논문

비밀기록을 관리하기 위한 시스템 설계 연구

A Study of System Design for Management the Confidential Records

홍덕용(Hong, Deok-Yong)*

1. 서론
2. 이론적 배경
   1) 비밀기록물관리에 관한 법률적 근거
   2) 선행연구
3. 비밀기록물시스템의 필요성과 정보공개청구·설문조사 분석
   1) 시스템 목적 및 필요성
   2) 정보공개청구·설문조사 분석
4. 비밀기록을 관리하기 위한 시스템 설계
   1) 시스템 구성 및 기능
   2) 시스템 보안
   3) 시스템 접근(메타데이터)
   4) 시스템 활용(열람 및 출력)
5. 결론

* 부산광역시 수영구청(igre@korea.kr)
■투고일 : 2017년 3월 31일 ■최초심사일 : 2017년 3월 31일 ■게재확정일 : 2017년 4월 24일

〈초록〉

비밀기록물관리에 관한 규정이 제·개정되면서 비밀기록물의 관리의 중요성이 커지게 되었지만 기록관리 현장에서 여전히 비밀기록물의 특성과 가치를 고려한 관리가 이루어지지 않고 있는 실정이다. 비전자환경에서 관리하던 비밀기록물을 전자환경에서 처리하여 효율적으로 비밀기록물에 대한 장기 보존 대책을 마련하고자 하였다. 공공기관에서 보유하고 있는 비밀기록물을 자체적으로 관리할 수 있는 시스템을 개발하고 비밀기록물의 멸실과 훼손에 따른 정보손실을 미연에 방지하고, 인가 받은 이용자의 디지털 보안 환경에서 편리하게 활용할 수 있는 체계를 확보하여 비밀기록물에 대한 상용 관리체계 기반을 설계하고자 하는 것이다. 이 연구에서는 비밀기록물을 관리하기 위한 시스템의 기록관리 국제표준에 맞는 시스템 구성 요구사항을 분석, 분석된 요구사항을 바탕으로 한 시스템 설계 등 시스템에 관련된 사항과 시스템의 보안 및 암호화, 메타데이터, 비밀관리기록부 정리 및 출력에 대한 전체적인 설계 과정과 표준 관리에 대하여 살펴보았다.

주제어 : 비밀기록물, 비밀기록관리시스템 설계, ISO 15489, OAIS 참조 모형, DoD 5015.2-STD

〈Abstract〉

With the enactment of regulations on confidential records management, the management of confidential records has become more important than ever. However, there remains no management method in the field of records management that takes the feature and values of confidential records into consideration. For this, this study processed electronically confidential records managed in a non-electronic environment. In addition, we developed a system that will allow public institutions to manage confidential records independently, that will prevent loss of information because of loss of or damage to the confidential records, and that can be used conveniently in the digital security environment of

authorized users to establish a foundation for commercial management. In this study, we analyzed the system configuration requirements according to the international standard for the records management of a confidential records management system and system-related issues such as system design based on the analyzed requirements, system security and encryption, and metadata, the overall process of establishing and outputting secret management records and standard management.

Keywords : Confidential Archives, Confidential Archives System Development and Management, ISO 15489, OAIS Reference Model, DoD 5015.2-STD

1. 서론

비밀은 그 내용이 누설되는 경우 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가기밀로서 비밀로 분류된 것을 말하며 비밀기록물은 공공기관이 생산한 문서 · 대장 · 카드 · 도면 · 시청각물 · 도서 · 전자문서 등의 기록물 중 비밀로 분류된 기록물 이라고 정의 내리고 있다(국가기록원 2012, 5). 2012년에 개정된 공공기록물관리에 관한 법률에 의하면 기록물관리기관의 장은 기록물이 전자적으로 생산 · 관리되도록 필요한 조치를 마련하여야 하며, 전자적 형태로 생산되지 아니한 기록물도 전자적으로 관리되도록 의무화되었다(공공기록물법 제6조). 이 조항은 종이기록물 보존, 업무결과 중심의 관리에서 벗어나, 업무 전(全) 과정의 기록을 전자적으로 관리 · 활용하는 선진 기록관리체계로 전환을 목적으로 행정업무의 투명성 및 업무활동과 처리행위에 관한 증거와 정보를 전자기록형태로 획득, 유지하기 위해서이다. 또한 보안업무규정에서는 전자적 방법을 사용하여 비밀을 관리할 수 있다(보안업무규정 제21조). 재정되었다. 이렇게 비밀기록물관리

에 관한 규정이 신설 또는 개정되면서 비밀기록물의 관리의 중요성이 커지게 되었지만 기록관리 현장에서 여전히 비밀기록물의 특성과 가치를 고려한 관리가 이루어지지 않고 있는 실정이다.

이러한 공공기관에서 생산되어진 비밀기록물을 체계적이고 효율적으로 관리하고 비밀의 보호기간 및 보존기간이 만료될 시, 직원들이 쉽고 효율적으로 접근 활용하기 위해서는 관리시스템이 필요하다.

이를 위해 비밀기록물을 관리하고 일반문서로 재분류되었을 때 직원들의 효과적인 활용을 위해 시스템 설계가 필요하다. 『공공기록물관리에 관한 법률』과 『보안업무규정』 등을 통하여 비밀기록물관리에 대한 이론적 배경을 마련하고, 기록관리에 관한 선행연구를 하였다.

그리고 비밀기록물의 관리를 위한 시스템 설계를 위해 비밀기록관리시스템이 기구축된 기관에 정보공개를 청구하고 자치단체 기록물전문요원을 대상으로 비밀기록관리시스템 관련 설문조사를 실시하였다. 위의 결과와 기록관리 국제 표준 측면에서 시스템 구성 절차, 시스템 보안, 시스템접근 · 활용 등에 대한 기술적인 측면을 위주로 설계하였다. 구체적으로는 시스템 구성 원칙, 시스템 설계, 효과적인 데이터 관리와 활용을 위한 단위모듈별 기능분석과 같은 기술 요구 사항과 시스템 운영 및 보안 등의 설계 방법을 기록관리 국제표준인 ISO15489, OAIS 참조모형, DoD5015.2를 통해 연구하였다.

본 연구에서는 기록물관리법과 보안규정 등에서 규정하고 있는 비밀기록물 자체에 대한 생산, 보존, 이관, 평가, 폐기 등에 대해서는 연구의 범위에 포함시키지 않았다.

본 연구의 목적으로는 공공기관의 비밀문서를 관리 하는 시스템을 설계해보고 비밀기록물 전담 관리요원과 비밀취급직원들이 시스템을 사용하기 위해 최대한의 접근 및 활용 서비스를 제공하고, 비밀기록물의 생산 · 접수에서부터 재분류까지 비밀기록물 관리와 활용을 위한 발전적인 청사진을 제시함으로써, 향후 비밀기록물관리를 위한 시스템 개발과 운영에 있어서 하나의 사례연구로 활용될 수 있을 것으로 기대한다.

2. 이론적 배경

1) 비밀기록물 관리에 관한 법률적 근거

비밀기록물의 관리에 대한 상용화를 위해 대책을 마련하고, 접근과 활용의 용이성을 높이기 위한 시스템을 설계하는데 있어서, 관련 법률에서 규정한 내용들을 〈표 1〉로 정리하였다. 이를 통하여 시스템 설계의 필요성과 당위성을 확인 할 수 있을 것이며, 실제 시스템을 설계하고 운영하는데 필요한 이론적 배경을 확보할 수 있을 것이다. 또한 비밀기록물의 관리 및 활용을 위한 업무를 수행함에 있어 그 정당성을 보장받을 수 있을 것으로 생각된다.

2) 선행연구

이를 위해 비밀기록물에 관련된 선행연구들을 검토하였다. 대부분의 선행연구가 비밀기록물 자체에 대한 생산 · 관리 · 현황에 관한 연구가 대부분을 차지하였고 비밀을 관리하기 위한 시스템을 설계 · 구축 · 활용하는 연구는 전무하였다.

연구에서는 국가기록원의 기록관리 공공표준 비밀기록물 관리(NAK/S 20 : 2016 v1.2)와 국가기록원 비밀기록물 관리 실무지침과 유형별 기록관리시스템 설계 · 구축과 시스템보안에 관련된 연구를 살펴보았다.

먼저 기록관리 공공표준비밀기록물 관리에서는 비밀기록물 관리를 위한 공공기관의 책임과 역할을 기술하였으며, 비밀업무에 대한 기록관리기준표의 관리에 대하여 기술되어있다. 그리고 비밀기록물의 생산과 보호기간, 보존기간 부여 그리고 생산현황통보를 위한 절차 및 방법 그리고 이관에 대한 내용이 기술되어 비밀기록물을 관리하는 담당자들에게 지원하게 하였다(국가기록원 2016). 다음으로는 국가기록원의 비밀

기록물 관리 실무지침을 살펴보았다. 지침에서는 공공기관에서 생산·보유하는 비밀기록물을 안전하고 효율적으로 관리하기 위해 필요한 세부적인 업무처리 기준과 절차를 정한 지침을 살펴보았다(국가기록원 2012).

〈표 1〉 비밀기록물관리에 관련 법률 조항 및 내용

구분	해당조항	내용
보안업무 규정	제4조 (비밀의 구분)	비밀은 그 중요성과 가치의 정도에 따라 다음 각 호와 같이 구분한다. 1. Ⅰ급비밀: 누설될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀 2. Ⅱ급비밀: 누설될 경우 국가안전보장에 막대한 지장을 끼칠 우려가 있는 비밀 3. Ⅲ급비밀: 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 비밀
	제8조 (비밀의 취급)	비밀은 해당등급의 비밀취급 인가를 받은 사람만 취급할 수 있다.
	제21조 (비밀의 전자적 관리)	① **각급기관의 장은 전자적 방법을 사용하여 비밀을 관리할 수 있다.** ② 각급기관의 장은 제1항에 따라 비밀을 관리할 경우 국가정보원장이 안전성을 확인한 암호자재를 사용하여 비밀의 위조·변조·훼손 및 유출 등을 방지하기 위한 보안 대책을 마련하여 시행하여야 한다.
공공기록물 관리법	제32조 (비밀기록물 관리의 원칙)	기록물관리기관의 장은 대통령령으로 정하는 바에 따라 비밀기록물 관리에 필요한 별도의 전용서고 등 **비밀기록물 관리체계를 갖추고** 전담 관리요원을 지정하여야 하며, 비밀기록물 취급과정에서 비밀이 누설되지 아니하도록 보안대책을 수립·시행하여야 한다.
	제33조 (비밀기록물의 관리)	① 공공기관은 비밀기록물을 생산할 때에는 그 **기록물의 원본에 비밀 보호기간 및 보존기간을 함께 정하여 보존기간이 끝날 때까지 관리**되도록 하여야 한다. 이 경우 보존기간은 비밀 보호기간 이상의 기간으로 책정하여야 한다. ② 비밀기록물의 원본은 대통령령으로 정하는 바에 따라 소관 **기록물 관리기관으로 이관하여 보존**하여야 한다.
	제34조 (비밀기록물 생산현황 등 통보)	공공기관의 장은 해당 기관이 생산한 비밀 기록물 원본에 대하여 대통령령으로 정하는 바에 따라 매년 **생산·해제 및 재분류 현황을 소관 영구기록물관리기관의 장에게 통보**하여야 한다. 이 경우 통보서식 등은 행정자치부령으로 정하되, 미리 국가정보원장과 협의하여야 한다.

공공기록물 관리법 시행령	제66조 (비밀기록물 관리 전용 서고 등)	① 기록물관리기관의 장은 법 제32조에 따라 **비밀 기록물을 관리하기 위한 전용 서고 및 시설·장비 등을 설치·운영**하여야 한다. ② 법 제32조에 따른 비밀기록물 관리 전담 관리요원은 비밀취급 인가를 받아야 한다. 이 경우 **비밀취급인가권자는 비밀의 누설 또는 유출방지를 위하여 비밀기록물 전담 관리요원에 대한 신원조사, 보안교육 등** 필요한 보안조치를 국가정보원장에게 요청하여야 한다. ③ 기록물관리기관의 장은 비밀기록물 및 비밀기록물 관리에 관한 정보를 취급하는 과정에서 비밀이 누설되지 아니하도록 국가정보원장이 정하는 보안대책을 수립·시행하여야 하며, 국가정보원장은 이를 확인할 수 있다.
	제67조 (비밀기록물의 보존기간의 적용)	① 법 제33조제1항에 따른 비밀기록물 원본(이하 "비밀기록물"이라 한다)의 보존기간은 기록물철 또는 건 단위로 정하되, 제25조제2항에 따른 기록관리기준표의 단위과제에 책정된 보존기간을 적용한다. ② 비밀기록물의 보호기간이 변경된 경우에는 변경된 보호기간 이상으로 보존기간을 재책정하여야 한다.
	제68조 (비밀기록물의 이관)	① 공공기관이 법 제33조제1항에 따라 생산한 비밀기록물은 다음 각 호의 어느 하나에 해당하는 사유 발생시 기록관 또는 특수기록관으로 이관하여야 한다. 1. 일반문서로 재분류한 경우 2. 예고문에 의하여 비밀보호기간이 만료된 경우 3. 생산 후 30년이 지난 경우 등... 이하 생략

다음은 기록물 유형별 시스템 설계·구축관련 연구이다. 임선화는 2004년 연구에서 수집기록물관리기관의 기록관리 업무의 전산화를 위해 수집기록물관리시스템을 설계하였다. 기록물관리시스템의 소프트웨어를 개발하기 위해서는 마르미를 사용하여 요구분석절차와 기록학방법론을 통해 수집기록물관리기관의 업무를 분석하여 프로세스모델링을 하였고 기록물 및 기록물관리정보분석을 통해 엔터티모델링을 수행하였다(임선화 2004).

신동헌외 2명은 시청각(사진/동영상)기록물 관리를 위한 시스템 구축과 운영 사례를 살펴보았는데 국방과학연구소에서 보유하고 있는 아날로그 형태 시청각 기록물을 디지털 변환을 통하여 이용자의 접근 용이성을 확보하고 시스템을 통한 보다 체계적인 관리를 위해 "영상기록관리시스템"을 구축하고 운영 중에 있다. 이에 시청각기록물의 디지털 변환을 통해 DB구축과

이용자의 직접적인 검색·활용을 통하여 기록물에 대한 보존과 활용에 대한 실제 사례를 기술하였다. 디지털변환을 통한 DB 구축 시 표준 업무절차 구현, 품질 기준 설정, 메타데이터 항목 설정 등에 관한 내용을 포함하고 있다(신동헌 외 2009).

위성현은 전자메일의 기록관리를 위한 메타데이터 요소를 제시하고 전자메일 기록관리시스템의 모형을 3단계로 도식화하고 등록, 처분, 검색/열람, 분류, 이관, 시스템 관리의 6개의 기능으로 분석하여 각각의 업무프로세스 과정을 설계하였다. 설계된 프로세스를 바탕으로 우리나라 기록관리 시스템 기능요건과 국제표준 ISO 15489[1]를 참조하여 각각의 기능별 기능요건을 설계하였다. 또한 시스템 기능과 전자메일 기록메타데이터를 중점으로 RDB방식[2]의 데이터베이스와 관계테이블, ER다이어그램 [3]등 데이터 요건을 설계하였다(위성현 2012).

강구민은 특수유형기록물관리시스템 구축에 대한 설계를 하였다. 특수유형기록물에는 시청각기록물, 정부간행물, 행정박물 등이 포함되어 있는데 이들에 대한 체계적인 관리와 장기보존을 위한 기반을 확보하기 위해 H군청에서 구축하여 서비스하고 있는 시스템을 살펴보았다(강구민 2014).

다음은 시스템 보안 관련 연구이다.

서영관은 컴퓨터 시스템 보급의 확대, 대량의 데이터베이스 시스템 구축과 여러 사용자에 의한 데이터 공유, 네트워크 확장과 개방으로 인하여 발생되는 보안의 문제점들을 분석하고, 보안 문제의 해결 방안으로 운영체제, 데이터베이스 시스템, 네트워크에서의 보안요구사항과 시스템 접근방법 그

1) "현용기록 및 준현용 기록관리를 위한 국제표준으로서 목적은 모든 기록을 적절히 처리하고 보호하며, 더 효과적이고 효율적으로 기록에 담긴 증거와 정보를 검색할 수 있도록 하기 위해 기록 관리 정책과 절차를 표준화"하는 것이다.
2) "관계형 데이터베이스라고 한다. 관계 모델에 의한 데이터베이스로서 수학에서의 관계 개념을 응용한 것"이다.
3) "개체-관계모델이라고 한다. 데이터 모델링 과정은 데이터 모델을 그림으로 표현하기 위해 표시하기 위함"이다.

리고 보안기법들을 비교하여 각각의 장단점을 분석하고 효과적인 보안기법 활용방안들을 제시하였다(서영관 1998).

이종열은 암호화와 접근제어 및 감사 기능을 활용한 복합적 DB보안 시스템의 실태와 위험성에 대해 살펴보고 안전한 정보화 자원 보호를 위한 통합 DB보안 시스템의 구축방안에 대해 연구하였다. DB 암호화와 데이터베이스 접근제어 및 감사 기능을 가진 두 가지 보안 분야의 시스템을 상호 연동 하여 관리가 가능하도록 시스템을 구축 하여 이를 통한 데이터베이스에 대한 비인가 사용자의 접근으로부터의 안전이었다. 특히 중요정보에 대해서는 암호화를 적용하여 인가된 사용자 이외에는 열람이 불가능하게 하였다. 또한, 인가된 사용자에게만 접근 권한을 부여함으로써 중요정보 유출을 사전에 차단할 수 있음을 밝혔다(이종열 2005).

이렇게 선행연구에서는 기관에서 보유하고 있는 다양한 기록물을 대상으로 시스템을 구축하고 기관 사용자들에게 효율적인 업무를 제공하고 접근할 수 있도록 하는 연구와 시스템 보안관련에 대한 연구가 이루어졌다. 기관에서 보유하고 있는 일반기록물과는 다르게 비밀기록물은 특성에 맞고 인가를 받은 직원만 접근이 가능하여야하며 강력한 보안이 필요하고 업무의 연속성을 위한 표준 메타데이터 설계와 보안감사를 위한 감사증적 기능이 포함되어야 할 것이다.

3. 비밀기록물시스템의 필요성과 정보공개청구 · 설문조사 분석

1) 시스템 목적 및 필요성

비밀기록을 관리하기 위한 시스템은 공공기관이 보유하고 있는 비밀기록을 통합관리와 네트워크 보안 이용접근 및 활용 체계를 설계함으로써

기관 내 직원들에게는 행정업무의 효율성에 대한 기여와 후대의 직원들에게 지난 비밀기록의 발자취를 남기기 위하여 필요하다. 구체적으로는 모든 공공기관에서 보유하고 있는 비밀기록물을 자체적으로 관리·활용할 수 있는 국가표준시스템을 개발하여 비밀기록물의 멸실과 훼손에 따른 정보손실을 미연에 방지하고, 인가 받은 이용자의 디지털 보안 환경에서 편리하게 비밀기록을 활용할 수 있는 체계를 확보함으로써, 모든 기관에서 비밀기록에 대한 상용 관리·활용체계 기반을 설계하고자 하는 것이다.

비밀기록물의 관리를 위한 시스템 설계의 필요성은 다음과 같다. 첫째, 공공기록물관리에 관한 법 제 6조와 보안업무규정 제21조에서 밝히고 있는 바와 같이 기록물이 전자적으로 생산·관리되도록 필요한 조치를 마련하여야 하며, 전자적 형태로 생산되지 아니한 기록물도 전자적으로 관리되도록 노력하여야 한다는 것에서 필요성을 찾을 수 있다.

둘째, 공공기관에서 관리의 연속성이 떨어져 활용이 되지 못하고 있던 비밀기록물에 대하여 효율적인 접근과 활용 및 체계적인 장기보존을 위한 기반을 마련함으로써 최종적으로는 공공기관의 기록관리 환경을 개선하고자 하는 것에서 필요성을 찾을 수 있다. 현재 공공기관의 각 부서에서는 부서별로 비밀기록관리기록부를 종이(비전자)대장에 관리를 하고 있어 멸실 및 훼손문제가 발생하고, 보안담당자가 인사로 변경이 되기 때문에 업무의 연속성이 떨어진다.

셋째, 비밀기록물은 그 내용이 누설되는 경우 국가안전보장에 유해한 결과를 초래할 우려가 있는 국가기밀로써 중요한 자료이며 그 보존 가치가 매우 높다고 할 수 있다(국가기록원 2012, 2). 그러나 비밀기록물을 비전자적인 대장으로 관리를 하게 되면 장기보존과 관리의 어려움이 있으며, 그로 인하여 영구멸실의 우려성이 높고 훼손가능성도 있다. 따라서 행정적·증거적·역사적 가치를 지닌 비밀기록물에 대하여 체계적인 통합관리 체계와 효율적인 서비스 체계를 설계함으로써 중요한 비밀기록물에 대한 관리 대

책을 마련하고, 접근도를 높일 필요성이 제기되었다. 손쉬운 접근 및 활용이 되지 못하고 있던 비밀기록물에 대하여 효율적인 접근과 활용 및 체계적인 표준관리를 위한 기반을 마련함으로써 최종적으로는 공공기관의 기록물관리 및 비밀기록관리 환경을 개선하는 것에서 그 필요성을 찾을 수 있을 것이다.

2) 정보공개청구 · 설문조사 분석

논문의 필요성을 검증하기 위하여 비밀기록관리시스템이 기구축 또는 예정인 국가기록원, 국정원, 통일부에 2016년 12월 정보공개를 청구하였고 부산광역시 · 구 · 군 자치단체 기록물관리담당자들을 대상으로 2017년 4월 17일부터 4월 19일까지 전자문서생산시스템(온나라시스템)의 메신저와 E-메일을 통해 설문조사를 실시하였다.

먼저, 국가기록원, 국정원, 통일부에서는 비밀기록관리시스템이 기구축 되어있는 기관으로 조달청 나라장터(www.g2b.go.kr)에서 구축관련 사업이 공개되어 있는 상태이다. 이 내용을 토대로 12월 1일 정보공개를 청구하였다.[4] 국정원과 통일부에서는 공공기관의 정보공개에 관한 법률 제9조 1항 2호에 따라 정보공개청구 답변을 비공개 하였다.[5] 하지만 통일부 담당자와 전화통화에서 별도의 보안이 강화(공개키 암호화 방식)된 시스템을 별도 구축 하여 비밀을 관리하고 있는 것으로 나타났다. 마지막으로 국가기록원 대통령기록관에서는 시스템 구성도, 매뉴얼에 대해서도 역시 정보공개법 제9조 1항 2호에 따라 비공개하였고 구축 당시 공고문은 공개하였다. 대통

4) 정보공개청구접수번호 : 비공개(국정원), 3789602(통일부), 3789603(국가기록원), 정보공개청구내용 : "조달청 나라장터 공고를 보니 비밀기록물관리시스템을 구축 또는 고도화 작업을 하였던것으로 나타납니다. 구축 당시 공고문과 시스템 구성도, 메뉴얼을 정보공개청구 합니다."

5) 공공기관의 정보공개에 관한 법률 제9조 1항 2호 : "국가안전보장 · 국방 · 통일 · 외교관계 등에 관한 사항으로서 공개될 경우 국가의 중대한 이익을 현저히 해칠 우려가 있다고 인정되는 정보"

령기록관리시스템인 PAMS에서 비밀기록관리시스템을 분리하여 구축하는 내용이었다.

대통령기록물관리시스템과 비밀기록물 분리구축의 목적을 아래와 같이 정리하였다.

○ 대통령기록관에서는 대통령기록물 생산기관에서 생산된 기록물을 이관받아 영구 보존·관리하기 위해 대통령기록물관리시스템(PAMS*)을 구축·운영('08.05.20~)하고 있음 * PAMS(Presidential Archives Management System) : 대통령기록물을 전자적으로 관리하기 위한 대통령기록관의 대통령기록물관리시스템 ○ 대통령기록물관리시스템은 일반기록물 영역과 지정·비밀기록물 영역으로 분리·운영하고 있으나, – '15년 「보안업무규정」이 전부개정되어 비밀기록물은 생산단계부터 일반기록물과 분리하여 보존·관리하여야 하며, – 전자적으로 생산하기 위해서는 '전자적 비밀처리규격'을 적용한 '비밀관리시스템'을 통해서만 생산·관리하도록 환경이 변화됨 ※「보안업무규정(대통령령 제26140호, 2015.03.11.)」 제21조 "비밀의 전자적 관리" 항목 신설 ○ 이에 지정기록물과 비밀기록물을 통합 관리하고 있는 대통령지정·비밀PAMS를 물리적으로도 완전 분리하여 보존·관리할 필요가 있음 ○ 이와 함께, 재난·재해 등 유사시 대책으로 대통령비밀기록물의 재난복구시스템 등 이중화시스템도 동시에 구축하여야 함

또한 비밀기록관리프로세스 등 정밀 분석을 통해 비밀PAMS를 설계하고 시스템 구축에 필요한 H/W, 상용 S/W 등 신규 장비를 일체 도입하여 구축하는 것으로 나타났다.

다음, 공공기관 기록물전문요원을 대상으로 한 설문조사를 분석한 결과이다. 부산광역시 시·군·구 기록물전문요원 20명과 자치단체 기록물전문요원 10명 총 30명을 대상으로 2017년 4월 17일부터 19일, 3일간 17명에게서 조사답변을 받았다.

〈표 2〉 설문조사 결과 1

연번	질문내용	매우 그렇다	그렇다	보통이다	아니다	매우 아니다
1	현재공공기관에서 이루어지고 있는 비밀기록물관리가 잘 이루어지고 있다고 생각하십니까?	–	5	6	9	–
2	귀하의 기관에서는 비밀기록물의 특성을 살려 보존 관리되고 있다고 생각하십니까?	–	3	7	7	–
3	현재 공공기관에서 이루어지고 있는 비밀기록물관리가 비전자종이대장으로 관리되고 있다면 효율적이라고 생각하십니까?	–	1	5	10	1
4	기관에서 비밀기록물을 기록관리시스템으로 관리한다면 효율적이라고 판단되십니까?	–	10	6	1	–
5	일반기록물과 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 기존 일반기록물을 관리하는 표준기록관리시스템에 비밀기록관리 기능을 탑재하는 것이 옳다고 생각하십니까?	–	6	3	8	–
6	일반기록물과는 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 보안을 강화한 별도의 시스템을 만들어 표준기록관리시스템과 연동하는게 옳다고 생각하십니까?	–	2	6	8	1
7	일반기록물과는 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 보안을 강화한 별도의 시스템을 만들어 별도로 운영하는 것이 옳다고 생각하십니까?	–	7	5	4	1
8	비밀기록관리시스템을 구축하여 운영할 때 필요한 메타데이터는 표준기록관리시스템 일반기록물과 동일하게 구현하면 되겠습니까?	1	3	2	11	–
9	비밀기록관리시스템을 구축하여 운영할 때 필요한 메타데이터는 별도로 비밀기록물의 특성을 살려 구현하면 되겠습니까?	–	14	3	–	–

설문조사 응답자들의 통계사항이다. 여성 10명, 남성 7명이었고 30대는 11명, 40대는 6명이었다. 기록물전문요원의 전공으로는 기록학 13명, 역사학 2명, 문헌정보 2명이 있었고 경력은 4년 이상 8년 미만이 14명, 2년 이상 4년 미만은 3명으로 나타났다. 그리고 답변한 기관 모두 비밀기록물을 비전자종이 대장으로 관리하고 있었다.

〈표 3〉 설문조사 결과 2

	비밀기록물이 비전자종이대장으로 관리될 때 장단점은 무엇이라고 생각하십니까?	비밀기록물이 전자시스템으로 관리될 때 장단점은 무엇이라고 생각하십니까?
장점	비용절감, 관리주체명확, 보안관리가능	체계적 관리, 표준관리 가능, 등록용이, 연속성증대, 효율성증대, 편리성 증대 등
단점	관리효율성낮음, 인수인계어려움, 손실위험, 연속성낮음, 종이대장누락	보안위험, 예산발생, 시스템 오류

질 : 비밀기록관리시스템을 구축한다면 가장 중요하게 관리되어야 기능은 무엇이라고 생각합니까?	
① 국가기록원 기록물생산현황보고 대비 비밀의 데이터 생산·재분류 현황 등록 기능	4
② 비밀의 접수에 대한 인수·검수·반려 기능	2
③ 비밀기록물 열람·대출·복사 기능	2
④ 비밀의 평가·이관 및 공개재분류 관리 기능	3
⑤ 비밀해제기록물 유형처리 관리 기능	2
⑥ 비밀 검색 기능	1
⑦ 보안감사대비 비밀관리대장 출력 및 저장 요청 기능	1
⑧ 비밀해제기록물 유형별 데이터 열람 기능	1
질 : 비밀기록관리시스템 개발 요구사항에 가장 중요한 내용은 무엇이라고 생각합니까?	
① 시스템보안(암호화)	8
② 비인가자에 대한 접근 금지	4
③ 문서외에 특정파일포맷암호화 구현	2
④ Print Screen, Capture 프로그램 등을 통한 화면캡쳐 방지	1
⑤ 암호화된 문서의 출력 시 워터마크/추적정보 삽입	1
⑥ 암호화된 이미지 데이터의 열람을 위한 전용 뷰어	1

공공기관에서 근무하고 있는 기록물전문요원들은 대부분 비밀기록물관리가 관리가 어렵고 비전자종이 대장으로 관리하는 것이 비효율적이라고 답변하였다. 대신 전자 환경의 기록관리시스템으로 관리하게 된다면 효율적이라고 답변하였고 보유한 비밀기록물의 상용관리와 활용을 위한 비밀취급인가를 받은 이용자들이 일반기록물관리시스템과는 별도로 보안이 강화된 시스템을 별도로 구축하기를 원했다. 별도로 구축된 시스템을 기반으로 비밀기록물의 특화된 기능을 탑재하고 비밀기록물의 특성을 살린 메타데이터를 데이터베이스로 완성하여 관리해야한다고 응답하였다. 기

록물관리전문요원들은 비밀기록물의 비전자종이 대장으로 관리될 때 장점으로는 비용절감, 관리주체 명확, 보안관리 가능 등을 답했고 단점으로는 관리효율성이 낮고, 인수인계어려움, 손실위험, 연속성이 떨어진다고 답했다. 비밀기록물이 전자시스템으로 관리될 때 등록용이, 연속성증대, 효율성증대, 편리성 증대, 체계적 관리를 장점으로 꼽았으며 보안위험, 예산발생, 시스템 오류 등을 단점으로 답했다. 다음으로 비밀기록관리시스템을 구축의 기능으로는 비밀 데이터 생산·재분류 현황 등록, 비밀 접수에 대한 인수검수반려기능, 비밀기록물 열람·대출·복사 기능, 비밀의 평가·이관 및 공개재분류 기능, 비밀해제기록물 유형별 데이터 열람 기능을 관리하도록 하였다. 비밀기록관리시스템 개발 요구사항에 필요한 내용은 시스템보안(암호화), 비인가자에 대한 접근 금지, 문서 외에 특정파일포맷암호화 구현, 화면캡쳐 방지, 암호화된 문서의 출력 시 워터마크/추적정보 삽입, 암호화된 이미지 데이터의 열람을 위한 전용뷰어기능을 중요하게 생각하였다.

정보공개청구 내용과 설문조사결과를 종합해본 결과 비밀기록관리시스템의 구축은 기관의 보안담당자와 기록관의 비밀기록물 전담 관리요원과 각 부서의 비밀취급인가자들이 비밀기록의 관리와 활용에 대해 효율적으로 하는 것을 목표로 하고 있는 것을 알 수 있다. 이를 위하여 시스템 설계는 기록관리 국제표준과 기록관리시스템 표준모델[6]을 통해 모든 유형의 비밀의 관리·활용을 위한 시스템적인 기반 구축 후 기 구축된 기반을 토대로 네트워크 보안 기능 확장, 그리고 시스템의 보안 활용 및 시스템을 통한 비밀관리의 완성을 이룬다는 추진과제를 세웠다. 시스템에 접근하기 위한 메타데이터는 기록관리 메타데이터 국제표준을 통해 비밀기록에 특화된 데이터로 설계하고 시스템의 활용으로는 비밀관리기록부 정리·출력을 통해 기관의 자산으로 활용한다는 추진과제를 세우게 되었다.

6) ISO15489, OAIS 참조모형, DoD5015.2 등.

이와 같은 추진 목표 달성을 위하여 상용 CMS[7]기법을 적용하여 공공기관 내 시스템 운영환경을 고려한 최적화 시스템을 개발하고 향후 지속적으로 생산되는 비밀기록물까지 수용할 수 있는 기반을 구축하고, 비밀기록물에 대한 '생산－활용－관리－보존－폐기'의 Life Cycle을 완성한다는 추진 전략을 수립하고 적용하였다.

4. 비밀기록물 관리를 위한 시스템 설계

1) 시스템 구성 및 기능

정보공개청구와 설문조사의 결과를 토대로 비밀기록물을 관리하는 시스템을 설계하기 위한 고려사항으로 비밀문서와 비밀취급인가자가 네트워크 보안을 통해 시스템에 접근하여 데이터를 입력하고 활용을 위한 "비밀기록" 관리, 다량의 데이터를 보존하고 관리할 수 있는 기능을 운영하여야 한다는 점이었다. 이러한 고려 사항을 반영한 시스템 구성 환경은 정보공개청구결과 및 기록관리국제표준 등을 참고하여 〈표 4〉로 만들었다. 〈표 4〉의 하드웨어 구성 환경을 살펴보면 시스템을 운영하는 SBC서버 1식과 DB를 관리하기 위한 DB서버 1식, 그리고 DB를 저장하기 위한 스토리지 1식이 필요하다. 그리고 시스템 소프트웨어 구성 환경을 살펴보면 기본적으로 운영체계 및 DBMS 1식이 필요하고 클라이언트의 요청을 받아 처리하고 그 결과를 웹 클라이언트에게 응답하기 위해 Web Server와 웹 서버에서 넘어온 동적인 페이지를 처리하여 웹 서버로 돌려주는 Was Server도 1식이 필요하다. 리포팅툴 1식은 시스템에서 추출한 비밀기록관리부의 값을 추출해서 그 값을 표나 그래프 등으로 보고서양식으로 출력해 주는 도구이며 문서보

7) "E-비즈니스에 포함되는 모든 콘텐츠를 생성, 보관, 관리하는 일련의 작업(Task)과 과정(Process)을 일컫고 기관 내에 존재하는 다양한 포맷의 콘텐츠인 문서, 이미지, 동영상, 소리 등을 제작, 출판, 관리하는 솔루션으로써, 보통 콘텐츠를 생성, 출판, 배포, 보관 등으로 정리되는 콘텐츠 라이프 스타일 전체를 관리하는 것을 말한다."(한경 경제용어사전)

안은 비밀문서의 보안을 위해 1식이 필요하다. SSO Agent는 직원과 행정포털과 비밀기록관리시스템을 연계해주는 프로그램이다.

다음과 같은 시스템 환경을 기반으로 비밀기록물의 체계적인 관리와 장기보존이 가능하며, 이용자의 접근 및 활용이 가능하도록 시스템을 구성하기 위해서는 명확한 시스템 구성 원칙을 수립할 필요성이 제기되었고, 이러한 필요성에 따른 시스템 구성 원칙은 다음과 같다.

첫째, 최신 전자 기반의 정보기술을 반영할 수 있어야 한다. 이는 전자기반의 편리한 관리와 이용기반을 설계·구축한다는 원칙으로 비밀기록물의 생산·관리·활용에 있어서 체계적이면서도 효율적인 Work Flow를 반영할 수 있어야 한다는 것을 의미한다.

둘째, 일반기록물의 단위과제와 효과적인 연계와 관리가 가능하도록 하여야 한다. 이는 문서를 관리함에 있어서 기록물철의 특성을 반영할 수 있도록 지방기능분류시스템(BRM)과 연계 되어있어야 한다는 점도 포함하고 있다.

〈표 4〉 시스템 구성 환경

구분		내용
H/W	업무 서버 (SBC[8])	▶ CPU : SMP 기반의 표준 개방형 운영체제, Network Switch, SAN Switch와 통합 운영할 수 있는 서버구성(LAN 및 SAN 가상화 기능 제공 가능) - Clok Speed : 서버별 최상위 - Processor(CPU) 수 : 2 CPU 8 Core 이상 제공 - Processor(CPU) 확장성 : 4개 이상 확장 가능, 최대 확장 시 8프로세서, 32코어 이상까지 장착 가능 ▶ 메모리- 32GB 이상 제공, Dual DRAM Chip 장애 복구 기능 ▶ 내장 디스크 : 300GB 10K RPM SAS 디스크 2개 이상 ▶ I/O 인터페이스- 10Gbps Ethernet : 8port 이상 등
	DB서버	▶ CPU : Six-Core Intel Xeon 5600계열 Processor 2개 이상 제공, CPU Clock 2.66GHz 이상, L3 Cache 12MB 이상 제공, Processor(CPU) 수 : 2 CPU 12 Core 이상 제공 ▶ 메모리 32GB 이상 메모리 제공 등 ▶ 시스템관리 : Smart Start CD,, Insight Control, Onboard, Administrator, Insight Dynamics 제공
	스토리지	▶ 디스크 용량 500GB × 20EA(10TB) ▶ 캐쉬 16GB 이상 제공, SSD를 이용하여 Read/Write 캐쉬를 최대 0.5TB이상 확장기능지원, 전원 장애 발생 시 캐시데이터를 RAID로 보호된 디스크로 자동저장 기능 제공 ▶ 서버 접속용으로 FC, FCoE, iSCSI 혼합 지원 ▶ 8G FC 16Port 이상,10G FCoE 4Port 이상,1/10G ISCSI 8/4Port 이상 지원 ▶ 디스크 접속용으로 6G SAS 4Port 이상 제공 등

S/W	운영체제	▶ Windows 서버 2012 이상 제공
	DBMS	▶ Oracle
	WAS	▶ J233 1.2 이상, Servlet 2.2 이상, JSP 1.1 이상 등
	WEB	▶ HTP 1.1 이상, Multi-thread, process지원 등
	개발언어	▶ JAVA
	리포팅툴	▶ 워드프로세서 수준의 강력한 표 편집기능 및 무한 Undo/Redo 등 ▶ WSDL/SOAP/XML을 기반으로 하는 웹서비스 지원 기능 ▶ 행가변/열가변 보고서, Cross-tab의 통계, 라벨문서 출력 지원 ▶ HWP, EXCEL, Word 등 외부 파일의 서식 Import 기능 ▶ Server-Side 원격 인쇄 및 Export 기능 ▶ 갑지/을지 지원 - 혼합된 용지 A3, A4, B4 종횡 혼합 사용가능 ▶ 다양한 출력 포맷으로 Export 기능(hwp(97이상), ppt, doc, xls, pdf, txt, bmp, mrr, jpg, tif 등) ▶ HWP, Excel등 외부파일의 서식 Import 기능
	문서보안	▶ 문서 전 유통구간을 암호화하여 외부유출 금지, 암호화 지원, 출력 시 스풀파일이나 가상프린터 드라이브를 이용한 파일의 외부유출방지 ▶ 전자문서, 비전자문서 등 모두조회 및 제어가 가능(전자문서의 경우 내용검색 기능 제공) ▶ 문서, 사용자, 기간 및 조건별 문서사용(조회, 출력 등)에 대한 이력관리 기능 제공 ▶ 공인된 국내표준 암호 알고리즘 사용(공공기관용 암호화 제품 등록 솔루션), 국가정보원 암호화 검증필 제품
	검색엔진	▶ 분야별 검색 기능, 검색 설정 기능 제공, 전자문서파일 본문 내용 검색 기능 ▶ HWP, PDF, MS-Office 제품군 등 全文 검색 및 이미지 검색 기능 제공 ▶ 한글, 영어, 일어, 중국어 등 형태소분석기를 보유한 제품 ▶ 확장성 및 유연성을 위한 JAVA 기반 검색엔진 ▶ UNIX 계열의 운영체제에 설치 가능 ▶ GS 인증 제품
	SSO Agent	▶ 새올행정시스템과 비밀기록관리시스템의 SSO구현용
	백 신	▶ Virus확산 및 유입차단기능, 인터넷 미연결 구간에서 실시간 업데이트 ▶ Virus 확산 및 유입차단 기능 ▶ 실행압축 파일에 대한 검사 기능 ▶ 업로드/다운로드 Virus 검사기능 ▶ 다수의 바일에 대한 동시 검사 기능 ▶ 엔진 업데이트 중 파일 검사 호출시 서비스 중단 방지기능

셋째, 데이터에 대한 임의적인 활용과 유출을 방지하기 위하여 보안시스템을 설계하여야 한다. 이는 비밀기록물의 특성을 고려하여, 데이터 활용 시 임의적인 출력·저장 방지, 워터마크 삽입, 접근관리 및 감사증적과 같은 적극적인 보호 대책을 강구하여야 하는 것을 말한다.

넷째, 비밀취급인가를 받은 담당자가 쉽게 접근할 수 있도록 정보서비스에 대한 편의성을 제고하여야 한다. 이는 이용자 중심의 인터페이스를 강화

8) 서버 기반 컴퓨팅, 분산된 업무용 개인컴퓨터의 애플리케이션을 중앙서버 한곳에서 관리하는 서버 기반 컴퓨팅(컴퓨터인터넷IT용어대사전)

하며, 효과적인 검색 · 활용이 가능하도록 시스템이 구성되어야 하는 것을 말한다. 이러한 시스템 구성 원칙은 하나의 정보시스템을 설계 · 구축함에 있어서 적용할 수 있는 일반적인 시스템 구성 원칙이 될 수 있다고 판단된다.

(1) 메뉴구성과 세부기능

〈표 5〉 시스템 메뉴구성

구분	영역	메뉴 내용	
시스템 메뉴구성	관리자	▶ 비밀관리	→ 비밀의 데이터 생산·재분류·삭제 기능
			→ 비밀의 접수에 대한 인수·검수·반려 기능
			→ 비밀의 열람·대출·복사 기능
			→ 비밀의 평가·이관 및 공개재분류 관리 기능
		▶ 비밀해제기록물 유형처리 관리 기능(Ⅰ, Ⅱ, Ⅲ[9])	
		▶ 서고 관리 및 이용 통계 산출 기능	
		▶ 이용자 페이지 관리 기능	
		▶ 보안 및 활용(출력 및 저장) 요청자료에 대한 확인 기능	
		▶ 시스템 환경 및 프로세스 관리 기능	
		▶ 데이터의 임의적인 유출 방지 기능	
	이용자	▶ Site Map 구성	
		▶ SSO(Single Sign On)를 통한 단일 접속/인증	
		▶ 기본검색/상세검색 기능	
		▶ 보안감사대비 비밀관리대장 출력 및 저장 요청 기능	
		▶ 비밀해제기록물 유형별 데이터 열람 기능	

전자 환경에서의 비밀기록물의 관리 · 활용을 위하여 관리자와 이용자 메뉴를 별도로 개발하여야 한다는 전제하에, 관리자 메뉴에서는 비밀 생산/재분류/인수/검수/반려 기능이 포함되어야 하며, 이용자 메뉴에서는 데이터의 편리한 검색 · 활용을 위한 인터페이스를 구성하고, 시스템 이용 간 시스템 부하 및 동시 접속자수를 고려한 시스템을 설계하여야 한다는 개발 요구사항을 도출 시켰다. ISO 15489가 기록관리와 기록관리 프로그램 마련 절차 표준에 따라 설계하고 기록관리시스템을 설계 시, OAIS Reference Model[10]를 참고하여 DoD

9) (유형1) 일반문서로 재분류한 경우, (유형2) 예고문에 의하여 비밀 보호기간이 만료된 경우, (유형3) 생산 후 30년이 경과한 경우

5015.2[11]에 따라 파일플랜을 실행하고, 기록관리스케쥴을 계획하고 메뉴를 설계하였다. 상세한 내용은 〈표 5〉와 같다. 〈표 5〉에서는 관리자메뉴와 이용자메뉴를 구분하여 설계하였는데 관리자메뉴에서는 시스템을 종합 관리할 수 있도록 설계하였고 이용자메뉴에서는 시스템을 활용할 수 있도록하였다. 설계·구축된 시스템에 비밀기록을 위한 시스템보안에 대한 내용은 설문조사에 따라 일반기록물관리시스템보다 강력한 보안 시스템이 요구된다. 설문조사에서는 보안을 강화한 별도의 시스템을 만들어 별도로 운영하는 것에 의견이 많아 이에 따라 설계하였다. 시스템 보안 고도화 요구사항은 〈표 6〉과 같으며 시스템 보안에 대한 보다 자세한 사항은 다음에서 구체적으로 살펴보도록 한다.

(2) 개발 요구사항 분석

〈표 6〉 보안 시스템 모듈

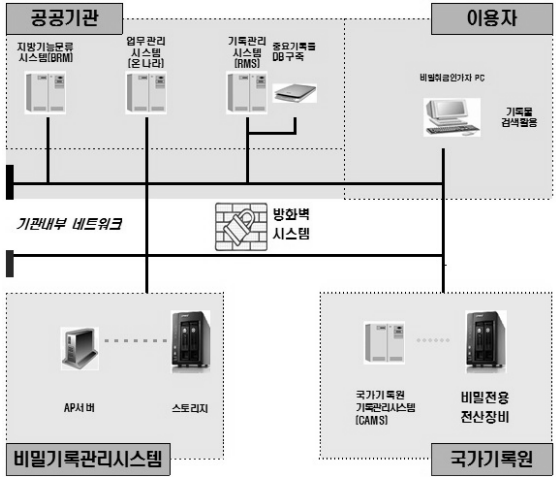
구분	세부 기능
Secure Node	· 데이터 암호화 · 보안프로그램 비인가자에 대한 접근 금지
Secure Document	· 문서(.hwp/.doc/.ppt 등) 외에 특정 파일 포맷(.jpg/.opt)에 대한 암호화 구현
Secure Web	· Print Screen, Capture 프로그램 등을 통한 화면 캡쳐 방지
Secure Print	· 암호화된 문서의 출력 시 워터마크/추적정보 삽입
Secure Image Viewer	· 암호화된 이미지 데이터의 열람을 위한 전용 뷰어

10) ISO 14721:2003으로 시간적·기술적 변화에 상관없이 모든 종류의 디지털 객체들을 장기보존할 수 있고, 또 한 계속적으로 디지털 객체에 접근과 이용을 허용할 수 있는 시스템 구성의 가장 기본이 되는 필수요소들을 개념화하고 표준화하기 위한 목적으로 설계. 즉, 아카이브시스템이 이루어지는 환경과 시스템이 구성되는데 필요한 정보생산자와 정보소비자를 정의하고, 아카이브시스템을 구성하는 엔티티 기능을 정의하고, 서로 간의 상호관계, 디지털 오브젝이 시스템에 접수되고 프로세스되고 아카이브에 저장되어지고 소비자에게 배급되어지는 단계를 정의·설명해주고, 아카이빙시스템이 구성되어지는 과정을 표준화된 개념과 프로세스로 설명(한국기록관리협회 2009, 138).

11) 미국 국방부에서 부서 내의 여러 기관에서 일괄적인 문서관리를 위한 연구프로젝트, 체계적인 문서관리는 동일기관에서 저장매체에 상관없이 문서를 관리할 수 있어야 하고, 시스템에서 문서를 캡쳐하고, 문서의 진본성과 신뢰성을 보장할 수 있도록 시스템에서 자동적으로 실행하고, 전자문서의 변경이나 폐기를 예방할 수 있고, 기존의 레가시 문서와 현용문서뿐 아니라 앞으로 생산될 문서도 잘 관리될 수 있는 시스템을 규정(한국기록관리협회 2009, 203-204).

시스템 메뉴와 세부기능을 분석하여 시스템 구축에 대한 개념을 정립할 수 있었다. 이를 통하여 실제 시스템 구성을 위한 각 항목별 구체적인 요소를 도출할 수 있었다. 각 부분별 요소를 정의함에 있어서 최우선적으로 고려된 사항은 관리자 영역에서는 활용 편의성보다는 체계적인 데이터 관리를 위한 기술적인 측면을 우선 고려하였고, 이용자 영역에서는 활용의 편의성을 최우선적으로 고려하였다. 분석된 개발 요구사항을 바탕으로 기본적인 시스템 구성도는 〈그림 1〉과 같다.

〈그림 1〉 시스템 구성도



기관에서 비밀취급인가를 받은 사용자들은 비밀기록물 생성 및 보존 그리고 국가기록원의 전송을 위하여 적용 가능한 네트워크 보안기술을 적용한 문서트래킹시스템의 고도화 시스템이다(전자기록물의 이해 2009, 176). 데이터베이스로 관리되는 문서를 네트워크를 통해 유통시킬 경우 불법적인 침입자가 네트워크에 침입하여 각종 보안위협을 감행할 수 있다. 따라서 방화벽[12] 보안응용기술을 활용하여 네트워크상 보안을 강화하도록 한다(조

은글터 2009, 138) 다음은 시스템 메뉴 및 활용 개념도는 〈그림 2〉와 같다. 비밀기록물에 대한 시스템 등록과 활용을 위해서는 관리자는 종이원본은 이중캐비닛 그리고 전자파일원본은 SBC스토리지에 분리등록을 한다. 그리고 관리자 페이지의 등록페이지를 통하여 시스템 등록을 하게 된다. 이렇게 등록된 데이터는 이용자가 검색을 통하여 비밀 해제 기록 유형(국가기록원 2012, 15)별로 활용을 할 수 있게 된다.[13]

2) 시스템 보안

비밀기록물은 진본성 · 신뢰성 · 무결성 · 이용가능성을 유지해야 한다. 이를 위해서는 비밀기록물을 생산하여 등록하고 관리하며 활용하는 과정에서 시스템 측면과 보안측면에서 면밀한 주의가 요구 된다. 비밀기록물의 메타데이터와 내용이 시스템에 입력이 되면 제3자에게 노출되는 것을 방지하기 위하여 적법한 사용자에게만 기록물을 개방하도록 하는 기술을 사용하여야 한다. 비밀기록물[14]과 대외비기록물[15]은 그 내용이 노출되지 않도록 비밀로 지정하여 별도로 관리되어야 한다(국가기록원 2012, 9). 이를 위해 전산시스템에 관리를 하게 되면 보안의 중요성이 커지게 된다. 전산환경에서 보안의 중요성이 점점 커지는 이유가 시스템에 외부침입자의 공격 형태가

12) "기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막거나 허가하고 인증된 트래픽만 허용하는 적극적인 방어대책이다."

13) "비밀기록관리시스템에서 관리자인 기관보안담당자 및 비밀기록물 전담 관리요원은 문서 내용에 따라 메타데이터 입력을 하고 BRM 단위과제에 맞게 분류하고 바코드를 각 문서에 부착하여 데이터베이스에 저장하고, 저장한 후 종이문서는 파일별로 이중캐비닛이나 전용서고로 옮겨 순서대로 보관한다. 부서의 비밀취급인가자의 이용하고자 하면 문서를 파일별로 찾아서 바코드로 검색하고, 이 바코드에 따라 데이터베이스에서 찾아서 서고에 방문하여 종이 원본을 찾아서 이용자에게 제공한다. 전자문서는 SBC스토리지로 옮겨져 유형에 따라 부서장의 승인을 받게 되면 열람을 하게 된다."

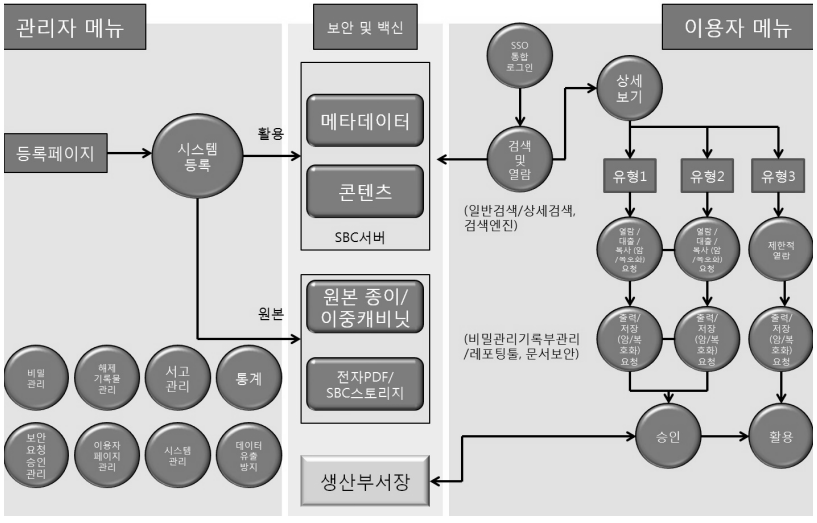
14) "그 내용이 누설되는 경우 국가 안전보장에 유해한 결과를 초래할 우려가 있는 국가기밀로서 「보안업무규정」에 의하여 비밀로 분류된 것"을 말함

15) "비밀 이외에 직무수행상 특별히 보호를 요하는 사항으로 「보안업무규정 시행규칙」에 의하여 대외비로 분류된 것"을 말함

점차 고도화, 지능화, 복잡화가 되어가기 때문에 기관 전산환경을 보호하기 위함이다. 즉, 오늘날의 환경에서는 다양한 정보 보호 시스템을 유기적으로 연관시켜 손쉽게 관리할 수 있는 보안 기술이 요구된다. 그러기 위해서는 지정/비밀영역의 프로세스 현황 및 전산 환경을 면밀히 분석하여 안정성, 보안성, 무결성 및 진본성 등을 보장하는 기술이 필요하고 국정원의 「보안업무규정」상의 전자적 비밀처리규격을 준수한 데이터를 안전하게 이전하고 이를 검증할 수 있는 기술도 필요하다. 마지막으로 비밀원본 및 재난복구 시스템에 대해서도 설계·구축되어야 할 것이다.

(1) 시스템 이중 암호화 설계

〈그림 2〉 시스템 메뉴 및 활용 개념도



시스템의 메인서버인 SBC서버에 데이터베이스 암호화 및 웹 트래픽 2중 암호화 구축하여, 비밀문서데이터, 사용자계정 등 중요 정보를 암호화 한

다. 암호화시스템은 응용프로그램의 수정 없이 데이터 암호화를 적용하여, GUI[16]를 통해 One Click으로 암호화를 설정하고 해제한다. 그리고 각 사용자별 권한에 따라 암호화 데이터에 대한 접근제어를 실시하며, 각 사용자별 권한에 따라 암호화 데이터에 대한 접근제어를 실시하며, 사용자 권한 관리 기능을 제공할 수 있다(이종열 2005).

· 접근제어

암호화된 칼럼에 대하여 출발지 IP, 응용프로그램, 데이터베이스 계정 별 세분화된 보안정책 설정을 통하여 비인가 접근에 대하여 차단한다.

· 암복호화 권한설정

암복호화 대상 컬럼을 선택하고 각 사용자에게 권한을 부여하거나, 사용자를 선택하고 각 사용자가 컬럼에 대하여 암복화 권한을 부여한다.

· 사용자 관리

보안 관리자가 암호화 컬럼에 대하여 접근 권한을 가진 사용자의 계정 및 패스워드를 관리하여 데이터 유출을 방지한다.

· 웹 트래픽 암호화시스템

웹 트래픽 암호화 시스템은 암복호화 대상 웹 페이지 원래 소스 분량을 기준으로 3% 미만의 응용프로그램의 수정만으로 간편하게 설치하고 사용한다. 또한 최적의 클라이언트 모듈을 제공으로 별도의 설정 없이 자동으로 설치되고 구동된다. 웹 세션 송수신 데이터를 강력한 암호화 알고리즘으로 암호화 하여 데이터를 보호한다. 또한 일회용 세션키를 사용하여 안전성을 더욱 강화한다.

16) "Graphical User Interface, 사용자가 컴퓨터와 정보를 교환할 때, 그래픽을 통해 작업할 수 있는 환경"을 말한다.

⑵ 데이터 보호

암호화 적용 및 복구 기능을 제공하여 〈그림 3〉과 같이 데이터를 안전하게 보호한다.

· 이용자가 안정된 접속권을 가진 것인지를 확인하기 위하여, 전자서명을 위한 공개키(Public Key Infrastructure : PKI)를 사용하여 해쉬(Hash) 알고리즘을 사용한다.

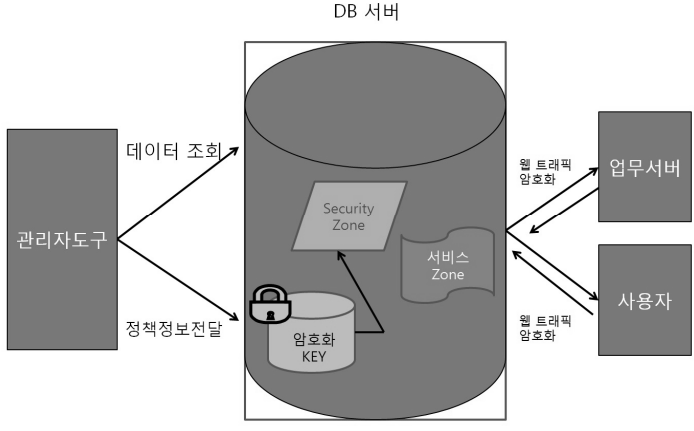
· 이용자의 세션에 대한 권한을 확인하기 위하여, 사용자의 등급에 따라 엑세스 권한 설정 및 정보에 대한 접근 범위를 설정한다.

· 시스템의 보안을 위하여, 비밀기록의 암호화 및 보안 통신을 사용한다.

· 비밀기록데이터의 정확성이 보장되고 통신 및 세션에서의 보안을 위하여 비밀기록의 무결성과 세션의 활성화 중 발생할 수 있는 보안 기능을 설치한다.

· 공개키의 관리를 위하여 공개키는 인증기관이 책임지고 관리하도록 한다.

〈그림 3〉 데이터 보호 구성도



· 비밀기록관리시스템의 접속 기록과 시스템에 저장 기록된 비밀정보에의 접속기록의 감사증적을 위하여 시스템에 접속한 모든 세션에 대한 기록들을 로그 파일로 철저히 관리한다.

· 스토리지와 DB서버에 관리되고 있는 비밀기록물의 무단 반출을 방지하기 위해 요구되는 사항들에는 웹을 통한 캡쳐(Capture)방지, 브라우져(Browser)를 통한 임의적인 출력/ 저장 방지, 마우스 오른쪽 버튼 클릭을 통한 출력/저장/복사 방지, 시스템을 통한 데이터 이용 시 암호화 상태 유지, 임시 저장 폴더에 저장되는 데이터에 대한 출력/저장/복사 방지를 한다.

요구사항 분석 결과에 따라 보안정책을 수립하면서 가장 우선적으로 고려한 사항이 이용자의 활용 편의성을 저하시키지 않으면서, 동시에 데이터의 안전한 활용을 도모하는 것이었으나, 이 둘을 동시에 만족시키기에는 기술적인 어려움과 프로세스 구현의 어려움으로 인하여, 다소의 불편이 야기되더라도 안전한 데이터의 활용에 보다 초점을 두고 보안 정책을 수립하였고, 이를 시스템에 적용하면 되겠다.

3) 시스템 접근(메타데이터)

비밀기록물을 시스템에 등록정보를 입력하고, 이용자의 검색 · 활용을 위하여 접근점(Access Point)역할을 하는 메타데이터[17]를 입력해야 한다.

기록관리시스템에 설계되고 첨가되어지는 메타데이터에 관한 기본적인 원칙과 기술적인 사양으로는 국제표준기구에서 제정하여 발표한 「ISO 23081-1」[18]

17) ""Data about data"라고 말하는데, 원본 소스데이터에 관한 기술(Description)이나 설명으로, 부가적인 2차정보데이타"를 말한다.

18) 두 부분으로 구성되어있는데, part 1은 기록관리 메타데이터에 대한 정의와 필요성 · 역할 · 종류 등을 설명하고 있으며, 이를 어떻게 관리하는지에 대한 내용이 자세하게 설명되어 있다. part2는 개별 기관에서 메타데이터를 개발하려고 할 때, 메타데이터 스키마를 개발하고 실용화 할 수 있는 설명과, 이것을 지체 평가할 수 있는 도구들을 설명하고 있다.

가 가장 기본적인 표준이다.

국제표준기구에서 제정한 DoD5015.2을 참고하여 〈표 7〉을 개발하였다.

메타데이터는 등록을 위한 메타데이터와 검색을 위한 메타데이터로 구분할 수 가 있는데, 시스템 구축을 위한 기록물을 등록할 때 입력하게 되는 메타데이터 정보가 기본적으로 검색을 위한 접근점으로 활용되며 파일 등록 시 시스템을 통하여 자동 생성되는 정보가 추가적으로 검색을 위한 메타데이터 항목으로 활용된다. 메타데이터 세트를 개발할 때 주의해야할 사항들에 대하여 ISO15489에서 설명하고 있듯이 가장 우선해야 할 작업은 기관에서 일하고 있는 직원들의 요구들을 먼저 파악하여야 한다(Kate Cumming 2005, 34).

그리고 이를 기본으로 현재의 문서관리시스템과 주요 업무흐름을 파악한다. 또 이를 기반으로 하여 기관이 직면하고 있는 문제점을 해결해 줄 수 있는 맞춤형 메타데이터 솔루션을 개발한다. 이 때 국제표준들을 시작점으로 하여 참고하여 기관에 적절한 메타데이터 세트를 정하도록 한다. 메타데이터 설계와 실행 시에는 이 메타데이터 세트가 기록관리기능을 통합하도록 한다. 메타데이터의 원정보가 어디서 제출되는지, 누가 작성할 것인지, 어떻게 저장할 것인지에 대해서 파악되어야 한다(Kate Cumming 2005. 35). 이러한 메타데이터를 실행할 때 주의점을 통해 비밀기록관리시스템의 메타데이터를 설계하였다. 비밀기록물철에 관한 메타데이터는 총 30개 항목이며, 이중에서 등록 시 입력하게 되는 메타데이터 항목은 비밀등급, 원본형태 등을 포함한 16개 항목을 입력하게 되며, 등록번호, 관리번호 등의 나머지 9개 항목은 등록 시 시스템을 통하여 자동적으로 부여하게 된다. 비밀기록물건에 관한 메타데이터는 총36개 항목으로 등록시 입력하게 되는 메타데이터 항목은 27개이며, 나머지 9개 항목은 기록물철등록 시와 마찬가지로 시스템을 통하여 자동적으로 부여된다(〈표 8〉 참조).

〈표 7〉 비밀기록물철/비밀기록물건 관련 메타데이터 항목

순번	구분	입력형식	자릿수	비고
1	비밀등급	Code	2	등록 시 입력
2	기록형태	Code	2	
3	기록물철명	Char	100	
4	부제목	Char	200	
5	생산기관	Char	30	
6	생산부서	Char	30	
7	생산년도	YYYY	4	
8	단위과제	Char	30	
9	권호 수	Char	100	
10	기록유형	Code	10	
11	보존기간	Code	2	
12	보호기간	Char	50	
13	재분류유형	Code	2	
14	소장위치	Char	50	
15	서고유형	Code	2	
16	상자번호	Num	10	
17	내용요약	Char	300	
18	직급	Char	20	
19	등록자명	Char	10	
20	등록일자	YYYYMMDD	8	
21	쪽수	Num	4	
22	등록번호	Char	100	시스템 자동부여
23	관리번호	Char	16	
24	분류번호	Code	50	
25	수량	Num	4	
26	수량단위	Code	1	
27	파일명	Char	30	
28	파일형태	Code	2	
29	용량	Char	12	
30	기록물건수	Num	300	

순번	구분	입력형식	자릿수	비고
1	비밀등급	Code	2	등록 시 입력
2	기록형태	Code	2	
3	기록물건명	Char	100	
4	부 제 목	Char	200	
5	사본번호	Num	4	
6	생산부서	Char	30	
7	생산년도	YYYY	4	
8	본문	Char	300	
9	붙임	Char	500	
10	기록유형	Code	10	
11	보존기간	Code	2	
12	보호기간	Char	50	
13	예고문보관	Code	2	
14	장소	Code	2	
15	직급	Char	20	
16	처리담당	Char	10	
17	수발일자	YYYYMMDD	8	
18	발신시행일자	YYYYMMDD	8	
19	쪽수	Num	4	
20	분류체계	Char	50	
21	등급변경	Char	8	
22	파기	CHAR	8	
23	파기확인	Char	300	
24	근거	Code	2	
25	영수증	Char	300	
26	수령자	Char	8	
27	접근범위	Code	2	
28	등록번호	Char	100	시스템 자용부여
29	관리번호	Char	16	
30	분류번호	Code	50	
31	수량	Num	4	
32	수량단위	Code	1	
33	파일명	Char	30	
34	파일형태	Code	2	
35	파일크기	Char	12	
36	생산/접수	Code	2	

이와 같이 시스템에 등록된 기록물에 대하여 안전한 보존 관리를 위한 별도의 스토리지를 확보하여 운영할 필요성이 제기되었고, 이에 따라 스토리지를 구성하기 위한 기능적 요소와 비용적 요소를 고려하였고 기능적 요소에는 운영성, 안정성, 확장성, 백업 운영성, 호환성, 접근 용이성이 고려되었다. 마지막으로 비용적 요소에는 초기 투입 비용, 유지보수 비용, 추가 확장 비용이 고려되었다. 데이터백업은 네트워크를 통한 월 2회 주기적인 백업(Incremental)이 이루어지게 설계하였다.

4) 시스템 활용(열람 및 출력)

부서의 장은 생산한 비밀기록물이 일반문서로 재분류되거나, 예고문에 명시된 비밀 보호기간이 만료된 경우, 또는 생산 후 30년이 지난 겨우 관할 기록관 또는 특수기록관으로 이관하여야 한다. 그리고 기록관 또는 특수기록관의 장은 일반문서로 재분류되거나 비밀보호기간이 만료된 기록물 중 보존기간이 30년 이상인 기록물과 생산 후 30년이 지난 비밀기록물을 관할 영구기록물관리기관으로 이관하여야 한다. 부서의 비밀기록물을 관리하고 있는 자는 관할 기록관 또는 특수기록관으로 이관하기 위하여 비밀관리기록부에 이력기재, 공개여부 분류, 이관목록 작성 등 사전준비를 하여야 한다. 그러기 위해서는 구축된 시스템 소프트웨어 중 리포팅툴(표 5 참고)을 사용하여 입력한 기록물건 메타데이터에 따라 비밀관리기록부를 생성하여 출력 · 보관하는 것이다.

부서의 비밀기록물관리 담당자(이용자)는 관리하던 비밀기록물이 일반문서로 재분류(유형1) '비밀등급'란부터 '사본번호'란까지 2개의 적색선을 긋고 '재분류－등급변경'란에 '일반문서'라고 기재 후 그 밑에 괄호 표시를 한 다음 그 안에 재분류 일자를 기재되도록 한다. '근거'란에는 '예고문' 또는 '직권'이라는 재분류 근거를 기재하고 '수령자'란에는 '기록관(특수기록관)이관', '이관일자' 및 '인계자명'을 기재하여 출력이 되도록 한다.

예고문에 의하여 비밀 보호기간이 만료된 경우(유형 2)인 경우 '비밀등급'란

부터 ‘사본번호’란까지 2개의 적색선을 긋고 ‘재분류-등급변경’란에 ‘비밀해제’라고 기재 후 그 밑에 괄호 표시를 한 다음 그 안에 재분류 일자를 기재되도록 한다. ‘근거’란에는 ‘예고문’이라는 재분류 근거를 기재하고 ‘수령자’란에는 ‘기록관(특수기록관)이관’, ‘이관일자’ 및 ‘인계자명’을 기재하여 출력이 되도록 한다.

생산 후 30년이 지난 비밀기록물(유형 3)은 ‘비밀등급’란부터 ‘사본번호’란까지 2개의 적색선을 긋고 ‘수령자’란에 ‘기록관(특수기록관) 이관’, ‘이관일자’, ‘인계자명’을 기재하여 출력되도록 한다.

시스템의 등록된 메타데이터에 따라 구축된 리포팅툴에 의거 비밀기록물 해제 유형1, 2에 따른 비밀관리기록부 출력의 예는 〈그림 4〉, 〈그림 5〉와 같다.

〈그림 4〉 비밀기록물 해제 유형 1에 따른 출력본 예시

관리 번호	수 발			문서 번호	비밀 등급	형태	건명	사본 번호	예고문
	년월일	발행처	수신처						
1	2012.2.28	000부 총무과	내부 결재	총무과-111호	III급	문서	보안업무 제무주정계획	-	2015.2.28. (끝)

처리 담당	보관 장소	재분류				참조	
		등급 변경	파기	파기 확인	근거	영수증	수령자(인)
홍길동	적계 금고	일반문서 (2015. 4. 1.)			예고문		기록관 이관(2016. 10. 20.) 인계자 : 홍길동

※ 지면 한계상 비밀관리기록부를 두 부분으로 나눔

〈그림 5〉 비밀기록물 해제 유형 2에 따른 출력본 예시

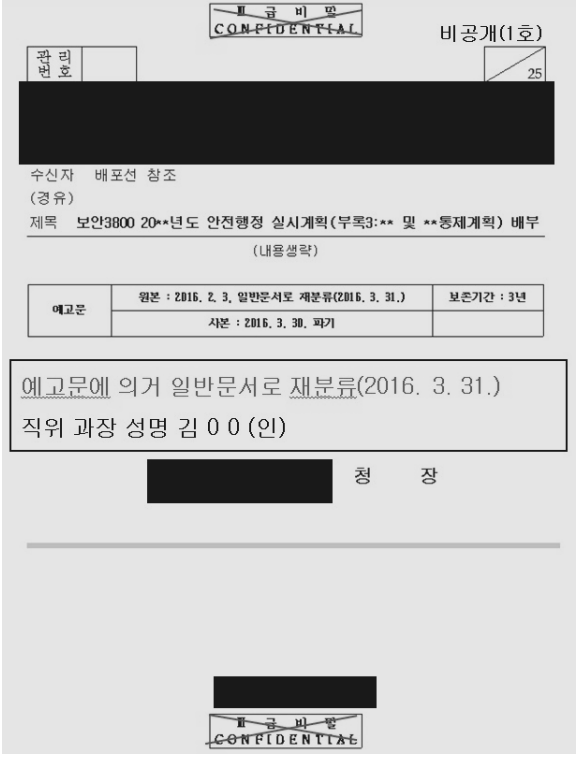
관리 번호	수 발			문서 번호	비밀 등급	형태	건명	사본 번호	예고문
	년월일	발행처	수신처						
1	2012.2.28	000부 총무과	내부 결재	총무과-111호	III급	문서	보안업무 제무주정계획	-	2015.2.28. (끝)

처리 담당	보관 장소	재분류				참조	
		등급 변경	파기	파기 확인	근거	영수증	수령자(인)
홍길동	적계 금고	비밀해제 (2015. 4. 1.)			예고문		기록관 이관(2016. 10. 20.) 인계자 : 홍길동

※ 지면 한계상 비밀관리기록부를 두 부분으로 나눔

또한 이관하기 위한 비밀기록물 원본에도 정리를 하여야 하는 데 비밀등급 표시를 대각선으로 삭제하고, 비밀재분류 근거를 첫 면의 적당한 여백에 기입 후 기명날인을 한다. 첫 페이지 우측 상단 여백에 「공공기관의 정보공개에 관한 법률」에 따른 공개여부를 기재한다. 재분류 표시(표지)는 「보안업무규정 시행규칙」 제22조에 따랐다. 시스템의 등록된 원본은 구축된 리포팅툴에 의거 비밀기록물 원본 정리의 비밀관리기록부 출력의 예는 〈그림 6〉과 같다.

〈그림 6〉 일반문서로 재분류한 비밀 원본의 출력본 예시



5. 결론

비밀기록물관리에 관한 규정이 신설 또는 개정되면서 비밀기록물의 관리의 중요성이 커지게 되었지만 기록관리 현장에서 여전히 비밀기록물의 특성과 가치를 고려한 관리가 이루어지지 않고 있는 실정이다. 또한 비밀기록물의 보관에 있어 비전자 환경의 기록물을 장기 보관하기 위해서는 상당한 노력이 필요하다.

이러한 상황에서 공공기관에서 비밀기록물을 관리하기 위한 시스템 설계는 보안업무 담당자가 바뀌어도 기록관리 표준과 보안규정에 맞게 관리가 가능하고 또한 비전자환경으로 관리하던 비밀기록물을 전자환경에서 처리하여 보다 적은 시간과 비용과 노력을 투입하여, 비밀기록물에 대한 장기보존 대책을 마련 할 수 있다. 이러한 비밀기록물을 관리하기 위한 시스템은 비밀기록물에 대한 관리 활용의 장을 마련하여 기록관리업무에 상당한 효과를 발휘할 수 있을 것으로 확신한다.

이 연구의 비밀기록물을 관리하는 시스템을 설계하기 위해 기 구축된 기관에 정보공개를 청구하였고 공공기관에서 근무하고 있는 기록물전문요원들을 대상으로 비밀기록물 관리에 대한 설문조사를 실시하였다. 이를 근거로 하여 기록관리 국제표준 즉, ISO15489, OAIS 참조모형, DoD5015.2 등에 맞게 시스템을 구성하고 요구사항을 분석하였다. 분석된 요구사항을 바탕으로 한 시스템 설계 등 시스템에 관련된 사항과 시스템의 보안 및 암호화, 메타데이터, 비밀관리기록부 정리 및 출력에 대한 전체적인 구축 과정과 표준 관리에 대하여 살펴보았다.

마지막으로 효율적인 비밀기록물을 관리하기 위해서는 국가비밀의 관리 주체인 국정원과 국가기록물의 관리 주체인 국가기록원과 비밀을 직접 생산하는 공공기관에서 효과적으로 관리할 수 있도록 표준적인 시스템 구축에 관한 합동 연구가 필요하다고 보여진다.

〈참고문헌〉

강구민. 2014.『특수유형기록물관리시스템 구축에 관한 연구』. 중부대학교 대학원 석사학위논문.

국가기록원. 2012.『비밀기록물 재분류 매뉴얼』.

국가기록원. 2016.『비밀기록물 관리(v1.2, NAK/S20 : 2016.)』.

서영관. 1998.『시스템보안기법의 비교 연구』. 목포대학교 경영행정대학원 석사학위논문.

신동헌외 2명. 2009. 시청각(사진/동영상)기록물 관리를 위한 시스템 구축과 운영사례 연구.『기록학연구』, 9, 33-50.

위성현. 2012.『전자메일 기록관리시스템 설계 방안 연구』. 명지대학교 기록정보과학전문대학원 석사학위논문.

이종열. 2005.『보다 안전한 정보화 자원 보호를 위한 DB보안시스템 구축 방안에 관한 연구』. 동국대학교 석사학위논문.

임선화. 2004.「수집기록물관리시스템 모델링」. 명지대학교 기록과학대학원 석사학위논문.

한국기록관리협회. 2009,『전자기록물의 이해』. 서울: 조은글터.

Consultative Committee for Space Data Systems. Reference Model for an Open Archival Information System(OAIS).(2002). CCSDS 650.0-B-1, Blue Book.

John Phillips. (2004). "E-Records Software Selection Guidelines." Proceedings of the ARMA International 49th Annual Conference. Long Beach.

Kate Cumming. (2005). "Metadata Matters." Managing Electronic Records. Ed. by Julie McLeod and Catherine Hare. London : Facet Publishing.

US Department of Defense. DoD5015.2-STD. (1997). Design Criteria Standard for Electronic Records Management Software Applications.

〈부록〉 비밀기록물을 관리하기 위한 시스템 설계 연구 설문지

본 연구는 '비밀기록물을 관리하기 위한 시스템 설계 연구'를 수행을 위해 자료로 활용하고자 작성되었습니다. 설문지에는 전문요원이 비밀기록물을 생산·관리하면서 발생될 수 있는 사항을 간단하게 통계 형태로 작성하였습니다.

귀하께서 답변해 주신 응답내용과 의견은 기관에서 비밀기록물을 관리하는 데 있어서 시스템이 설계되는 데 유용하게 활용될 것입니다.

아울러 본 설문은 무기명으로 실시되며, 귀하의 응답내용 및 조사결과는 통계법 제33조(비밀의 보호)에 의해 비밀이 완전히 보장되며, 연구 이외에 다른 목적으로 사용되지 않을 것입니다.

끝으로 바쁘신 중에도 설문에 응답해주셔서 감사합니다.

2017년 4월 17일

1. 통계를 위한 일반 사항입니다. 해당하는 곳에 ■ 표시해주십시오.

근무기관	ex) ○○구 ○○과	성별	□ 여 □ 남
연령	□ 20대 □ 30대 □ 40대 □ 50대 이상		
전공	□ 역사학 □ 문헌정보학 □ 행정학 □ 기록학 □ 기 타		
업무 경력	□ 2년 미만 □ 2년이상 ~ 4년 미만 □ 4년이상 ~ 6년 미만 □ 6년이상 ~ 8년 미만 □ 8년 이상		

2. 현재 공공기관에서 이루어지고 있는 비밀기록물관리가 잘 이루어지고 있다고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

3. 귀하의 기관에서는 비밀기록물의 특성을 살려 보존 관리되고 있다고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

4. 귀하의 기관에서는 비밀기록물이 생산하여 관리할 때 어떤 방식을 사용하십니까?

① 비전자종이대장 ② 전자시스템 ③ 기타

5. 현재 공공기관에서 이루어지고 있는 비밀기록물관리가 비전자종이대장으로 관리되고 있다면 효율적이라고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

6. 기관에서 비밀기록물을 기록관리시스템으로 관리한다면 효율적이라고 판단되십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

7. 비밀기록물이 비전자종이대장으로 관리될 때 장단점은 무엇이라고 생각하십니까?

장점 :

단점 :

8. 비밀기록물이 전자시스템으로 관리될 때 장단점은 무엇이라고 생각하십니까?

장점 :

단점 :

9. 일반기록물과는 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 기존 일반기록물을 관리하는 표준기록관리시스템에 비밀기록관리 기능을 탑재하는 것이 옳다고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

10. 일반기록물과는 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 보안을 강화한 별도의 시스템을 만들어 표준기록관리시스템과 연동하는게 옳다고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

11. 일반기록물과는 다르게 보안이 중요한 비밀기록물을 전자시스템으로 관리한다면 보안을 강화한 별도의 시스템을 만들어 별도로 운영하는 것이 옳다고 생각하십니까?

① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

12. 비밀기록관리시스템을 구축한다면 가장 중요하게 관리되어야 기능은 무엇이라고 생각합니까?

① 국가기록원 기록물생산현황보고 대비 비밀의 데이터 생산 · 재분류 현황 등록 기능

② 비밀의 접수에 대한 인수 · 검수 · 반려 기능

③ 비밀기록물 열람 · 대출 · 복사 기능

④ 비밀의 평가·이관 및 공개재분류 관리 기능
⑤ 비밀해제기록물 유형처리 관리 기능
⑥ 비밀 검색 기능
⑦ 보안감사대비 비밀관리대장 출력 및 저장 요청 기능
⑧ 비밀해제기록물 유형별 데이터 열람 기능
⑨ 기타

13. 비밀기록관리시스템 개발 요구사항에 가장 중요한 내용은 무엇이라고 생각합니까?
① 시스템보안(암호화)
② 비인가자에 대한 접근 금지
③ 문서외에 특정파일포맷암호화 구현
④ Print Screen, Capture 프로그램 등을 통한 화면캡쳐 방지
⑤ 암호화된 문서의 출력 시 워터마크/추적정보 삽입
⑥ 암호화된 이미지 데이터의 열람을 위한 전용 뷰어

14. 비밀기록관리시스템을 구축하여 운영할 때 필요한 메타데이터는 표준기록관리시스템 일반기록물과 동일하게 구현하면 되겠습니까?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

15. 비밀기록관리시스템을 구축하여 운영할 때 필요한 메타데이터는 별도로 비밀기록물의 특성을 살려 구현하면 되겠습니까?
① 매우 그렇다 ② 그렇다 ③ 보통이다 ④ 아니다 ⑤ 매우 아니다

설문에 응해주셔서 감사합니다.