情 報 保 護 學 會 誌
第18卷 第1號, 2008. 2

국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법제 현황

백 승 조*, 심 미 나*, 임 종 인*

요 약

최근 소송에서의 디지털 증거의 비중과 수사과정에서의 디지털 포렌식의 중요성과 관심이 높아지고 있으며, 미국을 포함한 여러 국가들은 이러한 추세를 반영하여 효과적인 디지털 증거 수집과 분석을 위한 법제들을 마련하고 있는 상황이다. 국내의 경우도 디지털 포렌식 기술에 대한 관심과 실제 사건해결에 있어서의 이용도가 높아지고 있음에도 아직까지 관련 법제들은 미비한 상황이다. 본고에서는 먼저 '국가 디지털 포렌식 법률 체계'를 제시하고 각각의 구성요소들에 대해 살펴본 후, 국가 디지털 포렌식 법률 체계에 기반하여 미국의 법제 현황과 국내 법제 현황을 비교한다. 또한 디지털 포렌식 수행 절차에 따른 법적 요구사항들을 정의해보고, 국가 디지털 포렌식 법률 체계 완성을 위한 추진방안을 제시한다. 마지막으로 효과적인 디지털 증거의 수집·분석과 디지털 포렌식 기술 활성화를 위해 국내 법제들이 나아가야 할 방향과 추진방법을 제시한다.

Ⅰ. 서 론

발달된 정보통신 인프라로 인해 다양한 디지털 역기능과 사이버범죄에 심각히 노출되어 있는 국내의 경우 디지털 증거가 효과적인 법적 증거로 활용될 수 있는 환경을 제공하고 정보·수사기관과 민간 기업들이 이러한 디지털 역기능과 사이버 범죄에 효과적으로 대응하는데 디지털 포렌식 기술을 널리 활용할 수 있도록 저변을 확대할 수 있는 관련 법제들의 제정 및 개정이 다른 국가들보다 더욱 더 시급히 요청되고 있다.

최근 들어 많은 판례에서 디지털 증거가 법적 증거로서 인정이 되는 등 국내 민·형사소송에서의 디지털 증거에 대한 의존도와 정보·수사기관들과 민간기업들의 디지털 포렌식 기술에 대한 관심도 꾸준히 높아지고 있다. 국내에서는 관련 법제의 미비로 인해 그 적법성과 활용범위가 매우 제한적인 상황이다. 일심회 사건의 경우에서처럼 디지털 증거의 법적 증거 허용성과 디지털 포렌식 툴과 절차의 유효성을 적극적으로 해석하려는 판결들이 늘어나고 있지만, 신정아 사건에서 볼 수 있는 것처럼 아직까지 법제의 미비와 명확한 원칙의 부재 등으로 인해 디지털 증거 허용성 기준과 디지털 수사 원칙을 두고 혼선이 일어나고 있는 상황이다.

이러한 배경에서 최근 들어 디지털 증거와 관련된 민사소송법 및 형사소송법에 대한 개정 요청이 높아지고 있다. 하지만, 국가 정보·수사기관 및 민간 기업에서의 디지털 포렌식 기술의 적절한 활용능력의 확보가 국가와 기업의 경쟁력이 되어가고 있는 상황에서 디지털 증거의 적법성 확보를 통한 법질서 확립과 정의구현 및 디지털 포렌식 기술 활성화를 통한 경쟁력 강화라는 궁극적인 목적을 달성하기 위해서는 한 두 개의 개별적인 법률의 개정이 아니라, 수사·정보기관, 민간기업, 관련 산업체와 같은 모든 주체들의 참여를 전제로 한 국가 디지털 포렌식 체계에 기반한 '국가 디지털 포렌식 법률 체계'의 수립과 각 법 요소 간 균형 있는 발전이 요구된다. 또한 2006년에 미국 기준 15억 달러 수준의 규모를 달성하고 매년 60% 성장률을 기록하고 있는 민간 디지털 포렌식 시장에서의 국내 업체들의 시장 형성 및 활성화를 통한 경쟁력 확보를 위해서도 형사소송법 등의 개별 법률의 개정이 아닌 민간 디지털 포렌식 시장과 국가기관의 포렌식 시장의 균형 있는 발전을 보장할

* 고려대학교 정보경영공학전문대학원 (nomadvirus@korea.ac.kr, mnshim@korea.ac.kr, jilim@korea.ac.kr)

수 있는 '국가 디지털 포렌식 법률 체계'의 확립과 이에 따른 지속적인 법제 제·개정 노력의 추진이 요구된다.

Ⅱ. 국가 디지털 포렌식 법률 체계

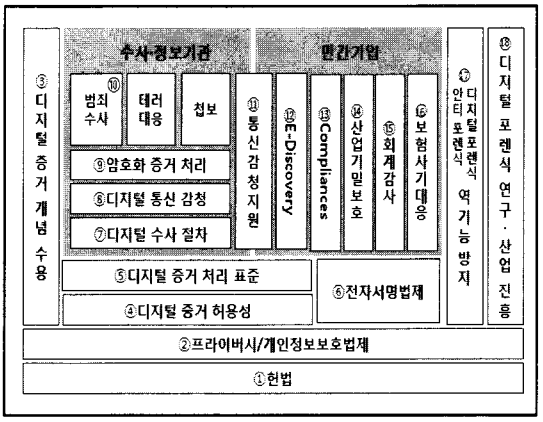
국가의 디지털 포렌식 기술 수준이 수사·정보기관과 민간기업, 그리고 관련 산업의 국가경쟁력의 핵심요소로 대두됨에 따라 국가 차원에서 민간기업, 국가기관의 국가경쟁력 향상과 기업과 국가차원의 효과적인 위험관리를 위한 디지털 포렌식 체계의 수립이 요청된다.

국가 디지털 포렌식 프레임워크는 국가적 차원의 디지털 증거 활용을 통한 법질서 확립과 정의 구현 및 디지털 포렌식 기술개발 촉진과 이용 활성화를 위한 관련 산업계, 수사 기관 및 정보기관, 그리고 민간기업과 같은 관련 주체들의 역할과 상호관계를 수립함으로써 적절한 역할분담을 통해 효과적으로 디지털 포렌식 프로세스를 추진하는 체계라고 정의할 수 있다. 이러한 국가 디지털 포렌식 프레임워크는 관련 법제들의 뒷받침이 있어야만 그 효과성을 보장받을 수 있다.

국가 디지털 포렌식 법률 체계는 개별적인 법률들의 단순한 집합이 아니라, 디지털 증거의 적법성 확보와 디지털 포렌식 기술 활용과 관계된 법 목표들의 유기적인 체계로 구성되어 있다. 각 국가들은 국가 디지털 포렌식 법률 체계를 이용하여 이러한 디지털 증거와 디지털 포렌식과 관련된 법원칙 및 법조항 요소들이 균형 있게 발전하고 있는지에 대해 검토하고 미비한 법률들을 제·개정을 통해 보강하는데 활용할 수 있다. 이러한 과정을 통해 국가 디지털 포렌식 법률체계 상의 각각의 부분들에 대해 법제들의 요구사항들을 만족시킬 수 있을 때 효과적인 수사권의 확보와 프라이버시와 같은 국민들의 기본권 보호간의 균형과 함께 국가와 민간의 디지털 포렌식 산업의 균형 있는 발전이 보장될 수 있다.

본고에서는 다음 [그림 1]과 같은 국가 디지털 포렌식 법률체계를 제시한다.

국가 디지털 포렌식 법률 체계는 크게 디지털 포렌식 및 디지털 수사 기본 법원칙과 국민의 기본권에 관한 부분, 디지털 증거 허용성에 관한 부분, 수사·정보기관의 디지털 수사 원칙에 관한 부분, 정보·수사기관의 디지털 포렌식 활용에 관한 부분, 정보·수사기관과 민간 기관의 디지털 수사 협업에 관한 부분, 민간기업의 디지털 포렌식 활용 촉진에 관한 부분, 건전한 디지털 포렌식 기술 이용 환경 조성을 위한 부분, 디지털 포렌식 연구 지원 및 산업 활성화를 위한 부분 등으로 구분할 수 있다.



〔그림 1〕. 국가 디지털 포렌식 법률 체계

Ⅲ. 국가 디지털 포렌식 법률체계와 국내·외 법제 현황

[그림 1]에서 국가 디지털 포렌식 법률 체계를 구성하고 있는 법 목표 및 영역들을 하단에서 상단, 왼쪽에서 오른쪽 순으로 살펴보고, 각각의 구성요소들에 해당하는 미국 법제 현황과 국내 법제 현황을 살펴보도록 하겠다.

3.1. 디지털 포렌식 및 디지털 수사 기본 법원칙과 국민의 기본권에 관한 부분

디지털 포렌식 기술을 이용한 디지털 수사는 명확한 법적 근거를 가지고 수행되어야 하며, 헌법에서 보호하고 있는 국민들의 기본권을 과도하게 침해하거나 디지털증거 수집 및 분석 시 국민들의 개인정보에 대한 처리 및 보호원칙을 담고 있는 프라이버시 법률 조항들과 모순되어서는 안 된다.

① 헌법

디지털 증거의 적법성과 디지털 증거 수집 및 분석과 같은 일련의 디지털 수사 과정의 적법성, 그리고 디지털 포렌식 기술의 적법성은 모두 근본적으로 헌법에 합치되고 모든 디지털 수사 행위는 헌법에 근거해야 한다. 특히 많은 국가의 헌법에서는 국민의 기본권으로 프라

이버시권을 두고 있으며, 디지털 정보에 대한 압수, 수색은 적법한 절차에 의해서만 이루어지도록 하고 있다. 법률에 의하지 않고는 국민의 기본권(사생활 보호 및 양심의 자유)을 제한할 수 없다는 헌법상 원칙을 위반해서는 안 된다.

미국의 경우 수정헌법 4조에서 영장에 의하지 않고서는 압수 수색을 당하지 않는다는 '영장주의의 원칙'을 제공하고 있으며, 다시 수정헌법 5조와 14조에서는 국가권력의 행사는 반드시 법률로 정해진 절차를 따라야 하며 이러한 적정절차를 따르지 않고 수집된 증거는 법적증거에서 배제될 수 있다는 '적법절차의 원칙(Due Process)'을 제공하고 있다. 미국에서의 디지털 수사는 이러한 수정헌법의 조항의 원칙들을 준수해야 하며, 원칙적으로 영장과 적정절차를 따라 디지털 증거 수집 및 분석을 수행해야 한다.

대한민국 헌법에도 12조에 체포, 구속, 압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다는 영장주의 원칙 및 적법절차 원칙을 명시하고 있다.

② 프라이버시/개인정보보호 법제

'개인이 혼자 있을 수 있는 권리' 혹은 '자기정보에 대한 통제권'을 의미하는 (정보)프라이버시는 유럽을 포함한 많은 국가에서 헌법상의 기본권으로 인정되고 있다. 디지털 증거의 수집과 분석과정을 포함하는 일련의 디지털 수사는 범죄 억제를 위한 수사권의 확보라는 목표와 프라이버시라는 헌법적 가치의 균형을 통해 이루어져야 한다. 국가 정보·수사기관에 의한 수사 목적의 개인정보의 수집·이용은 개인정보보호법제에 근거하여 이루어져야 한다. 국민의 프라이버시 권리와 충돌하지 않는 디지털 증거 수집과 분석을 위해서는 개인정보보호를 규율할 수 있는 명확한 법률이 우선 존재해야 한다. 또한 수집된 개인정보는 특정 수집 목적에 맞는 범위 내에서만 최소한도로 수집되고 합목적적으로 사용되어야 하며, 개인정보보호법에서 명시하고 있는 개인정보 수집, 전송, 이용, 폐기에 이르는 일련의 개인정보 라이프사이클에 따라 적절한 보호가 제공되어야 한다.

현재 많은 국가에서 OECD Privacy Guideline을 기초로 공공기관 및 민간기관이 보유하고 있는 개인정보를 규율할 수 있는 자국 프라이버시/개인정보보호 법제를 두고 있는데, 디지털 포렌식 기술을 이용한 디지털 수사는 이러한 프라이버시/개인정보보호법제에서 요구하고 있는 절차와 원칙과 충돌하지 않아야 한다. 미국의 ECPA(Electronic Communication Privacy Act)의 경우 국민들의 프라이버시 침해를 최소화하면서 수사권을 확보할 수 있는 디지털 통신 감청 절차와 원칙에 대해 규정하고 있다.

국내에서는 헌법 17조에 헌법적 권리로서 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다'는 프라이버시권을 규정하고 있으며, 개인정보보호를 위한 법률로서 민간기관이 수집한 개인정보에 대해 규율하는 '정보통신망이용촉진및정보보호에관한법률'과 공공기관이 수집한 개인정보에 대해 규율하는 '공공기관의개인정보보호에관한법률'을 두고 있다. 최근 들어 일관된 개인정보보호 원칙과 효과적인 집행력을 보장하기 위한 민관, 공공기관의 개인정보를 아우르는 일원화된 개인정보보호기본법에 대한 필요성이 지속적으로 논의되고 있는 상황으로, 디지털 포렌식을 이용한 민·형사 소송을 위해 디지털 증거 수집 및 분석과정에서 국민들의 프라이버시 기본권 침해를 최소화하기 위해서는 일원화된 개인정보보호기본법의 제정이 요구된다.

3.2. 디지털 증거 허용성에 관한 부분

디지털 포렌식을 통해 수집한 디지털 증거가 민·형사 소송 과정에서 법적 증거로서 인정받기 위해서는 기본적으로 관련 법제에 민·형사 사건의 법적 증거로 디지털 증거 개념이 포함되어야 하며, 관련 법제에 디지털 증거가 법적 증거로 인정받을 수 있기 위한 조건과 기준이 명시되어야 한다. 또한 디지털 포렌식 기술을 활용한 관련 법제에 적법한 디지털 증거 수집 및 분석 절차 표준이 제공되어야 하며 디지털 증거가 적법한 증거로 인정받을 수 있는 기술적 시스템으로 전자서명 등을 활용할 수 있는 인증기관의 법적 근거를 제공해야 한다.

③ 디지털 증거 개념 수용

디지털 증거는 물증과 같은 일반적인 증거와는 다른 특성을 갖는다. 디지털 증거는 일반적으로 눈에 보이지 않는 무형의 정보재이며 위변조가 쉽다는 점에서 다른 증거들과는 구분된다. 기존에 존재하던 증거 수집 및 분석과 관련된 대부분의 법률들은 눈에 보이는 아날로그 증거들을 대상으로 한 것들이기 때문에 관련 법률들은

기존의 법률에 디지털 증거 개념과 특성들을 포함하여 개정되어야 한다.

미국의 경우 민사소송법, 형사소송법, ECPA, CALEA를 포함한 여러 법률들에서 디지털 증거 및 컴퓨터 통신 증거 개념을 수용하고 있다.

국내의 경우 민사소송법과 형사소송법 그리고 그 외의 관련 법제에 법적 증거의 유형으로 디지털 증거가 아직까지 포함되어 있지 않은 상황이다. 통신비밀보호법의 경우, 현행법에서는 유선 전화 통신만을 대상으로 하고 있지만, 최근 개정안에서는 컴퓨터를 이용한 디지털 통신을 대상으로 포괄하고 있는 등 각종 법률에서 디지털 증거 개념의 수용이 고려되고 있다.

④ 디지털 증거 허용성

디지털 증거의 허용성은 디지털 증거가 민·형사소송의 법적 증거로서 인정되고 법정에서 활용되기 위한 조건을 말한다. 이를 위해서는 증거 수집 및 분석 관련 법률들에서 명확히 디지털 증거를 포함시킬 필요가 있으며, 디지털 증거는 위변조가 쉽다는 특성 때문에 기존의 아날로그 증거들보다 법적 증거로서 높은 허용성을 인정받기 위해서는 엄격하고 세밀한 허용성 판단 기준들을 필요로 한다.

미국의 경우 연방형사소송절차규칙과 연방증거규칙(FRE)에서 디지털 증거의 허용성에 대한 내용을 담고 있으며, Lorraine v. Markel 사건의 Paul Grimm 판사의 판결문에서처럼 판례를 통해 구체적인 디지털 증거 허용 기준을 제시하고 있다. 미국은 이처럼 다양한 판례들을 통해 디지털 증거와 디지털 포렌식이 법적 증거로서 유효성이 인정되고 있는데, 이는 디지털 증거 표준 처리 절차와 디지털 증거 허용성 평가 기준의 법적 정립과 함께 엄격한 과학적 기준에 근거한 디지털 포렌식 툴에 대한 유효성 검증절차를 통해 보장된다.

반면 국내는 2007년 10월 개정된 형사소송법 제134조의 7(컴퓨터용 디스크 등에 기억된 문자정보 등에 대한 증거조사)과 제134조의 8(음성, 영상자료 등에 대한 증거조사) 부분에 디지털 증거에 대한 간단한 언급을 하고 있지만, 미국과 달리 형사소송법상에 디지털 증거가 출력된 서증이 동일한지 여부를 입증할 수 있는 법적 기준이나 절차가 없으며 서증으로 전환이 불가능한 디지털 증거는 현행법상 어떤 방법으로도 증거에 포함될 수 없다는 문제점이 존재한다.

⑤ 디지털 증거 수집·분석 절차

디지털 증거가 법적 증거로서 인정받기 위해서는 헌법과 프라이버시 법제와 모순되지 않는 표준화된 수집 및 분석 절차를 갖추어야 한다. 디지털 증거는 적법한 절차에 의해 수집되고 처리되어야 하며 디지털 증거는 쉽게 위·변조될 수 있다는 단점이 존재하므로 수집된 디지털 증거가 수집 및 분석 과정에서 위·변조되지 않았음을 보증할 수 있는 표준화된 절차가 법적으로 마련되어야 할 것이다.

미국의 경우 NIST(National Institute of Standard Technology)에서 최초의 표준화된 디지털 증거 표준 가이드라인을 제시하고 이 가이드라인에 따라 증거 수집 및 분석이 이루어지도록 법적으로 보장하고 있다.

국내에서는 최근 경찰청에서 디지털 증거 처리 표준 가이드라인이 작성되었으나, 이러한 표준 준수를 의무화할 수 있는 법조항 등이 존재하지 않아 가이드라인의 실효성이 높지 않은 상황이다.

⑥ 전자서명 법제

위변조 가능성이 높은 디지털 증거의 법적 허용성을 높이기 위한 효과적인 기술적인 대응책 중의 하나는 전자서명-인증서 시스템을 이용하는 것이다. 디지털 문서 작성자의 전자서명은 수집된 디지털 증거에 대해 실제 정보를 생산한 사람이 누구인지, 데이터 증거 위변조는 없었는지에 대한 증명을 제공해주는 한편, 디지털 증거 인증기관의 전자서명-인증서는 디지털 증거에 대해 디지털증거인증기관의 전자서명을 한 후 보관함으로써 수집 이후에 디지털 증거가 위·변조되지 않았다는 사실을 보증하는 메커니즘으로 사용된다.

실제 전자서명과 인증서는 전자문서 및 전자거래 계약서가 적법하게 작성되었음을 증명하기 위한 기술로 사용되고 있으며, 미국에서는 전자서명법(ESign Act)과 통일컴퓨터정보거래법(UCITA)에서 이러한 전자거래의 인증기능을 위해 전자서명의 사용을 법제화하고 있으며 5년여 전부터 전자정보의 법적 증거 허용성을 제공해줄 기반 기술로 전자서명을 활용하는 방안을 모색해오고 있다.

반면 국내의 경우 세계 최대의 공인인증서 사용국임에도 불구하고 전자서명법은 금융거래 등의 목적의 전자서명 및 인증서 이용에 국한되어 있는 상황이므로 전

자서명을 디지털 문서 인증 및 디지털 증거의 허용성 확보를 위해 활용하고 PKI 시스템을 활용하여 디지털 증거 인증센터를 설립, 운영하기 위한 법적 근거를 마련하기 위한 법조항을 추가할 필요가 있다.

3.3. 수사 · 정보기관의 디지털 수사 원칙에 관한 부분

수사 · 정보기관의 디지털 포렌식 기술을 이용한 디지털 수사를 적법하고 효과적으로 수행하기 위한 필수적인 법 환경을 마련하기 위한 부분으로 수사 · 정보기관이 디지털 수사를 수행함에 있어 적법 절차를 따르도록 보장하는 법적으로 표준화된 디지털 수사 절차가 우선 제시되어야 할 필요가 있다. 주요 디지털 증거 수집 통로 중의 하나인 디지털 통신 감청 또한 적법 절차와 원칙에 따라 국민들의 기본권을 침해하지 않는 선에서 수행하게 하는 법제가 마련되어야 하며 효과적이고 원활한 합법적 디지털 통신 감청을 위해 정보통신사업자가 정보 · 수사기관에게 협조할 수 있도록 의무화하는 법안 및 적법하게 수집된 디지털 증거가 암호화되어 있을 경우 효과적으로 복호화하여 법적 증거로 제시할 수 있는 법제 또한 마련되어야 한다.

⑦ 디지털 수사 절차

수사 · 정보기관은 수사 및 첩보임무 수행과정에서 디지털 포렌식 기술을 적법한 절차에 따라 이용해야 한다. 일반적으로 디지털 수사 절차는 민간 기업이나 개인들이 컴플라이언스 및 자사 정보시스템과 데이터를 보호하기 위해 수행하는 디지털 정보 수집 및 분석 절차와는 다르게 수사과정에서 적법한 수사 절차를 준수해야 한다. 특히 이러한 수사절차를 준수하지 않고 불법적으로 취득된 증거는 '불법증거배제의 원칙'에 따라 법정에서 증거로 이용되지 못하게 될 뿐 아니라, '독수과실이론'에 의해 불법으로 획득된 증거에 의한 2차적 증거도 증거로서 인정되지 못하게 된다. 미국은 이러한 적법한 수사 원칙과 절차에 대해 연방형사소송절차에 명시하고 있다.

국내법에서 적법한 수사절차는 일반적으로 '형사소송법'에 법적으로 명시되어 있는데, 형사소송법에는 압수 · 수색영장과 같은 영장제도와 영장이 불필요한 예외상황을 명시해놓고 있다. 하지만 아직 디지털 증거 수집 및 분석과 관련한 표준화된 원칙이나 절차와 관련된 조항은 없는 상황이다.

⑧ 디지털 통신 감청

디지털 통신 감청은 정보수사기관의 디지털 증거 수집을 위한 주요한 수단으로, 디지털 통신 감청은 일반적인 디지털 수사의 경우와 마찬가지로 적법한 절차와 국민의 기본권 보호 원칙을 통해 수행되어야 한다. 현재 많은 국가에서는 국민들의 프라이버시권 침해를 최소화하면서 범죄 및 테러 억제 목적으로 수사권을 충분히 보장하기 위하여 적법하게 디지털 통신을 감청할 수 있도록 하는 법적 권한과 절차를 제공하고 있다.

미국은 실시간 통신내용, 저장된 내용, 통신사실 확인자료, 기본정보 등 수집하는 통신정보의 종류에 따라 Pen/Trap Act, Title III, ECPA 등으로 세분화하여 규정하고 있다.

국내의 경우 현행 통신비밀보호법에는 디지털통신에 대한 감청 조항이 제공되지 않고 유선 전화통신에 대한 감청만 허용하고 있지만, 최근 통신비밀보호법 개정안에서는 컴퓨터간의 디지털 통신 감청에 대해서도 법적으로 규정하고 있다.

⑨ 암호화된 증거의 처리

합법적으로 수집된 디지털 증거라도 암호화되어 있어 적절한 시간 내에 평문으로 복호화하지 못한다면 소송에서 유의미한 증거로서 사용될 수 없다. 따라서 적법하게 수집된 암호화된 정보를 적시에 복호화할 수 있는 제도적, 기술적 절차가 법적으로 마련되어야 한다.

일반적으로 암호화된 증거의 처리와 관련된 법제도적 대안은 강제로 복호화하도록 의무화하는 복호화 명령과 키위탁 및 복호화키를 제출할 것을 명령하는 복호화키 제공 명령을 들 수 있는데, 유일하게 영국이 복호화명령 및 키제공 의무화를 RIPA 법안을 통해 법제화하고 있다. 미국을 포함하여 국내에도 암호화 증거처리에 관한 법안 및 법조항은 존재하지 않은 상황이다.

3.4. 정보 · 수사기관의 디지털 포렌식 활용에 관한 부분

정보 · 수사기관은 범죄수사, 테러대응, 첩보임부 수행을 포함한 다양한 목적으로 디지털 포렌식 기술을 활

용하고 있으며, 이러한 임무 수행을 위해 디지털 포렌식 기술을 어떻게 활용할 것인가에 대한 법적 근거 마련이 필요하다.

⑩ 범죄수사, 테러대응, 첩보

현재 정보·수사기관은 범죄수사, 테러대응, 첩보임부 수행을 포함한 다양한 목적으로 디지털 포렌식 기술을 활용하고 있으며, 일반 범죄 및 사이버 범죄 수사, 테러대응, 첩보 관련 법제에서 디지털 포렌식 기술의 활용을 요구함으로서 디지털 포렌식 기술 및 디지털 증거 획득의 법적 근거를 마련할 수 있으며 디지털 포렌식 기술 활용을 촉진할 수 있다.

미국의 경우 특히 Homeland Security Act, Cyber Security Enhancement Act, Patriot Act와 같은 몇몇 테러 및 첩보 관련 법률에서 디지털 수사의 원칙과 디지털 포렌식 기술의 활용 및 연구 지원과 같은 조항을 두고 있는 반면, 국내에서는 형법, 국가보안법, 정보통신망법, 정보통신기반보호법, 국가사이버안전관리규정과 같은 관련 법률에서 디지털 포렌식 기술에 대한 구체적인 요구조항이 존재하지 않는다.

3.5. 정보·수사기관과 민간 기업의 디지털 수사 협업에 관한 부분

⑪ 디지털 통신 감청 지원

많은 국가에서 정보·수사기관의 적절한 절차를 통한 합법적인 디지털 통신 감청 요구에 대하여 정보·수사기관에 정보통신사업자 등으로 하여금 감청설비 등의 설치를 포함한 지원을 제공할 것을 요구하고 있는 법안을 제정함으로써 디지털 통신 감청을 원활하게 하고 있다.

미국에는 CALEA(Communication Assistance for Law Enforcement Act)가 있어서 정보수사기관의 적법한 감청 요청에 대해 정보통신사업자들이 정보를 제공하거나 감청설비를 설치할 것을 의무화하고 있다.

국내 현행법에는 이와 같은 법조항이 존재하지 않지만, 최근 통신비밀보호법 개정안에서 정보수사기관의 적법한 디지털 통신 감청요청에 대해 정보통신사업자등이 자사 네트워크에 디지털 통신 감청설비 등을 설치할 것을 요구하는 조항을 두고 있다.

3.6. 민간기업의 디지털 포렌식 활용 촉진에 관한 부분

현재 미국에서는 E-Discovery, 각종 컴플라이언스 준수, 회계감사, 산업기밀 보호, 보험사기 대응 등의 목적으로 민간기업의 디지털 포렌식 이용이 활성화되고 있는 상황이며 각각의 관련 법률에서 디지털 포렌식 이용을 권장, 의무화하는 조항을 추가함으로써 민간부분의 디지털 포렌식 산업 발전을 더욱 촉진하고 있다. 이러한 법률적 기반 하에 미국은 2006년 15억 달러에 이르는 민간 포렌식 시장의 성장을 달성할 수 있었다.

⑫ E-Discovery

민사소송에서 소송당사자들에게 소송관련 디지털 증거들을 제출할 것을 요구하는 E-Discovery는 현재 미국 디지털 포렌식 산업의 민간시장 수요의 많은 부분을 차지하고 있다. 많은 기업들은 E-Discovery 과정에서 소송 관련 디지털 증거 중 삭제된 증거물을 복구하거나 디지털 증거들의 위변조 여부를 파악하기 위해 디지털 포렌식 기술을 적절하게 활용하고 있다.

미국에서 E-Discovery 제도는 연방민사소송절차규칙(FRCP)에 의해 명시되어 시행되고 있는 반면, 국내 민사소송법에는 E-Discovery와 같은 제도가 명시되어 있지 않다. 이미 국제적 현대 비즈니스 환경에서 E-Discovery 준수는 필수적인 조건이 되었으므로 해외에 진출한 국내기업에서도 E-Discovery 준수를 위한 디지털 포렌식 기술의 사용은 필수적이 되고 있다. 향후 민사소송법 개정을 통한 E-Discovery 제도가 도입된다면 디지털 포렌식에 대한 민간부분 시장이 급속히 확대될 것으로 예상된다.

⑬ 각종 컴플라이언스들

현재 미국의 HIPAA, SOX, GLBA를 포함하여 해외에서는 각종 IT컴플라이언스들이 존재하고 있으며, 개인정보보호, 금융정보보호 등 관련 기관들이 준수해야 할 IT컴플라이언스 요구조건을 충족시키기 위한 목적으로 디지털 포렌식 기술이 민간시장에서 널리 이용되고 있다.

국내에도 '바젤II', '전자금융거래법', '회계개혁법', '금융권 재해복구 시스템 의무화' 등처럼 금융권과 개인정보보호를 중심으로 다양한 IT 컴플라이언스들이

생겨나고 있으며 보호를 위해 다양한 시스템 구축을 요구하고 있지만, 아직까지 디지털 포렌식 기술을 필수적인 시스템으로 요구하고 있는 상황은 아니다.

⑭ 회계 감사

미국의 대표적인 회계 관련 컴플라이언스인 SOX (Sarbanes-Oxley Act)가 내부통제강화를 위한 보호시스템을 갖추도록 의무화하면서 관련 판례와 법제 등을 통해 SOX 규제 준수를 위한 디지털 포렌식 도구의 사용을 권장하고 있는 반면, 국내의 주식회사의 외부감사에 관한 법률(외감법), 회계개혁법 등 관련 법안에서는 이러한 조항이 없다. 또한 미국에는 기업의 디지털 회계 자료에서 회계부정을 탐지해내는 포렌식 어카운팅 기술이 활성화되어 있는데 반해, 국내에서는 아직도 이러한 포렌식 어카운팅 기술의 이용과 활성화와 관련된 법제 및 법조항 또한 존재하지 않는다.

⑮ 산업기밀보호

전세계적으로 디지털 포렌식 기술은 산업스파이와 악의적인 내부자들로부터 산업기술과 영업 비밀을 보호하기 위한 핵심적인 기술로 널리 사용되고 있으므로, 산업기술보호를 위해 효과적으로 활용될 수 있도록 관련 법안에 디지털 포렌식 시스템의 도입을 권장 혹은 의무화하는 조항의 삽입이 요구된다.

현재 미국의 경제스파이법(Electronic Espionage Act)처럼 국내에도 산업기술유출방지법과 같은 산업스파이 등으로부터 영업비밀과 국가산업기술을 보호하기 위한 법제들이 존재하지만, 아직 영업비밀 및 산업기술 유출방지를 위한 디지털 포렌식 기술의 활용에 대해 요구하고 있는 조항은 포함되어 있지 않다.

⑯ 보험사기 대응

보험사기사건에서의 디지털 증거를 확보함으로써 보험범죄에 효과적으로 대응하기 위한 목적으로 디지털 포렌식 기술이 널리 사용되고 있다. 또한 향후에 디지털 증거 자체의 수집과 분석이 보험사기의 직접적인 증거가 되는 해킹보험, 전자상거래 보험 상품과 같은 사이버 보험(Cyber Insurance)에 대한 수요가 증가할 것으로 예상되므로, 이에 대한 적절한 대응을 할 수 있는 법제 마련이 요구된다고 할 수 있다.

국내에는 보험사기를 포함한 보험에 대한 전반적인 내용을 담고 있는 보험업법 등이 존재하고 있지만 사이버 보험사기에 대한 대책이나 보험사기 사건의 디지털 증거 확보 및 분석을 위한 디지털 포렌식 도구의 활용에 대한 법제 및 법조항은 아직까지 존재하지 않는 상황이다.

3.7. 건전한 디지털 포렌식 기술 이용 환경 조성을 위한 부분

⑰ 디지털 포렌식 · 안티 포렌식 기술의 역기능 방지

디지털 포렌식 기술과 안티 포렌식 기술은 법질서 확립과 정의구현을 위한 핵심적인 도구로 사용될 수 있는 반면, 악의적 목적으로 사용될 경우 심각한 범죄 도구나 타인의 프라이버시 침해도구로 사용될 수 있다는 위험성이 상존한다. 따라서 디지털 포렌식 기술은 명확한 법적 근거와 적법한 절차에 따라 가능한 권한 있는 자에 의해서 선의의 목적으로만 이루어질 수 있도록 함으로써 디지털 포렌식 기술의 역기능을 방지할 수 있어야 한다. 아직까지 대부분의 국가에서 디지털 포렌식 기술이 범죄자 등에 의해 범죄에 악용되거나 프라이버시에 대한 강력한 침해도구로 사용되는 것을 막기 위한 디지털 포렌식 기술의 역기능 방지 법제는 거의 없다. 극소수 국가의 경우 해커들이나 범죄자들이 주로 사용하는 안티 포렌식 기술도구를 불법화하는 강력한 법적 조치를 하기도 하지만 일반적이지는 않다. 앞으로 디지털 포렌식 도구 및 안티 포렌식 도구의 정당한 권한 없는 자의 이용 및 범죄적 목적의 이용의 경우 사용자에 대해 가중 처벌하는 등 법적 수단이 모색될 필요가 있다.

국내에서도 아직 디지털 포렌식 기술의 역기능과 안티 포렌식 기술의 역기능을 방지하기 위한 법제 및 법조항은 존재하지 않는다. 국내에서는 이제야 안티 포렌식 기술의 역기능에 대한 대응 기술과 법제도적 방지대책에 대한 논의가 이루어지고 있다

3.8. 디지털 포렌식 연구 지원 및 산업 활성화를 위한 부분

⑱ 디지털 포렌식 연구 및 산업 진흥

디지털 포렌식 기술의 국가적 중요성이 높아짐에 따라 국가적 차원의 디지털 포렌식 기술의 연구 지원 및 민간 디지털 포렌식 산업 진흥을 위한 법제도적 지원이 필요한 상황이지만, 아직까지 이러한 디지털 포렌식 기술의 연구 지원 및 민간 산업 활성화 법안은 거의 없는 상황이다.

미국의 경우 Patriot Act 등 법률을 통해 디지털 포렌식 연구센터에 대한 재정 지원을 할 수 있다는 조항을 법제화함으로서 지속적인 기술 개발과 함께 안전하고 지속적인 디지털 분석 기능을 수행할 수 있도록 하고 있다.

이에 반해 국내의 경우 경찰청 산하 디지털증거분석센터와 같은 디지털 포렌식 센터의 활동과 예산편성에 대한 법적 근거 조차 미비한 상황이며, 디지털 포렌식 기술 연구 지원과 민간 산업 진흥에 대한 법제 및 법조항이 존재하지 않는다. 디지털 포렌식 기술의 사용이 수사기관 중심으로 편중되고 민간 포렌식 산업이 발전하지 못한 국내의 경우 국가 정보·수사기관 및 민간기업의 국제경쟁력을 높이기 위해 디지털 포렌식 연구 및 민간 디지털 포렌식 산업 진흥을 위한 법제도적 노력을 기울여야 한다. 이러한 법제도적 노력에는 디지털 포렌식 기술연구 지원 조항의 마련, 각 기관 산하 디지털 포렌식 연구센터 및 디지털증거분석센터의 법적 근거 제공, 디지털 포렌식 민간산업 진흥법안 마련, 디지털 포렌식 교육의 의무화 및 전문가 양성을 위한 법조항 마련 등을 들 수 있다.

Ⅳ. 국내외 디지털 포렌식 법제 현황 비교

지금까지 국가 디지털 포렌식 법률 체계 구조 및 각 구성요소들의 법 목적 및 국내외 현황에 대해 살펴보았다.

미국은 각 법률 구성요소들에 대해 나름대로 균형 잡힌 법제화 노력들을 하고 있는 반면 국내의 경우 아직 기본적인 법제들조차 제대로 갖추고 있지 못하며, 최근들어 국내에서도 정보·수사기관의 디지털 수사에 대한 법률적인 관심과 고려가 많이 생겨나고 있을 뿐 아직도 민간 디지털 포렌식 시장에 대한 법제적 고려는 거의 없다는 사실을 알 수 있다.

구체적으로 살펴보자면 미국과 영국을 포함한 일부 선진국들은 단순히 디지털 증거 허용성이나 절차를 갖추는데 머물지 않고 수사·정보기관뿐만 아니라 민간 기업에서의 디지털 포렌식 기술 이용을 촉진하고 산업 활성화를 위한 다양한 법제도 마련을 위한 노력을 하고 있는 상황이다. 특히 디지털 포렌식 기술이 정보수사기관뿐만 아니라 민간 기업에 이르기까지 균형 있게 활성화되어 있는 선진국이라고 할 수 있는 미국은 특히 이러한 일련의 국가 디지털 포렌식 법체계의 다양한 법 목표와 기능들을 고르게 가지고 있다. 미국은 증거법과 민·형사 소송절차규칙과 증거법에서 디지털 증거 개념을 수용하였고 디지털 증거 처리 절차 가이드라인을 세계 최초로 제작하고 실제 수사와 재판에서 이용을 의무화하였으며, 디지털 증거가 허용될 수 있는 조건을 명확히 함으로써 디지털 증거의 신뢰도와 활용도를 높이는 한편, 법조항 명시나 판례를 통해 수사정보기관과 민간 기업에게 다양한 목적으로 디지털 포렌식 기술을 이용할 것을 권유 및 의무화함으로써 디지털 포렌식 기술의 저변을 확대하고 활성화하기 위한 기본적인 환경을 제공한다.

반면 국내에서는 디지털 증거의 가치와 디지털 포렌식 기술에 대한 관심이 높아짐에도 불구하고 여전히 디지털 포렌식 법제의 수준은 매우 낮은 상태라고 할 수 있다. 국가 디지털 포렌식 법률 체제에 비추어볼 때, 국내에는 민·형사소송법에서 디지털 증거 개념 자체도 명확하게 나와 있지 않고 디지털 증거의 법적 증거로서의 유효성에 대한 명확한 법적 근거와 같은 기본적인 법제조차 제대로 마련되지 못한 상황으로 민간부분에서의 디지털 포렌식 이용을 활성화시킬 수 있는 E-Discovery와 같은 제도 또한 존재하지 않는 상황이므로 디지털 포렌식 기술은 정보·수사기관의 이용으로 편향되어 있어 디지털 포렌식 서비스 및 기술개발 산업 발전은 활성화되고 있지 못하다고 할 수 있다.

Ⅴ. 디지털 포렌식 수행 절차에 따른 디지털 포렌식 법제 요구사항

국가 디지털 포렌식 법제 체계는 디지털 포렌식 기술의 적법한 활용과 디지털 수사에서의 효과성을 보장하고 디지털 포렌식 솔루션의 활성화를 목표로 한다. 디지털 포렌식 수행을 위한 법적 수단의 종류는 디지털 포렌식 수행 절차에 따라 구분된 기술들에 대해서 어떻게 법률적 정당성 확보와 지원 및 적절한 규제를 제공하는지에 따라 구분해 볼 수 있다. 본 장에서는 디지털 포렌식 수행 절차 흐름에 따라 각각의 시점에 국가 디지털

포렌식 법률체계상의 어떠한 디지털 포렌식 법원칙이 적용되는지 살펴보겠다.

디지털 포렌식 수행 절차는 데이터 수집 요구 및 준비 단계, 데이터 수집 단계, 데이터 분석 단계, 리포팅 단계, 증거 검증 및 인증 단계 그리고 디지털 포렌식 기술 및 인력 재생산 단계로 구성된다. 일반적인 디지털 포렌식 수행 절차별 분류에 데이터 수집 요구 및 준비단계와 디지털 포렌식 기술 및 인력 재생산 단계를 추가한 이유는 디지털 포렌식 기술 부분과 달리 정책 부분은 실제 디지털 포렌식 기술을 이용한 디지털 수집 및 분석 단계뿐만 아니라, 특정 법적 근거 하에 특정 목적을 위해 디지털 증거 수집을 요구하는 단계와 증거 수집을 위한 영장의 종류 등을 포함하여 어떠한 방식으로 적법하게 디지털 포렌식을 수행할 수 있을 것인지를 결정하는 준비 단계, 그리고 하루가 다르게 발전하는 디지털 범죄에 대항하여 어떻게 하면 디지털 포렌식을 안전하게 지속적으로 수행할 수 있을지에 대한 기술 및 수행 인력의 재생산 문제까지도 포괄해야 하기 때문이다.

아래의 디지털 포렌식 법제 분류표는 앞서 살펴본 포렌식 기술 분류표 항목들을 모두 포괄하고 있으며, 해당 디지털 포렌식 기술 분류에서 필요한 디지털 포렌식 법제가 무엇이고, 현재 이러한 기술들을 수행하는데 필요한 법제가 무엇인지, 향후 개발될 기술에서 요구되는 새로운 법제에 어떤 것들이 있는지를 용이하게 살펴볼 수 있다. 데이터 포렌식 수행 절차에 따른 포렌식 법제 요구사항들을 분류해보면 아래 [표 1]과 같다.

대부분의 각 법제 요구사항 및 세부 내용은 앞서 국가 디지털 포렌식 법률체계 부분에서 설명한 바와 같다. 본 분류에서 국가 디지털 포렌식 법률체계의 항목들을 제외하고 새롭게 추가된 내용은 수집단계에 새로운 통신 기술 및 새로운 디지털 미디어의 데이터 수집에 관한 법조항 마련과 새로운 디지털 포렌식 기술 방법에 대한 적법한 데이터 수집 원칙 및 절차 규정을 마련하는 것이다. 이 새로운 항목들에 대해 요구되는 구체적인 법 요구사항을 들자면, 첫 번째 항목에 대해서는 실시간 네트워크 데이터 수집 분석 항목에서 VoIP와 같은 새로운 통신 매체의 데이터 수집에 관한 법조항 마련을 들 수 있으며, 두 번째 항목에 대해서는 최근 새로운 디지털 포렌식 기술로 관심이 높아지고 있는 원격 포렌식(Remote Forensics)에서 프라이버시권과 균형을 이룰 수 있는 원격 포렌식 적법 절차를 포함한 관련 법제

〔표 1〕. 데이터 포렌식 수행 절차에 따른 디지털 포렌식 법제 요구사항 분류

절 차	디지털 포렌식 법제 요구사항
데이터 수집 요구 및 준비 단계	· 관련 법제에서 디지털증거 개념 수용 · 일반범죄 및 사이버범죄수사 관련 법제에 디지털 포렌식 기술 활용 요구조항 추가(형법, 정보통신망법, 정보통신기반보호법 등) · 테러대응, 첩보 관련 디지털 포렌식 기술 활용 요구조항 추가 · 민사소송법에 E-Discovery 조항 추가(민사소송법 개정) · 각종 컴플라이언스에 디지털 포렌식 기술 활용 요구조항 추가(GLBA, HIPAA 등) · 디지털회계감사에서 디지털 포렌식, 포렌식 어카운팅 기술 활용 요구조항 추가(SOX, 외감법) · 사이버보험 등 보험사기방지를 위한 법제에 디지털 포렌식 기술 활용 요구조항 추가(보험업법 개정) · 산업기밀보호를 위한 법제에 디지털 포렌식 기술 활용 요구조항 추가(산업기술유출방지법)
데이터 수집 단계	· 디스크 이미지 증거의 인증 및 검증 과정에 대한 표준화된 절차 마련(디지털증거처리표준 작성) · 디스크 이미지 증거에 대한 인증 목적의 인증서 기반 전자서명 활용 명시(전자서명법 개정 필요) · 휘발성 메모리에 일시적으로 저장되어 있는 데이터의 법적 증거로서의 허용성을 확보하기 위한 기준 및 표준화된 절차 마련(형사소송법 개정 및 디지털증거처리표준 작성) · 네트워크 포렌식에 대한 표준화된 절차 마련(디지털증거처리표준 작성) · 효과적 디지털 통신 데이터 증거 확보를 위한 통신감청법안 마련(통신비밀보호법 개정) - 디지털 통신 감청 포함 - 디지털 통신 관련 수집대상을 통신내용(실시간/저장된 컨텐츠), 통신확인사실, 사용자정보 등으로 세분화 · 효과적인 디지털 통신 데이터 증거 확보를 위한 ISP의 통신감청 지원을 의무화하는 법안 마련(통신비밀보호법 개정) - 디지털 통신 감청 지원 의무화조항 포함 · 관련 법제에서 디지털 증거 개념 수용(민사소송법, 형사소송법 등) · 헌법 관련 조항을 준수해야 하며 및 프라이버시법제와 모순되어서는 안 됨 · 전자서명법에 디지털 증거 인증 목적의 전자서명 활용을 명시하고, 증거인증기관 설립, 운영을 위한 법적 기반 제공(전자서명법 개정 필요)

	·통신 신기술 및 새로운 디지털 미디어의 데이터 수집에 관한 법조항 마련 - VoIP 등 새로운 통신 매체의 데이터 수집에 관한 법조항 마련 ·새로운 디지털 포렌식 기술 및 방법에 대한 적법한 데이터 수집 원칙 및 절차 마련 - 프라이버시권과 균형을 이룰 수 있는 원격 포렌식 적법 절차를 포함한 관련 법제 마련
데이터 분석 단계	·헌법 관련조항을 준수해야 하며 프라이버시법제와 모순되어서는 안됨 ·디지털 수사절차와 형사소송법, 디지털증거처리 가이드라인 준수 ·암호화된 증거의 복호화를 강제하거나 복호화 키 제공을 용이하게 할 수 있는 법적 장치의 마련 (영국 RIPA Part III 검토 및 관련 법제정) ·안티 포렌식 기술의 역기능 방지 법안 마련 - 범죄 목적의 안티 포렌식 기술 이용에 대한 가중처벌 조항 마련
리포팅 단계	·디지털 증거 분석 결과 리포팅에 대한 표준화된 절차 마련(디지털증거처리표준 작성)
증거 인증 단계	·디지털 증거의 인증 및 검증 과정에 대한 표준화된 절차 마련(디지털증거처리표준 작성) ·전자서명법에 디지털 증거 인증 목적의 전자서명 활용을 명시하고, 증거인증기관 설립, 운영을 위한 법적 기반 제공(전자서명법 개정 필요)
기술 /인력 재생산 단계	·디지털 포렌식 연구, 산업진흥을 위한 법안 마련 - 디지털 포렌식 기술 연구 지원 조항 마련 - 디지털 포렌식 연구센터 및 디지털증거분석센터 법적 근거 제공 - 디지털 포렌식 민간산업 진흥법안 마련 - 디지털 포렌식 교육 의무화 및 인력 양성 지원 조항 마련 ·디지털 포렌식 기술의 역기능 방지 법안 마련 - 디지털 포렌식 기술을 이용한 프라이버시 침해 방지를 위한 조항 마련

마련 등을 들 수 있다.

각각의 디지털 포렌식 수행 단계별 정보활동을 수행하기 위해서는 위의 표에 나오는 적절한 법적 수단을 효과적으로 활용할 수 있어야 하며, 이를 위해서 각 단계별, 각 수집 데이터 특성별 디지털 포렌식 법적 요구사항들을 만족시키기 위한 법제정 및 개정 노력이 요구된다.

Ⅵ. 국내 디지털 포렌식 법률 체계 수립 방향

국가 디지털 포렌식 법률 체계상의 각 법제들을 법제들의 중요도와 긴급성에 따라 분류해보면 [표 2]와 같다. 중요도는 디지털 증거 수집, 분석 절차에서 차지하는 위치와 필수적인지 여부, 다른 법률에 미치는 영향력, 그리고 전체 사회와 디지털 포렌식 산업에서 차지하

〔표 2〕. 중요도와 긴급성에 따른 국가 디지털 포렌식 법제 분류

중요성 / 긴급성	상	중	하
상	② 개인정보보호 기본법 마련 ③ 디지털증거 개념수용 (민사, 형사소송법) ④ 디지털증거 허용성 ⑤ 디지털증거 처리 표준 확립 (디지털증거처리가이드라인) ⑦ 디지털수사 절차 확립 (형사소송법)	⑥ 전자서명법 개정 (디지털 증거 허용성 및 인증센터 설치·운영)	
중	⑧ 디지털통신 감청 (통신비밀보호법 개정) ⑩ 범죄수사, 테러대응, 첩보 관련 디지털 포렌식 기술 활용 요구 조항 ⑪ 디지털통신 감청 지원 (통신비밀보호법 개정)	⑫ E-Discovery 제도화 (민사소송법) ⑬ 각종 컴플라이언스에 디지털 포렌식 기술 활용 요구 조항 ⑭ 산업기밀보호법에 디지털 포렌식 기술 활용 요구 조항 ⑮ 회계감사관련 법안에 디지털 포렌식 기술 활용 요구 조항 (외감법 등 반영) ⑯ 사이버보험 사기방지 관련 법안에 디지털 포렌식 기술 활용 요구 조항 (보험업법 등 개정)	
하		⑰ 디지털 포렌식 / 안티 포렌식 기술 역기능 방지 ⑱ 디지털 포렌식 기술 연구 산업 진흥	

는 비중 등을 기준으로 분류하였으며, 신속성은 해당 법제수립의 지연으로 인해 디지털 포렌식 및 디지털 수사에 미칠 파급력과 다른 법제와의 연관성 등에 의한 법제 제·개정의 용이성 정도 등을 기준으로 분류하였다.

이러한 두 가지 기준을 기반으로 국가 디지털 포렌식 법제들을 분류해보면 먼저 디지털 수사를 통해 수집, 분석된 디지털 증거가 법적 증거로 인정될 수 있도록 보장해주는 법제들이 가장 높은 중요성과 긴급성을 가지고 있음을 알 수 있고, 개인정보보호기본법 또한 디지털수사와 디지털 포렌식으로 인한 프라이버시 침해를 최소화하면서 개인정보보호와 수사권의 균형을 유지하기 위한 필수적인 환경이 된다는 점에서 중요성은 중간인 반면 긴급성이 높다고 할 수 있다. 디지털 증거의 허용성을 보장해주는 기술적 조치로서의 전자서명을 효과적으로 활용할 수 있게 해주는 전자서명법 개정은 중간 정도의 중요성을 가진 반면 신속하게 개정되어 조금이라도 빨리 디지털 증거의 허용성 실패로 인한 피해를 줄일 수 있는 신뢰성 높은 사회적 시스템을 만드는 것이 중요하므로 높은 긴급성을 요하는 것으로 분류하였다. 정보·수사기관의 디지털 통신 감청 및 디지털 수사의 경우 국가안보 및 범죄억제라는 공공의 이익을 위한 수사권 확보를 위해 중요한 반면 프라이버시 침해 등을 막기 위해 개인정보보호 기본법 마련이 선행될 것을 요구한다는 점에서 긴급성을 중으로 두었다. 또한 E-Discovery, 컴플라이언스, 산업기밀보호법, 회계감사관련, 보험사기대응관련 법안 등 민간에서의 포렌식 기술 활용할 수 있는 분야와 관련된 법제의 경우 중요도와 긴급성을 중간 정도로 두었다. 마지막으로 디지털 포렌식/안티 포렌식 기술 역기능 방지의 경우 디지털 포렌식의 적법한 사용을 위한 기본 환경을 제공함으로써 디지털 포렌식 기술에 대한 신뢰성을 제공하는 것과 디지털 포렌식 산업 진흥 법제는 중간 정도의 중요도를 가지고 있지만 디지털 포렌식 기술과 디지털 수사의 실제 수행에 있어서 긴급도는 낮은 것으로 분류된다.

국가 디지털 포렌식 법률체계에서 각 법률들의 제·개정 추진 단계는 다음과 같이 구분된다. 각 단계별 법적 정책과제를 도출하기 위해서 위의 표에서 살펴본 특정 법 목적의 중요성과 긴급성을 함께 고려한 결과, 단기적인 정책과제는 중요성이 중, 상이고 긴급성이 상 이상으로 높은 법 정책 과제들을, 중기적 정책과제는 중요성이 중, 상이고 긴급성이 중으로 높은 법 정책 과제들을, 마지막으로 장기적인 정책과제는 중요성과 상관없이 긴급성이 낮은 과제들로 구분해보았다.

국가차원의 효과적이고 적법한 디지털 포렌식 환경의 구축과 활성화를 위해서는 국가 디지털 포렌식 법제도 정책 추진과제를 수립함에 있어 그 법 목적의 중요성과 긴급성에 따라 단기, 중기, 장기과제로 구분하여 지속적으로 법제도 제·개정 작업을 수행해야 한다. 이를 위해 우선적으로 민·형사소송법을 포함한 관련 법률에 디지털 증거 개념을 명확하게 규정하는 작업과 디지털 증거의 법적 허용성을 확보하기 위한 법적 조건의 마련과 디지털 증거표준 및 디지털 수사절차의 확립과 같은 표준 가이드라인의 마련, 그리고 전자서명

〔표 3〕. 국가 디지털 포렌식 법제도 정책 과제

구 분	단 기	중 기	장 기
국가 디지털 포렌식 법제 과제	② 개인정보보호 기본법 마련 ③ 디지털증거개념수용 (형사소송법, 통신비밀보호법) ④ 디지털증거 허용성 확보 ⑤ 디지털증거처리 표준 확립 (디지털증거처리가이드라인) ⑥ 전자서명법 개정 (디지털 증거 허용성 및 인증센터 추가) ⑦ 디지털수사절차 확립 (형사소송법)	⑧ 디지털통신감청 (통신비밀보호법 개정) ⑨ 암호화증거처리 ⑩ 범죄수사, 테러대응, 첩보 관련 디지털 포렌식 기술 요구 ⑪ 디지털통신감청 지원 (통신비밀보호법 개정) ⑫ E-Discovery 제도화 (민사소송법) ⑬ 각종 컴플라이언스에 디지털 포렌식 기술 요구 ⑭ 산업기밀보호법에 디지털 포렌식 기술 요구 반영 ⑮ 회계감사 관련 법안에 디지털 포렌식 기술 요구 (외감법 등 반영) ⑯ 사이버보험 사기방지 (보험업법 등 개정)	⑰ 디지털 포렌식/안티 포렌식 기술 역기능 방지 ⑱ 디지털 포렌식 기술 연구·산업 진흥

을 디지털증거의 법적 허용성을 획득하는 효과적인 도구로 활용하기 위한 법제의 마련 및 디지털 포렌식 과정에서 발생할 수 있는 개인의 프라이버시 침해를 효과적으로 예방할 수 있는 민간기관 및 공공기관의 단일화된 개인정보보호 기본법의 마련 등을 단기과제로 생각해볼 수 있을 것이다. 또한 중기 과제로는 민간기업과 정보수사기관에서 컴플라이언스 준수, 포렌식 어카운팅, 산업기밀 보호, 범죄수사, 테러대응 및 첩보의 목적으로 디지털 포렌식의 활용을 장려하고 촉진하기 위한 관련 법안 개정 등이 수행되어야 하며, 마지막 장기적 과제로는 디지털 포렌식 기술의 역기능 방지 및 디지털 기술 연구 및 산업진흥 법안이 추진되어야 한다.

각 국가들은 이러한 국가 디지털 포렌식 법제도 정책 추진표에서 부족한 법제들에 대한 제·개정 작업을 단기, 중기, 장기과제로 정하고 추진해나가야 한다. 국내의 경우 대부분의 법제 현황이 미진한 상황이므로 위의 [표 3]에 나온 추진단계 순으로 부족한 법제 제·개정을 추진해나가는 것이 바람직할 것이다.

Ⅶ. 결 론

본고에서는 국가차원의 적법한 디지털 증거 활용 및 효과적인 디지털 포렌식 기술의 이용과 활성화를 위한 국가 디지털 포렌식 법률 체계를 제시하고 디지털 포렌식 수행 절차별 법률 요구사항을 살펴봄으로써 국내의 디지털 포렌식 관련 법제 현황에 대해 점검해보았다. 그 결과 국내 디지털 포렌식 관련 법제 수준은 국가 디지털 포렌식 법률 체계의 대부분의 법 목적과 절차상의 법적 요구사항을 만족시키고 있지 못함을 알 수 있었다. 따라서 국내에서는 디지털 증거 인증을 통한 법질서 확립 및 정의구현과 디지털 포렌식 기술 활성화를 위해 우선적으로 관련 법안에서의 디지털 증거 개념 수용과 디지털 증거 수집 및 분석 절차 작성을 포함하여 디지털 증거의 법적 유효성을 인정받을 수 있기 위한 기본적인 법제의 정비와 함께, 수사·정보기관 및 민간기업의 디지털 포렌식 이용을 활성화시킬 수 있는 법 환경의 조성 및 디지털 포렌식 연구, 공공·민간 포렌식 시장의 균형 있는 발전을 도모하기 위한 디지털 포렌식 산업 진흥을 위한 법제 마련을 위한 노력을 단, 중, 장기적 과제로 삼아 지속적이고 체계적으로 진행해야 할 것이다.

참고문헌

[1] 탁희성, "법정에서 디지털 증거의 허용가능성", 디지털포렌식연구 Nov. 2007

[2] 김정옥, "디지털증거의 증거능력 인정 요건 - 일심회 판결을 중심으로", 디지털포렌식연구 Nov. 2007

[3] 양근원, "형사절차상 디지털 증거의 수집과 증거능력에 관한 연구", 경희대학교 대학원 박사학위논문, Feb. 2006

[4] 김형성 외, "Computer Forensics의 법적 문제", 성균관법학 제18권 제3호, Dec. 2006

[5] 원혜욱, "전자증거의 압수 수색", 한국비교형사법학회 2003년도 하계국제학술대회 자료집 Aug. 2005.

[7] Daniel J. Ryan, "Legal Aspects of Digital Forensics"

[8] Andreas Mitrakas, "Law, Cybercrime and Digital Forensics: Trailing Digital Suspect", 2006

[9] 경찰청, 디지털증거처리표준가이드라인, Nov. 2006

〈著者紹介〉

백 승 조 (Seungjo Baek)
학생회원
2005년 2월 : 세종사이버대학교 정보보호학과 졸업
2007년 9월 : 고려대학교 정보경영공학전문대학원 석사 학위 취득
2007년 10월~현재 : 고려대학교 정보경영공학전문대학원 박사 과정
관심분야 : 정보법학, 개인정보보호, 지적재산권, 위험관리

심 미 나 (Mina Shim)
학생회원
1996년 2월 : 성신여자대학교 전산학과 졸업
2006년 2월 : 고려대학교 정보보호대학원 석사 학위 취득
2008년 2월 : 고려대학교 정보경영공학대학원 정보보호전공 박사 수료
관심분야 : 개인정보보호, 정보보호영향평가제도, 의료정보보호, 위험분석방법론, 정보보호법제

임 종 인 (Jongin Lim)
정회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사 학위 취득
1986년 2월 : 고려대학교 수학과 박사 학위 취득
현재 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장이며, 정부혁신지방분권위원회, 대통령 자문 전자정부 특별위원회, 법무부 형사사법 통합정보체계 추진단 자문위원 등
관심분야 : 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안