전자기록의 출처확인 지원전략

송 병 호*

* 상명대학교 컴퓨터과학부 교수

[국문초록]

전자기록을 잘 관리한다는 것은 결국 기록이 필요할 때 믿고 사용할 수 있도록 하려는 것이다. 전자기록은 진본성과 무결성 면에서 취약점이 있고 현행 표준이나 방법들은 이에 대한 보완 관리를 목적으로 해서 개발되었다. 그러나 전자기록은 진본성과 무결성을 독립적으로 고려하기 힘들므로 본 논문에서는 출처라는 개념을 도입하여, 출처확인이 우선 잘 이루어지는 지원 전략을 논의하였다. 이러한 측면에서 볼 때 현행 방식들은 검증 정보 수록 및 확인에 태만하며 장기검증에 문제가 있고 출처확인이 안되는 기록에 대한 대응책 마련이 미흡하다. 본 논문에서는 이러한 점을 개선하기 위하여한 출처확인에 필요한 요소들을 설명하고, 장기 검증이 가능하도록 전자기록보존포맷을 고정부와 변동부로 나누고 출처는 고정부에서만 확인하는 새로운 검증방법을 제안하며, 출처확인이 실패해서는 안되는 중요 기록물에 대하여 예방, 회피, 탐지복원 방안을 제시한다.

주제어 : 전자기록, 진본성, 출처확인, 인증, 장기보존

1. 머리말

기록이 전자적인 형태로 만들어지거나 관리되는 것을 전자기록 또는 디지털 기록이라고 한다. 20세기 후반부터 전자기록이 출현하더니 현재에는 공공분야는 물론이고 기업활동, 국민 생활에 이르기까지 사회 전반에 걸쳐 광범위하게 활용되고 있어서 사용하기 싫다고 사용을 안할 수는 없는 사회필수기반요소

로 자리잡고 있고 이러한 상황은 갈수록 심화될 것이다.

전자기록은 진본성(출처), 무결성(훼손없음), 신뢰성(충분하고 정확한 정보), 가용성(사용자의 이용편이성)이라는 기록의 4대요건 입장에서 볼 때 신뢰성과 가용성 측면에서는 월등한 이점이 있는 것이 분명하며, 진본성과 무결성 측면에서는 일반인들에게 종래의 종이기록보다 못 미더운 상황이므로 적절한 관리와 보장을 통하여 믿고 사용할 수 있도록 하는 것이 중요하다.

전자기록에서는 진본성・무결성이 취약할 수 있다는 점은 여러 연구와 자료에서 대체로 언급된 바 있다. 정리해 본다면 전자기록은 유체물이 아니므로 고정되지 아니할 우려가 있고, 품질저하 없이 위변조가 가능하기 때문에 위변조 사실을 파악하기 어렵고, 격리된 곳에 보관하지 않고 보통 시스템에 탑재하는데 그렇게 되면 여러 사람이 접근할 수 있으므로 위변조 기회가 상대적으로 많으며, 장치를 통하여 표현되어야만 사람이 육안 판독할 수 있으므로 (시스템의 자동 검증 기능을 믿지 못한다면) 위변조, 유실, 훼손, 뒤바뀌기 등의 사고를 알아채기 어렵다.

진본성과 무결성 개념은 기록관리에 대한 국제표준 ISO 15489에서 진본성, 무결성, 신뢰성, 가용성이라는 기록의 4가지 특성, 또는 4가지 요건을 정리한 이후 국내외 각종 학술연구나 공공사업, 법제도와 표준에 널리 인용되고 있지만, 두 개념간의 구별이 명확하지 않은 채 사용되는 경향이 있다. 이러한 혼란은 그에 대한 대비책을 마련하는 데에 있어서도 마찬가지의 혼란을 가져오고 있는 것으로 보인다. 결국 최종적인 기록 서비스의 입장에서 본다면 필요로 하는 사람에게 적시에 믿을 수 있고(진본성) 훼손되지 않은(무결성) 기록 정보를 제공할 수 있느냐가 중요하다고 판단된다. 따라서 본 논문에서는 불필요한 논란과 혼란을 줄이기 위하여 어원을 따져서 진본성을 "출처", 무결성

을 "훼손없음"으로 단순화시키고, 일단 주어진 기록정보의 출처를 확인할 수 있으려면 어떤 요소가 필요한지, 현행 국내방식이 이를 지원할 수 있는지, 그리고 임의의 전자기록물에 대하여 출처를 확인할 수 있으려면 어떠한 지원전략이 필요한지를 논의해 보고자 한다.

2. 출처확인의 현황과 과제

1) “진본성” 개념에서 “출처” 개념으로

진본성은 authenticity라는 영어 용어를 번역한 말이다. authenticity는 authentication과 함께 그리스어 αυθεντικός로부터 파생된 형용사 authentic(real or genuine)의 명사형이다. authentic은 즉 진짜, 원래(origin)를 그대로 재현, 또는 사실에 기반한다는 의미를 담고 있다.[1] authenticity는 authentic한 성질을 말하며 authentication은 특정 대상이 authentic한가를 입증하는 행위를 말한다. 그래서 IT 분야에서는 이 authentication이라는 용어를 “인증”이라는 말로 번역해 사용하고 있으며, 기록학계의 진본성에 국한되지 않고 사용자 인증, 출처 인증, 무결성 인증 등을 포괄하는 뜻으로 사용하고 있다. 실제로 기록정보화 사업을 수행하다 보면 기록학자와 IT학자 사이에 이러한 용어를 사이에 두고 오해

1) The New OXFORD American dictionary, 2nd ed., 2005
- made or done in the traditional or **original** way, or in a way that faithfully resembles and **origin**
- based on facts; accurate or reliable

가 종종 벌어지는 일이 있다.

무결성은 integrity를 번역한 말이다. integrity란 라틴어 integritas(complete and not damaged)로부터 파생된 말로서 온전하다, 완전무결하다, 통일성이 있다, 보전되었다를 의미한다.[2] IT분야에서도 동일하게 "무결성"으로 번역하고는 있지만, 기록학계에서 주로 위변조 없음을 의미하는데 비하여 IT분야에서는 주로 오류성의 값이 없음을 의미한다. 마찬가지로 기록학자와 IT학자 사이에 오해가 벌어질 소지가 많다.

국제표준 ISO 15489에서 진본성[3]과 무결성[4]을 설명하는 내용은 서로 일부 중첩된다. 둘 다 무단 변경을 불허하며, 적법한 변경 이력을 추적할 수 있어야 한다. 국내에서는 전자기록의 인증

---

2) Ibid
- the state of being whole and undevided; the condition of being unified, uninpaired, or sound in construction
- internal consistency or **lack of corruption** in electronic data

3) ISO 15489-1:2001
- An authentic record is one that can be proven
  a) to be what it purports to be,
  b) to have been created or sent by the person purported to have created or sent it, and
  c) to have been created or sent at the time purported.

  To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are **protected against unauthorized** addition, deletion, alteration, use and concealment.

4) ibid
- The integrity of a record refers to its being complete and unaltered. It is necessary that a record be **protected against unauthorized** alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

정보로서 전자서명 기법을 사용하는데, 전자서명의 효력을 진본성, 무결성, 또는 그 양자라고 혼란스럽게 설명하고 있는 것이 현실이다. 이러한 모든 혼란의 원인은 종이기록에 대한 개념을 전자기록에 그대로 적용하려고 했기 때문이다.

종이기록에서 진본성과 무결성의 개념을 구별하려면 진본성은 있는데 무결성은 취약한 경우와, 반대로 진본성은 취약하고 무결성은 확실한 경우를 상정해 보면 이해가 가능하다. 종이가 그때 그 문건은 맞는데, 일부 훼손되어 내용이 완전히 판독되지 않는 예가 전자에 속한다. 문건의 내용이 완전히 판독되는데, 이 문건의 출처가 불확실하면 후자에 속한다. 그러므로 종기기록에서 진본성과 무결성은 각기 독립적인 성질이라고 볼 수 있다. 전자기록의 경우에는 어떠한가 살펴보자. 전자기록은 육안판독으로 진본성을 확인하는 것이 아니다. 진본성을 확인하는 정보도 디지털 이진값화 되어 전자기록 객체의 정보로 포함되는 것이다. 그러므로 이 진본확인 정보가 훼손되면(즉, 무결성 침해) 진본성도 침해되는 결과가 된다. 반면에 주어진 전자기록 객체의 정보가 처음 생산당시의 이진값 그대로가 아니라 할지라도, 그 변경된 이유가 전산환경변화에 맞추기 위한 마이그레이션이거나 기록관리 업무를 반영하여 보존기간이나 인수인계값 등 메타데이터를 고친 것이라고 한다면(즉, 적법한 행위라는 진본성 확인) 무결성이 침해되는 것이 아니다. 즉, 전자기록에서는 무결성이 “그대로 보존되고 있음”을 뜻하는 것이 아니며 그대로 보존되고 있지 않더라도 그 이유가 적법하다는 진본성 확인이 된다면 무결성은 유지된다고 보아야 하고, 반대로 전자기록의 진본성은 진본확인값이 무결하게 유지되고 있다는 확인이 될때 비로소 진본성이 유지된다고 볼 수 있게 된다.[5]

5) 진본확인용 이진값은 그 자체로 마이그레이션, 기록관리업무 누적 등에 의하여

이 논의의 결과는 이렇다. 전자기록에서도 “진본성”과 “무결성”은 바람직한 특성이기는 하지만, 한쪽의 확인을 위해서는 다른 한쪽의 확인이 필요하게 되는 순환속에 빠지게 되어 각기 독립적으로 추구하기에는 곤란하다는 것이다. 지금까지는 이러한 사실을 간과하였기 때문에 많은 혼란이 있었고 이러한 논의가 전자기록을 어렵게 느끼게 하는 요인이 되었다는 것이 저자의 판단이다. 결국은 기록 수요자를 위한 보존이며 관리일 테이므로, 수요자의 입장에서 되돌아보자, 복잡한 이론을 떼 버리고 핵심에 집중해 보자는 것이다. 지금까지의 관리자(공급자) 입장이 아니라 최종 수요자의 관점에서 바라본다면, “지금 내 앞에 놓인 이 기록을 과연 믿고 사용해도 된다는 것인지?”가 중요할 것이다. 이를 위하여 기록관리자는 미리미리 대비하여야 한다. “그럼 어떻게 해 주면 일반인 기록수요자들이 기록들을 믿고 사용하도록 해 줄 수 있을까”가 되어야 할 것이다. 개별 방법의 논의가 아니라, 그 방법들의 총합적 효과가 과연 원하는 “목표 달성”을 이루는지를 살펴 보아야 할 것이다.

기록 사용자의 입장에서는 '주어진 기록이 진짜인가', '내용이 온전하게 남아있는가'일 것이다. 이러한 이해를 바탕으로 하여 본 논문에서는 전자기록 분야에서 혼란스러운 진본성, 무결성 개념 대신 출처와 훼손없음 개념으로 대치해 생각하는 것이 이슈를 단순화시키며 사용자의 직관적 기대치에 더 부응된다고 판단하였다.

또다른 국제표준 ISO 14721에서도 이와 같은 견해를 뒷받침하고 있다. 그림 1에서 보는 바와 같이 ISO 14721 OAIS 참조모델의

적법하게 변경될 수 있다. 따라서 진본확인값의 무결성 확인 자체도 기록물의 무결성 확인과 마찬가지로 “값 자체의 그대로 보존”이 아니라 “변경 이력의 진본성 확인”이라고 재귀적으로 정의되어야 함에 유의하여야 한다.

정보 패키지 모델에는 보존 기술 정보(Preservation Description Information) 블록이 있고 여기에는 Provenance Information(유래 정보)와 Fixity Information(고정화 정보)가 들어있다. Provenance Information은 기록 내용의 출처(origin)와 그 이후의 이력을 표현하며,[6] Fixity Information은 오류 검출 방식을 이용하여 기록 정보가 변형되지 않았다는 무결성 검사 또는 검증을 할 수 있는 정보를 표현한다.[7]

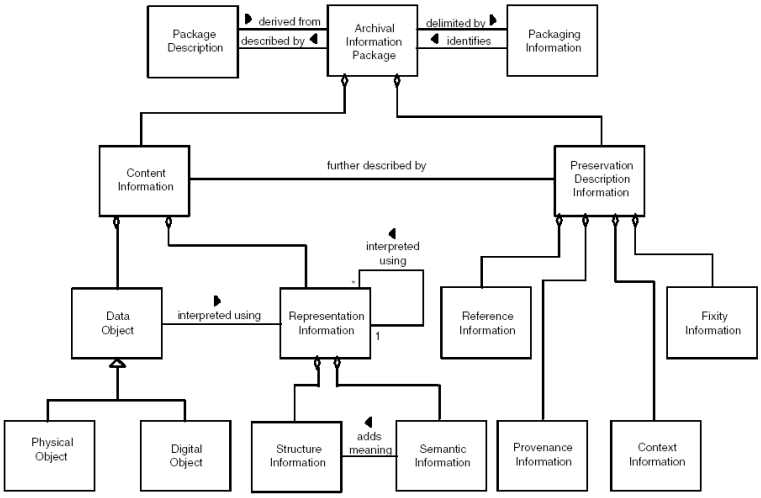
---

6) ISO 14721:2003, p.79

- Provenance Information: This information documents the history of the Content Information. This tells the **origin or source** of the Content Information, any changes that may have taken place since it was originated, and who has had custody of it since it was originated. This gives future users some assurance as to the likely reliability of the Content Information. Provenance can be viewed as a special type of context information.

7) ibid

- Fixity Information: This information provides the **Data Integrity checks or Validation/Verification keys** used to ensure that the particular Content Information object has not been altered in an undocumented manner. Fixity Information includes special encoding and **error detection schemes** that are specific to instances of Content Objects. Fixity Information does not include the integrity preserving mechanisms provided by the OAIS underlying services, error protection supplied by the media and device drivers used by Archival Storage. The Fixity Information may specify minimum quality of service requirements for these mechanisms.



〈그림 1〉 ISO 14721 OAIS 참조모델의 정보 패키지 모델 구성

이 모델에서는 즉 진본성보다는 유래를, 무결성보다는 고정(훼손없음)을 더 본질적인 요소로 파악하고 있음을 알 수 있다. 본 논문에서는 개념 구별을 확실하게 하기 위하여 전자기록의 첫 생성 기원을 출처(origin)로 부르고, 이를 포함하고 이력을 덧붙여 현재 기록에 이르기까지의 진본성 정보의 총칭을 유래(provenance)로 구별하였다.

2) 인증정보의 적용과 한계

현재 전자기록에 대한 진본성·무결성 보장 방법으로 대개 전자서명[8]을 이른바 "인증 정보"란 이름으로 사용하고 있다.[9]

8) RFC 4998: ERS(Evidence record syntax) 2007, Aug.

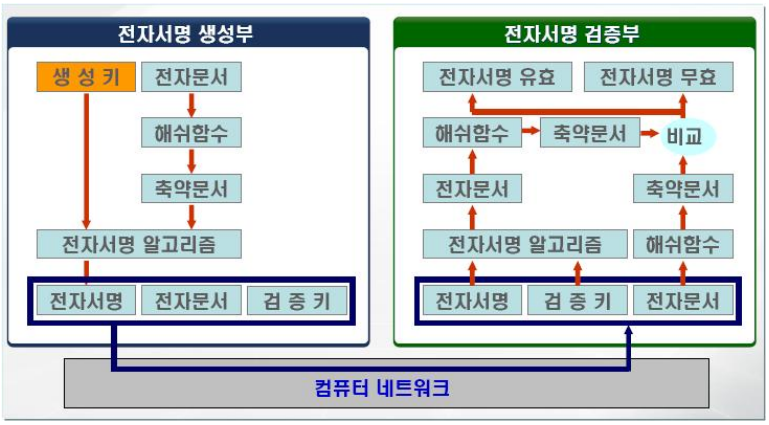
통칭 전자서명인 digital signature 기술은 비대칭 암호법, 즉 PKI 기술을 거꾸로 이용하는 것이다. 암호화를 하는 키(생성키)와 이를 복호화해서 해독하는 키(검증키)를 별개로 만들며 각 서명자에게 한쌍씩 제공한다. 서명자는 생성키를 자기만 알도록 가지고 있고, 자신이 암호화하는 메시지를 해독할 수 있는 검증키는 모든 사람에게 공개한다. 원래의 암호법은 전달하려는 메시지 자체를 은닉해서 해독키가 없으면 볼 수 없도록 하는 것이 목적인데, PKI는 암호화 대상 메시지 M의 내용 자체는 다들 알고 있어서 별 의미가 없고, 대신 동일한 M을 암호화한 결과는 사람마다 달라서, 공개되어 있는 해독 키들을 대입하여 B의 해독 키로는 M이 복원되지 않는데 A의 해독 키로는 원래대로 암호가 풀린다면 이 암호화는 A밖에는 수행할 수 없었음을 검증할 수 있다는 것이 핵심 아이디어이다.[10] 원문을 변조하면 전자서명이 일치하지 않게 되기 때문에 위변조를 확인할 수 있는 무결성 기능도 제공한다. 암호화 대상 메시지를 전자기록 전체로 잡는다면 암호화에 많은 시간이 걸리기 때문에 보통은 이를 정해진 방식으로 축약하여 축약값을 암호화하고, 이를 전자서명값이라고 하

- In many application areas of electronic data exchange, a non-repudiable proof of the existence of digital data must be possible. In some cases, this proof must survive the passage of long periods of time. An important example is digitally signed data. Digital signatures can be used to demonstrate **data integrity** and to perform **source authentication.**

9) 그런데 전자서명에 대한 국제표준 X.509에 따르면 한국어로 "전자서명"이라고 번역될 수 있는 용어가 하나가 아니고 두가지나 된다. 하나는 electronic signature인데 authentication, 즉 인증(신원확인 또는 진본성, 즉 출처)을 제공하는 일반적인 도구를 말하며, 다른 하나는 digital signature로서 source(출처)와 integrity(무결성)을 증명할 수 있는 특정 기술을 말한다. 말 그대로 번역한다면 전자가 "전자서명", 후자가 "디지털 서명"이 되겠는데 전자기록의 인증정보로 사용되는 전자서명이란 후자를 말한다.

10) 그래서 공개키 기반(Public-Key Infrastructure)라고 하는 것이다.

여 원본 기록에 부착시켜 유통시킨다. 이러한 비공개 생성키 - 공개 해독키는 외부의 공인된 인증기관이 발급하고 보증해 주며, 발급을 위하여 전자서명에 필요한 키, 명의, 유효기간 등 각종 정보를 공식적인 배포파일로 만들어 주는데 이를 공인인증서라고 한다. 그러므로 전자서명이라는 말은 종래의 친필서명과 기능적으로 동등하기 때문에 붙여진 이름이지[11] 눈으로 확인이 가능한 표식은 아니다. 그 개념은 그림 2와 같다.



〈그림 2〉 전자서명의 생성과 검증

전자서명이 이른바 출처(진본성)과 무결성을 증명하는 기능이 있다고 말들을 하지만, 이것은 전자서명을 한 기관이나 사람의

11) 김영진, "인터넷 환경에서의 보안기술(전자서명)", 국가기록원 2008 보존복원 기술세미나 (주)드림시큐리티 발표자료, p. 566
- 전자서명의 요구조건 1) 위조불가: 생성 키를 소유하지 않은 자는 전자서명 생성불가 2) 변경 불가: 생성 키를 소유하지 않은 자는 전자문서 변경불가 3) 서명자 인증: 생성 키를 소유한 자가 전자서명의 행위자임 4) 재사용불가: A 문서의 전자서명을 B문서의 전자서명으로 대치불가 5) 부인불가: 생성 키의 소유자가 전자서명 후에 행위에 대한 부인불가

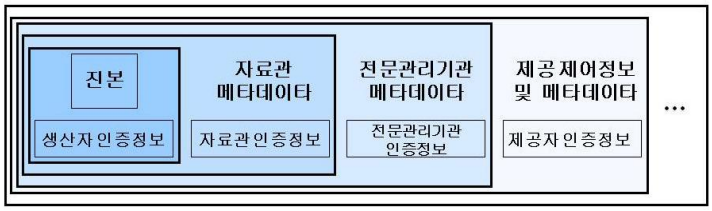
명의로 된 서명이 있다고 보며(진본성), 서명 이후에 그 내용이 변경되지 않았다는 추정(무결성)이라는 개념으로서의 진본성, 무결성 개념이다.[12] 이는 데이터 이진값 자체에 대해 문자 그대로 명의와 내용을 동결하는 기계적인 진본성, 무결성으로서, 우리가 추구하는, 기록관리 업무중 계속 수정이 이루어지면서도 유지시키는, 더 상위의 내용상의 진본성 무결성을 그대로 보장하는 것은 아님에 유의하여야 한다.

종이기록은 그대로 보존하는 것이 목표이지만 "전자기록은 그대로 보존하면 보존되지 않는다." 기록관리업무가 메타데이터에 반영되어야 하기 때문이기도 하며, 보존처리를 위하여 변환되기 때문이기도 하고, 긴 세월 속에서 계속해서 변화・발전되는 기술과 환경, 기록관리 방법에 맞추려면 최소한의 마이그레이션이 일어날 수 밖에 없기 때문이기도 하다. 전자기록의 보존은 계속적인 수정・변환을 수반하는데, 이 수정・변환이력을 유지하기 위해서는 호주 VERS에서 사용되고 한국 표준에서 인용된 "양파모델(onion model)"과 같이 이전 객체에 수정・변환 정보를 덧씌우는 방식으로 “수정된 전자기록 객체”를 만듦으로써 껍질이 계속 생길 수 있고, 그 수정・변환 작업이 적법한 양태, 적법한 담당자, 적법한 시기에 이루어졌음을 증명하기 위해서는 각 껍질에 대해서 전자서명을 누적시키는 것이 필요할 수 있다.(그림 3)[13] 그러므로 출처 확인의 입장에서 볼 때 전자서명은

12) 전자정부법[시행 2010. 5. 5][법률 제10012호] 제29조(행정전자서명의 인증)
② 중앙사무관장기관의 장은 행정전자서명에 대한 인증업무를 수행한다.
④ 제2항에 따라 인증받은 행정전자서명이 있는 경우에는 그 행정전자서명을 전자문서에 표시된 행정기관 및 공공기관의 관인・공인 또는 해당 기관에서 직접 업무를 담당하는 사람의 서명이 있는 것으로 보며, 그 전자문서는 행정전자서명이 된 후에 그 내용이 변경되지 아니하였다고 추정한다.

13) 송병호, “진본성 확보를 위한 전자기록물 관리방안”, 한국비블리아학회지 제16권2호, 2005, 12. p.52

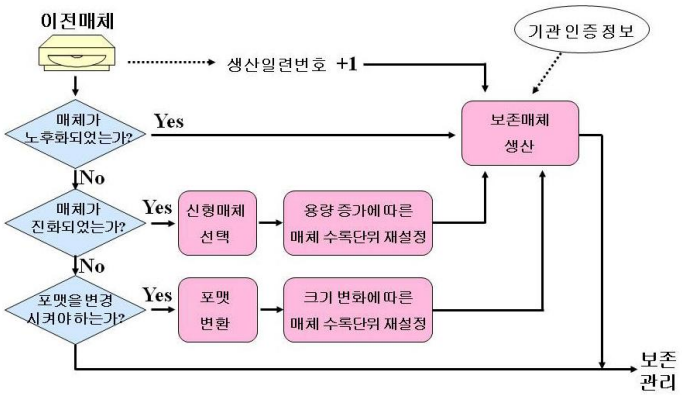
그러한 생산・수정・변환 이력을 발생시킨 각 당사자의 명의로 된 여러 전자서명의 연속이라는 유자 정보 체인으로 구성될 필요가 있다.



〈그림 3〉 양파껍질 모델의 예시

전자기록은 물리적 실체가 없으므로 보존매체가 필요하다. 보존매체는 내용 보호를 위하여 보통 한번 기록하고는 다시는 변경시킬 수 없는 WORM(Write-Once, Read-Many) 매체를 사용하고 있기 때문에 전자기록 객체가 수정・변환되면 새로 보존매체를 구성할 수밖에 없다. 매체 자체의 진화에 따른 신형매체 이전이나 매체 노후화에 따른 재생산(리프레시)도 고려하면 그림 4와 같이 보존매체도 긴 세월 속에서 계속적인 변환생산이 필요해진다.[14] 이때 보존매체 자체의 진본성・무결성 보장이 필요할 수 있는데 그럴 경우에는 매체에 수록된 개별 전자기록 객체에 적용되는 전자서명 인증 체인과는 별도로, 매체 자체에 대해서도 변환생산 이력을 증명하는 전자서명 인증체인이 필요할 수 있다.

14) 송병호, “전자기록물을 위한 보존매체의 관리”, 한국문헌정보학회지 제39권4호, 2005, 12. p.188



〈그림 4〉 보존매체 변환 개념의 예

이러한 인증정보 누적문제를 가중화시키는 또다른 요인은 전자서명의 유효기간 문제이다. 만일 전자서명을 검증하기 위한 인증서가 1년(민간 공인인증서 전자서명)이나 2년 3개월(행정전자서명)과 같은 유효기간 제한이 있다고 하면 장기 보존중인 전자기록에 과거로부터 누적되어 가해진 이 여러 껍질의 전자서명 하나하나에 대하여 주기적인 재 전자서명을 하는 등으로 유효기간을 늘일 방법을 찾아야 할 것이다.(2장 4절 4항 참조) 보존이 장기화되면 시간경과에 따라 생산·수정·변환 이력 단계별 누적 전자서명과, 그 각각에 대한 유효기간 연장용 주기적 재서명값이라는 식으로 누적된 인증정보가 산처럼 쌓여, 정작 진본성 및 무결성의 증명이 필요할 경우가 되었을 때 검증해 보아야 할 것이 너무나 많아지게 되는 문제가 생기는데, 여기에 대한 명확한 문제제기와 해법은 아직 제안되지 않은 실정이다.

이러한 이유들이 있기 때문에 비록 전자서명 기술이 진본성·무결성 증명을 다 할 수 있는 기본 기능이 있다 하더라도 실제 국외의 전자기록관리에서는 "무결성" 증명을 위해서 사용

하고 있는 것이 현실이다(VERS, ISO 14721 등). 국내에서는 막연한 기대감으로 진본성・무결성을 모두 지원한다고 생각하는건 아닌지 되돌아 보아야 할 것이다.

또한, 전자서명은 진본성・무결성을 증명, 즉 "검증"할 수 있는 전자적 첨가물에 불과한 것이고 그 자체로 진본성・무결성을 유지시켜 주고 "보장"해 주는 것은 아닌 데에 주의하여야 한다.[15] 전자서명값과 서명대상 정보객체와의 관계는 비유하자면 마치 중요한 상품에 한번 열면 다시는 닫히지 않는 포장을 한 것과 같다. 포장이 뜯기지 않는 것을 보고 상품이 한 번도 사용되지 않은 신품인 것을 "검증"할 수 있는 것과 같이 전자서명값이 전자기록과 일치하는지를 확인함으로써 우리는 해당 전자기록 객체가 서명 이후 한 비트도 변경되지 않았으며(무결성 확인) 이를 확인한 서명자는 다른사람이 될수 없고 해당 전자서명 권한자일 수밖에 없음을 확인할 수 있다(진본성 확인). 그러나 그러한 포장이 상품을 다른 사람이 뜯고 사용하지 못하도록 "막을 수" 수 없는 것과 같이 전자서명도 마찬가지이다. 전자서명 확인을 해 본 결과 검증에 이상이 없었으면 별문제가 없겠지만 일단 검증이 실패라는 결과를 내게 되면, 이 기록을 그대로 사용해도 될지, 원래 기록은 어디서 구해와야 할지 등에 대한 대책이 자동으로 만들어지는 것이 아니다. 호주 빅토리아 주의 VERS의 경우에는 전자서명을 보관중인 전자기록의 무결성을 증명하는 데이터로 사용하고, 이와는 별도로 전자기록 하나하나에 대하여 오류검출코드를 추출하여 이것에서 오류가 검출되면 상시 연동하고 있는 거울영상본(mirror image)으로부터 원본을 실시간 복구시키는 방법으로 무결성을 유지・보장한다.[16] 원본-진

15) Filip Boudrez, "Digital signature and electronic records", Arch Sci. 2007, 7. pp. 179-193

본에 대한 걱정이 우리나라보다 적은 서양의 마인드로는 이걸로 괜찮을 것이다.

국내의 경우에는 전자기록에 전자서명을 하여 보존하다가, 사용할 때가 되면 그 전자서명을 검증하여 올바르면 진본이라고 선언한다. 그러나 그뿐으로, 진본이 아니라고 나오거나 정보가 불충분하다고 할 경우는 어떻게 할 것인가에 대한 대비책이 불분명하다. 한국에서는 문서 위조가 항상 걱정거리이기 때문에 무결성은 어떻든지 간에 진본성을 좀더 단순화한 "출처"를 증명할 수 있는 방법을 생각해 보자는 것이 본 고의 취지이다.

3) 국내 전자기록 관리방법의 출처확인 기능분석

국내의 인증 방법으로 국가기록원의 공공기록물 장기보존포맷, 지식경제부 정보통신산업진흥원의 공인전자문서보관소 전자문서패키지와 증명서 규격, 행정안전부 전자문서유통센터의 진본성확보 및 검증시스템, 국가기록원의 전자기록물 전자서명 장기검증관리체계, 그리고 국가기록원의 기록관리 기능이나 운용절차를 살펴 본다.

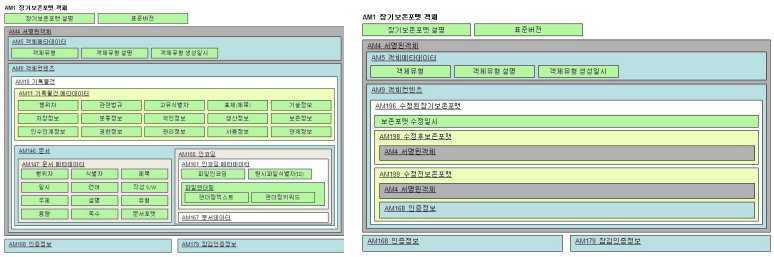
(1) 국가기록원의 공공기록물 장기보존포맷

공공표준으로 제정된 장기보존포맷[17]은 기록물철, 기록물건, 그리고 수정된기록물에 대한 포맷으로 개발되었으며 그 구성은 그림 5와 같다.

---

16) Howard Quenault, "VERS Background & VEOs", 국가기록원 기록관리시스템 혁신 정보화전략계획(ISP) 수립을 위한 선진사례 해외 벤치마킹 호주 빅토리아주 설명자료, 2005, 10.

17) 국가기록원 표준 NAK-P-2008-05 전자기록물 장기보존포맷 기술규격, 2008



〈그림 5〉 국내표준 장기보존포맷의 구조도(기록물건의 예)

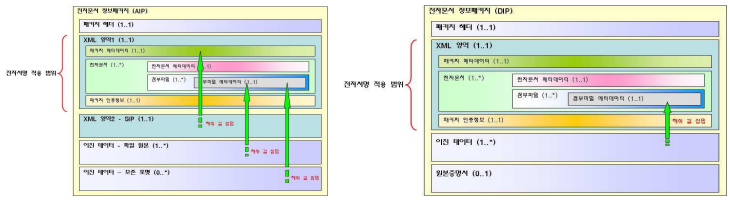
그림 5의 왼쪽 그림은 기록물건에 대한 장기보존포맷이다. 전자서명을 이중으로 적용하여 어느 일방의 마음대로 기록물을 변경 악용할 여지를 막는다. 생성 기록물관리기관의 명의로 된 인증서로 전자서명한 내용을 "인증정보", 생성 시스템에 부여한 인증서로 전자서명한 내용을 "잠김인증정보"라고 부른다. 세월이 흘러 기록물을 변경할 필요가 있을 경우에는 오른쪽 그림과 같이 양파모델을 적용하여 수정전 기록 객체를 그 이중 전자서명과 함께 그대로 보존하면서 여기에 수정후 개록객체를 병기하고 이 전체에 대하여 다시 이중 전자서명한다.

비판: 진본성, 즉 출처확인이 가능하려면 행위자 명의의 전자서명이 첨부되어야 하는데, 본 표준에서는 기록물관리기관 및 시스템 명의의 전자서명이 적용되었기 때문에 당초 의도에 상관없이 출처확인보다는 무결성 검증용이 되어 버렸다. 어느 일방의 단독 변경을 막기 위한 이중 전자서명은 상호 독립적인 명의여야 하는데, 기록관리기관과 그 구동 시스템 명의가 됨으로써 이 두 가지에 모두 접근 가능한 내부관계자의 악용 여지가 남아있다. 생성 당시부터 최근까지의 인증 이력이 여러 껍질로 분산되어 있어 그 체인 전체를 검증하기 곤란하며, 통상 마지막 인증정보만 검증함으로써 기껏 남겨놓은 수정전 인증정보 검증

을 소홀이 하는 오류를 범할 수 있다.

(2) 정보통신산업진흥원(구, 한국전자거래진흥원)의 공인전자문서 보관소 표준

고객이 제3자에게 위탁 보관하게 함으로써 거래당사자간에 전자문서에 대한 신뢰성을 확보할 수 있도록 하는 제도가 공인전자문서보관소 제도이다. 공인전자문서보관소는 ISO 14721의 세가지 정보패키지, 즉 신청정보패키지(SIP), 보존정보패키지(AIP), 배부정보패키지(DIP)의 세가지 포맷을 지원한다. 보존정보패키지의 구성은 그림 6의 오른쪽과 같다.[18] 전자서명의 범위는 XML 영역에만 한정하여 적용한다. 첨부 파일에 대해서는 해시(해쉬) 알고리즘을 이용하여 해쉬 값을 생성한 다음 XML 영역의 메타데이타에 삽입하는 것으로 끝나며, 첨부 파일에까지 전자서명의 범위에 포함시키지 않는다. 이러한 원칙에 따라 보존정보패키지는 XML 영역1만을 전자서명 적용범위로 한정한다. XML 영역 2는 이관시(SIP)의 XML 영역인데, 이를 첨부파일로 보고 동일한 방식으로 해시값을 생성하여 XML 영역1의 패키지 메타데이타에 삽입하는 방식을 취한다.



〈그림 6〉 공인전자문서보관소 표준 보존정보패키지와 배부정보패키지 구성도

18) 한국전자거래진흥원, 전자문서패키지 기술규격, 2006, 11.

배부정보패키지는 보관소에서 보관하고 있는 보존정보패키지를 사용자가 요청한 조건에 따라 열람이나 발급받을 수 있는 형태로 생산하여 사용자에게 전송하는 패키지로서, 구성은 그림 6의 오른쪽과 같다.[19] 전자문서의 원본과 변환본을 이용하여 원본증명서를 생성한 후 배부정보패키지에 첨부하여 사용자에게 전달한다. 그림의 이진 데이타 영역은 원본이나 장기보존본, 또는 업무활용본으로 다양하게 구성이 가능하다. 배부정보패키지의 경우에는 이진 데이타 다음에 첨부되는 원본증명서가 자체의 무결성 및 부인방지 기능을 제공하므로, 원본증명서의 해쉬값을 XML 영역의 메타데이타에 삽입하지 않는다.

한계점: 기본적으로 공인전자문서보관소가 보관한다는 사실 자체를 신뢰의 기반으로 삼고 있다. 전자문서 원본에 해당하는 "첨부 파일"에 전자서명 인증을 하지 않으며 그 축약값만 인증대상물에 삽입시킴으로서 결국은 부인방지 등의 전자서명 역할이 아니라 단순한 오류검증코드 역할을 하게 됨으로써 신뢰도 수준이 그만큼 저하된다. 보관중인 전자문서의 무결성은 대신 WORM 매체에 저장한다는 것으로 확보한다. 진본성, 즉 출처확인은 보관소 명의의 원본증명서로 보장하는 체계이다. 변환이력을 검증 관리하지 않으며, 전자서명의 유효기간 극복방안은 명시적으로 정의된 바가 없다.[20]

---

19) 한국전자거래진흥원, 전자문서 증명서 포맷 및 운용절차 기술규격, 2006, 11

20) 한국전자거래진흥원, 공인전자문서보관소 기술관련 이슈목록, 2006. 9. pp.49-50.
"전자문서에 삽입된 전자서명에 대한 장기검증에 대한 이슈"

(3) 행정안전부 정부전자문서유통센터의 전자문서 진본성 확보 및 검증시스템

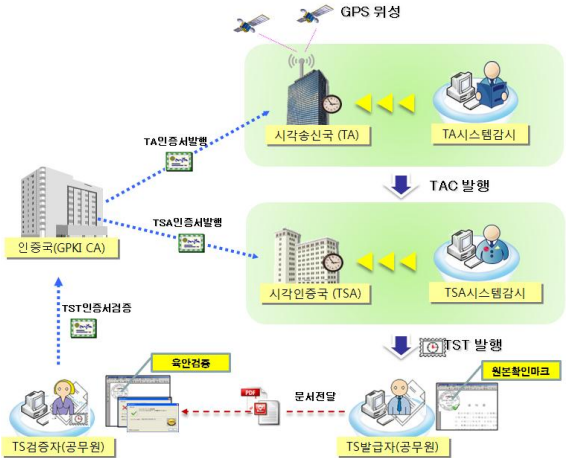
행정안전부 정부전자문서유통센터는 공공기관간에 전자적으로 공문서를 주고받는 유통망을 지원하고 있다. 그런데 종래에는 전자문서 위변조 방지가 시스템 내부 및 시스템간 연동기술에 의하여 보장되고 있었기 때문에, 시스템에서 벗어난 공무원 개인 업무영역에서는 그림 7에서 보는 바와 같이 진본성이 보장되지 않고, 또 시스템을 이용하지 않고 유통되는 e-mail 첨부 전자문서의 경우에도 별도의 위변조 방지 장치가 없어, 발신자가 보낸 문서에 대한 진본 여부를 검증할 방법이 없었다.

〈그림 7〉 종래의 전자문서유통 보안성 취약구간

아이디어는, 문서를 생성할 때 외부의 독립된 신뢰성있는 시각확인 및 시각정보발급 시스템으로부터 타임스탬프 토큰(시각정보를 담은 전자서명)을 받아 HWP 및 PDF 전자파일 내에 삽입해 놓아서, 해당 전자문서를 수신한 사람이 뷰어를 통해 열면 뷰어 속의 검증장치가 전자문서내의 타임스탬프토큰 정보를 확인하고 육안식별이 가능하도록 원본증명마크를 표시해 준다는 것이다.[21] 전체적인 발급 및 검증 흐름은 그림 8과 같다. 이 기술은 현재 정부통합민원포털(www.g4c.go.kr)에서 발급하는 온라인

21) 행정안전부, "전자문서 진본성 확보 및 검증시스템 구축 사업계획서(안)", 2008, 5.

민원서류 등 공공 전자문서유통에 많이 사용되고 있다.



〈그림 8〉 타임스탬프 발급 및 검증체계

비판: 외부공인기관이 "해당시점 이전에 그 전자기록이 존재했음을 증명"하는 형태의 서비스이다. 생산자의 전자서명이 아니기 때문에 출처를 증명하는 것이 아니라 존재시점을 증명하는 것으로 봄이 타당하다. 일반 전자문서에 내장시키는 것이기 때문에 기본적으로 내장이 가능하도록 허용된 문서포맷에만 적용될 수 있고 일정부분 원문 변환을 수반하여 원본성 훼손의 논란이 있을수 있다.. 해당문서가 기록관리시스템으로 이관되면 다시 여기에 (1)항의 국가기록원 표준 인증정보가 첨부되므로 두 인증정보간의 역할충돌 및 일관성 여부가 문제될 수 있다.

(4) 국가기록원의 전자기록물 전자서명 장기검증관리체계 프로젝트

전자기록에 첨부된 전자서명을 긴 세월 후에 검증해 보려면

해당 서명에 대한 검증키기 계속 유효하여야 한다. 그런데 이러한 정보를 제공하는 공인인증서는 유효기간이 몇 년에 불과하기 때문에 유효기간 경과후의 검증에는 인증기관이 그 결과에 책임을 지지 않는 문제가 있다. 국가기록원은 이를 해결하기 위하여 2007년 4월부터 동년 10월까지 6개월간 "전자기록물 전자서명 장기검증관리체계" 개발 사업을 실시하였고[22] 현재는 표준화되어[23] 광범위하게 적용되고 있다. 구체적으로는 그림 9처럼 "전자서명 장기검증 시스템", "원본 내용증명 시스템", "통합 전자서명관리 시스템"이라는 3가지 지원 시스템과 관련 연계모듈 등으로 구성되어 있다.

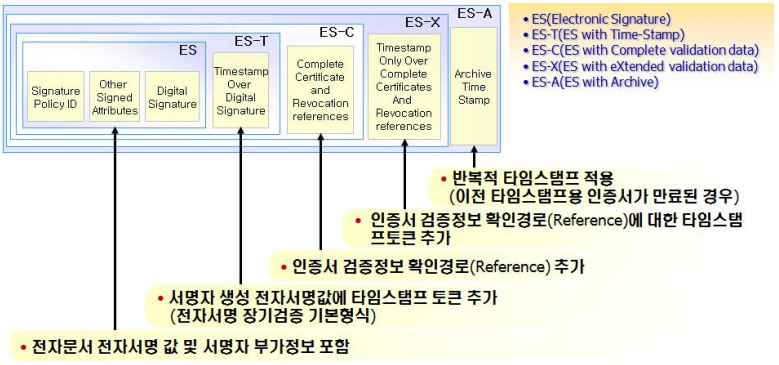
〈그림 9〉 전자기록물 전자서명 장기검증체계 추진 구성도

그 중에서 가장 핵심인 전자서명 장기검증 시스템을 살펴보

22) 국가기록원, "전자기록물 전자서명 장기검증관리체계 구축사업 완료보고회 자료", 2007, 11.
23) 국가기록원 표준 NAK-TS 4-1 2008 전자기록물 전자서명 인증서 장기검증 기술규격

자. 전자기록에 전자서명을 생성 첨부하고 보존하는 중에 전자서명의 유효기간이 끝나버리면 그 후로는 검증이 불가하므로 유효기간이 끝나기 전에 새 전자서명(여기에서는 타임스탬프)을 다시 발급받아 덧입히자는 것이다. 이를 계속 반복하면 가장 나중의, 그러나 아직 살아있는 전자서명이 그 직전의 전자서명을 입증하고, 이런 일을 시간 역순서로 하여 결국에는 최초의 생성시 전자서명이 입증된다는 논리이다. 그러므로 여기에는 각 전자서명의 시점이 중요하므로 공신력 있는 외부 시각정보시스템의 "타임스탬프"를 첨부하는 것이 중요하다.

이 아이디어의 출처는 국제 인터넷 표준화 기구 IETF(The Internet Engineering Task Force)의 RFC 3126인데, 원래의 방법은 그림 10처럼 최초의 기록물 전자서명에 타임스탬프를 누적시켜서 기록물 전자서명의 유효기간을 늘이는 것이었다.[24]



〈그림 10〉 RFC 3126의 전자서명 유효기간연장 개념

그런데 이 방법을 적용하면 모든 보존 기록물에 대하여 주기

24) IETF, RFC 3126: LTVS(Long-term electronic signature), 2001

적으로 양파껍질형태로 타임스탬프를 누적하여야 하고, 그에 필요한 전자기록 객체의 건수와 크기와 막대하게 증가한다는 것을 부담으로 여겨 연구팀은 간략화된 수정 아이디어를 채택하였다. 즉 기록물 건별로 유효기간을 연장하는 것이 아니라, 중앙 인증기관에서 매일 공시하는 인증서 폐기목록을 계속 수집하여 장기보존한다는 것이다. 검증할 때에는 전자기록의 전자서명에 해당하는 인증서가 서명당시 유효기간 안에 있으면서 당시 인증서 폐기목록에 없었으면, 유효한 전자서명으로 인정한다. 기록물 건수보다 수집되는 인증서 폐기목록이 훨씬 수량이 적기 때문에 효율적이라는 것이다.

〈그림 11〉 국가기록원의 장기검증방법 수정 아이디어

이밖에 "원본 내용증명 시스템"은 열람 제공되는 전자기록 내용이 기록원 원문과 동일함을 증명하는 원문내용증명서를 발급하는 시스템이며, "통합 전자서명관리 시스템"은 국가기록원 내에 중앙영구기록관리시스템(CAMS) 등 전자서명 활용 시스템이 여러개인데 이들 각각이 전자서명작업을 수행하면 전자서명키

에 대한 관리가 소홀할 수 있다고 보고 이들 모두를 독립적 운영이 가능한 통합 전자서명관리 서버를 통해 수행하도록 만든 시스템이다.

비판: 국제표준 RFC 3126을 따르지 않은 비표준으로서 그 정확성에 대한 신뢰성이 높지 않다. 유효기간을 직접 연장하지 않고 간접 연장하여, 결과적으로 기록의 검증효력을 늘인 것이 아니라 그동안 발급되었던 인증서의 검증효력을 늘였다. 이는 종이기록으로 비유하자면 당시 찍은 도장 낙인(인영)이 진짜임을 증명하는 것이 아니고 그때 사용했던 도장 자체가 진짜임을 증명하는 것으로서, 10년 전에 문서 하나를 위조하고 100년전 유효했던 도장을 찍어서 100년전 기록이라고 주장하는 식의 공격을 받을 수 있다. 그래서 이 표준을 국가기록관리위원회에서 최종 심의할 당시, 저자는 이 문제를 제기하여 표준의 이름을 당초 "전자기록물 전자서명 장기검증 기술규격"에서 "전자기록물 전자서명 인증서 장기검증 기술규격"으로 바꾸도록 하였다.[25] 인증서를 장기검증하는 방식도 인증서 건 자체를 직접 증명하는 것이 아니고 24시간마다 공시되는 폐기목록에 없으면 유효하다는 간접방식을 이용하고 있기 때문에 신뢰도는 그만큼 떨어진다. 원본 내용증명 시스템은 기록원이 관리한 자료를 기록원 스스로 원본증명하는 것이 타당한지 문제제기가 가능하며, 기본적으로 "등기취급을 전제로 ...(중간생략)... 발송인이 수취인에게 어떤 내용의 문서를 언제 발송하였다는 사실을 우체국이 증명"하는 내용증명[26] 기능이라기 보다는, 사본을 제작하여 제공하면서 보관중인 원본과 같다는 "원본대조필"을 찍어주는 것

25) 국가기록원, “국가기록관리위원회 제5차 정기회 회의 결과 보고”, 2008, 10.
26) 우편법 시행규칙 [시행 2008. 3. 3] [지식경제부령 제1호, 2008. 3. 3, 타법개정] 제25조제1항제4호 가목

과 유사하다고 볼 수 있다. 통합 전자서명관리 시스템은 각자가 자기 책임하에 전자서명을 하여야 함에도 중앙에서 대행하여 일괄 서명하는 것과 같기 때문에 책임소재를 불분명하게 만들어 진본성을 훼손한다는 문제제기가 가능하다.

(5) 국가기록원의 기록관리시스템 기능 및 표준 운용절차

국가기록원의 표준에서 이관, 보존처리, 열람검색 등 중요한 시기마다 출처확인을 하도록 명시하는지를 살펴 보았다. 국가기록원에서 표준화한 기록관리시스템은 RMS와 CAMS가 있다. RMS 표준을 살펴 보면 중요한 인증정보 탑재・재생성 시점이 명시되어 있지 않고 탑재된 인증정보를 검증할 시기와 방법도 명시되어 있지 않다.[27] CAMS 표준을 살펴 보면 기록물 포맷을 변환하기 전・후에 무결성을 검증하라는 정도의 내용은 있으나 진본성(출처확인) 내용에 대해서는 언급이 없으며 기록정보를 검색 제공할 때 등 다른 중요한 시점에 검증을 요구하는 내용도 미비하다.[28] 이밖에 영구기록물관리기관 표준운영절차의 경우에는, 진본성과 무결성을 위한 정보를 관리하고 유지하라는 요건은 명시되어 있으나 정작 관리되고 있는 그 정보들을 언제 어떻게 검증하라는 내용은 인수시에 대하여 간략히 언급된 것 외에는 미비하다.[29]

---

27) 국가기록원 표준 NAK-S 6 2007 기록관리시스템 기능요건 표준
- 2.1.12. 기록물을 인수하였을 때에는 인수전 기록물과 인수후 기록물이 일치하는지를 검증하는 기능을 지원해야 한다. 일치하지 않는 경우 그 검증의 결과를 포함하여 관련부서 또는 사용자에게 경고할 수 있어야 한다(M) 등 추상적이고 평이한 내용으로 기능요건이 이루어져 있다.

28) 국가기록원 표준 NAK-S 7 2008 영구기록관리시스템 기능요건

29) 국가기록원 표준 NAK-S 9 2008 영구기록물관리기관 표준운영절차. 7장 "전자기록관리 및 전산화"

4) 출처확인 필요요소

앞에서 살펴 본 바와 같이 현행 방법들은 출처확인 또는 진본성 확인에 필요한 정보가 정확히 규명되어 있지 않고, 기록관리 과정 중에서 이러한 정보를 수시로 확인, 관리, 보정하는 기능이 결여되어 있으며, 사용할 때 확인을 반드시 하여야 함에도 철저한 요건화에 실패하고 확인 절차의 명시가 미흡하다. 그리고 확인이 안될 경우에 대한 대응책이 미비하다. 출처확인 또는 책임소재를 가리는 데에 사용되어야 할 전자서명이 정작 그 기록 출처와 직접 관련이 없는 명의의 전자서명인 경우가 많다.

따라서 전자기록의 출처 확인이 가능하려면, 첫째 출처 정보를 정확히 명시하여야 하며, 둘째 출처 정보를 잘 관리하여야 하고, 셋째 수요자가 사용하려고 할 때 전자기록을 신뢰할 수 있도록 그 출처를 확인하여야 함을 요건화하고 수행 방법을 정하며, 넷째 출처가 확인되지 않을 경우에 대한 대응책을 마련해 놓아야 한다.

(1) 출처 정보의 정확한 명시

출처 정보는 적어도 "누가", "언제" 이 기록을 생성하였는지에 관한 정보를 포함하여야 한다. "누가" 즉 "명의"는 전자기록의 경우 ① 사람으로서의 담당자 명의거나, ② 담당 시스템 명의가 될 수 있겠지만, 법적인 행위주체는 사람이므로 ① 담당자 명의를 명시하는 것이 차후 그 기록을 가지고 과거를 판단할 때 책임소재를 판단하는 데에 더 적절할 것이다. 그런 의미에서 국가기록원 장기보존포맷의 잠김인증정보는 시스템의 전자서명이므로 개편하는 것이 좋을 것이다. 만일 처리 시스템을 명기하고

싶은 경우라도 시스템 자체의 전자서명이 아니라 그 시스템을 책임지는 사람의 전자서명이 더 바람직할 것이다.

경우에 따라서는 담당자 명의 대신 담당기관의 명의로 대체하는 것도 고려할 수 있다. 그 이유는 전문기록관리기관 등의 경우 최종적인 관리 책임은 그 기관이 지는 것이지 과거 근무하였던 개인이 지는 것이 아니기 때문이다. 개인을 추적하는 것보다는 상대적으로 변동성과 수량이 적은 기관을 추적하는 것이 효율적일 수도 있다.[30] 개인 대신 기관 명의로 출처 정보를 명시할 때에는, 대외적으로는 그 기관이 책임을 지지만 더 정확인 출처확인을 위해서 기관 스스로는 각 개인에 의한 행위명세를 내부적으로 기록하여 보존하고 있어서 언제든 소명요청에 응할 수 있어야 할 것이다.

"명의" 정보의 구체적인 양식을 제한할 필요는 없겠지만 최소한의 포함정보는 규정해 둘 필요가 있다. 왜냐하면 대개의 경우 담당자의 소속, 이름, 직위, 사용자 ID, 연락처 등으로 구성하고 있기 때문이다.[31] 이 정보만로는 긴 세월이 지난 후 담당자 개인을 추적하여 특정인으로 적시하기 곤란하다. 연락처 정보는 현재에나 의미있지 미래에는 무의미한 정보이며 소속 직위나 사용자 ID도 마찬가지이기 때문이다. 장기보존을 위한 메타데이터가 이처럼 현재적 시각에 의한 정보로 구성된다는 것은 문제가 있다. 이보다는 주민등록번호 등 장기적이고 고유성을 보장받을 수 있는 정보로 "명의" 정보가 구성되어야 할 것이다. 물론 주민등록번호가 부여되지 않는 대상자를 고려하여야 하고, 또 그 사람의 신원을 확인할 수 있어야 하기 때문에 실제로 기

30) 송병호, “진본성 확보를 위한 전자기록물 관리방안”
31) 국가기록원 표준 NAK-A-2007-06 기록관리 메타데이터 표준: 비현용 기록물용, p.13

록관리에 적용할 때에는 좀더 정교한 고려가 필요하다.

"언제", 즉 "시기" 정보도 누가 어느 시기에 보아도 해석이 가능한 형태로 구성되어야 한다. 현행 메타데이터 표준[32]의 일시(DATE) 형태도 가능한 방안의 하나일 것이다. 어떤 형태이든 각 기록의 생산시각이나 기록관리행위 사건의 선후관계를 확인할 수 있도록 유일한 값이 되도록 고려할 필요가 있다. 예를 들어 전자기록 생산시스템의 속도가 고속이어서 생산일시 값이 동일한 경우가 발생되어서는 곤란한 경우가 발생할 수 있다.

이 두 가지 정보항목 이외에 "어느 맥락에서", "어떤 근거로" 등의 정보가 출처 정보에 더 포함될 수 있겠지만 이러한 정보는 더 복잡·모호하며, 앞의 두 정보를 구성하는 방법에 따라서는 상당부분 포함이 가능하기 때문에 생략하기로 한다. 앞의 "명의", "시기" 두 가지 정보만 잘 관리된다면 최소한의 출처확인은 실현될 수 있을 것이다.

만일 출처 정보의 신뢰도가 중요한 요건이 된다면, 해당 출처 증거를 증명할 수 있는 정보가 더 필요하다. 출처 정보가 생산 이후 변경되지 않았음을 증명하는 무결성 기술로서 전자서명 등을 이용할 수 있다.

(2) 출처 정보의 적절한 관리

이상과 같은 출처 정보는 적절히 생산되고 관리되어야 한다. 최초에 획득된 출처 정보가 신뢰성을 확보할 수 있으려면 ISO 15489에서 기록의 4대 특성 중 "신뢰성(Reliability)"에 대하여 요구한 바대로 출처 정보도 획득되어야 할 것이다.[33] 즉 처음 기록

32) ibid, p.26

33) ISO 15489-1:2001 - Reliability에 대한 언급:

- Records should be created at the time of the transaction or incident to which they

이 생성될 그 당시에 출처 정보를 명시하여야 하며, 그것이 불가능하였을 경우에도 가급적 가까운 시일 내에 획득・명시되어야 한다.

출처 정보에 포함되는 정보항목들의 연계성을 확보하여야 한다. 즉 어느 한 항목이라도 뒤바뀌거나 누락되지 않도록 통합관리가 가능하여야 한다. 여기에 더하여 출처 정보와 해당 기록객체 자체와의 연계성도 확보되도록 관리되어야 한다. 전자서명 기술이 여기에 대한 가능한 방안으로 고려될 수 있다.

출처 정보는 변경할 수가 없고, 이력관리의 필요에 따라서는 첫 출처 정보로부터 그 이후 지금까지의 사건들 이력을 관리하여 지금에 이르는 "유래 정보"로 관리할 수 있다. 다만 이때 주의하여야 할 것은 그때마다 각 사건의 "명의"와 "시기" 정보가 처음 생산당시와 마찬가지의 신뢰성을 가지고 획득, 명시되어 누적 관리되어야 한다는 점이다. 그러한 면에서 볼 때 현행 메타데이터 표준에서는 "생산이력"과 "보존"이라는 사건 기록을 반복 누적시킬 수 있도록은 하고 있지만 양파모델의 보존포맷상에서 각 수정전 기록과 해당 이력을 연계시키지 못하고 있기 때문에 보완이 요구된다.

출처 정보를 누가 어디에 관리하는가 하는 것은 여러 방안이 개발될 수 있다. 그러나 어느 방안이 되었든 출처 정보는 항상 기록 자체를 이용(관리, 보존 포함)하기 전에 필수적으로 검증받아야 한다. 그래야만 그 이후의 후속행위 일체가 타당성을 가질 수 있기 때문이다. 따라서 출처 정보의 관리 방안은 결국 출처 정보 확인 방안과 함께 고려되어야만 한다.

---

relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

(3) 출처 확인 요건

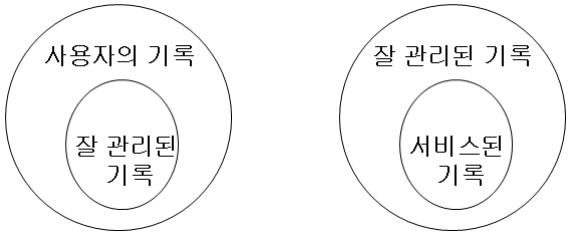
언제, 어떻게 출처 정보를 확인하여야 하는가를 정해서 시행하여야 한다. 출처 확인이 필요한 시점으로는 해당 기록을 이용하여 다음 업무를 수행하려 할 모든 시점이 해당하겠지만, 특히 대외적으로 해당 기록을 서비스하려고 할 때 특히 중요하다. 이 요건은 모든 시스템 요건과 운영 지침에 명시되어야 한다.

출처 정보 구성이 복잡하면 확인 또한 복잡해진다. 현행 메타데이터 표준이나 장기보존포맷 표준으로는 행위자와 인증정보의 명의가 일치하지 않고 행위 시기와 전자서명의 시기도 일치하지 않을뿐더러, 그림 5의 수정된 보존포맷의 경우에는 내부의 수정전기록에 들어있는 원래의 출처정보를 확인하라는 요건이 누락되어 있다. 이대로라면 최외곽의 인증정보만 확인하고 말 것이다. 그림 3과 같이 앞으로 여러 명의의 관리기관을 거쳐 여러 겹의 양파모델이 만들어지게 된다면, 출처 확인이 필요할 때마다 이 각 겹의 출처 정보를 시간의 역순으로 (즉, 외부에서 내부로) 확인하여 들어가는 절차를 정교하게 마련하고 필수 요건화하여 시행하여야 한다.

만일 전자서명의 효력을 연장시키기 위하여 앞에서 비판한 현행 장기검증체계 대신 원래 국제표준인 그림 10의 RFC 3126 방식을 따르기로 한다면, 각 이력단계마다 생성된 전자서명 각각에 대하여 주기적으로 계속 누적 전자서명(타임스팀핑)하여야 한다. 이러한 방식으로 출처 정보를 관리한다면, 출처를 확인하려고 할 때가 되어서는 검증하여야 할 인증정보가 막대하고 그 항목들이 분산되어 있어 매번 오랜 시간을 기다려야 할 것이므로, 실제 사용 가능한 개선된 방안이 필요하다. 여기에 대한 대안을 3장에서 제안하기로 한다.

(4) 출처 미확인시 대응책

출처정보를 잘 명시하고 관리한다고 해서 반드시 모든 출처 확인이 성공한다는 보장은 없다. 앞에서 말한 바대로 전자서명은 검증 기능은 있어도 보호 기능은 없기 때문이다. 게다가 그림 12의 왼쪽과 같이 모든 기록이 적절히 관리되어 온 것이 아닐 수도 있다.



〈그림 12〉 잘 관리된 기록과 사용하려는 기록의 포함관계

기록관리자들은 자신이 관리하고 있는 기록 중에서 사용자에게 서비스하기 때문에, 기록 수요자들이 앞에 놓고 그 출처를 의심하는 기록들은 모두 적법하게 관리되고 있던 기록이라고 단정하는 오류에 빠지기 쉽다.(오른쪽 그림) 그러나 실제로는 포함관계가 그 반대인 것이다. 정규적인 기록 포맷으로 가공 처리되지 않은 기록물로는, 일반 PC 내에서 흔히 볼 수 있는 전자파일, 백업 스토리지에 잔류한 과거 파일, 아직 보존포맷화되지 못하고 있는 시청각 기록물, 새로 도입된 행정시스템에서 생산될 신형 기록 등을 포함하여 무수히 생각해 낼 수 있다. 그러나 현행 기록관리의 표준, 지침, 법령 어디에도 이에 대한 대비책이 없는 실정이다.

사용자가 소지한 전자기록은 출처 확인이 되느냐에 따라 몇 가지 경우로 나누어 생각해 볼 수 있다.

① 출처 정보가 다 제대로 남아 있지만 확인해 보니 원래값이라는 검증에 실패한 경우: 현행 표준으로는 "검증실패"라는 결과를 사용자에게 줄 뿐이다. 실패 판정 이후에 사용자에게 제공할 수 있는 서비스가 존재하여야 할 것이며, 좀더 구체적인 대응책이 필요하다.

② 누락된 이력이 있어서 첫 출처부터 지금까지의 유래가 온전히 보전되어 있지 못한 경우: 현행 표준으로는 이력을 추적 검증하지 않으므로 마지막 인증값만 검증 성공하면 유효한 전자기록으로 판정해 준다. 그러나 이론상 이것은 진본성이 침해된 기록인 것이다. 그런데 검증 체인이 누락된 부분 이후부터 지금까지의 이력이 온전할 경우, 이 기록은 누군가가 한번 방치되었던 기록을 다시 잘 수집하여 기록물화한 것일 수 있는데, 이런 경우는 유효하다고 판정할 수도 있다. 또는 누군가가 도중에 마음대로 기록을 변경해 놓고 자신의 변경시점 이전 검증체인을 고의로 훼손시켜 확인을 무력화하려고 시도한 것일 수도 있다. 이에 대한 전략이 필요하다.

③ 출처 정보가 판독 불가능한 경우

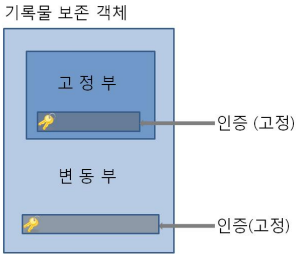
④ 출처 정보가 없는 경우: 이 두 경우는 해당 기록이 반드시 열람하여야 할 중요한 기록일 경우 다른 방식으로 대체해서 구할 방법을 찾는다든지 하는 대응책이 필요하다.

본 논문에서는 이러한 대응책을 위한 지원전략을 4장에서 논의하기로 한다.

3. 새로운 출처확인 장기검증 대안

1) 장기검증 대상의 최소화

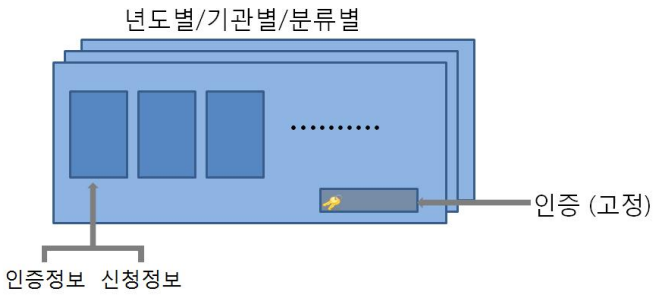
문제의 본질은 두가지로 생각된다. 하나는 전자서명의 유효기간이 기록물의 보존기간보다 짧다는 것이며, 다른 하나는 전자서명(및 타임스탬프)가 사건이 생길 때마다 계속 반복 적용된다는 것이다. 두 번째 문제를 완화하기 위하여 전자기록 객체를 구성하는 요소들을 생산 이후 불변인 부분(고정부)과, 관리하며 수정·변환이 지속적으로 이루어질 수 있는 부분(변동부)로 나누는 것을 제안한다. 그림 13처럼 고정부는 생애 단 한번 전자서명하며, 변동부는 새로 변동사항이 생길 때마다 고정부를 포함하여 새로 전자서명한다. 고정부는 생산 원본, 생산 맥락 등 기록물 생애동안 변하지 않을 내용들이고, 변동부는 재분류, 이관, 포맷변환 등 최초 출처와 상관없는 부분이다. 고정부 전자서명은 생산당시를 증명하므로 본 전략에서 출처 확인의 기본정보로 활용할 것이며, 변동부 전자서명은 기록물의 최근 모습을 증명하므로 무결성 증명용으로 사용할 수 있다.



〈그림 13〉 기록물 구성요소의 고정부와 변동부 구분

2) 장기검증 정보의 영구보존

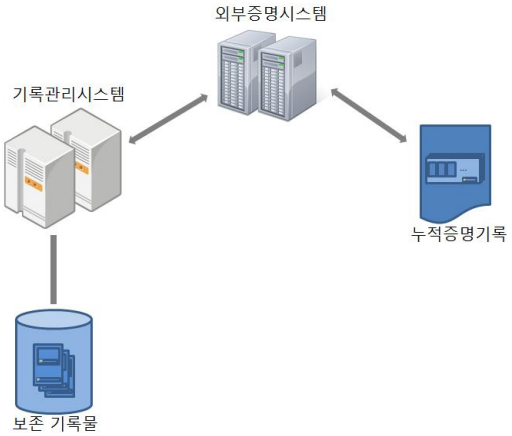
이처럼 출처 확인만을 위한 인증정보만 구별함으로써 반복 적용에 따른 과다한 정보용량이라는 두 번째 문제를 최소화한다. 이 정보들을 전자서명의 유효기간 만료에도 불구하고 계속 증명 가능하게 하기 위하여, 서양의 공증제도와 유사한 시스템을 구축하기로 한다. 즉, 장기 보존할 기록물에 대한 고정부 전자서명을 공증 가능한 신뢰성 있는 타 기관에 복사하여 공탁한다. 이 타기관에서는 증명시스템을 구축하여, 연도별이나 기관별, 분류별로 고정부 전자서명들을 신청당시맥락정보와 함께 모아 "단위컨테이너"를 구성한 후, 여기에 대하여 가장 긴 전자서명으로 다시 인증하고, WORM과 같이 삭제 불가능한 신뢰성 있는 스토리지에 그림 14처럼 영구 보존한다. 고정부 전자서명만 모았으므로 이후에 기록물에 대한 어떠한 수정·변환이 이루어지더라도 영향을 받지 않으며, 그 대신 최신 모습을 증명(무결성 증명)할 수는 없고 출처를 증명하는 것으로 용도가 제한될 것이다.



〈그림 14〉 장기검증정보 보존 단위컨테이너

3) 장기검증 방법

이러한 방법으로 보관하다가 검증이 필요하면 그림 15와 같이 외부 증명시스템에 접근하여 검증한다. 검증값은 해당 단위 콘테이너의 인증값과, 그 안에 보존된 해당 기록 고정부 인증정보, 그리고 대조용으로 필요한 신청당시 맥락정보의 3가지에 불과하며, 이 정보들이 한 위치에 있기 때문에 단한번의 액세스(접근)으로 검증이 완료된다. 이 방법은 수요자가 기록관리기관을 믿지 못할 경우에도 사용 가능하다. 만일 외부증명기관의 신뢰성이 고도로 요구된다면 서로 다른 별개의 외부증명시스템을 홀수(1, 3, 5)로 사용하여 교차 증명할 수도 있다.



〈그림 15〉 외부의 누적증명기록에 의한 검증방법

4. 출처확인 지원전략

1) 출처확인 방안

막상 수요자가 오래된 전자기록을 받아들고 이의 출처를 의심한다고 하자. 이 때에는 2장 3절의 고려사항들이 반영된 지원전략이 필요하다.

(1) 단순 확인

주어진 고정부 전자서명을 공탁된 외부증명시스템에 가서 검증 확인한다. 제안 방법이 여기에 해당한다.

(2) 증명 요청

이와 같은 체계가 마련되어 있지 못하다면 발급 기관에 대하여 직접 증명을 요청한다. 현행 표준이 여기에 해당한다. 발급기관 자체에 대한 신뢰성이 의심되는 경우에는 제3자의 보증이 필요할 수 있다.

(3) 추정

기록관리의 신뢰성과 정황증거, 찾아볼 수 있는 유사한 기록들의 출처 등을 통하여 비록 낮은 수준이긴 하지만 출처를 추정하여 사용한다. 만일의 경우에는 수사기법인 디지털 포렌식 기법을 동원할 수도 있다. 이렇게 되면 이후로는 이 기록에 출처정보가 생기게 되는데, 그 출처 정보는 원래 생산당시에 만든

것은 아니므로 생산 명의와 출처 증명의 명의는 일치하지 않는다. 따라서 바람직하기로는 권한있는 기관의 명의로 출처를 선포하고 그 이후부터 이력을 잘 관리하면 되는데, 그 후에 이 기록을 다시 출처 확인하려고 하면 마치 2장 4절의 ②번 경우와 같이 된다. "추정" 방안에 대해서는 좀더 많은 논의와 실험을 통하여 가이드라인이나 best-practice가 개발되는 것이 필요하다.

2) 출처 미확인 방지대책

출처가 확인되지 않거나 진정성이 의심되는 경우가 생기면 안되는 중요 기록물들에 대한 대비책이 반드시 필요하다. 저자는 이에 대하여 예방(prevention), 회피(avoidance), 탐지복원(detection and recovery)의 세가지 기법을 제안한다.

(1) 사전 예방

정말 중요한 기록물은 어떠한 경우에라도 소실되어서는 안될 것이다. 따라서 전자기록의 취약점과는 전혀 관련이 없는, 종이기록, 마이크로필름 등 성질이 다른 형태로 이중 보존한다. 만일 보관중인 기록의 출처 확인이 안될 경우에는 이렇게 이중 보존된 기록으로부터 출처를 확인하면 된다. 다만 전자기록과 해당 이중보존기록간의 연계성은 적절히 관리하여야 할 것이며, 기록의 처분행위 등에 있어서도 항상 동일하게 이중 적용되어야 할 것이다.

(2) 기록관리 과정중 회피

위험요소가 의심될 경우 비정기적으로, 또는 안전하다고 추

정된 주기마다 규칙적으로 안전한 곳에 보존사본을 생성하여, 조선시대의 4대 서고처럼 물리적으로 상호 독립적인 곳에 분산 보존한다. 원본의 계속적인 수정·변환에 맞추어 보존사본을 계속 갱신해 줄 것인지 구형 사본을 폐기할 것인지 등에 따라 사본의 유효성 수준이 달라짐을 인지하여야 하고 활용전략을 달리 수립하여야 하며, 원본에 준하는 보안이 보존사본에도 적용되어야 함에 유의하여 전략을 세운다.

(3) 탐지복원

가장 우려스러운 것은 전자기록의 관리상태가 출처확인이 안 될 정도로 훼손되었는데도 이를 인지하지 못하고 마냥 보관하고 있는 경우이다. 이렇게 되면 긴 세월 후에 해당 기록을 사용하려고 출처를 확인할 때에야 비로소 문제를 인식하게 된다. 시간이 경과함에 따라 언제부터 이렇게 되었는지, 원인은 무엇인지, 원래 정보는 어땠는지 등에 대한 확인이 어려워진다.

전자기록을 온라인 스토리지에 보관중이라면 시스템 기능에 의하여 실시간 감시를 수행할 필요가 있다. 그리하여 오류가 발생되는 그 시각에 실시간으로 탐지하여 중복본이나 사본으로부터 원래 정보를 복원하도록 하여야 한다. 만일 보관 캐비넷에 수납중인 DVD-ROM 등 오프라인 스토리지에 보관중인 기록이라면 정기적인 점검이 수반되어야 하며, 백업본을 그 정기점검 주기의 적어도 몇 배 이상에 해당하는 기간동안 생존하도록 관리하는 사항을 포함하여 재해복구 대책을 마련해 두어야 한다.

온라인 실시간이든 오프라인 주기적이든 기록의 오류를 탐지하여 기록을 복원하게 되면 그 행위에 대한 이력과 인증정보를 출처정보화하여 누적 관리하여야 한다. 이러한 정보를 포함할

수 있도록 현행 시스템 및 보존포맷 개선도 고려되어야 할 것이다.

3) 출처 신뢰성에 따른 평가

기록의 출처 정보가 잘 관리되었고 그 기록관리의 담당기관이나 담당자, 관리방법이 신뢰성이 있고, 출처 확인이 신뢰성이 있으며, 그러한 모든 신뢰도가 해당 기록에 필요한 신뢰도를 상회하게 되면 해당 기록은 믿고 사용할 수 있을 것이다. 정보관리, 기관/담당자, 출처확인, 기록이라는 4가지 신뢰도 각각의 신뢰도 수준을 평가할 지표와 계량 방법이 개발되어야 한다. 일반적으로 생각해 볼 때 4가지의 신뢰도 수준간 관계는, 이론의 여지는 있겠지만 일단 다음과 같아야 할 것으로 생각된다.

기록 〈 출처확인 〈 정보관리 〈 기관/담당자

따라서 각 기록에 대하여, 필요한 신뢰 수준을 정하는 것이 필요하다. 예를 들어 대통령지정기록물의 경우에는 세상에서 적법한 사용자가 단 한명(전직 대통령)이고 그 내부에 국가기밀도 들어 있을 수 있으므로 최고 수준의 신뢰도가 필요할 것이다. 그렇기 때문에 기록별 신뢰도 요구수준을 설정할 필요가 있는데, 여러 가지 방법이 있겠지만 관리의 효율성을 위해서 수준 단계를 3~5단계 정도로 나누어 설정하고, 각 신뢰도 수준별로 필요한 요건들을 명세하는 것을 제안한다. 이 수준별 요건이 도출되고 나면, 출처확인에 관련된 기관, 인원, 기술, 방법론, 시스템 등에 대하여 각각 해당 요건 수용여부 및 달성 수준을 인증해 줄 수 있다. 이에 대한 평가 인증 전략도 마련하는 것을 제안

한다.

마지막으로, 지금까지 논의한 관리, 출처확인, 대응, 평가 등에 대하여 모든 일을 반드시 공공기관에서만 수행할 필요는 없다. 그러할 경우 대행 민간단체나 개인에 대한 인증, 요금제, 교육, 감독에 대한 전략도 마련하는 것이 필요하다.

5. 맺음말

기록관리기관에서 전자기록을 관리하는 목적은 결국 이용자들에게 신뢰성 있는 서비스를 제공하는 것이라는 목적의식 하에, 지금까지 기록관리자의 고유업무(장기보존) 측면에서 진행하던 논의를 기록관리자의 외부서비스(장기검증) 측면으로, 더 나아가 수요자의 요구(출처확인) 측면으로 관점을 전환하기를 제안하며, 기록 자체보다는 기록의 활용에 의미가 있고 개별 방법이 중요한 것이 아니라 그들의 융합적 활용을 통하여 원하는 목표를 달성하는 것이 더 중요하다는 생각을 바탕으로 기존의 전자기록 관리 논의들을 비판적으로 바라보았다. 원래 종이기록도 모두가 생산할 때부터 장래의 보존을 생각하고 만들어지는 것이 아니며 나중에 기록관리자가 보존 관리하는 것이다. 인류가 기록을 이용할 때, 보존 관리된 것만 기록으로 인정하고 사용한 것도 아닐 것이다. 기록관리자의 입장에서는 장기보존을 위한 여러 대비책을 세우는 것이 당연하겠지만, 중요한 것은 최종 수요자의 관점에서 정작 사용하려고 할 때 닥칠 여러 상황에 대한 대응 전략을 세워두는 것이다.

본 고에서는 이러한 아이디어에 따라, 국내 수요자에게 필요

한 가장 중요한 요건중 하나라고 생각되는 출처확인에 대한 지원전략을 생각해 보았다. 기존의 논의들은 진본성과 무결성이라는 복잡 모호한 개념 속에서 진행되어, 필요한 개별 요소를 파악해 내기 힘들었고 그에 따라 대비책을 하나씩 마련해 나아가는 데에도 진행이 더디었다. 그러나 전자기록은 연구자, 전문가만의 영역을 벗어나 이미 일반인들 생활 저변에서 만들어지고 서비스되고 있는 것이다. 이러한 촉박감 속에서 일단 "출처"라는 정보가 기록 신뢰성을 따질 때 가장 중요한 개념이라고 생각하였고 이 출처의 확인 전략과, 출처가 검증되지 않은 기록에 대한 대처방안, 출처가 검증되지 않을 경우를 미리 방지하기 위한 예방, 회피, 탐지복원 방안을 논의하였다.

현행 국내 방안들이 출처 정보를 소홀히 다루고 확인할 때 명의가 일치하지 않으며 장기보존에 대한 검증에 약점이 있음을 보였으며, 그에 대한 대안으로서 출처 정보의 구성 요소를 제시하고, 장기 검증을 간단 명료하게 하는 방법으로서 기록 객체를 변동부와 고정부로 나누어 출처는 고정부에서 검증하도록 하는 기법을 제안하였다.

앞으로 기록의 출처에 관한 신뢰도 수준을 관리할 수 있고 그에 따라 필요한 곳에 필요한 만큼의 신뢰도를 확보해 제공할 수 있도록 여러 확인 지원전략, 수준 평가 인증방법, 평가 사업 관련 전략을 계속해서 연구・정립하여야 할 것이다.

ABSTRACT

A Verification Strategy for the Origin of Electronic Records

Byoungho Song

The target of managing electronic records should be the trusted record services to the end-users. The natural characteristics of electronic records yields the drawback in the authenticity aspect and in the integrity aspect, and current standards and methodologies have beed developed to treat this drawback. However the authenticity and the integrity concepts is hardly separated each other and too completed, so alternative "source" concept is introduced and a verification strategy for the origin of electronic records is discussed in this paper. According to this concept, current standards and methodologies may be criticized for the negligence of necessary information organizing/verification, the doubtful long-term verification, and the missing counter-strategy for the verification-failed records. To solve this, needed facters for origin verification is described, new preservation format divided into temporally-fluctuating (variable) part and immutable (fixed) part is proposed, and a strategy to prevent, avoidance, and detection/recovery important records is suggested.

key word: Electronic Records, Authenticity, Origin Verification, Authentication, Long-Term Preservation