한국기록관리학회지, 18(3), 2018, pp. 49-70

클라우드 컴퓨팅 환경 영구기록물관리 시스템 구축 방안 연구*

A Study on the Archives Management System in Cloud Computing

김 기 정(Ki-Jung Kim)**
신 동 수(Dong-Soo Shin)***

목 차

〈초 록〉

본 연구에서는 기존의 기록관리시스템, 영구기록관리시스템, 중앙영구기록관리시스템을 국가기록 클라우드로 통합하기 위한 클라우드 시스템 모델을 제시하였다. 또한 중앙영구기록관리시스템을 포함한 영구기록관리시스템을 클라우드 환경으로 전환하기 위한 구체적인 방안을 연구하였다. 국가기록 관련 시스템들을 하나의 클라우드 기반으로 통합하여 정보자원의 공유・활용 및 운영・관리 효율성 제고, 비용 절감을 도모하기 위한 클라우드 시스템 설계 전략 및 목표 모델을 도출하고, 특히 영구기록관리시스템의 단계적인 클라우드 구축 방안을 제시하였다. 또한, 클라우드 환경에서 노출되는 기술적 보안과 운영적 보안 사항을 분석하고 이를 해결하기 위한 방안도 제안하였다. 결과적으로 클라우드 기술을 도입하여 저비용・고효율 등의 효과를 볼 수 있고, 현용-준현용-비현용 단계에서의 업무 연속성을 높일 수 있는 설계가 가능하다.

주제어: 클라우드 컴퓨팅, 기록관리시스템, 영구기록관리시스템, 중앙영구기록관리시스템

〈ABSTRACT〉

This paper proposes a cloud system model for incorporating the existing Records Management System (RMS), Archives Management System (AMS), and Central Archives Management System (CAMS) into a cloud-based national records management system. To do this, research on concrete and stepwise ways to transform AMS, including CAMS, into a cloud computing environment was carried out. This study developed a cloud system design strategy and goal model to integrate national records - related systems into a single cloud system to share and utilize information resources, manage them efficiently, and reduce costs. In particular, this study analyzed technical security and operational security that are exposed in the cloud environment and suggested measures to solve them. As a result, cloud computing technology can be applied to achieve low-cost and high-efficiency effects.

Keywords: Cloud computing, Records Management System (RMS). Archives Management System (AMS), Central Archives Management System (CAMS)

---

* 본 연구는 2017년 국가기록원 연구개발사업 '차세대 기록관리 모델 재설계 연구'의 일환으로 수행된 연구임.
** ㈜에이더블유아이 기술이사(kjkim@awi.co.kr) (제1저자)
*** ㈜에이더블유아이 대표(shindongsoo@awi.co.kr) (공동저자)
■ 접수일: 2018년 7월 31일 ■ 최초심사일: 2018년 8월 8일 ■ 게재확정일: 2018년 8월 20일
■ 한국기록관리학회지 18(3), 49-70, 2018. 〈http://dx.doi.org/10.14404/JKSARM.2018.18.3.049〉

1. 서 론

1.1 연구배경 및 필요성

최근 IT 관련 기술의 수준이 높아지면서 제4차 산업혁명의 시대를 맞이하고 있다. 4차 산업혁명은 2013년 1월 B.Lovins에 의해 언급된 개념이다. 그 중, 클라우드 컴퓨팅 기술은 IT업계 최고의 키워드 중 하나로 급부상하였다. 클라우드 컴퓨팅은 인터넷을 통해 서비스로 제공되는 응용 프로그램과 해당 서비스를 제공하는 데이터 센터의 하드웨어 및 소프트웨어 모두를 의미한다. 클라우드 컴퓨팅 환경에 대해 국내외 많은 기업 뿐만 아니라 공공기관에서도 해당 서비스에 대한 관심이 높아지고 있고, 실제 적용한 사례들을 쉽게 볼 수 있다. 다양한 분야에서 클라우드를 도입하고 있는 만큼 기록관리 분야 또한 예외가 아닐 수 없다.

기존의 종이기록에서 전자기록관리체계로 전환하기 위해 행정기관에 전자기록관리시스템(Records Management System 이하 RMS)이 보급되었다. 또한, 주요 기록물의 체계적 수집·정리로 기록정보의 자원화를 추진하여 우리는 기존의 종이기록물 방식에서 보다 더 쉽게 정보를 저장 및 활용을 할 수 있게 되었다. 기록관리 체계는 일반적으로 기록관리 업무를 현용-준현용-비현용 3단계로 나눌 수 있다. 시간이 지날수록 기록물 보전에 대한 중요성이 높아지고 있으며, 이로 인해 국가는 생산, 중간보존, 영구보존 단계별로 3가지 시스템에 의해 기록관리를 하고 있다. 현용단계인 온-나라시스템, 준현용 단계의 RMS, 비현용 단계의 영구기록관리시스템(AMS; 이하AMS라고 함)에 의해 기록관리 업무를 수행중이며, 온-나라 시스템, RMS를 클라우드 서비스로 이미 전환을 하였다. 클라우드 전환은 범정부 협업기반 마련, 시스템 유지비용 절감, 업무효율 극대화 뿐만 아니라 혁신적인 기록관리의 기반을 마련할 수 있는 좋은 기회가 된다. 클라우드 환경을 적용하기 전에는 행정 환경변화와 IT기술 발전에 의해 각 시스템별로 고도화를 진행하게 되고, 이에 시스템간 데이터, 프로세스 등 서로 동일한 형태를 유지해야 되는 부분임에도 불구하고 서로 상이한 부분들이 발생하고 있었다. 이러한 문제는 시간이 지날수록 더욱 더 격차가 벌어질 것이고 이를 맞추기 위해 많은 비용을 소비해야 될 것이다. 클라우드 서비스가 반드시 좋은 결과를 가져온다는 보장은 없다. 하지만 클라우드 컴퓨팅 적용 시 가져올 이점은 간과하지 않을 수 없고 그에 따른 준비 및 선제적 대응이 필요하다고 생각한다.

외국의 내셔널 아카이브들은 클라우드 정책에 따른 기록관리 측면의 위험요소와 가이드를 제공하고 있으며, 점차 공공/민간 등 다양한 클라우드 인프라의 활용 프로세스를 제시하고 있다. InterPARES Trust 프로젝트에서 제시하는 인프라(Infrastructure), 보안(Security), 접근(Access), 통제(Control), 법(Legal Issues) 등 10개 주제분야 연구를 통해 인터넷 및 클라우드 환경에서 기록관리의 신탁(Trust)을 확보할 수 있는 방안을 모색하였다.

국내의 경우 범정부 클라우드 업무환경으로의 전환을 추진하고 있다. 법·제도 측면에서 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률' 시행('15.9)에 따른 1차 기본계획(K-ICT 클라우드컴퓨팅 활성화계획, 15.11) 3대 전략 중 "공

공부문의 클라우드 선제적 도입"과 함께 행정기관 및 공공기관이 전자정부사업을 효율적으로 추진할 수 있도록 행정・재정・기술 등을 지원하는 전자정부지원사업 중 '정부지식 공유활동기반 고도화 사업(2015)'을 진행하였다. 그 결과 기록 관련 시스템으로서 클라우드 온나라, 클라우드 RMS가 개발되었다. 클라우드 RMS는 2015년 클라우드 전환 검증 전보화전략계획을 추진한 뒤 2016년 클라우드 기록관리시스템을 개발하여 행정안전부 대상으로 시범 운영했고, 2017년 하반기부터 고용노동부, 공정거래위원회 등 15개 기관을 시작으로 2018년 27개 기관, 2019년 5개 기관으로 확산될 예정이다. 이 시스템은 다수 부처가 공동 결재한 문서 관리, 타 부처 기록물 검색 활용 기능을 제공하며, 인프라 면에서 정부조직 개편에 빠르게 대응할 수 있을 것으로 기대된다. 그러나 참여 개발자는 국가기록원이 주관하는 유지보수 사업의 참여 업체에 제한되기 때문에 기술적인 문제와 해결 방안에 대한 고찰 및 설계 방향을 제시하는 연구는 부족한 실정이다. 국내의 영구기록관리시스템(Archives Management System, 이하 AMS)은 중앙영구기록물관리시스템(Central Archives Management System, 이하 CAMS)외 지방영구기록물관리기관의 설립은 서울기록원이 가장 선도적이나 정보화전략계획 후 추진 1차년도 진행 중으로 영구기록물관리시스템의 요건이나 기술 기반에 대한 연구 또한 미비한 실정에 있다. 또한, 지속적으로 기능 개선 사업을 추진하고 있으나 기반 체계까지 광범위한 범위의 개선 연구가 부족하다.

현용, 준현용 단계의 시스템은 클라우드 시스템으로 전환이 되었다. 따라서 비현용 단계 시스템 또한 클라우드 시스템으로 전환되어야 한다. 전자기록의 유형이나 특성이 하나로 고정되어 있지 않고 업무적 환경이나 컴퓨팅 환경이 발전하고 고도화 되면서 새로운 유형에 대한 대응이 필요한데 비현용 단계의 시스템이 클라우드 환경이 아니면 이를 조율하는 부분에 대해 많은 비용이 들 것으로 예상된다.

따라서, 본 연구에서는 기존의 RMS, AMS, CAMS를 국가기록 클라우드로 통합하기 위한 클라우드 시스템 모델을 제시하고 특히 아직까지 클라우드 전환이 이루어지지 않은 영구기록관리시스템 클라우드 전환 방안에 대한 연구를 하였다.

1.2 사례분석

1.2.1 영국 국가기록원

영국 국가기록원(TNA: The National Archive)은 클라우드 가록관리 사례를 퍼블릭 클라우드를 활용한 전자기록과 전자기록용 특수 클라우드 사례에 대해 연구(The National Archives, 2014)를 수행하였다. 그 결과를 요약하면 다음과 같다.

- 퍼블릭 클라우드 전자기록관리의 경우 도입 비용과 운영 비용이 저렴하며, 글로벌 기업(아마존, 구글, MS 등)의 클라우드를 활용함으로, 기록의 안전한 저장과 클라우드 기업의 비즈니스연속성 보장이라는 측면에서 장점이 있음. 하지만, 전자기록 고유의 특성을 유지하고 관리하기에는 한계가 있음.
- 전자기록 전용 클라우드는 전자기록 관리만

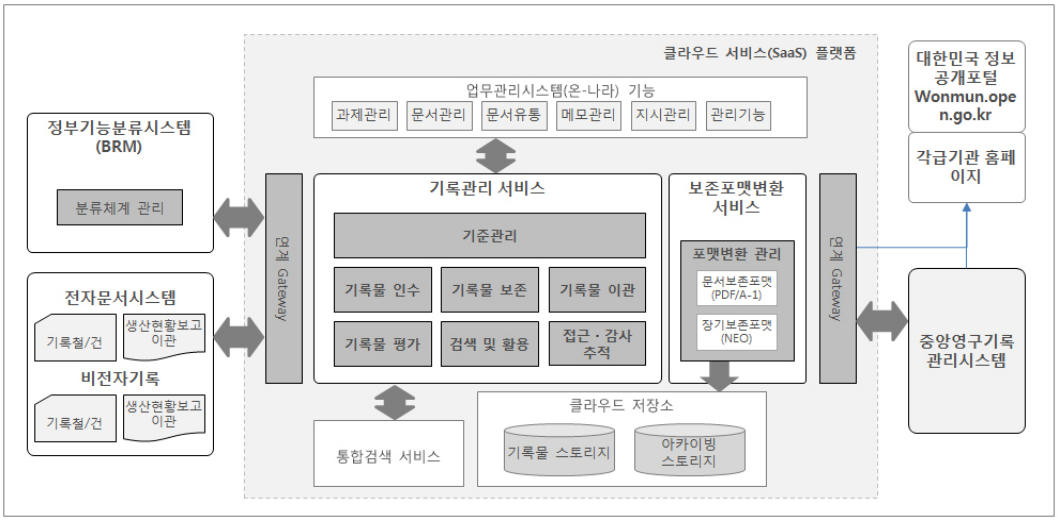
을 위한 여러 가지 서비스(아카이빙, 처분)를 제공하며, 전자기록의 신뢰성과 진본성, 무결성 유지에 많은 노력을 기울임. 클라이언트의 입장에서는 특별히 전자기록관리와 관계된 소프트웨어를 개발할 필요가 없음. 하지만, 초기 투자비용과 운용비용이 일반 클라우드에 비해서는 많이 들어가며, 일반 클라우드에 비해 전자기록 클라우드의 비즈니스 규모나 연속성은 떨어짐.

- 전자기록에 있어 클라우드 활용사례가 늘어나면서, 전자기록 전용 특수 클라우드의 비즈니스 전망도 높게 나타나고 있으며, 전자기록 서비스 차별화 및 각국의 정부 클라우드 추진 계획에 따라 글로벌화된 전자기록 특화 클라우드의 출현도 예상되고 있음.

1.2.2 클라우드 기록관리시스템

국가기록원은 범정부 G-클라우드 기반의 클라우드 기록관리 시스템 전환 구축을 수행하였으며 그 결과는 다음과 같다(국가기록원, 2017).

- 클라우드 기록관리시스템은 부처별로 구축·운영되던 기존의 기록관리시스템을 개선한 통합형으로 여러 부처가 협업하면서 공동으로 결재한 문서를 기록으로 관리하거나, 클라우드 기록관리시스템 내에서 타 부처 기록물을 검색·활용할 수 있음.
- 또한 국가정보자원관리원에 위치한 범정부 클라우드 인프라를 사용하여, 정부조직 개편에 따른 신규 구축 등에 빠르게 대응할 수 있게 되고, 유지관리 비용의 대폭적인 절감이 기대됨.
- 기록관리시스템이 클라우드로 전환되면, 기록관리 전문요원들의 기록관리시스템 운영·관리 업무 부담이 감소되고, 부처 간 기록정보의 통합 검색 및 활용 확대를 통해 협업과 소통이 촉진될 것.



〈그림 1〉 클라우드 기록관리시스템 구성도

2. 국가기록 클라우드 서비스 설계 방안

2.1 국가기록 클라우드 서비스 설계 방향

2.1.1 현행 기록관리 시스템의 문제점

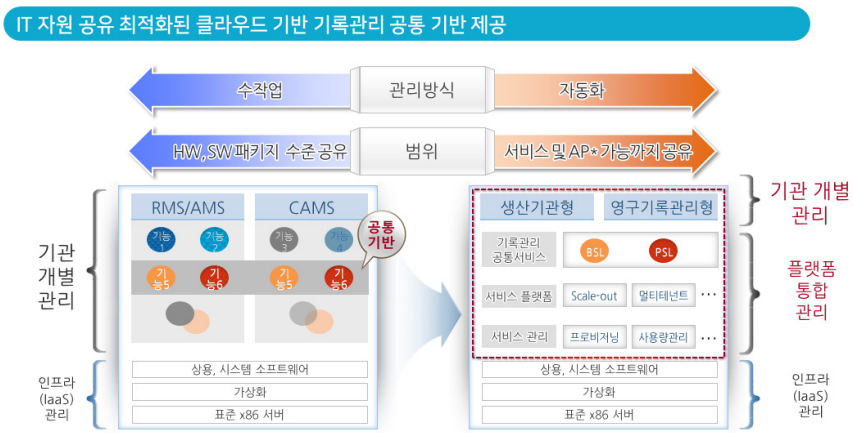
현행 기록관리 관련 시스템 구축 프로젝트 수행 시 국가기록원의 중앙 배포 방식의 SW패키지를 각 기관에 별도 설치 사용함으로써 하드웨어 자원의 공유가 어렵고 또한 반복적인 설치로 인한 중복투자의 비용 낭비 요소가 있다. 또한 소프트웨어의 개정도 각 기관별로 별도의 프로젝트로 진행됨으로써 표준화 및 시스템 유연성, 확장성이 부족하고 다양한 기록물 유형의 관리를 위한 기능 업그레이드도 어렵다. 최근 OSS,[1] 애자일 개발방법론, 마이크로서비스 아키텍처 시스템이 부상하고 있는 점을 고려하여 좀 더 효율적이고 유연한 업무 환경으로 변화가 필요하다

2.1.2 차세대 기록관리 시스템 방향성

현행 기록관리 시스템의 문제점을 해결하기 위해서는 〈그림 2〉와 같은 IT 자원 공유에 최적화된 클라우드 기반의 기록관리 공통 기반을 제공할 필요가 있다.

클라우드 기반의 기록관리 플랫폼은 기존의 수작업의 관리를 자동화 하고 그 자원 공유의 범위를 기존의 하드웨어 또는 SW패키지 정도만 공유하는 수준을 넘어서 서비스 및 공통 기능까지도 공유가 가능하다. RMS, AMS 및 CAMS의 공통 서비스 기능을 단일 플랫폼 하에서 공통 컴포넌트 또는 서비스 제공을 통해 기관에 필요한 기능들을 레고 시스템처럼 조립을 통하여 쉽게 구현할 수 있도록 하는 플랫폼 구현이 필요하다.

본 연구에서는 이러한 기록관리 공통 기반을 제공하기 위한 SaaS[2] 플랫폼을 실제로 구현하기 위한 방안에 대해서 구체적인 모델을 제시



〈그림 2〉 클라우드 기록관리 공통 기반

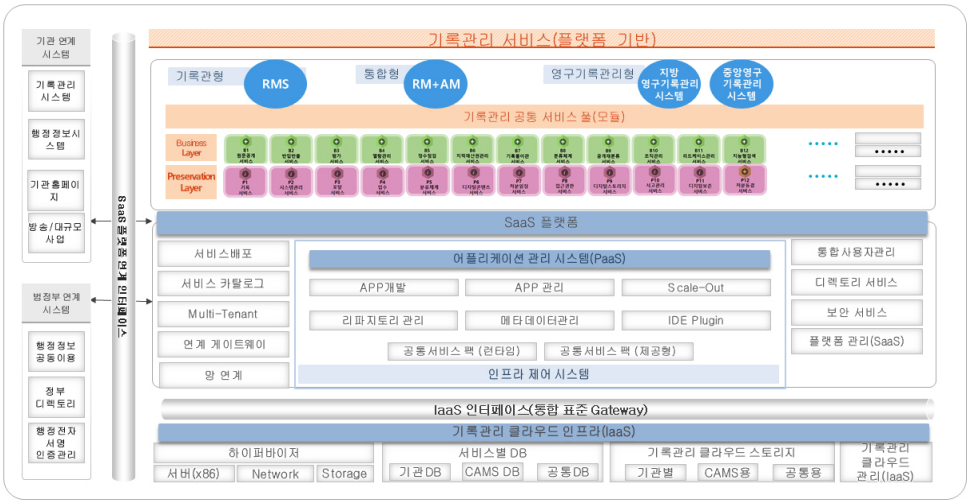
1) OSS(Open Source Software): 소스 공개 소프트웨어
2) SaaS(Software-As-A-Service): 자신의 하드웨어(서버, PC)에 설치하여 사용하던 소프트웨어를 제공자의 클라우드 서비스에 가입하여 이용하는 형태를 일컬음

하였다. 또한 이러한 기록관리 공통 플랫폼이 공유 인프라 서비스 플랫폼 위에서 구동되도록 하기 위한 IaaS[3] 구축 방안도 필요하다. 기록관리 IaaS 플랫폼에 오픈소스 기반의 소프트웨어 및 기술을 적용함으로써 비용에 대한 부분은 어느 정도 해소될 것으로 예상한다.

2.2 국가기록 클라우드 목표 모델

SaaS 플랫폼 기반 기록관리 서비스를 하게 되면 별다른 인프라 등을 설치할 필요 없이 어플리케이션 형태의 기록관리시스템 솔루션 제공과 함께 스케일아웃,[4] 멀티테넌트,[5] 프로비저닝[6] 등의 플랫폼 제공 및 상용 S/W, 시스템 S/W, 서버의 가상화 적용이 가능하다. 또한, 마이크로 서비스 아키텍처 기술을 적용할 수 있게 되고 설치비용 최소화, 손쉬운 커스터마이징 도구 및 모듈 제공으로 인한 맞춤으로 인해 기관 별 필요한 모듈을 선택함으로 인해 자체 효율적인 시스템 구축이 가능해 진다(이승억, 2015).

기록관리 공통서비스 모듈 풀을 보여주는 〈그림 3〉에서 각 기관 및 지자체는 RMS, AMS, CAMS 등 구축하고자 하는 시스템에 대해 국가기록원에서 제공하는 기록관리 표준안을 참고하여 시스템을 구축하면 된다. SaaS기반의 마이크로 서비스 아키텍처 기술의 큰 장점이라고 할 수 있다(임진희, 2017).



〈그림 3〉 SaaS 플랫폼 기반의 기록관리 서비스

3) IaaS(Infra-As-A-Service): 하드웨어, 데이터베이스 SW등과 같은 IT 인프라 자원을 제공자의 클라우드 서비스에 가입하여 이용하는 형태를 일컬음
4) Scale-Out: 계산 용량이 더 필요한 경우 한 대의 서버 용량을 늘리는 방식(Scale-In)이 아닌 서버 수를 확장하는 방식
5) Muti-tenant: 입주형 기숙사와 유사한 개념으로, 기관들이 IT자원을 같이 공유하는 공용영역과 한 기관이 독자적으로 사용하는 전용영역이 구분된 서비스 형태를 일컬음
6) 프로비저닝: 가상화된 CPU/메모리/각종 SW등의 자원을 요구에 따라 자동으로 할당 해주는 방식

SaaS 플랫폼은 클라우드 공통서비스 환경에서 제공되는 기록관리 서비스의 서비스 환경 제공을 목적으로 하며, 〈표 1〉과 같이 통합사용자관리를 기반으로 하는 통합인증과 서비스 배포 및 관리 등 서비스 제공환경으로 구성하여야 한다.

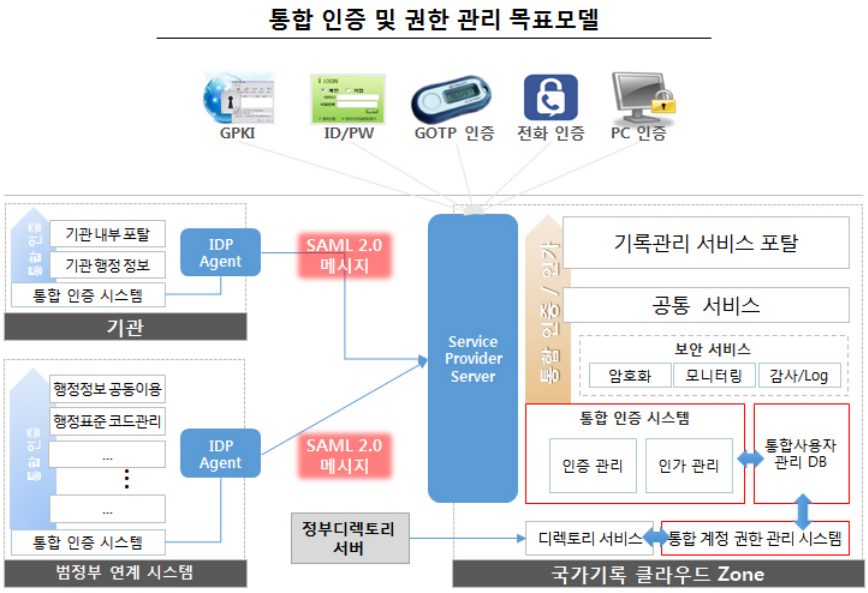
통합 사용자 관리 구성방안은 다양한 인증 수단에 대한 통합 인증 체계를 구성하고, 클라우드 외부 기관의 자체 인증 시스템과의 인증 연계를 위해 SAML 메시지 기반의 연계 표준을 구성하여야 한다. 또한 정부디렉토리를 원장으로 계정을 동기화하여 통합 계정 및 인증 정보를 구성하여, 클라우드 내 서비스에 대한 접근 인가 및 서비스 사용 권한에 대해 계정 속성과 역할을 기반으로 관리하도록 구성한다. 〈그림 4〉는 통합 사용자 관리 구성 방안에 대한 구조이다.

SaaS 플랫폼 서비스 배포 및 실행은 다음 절차를 따르는 방안을 제시한다.

1) 부처/기관별 정보화담당관이 서비스 신청
2) 웹 데스크탑에서 서비스카탈로그 항목 요청
3) 정보화담당관에게 서비스 카탈로그 항목을 기반으로 서비스 선택 요청
4) 요청된 카탈로그 정보를 서비스 리포지터리에서 취득
5) 선택된 서비스 카탈로그 내역을 서비스 배포기능에 전달
6) 서비스 배포기준에 따라 프로비저닝 준비
7) IaaS에 시스템 자원할당 요청 및 처리결과 수신
8) 할당된 시스템 자원에 AP 배포
9) 자원할당 및 AP배포 후 서비스 실행 요청
10) 서비스 실행 요청

〈표 1〉 SaaS 플랫폼 기능

SaaS 플랫폼 기능	설명
통합사용자관리 및 통합인증	• 정부 디렉토리시스템의 조직/직원정보와 기관별 포탈의 통합사용자관리서비스 기반으로 한 통합인증 서비스를 제공 • 디렉토리기능을 서비스화 하여 분산 효과를 가짐 • 통합인증(SSO)을 활용하여 외부 서비스 연계를 수행
서비스 배포 및 관리	• 서비스 구성을 위한 서비스 카탈로그 관리 및 제공 • 서비스 리포지토리 구성 및 관리 • 서비스 배포를 위한 인프라 환경 관리 기능과 연계
서비스 제공환경 구성	• 단일 시스템 자원을 다중 사용자/기관에게 서비스를 제공할 수 있는 multi-tenant 기능 제공 • 서비스를 위한 시스템 자원 구성 및 관리를 위해 IaaS 환경의 관리기능과 연계
서비스 연계 환경 제공	• 기관 내부 포탈, 기관 기록물, 영상 자료 등 외부에서 생산되는 자료에 대한 서비스 연계 환경 제공 • 연계 게이트웨이 및 통합인증(SSO)을 이용한 기록관리시스템 및 기관별 기록관리의 서비스 연계
자원 및 환경 관리를 위한 솔루션 활용	• 어플리케이션 관리 및 서비스 환경 구성을 위한 자원 관리를 위한 솔루션 도입 • SaaS 플랫폼의 관리 기능과 솔루션 관리 기능의 연계 • 공통 기능요건을 도출하여 솔루션 도입 또는 관련 기능 개발 시 기준 마련 필요



〈그림 4〉 통합 사용자 관리 구성 방안

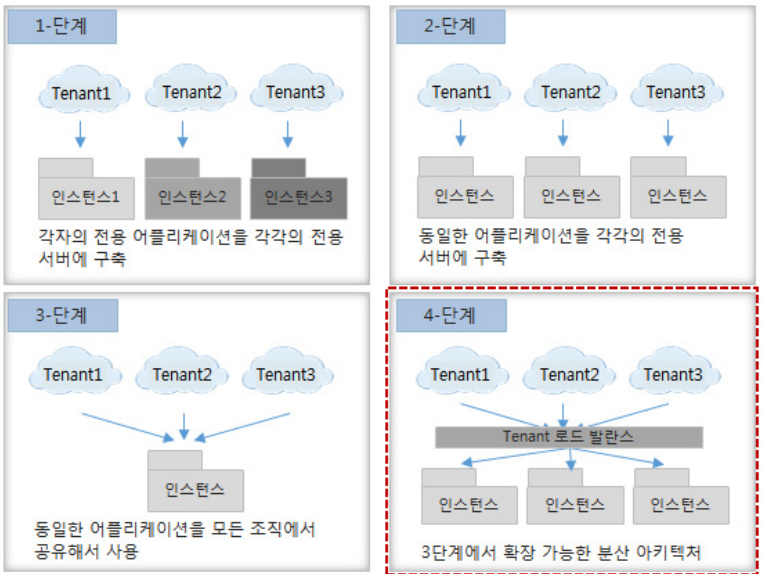
클라우드 서비스의 카탈로그는 메타정보를 기반으로 각 기록관리시스템을 담당하는 정보화 담당관이 서비스를 선택/조합하여 원하는 기록관리시스템의 환경으로 구성할 수 있도록 해준다. 즉, 서비스 리포지토리에 있는 메타정보에 기반하여 구성된 서비스 카탈로그를 이용하여 정보화 담당관이 서비스를 선택 및 조합할 수 있다. 메타정보에는 서비스 이름, 필수 서비스여부, 서비스간 연관관계, 유사서비스간 그룹화 등의 정보가 포함된다. 이 서비스 리포지토리 및 서비스 카탈로그는 클라우드 서비스 플랫폼 관리자가 관리하게 되며 운영정책을 반영하여 카탈로그 범위를 지정할 수 있도록 한다.

자원을 사용하는 구분에 따라 멀티테넌시의 4단계 모델을 구분하여 4단계 형식의 멀티테넌시를 권장한다. 〈그림 5〉와 〈표 2〉는 멀티테넌시 모델 및 기능내역을 설명한다.

서비스 연계 유형에 따라 데이터연계와 웹서비스 연계로 구분하며, 연계 서비스 대상에 따라 내/외부 연계로 구분할 수 있다. 각 연결 구간에 데이터 암호화를 적용하고, API제공 서비스를 위해 PaaS[7] 플랫폼에 제공되는 API 게이트웨이를 이용한다.

다음은 PaaS 플랫폼 구성방안이다. 일반적으로 3가지 유형의 구성방안에 대해 살펴본다. 먼저, RHEV[8]가상화 기반의 IaaS플랫폼 기반인 OpenShift Enterprise는 확장 기능(Auto-Scaling)에 대해서는 별도의 관리 시스템과의 연계 또는 기능 개발이 요구된다. CloudFoundry의 경우 아직까지 국내 적용사례가 없다. IaaS영역

7) PaaS(Platform-As-A-Service): 운영 및 개발 환경까지 같이 제공하는 클라우드 서비스
8) RHEV(RedHat Enterprize Virualization): 레드햇 회사의 가상화 브랜드명



〈그림 5〉 멀티태넌시 구축모델

〈표 2〉 멀티태넌시 기능 내역

멀티태넌시 기능 내역	설명
1단계	• 각각의 전용 어플리케이션을 각각 전용서버에 구축한 형태 조직별로 다른 인스턴스가 독립적 서버에서 운영되며 사용자별로 애플리케이션 코드도 별도로 관리된다.
2단계	• 동일한 어플리케이션을 각 전용서버에 구축한 형태 사용자별 기능 커스터마이징 환경을 통해 이루어진다. 1단계보다 진화되었지만 여전이 관리 비용이 많이 소요 된다.
3단계	• 동일한 어플리케이션을 모든 조직에서 공유해서 사용한다. 자원에 효율성은 좋지만 데이터 보안을 해결해야 하며, 중앙집중적 관리라 확장성이 떨어진다.
4단계	• 3단계에서 확장이 가능한 분산 아키텍처 구조로 바꾼 모델이다. Tenant의 데이터를 분산 관리하며 재구성이 가능한 메타데이터로 각 Tenant별 커스터마이징을 지원

을 PaaS에서 제어하여 자동확장을 가능케 한다. 별도의 라이선스 비용이 드는 점이 있다. 이에 반해, 오픈소스 기반인 Open Paas(PaaS-TA)가 있다. 한국정보화진흥원(NIA)에서 수행하고 있는 연구 과제 사업으로 전자정부 표준 프레임워크 기반의 Open PaaS이다. 17년 2월 구축 완료 후 서비스 확장중이며 가상화 의존 없이 구성이 가능하다. OpenStack을 통한 IaaS 플랫폼이 독립적으로 구축됨으로 기존의 클라우드 영역에 적용 불가능하다. 또한, OpenStack 구축 시 네트워크, 스토리지, 모니터링 영역을 각각 독립적으로 구성해야 한다.

PaaS 플랫폼을 종합적으로 정리를 하면 IaaS 제어, 가상화 의존성, 비용모델, 운영사례 등 4가지 측면에서 PaaS플랫폼 구축 모델을 비교한 결과 기록관리 클라우드에 적합한 구축 모델은 Open PaaS를 기반으로 PaaS-TA 플랫폼을 적용하는 것이 바람직해 보인다(〈표 3〉 참조).

〈표 3〉 PaaS 플랫폼 종합

서비스 자원 및 환경관리	IaaS 제어	가상화 의존성	비용 모델	운영사례	비고
OpenShift Enterprise	외부 기능 연계	의존성 없음	구독	• G-클라우드 IaaS • 광주통전 네트워크	• 별도의 관리 시스템과의 연계 또는 기능 개발이 요구(예: Auto Scaling)
CloudFoundry	직접 제어	VMware OpenStack	라이선스	• 국내 없음	• 국내 검증 사이트 없음
OPEN PaaS [PaaS-TA]	직접 제어 외부 기능 연계	의존성 없음	커뮤니티	• NIA개발 완료 후, KOSCOM 등 서비스 확산 중	• 국내 연구과제로 시작하여 현재 서비스 기능 확장 계획으로 연속성 보장

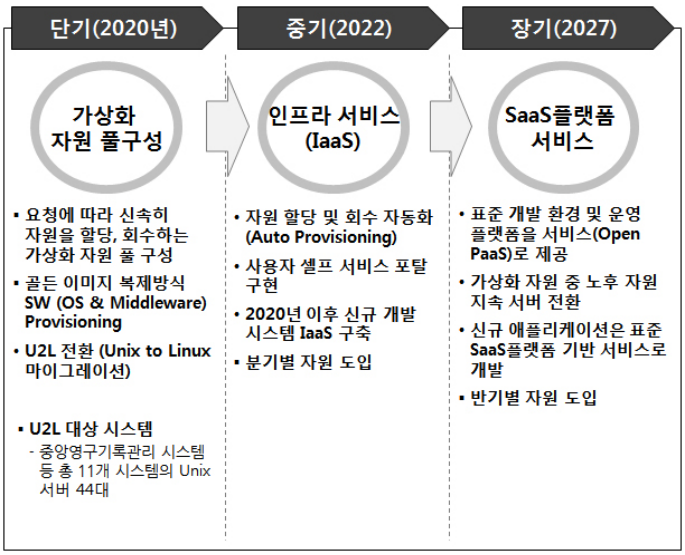
2.3 단계별 구축 방안

기 구축한 시스템에 변경이나 영향 없이 클라우드 서비스로 발전시킬 수 있도록 빅뱅방식이 아니라 점진적 아키텍처 확장으로 단계별 구축 계획을 마련하여 추진한다. 국가기록원의 인프라에 대해 단계별 발전 방향을 요약하여 〈그림 6〉에서 2027년까지의 발전 방향을 단기-중기-장기로 분리하여 제시하였다.

3. 영구기록관리물관리 클라우드 서비스 제공 방안

3.1 서비스 대상기관 정의

영구기록관리기관을 분류하면 〈그림 7〉과 같이 4개의 그룹으로 분류되고 이 중 지방기록관리기관은 특별시, 광역시・도, 특별자치시・도 및 해당 시도의 교육청을 포함하여 가장 많은



〈그림 6〉 영구기록물관리시스템의 인프라 단계별 발전 방향

〈그림 7〉 국가기록관리기관체계

*출처: 국가기록원 홈페이지(http://www.archives.go.kr/next/manager/nationalArchivesOrgan.do)

기관을 포함한다.

가장 많은 기관이 속한 지방기록관리기관을 대상으로 문헌을 통해 현황 조사를 실시하여, 지방기록물관리기관은 공공기록물관리법에 의해 영구기록물관리기관을 설치하여야 하나 2017년 현재 건립 중인 서울기록원과 건립 계획을 수립한 경상남도를 제외한 지방기록물관리기관은 설치 추진이 원활하지 못 한 상황인 것으로 확인되었다.

3.2 설계 방향

기록관리 대상의 확대와 정보시스템 환경 변화 및 정보기술의 비약적 발전으로 기록관리 프로세스의 전면적 개편이 필요해 졌다. 특히 클라우드를 기반으로 한 정보시스템 환경 변화와 다양한 애플리케이션간의 유기적 결합의 용이성은 기록정보자원 간 연계를 통한 보다 가치 있는 기록정보서비스를 실현할 수 있는 여건이 조성되었다.

3.2.1 기록관리 효율성과 유연성 반영

각 기관별 맞춤형 영구기록관리 시스템 환경을 구축해야 한다. 기관마다 하나의 업무에 대해 정해놓은 워크플로우가 상이하므로 기관별 특성을 고려하여 업무 형태 및 단계에 알맞은 기능을 구성할 수 있어야 한다.

이를 위해서는 기관 특성에 맞게 차세대 기록관리시스템의 Preservation Service와 Business Service를 맞춤형으로 구성 가능해야 하고(〈그림 3〉 참조), 기록관리업무 3단계(생산 -〉 보존 -〉 관리)에 적합한 기관과 자체적으로 보존 및 관리를 함께 하는 기관 등 다양한 기록관리 환경에 적합한 모델이어야 한다.

3.2.2 모듈성(modularity)을 지닌 기록관리 시스템 구성

모듈화된 마이크로 서비스 아키텍처(Micro Service Architecture)의 장점을 채택하여 서비스별 독립적 DB관리를 통한 서비스 독립성 확보하고, 쉬운 기능 변경 및 확장, 프로세스 변

화 및 사용자 요구에 빠르게 대응할 수 있다. 한편 클라우드 SaaS 구현으로 인프라 및 유지보수 비용절감할 수 있다.

마이크로서비스를 통한 명확한 모듈화를 통해 독립적으로 모듈화된 각 레이어의 서비스들은 마이크로서비스로 구성되며 모듈화된 서비스에 대한 명확한 경계 부여가 가능하고, 마이크로서비스를 적극 활용하여 상이한 기관별 세부업무에 적적용할 수 있다. 마이크로서비스로 구성된 서비스는 클라우드 환경에서의 어플리케이션의 수정 및 버전업데이트 등이 용이하고, 기능적으로 수정해야 하거나 커스터마이징 되어야 할 부분을 변경할 때 편리하다.

3.2.3 표준화된 영구기록관리시스템 클라우드 서비스 형태 제공

〈그림 8〉과 같이 클라우드 서비스 형태로 전환하면 별다른 인프라 등을 설치할 필요 없이 어플리케이션 형태의 기록관리시스템 솔루션 제공(SaaS)하고, Scale-out, 멀티테넌트, 프로비저닝 등의 플랫폼제공 및 상용 S/W, 시스템 S/W, 서버의 가상화가 가능하다. 마이크로서비스, 설치비용 최소화, 손쉬운 커스터마이징 도구 및 모듈 제공으로 인한 기관맞춤 가능하며, Open Source 및 Open API를 이용한 커스텀화 제공 및 타 서비스와의 연동성 증대할 수 있다.

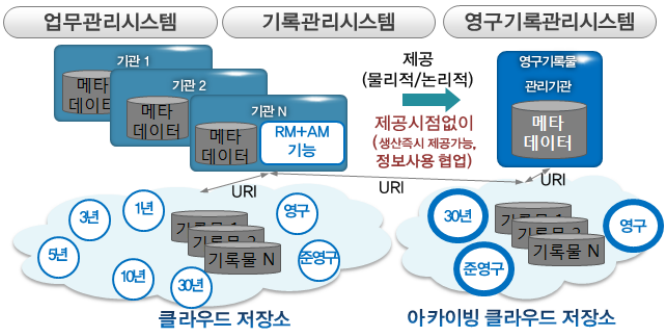
4. 영구기록관리시스템 IaaS 구축 방안

우리는 앞서 영구기록관리시스템을 클라우드 서비스로 전환하기 위해 SaaS, PaaS 플랫폼의 국가기록 클라우드 서비스 구축 전략을 수립하였다. SaaS 플랫폼 기반의 차세대 통합형 기록관리시스템으로 이행하기 위해 국가기록원 자체의 인프라 자원을 가상화 통합하고 IaaS서비스를 제공하는 단계적 시행이 필요하다.

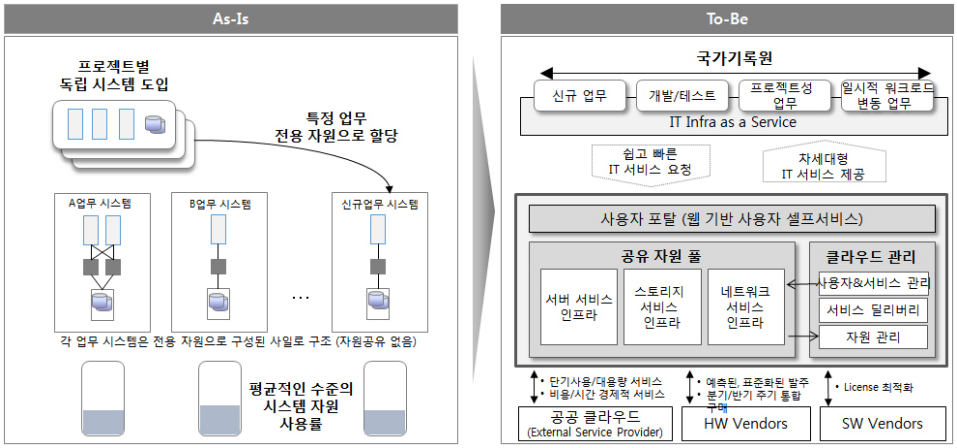
4.1 설계 방향

IaaS는 IT자원 공유가 최적화된 클라우드형 아키텍처 설계가 필요하다. 현행(As-Is) 아키텍처와 목표(To-Be) 아키텍처의 개요를 보면 〈그림 9〉와 같다.

가상화 기반 시스템은 자원 풀을 만들어 사



〈그림 8〉 영구기록관리시스템의 서비스 방식 전환



〈그림 9〉 클라우드형 아키텍처 개요

용자의 요청에 따라 즉시 제공하고 사용량 변동이나 요청에 따라 자원을 회수하거나 추가 할당하여 시스템 자원 활용률을 높이고 신규 인프라 자산 도입 비용, 전력비용, 그리고 상면 비용을 절감할 수 있다. 따라서 자원 할당과 회수가 용이한 표준 기반 가상 자원 풀 환경이 필요하고 사용자 요청에 따라 필요 자원을 즉시 할당하는 서비스를 제공해야 한다. 아키텍처의 To-Be모델이 나오면 기능 요건에 대한 설계를 한다. 이 때, 설계 원칙으로 국가기록원 차세대 AMS 목표시스템 구축을 위한 차세대 인프라 설계 요건 정의서를 통하여 4가지 설계 원칙을 도출하였다. 첫 째, 자원할당 최적화로 비용절감이다. 사용자 요구 또는 워크로드 변동에 따라 필요한 적정량의 자원을 할당하고 사용중인 서비스에 영향없이 자원을 추가 도는 일부 회수한다. 두 번째 요건으로 민첩성 향상이다. 사용자는 손쉽고 빠르게 서비스를 요청하고 요청 후, 1일 이내 신규 할당/추가/회수를 완료하여야 한다. 셋째로, 자원 요청, 자원 할당/회수의 운영관리 효율을 극대화 하여 최소의 인력으로 운영가능하게 끔 운영효율의 향상요건이 필요하다. 마지막으로 기관 기술 표준 준수 및 지속적인 강화 환경을 제공하여 기관 기술표준 강화요건이다. 〈표 4〉의 기능에 따라 요건을 적용시켜 아키텍처 설계 방안을 도출하였다.

4.2 클라우드 서비스 역량확보

클라우드 서비스 유형(IaaS, PaaS, SaaS)에 따라 운용모델과 서비스 유형의 두가지 측면을 고려하여 사용자와 공급자의 책임과 역할 구분이 필요하다(이종운, 서경진, 김희웅, 2014). 이러한 구분 모델에 따라서 클라우드 서비스를 제대로 제공 및 관리하기 위한 역량이 필수적이므로 이를 강화하기 위하여 요구되는 지식과 기술을 정의하고, 역량확보를 위한 방안을 수립해야 한다. 역량 모델은 서비스 제공을 위한 전문적인 역량과 서비스 전반에 걸쳐 관리 및 운영을 수행하는 역량으로 구성되며, 각 영역별로 유사한 성격의 역량을 그룹으로 묶어 역량군(Cluster)을 정의한다(〈표 5〉 참조).

〈표 4〉 AMS 클라우드 기능 설계

AMS 클라우드 기능 설계	설명
공유서비스	• 기관 업무에 자원 공유풀을 이용한 인프라 서비스를 제공
서비스 요청과 제공	• 사용자는 웹 포탈을 통해 손쉽게 서비스를 요청 • 요청 후 1일 이내에 서비스를 제공
사용자 셀프 서비스	• 사용자 포탈을 통해 서비스를 요청 하고 사용하는 시스템을 모니터링 하고 관리
인프라 서비스 제공	• 표준 x86 서버를 기반으로 하는 가상화 자원 풀로 시작하여 인프라 서비스(IaaS), 플랫폼 서비스(PaaS)를 단계적으로 제공
서비스 프로비저닝 및 관리	• 초기에는 수작업으로 서비스를 제공하고 단계적으로 서비스 운영 관리를 자동화(Auto Provisioning 등)
공개 SW 적용	• WEB/WAS, DBMS 등 주요 SW를 공개 소프트웨어로 점진적으로 전환함으로써 비용 절감

〈표 5〉 역량군 정의

역량 구분	역량군	정의	관련 역량
서비스 관리 역량	서비스 기획	• 기관이 필요로 하는 Cloud 서비스를 발굴하여 적용 가능한 서비스 모델을 기획하거나 전환 계획을 기획하는 역량군	- 사업모델 기획 - 서비스 기획 - 기술 컨설팅 - Migration 관리
	서비스 설계	• 서비스 기획에서 수립된 서비스 모델을 고객에게 제공하기 위해구체적인 Cloud 서비스 구조를 설계하고 Cloud 서비스를 구축을 관리하는 역량군	- 서비스 카탈로그 설계 - 아키텍처 모델링 - 미터링/빌링 설계 - Cloud 구축
	서비스 운영	• 기관이 Cloud 서비스를 신청하고 사용 및 비용 정산을 위해 필요한 관리를 수행하는 역량군	- Cloud 관리 시스템 운영 - Cloud 고객 관리 - Event 관리
서비스 제공 역량	Cloud Server	• Cloud Server 서비스 제공을 위해가상서버, 시스템 SW 및 DC 기반설비에 대한 설계, 구현 및 관리를 수행하는 전문 기술적인 역량군	- 서버 가상화 관리 - 서버 관리 - 시스템 SW 관리 - DC 기반 설비 관리
	Cloud Storage	• Cloud Storage 서비스 제공을 위해스토리지에 대한 설계, 구현 및 관리를 수행하는 전문 기술적인 역량군	- 스토리지 관리
	Cloud DR	• Cloud DR 서비스 제공을 위해 DR 구축과 Back up 구현에 대한 설계, 구현 및 관리를 수행하는 전문 기술적인 역량군	- DR 관리 - Back up 관리
	Cloud Network	• Cloud Network 서비스 제공을 위해 Network 및 보안 관리에 대한 설계, 구현 및 관리를 수행하는 전문 기술적인 역량군	- NW 장비 관리 - NW 가상화 관리 - 보안 관리

이에, 각 영역별 현재 역량 수준 진단을 통해 기술 확보 여부 정도와 외부 지원가능 정도를 파악하여, 역량 확보를 위한 실행방안 유형을 분류하고 분류된 유형에 따른 실행계획 수립이 필요하다. 클라우드 자원과 서비스 운영을 위해서 기술지원 조직이 전제되어야 한다.

5. 클라우드 환경 보안 구축 방안

5.1 개요

클라우드 컴퓨팅의 보안은 크게 기술적 보안과 운영적 보안으로 분류한다. 주로 서비스 제공자와 관련된 기술적인 보안에는 인프라, 데이터, 스토리지, 통신이나 어플리케이션에 관련된 보안으로 구성된다. 반면 운영적 보안은 서비스 제공자와 이용자 모두와 관련된 보안으로 서비스 정책 수립이나 조직의 운영 방안, 자산 통제, 사고 관리, 서비스 연속성과 같은 요소들이 포함되어 있다. 클라우드 서비스 핵심 보안 위협 요소를 정리해보면 〈표 6〉과 같다(CSA, 2010). 우리는 아래 제시 된 위협요소들로부터 안전한 클라우드 서비스 환경의 시스템 구축 및 운영을 위한 기술적 보안 요소를 도출 및 방안을 제시한다.

클라우드의 물리적인 구성으로는 Sever, Strogage, Network로 나누고 가상화 구성으로는 서버 가상화 하이퍼바이저(Sever Virtualization Hypervisor)와 저장소 가상화(Storage Virtualization)와 네트워크 가상화(Network Virtualization), 서버 관리(Service Management), 자원관리(Resource Management), 프로비저닝(Provisioning), 모니터링(Monitoring)으로 나눈다. 클라우드 서비스 구성은 소프트웨어나 어플리케이션을 제공해주는 SaaS(Software as a Service), 어플리케이션 제작에 필요한 개발환경, SDK 등 플랫폼을 제공하는 PaaS(Platform as a Service), 서버, 스토리지, 네트워크, CPU, 메모리 등 각종 컴퓨팅 인프라 장비를 제공하는 IaaS(Infrastructure as a Service)로 나눈다.

클라우드 서버 가상화 하이퍼바이저는 소프트웨어로 물리 서버의 CPU와 디스크에 직접 상호작용을 하며, 가상서버의 운영체제를 위한 플랫폼 역할을 한다. 각각의 가상 서버들을 완전히 독립적으로 운용하고 게스트 서버는 자체 OS에서 운영되기 때문에 리눅스 기반 게스트와 윈도우 기반 게스트를 동시 운영할 수도 있다. 하이퍼 바이저는 물리 서버의 자원을 모니터링하여, 가상 서버에서 어플리케이션이 구동

〈표 6〉 클라우드 서비스의 보안 위협

보안위협	위협내용
가상화 취약점 상속	• 악성코드 감염 및 확산위협 • 서비스 가용성 침해
정보위탁에 따른 정보 유출의 위협	• 소유와 관리 분리에 따른 정보유출 • 내부자에 의한 정보유출
사용 단말의 다양성과 분실에 따른 정보유출	• 단말기 분실 등에 의한 정보유출
자원 공유 및 집중화에 따른 서비스 장애	• 시스템 장애 시 모든 고객의 서비스 중단 • 중앙시스템 노출 시 DDoS등의 공격대상이 되기 쉬움
분산 처리에 따른 보안적용의 어려움	• 자원공유와 가상머신 동적 재배치로 인증/접근제어 복잡도 상승 • 분산 컴퓨팅 시스템에 일괄적인 인증/접근제어 적용의 어려움
법규 및 규제의 문제	• 정보유출시 책임소재 불분명 • 자원공유에 따라 감사증적이 어려움

될 때, 물리 서버의 자원을 적절한 가상 서버에 할당하여 준다.

스토리지 가상화는 스토리지 시스템과 서버 사이에 소프트웨어 또는 하드웨어 계층을 추가함으로써, 어플리케이션 구동 시 데이터를 찾기 위해 특정 드라이브, 파티션, 또는 스토리지 하위 시스템을 인식하지 않아도 되므로, 가용성과 부분 중단(interruption)에도 안전하다. 또한 스토리지 용량의 자동 확장, 수동 프로비저닝의 수고를 덜어주고, 구동 중에도 어플리케이션 성능에 영향을 주지 않으면서 스토리지 자원의 업데이트가 가능하다.

네트워크 가상화란 기존 네트워크에 논리적인 구역을 만드는 것으로 네트워크에 있는 두 도메인을 물리적으로 연결하지 않고 터널을 만들어 두 도메인을 서로 연결하는 것으로서, 기존 물리적인 네트워크에 오버레이를 구축, 그 위에 새로운 네트워크를 구성한다. 사용자가 특정 터널을 활성화 가능하게 하며 프로비저닝 기능을 제공하고, 네트워크 가상화에는 호스트, 링크, 라우터, 스위치 가상화로 나눔. 클라우드 보안요소는 시스템 보안, 네트워크 보안, 데이터 보안, 어플리케이션 보안, 가상화 보안으로 구분한다.

본 연구에서는 클라우스 요소 방안을 시스템 보안, 네트워크 보안, 데이터 보안, 어플리케이션 보안, 가상화 보안 등 5가지로 나누었고 요소별 취약점에 대한 해결 방안을 제시한다.

5.2 시스템 보안

클라우드 서비스에서는 불특정 다수의 이용자가 가상화 기술로 구현된 IT 인프라를 통해 IT자원의 공유기능을 제공한다. 이때, 악성코드의 신속한 전파로 인한 감염 확산이나 하이퍼바이저에 대한 공격 등 새로운 보안 위협이 존재하게 된다. 특히, 가상화 시스템 장애 발생 시 신속한 시스템 복구를 위해 가상머신의 구동 이력을 이미지 형태로 저장・관리하기에 이미지 저장에 오류가 생길 경우, 전체 시스템의 완전한 복구가 어려울 수도 있는 치명적인 단점이 있다. 이용자의 서비스 가용성・지속성을 보장하기 위해서는 서비스를 이용하면서 생성된 이용자 데이터를 안전하게 저장・관리해야 한다. 따라서 이용자의 데이터가 손실되거나 위・변조되어 서비스 이용을 제한받지 않도록 무결성을 보장해야 한다. 또한, 시스템 자원을 통합・재분배하기 위해 구현된 가상화 시스템으로 악성 코드 감염이 확산되거나 물리자원에 동적으로 재배치되는 과정에서 발생할 수 있는 데이터의 손실 등에 대해 대책을 마련해야 한다. 서비스 제공자는 기본적으로 시스템 백신 패치를 통한 주기적인 점검, 데이터 무결성 확보 대책 등 다음과 같은 정보보호 고려사항을 기반으로 시스템 보안을 강화한다(〈표 7〉 참조).

클라우드 서비스 이용자의 IT 자원공유, 다양한 무선 단말기의 원격 접속 등이 보편화됨에 따라 기존IT 서비스 환경보다 보안성이 강화된 사용자 인증 및 접근 관리가 필요하다. 서비스 제공자는 IT 자원에 접근이 허가된 이용자만이 서비스에 접속할 수 있도록 보장해야 한다. 따라서 서비스 이용자의 제한된 영역에 대한 접근 시도와 같은 부적절한 행위에 대한 보안관제 방안 수립 필하다. 클라우드 서비스는 사용자의 자원에 대한 인증 및 접근 관리를 사용자 계정과 부여된 역할에 따라 접근 가능

〈표 7〉 시스템 보안

구분	고려사항
기본적 시스템 보안	• 시스템 유효성 점검을 위한 백신패치는 최신 버전으로 관리하고 주기적 실행 • 이용자 데이터의 무결성 보장을 위한 데이터 오류검사, 해시함수, 데이터 유효성 검사 등을 적용 • 사용되는 소프트웨어 및 데이터의 무결성을 주기적으로 점검하고, 필요에 따라 소프트웨어 등의 사용을 재설계 • 악용 가능한 잠재적 시스템 취약점 정보는 밝히지 않고 관련 취약점의 접근이 발생 할 경우, 오류메시지 생성 등을 통해 관리
가상화 시스템 보안	• 가상화 백신을 주기적으로 갱신하고 악성코드 확산 방지 대책을 마련 • 가상머신별 자원 사용량 제한하여 특정 가상머신의 자원이 남용되지 않도록 한다. • 디스크를 분할하여 호스트와 가상영역 간의 경계를 명확하게 한다. • 가상화 OS에 백신을 탑재하여 관리 • Host OS 및 하이퍼바이저를 모니터링하고 이력관리 • 가상화 실행 이력은 스탭샷 등 이미지 형태로 저장·관리하는 방안을 고려하고 안전한 저장방법을 통해 관리 • 가상화 OS의 내·외부 데이터 이용에 대한 로그 정보를 관리

〈표 8〉 접근보안

구분	고려사항
원격접속 관리 및 제한	• 서비스 연결을 승인하기 전에 모든 단말의 무선 접속은 정책에서 규정된 절차에 따라 인증하고, 접속로그를 관리하며 모니터링을 해야 한다. • 무선접속을 인증과 통신 세션의 기밀성·무결성을 보장하기 위해 암호 기술을 적용해야한다. • 내부정책에서 제한하는 모바일 단말의 통제 대책 마련
계정 분할 및 권한 최소화	• 서로 다른 이용자 계정의 충돌을 최소화하기 위하여 접근을 허용하는 영역이나 권한 등을 분리해야 한다. • 이용자의 신분 및 지불 방식을 기술적으로 검증하는 방안을 적용해야 한다. • 사용자에 부여하는 역할·권한을 최소한의 범위로 제한해야 한다. • 내부정책에서 규정한 계정관리 주기에 따라 점검하고, 시스템 이용자 변경사항은 즉시 정책에 반영해야 한다. • 이용자의 잘못된 로그인 시도가 규정된 횟수만큼 발생할 경우, 로그인을 제한한다. • 이용자 로그인이 성공적으로 수행되었을 경우, 지난 로그인 일시 및 관련 정보 공지를 고려해야한다.
사용자 세션 관리	• 서비스상의 최대 세션 수, 계정 지역, 유형 등을 고려하여 세션을 정의하여 관리 • 하나의 사용자가 동시에 여러 세션을 소유하는 것을 제한한다. • 내부정책에서 규정한 활성화 허용 시간을

하도록 관리·감독함. 또한 어플리케이션과 시스템에 대한 사용자의 접근 권한에 따른 적절한 통제를 수행한다. 이에, 서비스를 이용하는 단말기의 원격 접속 제한, 계정의 책임 분할 및 권한 최소화 등의 적절한 대책 필요하므로, 서비스 및 데이터 접근 인증 및 시스템 접근보안에 대한 보안 대책을 수립한다(〈표 8〉 참조).

서비스 및 데이터 접근 인증 방안 또한 필요하다. G-Cloud 환경과 국기행정시스템의 권한 인증인 GPKI, 생산 시스템인 온-나라 시스템 내 자체 접근권한에 대한 대책 등을 수립한다(〈표 9〉 참조).

〈표 9〉 서비스 및 데이터 접근 인증 방안

구분	인증 영역	내용 및 대책
1	권한관리체계	• GPKI, GOTP 등 인증관련 정보가 계정 및 권한관리에 연계되도록 구현
2	구간 암호화	• 구간 암호화 영역에서 웹서비스의 신뢰성 확보와 암호화 통신을 위한 SSL 적용
3	서비스 및 데이터 접근	• 기존 온-나라 시스템과 동일한 사용자 인증 방식으로 인증서 기반 및 일반계정 인증방식 제공
4	클라우드 공통기반을 활용한 사용자 인증	• 통합사용자 관리 DB내 권한 DB로 권한 관리를 하며 클라우드 내의 서비스는 해당 권한 DB를 조회하여 사용자의 업무 권한을 통제함(SSO)
5	온-나라 시스템 자체 접근권한	• 온-나라 시스템 내 자체 접근권한 관리에 따른 접근권한 통제
6	연계대상 접근통제	• 업무관리 시스템과 연계 시스템간의 상호 연계 시 GPKI 서버 인증서로 적용

5.3 네트워크 보안

클라우드 서비스에서는 서비스 이용자의 모든 정보와 이용자가 임대한 IT 자원이 인터넷 환경을 통해 제공되므로 보안이 강화된 네트워크 구축이 요구된다. 특히, 서비스 제공자는 지리적으로 분리된 다수의 데이터 처리 서버의 운영에 따른 안전한 데이터 송. 수신을 위한 통신 암호화를 적용하고, 네트워크 서비스 거부 공격(DoS) 등에 대한 대응 방안을 마련해야 한다. 또한, 공공용 클라우드 서비스와 사설용 클라우드 서비스는 네트워크 구성에 따라 상이한 보안위협을 갖기 때문에 서비스 환경에 따라 적절한 대응 방안이 필요하다. 따라서 네트워크 보안강화를 위해 정보보호 고려사항은 다음과 같다.

- 네트워크 트래픽 도청이나 데이터 유출 방지를 위해 통신 암호화
- 사용자의 네트워크 접속, 인증을 위한 신분확인 메커니즘 도입
- 네트워크 접속을 통한 데이터 송・수신에 대한 부인방지 대책 마련
- 네트워크 가용성이 침해하는 서비스거부 공격(DoS)에 대한 대책 마련
- 이기종 네트워크의 연동에 따른 보안
- 네트워크 장애에 대비하여 네트워크 분할 또는 이중화
- 네트워크 장애에 대비하여 보안관제 체계 구축

네트워크 보안 방안으로 접근제어 및 접근권한은 공유・협업 환경에 적합하도록 사람, 서비스, 데이터 요소를 고려하여 기준 정책 수립이 필요하며 이를 토대로 접근통제(NAC)의 네트워크 보안 기술 요소를 접목하여 기술요소 반영 방안 마련한다. 인증 영역에서 도출된 통합 인증 플랫폼 구축 시 접근제어, 접근권한에 대한 정책요소를 반영할 수 있도록 고려하여 정책 수립 필요하다. 접근통제와 같은 기술적 요소는 클라우드 환경에 적합한 기술과 솔루션에 대한 다각적인 검토 후 기술 요소 반영 방안 마련하고 서비스별 인증을 포함한 접근제어 및 접근권한 등 보안 기술 요소에 따른 전자정부 클라우드 통합 접근권한 관리시스템 구축한다(〈표 10〉 참조).

〈표 10〉 접근권한 관리시스템

기술요소	방안
접근제어	• 인증 환경 변화에 따른 접근권한 체계 수립 • 접근제어의 원칙 수립시 클라우드 환경을 고려한 요소 결정 • 신분기반 정책, 직무기반 정책, 규칙기반 정책을 포괄하는 접근제어 정책 수립
접근권한체계	• 서비스 , 사용자, 데이터 관점으로 분석 • 데이터의 경우 문서, 파일, 폴더 로 세분화 하여 정책 수립 • 문서의 경우 문서등급의 재검토 또는 수립 • 사용자의 경우 Action에 대한 체계화 및 경우의 수를 수렵하여 확장성 있도록 시스템 및 정책 설계 • 서비스의 경우 저장소와 관련된 환경을 고려한 설계
접근통제(NAC)	• 기존 접근 통제 방식 및 접근 통제의 구간 정의 • 각 구간별 기술요소 검토 및 파악 • 기술요소 검토에 따른 관련 솔루션 및 통제 기술의 클라우드 환경 적합성 파악

5.4 데이터 보안

이용자의 안정적 서비스 접속, 이용을 보장하기 위해 서비스 이용에 따라 생성된 이용자 데이터를 안전하게 저장 관리 한다. 이용자 데이터는 데이터의 기밀수준에 따라 암호화하여 안전하게 전송한 후 저장 관리하며 주기적으로 백업한다. 기밀 정도가 높은 중요 데이터는 암호화할 뿐만 아니라, 클라우드 서버를 통과하지 못하도록 쿼리문을 활용하거나 관련 클라우드 서버의 접근 로그 기록 등을 자동화함. 데이터베이스의 접근제어 및 암호화를 통한 보안 대책을 수립한다(〈표 11〉 참조).

Data 암호화 방안은 대칭키 또는 비대칭키를 이용해서 암・복호화를 수행해야 하는 경우 한국인터넷진흥원의『암 호이용안내서』에서 정의하고 있는 암호화 알고리즘과 안전성이 보장되는 암호키 길이를 사용한다. 복호화 되지 않는 암호화를 수행하기 위해 해시함수를 사용하는 경우 안전한 해시 알고리즘과 솔트값을 적용하여 암호화해야 한다(〈표 12〉 참조).

난수 생성시 안전한 난수 생성 알고리즘을 사용해야 한다. 국가정보원 "암호알고리즘 검증기준 V2.0" 또는 FIPS 140-2 인증을 받은 암호모듈의 난수생성기와 256비트 이상의 시드를 사용하여 난수를 생성한다. 난수의 무작위성을 보장하기 위해 이전 난수 생성 단계의 결과를 다음 난수생성 단계의 시드로 사용하는 의사난수 생성기를 이용한다.

〈표 11〉 DBMS 보안 적용 방안

구분	방안
계정관리	• DBA 권한은 일반 사용자 사용금지
접근통제	• 사용자가 DB 접속 시 DBA 통제 • 클라이언트 IP 및 포트 접근 제한 적용
개인정보 암호화	• 개인정보 데이터의 암호화 유틸리티를 이용한 암호화를 적용하여 정보유출 방지
취약점 패치	• DBMS 보안패치 적용하여 취약점 적용

〈표 12〉 암호화 방안

암호화	알고리즘	설명
단방향	SHA-256	• 개인정보에 대해 패스워드와 같이 암호화 후 복호화 하지 않아도 되는 데이터에 적용
양방향	SEED	• 개인정보에 대해 암호화하여 저장되며 복호화 되어 사용이 필요한 데이터에 적용

5.5 어플리케이션 보안

정보시스템 소프트웨어 개발보안 가이드, OWAS_TOP10, 홈페이지 개인정보 노출방지 가이드라인을 참고하여 작성한다. 취약점 점검을 통한 외부로의 시스템 노출을 피하고 문제점 분석을 통한 적절한 대응체계 수립으로 중요 데이터에 대한 손실을 예방하며 시스템에 대한 보안성 및 무결성을 강화한다(〈표 13〉 참조).

시큐어 코딩에 대한 점검은 정보시스템 구축, 운영 지침, 정보시스템 소프트웨어 개발보안 가이드(행정자치부), JAVA 시큐어 코딩 가이드(행정자치부)을 근거로 작성한다. 개발 과정에서 발생할 수 있는 코드 상의 보안적 취약점을 최소화하며 사전의 점검 조치로 운영 및 유지보수 측면의 효율성을 제고한다.

5.6 가상화 모니터링

가상화는 하드웨어 가상화, 스토리지 가상화, 네트워크 가상화가 있다. 하드웨어 가상화는 물리적인 서버의 효율적 사용을 위해서 하나의 서

〈표 13〉 점검 항목

항목	내용
인증우회	• 관리자 페이지 등 사용자 인증이 필요한 페이지가 인증을 거치지 않고 접근이 가능한지 점검
XSS	• 게시판 등을 통해 XSS 취약점이 가능한지를 검사함. 가능한 경우 다른 사용자의 세션정보가 노출되며, 이를 통하여 타 사용자의 권한으로 웹 서버에 접근하여 수행이 가능(Cookie-sniffing, Cookie-Spoofing으로 발전)한지 점검
Cookie-sniffing	• XSS를 이용하여 타인의 쿠키 값 및 세션 값을 확보할 수 있는 취약점 점검
Cookie-Spoofing	• XSS를 이용하여 타인의 쿠키 값/세션 값을 확보하여 그 사용자의 권한으로 웹 서버에 로그인 할 수 있는 취약점 점검
파일	• 웹 서버의 다운로드 스크립트를 이용하여 서버 시스템의 주요 파일(웹 소스 스크립트, 웹 서버 설정 파일 시스템 파일, 패스워드 파일 등)이 외부로 노출 될 수 있는지 점검
다운로드	• 웹 서버에 파일 업로드를 시킴으로써 외부에서 웹 서버에 명령을 내릴 수 있는 원인이 되는 취약점 점검
업로드	• 웹 서버와 공격자 혹은 타 사용자의 client 사이에서 패킷을 가로채어 내용을 변조함으로써 홈페이지 게시판의 위/변조, DB정보의 획득 등에 사용되는 취약점 점검
패킷 변조	• 패킷 변조의 한 형태로 웹 서버로 전송되는 패킷을 가로채어 웹 서버와 DB 서버간에 이루어지는 SQL 질의문을 원하는 형태로 조작함으로써 불법적으로 로그인 하거나 DB정보를 빼 내올 수 있는 취약점 점검
SQL Injection	• 관리자 페이지 등 사용자 인증이 필요한 페이지가 인증을 거치지 않고 접근이 가능한지 점검

버를 논리적으로 분할하여 여러 개의 서버처럼 만드는 기술이다. 이 기술의 목적은 관리의 유용성과 비용 절감에 있으며 분할된 서버는 자체적으로 운영 체제나 어플리케이션을 실행할 수 있으므로 물리적인 컴퓨터와 동일 기능을 수행한다고 볼 수 있다.

가상 머신은 소프트웨어로만 구성되어 있으므로 하드웨어 리소스와 분리되어 사용하지는 못 한다. 스토리지 가상화는 물리적인 저장 공간이나 논리적 저장 공간 안에 존재하면서 간소화된 논리적 스토리지 리소스 보기를 제공하는 추상계층이라 볼 수 있다. 정확한 의사 결정을 내리기 위해서 기업과 조직, 조직 내 사용자들은 엄청난 데이터를 사용하고 있고, 최근에는 클라우드 빅 데이터와 같은 이슈들도 주목받고 있기 때문에 데이터를 저장, 관리할 수 있는 스토리지의 운영이 무엇보다도 중요해지고 있다. 가상화된 IT 자원에 대해 사용량을 모니터링할 수 있는 툴을 제공하면, 툴에 의해 사용량을 항상 모니터링하고 사용량에 따라 유연하게 자원할당이 가능하다. 따라서 도입 PaaS 플랫폼인 OpenShift의 모니터링 기능을 활용한 컨테이너의 상태를 모니터링한다.

6. 결 론

본 연구는 기존의 RMS, AMS, CAMS를 국가기록 클라우드로 통합하기 위한 클라우드 시스템 목표 모델을 제시하였다. 또한 영구기록물관리시스템(AM, CAM)을 클라우드 환경으로 전환하기 위한 단계적인 방안을 제시 하였다. 영구기록관리시스템은 서울, 경남을 제외하고 아직까지 시스템 구축을 위한 진행을 하고 있지 않는 상황이다. 기록물에 대한 중요도는 높아지고 있고, 영구적으로 보존해야 될 가치가 있는 기록물들 또한 계속해서 생성되고 있다. 현재 영구기록관리 시스템이 지속이 된다면 언젠가는 기록물의 대량 이고 및 증가하는 이용자 수, 심화된 전자기록물의 복합성에 의해 수용할 수 없는 문제점이 발생할 수 있다. 이러한 관리의 복잡성 및 각각의 기관이 별도의 시스템을 운용하므로써 발생되는 자원 공유의 제약점, 같은 기능의 중복 개발에 따른 중복투자의 문제점들을 해결하기 위해서는 클라우드 컴퓨팅 방식이 반드시 필요하다고 판단을 하였다. 또한, 최근에는 현용, 준현용 시스템 즉, 온나라 시스템과 RMS가 클라우드 서비스로 전환되어 그 업무와 IT자원의 효율성이 입증이 되었으나, 아직까지 영구기록관리시스템(AMS, CAMS)은 비클라우드 방식으로 별도 운영이 되고 있어 통합적 개념의 기록관리 클라우드 플랫폼이 구현되어야 한다.

표준 영구기록관리시스템이란 개념은 사실 각 기관 및 지자체의 특색과 자유로운 정보의 활용측면에서 많은 제약이 있다. 강제적으로 모든 기관 및 지자체에서 중앙영구기록관리시스템의 프로세스를 똑같이 하는 것은 혁신적이고 다양성이 중요시 되는 요즘 시대에 여러가지 문제점이 도출될 수 있다. 본 연구의 시스템은 영구기록관리시스템 클라우드 전환 방안을 제시하였지만 SaaS 형태의 클라우드 시스템 기반으로 마이크로서비스 아키텍처 기술을 적용하여 다양한 기관의 입맛에 맞게 손쉬운 시스템 구축이 가능하기를 기대하면서 본 연구를 수행하였다. 영구기록관리시스템은 영구적으로 보존해

야 될 아주 가치 높은 기록물들을 이관받아 보존하는 중요한 시스템이다. 본 연구에서 제시한 클라우드 차세대 영구기록관리시스템을 통해 많은 기관에서도 기록물의 가치와 보존을 중요하게 여기고 더 나아가 세계적으로 전자기록물 관리의 선진성을 인정받을 수 있기를 바란다.

참 고 문 헌

국가기록원 (2017). 클라우드 기록관리시스템(RMS) 구축 완료보고서. 대전: 국가기록원.

이승억 (2015). 전자기록 관리정책 전환을 위한 재검토. 기록인, 32, 22-29.

이종운, 서경진, 김희웅 (2014). 클라우드 서비스 생태계 활성화 방안: 공급자와 사용자 관점 기반. Entrue Journal of Information Technology, 13(3), 73-88.

임진희 (2017). 전자기록관리시스템 재설계 모형. 기록인, 41, 22-29.

Cloud Security Alliance (2010). Top Threats to Cloud Computing V1.0. Seattle:Cloud Security Alliance.

Neil Beagrie, Andrew Charlesworth, Paul Miller (2014). Guidance on Cloud Storage and Digital Preservation: How Cloud Storage can address the needs of public archives in the UK. Surry: The National Archives.

• 국문 참고자료의 영어 표기
(English translation / romanization of references originally written in Korean)

Lee, Jong Un, Seo, Kyung Jin, & Kim, Hee Woong (2014). A systems Thinking Approach for the Success of Cloud Service Ecosystem Based on the Viewpoints of the Service Providers and Users. Entrue Journal of Information Technology, 13(3), 73-88.

Lee, Seung-eok (2017). A Rethink of electronic records management policies. Girokin(IN), 32, 22-29.

National Archives of Korea (2017). Implementation of Cloud Records Management System. Daejeon: National Archives.

Yim, Jin-Hee (2017). Electronic Records Management System Redesign Model. Girokin(IN), 41, 22-29.