진본성 확보를 위한 전자기록물 관리방안

Management of Electronic Records to Ensure the Authenticity

송 병 호(Byoungho Song)*

초 록

전통적인 종이기록물은 그대로 보존하여야 진본이 유지된다. 그러나 전자기록물은 포맷과 메타데이터가 수정 변환되어야 하기 때문에 그 변환이 적법한지에 대한 증명과 적법하지 않은 변경은 없었다는 증명이 모두 필요하다. 이를 위해서는 전자기록물을 획득한 시점에서부터 진본임을 확인하고, 보존기간동안 유실을 방지하여야 하며 진본임을 증명할 방법이 있어야 하고 진본이 아님이 판명 났을 때의 사후 대처방안이 마련되어야 한다. 본 논문에서는 전자기록물 진본성의 취약성을 설명하고 필요기능을 파악하였으며 이를 실현할 방안들에 대하여 제안하고 그 결과 전체적인 전자기록물 관리 방안에 대하여 제시하였다.

ABSTRACT

Traditional paper records have to be preserved in the original form to ensure the authenticity. On the other hand, electronic records have to be continuously changed in content itself or metadata to be preserved in long-term period, so the proof of the legality of each change made so far and the proof of the protection against all the illegal changes are the essential, to ensure these requirements, We need some functions including the authentication of original captured records, the protection of records against the loss or forgery, the authentication of preserved records, and the treatment of authentication-failed records. This paper explains the fragility of authenticity for electronic records, identifies the functions needed, suggests the implementation idea, and describes the overall management polity for electronic records to ensure the authenticity.

키워드: 전자기록물, 진본성, 인증, 전자서명, 보존
electronic records, authenticity, authentication, digital signature, preservation

* 상명대학교 소프트웨어학부 교수(bhsong@smu.ac.kr)
논문접수일자 2005년 11월 18일 논문심사일자 2005년 11월 25일 게재확정일자 2005년 12월 7일

1. 서 론

기록물이란 조직체나 개인이 법적 의무를 수행하거나 업무를 처리하는 과정에서 증거 및 정보로서 생산, 접수, 관리하는 문헌을 말한다(ISO 2001). 여기서 문헌이란 '기록된 정보(recorded information)'이다(서혜란 2003). 우리나라는 공문서의 기안, 결재에서부터 수발신 유통까지를 전자적으로 수행하는 정부표준 전자문서시스템이 2000년부터 인증받아 각 기관에서 사용되고 있으며 인터넷 민원처리(G4C)가 가능한 전자정부 서비스가 2002년 하반기부터 개통되면서 이제 세계에서도 가장 앞서서 전자기록물이 업무나 생활의 증거물 및 정보물 역할을 담당하는 본격적인 정보화 사회가 되었다.

정부에서는 전통적인 종이문서 외에 전자기록물이 업무의 대상 또는 산물이 될 수 있음을 법적으로 뒷받침하고 그 이용을 촉진하기 위하여 "사무관리규정"을 개정하고 "전자정부구현을위한행정업무등의전자화촉진에관한법률"(이하 전자정부법)을 제정하였으며 종래의 서명을 전자적으로 대체할 근거 마련을 위하여 "전자서명법"을 제정하고 이렇게 만들어진 전자기록물의 보존관리의 법적 근거 마련을 위하여 "공공기관의기록물관리에관한법률"(이하 기록물법)을 개정하였다. 전자기록물 도입의 제도화는 행정부에서부터 시작하여 법원, 국회, 헌법재판소, 자치단체 등 전 국가기관과 공공기관에 파급되고 있을 뿐 아니라 이제는 민간부문의 상거래도 견적에서 계약, 송장에 이르기까지 전 과정이 전자적으로 수행 가능하게 되었다.

이처럼 지금까지는 정보 제공의 편이성 및 업무의 효율성을 위하여 전자기록물을 도입하였지만 이제는 전자기록물의 증거능력을 확보할 방법이 필요하다. 공공분야는 행정자치부 국가기록원(구 정부기록보존소)의 여러가지 사업 등으로 그 방안을 강구하고 있으며(국가기록원 2005), 민간 거래문서는 산업자원부 한국전자거래진흥원의 공인전자문서보관소 관련 사업 등으로 이루어지고 있다(한국전자거래진흥원 2005). 그러나 아직까지 구체적으로 결론이 나거나 시행 경험이 있는 것은 아니다.

전자기록물의 증거능력을 보장하기 위해서는 진본성을 유지하여야 하는데, 여기에 대하여 기본적인 개념은 정립된 바가 있지만 진본 보존의 효력을 달성하기 위한 필요요소와 이를 실현하기 위한 방법론에 대해서는 지금까지 연구된 바도 부족하며 경험도 없는 것이 현실이다. 수년 후 이에 대한 방안이 구체화되고 안정화되는 시점 이전까지 생산되고 보존될 전자기록물은 진본 인증을 받기에 미흡한 상태로 판명날 수도 있다. 본 연구는 좀더 세부적인 이슈 검토 및 방안 연구를 통하여 이러한 시행착오를 줄이는 것이 목적이다.

본 논문의 구성은 다음과 같다. 2장에서는 전자기록물의 특징이 종래의 종이기록물과 달라서 증거능력을 부여해 주는 진본성과 무결성 특성을 확보하기가 어렵다는 점을 살펴보았다. 3장에서는 전자기록물의 진본 보존 효과를 달성하기 위하여 필요한 기능들을 나열하고 설명하였다. 4장에서는 진본 보존 효과를 실현할 방안들에 대하여 논하였다. 5장에서는 이러한 필요 요소와 실현 방안에 의거하여 전자기록물을 관리하는 체제의 개념을 설명하고 마지막 6장

에서 결론을 맺었다.

2. 전자기록물 진본성 확보의 취약성

기록물관리에 관한 세계표준인 ISO 15489 (Information and Documentation - Records Management)에 따르면 기록물은 다음과 같은 특성을 가져야 한다(ISO 2001).

1. 진본성이 있어야 한다. 취해야 할 모습대로 이고 처리해야 할 사람이 처리하였으며 처리하여야 할 시간에 처리하였음이 증명될 수 있어야 한다.
2. 신뢰성이 있어야 한다. 즉 그 내용이 특정 업무 행위나 사실을 충분하고도 정확하게 표현하였다고 믿을 수 있도록 구성되며, 이에 따라 후속 행위나 업무 처리에 근거로 삼을 수 있어야 한다.
3. 무결성이 있어야 한다. 완전하고 변경되지 않은 내용으로 구성되어야 한다. 인가받지 못한 변경은 방지되어야 한다.
4. 가용성이 있어야 한다. 원하는 기록물에 접근해서 검색하고 정보를 꺼내고 그 내용을 해석할 수 있어야 기록물의 역할을 제대로 한다고 할 것이다. 해석할 수 있다 함은 기록물이 묘사하는 해당 사실이나 업무 행위와 직접 연계되어 파악할 수 있음을 말한다. 또한 개별 기록물이 어떠한 범주에 드는지 상위 대분류 측면에서 빨리 파악할 수 있도록 구성되어야 할 것이다.

신뢰성은 기록물의 정보가 사용하기에 충분한 내용을 담아야 한다는 것으로 이해할 수 있다. 가용성은 기록물의 정보를 실제로 사용할 수 있어야 한다는 것으로 이해될 수 있다. 기록물에 증거능력을 부여해 주는 특성은 진본성과 무결성이다. 진본성은 형상의 유래가 적법하다는 것이고 무결성은 그 형상이 변조되지 않았음을 의미한다. 전통적인 기록물은 이 두 가지 특성이 상호 밀접한 관계에 있다. 무결성이 확보된 기록물이면 진본성도 강화되는 것이다. 그래서 통상 "진본성"이라는 말로 증거능력을 대표할 수 있다. 호주 빅토리아 주의 VERS 표준(PROV 2003)에서는 증거능력을 광의의 "무결성"으로 부르고 있다. 혼란을 막기 위하여 광의의 진본성과 무결성에 대하여 협의의 진본성을 "ISO 진본성", 협의의 무결성을 "ISO 무결성"이라고 때때로 부르기로 한다.

전통적인 기록물에서도 이 두 가지의 특성에 대한 고의적인 공격이나 부주의에 따른 훼손이 있을 수 있다. 전자기록물은 전통적인 기록물보다 이 두 가지 특성을 달성하기가 더 어렵다. 그 이유는 공격에 대한 취약성, 원본 개념의 약화, 그리고 시스템 의존성에 있다.

첫째, 전자기록물에는 공격을 사전에 차단하는 것과 사후에 탐지하는 것이 모두 쉽지 않은 취약성이 있다. 접근에 물리적인 한계가 있는 종이 기록물과는 달리 전자기록물은 온라인으로 접근 가능하므로 불특정 다수에게 노출될 여지가 많아 공격이 비교적 쉽고 익명성 속에서 공격 욕구가 쉽게 생길 수 있는 경향이 있다. 또한 전자기록물은 불법복제, 변조, 삭제 등의 공격을 당한 이후에도 품질의 저하가 일어나지 않으므로 공격을 받았다는 사실을 탐지하기 어

렵다. 그러므로 주어진 전자기록물의 형상이 원래대로의 형상인가를 보장하여 진본성과 무결성을 증명하려면 더 정밀한 고려가 필요하다.

둘째, 전자기록물은 몇 번을 복사해도 원본과 품질이 같다. 이진 비트열 수준에서 원본과 사본(그렇게 부를 수 있다면)은 완전히 동일하다. 실물이 없는 가상적인(virtual) 이진 비트열이기 때문에 생산, 저장, 유통, 사용하면서 동일한 이진 비트열이 이 시스템에서 저 시스템으로, 이 저장공간에서 저 저장공간으로 복사되어 전달된다. 디스크에 저장된 문서 파일을 메모리로 읽어 올 때에는 디스크의 사본이 옮겨오는 것이 아니고 복사되어 오는 것이며, 인터넷을 통하여 파일을 전송하거나 홈페이지를 접속하여 그 내용을 볼 때에도 원래 사이트의 파일은 그대로 있고 단지 내용이 복사되어 전송되어 오는 것이다. 따라서 전자기록물은 원본이 "무수히 많다" 또는 "원본이 따로 존재하지 않는다"고 해야 할 것이다.

셋째, 전자기록물은 전산화(전산 시스템)의 산물이므로 특정 전산 시스템을 거치지 않고는 해독되고 사용될 수 없다. 그러므로 전자기록물은 사람이 그 상태를 직접 파악할 수 없으며, 해당하는 전산 시스템의 손실이 바로 기록물의 손실을 의미할 수 있게 되는 시스템 의존성이 존재하게 되는 것이다. 그런데 기술의 발전으로 환경이 변하게 되면 기존의 전산 시스템은 더이상 올바로 동작하지 않게 된다. 과거 MS-DOS 시대의 소프트웨어가 현재의 윈도우즈 환경에서 더 이상 동작하기 어려운 예를 흔히 본다. 또 근간이 되는 업무처리방법이 변하게 되면 해당 전산 시스템은 그 변화에 맞추어 같이 변해야 하고 기존의 전산 시스템은 수명을 다하게 된다. 사무관리규정에서 규정한 공문서의 양식과 결재방식이 바뀜에 따라 구 전자문서시스템은 더 이상 사용할 수 없게 되고 대신 신 전자문서시스템으로 대체된 예를 들 수 있다.

문제는 전산화의 산물인 전자기록물을 장기보존하려면, 해당하는 전산 시스템이 동작할 수 없는 수십년 후에도 당초와 동일하게 해독될 수 있도록 미리 준비해 두어야 한다는 데에 있다. 수십년 후 이 기록물을 사용할 시스템을 사전에 가늠할 수 없는 상황인 데에도 불구하고 이에 대응할 수 있도록 시스템에 대한 의존성을 탈피한 형태로 대비하여 보존하여야 한다. 이를 위해서는 원본을 장기 보존이 가능한 포맷으로 가공하는 작업이 필요하며, 그 결과로써 원본성이 어느 정도는 훼손되므로 전자기록물은 원본을 따지는 것이 무의미하고 대신 진본성을 따지는 것이 더 적절하다.

장기보존 중에 현재의 보존포맷이 적절하지 않고 새로운 보존포맷이 더 타당하다고 판단될 수 있으므로 포맷 변화는 보존기간 중 수차례 반복될 수 있다. 따라서 기록물 보존의 개념이 전통적인 종이 기록물 시대와는 다르게 된다. 종래의 종이 기록물은 원본을 처음 만들어진 모습 그대로임을 보장함으로써 원본성을 인정받게 되고 증거능력이 생긴다. 즉 "그대로 보존하면 보존된다." 이에 반하여 전자기록물은 포맷이 변환될 수 있고 진본성 추적을 위하여 이력정보를 포함한 메타데이터가 계속 수정되어야 하므로 "그대로 보존하면 보존 효과를 낼 수 없다." 동적인 환경 속에서 전자기록물의 진본성과 무결성 확보는 더욱 복잡해진다.

3. 전자기록물의 진본 보존 효과 달성을 위한 필요기능

개별 전자기록물관리기관 또는 시스템의 입장에서 전자기록물의 보존 효과를 달성하기 위해서는 1) 획득 당시 진본임을 확인함으로써 진본만 보존하도록 통제하여야 하고, 2) 보존기간 중 지속적으로 진본의 유실을 막아 보존할 수 있어야 하며, 2) 주어진 전자기록물이 진본인지 검증 가능하여야 하고, 3) 진본 훼손에 대하여 사후 대처 가능하여야 한다.

3. 1 획득 기록물 진본 확인

해당 기관 또는 시스템은 전자기록물을 직접 획득할 수도 있고 다른 기관 또는 시스템으로부터 이관받을 수도 있다. 그러나 이는 기록물법 상의 생산기관-자료관-전문관리기관의 단계에 따라 정해지는 것은 아니다. 왜냐하면 생산기관 단계에서는 비전자기록물 또는 비표준 전자기록물이었지만 자료관에서 이를 표준 전자기록물화하여 등록할 수 있고 이때 기록물로 보면 이관이겠지만 전자기록물로 보면 획득일 수 있기 때문이다. 이에 대한 논의는 앞으로 더 필요하다고 보이며 다만 본 논문에서는 이를 통칭하여 획득이라고 부르기로 한다.

획득 당시 진본임을 확인하기 위해서는 첫째 품질 검사가 이루어져야 하며 둘째 출처 확인이 되어야 하고 셋째 원본 선언이 되어야 한다. 품질 검사가 필요한 이유는 종이 기록물과 달리 전자기록물은 손상된 정보임을 바로 확인할 수 없기 때문이다. 손상된 파일일 수도 있고 포함되어야 할 도표가 누락되었을 수도 있다. 또한 전자파일의 특성상 바이러스나 스파이웨어에 오염되어 있을 가능성도 있다. 손상된 정보인지를 확인하는 수준은 여러 단계가 있을 수 있고 확인수준이 올라갈수록 시간과 비용이 들게 마련이므로 전자기록물의 중요도에 따라 그 수준을 정해줄 필요가 있다. 둘째 사항인 출처 확인은 ISO 진본성을 위한 출발점이다. 그러므로 보존 대상 기록물은 기록물 관리기관에서 모아오는 것이 아니라 생산기관이 기관인증을 거쳐 절차에 따라 이관해 주어야 한다. 생산자 기관인증이 부득이하게 이루어질 수 없는 경우라도 이에 준하여 출처가 확인될 수 있는 방안을 강구하여야 한다.

획득 당시의 전자기록물 형상을 부를 용어가 필요하다. 왜냐하면 전자기록물은 계속 변화할 수 있고 그 진본성 확인을 위해서는 적법 절차에 따라 변화해 온 것인지를 추적할 수 있어야 하는데 변화과정은 이력관리 등으로 이루어진다고 하더라도 원래의 형상이 어떠했는지를 확인할 수 있으려면 획득 당시의 형상이 있어야 하며 이것이 진본성 확인의 시발점이 되겠기 때문이다. 따라서 본 논문에서는 혼동의 우려가 있음에도 불구하고 이를 "원본"으로 부르기로 한다.

셋째 사항인 원본 선언은 이관한 기관과 이관받는 기관이 그 사실을 상호 부인할 수 없도록 당시의 상황과 형태를 기록하고 그 시점부터 기록물로 취급하는 것을 말한다. 이 시점부터 기록물의 내용은 수정될 수 없으며 수정을 하려면 생산기관측에서 고쳐 다시 이관하는 절차를 거쳐야 한다. 선언은 또한 생산기관에게 이관이 성공하였다는 통보의 역할도 할 수 있다.

3. 2 진본 유실 방지

진본의 유실을 막으려면 정보 보호가 이루어져야 한다. 정보 보호는 진본성 확보의 사전 예방조치에 해당한다. 이를 위해서는 사용자 인증, 기록물 보호, 시스템 보호, 네트워크 보호 등의 각종 기술이 필요하다. 기록물은 중복 보존이나 제공 등을 통하여 진본이 여러 곳에 복본으로 존재할 수 있다. 따라서 가장 중요한 정보 보호는 시스템에 상관없이 보호되는 기록물 보호이다.

3. 3 진본 검증

전자기록물도 종이기록물처럼 진본임을 입증할 수 있어야 한다. 그런데 전자기록물은 적절히 지속적으로 변환시켜야만 효력이 보존되고 효력 보존을 위한 포맷 변환은 용인하여야 되기 때문에, 보존되고 있는 형상이 보존의 의도로 적법하게 변환된 결과임을 증명하는 "ISO 진본성"과, 적법한 변환 이외의 변조는 없었음을 증명하는 "ISO 무결성"이 모두 필요하다.

"ISO 진본성" 확보를 위해서는 현재의 형상이 적법한 원천으로부터 시작해서 적법한 사람이 적법한 절차를 거쳐 처리한 현상인지 확인할 수 있어야 한다. 적법한 절차임을 확인하려면 그동안의 수정 이력 정보를 메타데이터에 포함시키는 방법으로 가능하다. 적법한 사람임을 확인하려면 해당 사람임을 확인할 수 있는 담당자 인증정보를 붙일 수 있다.

"ISO 무결성" 확보를 위해 사용 가능한 기술적 방안은 정보 보호 기능을 이용하여 허가되지 않은 변조가 사실상 불가능함을 믿도록 하는 능동적 방법과, 기록물이 권한 없이 변조되면 그 사실을 항상 확인할 수 있는 수동적인 방법의 두 가지로 분류할 수 있다. 능동적 방법은 현재 해킹 범죄 사례에서 볼 수 있듯이 완벽한 차단이 어려우며 보호 기능이 장착된 시스템을 통해서만 기록물을 활용할 수 있고 외부 제공 이후에는 더 이상 보호할 방법이 없다는 취약점이 있다. 수동적인 방법은 기록물 자체만으로 불법변조 사실을 확인할 방법이 있기 때문에 (4장 참조) 시스템에 대한 의존도를 낮출 수 있는 장점이 있어서 전자기록물을 보존만 하는 것이 아니라 배포까지를 고려한다면 바람직한 방법이다. 그러나 변조를 사전 차단하는 용도가 아니고 사후 변조여부의 확인용이기 때문에 앞의 진본 유실 방지 방안과 뒤에 설명할 진본 훼손시 대처 방안이 함께 필요하다.

3. 4 훼손된 진본에 대한 사후 대처

진본이 훼손되었음을 확인한 경우 그에 대한 대처도 필요하다. 기록물 관리는 향후 그 기록물을 사용할 가능성이 있기 때문인데, 전자기록물은 훼손되어 있는 상태를 육안으로 파악할 수 없으므로 훼손된 상태를 인지하지 못하고 장기 보존하다가 정작 사용하려고 할 때에 비로소 훼손 사실을 알게 될 가능성이 있다.

3.3의 진본 검증이 실패하면 당초 획득 당시 진본 확인(3.1)을 거쳤다고 할 때, 당해 전자기록물이 보존 도중 변조 또는 유실되었다는 의미이다. 가능한 한 3.2의 진본 유실 방지를 위하여 예방적 차원에서 최대한의 정보 보호를 하여야 하겠지만, 실제 이러한 경우가 발생하지 않으리라는 보장은 없다. 실제로 이러한 사실

이 사후에 발견되면 그동안의 기록물 효력을 소급해서 무효화해야 하는지와 같은 곤란한 상황이 초래될 것이다. 따라서 적어도 언제까지는 진본이었음을 파악할 방법이 있는 것이 좋다. 위변조 공격의 시점과 경로를 추적할 수 있다면 이 문제는 해결된다. 그것이 불가능한 경우에는 최근의 진본 검증(3.3) 성공 시점을 파악하여 효력 인정 하한 시점으로 삼아야 할 것이다. 그러므로 진본 검증 행위는 여건이 허락하는 한 자주 수행되는 것이 바람직하다.

진본을 복구할 수 있다면 가장 바람직하다. 백업이나 이중 보존이 이 목적으로 사용되는데, 좀더 확실한 복구가능성을 위해서는 전자기록물 획득 당시의 모습 그대로를 보존매체에 담아 격리 보관하는 것도 고려할 수 있다. 좀더 중요한 기간기록(essential record)이라면 전산 환경에 의지하는 것이 위험할 수 있다. 정전이나 전시 피란에 따라 전산 시스템을 사용할 수 없을 경우도 상정할 수 있다. 이러한 경우에 대비하여 엄선된 기간 기록은 비 디지털 양식의 사본을 유지하는 것도 고려할 수 있다.

4. 실현방안

이상과 같이 전자기록물 진본성 확보를 위해서는 여러 가지 기능이 연계되는 것이 필요하다. 그런데 각 기능을 실현할 기술적 수단으로 어떠한 것을 선택하느냐에 따라 실제 원하는 효과가 달성될 수도 있고 그렇지 않을 수도 있을 것이다. 특히 기록물이 권한 없이 변조되면 그 사실을 항상 확인할 수 있는 방법에 대한 구체적인 방안이 필요하다. 중요한 고려사항은 진본성 확보를 위한 현실성으로서, 기록물 자체만으로 진본 검증이 가능한 것이 바람직하며, 검증을 가급적 자주, 실시간으로 수행하여야 할 것이므로 검증 작업의 효율성을 높여야 한다는 것이다.

4. 1 변조 사실 확인 방법

적법한 변환이 아니고 허가 없이 위변조한 것을 기록물 자체를 통하여 알 수 있는 방법으로 전자서명(digital signature; 디지털 서명) 기술과 디지털 워터마킹(digital watermarking) 기술을 비교해 본다.

디지털 워터마킹이란 기록물에 일정한 정보를 은닉해 저장해 두는 기술을 말한다. 어원은 지폐를 제작할 때 젖어 있는 상태에서 은닉된 도안을 인쇄하면 마른 후에는 빛에 비추어 보아야 모양이 드러나는 기술인 워터마킹에서 유래하였다. 적용 사실을 은닉하면서도 효과를 달성하는 것이 목적이며, 변조 공격에 강인하도록 설계한다. 보통 저작권자/구매자 확인, 즉 핑거프린팅(fingerprinting)이 가능하여 유출자 추적(traitor tracing)에 매우 효과적이다.

디지털 워터마킹은 그림이나 사운드 등 멀티미디어 콘텐츠에 은닉하여, 콘텐츠의 출처를 확인할 목적으로 사용된다. 가령 사용자 A가 제공자 B로부터 적법하게 구입한 동영상을 허가 없이 타인 C에게 유통시키면, 제공자 B는 이 타인 C의 동영상 파일로부터 제공자 B가 당초 은닉해 두었던 디지털 워터마킹을 추출함으로써 A로부터 유출되었음을 알 수 있다. A가 이를 숨기려고 해상도 변환, 편집, 재코딩 등 변조 공격을 하여도 잔존할 수 있도록 하는

것이 이 기술의 핵심이다.

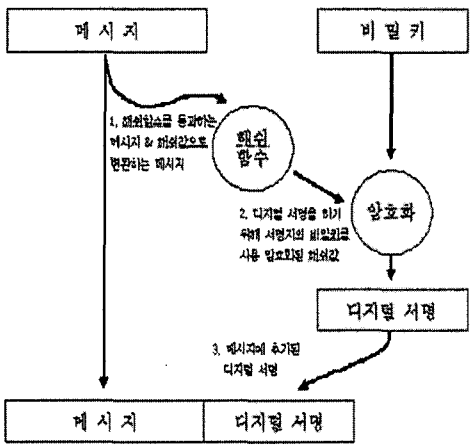
따라서 "ISO 진본성"을 위한 출처 정보 보존에는 용도가 맞겠지만, "ISO 무결성"을 위하여 변조 사실을 확인하는 용도에는 맞지 않는다. 변조 행위의 흔적이 나타나는 것이 아니고 변조하여도 출처 정보를 계속 잔류시킬 수 있도록 하는 기술이기 때문이다. 또한 디지털 워터마킹은 붙일 수 있는 파일 포맷이나 적용 횟수, 적용 가능한 자료의 최소크기 등이 제한되며 변조 공격에 100% 강인하지도 않다.

전자서명은 암호법을 기본으로 하여 기계가 인식하는 변조법인데, 자신의 서명을 표시할 수 있는 사람은 본인밖에 없는 것처럼 전자서명에 의한 변조를 할 수 있는 사람(또는 시스템, 기관)은 그 본인밖에 없음을 확률적으로 믿는 것이다.

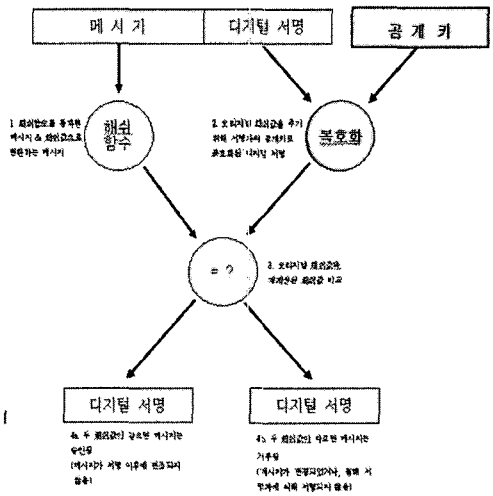
전자서명 중에서 현재 국제적으로 널리 사용하고 있으며 국내에서 사용자 인증용으로 공식 사용되는 기술이 비대칭키 기반, 또는 공개키 기반 인프라 구조라는 뜻의 PKI(Public Key Infrastructure) 기술이다. 이 기술의 기본 메커니즘은 그림 1 및 그림 2와 같다. 메시지(기록물)에서 해싱을 통하여 정보를 추출하여 여기에 생산자의 비밀키(개인키)를 적용해서 전자서명을 만든다. 이 전자서명을 본 메시지에 첨가하여 함께 보존한다. 해싱은 동일한 입력에 대해서는 동일한 값을 내는 함수이며, 해싱값을 변경시키지 않으면서 원 메시지를 목적에 맞게 변조하는 일은 불가능에 가깝다.

진본임을 검증할 때에는 전자서명 내용을 공개키로 푼 것과 메시지에서 추출한 정보가 같은지 비교한다. 같으면 진본인 것이고 다르면 진본이 아닌(위변조된) 것이다.

PKI는 원문을 변조하면 전자서명이 일치하지 않게 되기 때문에 위변조를 확인할 수 있는 무결성 기능을 제공한다. 그래서 전자정부법(법제처 2004c) 20조의 "인증받은 행정전자서명이 있는 문서는 서명 이후 그 내용이 변경되



(그림 1) 전자서명 적용 개념



(그림 2) 전자서명 확인 개념

지 않았다고 추정"하는 기능을 지원할 수 있다. 또한 본인임을 확인할 수 있는 인증 기능을 제공하므로 진본성 보장에도 도움이 된다. 그래서 동 20조의 앞부분에 명기된 "인증받은 행정전자서명이 있는 경우에는 당해 행정전자서명을 전자공문서에 표시된 행정기관의 관인·공인 또는 공무원의 서명이 있는 것으로" 볼 수 있는 기능을 지원한다.

다만 적용에 많은 시간이 걸리고, 적용한 문서는 부피가 커지는 단점이 있다. 또한 비밀키의 관리 책임이 각 생산자에게 요구되는 불편함이 있다.

전자서명과 디지털 워터마킹을 비교해 보면 표 1과 같다.

그러므로 무결성 보장을 위해서는 전자서명을 사용하는 것이 바람직하다. 전자서명은 진본성 보장에도 사용될 수 있으므로 이 한 가지 수단으로 진본 보장을 위한 두 가지 사항이 모두 만족된다. 다만 비밀키의 관리에 만전을 기하도록 생산자의 시스템이 신중히 구축되어야 한다.

4. 2 서명 재적용 방안

전자서명은 메시지를 변조하면 불일치하게 되므로 무결성 보장에는 좋은 성질을 가지지만, 전자기록물처럼 보존을 위하여 변환이 필요한 경우에는 이전 전자서명은 파괴되어 버리므로 전자서명을 다시 적용시키는 행위가 필요하다. 진본성 보장을 위하여 보존 전자기록물에 대하여 수행된 모든 적법 행위에 대한 이력 정보를 계속 유지관리 하여야 하고 이 정보들이 메타데이터에 포함되어야 하는데, 이 메타데이터도 무결성이 보장되어야 하기 때문에 전자서명 대상 메시지에 포함된다. 따라서 서명 재적용은 상당히 빈번히 필요할 것으로 예상된다.

호주 등지에서 제안하는 방법은 "양파 모델(onion model)"이다(PROV 2003). 이 방법은 새로운 정보가 추가되거나 수정될 때마다 행위 당사자의 전자서명을 덧씌운다. 각 행위 하나하나의 적법성이 인증되는 장점이 있지만 장기간에 걸쳐 보존되는 기록물의 경우 시일이 지나면 그 전자서명이 수없이 누적되기 때문에, 전자기록물의 크기가 지속적으로 증가하며 진본성 검증을 하여야 할 때에는 시간의 역순으로 각 전자서명을 일일이 검사하여야 한다. 미래에 진본성 검증이 온라인 검색 등 기록물 제공시마다 실시간으로 수행되어야 한다면 그때마다 그동안 누적된 전자서명을 당시의 담당자 정보와 대조하며 확인작업을 한다는 것은 실질

(표 1) 전자서명과 디지털 워터마킹의 비교

	전자서명	디지털 워터마킹
적용가능 기록물 종류	어떤 기록물에도 적용가능	적용 가능한 기록물이 제한됨
헤더등 부가적인 데이터 필요성	필요	불필요
법적근거	전자서명법, 전자정부법, 사무관리 규정등	없음
데이터변환시 매번 재적용 필요성	매번 재적용 필요	한번으로 계속유지가능
공격 난이도	비밀키가 유출되지 않는 한 공격이 어려움	위험한 공격 있음 - 압축, 변환(재변조등) - 공모공격

적으로 불가능할 수 있다. 현재까지는 어느 국가나 기관도 이러한 상황을 경험해 보지 못하였다.

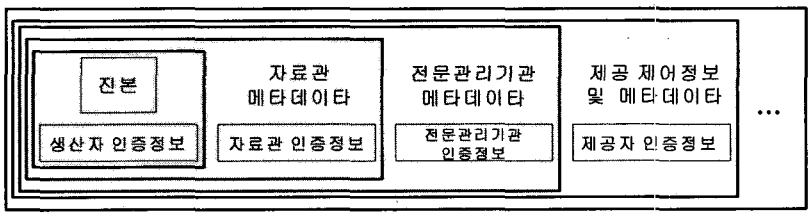
또 다른 극단으로, 언제이든 최후에 적용한 단 하나의 전자서명만 첨부하여 보존하는 방법을 생각해 볼 수 있다. 일단 전자서명된 기록물에 내용을 추가하거나 수정할 때에는 서명을 "벗겨 내고" 평문으로 만들어 작업을 수행한 뒤 담당자의 명의로 재서명 한다. 기록물에는 항상 하나의 전자서명만 존재하는 단순한 방법이다. 그동안의 이력 정보는 평문으로 저장되고 인증만 최후의 담당자가 일괄 수행하는 것이다. 마지막 담당자가 모든 정보를 위변조할 수 있는 큰 약점이 있다.

그러므로 현실적으로 사용할 수 있는 효율성과 진본을 보장하는 효과성을 동시에 확보하기 위하여, 이 양 극단의 타협점을 찾아 기관(시스템)별 1개씩의 전자서명을 유지하는 방안을 제안한다. 예를 들어 자료관에 일단 이관되어 들어 온 기록물에는 생산자의 기록물 원본과 생산자 명의의 인증정보(전자서명 포함)가 첨부된다. 여기에 전자서명이 되어 있기 때문에 자료관에서는 이 정보를 고칠 수 없다.

자료관의 수집 담당자가 수집하여 - 검수 - 분류 등의 절차를 거치면서 메타데이터가 추가되는데 그 때마다 자료관의 전자서명을 벗겨 버리고 작업한 후 전자서명을 새로 생성하여 첨부한다.

이러한 방식으로 한 기관을 거칠 때마다 하나의 전자서명이 붙도록 해서 양파 모델의 복잡성을 크게 줄인다. 이때 기관업무 수행에 따라 전자서명이 해지된 틈을 노려 기관 내부에서 위변조할 수 있는 위험이 있는데, 해당기관이 기록물을 전문적으로 다루는 기록물관리기관이고 교차점검 행정이 있으므로 일반적인 상황보다는 위험성이 크게 준다고 판단하였다. 이 방안의 개념을 도시하면 그림 3과 같다.

현재 정부가 생각하는 전자기록물 라이프 사이클은 전문관리기관으로 끝이 나지만,(국가기록원 2005) 향후 전자기록물 형태로 정보가 제공되어 계속 사용될 가능성이 있다. 예를 들어 국가기록원이 보존하고 있던 상명대학교 관련 과거 교육부 기록을 상명대학교 도서관이 제공받아서 관리하고 있다가, 이를 다시 절차에 따라 제3자인 D에게 제공할 수 있다. 이때 이 제3자 D가 가지게 된 전자기록물의 진본성 확인은 ISO 15489의 정의에 따라 적절한 절차를 거쳐 제공받았는지 확인하는 것이 필요하므로 제공자인 상명대학교의 전자서명이 첨부되어 있어야 한다. 이 시나리오에 따르면 1) 교육부생산 행위의 서명, 2) 교육부 해당 자료관의 서명, 3) 국가기록원의 서명, 4) 상명대학교의 서명이



(그림 3) 기관별 단일 전자서명 모델

라는 4개의 전자서명이 붙은 형태로 D에게 제공되게 된다.

4. 3 전자서명의 명의

담당자 개인 명의의 서명이 적용되는 것이 책임소재를 분명히 하며 담당자의 시스템 로그인 정보에 따라 자연스럽게 서명할 수 있다는 점에서 일단 타당한 것처럼 보인다. 반면에 단점도 있다.

앞의 시나리오에서 정보를 최종 제공받은 D의 입장에서 볼 때 기록물의 진본성에 대하여 책임을 물을 대상은 제공 기관인 상명대학교나 국가기록원, 교육부이지 그 당시의 담당자 개인이 아니다. 개인에 대한 책임 검증은 각 기관 내부의 일에 속한다. 기관 내부에서 과거의 업무행위에 대한 책임을 가릴 때 반드시 개인전자서명이 있어야 하는 것은 아니다. 전자화가 되어있지 않던 과거부터 이러한 책임소재는 기관 내부의 감시감독 등 행정행위로 이루어졌다. 따라서 대외적으로 기관 명의의 보장이 있다면 담당자의 개인 명의 서명이 반드시 있을 필요는 없다.

담당자의 서명을 적용하게 되면 담당자의 수와 담당자 교체의 횟수가 기관의 경우보다 훨씬 많을 것이기 때문에 검증시에 각 명의의 확인과 당시 유효한 인증서의 파악 등의 복잡도와 비밀키 유출의 위험성도 그만큼 더 커질 수 있다.

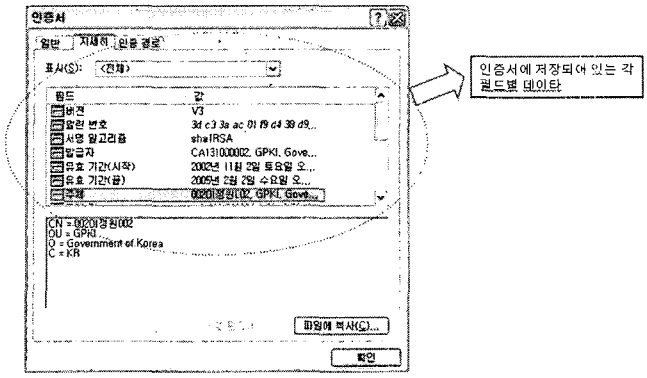
담당자 개인 명의의 서명을 적용하여 관리하고 유통시키게 되면 당시 실제 담당자가 아닌 사람의 명의로 서명된 기록물을 진본인 줄 알고 장기간 보존하는 경우, 또는 보존 도중 타 명의로 변조하여 재서명해 놓을 경우, 시일이 지난 후 진본 검증의 필요에 의하여 확인하는 시점에 가서야 이 사실을 알게 될 수 있다. 이것은 각 개인별 서명을 검증해야 할 뿐만 아니라 그 개인이 당시에 실제의 담당자였음을 확인할 다른 방도가 있어야 함을 의미한다. 기관 명의는 더 공신력이 있기 때문에 이러한 위협으로부터 상대적으로 안전할 것이다. 따라서 개인 명의보다 기관 명의의 서명 적용이 바람직하다. 표 2는 이러한 비교를 요약한 것이다.

4. 4 인증서의 보존 위치

인증서(certificate)란 전자서명을 검증할 수 있도록 그림 4처럼 인증서 버전, 인증서 일련번호, 인증서의 유효기간, 발급기관명 및 전자서명 알고리즘 정보, 가입자 이름 및 신원

(표 2) 전자서명 명의 비교

	개인 명의	기관 명의
사용자 입장의 신뢰도	낮음	높음
행위자 인증	분명하게 인증됨	담당자명을 평문으로 기록할 수는 있지만 사실 증명은 기관의 책임임
명의인이 담당자임의 확인	어려움	쉬움
인증의 효율성	비효율적	효율적
공격의 취약성	상대적으로 취약함	상대적으로 안전함



(그림 4) 행정전자서명(GPKI) 인증서의 예

확인정보, 전자서명 알고리즘 정보 등을 담은 정보객체이다. 현재 국내에서는 전자상거래 등 민간 부문의 사용을 위하여 전자서명법(법제처 2001)에 따라 한국전산원 등 6개 최상위 공인인증기관(certification authority)이 직접 또는 대행기관을 통하여 발급하고 있는데 이를 공인전자서명(NPKI)라 한다. 공인인증기관은 정해진 것이 아니라 정보통신부장관의 지정에 의하여 2년 단위로 갱신지정하며 인증업무의 정지 및 지정취소도 가능하다. 공공 부문은 전자정부법(법제처 2003b)에 의거하여 행정자치부 산하 행정전자서명인증관리센터에서 발급하고 있는데 이를 행정전자서명(GPKI)이라 한다. 인증서는 보통 1년 단위의 유효기간을 가지며 유효기간이 끝나면 새로 인증서를 발급받아야 하고 이에 따라 전자서명도 갱신된다.

보존되던 전자기록물이 진본인지 검증하기 위하여 적용된 전자서명값을 그림 2와 같이 대조하여 확인하려면 당사자 또는 기관의 공개키와 서명 방법 등을 담은 이 인증서가 필요하며, 유효 기간이 지정되어 있으므로 서명 당시에 유효했던 인증서가 필요하다. 그러므로 전자기록물에 적용된 모든 전자서명에 대한 인증서 정보가 어디엔가는 있어야 한다. 해당 법률에 의하면 공인인증기관은 인증서 정보를 안전하게 보관하여야 하고 GPKI의 경우에는 국가기록원으로 이관하도록 하고 있는데 아직까지 실현된 바는 없다. 지금까지 전자서명의 주 용도가 온라인 접속시 상호 인증용이었기 때문에 당시에 확인 가능한 기능에 초점이 맞추어졌다. 이제 전자기록물 중장기 보존에 전자서명을 적용하게 되면 적용 당시뿐 아니라 시일이 경과된 후에도 이를 확인 가능하도록 강구하여야 하는 것이다.

인증서 정보를 기록물과 별도로 보존 관리하여 두고 진본 검증 시점에 해당 인증서를 검색하여 대조하는 방법이 있다. 현재 국내 기록관리 관행대로 계속된다면 결국 이 방식으로 인증이 진행될 것이다. 이 방식은 기록물 위변조의 위험이 상대적으로 낮다. 그러나 모든 기록물에 대한 당시의 전자서명과 매 시점의 무효 인증서 목록들을 모두 관리하고 있어야 하고 해당 인증서를 실시간에 찾을 수 있어야 하며 검색된 인증서가 당시 유효하였는지 인증서 자

체에 포함된 유효기간 및 당시 인증기관이 게시한 무효 인증서 목록 포함여부를 대조하여 확인하여야 한다. 기록물과 인증서 어느 하나라도 망실되면 진본 확인이 불가능한 위험이 있다.

호주 빅토리아 주(PROV 2003)에서는 보존할 전자기록물에 인증서 정보를 함께 넣어 보존 객체를 생성하고 있다. 이 방식은 기록물 자체만으로 인증이 가능한 장점이 있지만, 전자서명을 포함한 인증정보 전체를 위조하는 공격에는 취약한 문제가 있다.

메타데이터를 기록물과 함께 넣어 보존 객체를 만드는 것이 현재 국제 추세이다. 필요한 내용들을 모두 모아 패키지화하는 것이 시스템과 기관을 옮겨 다니면서 중장기간 계속 보존 활용하여야 할 전자기록물에 관리상 편리하고 정보 누락의 위험이 적다. 이와 같은 이유로 당시 시점에서 유효한 인증서 정보도 기록물에 함께 넣어 보존 및 유통시키는 것이 바람직하다.

이때 인증서 전체를 자신의 것으로 바꿔치기 하여 위변조를 시도하는 공격에 대비한 방안이 필요하다. 인증서를 발급한 공인인증기관의 전자서명을 인증서에 포함시켜, 이 인증기관의 전자서명 인증정보를 별도 보관하는 방법으로 인증서 자체의 진본성을 검증한다면 인증기관의 수가 적고 인증기관 사칭이 거의 불가능하므로 안전한 방법이 된다.

4. 5 진본 제공 서비스

기록물관리기관 내에서 엄중히 전자기록물의 진본성을 보장하도록 유지한다고 하여도 일단 이 기록물이 기록물관리기관 및 시스템을 벗어나 제공되면 그 이후의 변조 가공을 막을 방법이 쉽지 않다. 국내 전자정부 서비스를 오용한 사례를 보면, 사용자 E가 자격증빙서류와 같은 전자문서를 자신의 PC로 다운로드받은 뒤 편집기로 그 내용을 변조한 내용을 종이 출력하여 제출하는 것이다. 이를 막기 위하여 종이 위에 바코드를 인쇄하여 그 바코드와 내용이 일치하는지를 확인할 수 있도록 하는 등의 기술이 상용화되어 있다.

문제는 종이기록물과 전자기록물의 진본성 확인 정보가 다르다는 데에 있다. 종이기록물은 육안이나 물리화학적인 방법을 통하여 실물을 상대로 검증을 하는 방식이지만, 전자기록물은 기본적으로 사이버 공간상의 이진 비트열에 불과하다. 전자서명도 기계를 통해서만 확인이 가능하며 일단 출력해 놓으면 전자서명의 진위 여부를 확인할 방법이 없다. 전자기록물은 전용 시스템을 통하여 서비스 받을 경우에만 진본성을 계속 유지하고 또 검증할 수 있다.

모든 기록물은 그 양식이 바뀌면 진본성이 현저히 침해된다. 종이기록물을 스캐닝하여 이미지 파일로 보존하거나 마이크로필름으로 촬영하여 보존하는 것은 보존성을 고려하여 만든 사본에 불과하다. 이의 증거능력은 "원본대조필"과 같은 별도의 장치가 추가로 결합될 때에만 비로소 유효하다. 마찬가지로, 전자기록물을 종이 위에 출력하게 되면 전산 기술에 의하여 보장받던 진본성, 무결성, 기밀성 등이 더 이상 보장받을 수 없게 된다. 전자기록물에 대하여 종이 출력물은 종이기록물에 대한 스캐닝 사본과 마찬가지로 사본에 불과하다.

그러므로 국내에서 현재 통용되고 있는 전자기록물 종이출력물의 증명용 활용 관행은 대단

히 위험하다고 판단된다. 전자기록물은 전자기록물 자체로 열람되고 제공, 활용되어야 한다. 사용자는 원본 전자기록물을 다운로드받는 것이 아니라 제공 기관 명의의 인증정보가 포함된, 진본성을 보장할 수 있는 형태의 패키지 정보를 다운받아 이를 그대로 제출할 기관에 제출하는 것이다. 이때 본인의 전자서명을 적용하여 그림 3의 껍질 하나를 더 만들어 씌운다. 이것은 증명서류 제출 시 본인 날인서명의 역할을 하게 된다.

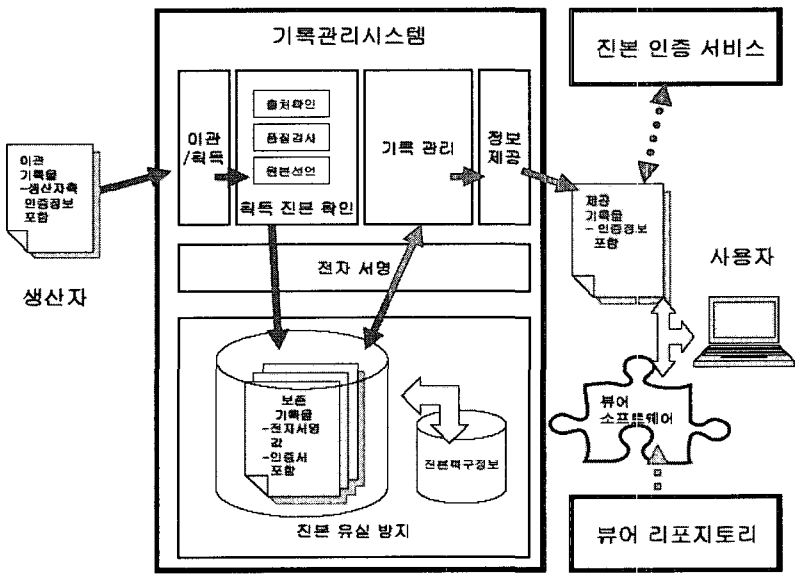
제출받은 기관은 이 전자기록물의 진본 여부를 판별하여야 하고 내용을 판독할 수 있어야 한다. 전자를 위해서 국가기록원 등의 공신력 있는 중앙기관에 인증서비스센터를 구축할 필요가 있다. 후자를 위해서는 뷰어(viewer) 모듈을 무료로 간단히 다운로드받아 설치할 수 있도록 중앙기관에서 제공하여야 할 것이다.

5. 전자기록물 관리 방안

3장과 4장에서 설명한 기능과 방안을 종합하면 그림 5와 같다.

이관되는 기록물은 이관 받는 기관의 자의적인 변조를 막기 위하여 생산자의 인증정보를 포함하여야 한다. 공공기관의 자료관처럼 생산자와 기록관리기관의 명의가 같은 경우가 생기면 생산측의 별도 검토자에게 원본선언에 대한 정보를 피드백시켜서, 동일인의 자의적인 위변조를 거를 수 있는 장치를 강구하여야 할 것이다. 생산자의 여건에 의하여 인증정보를 적용할 수 없거나 적용되지 않은 채 생산된 구 기록물의 경우에는 이관 받는 기록물관리기관 명의로 원본선언을 하고 이를 생산자에게 피드백시키는 정밀한 절차가 필요할 것이다.

이관받은 기록물을 기록물로 선언한 이후에



(그림 5) 전자기록물 진본성 관리 개념

는 이관받은 기관 명의의 전자서명을 적용하여 저장하였다가 수정시에는 일단 해지하고 다시 적용하는 서명 재적용 절차를 거치도록 한다. 서명 해지상태에서 변조가 일어날 경우에는 방어하기 곤란하므로 재적용을 할 때에는 반드시 사전과 사후에 이전 버전과 대조작업을 하여 안전성을 확인하여야 한다. 이를 위해서는 전자기록물 변환시에 이전 버전을 파기하지 않고 적어도 대조작업이 끝날 때까지는 유지하여야 한다.

저장된 전자기록물은 유실이 방지될 수 있도록 정보 보호 기술을 적용하도록 하며, 혹시 진본을 잃어버릴 경우에라도 중요 기록물은 복구할 수 있도록 방안을 마련해 둔다.

정보 제공은 진본성 확보를 위하여 인증된 형태의 전자기록물 자체를 서비스하도록 한다. 일반 사용자라도 이의 진본 확인과 내용 판독을 할 수 있도록 진본 검증 서비스와 뷰어 다운로드 서비스가 이루어지는 것이 바람직하다. 이를 위해서는 수십 년간 사용되어 온 다양한 인증 기술과 기록물 포맷들을 모두 처리 가능하도록 완벽한 등록저장소(registry/repository)가 구축되고 지속적으로 유지관리 되어야 할 것이다.

6. 결 론

공공부문과 민간부문에서 현재 다양한 형식과 용도로 생산해 내고 있는 전자기록물은 막대하다. 그런데 이 기록물들은 생산 당시의 유통을 목적으로 주로 사용되고 있으며 이 전자기록물들을 장기간 보존하였을 때 증거능력이 되는 진본성이 계속 확보될 수 있을 것인가와 그를 달성하기 위한 방법은 무엇인가에 대한 규명도 경험도 현재로서는 미흡하다.

이러한 문제의식에서부터 시작한 본 연구에서는 다양한 취약점과 공격가능성이 있음을 알게 되었고 진본 확보를 위하여 수행하여야 할 필요 기능들을 도출할 수 있었다.

이러한 기능들을 실현하기 위한 대안들을 검토하면서, 특정 방안을 채택하게 되면 그 방안의 특성상 활용측면에서 새로운 이슈가 대두되게 되며 이를 보완 관리할 세부사항을 다시 도출하여야 하였다.

상정한 경우들은 실제로 일어난 경우가 아직까지는 없고, 또한 제안 방안들을 실제 적용하여 사용가능성을 입증할 방법도 현재 없기 때문에 대부분의 연구는 상상력에 의존할 수밖에 없는 한계가 있었다. 그렇다 하더라도 고려해야 할 구체적인 경우들이 다양하였으며 그에 대한 최초의 세부적 연구검토가 본 연구의 공헌이 될 수 있을 것이다.

본 논문의 내용은 향후 전자기록물의 진본 보존을 위한 필요조건이 될 수 있다. 그러나 본 논문에서 다룬 내용만으로 전자기록물 진본성이 확보될 수 있다는 충분조건은 성립하지 않는다. 더욱 광범위하고 구체적인 연구가 필요하다. 이를 위해서는 전자기록물 관리에 관한 실무가 처음부터 완벽히 시행되기 힘들다는 사실을 인정하고 시범사업 등으로부터 시작하여 몇 단계의 발전 플랜을 수립하는 것이 필요하다. 또한 방법이 발전됨에 따라 그 이전 방법에 의하여 관리되었던 구 전자기록물의 진본성 확보가 어려워지는 상황이 발생하지 않도록 하는 대비책도 필요하다.

참 고 문 헌

국가기록원. 2005.『기록관리시스템 혁신 정보화전략계획(ISP) 수립 제안요청서』.

미국. NARA. 2001. Security Models for NARA ERM.

법제처. 1999.『공공기관의기록물관리에관한법률』.

법제처. 2004a.『공공기관의기록물관리에관한법률시행령』.

법제처. 2003a.『공공기관의기록물관리에관한법률시행규칙』.

법제처. 2003b.『전자정부구현을위한행정업무등의전자화촉진에관한법률』.

법제처. 2004b.『전자정부구현을위한행정업무등의전자화촉진에관한법률시행령』.

법제처. 2001.『전자서명법』.

법제처. 2002a.『전자서명법시행령』.

법제처. 2002b.『전자서명법시행규칙』.

법제처. 2004c.『사무관리규정』.

서혜란, 서은경, 이소연. 2003. 전자기록의 진본성 유지를 위한 전략.『정보관리학회지』, 20(2): 241-262.

송병호. 2000.『전자문서의 유통현황 및 보존방안』. 한국기록물관리협회.

송병호. 2001. 전자문서의 유통관련표준 및 고려사항.『전자정부특별위원회 전자정부 기반구조점검반 워크샵 발표자료』.

송병호. 2002. 전자문서의 효과적인 관리 및 활용에 관한 연구,『한국지역정보화학회지』, 5(1): 85-104.

송병호. 2004. 정부 전자문서유통의 발전방향에 관한 연구.『정보관리학회지』, 21(3): 185-202

영국. The Office of the e-Envoy. 2001a. e-Government Benchmarking Electronic Service Delivery.

영국. The Office of the e-Envoy. 2001b. e-Government interoperability framework.

이규철, 송병호. 2000. 현재의 전자문서 유통 시스템과 최적보존 방향.『기록관리보존』, 5: 51-76.

전자정부특별위원회. 2001a.『전자결재/전자문서유통 문제점과 대응 방안』.

전자정부특별위원회. 2001b.『전자정부기반구조검검 중간보고』.

전자정부특별위원회. 2002.『행정자치부 전자문서유통 확대를 위한 연구용역 사업 전자정부특위 점검회의 자료』.

정부기록보존소. 2003.『행정기관의 자료관시스템 규격』.

정부기록보존소. 2004.『전자문서시스템과 자료관시스템간 API 규격』.

행정자치부. 2002a.『행정기관의 전자문서시스템 규격』.

행정자치부. 2002b.『행정기관간 전자문서유통 표준』.

행정자치부. 2002c.『전자문서시스템과 행정정보시스템간 연계표준』.

행정자치부. 2000.『행정기관간 전자문서유통 시범사업 제안요청서』.

행정자치부. 2001a.『전자문서유통 확대를 위한 연구용역 사업 제안요청서』.

행정자치부. 2001b. 『전자문서 유통 확대를 위한 연구용역 사업 착수보고회 자료』.

행정자치부. 2002d. 전자정부 구현을 위한 문서관리제도 혁신방안 보고. 『장관보고회의 자료』.

한국소프트웨어산업협회. 2001. 『행정기관간 전자문서유통 표준 규격서 보완 요청 사항』.

한국전산원. 2001a. 『전자정부 및 정보공동활용 정책 분석: 영국과 호주를 중심으로』.

한국전산원. 2001b. 『전자정부분야 진단 및 해외 벤치마킹』.

한국전자거래진흥원. 2005. 『공인전자문서보관소 사업 정보전략계획(ISP) 수립 제안요청서』.

호주. NAA. 2002. Recordkeeping Implications of Authentication and Encryption within Public Key Infrastructure.

호주. PROV. 2003. VERS Standard Electronic Record Format.

ISO. 2001. ISO 15489: 2001(E) Information and documentation - Records management.

ISO. 2003. ISO 14721: 2003 OAIS(Open Archival Information System).

MacNeil, Heather et al. 2002. Establishing and Maintaining Trust in Electronic Records: Authenticity Task Force Report.