프라스트럭처 기술지침서 -Sigle Sign-On 기능제공여부	이용자의 인증절차 유무 검증 -Sigle Sign-On 기능 -패스워드, 쿠키 정책 -ACL 등	관련 표준
4.4	데이터의 기밀성을 위한 보안기술 적용 유무	관련문서 점검 및 실사 -인프라스트럭처 기술지침서	인프라스트럭처 접속시 생성되는 데이터의 보호를 위한 조치 점검	관련 표준
4.5	데이터의 무결성을 위한 보안기술 적용 유무	관련문서 점검 및 실사 -인프라스트럭처 기술지침서	인프라스트럭처 접속시 생성되는 데이터의 보호를 위한 조치 점검	관련 표준
4.6	인프라스트럭처 접속시 방화벽을 통한 접근 유무	관련문서 점검 -인프라스트럭처 기술지침서	방화벽지원 유무 점검	관련 표준
4.7	로그파일 분석을 통한 감사추적 기능 지원 유무	관련문서 점검 및 실사 -인프라스트럭처 기술지침서 -로그분석 보고서	비인가된자로부터의 접근을 보호하고 추적하기위한 관리 대책점검	관련 표준
4.8	메시지의 송수신 자가 송수신 사실을 부인하지 못하도록 하는 부인방지 기능 지원 여부	관련문서 점검 및 실사 -인프라스트럭처 기술지침서 -메세지 레벨의 전자서명기법을 이용한 부인방지 기능 점검	전송레벨은 제외하고, 메세지 레벨에서의 부인방지 기능 점검	관련 표준
4.9	개인의 프라이버시 보호와 관련된 보안 기능 점점	관련문서 점검 및 실사 -인프라스트럭처 기술지침서 -메세지 레벨의 프리이버시 보호기능 점검	전송레벨은 제외하고, 메세지 레벨에서의 개인 프라이버시 보호 기능 점검	관련 표준
4.10	자동 백업, 싱크 및 복구 기능 여부	관련문서 점검 및 실사 -인프라스트럭처 기술지침서	데이터의 자동 백업, 싱크 및 복구 기능 점검	관련 표준

이 영역은 주로 어플리케이션과 관련된 부분에 대한 보안평가로서 어플리케이션

자체내(소스내) 보안구현보다는 네트워크와 어플리케이션이 접속되는 서비스 환경에 대한 점검활동 및 통제활동을 평가하는 영역이다.

4.1 IaaS 서비스의 전체 보안정책을 가지고 서비스를 운영하는지와 보안채널 운영 여부를 심사

4.2 비인가된 사용자의 접근을 방지하기 위하여 접속권한에 따라 권한 설정의 기능이 구현되어 있는지를 심사

4.3 ID/패스워드, 쿠키 정책을 통한 인증절차의 기능구현 및 정책수립 여부를 심사하고 서비스 환경에서는 메시지가 다양한 보안 도메인을 경유하기 때문에 보안 토큰을 통한 Single Sign-On 기능이 제공되는지 여부 점검

4.4-4.5 인프라스트럭처 접속 및 구동시 생성·트랜잭션되는 데이터의 보호를 위한 기술 및 정책수립 여부를 심사

4.6 인프라스트럭처 접속시 방화벽을 경유하여 접근가능하도록 구현되어 있는지 심사

4.7 비인가된 사용자의 침해방지를 위한 관련 로그분석활동을 정기적으로 시행하고 있는지를 심사

4.8 메시지의 송수신자가 송수신 사실을 부인하지 못하도록 하기 위아여 전자서명 기법을 사용한 부인방지 기능 지원 여부

4.9 사용자와 제공자 양 당사자 측면에서 개인의 프라이버시 보호와 관련된 보안 기능 점점

4.10 IaaS 서비스의 특징상 데이터의 자동 백업, 싱크 및 복구 기능 점검

5) 고객지원, 유지보수 정책

이 영역은 인프라스트럭처의 유지보수, 교육, 콜센터 및 핼프데스크 운영 등의 대고객 서비스를 점검하는 영역으로서 서비스 상황을 모니터링하고, 핼프데스크를 운영하며, 교육활동을 실시하는가를 평가하는 영역이다.

<표 2-14> 고객지원 및 유지보수 정책영역 인증심사기준

심사항목		심사방법	심사내용	근거
5.1	인프라스트럭처의 문제발생시 고객에 대한 지원프로세스 존재 유무	관련문서 점검 -SLA -인프라스트럭처의 문제발생시 지원프로세스 문서	인프라스트럭처 문제발생시 사업자의 응대처리 점검 -이용자 대처방법, 개발자 문제해결방법을 기술한 문서의 유지관리 점검	SW품질 인증기준 (제18조)
5.2	서비스 제공자가 해당 인프라스트럭처를 제공시 지원하는데 유용한 문서 존재 유무	관련문서 점검 -인프라스트럭처 기술 지원 문서	서비스제공자가 이용자 지원을 위한 기술지원문서 유지관리 점검 -온라인 헬프, 웹페이지, 프로그램 로직 매뉴얼, 튜닝가이드 등	SW품질 인증기준 (제18조)
5.3	최적의 인프라스트럭처 서비스 환경유지를 위한 운영전략 수립 여부	관련문서 점검 -인프라스트럭처 기술 지원지침서	인프라스트럭처 서비스의 목표 이용수준을 유지하기 위한 업그레이드, 백업전략, 운영절차 수립 시행 점검	-
5.4	지속적인 서비스 제공을 위한 모니터링 기술이나 툴의 확보 및 지원 여부	관련문서 점검 -모니터링 보고서 -관련 기술 및 툴을 확인할 수 있는 증빙자료	사후 인프라스트럭처 서비스 제공자가 서비스 제공을 위한 시스템 모니터링 기술지원 점검 -서비스 실패요인 발견을 위한 기술 및 툴	SW품질 인증기준 (제18조)

5.1 인프라스트럭처어 서비스 장애 등 서비스 중단에 따른 문제발생시 신속하게 대응 처리할 수 있는 프로세스 수립 및 지원여부를 심사

5.2 해당 인프라스트럭처어를 서비스하는 제공자(IaaS 사업자)가 이용자(사용자)에게 신속하고 명확하게 지원가능하도록 관련 기술지원문서를 제공하고 유지관리하는지를 심사

5.3 인프라스트럭처어의 목표 이용수준을 유지하기 위한 업그레이드, 백업전략, 운영절차 등을 수립 · 시행하고 있는지를 심사

5.4 지속적인 서비스제공의 안정성을 확보하기 위한 활동으로서 어플리케이션 모니터링 기술 및 툴의 확보를 통한 주기적인 점검활동여부를 심사

다. IaaS 사업자(서비스 환경) 인증

본 항에서는 IaaS 사업자(서비스 환경) 인증을 위한 인증심사기준과 이에 대한 설명을 기술하기로 한다. IaaS 사업자(서비스 환경) 인증을 위하여 총 5개의 심사영역에 27개 항목심사항목이 개발되었는데, 이에 대하여 차례대로 기술하기로 한다.

1) 일반 영역

<표 2-15> 일반현황영역 인증심사기준

심사항목		심사방법	심사내용	근거
1.1	회사의 정체성	관련문서 점검 -사업자등록증 -하청(위탁)계약서 -기타 관련 증빙서류	회사의 일반현황 점검 -회사명 -회사의 규모 및 업종 -사업장규모 -협력업체의 서비스 범위 -서비스 명/종류	-
1.2	회사의 인적자원의 안정성	관련문서 점검 및 실사 -지원조직도 -인적자원관리 현황표	지원조직 및 인적자원관리 평가/점검 -조직 구성 -인력조직 현황 -헬프 데스크 조직 유무 -IT조직의 구성 (기능, 구성원수, 조직형태)	-
1.3	고객 대상의 확보	관련문서 점검 -서비스 계약서	서비스 계약 사실 확인 (최소 고객 2개이상 존재)	-
1.4	과금체계의 합리적/체계적 정립 유무	관련문서 점검 -서비스 비용산정을 증빙할 수 있는 서류 -표준계약서 -SLA -가격표	과금체계(비용산정)의 합리적 정립을 확인	-
1.5	회사의 평판	설문조사/면접 및 투표	IaaS 관련 업계에서의 평판 점검 -설문조사/면접/투표	

이 영역은 서비스 사업자의 일반현황을 점검하는 영역으로서 회사의 실제 존재여부, 인력자원의 확보 여부, 고객의 확보 여부를 파악하여 잠재적 능력 및 운용능력 등 회사의

기본적인 안정성을 점검하여 지속적으로 서비스를 제공할 제반환경이 갖추어져 있는가를 평가하는 영역이다.

1.1 회사명, 규모 및 업종 등을 심사

1.2 핼프데스크 조직 유무, 개발인력(기능, 구성원수) 등 인력조직 운용 현황을 심사

1.3 심사시점 현재 실제 IaaS 서비스를 이용하고 있는 고객의 유무를 통하여 IaaS 서비스에 대한 노하우 및 지속가능성 , 서비스 지속에 대한 사업자의 의지 여부를 파악

1.4 과금체계를 합리적이고 체계적으로 산정, 정립하고 있는지를 심사

1.5 서비스에 대한 소비자들의 평판을 점검하는 항목으로 서비스 품질 및 만족도, 신뢰성 등에 의하여 만들어지며 설문조사/면접 및 투표 등 여러 가지 방법을 통하여 측정가능하며, 궁극적으로 IaaS 관련 업계에서의 회사 평판을 점검

2) 네트워크 & 데이터센터 영역 - 보안성

이 영역은 물리적, 기술적, 관리적인 측면에서 비인가된 사용자로부터의 접근통제를 통하여 이용자의 데이터 보호 및 침해방지 등 보안활동의 체계적인 수립 및 시행을 점검하는 영역이다.

2.1 물리적 보안체계 점검

2.2 독립적인 전산실 확보/출입통제장치 유무 점검

2.3 보안 침해방지를 위한 활동 점검

2.4 보안 취약점검의 주기적 활동 점검

2.5 서버와 클라이언트간에 전송되는 정보에 대한 완전한 보안을 위해 암호화 제공여부 점검

2.6 보안을 위한 사업자의 주기적인 활동 점검

2.7 논리적 접근통제활동 점검/서버 및 네트워크 서비스 관련 SW점검 정책 유무

<표 2-16> 네트워크 및 데이터센터 영역의 보안성 심사항목

구분	심사항목		심사방법	심사내용	근거
물리적 보안	2.1	물리적 보안 대책수립 여부	관련문서 점검 및 실사 -보안정책서 -전산실무지침서	물리적 보안체계 점검	정보시스템 감리기준
기술적 보안	2.2	출입통제 유무	관련문서 점검 및 실사 -출입통제 관리 문서	독립적인 전산실 확보 출입통제장치 유무	정보시스템 감리기준
	2.3	침해방지 대책 유무	관련문서 점검 및 실사 -보안솔루션 계약서 (방화벽, IDS 등)	보안 침해방지를 위한 활동 점검	정보보호지침, IDC시설 안전신뢰성 기준
	2.4	보안취약점검 유무	관련문서 점검 -보안취약점검 보고서 (바이러스 점검 포함)	보안취약 점검의 주기적 활동 점검	정보보호지침, IDC시설 안전신뢰성 기준
관리적 보안	2.5	파일전송시 암호화 유무	관련문서 점검 및 실사 -파일암호화/무결성 체크 문서 -데이터암호화 지원 여부	서버와 클라이언트간에 전송되는 정보에 대한 완벽한 보안을 위한 데이터암호화 제공여부 점검	정보보호지침, IDC시설 안전신뢰성기준
	2.6	사업자 활동 점검	관련문서 점검 -보안정책 -시스템운영지침서	보안을 위한 사업자의 주기적인 활동 점검	정보보호지침
	2.7	시스템 통제 활동 점검	관련문서 점검 및 실사 -시스템 접근권한 명시문서 -서비스관련 SW점검표	논리적 접근통제활동 점검 서버 및 네트워크 서비스 관련 SW점검정책 유무	정보보호지침

3) 네트워크 & 데이터센터 영역 - 서비스제공 기반

<표 2-17> 네트워크 및 데이터센터 영역의 서비스제공 기반 심사항목

심사항목		심사방법	심사내용	근거
3.1	서비스 제공을 위한 전산 설비 공간 점검	관련문서 점검 및 실사 -호스팅 및 IDC사용 계약서 -현장검증	독립적인 전산설비 공간 유무의 점검	IDC시설 안전신뢰성기준
3.2	서비스 제공을 위한 서버, 스토리지 및 네트워크 장비/라인에 대한 점검	관련문서 점검 -서버, 스토리지 및 네트워크 장비목록표 -서버 및 스토리지 점검 활동표 -네트워크 장비/라인 점검표	서버, 스토리지 및 네트워크 안정성을 확보하기 위한 활동 점검	IDC시설 안전신뢰성기준
3.3	서비스 제공을 위한 인프라스트럭처 Software에 대한 점검	관련문서 점검 -인프라스트럭처 S/W 점검표	인프라스트럭처를 구성하는 컴포넌트들간의 최적화 점검	IDC시설 안전신뢰성기준
3.4	서비스 제공을 위한 인프라스트럭처의 외부 공급/유지보수업체와의 유지보수/기술지원 계약 여부	관련문서 점검 -제공업체와의 유지보수/기술지원 계약서	인프라스트럭처의 외부 공급/유지보수업체와의 유지보수/기술지원을 위한 활동 점검	IDC시설 안전신뢰성기준
3.5	서비스 제공을 위한 기술 지원 인력의 확보 여부	관련문서 점검 -직원경력증명서 -직원기술력을 입증할 수 있는 자격증	기술지원 가능한 인력의 확보 점검	-

이 영역은 서비스 제공을 위한 전산설비 및 인프라, 전문인력 등 전반적인 서비스 제공에 대한 기반시설의 확보 및 유지활동을 점검하는 영역이다.

3.1 독립적인 전산실 공간유무의 점검

3.2 서버, 스토리지 및 네트워크 안전성을 확보하기 위한 활동점검

3.3 인프라스트럭처를 구성하는 컴포너트들간의 최적화 점검

3.4 인프라스트럭처의 외부 공급/유지보수업체와의 유지보수/기술지원을 위한 활동 점검

3.5 기술지원 가능한 인력의 확보 점검

4) Ongoing Support 영역 - 서비스제공 지속성

<표 2-18> 지속지원영역의 서비스 제공 지속성 심사항목

심사항목			심사방법	심사내용	근거
4.1	서비스 확장 가능성(Vertical 혹은 Horizontal) 유무		관련문서 점검 -서비스 환경(인프라 스트럭처) 문서 -서비스 확장(투자) 계획서	서비스 확장에 따른 QoS 확보 점검 -미래의 요구사항을 산출하기 위한 용량 계획 수립유무 점검	정보시스템감리 기준
4.2	서비스 안정성을 위한 대책 유무	서비스 중단에 따른 복구프로세스 존재 유무	관련문서 점검 -SLA	비정상적인 상황에 대비한 대책 점검 - 장애내역 통지여부	정보시스템감리 기준
4.3		성능유지를 위한 기술적, 관리적 내부프로세스 존재 유무	관련문서 점검 -SLA -관련 SW등 툴의 사용계약서	-성능 향상 소프트웨어 -서비스 수준에 따른 성능 데이터에 대한 자동 분석 -실시간 장비 모니터링 수행 및 전문인력 상주유무 점검	정보시스템감리 기준
4.4	서비스 제공에 대한 백업, 싱크 및 복구 대책 유무		관련문서 점검 및 실사 - IDC이 백업(백업 주기체크), 싱트, 복구관련 계획서 등 관련문서점검 -서비스수준을 확인할 수 있는 서류	서비스 지속성 확보대책 점검 - 관련문서 점검	-
4.5	전담 영업 및 지원 인력확보 및 추가 확보 계획 수립 여부		관련문서 점검 및 실사 -인적자원관리 현황표	전담 영업/지원 인력 확보 여부 점검	-
4.6	서비스 중단 등 피해보상에 대한 대책 유무		관련문서 점검 -SLA, 보험가입 계약서	이용자 피해보상에 대한 대책 점검 -보상규정, 보험가입	-

이 영역은 사후 발생가능한 계획적/비계획적 서비스 중단에 따른 백업장치(기술적, 관리적)의 다양한 확보 및 활동에 대한 점검을 통하여 향후 서비스의 지속성을 담보할 수 있는가를 평가하는 영역이다.

4.1 고객수 증가 혹은 데이터의 증가에 따른 수직적/수평적인 관점 모두에서 서비스의 품질유지를 위한 서비스 확장계획을 체계적으로 수립, 시행하고 있는가를 심사

4.2-4.3 예기치 못한 서비스 중단 및 정기적인 서비스 유지관리 활동에 따른 서비스 중단에 대비한 서비스 성능 유지활동의 체계적인 계획수립 및 시행여부를 심사

4.4 사업자의 파산 등에 따른 서비스 중단에 대비하여 서비스 이전 등 지속성을 담보할 수 있는 구체적 방안 심사

4.5 서비스 지속성 확보를 위한 적절한 경력과 능력을 보유한 전담영업 및 지원 인력확보여부 심사 및 향후 추가인력확보계획안 심사

4.6 사후 서비스시 발생할 수 있는 이용자의 피해에 대한 범위 및 보상 등 피해 구제에 대한 대책이 있는가를 심사

5) Ongoing Support 영역 - 고객지원

<표 2-19> 지속지원영역의 고객지원 심사항목

심사항목		심사방법	심사내용	근거
5.1	서비스 구축 계획, 서비스 시행 계획의 사전 수립 여부 점검	관련문서 점검 -서비스 구축계획서 -서비스 시행 사전계획서	서비스 구축 및 시행 계획의 체계적 시행 및 유지 점검	-
5.2	고객 교육에 대한 준비 상태 및 실시 여부 점검	관련문서 점검 -교육지원 활동표	고객교육에 대한 실시 점검 -교육프로그램	-
5.3	고객 사후 지원 인력 확보 및 사후 관리 조직의 확보 여부 점검	관련문서 점검 -고객사후 지원/관리 계획서	고객 사후 지원 프로세스 점검	-
5.4	서비스 만족을 위한 서비스 만족(SLA 포함 기능)에 대한 점검 기준 및 계약서 명시 점검	관련문서 점검 -서비스수준협약서 (SLA)	고객에 대한 SLA를 통한 품질보증 활동 점검	-

이 영역은 SaaS 서비스의 구축/시행의 체계적인 수행과 고객교육, 품질보증 등 사후 관리에 대한 집중적인 점검을 통하여 고객 지원 및 A/S서비스의 지속적 활동을 평가하는 영역이다.

5.1 서비스 구축 및 시행 계획의 체계적 시행 및 유지 점검

5.2 고객에 대한 실시 점검/교육 프로그램

5.3 고객 사후지원 프로세스 점검

5.4 고객에 대한 SLA를 통한 품질보증 활동 점검

라. IaaS 인증 평가 방법

IaaS 인증은 SaaS 인증과 달리 어플리케이션과 사업자(서비스 환경) 인증을 동시에 받아야 하고, 위에 개발한 두 가지 영역의 모든 항목은 필수항목으로 반드시 필요한 요소들로만 구성되어 있어, 세부 항목들은 최저기준인 동시에 공통필수항목이다. 따라서, IaaS 인증을 위해서는 모든 필수항목에 대한 일정 점수를 이상을 반드시 받아야만 한다.

항목별 점수산정은 5점 척도법(SD법) 적용하여 최소한 3점 이상의 점수를 받도록 하는 영역별 과락과 총점 과락 모두를 적용한다. 현재 평가방법에는 항목간의 중요도 차이가 있음에도 불구하고 이에 대한 가중치 설정이 되어있지 않은 상황이다. 즉, 모든 평가항목의 가중치는 동일한데, 향후에는 국내 실정에 맞는 항목간 가중치 부여가 필수적이라 하겠다.

제 4 절 SaaS 인증제도의 개발 방향

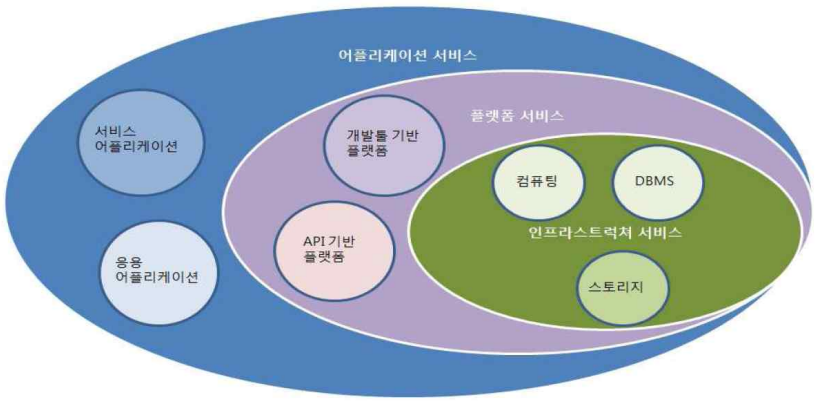
과거 네트워크를 통해 어플리케이션을 개별 단위로 임대하는 개념의 ASP 서비스 모델은 다양한 고객의 요구사항을 즉시 반영하기 어렵고, 개별 플랫폼으로 어플리케이션을 제공하기 때문에 운영에 많은 비용이 발생하였다. 이에 ASP 서비스를 개별적으로 관리하기보다 하나의 동일한 플랫폼을 이용하여 서비스를 제공하는 SaaS 방식이 등장하게 되면서 최근 IT 업계를 뒤흔들고 있다.

SaaS가 주목받는 이유는 SaaS가 국내 소프트웨어 시장에서 자리를 잡을 경우 파생될 수 있는 이슈가 산재되어 있기 때문이다. 사용자 입장에서 SaaS의 최대 강점은 굳이 비싼 비용을 들여 SW 라이센스를 구매하고 설치, 관리할 필요가 없다는 것이다. 또한 고객사의 소프트웨어 관리 작업을 단순화시키기 때문에 관리 업무량을 최소화 할 수 있다.

소프트웨어 업체 역시 SaaS를 통해 각 기업의 요구사항을 수렴해 신속하게 제품에 반영할 수 있으며 편리한 유지보수 및 업그레이드 서비스가 가능하다.

SaaS 서비스를 위한 요소는 아래의 그림과 같이 인프라, 플랫폼, 어플리케이션으로 구분할 수 있다.

< SaaS 서비스 분류 >



<그림 2-6> SaaS 서비스 분류

▪ SaaS 인프라

SaaS 인프라는 하드웨어, 네트워크, 데이터 등의 컴퓨팅 자원을 비즈니스 요구사항에 맞게 추상화 시키는 기술 전반을 말한다. 고객의 요구사항을 즉각 반영하고, 하나의 서비스를 여러 고객이 공유하여 사용하게 하는 하드웨어의 가상화, 분산화 및 병렬 기술을 들 수 있다.

SaaS 인프라는 소프트웨어적인 개발 및 실행 환경을 제공하는 플랫폼 제공자에게 기반 기술과 물리적 자원을 추상화하여 PaaS를 가능하게 하는 전반적인 기반 기술을 제공하는 역할을 한다.

▪ SaaS 플랫폼

SaaS 플랫폼은 인프라로부터 제공되는 하드웨어, 네트워크, 데이터 등의 컴퓨팅 자원을 소프트웨어적 측면에서 동일한 인터페이스로 접근하는 방법을 제공하며, 이를 통해 서비스 개발자들에게 동일한 개발 환경과 다양한 어플리케이션이 실행될 수 있는 운용 환경을 제공해 주는 기술로 개발 툴을 통해 서비스를 제공하는 방식과 API를 통해 제공하는 방식으로 구분 된다. SaaS 플랫폼은 개발자들에게 어플리케이션 개발, 인터페이스 개발, 데이터베이스 개발, 저장 공간 및 테스트 환경 등을 제공하는 역할과 SaaS 플랫폼을 이용해 개발한 소프트웨어를 일반 사용자에게 서비스하는 역할을 하게 된다.

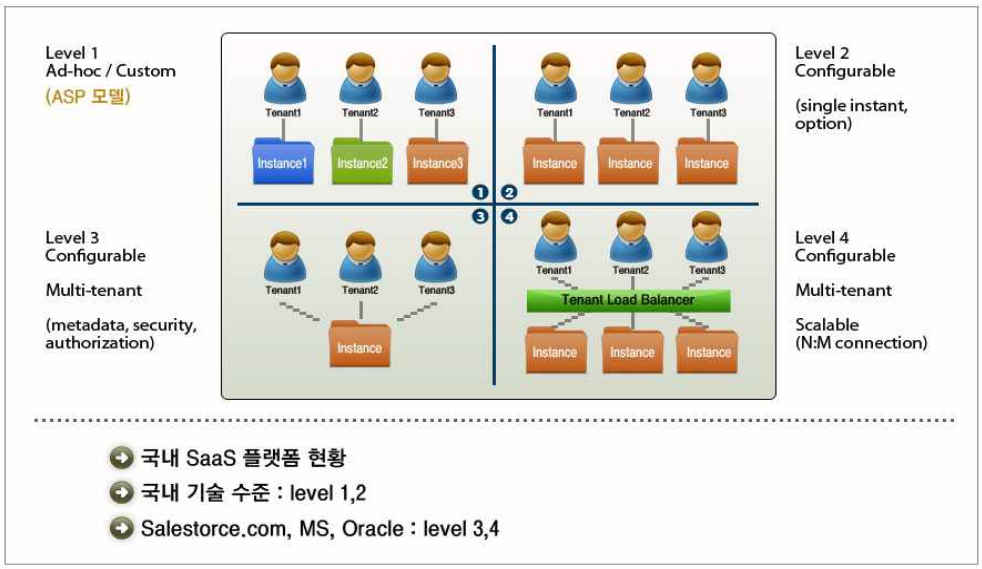
따라서 플랫폼은 개발자들에게 보다 저렴한 가격으로 온디맨드 형태의 소프트웨어 서비스를 개발하여 고객에게 제공할 수 있게 한다.

▪ SaaS 어플리케이션

SaaS 어플리케이션은 SaaS 플랫폼 기반 하에 개발된 웹 오피스, CRM, ERP등 각종 응용 서비스를 의미한다. 사용자의 요건에 맞는 다양한 서비스를 웹을 통해 고객이 직접 설정하여 이용할 수 있게 해준다.

위와 같은 SaaS 서비스를 위한 필요한 구성요소를 가지고 발전단계를 나눌 수 있다. SaaS 성숙도 모델은 SaaS 서비스가 갖는 통합과 고객 지향적 관점에서 성능

및 가용성의 정도를 몇 개의 단계로 구분한 체계를 말한다.



<그림 2-7> SaaS의 성숙도 모델

(출처 : 위키피디아 http://en.wikipedia.org/wiki/Software_as_a_service)

- 성숙도 1단계인 ad/hoc 단계의 SaaS 서비스는 네트워크를 통하여 고객의 요구사항에 맞는 소프트웨어를 일대일 방식으로 제공하는 전통적인 ASP 방식을 의미한다.
- 성숙도 2단계인 Configurable 단계의 SaaS 서비스는 코드 레벨의 수정 없이 다양한 사용자의 요구사항을 수용하고 사용자가 필요한 기능을 설정을 통해 지원하는 단계다. 이는 웹을 기반으로 한 표준화된 소프트웨어 인터페이스를 통해 비즈니스 프로세스를 정의하고 동적인 서비스 제공 환경을 실현 가능하게 한다.
- 성숙도 3단계인 Multi-Tenant Efficient 단계의 SaaS 서비스는 SaaS 서비스는 하나의 프로그램 인스턴스(instance)를 통하여 다양한 요구사항을 가진 고객을 지원하면서 개별 고객에 대하여 서로 다른 서비스 인스턴스를 운용하는데서 발생하는 부담을 줄이는 효과가 있다. 그러나 동일한 인스턴스에서 여러 응용 프로그램이 동시에 운용되기 때문에 데이터간 의미적 충돌이 발생할 수 있다.
- 성숙도 4단계인 Scalable 단계의 SaaS 서비스는 하나의 인스턴스 운용으로

인한 가용성 및 성능 이슈에 대해 유연하게 대응하는 단계를 의미한다. 즉 통합된 인스턴스가 가지고 있는 데이터 및 비즈니스 로직을 분산시키고, 병렬적으로 데이터를 처리하는 단계를 말한다. 고객의 입장에서는 동일한 인터페이스를 통하여 분산된 데이터와 컴퓨팅 자원을 제어할 수 있으며, 가상화, 분산/병렬 처리 프레임워크 등은 확장성 있는 서비스를 제공하는 핵심 기술이다.

SaaS의 성숙도 단계를 언급한 이유는 국내 SaaS 기술 수준을 쉽게 이해 할 수 있는데, 도움이 된다.

2009년도 1/4분기 국내 SaaS 사업체는 188개이며, 이중에서 SaaS 성숙도 1단계 사업체는 165개 업체인 87.8%를 차지하고, SaaS 성숙도 2단계 사업체는 19개 업체인 10.1%를 차지하며, SaaS 성숙도 3단계 사업체는 4개 업체인 2.1%를 차지하는 것으로 나타났다.

SaaS 서비스를 위한 요소는 인프라, 플랫폼, 어플리케이션으로 구분할 수 있다. 이 3가지 요소의 국내 수준은 다음과 같다.

▪ SaaS 인프라

SaaS는 차세대 소프트웨어 비즈니스 모델로 매우 빠르게 발전하고 있으며, 해외 글로벌 기업은 SaaS 서비스를 위한 인프라뿐만 아니라, 인프라 자체의 서비스에 필요한 기술을 개발하고 안정적 서비스를 제공하고 있으나, 국내에서는 아직 대표적인 인프라 사업자를 찾아보기 어려운 실정이다.

국내 대표적인 인프라 사업자 부재는 표준에 기반한 확장성을 중요시 하는 성숙도 4단계로의 발전을 어렵게 하는 장애 요인이 되고 있다.

국내 SaaS 서비스를 위한 인프라는 성숙도 3단계 수준이나, 인프라 자체의 서비스를 위한 기술 수준은 성숙도 2단계로 평가된다. 따라서 SaaS는 차세대 소프트웨어 비즈니스 모델로서 각광받고 있지만, 사용자의 요구사항에 유연하게 대응하기 위한

기술 개발이 추진 될 필요가 있다.

▪ SaaS 플랫폼

국내 플랫폼 기술 수준은 해외의 플랫폼과 비교할 때 사용자별 설정이나 메타데이터 관리 기능 등은 일부 지원하고 있으나, 온디맨드로 웹 어플리케이션을 개발하거나 인터넷 기반의 유연한 시스템 확장성은 현재 제공하고 있지 못하고 있다. 또한 서비스를 위한 API는 제공하고 있으나 개발 툴을 제공하지 못하는 실정이기 때문에 플랫폼 서비스로 분류하기에는 미약한 수준이다. 플랫폼 분야에서 국내의 기술수준은 선진국에 비해 3년 정도 뒤쳐진 것으로 평가되고 있다.

▪ SaaS 어플리케이션

SaaS 어플리케이션 개발 해외 사례로는 구글, 세일즈포스닷컴, 넷슈트, 페이스북, 번커넥트 등이 있으며, 국내 사례로는 한컴씽크프리 오피스, 애니티앤에스 CRM, 이카운트 ERP 등이 있다. 구글, 세일즈 포스닷컴 등 해외 SaaS 어플리케이션은 SaaS 성숙도 3단계 이상을 지원하고 있으나 국내 188개업체를 조사한 결과 SaaS 성숙도 1단계 사업체는 165개 업체인 87.8%를 차지하고, SaaS 성숙도 2단계 사업체는 19개 업체인 10.1%에 불과하다. 국내 어플리케이션 중 성숙도 2단계 이상 중 일부는 성숙도 3단계 이상 수준이더라도 웹 표준을 부분적으로 지키고 있어, 서비스가 인터넷 익스플로러에서만 작동하며, Open API의 개발 지원수준은 초보적인 수준이다. 어플리케이션의 기술 수준이 낮은 것은 기술개발 능력 자체가 부족한 것보다 국내에서 SaaS 시장의 느린 성장, SaaS로 전환 시 매출 규모 감소 우려 등으로 국내 기업들의 적극적인 사업 진출을 더디게 하고 있기 때문이다. 어플리케이션 분야에서 국내의 기술수준은 선진국에 비해 1.5년 정도 뒤쳐진 것으로 평가되고 있다.

따라서 본 보고서에는 이러한 국내 SaaS 시장현황을 충분히 고려한 SaaS 인증제도를 개발한다. 특히 ASP는 SaaS 성숙도 모델에서 Level 1에 해당하므로 SaaS 인증제도에서는 ASP 서비스도 포함하여 개발하는 것이 가능하다. 그리고

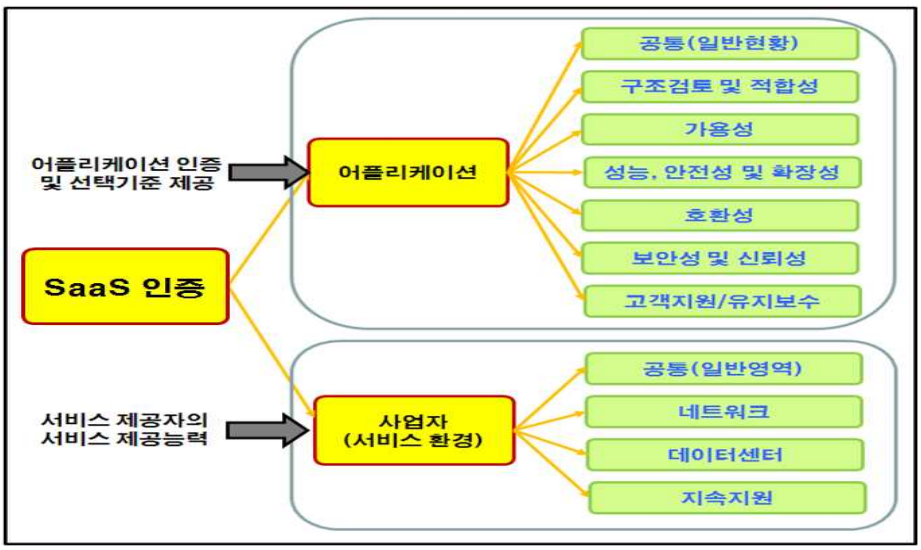
본 연구에서 개발한 SaaS 인증제도에서는 특히 어플리케이션의 SaaS 성숙도 모델중 Level 2이상인 것에 대한 차별화된 인증을 부여하는 방안도 제시하나(예를 들면 SaaS Level 1, SaaS Level 2, SaaS Level 3, SaaS Level 4 인증부여), 실제로 SaaS Level을 차별화하여 인증을 부여하는 제도의 시행을 위해서는 사전에 충분한 협의 및 합의가 필요하리라 사료된다.

제 5 절 SaaS 인증제도

1. SaaS 인증영역

SaaS 인증은 어플리케이션 인증과 사업자(서비스 환경) 인증으로 구분하여 개발할 수 있다. SaaS 인증의 핵심내용은 어플리케이션 인증이므로, SaaS의 기능, 특징 및 세부 기술적인 요소 등이 심사영역 및 항목으로 포함하여 SaaS 어플리케이션 영역의 인증을 위한 심사영역과 세부 심사항목을 개발하기로 하고 SaaS 사업자(서비스 환경) 영역의 인증을 위한 심사영역과 세부 심사항목도 동시에 개발하기로 한다.

본 보고서에서 개발한 SaaS 인증영역은 아래 <그림 3>과 같다.



<그림 2-8> SaaS 인증범위

2. SaaS 어플리케이션 인증

본 절에서는 SaaS 어플리케이션 인증을 위한 인증심사기준과 이에 대한 설명을 기술하기로 한다. SaaS 어플리케이션 인증을 위하여 총 7개의 심사영역에 35개 심사항목이 개발되었는데, 이에 대하여 차례대로 기술하기로 한다.

가. 일반현황

<표 2-20> 일반현황영역 인증심사기준

심사항목		심사방법	심사내용	근거
1.1	회사의 정체성	관련문서 점검 -사업자등록증 -하청(위탁)계약서 -기타 관련 증빙서류	회사의 일반현황 점검 -회사명 -회사의 규모 및 업종 -사업장규모 -협력업체의 서비스 범위	-
1.2	회사의 인적 자원의 안정성	관련문서 점검 및 실사 -지원조직도 -인적자원관리 현황표	지원조직 및 인적자원관리 평가/점검 -조직 구성 -인력조직 현황 -헬프 데스크 조직 유무 -IT조직의 구성 (기능, 구성원수, 조직형태)	-
1.3	고객 대상의 확보	관련문서 점검 -고객리스트 -라이센스 계약서 -서비스 계약서	실제 사용하고 있는 고객의 확인을 통한 노하우 점검 -ISV의 경우 1개이상의 SaaS사업자 -자체 서비스의 경우 3개 이상의 고객 확보	-
1.4	회사의 평판	설문조사/면접 및 투표	SaaS 관련 업계에서의 평판 점검 및 SaaS 어플리케이션 평판 점검 -설문조사/면접 -투표/전문가평가	-

이 영역은 SaaS 어플리케이션 개발업체(소유자)의 일반현황을 점검하는 영역으로서 회사의 실제 존재여부, 인력자원의 확보 여부, 고객의 확보 여부를 파악하여 잠재적 능력 및 운용능력 등 회사의 기본적인 안정성을 점검하여 지속적으로 서비스를 제공할 제반환경이 갖추어져 있는가를 평가하는 영역이다.

1.1 회사명, 규모 및 업종, 협력업체 (SaaS 사업자)의 서비스 범위 등을 심사

1.2 헬프데스크 조직 유무, 개발인력 (기능, 구성원수) 등 인력조직 운용 현황을 심사

1.3 심사시점 현재 실제 SaaS 어플리케이션을 사용하고 있는 고객의 유무를 통하여 SaaS 서비스에 대한 노하우 및 지속가능성 , 서비스 지속에 대한 사업자의 의지 여부를 심사

1.4 SaaS 서비스에 대한 소비자들의 평판을 점검하는 항목으로 서비스 품질 및 만족도, 신뢰성 등에 의하여 만들어지며 설문조사/면접 및 투표 등 여러 가지 방법을 통하여 측정가능하며, 궁극적으로 SaaS 서비스 관련 업계에서의 회사 평판 및 SaaS 어플리케이션의 평판을 점검

나. 구조검토 및 적합성

<표 2-21> 구조검토 및 적합성 영역 인증심사기준

심사항목		심사방법	심사내용	근거
2.1	어플리케이션 기능에 대한 명확하고 상세한 설명서 존재 유무	관련문서 점검 -어플리케이션 상세설명서 -어플리케이션 백서	이용자가 쉽게 이해하고 사용할 수 있는 문서관리 점검	SW품질인증기준 (제5조)
2.2	어플리케이션의 논리적 구조에 대한 다이어그램 설명서 존재 유무	관련문서 점검 -어플리케이션 논리적 구성도	이용자의 어플리케이션 이해도 증진 및 문제발생시 기본자료 제공 점검 -어플리케이션, 미들웨어, 데이터베이스, OS, 하드웨어, 네트워크의 구성 점검	SW품질인증기준 (제5,6조)
2.3	어플리케이션의 물리적 구조에 대한 다이어그램 설명서 존재 유무	관련문서 점검 -어플리케이션 물리적 구성도	이용자의 어플리케이션 이해도 증진 및 문제발생시 기본자료 제공 점검 -인프라 운영체제(OS), 데이터베이스 플랫폼, 어플리케이션 플랫폼, 어플리케이션 등 서비스 의 물리적 구조 점검	SW품질인증기준 (제5,6조)
2.4	어플리케이션의 적용된 기술의 성숙도 모델(Level) 설명서 존재 유무	관련문서 점검 -Level 1~Level4의 핵심기술을 적용하여 어플리케이션을 구현한 설명서	어플리케이션의 성숙도 모델을 점거하여 사용자의 어플리케이션의 기능 및 효과적 사용성 점검 - 메타데이터기반 configuration 가능성, 다중테넌트 구조 지원성, 다중테넌트 부하 분산, Scalability 기능 지원성 점검	어플리케이션의 Level 1-4 부여 가능

이 영역은 어플리케이션의 기본적인 구조를 검토하여 SaaS 서비스로서의 유용성

및 적합성을 심사하는 영역으로서 어플리케이션의 기능, 논리적 구조 및 물리적 구조를 점검함으로써 SaaS 어플리케이션으로서의 구조의 적합성 여부를 평가하는 영역이다.

2.1 기능에 대한 평가는 물론 이용자가 쉽게 이해하고 사용할 수 있도록 어플리케이션의 기능을 명확하고 상세하게 기술해 놓은 문서가 존재하고 그 유지관리를 시행하는지를 심사

2.2 어플리케이션에 대한 문제발생시(버그 등) 기본 자료로 제공가능한 문서의 존재 및 유지관리를 심사

2.3 어플리케이션이 서비스되고 있는 구조의 적합성 검토를 통해 어플리케이션의 이해 증진 및 문제해결을 위한 문서의 존재 심사

2.4 어플리케이션의 성숙도 모델을 점거하여 사용자의 어플리케이션의 기능 및 효과적 사용을 위한 문서의 존재 심사

다. 가용성

<표 2-22> 가용성영역 인증심사기준

심사항목		심사방법	심사내용	근거
3.1	다수의 사용자의 동시접속 사용 가능 여부(가능하다면 그 기술적 구현 방법 기술)	관련문서 점검 및 실사 -기술구현 증빙자료 -어플리케이션 운용검증	동시접속 기술구현 점검 접근제어 및 인증기술 점검	ASPIC USA
3.2	모든 기능 및 관리를 웹브라우저를 통하여 접근 및 운용 가능 여부	어플리케이션 운용검증 -지원하는 웹브라우저 : 버전/제작사	다양한 웹접속기반에서의 안정성 검증	ASPIC USA
3.3	어플리케이션의 기본적인 결함 점검	관련문서 점검 및 실사 -어플리케이션 무결성 테스트보고서	어플리케이션의 무결성 체크	SW품질인증기준 (제17조)
3.4	총사용시간과 접근가능시간 점검	총사용시간과 서비스 접근가능시간에 대한 비율 점검 및 분석보고서 심사	어플리케이션 서비스의 웹상에서의 가용성을 점검	-

이 영역은 어플리케이션이 웹을 통하여 다수의 사용자의 접속이 가능하고 기본

적인 결합 유무를 심사하는 영역으로서 다수 사용자의 동시접속 가능여부, 웹을 통한 접속가능성 및 기본적인 무결성을 점검함으로써 SaaS 어플리케이션으로서의 적합성 여부를 평가하는 영역이다.

3.1 SaaS 서비스의 기본기술인 다수 사용자의 동시접속 가능여부 점검 및 해당 어플리케이션이 매뉴얼상 표시된 동시접속 가능여부를 심사

3.2 어플리케이션을 웹브라우저를 통하여 접근 및 운용 가능여부를 심사

3.3 어플리케이션의 무결성을 점검하여 기본적인 결함여부를 심사

3.4 어플리케이션의 웹상에서의 가용성을 입증할 수 있는 분석 보고서의 존재 여부 심사

라. 성능, 안정성 및 확장성

<표 2-23> 성능, 안정성 및 확장성 영역 인증심사기준

심사항목		심사방법	심사내용	근거
4.1	주기적인 어플리케이션 성능(Performance) 테스트실시 점검	관련문서 점검 -성능테스트 보고서(응답시간 및 최대 처리량 테스트결과 필수)	어플리케이션 성능유지를 위한 서비스 활동 점검 -주요 기능 구동의 응답시간에 대한 최소, 최대, 평균시간, 최대처리량, 장애복구 시간 등	SW품질인증기준(제10조)
4.2	주기적인 어플리케이션 안정성 테스트실시 점검	관련문서 점검 -안정성테스트 보고서(이용가능성, 접근성, 신뢰성 테스트결과 필수)	어플리케이션 안정성 유지를 위한 활동 점검 -제공되는 서비스의 이용가능성, 접근성, 신뢰성 등	SW품질인증기준(제10조)
4.3	고객(사업)수의 증가에 대비한 성능유지가능 여부	관련문서 점검 -어플리케이션 기술지침서	어플리케이션 사용자수 증가에 따른 성능 유지관리 점검	ASPIC USA
4.4	고객(사업)수의 증가에 대비한 확장성(scalability) 확보 여부	관련문서 점검 -어플리케이션 기술지침서	어플리케이션 사용자수 증가에 따른 확장성 기술 점검 - 사용자에 대한 모니터일 및 확장을 동적으로 해줄 스케쥴러 및 프로비저닝 기능 점검 - 운영중 다운타임없이 사용자, 서버 등 확장성 점섬 - 확장성확보를 위한 메터데이터 플랫폼(Level 2) - 확장성 확보를 위한 메터 데이터 처리기술과 Multi-Tenant 지원 기술 (Level 2 & 3) - 하나의 인스턴스 운용으로 인한 가용성 및 성능 점검 및 이를 위한 병렬데이터를 처리 기술 (Level 3) - 고객입장에서 동일한 인터페이스를 통한 분산된 데이터처리, 컴퓨팅 자원을 제어가능성, 가상화, 분산/병렬 처리 프레임워크 등은 확장성 있는 서비스를 제공하는 핵심 기술 (Level4)	ASPIC USA

이 영역은 해당 어플리케이션의 성능, 안정성 및 확장성 유지를 위한 점검활동 및 향후 사업 확장에 대한 계획 등 제반 활동사항을 평가하는 영역이다.

4.1 어플리케이션 성능유지를 위하여 주요 기능의 구동시 응답시간에 대한 최소, 최대, 평균시간, 최대처리량, 장애복구시간 등을 주기적으로 테스트하고 유지관리하는가를 심사

※ 응답시간(Response Time)

요청(Request)을 보내고 응답(Response)을 받는데 걸리는 시간을 의미한다. 이러한 응답 시간은 실제 서비스 호출에서 시간을 측정하며 아래의 공식을 적용하여 산출한다. 시스템응답 완료시간은 시스템의 응답이 사용자에게 도착한 시간이며 사용자 요청 시간은 사용자가 요청을 보낸 시간을 의미한다. 대개의 경우 응답시간은 일정 시간동안의 평균값으로 구한다.

응답시간 = 시스템응답완료시간 - 사용자요청시간

※ 최대 처리량(Maximum Throughput)

서비스 제공 플랫폼이 단위 시간 동안에 처리할 수 있는 서비스의 최대 요청 수를 의미한다. 이러한 처리량은 서비스 제공자에 대한 성능 지표로 사용될 수 있다. 얼마만큼의 처리를 할 수 있는가는 웹 이라는 환경에 있어서 얼마나 많은 사용자를 처리할 수 있는가를 의미하기도 한다. 최대 처리량은 아래의 공식에 의해서 구해진다.

최대처리량 = 완료된 최대요청수 / 단위시간

4.2 어플리케이션 안정성 유지를 위한 활동 점검하는 항목으로 SaaS 서비스가 어느 정도 안정하게 서비스를 제공하는지를 점검. 즉, 처리량의 증가, 폭주, 시스템의 고장, 자연 재해 그리고 사람에 의한 고의적 공격에도 지속적이고

일관성 있으며 원래의 상태로 회복 가능한 서비스를 제공할 수 있는 능력을 점검하는데, 세부적으로 서비스의 접근성, 신뢰성 등을 주기적으로 테스트하고 유지관리하는가를 심사

※ 접근성(Accessibility)

이용가능성이 보장되는 상황에서 서비스의 접근 가능한 정도를 나타낸다. 즉, 한 시점에서 하나 이상의 서비스 요청에 대해서 성공적으로 응답할 수 있는지에 대한 정도를 의미한다. 어떤 경우에는 서비스 대해서 사용가능(Available)은 하지만 접근(Accessible)은 되지 않는 경우가 있다. 서비스의 높은 접근성(High Accessibility)에 대한 보장은 확장성이 뛰어난(High Scalable) 시스템을 구축함으로서 가능하다. 이러한 높은 확장성이란 볼륨량이 가변적인 요구에 대해서 일관되게서비스를 수행할 수 있는 시스템의 확장 능력을 말한다. 접근성은 동시에 보내지는 요청 메시지 수에 대해서 반환되는 응답 메시지의 수의 비율로 나타낸다. 아래의 공식에서 요청 메시지 수(Request Message Count)는 동시에 보내진 요청 메시지수를 응답 메시지 수(Normal Response Message Count)는 정상적으로 처리되고 나서 반환된 응답 메시지 수를 의미한다.

접근성 = 응답메시지수 / 요청메시지수

※ 신뢰성(Reliability)

주어진 기간 동안 약속된 서비스를 제대로 수행한 정도를 의미한다. 일별, 주별, 월별 또는 년별로 서비스 사용에 대해서 얼마만큼 신뢰할 수 있는지를 나타낸다. 신뢰성 품질을 측정하기 위해서는 단위 시간 동안에서 시스템다운뿐만 아니라 서비스 요청이 실패에 대한 로그 분석을 통해서 에러 간의 시간을 통해서 구해진다. 공식은 아래와 같다. 에러간 평균시간(Mean Time Between Error)은 발생한 에러간의 평균 시간을 의미하며 단위시간은 측정하는 단위 시간을 의미한다.

신뢰성 = 1 - 에러간 평균시간 / 단위시간

4.3 어플리케이션 사용자수 증가에 따른 성능(performance) 유지관리 능력 심사

4.4 어플리케이션 사용자수 증가에 따른 확장성 능력 심사하는 항목으로써 SaaS의 핵심기술인 메타데이터 처리기술, 멀티테너트 지원기술, 분산된 데이터 처리, 컴퓨팅 자원을 제어가능성, 가상화, 분산/병렬 처리 프레임워크 등은 확장성 있는 서비스를 제공하는 핵심 기술 능력 심사

마. 호환성

<표 2-24> 호환성 영역 인증심사기준

심사항목		심사내용	근거
5.1	EDI 오브젝트, 바이너리 파일, HTML 폼 등 다양한 데이터포맷 지원 여부	어플리케이션 구동시 생성되는 데이터포맷 지원여부 점검	ASPIC USA
5.2	O/S, DBMS에도 관계없이 구동가능한 플랫폼 독립적인지 여부	제3의 주요 구성요소와의 독립성 점검	ASPIC USA
5.3	팩스, 프린터 등 모든 하드웨어 장비 지원 여부	주변OA장치와의 호환성 검증	SW품질 인증기준 (제11조)
5.4	데이터 전송시스템이 윈도우, 리눅스, 유닉스 시스템 지원 여부	데이터전송의 호환성 점검	SW품질 인증기준 (제11조)
5.5	Active X 등의 독립성 여부	특정 OS에 독립적인지 점검	-

이 영역은 어플리케이션 구동시 생성되는 데이터포맷의 다양한 지원과 DBMS, OS 등 다양한 플랫폼 환경하에서의 운영여부와 사용자 운영환경하에 있는 다양한 주변장치를 지원하는지, 어플리케이션 구동시 생성되는 데이터의 전송에 있어 플랫폼 제약은 없는지, Active X의 독립성을 점검하여 해당 어플리케이션의 기본적인 호환성 확보여부를 평가하는 영역이다.

5.1 어플리케이션 구동시 생성되는 데이터 포맷 지원여부 점검

5.2 제3의 주요 구성요소의 독립성 점점

5.3 주변 OA 장치와의 호환성 검증

5.4 데이터 전송의 호환성 점검

5.5 특정 OS에 의존인지 독립적인지 점검

바. 보안성 및 신뢰성

<표 2-25> 보안성 및 신뢰성 영역 인증심사기준

심사항목		심사방법	심사내용	근거
6.1	보안정책 유무	보안정책 문서 점검 및 실사 -전체 보안정책 문서	어플리케이션 서비스 전체 보안정책 점검	관련 표준
6.2	접속 권한에 따른 접근 제어 유무	관련문서 점검 및 실사 -접근제어 기술문서 -어플리케이션 기술지침서 -ACL	비인가된 이용자로부터의 데이터 보호 장치 점검	관련 표준
6.3	검증을 통한 사용자의 인증 절차 유무	관련문서 점검 -어플리케이션 기술지침서 -Sigle Sign-On 기능 제공 여부	이용자의 인증절차 유무 검증 -Sigle Sign-On 기능 -패스워드, 쿠키 정책 -ACL 등	관련 표준
6.4	데이터의 기밀성을 위한 보안기술 적용 유무	관련문서 점검 및 실사 -플리케이션 기술지침서	어플리케이션 구동시 생성되는 데이터의 보호를 위한 조치 점검	관련 표준
6.5	데이터의 무결성을 위한 보안기술 적용 유무	관련문서 점검 및 실사 -어플리케이션 기술지침서	어플리케이션 구동시 생성되는 데이터의 보호를 위한 조치 점검	관련 표준
6.6	어플리케이션 접속시 방화벽을 통한 접근 유무	관련문서 점검 -어플리케이션 기술지침서	HTTPS지원 유무 점검	관련 표준
6.7	로그파일 분석을 통한 감사추적 기능 지원 유무	관련문서 점검 및 실사 -어플리케이션 기술지침서 -로그분석 보고서	비인가된 자로부터의 접근을 보호하고 추적하기위한 관리적 대책 점검	관련 표준
6.8	메시지의 송수신 자가 송수신 사실을 부인하지 못하도록 하는 부인방지 기능 지원 여부	관련문서 점검 및 실사 -어플리케이션 기술지침서 -메세지 레벨의 전자서명기법을 이용한 부인방지 기능 점검	전송레벨은 제외하고, 메세지 레벨에서의 부인방지 기능 점검	관련 표준
6.9	개인의 프라이버시 보호와 관련된 보안 기능 점점	관련문서 점검 및 실사 -어플리케이션 기술지침서 -메세지 레벨의 프리이버시 보호기능 점검	전송레벨은 제외하고, 메세지 레벨에서의 개인 프라이버시 보호 기능 점검	관련 표준
6.10	자동 백업, 싱크 및 복구 기능 여부	관련문서 점검 및 실사 -어플리케이션 기술지침서	데이터의 자동 백업, 싱크 및 복구 기능 점검	

이 영역은 주로 어플리케이션과 관련된 부분에 대한 보안평가로서 어플리케이션

자체내(소스내) 보안구현보다는 네트워크와 어플리케이션이 접속되는 서비스 환경에 대한 점검활동 및 통제활동을 평가하는 영역이다.

6.1 SaaS 서비스의 전체 보안정책을 가지고 서비스를 운영하는지를 심사

6.2 비인가된 사용자의 접근을 방지하기 위하여 접속권한에 따라 권한 설정의 기능이 구현되어 있는지를 심사

6.3 ID/패스워드, 쿠키 정책을 통한 인증절차의 기능구현 및 정책수립 여부를 심사하고 서비스 환경에서는 메시지가 다양한 보안 도메인을 경유하기 때문에 보안 토큰을 통한 Single Sign-On 기능이 제공되는지 여부 점검

6.4-6.5 어플리케이션 구동시 생성·트랜잭션되는 데이터의 보호를 위한 기술 및 정책수립 여부를 심사

6.6 어플리케이션 접속시 방화벽을 경유하여 접근가능하도록 구현되어 있는지 심사

6.7 비인가된 사용자의 침해방지를 위한 관련 로그분석활동을 정기적으로 시행하고 있는지를 심사

6.8 메시지의 송수신자가 송수신 사실을 부인하지 못하도록 하기 위아여 전자서명 기법을 사용한 부인방지 기능 지원 여부

6.9 사용자와 제공자 양 당사자 측면에서 개인의 프라이버시 보호와 관련된 보안 기능 점점

6.10 SaaS 서비스의 특징상 데이터의 자동 백업, 싱크 및 복구 기능 점검

참고로 SaaS 서비스 환경에서 제공해야 할 보안 서비스의 분류는 다음과 같다.

※ 데이터 기밀성 (Data Confidentiality)

데이터 기밀성이란 중요한 데이터를 공격자가 접근해서 읽는 것을 막는 품질로서 주로 이러한 기밀성을 제공하기 위해서 암호화기법을 사용한다.

※ 데이터 무결성 (Data Integrity)

데이터 무결성이란 데이터 전송 시 공격자가 데이터를 가로채서 불법적으로 삽입, 수정 그리고 변조하는 것을 탐지하는 품질을 말한다. 주로 해쉬 함수의 특징을 이용해서 데이터 무결성을 검증하지만 전자서명을 이용할 경우 전자서명 자체 안에 데이터 무결성을 검증하는 속성이 들어 있다.

※ 사용자 인증 (User Authentication)

어떤 사용자가 자신의 Identity 주장을 상대방에게 확신 시키는 과정으로 일반적으로 사용하는 인증 방식은 요청자가 알고 있는 지식을 이용해서 인증을 수행한다. 서비스 환경에서는 SOAP 메시지가 다양한 보안 도메인을 경유하기 때문에 보안 토큰을 통한 Single Sign-On 기능이 제공되어야 할 필요가 있다.

※ 접근 제어 (Access Control)

권한이 없는 사용자가 특정 자원에 접근하지 못하게 하는 보안 품질로서 서비스 환경에서 SOAP 메시지가 다양한 보안 플랫폼을 경유하기 때문에 하나의 서비스 보안 토큰을 통한 접근 제어가 가능해야 한다.

※ 부인방지 (Non-Repudiation)

메시지의 송수신자가 송수신 사실을 부인하지 못하도록 하는 방법으로서 전자서명 기법을 사용해서 이러한 부인방지 서비스를 달성할 수 있다.

※ 접근성 (Accessibility)

서비스 환경에서 접근성은 바로 서비스 거부 공격을 어떻게 탐지하고 예방하는 가에 달려있다. 특히 서비스 기반 환경에서 특정 서비스에 대한 접근이 보장되지 않는 것은 서비스 활성화에 부정적인 영향을 끼친다.

※ 감사 추적(Audit Trail)

특정 서비스에 공격 시도 행위에 대한 로그를 남겨서 사후에 보안 감사 시에 서비스 보안 취약점 및 공격에 대한 다양한 정보로 활용한다.

※ 프라이버시 보호(Privacy)

서비스 사용자와 서비스 제공자 양 당사자 측면에서 개인의 프라이버시 보호와 관련된 서비스를 말한다.

또한 SaaS 서비스 환경에서 위의 보안 서비스를 제공하기 위한 보안 메커니즘은 크게 다음과 같이 두 가지 레벨에서 제공할 수 있다.

※ 전송레벨 보안(Transport Level Security) - Non-Persistent Level Security

전송레벨 보안은 서비스의 프로토콜인 SOAP의 하위 네트워크 레이어에서의 보안을 의미한다. 이는 기존 웹 환경인 HTTP 프로토콜 기반에서 사용하던 SSL, TLS 등의 보안 메커니즘을 이용한 방법이다. 이러한 전송레벨에서 보안은 Point-To-Point 보안 컨텍스트 사용, 부분암호화 그리고 부분 전자서명과 같은 것들을 지원하지 않기 때문에 만일 이러한 특징을 반영하기 위해서는 메시지 레벨 보안을 사용해야 한다. 특히 전송 레벨은 Point-To-Point 보안 컨텍스트를 사용하기때문에 컨텍스트에 대한 정보가 하나의 Point를 벗어나면 잃어버리는 Non-Persistent Level Security이다.

※ 메시지레벨 보안 (Message Level Security) - Persistent Level Security

메시지레벨의 보안은 SOAP 메시지에 대한 데이터 기밀성, 무결성, 접근제어와 같은 보안 서비스를 제공하기 위해서 XML기반의 SOAP메시지를 이용해서 보안 서비스를 제공하는 방식이다. 이러한 메시지 레벨 보안은 End-To-End 보안 컨텍스트를 사용하기 때문에 SOAP 메시지 자체가 다양한 보안 도메인을 경유해도 컨텍스트 정보가 유지되는 Persistent Level Security이다.

사. 고객지원, 유지보수 정책

<표 2-26> 고객지원 및 유지보수 정책영역 인증심사기준

심사항목		심사방법	심사내용	근거
7.1	버그나 문제발생시 고객에 대한 지원프로세스 존재 유무	관련문서 점검 -SLA -버그 및 문제발생시 지원프로세스 문서	버그 등에 대한 개발자의 응대처리 점검 -이용자 대처방법, 개발자 문제해결방법을 기술한 문서의 유지관리 점검	SW품질인증기준(제18조)
7.2	서비스 제공자가 해당 어플리케이션을 제공시 지원하는데 유용한 문서 존재 유무	관련문서 점검 -어플리케이션 기술 지원 문서	서비스제공자가 이용자 지원을 위한 기술지원문서 유지관리 점검 -온라인 헬프, 웹페이지, 프로그램 로직 매뉴얼, 튜닝가이드 등	SW품질인증기준(제18조)
7.3	최적의 어플리케이션 서비스 환경유지를 위한 운영전략 수립 여부	관련문서 점검 -어플리케이션 기술 지원지침서	어플리케이션의 목표 이용수준을 유지하기 위한 업그레이드, 백업전략, 운영절차 수립 시행 점검	-
7.4	지속적인 서비스 제공을 위한 모니터링 기술이나 툴의 확보 및 지원 여부	관련문서 점검 -모니터링 보고서 -관련 기술 및 툴을 확인할 수 있는 증빙자료	사후 서비스제공자가 서비스 제공을 위한 어플리케이션 모니터링 기술지원 점검 -서비스 실패요인 발견을 위한 기술 및 툴	SW품질인증기준(제18조)

이 영역은 어플리케이션의 유지보수, 컨설팅, 교육, 콜센터 및 헬프데스크 운영 등의 대 고객 서비스를 점검하는 영역으로서 서비스 상황을 모니터링하고, 헬프데스크를 운영하며, 교육활동을 실시하는가를 평가하는 영역이다.

7.1 버그, 서비스 장애 등 서비스 중단에 따른 문제발생시 신속하게 대응 처리할 수 있는 프로세스 수립 및 지원여부를 심사

7.2 해당 어플리케이션을 서비스하는 제공자(SaaS 사업자)가 이용자(사용자)에게 신속하고 명확하게 지원가능하도록 관련 기술지원문서를 제공하고 유지관리 하는지를 심사

7.3 어플리케이션의 목표 이용수준을 유지하기 위한 업그레이드, 백업전략, 운영절차 등을 수립 · 시행하고 있는지를 심사

7.4 지속적인 서비스제공의 안정성을 확보하기 위한 활동으로서 어플리케이션 모니터링 기술 및 툴의 확보를 통한 주기적인 점검활동여부를 심사

3. SaaS 사업자(서비스 환경) 인증

본 절에서는 사업자(서비스 환경) 인증을 위한 인증심사기준과 이에 대한 설명을 기술하기로 한다. 사업자(서비스 환경) 인증을 위하여 총 5개의 심사영역에 28개 항목심사항목이 개발되었는데, 이에 대하여 차례대로 기술하기로 한다.

가. 일반 영역

<표 2-27> 일반현황영역 인증심사기준

심사항목		심사방법	심사내용	근거
1.1	회사의 정체성	관련문서 점검 -사업자등록증 -하청(위탁)계약서 -기타 관련 증빙서류	회사의 일반현황 점검 -회사명 -회사의 규모 및 업종 -사업장규모 -협력업체의 서비스 범위 -서비스 명/종류	-
1.2	회사의 인적자원의 안정성	관련문서 점검 및 실사 -지원조직도 -인적자원관리 현황표	지원조직 및 인적자원관리 평가/점검 -조직 구성 -인력조직 현황 -헬프 데스크 조직 유무 -IT조직의 구성 (기능, 구성원수, 조직형태)	-
1.3	고객 대상의 확보	관련문서 점검 -서비스 계약서	서비스 계약 사실 확인 (최소 고객 2개이상 존재)	-
1.4	과금체계의 합리적/체계적 정립 유무	관련문서 점검 -서비스 비용산정을 증빙할 수 있는 서류 -표준계약서 -SLA -가격표	과금체계(비용산정)의 합리적 정립을 확인	-
1.5	회사의 평판	설문조사/면접 및 투표	SaaS 관련 업계에서의 평판 점검 -설문조사/면접 -투표	

이 영역은 서비스 사업자의 일반현황을 점검하는 영역으로서 회사의 실제 존재여부, 인력자원의 확보 여부, 고객의 확보 여부를 파악하여 잠재적 능력 및 운용능력 등 회사의 기본적인 안정성을 점검하여 지속적으로 서비스를 제공할 제반환경이 갖추어져 있는가를 평가하는 영역이다.

1.1 회사명, 규모 및 업종 등을 심사

1.2 핼프데스크 조직 유무, 개발인력(기능, 구성원수) 등 인력조직 운용 현황을 심사

1.3 심사시점 현재 실제 ASP서비스를 이용하고 있는 고객의 유무를 통하여 ASP서비스에 대한 노하우 및 지속가능성 , 서비스 지속에 대한 사업자의 의지 여부를 파악

1.4 과금체계를 합리적이고 체계적으로 산정, 정립하고 있는지를 심사

1.5 서비스에 대한 소비자들의 평판을 점검하는 항목으로 서비스 품질 및 만족도, 신뢰성 등에 의하여 만들어지며 설문조사/면접 및 투표 등 여러 가지 방법을 통하여 측정가능하며, 궁극적으로 SaaS 관련 업계에서의 회사 평판을 점검

나. 네트워크 & 데이터센터 영역 - 보안성

<표 2-28> 네트워크 및 데이터센터 영역의 보안성 심사항목

	심사항목		심사방법	심사내용	근거
물리적 보안	2.1	물리적 보안 대책수립 여부	관련문서 점검 및 실사 -보안정책서 -전산실무지침서	물리적 보안체계 점검	정보시스템 감리기준
기술적 보안	2.2	출입통제 유무	관련문서 점검 및 실사 -출입통제 관리 문서	독립적인 전산실 확보 출입통제장치 유무	정보시스템감리기준
	2.3	침해방지 대책 유무	관련문서 점검 및 실사 -보안솔루션 계약서 (방화벽, IDS 등)	보안 침해방지를 위한 활동 점검	정보보호지침, IDC시설 안전신뢰성기준
	2.4	보안취약점검 유무	관련문서 점검 -보안취약점검 보고서 (바이러스 점검 포함)	보안취약 점검의 주기적 활동 점검	정보보호지침, IDC시설 안전신뢰성기준
관리적 보안	2.5	파일전송시 암호화 유무	관련문서 점검 및 실사 -파일암호화/무결성 체크 문서	서버와 클라이언트간에 전송대는 정보에 대한 완벽한 보안을 위해 128비트 암호화 제공여부 점검	정보보호지침, IDC시설 안전신뢰성기준
	2.6	사업자 활동 점검	관련문서 점검 -보안정책 -시스템운영지침서	보안을 위한 사업자의 주기적인 활동 점검	정보보호지침
	2.7	시스템 통제 활동 점검	관련문서 점검 및 실사 -시스템 접근권한 명시문서 -서비스관련 SW점검표	논리적 접근통제활동 점검 서버내 서비스 관련 SW 점검정책 유무	정보보호지침

이 영역은 물리적, 기술적, 관리적인 측면에서 비인가된 사용자로부터의 접근통제를

통하여 이용자의 데이터 보호 및 침해방지 등 보안활동의 체계적인 수립 및 시행을 점검하는 영역이다.

2.1 물리적 보안체계 점검

2.2 독립적인 전산실 확보/출입통제장치 유무 점검

2.3 보안 침해방지를 위한 활동 점검

2.4 보안 취약점검의 주기적 활동 점검

2.5 서버와 클라이언트간에 전송되는 정보에 대한 완전한 보안을 위해 암호화 제공여부 점검

2.6 보안을 위한 사업자의 주기적인 활동 점검

2.7 논리적 접근통제활동 점검/서버내 서비스 관련 SW점검 정책 유무

다. 네트워크 & 데이터센터 영역 - 서비스제공 기반

<표 2-29> 네트워크 및 데이터센터 영역의 서비스제공 기반 심사항목

심사항목		심사방법	심사내용	근거
3.1	서비스 제공을 위한 전산 설비 공간 점검	관련문서 점검 및 실사 -호스팅 및 IDC사용 계약서 -현장검증	독립적인 전산설비 공간 유무의 점검	IDC시설 안전신뢰성기준
3.2	서비스 제공을 위한 서버 및 네트워크 장비/라인에 대한 점검	관련문서 점검 -서버 및 네트워크 장비목록표 -서버 점검 활동표 -네트워크 장비/라인 점검표	서버 및 네트워크 안정성을 확보하기 위한 활동 점검	IDC시설 안전신뢰성기준
3.3	서비스 제공을 위한 Infra-Structure Software에 대한 점검	관련문서 점검 -Infra-structure S/W 점검표	어플리케이션을 구성하는 제3의 컴포넌트들간의 최적화 점검	IDC시설 안전신뢰성기준
3.4	서비스 제공을 위하여 Infra-Structure 제공업체와의 유지보수/기술지원 계약 여부	관련문서 점검 -제공업체와의 유지보수/기술지원 계약서	Infra-structure 제공업체와의 유지보수/기술지원을 위한 활동 점검	IDC시설 안전신뢰성기준
3.5	서비스 제공을 위한 기술 지원 인력의 확보 여부	관련문서 점검 -직원경력증명서 -직원기술력을 입증할 수 있는 자격증	기술지원 가능한 인력의 확보 점검	-
3.6	기업용 S/W(ERP, SCM, CRM 등)의 서비스 제공을 위한 기술 지원 인력의 확보 여부	관련문서 점검 -컨설턴트지원계획서 (경력증명서)	기업용 SW(ERP, SCM, CRM 등) 구축 및 활용을 위한 컨설턴트 인력확보 점검	-

이 영역은 서비스 제공을 위한 전산설비 및 인프라, 전문인력 등 전반적인 서비스

제공에 대한 기반시설의 확보 및 유지활동을 점검하는 영역이다.

3.1 독립적인 전산실 공간유무의 점검

3.2 서버 및 네트워크 안전성을 확보하기 위한 활동점검

3.3 어플리케이션을 구성하는 제3의 컴포너트들간의 최적화 점검

3.4 Infra-structure 제공업체와의 유지보수/기술지원을 위한 활동 점검

3.5 기술지원 가능한 인력의 확보 점검

3.6 기업용 S/W 구축 및 활용을 위한 컨설턴트 인력확보 점검

라. Ongoing Support 영역 - 서비스제공 지속성

<표 2-30> 지속지원영역의 서비스 제공 지속성 심사항목

심사항목			심사방법	심사내용	근거
4.1	서비스 확장 가능성(Vertical 혹은 Horizontal) 유무		관련문서 점검 -서비스 환경(인프라) 문서 -서비스 확장(투자) 계획서	서비스 확장에 따른 QoS확보 점검 -미래의 요구사항을 산출하기 위한 용량 계획 수립유무 점검	정보시스템감리 기준
4.2	서비스 안정성을 위한 대책 유무	서비스 중단에 따른 복구프로세스 존재 유무	관련문서 점검 -SLA	비정상적인 상황에 대비한 대책 점검	정보시스템감리 기준
4.3		성능유지를 위한 기술적, 관리적 내부프로세스 존재 유무	관련문서 점검 -SLA -관련 SW등 툴의 사용계약서	-성능 향상 소프트웨어 -서비스 수준에 따른 성능 데이터에 대한 자동 분석 -실시간 장비 모니터링 수행 및 전문인력 상주유무 점검	정보시스템감리 기준
4.4	서비스 제공에 대한 백업, 싱크 및 복구 대책 유무		관련문서 점검 및 실사 - 자체IDC이용시 관련 문서점검 -기타의 경우 협력 계약서(협약서) -협력업체의 선정 기준(서비스수준)을 확인할 수 있는 서류	서비스 지속성 확보대책 점검 -자체IDC 이용시 관련문서 점검 - 기타의 경우 협력업체 존재유무	-
4.5	전담 영업 및 지원 인력확보 및 추가 확보 계획 수립 여부		관련문서 점검 및 실사 -인적자원관리 현황표	전담 영업/지원 인력 확보 여부 점검	-
4.6	서비스 중단 등 피해보상에 대한 대책 유무		관련문서 점검 -SLA, 보험가입 계약서	이용자 피해보상에 대한 대책 점검 -보상규정, 보험가입	-

이 영역은 사후 발생가능한 계획적/비계획적 서비스 중단에 따른 백업장치(기술적, 관리적)의 다양한 확보 및 활동에 대한 점검을 통하여 향후 서비스의 지속성을 담보할 수 있는가를 평가하는 영역이다.

4.1 고객수 증가 혹은 데이터의 증가에 따른 수직적/수평적인 관점 모두에서 서비스의 품질유지를 위한 서비스 확장계획을 체계적으로 수립, 시행하고 있는가를 심사

4.2-4.3 예기치 못한 서비스 중단 및 정기적인 서비스 유지관리 활동에 따른 서비스 중단에 대비한 서비스 성능 유지활동의 체계적인 계획수립 및 시행여부를 심사

4.4 사업자의 파산 등에 따른 서비스 중단에 대비하여 서비스 이전 등 지속성을 담보할 수 있는 협력업체의 유무를 심사

4.5 서비스 지속성 확보를 위한 적절한 경력과 능력을 보유한 전담영업 및 지원 인력확보여부 심사 및 향후 추가인력확보계획안 심사

4.6 사후 서비스시 발생할 수 있는 이용자의 피해에 대한 범위 및 보상 등 피해 구제에 대한 대책이 있는가를 심사

마. Ongoing Support 영역 - 고객지원

<표 2-31> 지속지원영역의 고객지원 심사항목

심사항목		심사방법	심사내용	근거
5.1	표준 설치 계획, 서비스 구축 계획, 서비스 시행 계획의 사전 수립 여부 점검	관련문서 점검 -표준설치 계획서 -서비스 구축계획서 -서비스 시행 사전계획서	표준설치/구축/시행 계획의 체계적 시행 및 유지 점검	-
5.2	고객 교육에 대한 준비 상태 및 실시 여부 점검	관련문서 점검 -교육지원 활동표	고객교육에 대한 실시 점검 -교육프로그램	-
5.3	고객 사후 지원 인력 확보 및 사후 관리 조직의 확보 여부 점검	관련문서 점검 -고객사후 지원/관리 계획서	고객 사후 지원 프로세스 점검	-
5.4	서비스 만족을 위한 서비스 만족(SLA 포함 기능)에 대한 점검 기준 및 계약서 명시 점검	관련문서 점검 -서비스수준협약서 (SLA)	고객에 대한 SLA를 통한 품질보증 활동 점검	-

이 영역은 SaaS 서비스의 설치/구축/시행의 체계적인 수행과 고객교육, 품질보증 등 사후관리에 대한 집중적인 점검을 통하여 고객 지원 및 A/S서비스의 지속적 활동을 평가하는 영역이다.

5.1 표준설치/구축/시행 계획의 체계적 시행 및 유지 점검
5.2 고객에 대한 실시 점검/교육 프로그램
5.3 고객 사후지원 프로세스 점검
5.4 고객에 대한 SLA를 통한 품질보증 활동 점검

4. SaaS 인증 평가 방법

본 절에서는 SaaS 어플리케이션과 사업자(서비스 환경) 인증을 위한 평가방법을 간략하게 기술하기로 한다.

먼저, SaaS 인증은 어플리케이션과 사업자 인증 중 하나만 받을 수도 있고, 두 가지 모두를 받을 수 있는데, 이는 SaaS 서비스의 운영형태에 따라 다르다. 두 인증영역의 모든 항목은 필수항목으로 반드시 필요한 요소들로만 구성되어 있어, 세부 항목들은 최저기준인 동시에 공통필수항목이다. 따라서, 어플리케이션 인증 혹은 사업자 인증을 위해서는 모든 필수항목에 대한 일정 점수를 이상을 반드시 받아야만 한다.

항목별 점수산정은 5점 척도법(SD법) 적용하여 최소한 3점 이상의 점수를 받도록 하는 영역별 과락과 총점 과락 모두를 적용한다. 현재 평가방법에는 항목간의 중요도 차이가 있음에도 불구하고 이에 대한 가중치 설정이 되어있지 않은 상황이다. 즉, 모든 평가항목의 가중치는 동일한데, 향후에는 국내 실정에 맞는 항목간 가중치 부여가 필수적이라 하겠다. 그리고 어플리케이션 인증 영역중 가용성 영역의 3.1-3.4항목은 TTA 혹은 클라우드 컴퓨팅 테스트베드사업에서 개발하고 있는 시스템 등을 통한 어플리케이션의 실질적인 검사가 필수적이고, 또한 이 영역은 상대적으로 중요하므로 이 항목들에 대한 가중치를 높이는 것과, 어플리케이션과 사업자 인증의 보안성 영역도 매우 중요하므로 이의 가중치를 높이는 것이 필요하다고 할 수 있다.

제 6 절 클라우드 서비스 SLA

1. SLA의 기본개념

가. SLA 정의

SLA는 클라우드 서비스의 기본 계약서에 첨부되는 서류로 서비스를 제공하는 공급자와 그 서비스를 이용하는 이용자간 합의에 따라 서비스 수준을 결정하고 기록하는 합의서 및 협약서를 말하며 다양한 의미를 내포하고 있어 다음과 같이 설명할 수 있다.

o SLA는 이용자에게 제공하는 클라우드 서비스의 수준을 정량적으로 측정하여, 서비스 성과를 평가하고, 미흡한 부분을 개선하는 **서비스 수준의 성과관리 방식**에 관한 협약서이다.

o SLA는 공급자간 또는 공급자와 이용자간 체결하는 기본계약서와는 별도로 서비스 수준 등 구체적이고 기술적인 사항에 대한 상호간 협약사항을 기술한 부속서(협약서)를 말하며 **법적 구속력**을 갖는다.(<표 1-1> 참조)

<표 2-32> 기본계약서와 SLA의 비교표

구분	클라우드 서비스 기본계약서	클라우드 서비스 SLA
내용	목적	목적
	계약의 체결, 변경 및 해지	계약의 변경, 클라우드 서비스 계약의 해지
	클라우드 서비스 종류	클라우드 서비스 종류 및 내용
	요금	조건(기간, 요금)
	클라우드 서비스 이용 시간	
	시스템 보안	보안
	회사의 의무	고객 지원
	고객의 의무	
	손해 배상	
		위약금
		성능 분석표
		클라우드 서비스 제공 플랫폼 및 구조
		확장성
		데이터 백업 및 복구
		장애
		서비스 향상 및 개선
		서비스 보고 및 처리
		분쟁의 해결
성격	클라우드 서비스 계약관련 당사자 간의 법적, 운영적 측면에서의 기본계약서	클라우드 서비스에 대한 구체적이고 기술적 측면에서의 기본계약서와는 구분되는 별도의 부속서 및 협약서

o 이용자와 공급자 사이의 이해 조정을 위한 법률적 계약인 동시에 대상 서비스와 **책임소재 및 성과측정 기준을 정의**한 기술 협약서이다.

o SLA는 서비스 요구사항과 그 수준, 측정과 평가방법을 포함하며 서비스에 대한 비용 산정의 근거가 되며 분쟁의 발생시 **책임의 소재와 해결의 기초**를 제공한다.

나. SLA의 필요성

클라우드 서비스가 등장하고 비즈니스 모델이 발전・고도화되면서 서비스 수준과 가격의 관계에서 아래에 기술한 문제들이 발생하게 되었고, 이에 따라 서비스의 품질보증(수준)에 관한 공급자와 이용자간의 계약이라는 측면에서 SLA의 중요성이 있다.

o 문제점 : 고객이 클라우드 서비스를 이용할 때, 종래의 IT관련 하드웨어와 소프트웨어를 매매하는 것(즉, 물건을 사고파는 법)과는, 그 가격지불과 기능획득실현의 절차 면에서 아래에 제시한 점들에서 차이를 보인다.

(1) 클라우드 서비스는 물품을 구입할 수도 없고 눈으로 볼 수도 없는 서비스를 이용하는 계약형태이기 때문에 제품의 형태, 감촉 등에 대한 대가를 확인할 수 없는 부분이 많다.

(2) 통상적으로 시장에서 PC・서버・소프트웨어를 구입할 경우 '디자인・사양・성능・기능'과 '가격'의 관계를 타사와 비교해서 구입하는 '시장원리'의 구조가 존재한다. 클라우스 서비스 시장에서는 지불하는 가격과 이용하는 서비스의 관계를 이용자가 비교할 수 있도록, 공급자가 어떤 방식으로든 정보를 제공할 필요가 있으며, SLA는 이를 지원하기 위한 것이다.

또한 SLA는 클라우드 서비스의 기능・성능이나 품질의 정도가 제안되고, 이용자와 공급자간 확인이 가능한 요소로 구성되어야 그 의미가 있다. 즉, 다음과 같은 의미를 내포하고 있다.

예 1) 이 서비스는 SLA에 기술되어 있는 (높은 수준의) 품질·기능을 갖고 있기 때문에 이와 같은 (높은) 가격으로 책정되었다.

예 2) 이 서비스는 SLA에 기술되어 있는 (보급수준의) 품질·기능을 갖고 있기 때문에, (보급수준의) 가격으로 책정되었다.

따라서 SLA가 엄격하면 그 나름의 높은 품질을 얻을 수 있는 반면, 비용이 상승하게 된다. 그러므로 SLA 수준은 비용과 균형을 고려하면서 설정해야 하고 함부로 비용을 높여서도 안되며 역으로 함부로 비용을 낮게 책정하여도 안된다. 서비스 내용에 따라 이용자와 공급자간 합의하에 결정되어야 한다.

SLA 목적은 공급자가 제공할 서비스의 종류 및 수준을 명확히 하고 양사(혹은 공급자와 이용자)간 특히, 서비스를 제공하는 공급자의 책임사항을 분명히 하며 제공될 서비스 중에서 주기적으로 평가될 내용을 정하여 궁극적으로는 양사(혹은 공급자와 이용자)간의 파트너쉽을 증진시켜 클라우드 서비스 수준의 향상에 있다.

다. SLA 구성요소

일반적으로 SLA의 주요내용은 도입부, 서비스시간, 가용성(Availability), 신뢰성(Reliability), 지원력, 성능, 비용부담내용, 서비스보고서 및 검토 등으로 구성된다.

도입부의 내용은 계약의 주체, 서비스수준협약에 대한 제목 및 간략한 설명, 서명인, 포함될 내용의 범위, 양자의 책임 및 역할, 계약에 포함될 서비스에 대한 설명 등이 포함되며, 서비스시간 정의 부분에는 서비스 시간(예: 월-금 09:00-18:00), 특정일(공휴일), 서비스 연장정의 등에 관한 내용이 기술된다.

가용성(Availability)부분은 계약시간 내 가용성 목표치는 일반적으로 Percentage로 표현되며, 이 경우 반드시 측정기간 및 방법이 정의되어야 한다. 가용성은 전체서비스, 외부파트너 서비스, 중요 IT구성요소 또는 3가지 모두에 대해 표현될 수 있지만 서비스품질을 단순한 세 가지 수치로 연관시키는 것은 쉽지가 않다. 따라서 서비스

비가용성(Unavailability)을 측정하는 것이 더 좋은 방법일 수 있다.

신뢰성(Reliability)은 일반적으로 서비스장애 횟수로 표현하거나 Mean Time Between Failure (MTBF), Mean Time Between System Incidents(MTBSI)로 표현한다. 또한 지원력에 대한 부분에서는 지원시간(서비스 시간과는 다름), 특정시간(공휴일), 지원연장에 대한 부분, 응답목표시간 (예, Incident에 대한 전화응답, E-Mail응답 등)의 내용이 포함된다. 성능(Throughput)부분에서는 예상 트래픽 볼륨 및 성능(Throughput)지표 (예: 처리되는 트랜잭션 수, 동시사용자 수, 네트워크를 통해 전송되는 데이터 량), 트랜잭션 응답시간(Transaction Response Time),(예: 평균 또는 최대 응답시간에 대한 목표치), 배치작업 처리성능(배치작업의 성공적인 처리 율)등이 기술된다.

변경에 대한 부분에서는 변경요청(RFC ; Request For Change)를 승인, 처리, 구축할 때의 목표치, 일반적으로 변경유형 또는 변경 우선순위에 정의된다. IT서비스 연속성 및 보안(IT Service Continuity & Security)부분에서는 IT 서비스 연속성 계획에 대한 간략한 정의 및 계획을 실행에 옮기기 위한 방법과 보안항목에 대한 정의가 포함된다.

비용부담(Charging)부분에는 상세한 비용부과 및 기간 등이 기술되며, 서비스 레포트 및 검토에서는 서비스 레포트의 주기 및 분배, 내용, 서비스 검토회의 계획 주기 등이 작성된다. 마지막으로 성능에 따른 인센티브 및 페널티(Performance Incentive / Penalties)에서는 서비스 수준에 대한 성과에 따른 금전적 인센티브 및 페널티에 대한 상세한 내용 등이 기술된다.

1) 클라우드 서비스 SLA 도입부

SLA 도입부에는 SLA 작성의 기본취지, 사용지침 등 전반적인 SLA의 개요와 계약 대상자, 계약 일시, 승인 및 변경 절차에 대해 기술한다.

o 계약 대상자

공급자와 이용자의 상호를 기입하고 서명을 한다.

o 개정 이력표

SLA의 재・개정 여부와 내용, 일시를 기술한다.

2) 클라우드 서비스 SLA 본문

SLA 본문에서는 클라우드 서비스 관리를 위해 도출된 항목에 대한 기본 사항들과 적용범위, 그리고 서비스 항목을 평가하기 위한 기준 및 평가 방법에 대해 기술한다. 크게 4가지 부분으로 나누어 볼 수 있다.

o 목적, 서비스 내용, 조건

SLA 체결의 목적, 서비스에 대한 구체적인 제공 기능, 계약기간, 서비스개시 및 종료, 요금에 대한 내용을 기술

o 성능 메트릭스, 서비스제공 플랫폼 및 구조, 확장성, 데이터 백업 및 복구, 보안

서비스의 성능에 대한 측정기준, 항목 및 서비스가 제공되고 있는 시스템적 환경, 시스템에 대한 기술적 대응책에 대한 내용을 기술

o 고객지원, 장애, 위약금, 서비스 향상 및 개선, 서비스 보고 및 처리

이용자를 위하여 서비스에 대한 개선 노력, 장애시 처리문제, 서비스 수준에 대한 주기적 보고에 대한 내용으로서 전반적인 고객 지원에 대한 내용을 기술

o 계약의 변경, 서비스의 해지, 분쟁의 해결

SLA 계약내용의 변경, 해지, 분쟁해결 방법에 대한 내용을 기술

2. 클라우드 서비스에 대한 SLA 해설

가. 기본취지

o SLA는 공급자간 또는 공급자와 이용자간 체결하는 **기본계약서와는 별도로 서비스수준 등 구체적이고 기술적인 사항에 대한 상호간 협약사항**을 기술한 부속서를 말하며 법적 구속력을 갖는다.

o 본 SLA 가이드라인은 클라우드 서비스 산업의 안전·신뢰성을 확보하기 위한 일환으로 작성한 것이며, 계약당사자간 자율적인 적용을 권장한다.

나. 사용지침

o 제시한 SLA 항목 및 기타 서비스수준에 대한 구체적 항목은 SLA에 포함시켜 사용하고 그 이외의 서비스에 대한 기본적인 계약사항은 기본계약서에 포함시켜 사용할 것을 권장한다.

o 업계의 자율적인 서비스 품질경쟁을 유도하기 위해 주요 핵심사항은 **별첨처리(계약당사자간의 합의수준)** 하기로 한다.

o 서비스 내용, 서비스 Model, 서비스 형태, 사업특성, 업종 등에 따라 필요한 사항에 대해 조항추가, 삭제 또는 보완하여 사용할 것을 권장한다.

3. 클라우드 서비스에 대한 SLA 내용

Service Level Agreement (SLA)

서비스 사업자의 상호

고객사의 상호

Version. 1

개정 이력표

Version No.	개정 내용	개정 일자
1.0	최초 계약서	
	-이하 여백-	

◎ 해설

SLA 도입부의 첫페이지로 상단에는 계약 대상자인 서비스 공급자와 이용자의 상호를 기입하고 서명 또는 날인을 한다. 하단의 개정 이력표에는 SLA의 재·개정 여부와 내용, 일시를 기술한다. 보통 Version 1.0부터 시작을 하며 서비스 기간중 또는 재계약시점에 SLA 항목 수정 및 추가사항을 상호 합의하에 협약을 체결할 경우 그 개정내용과 개정일자를 기술하면 된다. 여기서 Version 1.0은 개발·제공된 SLA를 말한다.

- 목 차 -

(1) 목적

본 SLA(Service Level Agreement)는 클라우드 서비스 제공에 있어서 서비스 제공자 (을)가 고객 (갑) 에게 제공해야 할 서비스의 종류와 내용 및 서비스 수준을 정의하고 상호간의 역할과 서비스 제공 과정에서 발생할 수 있는 문제 해결 과정을 명확히 기술함으로써 고객 (갑)과 클라우드 서비스 제공 사업자 (을) 간의 협력관계를 수립하는데 그 목적이 있다.

◎ 해설
본 항목은 클라우드 서비스 제공 사업자와 이용자간 SLA를 체결하는 궁극적인 목적과 의의에 대하여 기술한다.

(2) 서비스의 내용

① 서비스의 내용 및 범위

본 서비스의 내용은 _____이며 이에 따른 서비스 범위는 _____ 이다. 본 서비스의 내용이 되는 인프라스트럭처와 소프트웨어 목록은 <별첨 1>과 같다.

② 업무내역 및 책임사항 정의

본 서비스에 따라 갑과 을은 상호 협의에 따라 업무 내역을 구분하여 상호 책임하에 수행하며 구체적 업무내역은 <별첨 2>와 같다.

◎ 해설
"서비스의 내용 및 범위"는 클라우드 서비스가 제공하는 주요기능을 기술하고 서비스 제공을 위한 인프라스트럭처(서버, 스토리지, 네트워크 등) 및 소프트웨어 구성에 대하여 이용자가 알기 쉽게 상세히 기술한다.

"업무내역 및 책임사항 정의"는 제공되는 서비스의 원활한 사용을 위해 취해야 할 시스템적 환경 및 기술적 조치사항에 대해 기술한다. 일반적으로 이용자에게 서비스 매뉴얼을 제공하나 본 항목에서는 이것뿐만 아니라 서비스 제공자가 취해야 할 내용까지 포함한다.

(3) 조건

① 계약기간(duration)

본 계약은 계약체결일로부터 효력이 발생하고 ____년 동안 유효하다. 본 계약의 갱신 여부는 계약기간 만료 1개월 전에 재협약하며 별도의 협의가 없는 경우에는 위 기간 동안 자동 연장되는 것으로 한다.

② 서비스 개시일(start date of service)

을은 갑에게 본 계약에 의한 서비스를 ____년 ____월 ___일로부터 제공한다.

③ 요금(Payment terms)

서비스제공에 대한 대금산정 및 대금지급방법에 관하여는 <별첨 3>과 같다.

◎ 해설
본 항목은 클라우드 서비스의 계약기간, 서비스 개시일, 서비스 요금 및 지급 방법에 관하여 상세히 기술한다.

(4) 성능 분석표

을은 제공되는 서비스가 갑의 요구를 충족시킬 수 있도록 다음 항목을 아래와 같이 유지하여야 한다.

(가) 서비스 시간

① 정의 및 계산 공식

사용자가 요구하는 서비스 가용시간으로 운영되는 시스템에 따라, 실제 근무시간만을 서비스 시간으로 설정할 수도 있고, 필요한 경우 교대근무를 통한 24시간 × 365일 가동체계를 마련할 수 있다.

② 목표 수준

서비스 시간은 계약서에 명시한 서비스 시간의 100%(일본은 99%)를 보

장한다.

(단, 계획된 유지보수, 천재지변 등은 예외로 한다.)

(※ 근거 1: IaaS 서비스중 랙스베이스(rackspace)의 클라우드 서버(Cloud Servers)와 클라우스 파일(Cloud Files) 서비스의 SLA 항목

근거 2: 일본 공공부분 ASP SLA: 99%)

③ 측정방법 및 측정도구

④ 보고 주기

년/월/주/일 단위로 주기를 정하여 보고할 수 있다

◎ 해설

"서비스 시간"은 클라우드 서비스 성능의 지속성 유지라는 측면에서 중요한 항목이며 서비스 내용에 따라 조정될 수 있으며 계약당사자간 합의에 따라 정할 수 있다.

"측정방법 및 측정도구"는 갑과 을이 측정을 실시하기에 앞서 측정도구, 측정시기 및 빈도, 측정 및 기록/ 보관 방법 등을 포함한 일체의 성능측정 프로세스와 지표 등을 사전에 협의하여 정의할 수 있으며 초기치 측정결과 정의된 기대 서비스 수준과 최소 서비스 수준의 초기치가 적절하지 않을 경우 쌍방은 공동으로 해당 서비스 수준의 초기치를 협의 조정할 수 있다.

※ 측정 절차

- 1단계는 해당 서비스 수준에 대한 측정 척도를 수합하며, 이때 측정된 자료의 가중치 및 불산입 사항/ 예외사항 등에 대한 고려사항을 반영하여 처리한다.
- 2단계는 해당 서비스 수준 산식의 분모에 해당하는 발생 총건수를 계산하며, 불산입 사항 및 예외사항 등에 대한 고려사항을 반영하여 처리한다.

(나) 가용성(Availability)

① 정의 및 계산 공식

정해진 운영시간 중에 서버에 접속 가능한 시간에 대한 백분율을 의미하며

다음과 같은 공식에 의하여 계산한다.

가용성 = (총 가동시간/예정가동시간) X 100

② 목표 수준

가용성은 99 %이상을 보장한다.

(※ 근거: 일본의 ASP/SaaS SLA)

③ 측정방법 및 측정도구

④ 보고 주기

년/월/주/일 단위로 주기를 정하여 보고할 수 있다

◎ 해설

"가용성"은 정해진 기간내에 제공받는 서비스를 네트워크를 경유하여 서버에 접속 가능한 시간을 측정하여 정하는 항목으로써 실제로 총 가동된 시간을 예정된(약속된) 가동시간으로 나누어 백분율로 나타낸 수치이다. 가용성은 <표 4-1>과 같은 형태로 기술하여 제공할 수 있다.

측정항목	가용성(Availability)
정의(or 목적)	정해진 운영시간 중에 서버에 접속 가능한 시간에 대한 백분율을 의미하며 다음과 같은 공식에 의하여 계산한다.
측정기준	가용성 = (총가동시간/예정가동시간) X 100
서비스 목표	o 기대수준 : XX% o 최소수준 : XX%
측정도구	XXX관리시스템
책임자	클라우드 서비스 제공업체의 시스템관리자
측정기간	매월/매주/매일/매시
보고 빈도	매월/매주/매일
측정대상	
기 타	

"측정방법 및 측정도구"는 상기한 서비스시간 항목과 동일하게 처리함

(가) 응답시간(response time)

① 정 의

시스템에 서비스를 조회를 요구한 직후부터 응답이 시작되는 때까지 경과된 총시간을 의미하며 다음과 같은 공식에 의하여 계산한다.

응답시간 = XXX초

② 목표 수준

을은 클라우드 서비스를 제공하기 위하여 갑이 서비스에 접속한 후 접속응답시간(response time)을 5 초 이내로 유지하여야 한다.

혹은

을은 클라우드 서비스를 제공하기 위하여 갑이 특정 트랜잭션(transaction) 실행 후 응답시간(response time)을 5 초이내로 유지하여야 한다.

(※ 근거: 학술논문중 컴퓨터 사용자가 트랜잭션후 기다릴 수 있는 심리적 응답시간이 5초라는 학술연구 결과.)

③ 측정방법 및 측정도구

④ 보고 주기

년/월/주/일 단위로 주기를 정하여 보고할 수 있다

⑤ 단서 조항

◎ 해설

“응답시간”은 일반적인 유·무선 인터넷 환경에서의 웹접속 혹은 앱접속에 대한 응답시간을 고려하여 특정 서비스의 접속응답시간(response time)이나 특정 트랜잭션(transaction) 실행 후 응답시간(response time)은 5 초 이내로 한다. 단, 클라우드 서비스 중 어플리케이션이나 플랫폼 등의 문제가 아닌 인프라스트럭처의 네트워크 장애 등으로 인한 응답시간의 지연에 대한 예외조항은 갑과 을이 사전에 협의하여 명시할 수 있으며, 특정 서비스의 응답시간이 5 초 이상이 걸리는 사항도 갑과 을이 사전에 협의하여 명시할 수 있다. 예를 들면, 이용자의 PC 및 모바일 디바이스 등의 단말기 사양, 네트워크 환경, 트래픽 등에 의해서 영향을 많이 받으므로 이를 SLA 작성시 단서 조항으로 삽입하여 명시할 수 있다.

측정항목	응답시간(response time)
정의(or 목적)	서비스를 시스템에 요구한 직후부터 응답이 시작되는 때까지 경과된 총시간을 의미하며 다음과 같은 공식에 의하여 계산한다.
측정기준	XXX초
서비스 목표	o 기대수준 : XX초 o 최소수준 : XX초
측정도구	XXX관리시스템
책임자	클라우드 서비스 제공업체의 시스템관리자
측정기간	매월/매주/매일/매시
보고 빈도	매월/매주/매일
측정대상	
기 타	

“측정방법 및 측정도구”는 상기한 서비스시간 항목과 동일하게 처리함

(5) 서비스제공 시스템 및 구조

을이 제공하는 클라우드 서비스에 사용되는 시스템 및 구조는 <별첨 4>(시스템 구성도)와 같다.

◎ 해설
본 항목은 클라우드 서비스가 제공되기 위해 필요한 시스템의 구성을 기술하는 항목으로서 이용자에게 알기 쉽고 상세하게 기술한다. 일반적으로 하드웨어, 네트워크 등의
인프라스트럭처 및 플랫폼 등을 포함하여 서비스를 제공하기 위한 시스템 구성도를 별첨하여 제공한다.

(6) 확장성

사용자가 증가하거나 기능의 확장이 필요한 경우 갑은 을에게 혹은 을은 갑에게 이 사실을 통지하여 추가적인 확장과 변경의 내용을 협의함으로써 본 계약에 의한 서비스 수준이 유지될 수 있도록 클라우드 서비스의 구조를 갖추어야 하며 확장과 변경에 따라 추가적으로 발생하는 소요 비용은 갑이 부담하도록 한다.

◎ 해설
본 항목은 클라우드 서비스의 안정성 및 지속성을 보장하기 위한 항목으로서 사용자 증가나 기능이 추가되어 확장된 경우 서비스가 유지될 수 있도록 서비스제공 사업자가 시스템 구조는 물론 이에 따른 변경계획 및 소요비용을 예측·대비하고 있어야 하며 서비스 구조 변경시 이용자에게 즉시 이에 대한 프로세스를 상세히 알려주어야 한다.

(7) 데이터 백업 및 복구

을은 갑의 데이터에 대한 신뢰성, 비밀성, 가용성이 보장 되도록 데이터를 보관하여야 하고, 보관 데이터가 손상될 경우에 대비하여 데이터의 백업(back up) 및 복구 체계를 갖추어야 한다. 백업주기, 백업준수율, 복구시간 등은 <별첨 5> (데이터 백업 및 복구 지침)와 같다.

◎ 해설
본 항목은 클라우드 서비스 이용과 더불어 생성되는 자료의 주기적인 백업절차 및 방법에 대하여 기술하는 항목으로서 백업주기, 백업준수율, 복구시간을 상호 협의에 따라 정하여 상세히 기술한다. 특히, 백업준수율이란 백업계획건수 대비 실시건수를 백분율로 정하는 것으로서 일반적으로 99 %이상으로 유지하여야 한다.
(※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 99%에 동의함)

(8) 보안

을은 사용승인을 받지 아니한 자로부터의 접근을 제어하기 위한 인증절차를 수행하고, 보안상의 취약점을 제거하기 위하여 클라우드 서비스를 제공하기 위한 어플리케이션, 플랫폼 혹은 인프라스트럭처에 대한 취약성 분석 및 제거 절차(분석 주기 포함)를 <별첨 6>(보안 절차 및 지침-보안준수율 포함)과 같이 구비하여야 하고, 갑이 그에 대한 보고를 요구할 경우 이를 제시하여야 한다.

◎ 해설
본 항목은 일반적인 정보시스템 보안정책 및 절차와 동일하므로 일반적으로 전산실에서 수행하는 보안 유지활동을 기술하면 된다. 시스템을 아웃소싱할 경우 호스팅업체 및 IDC의 보안 유지활동 내역을 기술하거나 관련서류를 첨부한다. 클라우드 서비스 제공업체중 서비스의 제공형태가 어플리케이션, 플랫폼 혹은 인프라스트럭처 서비스중 일부만 제공하는 경우에는 이에 대한 보안절차와 지침만을 기술하면 된다.

(9) 고객지원

① 갑은 서비스에 문제가 발생하였을 경우 전화(번호) 및 이메일(주소) 또는 FAX등으로 을의 고객지원 담당에게 연락할 수 있다.

② 을은 <별첨 7>과 같이 고객지원지침을 작성하고, 갑으로부터의 지원요청이 있을 경우 작성된 지침에 따라 조치를 취하여야 하며 필요한 조치를 취하지

못하였을 경우에는 고객지원책임자에게 즉시 보고하여 해결방법을 모색한다.

◎ 해설
본 항목은 갑인 고객을 위하여 고객지원지침을 구비하여 체계적으로 지원서비스 활동을 유지하도록 하는데 그 목적이 있으며 이용자에 대한 교육, 업무문의 대응, 시스템 고장시 대응방법을 상세히 기술한다. 시스템 오류시 복구시간을 정할 수도 있고 신뢰성 지수(MTTR; 평균수리시간, MTBF; 평균고장간격)를 활용하여 정할 수 있다. 또한 사용자의 서비스 지원 요청에 따른 콜처리율을 도입하여 수치화하고 기술할 수 있다.

(10) 장애

서비스 시간동안에는 서비스를 받을 수 없는 장애가 발생하게 되는데, 장애등급에 따라 가중치를 부여하여 장애건수를 계산할 수 있으며, 장애등급이 낮은 사소한 장애에 대해서는 그 건수를 제외시킬 수 있다. 장애등급은 크게 아래와 같이 예정된 장애와 불시의 장애로 나눌 수 있는데 이에 따른 가이드라인은 다음과 같다. 그리고 시스템 장애와 관련하여 <별첨 8>의 서비스 장애 발생건수 혹은 동일 장애 발생률과 같은 서비스항목을 이용하여 측정할 수 있다.

① 예정된 장애(planned outage)

㉮ 정의

예정된 장애란 클라우드 서비스의 유지 또는 관리를 위한 목적으로 야기된 사용상의 장애를 의미한다.

㉯ 시간

을은 예정된 장애의 경우 원칙적으로 업무시간(09:00부터 18:00까지의 시간)에 발생치 아니하게 한다.

㉰ 예고

을은 예정된 장애의 경우 장애예정일로부터 (____)일 전까지는 갑에게 장애 시기, 내용, 대처방법 등을 예고하여야 한다.

㉱ 제한

예정된 장애의 경우 원칙적으로 매월 (OO회, 총 OO분)을 초과하여서는 아니 된다.

② 불시의 장애(unplanned outage)

㉮ 정의

불시의 장애란 예정된 장애 이외의 일체의 장애를 의미한다.

㉯ 보고

을은 클라우드 서비스에 불시의 장애가 발생하였을 경우 즉시 갑에게 장애의 내용, 효과 및 대처방법 등을 보고한다.

㉰ 복구시간

불시의 장애의 경우 원칙적으로 그 복구는 장애의 정도에 따라 <별첨 8>(장애처리 지침)의 시간 내에 이루어져야 한다.

㉱ 단서조항

불시의 장애의 경우 여러 가지 원인(또는 원인을 규명하기 어려운 원인)에 의해 발생할 수 있으므로 이러한 여러 가지 원인들과 책임소재 들에 대하여 SLA 작성시 불시의 장애에 대한 단서 조항으로 삽입하여 명시할 수 있다.

◎ 해설

본 항목은 갑인 고객이 클라우드 서비스이용중 발생하는 장애에 대하여 장애의 정의 및 대처를 기술함으로서 서비스 성능의 최적화를 위한 을의 대책에 대해 주로 기술한다. 측정기준으로는 장애 발생 건수, 동일 장애 발생률을 주로 도입하여 적용하고 있다. 특히 동일 장애 발생률은 총장애 발생건수 대비 동일장애 발생건수를 백분율로 수지화한 것으로 일반적으로 5%이하로 유지하여야 한다.

(11) 위약금 및 인센티브

① 위약금

을의 귀책사유에 의하여 클라우드 서비스가 제대로 작동하지 아니한 경우 을은 그 정도에 따라 갑에게 <별첨 9>(위약금 및 인센티브)와 같이 위약금을 지급한다.

② 인센티브

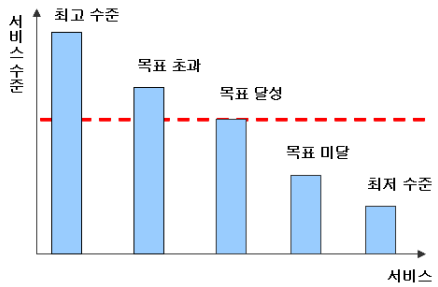
을은 계약에 따라서 계약 이상의 (혹은 계약에 따라) 서비스 성능을 갑에게 제공하였을 경우에는 갑은 그 정도에 따라 을에게 <별첨 9>(위약금 및 인센티브)와 같이 인센티브를 지급한다.

◎ 해설

본 항목은 SLA에서 정한 서비스 수준이 불이행되거나 제대로 제공되지 않을 경우 위약금에 대한 내용을 기술한다. 또한 서비스 수준이 계약 이상의 성능을 이용자에게 제공한 경우 인센티브 지급에 대한 내용을 상호 협의하여 정할 수 있다. 각각 서비스의 상대적 중요도를 반영하여 인센티브를 결정한다. 각각의 개별적인 서비스 수준을 달성된 결과를 토대로 목표 초과, 목표 달성, 목표 미달, 최저 수준으로 등급을 결정, 등급별 위약금 및 인센티브 기준을 마련한다.

<표 4-> 서비스 수준별 비중 및 등급 - 활용 예

서비스 영역	서비스 수준	비중(%)
데이터 센터	장애건수	15
	메인프레임 가동율	10
	DB 가동율	10
	Storage 가동율	10
	Back-Up 준수율	10
	변경조치율	10
	시간내 장애조치율	15
	소계	80%
Desk Top	변경조치율	8
	시간내 장애조치율	12
합계		100%



(12) 서비스 향상 및 개선

을은 서비스를 향상 및 개선할 수 있고, 이 경우 서비스의 변경내용을 통지하여야 하고 필요한 경우에는 교육을 실시할 수 있다.

◎ 해설
본 항목은 서비스제공사업자가 서비스 향상을 위한 개선활동을 할 경우 변경 내용을 갑인 이용자에게 통지하고 교육하도록 하기 위한 내용으로서 을의 서비스 향상을 위한 의무사항을 기술한다. 본 항목은 특히 클라우드 서비스중 어플리케이션 서비스의 SLA 작성시 유의하여 작성하도록 하며 플랫폼이나 인프라스트럭처 서비스에도 적용될 수 있다.

(13) 서비스 보고 및 처리

을은 <별첨 10>(서비스수준보고서)의 양식에 따라 주기적으로 갑에게 서비스 수준의 결과를 보고한다. 보고에 대하여 갑의 담당자는 을의 담당자에게 ____일 이내에 보고서의 접수를 서면으로 확인하여야 하며 갑이 을로부터 서비스수준보고서를 받은 후 ____이내에 갑의 서면확인이 없을 경우 서비스 수준 보고서를 접수한 것으로 본다.

◎ 해설
본 항목은 서비스제공사업자가 SLA에서 정한 기준에 따라 서비스 수준 유지 활동을 지속적으로 수행하고 있는 것을 갑인 이용자에게 주기적으로 보고함으로서 서비스에 대한 신뢰성, 안정성을 확보하도록 하는 내용으로서 <별첨 10>의 양식에 따라 간단하고 명료하게 작성하여 보고하여야 한다.

(14) 계약의 변경

본 계약서는 갑 또는 을의 요청에 의하여 상호 협의에 따라 변경할 수 있다.

(15) 서비스계약의 해지

갑(을)이 본 계약상의 의무를 중대하게 위반 또는 반복적으로 불이행하는 경우 을(갑)은 의무 불이행을 상대방에게 서면으로 통지하고, 서면 통지가 상대방에게 도달한 때부터 ____이내 불이행이 시정되지 않는 경우 본 계약을 해지할 수 있다.

(16) 분쟁의 해결

본 계약으로 인하여 또는 본 계약과 관련하여 발생하는 모든 분쟁은 상호 합의하에 따라 원만히 해결하기로 하며, 분쟁이 발생한 날로부터 ____일 이내에 상호 합의에 따라 해결되지 못할 경우 법적인 절차에 따라 분쟁을 해결하도록 한다.

◎ 해설
"계약의 변경, 해지, 분쟁의 해결" 항목은 일반적인 계약서 및 협약서에 포함되는 내용으로서 본 SLA에서도 준용한다.

※ 별첨자료

① 인프라스트럭처 및 소프트웨어 목록

▶ 인프라스트럭처 및 소프트웨어 목록은 스토리지, 서버, 네트워크 및 기타하드웨어와 소프트웨어(OS, DBMS, WEB/APP Server 등)로 구분하여 표시하고 각각의 사양을 명시한다.

② 각 당사자의 업무내역

▶ 이 별첨항목에는 을이 제공되는 클라우드 서비스와 관련하여 제공된 업무의 구체적인 범위 및 내용, 제공되는 서비스의 원활한 사용을 위한 제공화면의 구체적인 내용, 시스템의 동작요건 등을 기술하여 작성할 수 있다.

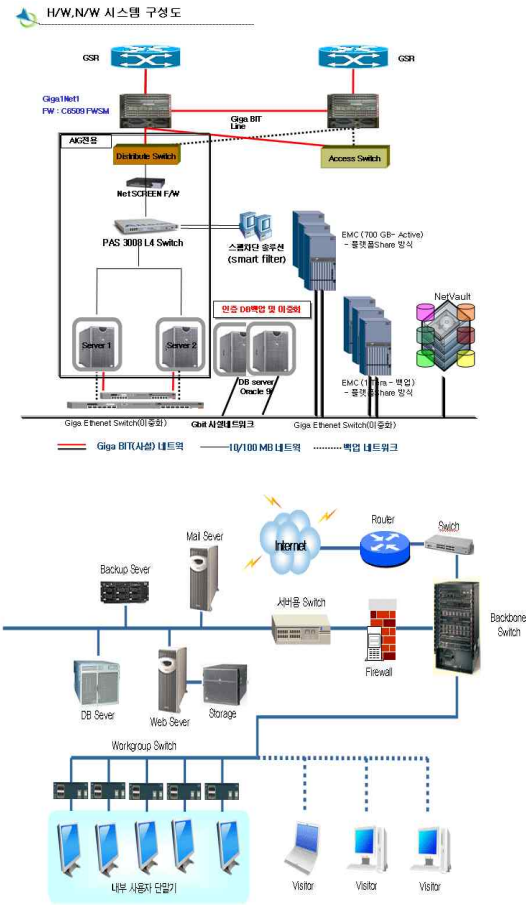
③ 대금산정 및 지급 방법

▶ 대금산정은 각 서비스에 소요되는 유지보수 및 초기개발비 등을 포함하여 산정 및 표시하도록 하며 지급방법은 주/월/년 혹은 사용시간별 표시를 하여 작성할 수 있다

④ 시스템 구성도

▶ 이 항목에는 하드웨어(스토리지, 서버 등) 및 네트워크를 포함한 인프라스트럭처를 위주로 알기 쉽고 명료하게 작성된다.

<예 - 시스템 구성도>



⑤ 데이터 백업 및 복구 지침

▶ 이 별첨항목에는 서비스 측정항목인 백업준수율이 포함하여 작성될 수 있는데, 이는 정기적으로 수행하는 백업과 수시로 수행하는 백업의 총 계획 건수 중 정상으로 실시된 백업의 비율을 의미한다.

- $\text{백업준수율}(\%) = \frac{\text{백업실시건수}}{\text{백업계획건수}} \times 100$

- 목표 수준

  을은 백업준수율을 __99__ %이상으로 유지하여야 한다.

  (※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 99%에 동의함)

⑥ 보안 절차 및 지침

▶ 이 별첨항목에는 보안 정책에 따라 정보시스템을 통한 보안 유지활동을 잘하고 있는지에 대한 품질지표인 보안 절차율을 포함할 수 있다. 보안 유지활동의 실패는 다른 업무 수행에 큰 영향을 끼칠 수 있기 때문에 관리되는 항목이다.

⑦ 고객지원지침

고객지원항목에는 다음의 항목들이 포함되어 작성되길 권고한다.

▶ 시스템 운용 조작 지도 등 사용자에 대한 교육 방법, 업무문의 방법, 그리고 회사의 특성을 고려한 컨설팅에 방법

▶ 시스템 고장이 발생 시 고장대응방법 - 이 항목은 <별첨 8>의 장애처리지침 항목을 상호 고려하여 작성한다.

예1) 명백한 시스템 오류시 ____시간 이내에 시스템을 복구한다.

예2) 시스템 고장시 유지보수를 신뢰성 지수(MTTR or MTBF)를 도입하여 SLA 안을 작성할 수 있다.

o MTTR(Mean Time to Repair : 평균 수리 시간)

- 정의 : 기기 또는 시스템의 장해가 발생한 시점부터 장해가 발생한 곳의 수리가 끝나 가동이 가능하게 된 시점까지의 평균 시간. 즉, 기기

또는 시스템이 장해에 의해 가동하지 못한 상태가 계속된 평균 시간

- 수식

· $MTTR = \frac{D_1 + D_2 + \ldots\ldots + D_n}{n}$ (Di : 고장중의 시간) n : 고장횟수

o MTBF(Mean Time Between Failure: 평균 고장 간격)

▶ 이 별첨항목에는 다음과 같은 평가지수를 포함하여 작성할 수 있다.

o 서비스 요청 적기 처리율

사용자가 시스템 운영조직에 요청한 서비스 중, 요청한 완료일 이내에 서비스를 제공해 준 비율을 의미한다.

-

$$\text{서비스요청 적기처리율}(\%) = \frac{\text{완료예정일자이내에 완료한 서비스 요청건수}}{\text{측정기간에 완료예정인서비스요청건수}} \times 100$$

- 목표 수준

을은 서비스요청 적기처리율을 99 %이상으로 유지하여야 한다.

(※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 99%에 동의함)

o 1차 Call 처리율

서비스데스크 상담원이 사용자의 서비스 요청을 접수한 즉시 전화를 끊지 않은 상태에서 사용자의 문의사항에 응답 및 해결한 비율을 의미한다.

$$\text{- 1차 } Call\text{처리율} = \frac{\sum \text{1차 } Call \text{ 처리건수}}{\sum Call \text{ 접수건수}} \times 100$$

- 목표 수준

을은 1차 Call 처리율을 95 %이상(5%미만)으로 유지하여야 한다.

(※ 근거: 일본 공공부문 ASP SLA는 5%미만

국내 ASP 사업자들이 1차 콜 처리율은 95%에 동의함)

o 2차 Call 처리율

'1차 처리'되지 못한 사용자 서비스 요청 중, 서비스데스크 상담원이 직접 필요한 조치를 수행하여 문제를 해결한 처리건수의 비율을 의미한다.

$$\text{- 2차 } Call\text{처리율} = \frac{\sum 2\text{차 } Call \text{ 처리건수}}{\sum 1\text{차에서 처리하지 못한 } Call\text{건수}} \times 100$$

- 목표 수준

을은 2차 Call 처리율을 99 %이상으로 유지하여야 한다.

(※ 근거: 일본 공공부문 ASP SLA는 5%미만
국내 ASP 사업자들이 2차 콜 처리율은 99%에 동의함)

o 변경요청 적기 처리율

사용자가 시스템 변경을 요청 하였을 때 납기 시간 이내에 처리되는 비율을 의미한다.

$$\text{- 변경요청 적기처리율}(\%) = \frac{\text{납기내 처리건수}}{\text{변경접수건수}} \times 100$$

- 목표 수준

을은 변경요청 적기 처리율을 95 %이상으로 유지하여야 한다.

(※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 95%에 동의함)

o 변경 적용 시 오류 건수

사용자의 서비스 요청에 대해 시스템 변경작업이 수행되었을 때, 오류가 발생한 건수를 의미한다.

- 목표 수준

을은 변경 적용시 오류 건수율을 5 %이하로 유지하여야 한다.

(※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 5%에 동의함)

⑧ 장애처리지침

▶ 이 별첨자료에는 장애의 급수에 따른 시스템 장애 조치시간을 포함하여 작성될 수 있는데, 시스템 장애조치시간은 시스템 장애 발생시, 조치를 시작하여 서비스가 제대로 사용되기까지 걸린 시간의 총합을 의미한다. 백업복구 및 하드웨어 교체 등으로 소요된 유지보수 절대시간은 합산에서 보통 제외하며, 등급에 따라 각각 조치시간 목표치를 설정할 수 있다.

예) 1급 장애 : 2시간 이내 / 2급 장애 : 6시간 이내

그리고 시스템 장애와 관련된 서비스 측정항목은 다음과 같은 서비스항목을 이용하여 측정할 수 있다.

o 서비스 장애 발생건수

서비스 시간동안 발생한 총 장애건수를 의미한다. 장애 등급에 따라 가중치를 부여하여 총 장애건수 계산할 수 있으며, 장애등급이 낮은 사소한 장애에 대해서는 그 건수를 제외시킬 수 있다.

o 동일 장애 발생률

이미 발생했던 장애와 동일한 장애가 재발한 비율을 의미한다. 이는 장애 발생 후 조치에 대한 측정기준으로써 사용된다. 동일 장애 발생률은 5% 이하로 유지하여야 한다.

- $\text{동일장애발생률}(\%) = \frac{\text{동일장애발생건수}}{\text{총장애발생건수}} \times 100$

(※ 근거: 국내·외 근거는 없으나, 국내 ASP 사업자들이 99%에 동의함)

⑨ 위약금 및 인센티브

▶ 위약금은 유사 서비스모델(예: IDC서비스)의 사례를 참조하여 작성할 수 있다.

예) 고객이 청구 받은 최근 3개월분(3개월 미만인 경우에는 해당 기간 적용) 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간수를 곱하여 산출한

금액의 3배의 금액을 기준으로 하여 이용고객과 협의하여 결정할 수 있다.

▶ 인센티브

예) 응답시간(response time)

갑과 을은 서비스 성능 매트릭스 중 응답시간(response time)에 대하여 아래 표의 중 레벨(moderate level)의 서비스를 제공하고 제공받기로 계약하였다. 또한 을이 갑에게 중(moderate level) 이상인 상 레벨(achieved level) 및 최상레벨(excellent level)의 서비스를 제공하는 경우에는 그 정도에 따라 갑은 을에게 인센티브를 제공한다. 만약 하 레벨(poor level)의 서비스를 제공하는 경우에는 을은 갑에게 위약금을 지급한다.

< 인센티브 제공을 위한 서비스 제공의 예 - 성능 매트릭스: 응답시간 >

응답시간	Poor	Moderate	Achieved	Excellent
응답시간(초)	<D	D~C	C~B	B~A
위약금 및 인센티브	위약금		인센티브 Ⅰ	인센티브 Ⅱ

⑩ 서비스수준보고서

▶ 서비스수준보고서는 주기적으로 아래 예를 참조하여 간단하고 명료하게 작성 보고할 수 있다.

< 예 - OO년 OO월/주/분기 서비스수준 성과보고서 >

평가항목		가중치	목표	측정결과	평가점수
구분	항목				
성능메트릭스	서비스시간				
	가용성		%	%	
	응답시간		초	초	
장애처리절차 준수율			%	%	
고객지원	서비스요청 적기처리율		%	%	
	변경요청 적기처리율		%	%	

⑪ 서비스 수준 측정 요약표

▶ 서비스 수준 측정 요약표는 주기적으로 아래 예를 참조하여 간단하고 명료하게 작성하여 서비스수준보고서와 함께 보고할 수 있다.

< 예 - 서비스수준측정 요약표 >

항 목	계산 기준	예 시	비 고
1. 가용성	총가동시간 / 예정가동시간 X 100	o 정의 : 각 온라인의 정상 가동 상태 o 측정 : 총 가동시간은 예정 가동시간에서 서비스 중단시간을 차감 o 수준 : IMS Region의 경우 xx%이상 o 보고 : 월단위 통계	성능 메트릭스
2. 응답시간	시스템 응답시간(초)	o 정의 : 트랜젝션별 유형분류 o 측정 : 시스템내에서 처리하는데 소요된시간 o 보고 : 월단위 통계	성능 메트릭스
3. 문제해결 시간	총가동시간 / 예정가동시간 X 100	o 정의 : 접수된 H/W, S/W 등 제공받는 서비스의 문제건수 일정기간내 해결건수의 비율 o 수준 : xx% o 측정 : Help Desk상의 일자로 측정 o 보고 : 월단위 통계	고객지원
4. 예고시간 준수율	예고시간준수 / 100 X 총시스템 변경건수	o 정의 : 일반적인 변경사항 OO일전에 공고 o 수준 : xx% o 측정 : 공고일자와 변경 실시일자 o 보고 : 월단위 통계	고객지원
4. 장애복구 처리시간	장애복구 처리 소요시간(시간)	o 정의 : 장애 복구에서 복구완료까지의 소요시간 o 수준 : x시간 o 측정 : 장애 처리시스템 이용 측정 o 보고 : 월단위 통계	장애처리

제 3 장 결 론

본 연구의 결과물인 클라우드 서비스 인증을 위한 심사기준, SLA 가이드라인 제시를 통해 클라우드 서비스 이용활성화를 도모하고, 국내 클라우드 산업 육성 및 글로벌 경쟁력 강화를 위한 밑거름이 될 것으로 예상된다. 특히, 국내 클라우드 서비스를 준비하고 있는 기업체들에 있어서 일정한 가이드라인을 제시함으로서 클라우드 서비스 제공자의 서비스 품질을 제고하고 심사기준을 클라우드 서비스 인증체계 구축에 있어서 적용함으로 이용자 신뢰기반 확립과 더불어 서비스 제공자의 홍보등에 이용하여 클라우드 서비스 산업 활성화를 촉진할 계기가 될 것으로 예상된다.

본 연구에서 다루지 못한 해설서는 인증체계 구축 후 인증심사를 진행하여 나타날 수 있는 문제점 등을 향후 2년간 수집하여 심사기준 및 SLA 가이드라인 갱신이 우선되어진 후 최종적인 심사기준을 토대로 해설서를 작성하는 것이 바람직하리라 사료된다. 또한, 클라우드 서비스 대국민 인식제고를 위해 현재 클라우드 컴퓨팅 포럼에 상정된 클라우드 서비스 심사기준 표준과제 개발 및 학술지 등의 논문 개제 등 추가적인 후속조치가 병행 되어야 할 것이다.

마지막으로, 클라우드 서비스는 클라우드 컴퓨팅 기술 발전과 서비스 모델의 다양화로 매우 빠르게 진화할 것으로 예상되며, 이에, 본 과제에서 연구된 심사기준 및 SLA 가이드라인 등이 이러한 진화에 따라 능동적이고 탄력적으로 운용이 가능하도록 연구 고도화가 필요할 것으로 예상된다. 또한, 이용자 신뢰기반의 확대를 위해 인증체계를 구축하고 클라우드 서비스 인증제도를 운영하여 클라우드 서비스 이용 활성화와 극대화를 유도하고, 법제 정비 등을 통해 클라우드 서비스 이용 기업의 지원책 발굴 등의 노력이 뒷받침 되어야 할 것이다.

참 고 문 헌

[1] 한국인터넷진흥원, 클라우드 서비스의 해외사례 비교분석, 2009.

[2] 윤병남, 김현곤, 손진락, 정보시스템 아웃소싱 방법론, 한국전산원, 1999.

[3] 김승윤, 김세한,김진화, 남기찬 "아웃소싱의 서비스 수준협약서에 관한 사례연구 “, 정보경영학연구, 제14권 제3호, pp. 23-54, 2004.

[4] 정보통신부, ASP 서비스에 대한 서비스수준 협약서 작성 가이드라인, 2006.

[5] 정보통신부 국무조정실, SLA를 강화한 정보시스템 운영계약 참조모델, 2005.

[6] TTA Standard: 클라우드 컴퓨팅 SLA수립을 위한 품질요소, 2010.

[7] ASPIC, 일본 ASP・SaaS 백서, 2010.

[8] 일본 ASPIC, 2009-2010 일본 ASP/SaaS 백서: SLA 작성을 위한 가이드라인, 2010.

[9] ASPIC America, ASPIC Guide to the ASP Delivery Model(Q3 2000 Version), Appendix B : Service Level Agreement, Appendix C : Network SLA Checklist and Appendix D : Application SLA Checklist, 2000.

[10] Andrew Hiles, The Complete Guide to IT Device Level Agreement (3rd Edition), 2002.

[11]Management Advisory Services Consulting Staff, Service Level Agreements for Application Service Provisioning, 2000.