클라우드 서비스 브로커를 이용한 클라우드 서비스 감사
Cloud Service Auditing using Cloud Service Broker Technology

김경훈, 박홍준, 유경택(강동대학교)

차 례

■ keyword : | Cloud Service | Service Level Agreements | Auditing |

1. 서론

최근 IDC에서는 전 세계의 클라우드 서비스에 대한 지출 규모가 2013년에만 474억 달러에 달하였고, 다가오는 2017년에는 1,080억에 이를 것으로 예상하였다. 이는 퍼블릭 IT 클라우드 서비스가 2017년까지 연평균 23.5%씩 성장할 것으로 예상한 것이며, 전체 IT 산업 성장률의 5배 큰 수치이다[1]. 클라우드 상에서 수행되는 서비스의 성능을 높이고자 하는 연구가 진행되고 있다. 이와 같은 클라우드 서비스는 서비스의 동적확장성, 사용자 기반의 요금체계를 통한 비용절감, 가상화 기술을 기반으로 한 조직 리소스의 효율적인 활용 등의 많은 장점을 가지고 있다.

클라우드 서비스는 위와 같은 장점을 가지고 있는 반면에, 다음과 같은 단점으로 인해 개인과 기업 사용자가 도입하기를 꺼려하고 있다. 첫 번째 이유는 보안과 프라이버시 문제이다. 클라우드 컴퓨팅은 인터넷이 연결된 환경에서 서비스를 제공하고 있어 해킹과 같은 위험에 노출되어 있어 보안이 취약할 수 밖에 없다. 두 번째는 가용성과 업무의 연속성에 있어 발생 가능한 문제에 대한 것이다. 클라우드 서비스는 인터넷이 가능한 환경에서만 사용이 가능하며 서비스 제공자나 사용자 측면에서 인터넷 연결이 어려운 경우 원활한 서비스를 제공하거나 제공받을 수 없다는 단점을 가지고 있다. 뿐만 아니라 비슷한 서비스에 대해서 서비스 제공자나 자원 공급자가 서로 다를 수 있어 이에 대한 관리도 필요하다.

최근 앞에서 언급된 문제를 해결하고 신뢰성(reliability) 확보를 위하여 서비스에 대한 감사(service audit)를 수행하는 방법이 연구되고 있다. 그리하여 본 논문에서는 서비스 수준 협약 수립(service level agreement)과 함께 신뢰성 확보를 목표로 하는 클라우드 서비스 감사를 위한 기술 동향에 대해 분석하고 감사를 위한 활동에 있어 필요한 기준을 정의하고자 한다.

2. 클라우드 보안 위협 및 요구사항

클라우드 보안 위협은 기존 컴퓨팅 환경의 보안 위협과 크게 다르지 않으며, 클라우드 서비스를 제공하는 데 있어 중요한 사항이다. CSA(Cloud Security Alliance)에서는 보안 위협[2]을 표1과 같이 7가지로 나누어 분석하였으며, 각각의 보안 위협에 대해 요구사항을 정의하였다.

표 1. 클라우드 컴퓨팅 보안 위협

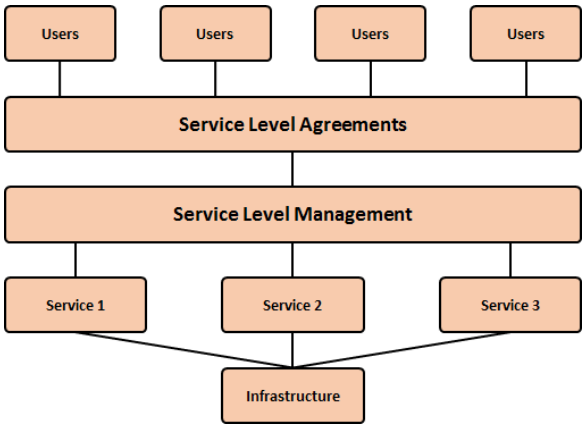
구분	내용
위협 1	클라우드 컴퓨팅의 오용과 비도덕적인 사용
위협 2	불안전한 인터페이스아 응용 프로그래밍 인터페이스
위협 3	악의적인 내부자
위협 4	기술 공유 문제
위협 5	데이터 유실 또는 유출
위협 6	계정 또는 서비스 하이재킹
위협 7	알려지지 않은 위협 프로파일링

정의된 요구사항 중 7번째 위협에 해당하는 '알려지지 않은 위협 프로파일링'은 서비스 제공자의 리소스에 대한 모니터링과 그에 따른 감사가 요구된다고 분석되었다. 더 자세하게 이야기하면, 그에 적용 가능한 로그와 데이터를 포함한 인프라 세부 정보를 부분적 또는 모두 공개하여 중요한 정보에 대한 감시와 그를 통한 위험 경보가 필요함을 강조하고 있다.

3. 서비스 감사 기술 동향 분석

3.1 서비스 수준 협약(Service Level Agreement)

클라우드 서비스를 위한 기본 구조는 그림 1과 같다. 서비스 제공자와 서비스 사용자 사이에는 서비스 수준 관리(Service Level Management)를 통한 서비스 모니터링 과정을 거치어 실제 제공될 서비스와 사용자 간의 계약이 실시되는 서비스 수준 협약(Service Level Agreement, SLA)이 실시된다. 사업자의 측면에 있어 SLA 제공에 대해 고려하여야 할 점은 타 서비스 사업자에 비해 서비스 품질에 있어서 확실한 우위에 있어 그 차이를 지속적으로 유지할 수 있는가 하는 것이다. 그렇다고 한다면 SLA를 타 서비스 사업자보다 먼저 도입함으로써 서비스의 품질 및 그에 대한 가격 차별화 전략을 통한 수익 확보의 방안이 될 수 있다. 그러나 그렇지 못한 경우 SLA를 먼저 도입하는 것이 오히려 불리하게 작용할 수도 있다. 만약 시장이 포화 상태에 근접하고, 경쟁 사업자의 입지가 작은 상황에서는 사용자들이 통신 사업자를 전환할 가능성이 작으므로 SLA 도입의 필요성은 작아진다.



▶▶ 그림 1. 클라우드 서비스를 위한 기본 구조

그러므로 SLA의 도입과 그에 대한 필요성을 확인할 수 있는 과정이 바로 서비스 감사(service audit)에 해당한다. 이와 같은 감사 과정을 통해 고객에게 정확한 서비스가 제공되었는지 판단하는 것이며, 표2는 정확한 서비스 제공에 대한 판단 기준이 되는 대표적인 SLA 관리 지표이다. 이와 같은 관리 주요 지표를 이용하여 IT 서비스를 수행한다.

표 2. SLA 관리 주요 지표

분류	지표명	내용
개통품질	개통지연	계약한 지표 값에 명시된 개통 청약일에 대한 준수 지연 시간
고장품질	고장처리지연	고장 발생시간부터 고장 처리 완료까지 소요 시간
	누적고장시간	요금 산정 시간(월)동안 총 누적 고장시간
	누적고장횟수	요금 산정 시간(월)동안 1시간 이상의 고장 발생 횟수
	가용도	가입자 전용 회선의 서비스 가용 (availability) 정보
통신품질	패킷지연	기준점으로부터 가입자의 접속장비까지의 측정 구간에 대한 월 평균 패킷 지연 시간
	패킷손실	기준점으로부터 가입자의 접속 장비까지 측정 구간에 대한 월 평균 손실 비율

서비스 감사를 위하여 실제로 이를 위하여 SLA 지표 리스트 및 요구수준을 분석하고 mapping을 수행한 후 수준에 따른 지표를 제시하여 사례 분석을 실시하는 연구 방법을 이용하였다. 그 결과 SLA 지표 가이드라인을 제시하는 성과를 이루었으나 국내 환경에 맞는 지표 정의와 업종/규모에 따른 지표 차별화와 수준의 제시가 필요한 한계점을 가지고 있었다. [4]에서는 클라우드 컴퓨팅 서비스 비용 산정에 있어 SLA를 연계한 청구 시스템을 제안하였지만, SLA 주요 관리 지표 및 긴급도별 처리 시간에 대한 언급만을 하였을 뿐 실제로 시스템의 설계나 구현은 하지 않았다.

3.2 Service Organization Control

Service Organization Control(SOC)[5]는 서비스 조직에서 제공하는 서비스 운영에 대한 독립된 감사인의 내부 통제 평가 보고서로써, 서비스 프로세스에 대한 신뢰 및 확산을 제공할 수 있도록 고안되었다. 아웃소싱 업무 통제 환경의 불확실성에 따른 관련 리스크를 평가하고 적절한 대응이 필요한 이용자(고객)에게 가치있는 정보 제공을 목적으로 한다.

3.3 ISACA Cloud IT Audit

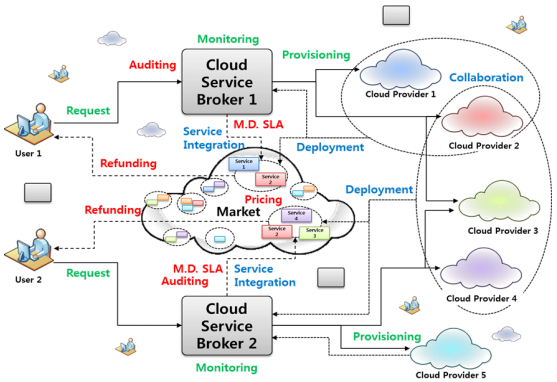
정보시스템 감사통제협회(ISACA, Information Systems Audit and Control Association)에서 발행한 클라우드 컴퓨팅 관리 및 감사를 위한 프로그램[6]으로 Cobit, COSO 등 기존의 내부 통제 프레임워크와 연계하여 정보를 제공한다. 뿐만 아니라 통제 성숙도 모델을 이용하여 조직의 현재 수준과 우수 운영 상태를 비교할 수 있도록 제시하였다.

3.4 FedRAMP

FedRAMP(Federal Risk and Authorization Management Program)[7]은 클라우드 서비스에 대한 보안평가, 인증 및 지속적인 모니터링의 표준화 된 접근 방법을 제공하기 위해 만든 미국연방정부의 프로그램이다. 이는 3PAO(Third Party Audit Organization) 제도를 두어 미국 정부에서 공식 인증한 민간 업체가 클라우드 서비스 제공자의 FedRAMP 인증 요건 준수 실태를 평가하도록 하였다.

4. 클라우드 서비스 브로커를 이용한 클라우드 서비스 감사

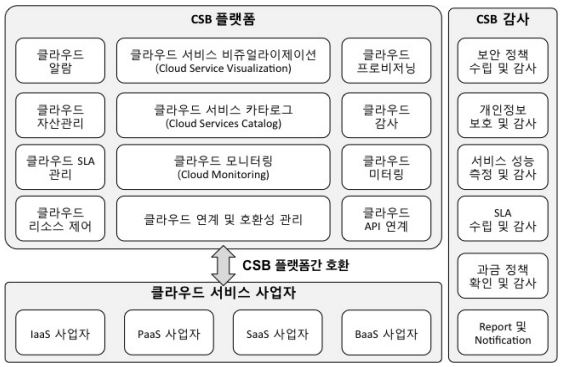
클라우드 서비스의 발전으로 서비스 제공하는 입장이 아닌 서비스를 사용하는 소비자의 관점에서도 서비스 품질과 보안, 프라이버시에 대한 보호와 감사 역할을 수행하여야 하고, 그 역할을 수행할 주체의 필요성이 높아지고 있다. 그를 위한 방안으로 클라우드 서비스 브로커(Cloud Service Broker, CSB)가 대두되었다. CSB는 기본적으로 개인과 기업과 같은 사용자가 클라우드 컴퓨팅을 이용함에 있어 필요한 제반 서비스를 공급. 관리하는 역할을 한다. 그러한 CSB가 부가적으로 클라우드 서비스 사용에 있어 발생하는 보안, 위험 등에 대한 문제를 체계적으로 대응하면, 서비스를 사용하는 소비자에게 신뢰성을 보장할 수 있다. 뿐만 아니라 CSB가 가지고 있는 다양한 클라우드 기술에 대한 깊은 이해를 바탕으로 클라우드 관련 기술에 대한 활성화가 가능하고, 나아가 클라우드 사용자가 원하는 서비스를 창출할 수 있을 것으로 예상된다.[8]



▶▶ 그림 2. 클라우드 서비스 브로커링 구조[9]

그러한 CSB의 클라우드 서비스에 대한 감사 역할을 수행함에 있어 접근 제어 방안, 보안 준수 방침 및 교육 방안, 감사 및 책임 준수 방안, 인증 및 권한 인가 방안, 비상 대책 수립 및 실행 방안, 유지 보수 및 업데이트 방안, 물리적/환경적 운영 방안, 위협 측정 방안, 시스템 및 통신 보안 방안의 9가지 기준을 바탕으로 감사 활동을 수행한다. 위와 같은 고려 요소들을 준수하고 사용자가 필요한 수준의 SLA(Service Level Agreement)를 정립하기 위해 클라우드 서비스 제공자만 참여해서는 실현이 어렵다. 그러한 과정에서 CSB나 정부 및 학계 등에서 체계적 지식, 기술 및 경험을 바탕으로 클라우드 SLA를 정립하고 이를 준수할 수 있는 법과 제도를 정립해야 하며, 이 가운데 CSB를 바탕으로 감사 및 감시를 할 수 있는 체계의 정립이 필요하다.

유럽에서는 클라우드 관련 기술을 모아 체계적으로 정립하고 오픈 소스로 활용할 수 있도록 지원하고 있으며, 대표 사례로 Compatible One 프로젝트를 들 수 있다. 이 프로젝트는 전문적 CSB를 위한 플랫폼을 유럽 차원에서 오픈 소스로 개발하는 과제이며, 이를 바탕으로 차세대 클라우드 서비스에 대한 경쟁력을 높이고자 하고 있다. 이와 같은 내용을 잘 정리한 것이 그림 3이다.



▶▶ 그림 3. CSB의 범위 및 핵심 요소

5. 결론 및 향후 연구과제

클라우드 서비스의 장점과 그로 인한 빠른 기술의 성장이 주목되고 있으나, 서비스 도입을 저해하는 요인들로 인해 클라우드 서비스를 위한 신뢰성 확보 방안에 대한 연구가 진행되고 있다. 본 논문에서는 그를 위해 클라우드 보안 위협과 그에 대한 요구사항을 알아보고 서비스 감사를 위한 기술 동향에 대해 분석하였다. 뿐만 아니라 클라우드 서비스에서 이슈가 되고 있는 클라우드 서비스 브로커에 대한 역할이 기존의 서비스 제공자와 사용자 간 중개에 국한하는 것이 아니라 감사 활동까지 아울러 수행함으로써 사용자를 위한 서비스 신뢰성을 확보에 힘쓰고 있음을 확인하였다.

결국, 클라우드 서비스를 위한 감사도 클라우드 서비스로써 제공되어야 한다는 것이다. 현재까지 발표된 SLA 평가 지표는 그 개수가 너무 적고 다양하지 못해 한계를 가지고 있다. 이를 개선하기 위해 평가 속성 및 지표를 더욱 많이 제시하고, 다양한 사례 연구를 수행하여야 할 것이다. 더불어 브로커 기반의 서비스 환경에서의 평가 지표에 대한 다양성 및 객관성을 확보하고 클라우드 서비스에 대한 감사 및 감시를 위한 체계를 정립하여야 한다.

참 고 문 헌

[1] IDC, “Worldwide and Regional Public IT Cloud Services 2013-2017 Forecast”, 2013.08

[2] Cloud Security Alliance, “Top Threats To Cloud Computing V1.0”, 2010.03.

[3] 박성순, 서정열, 임춘성, “IT Outsourcing 서비스 요구 수준에 따른 SLA 지표 개발에 관한 연구”, 한국경영정보학회 2004 춘계학술대회 논문집, pp.811-818, 2004년 6월.

[4] 박원일, 박명순, “SLA 연계한 클라우드 컴퓨팅 서비스 비용 산정”, 2013년 한국컴퓨터종합학술대회 논문집, pp.854-855, 2013년 6월.

[5] American Institute of CPAs, “Service Organization Control Reports®: Considerations for User and Service Auditors - Audit Alert”, 2013.

[6] Information Systems Audit and Control Association, “Cloud Computing Management Audit/Assurance Program”, (http://www.isaca.org).

[7] GSA, “The Federal Risk and Authorization Management Program (FedRAMP)”, 2014, (http://www.gsa.gov/portal/category/102371).

[8] 장선진, “CSB, 클라우드 서비스의 중심”, 정보통신산업진흥원 주간기술동향, pp.12-21, 2014년 4월.

[9] 신영록, 이승진, 허의남, “클라우드 서비스 브로커를 통한 사용자 중심의 서비스 가격결정 정책 수립 모델”, 한국정보처리학회 춘계학술발표대회 논문집, 2013년 5월

저 자 소 개

● 김 경 훈(Kyoung-Hun Kim) 정회원

- 2000년 2월 : 삼육대학교 컴퓨터과학과 (이학사)
- 2002년 2월 : 경희대학교 전자계산학과 (공학석사)
- 2012년 8월 : 경희대학교 전자계산학과 (공학박사)
- 2012년 3월 ~ 현재 : 강동대학교 컴퓨터정보과 교수

<관심분야> : 형상관리, 의료시스템, 컨텐츠, 클라우드, 사물인터넷

● 박 홍 준(Hong-Jun Park)

- 1985년 2월 : 아주대학교 전자계산학과 (공학사)
- 1987년 8월 : 한양대학교 전자계산학과 (공학석사)
- 2002년 2월 : 수원대학교 전자계산학과 (이학박사)
- 1994년 3월 ~ 현재 : 강동대학교 컴퓨터정보과 교수

<관심분야> : 디지털컨텐츠, 클라우드컴퓨팅, 정보보호, 사물인터넷

● 유 경 택(Kyeong-Taek Rhyu)

- 1988년 2월 : 원광대학교 전자계산공학과 (공학사)
- 1990년 8월 : 광운대학교 전자계산기공학과 (공학석사)
- 2006년 2월 : 원광대학교 컴퓨터공학과 (공학박사)
- 1995년 3월 ~ 현재 : 강동대학교 컴퓨터정보과 교수

<관심분야> : 분산컴퓨팅, 멀티미디어데이터베이스, XML, 시스템통합