Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Risk Factors and Issues in Record Management based Cloud Services

Uk-Hyun Lee[1], Young-Kon Lee[*2]

[1]*School of IT Convergence Engineering, Shinhan University*

[2]*Department of business management, Korea Polytechnic University*

ABSTRACT

Recently, many companies or organizations are introducing cloud services for managing digital records. Cloud services can dramatically reduce the cost of archiving and managing digital records, and provide a foundation for resilient management of digital records, depending on the business environment. However, due to the nature of the services provided by the cloud and the inherent risk inherent in the cloud, many companies are reluctant to apply cloud services to digital records management. In particular, the characteristics of digital records that should be stable and long-term preserved, and the characteristics of the cloud that needs to change the configuration of the server and storage from time to time in accordance with the user's request, often conflict with each other. These risk factors can vary widely depending on the nature and type of the cloud, which can seriously jeopardize the stability of digital records. In addition, cloud record management can be based on network-based locations where records are used and where they are stored locally or nationally, creating new legal and social issues that have not been experienced before in record management. In this paper, we analyze the risk factors of digital records management using cloud service and propose the countermeasures to solve them.

KEYWORDS: Cloud service, SOA, Record management, Risk factors, Rsik management, Digital records

ARTICLE INFO: Received 10 November 2017, Revised 7 December 2017, Accepted 12 December 2017.

[*]Corresponding author is with the Department of Business Management, Korea Polytechnic University, 237 SankiDaehak-Ro Siheung City, 15073, KOREA.
E-mail address: yklee2002@gmail.com

1. 개 요

클라우드 서비스는 사용자가 컴퓨팅, 스토리지, 소프트웨어 및 네트워크와 같은 IT 리소스를 통해 사용한 비용을 지불하는 데 필요한 만큼의 비용을 지불하는 서비스를 말한다. 클라우드 서비스는 정보 기술의 핵심적인 리소스 공유, 탄력적 리소스 운영, 온 디맨드 서비스 및 저렴한 비용으로 인해 정보 기술의 핵심으로 부각되고 있다.

클라우드 서비스를 이용하면 획기적인 비용 절감과 비즈니스 처리를 위한 정보시스템 도입을 빠르게 진행할 수 있다. 클라우드 서비스를 통해 규모의 경제를 실현하고, 시스템 구현, 동적 확장성 및 종량제 과금을 위한 초기 투자 비용을 절감할 수 있다. 클라우드 서비스를 도입하면 컴퓨팅 리소스를 준비하는데 소요되는 시간을 최소화함으로써 엔터프라이즈 민첩성을 대폭 향상시킬 수 있다. 또한 클라우드 서비스의 유연성, 복원력, 확장성 및 재해 방지를 통해 기업의 IT 경쟁력을 크게 향상시킬 수 있다.

현재 모바일, IoT 및 SNS를 비롯한 디지털 콘텐츠의 폭발적인 성장으로 인해 대부분의 기업들은 컴퓨팅 시스템을 클라우드 서비스로 신속하게 이동하고 있으며, 디지털기록관리 역시 클라우드로 전환하고 있는 중이다. 가까운 미래에 대부분의 디지털기록은 클라우드 서비스에 기반하여 제작, 보존 및 활용될 예정이다. 수많은 기업과 정부 기관이 이미 사내 비즈니스 시스템을 클라우드 서비스로 전환하고 있다.

하지만 많은 기업이 여전히 클라우드 서비스를 사용하는 것을 꺼리는 이유는 클라우드 서비스의 기록 관리와 애플리케이션 사례의 부족으로 인한 안전성 및 신뢰성 문제에 대한 우려 때문이다. 클라우드 서비스의 장점은 널리 알려진 반면 특히 클라우드 서비스의 기록 관리를 통한 클라우드 서비스의 단점은 잘 알려지지 않았다.

클라우드 서비스는 기본적으로 서비스 제공자가 제공하는 서비스 유형이며, 모든 비즈니스 규칙 및 시스템 운영 규칙은 서비스 제공자에 의해 결정된다. 따라서 서비스 공급자의 비즈니스 규칙 또는 시스템 운영 규칙이 기록의 기본 속성 요구사항을 충족할 수 없는 경우 이는 클라우드 서비스에 의한 기록 관리가 실패함을 의미한다. 클라우드 데이터 스토리지는 안정적인 엔터프라이즈 요구 사항을 충족하기 위해 유연한 프로비저닝에 보다 적합하며 장기적으로는 장기간 데이터 보존에 부적합할 수 있다.

또한 클라우드 서비스의 특성 때문에 클라우드 서비스의 계층화에 따른 전문화가 진행되고 있으며, 서비스 제공자의 역할도 분담되고 있다. 즉, 범용적인 클라우드 서비스, 기록관리전용 클라우드 서비스 및 기록관리 애플리케이션만을 제공하는 클라우드 서비스가 제공됨에 따라, 이러한 분산 서비스를 결합하여 기록관리 업무를 수행할 수 있게 되었다. 이것은 곧 기록 관리 태스크의 일관성과 품질을 보장하기가 매우 어렵게 되었다는 것을 의미한다.

클라우드 서비스는 개인 정보 보호 또는 데이터 액세스를 위한 법률 집행 등과 같은 사회적, 법률적 문제를 가질 수 있다. 예를 들어, 사용자와 클라우드 서비스 공급자의 물리적 위치가 하드웨어와 네트워크의 가상화로 인해 모호하기 때문에 정부 기관이 클라우드에 저장된 데이터에 액세스 하기를 원하는 국가 또는 지역 법률이 모호해 졌는데, 기술적 보안 문제는 클라우드 서비스 기반의 타사가 아닌 타사의 접근 방식으로 인한 디지털기록의 유출과 손실로 인해 점점 더 심각해 지고 있다. 개인 정보가 클라우드에 저장된 디지털기록물 사이에 누설되고 공개될 경우 개인 정보 침해와 같은 법적 위험 요소가 존재할 수 있다.

본 논문에서는 클라우드 서비스의 기록적인 관리 수명 주기에서 발생할 수 있는 위험요인 및 문제를 파악하고 분석한다. 또한 클라우드 기록 관리 거버넌스를 위해 참조할 수 있는 클라우드 서비스 기록관리 참조 모델을 제시하고 이를 기반으로 필요한 메타데이터 및 클라우드 기록관리 유스케이스들을 분석하고자 한다.

2. 관련연구 및 연구모델

클라우드 기록관리는 정부 주도 하의 실천 요강을 제공하기 위해 주로 선진국에서 시행되었다. 영국 국립 문서 보관소는 디지털 클라우드 기록 및 디지털 클라우드 기록을 사용하여 클라우드 기록 관리 관행을 조사하였다[1]. 미국에서는 클라우드 컴퓨팅 작업을 수행하는 과정에서 클라우드 컴퓨팅을 활용하는 디지털기록 관리 가이드가 개발되었으며[3], 호주는 클라우드 컴퓨팅과 관련된 기록 관리 위험 관리 지침을 개발하고 디지털 데이터 아카이빙을 위한 클라우드 서비스 인증 요구 사항 및 지침을 개발하였다[4]. 이러한 연구는 클라우드에서 국가 기록을 보관하는 지침으로 개발되었으며 위험 요소나 문제에 대한 체계적인 분석을 제공하지 않았다.

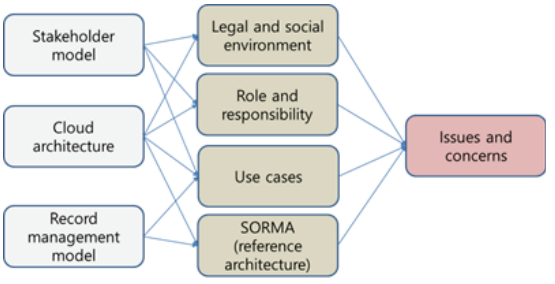

그림 1. 클라우드 기록관리 연구모델
Figure 1. Research model for cloud record management

이 논문에서는 클라우드 이해 관계자의 역할 및 책임과 클라우드의 법률적 및 사회적 환경 요인을 분석한다. 또한 퍼블릭 클라우드 아키텍처에서는 공공 환경에서 사용할 수 있는 사용 사례 분석 및 레퍼런스 아키텍처를 소개한다. 분석 결과를 토대로 클라우드 디지털기록을 사용할 경우 발생할 수 있는 문제와 우려 사항이 제시된다.

3. 라이프사이클 관리 및 SORMA 아키텍처

3.1 클라우드 디지털기록을 위한 라이프사이클 관리

클라우드 서버로 전송하여 기록하고 보존 기간이 끝난 시점에 보관하는 단계에서 디지털기록을 안전하고 안정적으로 관리하는 데 필요한 요구 사항이 있다. 일부 경우에는 클라우드 서버 간에 디지털기록을 재배치하거나 백업 데이터를 사용하여 복구할 수 있다. 이러한 프로세스에서는 다음과 같이 각 단계마다 클라우드 디지털기록이 필요하므로 기본적으로 필요한 요구 사항들이 있다.

- Creation : 클라우드 서비스에서 디지털기록의 신뢰성을 보장하기 위해 사용자들은 전자기록의 작성을 원본성, 신뢰성, 무결성을 보장하는 방식으로 디지털 기록을 만들고 관리해야 한다.
- Distribution : 클라이언트 측에서 생성하는 디지털기록물은 안전하고 안정적으로 클라우드 서버에 안정하게 전송할 수 있어야 한다.
- Preservation : 장기적으로 신뢰할 수 있는 디지털 콘텐츠를 제 3 자 저장소로 안전하고 안정적으로 저장하기 위해 IaaS 서비스를 제공해야 한다. 클라우드 스토리지에 보관된 기록은 항상 추적 가능해야 한다.

· Migration : 클라우드 스토리지에서 다른 클라우드 스토리지로 마이그레이션 할 경우 클라우드 아키텍처의 차이로 인해 기록의 변경사항이 발생하지 않아야 한다. 마이그레이션후에는 클라우드 스토리지에 저장된 모든 기록을 완전히 폐기해야 한다.

· Backup: 클라우드 서비스 공급자가 클라우드에서 장기간 백업할 수 있는 백업 방법 및 계획은 클라우드 서비스 제공자에 의해 제공되어야 한다.

· Disposal : 클라우드의 디지털기록 처리 및 파기 정책이 수립되어야 한다. 특히, 분산된 디지털 기록물의 완전한 폐기와 폐기 지점의 동기화가 이루어져야 한다.

3.2 신뢰성 있는 디지털기록관리를 위한 SORMA 아키텍처

신뢰성을 보장하면서 클라우드서비스를 기반으로 디지털기록관리를 수행하기 위해서는 필수적으로 필요한 서비스 요소들이 있다. 이를 클라우드 서비스 레이어별로 설명하고, 이러한 서비스들이 기본적으로 제공된다는 전제하에 클라우드기록관리 수행시 발생할 수 있는 여러 위험요소에 대해 분석한 결과를 제시하고자 한다.

클라우드 서비스 레이어는 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 등으로 구분된다. IaaS는 물리적 서버(CPU, 메모리, O/S), 스토리지 및 네트워크를 가상화하는 서비스를 제공하는 서비스이며, PaaS는 서비스로서의 플랫폼을 제공한다. 또한, SaaS는 서비스 형태로 애플리케이션을 제공한다. 이러한 클라우드 서비스에는 서비스 계층별로 핵심적인 서비스를 수행하는데 필요한 서비스 구성 요소가 있다.

기록물 관리에 클라우드 서비스를 적용하기 위해서는 기록 관리에 필요한 특수 서비스 구성요소가 추가로 이행되어야 한다. SaaS 계층에서, 사용자는 애플리케이션 형태로 기록 관리에 필요한 기능을 개발해야 한다. PaaS 계층은 기록관리 SaaS 애플리케이션의 구현과 서비스 형태 에서 개발된 애플리케이션을 관리하는 데 필요한 개발 플랫폼을 제공해야 한다. 또한 애플리케이션 개발에 필요한 API 및 서비스를 관리하는 서비스 도 제공해야 한다. IaaS 는 장기간 보존을 위한 기록을 제공하는 서비스를 제공해야 한다. 아카이브된 기록의 에스컬레이션 또는 해지와 관련된 서비스도 제공되어야 하며, 아카이빙 스토리지의 백업 및 복구를 위한 백업 및 복구가 제공되어야 한다. 클라우드는 서비스 기반 아키텍처이며 서비스 지향 아키텍처(SOA)를 기반으로 하는데, 모든 컴퓨터 리소스, 소프트웨어, 플랫폼, 미들웨어 및 데이터베이스는 양식 서비스로 제공한다. 본 논문에서는 SOA 기반의 SORMA(Service Oriented Record Management Architecture) 참조 아키텍처를 제시하며, 이는 제3자 기반의 디지털전자기록관리 국제표준(ISO 17068)[16]을 참조하여 SOA 형태로 구성하였다. SORMA서비스 컴포넌트는 <그림 2> 와 같다.

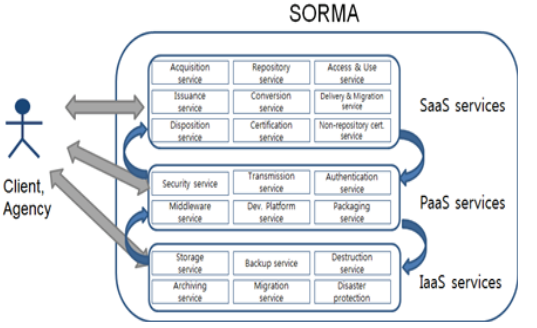

그림 2. SORMA 아키텍처
Figure 2. SORMA architecture

4. 클라우드 기록관리를 위한 관계자 모델

4.1 클라우드 기록관리 클라이언트

기업 및 기관의 디지털기록 제작자는 기록의 관리 원칙을 바탕으로 디지털기록의 신뢰성과 신뢰성을 보장하는 방법과 방법에 따라 클라우드 SaaS 서비스를 사용하여 디지털기록을 작성해야 한다. 디지털기록 제작자는 신뢰할 수 있는 디지털기록을 생산할 수 있어야 한다. 신뢰할 수 있는 기록은 의무, 활동 및 사실을 입증할 수 있는 완전하고 정확한 표현으로 신뢰할 수 있으며, 후속 작업 또는 활동의 과정에서 콘텐츠를 입증할 수 있다.

디지털기록물 생산조직은 기록의 신뢰성을 보장하기 위해 디지털기록물의 생산, 수령, 전송, 유지관리 및 처분을 위한 정책 및 절차를 수립하고 시행한다. 따라서 디지털기록의 추가, 삭제할 수 있는지 확인해야 한다.

생산된 디지털기록은 무단 변경으로부터 보호되어야 한다. 기록 및 녹음 절차에서 추가 또는 기록을 허용하는 조건에서 추가 또는 기록을 허용하는 조건에 따라 기록을 추가하거나 기록할 수 있는 기록을 지정해야 한다.

기록에 대한 문맥 연계 정보에는 기록이 작성되고 사용된 조치를 이해하는 데 필요한 정보가 포함되어야 한다. 보다 광범위한 사업 활동과 기능의 맥락에서도 기록을 식별할 수 있어야 한다. 순차적 방식으로 수행된 활동을 문서화한 기록 간의 연계성을 유지하는 것이 바람직하다.

4.2 클라우드 서비스 제공자

클라우드 서비스 제공자는 클라우드 서비스 계층의 수준에 따라 IaaS 제공자, PaaS 공급 업체 및 SaaS 제공자로 분류되어야 하며, 안전하고 안정적인 디지털기록 관리를 수행하기 위해 역할과 품질 보증을 제공해야 한다.

SaaS 제공자는 클라이언트와의 서비스수준계약(SLA) 품질 관리 계약을 체결하고 그에 따라 품질 수준을 유지하도록 노력해야 한다. 이를 가능하게 하기 위해 SLA 항목에 대한 상호 합의를 거쳐 SaaS 공급 업체와 클라이언트 간의 서비스 품질을 유지해야 한다. SaaS 애플리케이션은 정보 패키지 형식으로 클라이언트로부터 디지털기록을 수집하고, 보관 패키지 형태로 IaaS에 저장하고, 관련 메타 데이터를 안전하고 내결함성이 있는 방식으로 관리할 수 있어야 한다. SaaS 제공자들은 이러한 애플리케이션을 이용하여 클라이언트들과 계약을 맺으려고 노력하고 있다. 클라우드 환경에서 신뢰할 수 있는 정보 패키지의 항목과 관련된 메타 데이터 항목도 설정되어야 한다.

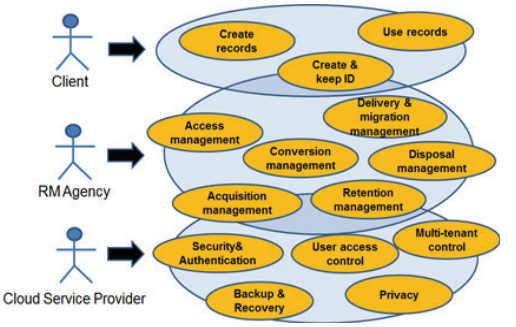

그림 3. 클라우드 기록관리를 위한 관계자 역할 구성도
Figure 3. Stakeholder model for cloud record management

PaaS 공급 업체의 역할은 안정성과 안정성을 갖춘 복구 SaaS를 구축하고 운영하는 플랫폼을 제공하는 것[4]. 그것은 배급 업체가 디지털기록을 제공할 수 있는 기능과 품질 표준을 유지하기 위해 노력해야 한다. IaaS 제공자의 역할은 신뢰할 수 있는 스토리지를 제공하는 것이다[5]. 가상화를 통해 기록 스토리지 서버 또는 스토리지의 변경 사항이 있더라도 디지털기록 메타 데이터와 디지털기록을 안정적으로 저장할 수 있어야 한다. IaaS 제공자는 분산 및 가상화된 스토리지 영역에서 안전하고 신뢰할 수 있는 디지털기록 관리를 위해 수행해야 하는 역할과 관리 항목을 제공해야 한다.

5. 클라우드 기록관리 유스케이스

클라우드 디지털기록 및 디지털기록에 사용되는 클라우드 서비스 유형을 사용하여 클라우드 디지털기록 관리에 대한 다양한 사용 사례 분석을 수행할 수 있다. 이 절에서는 사용 사례에 따라 장점, 단점 및 위험 요소를 제시한다.

5.1 클라이언트에 의해 공유되는 SaaS 애플리케이션

이는 클라우드 서비스를 이용하여 디지털기록 업무를 수행하는 가장 일반적인 형태이다[6]. 클라이언트는 SaaS 스타일 기록관리 애플리케이션을 사용하여 디지털기록 관리 업무를 수행한다. 기록관리 어플리케이션은 온라인 소프트웨어의 형태로 제공되며, 클라이언트의 요청에 따라 소프트웨어 구성을 부분적으로 수정 또는 변경하여 변경할 수 있다.

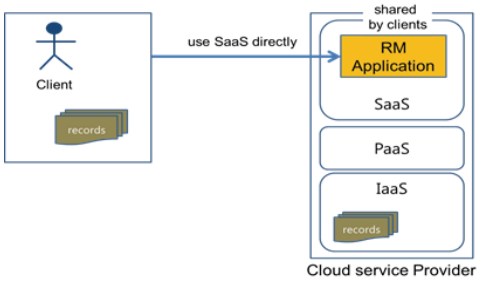

그림 4. 클라이언트에 의해 공유되는 SaaS 서비스
Figure 4. SaaS application shared by a client

5.2 클라이언트 SaaS를 직접 개발

이 유스케이스는 클라이언트가 PaaS를 기반으로 직접 개발하여 기록관리 애플리케이션을 사용하는 사례이다[7]. 클라이언트는 기록관리 애플리케이션을 원하는 형태로 개발하고, PaaS에 탑재함으로써 운영 및 활용한다. 이는 대개 자신의 요구 사항을 만족시키기 위해 특정 규모 이상의 기업 또는 기관을 위한 형태로 기록관리 소프트웨어를 개발하고 운영하는 목적을 가지고 있다.

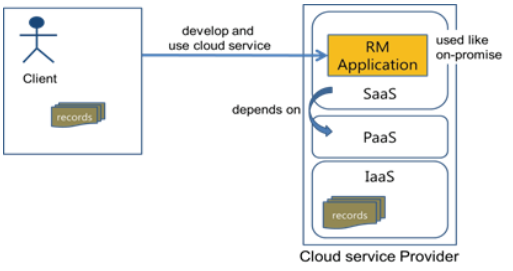

그림 5. 클라이언트에 의해 개발된 SaaS
Figure 5. SaaS application developed by a client

5.3 클라이언트가 SaaS를 활용

이는 클라이언트가 디지털기록 관리에서 IaaS만 사용하는 경우이다[8]. IaaS는 컴퓨터 하드웨어 리소스를 활용하기 위한 가장 저렴한 방법이므로, 방대한 양의 디지털기록을 IaaS에 저장하고 대부분의 다른 디지털기록 업무를 클라이언트 측에서 수행하는 방식이다.

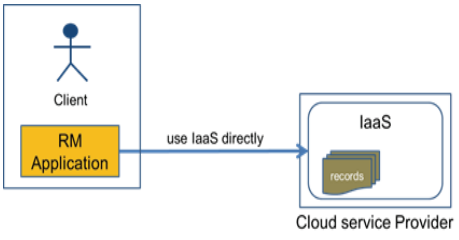

그림 6. 클라이언트에 의해 사용되는 IaaS
Figure 6. IaaS just used by a client

이 방법은 클라이언트가 대부분의 경우 고유한 디지털 레코딩 의무 및 소프트웨어를 유지하는 동시에 클라우드를 통해 많은 유지 관리 비용을 절감할 수 있다. 이 방법은 클라우드가 디지털기록 업무에 도입된 이후에 클라우드가 미치는 영향을

최소화하면서 클라우드의 다양한 위험 요인을 최소화할 수 있는 이점을 제공할 수 있다. 하지만, 기존 기록관리 애플리케이션과 IaaS 사이의 인터페이스는 계속 관리되어야 하며, 기록관리적용으로 IaaS 스토리지 매체에 대한 세심한 통제와 모니터링은 매우 어려울 수 있다. 또한 클라이언트와 IaaS 서비스 공급자 간의 디지털기록 저장 정책이 서로 상충되는 경우 솔루션에 대한 단서를 찾기 어려울 수 있다.

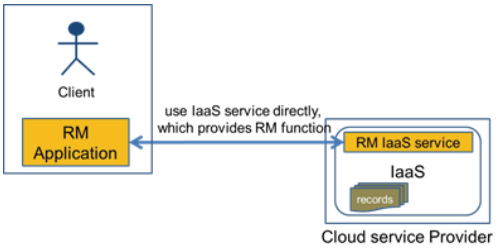

그림 7. 기록관리 기능을 가진 IaaS 활용
Figure 7. IaaS with RM functions

디지털기록 관리를 위한 일부 특수한 클라우드는 클라우드 내부의 기록관리와 관련된 기본적인 기능을 구현하여 클라우드가 이 기능을 통해 보다 쉽게 활용할 수 있도록 지원한다. 이 기본 기능은 클라이언트가 IaaS를 보다 쉽게 연동할 수 있도록 디지털기록의 검색, 저장, 전송 및 파기 등과 같은 업무를 처리하는 인터페이스를 제공한다.

5.4 다수의 IaaS 동시 활용

이는 클라이언트가 여러 IaaS를 사용하여 디지털기록을 저장하는 경우이다[9].

비즈니스 연속성에 대한 의심이 제기되거나 디지털기록을 안전하게 보관하려고 할 경우, 클라이언트는 하나 이상의 IaaS에서 디지털기록을 저장하고 관리할 수 있다. 이 방식의 장점은 IaaS 서비스 공급업체의 비즈니스가 단절되더라도 디지털기록을 저장하고 유지할 수 있다는 점이다. 단점은 클라이언트가 모든 IaaS에 저장된 디지털기록의 일관성을 유지하기 위해 지불을 담당해야 한다는 점이다.

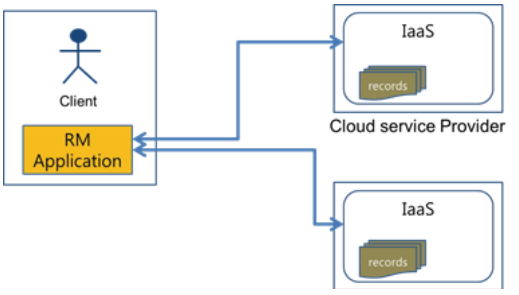

그림 8. 클라이언트에 의한 다수 IaaS 동시 활용
Figure 8. Multiple IaaS used by a client

6. 클라우드 서비스의 위험요소

6.1 서비스 위험요소

클라우드는 기본적으로 서비스 지향 아키텍처(SOA)를 기반으로 한 구성을 기반으로 한다. 따라서, 클라우드 디지털기록 관리는 SOA와 거의 동일한 위험을 가지고 있다. SOA에 따른 SOA의 비효율성 요인은 다음과 같다.

- 내부 논리, 관리 및 활동은 서비스 내부에 숨겨져 있음을 확인할 수 없음.
- 서비스를 사용하는 가장 좋은 방법을 아는 것이 어려움.
- 문제의 근본 원인을 파악하기 어려움.
- 서비스 공급자 중심의 구조물. 따라서 서비스 제공자에게만 종속될 수 있음.
- 내부 서비스 관리 방법을 파악하기 어려움.
- 디지털기록 관리를 위한 필수 기능이 제공되지 않을 경우가 있음.

클라우드 서비스 기술은 매우 빠르게 변화하고

있으며, 많은 표준, 제품 및 관련 위원회가 있다. 클라우드 기술의 변화, 클라우드 서비스 공급 업체 변경 또는 표준 변경으로 인해 비즈니스 연속성이 침해될 가능성이 항상 있다. 즉, 클라우드 서비스를 변경할 가능성이 항상 있다는 뜻이며, 클라우드 서비스의 클라이언트 요구에 따라 컴퓨터 리소스를 신속하게 프로버저닝 할 수 있다. 그러나, 프로비저닝은 안정적이고 장기적인 디지털기록 유지의 위험이 될 수 있으며, 데이터 소유권 문제와 지역 분배에 의해 저장되는 클라우드 데이터의 특성에 따라 디지털기록의 신뢰성을 저해할 수 있다.

6.2 클라우드 관계자 위험요소

클라우드는 다중 테넌트가 컴퓨터 리소스 풀을 공유하는 일종의 서비스이다. 따라서 중요한 정보나 개인 정보나 개인 정보 관리 시스템의 프라이버시 문제를 공개할 위험이 발생할 수 있다.

클라이언트 인증은 안전하고 신뢰할 수 있는 클라우드 기록 관리를 위한 시작점이며, 애플리케이션, 사용량 수준 및 디지털기록 소유권에 대한 관리 권한을 엄격하게 관리 해야 한다. 클라우드 디지털기록의 신뢰성 유지, 인증에 근거한 액세스 권한 관리, 수준 관리, 소유권 관리, 개인 정보 침해 및 보안 위협에 대한 대비를 유지할 수 있는 클라이언트 인증 방법이 항상 필요하다.

6.3 클라우드 시스템 위험요소

클라우드 환경에서는 서버 가상화, 스토리지 가상화 및 네트워크 가상화에 영향을 미칠 수 있는 가상화에 대처하기 위한 조치가 필요하다. 서버 가상화 및 프로비저닝은 디지털기록 관리의 성능, 가용성 관리 및 백업 복구 관리에 영향을 미친다.

스토리지 가상화의 스토리지 위치, 분산 처리로 인한 위험, 구성 관리의 변경으로 인한 메타 데이터 손실 위험 등의 위험이 있다. 또한 보안 및 액세스 위험으로 인해 보안 위협 요소로 인한 보안 위협이 발생하고 있으며, 이로 인해 네트워크 가상화, 멀티캐스트, SaaS 환경에서도 보안 위협이 발생한다.

멀티테넌시(Multi-tenancy)는 여러 테넌트가 애플리케이션을 공유하는 동시에 개별 사용 환경을 구성할 수 있는 기술이다. 이는 클라이언트 맞춤형 애플리케이션 구성을 위한 필수 기술이며, 클라우드 서비스의 특성상 성능을 유지한다. 그러나 애플리케이션의 핵심 정보는 공유되어야 하며, 사용자 지정 스크립트는 쉽게 노출되므로 보안을 강화할 수 있다. 따라서 각 계층에 대한 멀티테넌시(Multi-tenancy)로 인한 위험을 진단하고 안전하고 안정적인 디지털기록을 유지하는 데 필요한 관리 항목을 정의해야 한다.

디지털기록 메타 데이터에는 비즈니스 컨텍스트와 디지털기록의 설명 데이터가 모두 포함된다. 메타 데이터는 디지털기록의 검색 및 활용에 있어 매우 중요한 위치를 차지한다. 클라우드 서비스의 특성상, 메타 데이터와 디지털기록은 항상 서버와 동일한 스토리지에 저장되므로, 링크 손실, 분산 처리로 인한 일관성 문제, 잘못된 링크 정보 등과 같은 다양한 문제가 발생할 수 있다. 따라서 클라우드 서비스 유형에 적합한 메타 데이터 쓰기와 디지털기록 간의 연결 시스템이 반드시 필요하다.

클라우드 서비스 서버 또는 스토리지 구성의 구성 변경에 따라 안전하고 내결함성이 있는 메타 데이터 및 디지털기록 스토리지 및 활용 계획이 필요하다. 클라우드는 리소스 가용성 측면에서 여러 서버 또는 스토리지에 단일 파일을 배포하는 방법을 사용한다. 즉, 클라우드는 여러 분산 방식으로 파일을 저장하는 것을 기반으로 한다. 다수의 저장된 파일의 일관성과 무결성, 처분 및 폐기물의 일관성과 적법한 데이터의 활용 및 활용은 어려운

문제가 될 수 있다. 이러한 경우, 마스터 복사본은 여러 사본에 대해 결정되어야 하며 원본 복사본으로 제공되어야 한다. 복사본 중 하나의 내용이 의도치 않게 변경된 경우에는 이 복사본을 삭제하고 마스터 복사본을 다시 사용하여 복사해야 한다. 일반적인 클라우드 환경에서는 신뢰성과 무결성을 유지하기가 매우 어려우며, 또한 클라우드 서비스의 근본적인 구조적 변화를 필요로 한다.

디지털기록이 클라우드 서비스 전반에 걸쳐 배포될 경우, 문서의 진위성과 무결성을 보장하기 위해 따라야 할 행정적 및 기능적 요건을 정의해야 한다. 클라우드는 다수의 사용자가 컴퓨팅 리소스를 공유하는 시스템이므로 리소스 공유에 대한 철저한 대비가 필요하다.

클라우드 공유 스토리지를 사용하는 디지털 문서 전송에서는 디지털기록과 해당 메타 데이터의 구조적 관계를 유지하여 전송할 수 있어야 한다. 가상화로 인해 메타 데이터가 손실되고 컨텍스트 관계가 손상될 위험이 있다. 여러 구성 요소로 구성된 디지털기록을 획득할 경우 단일 기록으로 관리할 수 있도록 구성 요소 간의 관계를 유지해야 한다.

7. 결 론

본 논문에서는 클라우드에서 디지털기록 위험 요인을 분석하였다. 위험 요인은 클라우드가 본질적으로 서비스 유형, 클라우드 시스템 및 서비스 공급 업체에 의해 야기되는 문제, 클라우드가 본질적으로 미치는 영향 등의 문제이다. 이러한 문제는 클라우드 디지털기록 관리의 주요 문제를 야기할 수 있으며, 클라우드를 디지털기록에 적용하는 데 있어 기업의 주요 관심사가 되고 있다. 이러한 문제를 해결하기 위해 SLA를 기반으로 하는 클라우드 디지털기록 서비스의 품질 관리를 선행해야 하며, 클라우드 서비스 제공자, 조직 및 비즈니스에 대한 전반적인 거버넌스 시스템을 구축해야 한다.

References

[1] J. Na, *Qualitative study on service features for cloud computing,* Journal of Digital Contents Society, Vol. 12, No. 3, pp. 319-327, Sep. 2011.

[2] M. M. Qiu, Y. Zhou, and C. Wang, *Systematic analysis of public cloud service level agreements and related business values,* In Proceedings of International Conference on Services Computing, pp. 729-736, Jun. 2013.

[3] C. Wu, Y. Zhu, and S. Pan, *The SLA evaluation model for cloud computing*, In Proceedings of International Conference on Computer, Networks and Communication Engineering, pp. 331-334, May 2013.

[4] E. Badidi, *A cloud service broker for SLA-based saaS provisioning,* In Proceedings of International Conference on infomation Society, pp. 61-66, Jun. 2013.

[5] S. Venticinque, R. Aversa, B. D. Martino, M. Rak, and D. Petcu, *A cloud agency for SLA negotiation and management,* In Proceedings of Euro-Parallel Processing Workshops, pp. 587-594, Jan. 2011.

[6] Z. Wang, X. Tang, and X. Luo, *Policy-based SLAAware cloud service provision framework*, In Proceedings of International Conference on Semantics Knowledge and Grip, pp. 114-121, Oct. 2011.

[7] H. He, Z. Ma, H. Chen, and W. Shao, *Towards an SLA-driven cache adjustment approach for applications on PaaS,* In Proceedings of the Asia-Pacific Symposium

on Internetware, pp. 11-20, Oct. 2013.

[8] I. Ayadi, N. Simoni, and T. Aubonnet, *SLA approach for "Cloud as a Service"*, In Proceedings of International Conference on Cloud Computing, IEEE Computer Society, pp. 966-967, Jun. 2013.

[9] M. Alhamad, T. Dillon, and E. Chang, *Conceptual SLA framework for cloud computing,* In Proceedings of International Conference on Digital Ecosystems and Technologies, pp. 606-610, Apr. 2010.

[10] *Google cloud platform: Terms of service*. https://developers.google.com/cloud/terms/, Aug. 2016.

[11] Google Compute Engine, https://cloud.google.com/compute, Jun. 2016.

[12] Google App Engine, https://cloud.google.com/appengine, Apr. 2016.

[13] Office 365, http://office.microsoft.com/kokr/business/FX104051403.aspx, Oct. 2016.

[14] *EULA and terms of service,* Retrieved from https://www.greenqloud.com/eula/, Jan. 2017.

[15] ISO 17068 :2016, Information and documentation - The Trusted Third Party Repository for Digital Records, Dec. 2017.

클라우드 서비스를 활용한 전자기록관리에 있어서의 위험요소 분석

이욱현[1], 이영곤[2]

[1] *신한대학교 IT융합공학부*

[2] *한국산업기술대학교 경영학부*

요 약

최근 많은 기업 혹은 기관들이 디지털기록 관리를 위한 클라우드 서비스를 도입하고 있다. 클라우드 서비스는 디지털기록을 보관하고 관리하는 비용을 획기적으로 줄일 수 있으며, 기업 환경에 따라 디지털기록의 탄력적인 관리를 위한 기반을 마련할 수 있다. 하지만 클라우드에서 제공하는 서비스의 특성과 클라우드에 내재된 내적 위험요인 때문에 많은 기업들이 클라우드 서비스를 디지털기록 관리에 적용하는 것을 주저하고 있다. 특히 안정적이면서 장기적으로 보존될 수 있어야 하는 디지털 기록의 특성과 사용자의 요청에 따라 수시로 서버와 스토리지의 구성을 융통성 있게 바꾸어야 하는 클라우드의 특성이 서로 상치될 상황이 자주 발생하게 된다. 이러한 위험요인들은 클라우드의 특성과 종류에 따라 다양하게 발현될 수 있으며, 디지털기록의 안정성을 크게 위협할 수 있다. 본 논문에서는 클라우드 서비스를 활용한 디지털 기록관리의 위험 요인을 분석하고 이를 해결하기 위한 대처 방안들을 제시하고자 한다.

감사의 글

본 논문은 2017년도 신한대학교 학술연구비 지원으로 연구되었음

Uk-Hyun Lee is a Professor of School of IT Convergence Engineering, Shinhan Univ. Her Research Interests include big data computing and cloud service computing.

E-mail address: uhlee@shinhan.ac.kr

Young-Kon Lee is a Professor of Department of business management, Korea Polytechnic University. His Research Interests include e-business SOA, IT service QoS, cloud service computing, knowledge search based on ontology.

E-mail address: yklee2002@gmail.com