ERMS 표준에 나타난 접근통제 요건의 적용방안에 관한 연구

천 권 주*

[국문초록]

물리적인 환경에서는 기록관에 보관된 기록에 대해 출입을 통제하고 출입이 승인된 사용자에 대해서는 허가된 기록만을

* 육군기록정보관리단 기록물평가장교
주요논저: 「전자기록철의 구조와 관리방안」, 『한국기록관리학회지』, 2005; 「전자환경에서의 처분실행 방안에 관한 연구」, 『국가기록연구』 19, 2006; 「공공기관의 평가제도 」, 『한국기록관리학회지』, 2006; 「전자환경에서의 비밀의 속성 관리에 관한 연구」, 『국가기록원 기록인』, 2007 ; 「전자기록의 이관절차모형에 관한 연구 : OAIS 참조모형을 중심으로」, 『기록학연구』, 2007

www.kci.go.kr

이용하도록 제어함으로써 기록과 사용자 모두를 통제하여 기록을 안전하게 보호할 수 있었다. 그러나 기록관리환경의 전자화로 인해 고전적인 접근통제방식은 더 이상 고수하기 어렵게 되었으며 특히, 이용자중심의 기록관리 환경을 고려할 때 전자적 시스템에 의한 접근통제는 불가피해졌다. 이런 의미에서 본 논문은 전자적 접근통제의 기본적인 개념을 제공하고 전자기록관리시스템에서의 모범적인 모습을 서술한 영국, 유럽연합, 호주 및 미국의 ERMS 기능요건서를 분석, 상호 비교하였으며 비교적 상세한 가이드라인을 제공하고 있는 영국표준을 중심으로 적용가능한 표준 접근통제 기능요건을 제안하였다. 정리된 기능요건을 기록분류체계상에서 접근통제 준비, 배치 및 실행단계로 구분하여 적용함으로써 전자적 기록관리환경에서의 접근통제가 어떠한 방식으로 작동되는지 개념적으로 이해하고자 하였다.

주제어 : 접근, 접근통제, 기록분류체계, ERMS, 전자기록철, 기능요건

1. 서론

접근(access)이란 카탈로그, 색인목록, 검색도구 및 그 밖의 도구를 사용하여 적절한 정보를 찾게 하는 능력 또는 합법적으로 수립된 보안범주 내에서 참조 및 참고를 위해 정보를 검색하거나 찾아내도록 허가하는 것을 의미한다.[1] 한편, ISO 15489에서는 정보를 탐색하고 활용하거나 검색하는 권리, 기회 및 수단으로 설명하고 있다.[2] 종합해

1) Pearce-Moses, Richard, A Glossary of Archival and Records Terminology, Chicago: The Society of American Archivists, 2005, p.2

www.kci.go.kr

보면, 접근은 검색도구 등을 사용하여 일정한 권한 범위 내에서 이용자가 정보를 찾거나 활용 및 검색을 허용하는 것으로 설명할 수 있으며, 접근통제(access control)는 이러한 접근을 적절히 제어, 유지하는 것을 의미한다.

기록을 물리적으로 보존하던 과거의 방식에서는 서고의 출입문을 단속하고 기록이 보관된 공간에 대해 비인가권자의 접근을 인위적으로 제어함으로써 기록과 이용자 모두를 비교적 쉽게 통제할 수 있었다. 예를 들어, 보호되어야 하는 기록에 대해서는 보안등급을 부여하고 '관계자외 열람 금지'표시를 부착하며 이중 시건장치가 가능한 공간에 보관함으로써 기록이 불법적으로 이용되거나 변경되는 것을 차단할 수 있었다. 허가된 이용자가 기록을 열람할 경우에도 반드시 지정된 서식[3]에 따라 열람 일자, 열람자, 목적 등을 기록하게 하고 기록이 대여될 경우에도 일정한 권한을 가진 사용자가 이용자의 접근과 이용 여부를 확인하는 절차를 거치게 함으로써 허가된 사람만이 기록을 이용할 수 있었다.[4] 그러나 디지털시대에는 기록을 더 이상 물리적인 방식으로만 보존·관리할 수 없으며 비전자기록의 전자적 관리 경향, 온라인을 통한 실시간 서비스 보편화 등으로 기존과는 다른 형태의 접근통제 방식이 필요하게 되었다. 즉, 정보기기 사용의 보편화로 전자적 접근통제방식이 필요한데, 일차적으로는 일반적인 정보시스템의 위험요소인 해킹과 같은 불법적인 접근을 차단해야 함은 물론이고

---

2) ISO, ISO 15489-Information and Documentation - Records Management Part1 : General(ISO 15489-1), 2001, Clause 3.1

3) 국방부(육, 해, 공군 포함)에서는 해당 기록을 언제, 누가, 무슨 목적으로 열람했는지를 기록하도록 명시한 '비밀이력카드'제도를 적용하고 있다(군사보안업무시행규칙(부분개정:국방부 훈령 제797호('06.9.7)) 제1장 제3절).

4) 비밀의 경우는 대출과 지출의 반출행위가 있다. 전자는 비밀을 보관하고 있는 시설 내에서 참고의 목적으로 비밀을 이동시키는 행위이며, 후자는 비밀을 보관하고 있는 시설 밖으로 이동시키는 행위이다(군사보안업무시행규칙(부분개정:국방부 훈령 제797호('06.9.7)) 23조).

www.kci.go.kr

나아가서는 ISO 15489에서 적시하고 있는 기록의 접근요건도 만족시켜야 한다.[5] 따라서 네트워크 보안 등의 기술적 뒷받침을 바탕으로 조직에서는 누가 기록에 접근할 수 있는지 그리고 어떤 방식으로 접근할지를 규제하는 공식적인 지침을 보유해야 하며 조직의 내부 및 외부 이용자 모두에게 적용되어야 한다. 접근이 제한되는 기록은 업무요구나 규제환경과 같은 특별한 요구가 있을 경우에만 허가될 수 있고 접근을 제한할 필요성은 시간이 지남에 따라 변할 수 있으며 적절한 접근통제를 위해서는 기록과 개인 양쪽 모두에 접근조건을 부여해야 한다. 그리고 이러한 것들은 전자적 시스템으로 구현되어 체계적으로 관리되어야 한다.

따라서 본 논문의 목적은 과거의 단순한 물리적 방식의 기록보호와 이용자 제어에서 벗어나 ERMS라는 전자기록관리 환경하에서 기록에 접근하는 사람에 대한 통제는 물론, 불법적인 접근을 통한 임의삭제나 변경으로부터 기록을 보호하기 위한 방식이 어떻게 작동되는지를 고찰하는 데에 있다. 이를 위하여 문헌조사방법을 이용하고자 하며 우선, 각국의 ERMS 표준에 나타난 접근통제 기능요건을 비교분석하여 필수요건과 선택요건을 식별하였다. 식별된 표준 접근통제 요건을 접근통제 준비, 배치 및 실행이라는 세 단계로 구분하여 기록분류체계상에서의 실행방안을 모색해 보았다.

기록관리분야에서 접근통제를 직접적으로 다룬 연구결과는 찾아보기 힘들다. 다만, 이소연·김자경은 기록관리 국제표준인 ISO 15489를 기록관리 기능영역별[6]로 분석하여 기록관리원칙을 추출하고 미국, 영국, 유럽연합의 전자기록관리시스템 설계에 관한 표준 또는 모형의 기능요건을 ISO 15489의 기능영역별 요건에 대입하여 분석함으로써 기

5) ISO, 2001, Clause 9.7

6) '획득', '등록', '분류', '저장', '접근', '추적', '처분'의 7개 기능영역으로 구분하였다.

www.kci.go.kr

록관리시스템 설계를 위한 기능요건을 규명하고자 하였다.[7] 그러나 기록관리시스템 설계를 위한 기능요건 전체를 포괄적으로 다루다 보니 특정부분에 대한 세밀한 연구가 수행되지 못한 한계점도 있다.[8]

보존위주에서 이용중심의 기록관리 패러다임이 전환되고 있는 현시점에서, 사용자가 원하는 정보를 편리하고 쉽게 실시간으로 받아볼 수 있는 여러 조치들을 이행하여 고객만족을 달성하는 것은 분명 중요하다. 그러나 기록에 대한 불법적인 접근을 막고 비인가자에게 노출되거나 삭제되지 않도록 적절한 보호대책을 강구해야 함을 간과해서는 안된다. 아울러 사람에 대한 통제, 기록에 대한 통제, 사람과 기록의 동시 통제방안 등이 보다 더 자세히 연구되어야 하며, 전자환경에서의 접근통제 방안을 개념적으로만 다룬 한계점을 극복하기 위해서는 공학적 측면의 접근법을 포함한 보다 세밀하고 학계간의 연계된 연구가 병행되어야 한다.

2. 각국의 ERMS 접근통제 기능요건 분석 및 표준요건 도출

전자기록관리시스템을 설계함에 있어 반드시 필요한 요건들을 표준화한 문서들은 ISO 15489를 기반으로 전자기록관리를 역점적으로 수행하고 있는 나라에서 속속 발표된 바 있다.[9] 본 논문에서는 전자기록

7) 이소연 외, 「전자기록관리시스템(ERMS) 설계표준의 기능요건 분석-ISO 15489를 기준으로-」, 『정보관리학회지』 제21권 제3호, 2004

8) 대부분의 접근통제와 관련된 연구는 주로 컴퓨터, 네트워크, 정보보호 등 이공계분야에서 진행되고 있다.

9) 대표적인 ERMS 표준은 아래의 웹사이트를 통해 확인할 수 있다.
영국 : http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/default.htm
유럽연합 : http://www.cornwell.co.uk/edrm/moreq.asp
호주 : http://www.naa.gov.au/records-management/publications/ERMS-guidelines.aspx

www.kci.go.kr

관리시스템 설계를 위한 기능표준을 고찰하고자 하며 접근이 상대적으로 용이하고 비교적 자세한 가이드라인을 제공하고 있는 영국, 호주, 유럽연합, 미국의 4개국으로 한정하여 살피고자 한다.

각국의 ERMS 설계표준이나 참조모형은 서로 비슷하지만 일대일 대응관계가 아니며, 전개방식과 요건별 그룹핑 구조도 조금은 상이하다. 어떤 표준에서는 의무사항이지만 다른 표준에서는 선택사항이 되거나 혹은 배제되기도 한다. 무엇보다도 각국의 ERMS 설계표준 자체는 각각의 권위 있는 국립기록청에서 발표한 것으로 자국의 기록관리환경에 맞도록 모범적으로 작성되었으므로 신뢰할 수 있다고 판단된다. 그럼에도 불구하고 각국의 접근통제 요소를 매핑하여 분석하고자 하는 것은 보다 신뢰 있고 누구나 타당하게 수용할 수 있는 모범적인 표준요건을 제시하기 위함이다. 특히, 매핑의 기본틀은 4개국 중 보다 자세한 지침을 제공하고 있는 영국을 기준으로 하였다.[10]

각국의 접근통제와 관련된 1차 하위영역은 <표 1>과 같이 정리할 수 있다. <표 1>을 바탕으로 1차 하위영역에 포함된 세부 기능요건들을 매핑[11]하여 분석하였으며, 적어도 2개 국가 이상에서 공통적으로 식별되는 요소이면 받아들일 수 있는 요건으로 제안하였다.[12]

미국 : http://jitc.fhu.disa.mil/recmgt/p50152stdapr07.pdf

10) 호주에서는 국제기록관리 표준인 ISO 15489의 전신인 AS ISO 15489를 제정하였으며, 영국은 2002년에 표준요건을 발표한 이래 전자기록관리에 관한 다양한 지침서를 제시하고 있다. 유럽연합의 경우는 2001년 최초 출시된 MoReq을 보완하여 2008년 4월에 MoReq2를 발표하였고 미국도 기존의 DoD를 2007년 4월에 보완한 바 있다. 따라서 4개국의 ERMS 표준들만을 벤치마킹하여도 충분히 신뢰할 수 있다고 판단된다.

11) 각국의 ERMS 기능요건 설계표준의 매핑은 영국 국립기록청의 'Requirements for Electronic Records Management systems, 3: Reference Document(2007)'를 기준으로 하되 호주 국립기록청의 기능표준도 함께 참조하였다. 자세한 요건별 매핑은 부록을 참조하라.

12) '보관인(Custodian)', '프라이버시와 기록열람'은 영국에서만 채택하고 있는 요건이므로 논의에서 배제하였다. '보관인'은 사용자나 일정한 그룹이 전자기록철이나 기록에 대한 책임 있는 보관자로 식별되도록 정의한 요건이고, '프라

www.kci.go.kr

<표 1> 각국의 ERMS 설계표준(요건모형)에 나타난 접근통제와 그 하위요소의 1차 분류

영국 (Access control)	유럽연합 (Controls and Security)	호주 (Access and Security)	미국 (Access controls)
ERMS로의 접근 접근통제 표시 사용자 프로파일 역할 그룹 접근통제의 배치 보관인(Custodian) 접근통제 표시 실행 프라이버시와 기록열람	접근 감사증적 백업과 복구 기록추적 진본성 보안범주	시스템 접근 접근과 보안통제 사용자 프로파일 접근과 보안어플리케이션 접근과 보안메타데이터 발췌사본(Extraction) 감사증적	별도의 하위요소 없이 7가지 개별 요건으로 설명

* 주 : MoReq2에서는 MoReq(2001)의 '통제와 접근'의 하위요소 중, '기록추적', '진본성' 및 '보안범주'가 다른 영역으로 이동되었으며, 최종적으로는 '접근', '감사증적', '백업과 복구', '필수기록'으로 발표되었다. 미국의 DoD는 '일반사항', '의무요건', '비밀기록 관리', '프라이버시 및 정보공개법을 위한 기록관리', '이관', '선택요건', 으로 구성되어 있으며 접근통제는 의무요건의 하위요소에서 설명되고 있다.
* 자료 : 각국의 ERMS 설계표준(요건모형)서의 목차 부분을 재정리

1) ERMS로의 접근

이 영역에서는 ERMS에 접근하기 위해 일정한 인증 및 접근에 관한 메커니즘을 제공해야 한다는 요건을 중점적으로 다루고 있다. 예를 들어, 통합 네트워크 로그인 장치를 통해 전자기록관리시스템으로 접근을 지원할 수 있어야 하고 '신규 사용자 정의 및 식별', '현사용자를

이버시와 기록열람'은 데이터 보호(DP), 정보공개(FOI), 환경 정보취득(EIR)에 대한 전자기록철이나 기록 그리고 발췌기록(extract)의 점진적인 추가(addition)를 지원하도록 한 요건이다.

www.kci.go.kr

비활성(inactive)상태로 전환', '현 사용자 삭제' 기능도 포함되어야 한다. 또한 기록분류체계내의 일부 영역에 대한 관리행위를 일정한 권한을 가진 사용자가 수행할 수 있어야 한다. 즉, 조직 전체의 기록분류체계는 해당 조직의 관리자만이 담당하도록 해야 하지만, 인사와 같은 특정분야의 경우는 인사담당 부서에서 관리할 수 있다. 각국의 기능요건을 매핑하여 4가지 모두를 의무요건으로 채택하였다.

요건 1. 일정한 인증 및 접근통제에 관한 메커니즘 제공.
요건 2. 로그인 장치를 통한 접근지원 메커니즘 제공.
요건 3. '신규 사용자 정의 및 식별', '사용자 비활성(inactive)상태로 전환', '사용자 삭제' 기능 구비.
요건 4. 특정 사용자가 분류체계의 일부에 대한 관리권한 수행.

2) 접근통제 표시

접근통제 표시는 일정한 권한에 따라 등급화되는 사용자를 포함하여, 전자기록철이나 기록이 기록분류체계로 배치되기 전에 적용되어야 한다. 이러한 임무는 조직내의 기록관리책임자나 관리자와 같이 일정한 권한을 부여받은 사람이 수행하는데 초기단계에서 특별한 조치가 없다면 사람과 기록 모두에는 기본 값이 부여된다. 조직의 환경과 정책 등이 변경되어 접근통제를 강화할 필요가 있는 경우라면 초기값은 변경될 수 있다. 이 영역에서는 6개요건 모두를 의무로 채택하였다.

요건 5. 접근통제표시를 사용자 및 기록 객체가 파일플랜[13]에 배치

13) 영국국립기록청에서는 전자기록의 계층구조를 '클래스-폴더(파트)-기록-컴포넌트'로 구분하여 설명하고 있는데 '클래스-폴더(파트)-기록-컴포넌트'는 여러 객체 세트로 구성될 수 있다. 이러한 세트의 집합을 파일플랜이라 부르는데 분

www.kci.go.kr

되기 전에 적용.

요건 6. 접근통제에 관한 사항은 권한을 가진 사용자만 수행.

요건 7. 사용자가 기록관리환경에서 접근행위를 수행토록 지원

요건 8. 허가받지 않은 사용자가 접근통제 사항을 전자기록철이나 기록에 적용할 수 없도록 제한.

요건 9. 최소 5가지 계층적 보안범주(평문, 취급제한, III급, II급, I급)를 지원.

요건 10. 사전 정의된 개별 사용자, 사용자 그룹의 식별을 지원.

3) 사용자 프로파일

사용자 프로파일은 개인의 접근권한에 관한 사항과 기록분류체계 내에서 사용할 수 있는 특정 기능에 대한 세부사항을 정의해 놓은 것이다. 따라서 프로파일의 값에 따라 사용자는 특정 기록에 접근할 수도, 못할 수도 있다. 권한을 부여 받은 사람은 특정 전자기록철에 접근하여 기록건을 추가하고 철을 종결할 수 있는 반면, 다른 사용자에 대해서는 전자기록철에 포함된 기록에 대한 열람권만 주어지기도 한다. 프로파일은 고정된 것이 아니라, 업무가 변화함에 따라 개별적으로 서로 다른 접근 요구에 의해서 또는 조직의 변화에 따라 변경되기도 한다. 이 영역에서는 6개의 의무요건을 채택하였다.

요건 11. 사용자별 권한과 의무의 정의, 이에 대한 프로파일 지원.

요건 12. 단일 보안 카테고리, 사전 정의된 여러 접근그룹의 멤버쉽 지원(수행주체 : 관리자).

류체계와 유사한 개념이다(설문원 외, 「전자기록철의 구조와 관리방안:영국 ERMS 표준을 중심으로」,『한국기록관리학회지』 제5권 제2호, 2005, 51쪽). 따라서 본 논문에서는 기록분류체계와 파일플랜을 혼용하도록 한다.

www.kci.go.kr

요건 13. 사용자는 여러 그룹에 소속될 수 있으며 기본적으로 최하위 보안카테고리를 보유.

요건 14. 보안범주는 역할(role)로부터 자동 상속, 필요시 다른 값으로 변경.

요건 15. 사용자는 하나 이상의 그룹의 구성원이 될 수 있음.

요건 16. 사용자 프로파일(개인, 그룹)의 변경은 어떤 시기라도 가능.

4) 역할

역할(role)은 예견되는 행위나 권한 또는 의무사항들이 담기게 되는 일종의 세트로 전자기록관리시스템에서는 사용자 역할 세트[14] (definition of a set of user roles)를 정의하여 모든 사용자에게 지원한다. 역할을 통해 사용자는 일정한 기능을 행사할 수 있는 권한을 부여받게 된다. 요건을 매핑한 결과 4개의 의무요건과 1개의 선택요건으로 정리하였다.

요건 17. 특별한 기능 혹은 그룹 기능에 대해 일정한 배치권한(기능통제)을 통제하는 사용자 역할 세트 필요. 역할의 정의와 커스터마이즈 권한은 관리자에게만 부여.

요건 18. 모든 사용자들은 하나 이상의 사용자 역할에 배치.

요건 19. 사용자 역할에 의해 허가된 기능만을 수행할 수 있도록 전자기록관리시스템에 대한 접근을 제한해야 함.[15]

---

14) 전자기록관리환경에서 관리자는 조직에 부합되는 적절한 역할을 정의할 수 있다. 역할은 사용자들에게 기능적 권한(functional rights)을 취급하거나 부여함에 있어 편리한 방법을 제공한다. 예를 들어, 전형적인 일반 사용자는 파일플랜내의 기능권한 중 기본 수준만을 제공받는다.

15) 유럽의 경우는 전자기록의 진본성 보호를 위해 '사용자 역할 및 엄격한 시스템관리기능'이라는 기준에 따라 시스템으로의 접근을 제한하도록 하고 있다.

www.kci.go.kr

요건 20(선택요건). 일정한 기능을 사용자에게 지원할 수 있는 사용자 역할 모델의 지원.[16]

요건 21. 보안범주와 정의된 접근통제그룹멤버쉽을 역할로 배치할 수 있어 함.

5) 그룹

기록관리시스템에서는 필요에 따라 접근통제 그룹을 미리 정의함으로써 효율적인 접근통제를 달성할 수 있다. 이 방법을 통해 사용자들은 접근통제 그룹에서 추가되거나 삭제될 수 있다. 경우에 따라서는, 사용자 그룹을 특정 클래스로 배치함으로써 그룹 구성원들은 해당 클래스와 하위의 기록철 및 기록에 모두 접근할 수 있다. 각국의 요건을 비교한 결과, 4개의 요건 모두를 의무로 채택하였다.

요건 22. 이미 정의된 접근통제그룹의 정의를 지원. 사전 정의된 접근통제그룹에서는 업무와 다른 기능그룹(functional groups)의 식별을 통해 사용자는 그룹의 회원이 될 수 있음.

요건 23. '새로운 그룹의 정의', '특정 그룹 비활성화(inactive) 조치', '그룹 삭제' 기능을 보유해야 함.

요건 24. 어떠한 사용자에 대해서라도 접근통제그룹에서 추가되거나 삭제될 수 있는 기능을 지원.

요건 25. 필요시, 하나의 접근통제그룹을 클래스에 배치할 수 있어야 함. 이를 통해 그 그룹에 속한 모든 사용자들은 승인된 클래스와 하위 클래스만으로 접근 가능함.

---

16) 두개 이상의 요건에서 채택되지 않았지만, 역할모델은 참고의 필요성이 있으므로 선택요건으로 제시하였다. 2008년에 출시된 MoReq2에서도 역할모델을 채택하고 있다.

www.kci.go.kr

6) 접근통제의 배치

이 영역에서는 모든 유형의 접근통제 표시를 기록분류체계내의 객체에 배치하는 것과 관련된 요건을 다루고 있다. 즉, 모든 비밀의 표시(보호표시)나 사전에 정의된 사용자 그룹, 개별 사용자들의 모든 조합을 기록 객체에 적용함으로써 분류체계내에서 효과적인 접근통제를 달성하고자 하였다. 각국의 요건을 분석한 결과 13개의 의무요건과 2개의 선택요건으로 정리할 수 있다.

요건 26. 모든 유형의 접근통제표시를 클래스, 전자기록철, 전자기록으로 배치할 수 있어야 함.

요건 27. 보호표시, 정의된 사용자 그룹 및 개별 사용자의 모든 조합을 클래스, 폴더와 기록으로 배치.

요건 28. 전자파트는 해당 전자기록철의 접근통제를 항상 상속.

요건 29. 하나의 보안범주가 하나의 기록객체에 배치되어야 함(초기값 : 파일플랜의 최하위 값으로 자동으로 부여)

요건 30. 클래스 하위에서 생성되는 모든 전자기록철의 접근통제값은 클래스로부터 상속됨. 필요시 전자기록철 수준에서 특별한 보안범주가 배치될 수 있음.

요건 31. 전자기록철에 상위의 보안범주가 배치된 경우, 해당 철의 하위에 생성된 전자기록철의 보안범주는 자동으로 업그레이드되어야 함.

요건 32. 필요시, 관리자는 어버이 전자기록철에 배치된 기록이 해당 철의 보안범주 보다 낮게 유지되도록 지원.

요건 33. 전자기록철에 배치된 기록의 최고 보안 범주로 전자기록철의 보안범주를 갱신할 수 있어야 함.

www.kci.go.kr

요건 34. 관리자는 특정 기록에 대해, 상위의 전자기록철보다 높은 보안범주를 지정할 수 있어야 함.

요건 35. 파일플랜내의 보다 유연한 관리를 위해 기술자(descriptor)를 전자기록철이나 기록에 대한 메타데이터의 한 요소로서 추가할 수 있어야 함.

요건 36. 클래스, 전자기록철, 기록에 대한 접근통제표시를 수정할 수 있는 기능을 보유해야 함.

요건 37. 클래스, 전자기록철, 기록에 대한 과거의 접근통제 표시, 수정날짜 등을 이력 메타데이터로 보유.

요건 38. 보안범주들은 일정한 기간 동안 유효해야 하며, 유효기간이 종료되면 모든 사용자들이 접근할 수 있도록 최하위 또는 이미 설정된 값으로 갱신되어야 함.

7) 접근통제 표시 실행

이 영역에서는 기록분류체계내에 배치 또는 부여된 접근통제 사항들이 사용자나 기록을 중심으로 어떻게 실행되는 지에 대해 논의되고 있다. 예컨대 어떤 사용자가 전자기록철에 접근하고자 하면, 시스템에서는 사용자의 접근통제 값과 전자기록철에 대한 접근통제 값을 비교함으로써 접근을 허가하거나 통제하게 된다. 사용자가 전자기록철에 접근하더라도 사용자의 보안범주가 특정 기록건의 등급보다 하위일 경우에는 그 기록을 열람할 수 없다. 사용자가 검색행위를 수행할 경우, 열람이 제한되는 기록 객체에 대한 메타데이터 자체는 결과값으로 제공조차 되지 않을 수 있다. 각국의 요건을 비교·분석한 결과 8가지 요건을 의무로 채택하였다.

요건 39. 특별한 제한이 없다면, 최하위 보안범주로 지정된 모든

www.kci.go.kr

사용자들은 파일플랜 전체로 접근할 수 있어야 함.

요건 40. 특정 보안범주와 동등 또는 그 이상의 수준인 사용자를 제외하고는 파일플랜내의 접근을 제한할 수 있어야 함.

요건 41. 사전에 정의된 접근통제 그룹이 배치된 클래스, 전자기록철 및 기록에 대한 접근을 해당 그룹의 멤버들로만 제한.

요건 42. 사전에 정의된 하나 이상의 접근통제 그룹에 배치된 클래스, 전자기록철 및 기록에 대한 접근을 제한할 수 있어야 함.

요건 43. 사전에 하나 이상의 사용자로 구성된 접근통제표시를 클래스, 전자기록철 및 기록에 배치하여 접근을 제어할 수 있어야 함.

요건 44. 하나 이상의 형태로 구성되는 접근통제표시에 따라 클래스, 전자기록철 및 기록으로의 접근을 제어할 수 있어야 함. 이때 모든 등가의 접근통제 표시(equivalent access control markings)를 가진 사용자로만 제한됨.

요건 45. 아래와 같은 접근통제메커니즘 행위를 정의할 수 있는 구성옵션을 제공해야 함.

- 접근이 허용되지 않는 사용자는 객체 자체와 메타데이터를 확인하거나 찾을 수 없도록 해야 함.
- 필요하다면, 검색결과 내의 메타데이터 정도는 볼 수 있도록 허용되어야 함(기록의 내용은 제외).

요건 46. 접근이 허용되지 않은 사용자는 풀텍스트(full-text) 검색의 결과에도 불구하고 객체의 내용과 메타데이터 등 어떠한 검색값도 확인할 수 없어야 함.

www.kci.go.kr

3. 표준요건의 적용

분류체계는 검색은 물론, 평가와 처분, 접근제한과 보안관리 등 기록관리의 여러 기능을 수행하는 데에 근간이 되므로 기록관리시스템의 심장이라고 일컫는다.[17] 따라서 분류체계는 엄격한 업무분석에 따라 개발되어야 하며 기록은 이러한 분류체계상에서 적절한 위치를 할당받게 된다.[18] 그리고 배치된 기록을 관리하거나 이용하기 위해서는 분류체계에 접근해야 한다.[19] 이런 의미에서 기록이나 이용자에 대한 접근통제가 분류체계내에서 어떠한 모습으로 이행되는지 살펴보는 것은 의미 있는 작업이다. 본 장에서는 앞서 정리된 표준 접근통제요건을 비교적 자세한 설명과 지침을 제공하고 있으면서 기록분류체계와 유사한 영국의 '파일플랜'을 중심으로 고찰하고자 한다. 이를 통해 파일플랜을 구성하고 있는 객체 즉, 클래스, 전자기록철에서 접근통제기능이 어떤 방식으로 작동되는지 이해할 수 있다. 다만, 2장의 '1)ERMS로의 접근'~'5)그룹'영역은 대부분 접근통제를 위한 전제사항에 해당되므로 준비단계로 통합하여 고찰하였다.

1) 접근통제 준비단계

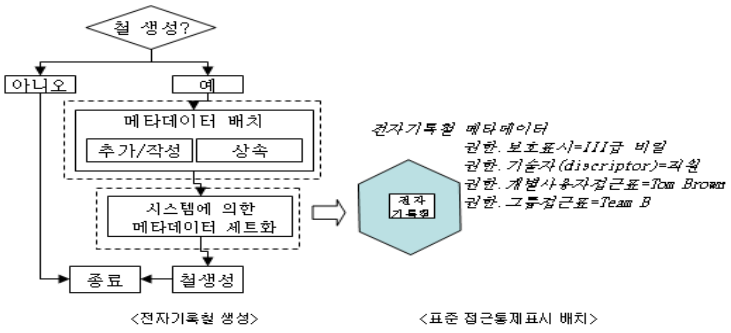
개별 사용자는 조직이 정한 일정한 인증절차 즉, 공인인증서나 패스워드를 통해 사용자 권한을 부여 받는데(요건 1, 요건 2), 이것은 비단 접근통제만이 아니라 기록관리시스템 사용을 위한 가장 기초적인 사항이다. 만약, 특정 사용자가 해당 조직을 떠나 장기간 타기관이나 부

17) 설문원 외, 2005, 50쪽
18) 같은 글, 51쪽
19) 불특정 다수의 이용자가 기록을 이용하고자 할 경우, 분류체계가 아닌 일반적인 검색창으로 접근할 수도 있다.

www.kci.go.kr

서에 장기 파견 근무를 한다면, 일정한 권한을 가진 사용자는 사용자 프로파일 속성을 '활성'상태에서 '비활성'으로 변경하여 원소속 부서의 권한으로 관리되는 기록분류체계내에서 기록관리에 관한 권한을 행사할 수 없도록 조치할 수 있다(요건 3). 한편 기관의 기록관리자는 처리과의 기록관리자들이 자신이 속한 처리과의 기록분류체계상의 개체만 관리할 수 있도록 해야 하며 다른 처리과의 분류체계로는 접근할 수 없도록 제한함으로써 기록의 불법적인 변경과 삭제를 막을 수 있다(요건 4).

전자기록관리시스템에서 기록객체가 생성되려면 '추가 및 작성' 또는 '상속'의 방식에 따라 기록객체에 대한 메타데이터 생성이 선행되어야 한다. 생성된 메타데이터는 시스템을 통해 세트화 과정을 거치게 되며 기록객체들이 기록분류체계에 배치됨과 동시에 시스템에 의해 감사증적도 시작된다. 이때, 기본적인 표준 접근통제 사항이 배치된다 (<그림 1>).



<그림 1> 전자기록철을 통해본 기록객체의 생성과 메타데이터 배치

* 주 : 점선은 시스템에 의한 자동 감사증적의 시작을 의미.

* 자료 : U.K, Requirements for Electronic Records Management systems, 3: Reference Document(2007), p. 41과 2002 rational for functional requirements <http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

www.kci.go.kr

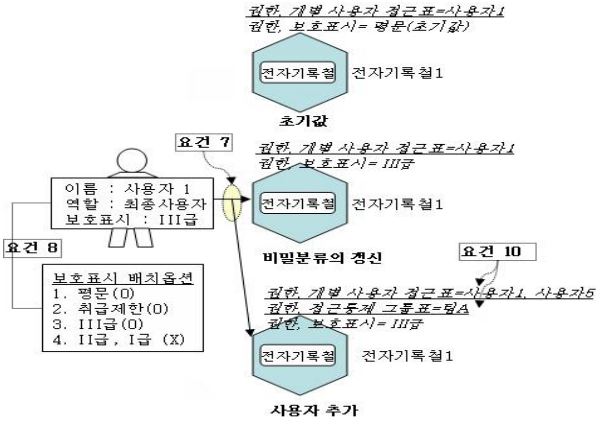
이때 적용되는 접근통제는 전자기록관리시스템 사용자를 위한 표준 접근통제표시와 기록분류체계의 객체들에 적용되는 표준접근통제표시가 있는데, 전자는 '단일 보안범주', '보안기술자', '특정 접근그룹에 대한 멤버쉽'으로 구성되고 후자는 '보안범주', '보안기술자(security descriptor)', '두 개의 분리된 접근통제표(개별 사용자, 사용자 그룹)'로 구성된다. 이러한 접근통제표시 메타데이터 배치는 일정한 권한을 가진 사용자만이 수행(요건 6)할 수 있으며, 기록관리 메타데이터 요소 중 '권한(Rights)'에 '권한.***'와 같은 방식으로 기록된다.[20] 표준 접근통제 메타데이터 중 보안범주는 평문으로부터 I급에 이르는 최소 5가지로 정의되는 등급이 사용자와 기록객체 모두에 한 등급씩 부여된다(요건 9). 보안기술자 메터데이터는 기록분류체계내의 객체에 대해 어떤 보안기술자가 배치 또는 상속되었는지를 나타내는 것으로 '0', '1' 또는 '다수 값'이 지정될 수 있다. 객체에 대한 접근은 일정한 동일 자격의 다수로 형성되는 접근그룹이나 개별적인 사용자의 형태로 적용된다.

'요건 5'에 따라 사용자와 기록객체에 대한 접근통제표시는 파일플랜에 배치되기 전에 이루어져야 한다. 파일플랜에서 전자기록철은 클래스 하위에서 생성되면서 접근통제 사항이 설정되는데, 기록관리시스템에서는 사용자 및 전자기록철의 배치에 앞서, 요구되는 모든 접근통제 표시를 정의할 수 있도록 지원해야 한다. 따라서 기록관리시스템에서는 사용자, 클래스, 전자기록철, 기록건의 배치 준비를 갖추고 접근통제 표시속성(access control marking properties)을 정의하고 유지할 수 있어야 한다. 그러나 특별한 이유가 없다면, 대부분의 접근통제 메타데이터 값은 상속의 방식에 의한다. <그림 2>에서 ERMS 관리자는 '전자기록철1'에 대한 메타데이터를 갱신하여 사용자1을 '권한. 개별 사용자 접근표'필드에 등록하였다. 보안분류 III급은 사용자1의 프로파

20) <http://www.nationalarchives.gov.uk/documents/metadatafinal.pdf>[2008.10.25 인용]

www.kci.go.kr

일에 배치되어 있다(<그림 2의 상단부분>). 이때, 최초 사용자1에게 부여되는 접근통제 등급으로는 전자기록철의 메타데이터를 수정할 수 없다. 그러나 사용자1이 해당 전자기록철의 메타데이터를 수정할 수 있는 권한을 보유한 경우라면 전자기록철1의 접근메타데이터를 평문에서 III급으로 갱신할 수 있다. 또한 사용자1이 부여된 권한에 따라 사용자5와 사용자 그룹인 팀A를 접근통제표에 추가하였으므로 이들은 전자기록철1에 접근할 수 있다(요건 7). 다만 사용자1은 III급 이하의 보안수준에 대해서만 관여할 뿐 II급 비밀과 같은 값은 배치할 수 없으며(요건 8), 시스템에서는 메타데이터 값의 비교를 통해 사용자1이나 사용자5, 팀 A와 같은 개별 및 그룹사용자를 식별할 수 있다. 이것은 이용자들이 전자기록, 전자기록철 및 클래스로 접근할 수 있도록 개별 사용자나 정의된 사용자 그룹을 식별해 낼 수 있는 접근통제 표시의 사용을 지원해야 하는 '요건 10'에 해당한다.



<그림 2> 메타데이터 갱신, 보호표시 배치권한 제한, 사용자 식별지원

* 자료 : 2002 rationale for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

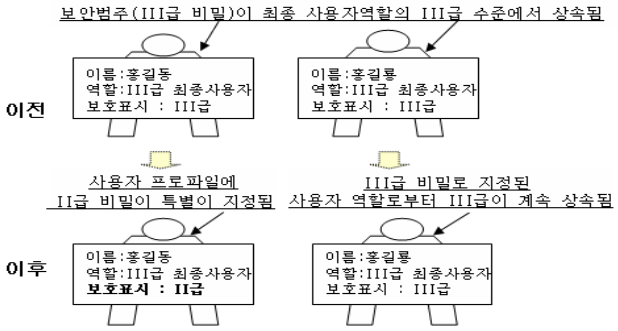
www.kci.go.kr

기록관리시스템에서는 시스템에 알려져 있는 개별 사용자를 위한 사용자 프로파일에 대한 정의를 할 수 있어야 한다. 하나의 사용자 프로파일은 사용자에 해당하는 기능적 역할을 항상 식별할 수 있어야 하며 그 사용자에게 접근통제표시를 배치할 수 있도록 허용해야 한다(요건 11). 사용자 아이디 및 패스워드와 같이 인증을 위한 정보가 필요하며, 관리자는 시스템 내에서 사용자 프로파일을 생성, 편집, 삭제할 수 있어야 한다(요건 16). 만약 프로파일이 존재하지 않으면 전자기록관리시스템 내에서의 사용자 행위를 추적 및 관리할 수 없게 된다. 앞의 <그림 2>에서와 같이 사용자1은 III급이라는 보안등급을 부여받고 있고 전자기록철에 팀A와 같은 접근그룹을 배치할 수 있는 것처럼 관리자는 단일 보안 카테고리, 사전 정의된 여러 접근그룹의 멤버쉽 지원할 수 있어야 한다(요건 12). 이때 사용자는 하나 이상의 접근그룹에 소속될 수 있지만 반드시 하나의 보안등급만을 부여 받아야 한다(요건 13)(요건 15). 한편, 보안범주가 하나의 역할(role)로부터 상속되어질 수 있도록 설계된 전자기록관리시스템에서는 상속된 역할을 대치할 수 있는 다른 역할을 개별 사용자 수준으로 배치될 수 있어야 한다(요건 14).

기록관리시스템의 관리자는 개별 사용자 프로파일에 접근통제 표시를 배치할 수도 있지만 일련의 예견되는 행위, 권한과 의무의 집합을 의미하는 '역할'의 정의를 통해 접근통제를 수행할 수도 있다. 사용자들은 관리자로부터 역할을 통해 일정한 기록관리행위를 행사할 수 있는 하나 이상의 권한을 부여받을 수 있는데, 일반 사용자에게는 기본적인 기록관리행위를 수행할 수 있는 수준의 권한만이 제공되며 부여받은 사용자 역할 이상의 수준이 요구되는 클래스나 전자기록철로는 접근이 허용되지 않는다(요건 17)(요건 18)(요건 19). 필요하다면 일반 사용자, 처리과 책임자, 부 및 실 책임자, 기관책임자 등으로 구분되는

www.kci.go.kr

수준별 역할을 개별적으로 정의하여 지원할 수도 있다. 이것을 사용자 역할모델[21]이라 하는데 각각의 사용자는 역할모델에 따라 차등화된 기록관리행위를 수행하게 된다(요건 20). 예를 들어, 일반 직원은 파일 플랜내에서 클래스를 추가할 수 없지만 기관의 기록관리자는 가능하다. 역할의 마지막 요건으로, 전자기록관리시스템에서는 보안범주와 사전에 정의된 접근통제그룹멤버쉽을 역할로 배치할 수 있는 기능도 보유해야 한다(요건 21).



<그림 3> 사용자 역할 프로파일의 상속과 갱신[요건 21 적용]

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

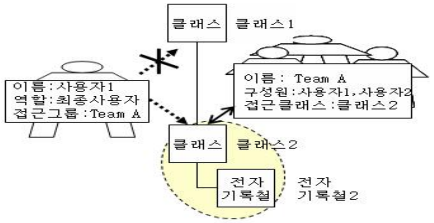
<그림 3>에 따르면, 홍길동과 홍길룡에는 III급 비밀이 적용된 사용자이다. 관리자가 홍길동의 역할 프로파일을 한 단계 높은 수준인 II급으로 상향 조정하면, 최초 상속된 III급 대신 II급이 우선 적용된다. 반면, 아무런 갱신작업이 없었던 홍길룡의 비밀등급은 III급으로 계속 유지된다.

전자기록관리시스템에서는 <그림 4>의 Team A와 같이 이미 정의된

21) 세부적인 내용은 http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/default.htm 의 'Revised Reference Document'를 64쪽을 참조.

www.kci.go.kr

접근통제그룹의 정의를 지원해야 한다. 사전 정의된 접근통제그룹에서는 업무와 다른 기능그룹(functional groups)을 식별해서 원칙적으로 어떤 사용자는 특정 그룹의 한 회원이 될 수 있다. 그리고 이러한 배치 및 재배치에 관한 권한은 관리자에게로만 국한시켜야 한다(요건 22).



<그림 4> 제한된 클래스 접근 허용[요건 22, 25 적용]

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

접근통제그룹의 멤버쉽(Membership of an access control group)은 권한을 가진 사용자만이 일정한 ERMS 영역에 접근하여 필요한 행위를 수행하도록 보장해주는 하나의 방법으로 보통, 개별 사용자의 이름이 포함된다. 특정 그룹에 대해서 이 그룹이 처음 만들어지는 시점 또는 경우에 따라 생애내내 동안 줄곧 비어있을 수도 있고 개별적인 사용자들이나 다른 접근통제 그룹들이 포함될 수 있다. 한편, '요건 3'에서 사용자의 기능에 대해 '활성화' 또는 '비활성화' 조치를 취한 것처럼 특정 접근통제그룹에 대해서도 동일한 개념의 행위를 수행할 수 있으며 접근통제그룹내의 사용자가 삭제되거나 추가될 수 있다(요건 23)(요건 24). 또한 반드시 요구되는 것은 아니지만, 하나의 접근통제그룹을 클래스에 배치할 수 있어야 하며, 이를 통해 그 그룹에 속한 모든 사용자들은 승인된 클래스(하위 클래스 포함)로만 접근할 수 있다(요건 25)(<그림 4> 참조). <그림 4>에 의하면, 관리자는 '클래스2'를

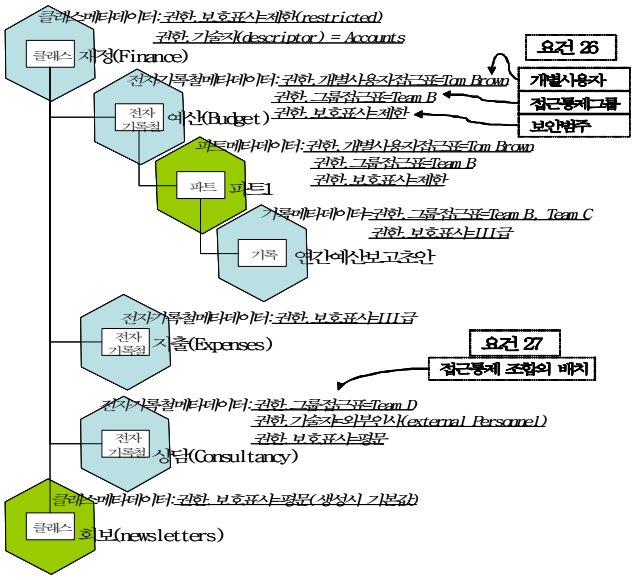
www.kci.go.kr

'Team A'로 배치했다. 다른 조치가 이루어지지 않으면, Team A의 멤버인 사용자1은 클래스2와 하위의 전자기록철로만 접근이 허용된다.

2) 접근통제 배치단계

기본적으로, 모든 유형의 접근통제표시를 클래스, 전자기록철, 전자기록으로 배치할 수 있어야 한다(요건 26)(<그림 5>). 접근통제표시는 앞서 제시된 바와 같이, '보안범주', '사전 정의된 접근통제 그룹', '하나 이상의 개별 사용자 이름이 포함된다. 그리고 전자기록관리시스템에서는 모든 보호표시, 사전 정의된 사용자 그룹 및 개별 사용자 이름들의 모든 조합을 클래스, 전자기록철과 기록으로 배치할 수 있어야 한다(요건 27)(<그림 5>). 즉, 전자환경에서는 물리적인 환경에 비해 보다 더 조직적인 방식으로 접근통제가 적용되어야 하며 따라서 효율적인 기록관리를 위해 여러 가지 최선의 조합을 통해 분류체계 전반에 대한 보안통제를 지원할 수 있는 다양한 접근통제표시가 적용될 수 있어야 한다. 또한 전자기록관리시스템에서, 일정한 권한을 가진 사용자는 요구되는 어떤 접근통제 조합에도 불구하고 가용한 접근통제 표시를 클래스, 폴더와 기록으로 배치할 수 있어야 한다. 따라서 평문으로 간단히 지정될 수도, 복잡한 서로 다른 통제표시가 담겨질 수도 있다.

www.kci.go.kr



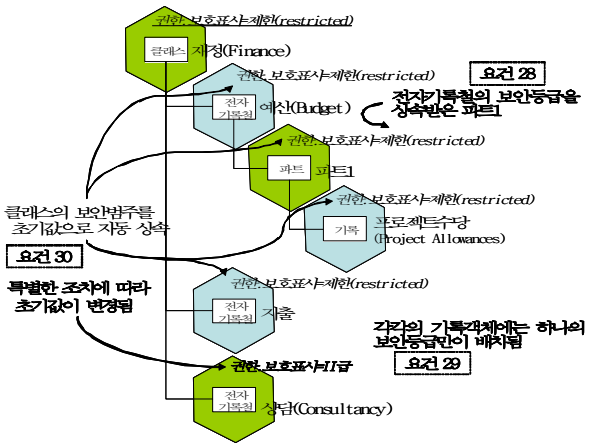
<그림 5> 다양한 접근통제표시의 배치

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

클래스 하위에서 생성되는 모든 전자기록철은 초기값으로 클래스의 보안범주를 상속 받는다. 다만, 필요시 전자기록철 수준에서 특별한 보안범주를 배치할 수도 있다(요건 30)(<그림 6>). 전자파트는 전자기록철을 편리하게 관리하기 위해 전자기록철을 분할한 것인데, 해당 전자기록철에 배치된 접근통제표시를 항상 상속받는다(요건 28)(<그림 6>). 결국 원칙적으로 보면 하위의 객체는 어버이 객체의 접근통제표시에 따르며 특별한 경우를 제외하고는 사용자가 임의로 변경하거나 다른 접근통제를 배치하도록 해서는 안된다. 한편, <그림 6>에서와 같이 기록분류체계 내에서의 개별적인 기록객체에는 하나의 보안범주만이 배치되며 초기값은 해당 파일플랜 구조하의 최하위 값이 자동으

www.kci.go.kr

로 생성된다(요건 29). <그림 6>의 전자기록철 '상담'은 최초 클래스 '재정'의 보호표시인 '제한'을 상속받았지만 기록의 중요성 등 조직내의 원칙에 따라 관리자가 III급 비밀로 보안등급을 상향조정하였다. 그러나 나머지 전자기록철에 대해서는 특별 조치가 수행되지 않아 최초의 상속값인 '제한'이 유지된다.



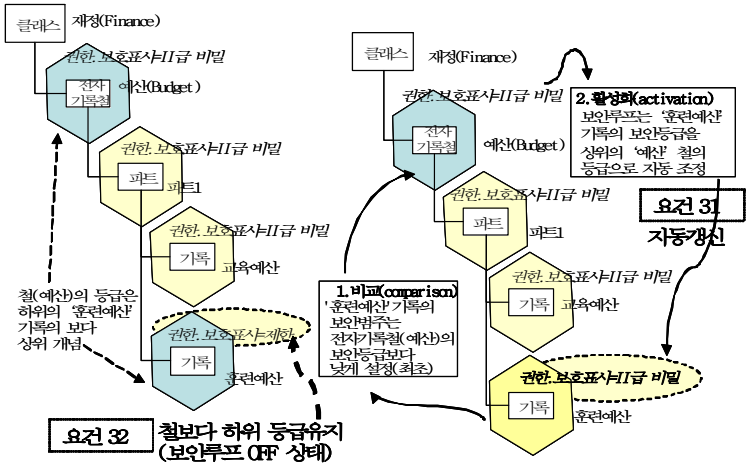
<그림 6> 보안범주의 상속과 단일 보안범주의 배치

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

'요건 30'에도 불구하고 하나의 전자기록이 해당 전자기록철의 보안범주 보다 낮게 지정되어 있을 경우, 하위의 개별기록의 보안범주를 전자기록철의 값과 일치시키는 자동갱신 행위가 수행될 수 있다(요건 31). 이것은 개별 기록건이 전자기록철에 추가될 경우 각각의 보안범주를 시스템에 의해 자동으로 갱신시켜 기록을 보호하자는 취지이고 이때, 보안등급 자동갱신 기법인 보안루프(security loop)를 사용할 수 있다. 그러나 관리자는 전자기록철에 배치된 기록이 해당 전자기록철

www.kci.go.kr

보다 낮거나 높은 보안범주를 유지하도록 할 수도 있다(요건 32)(요건 34). 따라서 시스템에서는 보안범주를 갱신할 것인지 또는 유지할 것인지를 결정할 수 있는 일정한 '알림장치' 기능을 제공해야 한다.



<그림 7> 보안루프 시스템을 통한 접근통제 갱신(I)

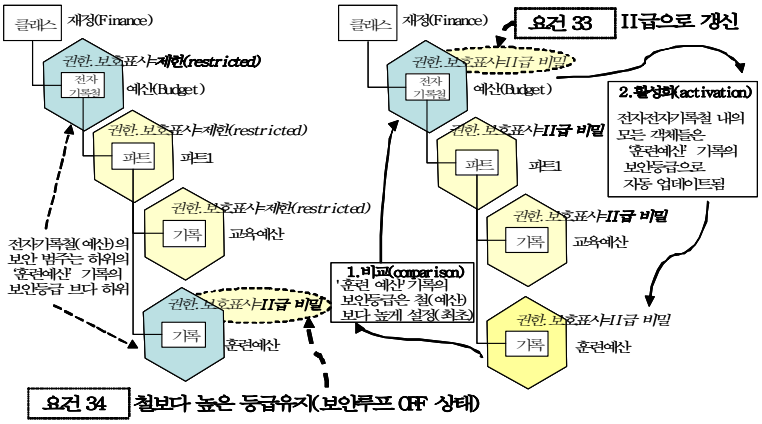
* 주 : 철보다 하위로 배치된 기록 '훈련예산'의 보안범주(좌)
전자기록철 '예산'의 보안범주로 갱신된 기록 '훈련예산'(우)

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

<그림 7>에 의하면, 보안루프가 활성화되기 전에는 '예산'전자기록철의 하위 폴더인 파트1에 전자기록철보다 보안수준이 낮은 '훈련예산'이라는 기록이 배치되어 있다. 즉, 전자기록철이 II급 비밀로 허가되어 있음에도 불구하고 하위의 기록에는 일부 인원에 대해 제한적으로 접근을 허용하도록 비밀등급을 '제한'으로 유지할 수 있다. 그러나 필요에 의해 <그림 7>의 우측과 같이 보안루프가 활성화되자 '훈

www.kci.go.kr

련예산'의 보안범주는 전자기록철의 보안범주와 동일하게 자동으로 갱신되었다. 한편, 전자기록철보다 상위의 보안범주를 가진 기록이 해당 전자기록철에 배치된다면, 전자기록철에 배치되었던 최초 등급은 기록의 보안범주로 갱신될 수 있어야 한다(요건 33).



<그림 8> 보안루프 시스템을 통한 접근통제 갱신(II)

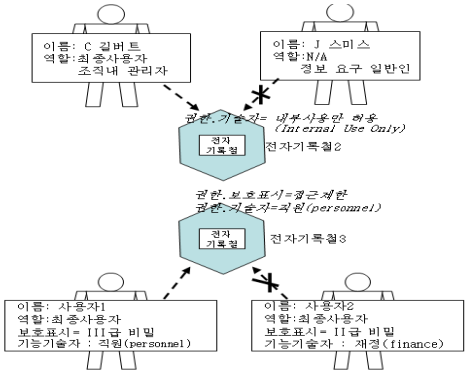
* 주 : 기록보다 하위로 배치된 전자기록철 보안범주(좌)
'예산' 전자기록철의 모든 객체가 최신화(우)

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

<그림 8>에서, 보안루프가 작동되기 전에는 전자기록철에는 '제한'이, 하위의 기록에는 'II급 비밀'이라는 보안범주가 배치되었다. 그러나 보안 루프가 작동되자 시스템에서는 파일플랜내의 객체를 비교하여 전자기록철의 보안범주를 최고의 수준인 II급으로 갱신시켰다. 이와 함께 전자기록철의 메타데이터를 상속받는 파트1과 '교육예산'도 갱신된 II급 비밀을 다시 상속받았다.

www.kci.go.kr

전자기록관리시스템에서는 전자기록철이나 기록에 대해, 메타데이터의 한 요소로서 기술자(descriptor)를 추가할 수 있어야 한다(요건 35). 기술자는 접근통제를 목적으로 계층적인 보안범주 구조하에서 일정한 자격을 주는 사람(qualifier)과 같은 역할을 하는 것이며, 정보로서의 기술자(Descriptors-Informative)와 기능적 기술자(Descriptors-Functional)로 구분한다. 전자는 접근제한을 기술함에 있어 단지 유용성(usability)을 제공함으로써 접근통제에 있어 중요한 역할을 수행한다. 예를 들어, 정보로서의 기술자는 '내부적인 사용만 허용', '관리자 및 이해당사자들'과 같은 전자기록철의 세부상태를 포함할 수 있다. 이를 통해 사용자들은 전자기록관리시스템 외부로 전자기록철의 내용이 공개될 수 있는지 없는지를 즉시 알 수 있게 된다.



<그림 9> 보안기술자와 접근통제[요건 35적용]

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

<그림 9>에 의하면 '내부직원에게만 허용'이라는 정보적 기술자가 배치되어 있다. C 길버트가 전자기록철2로 접근하게 되면 정보적 기술자 메타데이터가 확인되며 길버트가 조직의 관리자이므로 권한을

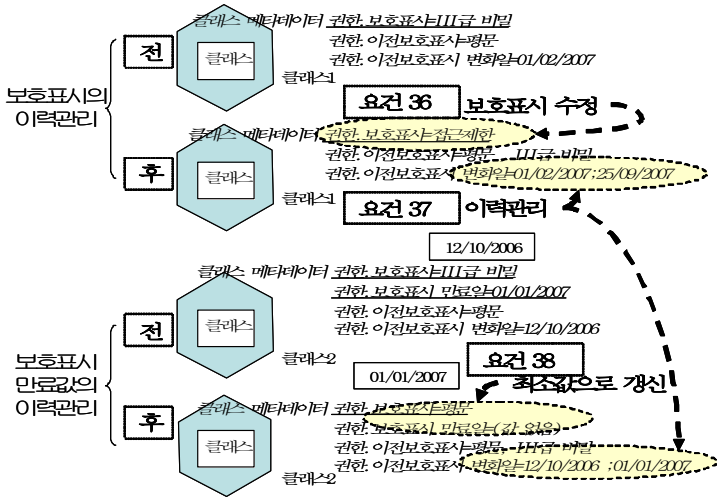
www.kci.go.kr

가진 내부 이용자로 식별된다. 따라서 C 길버트는 전자기록철2에 접근할 수 있다. 그러나 J 스미스는 외부 이용자이므로 접근할 수 없다. 한편, 기능적 기술자는 접근허가를 결정하기 위해 다른 접근통제수단과 함께 사용되는 것으로 정보적 기술자보다 엄격하다. <그림 9>에서와 같이 전자기록철3에는 '접근제한'이라는 보안범주와 함께 직원(personnel)이라는 기술자가 배치되어 있다. 사용자1은 III비밀 허가권자이며 기능기술자인 '직원'으로 지정되어 있으므로 전자기록철3에 접근할 수 있다. 그러나 사용자2는 접근할 수 없다. 왜냐하면 II급 인가자임에도 불구하고 전자기록철 접근에 필요한 특성화된 기능보안기술자를 배치받지 못했기 때문이다.

클래스, 전자기록철, 기록에 배치된 접근통제표시는 수정할 수 있어야 하며(요건 36), 과거의 접근통제 표시, 수정날짜 등을 이력관리 메타데이터요소로 보유해야 한다(요건 37). 또한 클래스나 전자기록철, 기록에 배치된 보안범주는 일정한 기간 동안 유효해야 하고 제한된 기간이 종료되면 모든 사용자들이 그 기록을 열람하고 이용할 수 있도록 최하위 수준의 보안범주로 자동 갱신되어야 한다(요건 38). 즉, 전자기록철이나 클래스 등에 배치된 접근통제 표시는 조직의 정책이나 환경에 따라 변화될 수 있고 기록이 특정 사용자들에게만 일시적으로 필요할 수도 있기 때문에 지속적으로 변경되어야 한다. 그리고 접근통제표시의 배치는 감사될 수 있지만 감사증적 전체를 조사하지 않고 사용자들이 파일플랜 객체의 접근통제 이력을 즉각 열람하고자 할 경우도 있다. 따라서 전자기록관리시스템에서는 개별 객체에 대한 접근통제 이력을 모니터링하고 보여줄 수 있어야 한다. <그림 10>과 같이 '권한.이전보호표시', '권한.이전 보호표시 변화일' 메타데이터 필드에는 객체의 변화 정보가 담겨지게 된다. 즉, 클래스1은 만료일이 2007년 1월 1일으로 설정된 III급 비밀이었다. 2007년 1월 1일이 도래하면 시스템에서는 자동으로 클래스 메타데이터를 업데이트하게 된

www.kci.go.kr

다. 그 결과 보안범주는 평문으로 하향 조정되고 만료일의 필드값은 특별한 날짜가 지정되지 않는 초기값으로 변경된다.



<그림 10> 접근통제의 변화관리

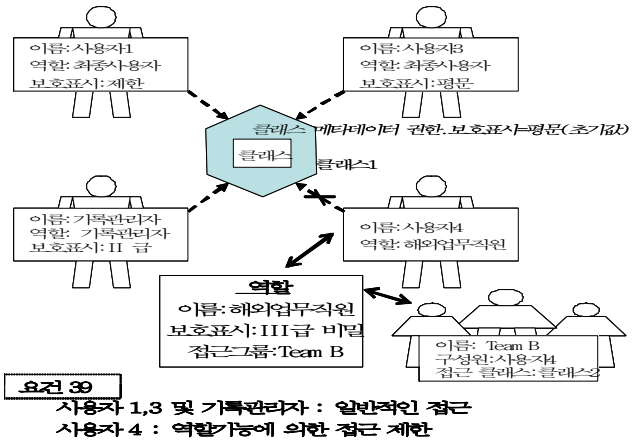
* 주 : 클래스1에서는 평문으로 지정된 보안범주가 III급 비밀, 접근제한으로 변화되었고 그 이력이 관리되고 있다. 클래스2에서는 보호표시가 만료되자 관련 메타데이터가 초기화되었다.

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

3) 접근통제 실행단계

접근통제 실행은 일정한 권한을 가진 사용자에 의해 기록분류체계 내의 여러 객체에 부여된 접근통제사항을 적용하는 단계이다. 여기에는 사용자들의 객체접근, 접근된 사용자들에 대한 적절한 통제방식 등이 포함된다.

www.kci.go.kr



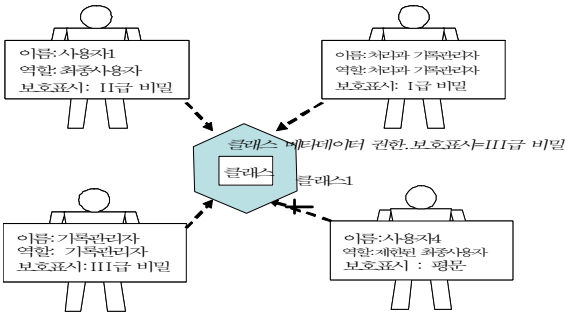
<그림 11> 이용자에 대한 접근허용

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

기본적으로, 최하위 보안범주와 같은 접근통제표시가 배치되어 있는 경우이면서 특별히 다른 기능에 의해 제한되지 않는다면 모든 이용자가 모든 클래스, 전자기록철과 전자기록으로 접근할 수 있어야 한다(요건 39). <그림 11>에 따르면 클래스1이 생성되는 시점에서는 '평문'이라는 보안범주가 기본값으로 배치되었다. 이후에 아무도 클래스1에 대한 보안값을 정정하지 않았다면 역할에 의해 그 기능이 제한된 사용자를 제외한 모든 사용자들이 클래스1에 접근할 수 있다. 따라서 사용자1, 사용자3, 기록관리자 모두는 최소 '평문'이상의 수준인 보안범주를 각각 보유하고 있고 클래스1에 접근할 수 있다. 특별히, 사용자4는 지정된 접근통제 그룹의 '해외업무직원'역할로 지정되었다. 따라서 사용자4와 같은 외부인은 클래스1에 대한 접근이 불가하다. 사용자4는 Team B에 지정된 역할을 통해 조건을 만족시키는 파일플랜내의 다른 객체인 클래스2에만 접근할 수 있다.

www.kci.go.kr

적절한 보안범주의 배치를 통해 해당 보안값과 동등하거나 이상의 수준을 보유한 사용자를 제외하고는 파일플랜내의 클래스, 전자기록철, 기록으로의 접근은 제한된다(요건 40).



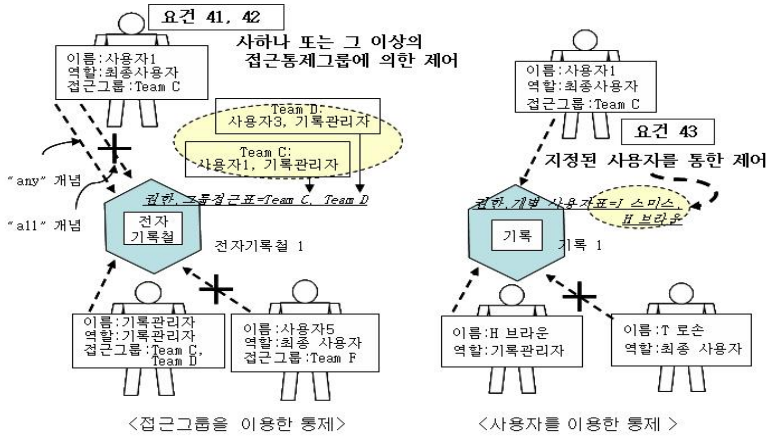
<그림 12> 보안범주에 부합되는 접근허가[요건 40적용]

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

<그림 12>에 따르면, 전자기록관리시스템의 관리자는 클래스1에 III급 비밀이라는 보안범주를 배치했고 다른 접근통제 조건은 아무것도 배치되지 않았다. 사용자4를 제외한 모든 사람들은 클래스 메타데이터의 보안조건과 동등하거나 그 이상이므로 접근이 가능하다. 그러나 사용자4는 클래스의 보안수준과 일치하지 않으므로 클래스1에 접근할 수 없다.

전자기록관리시스템에서는 사전에 정의된 하나 또는 그 이상의 접근통제 그룹, 하나 이상의 사용자로 구성된 접근통제표시를 통해 접근통제를 수행한다(요건 41)(요건 42)(요건 43).

www.kci.go.kr



<그림 13> 접근그룹과 개별 사용자를 이용한 접근통제

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

<그림 13>의 좌측부분에 의하면, 전자기록관리시스템 관리자가 'Team C', 'Team D'를 전자기록철1의 접근통제그룹으로 지정하였고 그 외의 다른 접근통제 수단은 적용되지 않았다. 이 경우 전자기록관리시스템에서는 전자기록철1에 배치된 접근표에 따라 접근이 통제되는데 하나 이상의 조건만 충족시키면 되는 'any'의 개념에서는 다음과 같이 접근통제가 수행된다.

- 기록관리자 : 'Team C, D'의 구성원으로 전자기록철1에 접근
- 사용자 1 : 'Team C'의 구성원이므로 접근 가능
- 사용자 5 : 전자기록철1의 접근표에 등록되지 않아 접근 불가

이와 달리, 모든 조건을 충족시켜야 하는 'all'의 개념을 적용받고 있는 전자기록관리시스템이라면 다음과 같이 통제된다.

www.kci.go.kr

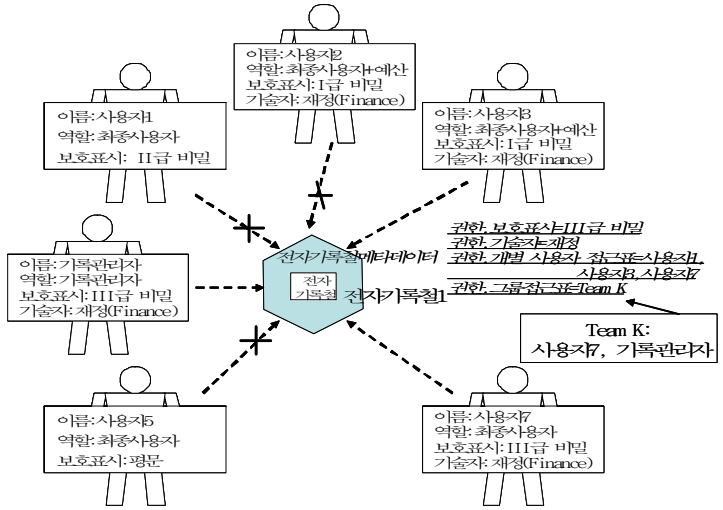
- 기록관리자 : 'Team C, D'의 구성원, 전자기록철1에 접근 가능
- 사용자 1 : 'Team C'의 구성원이지만 'Team D'의 구성원을 동시에 만족시키지 못하므로 접근 불가
- 사용자 5 : 전자기록철1의 접근메타데이터와 무관하여 접근 불가

한편, <그림 13>의 우측과 같이 전자기록관리시스템에서는 어떤 사용자가 접근할 경우 사용자와 객체에 대한 접근제한 사항을 비교하게 되는데 파일플랜내의 특정 객체에 접근하기 위해서는 사용자 접근통제수준은 해당 객체와 동일하거나 그 이상 이어야 한다. 만약, 개별 사용자 접근통제표만이 적용되는 전자기록관리시스템이라면 권한이 부여된 사용자를 제외한 어떠한 다른 사용자들도 객체에 접근할 수 없다. 따라서 기록1에 접근 가능하도록 설정된 사용자는 'J 스미스'와 'H 브라운'뿐이므로 이들을 제외한 다른 사람들은 접근이 금지된다.

전자기록관리시스템에서는 하나 이상의 형태로 구성되는 접근통제표시에 따라 클래스, 전자기록철 및 기록으로의 접근을 제어할 수 있어야 한다(요건 44). 이때 모든 등가의 접근통제 표시(equivalent access control markings)를 가진 사용자로만 제한하며 일부 접근통제 표시를 가진 사용자는 접근이 불가하다. 예를 들면, 홍길동이라는 III급 비밀취급자는 III급으로 분류된 기록 또는 하위 등급인 접근제한으로 분류된 기록에 접근이 가능하다. 하지만 특정 기록에 예산접근통제그룹(a Budget access control group)이 추가로 배치된다면 권한이 없는 홍길동은 이 기록에 접근할 수 없다.[22]

22) 기록관리시스템의 제품에 따라 차이가 있을 수 있지만, 아래와 같은 조건을 만족시키면 접근을 허용한다(각각은 AND의 관계임).
◦ 만약, 두 가지 접근통제표(개별 사용자, 그룹)가 활성화된 경우, 사용자가 개별적으로 명명된 경우 혹은(or) 일정한 접근통제 그룹의 멤버이다.
◦ 그 사용자가 보유한 보안범주가 분류체계내의 객체보다 높거나 동일해야 한다.
◦ 만약 기능적 보안기술자가 사용되는 경우라면, 그 사용자는 분류체계내의 객체보다 높거나 동일한 보안기술자를 보유해야 한다.

www.kci.go.kr



<그림 14> 다양한 접근통제의 적용[요건 44적용]

* 주 : 개별 사용자의 접근통제 메타데이터는 전자기록철1에 세팅된 접근통제사항과 비교되고, 모든 조건을 만족하는 기록관리자, 사용자3 및 사용자7에 대해서만 접근이 허가된다.

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>

<표 2> 사용자별 접근통제의 승인 및 거부[요건 44적용]

사용자	전자기록철 메타데이터				접근 여부
	OR의 관계		AND	AND	
	지정된 사용자	그룹멤버	보안범주	기능적 기술자	
사용자7	가능	가능	가능	가능	**가능**
기타	가능	가능	가능	불가	불가
기타	가능	가능	불가	가능	불가
기타	가능	가능	불가	불가	불가
사용자3	가능	불가	가능	가능	**가능**
사용자1	가능	불가	가능	불가	불가
기타	가능	불가	불가	가능	불가
기타	가능	불가	불가	불가	불가
기록관리자	불가	가능	가능	가능	**가능**

www.kci.go.kr

기타	불가	가능	가능	불가	불가
기타	불가	가능	불가	가능	불가
기타	불가	가능	불가	불가	불가
사용자2	불가	불가	가능	가능	불가
기타	불가	불가	가능	불가	불가
기타	불가	불가	불가	가능	불가
사용자5	불가	불가	불가	불가	불가

* 주 : OR의 및 AND에 해당하는 값을 동시에 충족시켜야 접근이 허가된다.

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

<그림 14>에 따르면, 기록관리시스템의 관리자는 전자기록철1에 아래와 같은 접근통제표시를 배치하고 있다. 이때, 사용자가 전자기록철에 접근하기 위해서는 요구되는 모든 접근통제 세팅을 갖추어야 한다. <그림 14>의 이용자별 상세한 접근통제 승인과 거부는 <표 2>와 같이 정리될 수 있다.

- 보안범주 : III급
- 기능보안기술자 : 재정(Finance)
- 지정된 사용자 : 사용자1, 사용자3, 사용자7
- 접근통제그룹 : Team K(회원 : 사용자7과 기록관리자)

클래스, 전자기록철, 기록으로의 접근이 허용되지 않는 사용자는 해당 객체의 메타데이터를 포함하여 객체 자체, 풀텍스트(full-text) 검색 등 여하한의 검색결과에서 객체를 확인하거나 메타데이터 값을 열람할 수 없도록 해야 한다. 그러나 경우에 따라서는 접근이 허용되지 않는 사용자도 기록의 내용은 볼 수는 없지만 검색결과 내의 메타데이터 정도는 볼 수 있는 구성옵션을 제공할 수 있어야 한다(요건 45)(요건 46). 이러한 개념에 의해 기록관리시스템의 관리자는 아래와 같이 제한된 파일플랜 객체의 메타데이터를 다룰 수 있는 서로 다른 접근

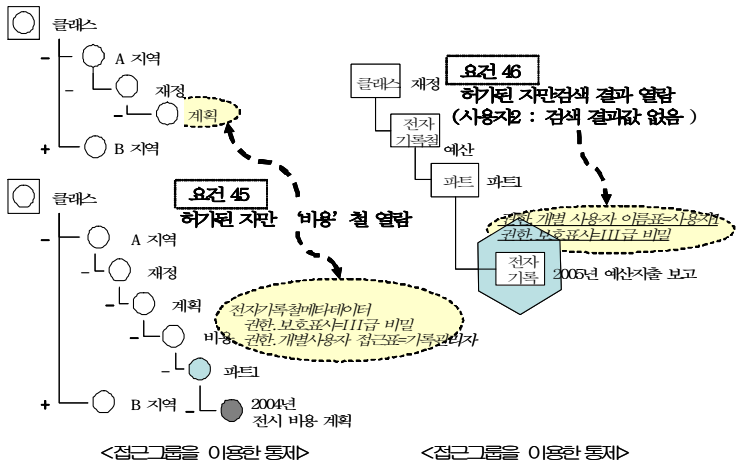
www.kci.go.kr

법을 구성할 수 있어야 한다.

첫째, 요망되는 접근세팅을 미보유한 사용자는 제한된 객체(restricted objects)의 메타데이터와 내용에 대한 정보를 열람, 검색할 수 없어야 한다. 따라서 이러한 사용자는 객체의 존재사실 자체를 인지할 수 없다.

둘째, 요구되는 접근세팅을 보유하지 않은 사용자가 기록의 내용은 아니더라도 접근이 제한된 객체의 메타데이터 정도는 검색 또는 열람할 수 있다. 이때 쓰기 권한은 부여되지 않는다. <그림 15>의 좌측의 상단은 최하위 접근통제를 적용받는 사용자의 인터페이스로 '계획'의 하위에 배치된 전자기록철 '비용'에 접근할 수 없다. 하지만, 관리자가 접근통제 메타데이터 값을 상향 조정했다면 '계획'클래스 하위의 전자기록철과 파트 및 기록들이 활성화되어 있어 계층구조를 모두 열람함은 물론, 관련 객체의 메타데이터도 확인할 수 있다. 그러나 제한된 분류체계이므로 기록의 내용은 열람할 수 없다. 한편, <그림 15>의 우측에 의하면 ERMS 관리자가 전자기록철의 메타데이터에 접근할 수 있는 권한과 III비밀등급 표시를 배치했으며 기록의 내용과 제목은 '지출'이라는 단어를 포함하고 있고 보안범주가 평문으로 지정된 일반적인 사용자2가 있다고 하자. 사용자1이 '지출'을 검색어로 하여 검색을 하면 기록의 내용과 메타데이터를 확인할 수 있다. 그러나 권한을 부여받지 아니한 사용자2가 검색을 했을 경우 접근이 제한되거나 허용되지 아니한 사용자임을 알려주게 된다.

www.kci.go.kr



<그림 15> 서로 다른 접근법의 구성과 허용되지 아니한 사용자의 통제

* 자료 : 2002 rational for functional requirements
<http://www.nationalarchives.gov.uk/documents/a5.pdf>를 재구성

4. 결론

접근통제는 보이지 않는 설정과 장치를 통해 수행되는 만큼 추상적이고 개념적이어서 다루기 쉽지 않다. 특히 전자환경에서 기록관리를 원만하게 수행하기 위해서는 많은 내부 및 외부 사용자와 전자기록철, 기록 등을 잘 정비된 시스템 속에서 체계적으로 관리해야 한다. 따라서 전자적 접근통제를 구현하는 시발이 잘 설계된 기록관리시스템에 달려있다는 것은 부인할 수 없는 사실이다. 이에 본 논문에서는 ERMS 설계시 기록관리시스템에서 구비해야 하는 여러 가지 필수 및 선택기능이 망라되어 있는 각국의 기능요건서 중 접근통제에 관한 부분을 비교 및 분석하여 모범적인 접근통제 기능요건으로 정리하고 기록분류체계에서 어떠한 모습으로 구현되어야 하는지를 접근통제 준

www.kci.go.kr

비, 배치와 실행이라는 세 단계로 구분하여 개념적으로 다루어 보았다. 특히, 기록관리분야에서 접근통제 연구실적이 제시되지 않고 있는 상황에서 개념적으로나마 접근통제 실행방안을 제시한 점은 본 논문의 작은 성과라 할 수 있다. 그러나 2장에서 비교적 자세한 가이드라인을 제공한다는 이유로 영국의 표준을 분석의 기준틀로 사용한 점은 지적의 대상이 될 수 있다. 또한 제한된 지면사정으로 2장에서 도출한 여러 요건을 보다 치밀하고 자세히 다루지 못한 점과 기록의 진본성과 무결성 유지와 같은 국내외의 문제점을 진단하여 우리나라 기록관리 환경에서 어떻게 해석되고 적용될 수 있는지에 대한 내용이 제시되지 못한 점, 3장에서 도출된 요건을 적용함에 있어 영국의 표준을 중심으로만 기술한 점은 이 논문의 한계로 지적될 수 있다. 아무쪼록 본 연구를 시발점으로 하여 기록관리 분야에서의 접근통제 연구가 활발히 진행되기를 기대한다.

www.kci.go.kr

부록 각국의 ERMS 표준에 나타난 접근통제 요건 매핑[23)]

(1) ERMS로의 접근

A.5.1(영국) - 4.1.2(유럽연합) - A.3.1/A.3.5(호주) - C2.2.8.3(미국)
A.5.2**(영국) - 없음(유럽연합) - A.3.2(호주) - 없음(미국)
A.5.3(영국) - 없음(유럽연합) - A.3.6(호주) - 없음(미국)
A.5.4**(영국) - 4.1.2(유럽연합) - 없음(호주) - 없음(미국)

(2) 접근통제 표시

A.5.5(영국) - 없음(유럽연합) - A.3.7(호주) - 없음(미국)
A.5.6(영국) - 4.1.1(유럽연합) - A.3.8(호주) - 없음(미국)
A.5.7(영국) - 4.1.7*(유럽연합) - A.3.21(호주) - 없음(미국)
A.5.8(영국) - 4.6.1(유럽연합) - A.3.22(호주) - 없음(미국)
A.5.9(영국) - 4.6.6(유럽연합) - A.3.12(호주) - 없음(미국)
A.5.10(영국) - 4.1.4(유럽연합) - A.3.10(호주) - C2.2.8.5(미국)

(3) 사용자 프로파일

A.5.11(영국) - 4.1.2/9.1.8(유럽연합) - A.3.13(호주) - C.2.2.8.4(미국)
A.5.12(영국) - 4.1.2(유럽연합) - A.3.14(호주) - 없음(미국)
A.5.13(영국) - 4.6.9(유럽연합) - A.3.15(호주) - 없음(미국)
A.5.14(영국) - 없음(유럽연합) - A.3.20R(호주) - 없음(미국)
A.5.15(영국) - 4.1.5(유럽연합) - A.3.14(호주) - 없음(미국)
A.5.16(영국) - 4.1.8(유럽연합) - A.3.16(호주) - 없음(미국)

---

23) '**'표시는 의무사항은 아니지만, 매우 권고할만한(Highly Desirable) 요건을, '*' 표시는 권고할만한(Desirable)요건, 'ε'는 비의무조건(Non-Mandatory)을 의미한다. 'R'는 호주의 기능요건의 분류(호주는 Mandatory, Required, Desirable로 구분함)성격 중 'Required'를 의미하는 것으로 호주의 기능요건에서는 핵심요건과 부가요건이 있다. 이때 'R'은 기록관리시스템을 설계함에 있어 부가요건을 채택했을 경우에 한해서만 의무적으로 고려해야하는 강제조건이라는 의미를 담고 있다. 별도의 표시가 없는 경우는 의무사항이다.

www.kci.go.kr

(4) 역할

A.5.17(영국) - 4.1.3(유럽연합) - A.3.17(호주) - C.2.2.8/C.2.2.8.2(미국)
A.5.18(영국) - 없음(유럽연합) - A.3.18(호주) - 없음(미국)
A.5.19(영국) - 4.5.1(유럽연합) - A.3.18(호주) - C.2.2.8(미국)
A.5.20(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)
A.5.21**(영국) - 없음(유럽연합) - A.3.19(호주) - 없음(미국)

(5) 그룹

A.5.22(영국) - 4.1.4/4.1.6(유럽연합) - A.3.8/A.3.10(호주) - C.2.2.8.5(미국)
A.5.23(영국) - 없음(유럽연합) - A.3.11(호주) - 없음(미국)
A.5.24(영국) - 4.1.1/9.11.7(유럽연합) - A.3.14(호주) - 없음(미국)
A.5.25**(영국) - 4.1.2(유럽연합) - 없음(호주) - C.2.2.8.5(미국)

(6) 접근통제의 배치

A.5.26(영국) - 4.1.1/4.6.1(유럽연합) - A.3.24(호주) - 없음(미국)
A.5.27(영국) - 없음(유럽연합) - A.3.25(호주) - 없음(미국)
A.5.28(영국) - 3.3.3(유럽연합) - 없음(호주) - 없음(미국)
A.5.29(영국) - 4.6.1/4.6.2(유럽연합) - A.3.36(호주) - 없음(미국)
A.5.30(영국) - 3.2.5(유럽연합) - A.3.33/A.3.34(호주) - 없음(미국)
A.5.31(영국) - 4.6.5*(유럽연합) - A.3.35(호주) - 없음(미국)
A.5.32**(영국) - 없음(유럽연합) - A.3.34/A.3.35(호주) - 없음(미국)
A.5.33(영국) - 4.6.10*(유럽연합) - A.3.35(호주) - 없음(미국)
A.5.34**(영국) - 없음(유럽연합) - A.3.34/A.3.35(호주) - 없음(미국)
A.5.35(영국) - 없음(유럽연합) - A.3.26(호주) - 없음(미국)
A.5.36(영국) - 9.3.3/9.3.5(유럽연합) - A.3.27(호주) - 없음(미국)
A.5.37**(영국) - 9.3.6*(유럽연합) - A.3.40(호주) - 없음(미국)
A.5.38**(영국) - 4.6.12*(유럽연합) - 없음(호주) - 없음(미국)
A.5.39*(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)
A.5.40*(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)

www.kci.go.kr

(7) 보관인(Custodian)

A.5.41(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)
A.5.42(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)
A.5.43(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)
A.5.44(영국) - 없음(유럽연합) - 없음(호주 - 없음(미국)

(8) 접근통제 표시 실행

A.5.45(영국) - 없음(유럽연합) - A.3.31(호주) - 없음(미국)
A.5.46(영국) - 4.6.8(유럽연합) - A.3.32(호주) - 없음(미국)
A.5.47(영국) - 4.1.1(유럽연합) - A.3.28(호주) - 없음(미국)
A.5.48(영국) - 4.1.1(유럽연합) - A.3.29(호주) - 없음(미국)
A.5.49(영국) - 없음(유럽연합) - A.3.30(호주) - 없음(미국)
A.5.50(영국) - 4.1.1(유럽연합) - A.3.37(호주) - 없음(미국)
A.5.51**(영국) - 4.1.9(유럽연합) - A.3.38(호주) - 없음(미국)
A.5.52(영국) - 4.1.10(유럽연합) - A.3.38(호주) - 없음(미국)

(9) 프라이버시와 기록열람

A.5.53(영국) - 없음(유럽연합) - 없음(호주) - 없음(미국)

www.kci.go.kr

ABSTRACT

A study on application plan of access control requirements in ERMS Standard

Cheon, Kwon-Ju

Under the physical records management system, both the records and users could be controlled and secured by closing the door of Archives or using permitted records which is used only approved users. According to the electronic records management system and the concept of service on the basis of users, we have to give up the classical manner. As an alternative, we have to consider the electronic access control system. To accomplish this purpose, functional requirements of ERMS that is issued by UK, EU, U.S and Australia must be compared and analyzed. On the basis of U.K ERMS which is more detailed, 'common access control functional requirements' are arranged. As the access control functional requirements is applied in the records classification scheme, we could find out how the access control is executed in ERMS.

Keywords : Access, Access control, Classification Scheme, ERMS, Electronic folder, Functional Requirements

www.kci.go.kr