기록정보의 안전한 보호와 접근통제에 관한 인식과 과제*

The Awareness and the Challenges about Protection and Access Control of Record

임미현 (Mi-Hyun Lim)**
임진희 (Jin-Hee Yim)***

초 록

4차산업 혁명으로 상징되는 IT 기술의 발달과 전자정부의 등장 및 환경의 변화 등에 따라 기록관리 영역에도 급격한 변화가 나타나고 있다. 대부분의 정부산하 공공기관은 전자문서시스템과 기록관리시스템, 온나라시스템 등 정보보호의 대상이 되는 정보시스템을 이용한다. 이용자중심의 기록관리 환경에서 물리적 환경과 전자시스템을 통한 기록정보의 접근통제는 기록정보의 보호를 위한 필수적인 요소라고 할 수 있다. 이에 본 연구는 공공기관 기록물관리 전문요원들의 기록정보의 안전한 보호와 접근통제에 대한 인식을 조사하여 개선해야 할 과제를 도출하고, 이를 개선하기 위한 논의와 제안점을 제시하였다. 먼저, 우리나라 정보보호 체계에 대한 법・제도 현황을 살펴보고, 접근통제에 대한 규정을 분석하여 기록관리 법・제도 및 접근통제 현황과 비교함으로써 시사점을 도출한다. 다음으로 질적연구 방법을 활용하여 정부산하 공공기관에서 근무하고 있는 전문요원들을 대상으로 심층인터뷰를 진행하였고, 그 결과를 분석하였다. 본 연구는 기록정보의 안전한 보호와 접근통제를 위하여 기록관리 영역의 체계 개편 등을 제안하여 정부산하 공공기관 기록관리의 개선과 전문요원들이 실질적인 권한과 통제권을 가지기 위한 제안을 통하여 기록관리 내실화를 꾀하였다는데 의의가 있다.

ABSTRACT

The development of IT technology that has come to symbolize the fourth industrial revolution, the introduction of online government, and the change in environment has caused radical changes in record management. Most public institutions under the government make use of information systems that are objects of information protection such as electronic document system, document management system, and Onnara system. Further, protection and access control of record information through physical environment and electronic system in a user-centered record management environment is an essential component. Hence, this study studies how professional records management professionals in public institutions recognize safe protection and access management of record information, deriving areas that require improvement and providing a discussion and suggestions to bring about such improvement. This study starts by examining laws and policies on information protection in Korea, analyzing items on access control to compare them with laws and policies, as well as the current situation on records management and derive implications. This study is meaningful in that it aims to substantialize records management by suggesting areas of improvement necessary for the protection and management of record information in public institutions and providing professionals with tangible authority and control.

키워드: 기록정보, 기록정보의 보호, 접근통제, 접근권한, 인식제고, 심층인터뷰, 질적연구
record information, protection of record information, access control, access rights, raised awareness, in-depth interview, qualitative research

---

* 본 논문은 임미현의 박사학위논문 「기록정보의 안전한 보호와 접근통제에 관한 인식과 과제」(2021) 내용 일부를 수정・보완한 것임.

** 명지대학교 기록정보과학전문대학원 기록정보학 박사(bluebear-8318@hanmail.net) (제1저자)
*** 명지대학교 기록정보과학전문대학원 기록관리전공 조교수(yimjhkr@mju.ac.kr) (교신저자)

■ 논문접수일자 : 2021년 2월 24일 ■ 최초심사일자 : 2021년 3월 11일 ■ 게재확정일자 : 2021년 3월 19일
■ 정보관리학회지, 38(1), 191-219, 2021. http://dx.doi.org/10.3743/KOSIM.2021.38.1.191

1. 서 론

1.1 연구배경 및 필요성

4차 산업혁명으로 상징되는 IT 기술의 발달과 전자정부의 등장 및 전자적 환경으로의 변화 등에 따라 기록관리 영역도 급격한 변화가 나타나고 있다. 보존가치에 중점을 두고 기록관으로 이관되어 관리되던 기록물관리에서도 새로운 기술과 정보시스템의 보편화, 이용자 중심 기록관리 환경으로의 변화에 따라 새로운 이슈들이 등장했다.

기록관리의 측면에서도 과거 물리적인 환경에서는 기록관에 보관된 기록에 대하여 출입의 통제와 허가된 사용자만 기록에 접근할 수 있게 제어함으로써 기록과 사용자 모두를 통제하여 기록을 보호할 수 있었다. 기록을 물리적으로 보존하던 과거에는 서고의 출입문을 단속하고 기록이 보관된 공간에 대해 비인가자의 접근을 인위적으로 제어함으로써 기록과 이용자 모두를 비교적 쉽게 통제할 수 있었다. 또한, 기록의 이용이 허가된 이용자가 기록을 열람할 경우에도 일정한 권한을 가진 관리자가 이용자의 접근과 이용여부를 확인하는 절차를 거치게 함으로써 허가된 사람만이 기록을 이용할 수 있었다(천권주, 2008).

그러나 정보시스템의 활용이 보편화된 요즘, 기록정보의 안전한 보호를 위해서는 외부에서의 침입 등 해킹과 같은 불법적인 접근을 차단해야 하고, 사람에 의하여 정보가 유출되는 것을 방지하여야 한다.

이처럼 기록정보의 보호를 위해서는 물리적 환경의 구성과 함께 전자시스템을 통한 기록정보에 대한 보호와 접근통제가 기록관리에 필수적인 요소이다. 그러나 실제 기관 내에서의 업무과정을 살펴보면, 종이기록은 생산부서에서 생산・활용・보관 되다가 기록관으로 이관되었을 때 기록물관리 전문요원이 기록정보를 접할 수 있다. 또한 전자기록은 표준 RMS로 이관되어도 전자문서시스템 내부에 있는 기록정보를 삭제하지 않고 계속 활용하고 있어, 기록물관리 전문요원들에게 기록정보를 관리할 수 있는 실질적인 권한이 없다. 따라서 정부산하 공공기관에 근무하고 있는 기록물관리 전문요원을 대상으로 기록정보의 보호와 접근통제에 관하여 어떻게 인식하고 있는지, 실제 얼마나 관련 업무에 관여하고 있는지 등 현황에 대하여 알아볼 필요가 있다.

본 연구에서는 우리나라 정보보호 체계와 접근통제에 대한 규정 및 제도를 살펴보고, 기록관리 영역에서의 접근통제에 대한 규정을 살펴봄으로써 시사점을 도출한다. 또한 정부산하 공공기관에 근무하고 있는 기록물관리 전문요원을 대상으로 심층인터뷰를 통하여 기록정보의 접근통제와 기록관리 현황에 대한 인식을 조사하였다. 심층인터뷰 자료를 분석하여 해결해야 할 과제를 도출하고, 향후 우리나라 기록관리에서 기록정보의 보호와 접근통제를 위한 개선방안과 제안점을 제시하고자 한다.

1.2 연구목적 및 연구질문 설정

정보보호는 정보통신망을 대상으로 하며 정보보호의 대상이 되는 정보통신망에는 전자문서시스템과 기록관리시스템, 온나라시스템 등 대부분의 문서관리시스템이 포함된다. 공공기

관이 보유한 기록정보의 보호와 접근통제는 기록관이 보안, 감사, 개인정보를 담당하는 부서와 같이 협업을 통하여 수행해야 할 업무영역 중 하나이다. 따라서 실제 공공기관에 근무하는 기록물관리 전문요원을 대상으로 기록정보에 대한 접근통제에 대하여 전문요원의 업무인지 여부와 개입의 정도, 협업이 잘 이루어지고 있는지 등에 대한 인식을 통해 앞으로 수행해야 할 과제를 도출하는데 그 목적이 있다.

본 연구에서는 문헌연구를 통하여 우리나라 정보보호 체계에서의 접근통제와 기록관리 체계에서의 접근통제에 대하여 살펴보고, 그 내용과 연구자의 경험을 바탕으로 정부산하 공공기관 기록물관리 전문요원들의 인식을 조사하고자 한다. 앞으로 수행할 과제를 도출하기 위하여 기록정보의 보호를 위한 시스템과 프로세스, 전문요원들의 대응, 기록정보에 대한 접근통제 정책결정에 대한 인식개선이 필요한 사항으로 연구질문을 구성하였다. 구체적인 질문은 다음과 같다.

〈연구질문〉

(1) 기록정보의 보호를 위하여 정부산하 공공기관은 접근권한에 관한 내부 시스템 및 프로세스가 설정되어 있는가?

(2) 기록정보의 보호를 위하여 정부산하 공공기관의 전문요원(기록관)들은 내부직원에 접근권한 설정에 관한 정보를 제공하고 있는가?

(3) 기록정보의 접근통제 관련 정책결정에 대하여 정부산하 공공기관 전문요원들은 어떻게 인식하고 있는가?

(4) 기록정보의 보호와 접근통제를 위하여 개선되어야 할 사항은 무엇인가?

연구질문을 토대로 정부산하 공공기관의 기록물관리 전문요원의 심층인터뷰를 진행하였고, 인터뷰 결과를 토대로 정부산하 공공기관의 기록관리 개선을 위한 과제와 기록관리 체계 개편을 위한 제안점을 제시하였다.

본 연구를 통해 연구자는 공공기관 기록물관리 전문요원들의 인식의 차이를 발견하고 이해하고자 했으며, 전문요원들이 앞으로 수행해야 할 과제를 도출하고, 이 과정에서 전문요원들이 느끼는 애로사항을 충분히 담고자 하였다.

1.3 연구의 설계 및 공헌

본 연구는 연구참여자들이 그들의 관점에서 기관이 보유한 기록정보에 대한 접근통제에 대하여 관련 업무에 개입 여부, 개입 정도, 관련 부서와 협업이 잘 이루어지고 있는지에 대한 인식조사를 통하여 앞으로 수행해야 할 과제를 도출하는 것을 연구목적으로 설정하였다. 연구목적에 따라 정보보호와 기록관리에서의 접근통제에 관한 내용과 연구자가 실제 현장에서 경험한 내용을 바탕으로 연구질문을 구성하였다.

연구질문과 관련된 기존 연구가 미비하고 이론이 정립되어 있지 않으므로, 가설없이 출발하는 탐험적 연구가 필요하다고 판단했다. 따라서 연구질문을 설정하고, 질문에 대한 연구참여자의 인식을 이끌어내기 위하여 질적 연구가 적합하다고 판단하였다.

질적연구 방법이란 수치적 방법 이외의 방법으로 현상을 해석하고, 분석하고, 설명하는 다양한 방법론을 의미한다(임도빈, 2009). 질적연구는 매우 다양하고 다중적인 방법론을 포괄하는 것으로 비교적 덜 알려진 영역에서의 사

회적 실체와 현상이 어떻게 해석・이해되고 경험되거나 생성되는가에 관심을 두기 때문에 무엇보다도 연구대상의 사회적 맥락에 큰 관심을 갖는다. 질적연구 방법에는 사례연구, 문화기술적 방법, 근거이론, 행위연구, 현상학적 연구, 해석학 등이 있다.

다음으로 연구목적에 따른 연구대상을 선택하였다. 본 연구는 정부산하 공공기관에서 근무하는 기록물관리 전문요원의 관점에서의 인식조사를 목적으로 한다. 따라서 연구자[1]가 속한 커뮤니티를 통해 오랜 시간 교류해온 정부산하 공공기관 기록물관리 전문요원들을 대상으로 선정하였다. 그밖에 타 지역의 정부산하 공공기관 기록물 관리 전문요원도 일부 포함하였다. 정부산하 공공기관에 근무하는 기록물관리전문요원들을 대상으로 심층인터뷰를 진행하면서 자료가 포화될 때까지 지속적으로 수집하였다.

질적연구에서 연구의 타당성과 신뢰도를 확보하는 것은 중요한 문제이다. 본 연구에서는 타당도 기법들 중 참여자의 렌즈를 이용하였다. 한석실(2010)은 '연구 참여자 렌즈'는 질적 연구의 현상학적 패러다임에서 객관적 실체는 존재하지 않으며, 실제란 사회적으로 생성된 것이며, 더욱이 연구참여자가 '어떻다'라고 지각하는 것이라고 가정한다. 따라서 연구에서 연구참여자가 인식하고 있는 실제가 연구에서 얼마나 정확하게 기술되고 설명되고 있는지를 확인하는 것은 연구자가 타당하게 이루어졌는지를 확인할 수 있는 하나의 방법이 될 수 있다고 보는 것이다. 또한, 연구참여자들의 신분 노출을 막고 정보를 보호해주는 기밀성을 유지하는 것이 질적연구 윤리성 확보의 핵심이라고 할 수 있다. 본 연구의 인터뷰 참여자들은 모두 정부산하 공공기관에 근무하는 직원들이기 때문에 몇몇 인터뷰 참여자들은 신분노출에 대한 걱정을 드러내며, 상세한 내용을 밝혀도 되는지 고민하는 것을 경험할 수 있었다. 따라서 인터뷰 시작 전, 인터뷰 참여자의 실명과 기관명을 노출시키지 않겠다는 내용을 담은 『연구참여 동의서』를 참여자에 확인하고 서명을 받았으며, 참여자의 보호를 위한 조치로써 각각 코드를 부여하여 익명성을 추구하였다.

연구의 결과는 외부에서 알 수 없었던 정부산하 공공기관의 실제 기록관리 현황을 드러내어 향후, 정부산하 공공기관 기록관리 정책수립 등에 도움을 줄 수 있다. 실제 현장에서 느끼는 문제점과 개선점의 제안을 통하여 향후 기록관리 업무 내실화에 기여할 수 있다. 마지막으로 기록물관리 전문요원들이 기관 내 기록정보의 보호와 접근통제가 기록관리에 필수적인 요소임을 인식하여, 이를 위한 정책결정 및 집행에 적극적으로 참여하도록 변화하는데 기여할 수 있다.

---

1) 연구자는 기록물관리 전문요원 자격을 취득하고, 정보보안을 주로 담당하는 정부산하 공공기관에 8년째 근무하고 있으며, 그동안 기록관리를 위한 기록관리 규칙 및 분류체계 수립, 표준 RMS 도입 등 기본 인프라를 구축하였다. 연구자는 기록물관리 전문요원으로 근무하면서 기록정보의 체계적인 관리를 통하여 보호할 정보와 활용할 수 있는 정보를 확실히 구분할 필요가 있으며, 보호대상이 아닌 활용 가능한 정보는 적극적으로 제공해야 한다는 생각을 가지고 있다. 따라서 각 기관이 보유하고 있는 각종 기록정보 중 보호가 필요한 기록정보에는 적절한 접근통제가 이루어져야 하며, 그 밖의 기록정보에 대하여는 활발한 활용기반을 마련하는 것이 중요하다고 생각한다.

2 선행연구 및 이론적 배경

2.1 선행연구

본 연구는 기록정보의 안전한 보호와 접근통제가 이루어질 수 있도록 공공기관의 기록물관리 전문요원의 인식을 조사하고 과제를 도출하는데 목적이 있다. 따라서 정보보호 체계의 접근통제 관련 연구와 기록학에서 접근통제 관련 연구로 나누어 살펴보고자 한다.

전통적인 접근통제 기술의 개념과 국제표준의 핵심내용을 분석하여 일목요연하게 정리하여 제시한 것으로 김의탁, 최용락, 김기현, 박정호(1998)의 접근통제 기술동향 연구가 있다. 이 연구에서 접근통제는 컴퓨팅 자원, 통신자원 및 정보자원 등에 대하여 허가되지 않은 접근을 방어하는 것으로 각 자원에 대한 기밀성, 무결성, 사용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하는 것이며, 권한부여를 위한 수단이라고 주장한다.

정보에 대한 접근통제를 다룬 연구에는 역할기반 접근통제(RBAC) 모델을 적용한 연구들이 있다. 양성훈, 오정현, 이경효, 임도연, 오병균(2005)은 역할기반 접근통제(RBAC) 모델을 적용할 때 접근권한의 상속성 관계에 의해 하위역할에 할당된 사용자의 모든 접근권한은 상위역할에 할당된 사용자의 접근권한에 상속됨으로써 권한의 집중이 발생함을 지적하고, 역할기반 접근통제(RBAC) 모델을 기반으로 특정 계층내에서 역할의 주체와 객체에 보안등급을 부여함으로써 접근권한의 상속성과 정보흐름을 통제할 수 있는 모델을 제안하였다. 또한 다단계 보안시스템에서 효율적으로 접근을 통제할 수 있는 방법을 제안하여 접근을 통제하는 모델개발의 연구를 제시하였다. 엄정호, 박선호, 정태명(2010)은 내부자에 의한 정보유출의 심각성을 지적하고, 내부자에 대한 침입차단 및 탐지, 오용차단을 위하여 역할기반 접근통제(RBAC) 모델과 상황인식 역할기반 접근제어(C-RBAC) 모델을 제시하고 있으며, 이주영, 이구연, 권호열(2020)은 내부자에 의한 정보 유출사고는 내부 직원들이 자신들이 가진 정보 접근 권한을 남용하여 잘못 사용한 사례이며 이를 예방하고, 유출시 빠른 대응을 위해서 물리적・기술적・관리적 측면에서 지속적인 대책연구가 필요함을 지적하고 있다. 또한 문서관리시스템, DRM(Digital Rights Management), DLP(Data Loss Prevention) 등 보안솔루션과 내부 정보유출 탐지기법을 분석하여 시나리오를 설계하여 내부자 정보유출 탐지방안을 제시하고 있다.

그밖에도 심재윤, 이경호(2015)의 금융IT인력의 보안사고 위험도에 기반한 정보접근 통제 연구, 최은복(2009)의 비밀성과 무결성을 보장하는 격자개념의 역할그래프 보안모델 등 정보보호를 위한 접근통제와 관련하여 다양한 연구가 있다.

기록관리 분야에서 접근통제 영역에 관한 연구는 천권주(2008)의 ERMS 표준에 나타난 접근통제 요건의 적용방안에 관한 연구와 용마루(2016)의 기록관리시스템의 접근통제기능 개선방향 연구가 있다. 천권주(2008)는 영국, 유럽연합, 호주 및 미국의 전자기록관리시스템(ERMS) 기능요건을 문헌조사 방법을 이용하여 분석, 비교하여 표준 접근통제 기능요건을 제안하였다. 이 연구는 접근통제 영역을 중심으로 실행방안

을 제시한 것에 의의가 있다. 용마루(2016)는 국내 사용 중인 표준 기록관리시스템(RMS)의 접근통제 기능과 국내에서 사용 중인 기록관리 시스템 기능요건을 통하여 접근통제 기능의 개선사항을 제안하고 있다. 기록관리 측면에서 국제표준의 접근통제에 관한 사항을 분석하고, 해외 패키지 시스템의 접근통제 프로세스를 분석하여 국내 표준 RMS의 개선사항을 제안하는데 의의가 있다.

그 외에 기록관리 분야에서의 접근통제는 전자기록관리시스템과 표준 기록관리시스템의 기능분석을 통한 요건도출과 시스템 설계 등을 제시하는 연구가 있으며, 시스템 영역 중 일부분으로 다루고 있다. 이소연, 김자경(2004)은 전자기록관리시스템(ERMS) 설계표준의 기능요건 분석' 연구에서 기록관리 국제표준인 ISO 15489를 기록관리 기능영역별(획득, 등록, 분류, 저장, 접근, 추적, 처분 등 7가지 영역)로 분석하여 기록관리 원칙을 추출하고 미국, 영국, 유럽연합의 전자기록관리시스템 설계 표준과 비교・분석함으로써 공통적인 시스템요건을 규명하였다. 김용(2007)은 전자기록관리시스템 구축에 있어 요구되는 기본적인 요구사항을 포함하여 유관시스템과의 호환성, 보안이슈 및 백업방안 등을 중점적으로 다룸으로써 기록관리를 둘러싼 환경변화에 대비한 기능적 요구사항과 시스템 구조를 제안하였다. 손성근(2008)은 호주의 기록연속체 개념을 바탕으로 분석 틀을 도출하고, 무결성과 진본성을 유지하며 기록관리 서비스를 제공하기 위한 방안을 모색 하였으며, '접근통제 및 감사추적'에 대한 분석결과로 보안, 메타데이터, 감사증적 기능보다도 기록물에 대한 접근 기능에 대한 불만족과 기록물 접근에 대한 과도한 허용 또는 제한이 없는지, 이로 인해 업무 활용 또는 보존에 어려움이 없는지 살펴봐야 한다고 지적하고 있다. 박민영(2013)은 표준기록관리시스템 기능 평가 중에서 접근관리 기능에 대해 국내외 기능요건 및 표준에서 최소한의 필수항목을 추출하고, 이를 바탕으로 접근관리의 기능을 제대로 구현했는지 평가했으며, 평가결과 접근관리 기능이 대부분 제대로 사용되고 있지 않음과 명확한 규정, 기록관리시스템 정비, 시스템 기능개선 등 개선이 필요한 사항들을 지적하였다. 김형주, 김수현(2017)은 정부산하 공공기관을 위한 범용 기록관리시스템이 없는 상황에서 기타 공공기관으로 분류되는 국방품질원의 기록관리시스템 구축 사례를 중심으로 기능요건을 도출하고, 적용방안을 제안하면서 '분류체계 및 기록관리기준의 통제' 영역에서 접근권한에 대한 적용 정도를 다루고 있다. 이정은, 윤은하(2018)는 ISO 15489 개정판의 주요 특징에 관한 연구에서 정보보호의 목표인 보안성, 무결성, 가용성을 받아들여 기록시스템의 품질요건에 보안성을 추가하였고, 기록통제 항목을 새롭게 제시하고 있다. 오진관(2019)은 기록관리시스템 설계모형과 기능요건 연구에서 접근영역에 대하여 기록관리시스템을 접근할 수 있는 모든 사용자가 기록을 검색활용 할 수 있는 기록서비스, 기록관리시스템의 접근권한을 통제하는 접근권한 관리 서비스로 구성하여 제시하고 있다.

기록관리 분야에서 접근통제에 관한 선행연구는 대부분 기록관리시스템 기능요건의 하나로 제시되고 있다. 접근통제가 적절하게 이루어지기 위해서는 잘 설계된 기록관리시스템 구축이 필수요소임은 부인할 수 없는 사실이다. 개

정된 ISO 15489가 정보보호의 목표인 보안성, 무결성, 가용성을 받아들여 기록시스템[2]의 품질요건에 보안성을 추가한 것처럼(이정은, 윤은하, 2018) 기록정보의 접근통제와 관련하여 기록관리시스템 외에 정보시스템과 다른 요소를 포괄하는 정보보호 개념에서의 접근통제가 논의될 필요가 있다.

2.2 접근통제 관련 이론적 배경

정보보호와 관련하여 「국가정보화 기본법」[3]은 "정보보호란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적 기술적 수단을 마련하는 것을 말한다."라고 정의하고 있으며, 「정보보호산업 진흥에 관한 법률」[4]에서는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것, 암호・인증・인식・감시 등의 보안기술을 활용하여 재난・재해・범죄 등에 대응하거나 관련 장비・시설을 안전하게 운영하기 위한 관리적・기술적・물리적 수단을 마련하는 것으로 정의하여 국가정보화기본법과 유사하게 '정보보호'의 개념을 정의하고 있다.

정보보호에서는 보호해야 할 대상을 선별하고 구분하는 것이 가장 중요하다. 보호해야 할 가치가 있는 대상은 컴퓨터 하드웨어뿐만 아니라 정보를 사용하는데 필요한 자산으로 소프트웨어, 하드웨어, 데이터, 인적요소, 문서, 네트워크 등이 있다.

정보보호 측면에서 접근이란 주체와 객체 사이의 정보의 흐름으로서, 사용자가 파일이나 데이터베이스 내의 정보를 읽거나 쓰거나 실행하는 등의 모든 활동을 의미한다. 다음으로 통제는 조직의 목표가 달성될 것이며, 바람직하지 못한 사건들이 예방, 적발 및 교정될 것이라는 합리적인 수준의 보증을 제공하기 위하여 설계된 정책, 절차, 실무관행과 조직구조 등을 의미한다. 따라서 접근통제는 정보보호 체계의 항목 중 하나로 외부에서 접근하는 사람, 시스템 등의 주체와 보안상의 노출, 위협, 변조 등과 같은 객체의 제반환경을 보호하기 위한 보안대책을 의미한다. 즉, 접근통제란 정보보호 체계의 항목 중 하나로 외부에서 접근하는 사람, 시스템 등 주체와 보안상의 노출, 위협, 변조 등과 같은 객체, 제반환경을 보호하기 위한 보안대책을 의미한다(장상수, 2019). 접근통제의 절차는 식별

2) 기록시스템: 장기간에 걸쳐 기록을 획득, 관리 및 접근을 제공하는 정보시스템을 의미함(ISO 15489:2016). 기록시스템은 소프트웨어와 같은 기술적 요소와 기술 외적인 요소(방침, 절차, 사람 및 기타 행위주체 그리고 부여받은 책임을 포함)로 구성될 수 있다.

3) 「국가정보화 기본법」 제2조(정의) 제1항 제6호 "정보보호"란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적・기술적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.

4) 「정보보호산업의 진흥에 관한 법률」 제2조(정의) 제1항 제1호 "정보보호"란 다음 각 목의 활동을 위한 관리적・기술적・물리적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.

가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것.

나. 암호・인증・인식・감시 등의 보안기술을 활용하여 재난・재해・범죄 등에 대응하거나 관련 장비・시설을 안전하게 운영하는 것.

(Identification), 인증(Authentication), 인가(Authorization) 등 3단계로 구성된다(〈표 1〉 참조).

ISO/IEC 27001의 요구사항 중 접근통제는 접근통제 정책을 수립하여 정보 및 정보처리 시설에 대한 접근을 제한하고, 사용자 접근관리를 통하여 시스템과 서비스에 인가된 사용자의 접근을 보장하고 있으며, 비인가된 접근을 금지하는 것을 목적으로 한다. 또한 사용자에게 자신의 인증정보를 보호할 책임을 부과하고 시스템과 애플리케이션에 대한 비인가 접근의 방지를 목적으로 한다. 접근통제는 주체가 객체에 접근 시 직무분리와 최소권한의 원칙이 요구된다. 직무분리란 업무의 발생부터 승인, 수정, 확인, 완료 등이 처음부터 끝까지 한사람에 의해 처리될 수 없게 하는 보안정책을 말하며, 단계별로 업무를 분리하는 것을 의미한다. 최소권한이란 허가받은 일을 수행하기 위한 최소한의 권한만을 부여하여 권한 남용으로 인한 피해를 최소화 시키는 것을 말한다. 정보등급 분류, 접근통제 리스트 등을 들 수 있다(장상수, 2019).

기록관리는 기록의 생산, 접수, 유지, 이용, 처분을 능률적이고 체계적으로 통제하는 관리 영역으로서 업무 활동과 처리행위에 관한 증거와 정보를 기록의 형태로 획득, 유지하는 프로세스를 포함한다. 기록은 형태나 구조에 관계없이, 업무 이벤트 또는 처리행위에 대한 공신력 있는 증거로 간주되고 업무상 요구사항을 완전히 충족시킬 수 있도록 진본성, 신뢰성, 무결성, 이용가능성을 갖추어야 한다.[5)]

기록적 측면에서의 접근이란 카탈로그, 색인 목록, 검색 도구 및 그밖의 도구를 사용하여 적절한 정보를 찾게 하는 능력 또는 합법적으로 보안범주 내에서 정보를 검색하거나 찾아내도록 허가하는 것을 의미한다. ISO 15489에서는 정보를 탐색하고 활용하거나 검색하는 권리, 기회 및 수단으로 설명하고 있다. 따라서 접근통제란 검색도구 등을 사용하여 일정한 권한 범위 내에서 이용자가 정보를 찾거나 활용 및 검색을 허용하는 것을 적절히 제어, 유지하는 것을 의미한다(용마루, 2016).

접근통제[6)]는 기록과 기록이 담고 있는 정보를 보호하기 위하여 기록에 대한 접근을 제한하거나 허용하는 기록 관리 과정을 말한다. 접근에는 서로 상반되는 2가지 측면이 있는데, 첫째는 접근 통제를 통하여 기록과 그 속의 정보를 보호하는 것이고, 둘째는 이용자가 기록에 접근

〈표 1〉 접근통제 3단계

단계	설명	접근매체
식별	본인이 누구라는 것을 시스템에 밝히는 것	사용자명, 계정번호 등
인증	주체의 신원을 검증하기 위한 사용 증명 활동	패스워드, 토큰 등
인가	인증된 주체에게 접근을 허용하고 특정 업무를 수행할 권리를 부여하는 과정	접근제어목록, 보안등급 등

출처: 장상수, 「4차 산업혁명의 정보보호 개론」, 2019.

5) 국가기술표준원, 2016, 「KS X ISO 15489-1:2016 문헌정보-기록관리-제1부: 개념과 원칙」.
6) 접근 통제 [access control, 閱覽] (기록학용어사전, 2008. 3. 10., 한국기록학회).

할 기회를 최대한 제공하여 기록의 이용을 촉진하는 것이다. ISO 15489가 제시하는 접근의 3가지 원칙은 다음과 같다.

첫째, 누가 어떤 환경에서 기록에 접근하도록 허가할지를 규정하는 공식적인 지침이 있어야 한다. 둘째, 효과적으로 접근을 통제하려면 기록과 개인 모두에게 접근 조건을 부여해야 한다. 셋째, 기록에 시의적절하고 효과적으로 접근하여 검색할 수 있도록 해야 한다. 여기서 첫째와 둘째 원칙은 접근통제를 위한 것이고, 셋째 원칙은 접근 제공을 위한 것이다

과거 전통적인 기록관리에서는 신뢰성, 진본성, 무결성, 이용가능성 확보가 기록시스템의 품질 요건이었다면, ISO 15489:2016 개정판에서는 정보보호의 목표인 보안성, 무결성, 가용성을 받아들여 기록시스템의 품질 요건에 보안성을 추가하였다(이정은, 윤은하, 2018). ISO 15489에서 기록에 대한 접근은 승인된 프로세스를 통해 관리하여야 하며, 기록시스템은 행위주체의 기록에 대한 접근제공 및 제한을 개별적으로 혹은 집단별로 지원하도록 설계하여야 한다고 제시하고 있다.

공공 표준에서의 접근통제 관련내용은 필수기록물 선별 및 보호절차 표준[7]에서 필수기록물의 보호절차를 규정하고 있으나 접근통제보다는 분산 및 이중화 등 보존에 초점이 맞추어져 있다. 기록관리시스템 기능요건[8]에서는 접근권한 관리영역을 별도로 규정하고 있다. 기록관리 메타데이터 표준[9]에서 권한(Right) 요소에 대하여 기록물의 이용 및 접근을 관리하고 통제하기 위한 권한 정보로 정의하고, 그 하위요소로 비밀의 분류, 접근범위, 공개, 공공저작물 관리로 구분하여 제시하고 있다.

기록적 측면에서도 접근권한을 포함한 접근통제에 관하여 ISO 15489와 국내 기록관리 법령, 국가표준 등에서 규정하고 있다. 그러나 접근권한 관리 또는 접근통제에 대한 당위성만 규정하고 있고, 구체적 실행계획 또는 통제항목 등은 제시하고 있지 않다.

3. 자료수집 및 분석방법

3.1 파일럿 자료수집의 결과

연구자는 연구초기 정부산하 공공기관의 기록물관리 전문요원들의 업무상황 등에 대하여 파악이 되어있지 않아 연구질문을 구체화하기 어려웠다. 연구자는 파일럿 자료수집을 통해 공공기관 기록물관리 전문요원들의 내부 기록정보의 보호와 접근통제에 대한 전반적인 인식과 기관 내 전문요원의 위상 및 기록관리 현황을 확인 할 수 있었다. 또한 파일럿 자료분석을 통해 연구의 기본배경을 확인하고 연구질문을 정제하고 보완할 수 있었다(〈표 2〉 참조).

파일럿 인터뷰는 2020년 8월 27일부터 9월 15일까지 총 5명에 대한 질적 심층인터뷰를 통해 이루어졌다. 연구의 배경과 질문이 명확해지지 않은 상태에서 파일럿 인터뷰를 통해 기관의 비밀문서 관리에 대한 내용은 제외하게

7) NAK 2-2:2012(v 1.0) 필수기록물 선별 및 보호절차.
8) NAK 6:2020(v 1.3) 기록관리시스템 기능요건.
9) NAK 8:2016(v 2.1) 기록관리 메타데이터 표준.

〈표 2〉 파일럿 인터뷰 참여자 목록

코드	성별	직위	경력(년)	인터뷰 날짜	인터뷰시간(분)	기록
A	남	과장 (정규직)	6	2020.8.27	70	녹취
B	여	주무관 (무기계약직)	5	2020.9.10	110	녹취
C	여	대리 (정규직)	5	2020.9.11	60	녹취
D	남	과장 (정규직)	6	2020.9.11	100	전화인터뷰
E	남	주임 (무기계약직)	1	2020.9.15	90	녹취

되었다. 비밀관리는 별도의 규정에 따라 담당자가 지정되어 있어 기록물관리 전문요원의 업무영역에서 벗어나 있기 때문이다.

3.2 심층 인터뷰 과정과 결과

본 연구는 기존 연구자료가 없어 실제 공공기관에서 근무하고 있는 기록물관리 전문요원을 대상으로 심층인터뷰를 통해서 자료를 생성하는 방법으로 진행하였다. 연구참여자는 지역 기록물관리 전문요원 커뮤니티를 통해 기존부터 교류가 있었던 사람들과 개인적으로 오래전부터 교류를 해오던 기록물관리 전문요원을 중심으로 구성하였다. 그 이유는 연구자와 같은 지역에서 정부산하 공공기관 근무로 인한 공감대 등 라포(rapport)[10]가 형성되어 있어 연구참여자 개개인의 솔직한 대답을 이끌어 낼 수 있었기 때문이다. 연구를 위한 심층인터뷰를 진행하는 과정에서 '코로나-19'로 사회적 거리두기가 강화되어 대면으로 수행하던 심층인터뷰가 취소되거나 전화인터뷰로 대체되는 등 연구과정에 어려움이 있었다(〈표 3〉 참조).

인터뷰는 2020년 8월 27일부터 11월 3일까지 총 14명을 대상으로 대면 또는 전화인터뷰로 이루어졌으며, 참여자의 편의성을 고려하여 그들이 원하는 시간에 편한 장소에서 진행되었다. 참여자들에게 연구목적과 내용을 충분히 설명해 주었고, 사전동의를 얻어 음성녹음기로 인터뷰 내용을 녹취하였다. 심층인터뷰는 보통 1-2시간 정도 진행되었고, 모두 1125분의 인터뷰를 진행하였다. 인터뷰 진행과정에서 참여자의 핵심발언 내용이나 추후 질문내용은 메모하면서 진행하였다. 녹음된 인터뷰 내용은 음성파일로 저장하여 코딩을 용이하게 하기 위하여 모두 전사하여 문서로 저장하였다.

한명의 인터뷰 참여자 녹취를 전사하는데 인터뷰 시간 대비 평균 2-3배의 시간이 소요되었다. 전체 인터뷰 참여자 녹취를 모두 전사하는

10) 라포(rapport): 상담이나 교육을 위한 전제로 신뢰와 친근감으로 이루어진 인간관계이다. 상담, 치료, 교육 등은 특성상 상호협조가 중요한데 라포는 이를 충족시켜주는 동인(動因)이 된다. 라포를 형성하기 위해서는 타인의 감정, 사고, 경험을 이해할 수 있는 공감대 형성을 위하여 노력하여야 한다(특수교육학 용어사전, 2009, 국립특수교육원).

〈표 3〉 인터뷰 참여자 목록

코드	성별	직위	경력(년)	인터뷰 날짜	인터뷰시간(분)	기록
A	남	과장 (정규직)	6	2020.8.27	70	녹취
B	여	주무관 (무기계약직)	5	2020.9.10	110	녹취
C	여	대리 (정규직)	5	2020.9.11	60	녹취
D	남	과장 (정규직)	6	2020.9.11	100	전화 인터뷰
E	남	주임 (무기계약직)	1	2020.9.15	90	녹취
F	여	대리 (정규직)	3	2020.9.17	100	녹취
G	여	업무지원직 (무기계약직)	1	2020.9.19	50	녹취
H	여	대리 (정규직)	5	2020.9.21	50	녹취
I	남	대리 (정규직)	4	2020.9.22	75	녹취
J	남	연구원 (정규직)	1	2020.9.23	110	녹취
K	여	책임연구원 (무기계약직)	2	2020.9.29	40	녹취
L	여	주임 (정규직)	2	2020.10.5	100	녹취
M	남	연구원 (무기계약직)	2	2020.11.2	70	녹취
N	여	대리 (별정직)	6	2020.11.3	100	녹취

데 총 3,000여분(약 50시간) 정도가 소요되었으며, 전사 자료는 11pt로 A4 166 페이지에 달한다.

3.3 수집된 자료의 분석방법

심층인터뷰를 통해 수집된 자료는 개방코딩(Coding)을 통해 분석하였다. 개방코딩은 근거가되는 자료들을 분석하여 이름을 붙이고 개념들을 도출하여 범주화하는 단계이다. 개방코딩을 위하여 참여자들의 인터뷰 전사자료를 읽을 때 그 내용의 맥락을 고려하여 추론해 낼 무엇이 있는지 생각하는 해석적 읽기를 수행하였다. 이를 위하여 심층인터뷰 녹취 전사자료를 여러 차례 반복하여 읽으면서 자료를 개념화하였고, 개념을 명명화하면서 명명화된 개념들이 축적되기 시작하면 이를 묶어서 분류하는 과정을 거쳤다. 이 과정에서 범주에 대한 간략한 설

명을 말하는 것이 하위범주라고 하며, 이들 범주를 구체화하여 상위범주를 도출하였다. 그 결과 총 7개의 상위범주와 28개의 범주를 도출하였다.

4. 기록정보의 보호와 접근통제에 관한 인식 분석결과

정부산하 공공기관의 기록물관리 전문요원을 대상으로 기록정보의 보호와 접근통제에 대한 인식을 조사한 결과, 연구참여자들은 대부분 기관 내 기록정보의 보호를 위한 접근권한 설정 과정에 대하여 파악하고 있으며, 내부 시스템과 프로세스에서 개선이 필요한 사항도 파악하고 있었다. 또한 기록정보의 접근통제 정책에 관여해야 하며 이는 시스템 담당부서 또는 정보화 부서와 협의가 필요하다고 인식하고 있었다. 다만, 접근권한 설정과정에 필요한 기준 또는 가이드 등 관련정보 제공에 대해서는 인식의 차이가 나타났다. 기록정보의 접근통제 관련 업무수행에 기관 내 전문요원의 지위와 기록관리 체계 구축 정도 등이 영향을 미치는 것으로 나타났다. 또한, 각 기관의 담당업무 및 보안시설 보유여부 등에 따라 보안정책의 강도가 달라졌으며, 그 결과 정보 유출 등 사고 발생유무에도 영향을 미치는 것으로 나타났다.

위 내용을 토대로 기록정보의 보호를 위한 접근권한 설정과정, 기록정보의 접근통제 정책의 특징과 이에 영향을 주는 전문요원의 지위, 기록관리 체계 및 기록정보 특성을 상위범주로 도출하였다. 따라서 기관의 특성과 보안정책 및 보안이슈, 기록정보의 보호 및 접근통제를 위하여 기록관리와 전문요원에 대한 인식변화를 위한 요소 등 총 7개의 상위범주를 도출하였다.

4.1 기록정보의 보호를 위한 접근권한 설정 과정

연구참여자들이 기록정보의 보호를 위한 접근권한 설정 과정에서 느끼는 중요한 특성으로는 각 기관별 문서 접근권한의 세부단계와 내부직원들의 접근권한 설정행태, 접근권한 설정에 대한 내부직원들의 인식, 문서 접근권한 설정의 기준제시 등의 범주가 도출되었다(〈표 4〉 참조).

각 범주별 주요개념을 살펴보면 다음과 같다.

공공기관의 접근권한 세부단계는 대외 공개 구분의 경우 정보공개에 관한 법률에 따라 공개, 부분공개, 비공개로 구분하고, 내부 열람범위에 관해서는 기관 전체공유, 부서공유, 결재선공유(열람제한) 3가지를 기본으로 한다. 다만 자체개발 시스템을 사용하는 경우 좀 더 세분화된 4단계로 구분하여 적용하는 경우도 있었다(참여자L).

> “저희는 일단 문서시스템의 접근권한이 4개예요. 외부에는 정보공개 때문에 공개/비공개/부분공개 이거구요. 내부에는 공개/사내한/부서공개/결재선 공개 이렇게 4가지예요. 점점 범위가 적어진다고 보시면 될거 같아요.” (참여자 L)

내부직원들의 접근권한 설정행태와 관련하여 연구참여자들은 직원들이 대외등급은 공개로 지정하고, 내부 열람범위는 팀 또는 부서, 결재선 공유를 설정하여 정보의 접근에 모순이

〈표 4〉 기록정보의 보호를 위한 접근권한 설정 과정

상위범주	범주	개념
기록정보의 보호를 위한 접근권한 설정 과정	문서 접근권한의 세부단계	- (공통) 기관 내부 공유범위: 기관공유, 부서공유, 결재선 공유(열람제한) - (공통) 대외 공개설정: 공개/부분공개/비공개 - 전체공개, 4등급(처/부서공개), 3등급(팀 공개), 2등급(결재선 공개) - 인트라넷: 공개/비공개/부분공개, 보고서 제출시: 외부비공개, 공개주의 - 대외 공개구분 없음(원문공개 시행되면서 대외 공개구분 도입됨) - 직원들이 습관적으로 비공개 설정 하고 있어 안내를 해도 인식이 바뀌지 않음 - 전체공유/부서공유/결재선 공유 운영 안함
	내부직원들의 접근권한 설정행태	- 내부공유는 부서공유 또는 전체공유, 대외 공개는 공개를 많이 설정함 - 내부공유와 대외 공개 설정간의 부조화 발생 - 내부공유와 대외공개 설정이 연계되지 않아 직원들이 혼동을 일으킴
	내부직원들의 인식	- 보호가 필요한 문서의 경우 시스템에 등록하지 않고 수기로 보관함 - 내부공유, 대외공개 설정이 번거롭다고 느낌
	문서 접근권한의 설정 기준	- 개별 설정할 필요없이 정보공개 세부기준과 동일하게 운영하면 된다고 판단 - 내부공유 문서의 설정기준 별도 수립이 필요하다고 판단 - 별도 기준제공 없이 기안자의 판단에 맡겨야 한다고 판단

생기는 사례를 확인하고 내부교육 등을 통하여 직원인식 제고에 노력하는 것으로 나타났다(참여자N). 그러나 연구참여자들은 자신들이 발견하여 바로잡는 것보다 훨씬 많은 사례들이 있을 것이라고 예상했다. 이러한 행태는 대외공개여부 설정과 내부 열람범위 설정 기능이 연계되지 않은 데서 나타나는 문제점으로 인식하고 있었다(참여자 N, L).

"내부교육을 할 때 안내한 적이 있어요. 실제 대외 공개/내부 3등급(팀공유)를 설정한 사례가 있어서 이게 무슨 부조화지 싶어서 교육 때 내용으로 설명을 한 적은 있는데. 나중에 '이상하지 않나요?' 물어보면 그 직원이 '이상하네요' 그러지만 그거를 다 점검할 수가 없어요. 그게 충돌해서 뭐가 문제가 되서 안된다는 그런거 아니니까요. 그런데 가끔 발견되요. 교육때도 안내를 하고, 발견되면 말씀을 드려요. 앞뒤가 안맞지 않냐고, 2가지를 따로 설정하다 보니까 간혹 발견되요. 근데 제가 발견하는 것보다 훨씬 많을 거라는 생각이 들죠."(참여자 N)

내부직원들의 인식과 관련하여 실제 민감정보를 포함하고 있어 정보의 보호가 필요하다고 생각하는 경우 비공개 문서 또는 열람을 제한하는 문서로 설정하기 보다는 시스템에 등록하지 않고 수기로 보관하여 기관 내 전문요원의 기록관리 사각지대가 발생하는 것으로 나타났다(참여자 C). 문서의 접근권한 설정에 대외공개여부와 내부 열람범위 설정에 대하여 직원들의 번거로움을 느끼고 시스템 개선을 필요로 하고 있는 것으로 나타났다(참여자 D). 그러나 직원들이 필요에 의해 정보를 요청할 경우 안내를 해주는 것이 인식제고에 영향을 미치는 것으로 나타나(참여자 N) 내부직원 인식교육을 위한 적절한 교육 프로그램의 개발 및 확대 등 기록관리 관련 교육의 개선이 필요하다고 생각한다.

"(교육)내용은 기억이 하나도 안나죠. 그래도 기록을 하는 사람이 있고, 그게 나고, 문서기안 하다가 모르겠으면 전화한다. 이것만 기억해요

… (중략) …

그런데 효과가 있어요. '기록이라는 것이 있고 기록을 하는 사람이 있고, 문의하면 되는구나' 이것만 알아도 전자결재 교육을 하고 이러면 그 부분에 대한건 전화를 하니까요. 인식이 중요하더라구요." (참여자N)

문서 접근권한의 설정 기준과 관련하여 연구참여자들은 설정 기준 제공에 대하여 조금 상이한 인식을 보였다. 정보의 접근권한 설정에 대한 오너십은 직원 본인한테 있으므로 전문요원의 별도 기준제공 없이 기안자의 판단에 맡겨야 한다는 경우(참여자 C)와 기관 전체공유는 대외 공개여부를 공개로, 기관 내 부서 또는 팀 공유의 경우는 비공개세부기준에 따라 비공개 문서로 설정하도록 기준을 제시하고 있는 경우(참여자 D, I), 내부 직원들의 요청이 있어 내부열람 범위를 나누어 운영하는 구별기준을 만들어 제공해야 할 필요가 있다고 인식하는 경우(참여자 N)로 나타났다.

"(내부 열람범위 설정기준) 만들어야겠다는 생각은 해요. 질문을 되게 많이 받아요. '무슨 기준에 의해서 내부 열람등급을 정해야 하나요?' '내가 못 정하겠어요 그 범위를'. 이런 질문을 많이 받아요. 그런데 기준이 딱히 없죠.

… (중략) …

'담당자가 사안에 따라서 알아서 판단하세요' 해야되잖아요. 그런데 기준을 뭐라고 말해줄 수가 없어요. 그거는 좀 기준을 검토를 해보겠다고는 답변을 했어요. 그래서 '아! 만들어야겠다, 필요하겠다' 생각해요." (참여자 N)

열람범위 및 접근권한의 판단을 직원 자체에 맡겨야 한다는 의견이나 비공개세부기준을 적용하여 내부 접근권한을 설정해야 한다는 의견을 제시한 연구참여자들은 공통적으로 정보유출 등 문제 발생 시 누구에게 책임이 있는지와 연관지어 대답하는 특징이 있었다. 문제 발생 시 누군가는 책임을 져야 하는데, 내부 직원들이 알면서도 일부러 문의를 하는 것이라고 생각하고 있었으며, 그에 따라 「공공기관의 정보공개에 관한 법률」 비공개대상정보를 바탕으로 만들어진 비공개세부기준을 제시하고 있었다.

대외 공개여부와 내부 열람범위의 연계는 필요하지만, 비공개세부기준 자체를 적용하기 보다는 기록물관리와 관련하여 열람범위 설정에 관한 지침 등이 마련될 필요가 있다.

4.2 기록정보 접근통제 정책의 특징

연구참여자들이 생각하는 기록정보 접근통제 정책의 특성으로 개인(사람, 조직)에 대한 접근권한 관리, 기록(문서, 정보)에 대한 접근권한 부여, 접근통제 정책수립에 관한 인식 등의 범주가 도출되었다(〈표 5〉 참조).

각 범주별 주요개념을 살펴보면 다음과 같다.

기록정보 접근통제 정책 중 개인(사람, 조직)에 대한 접근권한 관리와 관련하여 대부분은 별도 열람 및 권한부여에 대한 절차가 없는 것 나타났으나 기관에 따라 문서 열람에 대하여 승인절차를 운영하는 것으로 나타났다(참여자 A). 또한 감사 또는 보안 등 특정부서에

〈표 5〉 기록정보 접근통제 정책의 특성

상위범주	범주	개념
기록정보 접근통제 정책의 특성	개인(사람, 조직)에 대한 접근권한 관리	- 열람이 제한된 문서에 열람자 추가할 수 있는 기능이 있음 - 문서의 대외 공개설정이 공개면 바로 열람가능, 비공개면 공람신청 후 담당부서 승인 후 열람이 가능함 - 특정부서(감사, 보안)에 문서 전체 접근권한 부여함에 대해 논쟁이 있음 - 문서 열람권한 부여를 위한 별도 심의위원회를 운영 하고 있음 - 별도의 열람요청 및 승인절차 운영하지 않음
	기록(문서, 정보)에 대한 접근권한 부여	- 외부공개, 열람이 제한된 보고서 인쇄 후 공개재분류 절차 없음 - 대외비, 비공개 속성관리 관련 부서간 논쟁이 발생함 - 저작권성 판단(공공저작물 등)에 대한 이슈가 있음 - 원문공개 등 대외 공개 관련 내용에 대하여 직원들 관심없음
	접근통제 정책수립에 관한 인식	- 정보보안 부서와 협의하여 외부에서 내부로 들어오는건 정보보안, 내부직원 대상은 기록물로 구분하여 운영함 - 전문요원이 열람권한 등 접근통제 정책을 수행해야 한다고 인식함 - 전문요원을 통한 정책 결정 후 정보화부서 실행 등 부서간 협의가 필요하다고 판단 - 전자, 전산 관련 업무는 정보화 관련 부서에서 전담하여 전문요원이 관여하지 않음

대한 열람권한 부여에 대하여 기관 내 전문요원과의 논쟁이 발생하고 있으며(참여자 E), 필요시 기간을 명시하여 신청하도록 운영하거나(참여자 M), 별도의 열람권한 부여를 위한 심의위원회를 운영(참여자 F) 하는 것으로 나타났다.

"저희는 열람에 대한 승인 제도가 따로 있죠. 열람승인 심의위원회라고 해서 별도 심의회가 있어요. 전체문서 열람 권한 승인 심의회요. 그래서 접근권한의 제한을 걸어놨잖아요. 열람제한을 걸었음에도 불구하고 전체문서를 보고 싶은 사람들은 이 심의회를 거쳐서 승인을 받으면 볼 수 있게 해주는 거예요." (참여자 F)

연구참여자들은 기록(문서, 정보)에 대한 접근권한 부여에 대하여 처음 만들어질 때 대외공개와 내부 열람이 제한된 보고서의 인쇄 후 공개재분류 절차가 없는 것이 문제라고 인식하는 것으로 나타났다(참여자 B). 또한, 대부분의 연구참여자들은 원문공개 등 대외 공개여부 내용에 대하여 내부직원들이 관심이 없다고 느끼고 있으며, 인식제고를 위한 내부교육이 필요하다는 데도 공감대를 형성하고 있었다(참여자 J).

"(외부 공개주의, 대외비로 분류된 경우) 따로 정리해두거나 누가 기한을 정해주거나 하지 않는 거죠. 그냥 막연하게 가지고 있어요. 리스트도 별도로 관리하지 않아요." (참여자 B)

"사실 제대로 하려면 직원들 교육이나 이런게 제공되어야 하는거죠. 저희는 원문공개 관련해서 직원들이 아예 관심이 없어요. 그렇게까지 고민해서 하질 않는거예요. 그냥 두는 거죠." (참여자 J)

연구참여자들은 기관 내 기록정보의 접근통제 정책수립과 관련하여 정보보안 부서와의 협

의를 통해 업무를 구분하여 운영하거나(참여자 A), 전문요원이 적극적으로 접근통제 정책결정에 참여해야 한다고 인식하고 있었다(참여자 N). 그러나 이와 반대로 접근통제 정책은 당연히 정보화부서에서 담당하고 있어 전문요원이 관여해야 하는 영역이라고 인식하지 못하는 경우도 있었다(참여자 E).

"기록물의 보안과 정보보안의 개념이 다르다는 거죠. 기록물은 내부고객인거고, 정보보안은 외부에서 내부로 들어오는거라 다른거다 라고 설명했죠. 기록정보에 대한 고객의 접근개념으로 나누었죠. 4-5년 전에 가르마를 탔어요. 애매하게 중첩되는 부분은 거의 없어요. 걸리는 부분도 약간 시스템 비중이 높으면 정보보안 쪽으로, 문서쪽에 비중이 높으면 문서쪽으로 나누어서 95% 정도는 업무를 나누었어요. 그런데 5%가 행정정보데이터세트 이슈 인거죠." (참여자 A)

기록정보 접근통제 정책은 개인 또는 조직에 권한을 부여하는 것과 정보 또는 문서 자체의 등급을 부여하는 것으로 구분할 수 있다. 기관 내에서 정보를 생성할 때 책정한 정보를 기준으로 접근할 수 있는 것과 접근을 차단해야 하는 것을 나누지만, 경우에 따라 접근권한의 변경이 필요한 경우, 정보화부서를 통해 직접 열람하거나 전문요원에 열람을 요청하는 것으로 나타났다. 접근권한의 변경여부 결정 및 열람을 전문요원이 직접 수행하는 경우 판단에 부담을 느끼고 있는 것으로 나타났다. 따라서 보안 및 감사 등 관련부서와 협업체계를 구성하고, 접근권한의 요청-검토-승인 등 별도의 절차를 구성할 필요가 있다.

4.3 전문요원의 지위

연구참여자들이 본인이 속한 기관 내에서 느끼는 전문요원의 지위는 채용형태, 근무기간, 수행업무, 기관 내 전문요원에 대한 인식, 전문요원에 대한 권한 부여 수준 등이 복합적으로 작용하는 것으로 나타났다. 이러한 전문요원의 지위는 기관 내 업무수행 과정 및 기록정보의 보호와 접근통제를 인식하는데 중요한 영향을 미치고 있다(〈표 6〉 참조).

〈표 6〉 전문요원의 지위

상위범주	범주	개념
전문요원의 지위	전문요원 업무	- (공통)기록물 관리, 원문공개, 정보공개, 정보목록 - (기관별) 공공저작물, 데이터, 알리오, 인장, 전자결재, 시스템 운영, 보안업무, 내규관리, 공공, 대외문서수발신, 우편, 통신비 등 행정처리, 단체 및 협회관리, 도서관리
	채용형태	- 정규직, 무기계약직, 별정직 - 과장, 대리, 주무관, 주임, 전문업무지원직, 책임연구원, 선임연구원, 연구원
	전문요원의 근무기간	- 1년 이상 근무 ~ 8년 미만 근무
	기관의 전문요원에 대한 인식	- 기록물 업무수행만으로도 일이 많고 벅차다고 느낌(추가업무 배정 안함) - 문서배부 담당자, 행정부서 직원 정도로 인식 한다고 느낌 - 정보공개 전문가로 인식함
	전문요원에 대한 접근권한 부여 수준	- 기록물 담당자니까 당연히 문서관리자 권한 부여함 - 직급이 낮거나 계약직이라는 이유로 문서관리자 권한 부여하지 않음

각 범주별 주요 개념들을 살펴보면 다음과 같다.

실제 대상자 인터뷰 결과 정부산하 공공기관 전문요원들의 근무기간은 1년~8년 이내인 것으로 나타났다. 정규직과 별정직, 무기계약직이 혼재되어 있으며, 기관 내 수행업무도 기록물 관리 외에 원문공개, 공공저작물, 도서관리, 인장관리 및 기타 행정업무 등 다양한 업무를 수행하고 있어(참여자J) 기관 내 기록물을 관리하는 전문가라는 인식보다는 문서 수발신 또는 정보공개 담당자로 인식하는 것으로 나타났다. 정부산하 공공기관에 배치된 기간이 짧아 내부적으로 지위가 낮아 기관에 새롭게 적용시켜야 하는 기록물관리 업무수행에 곤란을 겪고 있는 것으로 나타났다.

"기록물 관리, 원문공개, 내규관리랑 기재부 업무연락방(알리오), 대외문서 수발신, 우편, 그밖에 잡다한 통신비 등 행정처리. 전화기 관리 이런 거요. 그런데 이것도 업무가 안 크다고 봐요. 일이 자질구레하게 여러 개가 있는데 안 크다고 봐요." (참여자 J)

기관의 전문요원에 대한 인식과 관련하여 연구참여자들은 기관에서 본인을 문서배부자 또는 업무의 보조자로 인식하고 있는 것으로 나타났다. 전문요원에 대한 접근권한 부여 수준에 대해서도 기록물 관리자니까 당연히 관리자 권한을 부여해야 한다고 인식(참여자 J, L)하는 반면, 직급이 낮아 관리자 권한을 부여받지 못하거나(참여자G) 계약직으로 입사하여 권한부여에 오랜 시간이 걸리는 경우(참여자A)도 있는 것으로 나타났다. 연구참여자들은 기록관리 업무의 수행과 기록정보의 보호 및 접근통제에 있어서 관리자 권한을 부여받는 것도 중요한 요소라고 생각하는 것으로 나타났다.

"일을 하고 싶어도 감사실이나 보안팀에서 권한을 제한시켜 버리는 거죠. 슈퍼관리자의 권한을 받아야 하는데, 계약직은 guest의 권한을 부여하는 거예요. 실제 계약직으로 입사해서 정규직 전환 후에 슈퍼관리자 권한 받는데만 4년이 소요되었어요." (참여자 A)

4.4 기관의 기록관리 체계 및 기록정보 특성

연구참여자들의 인터뷰결과 기관의 기록관리 체계 및 기록정보의 특성으로 기관의 기록물 보유량, 비밀기록물 관리, 보호가 필요한 기록정보의 보유, 행정정보데이터세트 관리, 기록관리 인프라 확충 등의 범주가 도출되었다(〈표 7〉 참조).

각 범주별 주요개념을 살펴보면 다음과 같다.

대부분의 연구참여자들은 기관내 전자, 비전자 기록물의 보유량은 관리하고 있는 것으로 나타났다. 그러나 시청각 및 박물류의 자료들은 홍보실, 대외협력실, 비서실 등에서 개별관리하여 전문요원이 관여하지 못하는 경우도 있는 것으로 나타나 아직까지 기관 내에서 문서가 아닌 다른 형태의 기록물에 대한 인식이 부족하다는 것을 느낄 수 있었다(참여자 C, F).

비밀기록물 관리에 있어서 비밀업무는 비상계획관 등 별도 담당자가 있어 업무가 구분되어 있는 경우가 대부분 이었으나, 기관에 따라 기록물관리 전문요원이 보안 중 문서보안 업무

〈표 7〉 기관의 기록관리 체계 및 기록정보 특성

상위범주	범주	개념
기관의 기록관리 체계 및 기록정보 특성	기록물의 보유량	- 전자, 비전자는 전문요원이 관리하여 보유수량을 파악함 - 시청각, 기타 행정박물 등 홍보실, 대외협력실, 비서실 등 별도의 부서에서 관리하는 경우 파악이 어려움
	비밀기록물 관리	- 대부분 2급, 3급, 대외비 보유 - 3급 부터 보유 하거나 보유하지 않음 - 별도 관리부서 또는 관리 담당자가 있음 - 비밀관리대장도 전문요원이 관리함 - 보안심의위원회를 운영, 심의회를 통하여 일반문서 전환시 기록관 이관
	보호가 필요한 기록정보	- 업무수행 관련 정보 중 자금지원 및 투자정보, 개인정보 등 - 연구수행 결과 관련 예비타당성 조사 등 - 별도로 보호가 필요한 기록정보 없음
	행정정보데이터 세트 관리	- 행정정보데이터세트 관련 TF를 운영함 - 행정정보데이터의 오너십은 담당부서에 있다고 인식 - 행정정보데이터세트 관리방향만 설정함 - 향후 평가에 반영되면 관리 시작할 예정
	기록관리 인프라 확충	- 전문요원 입사 전 기록관 공간 확정되어 서고, 모빌렉 설치 됨 - 서고 및 모빌렉 설치 중 - 부서별 담당자 지정함 - 분류체계 수립 및 기록물관리 규칙 제정 중 - 표준 RMS 설치를 위한 예산 확보 중 - 표준 RMS 설치 및 활용 중

를 담당하면서 비밀관리도 같이 수행하고 있는 것으로 나타났다(참여자 I). 이 기관의 경우, 앞서 살펴본 전문요원에 대한 인식에서 전문요원을 문서배부 담당자로 인식하고 있어 지침에 따라 문서접수 담당업무의 하나로 비밀문서접수대장 관리 및 비밀관리도 같이 수행하고 있었다.

"비밀접수는 문서담당이 하래요. 제가 맡은 이유가 뭐냐면요. 비밀문서가 오면 문서배부 담당자가 해요. 그래서 기록물 담당자가 비밀취급인가를 받는거예요. 지침에 문서접수 담당자가 받는거죠." (참여자 I)

보호가 필요한 기록정보에 대해서는 기관별 고유업무 수행과 관련한 정보들을 보호대상 정보로 인식하는 것으로 나타났다. 예를 들어 정부투자 관련 정보, 자금지원 정보, 기관에 신청서를 제출한 사람의 개인정보 등이 별도의 보호가 필요한 정보에 포함된다(참여자 B, D).

"저희는 OOO 관련 자료가 있죠. OOO는 우리가 입는 피해가 얼마인지 산정하고 이런 과제는 내부직원한테도 제목까지 비공개예요. 이런 자료는 과제수행 책임자, 수행자, 인가를 해주는 기관장 정도만 접근이 가능한거죠." (참여자 B)

행정정보데이터세트 관리에 관해서는 최근 개정된 공공기록물관리법이 시행되었지만 기관의 기록관리 여건상 법률에 정해진 관리체계 수립이 어렵다고 느끼고 있는 것으로 나타났다.

특히, 기관 내에서 행정정보데이터세트 관리와 관련된 고민은 시스템 또는 정보보안과 같은 해당 부서에서 결정할 사안이라고 생각하는 경우(참여자 F), 내부직원들의 요청에 따라 이미 TF를 구성・운영하여 내부 관리체계를 만들어 놓은경우(참여자 C) 등 기관별로 정책수행에 대한 차이가 나타났다.

"(국가기록원 지침에) 관리등급을 나눠서 단순한 단위업무 페이지 등은 제외하고 업무시스템 중에 어떤 건 해라 등 가이드가 있거든요. 그런데 우리는 시스템을 그렇게 판단할 수가 없다고 해서 시스템을 관리하는 부서에서 자체적으로 시스템을 선별해 오고 그 보존기간이 다했다고 하면, 우리가 심의는 해주겠다 정도로 결론이 났어요. 시스템 관리부서가 오너십을 가지고 해오는 걸로 했어요." (참여자 C)

연구참여자들은 기록물관리 인프라 확충 수준에 따라 업무수행에 차이를 느끼는 것으로 나타났다. 정부산하 공공기관 중 중앙부처 수준의 인력, 시설, 환경 등 인프라를 갖춘 기관이 있는반면, 아직 분류체계가 갖춰지지 않은 기관(참여자 J, M), RMS 도입을 계획 중인 기관(참여자 N) 등 인프라 확충 수준이 상이한 것으로 나타났다. 참여자들은 앞서 살펴본 전문요원의 지위에서 도출된 바와 같이 기관 내 지위가 낮아 초기비용이 많이 드는 기록물 관리체계 구축이 힘겨운 것으로 나타났으며, 기관의 정보 접근 및 열람 등 보안정책 수립과 내부직원 인식제고를 위한 교육 등을 수행할 여력이 없다고 느끼고 있었다.

"철 단위로 관리할 수 있게끔 철 생성하고 할수 있는게 있긴 있는데, 이게 너무 복잡해서. 복잡하기보다 너무 번거로워요. 기능 자체가 되게 불편하게 만들어져 있고 특정 계정으로 접속을 해서 만들어야 되는 번거로움이 있어요. 관리도 안되고. 그래서 그거를 하려다가 접었어요. 왜냐하면 그렇게 건 단위로 해서 철을 만들고 거기다 집어넣더라도 이 철이 식별이 안되요. 의미가 없는 거예요. 그래서 BRM 시스템 도입하려고 했던거구요." (참여자 M)

4.5 기관의 특성

연구참여자들의 인터뷰결과 기관의 특성으로 기관의 수행업무에 따른 특징, 기관 시설 및 규모에 따른 특징 등의 범주가 도출되었다(〈표 8〉 참조).

〈표 8〉 기관의 특성

상위범주	범주	개념
기관의 특성	기관의 수행업무에 따른 특징	- 연구과제 수행을 많이 하는 기관의 경우 저작권 이슈 발생 - 투자정보, 개인정보 등 민감정보를 많이 보유한 경우 별도 접근절차가 있음 - 기술, 전산을 중심으로 하는 경우 행정직은 보조적으로 인식
	기관 시설 및 규모에 따른 특징	- 국가중요시설로 지정된 경우 보안에 관심이 많음 - 여러 개의 기관이 합쳐져서 설립된 기관의 경우 각 기관의 성격이 남아있음 - 기관 규모가 큰 경우, 보안과 시스템 등 업무가 세부적으로 나뉘어 있음

기관의 수행업무에 따른 특징으로는 해당기관의 성격에 따라 원문공개를 시행하지 않는 기관이 있었으며(참여자 B, G), 특히 연구를 주요 업무로 수행하는 기관의 경우, 연구자가 연구산출물은 본인자료라는 인식이 있어 연구산출물을 전문요원이 확보하기가 힘들다고 느끼는 것으로 나타났다(연구자 B). 연구를 수행하는 이 기관의 경우, 내부적으로 보안정책도 다른 기관에 비하여 느슨하게 적용되어 있는 것으로 나타났다. 뿐만 아니라 직원들도 본인들의 행동이 정보유출에 해당 된다는 인식이 부족한 것으로 나타났다. 따라서 전문요원이 보안에 문제가 있다고 인식하고 있지만, 혼자 기관의 인식을 바꾸기에 역부족이라고 느끼고 있었다.

"중간산출물은 아예 관리가 안되고 있죠. 중간산출물은 아예 (작성자) 본인꺼라고 생각해서 다 가져가요." (참여자B)

또한, 연구, 기술, 전산, 검사 등 특정 직렬을 중심으로 기관이 구성된 경우 행정직은 보조적 역할로 인식하는 것으로 나타났다(연구자 B, I). 따라서 연구참여자들은 전문요원이 전문성을 인정받고 본연의 업무를 수행하기 어려운 상황이라고 느끼고 있었다.

4.6 기관의 보안정책 및 보안이슈

연구참여자들은 생각하는 기관의 보안정책 및 보안이슈와 관련하여 보안정책 적용과 정보유출 등 이슈사항을 도출하였다(〈표 9〉 참조).

각 범주별 주요 개념들을 살펴보면 다음과 같다.

보안정책의 적용은 기관의 특성과도 연관이 있는 부분으로, 대부분의 기관은 기본적으로 망 분리를 비롯하여 DRM 도입, 보안USB 사용 수준의 보안정책이 적용되어 있는 것으로 나타났으며, OTP를 추가적으로 사용하는 경우도 있었다(참여자 L). 그러나 특정기관의 경우 망 분리 미적용을 포함하여 외부 포털 메일

〈표 9〉 기관의 보안정책 및 보안이슈

상위범주	범주	개념
기관의 보안정책 및 보안이슈	보안정책 적용	- 대부분 망분리, DRM, 보안 USB, 워터마크 등 보안정책을 도입, 운영하고 있으며, 보안정책은 필요하다고 인식하고 있음 - 기관 내 DRM 도입시, 주관부서와 협업하여 전자문서시스템에 원하는 규격으로 커스터마이징 추진 - 직원 편의가 우선 고려사항으로 보안정책을 도입하지 않은 경우가 있음
	정보유출 등 이슈사항	- 투자정보에 무단접근하여 사익추구 - 열람범위 설정 오류로 인사정보, 평가정보, 급여정보 등 직원공유가 발생함 - 이메일을 통한 내부정보의 외부 유출, 외부 파견직원의 내부정보 요청 및 외부 전달 - 연구결과 등 내부산출물에 대해 본인꺼라는 인식으로 외부로 가져감 - 친분에 의해 접근권한을 부여받아 무단 정보 열람 및 외부 유출함 - 전문요원 입사 전 내부 정보의 무단삭제 발생 했을 거라고 추정함 - 정보유출 등 보안사고에 대하여 직원 개인의 도덕성에 기대함 - 내부 기록정보의 유출방지를 위해 기록정보 접근에 대한 이력관리가 필요하다고 판단함 - 정보유출이 발생했지만, 내부적으로 별다른 문책 및 징계가 없음

접속은 물론 외부 드라이브 사용 등 보안정책이 적용되지 않은 경우도 나타났다(참여자 B).

"저희 내부 망분리도 안되어 있거든요. 얼마 전까지 OO 드라이브도 사용가능 했어요 막힌지 얼마 안됐어요. 업무 관련 내용으로 외부 상용메일도 보내지 말라고 하는데 가능은 하죠. 정책적으로 막혀있지는 않아서요 접속기록은 남고, 보낼 때는 내부메일에 첨부파일이 뭔지 이런건 확인이 되지만, 외부 상용메일 모바일 웹주소 넣으면 접속이 되요. 사실 카페에 올려놓거나, 개인 드라이브에 넣어놓을 수 있을 거에요. 내부망에서 주식사이트 이런거 빼고는 거의 다 열려있어요." (참여자 B)

정보유출 및 이슈사항으로는 대부분의 기관이 기관 내·외부에 정보유출이나 이로 인한 이슈사항이 발생하였으나, 별도의 문책이나 징계로 이어지는 경우는 거의 없는 것으로 나타났다. 평소에 별로 중요하게 신경쓰지 않았던 사안으로 인하여 기관 내부에 결정되지 않은 정보가 먼저 알려진 경우로 내부 보안정책을 강력하게 적용할 필요가 있음을 나타내는 사례라고 할 수 있다.

실제로 직원의 실수로 외부에 개인정보를 유출한 경우(참여자 A) 개인정보 유출로 인한 관할기관의 조사와 담당자 징계가 이루어졌다. 이는 내부직원들의 인식제고가 필요한 사례라고 할 수 있다. 또한, 기관 내부의 연구수행과 관련하여 모형의 운영을 담당하던 직원이 이직을 하면서 외부에서 이 모형에 접근하여 추가적인 활용하는 경우도 있는 것으로 나타났다. 이는 명백히 정보유출에 해당하지만, 연구자들은 대부분 본인이 연구한 결과는 본인의 소유라고 생각하고 있는 것으로 나타났다(참여자B).

"센터를 운영하는데 거기서 예측을 위해 OO을 운영하거든요. 이게 저희 자산이잖아요. 오랜시간 동안 개발시킨 거니까요. 그런데 이 연구를 계속했던 직원이 이직을 하셨어요. 그런데 이 연구로 자꾸 (외부에서) 논문을 쓰는거에요." (참여자 B)

내부 시스템의 전체문서함 접근권한을 전문요원이나 다른 분과의 협의없이 요청한 경우 부여해줘 내부문서가 유출되는 사고가 발생하기도 하였다(참여자D).

"전체 문서함을 다 들어갈 수 있는 권한을 다른부서 임원들이나 친한 직원들이 요청하면 권한을 부여해준 거에요. 원래는 감사실도 어떤 기간에만 부여해주는 권한인데 그냥 권한 열어주고 내버려 둔거죠. (그래서) 외부에 내부문서가 나갔어요." (참여자 D)

이러한 정보유출 및 이슈사항에 대하여 연구참여자들은 내부 문서에 대한 접근이나 열람을 승인해 줄 때, 기록물관리전문요원이 관여해야 한다고 인식하고 있었다.

4.7 기록관리와 전문요원에 대한 인식변화를 위한 과제

연구참여자들이 생각하는 기록관리와 전문요원에 대한 인식변화를 위하여 개선이 필요한 과제로 내부 기록관의 독립 및 독자적 업무수

행 환경 구성, 국가기록원의 역할 확대, 전문요원의 역할 확대, 시스템 기능개선, 법률개정, 타 부서와의 업무연계, 전문요원 자격증 호칭의 변경 필요성이 도출되었다(〈표 10〉 참조).

각 범주별 주요 개념들을 살펴보면 다음과 같다.

먼저 다수의 연구참여자들은 기록관의 독립 및 독자적 업무수행 환경을 구성해야 한다고 느끼고 있었다. 특히 기록관 업무의 독립성 보장이 가장 필요하다고 생각하고 있었다(참여자 A,E). 현재 대부분의 기록물관리 전문요원들은 총무부서 소속으로 기록물관리 업무 외에 수많은 행정업무들을 수행하고 있어 전문성을 가진 기록물관리 업무에 소홀하게 되는 상황이 발생하는 것이다. 따라서 기록물관리 업무를 독립적으로 수행할 수 있는 개별 조직이나 팀, 센터 등의 구성이 필요하다. 특히 기록물관리 업무는 정보서비스, 보안, 개인정보, 공공데이터 등과 연관되어 있어 독립된 조직에서 관련 부서와 협업을 할 수 있도록 조직의 개편이 필요하다고 생각한다.

"기록관이 독립했으면 좋겠어요. 기록관 업무에 개인정보보호도 같이 들어왔으면 좋겠어요. 기

〈표 10〉 기록관리와 전문요원에 대한 인식변화를 위한 과제

상위범주	범주	개념
기록관리와 전문요원에 대한 인식변화를 위한 요소	내부 기록관의 독립 및 독자적 업수수행 환경 구성	- 기록관 독립: 홍보, 발간, 출판, 서비스 제공 등 관련 업무 중심으로 개별 팀 구성 및 독자적 운영이 필요하다고 느낌 - 기관 크기에 따른 전문요원 수 의무채용 및 기록물 팀 구성이 필요하다고 느낌 - 내부 시스템,아카이브로 구축을 계획하고 있음
	국가기록원 역할 확대	- 통합관리 기준을 수립할 필요가 있음 - 기록관리의 사각지대를 없애는 방안이 필요함 - 평가대상 확대 운영, 포상제도 확대 운영 - 다양한 교육과정 개설이 필요 - 외부 전문강사 양성 및 기관별 컨설팅 시행 =〉 기관이 기록관리에 관심을 가질 수 있는 방안 마련이 필요
	전문요원의 역할 확대	- 내부 문서생산 교육, 기준수립 등 업무수행 필요 - 기록물 무단반출에 대한 직원 인식개선이 필요함 - 내부직원 인식제고를 위한 신입사원 교육, 외부강사 활용한 교육과정 개설 등 필요
	시스템 기능개선	- 기록 생성시 메타데이터 다양하게 설정할수 있는 기능이 필요함 - 기관 내부 시스템에 접근권한, 열람제한 등 관련 개념 추가해서 관리 필요함 - 비밀/대외비 관련 설정기능이 없어 개선이 필요함
	법률개정	- 정보공개 접수 관련 내용 삭제 - 기관 규모에 따른 전문요원 수에 대한 규정 필요 - 전문요원의 정규직 채용 의무화
	타부서와 업무연계	- 보안, 감사부서와 연계 - 정보공개, 저작물 이용허락 등 서비스 제공 업무 포괄하여 관련부서와 연계
	전문요원 자격증 호칭 변경 필요성	- 기록연구사, 전문요원 호칭 통일 필요

록물, 개인정보, 저작권, 정보공개, 공공데이터 이렇게 5가지가 들어오면 한 팀이 구성되면 문서와 다 관련 있는 내용이고, 이렇게 정보팀을 구성했으면 좋겠어요.

… (중략) …

기록관에 보안업무, 개인정보, 정보공개, 비상계획 등등 관련업무를 다 포함시키도록 개정할 필요가 있다고 생각해요. 기관 전문요원의 가장 중요한 역할 중 하나가 접근권한을 통제하고 기록관의 문서를 통제하는 것이니까요." (참여자A)

연구참여자들이 개선이 필요하다고 느끼고 있는 부분은 국가기록원의 역할 확대에 관한 내용이었다. 실제 개인정보, 공공저작물 등 기록물법과 충돌지점이 생기는 법안에 대한 명확한 해석이 필요하고(참여자 A), 공공기관의 사각지대를 해소할 수 있도록 강제성을 부여해줄 필요가 있다고 느끼는 참여자(참여자 B)도 있었다. 그밖에 평가체계를 개편하여 누락되는 기관이 없도록 하는 방안(참여자 B,J,K,L,M,N), 교육제도 확대(참여자 E), 통합관리 기준마련(참여자 D), 포상제도의 확대(참여자 L,M,N)가 필요하다고 느끼고 있었다.

"저는 사각지대를 없애줬으면 좋겠어요. 저희 같은 기관이 사실은 사각지대 잖아요. 할거면 국가기록원에서 강제성을 가지고 하도록 했으면 좋겠어요. 아무리 법에 규정되어 있다고 해도 '그동안 안 했어도 아무 일도 없었잖아~' 이런 논리로 계속 업무수행이 안되고 있어요. '다른 기관 아직도 없어.. 우리기관은 빠른 편이야~' 이런 논리로 업무를 안하고 있죠. 그러니까 강제성, 당위성 이런 게 부족하고 국가기록원이 힘이 없고, 담당자도 너무 자주 바뀌죠. 국가기록원 업무순환이 너무 빨라요. 그래서 뭘 물어볼래야 물어볼데도 없죠. 아니면 같은 기관 협의체라도 지원을 많이 해서 묶어주던지 했으면 좋겠어요. 분류체계도 저희도 관련기관별로 각자 따로 개발할 것이 아니고 한 5개 정도만 선제적으로 개발하면 그거 기관에 맞게 수정해서 적용할 수 있는데 예산도 안주고 해야된다고 하니까 등 떠밀려서 어쩔 수 없이 하고 있어요." (참여자 B)

연구참여자들은 전문요원의 역할 확대에 대한 개선도 필요하다고 느끼고 있었다. 특히 내부직원들의 문서정보 생성 시 문의사항에 대한 응대 및 관련 교육을 제공해야 한다고 인식하고 있었고(참여자 A), 기관 내 전문요원의 역할에 대한 인식이 필요하다고 생각하는 것으로 나타났다(참여자 E,F). 또한, 내부직원의 인식제고를 위한 교육이 수행되어야 한다고 생각하는 것으로 나타났다(참여자 H). 기관 내 인식제고를 위해서는 내부직원을 대상으로 하는 교육이 실시되어야 하지만, 실제 전문요원들이 기록물관리가 아닌 정보공개, 기타 행정업무에 투입되어 있어 실제 직원들이 필요로 하는 정보를 제공하거나 교육제도를 마련하기 힘든 상황이다.

"내부직원들은 공문서 작성, 전자직인, 행정효율과 협업에 관한 규정, 직인 등등 '이런거 어떻게 해요?'라는 질문이 많아요. 실제 기록물을 생산하는 것과 관련된 것들은 대학원에서 가르치지도 않죠. (전문요원들은) 정보공개 업무에 치여서 실제 생산과정에서 직원들이 필요로 하는 내용은 기관 담당자들이 전혀 대응하지 못하고 있죠.

… (중략) …

중앙부처는 문서 생산단계의 기준이 잘 잡혀있는데, 공공기관은 아직 잡혀진 틀이 없고 지방 공공기관은 더하다는 거죠. 지방 공공기관들은 거의 아무것도 없어요. 직인, 인감에 대한 개념도 없고, 공문서를 왜 이렇게 작성해야 하는지도 모르는 기관들이 많아요. 그러다보니 1차적으로 기관에 배치된 전문요원들이 해줘야 하는 역할이 (기록을) 생산하는 부서와의 협업과 기준마련 인거죠. 그러나 정보공개 업무에만 매달려 있으니까 문제인거예요. 그러니까 거꾸로 서비스를 신경 쓰느라 생산에 문제를 해결하지 못하고 있는 거죠." (참여자 A)

연구참여자들은 개선이 필요한 사항으로 기록정보 생성 시 메타데이터를 다양하게 설정할 수 있는 기능(참여자 B)과 비밀 대외비 관련 설정기능(참여자 G)을 추가하는 등 시스템 개선이 필요하다고 느끼고 있었다. 현재 대부분의 공공기관들이 사용하는 전자문서시스템에는 비밀이나 대외비를 설정하는 기능이 없는 것으로 나타났다. 이는 시스템의 기능 보다 현재 업무처리 방식이 비밀, 대외비는 서면위주로 구성되어 있기 때문이기도 하다. 그러나 전자문서가 보편화되어 비밀, 대외비 또한 전자적 형태로 관리될 필요성이 있다. 따라서 전자문서시스템이 정보를 관리하는데 조금 더 탄력적으로 개선될 필요가 있다고 생각한다.

"기본적인 메타값을 다양하게 해줬으면 좋겠어요. 공개시한 정보도 들어가야 할거 같아요. 처음부터 생산될 때 여러 가지 메타값을 지정할 수 있으면 좋을거 같아요." (참여자 B)

기록물 관리 법률개정에 대하여 연구참여자들은 전문요원 정규직 채용 의무화, 정보공개 관련사항 삭제, 적용기관의 특성에 따른 시행령, 시행규칙 구분 등이 필요한 사항(참여자 A), 처벌규정의 강화(참여자 N) 라고 생각하는 것으로 나타났다.

"처벌규정이 있나요? 시스템을 언제까지 안 만들면 처벌규정이 있나요? 이렇게 물어보는데 처벌규정이 없잖아요. 그러니까 예산 순위에서 계속 밀리더라구요. 전자문서 관리시스템 구축을 안하면 그 다음단계 업무를 못하는게 문제지, 시스템 구축을 안한다고 처벌하는 규정은 없죠." (참여자N)

5. 맺음말

기록정보를 보호하기 위한 접근통제는 물리적 환경에서 뿐 아니라 전자적 환경에서도 이루어져야 한다. 연구참여자들의 인터뷰에서도 나타났듯이 각 기관들은 물리적으로 접근을 통제할 수 있는 보존서고 등 보존환경 구성, 열람실 설치 등 물리적인 환경 뿐 아니라 전자적으로도 전자문서생산시스템, 표준 RMS, 기관 내 행정정보시스템과 함께 기록을 통제할 수 있는 분류체계 및 처분지침 등 기록관리를 위한 기본 인프라가 갖추어져 있어야 한다. 또한, 이를 적절하게 제어하고 운영할 수 있는 관리자 권한과 통제권이 전문요원에게 부여되어야 하며 기관 내 기록물관리 전문요원과 기록관리 업무에 대한 인식제고가 이루어져야 한다.

기관 내 기록정보의 접근을 통제하기 위해서

는 물리적인 기록물의 보존환경 구성과 전자적 시스템 구축 및 분류체계, 관리규정 등을 포함한 기본 인프라의 확충이 필수적이다. 따라서 접근권한을 부여하고, 정책을 집행할 수 있는 최소한의 기반이 마련될 수 있도록 국가기록원의 관심과 지원이 필요하다. 또한, 전문요원들이 기관 내에서 권한과 통제권을 가지고 적절하게 기록정보의 접근통제를 수행하기 위해서는 정보시스템의 접근통제 정책결정 과정의 참여, 기록관 조직의 독자적 업무수행을 위한 환경이 구성되어야 한다. 마지막으로 기록물관리 전문요원들이 기관 내 입지를 다지고 전문가로서 인식시키기 위해서 국가기록원의 포상제도 개선, 직원 인식제고를 위한 교육 전문강사 양성이 필요하다.

기록물관리 전문요원이 기록정보의 보호와 접근통제를 수행하기 위하여는 기록관리 체계의 개편이 필요하다. 첫째, 현재 국가기록원 중심의 기록관리 체계를 탈피하고 공공기관 기록관리 업무체계 확립을 지원하기 위하여 전문기관의 설치・운영과 함께 기록물관리 전문요원의 접근통제 관련 권한과 책임을 명시한 표준(안)이 마련될 필요가 있다. 이는 향후 민간으로의 기록관리 확대를 위해서도 필수적이 사항이라고 할 수 있다. 둘째, 기록관리 전담조직의 설치 또는 기록관 독립과 함께 관련분야를 포함하는 정보거버넌스형 기록관리 조직의 구성이 필요하다. 마지막으로 접근권한 통제를 위하여 역할기반 접근제어 방식의 적용 및 DRM(Digital Right Management) 시스템 적용과 함께 대외비 문서를 포괄하여 관리할 수 있도록 전자문서시스템의 기능개선이 필요하다. 또한, 기록물의 메타데이터를 활용한 논리적 이관 및 기록관의 영구기록물 보존절차 마련 등 기록관리 프로세스의 개선도 이루어져야 한다.

앞으로 기록물관리 전문요원들이 기관 내 기록정보의 보호와 접근통제가 기록관리에 필수적인 요소임을 인식하여, 이를 위한 정책결정 및 집행에 적극적인 참여가 필요해 보인다. 향후, 정부산하 공공기관의 상황과 기록물관리 전문요원들의 업무환경 등에 관한 좀 더 활발한 연구가 이루어지길 기대해본다.

참 고 문 헌

김용 (2007). 전자기록관리시스템의 기능 설계에 관한 연구. 한국기록관리학회지, 7(1), 61-82. https://doi.org/10.14404/JKSARM.2007.7.1.061

김의탁, 최용락, 김기현, 박정호 (1998). 접근통제 기술 동향. 정보보호학회지, 8(4), 77-96.

김형주. 김수현 (2017). 기록관리시스템 기능요건 표준의 정부산하공공기관 적용에 관한 사례 연구. 한국비블리아학회지, 28(2), 35-56. https://doi.org/10.14699/kbiblia.2017.28.2.035

박민영 (2013). 표준기록관리시스템 기능 평가: 접근관리 기능을 중심으로. 기록학연구, 38, 3-35. https://doi.org/10.20923/kjas.2013.38.003

손성근 (2008). 정부표준 기록관리시스템의 현황과 문제점 분석. 석사학위논문, 서울대학교 기록관리 협동과정.

심재윤, 이경호 (2015). 금융IT인력의 보안사고 위험도에 기반한 정보접근 통제 정책 연구. 정보보호학회논문지, 25(2), 343-361. http://dx.doi.org/10.13089/JKIISC.2015.25.2.343

양성훈, 오정현, 이경효, 임도연, 오병균 (2005). 접근권한의 상속성을 이용한 역할계층 접근통제 모델. 한국정보과학회 학술발표논문집, 32.2, 94-96.

엄정호, 박선호, 정태명 (2010). 내부자의 불법적 정보 유출 차단을 위한 접근통제 모델 설계. 정보보호학회논문지, 20(5), 59-67.

오진관 (2019). 기록관리시스템 설계모형과 기능요건 연구. 박사학위논문, 명지대학교 기록정보과학전문대학원 기록관리전공.

용마루 (2016). 기록관리시스템의 접근통제기능 개선방향 연구. 석사학위논문, 명지대학교 기록정보과학전문대학원 기록관리전공.

이소연, 김자경 (2004). 전자기록관리시스템(ERMS) 설계표준의 기능요건 분석: ISO 15489를 기준으로. 한국정보관리학회, 정보관리학회지, 21(3), 227-250. https://doi.org/10.3743/KOSIM.2004.21.3.227

이정은, 윤은하 (2018). ISO 15489 개정판의 주요 특징에 관한 연구. 기록학연구, 57, 75-111. https://doi.org/10.20923/kjas.2018.57.075

이주영, 이구연, 권호열 (2020). 시나리오 기법을 이용한 내부자 정보 유출 탐지 방안. 한국디지털콘텐츠학회논문지, 21(3), 617-626. https://doi.org/10.9728/dcs.2020.21.3.617

임도빈 (2009). 질적 연구 방법의 내용과 적용전략: 양적인 질적 연구와 질적인 질적 연구. 정부학연구, 15(1), 155-188.

장상수 (2019). 4차 산업혁명의 정보보호 개론. 배움터.

천권주 (2008). ERMS 표준에 나타난 접근통제 요건의 적용방안에 관한 연구. 기록학연구, 18. https://doi.org/10.20923/kjas.2008.18.179

최은복 (2009). 비밀성과 무결성을 보장하는 격자개념의 역할그래프 보안 모델, 한국컴퓨터정보학회논문지, 14(6), 91-98.

한국기록학회 (2008). 기록학 용어 사전. 서울: ㈜역사와비평사.

한석실 (2010). 질적연구방법의 질에 대한 쟁점 고찰. 인간과 문화 연구, 16, 5-44.

[표준 및 법령]

공공기록물관리에 관한 법률 시행령. 대통령령 제30584호.

공공기록물관리에 관한 법률. 법률 제16661호.

국가사이버안전관리 규정. 대통령 훈령 제316호.

국가정보화 기본법. 법률 제16749호.
기록관리 메타데이터 표준(v 2.1). NAK 8:2016(v 2.1).
기록관리시스템 기능요건(v1.3). NAK 6:2020(v1.3).
문헌정보-기록관리-제1부: 일반사항. KS X ISO 15489-1.
문헌정보-기록관리-제2부: 지침. KS X ISO TR 15489-2.
정보기술 - 보안기술 - 정보보호 경영시스템 - 요구사항. KS X ISOIEC27001.
정보기술 - 보안기술 - 정보보호 경영을 위한 실무지침. KS X ISOIEC27002.
정보보호산업의 진흥에 관한 법률. 법률 제17344호.
정보통신망 이용촉진 및 정보보호 등에 관한 법률. 법률 제17358호.
정부산하공공기관 등의 기록관리를 위한 시스템 기능요건(v1.1). NAK 20:2020(v1.1).
필수기록물 선별 및 보호절차(v 1.0). NAK 2-2:2012(v 1.0).

• 국문 참고문헌에 대한 영문 표기
(English translation of references written in Korean)

Cheon, Kwon-Ju (2008). A study on application plan of access control requirements in ERMS Standard, The Korean Journal of Archival Studies, 18, 179-220. https://doi.org/10.20923/kjas.2008.18.179

Choi, Eun-Bok (2009). A lattice-based role graph security model ensuring confidentiality and integrity. Journal of the Korea Society of Computer and Information, 14(6), 91-98.

Eom, Jung-ho, Park, Seon-ho, & Chung, Tai M. (2010). An architecture of access control model for preventing illegal information leakage by insider. Journal of the Korea Institute of Information Security and Cryptology, 20(5), 59-67.

Han, Seok-sil (2010). The study on the issues about qualitative research method. The Journal for the Study of Humans and Culture, 16, 5-44.

Im, To Bin (2009). Qualitative methodology: Approach and application. Journal of Governmental Studies, 15(1), 155-188.

Jang, Sang soo (2019). Introduction to information security. Seoul: baeumteo.

Kim, Eui-Tak, Choe, Yong-Rak, Kim, Gi-Hyeon, & Park, Jeong-Ho (1998). Access control technology trend. Review of KIISC, 8(4), 77-96.

Kim, Hyung-Joo & Kim, Soo-Heon (2017). A case study on the application of requirements standard of systems for government-affiliated organizations. Journal of the Korean Biblia Society for Library and Information Science, 28(2), 35-56.

https://doi.org/10.14699/kbiblia.2017.28.2.035

Kim, Yong (2007). A study on functional design of electronic management system in records centers. Journal of Korean Society of Archives and Records Management, 7(1), 61-82. https://doi.org/10.14404/JKSARM.2007.7.1.061

Korean Society of Archival Studies (2008). Archival terms dictionary.

Lee, Jeong-eun & Youn, Eun-ha (2018). A study on the major characteristics of the revised ISO 15489 in 2016. The Korean Journal of Archival Studies, 57, 75-111. https://doi.org/10.20923/kjas.2018.57.075

Lee, Ju Young, Lee, Goo Yeon, & Kwon, Ho Yeol (2020). Insider information leakage detection method using scenario technique. Journal of Digital Contents Society, 21(3), 617-626. https://doi.org/10.9728/dcs.2020.21.3.617

Lee, So-Yeon & Kim, Ja-Kyoung (2004). An analysis of functional requirements for electronic records management systems: Based on the records management principles extracted from ISO 15489. Journal of the Korean Society for Information Management, 21(3), 227-250. https://doi.org/10.3743/KOSIM.2004.21.3.227

Oh, Jin-Kwan (2019). A study on record management system design model and functional requirements. Doctoral dissertation, Major of Records and Archival Information Management, Graduate School of Records, Archives & Information Science, Myongji University.

Park, Minyoung (2013). Evaluation of access control function of the standard records management system. The Korean Journal of Archival Studies, 38, 3-35. https://doi.org/10.20923/kjas.2013.38.003

Sim, Jae-yoon & Lee, Kyung-ho (2015). A study on information access control policy based on risk level of security incidents about it human resources in financial institutions. Journal of the Korea Institute of Information Security and Cryptology, 25(2), 343-361. http://dx.doi.org/10.13089/JKIISC.2015.25.2.343

Son, Sung-Keun (2008). Analysis the issues and the present situation of the Korea government standard Records Management System. Master's thesis, Archival Science The Graduate School Seoul National University.

Yang, Seong-Hoon, Oh, Jung-Hyun, Lee, Kyoung Hyo, Im, Do-Yoen & Oh, Byeong-Kyun (2005). Role hierarchy access control model using permission inheritance. Proceedings of the Korean Information Science Society Conference, 32(2), 94-96.

Yong, Maroo (2016). Research on the access control to improve records management system. Master's thesis, Major of Records and Archival Information Management, Graduate School

of Records, Archives & Information Science, Myongji University.

ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION, ETC.. Act No.17358.

ACT ON THE PROMOTION OF INFORMATION SECURITY INDUSTRY. Act No.17344.

ENFORCEMENT DECREE OF THE PUBLIC RECORDS MANAGEMENT ACT. Presidential Decree No30584.

FRAMEWORK ACT ON NATIONAL INFORMATIZATION. Act No.16749.

Functional Requirements of Records Management Systems(v1.3). NAK 6:2020(v1.3).

Functional Requirements of Systems with Records Management for Government-Affiliated Organizations, etc.(v1.1). NAK 20:2020(v1.1).

Information and documentation - Records management - Part 1: Concepts and principles. KS X ISO 15489-1.

Information and documentation - Records management - Part 2: Guidelines KS X ISO TR 15489-2.

Information technology - Security techniques - Code of practice for information security management KS X ISOIEC27002.

Information technology - Security techniques - Information security management systems - Requirements. KS X ISOIEC27001.

Metadata Standard for Records and Archives Management(v 2.1). NAK 8:2016(v 2.1).

NATIONAL CYBER SAFETY MANAGEMENT REGULATION. Presidential directive No. 316.

PUBLIC RECORDS MANAGEMENT ACT. Act No16661.

Vital Records Identification and Protection(v 1.0). NAK 2-2:2012(v 1.0).