한국항행학회 논문지 제 15 권 제 6 호 2011년 12월

개인정보보호법 기반 디지털 포렌식 수사 모델 연구

Study on Digital Investigation Model for Privacy Acts in Korea

이창훈*

Chang-Hoon Lee*

요 약

최근 개인정보보호법이 시행됨에 따라 국내 기업의 개인 정보 관리에 대한 안전 조치 의무의 요구가 높아지고 있으며, 이는 곧 개인정보의 수집, 이용, 제한, 관리, 파기 등과 같이 개인정보 처리에 대한 구체적 규제 조항에 따른 기술적 대응이 필요하고 있다. 이에 따라 기업에 대한 침해 사고가 발생하였을 경우, 개인정보 관리체계가 올바르게 동작하도록 운영되었는지 확인할 수 있도록 안전 조치를 취해야 하며, 이를 확인할 수 있는 구체적인 준비 과정이 수행되어야 하므로, 이는 곧 디지털 포렌식 수사 모델의 첫 번째인 조사 준비 단계에 해당한다. 또한 현장에 출동한 조사팀은 이러한 조치 행위가 올바르게 수행되었는지 점검할 수 있도록 적절한 조사를 수행해야 하므로 이는 현장 대응 단계와 관련이 있다. 본 논문에서는 디지털 포렌식 수사 모델의 조사 준비 및 현장 대응 단계에 대하여 개인정보보호법 이행 및 점검을 위해 보완해야 할 점은 무엇이고, 이를 통해 개인정보보호법에 대응하는 디지털 포렌식 수사모델의 개선 방안을 제시한다.

Abstract

As recently Privacy Acts in Korea enforced in domestic companies' personal information management needs of a growing obligation for the safety measures and the right of personal information collection, use, limitations, management, and destroyed specifically for handling personal information. Such this regulations should be required technical and policy supports. Accordingly, for the enterprise incident has occurred, the personal information management system behave correctly operating to verify that the safety measures taken, and be determined by the specific preparation to be done. So the first, preparation phase corresponds to the upcoming digital forensic investigation model. On the other hand, the response team also carried these measures out correctly, it needs to be done to check the compliance of Privacy Act. Thus a digital forensics investigation model is strictly related with the implementation of the Privacy Acts and improve the coping strategies are needed. In this paper, we suggest a digital forensic investigation model corresponding to Privacy Act.

Key words : Digital Forensic, Digital Investigation Model, Privacy Act, Forensic Readiness

Ⅰ. 서 론

최근 각종 컴퓨터 범죄와 개인의 사생활 침해 등 정보화 사회의 역기능을 방지하기 위해 개인정보보호법이 제정되어 최근부터 시행되고 있다. 개인정보보호법은 “개인 정보의 수집・유출・오용・남용으

* 한신대학교 컴퓨터공학부 (School of Computer Engineering, Hanshin University)
・제1저자 (First Author) : 이창훈
・투고일자 : 2011년 11월 22일
・심사(수정)일자 : 2011년 11월 22일 (수정일자 : 2011년 12월 19일)
・게재일자 : 2011년 12월 30일

로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인 정보 처리에 관한 사항을 규정함을 목적으로 한다.”라고 제1조에 명시하고 있다. 또한 적용 대상을 공공 및 민간 부분으로 확대하고 온/오프라인을 통합하여 규제/관리하기 위한 기본법으로 제정하였고, 이를 통해 법률 적용을 받지 않는 사각지대를 해소하는 것이 제정 취지이다. 또한 개인정보의 수집, 이용, 제공, 위탁, 파기와 같이 처리 단계별 보호기준을 구체적으로 규정하여 국민의 개인정보보호를 강화하였다.

한편 제29조에서 “개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.”라고 안전조치의무를 명시하였다. 따라서 기업 내 보안사고가 발생하였을 경우, 현장에 도착한 수사기관 또는 조사기관은 피조사 대상이 안전조치의무를 충실히 이행하였는지 확인해야 하며, 이러한 과정을 검토할 수 있도록 디지털 포렌식 모델이 개선되어야 한다.

본 논문은 이와 같이 최근 시행되고 있는 개인정보보호법에 대응하는 디지털 포렌식 수사 모델에 대하여 살펴보고자 한다. 앞서 살펴본 제29조 안전조치의무를 점검하는 과정은 침해사고가 발생한 당시 상황에 대한 대응 체계와 관리가 제대로 운영되었는지를 점검하고 현장에 도착한 조사팀은 현장 대응을 통해 필요한 증거자료가 수집될 수 있도록 준비해야 한다. 이는 곧 포렌식 조사 모델의 첫 번째 단계인 조사 준비 단계와 두 번째 현장 대응 단계와 관련이 있다. 본 논문에서는 개인정보보호법의 세부 시행 규칙에 따르는 디지털 포렌식 수사 모델을 제시하고자 한다.

다음 장에서는 개인정보보호법에서 살펴보아야 할 주요 조항을 살펴보고, 3장은 현재 디지털 포렌식 수사 모델과 포렌식 준비 (Forensic Readiness) 에 대해 살펴본다. 4장에서는 개인정보보호 요구 조항에 따르는 디지털 포렌식 수사 모델의 조사 준비와 현장 대응 단계를 제시한다.

Ⅱ. 개인정보보호법과 디지털포렌식

본 논문에서 초점이 되는 개인정보보호법과 디지털 포렌식이 관련되어 있는 주요 조항을 살펴본다. 앞서 살펴본 것처럼, 제29조는 개인정보에 대한 안정성 확보에 필요한 기술적, 관리적 및 물리적 조치를 취해야 함을 명시한다. 또한 제24조에서는 개인의 고유식별정보를 처리하는 경우, 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 해야 한다고 명시하고 있다. 이는 곧 프라이버시 강화 기술(Privacy Enhanced Technology)과 같은 기술이나 데이터베이스 암호화 기술을 도입하여 개인정보에 대한 안전성을 강화해야 함을 나타낸다.

디지털 포렌식 관점에서 살펴볼 조항은 입증 책임과 접속 기록 보관 및 위변조 방지에 대한 요구 조항이다. 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담해야 하며 (제16조 1항), 또한 사고 발생 시 고의 또는 과실이 없음을 입증하여 책임 소지를 밝혀야 함을 명시하고 있다.(제39조 1항) 또한 “개인정보처리자가 이 법에 따른 의무를 준수하고 상당한 주의와 감독을 게을리 하지 아니한 경우에는 개인정보의 분실・도난・유출・변조 또는 훼손으로 인한 손해배상책임을 감경 받을 수 있다.” (제39조 2항) 라고 입증 책임을 기업에 전환하고 있다. 또한 제29조는“개인정보처리자는 개인정보가 분실・도난・유출・변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다.”라고 접속 기록 보관 및 위변조 방지에 대해 명시하고 있다. 따라서 디지털 포렌식 관점에서는 사건이 발생하기 이전부터 실시간 모니터링과 같이 포렌식 준비(Forensic Readiness) 정책 및 기술이 필요함을 나타내며, 개인정보 유출 시 과실에 대한 책임 소지를 분별하기 위한 증거 자료 확보와 보존이 필요함을 나타낸다.

Ⅲ. 디지털 포렌식 수사 모델과 Forensic Readiness

3-1 디지털 포렌식 수사 모델

디지털 포렌식 수사 모델을 간단히 살펴보면 디지털 포렌식 조사를 수행하기 위한 절차로 정의할 수 있다. 디지털 포렌식 진행 과정을 살펴보면, 사건 발생을 인지한 순간부터 수사 준비, 현장 대응, 증거 수집, 조사 과정을 거친 후, 그 결과를 법정에 제출하는 형태로 진행된다. 포렌식 수사 모델은 과학적 체계, 기술적인 방법, 조사 절차, 법적 절차 등 다양한 초점에 맞춘 조사 모델이 존재한다. 국내 수사 기관의 경우는 초창기의 미국 수사기관에 제안한 수사 가이드라인을 그대로 적용하였고, 향후 대검찰청 디지털 증거 압수수색 모델과 같은 형태로 발전하였다. 디지털 포렌식 조사 모델을 구체적으로 정리하면“조사 준비”, “현장 대응”, “증거물 확보 및 수집”, “운반 및 확인”, “조사 및 분석”, “보고 및 증언"까지 6 단계로 정의할 수 있다.

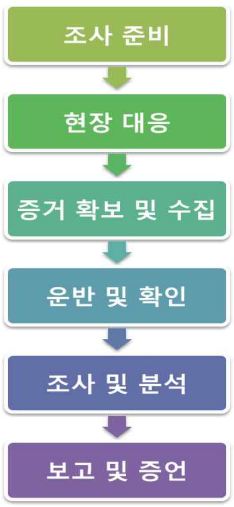

그림 1 . 디지털 포렌식 수사 모델 개관
Fig. 1. Digital Forensic Investigation Model

국내 관련 연구로 대검찰청 디지털 증거 압수 수색 모델과 경찰청 디지털 증거 처리 가이드라인을 소개한다. 먼저 그림 2 대검찰청 디지털 증거 압수 수색 모델 [17]은 수사 기관에서 수행하는 절차이므로 영장 집행 위주로 구성된 것이 특징이며, 증거수집 준비단계, 영장 집행 및 증거 수집, 운반 및 보관, 분석 및 조사, 보고서 작성 단계로 나누어진다.

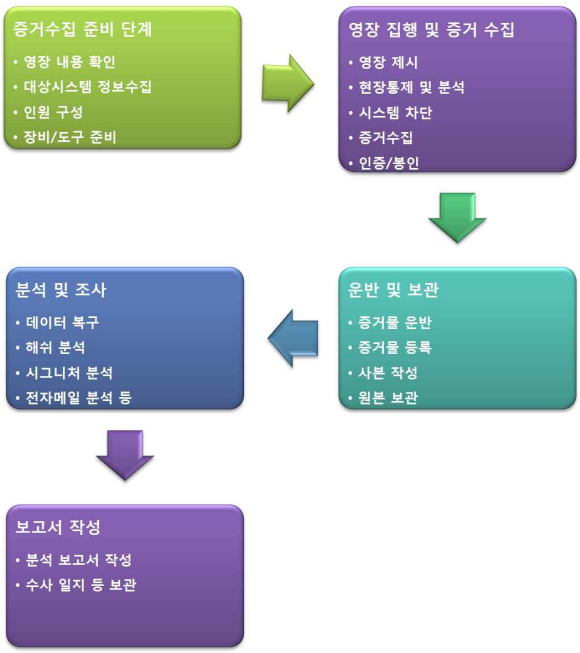

그림 2. 대검찰청 압수수색 모델
Fig. 2. Seizure and Search Model by Prosecutors's Office

“증거수집 준비단계”는 현장 출동 전에 수사를 위한 준비사항을 점검하는 단계이다. 수사를 시작하기에 앞서 사건 정보와 영장 내용을 확인하고, 필요 인원과 장비・도구 등을 준비하는 단계이다. 먼저 사건 관련 확인 사항을 숙지하여 사건 유형, 영장의 내용과 범위, 수사 대상 시스템 파악, 증거 수집 장비와 도구를 준비한다. 또한 현장에서 증거 자료의 수집에 어려움이 없도록 준비 사항을 면밀히 검토하고, 수사 진행을 위한 전체 과정을 면밀히 확인한다.

“영장 집행 및 증거 수집 단계”는 사건 현장에서 조사를 수행하는 과정으로, 현장에서의 대응 요령, 증거 수집, 증거 포장 및 인증 절차로 진행된다. 먼저 영장을 대상 기관에 제시하여 수사 협조를 구한 뒤, 현장을 통제하여 증거 인멸 시도를 차단한다. 나아가 현장의 시스템 접근을 차단하고, 주요 조사 시스템을 선별하여 필요한 증거 시스템을 확보하거나 필요한 증거 데이터를 수집한다. 확보한 시스템이나 수집한 증거 자료는 제3자의 공증이나 피수사 담당자의 확인 과정을 거쳐 봉인한다.

"운반 및 보관" 단계는 봉인된 증거 자료를 해제하고 증거물의 법적 효력을 위해 기록·등록한다. 원본 증거 자료는 사본을 생성하여 향후 분석할 수 있도록 하며, 원본은 전자기장 및 충격으로 부터 보호할 수 있는 공간에 별도로 보관한다.

"분석 및 조사" 단계는 생성한 사본을 바탕으로, 삭제 데이터 복구, 해쉬값 분석, 파일 시그니쳐 분석, 응용 프로그램 사용 흔적 분석(전자메일을 비롯한 인터넷 메시징 서비스 등)을 수행한다. 분석된 결과는 분석 보고서를 작성하여 보관하며, 향후 법정에서 증거 자료로 제시할 수 있도록 문서화한다.

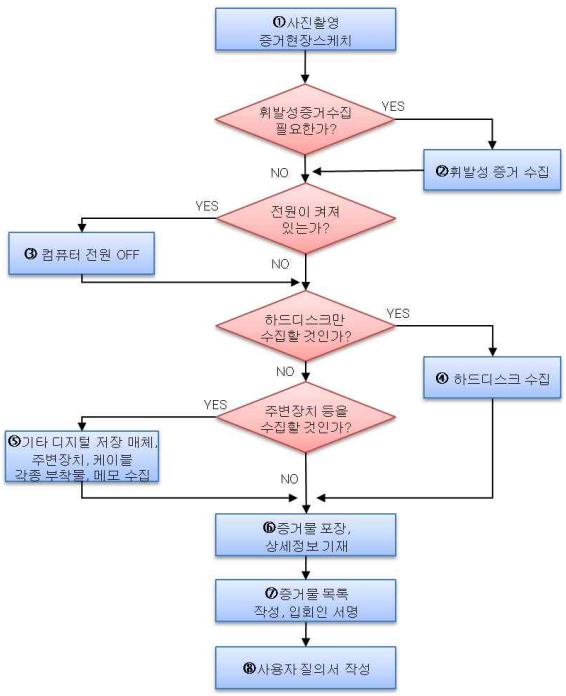

그림 3. 경찰청 디지털 증거 압수 절차
Fig. 3. Digital Evidence Seizure Process by National Police Agency

경찰청 디지털증거 처리 표준 가이드라인 [16] 은 전반적인 수사 전체에 대한 모델을 제시하기 보다는 전반적인 증거 처리 원칙부터 증거 수집, 분석, 결과 보고서 작성 등에 대해 상세히 다루고 있는 것이 특징이다. 가이드라인에서 제지한 수사 모델은 증거수집, 증거분석 의뢰, 증거분석, 결과보고서로 나뉜다. 그림 3 가이드라인에서 제시한 디지털 증거 수집 절차도를 나타내며, 이처럼 가이드라인은 세부적인 수사 절차와 주의 사항을 설명하는 것에 중점을 둔다. 증거분석 과정은 유형별로 증거분석 표준절차를 나눈 것이 특징으로, 디스크 분석, 네트워크 분석, 웹 사용 분석, 전자우편, 악성코드, 데이터베이스, CCTV, 휴대폰, 암호화 파일 등으로 나뉜다.

3-2 포렌식 준비 (Forensic Readiness)

디지털 포렌식 수사 모델은 일반적으로 사고 발생 후에 현장에 도착하여 조사를 수행하여 원인을 분석한다. 사건 발생 이후 수집한 정보를 바탕으로 오랜 기간 동안 조사 과정을 거치더라도 귀중한 정보는 이미 삭제될 가능성이 높다. 따라서 보안 사고 발생 전부터 이러한 보안 사고를 능동적으로 대처하기 위한 방법론이 대두되고 있으며, 이를 사전 포렌식 대응 (Proactive Forensics) 이라고 한다. 사전 포렌식 대응은 포렌식 준비인(Forensic Readiness)에서 출발한 개념으로, 사건 대응을 위한 준비 과정을 보다 세밀하게 설립하여, 보안 사고를 발생 이전에 방지하거나 사고 발생 후에 원인 분석을 빠르게 하기 위한 시스템을 구축하는데 의미를 둔 방법론이다. 이는 곧 개인정보보호법의 요구조항과도 부합한다고 볼 수 있다.

Forensic Readiness와 관련된 국외 연구를 간단히 살펴보면, 영국 연방 국가에서 사용하도록 영국 정부에서 발간하는 가이드라인 HMG Security Policy Framework [13] 의무 준수 37항에서 이를 언급하고 있다. 37항의 내용은 포렌식 준비 정책 (Forensic Readiness Policy) 은 정보통신시스템에 의해 생성되는 데이터는 법적 및 관리적 목적에 부합하도록 보존과 분석이 가능해야 하며, 반면 정보의 가용성이 최대화 될 수 있음을 보장해야 함을 명시하고 있다.

Solms [9] 논문은 디지털 포렌식 기반으로 한 기업 통제 프레임워크 (A Control Framework fo Digital Forensics) 를 제시했으며, 계획 및 준비, 사건 대응, 조사, 증거 처리 단계로 나누었다. 포렌식 준비 단계는 디지털 증거를 최소한의 비용으로 최대한의 데이터를 수집한다는 기준을 정립하고 업무에 방해되지 않는 선에서 수행하도록 정의하며 각각의 세부 절차를 정의하였다. 예를 들면, 디지털 증거에 필요한 비즈니스 시나리오 정의, 잠재적 증거를 확보할 수 있는 출처와 종류 식별, 증거 수집 요구사항 결정, 요구사항에 부합하는 가용 증거 데이터를 안전하게 수집

하기 위한 방안 마련 등을 제시하고 있다.

G. Pangalos [10] 논문은 보안 감사와 포렌식 준비(Information Assurance and Forenisd Readiness) 에 대해서 발표하였다. 먼저 보안 감사 측면에서 IT 컴플라이언스 와 감사 절차를 설명하고 여기에 포렌식 준비 단계에서 절차들의 상충 관계를 설명하였다. 이 논문은 단순히 상호 관계에 대한 비교와 서로 간의 시너지를 위한 필요성만을 언급하였다.

이처럼 개인정보보호법의 요구조항과 포렌식 레디니스는 밀접한 관계를 지니며, 개인정보의 안전한 관리 및 사용을 위해서는 정보보호 관리체계에서부터 이에 대한 대응하기 위한 사항들을 도입하여 개정하고, 이를 평가하기위한 체계가 마련되어야 한다. 본 논문에서는 디지털 포렌식 수사 모델 관점에서만 개인정보보호법의 요구조항에 대응하기 위한 수사 모델을 제안한다.

Ⅳ. 개인정보보호법의 요구조항을 적용한 디지털 포렌식 수사 모델

4-1 조사 준비 단계와 개인정보보호법

조사 준비 단계는 보안사고 발생 시 현장에 출동하는 수사기관 및 조사기관이 사고와 관련된 증거 자료를 확보할 수 있도록, 조사 대상 업체 즉 개인정보처리자가 포렌식에 활용할 수 있는 정보들을 관리·보관하고 있음을 입증할 증거 자료를 보존하고 있어야 한다. 따라서 조사 준비 단계는 개인정보처리자는 포렌식 레디니스 관련 관리 정책 또는 기술을 적용하여 사고 발생 이전에 일련의 관리체계나 보안 시스템을 마련하여 준비해야 한다.

표 1은 개인정보보호처리자 관점에서 개인정보보호법에 대한 대응전략을 요약한 것이다. 입증 책임의 경우, 개인정보를 열람하는 정보시스템에 대하여 실시간 모니터링 솔루션을 도입하여 사고 발생 시 즉각적으로 대처할 수 있는 시스템을 구축한다. 이는 기존의 기밀 유출 방지 시스템의 기능을 확장하여 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 해야 한다. 또한 개인정보에 접근하는 시스템은 정보 사용에 대한 각종 로그 정보를 저장하고 보관하도록 하는 솔루션을 도입해야 한다.

표 1.개인정보처리자의 개인정보보호법 대응전략
Table 1. Response Strategy for Privacy Information Handler

조항	핵심내용	대응전략
제16조 1항 제39조 1,2항	입증 책임	- 개인정보가 저장된 정보시스템에 대한 각종 로그를 남길 수 있는 포렌식 솔루션 도입 - 개인정보 열람 시스템에 대한 실시간모니터링 시스템 도입
제24조 3항	고유식별정보 보호	- 고유식별정보에 대한 암호화 솔루션 또는 PET 솔루션 도입
제29조	안정성 조치 점검	- 정보보호관리체계 인증 - 시스템/네트워크 보안 장비 또는 솔루션 구축 - 관련 시스템에 대한 물리적 접근 통제

고유식별정보 보호는 개인정보의 고유식별정보 암호화, 데이터베이스 암호화, PET 기술, 익명화 기술 등과 같은 솔루션을 도입해야 한다.

안정성 조치 점검은 정책적 관점에서는 정보보호 관리체계의 도입하여 유관 기관의 인증을 받도록 체계를 정비하는 것이 필요하며, 기술적 관점에서는 기존 보안 시스템 또는 장비와 더불어 e-discovery 솔루션과 같이 기술적 대응이 필요하다. 물리적 관점에서는 개인정보가 저장된 시스템에 대한 철저한 접근 통제와 CCTV를 통한 모니터링이 필요하다.

4-2 현장 대응 단계의 개선 방안

보안사고 발생 시, 현장에 도착한 사고 조사팀은 앞서 제시한 대응 전략에 대해 이행 여부를 점검하며, 이를 요약하면 표 2와 같다.

개인정보보호법 준수를 확인하기 위한 절차는 기존의 디지털 포렌식 조사 모델의 현장 대응 단계를 보완하여 한다. 현장 대응 단계의 세부 절차는 현장 통제, 현장 분석, 조사 대상 시스템 확보로 정의할 수 있다. 현장의 통제는 증거물을 최대한 원본 상태로 보존할 수 있고, 이를 통해 사건이 발생한 원인을 파악함으로써 본격적인 조사를 시작할 것인지를 판단할 수 있는 근거가 되며, 또한 증거 훼손을 막아 예기

하지 못한 실수로 인해 중요한 증거 자료가 손실되지 않게 막을 수 있다.

표 2.조사기관에서의 개인정보보호법 준수 점검 위한 현장 대응 전략
Table 2. Response Strategy for Incident Response Organization

조항	핵심내용	현장대응 세부절차	현장 대응
제16조 1항 제39조 1,2항	입증 책임	-현장 분석 -조사 대상 시스템 확보	고의 또는 과실 유무 입증을 위한 증거자료 보관 여부 확인 및 증거자료확보
제24조 3항	고유식별정보 보호	-현장 분석	고유식별정보에 대한 보안 솔루션 도입 여부 확인
제29조	안정성 조치 점검	-현장 통제	관리적, 기술적, 물리적 안전성 조치 확인

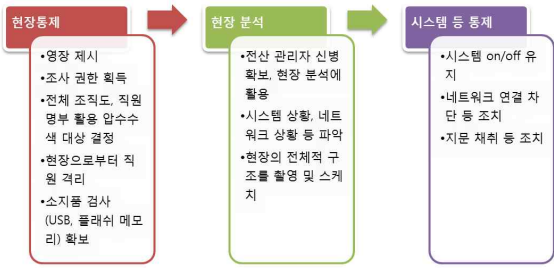

그림 4. 일반적인 현장대응 절차
Fig. 4. General On-Site Response Procedure

현장 대응 단계는 각 조사기관의 정책과 권한에 의거하여 정의한 현장 대응 지침서나 증거 처리 규칙에 따라 조사를 수행하게 되며, 세부적인 절차는 각 기관이 정한 현장 조사 절차를 준수하면서 상황에 맞게 적용한다. 예를 들어 수사 기관의 경우는 피조사 기관에 영장을 제시하여 필요한 물리적 증거 혹은 디지털 증거 자료를 획득하기 위해 현장을 통제하고 압수 수색을 실시하게 된다. 반면에 민간 기관의 경우는 의뢰인의 협조를 통해 조사가 이루어지므로, 현장 통제 과정이 불필요하고 범법 사실 회피 가능성이 존재하지 않는다. 또한 조사가 필요한 시스템은 의뢰인의 협조로 파악이 가능하므로 시스템 확보 과정이 필요하지 않다.

먼저 입증 책임은 디지털 포렌식에서는 증거자료 보관 여부와 증거 자료 확보에 해당하며, 이는 현장 보존과 조사 대상 시스템 확보와 관련이 있다. 고유식별정보보호는 개인정보의 고유식별정보에 대한 보안 솔루션 도입 여부를 판별하는 과정이므로 현장 조사과정에서 수행된다. 안전성 조치 점검은 개인정보 처리에 대한 관리적, 기술적, 물리적 안정성 조치에 대한 확인 과정이므로, 현장 통제와 현장 조사과정과 연관된다. 이를 바탕으로 디지털 포렌식 조사 모델의 현장 대응 단계를 개선하면 그림 5와 같다.

개인정보 침해사고 발생 시, 현장에 도착한 조사팀은 현장 통제를 실시하고, 개인정보 관리 정책이 올바르게 수행되었는지 확인하며, 개인정보에 대한

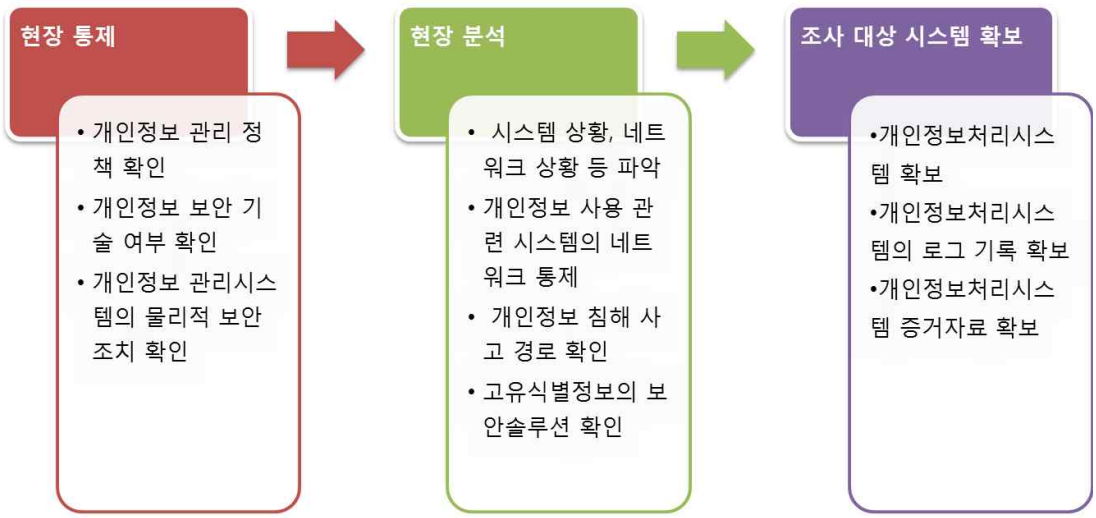

그림 5. 개인정보 침해 사고 시 현장대응 절차
Fig. 5. On-Site Response Procedure for Privacy Leakage Incident

솔루션이 도입되어 동작하고 있는지 확인한다. 또한 개인정보 사용과 관련이 있는 시스템에 대한 물리적인 보안 체계가 동작 중인지 확인하여, 사고 발생에 대한 책임이 있는지 여부를 점검한다.

현장 분석 과정에서는 개인정보를 사용 혹은 관리하는 시스템 및 네트워크 상황을 파악하여 악성코드 감염과 같이 해킹의 피해가 없는지 확인하고 관련 시스템의 네트워크 사용을 통제한다. 또한 이 과정에서 사고 발생 경로를 확인하여 피해 시스템의 위치를 파악하며, 해당 시스템이 개인정보의 고유식별정보에 대한 안정성 조치를 취했는지 확인한다.

피해 시스템의 위치를 파악하면, 조사 대상 시스템을 확보하고 해당 시스템의 개인정보와 관련된 로그 기록을 확보하고 개인정보의 분실・도난・유출・변조 또는 훼손 여부를 확인할 수 있도록 증거자료를 확보한다.

Ⅴ. 결 론

본 논문은 이와 같이 최근 시행되고 있는 개인정보보호법에 대응하기 위해 디지털 포렌식 관점에서 개선된 수사 절차를 제시하였다. 앞서 살펴본 개인정보보호법 제29조 안전조치의무 수행과 같이 이를 준수하는 개인정보처리자 관점에서는 이행 의무를 충실히 수행하기 위한 대응전략을 살펴보았으며, 이를 점검하는 조사기관의 관점에서는 침해사고가 발생한 당시 상황에 대한 사고 대응 체계 및 관리가 제대로 운영되었는지를 점검하기 위한 현장 대응 전략을 제시하였다. 개인정보보호법의 충실한 이행과 평가를 위해서는 평가체계나 인증제도 및 관련 보안 솔루션이 마련되어야 한다. 나아가 정보보호 관리체계에서부터 개인정보 보호에 대응하기 위한 관리적, 기술적, 물리적 사항들을 도입하여 개정하고, 이를 평가하기위한 체계가 마련되어야 한다.

감사의 글

본 논문은 한신대학교 학술연구비 지원에 의하여 연구되었음.

참 고 문 헌

[1] Sundresan Perumal, Digital Forensic Model Based On Malaysian Investigation Process, *International Journal of Computer Science and Network*

[2] Ricci S.C. Ieong, FORZA - Digital forensics investigation framework that incorporate legal issues, Digital Investigation, Volume 3, Supplement 1, *The Proceedings of the 6th Annual Digital Forensic Research Workshop* (DFRWS '06), 2006

[3] Séeamus Ó Ciardhuáain, An Extended Model of Cybercrime Investigations, *International Journal of Digital Evidence*, Volume 3, Issue 1, 2004

[4] Mark Reith, Clint Carr, Gregg Gunsch, An Examination of Digital Forensic Models, *International Journal of Digital Evidence,* Volume 1, Issue 3, 2002

[5] DFRWS TECHNICAL REPORT-A Road Map for Digital Forensic Research, 2001

[6] Eoghan Cesay, Digital Evidence And Computer Crime-Forensic Science Computers And The Internet 2nd edtion, Elsevier, 2004

[7] Warren G Kruse, Jay Heiser, Computer Forensics: Incident Response Essentials, *Addison-Wesley Professional,* 2001

[8] Timothy Palmbach, Marilyn Miller, Henry Lee, Henry Lee's Crime Scene Handbook. San Diego, *Academic Press*, 2001

[9] S. von Solms, C. Louwrens, C. Reekie and T. Grobler, A Control Framework for Digital Fornesics, Advances in Digital Forensics II. *IFIP Advances in Information and Communication Technology*, 2006, pp.343-355

[10] Georgios Pangalos and Vasilios Katos, Information Assurance and Forensic Readiness, Computer Science Next Generation Society. Technological and Legal Issues, LNCS, *Social Informatics and Telecommunications Engineering*, 2010, Volume 26, Part 6

[11] T. Grobler, and B. Louwrens, "Digital forensic readiness as a component of information security best practice", in IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security,

Privacy and Trust in Complex Environments, Springer, 2007, pp. 13-24
[12] Pangalos G. Ilioudis, C. Pagkalos, I. The Importance of Corporate Forensic Readiness in the Information Security Framework, *2010 19th IEEE International Workshop on Infrastructures for Collaborative Enterprises (WETICE)*, June 2010, pp. 12-16
[13] Cabinet Office of United Kingdom, HMG Security Policy Framework ver6.0, May 2011
[14] *개인정보보호법*, 제정 2011.3.29 법률 제10465호
[15] 이창훈, 임경수, "국내 환경을 고려한 디지털 포렌식 조사 모델 정립 방안," *한국정보처리학회 추계 학술발표대회 논문집 제18권, 제2호*, 2011.11
[16] *경찰청*, 디지털 포렌식 증거 처리 가이드라인, 2008
[17] *대검찰청*, 디지털증거압수수색모델, 2009

이 창 훈 (李昌勳)

2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2008년 2월 : 고려대학교 정보경영공학전문대학원 박사
2009년 3월~2010년 2월 : 한신대학교 컴퓨터공학부 전임강사
2011년 3월~현재 : 한신대학교 컴퓨터공학부 조교수
관심분야 : 암호학, 디지털포렌식, 정보보호