Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1153

디지털 포렌식 수준 평가 지표 개발에 관한 연구*

박 희 일,† 윤 종 성, 이 상 진‡
고려대학교 정보보호대학원

A Study on Development of Digital Forensic Capability Evaluation Indices*

Hee-il Park,† Jong-seong Yoon, Sang-jin Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

정보통신기술의 급속한 발달로 정보의 디지털화가 가속화되면서 범죄수사뿐만 아니라 기업 및 개인 분쟁에 이르기까지 디지털 포렌식의 활용이 증대되고 있으나 디지털 증거가 갖는 위·변조의 용이성으로 인해 가치를 제대로 인정받지 못하고 있다. 특히, 국내에서는 디지털 포렌식 수행 조직의 수준에 대한 객관적인 검증 제도나 평가 방법이 부재하여 이에 대한 신뢰성 판단을 법관의 심증에 의존하고 있는 실정이다. 따라서 본 연구에서는 국내외 디지털 포렌식과 정보보호 분야의 수준 평가 방법 및 기준을 검토하여 디지털 포렌식 조직, 인원, 기술, 시설 그리고 국내 사법기관에서 적용하고 있는 수행 절차를 중심으로 국내 실정에 적합한 디지털 포렌식 수준 평가 모델 및 지표를 개발하였다. 이를 통해 디지털 증거의 신뢰성에 관한 사법기관의 판단 기준과 디지털 포렌식 조직의 구성·운영·평가를 위한 기준이 마련될 수 있을 것이다.

ABSTRACT

With the acceleration of information digitization caused by fast growth of Information Technology, the application of digital forensics has increased but it is underestimated because digital evidence is easy to forge. Especially, the evaluation of the reliability of digital forensics organization is judged only by judges domestically because there is no objective verification system or evaluation method of the capability of digital forensics organization. Therefore, the evaluation model and indices of the capability of digital forensics concentrated on the digital forensics organization, personnel, technology, facilities and the procedure in domestic justice system was presented in this research after reviewing the domestic and foreign evaluation method and the standard of the capability of digital forensics and information security. The standard for judicial evaluation of digital evidence and composition, management, evaluation of digital forensics organization would be presented based on this research.

Keywords: Digital Forensics, Digital Forensic Capability Evaluation, Capability Evaluation Indices

I. 서 론

최근 정보통신기술의 급속한 발달에 따라 개인, 기업, 정부기관에 이르기까지 IT 서비스와 디지털 기기의 활용이 증대되면서 대부분의 사회 활동 정보가 디지털 형태로 기록되고 있다. 이에 따라 범죄 행위의 입증, 정부기관 및 기업의 각종 감사나 조사 등 다양한 분야에서 디지털 정보를 수집, 분석하는 디지

접수일(2015년 7월 13일), 수정일(2015년 8월 12일), 게재 확정일(2015년 8월 27일)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, phi0105@gmail.com
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

털 포렌식 기술이 널리 활용되고 있다. 특히, 사이버 범죄뿐만 아니라 살인, 폭행 등 전통적인 일반 범죄와 관련된 수사 및 재판에서도 범행 동기와 계획, 범행 사실 등의 입증을 위해 디지털 기기에 보관된 정보가 적극 활용되고 있으며, 재산 문제・명예훼손 등 개인 간 분쟁해결에서도 디지털 증거가 중요한 단서가 되고 있다. 또한, 정부기관 및 기업 등에서도 첨단기술 유출 차단을 위한 보안 점검 및 직원 감사 등에 디지털 증거를 적극 활용하면서 이를 뒷받침하는 디지털 포렌식 기술이 더욱 중요하게 되었다.

디지털 증거의 활용이 광범위해지고 디지털 포렌식의 중요성이 부각되었지만, 일반 물리적인 증거와 달리 디지털 증거의 위・변조 및 훼손이 용이한 특성으로 인해 그 신뢰성에 논란이 제기되며 법정에서 디지털 증거의 증거능력이나 증명력은 본래의 가치만큼 인정되지 못하고 있는 실정이다. 이를 극복하고 디지털 증거의 실질적인 가치를 인정받기 위해서는 신뢰성 있는 디지털 증거의 수집 및 처리가 보장되어야 한다.

디지털 증거의 신뢰성은 증거 자체만으로 증명되는 것이 아니라 디지털 증거를 취급하는 인원의 전문성, 신뢰할 수 있는 디지털 포렌식 도구의 사용 여부, 디지털 증거 분석실의 신뢰성 그리고 디지털 증거의 수집에서 법정 제출에 이르기까지의 무결성과 관리의 연속성(Chain of Custody)이 보장되었는지에 대한 검증을 통해 간접적으로 증명된다.

이를 위해 국제적으로는 시험기관 또는 교정기관의 능력에 관한 국제표준인 ISO/IEC 17025에 의거 디지털 포렌식 분석실에 대한 인증을 시행하고 있으나 화학 실험 등 일반 시험・교정기관에 대한 인증을 중심으로 설계되어 디지털 포렌식에 적절치 못하다. 미국의 경우 ISO/IEC 17025에 기초하여 ASCLD/LAB(American Society of Crime Laboratory Directors/Laboratory Accreditation Board)에서 포렌식 실험실에 대한 인증을 수행하고 있으나 미국의 법체계 등을 중심으로 설계되어 미국 외 국가 실정이 고려되지 않았으며, 인증에 많은 비용과 시간이 소요된다. 우리나라는 한국인정기구(KOLAS, Korea Laboratory Accreditation Scheme)에서 ISO/IEC 17025에 의거 인증을 하고 있으나 화학, 전기 등 일반적인 시험・교정기관을 대상으로 하며, 법과학 시험기관은 지문・필적 등 전통적인 법과학 분야로 국한되어 있다.

디지털 포렌식과 직・간접적으로 관련된 정보보호 분야의 경우 ISO/IEC 27001, 정보보호관리체계(ISMS)와 같은 인증, 평가방법이 제도화 되어 정착되고 있는 반면, 국내 환경에 적합한 디지털 포렌식에 관한 검증 제도나 수준 평가 방법 및 기준에 대한 연구 및 적용은 부족한 실정이다.

이에 본 연구에서는 디지털 포렌식 수준 평가에 관한 기존 제도 및 최근 연구 동향을 살펴보고, 정보보호 분야의 수준 평가 방법 및 기준, 최근 연구 동향 등을 검토하여 국내 실정에 적합한 디지털 포렌식 수준 평가 모델과 지표를 제시하고자 한다. 이를 통해 디지털 증거의 신뢰성에 대한 사법기관의 판단 기준과 정부기관・기업 등에서 디지털 포렌식 조직의 구성・운영・평가를 위한 객관적인 지표가 마련될 수 있을 것이다.

II. 관련 연구

2.1 디지털 포렌식 수준 평가

2.1.1 ISO/IEC 17025

ISO/IEC 17025는 ISO 9001을 기초로 국제표준화기구에 의해 제정된 시험기관 또는 교정기관의 능력에 관한 일반 요구사항의 국제 표준이자 인증 기준으로써 안전하고 신뢰성 있는 측정 장비를 가지고 있다는 전제 하에 해당 시험기관 또는 교정기관의 자격을 인증해 준다. 적용범위는 조직, 경영시스템 등에 관련된 경영 요구사항과 직원, 시설 및 환경조건 등에 관한 기술 요구사항으로 구분되어 있다[1].

2.1.2 ASCLD/LAB

ASCLD/LAB은 공공 및 민간 범죄 연구실의 인증을 전문으로 하는 기관으로, 1982년부터 미국 전역의 연방, 주, 지방의 범죄 연구실뿐만 아니라 타국의 포렌식 연구실에 대해 인증하고 있다. 이 기관에서는 ISO/IEC 17025를 기초로 자체적인 추가 요구사항을 반영한 인증 기준을 마련하여 포렌식 시험분야와 호흡 알콜 교정에 관한 범죄 연구실 인증을 제공하고 있다. 평가는 연구실 경영과 운영, 개인별 자격, 물리적 설비 분야 등으로 구성된다[2].

2.1.3 한국인정기구

한국인정기구는 국가표준제도 확립 및 산업표준화 제도 운영 등을 목적으로 1992년 3월 30일 한국교정시험기관 인정기구로 설립되었으며, 2007년 4월 한국인정기구로 개칭되었다. 국제표준화기구가 정한 국제표준인 ISO/IEC 17025에 따라 교정·시험기관 등 인정 등의 업무를 수행하며, 표준화 관련 각종 국제협력 및 교류를 통해 아시아태평양 시험기관 인정 협력체(APLAC, Asia-Pacific Laboratory Accreditation Cooperation)와 국제 시험기관 인정 협력체(ILAC, International Laboratory Accreditation Cooperation)와 상호인정협정(MRA, Mutual Recognition Arrangement)을 체결하였다. 주요 공인 시험분야는 화학, 역학, 전기, 열, 음향 및 진동 등 일반적인 시험·교정기관을 대상으로 인증을 하고 있다[3]. 법과학 분야도 포함되나 혈중 알콜농도, 필적 및 공구흔 검사 등 전통적인 법과학 측면에 한정되어 디지털 포렌식 측면에서의 적용은 어려움이 있다.

2.1.4 최근 연구 동향

Ebrahim Hamad Al-Hanaei 등[4]은 현재 디지털 포렌식의 인증 기준인 ISO/ICE 17025와 미국의 ASCLD/LAB의 국제 요구사항은 화학 실험과 같은 일반적인 시험·교정기관을 위해 설계된 표준으로 전통적인 법과학 수사에 적용할 수 있으나 디지털 포렌식 분석실에 특화되어 있지 못함을 거론하며 비즈니스와 법적 요구사항을 충족하기 위한 디지털 포렌식 조직의 능력 성숙도 모델(DF-C^2M^2)을 제시하였다. 해당 모델은 디지털 포렌식 연구실의 역량 성숙도를 6단계로 정의하고 있으며, 절차, 조직, 인력, 도구 및 방법의 측면에서 성숙도를 평가한다. 하지만 평가 요소별 구체적인 평가 방법이나 지표를 제시하지 않고 있다.

2.2 정보보호 수준 평가

2.2.1 ISO/IEC 27001

ISO/IEC 27001은 영국 표준(BS, British Standard)인 BS7799를 기반으로 2005년 11월 국제표준화기구(ISO, International Organization for Standardization)와 국제전기기술위원회(IEC, International Electrotechnical Commission)의 표준으로 제정되었다. 이후, 2013년 7월 최종 국제 규격안(FDIS, Final Draft Internal Standard)의 통과로 개정되어 정보보호관리체계(ISMS, Information Security Management System) 인증에 적용되고 있는 대표적인 국제 표준이자 국제 인증이다. 적용범위는 정보보호정책, 통신·운영 등 정보보호 관리 14개 영역, 114개 항목으로 구성되어 있으며, PDCA(Plan-Do-Check - Act) 관리모델에 따라 정보보호관리체계를 구축, 실행, 유지 및 개선토록 요구하고 있다[5].

2.2.2 K-ISMS

K-ISMS는 2001년 7월 '정보통신망이용촉진및정보보호등에관한법률(이하 정보통신망법)'에 따라 한국인터넷진흥원에서 국내 기업의 실정을 반영하여 개발한 국내 정보보호관리체계 인증 제도로써, 2012년 2월에 개정된 정보통신망법에 의거 2013년 2월부터는 정보보호 안전진단 제도를 폐지하고 주요 정보통신서비스 제공자를 정보보호관리체계 인증 의무대상자로 지정하여 운영하고 있다. 추진체계는 미래창조과학부, 단일 인증기관인 한국인터넷진흥원, 인증위원회, 인증심사원으로 이루어지며, 인증 기준은 정보보호 관리과정(5단계) 12개 통제항목, 정보보호대책(13개 분야) 92개 통제항목으로 구성되어 각각의 통제항목에 해당되는 세부점검항목에 대해 평가를 받는다[6].

2.2.3 최근 연구 동향

최재규 등[7]은 클라우드 컴퓨팅 환경 성장에 따라 발생 가능한 보안 문제 해결을 위해 사용자 입장에서 클라우드 컴퓨팅 보안 평가 요소를 제시하였고, 허옥 등[8]은 한국형 스마트 그리드의 정보보호 관리체계 평가와 관련하여 가용성을 중심으로 한 국제표준을 비교·분석하여 새로운 평가항목을 제시하였다.

III. 디지털 포렌식 수준 평가 지표의 필요성

디지털 포렌식이란 디지털 기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 규명하고 증명하는 분야로서, 디지털화된 흔적이나 증거를 수집하여 분

석하고 보관하는 응용과학 분야를 의미한다. 또한, 국제 디지털 포렌식 학회인 DFRWS(Digital Forensics Research Workshop)에서는 디지털 포렌식을 '범죄의 재현이나 혼란을 야기하는 인가되지 않은 행동에 대해 쉽게 예측하기 위해 디지털 출처에서 파생된 디지털 증거에 대한 보존, 수집, 확인, 식별, 분석, 해석, 기록, 현출을 과학적으로 검증된 방법을 통해 수행하는 것'으로 정의하고 있다[9].

디지털 증거는 물리적 증거와 다르게 비가시성, 변조가능성, 복제용이성, 대규모성, 휘발성, 초국경성과 같은 특징을 가지고 있어, 디지털 포렌식 수행 과정에서 증거능력이 훼손되지 않도록 주의하여야 하며 법정에서 요구하는 증거능력을 확보해야 한다. 디지털 증거가 법정에서 증거로 받아들여지기 위해서는 진정성(Authenticity), 무결성(Integrity), 원본성(Originality), 신뢰성(Reliability)이 보장되어야 한다. 디지털 증거의 증거능력 요건을 간략히 살펴보면 다음과 같다[10].

- 진정성(Authenticity)은 해당 디지털 증거가 수집·저장 과정에서 오류가 없었으며, 의도된 결과가 정확하고, 그로 인해 생성된 자료임이 인정됨을 의미한다. 이를 보증하기 위해서는 최초 디지털 증거의 수집부터 법정 제출 시까지 확실한 인수인계를 통해 변경이나 훼손이 없도록 절차의 연속성이 유지되어야 한다.

- 무결성(Integrity)은 디지털 증거가 원본에서 수집되어 보관, 분석되는 과정에서 부당하게 수정, 변경, 손상되지 않도록 유지되어야 하고, 이를 검증할 수 있어야 함을 말한다.

- 원본성(Originality)은 자체적인 가시성, 가독성이 없는 디지털 증거를 가시성 있게 변환하여 법원에 제출함에 있어서 제출된 증거가 원본 매체에 있는 데이터와 동일함을 의미한다.

- 신뢰성(Reliability)은 증거 데이터의 분석 등 처리과정에서 증거가 위·변조되거나 의도되지 않은 오류를 포함하지 않았음을 의미하며, 디지털 증거 자체의 특성이 아니라 이를 취급하는 절차, 인력, 도구, 시설 등의 신뢰성 증명을 통해 간접적으로 증명한다.

국내에서는 디지털 증거의 증거능력에 대한 판단이 법관에 의해 이루어지며, 전문적인 기술적 요소로 인해 판단이 어려울 경우 전문가 진술에 의존하기도 한다. 따라서 디지털 포렌식을 수행하는 조직과 제반 요소, 수행절차 등을 평가할 수 있는 객관적인 방법과 지표에 대한 연구와 개발이 필요한 실정이다.

디지털 포렌식 수행 조직에 대한 객관적인 수준 평가 방법 및 결과는 법정에서 뿐만 아니라 정부, 기업 내의 감사를 위한 포렌식 조직의 역량을 측정하기 위해 활용될 수 있으며, 산업적인 측면에서는 디지털 증거를 분석, 감정, 처리하는 법무법인, 회계법인, 컨설팅 업체 등에 대한 객관적인 평가를 통해 고객들에게 신뢰할 수 있는 정보를 제공함으로써 디지털 포렌식 분야 산업 발전에도 기여할 수 있다.

IV. 연구 방법

디지털 포렌식 수준 평가 지표 개발을 위해 Fig. 1.과 같이 '자료 수집·검토, 모델 수립, 평가 지표 개발, 평가 지표 검토·개선'의 절차를 수행하였다.

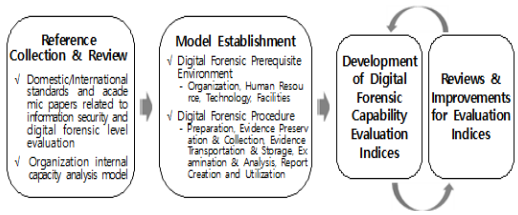

Fig. 1. Development Process of Digital Forensic Capability Evaluation Indices

4.1 자료 수집 및 검토

본 연구의 2장에서 살펴본 바와 같이 디지털 포렌식 수준 평가 모델 및 지표 개발을 위해 현재 시행중인 수준 평가 체계에 관한 자료를 수집, 검토하였다. 먼저, 현재 국내외에서 디지털 포렌식 조직이나 분석실 인증에 관하여 적용하고 있는 표준, 지침과 연구논문 등을 수집, 검토하였다. 다음으로 가장 체계적으로 시행되고 있는 기업 및 조직의 정보보호 관리체계 인증 제도와 관련된 국내외 표준 및 평가지표, 연구논문 등을 수집, 검토하였다. 마지막으로 기업이나 조직의 구성요소, 경쟁우위, 구성원의 역량 등을 종합적으로 분석 및 평가하는 내부역량분석 모델을 살펴보고 디지털 포렌식 수준 평가에 적용할 수 있는지

에 대해 검토하였다.

4.2 디지털 포렌식 수준 평가 모델 수립

디지털 포렌식 수준평가를 위한 모델은 조직의 역량 분석에 활용되는 모델인 가치 사슬 모델(Value Chain Model)을 적용하여 개발하였다.

가치 사슬 모델은 기업의 부가가치 창출에 관련된 일련의 업무 활동인 '본원적 활동'과 기업 인프라, 인적자원관리, 구매조달 등의 '지원 활동'으로 구분하여 역량 및 수준을 평가한다. '본원적 활동'은 기업이 부가가치를 창출하는 업무 흐름과 연계성을 분석한다는 측면에서 관리의 연속성과 절차를 중요시하는 디지털 포렌식 업무에 대한 평가 모델로 적합하며, '지원 활동'은 디지털 포렌식 수행을 위해 갖추어야 할 제반 여건 및 기본 요구사항 평가에 적용할 수 있다.

본 연구에서 수립한 디지털 포렌식 수준 평가 모델은 Fig. 2.와 같으며, 포렌식 조직의 활동을 지원 활동에 해당하는 디지털 포렌식 제반 환경 평가와 본원적 활동에 해당하는 디지털 포렌식 수행 절차 평가로 구분된다.

디지털 포렌식 제반 환경은 조직 경영, 인적자원 관리, 기술 수준, 시설 운영을 평가하고 디지털 포렌식 수행 절차는 '사전준비, 증거 확보 및 수집, 증거 운반 및 보관, 조사 및 분석, 보고서 작성 및 활용'의 5단계 절차로 구분하여 각 단계별 수행 능력을 평가한다.

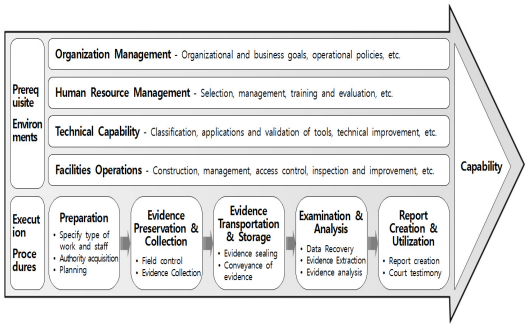

Fig. 2. Digital Forensic Capability Evaluation Model

4.3 수준 평가 지표 개발 및 개선

수준 평가 지표는 ISO17025, ASCLD/LAB, ISO27001, 정보보호관리체계, 법 집행기관의 디지털 포렌식 수행 지침 등을 참고하여 평가 모델에 따라 개발하였으며, 개발한 지표는 법 집행기관, 디지털 포렌식 관련 연구기관 및 업체 전문가들의 평가 및 검토를 통해 점증적으로 개선하고 정제하였다.

V. 디지털 포렌식 수준 평가 지표 개발

5.1 디지털 포렌식 제반 환경 평가

디지털 포렌식 제반 환경은 디지털 포렌식의 신뢰성 있는 처리를 위해 기본적으로 갖춰야 할 요소들로서 조직 경영, 인적자원 관리, 기술 수준, 시설 운영에 대해 평가한다. 평가 지표는 Table 1.과 같고, 각 지표별 세부 내용은 아래의 소절에서 설명한다.

5.1.1 조직 경영

조직 경영은 디지털 포렌식 조직의 구성 및 업무 목표·유형 등에 대한 정의, 조직 운영에 관한 지침 및 규정 제정, 운영계획의 수립 등에 관한 평가 지표로서, 세부 내용은 다음과 같다.

① 디지털 포렌식 조직 구성
디지털 포렌식 업무를 효율적이고 체계적으로 수행할 수 있도록 적절한 권한과 책임이 부여된 조직을 구성하고 필요한 자원(예산)을 확보하여야 한다.

② 범위 설정
디지털 포렌식 조직의 업무 목표 및 유형, 범위가 명확히 정의되어야 한다.

③ 경영 전략
디지털 포렌식 조직 구성 및 운영, 감사(평가), 인사, 보안, 예산 등에 관한 기준과 지침이 마련되어야 한다.

④ 디지털 포렌식 업무 수행 정책
조직이 수행하는 모든 디지털 포렌식 활동에 대한 정책(지침, 절차)과 업무수행체계를 마련하고, 해당 정책은 관련 법·제도의 요구사항을 만족하여야 한다. 특히, 디지털 증거의 무결성과 관리의 연속성을 보장하기 위한 지침은 반드시 포함되어야 한다.

Table 1. Digital Forensic Prerequisite Environments Evaluation Indices

Evaluation Areas		Evaluation Indices
Digital Forensic Prerequisite Environments	Organization Management	Digital forensics organization
		Establishing business scope
		Management strategy
		Digital forensics policy
		Authority and responsibility
		Supervision
		Security management
	Human Resource Management	Recruitment
		Personnel management system
		Qualification management
		Separation of duties
		Education and training
	Technical Capability	Target definition
		Classification of tools
		Application of tools
		Verification of tools
		Performance management
		Introduction and improvement of technology
		Response to anti-forensics
	Facilities Operations	Construction of necessary facilities
		Management of facilities
		Protective equipment
		Access control
		Assessment and improvement of facilities

⑤ 권한과 책임
디지털 포렌식 조직의 책임자와 각 구성원들의 권한과 책임이 정의되어야 하고, 그 활동을 평가할 수 있는 체계를 마련해야 한다.

⑥ 관리 감독
구성원들의 동기 부여 및 소통, 업무 지도를 위한 주요 직무자를 지정하여야 한다.

⑦ 보안 관리
디지털 포렌식 업무 수행과정에서 발생한 정보(개인정보 등) 및 자료(사건과 무관한 자료, 분석결과 등)에 대한 보안관리 지침이 마련되어야 한다.

5.1.2 인적자원 관리

인적자원 관리는 디지털 포렌식 조직의 구성원들에 대한 관리 체계, 선발지침, 교육·훈련·평가 과정 등에 관한 평가 지표로서, 세부 내용은 다음과 같다.

① 인원 선발
디지털 포렌식 조직의 업무 수행에 적합한 인원 선발지침(학력, 경력 등에 대한 평가기준 및 가중치 부여 등)이 마련되어야 한다. 선발 요건은 디지털 포렌식 관련 학위 및 자격증, 근무 경력 및 분야, 수상 경력 등을 포함하여 선정한다. 그 예는 다음과 같다.
- 관련 학위 : 전산 및 정보통신, 정보보호 분야의 학사·석사·박사학위
- 관련 자격증 : EnCE(EnCase Certified Examiner), ACE(AccessData Certified Examiner), CEH(Certified Ehical Hacker), CHFI(Computer Hacking Forensic Investigator), 디지털 포렌식 전문가 1·2급, 정보보안(산업)기사 등
- 근무 경력 및 분야 : 근무 기간 및 분야에 따른 자격 분류
- 디지털 포렌식 관련 수상 경력

② 인원 관리체계
디지털 포렌식 조직의 근무인원에 대해 직위·자격, 담당 업무, 요구 능력, 교육 및 훈련, 평가 등에 대한 종합적인 관리체계가 마련되어야 한다.

③ 자격 관리
각 구성원은 교육 및 훈련, 경험 등을 토대로 자격과 직위를 구분하고 적절한 권한과 책임이 부여되어야 한다.

④ 직무 분리
각 구성원은 운영체제, 데이터베이스, 네트워크, 모바일 등 분야(주·부 담당 지정)별 전문가로 세분화하여 직무기술서를 유지하고, 그에 맞는 임무 수행 절차를 수립하여야 한다.

⑤ 교육 및 훈련
구성원에 대한 교육 및 훈련, 평가 과정이 마련되어야 하며, 관련 기록을 문서로 유지하여야 한다. 교육 및 훈련 프로그램은 다음과 같은 내용으로 구성해야 한다.
- 교육 시기, 대상, 내용, 방법 등이 포함된 연간 교육계획
- 디지털 포렌식 관련 이론·실습, 신규 발표 또는 연구중인 내용(자체 교육 또는 디지털 포렌식 관련 외부 교육 활용)
- 적법절차, 법정 증언 시 준수사항, 보안 지침 및 윤리의식 등 교육
- 전문지식에 대한 정기평가 및 재교육, 재평가 시행

5.1.3 기술 수준

기술 수준은 디지털 포렌식에 필요한 소프트웨어(도구, 프로그램 등) 및 하드웨어(장비) 등에 관한 기술적인 준비 수준을 평가하는 지표로서, 세부 내용은 다음과 같다.

① 적용 대상 정의
디지털 기기와 디지털 데이터의 종류, 유형이 구체적으로 분류 및 정의되어야 한다.

② 도구 분류
디지털 포렌식 수행 과정에 따라 사용되는 소프트웨어 및 하드웨어를 사용 목적 및 기능에 따라 적절하게 분류하여야 한다. 분류기준은 다음과 같다.
- 활성 데이터 수집 도구 : 물리 메모리, 네트워크 등 휘발성 데이터와 파일시스템 메타데이터, 운영체제별 아티팩트(레지스트리 하이브, 프리패치, 이벤트로그, 바로가기 파일 등) 등 비휘발성 데이터 수집
- 비활성 데이터 수집 도구 : 저장장치 복제/이미징 도구, 쓰기방지 장치 등
- 데이터 운반 및 보관 : 대용량 저장장치, 전자파 차단 장비, 충격 완화용 보호 박스 등
- 데이터 분석 도구 : 데이터 복구 도구, 통합 분석, 파일 시스템 분석, 운영체제별 아티팩트 분석 도구 등
- 데이터 파기를 위한 도구

③ 도구 적용
각종 포렌식 도구의 기술 및 한계 등에 관한 운영 지침 및 절차가 마련되어야 한다.

④ 도구 검증
디지털 증거 처리에 사용되는 도구의 신뢰성에 대한 검증이 이루어져야 한다. 특히, 분석 도구에 대한 신뢰성 검증은 더욱 중요하다. 각종 도구의 신뢰성 충족 기준은 다음과 같다.
- 국내외적으로 인정되어 널리 사용
- 분석 결과의 증거력을 인정받은 도구
- 디지털 포렌식 도구 검증제도(NIST CFTT)에 의해 검증
- 디지털 포렌식 전문업체나 연구기관에 의해 개발되어 과학적·객관적인 검증(Daubert Test)

⑤ 성능 관리
모든 도구의 성능 유지 및 향상을 위한 관리체계를 마련하여야 하고, 신규 도입 시, 사용 전·후, 그리고 주기적인 성능평가를 시행하여 성능 미달 도구에 대한 지속적인 보완·발전이 이루어져야 한다.

⑥ 신규 기술 도입 및 기술 향상
신규 ICT 기기와 적용된 기술에 대해 지속적으로 모니터링하고 이에 대한 디지털 포렌식 수행 방법을 강구하여야 하며, 디지털 포렌식 조사(수사) 방법에 관한 연구를 계속 진행하여야 한다.

⑦ 안티포렌식 대응
디지털 증거의 수집·분석 시 안티포렌식 대응 체계가 마련되어야 한다. 예를 들어, 수집 시에

는 안티포렌식 행위 탐지, 접근제한 우회, 저장매체 은닉영역 탐지, 보안솔루션 대응 방안을 갖춰야 한다. 분석 시에는 삭제·손상 데이터 복구, 암호데이터 탐지·해독, 은닉데이터 탐지·추출 기술을 보유해야 한다.

5.1.4 시설 운영

시설 운영은 디지털 포렌식 관련 시설의 설치, 운영, 관리, 개선에 관한 제반사항의 준비 수준을 평가하는 지표로서, 세부 내용은 다음과 같다.

① 필요 시설의 구축
디지털 포렌식의 신뢰성을 보장할 수 있도록 주요 설비의 목적, 유형, 기능 등 관련사항에 대해 규정하고, 분석, 보관 등 업무 수행 목적과 특성에 따라 별도의 설비를 구비해야 한다. 또한, 구성원들이 업무 수행에 활용할 수 있도록 관련 서적·자료, 업무 결과 등의 보관시설을 갖춰야 한다.

② 시설 관리
디지털 포렌식 관련 설비의 설치, 운영, 관리, 보안에 관한 지침 및 체계가 마련되어야 한다.

③ 보호 설비
주요 시설의 안전한 운영을 위해 전력시설, 화재예방시설, 보안시설 등이 마련되어야 한다.

④ 출입 통제
주요 시설은 출입통제 장비를 설치하여 인가자에 한해 출입토록 접근을 제한하고, 책임성 추적을 위해 CCTV, 기록문서 등을 활용하여 모든 출입 및 접근 이력을 기록·저장하여 검토하여야 한다.

⑤ 시설 평가 및 개선
시설의 미흡·보완사항을 확인하고 개선하기 위한 주기적인 점검이 이루어져야 한다.

Table 2. Digital Forensic Procedures Evaluation Indices

Evaluation Areas		Evaluation Indices
Digital Forensic Procedure	Preparation	Specification of business type and personnel
		Determination of adequacy
		Acquisition of authority
		Planning
		Participants selection
		Education of manual
		Readiness of tools and equipment
	Evidence Preservation and Collection	Field control
		Target identification
		Determination of collection methods
		Records of the collection process
	Evidence Transportation and Storage	Evidence sealing
		Maintenance of evidence list
		Conveyance of evidence
		Secure storage of evidence
	Examination and Analysis	Policy on Examination and analysis
		Division of task
		Analysis laboratory control
		Records of the analysis process
		Preventing damage of the original evidence
		Verification of results
		Documentation of results
	Report Creation and Utilization	Standardization of report
		Verification of report
		Submission and utilization
		Evidence processing
		Improvement and development

5.2 디지털 포렌식 수행 절차 평가

디지털 포렌식 수행 절차 평가는 디지털 증거의 무결성과 관리의 연속성을 보장하기 위해 디지털 포렌식 절차에 따라 각 단계별 업무 수행 능력을 평가하는 것으로, 평가 지표는 Table 2.와 같다.

국내 환경에 적합한 디지털 포렌식 수행 절차 평가 지표를 개발하기 위해 국내 사법기관에서 적용되고 있는 디지털 포렌식 수행 절차를 분석하였다.

대검찰청에서는 2006년부터 디지털 증거를 수집·분석 또는 현출하는 과정에서 준수해야 할 기본적인 사항을 정한 디지털 증거 수집 및 분석 규정(대검예규 616호, 2012.11.6. 개정)을 시행하고 있으며, 그 절차는 '수사 준비, 증거물 획득, 운반 및 보관, 분석 및 조사, 보고서 작성'으로 구성되어 있다[11].

경찰청에서도 2006년에 학계, 민간 전문가 등과 공동연구를 통해 '사전 준비, 증거 수집, 증거분석 의뢰, 증거 분석, 결과보고서 작성' 절차로 구성된 디지털증거 처리 표준 가이드라인을 발간하여 디지털 증거 취급과 관련된 각종 조사 및 수사행위에 적용하고 있으며[12], 2015년 5월에는 디지털 증거의 수집·분석·보관 등 전 과정에서 무결성, 신뢰성 등 사법절차상 요구조건을 준수하고 디지털 증거의 증거능력을 유지하기 위해 디지털 증거 수집 및 처리 등에 관한 규칙(경찰청 훈령 제766호, 2015.5.22. 제정)을 제정하였다[13].

본 연구에서는 대검찰청과 경찰청의 디지털 포렌식 수행 절차를 비교·검토 후, 공통 요소를 선별하여 '사전 준비, 증거 확보 및 수집, 증거 운반 및 보관, 조사 및 분석, 보고서 작성 및 활용'이라는 5단계의 디지털 포렌식 수행 절차를 구성하고, 각 단계별로 수행 능력 평가를 위한 지표를 도출하였다.

5.2.1 사전 준비

사전 준비는 효율적인 디지털 포렌식을 위한 준비 과정에서 수행할 업무의 구분, 필요한 권한의 획득, 계획의 수립 및 교육 등에 대한 평가 지표로서, 세부 내용은 다음과 같다.

① 업무 유형 및 담당 지정
업무 유형과 구성원의 자격에 적합토록 사건 유형, 담당자의 전문성 등을 고려한 그룹을 구성하고 그에 따른 업무분장표가 마련되어야 한다.

② 적절성 판단
디지털 포렌식 조사(수사)의 적절성을 판단하는 확인 절차가 있어야 한다.

③ 조사 권한 획득
범위를 지정하고 조사(수사)에 적합한 권한을 획득하여야 한다.

④ 계획 수립
효율적인 디지털 포렌식을 위해 사건 유형(성격)에 따라 대상, 수행 전략 및 방법 등을 구분하여 세부 조사(수사)계획이 수립되어야 하고, 형사소송법 등 관련 법규 및 지침에 규정된 원칙과 절차를 준수해야 한다.

⑤ 참여인원 선정
직위/자격, 담당분야 등을 고려하여 디지털 포렌식 조사(수사) 참여인원을 선정하여야 한다.

⑥ 조사(수사) 주요사항 교육
디지털 포렌식 참여인원을 대상으로 조사(수사) 중점 및 계획, 유의사항, 적법절차, 이상상황 발생 시 대처방안 등에 대한 사전 교육이 시행되어야 한다.

⑦ 도구 및 장비 준비
디지털 포렌식에 필요한 도구 및 장비를 선정하고, 사전 성능점검을 통해 사용 가능여부를 확인하며, 사용법 및 제한사항 등에 대한 참여인원들의 숙지상태를 점검한다.

5.2.2 증거 확보 및 수집

증거 확보 및 수집은 증거 확보를 위한 현장보존, 조사해야 할 대상의 식별·수집 등에 관한 수행 능력을 평가하는 지표로서, 세부 내용은 다음과 같다.

① 현장 통제
증거 훼손 방지 및 효율적인 증거 수집을 위해 디지털 증거 수집 과정에 피조사자(피압수자) 또는 참고인의 참관 조치 등이 포함된 현장 통제 및 보존 절차가 수립되어야 한다.

② 대상 식별
현장에서 확보 및 수집해야 할 대상(휘발성 데

이터, 하드웨어, 소프트웨어, 저장매체, 데이터베이스 등)을 식별하는 절차가 마련되어야 한다.

③ 수집 방법 판단
현장 여건 및 증거 유형을 고려하여 적절한 증거 수집 방법을 판단, 적용하는 절차가 마련되어야 한다.

④ 수집 과정의 기록
수집 과정의 모든 행위는 동영상 또는 사진으로 촬영하고, 수집 증거의 세부 정보 등이 기록된 증거목록을 작성해야 한다. 증거 목록에 포함되어야 할 세부 정보는 다음과 같다.
- 증거물 번호, 증거물 압수장소, 증거물 종류, 제조사, 모델명, 일련번호, 해시값 등
- 조사자 또는 책임관, 피조사자 또는 참관인의 확인 서명

5.2.3 증거 운반 및 보관

증거 운반 및 보관은 수집된 증거를 분석 장소로 안전하게 운반하여 보관하는 과정의 수행 능력을 평가하는 지표로서, 세부 내용은 다음과 같다.

① 증거 봉인
증거의 훼손 방지를 위해 전자파 차단 및 충격 완화 장비를 이용하여 포장 및 봉인 절차를 수행해야 한다.

② 증거 목록 유지
증거의 누락 및 분실 방지를 위해 정해진 양식에 따라 증거 목록, 분실 목록 등을 작성해야 한다.

③ 인수인계
증거 누락 및 분실을 방지하기 위해 관리의 연속성을 보장하는 증거 인수인계 절차 및 위치 추적 체계가 마련되어야 한다. 예를 들어, 증거와 증거목록 대조, 각 증거의 밀봉전용 특수테이프의 훼손여부 확인, 모든 증거의 무결성 확인 후 책임자의 확인서명 등이 있다.

④ 증거의 안전한 보관
디지털 증거의 안전한 보존을 위해 출입통제 장비가 설치된 별도의 보관시설에 보관하고, 증거 접수일자, 접수자, 관리자, 사유 등을 기록하여야 한다. 보관 증거는 접근 권한을 설정하여 권한을 보유한 인원에 한해 접근을 허가하여야 한다.

5.2.4 조사 및 분석

조사 및 분석은 수집된 증거로부터 데이터를 추출하여 사건 해결을 위한 결과를 도출하고, 결과가 올바른지 검증하는 과정의 수행 능력을 평가하는 지표로서, 세부 내용은 다음과 같다.

① 조사 및 분석 방침
디지털 증거 유형별 분석 표준절차나 매뉴얼에 의거 조사 및 분석을 수행해야 한다.

② 업무 분장
분석 인원의 전문성을 고려하여 수행 업무를 부여해야 한다.

③ 분석실 통제
분석 자료의 신뢰성을 보장하기 위해 인가자를 지정하여 출입인원을 통제해야 한다.

④ 분석 과정의 기록
디지털 증거의 분석과정, 분석자 신원사항, 분석일자, 분석방법 및 도구, 작업 로그 등에 대해 상세히 기록하고, 주요 분석 장면은 사진촬영 또는 영상녹화 해야 한다.

⑤ 증거 원본의 훼손 방지
디지털 증거 원본의 안전한 보존을 위한 수행 절차가 수립, 시행되어야 한다. 수행 절차는 다음을 포함해야 한다.
- 디지털 증거 분석은 원본의 분석용 사본 이미지를 생성하여 수행
- 분석前 원본과 사본 이미지의 해시값 동일성 여부 확인
- 디지털 증거 접수·반환시 책임자, 관리자, 날짜, 장소, 사유 등을 기록부에 기록

⑥ 결과 검증
분석자, 분석도구 등에 상관없이 동일한 증거에 대해 일관된 분석결과가 도출되는지 검증하는 절차 및 방법이 마련되어야 한다.

⑦ 결과 유지
모든 조사 및 분석 기록은 보존기간을 지정하고 문서화하여 보존한다.

5.2.5 보고서 작성 및 활용

보고서 작성 및 활용은 디지털 증거로부터 발견된 결과를 정리하여 보고서를 작성·제출하고, 법정 증언 등에 활용하는 것에 대한 평가 지표로서, 세부 내용은 다음과 같다.

① 결과보고서의 표준화
결과보고서는 분석자, 분석일시, 분석방법 및 도구, 분석내용 등이 포함된 표준 포맷(양식, 서식 등)이 갖추어져야 한다.

② 결과보고서의 검증
작성된 결과보고서 내용의 적절성 판단을 위한 검증 및 보완이 이루어져야 한다.

③ 분석 결과 제출 및 활용
분석 결과 제출 및 법정 증언 시 표준 절차, 결과에 대한 이의제기 시 대응방안 등을 수립, 시행해야 한다.

④ 증거 처리
디지털 증거의 조사 및 분석 결과를 토대로 증거의 보관, 이송, 환부, 파기 여부를 판단하고 그에 따라 증거를 처리하는 절차가 마련되어 있어야 한다. 특히, 보관하는 증거의 경우 다른 사건에서 사용될 수 없도록 접근권한을 부여하여 통제하여야 한다.

⑤ 개선 및 발전
결과보고서를 토대로 전체 디지털 포렌식 과정을 검토하여 절차적·제도적·기술적 보완점을 식별하고 개선하는 절차가 있어야 한다.

VI. 디지털 포렌식 수준 평가 지표 적용

개발된 디지털 포렌식 수준 평가 지표의 타당성과 수준 평가의 적합성 등을 검증하기 위해 국내 법 집행기관 A와 법무법인 B의 디지털 포렌식 조직을 대상으로 평가를 실시하였다. 평가는 해당 조직에서 최소 2년 이상의 경력이 있는 디지털 포렌식 전문가를 대상으로 각 평가 지표에 대한 충족 수준을 0점에서 5점으로 부여하고 해당 조직의 현재 여건을 구체적으로 서술토록 하였고 이를 종합하여 결과를 도출하였다.

먼저, 디지털 포렌식 제반 환경 평가 결과는 Fig. 3.과 같다. 국내 법 집행기관 A는 대부분 항목에서 4점대의 점수를 얻어 대체적으로 평가 지표를 충족하고 있다. 특히, 기본적인 제반 여건이 잘 갖춰진 정부 조직의 일반적인 특성대로 조직의 체계적인 구성 및 운영, 인원 선발, 시설 구축 등 기본 환경 구성 측면에서 높은 수준의 충족도를 보여주고 있다. 하지만 증가하고 있는 디지털 포렌식 수요에 맞춰 업무

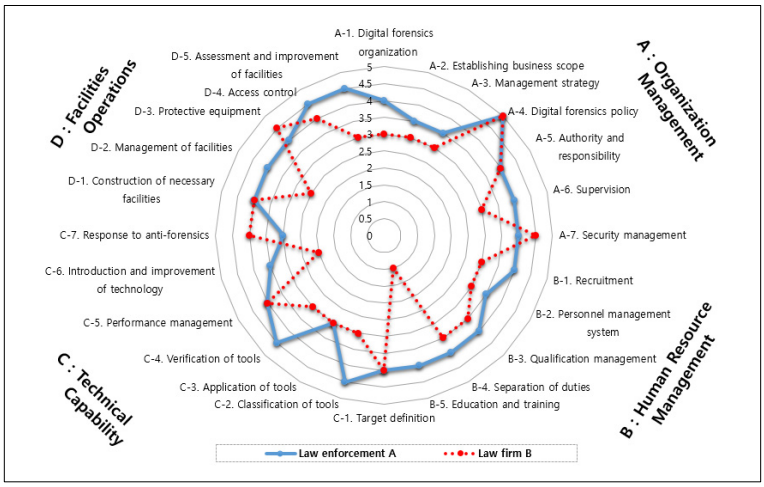

Fig. 3. Result of Applying the Digital Forensic Prerequisite Environments Evaluation Indices

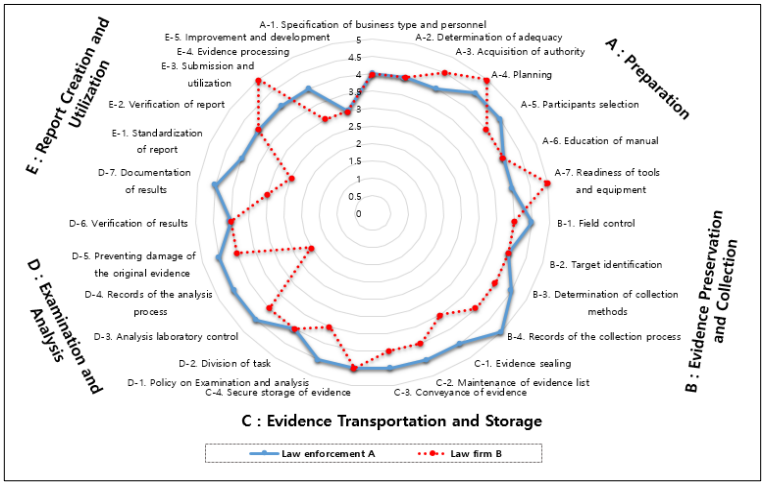

Fig. 4. Result of Applying the Digital Forensic Procedures Evaluation Indices

범위와 경영 전략 등 내부 여건을 융통성 있게 조정·운영하는 측면에서는 다소 미흡한 부분이 확인되었으며, 도구 적용에 대해서는 일관된 운영지침 없이 담당자의 경험과 선호도에 좌우되는 경향도 확인되었다.

반면, 이익 창출을 목적으로 하는 법무법인 B는 정부 조직인 법 집행기관 A에 비해 제반 환경 요소의 충족 수준이 전반적으로 낮게 나타났다. 구체적으로 조직 운영 및 관리, 구성원 교육 및 훈련, 시설 관리 등 조직의 체계적인 발전을 위한 시스템 구축 분야는 상당히 미흡하였다. 하지만 고객과의 계약을 토대로 업무가 진행됨에 따라 필요한 증거를 정확하게 획득하기 위해 도구의 성능 관리 및 안티포렌식 대응 역량이 높고, 고객의 비밀 보호와 관련된 보안 관리에 있어서도 수준이 높게 평가되었다.

다음으로 디지털 포렌식 수행 절차에 대한 평가 결과는 Fig. 4.와 같다. 국내 법 집행기관 A의 경우에는 디지털 증거 수집을 위한 준비부터 분석 결과의 활용에 이르기까지 디지털 포렌식 업무 절차가 단계별로 체계화되어 있음을 확인할 수 있다. 다만, 업무 수행 과정에서의 보완점을 식별하고 개선하기 위한 피드백 체계가 다른 요소에 비해 미비함을 알 수 있다.

법무법인 B도 디지털 포렌식 업무 수행 결과를 법정에서 활용함에 따라 관련 법규 및 지침을 토대로 디지털 증거의 수집에서 법정 제출에 이르기까지 관리의 연속성 보장과 관련된 지표의 충족도가 높게 나타났다. 하지만 분석 과정에 대한 기록이 명확하지 않고, 표준화된 포맷 없이 고객의 요구에 의해 결과 보고서의 양식과 내용이 결정됨에 따라 분석 결과에 대한 객관성 보장이 미흡하였다.

개발된 지표를 적용한 결과, 디지털 포렌식 수행을 위한 제반 환경과 단계별 업무 수행 능력 측면에서 각 평가 대상 조직에 대한 객관적이고 종합적인 역량 측정이 가능하고, 평가 대상별로 보완·개선이 요구되는 사항을 정확하게 확인할 수 있으며, 평가 대상의 장·단점 식별이 용이하다. 이러한 평가 결과는 법정에서 디지털 포렌식 수행 조직의 수준을 판단할 수 있는 합리적인 참고자료로 사용될 수 있고, 디지털 포렌식 조직을 활용하려는 고객들에게 신뢰할 수 있는 판단 정보를 제공할 수 있을 것이다.

VII. 결 론

최근 수사 및 조사, 감사 등 다양한 분야에서 디지털 포렌식 기술이 널리 활용되고 있음에도 디지털 증거의 신뢰성에 대해 지속적으로 논란이 제기되고 있다.

이에 본 연구에서는 디지털 포렌식의 신뢰성 있는 처리를 보장하고, 디지털 증거의 증거능력에 관한 사법기관의 판단 기준과 정부기관·기업 등의 디지털 포렌식 수행 조직의 역량 측정에 활용이 가능한 디지털 포렌식 수준 평가 지표를 개발하였다.

개발된 지표는 디지털 포렌식 수행을 위해 갖추어야 할 제반 여건 및 기본 요구사항과 국내 사법기관에서 적용하고 있는 디지털 포렌식 절차를 토대로 구성한 디지털 포렌식 절차의 각 단계별 업무 수행 능력에 관한 항목으로 구성되어 있다. 해당 지표를 국

내 디지털 포렌식 조직에 적용한 결과, 평가 대상에 대한 종합적인 역량 측정이 가능하고, 평가 대상의 미비점을 쉽게 식별하고 보완할 수 있어 신뢰성 있는 디지털 포렌식 조직의 구성 및 관리체계 수립, 객관적이고 체계적인 디지털 포렌식 수준 평가에 기여할 것으로 기대된다.

향후에는 개발된 지표를 기초로 구체적인 평가 항목을 도출하고, 수준 평가 결과의 등급화를 통한 디지털 포렌식 인증 방안에 대하여 연구를 진행할 계획이다.

References

[1] ISO, "ISO/IEC 17025:2005(General requirements for the competence of testing and calibration laboratories)," May 2005.

[2] ASCLD/LAB, http://www.ascld-lab.org/

[3] KOLAS, http://www.kolas.go.kr/usr/gud/abt/Introduce.do

[4] Ebrahim Hamad Al-Hanaei and Awais Rashid, "DF-C^2M^2: A Capability Maturity Model for Digital Forensics Organisations," 2014 IEEE Security and Privacy Workshops, pp. 57-60, May 2014.

[5] ISO, "ISO/IEC 27001:2013(Information technology-Security techniques-Information security management systems-Requirements)," Oct. 2013.

[6] ISMS(Information Security Management System), http://isms.kisa.or.kr/kor/intro/intro01.jsp

[7] Jae-Gyu Choi and Bong-Nam Noh, "Security Technology Research in Cloud Computing Environment," Journal of Security Engineering, 8(3), pp. 371-384, Jun. 2011.

[8] Ok Heo and Seungjoo Kim, "Information Security Management System Evaluation Criteria with availability for Korean Smart Grid," Journal of The Korea Institute of Information Security & Cryptology 24(3), pp. 547-560, Jun. 2014.

[9] DFRWS Technical Report, "A Road Map for Digital Forensic Research," pp. 16, Aug. 2001.

[10] Sangjin Lee, Introduction to Digital Forensics, eroon, Jul. 2010.

[11] Supreme Prosecutors Office, "Digital evidence collection and analysis rule," 2012.

[12] The national police agency, "Digital evidence processing standard guideline," 2006.

[13] The national police agency, "Rule on collection and processing, etc. of Digital evidence," 2015.

〈저자소개〉

박 희 일 (Hee-il Park) 학생회원
2003년 3월: 공군사관학교 국방학과 학사
2014년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 디지털 포렌식, 정보보호

윤 종 성 (Jong-seong Yoon) 학생회원
2005년 3월: 공군사관학교 전산과학과 학사
2013년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석·박사통합과정
〈관심분야〉 디지털 포렌식, 정보보호, 악성코드 분석

이 상 진 (Sang-jin Lee) 종신회원
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해시 함수