情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

웹 게시물 증거를 위한 공증 시스템 도입 연구*

김 아 름,[1†] 김 역[2], 이 상 진[1‡]
[1]고려대학교 정보경영공학전문대학원, [2]한신대학교 컴퓨터공학부

A Study on Notary System for Web Postings Digital Evidences*

Ahreum Kim,[1†] Yeog Kim[2], Sangjin Lee[1‡]
[1]Graduate School of Information Management and Security, Korea University,
[2]School of Computer Engineering, Hanshin University

요 약

인터넷을 통한 루머나 악성 댓글이 사회적인 문제로 대두되고 있다. 이를 고발하기 위하여 해당 웹 게시물을 캡처한 이미지나 출력물이 증거로 활용될 수 있으나, 이는 포토샵 등의 도구를 이용한 위·변조에 취약하다. 악의적인 목적으로 타인이 작성한 정상적인 글을 캡처한 화면에 비방하는 내용이 포함되도록 위조한다면 무고한 자가 처벌을 받게 될 수도 있다. 이처럼 웹 게시물의 캡처 화면은 정확한 사실 관계를 반영하기에는 증거로서의 진정성과 무결성에 흠결이 있다. 웹 게시물의 증거화를 위한 인증 시스템이 제공되면 진정성이 입증된 증거의 제시가 가능하고 효율적인 수사에도 도움이 되므로 관련 기술과 정책의 빠른 정착이 요구된다. 이에 본 논문에서는 웹 게시물 증거화의 중요성을 역설하고, 웹 게시물 공증 시스템에 요구되는 법률적, 기술적 요구 사항 및 설계 방안을 제안한다.

ABSTRACT

Rumor or abusive web postings in internet has become a social issue. Web postings may be proposed on evidence in form of a screenshot in libel suit, but a screenshot can be easily modified by computer programs. A person can make ill use of the screenshot which is modified deliberately original contents to opposite meaning in a lawsuit. That makes an innocent person to be punished because it can have difficulties to verify despite analyzing the server data. A screenshot of web postings is likely to fail to prove its authenticity and it is not able to reflect the fact. If notarization for web postings is offered, clear and convincing evidence can be submitted in a court. So, related techniques and policies should be established. In this paper, we propose some technical and legal conditions and design for notarization and archive system of web postings for litigation.

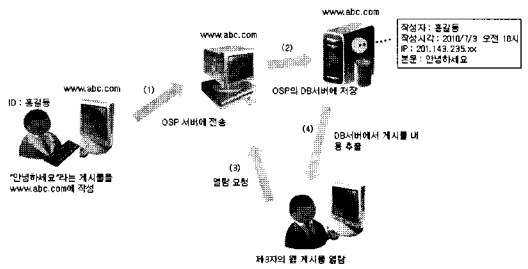
Keywords: web postings evidence, web postings notary, digital forensic evidence

I. 서 론

인터넷은 누구나 접근하기 용이하고 그로 인한 파급력이 강하므로 정치인들의 선거나 연예인의 인지도를 얻기 위한 광고나 활동에 많이 이용된다. 이와 동시에 상대방의 인지도 하락을 위한 비방이나 근거 없는 자료 유포의 장으로 이용되기도 한다. 타인이 작성한 비방글로 인해 본인의 명예가 실추되었음을 이유로 해당 글의 작성자를 고발하는 경우에는, 추후 작성자에 의해 해당 비방글이 수정 혹은 삭제될 수 있으므로 고발 당시에 비방글이 존재했던 사실을 입증할 수 있어야 한다.

현재는 이를 입증하기 위해 고발하는 측에서 웹 게

접수일(2010년 8월 24일), 게재확정일(2010년 9월 24일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발 사업의 일환으로 수행하였음 [10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발].
† 주저자, nestop14@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr



〔그림 1〕 웹 게시물을 작성하고 제3자가 열람하는 과정

시물을 캡처한 화면을 사용하거나, 이를 확보하지 못한 형사 사건의 경우에는 수사 기관이 해당 사이트의 서버에서 웹 게시물의 내용을 획득하여 증거로 제시한다. 웹 게시물을 단순히 캡처한 화면은 위·변조에 매우 취약하여 증거의 진정성을 만족하지 못하기 때문에 이를 증거로 채택하는 경우 잘못된 법적 판단을 내릴 우려가 있다.

'갑'이 '을'을 비방하는 내용의 글을 어떤 웹 사이트의 게시판에 작성하였고, 이를 본 '을'이 해당 웹 게시물을 근거로 '갑'을 명예훼손 혐의로 고발하려는 상황을 가정해보자. 이 경우 해당 웹 게시물의 작성자인 '갑'이 본인을 고소하려는 '을'의 움직임을 눈치 채고 해당 게시물을 삭제하거나 수정하여 비방한 내용을 없애버리고 현 게시물의 내용과 캡처한 증거의 내용이 다름을 근거로 혐의 없음을 주장할 수 있다. 수사 기관에서 웹 서버에 기록된 로그, 게시물의 내용에 대한 수사를 실시하더라도 일반적으로 과거의 모든 기록을 저장하는 서버는 거의 없으므로, 서버에 최종적으로 남게 되는 웹 게시물은 '갑'이 수정 혹은 삭제한 내용이므로 갑의 행위는 입증하기 힘들어진다. 따라서 수사 기관이 해당 사이트의 서버에서 증거를 확보하기 전에 갑이 게시물을 수정 혹은 삭제한다면 사실 관계를 떠나 갑의 죄를 물을 수 없게 된다. 이처럼 서버를 수사하고도 진실을 완벽하게 규명하기 어려운 경우가 발생할 수도 있다. 만일 을이 제시하는 증거가 진정성에 이의를 제기할 수 있는 단순한 캡처 화면이나 서버에 저장된 내용이 아니라, 고발 시점에 비방 내용이 담긴 웹 게시물이 있었다는 것을 확증할 수 있는 방안이 있다면 정확한 사실 관계 파악과 수사 효율화에 상당히 도움을 줄 수 있을 것이다.

따라서 나날이 증가하는 인터넷 상의 위법 행위에 대한 정확한 법적 판단을 위해서는 기존의 화면 캡처 방식이 담보하지 못하는 진정성 및 무결성을 보장할 수 있는 새로운 방식의 웹 게시물의 증거화 방안이 요구된다. 새로운 방식은 증거를 생성한 당시 웹 게시물의 내용을 의심 없이 증명할 수 있어야 하고, 생성된 증거가 수집 이후 가해질 수 있는 위·변조 행위로부터 안전하게 보관되어야 한다. 이를 위해서 웹 게시물에 대한 공증 개념이 도입될 수 있다. 공증은 특정 시각에 특정 내용의 문서가 존재하였다는 사실을 자격을 갖춘 제 3자에게 확인받는 것으로, '공증인법'에 의해 자격을 갖춘 제 3자의 확인을 받은 문서에는 법적 효력이 부여된다. 현재 전자 문서를 대상으로 하는 전자문서 공증시스템은 상용화 되어 있으나 웹 게시물은 그 특성으로 인해 단순히 전자문서공증시스템으로는 진정성을 확보할 수 없다. 이에 본 논문에서는 웹 게시물의 특성을 고려한 웹 게시물 공증 방안을 도출하고 이를 구현한 시스템이 갖추어야 할 사항에 대해 살펴본다. 또한 웹 게시물 공증 시스템을 도입하기 위해 뒷받침되어야 할 법률적·제도적인 요소도 다룰 것이다.

II. 웹 게시물의 증거 능력

증거 능력이란 사실 입증 자료가 증거로서 채택되어 법률상의 자격을 가질 수 있는가의 문제로, 제출된 자료가 증거 능력이 있어야만 재판에서 주장을 뒷받침하는 데에 사용될 수 있다[1]. 웹 게시물은 고유의 특성으로 인해 웹 게시물을 증거로 생성하는 방법에 따라 증거 능력을 얻지 못할 가능성이 있다. 본 장에서는 제출 자료가 증거 능력을 갖는지 여부를 판단하는 기준을 살펴보고, 이 기준과 웹 게시물의 속성을 비교함으로써 웹 게시물이 증거로 채택되기 위해서 갖추어야 할 요건을 파악한다.

2.1 증거 능력

국내법에는 증거와 관련된 개별법이 존재하지 않고, 형사소송법이나 민사소송법의 일부로만 증거 관련 규정을 다루고 있다. 형사소송법에 따르면 법정에서 유효한 증거가 되기 위해 갖추어야 할 조건으로 증거 능력과 증명력을 들 수 있다. 증거 능력은 증거조사의 대상이 될 수 있는 일반적인 자격을 의미하며, 증명력은 실제 법정에서 해당 증거가 사실을 판단하는 데에 기여하는 정도를 의미한다. 따라서 증거가 채택되어 법정에서 주장하는 내용을 뒷받침하기 위해서는 증거 능력을 가져야 한다. 국내법 하에서는 대부분의 증거에 대한 증거 능력을 인정하고, 위법수집증거배제의 원칙과 전문증거배제 원칙만을 강력하게 적용한다.

비교적 증거법이 발달한 미국의 연방 증거법에서는

사실 입증 자료가 법적 허용성을 갖기 위한 조건으로 관련성의 원칙, 진정성 입증, 원본서류의 원칙, 전문증거배제 원칙을 들고 있다[2]. 각 원칙의 내용을 살펴보고, 웹 게시물 증거의 인증 및 보관 시스템이 증거 능력을 갖춘 웹 게시물 증거를 획득할 수 있기 위한 원칙을 파악한다.

- ○ 관련성의 원칙 : 증거가 담고 있는 정보는 반드시 사건과 관련되어야 함
- ○ 진정성 입증 : 제출된 증거가 주장 내용과 동일함을 보장할 수 있어야 함
- ○ 원본서류의 원칙 : 서면, 기록물 또는 사진의 내용을 입증하기 위해서는 법에서 예외사항으로 규정한 몇 가지 예를 제외하고는 원본을 제출해야 함
- ○ 전문증거배제원칙 : 진실을 입증하기 위해서 법정 밖에서 진술된 전문 증거는 배제되어야 함

관련성의 원칙은 증거가 사건의 해결에 도움이 되는지를 판단하는 것으로, 증거가 담고 있는 내용 자체에 초점을 맞춘다. 예를 들어 저작권을 침해하였다는 사실을 입증하기 위해 저작물이 첨부된 웹 게시물이 증거로 제출된다면, 관련성의 원칙은 증거로 제출된 웹 게시물의 내용이 저작권을 침해한 사실과 관련 있는지의 여부를 판단한다. 즉, 관련성의 원칙을 만족시키기 위해서는 증거 제출자가 적절한 내용의 웹 게시물을 선택하는 것이 중요하며, 웹 게시물의 캡처 이미지를 제출하든, HTML 코드를 제출하든, 어떠한 형식의 웹 게시물 증거를 제출하는지는 고려치 않는다.

웹 게시물은 디지털 자료의 특성으로 인해 변조나 조작이 용이하므로 주장에 맞춰 내용을 조작할 수 있다. 따라서 웹 게시물은 보다 엄격한 진정성의 확인이 요구되며, 웹 게시물의 인증 및 보관 시스템은 진정성을 명확하게 확보할 수 있도록 설계되어야 한다.

미 연방증거법 Rule 1001에서는 '자료가 컴퓨터나 이와 유사한 장치에 저장된 때에는 육안으로 읽을 수 있는 인쇄물이나 그 외 어떠한 형태의 출력물도 자료를 정확히 반영하고 있는 경우는 원본이다'고 적시하였다[3]. 즉, 웹 게시물은 웹 서버와 데이터베이스의 내용을 출력한 한 형태이므로 원본서류의 원칙을 만족한다.

전문은 법정에서 진술되지 않은 '전해들은 말'로, 보조적인 증언을 통해 사실성이 입증되지 않으면 증거로 채택될 수 없다. '웹 게시물은 법정에서 원진술자가 증언한 진술 그 자체가 아니라, 주장하는 내용이 진실함을 입증하기 위해 제공되는 것'이라는 판례에 의하면 웹 게시물은 전문이고, 전문은 기재 내용의 진실성을 담보하지 않는다. 하지만 모든 전문증거가 배제되는 것은 아니고, 공공기관에서 작성한 문서, 일상적인 업무 처리 과정에서 생성된 문서 등 일부 예외 사항에 해당하는 경우에는 법적 허용성을 인정한다. 따라서 웹 게시물 증거가 전문증거배제원칙에 적용되지 않고 법적 허용성을 얻기 위해서는 예외 사항에 포함될 수 있도록 해야 한다.

〔표 1〕 웹 게시물 증거화 측면에서 고려해야 할 증거 능력의 원칙

조건	웹 게시물의 증거화 측면에서의 고려 여부
관련성의 원칙	×
진정성 입증	○
원본서류의 원칙	×
전문증거배제원칙	○

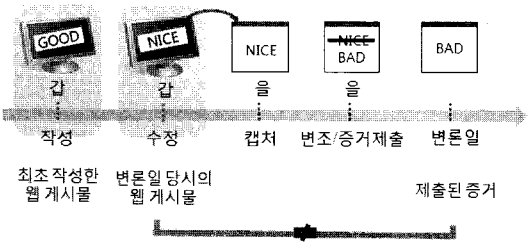
2.2 웹 게시물의 특성

웹 게시물의 특성을 살펴보면 다음과 같다.

- ○ 변조 가능성 : 디지털 자료
- ○ 접근 용이성 : 웹 사이트에 게시되어 화면 상에서 확인 가능
- ○ 빈번한 수정 가능성 : 권한을 가진 자에 의한 수정 및 삭제가 용이
- ○ 전문증거 : 주장을 입증하기 위해 법정 밖에서 진술

디지털 자료는 일반적으로 물리적인 자료에 비해 쉽게 변경될 수 있다. 변경 가능성은 증거로 제출된 자료의 진정성을 약화시키므로, 증거가 법적 효력을 갖기 위해서는 적절한 방법을 통해 진정성이 입증되어야 한다.

웹 게시물은 접근 제한을 두지 않으면 웹을 통해 누구나 접근가능하고, 접근 제한을 둔 경우에는 권한을 가진 사용자만이 확인, 수정 및 삭제 등의 행위가 가능하다. 둘 중 어떤 경우라도 웹 페이지의 내용을 모니터로 확인할 수 있다. 이러한 접근 용이성으로 인해 웹 게시물을 증거로 한 경우 서버나 DB로 직접 접근하지 않고도 화면상의 내용을 캡처한 자료나 HTML



〔그림 2〕 웹 게시물이 변조되어 증거로 제출되는 과정

코드를 제출하는 방법을 사용할 수 있다. 그러나 캡처 화면이나 HTML 코드는 악의적인 목적을 가진 사람에 의해 조작되어 허위의 증거를 생성할 가능성이 있다.

예를 들어 '갑'에게 반감을 품은 '을'이 있고, '갑'은 웹 사이트에 정상적인 글을 게시한 경우를 가정하자. 〔그림 2〕와 같이 '을'이 '갑'의 웹 게시물을 캡처하고 도구를 이용하여 갑이 작성한 정상적인 내용을 '을'을 비방하는 내용으로 이를 조작할 수 있다. 이 조작된 캡처 자료를 '을'이 법정에 증거로 제출하고, '갑'이 서버 등에서 이를 반박할 수 있는 증거를 찾지 못한다면 무고한 '갑'이 법적 책임을 지게될 수 있다. 캡처 화면과 같은 기존의 웹 게시물의 증거화 방법은 조작 가능성이 있고, 따라서 항상 진정성을 담보하지 않는다.

웹 게시물은 권한을 가진 자에 의한 수정 및 삭제가 용이하므로 시시각각 그 내용이 바뀔 수 있다. 특히 증거의 상대방에서 작성한 게시물을 수정하거나 삭제한 경우 캡처 화면이나 당시의 HTML 코드는 현재의 웹 게시물 상태와 동일하지 않게 된다. 따라서 캡처 화면이 조작되지 않았고 발견 당시의 내용을 그대로 포함하고 있다 하더라도, 이후에 작성자에 의해 수정되고 증거의 상대방에서 최종적인 웹 게시물의 내용과 캡처 화면의 내용이 다름을 근거로 진정성이 없음을 주장할 수 있다. 즉, 앞서 설명한 웹 게시물의 변조 가능성, 접근 용이성, 빈번한 수정 가능성으로 인해 웹 게시물을 증거화하는 방법에 따라 진정성 입증 여부가 달라진다.

웹 게시물은 앞 절에서 언급하였듯 전문증거이다. 전문증거는 원칙적으로 전문증거배체 원칙에 의해 증거 능력이 부인된다. 그러나 형식적으로 전문증거인 경우라도, 전문법칙 적용이 부정되거나 전문법칙의 예외에 포함되는 경우도 있다. 따라서 전문증거인 웹 게시물이 증거 능력을 부여받기 위해서는 전문법칙의 부정 혹은 예외 사항에 포함될 수 있도록 증거화 해야 한다.

2.3 웹 게시물이 증거 능력을 갖기 위한 요건

웹 게시물 자료가 증거 능력을 갖기 위해서는 웹 게시물의 특성으로 인해 약화될 수 있는 진정성의 입증과 전문법칙의 요건을 명확하게 만족해야 한다.

진정성을 명확하게 입증하기 위해서는 증거 상대방이 증거의 변경가능성에 대해 이의를 제기할 여지를 남기지 말아야 한다. 증거에 대한 변경은 증거 수집 중에 발생할 수 있고 이후 증거를 보관하는 과정에서 발생할 수 있다. 증거 수집 중의 조작 가능성을 제거하기 위해서는 웹 게시물을 증거제출의 목적으로 획득할 때 개인이 PC에서 획득하기 보다는 신뢰성이 입증된 시스템을 통한 획득이 이루어져야 한다. 이렇게 획득된 증거는 미국 연방증거법 Rule 901 (b)에서 진정성 입증 방법으로 예시한 '절차나 시스템'을 통해 수집된 증거에 해당한다. 수집하는 증거에 증거 제출자의 주장을 뒷받침하기 위해서 다음의 내용을 포함해야 한다〔4〕.

- ○ 작성자
- ○ 작성 시각
- ○ 증거 생성 시각
- ○ 첨부파일
- ○ 본문
- ○ IP 주소

위 항목들을 모두 포함하면서 자동화 된 시스템에 의해 웹 게시물을 수집하면 증거 수집 과정에서의 진정성을 입증할 수 있다. 웹 게시물 증거는 앞 절에서 언급하였듯 전문증거에 포함되므로 진정성을 만족하더라도 전문증거의 예외로 간주되지 않는 이상 증거능력을 만족시킬 수 없다. 국내에서는 형사소송법 제313조~316조에서 전문서류와 전문진술에 대한 몇 가지 전문법칙 예외 규정을 마련하고 있다. 특히 제315조에서는 '당연히 증거능력이 있는 서류'에 대해 규정하여 공적인 증명문서와 업무상 작성된 통상 문서에 대해 전문 법칙의 예외로 삼고 있다. 업무상 작성된 통상 문서는 기계적 기재를 포함한다. 즉, 웹 게시물 증거가 웹 게시물 공증 시스템에 의해 기계적으로 생성되고 법률의 위임을 받은 공증인에 의해 공증된다면 전문증거 배제원칙의 예외가 되어 증거 능력을 가질 수 있다.

III. 웹 게시물 공증 시스템의 설계

3.1 기존 공증 시스템과의 비교

미국 Surety LLS 사는 'AbsoluteProof'라는 디지털 공증 시스템을 개발하였는데, 이 시스템은 전자문서가 특정한 시각에 생성되었고 생성된 이후에는 변경되지 않았음을 보장해준다[5]. 즉, 전자 문서의 작성 시간과 내용에 대해 공증을 하는 시스템이다. 하지만 이 시스템은 사용자 PC에 저장된 파일에만 적용할 수 있다는 한계가 있다. 따라서 이 시스템을 이용하여 웹 게시물을 공증하려면 일단 웹 게시물을 파일 형태로 저장해야 하는데, 웹 게시물의 캡처 이미지 파일이나 웹 게시물의 HTML 코드를 저장한 파일이 그 대상이 될 수 있다. 일견 이 파일을 대상으로 'AbsoluteProof'를 이용하여 공증하면 새로운 공증 시스템의 개발 없이 기존 기술로 웹 게시물을 공증할 수 있는 것처럼 보인다. 그러나 캡처 이미지나 HTML 코드는 쉽게 조작이 가능하므로, 이를 대상으로 공증한 결과물이 특정 시각의 웹 게시물의 상태를 항상 그대로 반영하는 것은 아니다. 웹 게시물을 공증하기 위해서는 조작의 우려가 있는 파일 등의 가공된 형태가 아닌, 웹에 게시된 내용 그대로를 공증 대상으로 삼을 수 있어야 한다. 기존 공증 시스템이 사용자 PC에 설치된 클라이언트와 공증 웹 서버 간의 통신으로 파일에 대한 공증이 완료된다면, 웹 게시물 공증 시스템은 웹에 게시된 내용을 받아오기 위해 OSP(온라인서비스제공자) 서버의 중개자 역할이 추가적으로 요구된다. 위 내용을 바탕으로 웹 게시물을 기존의 공증 시스템을 사용하여 공증하는 경우와 웹 게시물 공증 시스템으로 공증하는 경우를 비교하면 [표 2]와 같다.

3.2 웹 게시물 공증 시스템의 구성 요소

웹 게시물 공증 시스템은 웹 사이트의 특정 사용자가 작성한 게시물에 대한 진정성을 확보하는 시스템으로서 웹 게시물의 증거화를 요청하는 공증 요청자, 해당 웹 게시물이 게시된 OSP의 서버, 공증 결과물을 산출하는 공증 서버, 시점확인을 담당하는 시점확인 인가자로 구성된다. 공증 서버에 의한 공증의 결과물은 Digital Evidence Bag(이하 'DEB'로 표기)의 형태로 생성된다.

[표 2] 기존의 공증 시스템과 웹 게시물 공증 시스템 비교

	기존 공증 시스템	웹 게시물 공증 시스템
대상	파일 (캡처 이미지/HTML 코드)	OSP 서버에 저장된 내용
조작 가능성	있음 (이미 파일이 조작된 경우)	없음 (OSP 서버의 내용 그대로를 반영)
OSP 역할	없음	사용자와 공증 시스템의 중개자 역할

3.2.1 공증 요청자

공증 요청자는 공증 시스템에 특정 웹 게시물에 대한 공증을 요청하는 사용자이다. 공증 요청자는 사이버 명예훼손이나 인터넷 거래 사기 등 웹 게시물과 관련된 다양한 사건에서 웹 게시물의 내용을 증거로 제시하기 위해 공증을 요청할 수 있다. 공증 요청자는 웹 게시물의 공증을 요청함으로써 공증 작업을 개시하는 역할을 한다.

3.2.2 OSP 서버

OSP 서버는 공증 요청자가 특정 웹 게시물에 대한 공증을 요청하면 해당 웹 게시물에 대한 정보를 공증 서버에 전달하는 역할을 한다. 여기서 말하는 OSP 서버란, 요청된 웹 게시물이 게시된 사이트를 운영하는 OSP의 DB 서버를 의미한다. 웹 게시물 증거가 진정성을 얻기 위해서는 게시된 상태 그대로를 공증해야 하며, 이를 위해서 캡처 화면이나 HTML 코드가 아닌, OSP의 서버에 기록된 웹 게시물의 정보를 가져온다. OSP 서버는 공증을 요청한 특정 웹 게시물에 대한 정보만을 공증 서버에게 안전하게 전달해야 한다.

3.2.3 공증 서버

공증 서버는 공증 요청자가 공증을 요청한 웹 게시물의 정보를 OSP로부터 전달받아 이를 바탕으로 공증 결과물을 생성하는 역할을 한다. 웹 게시물에 대한 공증은 법적 허용성을 가진 웹 게시물 증거를 생성하기 위해 실시하는 것이므로 작성자, 작성 시각, 내용과 같은 특정 내용을 반드시 포함하고 있어야 한다. 또한 이러한 정보가 OSP 서버의 DB에 흩어져 있으므로 이들을 조합하여 형태를 갖춘 웹 게시물 증거를 생성해야 한다. 이러한 웹 게시물 증거의 형태로 본 논문에서는 Web Postings Evidence Bag(이하

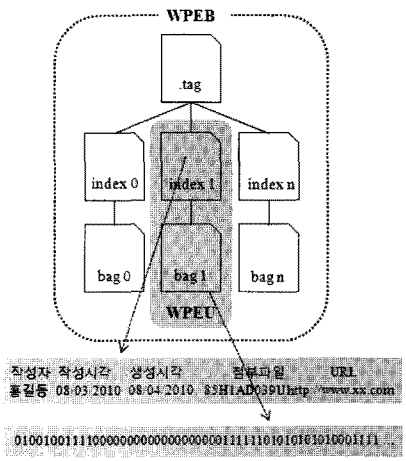
'WPEB'로 표기)를 제안한다. WPEB는 웹 게시물 증거를 위한 일종의 DEB이다. DEB는 머리카락, 흉기와 같은 물리적 증거를 연계 보관성과 무결성 유지를 위해 증거 보관용 봉투에 밀봉하여 보관하는 것처럼 디지털 증거를 변경되지 않도록 안전하게 보관할 수 있도록 하는 디지털 증거 보관소이다. DEB는 여러 개의 Evidence Unit(이하 'EU'로 표기)으로 구성되는데, 활성 데이터가 증거 수집 대상이라 하면 네트워크 정보, 물리 메모리 정보 등이 각각 EU를 구성하고 DEB는 활성 데이터 전체를 관리하는 역할을 하게 된다[6]. DEB는 각 EU에 대한 정보와 해당 DEB의 생성자, 생성시각, 관련 사건번호 등을 기록한 tag file을 통해 해당 DEB 내의 증거를 관리한다. EU는 index file과 bag file로 구성되는데, index file에는 해당 디지털 증거의 메타데이터를 기록하고 bag file에는 실제 증거의 내용을 보관한다.

WPEB는 DEB와 같은 형태를 가지며, 여러 개의 Web Postings Evidence Unit(이하'WPEU'로 표기)으로 구성된다. WPEU는 웹 게시물의 최소 보관 단위이며, 하나의 웹 게시물 자료 당 하나의 WPEU를 생성한다. WPEB를 구성하는 tag file은 여러 개의 WPEU를 관리하기 위한 헤더 부분이고 index와 bag file은 각 WPEU의 메타데이터와 내용을 저장한다. WPEU에는 웹 게시물의 실질적인 정보가 기록되는데, index file에는 웹 게시물 증거의 진정성을 입증하기 위해 필요한 작성자, 작성시각, 증거 요청자, 증거 생성 시각, 웹 게시물이 위치한 IP 주소, 첨부파일의 해쉬값 정보를 저장하고 본문내용은 bag file에 나누어 저장한다. 이를 도식화 하면 [그림 3]과 같다.

웹 게시물을 WPEB 형태로 관리하면 보관하기 용이하고, 인증 및 보관 단계부터 법정에 제출되는 일련의 과정에서 절차 연속성과 무결성을 유지할 수 있으며, 한 사건에서 발생할 수 있는 디지털 증거를 DEB로 관리할 때 WPEU를 그대로 DEB의 EU로 가져갈 수 있으므로 사건의 증거 관리 차원에서도 유리하다.

3.2.4 시점확인 인가자

시점확인 서비스란 임의의 디지털 데이터가 특정한 시점에 존재하였으며, 특정 시점 이후에는 데이터의 내용이 변경되지 않았음을 증명해주는 서비스이다[7]. 전자 공증은 전자 문서의 '내용'과 '시점'에 대한



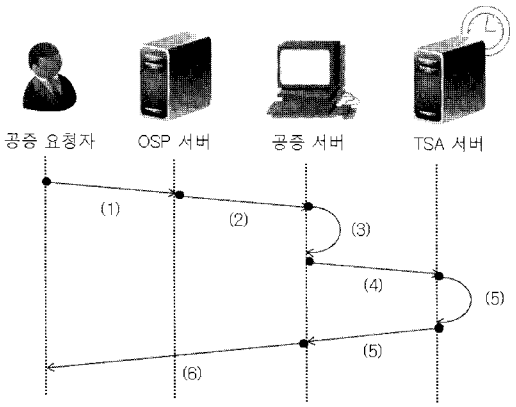
[그림 3] WPEB 구조도

증명을 해주는 것인데, 여기에서 '시점'에 대한 증명을 시점확인 인가자(TSA)로부터 얻는다. 시점확인 인가자는 디지털 데이터와객관적인 시각 정보를 결합한 뒤 시점확인 인가자의 전자 서명을 넣어 시점확인 토큰을 생성한다[8]. 시점확인 토큰은 일종의 시각이 찍힌 도장 역할을 하여 특정 시각에 해당 데이터가 존재하였음을 증명한다. 공증 서버는 OSP 서버에서 획득한 웹 게시물의 정보를 바탕으로 WPEB를 생성한 뒤, 시점확인 인가자에 WPEB의 정보를 전달하여 WPEB에 대한 시점확인 토큰을 획득한다.

3.3 웹 게시물 공증 시스템의 작동 방식

웹 게시물 공증 시스템은 앞서 설명한 공증 요청자, OSP 서버, 공증 서버, 시점확인 인가자가 신뢰할 수 있는 프로토콜을 통해 상호 통신하면서 WPEB를 생성한다. 웹 게시물 공증 시스템의 작동 방식은 [그림 4]와 같다.

(1) 공증 요청자가 특정 웹 게시물에 대한 공증 요청을 OSP 서버에 보낸다.
(2) OSP 서버는 해당 웹 게시물에 대한 정보를 DB로부터 추출하여 공증 서버에 전달한다. 공증 서버와의 통신은 신뢰할 수 있는 프로토콜을 이용한다. 이 때 전달하는 웹 게시물 정보는 웹 게시물 증거가 법적 효력을 얻기 위해 필요한 작성자, 작성 시각, 작성자 IP 주소, 증거 요청자, 첨부 파일이다.
(3) 공증 서버는 OSP 서버로부터 전달 받은 웹 게시물 정보를 바탕으로 WPEB를 구성한다.



〔그림 4〕 웹 게시물 공증 시스템 동작 과정

(4) 공증 서버는 TSA 서버에 구성한 WPEB에 대한 시점확인 토큰 발급을 요청한다.
(5) TSA 서버는 시각 원천으로부터 얻은 객관적 시각 정보를 공증 서버로부터 받은 WPEB의 정보와 결합한 시점확인 토큰을 공증 서버에 전달한다.
(6) 공증 서버는 WPEB와 시점확인 토큰을 결합하고 여기에 공증 시스템 운영 기관의 전자 서명을 첨가한다.

3.4 웹 게시물 공증 시스템의 요구 사항

3.4.1 첨부 파일의 해쉬값 획득

첨부 파일은 문서, 사진, 음악, 동영상 파일 등이 될 수 있고, 파일에 따라 많은 용량을 차지한다. 웹 게시물에 첨부된 모든 파일을 그대로 WPEB에 넣어 저장하는 경우 공간을 비효율적으로 많이 차지하게 된다. 따라서 첨부 파일은 공증 요청자가 개별적으로 보관하도록 하고, WPEB에는 그 해쉬값만을 저장하여 차후 첨부 파일의 진정성 여부가 쟁점이 될 때에 두 해쉬값을 비교할 수 있도록 한다. 첨부파일의 해쉬값은 WPEU의 메타데이터가 되어 index file에 저장된다.

3.4.2 신뢰성 있는 시스템

웹 게시물 공증 시스템은 다음의 두 가지 측면에서 신뢰성을 가져야 한다.

첫째, 이 시스템을 통해 생성된 웹 게시물 증거는 법적 효력을 발휘하므로, OSP 서버로부터 정확한 정보를 받아 오류 없이 WPEB를 생성해야 한다. 또한 공증 시스템의 전자 서명을 거친 공증된 웹 게시물 증거는 어떠한 위·변조 행위에 대해서도 안전해야 한다.

둘째, 공증 시스템을 이루는 각 구성 요소 간의 통신이 신뢰할 수 있는 프로토콜을 통해 이루어져야 한다. 즉, 이들의 통신 채널은 안전하게 암호화 되어야 하고, 공증 서버를 가장한 침입자가 OSP 서버에 접근할 수 없어야 한다. 이는 OSP 서버-공증 서버, 공증 서버-TSA 서버 간의 통신에 모두 적용된다.

IV. 웹 게시물 공증 시스템 도입을 위한 법률적·제도적 요구사항

3장에서는 웹 게시물 공증 시스템 구축을 위한 기술적 요소들에 대해 살펴보았다. 하지만 이러한 기술적 요소를 바탕으로 한 공증 시스템이 도입되어 실제 사용되기 위해서는 법률적, 제도적으로 뒷받침되어야 할 요소들이 존재한다. 우선 공증 시스템을 공정하게 운영할 수 있는 기관이 선정되어야 하고, 공증 시스템에서 나온 결과물에 오류가 없는지 검증도 되어야 한다. 또한 무엇보다 웹 게시물의 정보를 얻기 위한 OSP의 협조를 이끌어내야 할 필요성도 있다. 이를 위해서 요구되는 법률적, 제도적 요구사항에는 어떠한 것들이 있는지 본 장에서 살펴본다.

4.1 운영 기관에 대한 인증

웹 게시물 공증 시스템의 도입을 위해서는 공증 서버를 운영할 기관의 참여와 시스템의 구축이 요구된다. 공증 서버를 운영하는 기관은 증거 생성 과정에서 공정성을 유지할 수 있도록 수사 기관에서 독립적이고 신뢰할 수 있는 제 3의 기관(TTP, Third Trusted Party)이어야 한다. 공증된 웹 게시물을 법적 허용성을 가진 증거로 인정하기 위해서는 공증 시스템의 기술적 완전성도 중요하지만 시스템을 운영하는 기관의 공정성 및 신뢰성 또한 중요하기 때문이다.

'공증인법'에서는 공증 직무를 담당할 수 있는 자격조건을 명시하여 특정 자격을 갖춘 사람만이 공증인이 될 수 있도록 제한하였다. 이 법은 2009년 일부 개정되어, 공증력을 부여하는 대상에 전자문서를 포함하고 전자문서 공증 방식에 전자서명을 이용하는 방안을 담았다. 이처럼 웹 게시물 공증 시스템 인증에도 새로운 법률을 도입하기 보다는 기존의 공증인법과 공증인법 시행령을 개선하는 방안을 사용할 수 있을 것이다. 웹

게시물 공증 시스템 운영 기관은 기술적인 전문성이 요구되기 때문에 법률적 지식만을 가진 기존의 공증인이 운영하기에는 어려움이 있으며, 따라서 시스템과 보안에 전문적인 지식을 가진 자를 포함한 기관에 공증인에 자격을 부여하도록 해야 한다.

4.2 시스템 산출 증거에 대한 검증 절차 제도화

웹 게시물 공증 시스템은 단순히 이미 생성된 자료에 법적 효력을 부여하는 것이 아니라 OSP 서버에서 웹 게시물 정보를 가져와 WPEB 형태의 증거를 생성한다. 따라서 웹 게시물 증거에 법적 효력을 부여하기 위해서는 시스템이 오류 없이 정확한 결과물을 산출한다는 것을 보증할 수 있어야 한다. 이를 위해 정확한 결과물을 산출하는지에 대한 검증 절차를 제도화하여야 한다. 현재 미국의 NIST(National Institute of Standards and Technology)에서는 디지털 포렌식 도구를 검증하는 Computer Forensic Tool Testing(이하 'CFTT'로 표기) 제도를 운영하고 있다. CFTT는 까다로운 검증 절차를 거쳐 모든 테스트를 통과한 디지털 포렌식 도구에 그 정확성과 신뢰성을 인증하는 제도이다. CFTT 인증을 받은 디지털 포렌식 도구를 통해 산출된 결과는 일반적으로 법정에서 신뢰성있는 과학적 증거로 받아들여진다[9]. 따라서 웹 게시물 공증 시스템에도 CFTT와 같은 검증 프로그램을 통해 과학적 신뢰성을 인정받을 수 있도록 하는 검증 제도가 요구된다.

4.3 OSP 협조를 위한 컴플라이언스 형성

공증 요청자가 요청한 웹 게시물에 대한 정보를 공증 서버가 얻기 위해서는 OSP 서버의 중간자 역할이 필요하다. 하지만 공증 서버가 요청하는 웹 게시물 관련 정보를 제공하게 되면, 서버에 대한 트래픽과 OSP의 업무가 증가할 뿐만 아니라 보안 상에도 취약점이 발생할 가능성이 생긴다. 이 때문에 OSP가 협조를 꺼려할 수 있는데, 이를 막기 위해 OSP가 공증 서버에 웹 게시물 관련 정보를 제공하도록 법적으로 강제할 수 있다. 하지만 공증 시스템 도입과 관련하여 해결해야 할 문제를 무조건 법적으로 해결하려면 시간적, 경제적인 비용이 많이 발생한다. 따라서 이보다는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 제44조의 4에서 규정한 정보통신서비스 제공자 행동강령을 활용하여 OSP의 협조를 이끌어낼 수 있다. 정보통신망법 제44조 4에서는 '정보통신서비스 제공자단체는 이용자를 보호하고 안전하며 신뢰할 수 있는 정보통신서비스를 제공하기 위하여 정보통신서비스 제공자 행동강령을 정하여 시행할 수 있다'고 명시하고 있다. 이용자의 명예 훼손과 경제적 손실을 가져올 수 있는 악의적인 웹 게시물을 향후 법정에서 증거로 활용하도록 하는 것도 하나의 이용자 보호의 방법이다. 따라서 웹 게시물 공증 시스템에 대한 OSP 협조 항목을 정보통신서비스 제공자 행동강령에 포함하도록 한다면 새로운 법률의 제정 없이도 OSP의 협조를 이끌어낼 수 있을 것이다.

V. 결 론

웹 게시물은 수정 및 삭제가 용이하여 진정성을 입증하기 위해서는 전통적인 디지털 증거보다 철저한 방법의 수집 및 보관이 이루어져야 한다. 웹 게시물의 화면 캡처 및 HTML 소스 코드 획득의 방법은 악의적인 목적에 의해 정확한 사실 관계를 나타내기 어려우므로 진정성에 대한 이의가 제기될 가능성이 높다. 진정성을 입증하기 위해서는 사용자가 증거화 하기 원하는 웹 게시물이 있는 서버에 접근하여 자동적으로 획득하고, 수사 혹은 재판 절차가 종결될 때까지 변화하는 과정을 기록하면서 보관해야 한다. 이러한 웹 게시물 공증 시스템에 공증력을 부여하기 위해서는 신뢰성과 독립성을 가진 제 3의 기관에 운영을 맡겨야 하며 이 기관을 인증할 수 있는 법률이 필요하다. 뿐만 아니라 본 시스템의 성공 여부는 OSP의 협조 여부에 달렸으므로 컴플라이언스 형성을 통한 협조를 이끌어내야만 한다.

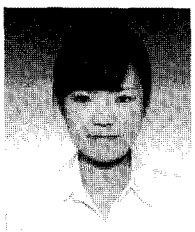
본 논문에서는 새로운 웹 게시물 증거화 방안이 도입되어야 하는 이유를 역설하였고, 웹 게시물이 법적 효력을 갖기 위해 갖춰야 할 조건에 대해 살펴보았다. 또한 이러한 조건을 갖춘 웹 게시물 증거를 생성할 수 있는 웹 게시물 공증 시스템의 구성 요소와 작동 방식 그리고 요구 사항에 대해 제안하였으며, 이 시스템이 성공적으로 도입될 수 있도록 뒷받침되어야 할 법률적, 제도적 요구 사항을 살펴보았다.

참고문헌

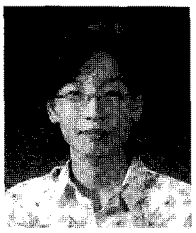
[1] Sara J. Piasecki, "Legal Admissibility of Electronic Records as Evidence and Implications for Records Management,"

American Archivist, vol. 58, pp. 54-64, Winter 1995.
[2] Arthur Best, Evidence : examples and explanations, Aspen Publishers, 2007.
[3] Cornell University Law School, Federal Rules of Evidence, http://www.law.cornell.edu/rules /fre.
[4] Gregory P. Joseph, Internet and Email Evidence 2008, http://www.josephnyc.com /articles/viewarticle.php?58K.
[5] Surety LLC, "Ensuring Record Integrity with AbsoluteProofSM," Technical Whitepaper, Surety LLC, 2003.
[6] Philip Turner, "Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags," Digital Investigation, vol.4 , no.1, pp.30-35, 2007.
[7] 장혜진, "전자 서명과 시점 확인 서비스의 결합," 한국산학기술학회논문지, 10(2), pp.337-387, 2009.
[8] 이상진, 디지털 포렌식 개론, 이룬, 2010.
[9] James R. Lyle, Ph.D., "NIST CFTT: Testing Disk Imaging Tools," International Journal of Digital Evidence, vol.1, no.4, 2003.

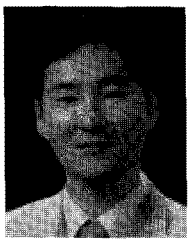
〈著者紹介〉



김 아 름 (Ahreum Kim) 학생회원
2009년 2월: 고려대학교 산업시스템정보공학과 졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 디지털 포렌식, 포렌식 어카운팅, 내부통제, e-Discovery



김 역 (Yeog Kim) 학생회원
1992년 2월: 성신여자대학교 전산학과 졸업
2003년 2월: 고려대학교 정보보호대학원 공학석사
2010년 8월: 고려대학교 정보보호대학원 공학박사
2010년 9월~현재: 한신대학교 컴퓨터공학부 초빙강의교원
〈관심분야〉 디지털 포렌식, 포렌식 어카운팅



이 상 진 (Sangjin Lee) 정회원
1987년 2월: 고려대학교 수학과 졸업
1989년 2월: 고려대학교 수학과 이학석사
1994년 2월: 고려대학교 수학과 이학박사
1989년 10월~1999년 8월: ETRI 연구원
2001년 9월~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수