전자증거 관리시스템의 설계

1)김종섭
2)하옥현
3)김귀남

ABSTRACT

DESIGNIN AND OPERATION OF DIGITAL EVIDENCE MANAGEMENT SYSTEM APPLYING COMPUTER FORENSICS AND ELECTRONIC CERTIFICATION

Digital evidence will be used as a term, which means the electronic form of information which is necessary to confirm or prove the factum of all kinds of behaviors committed through the devices which have data processing ability including computer.

It is expected that there will be the increase of legal conflicts surrounding electronic commerce activities as well as the increase of cyber crimes, as the number of Internet users are getting bigger. In order to solve the problems of conflicts derived from electronic commerce, the factum of electronic commerce activities must be confirmed. In order to confirm the factum of electronic commerce activities, the evidence is prerequisite. Almost all evidences relating to the electronic commerce activities exist in digital form.

For the reason that the digital evidence can be easily damaged and changed, special management is required to collect, analyze, and preserve the digital evidence. In order to meet this requirement, this study proposes a basic model of digital evidence management system applying computer forensics and electronic authentication.

1) 경기대학교 정보보호기술공학과
2) 경찰청사이버테러대응센터
3) 경기대학교 정보보호기술공학과

1. 「전자증거 관리시스템」

인터넷 사용인구가 증가하면서 사이버범죄도 함께 증가하여 경제적으로 많은 손실을 야기할 뿐만 아니라 인터넷을 통한 전자상거래의 활성화에 큰 장애로 등장하고 있다. 최근 사이버범죄에 대응해서 안전한 전자상거래를 위한 여러 가지 보안 제품들이 등장하고 있지만 여전히 전자적 거래행위를 둘러싼 법적 분쟁은 증가할 것으로 예상된다. 이러한 분쟁의 해결을 위해서는 전자적 거래행위의 사실관계가 확정되어야 하며, 사실관계의 확정을 위해서는 증거를 필요로 하게 된다. 전자적 거래행위와 관련된 많은 부분의 증거가 디지털 형태로 존재하기 때문에 디지털 형태로 존재하는 「전자증거」를 특별히 관리할 필요가 대두된다. 또한 디지털 형태로 존재하는 「전자증거」는 손상되기 쉽고, 변경되기 쉬운 특성을 갖고 있기 때문에 수집, 분석, 보존에 있어서 특별한 관리가 요구된다. 이를 소홀히 하면 법정에서 증거로서의 자격(증거능력)을 인정받지 못하거나 증거로서의 가치(증명력)를 인정받지 못하는 경우가 발생한다. 따라서 「전자증거」는 수집과정은 물론이고, 분석과정과 보존과정에 있어서 특별한 관리를 해야 한다. 이러한 요청을 충족할 수 있는 유용한 도구가 「전자증거 관리시스템」이다.

2. 「전자증거 관리시스템」의 설계

2.1 시스템 설계의 기본원칙 및 구조

「전자증거 관리시스템」 설계의 기본원칙은 안전성과 신뢰성의 보장이다. 「전자증거 관리시스템」은 법적 분쟁의 해결과 예방을 위한 「전자증거」를 관리하는 중요한 임무를 수행하기 때문에 자신의 안전성과 신뢰성에 의심을 받게되면 관리하고 있는 전체의 「전자증거」는 자연히 법적 가치에 치명적인 손상을 입게 된다. 따라서 어떤 시스템보다도 안전하고 신뢰할 수 있는 구조로 설계되어야 하며, 「전자증거」를 수집하는 절차에서부터 분석절차, 보존절차에 이르는 모든 절차를 투명하게 기록하고 관리할 수 있는 시스템이 되어야 한다.

2.2 시스템의 기본구조와 기능

「전자증거 관리시스템」은 크게 수집 프로세스, 분석 프로세스, 보존 프로세스, 인증 및 공증 프로세스, 일반접속지원 프로세스와 같은 주요 분야별 프로세스로 구성된다. 각 구성별 기능은 [표 2-1]과 같다.

[표 2-1] 「전자증거 관리시스템」 구성 및 기능

시스템 구성	프로세스별 기능
수집 프로세스	·증거기초자료 수집 ·타임스템프, 관계자 인증, 무결성 확인 정보 생성
분석 프로세스	·증거자료 분석 및 전자문서화 ·분석 결과에 대한 타임스템프, 인증, 무결성확인
보존 프로세스	·공증된 전자증거의 보전 ·보전자료에 대한 무결성 확인 및 접근통제
인증 프로세스	·전자증거 절차별 인증 및 공증 ·타임스템프, 사용자 인증, 무결성 확인 정보 생성
지원 프로세스	·증거관리시스템의 일반접속 서비스 ·시스템 운영에 필요한 보안지원

2.3 「전자증거 관리시스템」의 요소기술

2.3.1 전자서명 기술

일반적으로 전자서명은 크게 두 가지 의미로 나뉘어 사용한다. 먼저 광의의 전자서명으로서 「Electronic Signature」를 의미하는 것이며, 두 번째는 협의의 전자서명으 「Digital Signature」를 말하는 것이다. 광의의 전자서명으로서 「Electronic Signature」의 가장 일반적인 예는 전자펜을 이용한 그래픽 기반의 서명방식이다. 즉, 전자문서에 대한 전자결재를 수행하는 경우, 송신자는 전자펜을 이용하여 전자문서의 결재란에 자신의 수기서명과 동일한 서명을 기입한 후, 수신자에 송신한다. 이후 전자서명된 문서를 수신한 수신자는 시각적으로 전자서명의 진위를 확인한 후 전자문서의 접수여부를 결정하게 된다.

최근 선진 각국에서 시행 또는 제정 중에 있는 전자서명법은 일반적으로 협의의 전자서명으로서 「Digital Signature」의 개념을 법적으로 인정하고 있으며, 이것은 광의의 전자서명으로서 「Electronic Signature」의 방식이 안전·신뢰성 측면에서 많은 취약점을 가지고 있기 때문이다. 다음 [표 2-2]은 「Electronic Signature」와 「Digital Signature」를 안전·신뢰성 측면에서 비교·분석한 것이다.[20]

[표 2-2] 「Electronic signature」와 「Digital signature」의 비교

구분		Electronic signature	Digital signature
내용		전자펜을 이용한 수기서명 모사방식의 전자서명	비대칭형 암호기술을 이용한 전자서명
진정성 비교	서명자인증	불만족	만족
	위조불가	불만족	만족
	변경불가	불만족	만족
	부인불가	불만족	만족
전체적인 안전성		안전성에 대한 객관적 증명이 어려움	안전성에 대한 정량화 접근방식의 증명이 가능

2.4 「전자증거 관리시스템」의 단계별 프로세스

2.4.1 「전자증거」 수집단계

전자적 거래행위나 사이버범죄로 인하여 발생하는 많은 전자적 자료에서 법적 분쟁의 소지가 있는 부분을 추출하여 「전자증거」의 기초자료로 모으는 단계이다.

「전자증거」 수집단계에서 고려되어야 할 기술적 요소로는 「전자증거」를 수집하는 주체와 참여자에 대한 신분인증과 증거내용에 대한 공증이 필요하다. 신분인증은 이미 법률로 그 효력을 보장받고 있는 전자서명(Digital Signature) 제도를 이용하면 좋을 것이다. 「전자증거」를 수집하는 자가 자신의 개인키를 이용하여 서명하고 이해관계자나 참여자가 있는 경우에는 이들의 전자서명키로 함께 서명하는 방법으로 신분인증을 한다. 여기서 수집자나 참여자의 전자서명키가 위조되지 않았다는 사실을 증명하기 위하여 공인인증기관의 인증서를 필요로 하게 된다.

또한 「전자증거」를 입수한 순간에 시점확인(Time Stamping)을 하여 「전자증거」 입수 시점을 확정하고 시점확인을 시행한 후에는 변경이 없었다는 사실을 무결성 확인도 아울러 시행한다. 「전자증거」가 입수된 최초의 상태에 대한 무결성을 보장하기 위한 해쉬값과 같은 정보를 확인하여 부착시키는 작업이 필요하다.

2.4.2 「전자증거」의 분석단계

「전자증거」를 분석하는 과정에서 기술적으로 고려해야 할 사항은 최초 수집 「전자증거」의 원본과 분석을 위한 복사본의 제작과정이 투명하게 기술되어야 하며 변경된 사항에 대한 추적기록이 반드시 작성되어야 한다. 분석작업을 담당할 주체는 「전자증거」를 수집한 주체와 동일하겠지만 이때에도 컴퓨터 포렌식스 전문가가 참여하여 증거의 가치를 상실하지 않도록 주의할 필요가 있다. 그러나 프렌식 전문가가 많지 않은 현실에서는 「전자증거」의 수집과 분석을 돕는 포렌식 도구들을 개발하여 확대시켜 나감으로써 「전자증거」의 효용성을 높여 나가야 할 것이다.

2.4.3 「전자증거」의 보존단계

「전자증거」의 보전단계에서 고려되어야 할 기술적 요소는 무결성과 가용성이 보장되어야 할 것이며, 경우에 따라서는 내용의 비밀성이 유지되어야 할 것이고, 특수한 경우에는 「전자증거」자체의 존재마저 비밀에 붙여져야 할 경우가 있을 것이다. 문서의 보존이 법적 의무로 되어 있는 경우가 많다. 최근 전자문서의 보존으로 문서의 보존에 가름하는 경우가 많아서 특별히 「전자증거」보존과 관련된 기술들이 많이 개발되고 있다.

2.4.4 「전자증거」의 법정제시단계

「전자증거」는 최종적으로는 법정에 제시되어 소송의 자료로 사용되게 된다. 소송은 형사소송과 민사소송이 서로 성격이 달라 증거에 대한 취급에 있어서도 서로 차이가 난다. 일반적으로 소송의 주체인 법원과 당사자들이 「전자증거」에 대하여 어떠한 인식을 갖고 있느냐에 따라서 법정제시방법도 차이가 있을 것이다. 일반적으로 「전자증거」가 법정에 제시되는 경우에 가시적인 형태로 현출되어 증거조사가 이루어져야 할 것이다. 이렇게 증거조사가 가능할 수 있는 형태로 현출시키고, 현출된 증거자료와 「전자증거」원본이 동일하다는 사실을 증명할 수 있어야 할 것이다.

3. 결론

인터넷 사용인구가 증가하면서 사이버범죄의 증가는 물론이고, 전자적 거래행위를 둘러싼 법적 분쟁이 증가할 것으로 예상된다. 전자적 거래행위에 따른 분쟁을 해결하기 위해서는 전자적 거래행위의 사실관계가 확정되어야 하며, 사실관계의 확정을 위해서는 증거가 필요하게 된다. 전자적 거래행위와 관련된 많은 부분의 증거가 디지털 형태로 존재한다. 컴퓨터 포렌식스(Computer Forensics)는 「전자증거」를 수집하고 관리하는 유용한 방법론의 하나이다. 최근 포렌식 도구가 속속 개발되고 있는데 「전자증거 관리시스템」은 수사기관이나 법원과 같은 법집행기관에서 직접 구축하여 운영함으로써 사이버범죄나 사이버거래에서 발생하는 분쟁을 해결하는 데 유용하게 사용될 수 있다고 본다.

[참고 문헌]

[1] 한국정보보호센터, "컴퓨터 포렌식스 도구 및 절차", 정보통신기반구조 보호기술 개발, p301, 1999.

[2] Rodney McKemmish, "Forensic Computing Tools: Their Nature, Adequacy and Development",11th Annual FIRST Conference: Computer ForensicsWorkshop(Monday June 14th 1999).

[3] A. Anderson, G. Monhay, L. Smith, A. Tickle, S. Gillett, I. Wilson, "Moment of Truth: The Admissibility and Weight of Computer Forensic Evidence in the Austraian Legal System", 11th Annual FIRST Conference: Computer Forensics

Workshop(Monday June 14th 1999).
[4] Byron S. Collie, "INTRUSION INVESTIGATION AND POST-INTRUSION COMPUTER FORENSIC ANALYSIS", 11th Annual FIRST Conference: Computer Forensics Workshop(Monday June 14th 1999).
[5] 한글과 컴퓨터사, 한컴사전, 1997.
[6] 김종섭, "사이버범죄의 현황과 대책", 한국형사정책학회 2000년도 동계학술회의 자료, 2000.
[7] Computer Analysis and Response Team [FBI], "Conducting Searches in a Computer Environment", International High-Technology White Collar Crime Conference, 2000.
[8] 한국정보보호센터, '99 정보시스템 해킹 · 바이러스 현황 및 대응, p4, 정보통신부[정보통신연구개발사업 연구결과], 1999.
[9] 강동범, "사이버범죄와 형사법적 대책", 제25회 형사정책세미나 자료, 2000.
[10] 경찰청, 경찰백서, 2000.
[11] 김종섭, "컴퓨터 포렌식스에 관련된 법률 문제와 컴퓨터범죄 수사절차에 대한 분석", 정보통신기반구조 보호기술 개발[한국정보보호센터] 연구자료, 1999.
[12] 차용석, 형사소송법연구, 1998.
[13] 이재상, 형사소송법, 박영사, 1998.
[14] 백형구, 형사소송법강의, 1997.
[15] 강구진, 형사소송법원론, 법문사.
[16] 법원행정처, 법원공보
[17] 한국정보보호센터, "컴퓨터 포렌식스 도구 및 절차", 정보통신기반구조 보호기술 개발, p301-371, 정보통신부[정보통신연구개발사업 연구결과], 1999.
[18] 손경한, "전자상거래 활성화를 위한 관련 법제의 개정 방향", 디지털 경제 발전과 법제개정에 관한 심포지엄 [한국법학원, 대한상공회의소] 발표자료, 2000. 4. 19.
[19] 한국정보보호센터, 전자서명 인증업무와 전자공증업무의 상호관계 연구, 정보통신부[정보통신연구개발사업 연구결과], 1998. 12.
[20] 홍기융, "인증관리센터 구축 및 운영계획", 제4회 정보보호 심포지움(SIS '99) 자료집, pp 31-112, 1999.
[21] 송유진 외1인, 현대암호, pp 179-195, 생능출판사, 1999.
[22] 한국정보보호센터, CALS/EC를 위한 전자문서 시점확인 기술 개발, 정보통신부[정보통신연구개발사업 연구결과], 1999. 7.
[23] 한국정보보호센터, 부인방지 메커니즘 표준(안) 개발, 정보통신부[정보통신연구개발사업 연구결과], 1999. 10.
[24] 한국정보보호센터, 정보보호시스템 신분확인기능 및 무결성기능 평가방법 연구, 정보통신부[정보통신연구개발사업 연구결과], 1999. 12.