情報保護學會論文誌
第18卷 第5號, 2008. 10

E-Discovery를 위한 디지털 증거 전송시스템에 대한 연구

이 창 훈†, 백 승 조, 김 태 완, 임 종 인‡
고려대학교, 정보경영공학전문대학원

A Study on Digital Evidence Transmission System for E-Discovery

Chang-Hoon Lee†, Seung-Jo Baek, Tae-Wan Kim, Jong-In Lim‡
Graduate School of Information Management and Security, Korea University

요 약

2006년 12월 미국의 민사소송규칙(FRCP) 개정으로 e-discovery(전자증거개시) 제도가 시행되고 있으나, 이 제도는 디지털 증거의 관리와 제출과정에서 발생할 수 있는 과도한 비용과 시간의 낭비와 같은 다양한 문제점들을 가지고 있다. 현재 e-discovery 제도의 국내 도입 논의가 진행되고 있는 상황에서 본 논문에서는 e-discovery의 절차 중 디지털 증거를 소송상대방에게 제출하는 production 단계에서 발생할 수 있는 민감한 자료 유출, 읽기 불가능, 위·변조 및 손상 등과 같은 문제점에 대해 살펴보고, 이 문제점들을 해결하고 비용과 시간의 낭비를 최소화 할 수 있는 안전한 온라인 디지털 증거 전송 시스템을 제안한다.

ABSTRACT

This paper also suggests the Digital Evidence Transmission System for E-Discovery which is suited to domestic environments in order to solve these problems and promote safe and convenient transmission of the electronic evidences. The suggested Digital Evidence Transmission System for E-Discovery is the system that submit digital evidences to Court's Sever through the Internet using Public Key Infrastructure and Virtual Private Network, and solves the problems - such as privileged and privacy data, trade secret of company, etc.

Keywords : E-Discovery, Transmission system, Digital Evidence

Ⅰ. 서 론

미국의 민사소송규칙(FRCP) 개정으로 2006년 12월 1일 부터 E-Discovery가 의무화가 됨에 따라 기업은 외부로 나가는 모든 전자정보를 보존 및 검색할 수 있는 시스템을 구축하여야 하며 소송에 처한 기업은 이메일을 비롯한 소송과 관련된 기업 내 모든 전자정보를 제출하여야 한다. 이 제도는 아직 국내에 법제화 되지 않았으며 디지털 증거에 관한 구체적인 규정도 없는 상황

접수일 : 2008년 7월 30일; 수정일 : 2008년 9월 11일;
채택일 : 2008년 10월 8일
*본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.(IITA-2008-(C1090-0801-0025))
† 주저자, lookee@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

이지만, 국내 법정에서 일부 디지털 자료의 증거 채택과 개정 형사소송법의 증거개시제도(discovery) 도입, 미국 배심제도 도입, 디지털 증거의 중요성 인식 등 여러 상황을 고려해 볼 때 국내에도 차후 도입이 될 것으로 전망한다. 하지만 e-discovery는 과다한 시간과 비용 문제뿐만 아니라 다양한 문제점들을 내포하고 있으며, 특히 상대방에게 디지털 증거를 제출하는 production 단계에서 많이 발생한다. 따라서 그 production 단계의 문제점들의 해결 방안 없이 국내 도입이 된다면 동일한 문제점들을 유발하게 될 것이다.

본 논문에서는 미국의 e-discovery의 production 단계에서 발생가능한 문제점들을 분석하였으며, 이런 문제점들을 해결하기 위해 디지털 증거 전송 시스템을 제안한다. 이 시스템은 PKI, 해쉬 알고리즘, VPN 등을 사용하여 production을 해야 하는 소송 당사자가 네트워크를 통해 법원의 서버로 직접 ESI(Electronically Stored Information)를 전송하며, 전송 후 응용 프로그램 가상화를 통해 전송된 ESI를 확인하는 방식이다. 이 시스템을 통해 production 단계에서 발생 할 수 있는 문제점들이 해결될 것으로 기대된다.

본 논문의 구성은 2장에서 e-discovery 개요와 국내 도입 가능성 및 ESI 법적 증명력에 대해 살펴보고 3장에서는 e-discovery의 세부 절차를 소개하고 세부 절차 중의 하나인 production 단계에서 발생할 수 있는 문제점들을 분석한다. 4장에서는 이 문제점들을 해결하기 위한 디지털 증거 전송 시스템 제안 및 분석하고 5장에서 결론을 맺는다.

Ⅱ. 연구 배경

2.1 E-Discovery 개요

Discovery(증거개시)제도란 소송당사자가 공판 전에 공판의 준비를 위해 법정 외에서 법정의 방법에 의하여 소송의 issue(쟁점 혹은 쟁점사실)를 명확히 하는 정보 및 증거를 공개 · 수집하는 제도를 말한다. 미국은 우리나라 민사절차와 달리 소송에 처하게 된 당사자가 소송과 관련하여 자신이 무엇을 가지고 있는지 발견하여 상대방에게 공개해야 하여 서로 상대방이 보유한 증거물, 서류, 증인 등을 공개하도록 요청함으로 서로 대등한 조건하에서 소송이 진행 되는데 이 절차가 Discovery이다.

미국 민사소송 당사자는 원칙적으로 우리 민사소송의 "소장과 답변서 교환"에 해당하는 pleadings(소답)를 경유하고, 공판절차가 진행되기 이전에 스스로 자신이 보유한 증거를 공개함과 아울러 상대방 당사자나 제3자에게 증거의 개시를 요구할 수 있다. 즉 당사자는 제소 후 discovery 제도를 통하여 공판절차 이전에 각각 스스로 증거를 수집·보존 해야만 한다. 따라서 소송 당사자가 서로 상대방이 보유한 증거물, 서류, 증인 등을 공개하도록 요청함으로써 서로 대등한 조건하에서 소송이 진행 된다.

2006년 12월 1일 발효된 '미연방민사소송법(FRCP)'에는 discovery의 대상이 되는 증거물의 범위에 ESI를 포함시켰는데 이것이 바로 E-Discovery 이다. 이 법안에 따라 소송에 처한 모든 기업은 소송과 관련된 이메일, 데이터 자료 등을 비롯한 기업 내 모든 전자정보를 수집 및 저장하여 소송개시일로 부터 120일 이내에 제출해야만 한다.

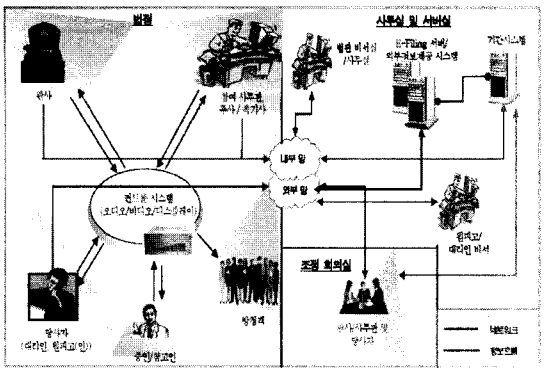
2.2 E-Discovery 국내 도입 예상

2.2.1 민사 소송의 증가

현재 국내 민사 소송은 2000년 이후부터 계속 증가하고 있는 추세이며, 또한 배심제도처럼 국내에 미국 법제 도입, 증거로서의 ESI 중요성 부각 등으로 인해 국내에도 e-discovery의 법제 도입이 될 전망이다. 따라서 민사 소송 절차에서 e-discovery를 위한 디지털 증거 전송 시스템과 같은 체계 없이 도입이 된다면, 디지털 증거 제출과 검토에 따른 시간 및 비용, 업무 부담은 지금보다 더욱 증가 할 것이다. 따라서 증가하는 민사소송의 원활한 업무 진행을 위해 디지털 증거 전송 시스템의 구축이 필요하다.

2.2.2 사법체계의 정보화 추진

사법부는 급변하는 업무환경에 대처하고 업무 효율화와 정보기술의 활용을 통한 대국민서비스를 최우선으로 하는 선진사법행정의 구현을 위하여 사법 정보화를 매년 추진하고 있다. 현재 추진하고 있는 내용으로는 [그림 1]에서 보듯이 2008년 12월을 목표로 진행 중인 법정의 재판진행정보를 실시간으로 디지털화하여 재판사무의 효율성을 증대하기 위한 전자법정시스템 구축과 배심제도 도입에 따른 재판사무시스템을 구축, 전자법



〔그림 1〕 전자법정 시스템 개념도

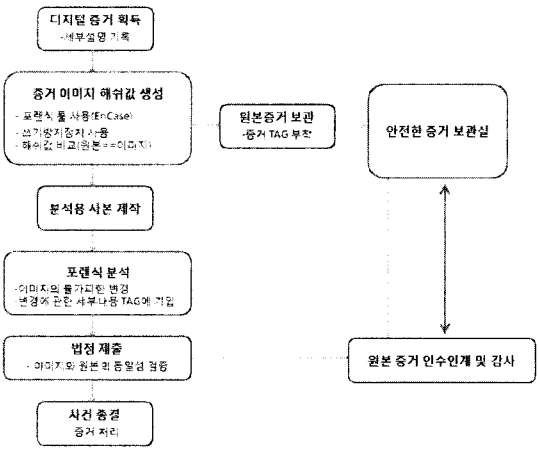
원 및 전자민원 포털 구축 등이 있으며, 또한 형사사법 관련 기관과 중앙 행정부처 및 자치단체의 모든 형사 관련 정보를 통합하여 하나의 시스템으로 구축하는 사업인 형사사법통합정보체계를 추진 중에 있다.

2008년부터 시행한 배심제도에 따른 재판사무시스템을 구축 및 개발을 한 것처럼, 사법부는 새로운 법률 도입 및 시행에 맞춰 정보화 사업을 추진하고 있다. 따라서 e-discovery가 국내 도입 시에 사법부는 그에 맞는 정보화 사업 또한 실시 할 것으로 예상되며, 그 사업의 일환으로 디지털 증거 전송 시스템을 구축함으로써 원활한 민사 소송을 지원하고 사법체계의 정보화에도 동조할 수 있을 것이다.

2.3 ESI의 법적 증명력

디지털 증거는 다른 증거와는 달리 변경, 훼손이 용이하다는 특징이 있으므로 최초 증거가 저장된 매체에서 법정에 제출되기까지 변경이나 훼손이 없었다는 점이 입증 되어야 한다. 국내 형사소송법에 의하면 컴퓨터 관련증거의 증거능력을 인정하기 위해서 우선 당해 기록이 진정(眞正)하게 성립되어야 하고 무결성이 보장되어야 하기 때문에, 현재 국내·외 수사 기관에서는 ESI의 법적 증명력을 갖추기 위해 해쉬(hash) 함수나 암호기술 등을 이용해 [그림 2]와 같은 절차를 통해 디지털 증거를 취급하고 있다.

- 진정성(眞正性, Authenticity) : 저장 및 수집과정에서 오류가 없었으며, 특정한 사람의 행위의 결과가 정확히 표현되었고 그로 인해 생성된 자료임이 인정되어야 한다는 것
- 무결성(無缺性, Integrity) : 최초 저장된 매체에서



〔그림 2〕 일반적인 디지털 증거 취급절차

법정에 제출되기까지 변경이나 훼손이 없었다는 점이 입증되어야 한다는 것

또한 민사소송의 e-discovery에서 ESI 진정성의 문제점이 부각이 되고 있어 이에 대한 해결 방안으로 해쉬함수를 포함한 PKI나 전자서명 등을 거론 하고 있으며, 특히 Utah 주에서는 Digital Signature Law를 1995년에 시행하여 ESI의 디지털 서명을 통해 법적 증거로써 활용하고 있다.

따라서 수집된 ESI를 오프라인(Off-Line) 방식이 아닌 온라인(On-Line) 방식으로 법원이나 소송 당사자 등의 특정 대상에게 전송 할 경우, ESI의 진정성과 무결성을 보장하면서 전송이 된다면 ESI가 증거로써 법적 증명력을 가질 수 있게 된다.

2.4 On-Line과 Off-Line의 전송 방식 비교

ESI를 상대방에게 전달하는 방식은 네트워크를 이용한 온라인(On-Line) 방식과 사람이 직접 전달하는 오프라인(Off-Line) 방식으로 구분할 수 있으며, 온라인은 다시 인터넷과 같은 공중통신망과 공중통신망 일부를 독점적으로 사용하는 전용 회선망으로 나눌 수 있다. 각 방식에 의해 ESI 전달 시, 시간과 비용 등의 특징은 [표 1]에서 보듯이 온라인 방식이 오프라인 방식보다 유리하며, 그 중 공중 통신망은 기존 인터넷 망을 사용함으로써 전용 회선망보다 훨씬 저렴하며, 편리성과 확장성 또한 보장이 된다.

따라서 ESI의 보안성과 무결성이 보장 된다면 오프라인으로 전송하는 것 보다 공중망을 이용하여 온라인

〔표 1〕 전송 방식 비교

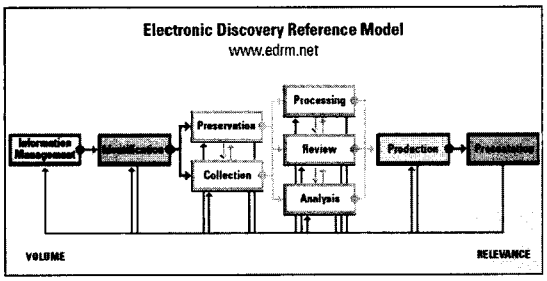
구 분		전달 시간	비 용	편리성 및 확장성
온라인 전송	공중 통신망	빠름	기존 인터넷 망 사용으로 저렴	확장성과 이동성 제공
	전용 회선망	빠름	구축 및 유지 비용 증가	광역화 및 확장성 한계
오프라인 전송		느림	거리 차에 비례	해당사항 없음

으로 전송하는 것이 더 효율적으로 볼 수 있다.

Ⅲ. E-Discovery의 production 단계의 문제점

3.1 E-Discovery 절차

2005년 5월에 만들어진 EDRM(Electronic Discovery Reference Model)이 제시한 e-discovery의 절차는 [그림 3]에서 보듯이 문서 보유와 관리 정책을 펴는 information management 단계부터 법정에서 전자증거를 제시하는 presentation 단계까지 총 9단계로 구분되어 진다. 각 단계별에서 수행하는 내용은 [표 2]에서 보는 바와 같다.



〔그림 3〕 E-Discovery 절차

3.2 production 단계에서의 문제점

3.1에서 소개한 e-discovery 절차의 각 단계마다 다양한 문제점들을 가지고 있으나, 이 장에서는 production 단계에서 발생할 수 있는 문제점에 대해 분석하였다.

3.2.1 민감한 자료 유출

제출 이전의 Review 단계에서 민감한 자료에 대한 검토를 실시하지만, 경우에 따라 수십 수백만 건이 넘는 자료를 모두 검토한다는 것은 거의 불가능하다.

상대방에게 ESI를 production 한 후에, 그 내용 중에 실수로 고객과 변호사간의 상담 내용과 같은 privileged 된 자료나 고객 및 개인의 신상정보, 사생활이 담긴 e-mail 등의 privacy 자료, 기업의 영업 비밀 등이 포함될 수 있다. 만약 그 자료를 받은 상대방은 그것을 역이용하여 재판이나 개인 이득을 위해 사용할 수도 있으며, 관리 소홀이나 분실로 인해 기업의 고객 정보와 같은 정보가 유출 되었을 경우에는 기업 이미지 실추뿐만 아니라 고객에 의한 집단 소송까지 발생할 수도 있다.

이와 관련한 판례로 'Chan v. Dynasty Executive Suites Ltd' 소송과 'Dublin v. Montessori Jewish Day School of Toronto' 소송은 피고가 production한 내용 중에 실수로 privileged documents나 이메일이 포함된 것을 안 뒤, 원고의 변호사에게 반환을 요구했으나 원고

〔표 2〕 e-discovery 각 단계별 수행 내용

절 차	수 행 내 용
Information Management	· 조직 내의 문서보유 및 관리 정책을 통하여 특정 정보를 유지하고 관리하는 단계
Identification	· 보존해야할 의무가 있는 데이터나 소송이 발생할 경우에 필요한 모든 관련 정보의 위치를 확인하는 단계
Preservation	· ESI가 파괴나 변형되지 않도록 보장해야 하는 단계
Collection	· tape, drive, 이동식 저장장치 등 모든 소스(source)에서 자료 수집을 하는 단계
Processing	· 전체적인 데이터에서 중복되거나 관련이 없는 데이터를 필터링을 하며 또한 수집된 데이터를 상대방이 확인할 수 있는 포맷으로 변환하는 단계
Review	· 수집된 데이터에 중에 비밀성을 요구하거나 privileged 된 데이터가 있는지에 대한 탐색과 평가를 하는 단계
Analysis	· ESI에 관련된 핵심 단어, 증인, 전문용어, 중요한 문서를 요약하여 평가하는 단계
Production	· 상대방의 당사자나 변호사 등에게 소송 지원 소프트웨어인 Automated Litigation Support(ALS) 등을 이용하여 ESI를 다양한 미디어에 저장 후 상대방에게 제출하는 단계
Presentation	· 증언조서, 청문회, 법정 등에서 효과적인 방법으로 ESI를 제출하는 단계

가 거부하여 발생한 소송이며, 'Shred-Tech Corp. v. Viveen' 소송은 원고가 production한 내용 중에 에 피고의 전화 통화 기록이 포함되어 있었으나, 이것

은 피고의 동의나 법원의 허락 없이 녹음을 한 것이여서 privacy에 대한 침해로 소송한 경우가 있다.

3.2.2 읽기 불가능

소송지원 소프트웨어인 ALS(Automated Litigation Support)를 사용하여 ESI를 저장한 경우에 대부분은 상대방이 쉽게 원하는 디지털 자료를 검색하거나 읽는 것이 가능하다. 하지만 그렇지 않은 경우에는 당사자는 해당 데이터에 맞는 프로그램이 설치되어 있어야 하며, 고가의 프로그램일 경우 license 구매에 따른 비용 부담이 있으며, 특히 해당 프로그램이 있더라도 버전이 상이할 시에 읽는 것이 불가능할 수도 있다. 이와 관련한 판례로는 'Logan v. Harper' 의 소송에서 피고가 전자적인 형태에서 검색할 수 있는 인덱스를 사용한 문서를 원고에게 production 하였으나, 인덱스는 전문검색(full-text)이 되지 않았고, 또한 피고의 변호사가 사용한 프로그램을 제공하지 않아 원고는 production한 자료를 확인 불가하여 소송한 사례가 있다.

3.2.3 위·변조 및 손상

민사소송과 관련된 e-discovery의 증거자료 이송 방법은 검찰이 압수수색하여 직접 증거를 이송해가는 방법이 아닌, 검찰의 개입 없이 당사자들에 의해 증거자료를 주고받는 방식이다. 따라서 증거자료는 기업 관련자에 의해 상대방에게 직접 전달되거나 우편이나 배송업체를 통해 전달할 수밖에 없다.

하지만 디지털 증거는 온도, 습기, 물리적 충격, 전자기파 등에 민감하여 이송 중에 증거가 손실 될 수 있다. 또한, 제 3자에 의해 위·변조 및 분실 가능성의 우려 또한 존재하고 있어 증거의 이송 단계 간에 자료가 조작되지 않았다는 것을 의미하는 chain of custody(절차 연속성)를 완벽히 보장할 수 없다.

3.2.4 시간과 비용

저장매체 기술의 발달과 및 디지털 자료량의 증가로 e-discovery를 해야 하는 자료의 양은 커질 수밖에 없다. 따라서 디지털 자료를 보관, 수집 및 분석에 따른 시간과 비용도 크지만 수집된 자료를 production 하기 위해 disk imaging 등의 작업에 소요되는 시간과 비용의 부담뿐만 아니라 이송에 따른 시간과 비용의 부담도 생기게 된다. 특히 타 국가의 기업과 소송이 발생될 경우에는 ESI 이송의 시간과 비용의 부담은 더욱 더 증가하게 된다.

3.2.5 부인(否認) 가능성

ESI를 정상적으로 production 하였지만 상대방이 ESI 자료를 받지 않았다고 부인할 경우나 production 하지 않았는데 했다고 부인할 경우에, 서로 주고받았다는 것을 증명할 증거가 없을 시 이를 확인하기 어려운 경우가 생길 수 있다.

Ⅳ. 디지털 증거 전송 시스템 제안

본 장에서는 앞서 소개한 e-discovery의 production 문제점 해결 및 ESI 제출의 편리성을 도모하는 방안으로 PKI, VPN, Application Virtualization 기술 등을 활용하여 민사 소송 시 기밀성, 무결성, 가용성을 보장하면서 신속하게 ESI를 법원으로 전송 및 열람하기 위한 e-discovery 디지털 증거 전송 시스템을 제안한다.

4.1 시스템 요구 사항

ESI의 무결성, 기밀성, 가용성을 보장하기 위해 디지털 증거 전송 시스템에서 갖추어야 할 각 단계별 요구사항은 [표 3]과 같다.

〔표 3〕 각 단계별 요구사항

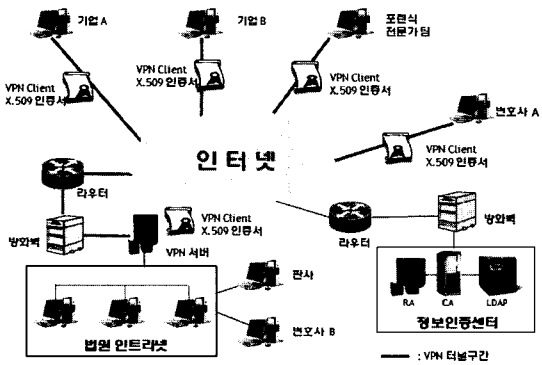
단계	요 구 사 항
전송	1.1 ESI 전송은 보안 통신채널을 통해 암호화 통신을 해야 한다. 1.2 인증된 사용자만 전송이 가능해야 한다. 1.3 전송 간에 ESI의 무결성을 보장해야 한다. 1.4 전송 간에 ESI의 진정성을 보장해야 한다. 1.5 ESI의 Chain of Custody가 보장되어야 한다. 1.6 인터넷 망을 이용하여 전송하여야 한다. 1.7 필요시 수정 후 재전송이 가능해야 한다. 1.8 전송 비용이 저렴해야 한다. 1.9 전송 시점이 명확히 증명 되어야 한다.
인증	2.1 ESI 전송자 및 열람자의 신원확인이 용이해야 한다. 2.2 전송된 ESI의 무결성 검증이 가능해야 한다.

단계	요 구 사 항
인증	2.3 전송 시점 확인이 되어야 한다. 2.4 전송 및 열람 기록은 유지되어야 한다.
저장	3.1 ESI의 무결성 검증 된 후 저장 되어야 한다. 3.2 ESI 송신자의 신원 확인 후 저장되어야 한다. 3.3 저장된 ESI의 기밀성이 보장되어야 한다. 3.4 ESI의 privacy 보호가 가능해야 한다. 3.5 ESI의 보관, 삭제 등의 전반적인 데이터의 관리가 가능해야 한다. 3.6 ESI를 받은 날짜, 시간, 사람의 이름이 기록되어야 한다. 3.7 ESI의 특징(용량, 타입, 속성) 등이 기록되어야 한다.
이용	4.1 인터넷을 통해 열람이 가능해야 한다. 4.2 허가된 인원만 열람이 가능해야 한다. 4.3 이용자는 응용 프로그램 설치 없이 열람이 가능해야 한다. 4.4 재판 시 법정에서도 열람이 가능해야 한다. 4.5 ESI 분석을 위해 디지털 포렌식 전문가 팀과 연동이 되어야 한다. 4.6 ESI 이용 권한 관리가 가능해야 한다.

4.2 구성 방안

전체적인 개념은 production을 해야 하는 각 사용자는 정보인증센터에서 발급 받은 공인인증서와 해쉬 알고리즘 등을 이용하여 인터넷을 통해 법원의 VPN 서버에 접속 후 ESI를 전송하는 것이다. 전송된 ESI는 접근이 허가된 양측 변호사, 당사자 및 판사가 자료를 열람하는 방식으로 [그림 4]와 같은 개념도를 제시한다. 각 구성요소의 역할 및 기능은 [표 4]에서 보는바와 같다.

[그림 4]에서 제시한 개념도를 만족시켜주기 위해서 법원 인트라넷에서는 사용자 인증과 전송된 ESI에 대한 무결성 검증 및 보관, ESI 접근권한에 대한 책임을



〔그림 4〕 디지털 증거 전송 시스템 개념도

〔표 4〕 구성요소의 역할 및 기능

구성 요소	역할 및 기능
기업, 포렌식 전문가	· ESI를 수집/분석 후 법원에 제출 · 상대방이 제출한 ESI 열람 및 분석
정보인증센터	· 신원 확인 후 공인인증서 발급 · 인증서 폐지 목록 제공
법 원 인트라넷	· 디지털 증거 관리 센터 운영 · 사용자 인증, ESI 무결성 검증 및 보관에 관한 책임 · ESI의 열람 가능한 환경 제공
변호사	· 의뢰인 및 상대방의 ESI 열람 및 분석
판 사	· 재판에서 필요 시 ESI 열람

〔표 5〕 디지털 증거 센터의 요구사항, 관련기술 및 효과

단계별 요구 사항		관련 기술	효 과
전송	1.1, 1.2, 1.3, 1.4 1.6, 1.8, 1.9	PKI, 타임스탬프 해쉬 알고리즘	· 무결성 · Chain of Custody
인증	2.1, 2.2, 2.3	PKI, VPN, 타임스탬프	· 기밀성 · 무결성
저장	3.4, 3.5, 3.6, 3.7	Management S/W	· Privacy
이용	4.1, 4.2, 4.3, 4.6	PKI, ACL Application Virtualization	· 기밀성 · 가용성

갖는 디지털 증거 관리 센터의 구축이 필요하다. 4.1의 시스템 요구사항 중 디지털 증거 관리 센터가 갖추어야 하는 요구사항과 이를 만족시켜주는 관련 기술 및 효과는 [표 5]에서 제시하였으며, 관련 기술의 개략적인 설명은 [표 6]과 같다.

4.3 절 차

4.3.1 사전 단계

각 사용자들은 공인인증서비스의 절차에 따라서 인증서를 발급받아 저장한다. VPN 클라이언트 프로그램에서는 저장된 인증서를 불러들여 내장(import)하게 된다. VPN 서버 장비의 경우도 관리자를 통하여 인증서를 받아 장비에 내장하게 된다.

VPN 클라이언트와 서버 장비는 각각에 내장된 인

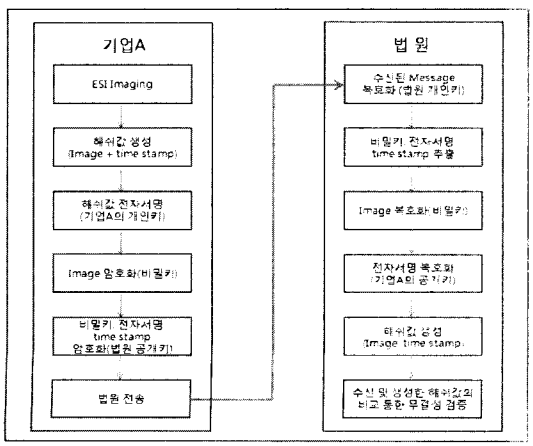
〔표 6〕 관련 기술 설명

기 술	기 능 설 명
PKI (Public Key Infrastructure)	· 공중망 사용자들이 신뢰할 수 있는 기관에서 부여한 한 쌍의 공개키와 개인키를 사용함으로써, 안전하고 은밀하게 데이터나 자금을 교환할 수 있게 해주는 기술 · 메시지 송신자의 인증 및 메시지 암호화 가능
VPN (Virtual Private Network)	· 일반 공중 TCP/IP 망을 통해 연결된 두 개 이상의 네트워크가 서로 연결된 네트워크로 인식 되도록 하는 기법 · 전용회선 보다 저렴하게 WAN(Wide Area Network)을 구축
해쉬 알고리즘 (Hash Algorithm)	· 데이터 무결성 및 메시지 인증 등에서 사용할 수 있는 함수로써 정보보호의 여러 메커니즘에서 이용되는 핵심 요소기술 · 임의의 길이의 비트 열을 고정된 길이의 출력값인 해쉬코드로 압축시키는 함수
타임 스탬프 (Time Stamp)	· 어느 시점에 데이터가 존재했다는 사실을 증명하기 위하여 특정 위치에 표시하는 시각 · 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개 변수
응용프로그램 가상화 (Application Virtualization)	· 어플리케이션을 사용할 때 참조되는 파일 시스템(File System)이나 레지스트리(Registry)와 같은 사항을 가상화하는 기술 · 어떠한 PC에서도 원하는 어플리케이션을 설치하지 않고도 가상화된 파일 및 레지스트리를 통하여 어플리케이션을 바로 사용 가능
접근제어 목록 (ACL : Access Control List)	· 특정 자원에 대하여 접근이 허가되는 역할을 기록해 놓은 목록 · 사용자에게 부여된 접근권한에 따라 작업의 허용 여부 결정

증서를 서로 주고받음으로써 사용자 인증 및 세션 키를 공유하게 되고, 이를 이용하여 구축된 터널링(tunneling)을 통해 각 사용자와 VPN 장비는 안전한 암호 통신을 할 수 있다.

4.3.2 자료 전송 및 검증 단계

법원으로 ESI를 전송할 때 중간에 악의적인 의도를 가진 사람이 메시지를 탈취 및 변조하거나, 송신자로 가장해서 전송하는 경우를 방지하여야 전송된 ESI의 무결성을 보장받는다. 이를 위해서 해쉬 알고리즘, 비밀키, PKI 기술 등의 암호화 기술을 사용하여 ESI를 전송한다. 특성상 대부분 ESI의 Image 데이터는 대용량이므로 공개키로 암호화할 경우 시스템에 효율을 저하시킨다. 따라서 hybrid 암호화 방식을 사용하여 Image 데이터를 비밀키 암호 알고리즘으로 암호화 하고, 이때 사용된 비밀키를 법원의 공개키로 암호화해서 전송한다. 예를 들어 [그림 4]에서 기업A가 기업B에게 소송과 관련된 disk Imaging 파일을 production 하기 위해 법원에 전송 및 검증 절차는 아래와 같다. [그림 5] 참조



〔그림 5〕. 전송 및 검증 절차

① 기업A는 소송과 관련된 disk의 Imaging 처리
② 기업A는 Image 데이터와 타임 스탬프(time stamp)의 해쉬값 생성
③ 기업A는 자신의 개인키로 해쉬값에 전자서명
④ 기업A는 Image 데이터를 비밀키 암호 알고리즘의 비밀키로 암호화
⑤ 기업A는 비밀키, 전자서명, 타임 스탬프를 법원의 공개키로 암호화 후 암호화된 Image 데이터와 함께 전송
⑥ 법원은 자신의 개인키로 메세지를 복호화 하여 비밀키, 전자서명, 타임 스탬프 추출
⑦ 법원은 추출한 비밀키로 Image 데이터를 복호화
⑧ 법원은 기업 A의 공개키로 전자서명을 복호화 하

여 해쉬값 추출

⑨ 법원은 수신된 Image 데이터와 타임 스탬프를 해쉬 알고리즘을 이용하여 해쉬값 생성

⑩ 법원은 두 개의 해쉬값을 비교를 통한 ESI의 무결성 검증

4.3.3 자료 이용 단계

무결성 검증이 완료된 ESI는 법원의 디지털 증거 관리 센터에 저장이 된다. 저장된 ESI는 관리자가 접근권한을 부여한 해당 소송 관련자만 열람 할 수 있으며, ESI의 무결성을 위해 검색 및 읽기 기능만 가능하다. 열람 방법은 공인인증서를 이용하여 디지털 증거 센터의 인증을 거친 후에 가능하며, [그림 4]에서 보듯이 판사나 변호사B의 경우처럼 법원의 인트라넷 PC를 통해서도 가능하다. 사용자는 응용 프로그램 가상화를 통해 자신의 PC에 해당 응용프로그램의 설치 없이 모든 형태의 ESI를 열람할 수 있다.

4.4 제안 시스템 분석

앞에서 제시한 디지털 증거 전송 시스템을 통해 ESI를 전송할 경우, 전송된 ESI에 대한 보안정책이 병행된다면, 3장에서 분석된 e-discovery의 production 단계에서 발생할 수 있는 문제점들을 해결할 것으로 기대 된다.

디지털 증거 전송 시스템에서는 ESI를 PKI와 해쉬 알고리즘 등을 이용하여 암호화 후 VPN을 통해 법원으로 직접 전송된 후 복호화 과정을 통해 무결성이 검증되기 때문에, Off-Line으로 ESI를 전송할 경우와 비교하여 시간과 비용을 줄이면서 ESI의 위·변조 및 손상을 방지할 수 있다. 또한 공인증서를 이용한 ESI의 전자서명과 법원 서버의 접속 및 전송 로그를 통해, ESI 제출 및 열람에 대한 사실을 부인할 수 없다.

법원에 전송된 후에는 ACL을 통해 인가된 당사자만이 ESI를 확인 할 수 있어 제 3자로의 자료 유출을 방지 할 수 있으며, production한 ESI에 실수로 privileged data, 영업 비밀 및 고객정보 등의 자료가 포함 되었더라도 법원이 정한 제출 기한 내에 수정 후 재전송이 가능하여 상대방과의 마찰 없이 민감한 자료 유출 문제를 해결할 수 있다. 또한 응용 프로그램 가상화를 통해, ESI를 열람할 수 있는 인가된 사용자는 추가적인 소프트웨어나 라이선스를 구매할 필요가 없이 다양한 버전의 모든 ESI를 읽을 수 있는 환경을 제공하여 읽기 불가능 문제를 해결할 것으로 기대되며, ESI 열람 시 사용자 PC에 저장하지 않고 viewer 기능만을 제공하기 때문에 ESI의 유출 문제도 예방할 수도 있다.

추가적인 기대효과로는 전자법정 시스템 및 포렌식 전문가 팀과의 연동성을 기대할 수 있다. [그림 1]에서 보듯이 전자법정 시스템은 내·외부망 모두 접속이 가능하여, 재판 시 법원 내부망에 연결된 디지털 증거 전송 시스템에 접속하여 소송과 관련된 ESI를 법정에서 열람 할 수 있어 재판 진행에 도움을 줄 수 있다. 또한 제출된 ESI가 포렌식 전문가 팀에 의해 분석이 요구될 시, 법원의 인트라넷에 ESI 분석을 위한 서버를 추가 운영한다면 virtual digital forensic 기술을 통해 무결성을 보장하면서 ESI를 분석 할 수 있는 환경을 제공할 수 있다.

V. 결 론

본 논문은 e-discovery의 국내 도입에 대비하여 e-discovery 절차 중의 하나인 production 단계에서 발생할 수 있는 문제점들을 분석을 하였으며, 이 문제점들을 해결하는 방안으로 안전한 온라인 디지털 증거 전송 시스템을 제안 하였다. 이 시스템은 PKI, 해쉬 알고리즘 및 VPN 기술 등을 이용하여 법원에 구축된 디지털 증거 관리센터에 ESI를 전송하는 방식으로써, 지금의 Off-Line 방식으로 상대방에게 ESI를 production 할 경우 발생하는 시간과 비용 문제뿐만 아니라 민감한 자료 유출, 읽기 불가능, 위·변조 등의 문제점들을 해결 하여 차후 e-discovery가 국내 도입이 될 시 원활한 민사소송에 기여할 것으로 기대 된다.

참고문헌

[1] 이백훈, "미연방 민사소송규칙상의 discovery 제도", 원광대 대학원, pp.7-8, 2005.

[2] Maria Perez Crist, "Preserving the Duty to Preserve : The Increasing Vulnerability of Electronic Information", *South Carolina Law Review*, Vol. 58, November., 2006.

[3] 사법부, 2008년도 사법 정보화촉진시행계획(안), 의안번호 제368호, 2008.

[4] 양근원, 형사절차상 디지털 증거의 수집과 증거

능력에 관한 연구, 경희대 대학원, pp. 215-218, 2006.

[5] 신재룡, 디지털 포렌식 수사 절차 모델에 관한 연구, 고려대 대학원, pp. 41-45, 2006.

[6] George L.Paul, "The Authenticity Crisis In Real Evidence", *Law Practive Today*, 2006. 3.

[7] http://www.edrm.net

[8] Jeanine M.Anderson, Richard P.Barkley, "The Brave New World of E-Discovery-Part I", *The Colorado Lawyer*, Vol.36, No.8, pp. 83-90, 2007. 8.

[9] Chan v. Dynasty Executive Suites Ltd. [2006] O.J. No. 2877 (Ont. Sup. Ct.)

[10] Dublin v. Montessori Jewish Day School of Toronto (2007) 85 O.R. (3d) 511.

[11] Shred-Tech Corp. v. Viveen, [2006] O.J. No. 4893 (QL) (S.C.J.).

[12] Logan v. Harper, 2003 CanLII 15592 (ON S.C.).

[13] 양근원, "디지털 증거의 특징과 증거법상의 문제 고찰", *한국경찰학회보* 12호. pp. 137-139, 2006.

[14] 염흥열, ITEF 공개키 기반구조 및 PKI-기반 응용 표준화 동향, *정보보호학회지*, 제14권 제2호, 2004.

[15] 박용우, "인터넷 보안기술에 따른 VPN 시장현황 및 전망", *정보통신정책*, 제13권 제19호 통권 제288호, pp. 2-5, 2001.

[16] 대검찰청, "디지털증거의 무결성 유지를 위한 절차와 시설에 관한 연구, pp. 60-70, 2006.

[17] http://www.microsoft.com

[18] 김재홍, "PKI VPN을 위한 디렉토리 기반 실시간 클라이언트 검증 방안에 관한 연구", 경희대 대학원, pp. 23-24, 2003.

〈著者紹介〉

이 창 훈 (Chang-Hoon Lee) 정회원
2002년 2월 : 계명대학교 컴퓨터공학과 졸업
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 정보보호, 개인정보보호, 디지털 포렌식

백 승 조(Seung-Jo Baek) 정회원
2005년 2월 : 세종사이버대학교 정보보호학과 졸업
2007년 9월 : 고려대학교 정보경영공학전문대학원 석사 학위 취득
2007년 10월~현재 : 고려대학교 정보경영공학전문대학원 박사 과정
<관심분야> 정보법학, 개인정보보호, 지적재산권, 디지털 포렌식

김 태 완(Tae-Wan Kim)
1999년 2월 : 서울대학교 산업공학과 졸업
현재 (주)소만사 기술연구소 수석연구원
<관심분야> 패킷 분석 기법을 이용한 응용프로토콜 패턴 분석 및 콘텐츠 추출

임 종 인(Jong-In Lim) 종신회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사 학위 취득
1986년 2월 : 고려대학교 수학과 박사 학위 취득
현 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장, 정부혁신지방분권위원회, 대통령 자문 전자정부 특별위원회, 법무부 형사사법 통합정보체계 추진단 자문위원 등
<관심분야> 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안