Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1171

국내 특성을 반영한 e-Discovery 대응절차

이 신 형,† 이 상 진‡
고려대학교

Effective Domestic e-Discovery Procedures

Shin-Hyung Lee,† Sangjin Lee‡
Korea University

요 약

오늘날 많은 국내 기업들이 미국 시장에 진출하여 해외사업을 확장함에 따라 미국 기업들과의 소송에 직면하는 경우가 빈번해지고 있으며 이에 대해 체계적으로 대응할 수 있도록 e-Discovery에 대한 준비가 필요하다. 아직 우리나라에 e-Discovery 제도가 확립되지는 않았지만 국내 기업들은 몇몇 대기업들의 소송 사례들을 계기로 e-Discovery에 대한 관심이 높아지고 있으며 그에 대한 대응방법 등을 모색하고 있는 실정이다. 미국의 e-Discovery 제도를 우리나라에서 실행할 시 고려해야 할 부분은 크게 세 가지로, 법률 차이, 기업 시스템 차이, 그리고 언어와 기업문화 차이가 있다. 본 논문에서는 실무를 바탕으로 국내 기업들이 미국소송에 대응하는 데 있어서의 문제점들을 도출하여 그것들을 효과적으로 극복할 수 있는 특화된 e-Discovery 절차와 과정을 제안하려고 한다.

ABSTRACT

Today, many domestic companies often face the lawsuits from the U.S. companies as they expand their business in the U.S. market and it is necessary for the domestic companies to prepare for the e-Discovery process in the systematic manner. Yet, the e-discovery system has not been properly established in Korea, however, domestic companies are growing more and more interests in e-Discovery processes and procedures so that they are seeking for the appropriate actions that they should take when facing lawsuits. When adopting the e-Discovery system in Korea, there are three main considerations including the differences in laws and regulations, enterprise system and language and company culture. This study aims to draw the problems for the Korean domestic companies in responding the U.S. lawsuits and to suggest the specialized e-discovery processes and procedures to effectively overcome them.

Keywords: e-Discovery, EDRM, Litigation Readiness, Computer Forensics, Enterprise DRM, Groupware

I. 서 론

미국 민사소송절차에는 소송이 제기되면 공판이 이루어지기 전에 당사자들이 소송에 관련된 정보와 증거를 소송 상대방으로부터 요구해서 얻을 수 있도록 하는 증거개시제도(Discovery 제도)가 있다. 이는 공판 전에 당사자들이 서로 소송에 관련된 정보와 증거를 공유함으로써 사건의 쟁점을 명확히 하여 소송의 효율성을 높이고 올바른 판결을 내리고자 하는 것이다[1]. 이 제도는 2006년 민사소송규칙(Federal Rules of Civil Procedure)을 개정하여 전자적으로 저장되어 있는 자료(Electronically Stored Information)에 대해서도 증거개시(전자증거개시 또는 e-Discovery)를 시행하도록 하였다.

최근 체결된 FTA는 지식재산권에 관한 분쟁해결을 위해 영업 비밀을 포함한 정보의 일반적 제공의무를 규정하고 있고, 이는 영미법상의 증거개시 제도에

Received(08. 09. 2016), Modified(09. 30 2016), Accepted(10. 01. 2016)
† 주저자, sophie.shlee@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

대한 대응과 맞물려 있다. 이 체결의 영향으로 미국과의 지식재산권 분쟁은 증가할 것이고, 이런 지식재산권 분쟁에서 미국의 전자증거개시제도를 활용할 가능성이 대두되고 있다[2]. 우리나라의 많은 기업이 미국과 같은 선진국들과 국제교류를 하고 해외사업을 확장함에 따라 국제적 분쟁에 대한 대비가 필요한 실정이며 이에 대해 체계적으로 대응할 수 있도록 e-Discovery에 대한 준비가 필요하다.

미국의 e-Discovery 제도를 우리나라에서 실행할 시 고려해야 할 부분은 크게 세 가지로, ① 법률 차이, ②기업 시스템 차이, ③언어와 기업문화 차이이다.

첫째, 법률 부분에 있어서 미국에서 일어난 소송이라도 경우에 따라서는 현지의 법률이 준거법이 되거나 현지에서 법률상의 문제가 발생할 수 있기 때문에 기본적으로 현지 법률사무소가 대리인이 되는 경우가 많다. 처음부터 현지 법률사무소를 거치지 않고 미국 법률사무소에게 문서검토를 의뢰한다면 방대한 분량의 자료를 영어로 번역해서 그것을 그대로 상대방에게 공개하는 상황이 되기도 쉽다. 또한 문서 검토는 e-Discovery 과정에서 전체 비용의 가장 큰 부분인 약 60% - 80%를 차지한다는 통계[3]에 덧붙여 번역이라는 또 다른 과정을 추가함으로써 비용이 늘어나기 때문에 현지 법률사무소에 의뢰하는 것이 비용절감 차원에서 효율적이다. 그러나 우리나라에서 국제소송 경험이 있고 소송전략에 대하여 정확한 조언을 할 수 있는 변호사가 아직까진 극소수에 지나지 않는다. 즉, 우리나라 기업은 글로벌화가 되고 있음에도 불구하고 국제소송에 대한 노하우는 아직 일반화되지 못하고 있으므로 이에 대한 대책이 마련되어야 한다.

둘째, 국내 기업들은 미국의 기업 시스템 체계와 상이한 부분이 존재하며 기업 내부 정보가 외부로 유출될 것을 우려하여 문서 암호화를 위해 enterprise DRM을 적용하는 기업들을 종종 접하게 된다. 국내 굴지의 기업들에서 연달아 발생한 정보유출사건으로 인해 문서보안이라 일컬어지는 enterprise-DRM 시장이 가장 적합한 솔루션으로 인식되어 기업 시장을 중심으로 조직 내 정보유출 방지를 위한 솔루션을 도입하는 양상이 두드러지고 있기 때문이다[4].

또한, e-Discovery 소송에 직면하기 쉬운 대기업들은 내부에서 개발한 그룹웨어를 적용하여 시스템을 구축하는 경향이 있다[5]. 2002년 KRG Annual Report에 따르면 국내 주요기업의 79.5%가 그룹웨어를 사용하고 있는 것으로 조사되었다. 이는 미국에서 일반적으로 상용화된 문서 DB 시스템을 사용하는 것과는 다른 방식으로 데이터를 다루기 때문에, 국내 기업들이 미국기업들과 소송에 직면할 때를 대비하여, 이러한 enterprise DRM과 그룹웨어에 적합한 절차를 e-Discovery 과정에 적용해야 한다.

셋째, 국내 기업들이 가지고 있는 또 다른 문제점은 e-Discovery 제도에 대한 이해와 지식이 부족하다는 것이다. 우리나라의 몇몇 판례에서도 중요하게 언급되었듯이 소송이 합리적으로 예상되는 시점에서 보존 의무가 시작되면 관련 자료들은 반드시 보존되어야 한다.

일반적으로 이 단계에서는 기업 법무팀이 관련 자료들에 대해 보존 명령(litigation hold)을 관련 당사자들에게 사내 e-mail을 통하여 고지하게 된다. 하지만, 이를 처음 접해보는 관련 당사자들은 충분한 지식과 이해가 없으며 이로 인해, 자료에 대한 보존 의무의 중요성을 깨닫지 못하고 고의로 또는 의식치 않게 삭제하는 경우가 생길 수 있다. 심지어는 영어로 되어 있는 보존명령 그대로를 전달하는 방식으로 e-mail을 보내어 해당 당사자들이 언어의 장벽으로 이해하지 못하는 경우도 있다. 이는 e-Discovery 제도에 있어 치명적인 소송 패소로 이어질 수 있으므로 적절한 대처방안이 필요하다.

본 논문에서는 실무를 바탕으로 국내에서 효과적으로 e-Discovery 소송에 대응하기 위한 절차와 과정에 대해 제한하고자 한다. 국내 기업들이 미국소송에 대응하는 데 있어서의 문제점들을 도출하여 그것들을 극복할 수 있는 특화된 e-Discovery 절차와 과정을 제안하려고 한다.

II. 연구배경

2.1. EDRM(Electronic Discovery Reference Model)

2005년, e-Discovery에 대한 표준과 가이드라인을 제공하기 위해서 EDRM 프로젝트가 착수되었다. 현재 EDRM은 미국의 다양한 e-Discovery 모델 중 가장 대표적이며 e-Discovery 제품과 서비스를 개발, 선택, 평가하고 사용하기 위해 실행 가능한 프레임워크로 인정받고 있다[6].

EDRM은 일상적으로 기업에서 이루어지는 정보 또는 데이터 관리를 시작으로 최종 증거 제출단계까지의 9가지 절차를 제시하고 있다. 첫 번째 단계로는, 실제 e-Discovery가 개시되면 관련 데이터를 구체적으로 식별(identification)하고 해당 데이터에 대한 위치를 파악하여 이것들에 대한 데이터 보존(preservation) 및 수집(collection)이 이루어지게 된다. 그 다음 방대한 데이터의 양을 줄일 수 있도록 중복 또는 관련 없는 것들을 제외하여 범위를 좁혀나갈 수 있도록 하는 처리(processing) 과정을 거친 후, 이 데이터에 대해 사람에 의한 직접적인 검토(review)와 분석(analysis)이 진행된다. 이 과정들을 거쳐 최종적으로 제출할 데이터가 결정되고 그것을 합의된 파일 형식으로 변환하여 생산(production) 과정을 통해 법정에 제출(presentation)을 하게 되는 일련의 과정들을 포함하고 있다.

2.2. e-Discovery 과정에서 우리나라와 미국의 차이점

2.2.1 법률의 차이

우리나라는 아직 e-Discovery 법을 제정하지 못하고 있기 때문에 e-Discovery 발생 시 일어날 수 있는 법적인 쟁점들에 대해 충분히 식별되어야 한다. 기업 내부 법무팀은 IT팀, 외부 법무팀과의 협의를 통해 소송/조사와 관련된 데이터가 식별되면 해당 데이터를 어떻게 보존 또는 추출할 것인가에 대해 국내 산업기술의 유출 방지 및 보호에 관한 법률, 개인정보법률 등을 고려하여 결정해야 한다[7].

2.2.2 기업 시스템의 차이

국내 기업들은 외국 기업들보다 내부 데이터를 더 암호화 시키는 경향이 있기 때문에 문서 보안을 위한 enterprise DRM 솔루션을 구축하는 사례가 늘어나고 있다. 또한 국내 기업들은 일반적으로 상용화된 그룹웨어 솔루션을 사용하는 미국의 기업들과는 다르게 업무 목적에 맞게 기업 맞춤형으로 자체 솔루션인 그룹웨어를 개발하여 쓰는 경우가 많다[8].

2.2.2.1 Enterprise DRM(Digital Right Management)

국내에서는 문서 보안을 위해 문서 암호화 소프트웨어 즉, enterprise DRM을 기업 시스템에 적용하는 경우가 다수 존재한다. 이를 통해 기업은 기업 내부 혹은 외부의 합법적 사용자의 고의나 부주의로 인한 정보의 유출을 막을 수 있다[9].

이 DRM은 각 기업마다 가지는 시스템 환경과 특성에 맞추어 구축되므로 여러 방식의 암호화 체계가 혼재되어 있다. 이로 인해 e-Discovery 대응에 있어서의 문제는 주로 암호화 상태인 문서들을 성공적으로 수집하더라도 그 내용이 암호화 되어 있기 때문에 문서 검토 시에는 일반 e-Discovery 어플리케이션 또는 일반 시스템으로는 문서내용파악이 불가능하게 된다.

따라서 암호화가 되어 있는 문서에 대한 검토를 위해서는 사전에 암호화 해제, 즉 복호화 작업이 데이터 수집 전에 진행되어야 한다.

2.2.2.2 그룹웨어

국내 기업들은 기업 내부 특성을 반영하여 기업 고유 시스템을 구축하는 경우가 종종 있다. 이러한 시스템은 금융, 급여, 현금지출, 비용상환, 물품목록, 판매, 문서관리시스템 및 많은 주요 비즈니스 기능을 수행하며 이와 관련된 데이터를 관리할 수 있다.[6] 이 경우, e-Discovery 소송에 관련된 데이터를 식별하고 범위를 정하는데 어려움이 따르게 된다.

그 이유는 자체 개발한 어플리케이션을 통해 데이터베이스에 분산 저장되어 있는 업무 데이터를 통합적으로 관리함으로 인해 그 어플리케이션을 이용해서만이 관련 데이터를 식별할 수 있기 때문이다[10].

따라서 데이터베이스에 저장되어 있는 정형 데이터(structured data)의 식별을 위해서는 워드문서와 같이 독자적인 형태로 존재할 수 있는 비정형 데이터(unstructured data)와는 다르게 시스템에 대한 이해가 부가적으로 먼저 이루어져야 한다[11]. 이는 비용과 시간이 더 소요될 수밖에 없기 때문에, 이러한 데이터베이스에 저장되어 있는 관련 데이터의 위치를 정확하고 신속하게 파악하여 검토를 가능케 할 수 있는 전략이 필요하다.

2.2.3 기업 문화 및 언어의 차이

미국 문화에 익숙하지 않은 우리나라는 e-Discovery에 대한 정보가 부족한 실정이다. 실제로 e-Discovery 소송에 연루되면 어떤 단계들을 거쳐야 하고 주의할 사항들은 무엇이며 어떤 방식으로 진행되어야 하는지에 대해 인지하지 못하고 있는 경우가 많다. 막상

자료보존명령 공지를 받게 되는 당사자들은 그 내용이 얼마나 중요한 것인지 또는 영어로 된 공지가 어떤 내용인지 자세히 이해 못하는 경우가 생길 수 있다[12]. 또한, 소송과 관련된 데이터를 보존해야 하는 의무의 중요성을 이해하지 못하기 때문에 자신이 연루되어 있을 법한 사안이 되는 문서들을 삭제하는 경향이 있다.

e-Discovery 소송은 미국을 포함한 영어권 국가에서 발생하기 때문에 다국어를 포함하는 생산 과정에서 야기되는 이에 대한 여러 가지 특이사항들을 고려해야 한다. 문서 생산을 위한 이전 단계인 문서 검토 과정은 대개 세 가지 방법 중에 하나로 진행된다. ① 한국어를 구사하는 변호사 또는 전문가를 사용하여 검토, ② 미국 변호사가 검토할 수 있도록 모든 문서를 사람 또는 기계에 의해 영어로 번역, 또는 ③,①과 ②의 두 가지 방법들을 혼합할 수 있다[13]. 만약, 미국 번호사에 의해 검토가 이루어져야 한다면, 번역되어야 하는 문서들의 양과 더불어 그만큼의 번역 비용이 증가할 뿐만 아니라 특화된 산업에서의 업무 내용을 파악하지 못하는 사람이 번역할 경우 부정확한 번역을 초래할 가능성도 존재한다.

또 다른 우리나라 기업 문화의 특징으로는, 국내 대기업들은 IT 분야를 전문적으로 하는 자회사들이 대다수 존재한다. 그리고 IT 회사는 대부분 그 대기업 내의 다른 자회사들의 정보시스템을 관리하도록 하는 시스템으로 이루어진다. 이는 IT 시스템 관리의 분리로 인하여 데이터 제공의 어려움이 존재하기 때문에 e-Discovery 대응에 있어 불리한 점으로 작용할 수 있다.

첫째, 관련 데이터의 식별 또는 수집에 있어서 승인을 받는 절차가 복잡하여 신속하게 이루어지지 않는다. 둘째, 데이터의 식별과 데이터 제공에 대한 책임 문제에 있어서, 현업 담당자와 자회사의 IT 시스템 담당자 사이에 의사소통이 제대로 이루어지지 않거나, 서로 책임을 떠넘기는 등으로 인해 올바른 수집이 이루어지지 않을 수 있다.

이는 미국 기업들이 기업 내부에 독립적으로 IT 부서를 두어 데이터를 담당하게 하는 것과는 상반되는 경우이다.

III. 효과적인 e-Discovery를 위한 대응방법

EDRM은 소송 주기 전반에 걸쳐 e-Discovery에 대한 산업에서 용인된 작업 흐름도이다. 이를 국내 기업 환경에 맞게 우리나라에 적합한 KEDRM(Korean E-Discovery Reference Model)을 제안하고자 한다.

여기서 특히 주목해야 할 점은 미국의 EDRM 모델에서는 포함되지 않은 소송 준비도(litigation readiness)에 대한 개념이다. 이것은 e-Discovery와 연관은 있지만 정보관리에 대한 다른 개념으로서의 IGRM(Information Governance Record Managament) 모델의 독자적인 형태로 소개되고 있다. 하지만 미국과는 법률 문화가 다른 우리나라에서 e-Discovery를 효과적으로 진행하기 위해서는 소송준비도 절차가 KEDRM의 과정에서 체계화 될 필요성이 있으며 본문에서는 이에 대한 방안을 제시하고자 한다.

3.1 소송준비도(litigation readiness)

소송에 대한 '준비를 하는 것'은 간단히 말해서 '소송 준비도'라 언급한다. 소송 준비도를 계획하는 것은 표준작업절차서와 모범사례를 통하여 그 조직의 데이터와 잠재적인 증거에 대한 통제를 가지기 위한 목적으로, 사전대책을 강구해 개발하고 사용하는 과정을 말한다. 이로 인해 소송이 발생할 시 조직은 효율적, 효과적이고 방어 가능한 방법으로 잠재적으로 관련된 증거를 식별, 보존과 수집을 수행할 수 있도록 준비되어있을 수 있으며 조직이 요청에 따라 필요한 정보가 사용가능하고 제공될 수 있도록 함으로써 능숙하고 성공적인 방법으로 자신을 방어할 수 있게 된다[14].

당사자를 대표하는 법무팀은 잠재적으로 관련된 데이터를 빠르게 파악하여 관련된 증거를 식별, 수집하고 생산하기 위해 찾고자 하는 시스템에 대해 상대방과 법원에게 정확한 설명을 일관적이고 시기적절하게 제공해 줄 수 있어야 한다. 법무팀은 시스템 운영과 데이터에 대한 상대적인 접근성과 쟁점에서 빠른 전략적 결정을 내기 위해 보존과 추출 단계에 드는 추정 비용, 부담과 관련된 정보를 정리하여 평가할 필요가 있다[15].

사전교육이 적절히 이루어지지 않는다면, IT팀은 계류 중이거나 예상된 법적 쟁점에 관련된 데이터를 데이터의 생성주기에 맞춰 파기하거나 또는 마이그레이션을 통해 데이터를 이동시킬 가능성이 커진다. 이것은 의도치 않은 행위라 하더라도 법원은 이것을 지속적이고 철저한 의사소통이 법무팀과 IT팀에서 이

루어지지 않아 데이터에 영향을 미쳤을 경우 합리적인 불찰로 여기지 않기 때문에 증거 훼손 혐의를 피할 수 없다[15].

따라서 조직은 조직 내의 IT 구조를 이해하고 조직 구성원들을 사전 교육하여 소송에 대비할 수 있도록 하는 효율적인 소송 준비도 체계를 반드시 도입함으로써 소송이 발생할 경우 e-Discovery 비용을 최소화 할 수 있고 대응 시간을 줄일 수 있도록 해야 한다[16].

3.1.1 IT 시스템 구조에 대한 이해

소송과 IT는 불가분하게 연관되어 있기 때문에, 소송 준비도를 구축하는 것은 효율적인 계획을 실행할 수 있도록 IT 기반시설을 준비하도록 하는 것에 달려있다[17]. 이를 위해서는 첫 번째로 Discovery 기한 내에 관련 있는 정보를 신속히 검색할 수 있도록 데이터에 대한 유형과 위치를 정확히 보여주는 데이터 맵(data map)을 만들어야 한다.

포괄적인 데이터 맵은 법무팀과 IT팀에게 조직 도처에 있는 데이터에 대한 물리 및 가상의 위치와 함께 담당자, 과정, 기술과 데이터 유형에 대한 가이드를 제공해 줄 수 있다. 또한, 데이터 보유 정책과 전사적 관리시스템에 대한 정보를 포함하며 조직 내에서 다양한 부서들 또는 실용적인 부분들에 대한 데이터를 가지고 있는 서버를 식별할 수 있도록 작성되어야 한다[18].

이 데이터 맵으로 인해 사전에 활성 시스템, 백업, 아카이브 시스템 등에 있는 데이터를 효율적으로 식별하고, 시기적절하게 보존할 수 있도록 관련 대상자들에게 연락할 수 있는 방법을 구현함으로써 향후 자료보존명령을 효과적으로 행할 수 있게 할 수 있다[19].

3.1.2 사전 교육

조직은 직원들이 적절하게 정보와 기록을 생성, 사용, 보유하고 파기하는 것에 대한 책임을 이해하도록 노력해야 한다. 각 기록에 대한 생성주기와 관련된 영역들은 각각 모두 중요하고 그에 따른 위험부담이 존재하므로 조직은 포괄적인 교육을 통해 직원들과 가장 효과적으로 내부 정책과 절차를 소통할 수 있는 방법을 결정해야 한다[20].

또한, 선택된 교육방식을 통해 직원들이 자료보존 명령 고지를 받았을 경우 따라야 하는 절차와 유의사항에 대한 중요성을 깨닫게 해야 한다. IT 관리자를 포함한 IT팀에는 소송과 관련된 데이터가 수정, 덮어쓰기, 파기 등으로부터 데이터 변조를 막기 위해 자동 삭제 기능 정지 등을 포함한 적절한 대응조치를 취하도록 교육해야 한다[3].

그리고 내부 법무팀은 e-Discovery 과정에서 데이터 제공의 중요성에 대해 경영진을 이해시키는 과정이 필요하다. 아시아에서 보통 조직 또는 기업 내 데이터를 외부로 공개하는 것을 꺼리는 경향이 강하기 때문에 데이터를 제출하지 않았을 때 제재 조치를 받는 등의 불이익이 생기는 것을 설명하여 원활한 e-Discovery 과정이 이루어질 수 있도록 고위 경영진의 적극적인 지원이 필요하다[20]. 이는 필요한 자원을 얻고 변경에 대응하는 과정을 가능하게 하는 데에 필수적인 요소이다.

3.2 식별(identification)

소송이 합리적으로 예상되는 때 또는 법원에서 데이터 제출 명령에 대한 요청을 받게 되면, 내부 법무팀은 IT 팀, 인사팀과 협력하여 이 소송 관련 대상자들 또는 부서를 식별하여 제출해야 하는 데이터가 저장되어 있을 법한 모든 가능한 곳을 파악하도록 해야 한다. 또한, IT 팀은 법무팀이 기업 내 문서보유 정책들 중 소송 쟁점과 관련된 데이터를 식별할 수 있도록 지원하며 이것이 자동적으로 삭제되지 않도록 적절한 조치를 취해야 한다. 즉 잠재적으로 소송과 관련된 데이터에 대해 보존조치가 시행되어야 하며 이 내용에 대한 공지는 조직에서 소송에 관련된 부서 또는 내부 법무팀의 고위 경영진, 또는 다른 높은 계급의 관리자에 의해 관련 당사자들에게 공식적인 문서의 형태로 발행되어야 한다[21].

더불어, 우리나라 대기업이 많이 보유하고 있는 DRM과 그룹웨어에 대해서는 일반적인 데이터 식별 단계보다 세심한 데이터 분석이 이루어져야 한다.

3.2.1 자료보존명령 공지 준비

자료보존명령에 대한 공지는 핵심 당사자들, IT, 기록 관리 및 HR 담당자에게 배포되어야 하며, 그 기업 내 핵심 인물들과 퇴직 예정 또는 재고용된 직원들을 포함하여 관련된 자료들을 가지고 있는 모든 이에게 소통되어야 한다[22].

기업 내부 법무팀은 자료보존명령 공지의 대상인 개개인에 대한 기록을 가지고 있어야 하며 이 공지가 모든 수령인에게 배포되어 검토되었음을 증명하는 기록을 가지고 있어야 한다. 예를 들면, 공지를 받은 개인은 공지를 수령하여 검토했음을 확인해 주는 메일을 보내거나 공지를 받음에 따라 그것에 준수할 것을 동의한다는 증명서에 서명할 것을 요구해야 한다[23]. 공지에 대한 수령과 검토를 확인하는 모든 자료들은 기업 내부 법무팀 또는 자료보존명령을 감독하는 담당자에 의해 보관되어야 하며 이로써 기업이 자료보전명령을 구축하는 대응에 있어서 나중에 문제가 될 경우, 쉽게 그 자료들에 접근하여 방어 가능할 수 있게 된다.

자료보존 명령 공지가 효과적으로 배포되기 위해서는 회사 전반에 걸쳐서 단순히 email을 보내는 것으로는 충분하지 않을 수 있다. 법무팀은 핵심 인물들이 가지고 있을 법한 정보의 유형과 저장된 위치를 결정한 후, 핵심 인물들과의 인터뷰를 통해 그들이 보존해야 하는 의무와 기업이 법적 제재를 피할 수 있도록 돕는 의무의 심각성을 이해시켜야 할 것이다[22].

3.2.2 식별 - enterprise DRM

소송과 잠재적으로 관련된 데이터를 식별하는 과정에서 기본적으로 그 조직이 가지고 있는 enterprise DRM 시스템에 대해 고려해야 한다. 그 시스템으로 인해 암호화 되어 있는 데이터는 이용할 수 없는 상태로 제공됨에 따라 문서 생산 실패로 인해 제재를 받을 수 있게 되기 때문이다.

따라서 내부 법무팀은 e-Discovery를 진행함에 있어 고용된 e-Discovery 전문가가 내부 IT팀과 협력하여 기업내부 암호체계와 그에 따른 암호 수준에 대한 쟁점을 다룰 수 있도록 지원해야 한다. 이로써 e-Discovery 전문가들은 법무팀에게 타당한 수집 시나리오를 추천해 주고 타임라인과 일상 업무에의 영향 등과 같은 고려사항을 충족시키기 위해 법무팀의 요청대로 시나리오를 수정하며 수집을 위한 시간과 비용에 대한 추정치를 제공할 수 있다[6].

이를 위해서는 사전에 미리 준비된 데이터 맵을 통해 관련 데이터를 식별하고 핵심 인물들과의 인터뷰를 통해 IT 관리자와 함께 데이터 암호화 과정이 어떻게 이루어지는 지에 대한 분석이 필요할 것이다[24].

해당 데이터의 암호 해제를 위해서는 기술적인 측면 뿐 아니라 기업 문화적인 측면에서 접근할 필요성이 있다. 기업은 IT 컴플라이언스와 더불어 e-Discovery 제출에 대한 요구사항을 준수하지 못했을 경우 경영진의 직접적인 법적 책임, 벌금 및 규제 당국의 직, 간접적인 간섭, 민사소송으로 인한 경제적 피해와 같은 리스크에 직면할 수 있기 때문에 경영진의 적극 지원이 필요하다. 즉, 경영진은 Discovery 요청에 의해 제공되어야 하는 문서들이 빠르고 효율적인 방법으로 암호 해제가 이루어지도록 지원해야 할 의무가 있다. 따라서 모든 DRM 솔루션에는 암호화를 해제할 수 있는 복호화 키값이 존재하기 때문에[25] 경영진은 법무팀이 복호화 키를 해당 데이터 수집 전 사전에 미리 준비하여 획득하도록 지원하는 것이 중요하다[26].

많은 양의 파일들이 암호화 되어 있는 경우, 사전에 DRM을 해제할 수 있는 복호화 키를 사용하여 일괄적으로 암호 해제할 수 있는 프로그램 배치(batch)를 준비하여 실행한다면 암호해제에 소요되는 비용과 시간을 훨씬 절감할 수 있을 것이다.

만약 기업 내부에서 DRM 알고리즘과 암호 해제 키를 관리하고 있다면 해당 관리자에게 암호화 해제 배치를 준비시킬 수 있다. 그렇지 않다면, 외주 DRM 업체와 조율하여 암호화 해제 배치를 사전에 준비해 놓는 것이 비용 및 시간 측면에서 효율적으로 암호화 해제 작업을 진행할 수 있다.

3.2.3 식별 - 그룹웨어

Sedona Database Principle 2에 의하면, 데이터베이스에 저장되어 있는 정보에 대한 요청은, 각 정보가 저장되어 있는 방식이 다르고 모든 정보가 동일하게 접근할 수 있는 가능성이 없을 수 있기 때문에, 소송에 대한 관련성과 비례의 원칙이 적용하는지에 대한 분석이 이루어져야 함을 명시하고 있다[11].

또한, Database Principle 3에 따르면, 요청하는 당사자와 요청받는 당사자는 데이터베이스에 저장된 정보를 제공하기 위한 부담을 확인하고 테스트 쿼리와 실험 작업에서 발생한 것과 같은 실증적인 정보를 사용하여 Discovery의 범위에 대해 의견일치를 보도록 권장하고 있다[11].

그룹웨어에서 소송과 관련된 데이터가 정보체계 내에서 어디에 어떤 방식으로 저장되어 있는지를 파

악하기 위해서는 먼저 데이터베이스 스키마(schema) 구조를 이해하고 해당 데이터가 저장된 데이터베이스의 설계 및 개발논리의 분석이 필요하다.

데이터 매핑(data mapping)과 데이터 사전(data dictionary) 또는 스키마와 문서화된 데이터 흐름(data flow)과 개체 관계 다이어그램(entity relationship diagram)은 데이터베이스 연결을 추적하는 데 유용하다. 정형 데이터 시스템은 조직 내에서 보통 여러 시스템들과 다양한 방법으로 연결되어 있기 때문에 이러한 연결들을 파악하지 못한다면 입력, 출력 및 관련 데이터를 놓칠 수 있다[27].

그룹웨어에 대한 식별 단계에서는 사용 또는 제출해야 하는 해당 데이터를 가지고 있을 법한 시스템이 어떤 것들인지에 대한 결정과 데이터 상태 및 사용가용성에 대한 현재 상태 확립과 데이터 위치 파악 등이 이루어져야 한다[27].

이에 대한 합리적인 이해력을 키우기 위해서 최종 사용자와 데이터베이스 지식을 가지고 있는 IT 전문가와의 인터뷰를 염두에 두어 계획해야 한다[27].

3.3 보존(preservation)/수집(collection)

e-Discovery 보존 과정에서는 일반적으로 전체 하드 드라이브 또는 다른 ESI(Electronically Stored Information) 형태로부터 법과학적인 방법(forensically)으로 데이터를 수집할 필요는 없다. 미국 법원은 포렌식 이미지(forensic image)가 필요하다고 결정하는 데에 있어 5가지 요소를 평가한다: ① 소송에서의 필요성; ② 성패가 달려있는 정도; ③ 당사자들이 보유하고 있는 자원; ④ 성패가 달려있는 쟁점에 대한 중요도; ⑤ 소송에서 쟁점에 대한 Discovery의 중요도[15].

포렌식 이미징(Forensic imaging, bit-by-bit 또는 byte-by-byte capture)은 증거에 대한 삭제 또는 훼손이 쟁점이 될 수 있을 때 필요하며, 법무팀은 다음과 같은 특정 유형의 소송에서 보존 목적, 잠재적인 증거 훼손을 피하기 위해 포렌식 이미징을 사용할 것인지에 대해 고려해야 한다[15].

- 직원 또는 제 삼자의 위법행위에 대한 내부조사
- 한 기관이 조사 중에 있거나 그 기관 데이터에 관련된 대배심 소환에 대응하는 형사상 또는 규제 사안
- 관련된 정보가 자료보존명령 공지가 발행되기 전에 삭제되었다는 것에 대한 사실이 통보된 민사소송
- 그 기관이 잠재적으로 관련된 정보가 해당 직원이 부서이동 또는 퇴사로 인해 분실되었으리라는 합리적인 믿음이 있는 경우
- 한 개인 직원이 자료보존명령 공지에 대한 조항들을 따르지 못하여 정보가 삭제되었음을 합리적인 통보를 받은 사실을 알게 되는 경우

위의 경우에 해당되지 않거나 삭제되지 않은 활성 데이터에 대한 수집만 필요할 경우, 파일에 대한 메타데이터(metadata)를 보존하면서 파일을 복사하는 Robocopy 또는 XXCOPY 등을 사용할 수 있다. 수집/보존 프로그램이 메타데이터를 취급하는 방법은 핵심적인 쟁점이며 이로 인해 파일 내력에 대한 메타데이터 영역이 영향을 받지 않도록 하는 것이 매우 중요하다. 이를 위해 데이터 수집할 때에는 쓰기 방지 소프트웨어 또는 하드웨어 장비를 사용하여 해당 파일이 복사될 시 기존의 메타데이터를 건드리지 않고 보존할 수 있도록 할 수 있다[28].

메타데이터의 보존은 증거에 대한 근원과 원본성이 쟁점이 될 때 필수적이며[26] 문서 검토 시 메타데이터 정보는 더 빠르고 정확한 검색 기능을 제공해 줄 수 있기 때문에 비용을 절감하고 생산성을 향상시킬 수 있다[29].

또한, 서버의 경우, 포렌식 이미징을 위해 서버를 다운시킴으로써 야기되는 운영중단, 비용과 서버 데이터가 신속하게 바뀜에 따라 관련 데이터를 삭제된 영역에서 찾을 가능성이 희박한 사실 등으로 인해 서버에 저장되어 있는 정보를 보존하기 위해서는 활성 데이터 수집이 일반적으로 선호된다[15].

우리나라에서는 DRM과 그룹웨어를 쓰는 기업이 다수 존재함에 따라 그들만의 특성을 고려하여 전형적인 데이터 보존/수집과는 차별화된 절차를 따라야 한다.

3.3.1 보존/수집 - DRM

연방민사소송규칙 34(a)(1)(A)은 당사자들이 정보가 필요하다면 상대방이 적절하게 사용할 수 있는 형태로 변환한 후에 데이터를 제출하도록 요구하고 있다. 따라서 최소한도로 데이터를 제출해야 하는 당사자는 모든 잠재적으로 관련 있는 암호화된 데이터를 식별해야 하며, e-Discovery를 위해 데이터를

복호화 하도록 준비해야 한다[30]. 의미 없는 암호화된 내용을 원래 상태로 되돌리기 위해서는 적절한 복호화 키가 필요하며[6] 암호화된 파일들을 복호화 하기 위해서는 그것들을 그룹으로 묶어 한꺼번에 배치 기반으로 처리하는 것이 경제적이다[31]. 따라서 이전 식별단계에서 사전에 준비한 복호화 키로 한꺼번에 암호화 해제 배치를 실행하는 것이 시간과 비용면에서 훨씬 효율적일 것이다.

이에 앞서, DRM이 구축된 환경에서 관련 데이터가 저장된 PC 또는 서버의 사용 행위 분석이 필요한 지에 대한 여부를 고려해야 한다.

그 이유는, 암호화를 해제하는 과정은 DRM 어플리케이션 마다 각기 다른 알고리즘을 적용하겠지만 보통 복호화 하는 과정에서 시스템 파일이 변경되거나, 복호화 작업이 이루어지는 문서들의 파일 이름이 변경되거나, 또는 최종 수정 또는 사용시간이 변경되는 등의 메타데이터가 변경될 가능성이 크기 때문이다. 즉, 해당 시스템에서 사용 행위 흔적이 지워지거나 변경될 가능성이 크기 때문에, 수집된 데이터의 원본문제가 제기될 수 있거나, 그 문서들에 대한 기록인 메타데이터가 보존되어야 하는지, 또는 사용 행위 분석이 필요한지에 대한 판단이 먼저 이루어져야 한다.

이 경우, 암호화 해제 전 먼저 관련 데이터에 대한 수집 또는 이미징이 이루어진 후 암호화 해제가 이루어지게 하여 원본 데이터에 대한 분석이 가능하게 하는 것이 복호화로 인한 데이터 변경으로부터의 분쟁을 막을 수 있는 합리적인 방법일 수 있다.

결론적으로, DRM으로 인해 데이터 수집에 대한 비용은 기존의 데이터 수집보다 두 배로의 시간과 비용이 들 가능성을 고려해야 한다.

이와는 다르게, 단순히 데이터의 내용만이 쟁점이 될 경우에는 암호화 해제 전의 데이터 수집 없이 복호화 상태의 수집만을 진행하는 것이 합리적이다.

3.3.2 보존/수집 - 그룹웨어

대부분의 e-Discovery에서는 비용과 시간을 고려하여 그룹웨어 전체 보다는 소송과 관련된 일부분만을 보존하여 활성 상태의 해당 데이터를 수집한다. 앞서 식별단계에서 데이터 흐름과 객체 관계 다이어그램 등에 대한 분석을 통해, 관련 데이터가 저장된 데이터베이스의 설계 및 개발 논리를 파악한 후, 원하는 데이터를 추출하도록 데이터베이스 쿼리(query)를 구성해야 한다[27].

그룹웨어에서 데이터를 추출하기 위한 또 다른 방법은 일상적인 업무수행과정에서 업무 사용자에게 제공하는 기본 보고서를 활용하는 방법이 존재한다. 시스템 상에서 관련된 데이터를 포함한 보고서를 제공해 주는 기능이 존재한다면 그 기능을 통한 데이터 수집을 고려해 볼 수 있다[11].

이 보고서들은 당사자가 어느 정도 어떤 데이터가 보고서에 포함되었는지 알고 있어 사전 검증되었기 때문에 Discovery에서 잠재적인 가치를 가지고 있다[15]. 업무용 보고서를 사용함으로써 가장 쉽고 적게 비용이 들며 또한 가장 부담이 적게 드는 방법으로 정보를 획득하여 제공할 수 있을 것이다[11].

맞춤형 보고서를 구축하는 것은 기존의 존재하는 보고서를 사용하는 것 보다 관련된 데이터, 데이터 필드와 시기를 특정할 수 있는 융통성을 제공할 수 있다.

동적(dynamic) 데이터, 다른 필드 또는 행위에 근거하여 변경될 수 있는 데이터는 보존 과정 내내 특별한 주의를 필요로 한다. 지속적으로 변경되는 데이터를 보존하기 위해 한 가지 제안된 접근법은 특정 기간에 데이터베이스에 대한 쿼리를 실행하여 조회함으로써 얻은 정보의 스냅숏을 보존하는 것이다[15].

이와 비슷하게, 지금은 잘 허용되지 않지만 오래된 방법 하나로는 화면에서 보이는 시스템 출력물을 사진 촬영하여 TIFF 이미지로 만들 수 있다. 이 방법은 검색이 가능한 글자를 포함하지 않을 수 있기 때문에 권장되지는 않지만 너무나 제한된 출력 기능을 가지고 있는 특정 데이터베이스 시스템에서는 이러한 데이터 수집 방법이 유일한 방법일 수 있다[27].

3.3.3 자료보존명령 공지에 대한 주기적 관리

자료보존명령 공지가 배포된 후, 직원들이 지속적으로 컴플라이언스 의무를 염두에 두도록 상기 공지가 주기적으로 발행되어야 한다. 추후 소송과 관련이 있다고 판단된 자료가 기존의 공지에는 포함되지 않는다면 새로운 공지가 배포되어야 한다[32].

상대방과 법원에게 자료보존명령에 대한 과정이 적절하고, 일관성 있게 선의의 방법으로 구현되었음을 입증하기 위해서는 이에 대한 기록을 충분히 작성하는 것이 필요하다. 대개의 경우, 이를 위해 자료보존명령 공지를 발행하고 구현하는 과정과 더불어 데

이터 보존을 위한 후속조치에 관련된 기록들을 제공함으로써 충족시킬 수 있을 것이다[33].

이러한 모든 단계들을 구현하는 것은 시간과 비용이 많이 들 수 있지만, 효과적인 자료보존명령에 대한 비용은 제재 신청에 대한 방어 비용보다 훨씬 적은 비용이 소요된다.

3.4 검토(review) 언어

관련된 데이터에 대한 수집이 완료되면 전형적인 중복제거(de-duplication), DeNisting, 키워드 검색 등을 포함한 처리 과정을 거쳐 관련성(responsiveness)과 비닉특권(privilege)을 결정하기 위해 데이터 검토 단계에 이르게 된다.

초기검토(first review)를 통하여 비닉특권, 쟁점 또는 관련성에 따라 총 검토 문서 양의 약 20% 정도로 줄여지며 두 번째 검토(second review) 과정을 거쳐 상대방에게 제공되어야 하는 문서들이 결정된다.

이 과정에서 국내 기업들은 많은 양의 문서가 한국어로 작성되어 있음으로 인해 생산 과정에서 영어로 제출되어야 하는 해당 문서들의 번역 문제에 대해서 문서를 어떤 방식으로 검토할 것인지에 대해 가장 비용 효율적인 방법을 모색해야 한다.

문서 검토 과정은 대개 세 가지 방법 중에 하나로 진행된다. ① 한국어를 구사하는 변호사를 사용하여 검토, ② 미국 변호사가 검토할 수 있도록 모든 문서를 사람 또는 기계에 의해 영어로 번역, 또는 ③ 이 방법들을 혼합할 수 있다[7].

먼저 번역을 할 것인지, 또는 한국어로 검토를 할 것인지는 정확성, 시간, 비용 등의 요소에 따라 결정된다.

소송의 쟁점과 규모에 따라서 달라지겠지만, e-Discovery 검토에 있어서 100GB의 데이터가 있다고 가정해보자. 1GB는 약 5000개에서 25,000개의 문서를 가지고 있다고 추산하면 1GB당 평균적으로 10,000 개의 문서로 추정될 수 있다. 한 자료에 따르면, 초기검토는 미국에서 평균적으로 시간 당 $65의 비용이 소요되며, 산업 기준은 문서를 검토하는 자들은 한 시간당 50개 또는 하루에 400개의 문서를 읽고, 이해하며 기록할 수 있다고 제시하고 있다[35]:

- 한국어를 구사하는 미국 변호사 초기검토 비용: $75/hour[36]
- 한국어를 구사하지 못하는 미국 변호사 초기검토 비용: $65/hour
- 변호사 한 사람이 검토할 수 있는 총 문서의 개수: 50개/hour
- 한 개의 문서 당 평균 페이지 수: 9 pages/doc [37]
- 한 페이지 당 번역 비용: $10/page
- 소송과 매우 연관성이 있는 데이터 산출 비율(hot responsive yield rate): 20%[38]

100GB 중에서 불필요하고 관련 없는 문서들은 핵심 용어, 검색 매개변수와, 수집과 검토에 대한 범위를 정의하는데 있어서 감수할 수 있는 위험 정도에 따라 제거되겠지만, 여기서 제거되는 비율(cull rate)은 보통 80%라고 가정할 수 있다. 따라서 문서 검토 양은 100GB에서 20GB, 즉, 1,000,000 개에서 200,000 개로 줄어들게 되며[37] 한국어로 된 문서의 양을 전체의 50%라고 가정했을 경우 두 번째 검토 전까지의 과정으로 다음과 같은 시나리오를 예상할 수 있다.

① 200,000개의 문서들에 대해 한국어를 구사하지 못하는 미국 변호사가 초기검토 진행 - 전체문서의 약 50%인 한국어로 된 문서는 차후 다시 검토를 위해 표시(flag)하고 전문가에 의한 문서 번역 후 영어로 번역된 문서들을 다시 검토

② 200,000개의 문서들에 대해 한국어를 구사하는 한국인 미국 변호사 초기검토 진행 - 전체 문서의 약 20%인 초기검토에서 걸러진 비닉특권 또는 관련 있는 문서들에 대해 문서 번역

위 시나리오를 바탕으로 예상한 미국 변호사의 검토 비용과 번역 비용 등을 고려했을 때, 초기검토를 위해서는 다음과 같은 비용이 발생하게 된다.

즉, 일반적으로 초기검토에서 걸러진 문서의 비율을 전체 초기검토 양의 20%라고 했을 경우, 이 결과 문서들이 모두 번역이 필요하다고 가정하더라고

Table 1. First Review - Estimated Costs

	Translation Cost	Hourly rate * Total Hours	Total
①	$10 * 9 * (200K* 50%)	$65 * (200K/50)	$ 9,260K
②	$10 * 9 * (200K* 20%)	$75 * (200K/50)	$ 3,900K

총 비용은 $ 3,900,000으로 추정할 수 있다. 하지만 처음부터 모든 한국어 문서에 대해 번역을 할 경우, 적어도 그 양의 50%만 번역작업이 필요하다 하더라도 총 검토 비용은 $ 9,260,000 정도로 예상된다. 따라서 한국어를 구사하는 미국 변호사가 처음부터 개입하여 검토한 다음 초기검토에서 걸러진 문서들에 대해서만 번역하여 검토하는 것이 훨씬 더 비용 효율적인 것을 예상할 수 있다.

3.5 생산(production)

생산 과정에서는 양측 변호사들이 미리 합의한 일정과 양식에 의해 마지막 검토 단계에서 추출된 데이터를 상대방에게 제출하게 된다. 이 데이터에 대한 제공 양식에는 파일 고유(native) 포맷, 그래픽 파일(TIFF, PDF) 등을 포함한다.

영어로 된 문서 이외에 한국어로 된 원본 문서의 제출을 원할 경우, 생산 방식과 형태에 대해 그 한국어가 지원될 수 있는지를 확인해야 하며 생산 언어, 형식과 순서 및 배치는 합의 회의(Meet & Confer conference)에서 미리 논의되어 결정될 수 있다[7].

관련된 데이터가 저장되어 있는 그룹웨어 고유의 데이터베이스 형식은 읽을 수 없는 형태일 수 있기 때문에 요청하는 당사자에게 합리적으로 사용될 수 없다. 따라서 데이터가 일상 업무과정에서 저장되는 방법과는 다르게 데이터를 변경하는 변형된 생산 형태가 Discovery 관행으로 흔히 더 인정되고 있다[11].

IV. 국내 특성을 반영한 e-Discovery 전략

앞서 언급한 문제점들에 대한 해결방안을 고려하여 우리나라 환경에 맞는 EDRM 모델을 합리적으로 소송/조사가 예상되는 시점부터 생산까지 과정을 Fig. 1과 같이 제안할 수 있다. 기존의 EDRM 과정을 준수하지만 음영으로 차별화된 부분을 나타낸 것처럼 우리나라의 기업문화와 기업 시스템 성격을 반영하여 e-Discovery를 위한 사전 준비 단계부터 데이터 제출까지의 과정을 제시하고 있다.

기존의 EDRM의 단계에는 사전 준비도에 대한 개념이 포함되지는 않았지만 미국의 법률 문화와 다른 우리나라에서는 체계화 될 필요성이 있다. 국내에서는 증거가 없으면 제출하지 않아도 된다는 문화적

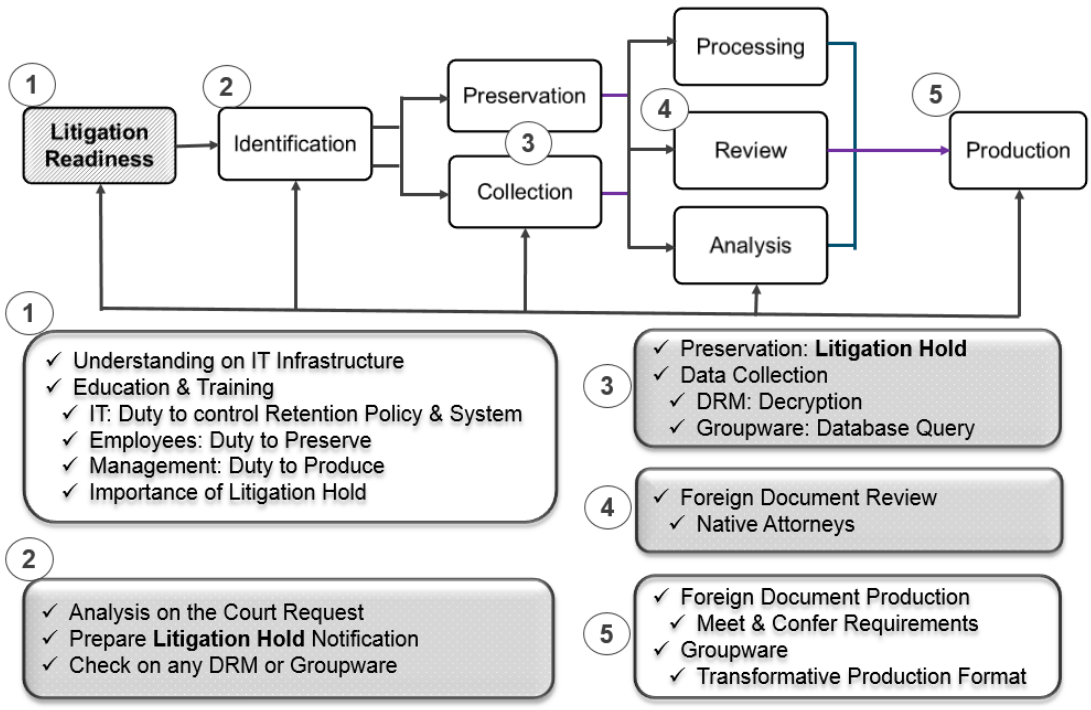

Fig. 1. Proposed Korea E-Discovery Reference Model

인 사상이 자리 잡아 데이터를 삭제하는 경향이 있기 때문에 이를 방지하기 위해 사전 준비도 개념을 도입해야 한다. 이로써 기업 IT 인프라스트럭처에 대한 이해를 바탕으로 소송에 효율적으로 대비할 수 있도록 법무팀은 직원, IT부서 등을 대상으로 소송 발생 시 취해야 하는 조치들에 대해 사전교육이 이루어지도록 해야 한다.

그리고 합리적인 소송이 예상되는 시기에 해당 데이터에 대한 식별이 이루어지는 과정에서 법무팀은 법원에서 요청한 자료에 대한 분석과 더불어 관련 데이터를 보존할 수 있도록 자료보존명령 공지를 작성해야 한다. 또한, 국내 기업 시스템 특성 상 가지고 있을 법한 DRM 또는 그룹웨어에 대해 파악하여 DRM의 경우, 암호화 해제키와 암호해제 배치를 준비하도록 해야 하며, 그룹웨어의 경우에는 DB 아키텍처를 이해하여 관련 데이터가 어디에 어떤 방식으로 저장되어 있는지를 분석해야 한다.

그 다음 수집/보존 단계에서는 식별된 데이터에 대해 DRM의 경우 앞서 준비한 복호화 Batch를 사용하여 암호화 해제 후 수집하도록 한다. 그룹웨어의 경우에는 데이터베이스 쿼리를 이용하거나 그룹웨어 시스템 상에서 제공하는 보고서 등의 기능을 이용하여 데이터를 수집할 수 있다.

검토 단계에서는 수집된 데이터가 영어가 아닌 한국어로 되어 있을 경우, 모든 문서에 대해 번역하기보다는 한국어를 구사하는 미국 변호사가 초기검토와 두 번째 검토 후 연관성이 있는 데이터에 대해 번역을 하는 것이 훨씬 비용 효율적이다.

마지막 생산 단계에서는 한국어 문서 제공에 대해 가장 합리적인 제공 방법을 합의회의에서 사전에 협의할 수 있다.

아직 우리나라의 e-Discovery 제도가 확립되어 있진 않지만, 이러한 국내 특징을 반영하여 국내에서 e-Discovery를 실행할 경우, 시간과 비용 면에서 상당히 효과적으로 소송을 진행할 수 있을 것으로 기대한다.

References

[1] Jin-suk Byun, "US civil litigation and discovery: its contributions and limitations," Study on the American Institution, Vol .23 No. 3, pp 129-162, Dec. 2012.

[2] Bokman Jun and Jinhoon Park, "A study on maintenance of the e-discovery for intellectual property disputes in the arbitration," Law of Science & Technology, Vol. 18 No, 3 pp 369-404, Nov. 2012.

[3] Nicholas M. Pace and Laura Zakaras, "Where the money goes: understanding litigation expenditures for producing electronic discovery," A RAND Law, Business, and Regulation Institute, 2012.

[4] "Reviewing document security solutions for the internal information security," Security World, Jan. 2009.

[5] "'Groupware? ERP? DW? CRM' Major Corporation Solution Market Trend," KRG Annual Report, May 2002.

[6] Karen Schuler, Cathleen P. Peterson and Eva Vincze, "E-discovery: creating and managing an enterprisewide program." Syngress, Nov. 2008.

[7] "Multilingual e-disclosure: options, obstacles and opportunities report," Kroll Ontrack, 2014.

[8] Wayne Wong, "Six practical tips for eDiscovery in Asia and the Pacific," Inside Counsel, Jul. 2012.

[9] Gyugon Cho, "Implementing enterprise DRM," Journal of The Korean Institution of Information Scientists and Engineers, Vol. 23, No. 8, pp 31-36, Sep. 2005.

[10] Dongchan Lee and Sangjin Lee, "Research of organized data extraction method for digital investigation in relational database system," Korea institute of Information Security & Cryptology, Vol 22, No.3, Jun. 2012.

[11] A project of the Sedona Conference Working Group on electronic document retention & production (WG1), "Database Principles: addressing the preservation and production of database and database information in civil litigation." The Sedona Conference®,

2014.
〔12〕 Suzanne Herrmann Brock ,"DuPont v. Kolon: a lesson in how to avoid sanctions for spoliation of evidence," E-Discovery Law Alert, Sept. 2011.
〔13〕 Daryl Shetterly, "The world is flat: handling foreign language documents in e-discovery projects," LexisNexis® Legal Newsroom , Sept. 2011.
〔14〕 John T. Philips, "Implementing litigation readiness principles and practices," ARMA International Educational Foundation, Dec. 2012.
〔15〕 Michael D. Berman, Courtney Ingraffia Barton and Paul W. Grimm, "Managing e-discovery and ESI from pre-litigation through trial," Americal Bar Association, 2011.
〔16〕 Sally A. Kane, "Breaking into e-Discovery," Law Practice Today, Jan. 2012.
〔17〕 Veritas Official Blog, "Litigation readiness and your IT infrastructure: spring cleaning," Veritas Official Blog, May 2011.
〔18〕 A project of the Sedona Conference Working Group 7, "The Sedona Canada commentary on practical approaches for cost containment: best practices for managing the preservation, collection, processing, review & analysis of electronically stored information," The Sedona Conference®, Apr. 2011.
〔19〕 Stephanie F. Stacy, "Litigation holds: ten tips in ten minutes," Baylor, Evnen, Curtiss, Gimit & Witt, LLP, Jul. 2010.
〔20〕 A project of the Sedona Conference Working Group on best practices for electronic document retention & production, "The Sedona guidelines, best practice guidelines & commentary for managing information & records in the electronic age," The Sedona Conference®, Nov, 2007.
〔21〕 Patricia E. Antezana and Steven C. Bennett, "ESI preservation in employment litigation: counsel s guide to new FRCP ediscovery amendments," Park Jensen Bennett LLP & Reed Smith LLP.
〔22〕 Nicholas Panarella and Wook Kim, "Implementing a litigation hold," Kelley Drye LLP, Apr. 2012.
〔23〕 Legal Update, "Litigation law alert: litigation holds," Stoel Rives LLP, Jun. 2011.
〔24〕 Akers, S., Mason, J. K., & Mansmann, P. L., "An intelligent approach to e-Discovery," University of Maryland, Dec. 2011.
〔25〕 Cory Doctorow, "Microsoft research DRM talk," Microsoft Research Group, Jun. 2004.
〔26〕 Erik Hammerquist, Jim Scarazzo and Daniel Roffman, "Understanding remote collections for e-discovery: benefits, pitfalls and use cases (part 2): remote collections can be less time consuming and less intrusive than on-site collections," Inside Council, May 30, 2014.
〔27〕 Conrad Jacoby, Jim Vint and Michael Simon, "Database lie! successfully managing structured data, the OFT-overlooked ESI," Richmond Journal of Law & Technology Volume XIX Issue 3, 2013.
〔28〕 Craig Ball, "Beyond data about data: The litigator's guide to metadata," 2011.
〔29〕 Gregory Schodde, "E-Discovery: collect metadata to avoid ESI headaches," Inside Counsel, Oct. 2012.
〔30〕 Chris Pavan and Nick Ringold, "Overcoming data encryption for forensic imaging and collections, litigation support: document forensics and legal holds," ILTA White Paper, May 2009.
〔31〕 Gregory L Fordham, "Eleven steps to designing an e-Discovery plan and protocol: a systems engineering approach to modern litigation," Fordham Forensics, Dec. 2015.
〔32〕 Alan M. Anderson, "Issuing and manag-

ing litigation-hold notices," Bench & Bar of Minnesota, Aug. 2007.
〔33〕 A project of the Sedona Conference Working Group on electronic document retention & production (WG1), "Commentary on legal holds: the trigger & the process," The Sedona Conference®, 2010.
〔34〕 Staff Writer, "Trials and translation," Inside Counsel, Jan. 2009.
〔35〕 Shira A. Scheindlin, Daniel J. Capra and the Sedona Conference®, "Electronic discovery and digital evidence: cases and materials," West, May 2012.
〔36〕 Wanted: temp attorneys with foreign language skills," Wall Street Journal, Jul. 2012.
〔37〕 David Degnan, "Accounting for the costs of electronic discovery," Minnesota Journal of Law, Science & Technology Volume 12 Issue 1 Article 7, 2011.
〔38〕 "Predictive review: practical uses of active learning technology to improve the quality of e-Discovery and control costs," Servient™, Dec. 2010.

〈저자소개〉

이 신 형 (Shin-hyung Lee) 정회원
2000년 7월: University College London 수학과 졸업
2004년 9월: University College London 컴퓨터공학 석사 졸업
2010년 3월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, e-Discovery, Digital Forensics

이 상 진 (Sangjin Lee) 정회원
1989년~1999년: ETRI 연구원
1999년~현재: 고려대학교 교수
〈관심분야〉 e-Discovery, 디지털포렌식, 모바일포렌식, 심층 암호, 해쉬 함수