

RFID 유틸리티스 영구기록물관리시스템 구축과 보안 연구

장영상*, 이승룡**

RFID Ubiquitous Public Information Documental Administration System construction and Security research

Young-Sang Jang*, Sung-Yooung Lee**

요약

행정부, 입법부, 사법부 등의 국가기록물은 영구기록물로 관리가 필요하다. 범죄사건이 발생 시마다 사법부의 기록물은 참고자료로 빈번하게 대출되고 반납되는데, 영구기록물의 관리를 위해서는 기록물들의 사건등록, 이력조회, 대출/반납, 보존 검색, 기록물 폐기관리가 이루어져야 한다. 최근의 유틸리티스 정보화의 활용방안으로 RFID가 활용되고 있다. 본 논문에서는 RFID를 이용한 영구기록물에 태그를 부착하여 기록물을 등록 관리하고, 이력을 추적하고, 보존, 검색하기 위한 영구기록물의 현황 분석, S/W, H/W, 네트워크 설계, 유틸리티스 RFID 영구기록관리시스템 설계를 한다. 900MHz 대역의 RFID 태그를 부착한 현장에서 적용되는 성능 실험과 추적실험 후에 영구기록관리시스템을 구축한다. 구축 실행 후에 관련 시스템과의 연계성, 보안성 분석과 포렌식 자료를 생성하고 개선효과를 분석한다. 본 논문의 연구를 통하여 국가기록물 관리에 유틸리티스 정보화 기술 적용과 포렌식 기술 발전에 기여하게 될 것이다.

Abstract

Public Information Documental of the administrative, legislative and judicial etc. is lastingness documental and need administration. Whenever the crime event happens, judicature's documental is lent frequently to reference data and is returned, event posting of documental, hysteresis inquiry, lending/return, conservation search, documental exhaust management must consist for administration of lastingness documental. RFID is utilized by the practical use plan of recent Ubiquitous information. Because attaching tag to lastingness documental that use RFID in this treatise, register and manage documental, and chase hysteresis, and design upkeep, present condition analysis of lastingness documental to search, S/W, H/W, network layout, Ubiquitous RFID lastingness recording administration system. Construct lastingness recording administration system after a performance experiment and a chase experiment that is applied in spot that attach 900MHz important duty's RFID tag. After construction practice, create link sex with connection system, security analysis and Forensic data and

• 제1저자 : 장영상

• 투고일 : 2009. 09. 28, 심사일 : 2009. 09. 30, 게재확정일 : 2009. 10. 13.

* 호서대학교 평생교육원 사이버해킹보안과 주임교수 **경희대학교 전자계학공학과 교수

analyze improvement effect. Is going to contribute Ubiquitous information technology application and Forensic technology development in country documental administration through research of this treatise.

▶ Keyword : RFID(Radio Frequency Identification), 유비쿼터스(Ubiquitous), 포렌식(Forensic), 영구기록(Public Information

I. 서론

국가는 국가 간의 외교문서, 법정에서의 판결, 형사기록물 등에 대해서 기록물관리를 하고 있다. 국가기록물이란 행정부, 입법부, 사법부 등의 국가기관에서 생산·활용·보존되는 기록물로서, 당대에는 정책의 실상이고, 사건에서는 참고자료이며, 후대에서는 국가의 역사 자료가 된다.

국가기록물을 잘 보존·활용하는 일은 정책의 투명성과 공정성을 보장하는 일이며, 정책의 노하우를 전달하는 일이며, 국민의 권리를 보호하는 일이며, 나아가 그것은 국력을 신장시킬 수 있는 바탕이 된다. 그러므로 선진국에서는 전문인을 배치하여 국가기록을 잘 보존·활용하고 있다.

이들 국가기록물은 영구기록물(1)과 준영구기록물로 등록하고, 필요에 따라 각 기관에서는 기록물을 추적하여 대출하고, 반납을 받으면서 이력을 작성하고, 기록물 보존 연한에 폐기를 하고 있다. 공무원들은 영구기록물을 보호 관리할 의무가 있고, 기록물 관리에 관하여 다른 특별한 규정이 있는 경우를 제외하고는 공공기록물 관리(2)에 관한 법률이 정하는 바에 따르며, 기록물의 생산부터 활용까지 전 과정은 그림 1처럼 생산이전단계, 생산단계, 준현용단계, 비현용단계로 구분하여 진본성, 무결성(3), 신뢰성을 유지한다.



그림 1. 영구기록물 라이프 사이클 4단계 모형
Fig 1. Public Information Documental Life Cycle 4 steps Model

하지만 국가의 부처에서 영구기록물의 보관 및 기록 대출과 자료의 이동과정에서 보존이 완전치 않아, 기록물의 유실과 손상되는 사례가 발생하고 있다. 또한 영구기록물의 정확한 위치 및 소재 파악의 어려움으로, 국가의 중요 의사결정에

즉시적으로 필요한 기록관리 업무에서 신속히 대처하지 못해, 국가적인 손해나 기관에서의 사건처리에 어려움을 겪고 있다.

예를 들면 형사사건을 담당하고 있는 검찰에서는 영구형사사건기록물과 준영구형사사건기록에 대한 자료 및 문서의 이동과 분류 및 보존 등에 대한 기록관리시스템의 부재로 인하여 형사사건기록의 훼손이 심각하며, 또한 사건기록물의 목록이 서류 문서화 되거나 전산화되어 있지 않아, 검찰 직원 및 민원인의 열람 등 검색과 자료 활용이 어려우며, 사건기록물의 보존 및 위치 현황에 대한 정확한 통계 산출이 곤란을 겪고 있다.

이러한 이유로 본 논문에서는 사건기록과 재판서 등의 중요한 영구기록물의 보존, 열람, 대출, 폐기 단계에서 정보의 조회 및 영구기록물의 신속하고 안전한 기록물 관리를 위해 RFID를 이용한 유비쿼터스 정보화(Ubiquitous information)환경을 만들어 줄 시스템과 인프라에 대한 연구를 한다.

II. 관련 연구

2.1. 유비쿼터스 정보화

유비쿼터스라는 용어는 Mark Weiser에 의해 처음으로 사용되었다(4). 유비쿼터스는 라틴어에서 '언제 어디서나(any time, any where) 동시에 존재한다'는 뜻으로 사용된다(5). 유비쿼터스 정보화(6)는 인간과 동물과 사물이 네트워크로 연결되어 하나의 거대한 시스템으로 형성하며 정보망을 통해서 이루어지는 자원의 효율적 사용은 한정된 자원에 대한 인간의 필수적인 생존조건에 해당한다. 유비쿼터스 무선 기술인 센서의 경우에는 디바이스의 상태를 감지하기 위해 서 근접거리에서 사용될 수 있는 RFID(Radio Frequency Identification) 기술(7)이 사용된다.

우리나라도 유비쿼터스 기술을 사용하는 정보화도시인 U-City(8)로 예를 들면 부산시는 2010년까지 1조원을 투입해 첨단 정보통신기술을 향만, 교통, 산업, 관광, 컨벤션, 전자정부, 시민생활 등 도시 전체에 적용하는 '유비쿼터스 시티사업'을 추진하기로 했다.

2.2. FRID와 보안 취약점

RFID란 "마이크로 칩을 내장한 태그, 레이블, 카드 등에

저장된 데이터를 무선주파수를 이용하여 리더에서 자동 인식 하는 기술”(유승화,2005:55)로 RFID는 그림 2와 같이 판독 및 해독 기능[9]을 하는 RF 판독기(Reader)(10)와 정보를 제공하는 RF 태그 또는 transponder(11)로 구성된 무선통신 시스템이다. 근거리 통신망인 LAN 및 블루투스 등 데이터통신망과 연동할 수 있다. 무선 인식 시스템은 무선통신 접속 방식에 따라 상호 유도(Inductively coupled)방식과 전자기파(Electromagnetic wave)방식으로 나눌 수 있다. 또 데이터를 주고받을 수 있는 기능을 제공 한다.



그림 2. RFID 운영 관리 시스템 구성
Fig 2. RFID Operation Administration System composition

상호 유도 방식은 근거리(1m이내), 전자기파 방식은 중·장거리용으로 사용된다. 상호유도 방식은 코일 안테나를 이용하며 전자기파 방식은 고주파 안테나를 이용해서 서로 무선접속을 한다. 전자기파 방식의 태그는 마이크로 칩을 구동하기 위한 충분한 전력을 판독기로부터 공급을 받지 못하므로 추가적인 전지를 포함한다.

RFID 시스템에서 보안성 취약점[12]은 다음과 같다.

■ 위조 : 태그에는 메모리에 데이터 항목에 대해 공격자는 데이터 항목을 지우거나 대신할 수 있는 방법을 사용할 수 있다. 또한, 리더의 위조로 인해 태그의 데이터 항목이 노출되며, 태그간의 통신에 잘못된 데이터를 교환하는 위험이 존재한다.

■ 트래픽 분석 : 공격자가 특정 지역과 태그에서 리더와 태그간의 트래픽을 분석할 수 있다면, 물품의 출입 내역과 위치추적 등 중요정보가 노출되는 취약점이 존재한다.

■ 도청 : 공격자가 리더를 이용해 수 미터의 범위 내에서도 태그를 스캐닝하는 적극적 공격과, 리더와 태그간 통신을 RF 수신하는 수동적 공격을 통해 악의적인 사용에 대한 보안 문제점이 있다.

■ 서비스 거부 공격(Denial of Service Attack) : 리더가 태그간에 질의와 반응 메커니즘에 대해 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보낸다면 많은 계산

이 요구되고, 정상적인 기능을 못하게 만드는 취약점이 존재한다.

2.3. 포렌식(Forensic)

포렌식은 ① 법정에서 변론, 토론 ② 변론에 접합한, 수사적인 ③ 법의학에서 범죄에 대한 과학수사의 의미를 가지고 있으며 디지털증거(Digital Evidence)[13]를 수집한다. 디지털증거는 디지털과 증거의 복합어로서 데이터나 물리적인 양을 0과 1이라는 2진부호로 만들어진 자료를 법정에서 증거로 채택되는 증거로 확보하는 것을 말한다. ‘디지털 포렌식’이란 이산적으로 표현되는 데이터 속에서 법정에서 신뢰성 있게 채택되도록 과학수사의 일환으로 수집되고 분석하는 일련의 과정이라고 말할 수 있다.

포렌식은 주로 형사사건에서 범죄의 증거자료로 압수수색된 컴퓨터와 관련한 자료를 증거로 하였으나, 미국에서 민사사건에 대한 증거자료로 e-discovery[14]관한 법률이 통과되어 일반적인 업무활동에 대한 법률적인 증거자료로서의 포렌식 자료의 생성이 필요하게 되었다.

컴퓨터 포렌식[15]은 컴퓨터를 매개로 이루어지는 범죄에 대한 법적증거자료를 확보하기 위해 컴퓨터 저장매체와 네트워크로부터 자료를 수집, 분석 및 보존하여 원본성과 무결성 증명을 위하여 해시함수 SHA-1 등을 사용하며 법적 증거물로서 채택 될 수 있는 증거물로 제출하는 일련의 법적인 증거수집 절차 행위를 말한다.

네트워크를 경유한 침입자는 침입 후에 다양한 방법을 통해서 자신의 침입 흔적을 지우게 되는데, 침입자의 실수나 침입을 당한 시스템의 로그분석[16]을 통하여 침입자의 Source Address 등 정보를 이용하여 추적을 하면서 네트워크 포렌식 수사가 시작되어 진다. 그림 3은 디지털 포렌식 시스템의 구성도이다.

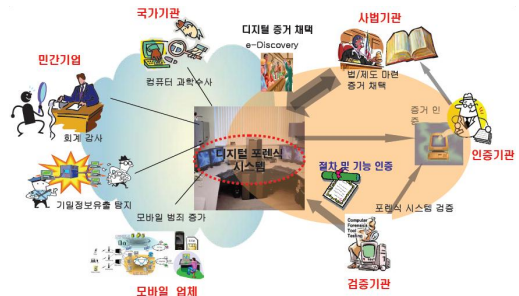


그림 3. 디지털 포렌식 시스템 구성
Fig 3. Digital Forensic System composition

포렌식의 구별은 디스크 포렌식, 네트워크 포렌식, 인터넷 포렌식, 시스템 포렌식, 데이터베이스 포렌식, 암호 포렌식, 회계 포렌식, 모바일 포렌식, 휴대폰 포렌식, 자동차 포렌식,

선박 포렌식, 항공기 포렌식으로 한다[17].

2.4. 영구기록물

6.25전쟁으로 인하여 국가기록물 이 제대로 관리, 보존되지 못하고, 없어지거나, 폐기, 방치되어 옴으로써, 국가 발전에 자료로서 이용되지 못하였다. 1999년 1월 29일 ‘공공기관의 기록물관리에관한법률’(이하 ‘기록물관리법’)이 제정되었다.

기록물관리법의 주요사항을 살펴보면 다음과 같다. * 공공기관은 기록물의 보존기관, 공개여부, 비밀여부, 접근권한 등 분류 관리 (법제 19조 1항), * 30년 이상 기록물은 영구기록물관리기관으로 이관(19조 3항), * 공공기관이 폐지된 후에 그 사무를 승계하는 기관이 없을 경우 기록물을 소관 영구 기록물관리기관으로 이관(25조 1항) 폐지기관의 기록물 관리를 위해 영구기록물 관리기관 직원을 파견할 수 있음(2항), * 기록물이 유출되어 민간인이 소유 또는 관리하는 경우 당해 기록물은 회수. 선의 취득자에게는 보상 가능.(26조 1항), * 비공개로 분류한 기록물은 5년마다 공개여부 재분류(35조 2항)이다.

III. RFID 유비쿼터스

영구기록물관리시스템 설계

중요한 영구기록물은 ‘기록물관리법’에 의하여 관리하되 정보의 효율적인 확대 재생산을 위해 RFID와 유비쿼터스 정보 통신기기를 이용한 RFID 유비쿼터스 영구기록물관리시스템을 설계하고자 한다.

3.1. RFID 영구기록물관리시스템 현황 분석

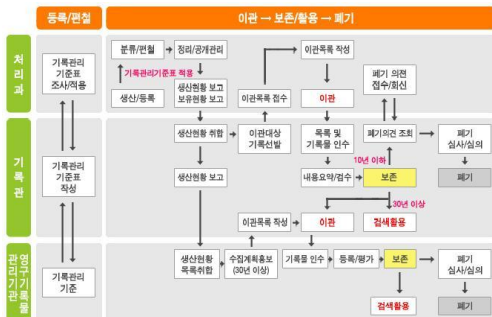


그림 4. 영구기록물 관리의 표준 업무 처리도
Fig 4. Public Information Documental administration's standard processing

그림 4는 영구기록물 관리의 표준 업무 처리도에 따르는

실제 기록물관리 시스템에서 기록관리를 실행하는 기록물관리부서의 프로세스이다. 영구기록물 관리부서에서는 기록관리의 효율성과 국가기록물의 추적 및 이력 조회, 대출, 반납, 폐기 정보의 추적을 위하여 RFID를 이용한 유비쿼터스 영구기록물관리시스템의 세부 설계가 필요한 부분이다.

표 1은 본 논문에서 표본이 되는 RFID를 이용한 유비쿼터스 영구기록물관리시스템을 설계하기 위한 데이터 내용을 분석한 것이다.

표 1. 영구기록물관리시스템 데이터 정보 내역

Table 1. data information particulars of Public Information Documental System

정보구분	지역	구축건수	데이터크기	용량
기록보존	인천	64만 건	400 byte	420Mbyte
	대전	35만 건		210Mbyte
	부산	60만 건		420Mbyte
기록대출	인천	10만 건	400 byte	70Mbyte
	대전	10만 건		70Mbyte
	부산	5만 건		35Mbyte
영구·준영구 사건기록	서울중앙	2만 건		2TB
	서울남부			
	대전			
	고양			

3.2. S/W, H/W, 네트워크 설계

위 표 1의 영구기록물관리시스템 데이터 정보를 바탕으로 유비쿼터스 RFID 영구기록물관리시스템에 대한 S/W와 H/W를 설계한다.

표 2는 영구기록물관리시스템 S/W 부문으로 기록 보존, 대출시스템과 RFID기반 기록관리 시스템으로 구성되며, 웹서버, WAS, DBMS에 관한 S/W의 내용과 품명 수량을 나타내었다.

표 2. 영구기록물관리시스템 S/W

Table 2. Public Information Documental Administration System S/W

구분	용도	품명	수량	비고
기록보존, 대출시스템	웹서버	IBM Http Server	1	3개 기관
	WAS	IBM Websphere	1	
	DBMS	IBM DB2	1	
RFID기반 기록관리 시스템	웹서버	RESIN	1	3개 기관
	WAS	RESIN	1	
	DBMS	ORACLE 10g	1	

표 3은 영구기록물관리시스템 H/W 부문으로 기록 보존, 대출시스템은 독립적인 보안 관제를 위하여 OS는 Linux로 구성되며, RFID기반 기록관리 시스템의 H/W타입으로 연간 무휴 유지관리의 안정성을 위해 Unix서버를 도입하여 H/W를 구성하였다.

표 3. 영구기록물관리시스템 H/W
Table 3. Public Information Documental Administration System H/W

구분	모델	수량	OS	CPU	메모리	용도
기록 보존, 대출시스템	IBM 9672-R26	1	OS	219 MIPS	6GB	DB서버
			Linux 390	110 MIPS	1GB	웹서버
RFID기반 기록관리 시스템	IBM P555A	각 1	Unix	1.65GHz * 8cOre	16GB	DB서버 웹서버

그림 5는 RFID 유비쿼터스 영구기록물관리시스템의 네트워크 구성도이다. 외부와의 연결에 라우터와 네트워크 보안 장비인 방화벽(Firerwall)[18]과 DDoS공격[19]과 순간 과다 패킷량에 대비한 L4스위치를 구성하고, AP1서버, AP2서버, 개발서버, DB, 백업서버를 구축하고 트래픽이 많은 데는 광(Fiber)케이블로 연결하였으며, 백업 디바이스를 지원하기 위하여 SAN스위치를 연결하였다.

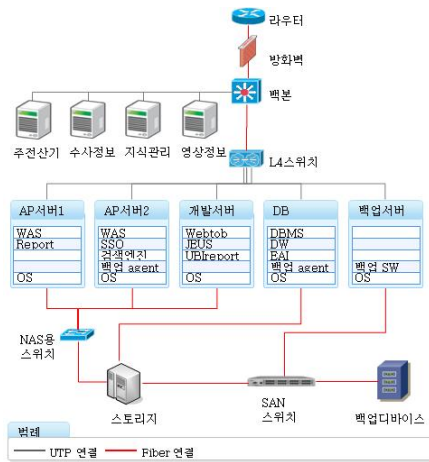


그림 5. 영구기록물관리시스템 네트워크 구성도
Fig 5. Public Information Documental Administration System network schematic diagram

3.3. RFID 유비쿼터스 영구기록물관리시스템 설계

영구기록물관리시스템의 통합 관리시스템을 구축하려면 영구기록물에 대한 현재 보관, 대여 상태에 대한 추적과 통계자료의 생성이 필수적이다. 이를 위해서는 영구기록물에 RFID 기술을 적용하면 된다.

표 4는 영구기록물에 RFID를 적용하여 영구기록물관리시스템을 운영할 때의 정보 입력, 보존, 대출, 반납, 열람, 검색,

비인가 반출 방지, 현황 관리, 로그인관리, 사용자 권한관리, 코드관리 등을 위한 내용 및 장비를 설계한 것이다.

위 표 4는 RFID 영구기록물관리시스템 내용 및 장비에 적용하기 위한 RFID 설비 계획이다.

- 1) 인천, 대전, 부산 지방청 등의 RFID 인프라 구축
- 2) 900MHz 대역 RFID(13.56MHz 대치) 태그 공급
- 3) RFID 태그 부착, DB자료 등록 및 이관
- 4) RFID 응용 프로그램 기능 추가 및 고도화

국내에서 적용되고 있는 RFID 900MHz와 13.56MHz에 대한 표준화 규격 내용으로 국가 표준원의 홈페이지에 있는 것을 표준으로 하여 설계하였다.

표 4. RFID 영구기록물관리시스템 내용 및 장비
Table 4. RFID Public Information Documental Administration System Service contents and Embodiment equipment

구분	상세구분	내용	구현 장비
정보 입력	기록 정보 전산 입력	시스템에 기록물 세부 사항 입력 보존	웹
보존	분류 및 전산 보존	기록물의 위치 지정 및 전산적인 위치 등록	웹
	서고내 기록보존	기록물을 보관하는 보존	웹 휴대형 리더기
대출	RFID태그로 대출인식	기록물의 대출시 직접 키보드로 내역을 입력하는 대신 RFID리더를 활용하여 자동입력	웹 무인대출 반납기
	대출정보 전산입력	시스템에 기록물 대출신청, 대출승인, 대출 정보 입력	
반납	RFID태그로 반납 인식	기록물의 반납 시 직접 키보드로 내역을 입력하는 대신 RFID리더를 활용하여	웹 무인대출 반납기
	반납정보 전산입력	시스템에 기록물 반납정보입력	
열람	조회	기록물의 보존, 대출 반납 현황 조회	웹 이동형 리더기 휴대용 리더기
		정수 점검	기록물의 보존위치 점검
검색	오보존 검색	랙에 보관된 기록물 중 잘못된 위치에 보존된 기록물을 검색	휴대형 리더기 이동형 리더기
		비인가 반출 방지	대출 대상 목록에 포함 되지 않은 기록물이 반출될시 경고 출력
현황 관리	현황정보 표시	기록물의 다양한 현황정보 표시	웹 현황판
기타	로그인관리, 사용자 권한관리, 코드관리 등		웹

3.4. FRID 성능 분석

기존에 사용하던 RFID 13.56MHz 대역의 태그와 신규로 공급되는 RFID 900MHz 대역의 태그를 이용하여 성능 실험을 하였다.

900MHz RFID 와 13.56MHz 비교 실험 결과는 표 5에 나타내었다 실험결과 900MHz RFID가 인식영역과 거리 및 장거리 인식에서 모두 우수한 인식 결과를 나타내었고, 기록물 중첩에 따른 태그 중첩과 인식 이동 방향에서도 실험결과 상대적으로 우수한 성과를 나타내어 900MHz대역의 RFID를 채택하도록 하였다.

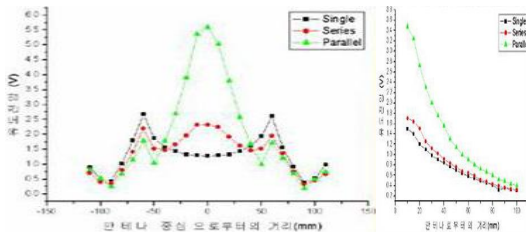


그림 6. RFID 900MHz와 13.56MHz 안테나 인식율
Fig 6. RFID 900MHz and the 13.56MHz antenna awareness rate

표 5. RFID 900MHz와 13.56MHz 비교 실험
Table 5. 900MHz RFID vs 13.56MHz comparison experiment

항목	RFID 900MHz	RFID 13.56MHz
미인식영역	존재하지 않음	존재함
단거리인식	1m이내	30cm이내
장거리인식	4m / 최대 10m 가능	지원 안됨
Near, Far coupling	지원 함	지원 안함
동시 인식 수량(100%)	200권 이상	10~20권 이하
상황별 인식거리	120cm이상 (게이트기준) 40cm 이상 (휴대용 기준)	70cm 이하(게이트기준) 30cm 이하(휴대용기준)
태그 사이즈	0.5cm x 10cm Strip 형태 및 소형 지원 기능(인식거리 보장)	태그 사이즈가 작은 경우 인식 거리가 짧음
태그 비용	저가(900MHz칩 생산 공급업체 증가)	고가(13.56MHz칩 전용 생산 공급 업체 수 감소)
태그 이동 방향 인식	태그 Direction 기능 개발 태그의 이동 방향 인식	불가능
기록자료 양과 중첩 태그 점검	태그 중첩, 인식 방향에 무관하게 인식 (20 페이지 이상 중첩된 경우도 99%이상 인식)	태그 중첩, 인식 방향 등으로 인식 성능 떨어짐 (100 페이지 정도의 자료 중첩된 경우 70%이하 인식)

실험실에서 안테나 중심으로부터의 거리 인식율 시험에서

RFID 900MHz와 13.56MHz 안테나 인식율에 관한 내용을 테스트 한 결과 그림 6처럼 RFID 900MHz 대역은 안테나에 근접 100mm 반경 내에서 유도전압이 효율적으로 인식되어지나, 13.56MHz 대역은 안테나 근접 100mm 반경을 벗어나면 급격하게 유도전압이 약화되어 인식율이 낮아짐을 알 수 있다.

영구기록물관리시스템을 구축을 하는 현장에서 그림 7처럼 RFID 게이트형 리더기에 대한 실험을 하였고, 그림 8처럼 RFID 휴대형 리더기에 실험을 하였다.



그림 7. RFID 게이트 형 리더기 실험
Fig 7. RFID Gate Type Leader flag experiment



그림 8. RFID 휴대형 리더기 실험
Fig 8 RFID carrying Mobile Style Leader flag experiment

표 6. RFID 900MHz 규격, 성능, 반출입 인식 실험
Table 6. RFID 900MHz standard, performance, carrying in out awareness experiment

실험 항목		실험 항목 상세	시험결과
규격 시험	주파수 범위	917MHz ~ 923.5MHz	적정
		최대 출력 전력(dBm)	적정
		채널 수	적정
성능 시험	게이트형 리더태그 인식율 시험	기록물 100권, 보통 속도	100%
		기록물 100권, 빠른 속도	100%
		기록물 200권, 보통 속도	100%
		기록물 200권, 빠른속도	100%
	휴대형 리더태그 인식시험	기록물 200권, 1분내 인식 건수	200권 이내
기타 시험	무단반출 체크시험	기록물과 게이트를 뛰어서 통과	감지
		게이트 상, 하단으로 기록물 통과	감지
		게이트 상, 하단으로 기록물 통과	감지
		몸속에 은닉 후에 기록물 통과	감지

실험 내용은 제품평가방법으로 규격 및 성능에 관한 실험으로 규격시험은 주파수, 출력, 채널, 호핑에 관한 기준 규격 판정 실험, 성능시험으로 게이트형 리더 및 휴대형 리더 인식 시험, 기타 시험으로 무단반출 체크 시험, 태그의 안정성, 인식 패턴 등을 실험 하였으며, 실험 결과는 표 6에서 정리하였다.

3.5. 영구기록물 관련 시스템과의 연계방안 설계

영구기록물의 대여를 위해서는 등록된 영구기록물에 대한 이력등록과 자료의 추적 등의 내용을 영구기록물관리시스템에서 통합관리하고, 프로세스 표준화, 인프라의 최적화를 위해서는 기록을 관리하는 기록자동추적시스템과 영구기록관리 시스템을 통합 개발하고 구축 운영할 필요가 있다. 영구기록관리시스템의 통합 관리를 하면 기록 업무의 효율성 증진, 업무 부담 감소, 장비 도입과 관리 비용의 감소 효과가 있다.

그림 9는 정보시스템의 EAI 구성과 실시간 처분 반영, 통합인증 구현 효율적 DB 구성방안을 토대로 하여 기록자동추적시스템과 영구기록관리 시스템을 연계 관리하는 방안에 대해 설계를 하였다.

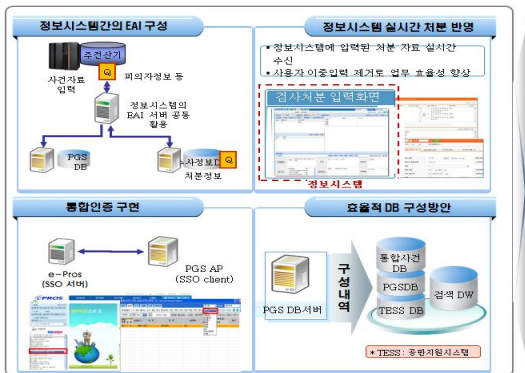


그림 9. 유틸리티스 RFID 영구기록물관리시스템의 연계 방안
Fig 9. Ubiquitous RFID Public Information Documental Administration System S/W construction

표 7은 유틸리티스 RFID 영구기록물관리시스템 전체 설계 내용을 계획에서 인도까지의 진행도표를 나타낸 것이다. 설계 내용에 의하여 구축 작업을 진행 할 때에 진도를 체크하고 계획에 의하여 구축 일정을 수행한다.

표 7 유틸리티스 RFID 영구기록물관리시스템 구축 진행표
Table 7. Ubiquitous RFID Public Information Documental Administration System construction progress ticket

단계	수행업무	M	M+1	M+2	M+3	M+4	M+5
계획	프로젝트팀 편성	■					
	세부개발 계획 수립	■					
분석	요구 분석	■					
	환경 분석	■					
	현행 시스템 분석	■					
설계	연계 시스템 설계		■	■			
	응용프로그램 설계		■	■			
	설치도면 설계	■	■				
	장비 발주		■				
구현	응용 프로그램 개발			■	■	■	
	장비설치			■	■	■	
	서버 셋업		■	■			
	단위 테스트				■	■	■
표준화	업무 분석	■					
	업무 표준화		■				
태그	대상기록물 선정	■	■				
	태그 발주	■	■				
교육	태그 부착		■	■	■	■	
	운영자 교육					■	■
통합 시험	사용자 교육					■	■
	통합 시험					■	■
이전	자료 이관					■	■
	기술 이전					■	■
인도	인수 시험						■
	운영						■

IV. RFID 유틸리티스 영구기록물관리시스템 구축 및 분석

4.1. RFID 영구기록물관리시스템 구축

표 7의 내용에 의해서 영구기록물관리시스템을 구축을 위한 RFID 유틸리티스 영구기록물관리시스템 구축에 필요한 S/W와 H/W를 구축한다. S/W 부문은 기록보존 / 대출시스템과 RFID기반 기록관리 시스템을 구축하였으며, 웹서버, WAS, DBM에 관한 S/W를 구축하였다.

그림 10은 유틸리티스 RFID 영구기록물관리시스템 S/W 구축 내용이며, 그림 11은 RFID 영구기록물관리시스템 H/W구축 구성도이다.



그림 10. RFID 유틸리티스 영구기록물관리시스템 S/W구축
Fig 10. Ubiquitous RFID Public Information Documental Administration System H/W construction



그림 11. RFID 유틸리티스 영구기록물관리시스템 H/W구축
Fig 11. RFID Public Information Documental Administration System hardware schematic diagram

RFID 시스템은 RFID labels(트랜스폰더), RFID label 리더 또는 트랜시버, Application system으로 구축된다. 영구기록물에 RFID 부착이 되면서, 영구기록물 무단 반출입을 막는 게이트형 리더기가 입출고 시스템을 통해 이루어지며, 휴대형 리더기를 이용한 기록물 확인과 무인 대출/반납기와 RFID 리더기 및 입출고될 때 입출고 게이트를 지나도록 한다. 이때 인식된 기록물에 부착된 RFID태그에서 인식된 정보는 LLRP(Low Level Reader Protocol)를 통해서 RFID 미들웨어와 통신을 하며, 기록은 Time Stamp와 해시함수 SHA-1

을 통해서 보안 감시서버와 영구기록물관리시스템에 2중 저장된다. 유틸리티스 RFID 영구기록물관리시스템 구축에서 가장 많은 시간과 내용을 차지하는 부분은 그림 12처럼 RFID 900MHz 태그 부착 과정이다. 태그 부착 관리 과정을 표준화하여 작업의 양을 줄이고, 태그 부착의 정확성을 높이기 위해 RFID 900MHz 태그 부착 과정을 표준화하였다.



그림 12. 영구기록물 RFID 태그 부착 관리
Fig 12. Public Information Documental RFID tag sticking administration

영구기록물관리시스템의 구축 내용은 그림 13과 같다. 영구기록물을 보관하고 있는 기존의 서고를 개조하여, 서고를 설치하여 영구기록물에 RFID 900MHz 태그를 표준화 지침대로 부착하고, RFID 휴대형 리더기와 게이트 형 리더기와 연계된 휴대형 리더기와 게이트 형 리더기 인식 시스템을 구축하고 테스트 하였다.

계획된 S/W와 H/W 시스템을 인스톨하고 운영 프로그램을 적용하여 영구기록물관리시스템을 구축 하였다.



그림 13. 영구기록물관리시스템 시스템 구축
Fig 13. Public Information Documental Administration System construction

4.2. 영구기록물 관련시스템과의 연계 구축 분석

4.2.1. 영구기록물자동추적관리시스템 연계 구축

RFID를 이용한 영구기록물 보존사무의 표준화를 통해 영구기록물자동추적관리시스템의 관리체계를 구축하기 위해 모빌렉, 기록물 등에 900MHz대역의 RFID태그를 부착하여 기록물관리의 정확한 입·출고 및 오보존 방지, 열람, 대출업무, 폐기대상 기록물에 대한 종류별 대상 선정 및 자동 분류를 실시한다. 영구기록물의 RFID 태그 및 관리시스템으로부터 수집된 정보는 기존의 공공기관 DB서버와 연계하여 타기관으로 부터 인수된 영구기록물들을 통합하여 연계 구축하여 정보를 공유하게 한다.

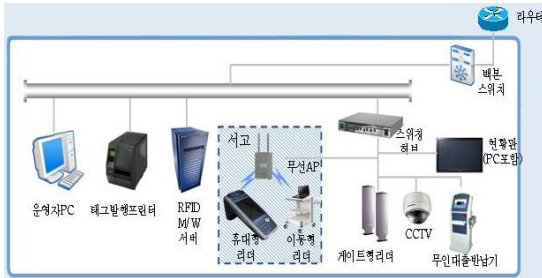


그림 14. 영구기록물자동추적관리시스템 연계 구축
Fig 14. Public Information Documental Automatic Tracking Administration System link construction

4.2.2. 영구기록물자동추적관리시스템 연계 분석

그림 14처럼 휴대형 RFID 리더기, 이동형 RFID 리더기, 게이트형 RFID 리더기, 무인대출 반납기를 구축하여 영구기록물의 보존, 열람, 대출, 폐기 등의 유비쿼터스 정보화를 통한 관리 업무가 가능하고 영구기록물자동추적관리시스템과 연계하여 영구기록물 관리와 오보존 기록물의 현재 기록물 위치추적과 대여, 보관, 폐기 등의 관리가 가능하여 타 기관이나 민간에서 공공기관의 영구기록물에 대한 자료 요청과 상태를 즉시적으로 확인 할 수 있어 유비쿼터스 영구기록물관리시스템으로서의 역할이 가능하다.

4.3. 영구기록관리시스템 보안성 분석

4.3.1. 영구기록관리시스템 보안 항목

RFID를 이용한 영구기록관리시스템의 보안 취약점을 강화시키기 위해서는 RFID는 RF 태그와 리더와 연계 시스템에서 다음과 같은 보안성을 체크하고 보안을 강화 하였다.

- 인증이 되지 않은 리더는 접근차단하고, 태그에 대해

긴 시간동안의 추적(long-term tracking)이 불가능하다.

- 태그 내용은 접근제어 기법에 의해 질의채널(interrogation channel)이 안전하지 않으면 암호화전송을 실시한다.

- 외부로 돌출된 태그는 랜덤화 태그와 보유자 사이의 장기간 관련성을 회피하는 장치를 갖춘다.

- 태그와 리더는 모두 상호인증(mutual authentication)을 거친다.

- 전원공급차단에 의한 RFID 프로토콜의 손상과 가로채기 공격(hijack)에 노출되지 않는다.

- 태그와 리더는 재생공격(replay attack) 및 공격자 중간공격(man-in-the-middle attack)에 저항력을 갖춘다.

- 태그와 리더에 대한 스푸핑이 어렵다.

4.3.2. 포렌식 자료 생성

리더기에서 인식된 접속 Log History를 영구기록물자동추적관리시스템과 보안감사서버에 기록 할 때 해시함수 SHA-1을 사용하여 2중으로 저장하고, 영구기록물관리시스템과 보안감사서버에 저장된 것과 기록보관실에 기록과의 해시함수 비교 하여 무결성을 검증한다.

그림 15처럼 보안 서버에서 해시함수를 SHA-1을 생성하여 영구기록물관리시스템과 보안감사기록 서버에 2중으로 저장할 때 생성된 해시함수와 함께 저장을 한다.

COM2	Read	Stop	Reader Info
Reader2	3512345602FABAB19A5A79CA	Sat Feb 11 11:29:33 KST 2006	
Reader2	3512345602FABAB181DE3B7F	Sat Feb 11 11:29:34 KST 2006	
Reader2	331233043210148132AD85C8	Sat Feb 11 11:29:34 KST 2006	
Reader2	3512345602FABAB181DE3B7F	Sat Feb 11 11:29:36 KST 2006	
Reader2	3512345602FABAB10B11DC59	Sat Feb 11 11:29:37 KST 2006	
F1019	30111114321022111115E900	FFFF0000FF0000F000000000	
F1020	331301230200023111112F5A	FFF80000FF0000F000000000	
F1021	315115211026211211403243	FFFF0000FF8000F000000000	
F1022	331230101130432102FAD0F8	FFFF0000FF0000F000000000	
F1023	33123010113043210254315E	FFFF0000FF0000FC00000000	

Reader2 Using Cache
Filtering Mode Normal Bit Parallel ABV

그림 15. 영구기록물관리시스템 해시함수 생성
Fig 15. Public Information Documental Hash function creation

중요 영구기록물의 RFID을 이용하여 등록, 보관 및 수정과 폐기를 할 때마다 Time Stamp을 이용해서 영구기록물관리시스템과 보안감사서버에 2중으로 저장하고 그림 16처럼 Time Stamp값과 해시함수 상호비교 원본성과 무결성을 증명한다.

태그 식별자	판독기	인식 시간
10.10.4	Gate A	12:00:00
10.10.2	Gate A	12:00:00
10.10.5	Gate A	12:00:01
10.10.1	Gate A	12:00:02
...

그림 16. Time Stamp값을 적용한 판독기 값
Fig 16. Optical bar-code reader value that apply Time Stamp value

4.4. 영구기록물관리시스템 효과 분석

표 8처럼 RFID 설치 전과 후의 개선효과를 900MHz RFID, 보안 시스템, 통합 연계 시스템, 담당 기관 업무, 유관 기관, 기술효과로 구분하여 시스템관리자와 20명과 업무 담당자 80명을 합한 총 100명에게 설치 후 만족도 조사를 하여 완전만족 100점, 매우 만족 95점, 만족 90점, 충분 85점, 보통 80점, 보완 필요 75점, 불만족 70점을 기준으로 하여 설문으로 평가 하였으며, 통계 결과 평균 92점으로 매우 만족과 만족 사이로 나타나, 기존의 영구기록물관리에서 유비쿼터스 RFID 영구기록물관리시스템 구축으로 개선된 효과를 나타내었다.

표 8. RFID 설치 전과 후의 개선효과
Table 8. Improvement effect after RFID establishment whole curriculum

항목	RFID 설치 전	RFID 설치 후	만족도 (점)
900MHz RFID	13.56MHz 인식률 낮음	900MHz RFID 인식률 향상, 만족, 유비쿼터스시스템 작동	95
보안 시스템	기본 보안시스템	RFID 보안성 강화, 비인가 반출 가능성 차단, 개인 보안 책임제 정착, 시스템보안에서 자료별보안성 강화	90
통합 연계 시스템	시스템 연계 작동 않됨	국가 문서관의 체계 및 문서 검색서비스와의 연계를 통한 문서 등록, 보관, 대출, 추적 기능, 표준화 선도, 데이터 통합, 인프라 최적화, 프로세스 표준화	93
담당 기관 업무	수작업으로 영구기록물관리	기록물 관리, 업무 절차 표준화로 시간 비용 절감, 실시간 문서의 위치, 개요, 이용 상황 등의 업무 프로세스의 유비쿼터스 정보화 모니터링 가능	93
유관 기관	공문 작성, 수발, 요청, 수작업 시간 비용 증가	기록물에 대한 정보를 제공, 기록 신속 대출로 인한 유기적인 업무 가능, 공공기관 협조, 대민서비스 향상	91
기술 효과	원본문서 수기 기록, 관리	원본문서의 전자문서 이중 보존, 시스템 개발로 유비쿼터스 기술 발전, 국가 경쟁력 향상	90

V. 결론

본 논문에서는 900MHz RFID가 기존의 13.56MHz RFID에 비해 성능과 인식율에 우수성을 실험을 통해 검증하고, 영구기록물에 태그를 부착하여 기록물을 등록 관리하고, 이력을 추적하고, 보존, 검색하기 위한 영구기록물의 현황 분석을 위하여 S/W, H/W, 네트워크 설계를 통한 유비쿼터스 RFID 영구기록물관리시스템 설계하고 구축하였다. 구축에서 영구기록물추적시스템과의 연계를 하고 보안 점검과 포렌식 자료를 생성하여 개선효과를 분석하였다. 본 논문의 연구를 통하여 국가기록물 관리에 유비쿼터스 정보화 기술 적용과 포렌식 기술 발전에 기여하게 될 것이다.

향후 연구로는 영구기록물관리시스템의 유비쿼터스 정보화 시스템과의 연계 효율성 검증 및 개선과 국가기록물관리 전체 시스템에 대한 효율성 검증에 대한 연구가 이루어지면 좋겠다.

참고문헌

- [1] 윤여진, 김순희, "영구기록물관리기관의 공개제도 운영방안 연구," 한국기록관리학회, 제9권, 1호, 51-75쪽, 2009년 6월.
- [2] 김세경, "우리나라 공공기록물 관리에 관한 법규의변천," 한국기록관리학회, 제7권, 1호, 5-38쪽, 2007년 6월.
- [3] 이규안, 박대우, 신용태, "포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법," 한국컴퓨터정보학회, 제11권, 6호, 175-184쪽, 2006년 12월.
- [4] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing, Communications of the AC M," Vol. 36, No. 7, pp.75-84. 1993.
- [5] 조영섭, 조상래, 유인태, 진승현, 정교일, "유비쿼터스 컴퓨팅과 보안요구사항 분석," 한국정보보호학회, 제14권, 1호, 21-34쪽, 2004년 2월.
- [6] David Bell Brunel, "Emergent application integration of ubiquitous information systems (UBIS)." Proceedings of the 4th international workshop on Services integration in pervasive environments. pp.13-18. July 2009.
- [7] 유승화, "RFID 기술 현황 및 활용분야," 한국정보과학회, 제23권, 7호, 64-70쪽, 2005년 9월.
- [8] 양단희, 김연수, "u-City의 서비스, 인프라, 기술," 한국

- 인터넷정보학회, 제10권, 1호, 93-98쪽, 2009년 3월
- [9] 박현성, 김종덕, "고속 RFID 필처링 엔진의 설계와 캐쉬 기반 성능 향상," 한국통신학회, 제31권, 5A호, 517-525 쪽, 2006년 5월.
- [10] Y. Chen, J. S. Chou, and H. M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems", Computer Networks, Vol. 52, pp. 2373-2380, 2008.
- [11] A. Juels, R. L. Rivest, M Szydlo "The blocker tag: selective blocking of RFID tags for consumer privacy," InProceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.
- [12] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System," Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pp. 201-212, 2004.
- [13] Michael G. Noblett, Mark M. Pollitt, Lawrence A. Presley, "Recovering and Examining Computer Forensic Evidence," Forensic Science Communication, Vol. 2 No. 4, Oct. 2000.
- [14] Jeanine M. Anderson, Richard P. Barkley, "The Brave New World of E-Discovery-Part I," The Colorado Lawyer, Vol. 36, No. 8, pp. 83-90, Aug. 2007.
- [15] Warren G. Kruse II, etc., "Incident Response Essentials," Computer Forensics, Addison Wesley, 2002.
- [16] 정정기, 박대우, "로그 히스토리 분석을 사용한 웹 포렌식 알고리즘 연구," 한국컴퓨터정보학회, 제 12권, 제 1호, 117-126쪽, 2007년 3월.
- [17] 박대우, "Mobile Forensic," 숭실대학교대학원, 2008년 8월.
- [18] 박대우, "무선방화벽의 설계 및 구현에 관한 연구," 한국컴퓨터정보학회논문지, 제 8권, 제 1호, 44-50쪽, 2003년 3월.
- [19] Felix Lau, Stuart H. Rubin, Michael H. Smith, Ljiljana Trajkovic, "Distributed Denial of Service Attacks," 2000 IEEE International Conference on Systems, Man and Cybernetics, Volume:, pp. 2275-2280, Mar. 2000.

저 자 소 개



장 영 상

1987: 성균관대학교 정보공학과(학사)
 1991: 경희대학교 대학원 전자계산공학과(석사)
 1996: 경희대학교 대학원 전자계산공학과(박사수료)
 1991~현재: 호서대학교 평생교육원 사이버해킹보안과 주임교수
 관심분야 : 이동통신, 네트워크 보안, 유비쿼터스 시스템, 암호화, 정보보호, 해킹과 보안



이 승 룡

1978: 고려대학교 재료공학과(학사)
 1986: Illinois Institute of Technology 전산학과(석사)
 1991: Illinois Institute of Technology 전산학과(박사)
 1992~1993: Governors State university 조교수
 1993~현재 : 경희대학교 전자계산공학과 교수
 관심분야 : 실시간시스템, 실시간 보장 허용 시스템, 멀티미디어 시스템