# 전자기록의 진본 인증 요건 개발 연구

## A Study on Developing the Requirements for Authentication of Digital Records

**이경남** (Kyungnam Lee) | 한신대학교 대학원 기록관리학 강사 | coarchivist@gmail.com

목 차

1. 서론
2. 진본 인증의 개념
3. 진본 인증 요건 연구 설계
3.1 분석 자료
3.2 연구 방법 및 설계
4 진본 인증 요건 제안
4.1 기관 운영 인증 체계
4.2 기록 품질 인증 체계
4.3 보안 인증 체계
5. 결론

### 초 록

이 연구는 전자기록의 진본 인증과 관련한 자료의 내용을 분석하였던 2018년 연구의 후속 연구로서 전자기록의 진본 인증을 위한 프레임워크를 개발하고자 하였다. 이를 위해 인증 기준 관련 자료 분석 결과를 아카이브 기능 요소들과 매핑하고, 아카이브 기능 요소와 진본 인증 영역의 범주화를 통해 인증 요건들을 구성하였다.

이 연구에서 진본 인증 영역을 기관 운영 인증 요건, 기록 품질 인증 요건, 보안 인증 요건의 세 영역으로 제시하였으며, 각 영역별 세부 인증 영역과 인증 요건들을 제안하였다.

이 연구에서 제안한 인증 요건 초안은 진본 인증 표준의 개발과 정책 수립, 아카이브 시스템 설계 등에 활용할 수 있을 것이다.

* **키워드 :** 진본 확인, 진본 인증, 진본 인증 요건, 신뢰할 수 있는 디지털 아카이브

### ABSTRACT

This study is a follow-up of paper in 2018 that reviewed research papers related to the authentication of digital records.

The purpose of this study is to develop a framework for authentication. For this purpose, the result of an analysis of the relevant research papers were mapped with functional requirements of archival system. Next, the authentication requirements were derived from the categorizing these functional requirements and components of authentication.

As a result, this study proposed three domains of authentication: Organizational Requirements, Quality Requirements, and Security Requirements. Finally, the detailed requirements of each domain are suggested. The draft of authentication requirements proposed in this study can be used to develop authentication standards, establish policies, and design relevant systems.

* **Keywords : authentication, certification, requirements of authentication, trusted digital repository**

• 논문접수일 : 2020년 8월 21일 • 최초심사일 : 2020년 8월 22일 • 게재확정일: 2020년 9월 22일

## 1. 서론

기록의 진본성 확보는 전자기록 관리의 핵심이다. 기록에 증거로서의 가치를 부여하는 것은 기록이 생성된 당시의 그 기록으로 존재하는 것, 즉 진본성이기 때문이다. 전자기록은 생산 이후 유지 및 보존, 이용에 이르는 전 과정에서 끊임없이 재생산되기 때문에 진본임을 확인하고 인증하는 것이 중요하다. 그러므로 진본확인 전략과 정책을 수립하고, 전자기록관리시스템에 진본확인을 지원하는 도구가 반영되어야 한다. 이 과정은 아카이브의 보존전략체계 내에서 개발되고 설계되어야 할 것이다.

전자기록의 진본 인증을 지원하는 체계적인 프레임워크는 전자기록 관리 전반에서 정책 마련, 기관 운영, 시스템 요건 등의 전반을 아우르며 제시되어야 한다. 그러나 국내의 전자기록 진본 인증에 관한 요건 및 지원 도구에 관한 표준이나 정책적 제안은 미흡한 실정이다.

이 연구에서는 진본 인증에 관한 표준화된 요건을 제안하기 위해 진본 인증 기준에 참고할 수 있는 자료를 선정하고 분석 과정을 소개함으로써 표준 제안의 방법론을 제시하고자 하였다. 이와 함께 분석 결과로부터 도출한 진본성 확보 요소들을 토대로 진본 인증 요건의 초안을 제안하였다. 이 연구에서 제안된 진본 인증 요건 세트의 초안은 전자기록관리 체계 속에서 진본성 확보 정책 및 전략 시스템 개발의 기반으로 활용될 수 있을 것이다.

## 2. 진본 인증의 개념

기록이 진본임을 확인(authenticate)하는 것의 의미는 기록의 정체성을 확인한 후 기록이 표방하는 바 그대로의 객체임을 구두나 서면, 또는 인장을 첨부하여 선언한다는 것이다(IP2 Dictionary). 이 연장선에서 진본임이 확인된 기록(authenticated record)은 권한을 위임받은 법인이 특정 시점에 진본임을 선언한 기록으로 본다(IP2 Dictionary). 진본기록임을 확인하는 요건으로는 ISO15489에서 명시한 바와 같이, 그것이 생산된 취지와 일치하여 존재하는지, 그것을 생산하거나 보낸 것으로 되어 있는 그 사람에 의해 생산되거나 보내졌는지, 명시되어 있는 시간에 생산되거나 보내졌는지 증명되어야 함을 들 수 있다.

기록의 진본성은 정체성의 확인과 무결성의 입증으로 확보될 수 있다(IP2 Ontology). 다시 말해 진본 확인은 기록의 정체성과 무결성에 대한 정보를 확인하여 진본임을 판단하는 것으로 정의할 수 있다. 진본성의 판단은 일정 조건을 갖추었을 때 진본으로 추정할 수 있다는 진본 추정의 개념으로 사용되는데(기록학 용어 사전, 2008), 진본 추정(presumption of authenticity)은 기록의 생산부터 관리, 유지되는 방식에 관한 사실로부터 도출되며, 각 기준 요건을 충족하는 수와 정도에 따라 결정된다. 즉 충족하는 요건의 수가 많을수록, 요건을 충족시키는 정도가 클수록 진본성의 추정이 강해지는 것이다

(IP1, 2002a).

인증(authorization)이란, SAA에서는 어떠한 것에 조치를 취하거나 접근하기 위해 부여된 권리 및 허가로 정의하였다. 즉, 진본 인증은 기록의 진본 확인 절차를 거쳐 그 기록이 진본임을 공식적으로 증명한다는 의미를 갖는다. 진본사본은 법정에서 법적으로 채택될 수 있도록 구현하여 이러한 기능을 수행할 수 있도록 공식적으로 권한을 부여받은 인증된 사본이다(IP2 Dictionary).

기록의 컨텐츠에 중점을 두고 컨텐츠가 동일하면 동일한 기록이라 주장하는 것에 대해 듀란티는 "저장 위치와 관련한 메타데이터가 적어도 하나 이상 다를 수 있으므로 동일하다고 할 수 없다. 따라서 기록(의 컨텐츠)이 같아도 전송상태가 다르고, 다른 사본 혹은 다른 버전일 수 있다. 그러므로 문제는 어떤 것이 진본이냐가 아니라 어떤 것이 가장 권위 있는가의 문제이다"라고 지적 하였다(Corinne Rogers, 2015 재인용). 권위 있는 사본(authoritative copy)이란 생산자가 공식 기록으로 간주하는 사본으로, 일반적인 다른 사본에는 필요하지 않은 절차상의 통제가 적용되는 기록을 의미한다(IP2 Dictionary).

전자기록은 끊임없이 재생산 되는데 재생산 전의 원본과 재생산 후의 사본의 평가 확인을 거쳐 진본임을 인증해야 하며, 이 절차와 방법은 기록 생산, 관리, 보존 시스템 기능에 구현되어 있어야 한다.

논의를 정리해보면 진본 인증의 내용은 두 가지 범주로 나눌 수 있다. 첫 번째는 기관에 대한 인증이다. 믿을 수 있는 보관자에 중점을 두고, 이 신뢰할 수 있는 보관자가 보관한 기록은 진본이라 인정할 수 있도록 요건을 명시하는 것이다. 전자기록 관리 시스템에서 진본 인증 기능을 어떻게 구현할 것인가의 내용이다.

두 번째는 개별 기록의 진본 인증이다. 믿을 수 있는 보관자에 보관되지 않은 기록, 혹은 믿을 수 있는 보관자가 보관했더라도 개별 기록이 사용자에게 배포되거나 증빙자료 등으로 제출되어야 할 경우 재생산 된 사본이 진본인지를 인증하는 요건에 관한 내용이다.

한편 진본 인증 시점을 기준으로도 구분할 수 있다. 생산단계에서의 요건과 보존단계에서의 요건, 이관 시점의 요건, 배포 및 제출 시의 요건은 그 시점별로 인증 내용이 달라야 하므로 인증 시점을 구분하여 요건을 설계해야 한다.

이 연구에서는 위의 범주 가운데 첫 번째인 기관의 아카이브 체계 속에서 진본 인증을 위한 프레임워크를 설계하기 위한 인증 요건을 제안하고자 한다.

## 3. 진본 인증 요건 연구 설계

### 3.1 분석 자료

이 연구에서는 전자기록의 진본인증을 위해 표준화된 인증 요건의 초안을 제안하고자 한다. 이 연구에서 제안하는 진본 인증 요건은 일정한 요건을 갖춘 기관에서, 일정한 요건을 갖춘 시스템과 프로세스를 거쳐 생산되고 유지 보존된 기록은 진본으로 인정할 수 있다는 의미를 갖는다. 즉 이러한 요건을 갖추어 전략과 정책을 수립하고 기록의 품질을 유지할 수 있도록 방안을 마련하고 시스템 설계에 반영하고자 함이다.

이를 위해 국내외의 진본성 연구 성과를 검토하여 전자기록관리 프로세스와 아카이브 기능을 고려하여 인증 요건의 범위를 설정하고, 인증 요건을 3가지 범주로 구성하였다. 첫째는 기록 관리 기관을 신뢰할 수 있는 기관으로서 인증하기 위한 기록관리 기관 운영 측면의 기준을 명시하였다. 두 번째로는 기록의 품질 평가 기준을 제안하는 기록 품질 측면의 인증 기준을 제시하였고, 마지막으로 기록을 관리하는 시스템 보안 측면에서의 인증 체계를 제안하였다.

표준화된 진본 인증 요건을 제안하기 위해 검토한 연구는 신뢰할 수 있는 디지털 아카이브 인증에 관한 국제표준 ISO 16363과 국내 데이터인증센터에서 정보시스템 데이터 품질에 관한 심사 및 인증에 활용하고 있는 데이터 인증 기준(DQC-Management), 그리고 디지털 기록의 보존과 관련된 InterPARES의 연구결과물이다.

진본성 추정의 기준에 관한 자료로 InterPARES의 연구 결과인 '벤치마크' 요건과 '베이스라인' 요건이라 불리는 요건을 분석 대상으로 하였다. '벤치마크'요건의 본래 명칭은 Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records로서 기록이 진본임을 증명하거나 추정하기 위한 요건으로 기록이 보존 기관으로 보관권이 이전되기 전에 기록의 진본여부를 판단하기 위한 것이다. 기록관리시스템이 갖추어야 할 요건들로 볼 수 있다. 한편 '베이스라인' 요건은 Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records로 진본이라고 인정할 수 있는 품질의 사본 생산을 지원하는 요건으로, 기록의 보관권이 보존 기관으로 이동한 후의 믿을 수 있는 보관자로서의 관점에 기초한 요건이다. 또한 InterPARES의 연구 결과물 가운데 전자기록의 보존을 위한 전략 및 정책, 표준 개발을 위한 InterPARES 지적 프레임워크(Strategy Task Force Report) 및 정책 프레임워크(A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records), 생산자 가이드라인(Creator Guidelines), 보존자 가이드라인(Preservation Guideline), 진본성 확보를 위한 메타데이터인 InterPARES Authenticity Metadata(IPAM)을 분석하였다. 이들 연구의 특성과 주요 내용을 분석하여 진본 인증 요건의 자료로 활용하였다.[1)]

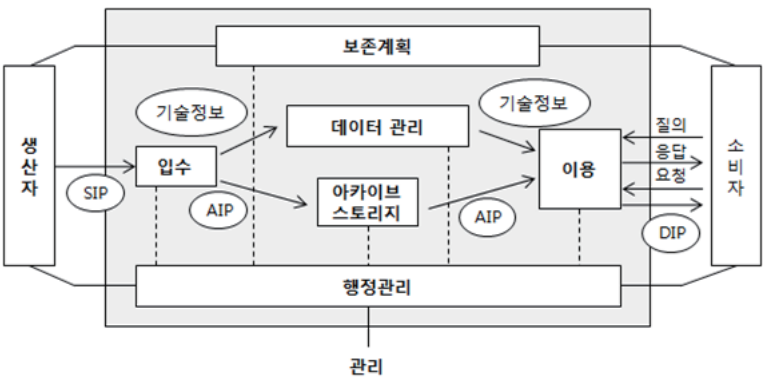
1) 이 연구들의 특성과 주요 내용의 분석 결과는 이경남 (2018). 전자기록의 진본인증 요건 선행 연구 분석. 기록과 정보·문화 연구, 7, 101-134.을 참고할 수 있다. 본 연구는 위 연구의 후속 연구로서 진행되었다.

### 3.2 연구 방법 및 설계

#### 3.2.1 연구 방법

위의 자료의 분석 결과를 토대로 아카이브의 보존전략 측면에서 진본 인증 요건을 제안하기 위해 3가지 범주를 설정하였다. 기관 운영 인증 요건(Organizational Requirement)과 기록 품질 인증 요건(Quality Requirement), 보안 인증 요건(Security Requirement)이 그것이다. 아카이브 기능 요소들과 진본 인증에 관한 선행 연구 분석 결과를 통해 기관 운영 및 기록 품질, 보안 인증 요건의 범주가 도출되었다.

인증 요건 분석을 위해 사용된 구조적 프레임워크는 국제표준 ISO 14721: Reference Model for an Open Archival Information System(OAIS)로서, 디지털 정보의 장기적 보존과 지속적 접근을 제공하기위한 디지털 아카이브의 구조와 기능을 정의한 OAIS 참조모형을 참고하였다. OAIS 참조모형은 다음 그림과 같이 디지털 아카이브의 기능을 입수, 저장, 데이터관리, 행정관리, 보존계획, 이용 기능으로 6개 엔티티로 정의하였다. 각각의 기능별로 세부 하위 기능을 두고 있다.




<그림 1> OAIS 기능모델
출처: CCSDS, 2012, OAIS, p.4-1

OAIS의 기준에 따라 아카이브의 기능 요건들을 세분화하고, 각각의 기능들이 진본 인증의 어느 범주와 관련되는 기능인지를 구분하고자 하였다. 이는 진본 인증의 범주별로 관련 기능들을 재구조화하고 인증 범위와의 상호 관계를 검증하기 위한 선행 작업의 의미를 갖는다.

먼저 기록의 생애주기에 따라 생산 기능과 OAIS 참조모형에서 정의한 디지털 아카이브의 6개 기능 엔티티를 기능 범주로 설정하고 하위의 세부 기능 요건들을 도출하였다. 다음으로 기관 운영, 기록 품질, 보안 인증의 세 가지 진본 인증 요건의 범주에 따라 [표1]과 같이 구분하였다.

<표 1> 아카이브 기능에 따른 진본 인증 요건 범주 1

| 기능 범주 | 세부 기능 요건 | 인증요건 범주 |
|---|---|---|
| 생산 | 기록 속성 표현 | QR |
| 이관 | 기탁물 접수 | QR |
| | 품질확인 | QR |
| | AIP 생성 | QR |
| | 기술정보 생성 | QR |
| | 객체 정보 업데이트 | QR |
| 저장 | 데이터 접수 | QR |
| | 저장 계층 관리 | QR |
| | 매체 변환 | QR |
| | 오류 확인 | QR |
| | 재난 복구 | QR |
| | 데이터 제공 | QR |
| 데이터관리 | 데이터베이스 관리 | QR |
| | 질의 수행 | QR |
| | 보고서 생산 | QR |
| | 데이터베이스 업데이트 수신 | QR |
| 행정관리 | 기탁협약 협의 | OR |
| | 시스템 환경 설정 | SR |
| | 기록관리 정보 관리 | QR |
| | 물리적 접근 통제 | QR |
| | 정책과 표준의 수립 | OR |
| | 기탁 감사 | QR |
| | 요청 활성화 | QR |
| | 이용자 서비스 | OR |
| 보존계획 | 지정공동체 모니터링 | OR |
| | 기술동향 모니터링 | QR |
| | 보존전략 표준 개발 | OR |
| | AIP 패키징 설계 | QR |
| 이용 | 이용 활동 조정 | QR |
| | DIP 생성 | QR |
| | 이용 요청 결과물 전달 | QR |

기관 운영 인증 요건(OR) 기준으로 분류된 항목들은 주로 행정관리 기능과 보존계획 기능에서 도출되었다. 행정관리에서는 기탁협약, 기록관리 정보 업데이트, 정책과 표준의 수립, 이용자 서비스의 기능이며, 보존계획에서는 지정공동체 모니터링과 보존 전략과 표준 개발 기능이다.

기록 품질 인증 요건(QR)은 생산, 이관, 저장, 데이터관리, 행정관리, 보존계획, 이용의 모든 기준 영역에서 추출되었다.

보안 인증 요건(SR)은 시스템 환경설정 기능이 포함된다.

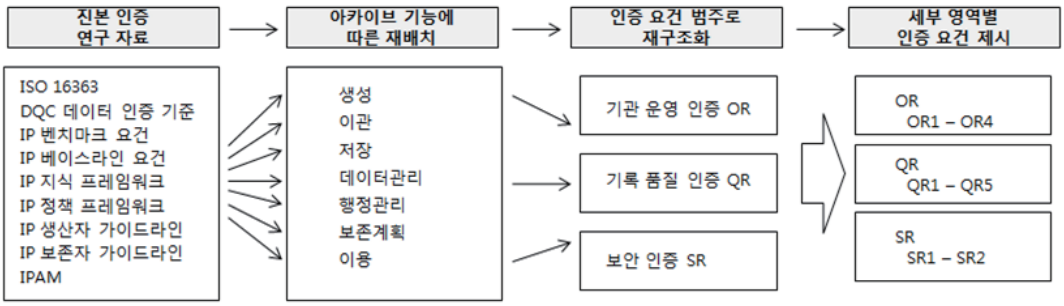
이 매핑 결과를 기반으로 각 범주별로 인증 요건을 제안하기 위해 인증 요건 범주에 따라 분리된 기준 영역들을 재구조화하여 각 범주별 세부 영역을 구성하였다. 즉 인증 요건 범주 별로 세부 영역을 설정하고 하위에 인증요건을 제시하는 구조로 설계하였다.

### 3.2.2 진본 인증 프레임워크

이 연구에서 제안하는 진본 인증 요건은 앞서 설명하였듯이 3가지 범주로 구성된다.

- 기관 운영 인증 요건(Organizational Requirement)
- 기록 품질 인증 요건(Quality Requirement)
- 보안 인증 요건(Security Requirement)

이 요건 범주를 도출하기 위해 [그림2] 와 같이 네 단계의 방법론을 거쳤다.




<그림 2> 진본 인증 요건 도출 방법

첫째, 진본 인증과 관련된 선행 연구 자료의 기준들을 OAIS 프레임워크를 기반으로 아카이브 기능 영역을 설정하고 7개의 기능영역에 따라 재배치하였다. 두 번째 단계로, OAIS 기능요건에 따라 분류된 기준들을 이 연구에서 제시한 3가지 범주로 재구조화 하였다. 세 번째 단계로 각 범주별로 세부 인증 영역을 설정하였다. 마지막 단계는 세부 인증 영역 하위에 인증 요건을 제안하였다.

각 범주별 영역은 다음과 같다.

첫째, 기관 운영 인증 요건이다.

<표 1>의 OAIS  기능 요건과 진본 인증 요건 매핑 분석 결과를 기반으로 4개 영역으로 구분하여 기관 운영 진본 인증 범위를 제안하였다.

- OR1. 조직 구조 및 관리
- OR2. 직원 역량
- OR3. 정책 및 표준 개발

- OR4. 이용자 관리

ISO 16363의 조직인프라 요건과 데이터 관리 인증(DQC) 요건을 분석하여 제시된 4개 범위별로 기관 운영 인증요건을 제안하였다. 단, DQC 관리 요건중 보안성 기준들은 이 연구에서 제안하는 보안 인증 요건에서 분석하였다. ISO 16363 표준과 DQC 인증 요건 분석 결과에서 진본성과 관련된 부분이 아닌 요건들은 기준에서 제외하였다.

두 번째, 기록 품질 인증 요건이다.

아카이브의 기능에 따라 생산, 이관, 저장, 데이터관리, 행정관리, 보존계획, 이용의 7개 기준 영역을 재구조화하여 진본 인증을 위한 기록 품질 인증 요건을 5개 영역의 기준과 하위의 인증 요건으로 제시하였다.

- QR1. 생산
- QR2. 입수
  - QR2.1 SIP 생성 및 접수
  - QR2.2 품질확인
  - QR2.3 AIP 생성 및 정보관리
- QR3. 저장
  - QR3.1 객체저장
  - QR3.2 매체교체
  - QR3.3 오류점검
  - QR3.4 재난복구
- QR4. 보존
  - QR4.1 지정공동체 모니터링
  - QR4.2 기술동향 모니터링
  - QR4.3 데이터 관리
  - QR4.4 감사
- QR5. 이용
  - QR5.1 접근통제
  - QR5.2 DIP 생성 및 제출

특히, 품질 인증 요건들은 요건을 확인하는 시기를 기록의 생애주기와 기능 범주를 고려하여 제시하였다.

셋째, 보안 인증 요건이다.

보안 관련 시스템 환경 설정과 관련하여 두 가지 영역으로 제안하였다.

- SR1. 시스템 보안 계획
- SR2. 위험 평가

<표 2> 아카이브 기능에 따른 진본 인증 요건 범주 2

| 범주 | 영역 | |
|---|---|---|
| OR. 기관 운영 | OR1. 조직 구조 및 관리 | |
| | OR2. 직원 역량 | |
| | OR3. 정책 및 표준 개발 | |
| | OR4. 이용자 관리 | |
| QR. 기록 품질 | QR1. 생산 | |
| | QR2. 입수 | |
| | | QR2.1 SIP 생성 및 접수 |
| | | QR2.2 품질확인 |
| | | QR2.3 AIP 생성 및 정보관리 |
| | QR3. 저장 | |
| | | QR3.1 객체저장 |
| | | QR3.2 매체교체 |
| | | QR3.3 오류점검 |
| | | QR3.4 재난복구 |
| | QR4. 보존 | |
| | | QR4.1 지정공동체 모니터링 |
| | | QR4.2 기술동향 모니터링 |
| | | QR4.3 데이터 관리 |
| | | QR4.4 감사 |
| | QR5. 이용 | |
| | | QR5.1 접근통제 |
| | | QR5.2 DIP 생성 및 제출 |
| SR. 보안 | SR1. 시스템 보안 계획 | |
| | SR2. 위험 평가 | |

이상의 진본 인증 요건의 구조를 표로 정리하면 다음과 같다.

모두 3개 범주의 11개 영역으로 구성하였고 각 영역에 진본 인증 요건을 제안하였다. 경우에 따라 하위 영역을 두고 그룹화 하기도 하였다.

## 4. 진본 인증 요건 제안

전자기록의 진본 인증 요건 체계를 기관 운영, 기록 품질, 보안의 3가지 범주로 구분하고, 범주별로 정의한 각 영역별 인증 요건을 다음과 같이 제안한다. 제안된 요건을 갖추어 관리된 기록은 진본으로

인정할 수 있다는 의미를 가지며, 진본 전자기록을 생산하고 유지하기 위해 다음의 조건을 기준으로 정책 및 설계 단계에서 활용할 수 있을 것이다.

### 4.1 기관 운영 인증 체계

신뢰할 수 있는 보관자로서의 기록관리 기관이 갖추어야 할 요건들을 기관 운영 인증 요건으로 제시하였다. 이 요건들은 ISO 16363과 데이터인증 제도의 데이터관리 인증 기준을 분석하여 도출하였다. 주로 아카이브 기관 차원에서의 관리와 운영에 관한 요건들로 구성하였다.

#### 4.1.1 조직 구조 및 관리

조직 구조 및 관리 요건은 조직의 전반적인 운영과 관련된 사명문이나 정책문이 존재하는지의 여부를 기준으로 둔다. ISO 16363의 인증기준을 주로 활용하였으며, 관련 기준은 다음과 같다.

<표 3> 조직 구조 및 관리 영역 진본인증 요건

| 범주 | OR 기관 운영 |
|---|---|
| 영역 | OR1 조직 구조 및 관리 |
| 인증 요건 | |
| OR1.1 | 디지털 아카이브가 소장 정보 자료의 수집과 관리, 장기 보존, 접근, 이용에 관련된 책무를 사명문으로 성문화 한다. |
| OR1.2 | 디지털 아카이브가 획득하여 관리해야 할 정보의 유형을 구체적으로 명시한 수집정책문을 마련한다. |
| OR1.3 | 디지털 아카이브가 소장 자료를 장기적으로 보유, 활용할 수 있는 보존 전략 계획을 수립한다. |

#### 4.1.2 직원 역량

직원 역량은 디지털 아카이브가 수행해야 할 책무를 확인하고 그 범위를 설정해야 하며, 이러한 책무를 수행하는데 적합한 직원을 임용하고 역량을 개발할 수 있도록 지원해야 한다는 기준들이 포함되어 있다. ISO 16363의 인증기준과 DQC-관리 인증 요건을 참고하였다.

<표 4> 직원 역량 영역 진본인증 요건

| 범주 | OR 기관 운영 |
|---|---|
| 영역 | OR2 직원 역량 |
| 인증 요건 | |
| OR2.1 | 디지털 아카이브가 수행해야 할 책무를 확인하고 그 기능별 범위를 설정한다. |
| OR2.2 | 기능별 영역별 업무 담당자를 지정하고 책임과 역할을 명시한다. |

### 4.1.3 정책 및 표준 개발

정책 및 표준 개발 기준은 디지털 아카이브의 사명에 부합하는 정책문과 이를 지원하는 표준과 관련된 요건들이다. ISO 16363와 DQC-관리 인증 요건의 정확성, 일관성, 적시성 기준을 재구성하였다.

<표 5> 정책 및 표준 개발 영역 진본인증 요건

| 범주 | OR 기관 운영 |
|---|---|
| 영역 | OR3 정책 및 표준 개발 |
| 인증 요건 | |
| OR3.1 | 디지털 아카이브의 수집정책문을 지원하는 수집 정책을 마련한다. 수집을 위한 계약 및 기탁협약에는 모든 필요한 보존 권한을 명시하고, 이전에 관한 내용을 분명히 한다. 또한 수집, 유지, 접근, 철회가 명시되어야 하며, 수집된 정보 객체의 책임이 적용되는 시점을 나타낸다. |
| OR3.2 | 디지털 아카이브의 보존 전략 계획을 지원하는 다존 정책이 있어야 하며 지속적인 검토 및 갱신, 개발 메커니즘을 포함한다. |
| OR3.3 | 디지털 아카이브의 장·단기 업무 계획 절차를 수립한다. |
| OR3.4 | 재정 운영의 투명성을 확보하고 법적 절차를 준수하 고 관련 표준과 실무에 부합하도록 제3자의 감사를 받는다. |
| OR3.5 | 재정적 위험 및 이익, 투자, 지출에 관한 분석 및 보고를 지속적으로 수행한다. |
| OR3.6 | 자산, 라이선스, 계약에 따른 컨텐츠 이용의 지적 재산권 및 제한을 추적하고 관리한다. |
| OR3.7 | 소유권 및 권리에 관한 법적 책임을 다루는 정책을 마련한다. |
| OR3.8 | 디지털 아카이브의 운영과 관리에 관한 절차 및 변화 이력을 기록화하여 설명책임성을 확보한다. |
| OR3.9 | 디지털 아카이브의 자체 평가와 외부 인증을 정기적으로 실시한다. |
| OR3.10 | 업무 규칙을 정의하고 관리하는 방법이 있으며 주기적으로 수행하여 보고한다. |
| OR3.11 | 데이터베이스 관리 절차를 정의하고 관리하며 성능 개전 절차와 방안을 마련한다. |
| OR3.12 | 데이터 흐름을 관리하는 도구와 방법을 정의하고 관리한다. |

### 4.1.4 이용자 관리

이용자 관리 기준은 지정공동체를 파악하고 이용자 요구사항의 관리와 대응을 수행하는 내용을 포함한다. ISO 16363과 DQC-관리 인증요건의 유용성과 접근성 부분을 고려하였다.

<표 6> 이용자 관리 영역 진본인증 요건

| 범주 | OR 기관 운영 |
|---|---|
| 영역 | OR4 이용자 관리 |
| 인증 요건 | |
| OR4.1 | 지정공동체를 정의하고 이와 관련된 지식 베이스를 갖추고 적절히 접근할 수 있어야 한다. |

### 4.2 기록 품질 인증 체계

기록 품질 인증 체계는 기록이 진본임을 인증 받을 수 있는 요건을 갖추도록 기록 품질에 대한 인증 내용으로 구성하였다. 기록 자체의 진본성을 평가하는 기준으로 기록의 생산부터 보존활동, 이용자 서비스로의 제출까지의 기록관리 활동 시점별로 인증 요건을 설정할 필요가 있다. 이 요건들은 주로 InterPARES 프로젝트의 결과물로부터 도출하였다. 또한 ISO 16363과 데이터 인증 제도의 DQC 품질 기준도 참고하였다.

제안한 인증 요건별 인증 시점을 생산, 입수, 저장, 매체교체, 정기점검, 보존, 이용의 7가지 유형으로 구분하여 제시하였다. 각 시점별로 인증 요건을 확인할 수 있으며, 이는 시스템 기능의 각 시점에 이러한 요건이 반영되어 설계될 수 있도록 활용할 수 있다.

#### 4.2.1 생산

기록 생산 영역은 기록이 생산될 때부터 고려해야 하는 요건들이 포함된다. 기록과 기록 속성은 분리되지 않도록 연계되어 있어야 한다. 이러한 속성에는 기록의 정체성과 무결성이 포함되며, 이를 보장하기 위한 방안이 마련되어 있어야 한다. 벤치마크 요건과 생산자 원칙, 생산자 가이드라인을 기반으로 요건을 구성하였다.

<표 7> 기록의 생산 영역 진본인증 요건

| 범주 | QR 기록 품질 | |
|---|---|---|
| 영역 | QR1 생산 | |
| 인증 요건 | | 인증 시점 |
| QR1.1 | 기능과 프로세스, 자원 명세를 갖춘 믿을 수 있는 기록생산시스템을 사용하여 기록을 생산한다. | 생산 |
| QR1.2 | 기록의 정체성을 표현하는 속성을 기록에 연계한다. | 생산 |
| QR1.3 | 기록의 무결성을 표현하는 속성을 기록에 연계한다. | 생산 |
| QR1.4 | 기록의 접근권한 및 지적재산권을 정의하여 실행한다. | 생산 |
| QR1.5 | 기록의 관리에 관한 속성을 정의하여 실행한다. | 생산 |

기록을 생산할 때부터 진본임을 증명하거나 추정하기 위해 고려해야 하는 요소로서 5개의 인증 요건을 정의하였다. 믿을 수 있는 기록생산시스템을 사용하여 기록을 생산할 것, 기록의 정체성과 무결성에 관한 속성 정보를 기록 생산 시에 반드시 기록과 연계하여 관리할 것을 제안하였다. 기록의 정체성 속성은 기록의 생산에 관계된 행위자의 정보와 관련 업무명, 그리고 생산일 및 기록관리 행위의 발생일, 분류코드나 파일 식별자 등의 기록의 결합관계 정보, 첨부기록의 지시자 등이 포함된다. 기록의 무결성 속성은 기록을 생산한 행위주체의 정보와 기록에 추가된 자료의 유형과 기술적인 수정여부의

정보를 나타낸다. 기록의 접근권한 및 개인정보보호, 지적재산권과 관련된 정보를 함께 관리해야 하며, 마지막으로 기록의 관리에 관한 정보가 정의되어 실행되어야 함을 포함하였다. 기록 생산 시부터 관련 업무와의 연계정보, 관련 기록과의 관계, 관리절차 및 방법, 보존기간 및 방법, 이용의 제한사항 등이 각 기록의 관리에 관한 속성으로 정의되어 있어야 함을 제안하였다.

이 5개 인증 요건은 모두 기록의 생산 시에 충족되어야 하는 기준들이다.

### 4.2.2 입수

기록 입수 영역은 기록 생산자가 이관대상을 선정하고 이를 입수 기능으로 보낸다. 인수한 기록들을 품질확인 절차를 거쳐 보존포맷 변환 및 데이터 변환을 수행하며 AIP를 생성하고 AIP의 기술정보를 업데이트하여 아카이브의 데이터 관리 기능으로 보내져 정보를 연계시킨다.

입수 기능의 이러한 과정은 3개의 하위 기능으로 구분하였다. SIP의 생성 및 접수기능과 품질확인, 그리고 AIP 생성 및 정보관리 기능으로 나누어 인증 기준을  모두 11개의 세부 요건으로 제안하였다.

<표 8> 이관 및 입수 영역 진본인증 요건

| 범주 | | QR 기록 품질 | |
|---|---|---|---|
| 영역 | | QR2 입수 | |
| 인증 요건 | | | 인증 시점 |
| QR2.1 | | SIP 생성 및 접수 | |
| | QR2.1.1 | 이관 대상 객체 정보와 정보 속성을 식별하고 기록화한다. | 입수 |
| | QR2.1.2 | 이관 시점에서 연계되어야 할 특정 컨텐츠 정보를 명시한다. | 입수 |
| | QR2.1.3 | SIP 생성 절차와 해석을 위한 명세서를 작성한다. | 입수 |
| | QR2.1.4 | 보존 대상 객체를 보존할 수 있는 통제권을 확보한다. | 입수 |
| | QR2.1.5 | 이관 과정을 기록화한다. | 입수 |
| QR2.2 | | 품질확인 | |
| | QR2.2.1 | 입수 대상의 정체성을 검증하는 메커니즘을 갖는다. | 입수 |
| | QR2.2.2 | 이관 대상의 완전성과 정확성을 검증한다. | 입수 |
| QR2.3 | | AIP 생성 및 정보관리 | |
| | QR2.3.1 | AIP를 해석하고 장기간 보존에 적합한 AIP 정의를 갖는다. | 입수 |
| | QR2.3.2 | SIP로부터 AIP를 구성하는 방식을 기술하며, SIP가 AIP로 통합되지 않거나 폐기되는 경우의 절차와 이유를 기록화한다. | 입수 |
| | QR2.3.3 | AIP를 고유하게 식별할 수 있도록 하며, 이를 검색할 수 있도록 한다. | 입수 |
| | QR2.3.4 | AIP의 완전성 및 생성시점의 정확성을 확인한다. | 입수 |

SIP 생성 및 접수는 생산자가 아카이브 시스템으로 이관할 때의 요건이다. 이관할 기관이 인수할 기관과 협의하여 이관 대상을 확정하고, 이관 대상 객체정보와 정보 속성을 확인하여 기록화한다. 이관 시점에서 특정 객체와 연계되어야 할 정보를 명확히 명시하며, SIP에 관한 명세서를 갖고 있어야 한다. 또한 보존 대상 객체를 보존하는데 요구되는 통제권의 이전도 확보해야 한다. 이 모든 이관 과정을 기록화하는 방안이 마련되어야 한다. 이 모든 요건은 입수 과정에서 확인되어야 한다.

품질확인 기능은 이관된 객체의 품질을 확인하는 기능이다. 인수 기관은 입수 대상의 생산자 정보를 검증하여 기록의 정체성을 확보해야 하며, SIP의 완전성과 정확성을 검증해야 한다. 이 두 가지도 입수 시점의 요건이다.

인수 기관은 보존에 적합한 포맷으로 SIP를 AIP로 변환해야 한다. 각각의 AIP를 해석하고 장기간 보존하는데 적합한 AIP 정의를 가짐으로써 이러한 AIP의 모든 구성요소를 식별하고 해석할 수 있어야 한다. SIP로부터 AIP로 변환하는 방식을 설명해야 하며, SIP가 AIP로 통합되지 않거나 폐기되는 경우 이 과정에 대한 절차가 존재해야하며, 이를 기록화하여 SIP의 최종 처분을 문서화해야 한다. 마지막으로 AIP를 지속적으로 고유하게 식별할 수 있는 규칙을 갖고 사용해야 하며, 물리적 위치에 관계없이 고유하게 식별된 객체를 검색할 수 있어야 한다. 또한 AIP의 완전성과 생성시점의 정확성을 확인해야 한다. 이러한 요건들은 입수 과정에서 확인되어야 한다.

### 4.2.3 저장

저장 영역은 AIP의 저장과 유지, 관리 기능을 수행한다. AIP를 저장하고, 저장 매체를 주기적으로 새로운 매체로 교체하며, 오류를 점검하고 재난복구 기능을 포함한다. 이러한 기능을 '객체 저장', '매체교체', '오류점검', '재난복구' 4개의 하위 기능으로 구분하여 인증 요건을 제시하였다.

<표 9> 저장 영역 진본인증 요건

| 범주 | | QR 기록 품질 | |
|---|---|---|---|
| 영역 | | QR3 저장 | |
| 인증 요건 | | | 인증 시점 |
| QR3.1 | | 객체 저장 | |
| | QR3.1.1 | 각각의 객체를 식별하기 위한 도구와 방법을 마련한다. | 저장 |
| | QR3.1.2 | 각각의 객체를 지정공동체가 이해할 수 있도록 하는 표현정보를 제공하기 위한 도구와 방법이 있어야 하며, 표현정보는 객체와 지속적으로 연결되도록 한다. | 저장 |
| | QR3.1.3 | 내용정보의 보존기술정보는 성문화된 절차에 따라 획득되어야 하며, 지속적으로 연결되도록 한다. | 저장 |
| | QR3.1.4 | AIP가 비트단위까지 저장되는 방법에 관한 명세서를 작성한다. | 저장 |
| | QR3.1.5 | AIP의 저장 및 보존 활동을 기록화한다. | 저장 |

| 인증 요건 | | | 인증 시점 |
|---|---|---|---|
| | QR3.1.6 | 적합한 저장 방법과 저장매체를 사용하여 저장소를 유지한다. | 저장 |
| QR3.2 | | 매체교체 | |
| | QR3.2.1 | 하드웨어 기술 변화가 필요할 때를 감정하여 통지하고, 교체를 실행하는 절차를 갖는다. | 매체교체 |
| | QR3.2.2 | 소프트웨어 기술 변화가 필요할 때를 감정하여 통지하고, 교체를 실행하는 절차를 갖는다. | 매체교체 |
| | QR3.2.3 | 주기적으로 새로운 저장 매체에 기록을 이전하는 계획을 실시한다. | 매체교체 |
| | QR3.2.4 | 저장 매체 및 하드웨어 변경 프로세스를 정의한다. | 매체교체 |
| | QR3.2.5 | 이용가능성을 고려하여 파일 포맷을 선택한다. | 매체교체 |
| QR3.3 | | 오류점검 | |
| | QR3.3.1 | AIP가 손상되지 않았음을 주기적으로 확인하고 증명한다. | 정기점검 |
| | QR3.3.2 | 하드웨어와 소프트웨어의 오류를 주기적으로 확인한다. | 정기점검 |
| QR3.4 | | 재난복구 | |
| | QR3.4.1 | 손상이나 손실 감지를 위한 방법을 갖추고 있어야 하며, 이를 기록하고, 복구 및 교체 메커니즘을 갖는다. | 저장 |
| | QR3.4.2 | 주기적인 백업과 물리적으로 분리된 시설로 사본을 중복 소장한다. | 저장 |

객체 저장은 AIP를 저장소에서 입수하여 저장하는 과정으로 AIP의 식별정보를 함께 저장하도록 해야 하며, 객체를 지정공동체가 활용할 수 있도록 랜더링 하는 표현정보를 제공하는 방식을 정하고 이러한 표현정보와 객체의 연결을 유지해야 한다.

한편 AIP의 저장 과정에 관한 기준을 제시함에 있어 AIP의 구조에 대한 이해가 필요하다. OAIS의 정의에 따르면 AIP는 정보객체 집합으로서 컨테이너로 이해된다. AIP는 내용정보(Content Information)와 이 내용정보를 해석하는데 필요한 보존기술정보(Preservation Description Information)가 포함되어 있다. 이 AIP는 패키징 정보(Package Description)로 구별되고 식별되며, 구조화된 기술정보인 패키지 기술(Package Description)로 이용자가 정보를 찾고 분석하고 이용을 요청하게 된다.

이러한 정의에 따라 내용정보의 보존기술정보를 획득하기 위한 절차는 문서화되어 있어야 하며, 이렇게 획득된 보존기술정보의 연결은 지속되어야 한다.

또한 AIP의 저장과 관련하여 비트단위까지 저장되는 방법에 관한 명세서를 마련해야 하며, AIP의 저장과 보존에 대한 모든 활동을 기록화 하여야 함을 기준을 제안하였다. 그리고 적합한 저장 방식과 매체를 사용하여 저장해야 한다.

객체저장과 관련된 6개의 기준은 아카이브에 객체가 저장되는 과정에서 인증이 이루어져야 한다.

매체교체는 시간의 경과에 따라 변화가 필요한 시점에 적절한 매체로 이전하는 과정에 관련된 기준들을 제시하였다. 하드웨어 및 소프트웨어의 교체, 새로운 매체로의 마이그레이션 등이 정해진 절차

에 따라 이루어져야 하며, 이용가능성을 고려하여 보존 매체를 선택하는 기준을 제안하였다. 매체교체 시 위의 기준들이 인증되어야 한다.

오류점검은 저장된 AIP를 주기적으로 확인하여 손상 여부를 증명하고, 하드웨어 및 소프트웨어의 운영에 관련된 오류도 확인하도록 하였다. 역시 저장 과정에서 인증되어야 하는 기준들이다.

재난복구는 위험관리 사항으로서 손상 및 손실 감지에 관한 사항, 백업 및 사본 저장의 기준을 마련해야 함을 제시하였으며 인증 시점은 저장 시로 구분하였다.

### 4.2.4 보존

보존 기능은 저장된 객체를 아카이브에서 이용할 수 있도록 접근을 보장하고 서비스를 제공할 수 있도록 아카이브의 보존 객체를 관리하고 이용자 집단의 요구사항을 확인하며, 새로운 기술 환경의 변화를 분석하고 이를 아카이브 운영에 반영하는 기능 등을 포함한다. 이 과정을 '지정공동체 모니터링', '기술동향 모니터링', '데이터 관리', '감사' 4가지 기능을 세분화하여 인증기준을 제시하였다.

<표 10> 보존 영역 진본인증 요건

| 범주 | | QR 기록 품질 | |
|---|---|---|---|
| 영역 | | QR4 보존 | |
| | | 인증 요건 | 인증 시점 |
| QR4.1 | | 지정공동체 모니터링 | |
| | QR4.1.1 | 지정공동체가 객체에 접근하고 확인하는데 필요한 최소한의 기술 정보 요건을 명시한다. | 보존 |
| | QR4.1.2 | 지정공동체의 서비스 요구사항을 모니터링 한다. | 보존 |
| QR4.2 | | 기술동향 모니터링 | |
| | QR4.2.1 | 기술 감시 및 기술 동향 모니터링 시스템을 갖추고 있다. | 보존 |
| | QR4.2.2 | 새로운 기술에 대한 평가 결과를 보존 계획에 반영하는 절차를 갖추고 있다. | 보존 |
| QR4.3 | | 데이터 관리 | |
| | QR4.3.1 | 객체의 모든 변화에 대한 정보를 포함한 기술 정보를 갖는다. | 보존 |
| | QR4.3.2 | 기술 정보와 시스템 정보를 포함하는 데이터베이스의 관리로 무결성을 유지한다. | 보존 |
| | QR4.3.3 | 시스템과 데이터베이스의 상태를 업데이트하고 결과를 보고하는 메커니즘을 갖는다. | 보존 |
| | QR4.3.4 | 모든 디지털 구성요소를 확인하고 주기적인 진본성 평가를 실시하여 그 결과를 기록화한다. | 보존 |
| | QR4.3.5 | 디지털 객체의 수와 위치를 관리한다. | 보존 |
| | QR4.3.6 | 보유 사본을 동기화하는 메커니즘을 갖는다. | 보존 |
| QR4.4 | | 감사 | |
| | QR4.4.1 | 아카이브의 보존 환경을 모니터링하고 결과를 보존 계획에 반영한다. | 보존 |

지정공동체 모니터링은 이용자들이 장기간 아카이브 소장 객체에 접근하고 확인할 수 있도록 기술 정보 요건을 명시하여 관리하도록 기준을 제안하였다. 또한 서비스 요구사항을 확인하여 이를 정책 및 절차에 반영해야 한다.

기술동향 모니터링은 새로운 기술을 감지하고 이러한 기술의 아카이브 적용 가능성을 검토하여 보존 계획에 반영하는 절차를 수립하는 기준을 제시하였다.

데이터 관리는 보존하고 있는 객체의 모든 변화에 대한 이력 정보를 포함한 기술 정보를 관리해야 할 것과 무결성 보장을 위해 데이터베이스를 관리하고, 시스템과 데이터베이스의 상태 업데이트와 결과를 보고하는 기능을 갖추어야 한다. 또한 모든 디지털 구성요소를 확인하여 주기적으로 진본성 평가를 실시하며, 소장 객체의 수와 위치를 관리해야 함을 제안하였다.

감사 기능은 아카이브의 보존 환경의 전반적 점검과 그 결과를 보고하는 기능을 갖추어야 한다.

보존 영역의 인증 요건은 모두 보존 과정에서 확인하여 인증해야 하는 요건들이다.

### 4.2.5 이용

이용은 아카이브에 저장된 객체에 접근하여 이용할 수 있는지를 확인하는 과정과 이용자가 이용대상 객체를 요청하고, 아카이브에서 이용자에게 객체를 제출하는 기능이다. 이 과정에서 '접근통제'와 'DIP 생성 및 제출', 두 가지 기준을 충족해야 함을 제안하였다.

접근통제는 기관의 접근정책에 따라 이용자 접근 기능을 갖추어야 하며, 권한 밖의 행위로부터 저장된 객체를 보호하고, 비정상적인 접근 발생 시 이를 기록하고 확인해야 하는 기준을 제안하였다.

<표 11> 이용 영역 진본인증 요건

| 범주 | | QR 기록 품질 | |
|---|---|---|---|
| 영역 | | QR5 이용 | |
| 인증 요건 | | | 인증 시점 |
| QR5.1 | | 접근통제 | |
| | QR5.1.1 | 접근 정책을 준수한다. | 이용 |
| | QR5.1.2 | 허가받지 않은 행위로부터 저장 객체를 보호해야 하며, 접근 관리 실패 및 이상상황을 기록하고 검토한다. | 이용 |
| QR5.2 | | DIP 생성 및 제출 | |
| | QR5.2.1 | 이용자를 식별하고 요청된 객체의 전송 절차를 결정한다. | 이용 |
| | QR5.2.2 | DIP 생성 절차와 방식에 관한 명세서를 작성한다. | 이용 |
| | QR5.2.3 | DIP를 이용자에게 제출(전달)하는 성문화된 방식이 있다. | 이용 |

DIP 생성 및 제출은 이용자가 요청한 객체를 다포정보패키지(Dissemination Information Package)로 하여 이용자에게 제출하는 기능이다. 이 과정에서 이용자를 식별하고 요청된 전송 절차를 확인하는 기준을 제안하였다. DIP 생성 절차와 방식에 관한 명세서를 갖추어야 하며, DIP를 제출(전달)하는 방식에 대해서도 문서화되어 있어야 함을 기준으로 삼았다.

이용관련 인증 요건들은 이용 시점에서 확인되어야 한다.

### 4.3 보안 인증 체계

보안 인증 요건은 정보시스템의 중요 정보를 보호하고 처리하는 메커니즘을 제공하는 요건들로 인증 요건을 구성하였다.

#### 4.3.1 시스템 보안 계획

시스템 보안 계획은 시스템 보안 계획 및 유지 계획을 수립하고 시행하는 기준으로 3개의 인증 요건을 제시하였다. 이 계획에는 보안의 목적과 범위를 나타내며 책임을 구체적으로 명시하며, 시스템의 유지와 지원, 대체 자원 등이 포함되어 있어야 한다. 또한 직원의 역할과 책무를 이행하는 권한을 명시하고, 변경사항의 실행에 관련된 권한 사항을 관리해야 한다.

<표 12> 시스템 보안 계획 영역 진본인증 요건

| 범주 | SR 보안 인증 |
|---|---|
| 영역 | SR1 시스템 보안 계획 |
| 인증 요건 | |
| SR1.1 | 시스템 보안 계획을 수립한다. |
| SR1.2 | 시스템 유지 전략을 수립한다. |
| SR1.3 | 직원의 권한을 명시하고 관리한다. |

#### 4.3.2 위험 평가

위험평가는 아카이브의 운영에 관련된 위험 요인을 분석하고 대응하는 기준들로 3개의 인증 요건을 제안하였다.

<표 13> 위험 평가 영역 진본인증 요건

| 범주 | SR 보안 인증 |
|---|---|
| 영역 | SR1 위험 평가 |
| 인증 요건 | |
| SR3.1 | 보안 위험 요인을 분석하고 대응방안을 마련한다. |
| SR3.2 | 위험 및 이익 평가를 실시하고 그 결과에 따라 보안업데이트를 실시한다. |
| SR3.3 | 자체평가와 외부 인증을 정기적으로 실행한다. |

시스템, 데이터, 인력, 설비와 관련된 보안 위험 요인을 분석하고 보안 위험 요인별 대응방안에 따라 통제를 실시해야 한다. 위험 및 이익 평가를 실시하고 보안 업데이트를 실행해야 한다. 주기적인 자체 평가와 외부 인증을 실시해야 함을 제안하였다.

## 5. 결론

이 연구는 진본성에 관한 문헌 분석을 기반으로 진본인증을 위한 표준화된 요건을 제시함으로써 각 기관에서 정책수립, 아카이브 구성, 시스템 설계 등에 반영하여 활용할 수 있도록 하였다. 제안된 진본 인증 요건은 기관 운영 측면, 기록 품질 측면, 시스템 보안 측면으로 세분화하였으며, 기록관리의 프로세스에서 확인해야 하는 요건들로 구성하였다. 그러나 이 연구에서 초안 형식으로 제시한 요건들은 표준화된 형식으로 고도화 할 필요가 있다.

또한 진본 인증 요건의 연구 범위를 전자기록으로만 한정하여 다양한 디지털 객체의 진본인증 방안을 포괄하지 못한 한계를 갖는다. 그리고 아카이브 체계에서 포괄하지 않은 개별 기록의 인증 방식도 다루지 못하였다. 이와 관련한 후속 연구를 통해 범디지털 자료의 진본 인증 프레임워크 설계 연구가 지속되어야 할 것이다.

## 참고문헌

이경남 (2018). 전자기록의 진본인증 요건 선행 연구 분석. 기록과 정보·문화 연구, 7, 101-134.

이윤주, 이소연 (2009). 진본 전자기록의 장기보존을 위한 정책프레임워크. 기록학연구, 19, 193-232.

한국기록학회 (2008). 기록학 용어 사전. 서울: 역사비평사.

한국데이터산업진흥원 (2020). 데이터인증. 검색일자: 2020.08.31. http://www.dqc.or.kr

CCSDS (2012). Reference Model for An Open Archival Information System (OAIS). CCSDS 650.0-M-2. Magenta Book.

Corinne Rogers (2015). Virtual Authenticity: Authenticity of digital records from theory to practice. UBC doctoral thesis.

InterPARES 1 Project Authenticity Task Force (2002a). InterPARES 1 Book: Appendix 2- Requirements for Assessing and Maintaining the Authenticity of Electronic Records.

InterPARES 1 Project Strategy Task Force (2002b). Strategy Task Force Report.

InterPARES 2 Project Policy Cross-domain (2008a). A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records.

InterPARES 2 Project Dictionary, version 2020.5.

InterPARES 2 Project (2008b). InterPARES 2 Report Book: Appendix 14 - Chain of Preservation Model Diagrams and Definitions.

InterPARES 2 Project (2008c). InterPARES 2 Report Book: Appendix 20 - Creator Guidelines - Making and Maintaining Digital Materials: Guidelines for Individuals.

InterPARES 2 Project (2008d). InterPARES 2 Report Book: Appendix 21 - Preserver Guidelines - Preserving Digital Records: Guidelines for Organizations.

InterPARES 3 Project (2016). General Study 15- Application Profile for Authenticity Metadata: General Study Report.

OCLC (2007). Trustworthy Repositories Audit and Certification: Criteria and Checklist.

**국한문 참고문헌의 영문 표기**

(English translation / Romanization of reference originally written in Korean)

Korea Data Agency (2020). Data Certified. Retrieved August 31, 2020, from http://www.dqc.or.kr

Korea Society of Archival Studies (2008). Dictionary of records and archival terminology. Seoul: Yuksabipyongsa.

Lee, Kyung-nam (2018). A Literaturea Review on Requirements for Authentication of Digital Records. The Korean Journal of Archival, Information and Cultural Studies, 7, 101-134.

Lee, Yoon-ju & Lee, So-yeon (2009). A Policy Framework for the Long-term Preservation of Authentic Digital Records: Based on InterPARES Studies. The Korean Journal of Archival Studies, 19, 193-232.