JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 7 : 1495~1504 July. 2014

정부 ICT R&D 중장기전략과 ICT 패러다임 변화를 반영한 디지털 포렌식 표준정립을 위한 기술-정책적 통합프로세스 프레임워크

신준우*

A Technology-Strategy Integrated Digital Forensic Process Framework Considering Government ICT R&D Strategy and ICT Paradigm Shift

Jun Woo Shin*

National IT Industry Promotion Agency, Daejeon 305-348, Korea

요 약

인터넷 뱅킹과 같은 부가서비스, 채팅 등과 같은 대화형 서비스를 이용하는 정보화 사회가 정착되었고, 더욱이 스마트기기를 이용한 서비스 사용이 급속하게 발전함에 따라 신규 보안기술 분야로 디지털 포렌식에 관한 연구가 활발히 진행되고 있다. 본 논문에서는 디지털 포렌식에 관한 기존의 연구를 체계적으로 분석하고 앞으로 정부의 ICT R&D 중장기 전략과 ICT 패러다임 변화를 반영하여 첨단 IT기술과 우리나라 법체제를 융합하는 체계적인 디지털 포렌식 표준정립을 위한 기술-정책적 통합프로세스 프레임워크를 제안한다.

ABSTRACT

Currently information related service such as internet banking, chatting, social network services are quite well smeared into our daily life. Moreover, a rapid growth of service using smart devices brought an importance of security in internet services and a research activation of digital forensic in a crime investigation. This paper presented a previous digital forensic research trend and based on this, suggested a technology-strategy integrated digital forensic process platform, taking a mid-long term government leading ICT R&D strategy and ICT paradigm shift into account.

키워드 : 디지털 포렌식, 기술-정책적 프로세스, ICT R&D, ICT 패러다임

Key word : Digital Forensic, Technology-Strategy Process, ICT R&D, ICT paradigm, etc

접수일자 : 2014. 04. 08 심사완료일자 : 2014. 04. 28 게재확정일자 : 2014. 05. 16

* **Corresponding Author** Jun Woo Shin(E-mail:sjw@nipa.kr, Tel:+82-42-710-1450)
Natioanl IT Industry Promotion Agency, Daejeon 305-348, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.7.1495 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

디지털 포렌식에 관한 IT기술 연구논문은 다수 존재하지만 사회과학 및 법학과 관련한 연구논문은 매우 부족한 실정이다. 하지만, 이러한 IT기술 연구는 디지털 증거가 가지고 있는 다양한 법학적 문제에 대한 접근이 어렵다고 할 것이고 앞으로 발생하게 될 디지털 증거의 문제를 해결하기에는 많은 어려움이 발생할 것이다. 따라서, 디지털 포렌식에서 사회과학 및 법학적 측면의 접근을 하면서 디지털 기술을 융합하는 학문적 연구가 절대적으로 필요하다. 즉, 빠르게 변화하는 첨단 IT기술과 이를 법제 표준에 적용할 수 있는 법학분야를 융합하여 연구를 하는 것이 필요하다.

본 논문에서는 이공분야 관점의 디지털 포렌식 기술이 객관적으로 증명되어 법제 요구사항을 충족시킬 수 있도록 체계적인 디지털 포렌식 시스템 구축을 위한 기술적, 정책적 통합 프로세스 정립에 대해 연구하고, 정부의 미래 ICT R&D 중장기 전략과 ICT 패러다임 변화를 반영하여 급변하는 ICT 기술과 정책이 연계되어 융합되는 연구추진 방안을 검토한다. 이러한 검토를 바탕으로 디지털 포렌식 표준정립을 위한 기술-정책적 통합 프로세스 프레임워크의 일례를 제안하여 향후 기술과 정책이 융합되는 방안을 제시한다.

Ⅱ. 디지털 포렌식 관련연구

2.1. 디지털 포렌식 절차

디지털 포렌식은 크게 증거 수집, 증거 분석, 증거제출 절차로 이루어진다. [그림 1]과 [표 1]에 보인 바와 같이 디지털 포렌식 절차는 증거 수집을 위한 사전단계에서 부터 증거 수집과 증거 분석 및 데이터 복구, 결과에 대한 보고서 작성까지의 절차이다[1].

그림 1. 디지털 포렌식 절차[1]
Fig. 1 Digital Forensic Process

표 1. 디지털 포렌식 절차 및 기술[1]
Table. 1 Digital forensic process and technology[1]

Process		Content and Technology
Prior evidence collection step	-Establish application plan for Professional Manpower Training and forensic tool -Establish plan for continuity of storage -Establish plan for maintain of data integrity	-Expert who has knowledge of various operating system and file system, network, data base, and accounting system should be educated about digital forensic. They attend as an investigator to collect the evidence with speed and accuracy by using specialized tools. -Establish the detailed plan to prove that the evidence is not destroyed and show that the evident is integrity by obtaining some information such as person who has the evidence, time, and reason why taking the evidence.
Evidence collection step	-Priority of volatile evidence collection -Make a decision whether to power down or not -Flexible action for evidence collection object -Evidence collection	-Data should be read from storage media (computer memory, hard disks, USB, etc) for digital evidences, which can be easily damaged and lost, with a guarantee of the integrity of the data.(Integrity: It means that data modulation is not caused by raw storage media.) -One of useful technique for evidence collection is Imaging technique guaranteeing integrity
Evidence analysis step	-Data recovery -Evidence analysis	-Useful information should be extracted from the data obtained from evidence collection. -Useful information can usually exist inside or outside the file system of storage media. For example, criminals can hide important information inside the NTFS or in the blocks which are not used by the NTFS. -Recovery technique for deleted files, decoding of encrypted files, and string Searching technique are useful techniques for evidence analysis.
Evidence submission step	-Write final report -Evidence submission	-Reliability of evidence data should be secured so that the impounded digital evidences are chosen as legal evidences. -Legal standard procedure for digital forensic and verification procedure for forensic tools should be made.

디지털 포렌식의 분석대상에 따라 다음과 같이 몇 가지 포렌식 유형으로 분류할 수 있다.

표 2. 디지털 포렌식 분석대상에 따른 유형
Table. 2 Digital forensic types according to analysis objects

Type	Content
Computer forensic	Digital forensic for a general-purpose computer using Windows or Unix as operating system
Embedded (moblie) forensic	Digital forensic for various device such as mobile device (e.g. smart phone), digital camera, camcorder, or PDA
Network forensic	Forensic for collecting and analyzing data such as network information, user log, and internet browsing history from communication device in case of communication by computer of smartphone

2.2. 디지털 포렌식 시스템 및 분석 툴

현재 상용화되어 있는 컴퓨터 포렌식 증거 수집 및 분석 소프트웨어는 Guidance Software사의 EnCase와 AccessData사의 ForensicToolkit이 가장 널리 사용되고 있다. Paraben사는 모바일 기기에 대한 전문 분석가들을 위해서 Cell Siezure, PDA Siezure 등의 소프트웨어와 각종 휴대용 기기와의 연결을 지원하는 툴박스 형태의 상용 제품을 제공하고 있으며, 메모리를 직접 분석할 수 있는 소프트웨어도 개발하여 제공한다. 디지털 포렌식 툴 중에서 컴퓨터 포렌식 툴의 현황은 [표 3]과 같다[2].

2.3. 디지털 포렌식 시스템 및 분석 툴

디지털 포렌식 법률 체계는 개별적인 법률의 단순한 집합이 아니라, 디지털 증거의 적법성 확보와 디지털 포렌식 기술 활용과 관계된 법 목표들의 유기적인 체계로 구성되어 있다. 현재 디지털 포렌식 법률 체계의 구성요소들에 대해 국외 법제 현황과 국내 법제 현황을 비교함으로써 국내 법제에 요구되는 사항들을 분석하여 정리하면 [표 4]와 같다[3].

Ⅲ. ICT 패러다임변화를 반영하는 기술-정책적 통합프로세스

현재 디지털 포렌식의 분류는 분석 대상에 따라 디스크 포렌식, 시스템 포렌식, 네트워크 포렌식, 인터넷 포렌식, 모바일 포렌식, 데이터베이스 포렌식, 암호 포렌식, 회계 포렌식 등 8개로 분류 할 수 있다. 그렇지만 현재 웹기술의 발전(웹 메일, 블로그, 카페, SNS, 클라우드 컴퓨팅)으로 증거데이터 수집의 어려움이 있으며, 분석대상 장치의 증가, 저장장치의 용량증가, 운영체제(OS)와 파일 포맷(file format)의 증가)로 데이터간 연관관계 분석을 위한 데이터 추출, 분석시간 및 비용 증가하고 있다. 또한, 안티 포렌식 솔루션(데이터 완전 삭제(wiping), 데이터 암호화(encryption), 데이터 은닉

표 3. 컴퓨터 포렌식 툴의 현황 분석
Table. 3 Analysis of computer forensic tools

Tool	Operating system	Possibility to open to the public1	Image creation and test2	Integrity test3	Low level recovery4	Additional facility5
ForensicX	Unix/ Linux	Com	Disk, OS, Traffic	Hard, File, Finger	Delete	Plug, Report
Mares Ware	Windows	Com	Disk	Hard, File		
	Linux	Ccom	Disk	File		
The Coriner's Toolkit	Unix/ Linux	Free	Disk	Hard	Delete, Key	
Tom's Rootboot	Linux	Free	Disk, OS			Boot
EnCase	Windows	Com	Disk, OS	Hard, File, Finger	Raw, Delete	Plug, Report
Byte Back Ⅲ	Windows	Com	Disk, OS, Traffic	Hard, File	Raw, Delete	
ForensicToolkit	Window	Com	Disk	Hard, File	Raw, Delete	Report

1. Possibility to open to the public: Com(common use), Free(public)
2. Image creation and test: Disk(disk image), OS(operating system image), Traffic(IP traffic image)
3. Integrity test: Hard(change of hardware test), File(file integrity test), Finger(electrical finger print test)
4. Low level recovery: Raw(low level file edit), Delete(deleted file recovery), Key(encrypted key recovery)
5. Additional facility: Boot(emergency booting support), Plug(plug-in support), Report(automatical report support)

표 4. 디지털 포렌식 법률체계의 구성요소와 국내 법제에 요구되는 사항
Table. 4 Element of digital forensic legal system and requirements in domestic forensic law

Division	Legal system component	Internal law requirement based on international law current state
Section for digital forensic, digital investigation fundamental law principle, and people's fundamental human rights	①Constitution	- Warrant requirement and legal process principles are stated in the Constitution of the Republic of Korea.
	②Privacy/Personal information secure law	- Establishment for unified personal data protection law is required to minimize invasion of people's privacy in pursuance of digital evidence collection and analyze.
Section for digital evidence admissibility	③Digital evidence concept acceptance	- Digital evidence concept and characteristic should be included in the civil procedure, criminal procedure, and the rest of related laws.
	④Digital evidence admissibility	- Legal standards or procedures are required to prove that digital evidence is same as documentary evidence in the law of criminal procedure.
	⑤Digital evidence collection · analysis procedure	- Standard procedure is required as the law to prove that collected digital evidence is not forged and falsified during collecting and analyzing processes.
	⑥Electronic signature law	- Electronic signature is utilized to obtain the admissibilities of digital evidence and digital document certification. A legal basis is required to establish and operate the digital evidence certification center by utilizing PKI system.
Section for digital investigation principles in investigation · intelligence agencies	⑦Digital investigate procedure	- Law for standardized principle and procedure related in digital evidence collection and analysis is required.
	⑧Digital communication monitoring	- Digital communication between computers monitoring should be included in the protection of communications secrets law.
	⑨Encrypted evidence handling	- Institutional and technically procedure is required as the law to decode timely the legally collected encrypted data
Section for digital forensic application in investigation · intelligence agencies	⑩Criminal investigation, anti- terrorism, intelligence	- Article that is demanded for application of digital forensic technology in the legislative systems of criminal investigation, anti-terrorism, and intelligence should be supplemented
Section for cooperative work between investigation · intelligence agencies and private enterprise	⑪Digital communication monitoring support	- Communication monitoring support of ISP for secure the effective digital communication data evidence should be arranged as the law
Digital forensic application promotion of private enterprise	⑫E- Discovery	- E-Discovery article should be supplemented in the civil procedure law
	⑬Various compliance	- Digital forensic technology requirement should be supplemented in various compliance
	⑭Financial auditing	- Article that is demanded for application of digital forensic and forensic accounting technology in the digital audit law should be required in audit law such as external audit system law
	⑮Industrial security	- Requirement of digital forensic technology application should be supplemented in legislative system for industrial secret secure
	⑯Anti-insurance fraud	- Requirement of digital forensic technology application should be supplemented in legislative system for anti-insurance fraud
Section for create a healthy digital forensic technology utilizing environment	⑰Digital forensic · prevention of adverse effect of anti forensic technology	- A article that someone who tries to abuse or doesn't have a properly authorization of digital forensic tool and anti-forensic tool suffers additional punishment should be arranged
Section for digital forensic research support and invigorate the industry	⑱Digital forensic research and industry promotion	- Digital forensic technology research support article should be arranged and logical basis about digital forensic research center and digital evidence analysis center should be provided - In addition, promotion bill of digital forensic private industry and prevention law of adverse effect of digital forensic technology should be arranged - Obligation of digital forensic education and manpower training support article should be arranged. In addition, article to prevent invasion of people's privacy by using digital forensic technology should be arranged

(steganography) 증가에 따른 데이터 증거수집의 어려움이 있다.

특히, 스마트폰의 사용이 급증하고, 다양한 스마트폰 OS가 존재하며, 250,000개 이상의 어플리케이션이 존재함으로 인해 모바일 포렌식의 한계점을 노출하고 있다. 모바일 포렌식의 한계점은 모든 OS와 어플리케이션에 대한 포렌식은 현실적으로 어려움이 있으며, 데이터 추출을 위한 표준화된 프로토콜이 존재하지 않기 때문이다.

즉, 적절한 다중시스템 또는 보조적인 클라우딩 컴퓨팅과 같은 환경을 효과적으로 이용함으로써 대용량 디지털 포렌식 서비스 시간 단축과 분석의 효율성을 추구하는 IT융합연구 체계정립이 필요하다. 또한 SW 패러다임 변화 및 5개 분야(콘텐츠(C)-플랫폼(P)-네트워크(N)-디바이스(D)-정보보호(S))를 밀접하게 연계시키는 스마트 융합시대에 부합하는 정부의 ICT R&D 중장기 전략(ICT WAVE 전략)을 고려한 디지털 포렌식 표준정립을 위한 기술-정책적 통합 프로세스의 고려가 필요하다.

따라서 본 논문에서는 다중시스템이나 클라우딩 컴퓨팅 환경 등의 첨단 IT기술을 접목하는 디지털 포렌식 표준정립을 위한 기술-정책적 통합 프로세스를 제안한다. 이를 위해서 현재 정부에서 추진하고 있는 IT정책의 동향을 고려하고 각 기관과의 효율적이고 신속한 처리가 가능한 통합프로세스를 제안한다.

3.1. 정부의 ICT R&D 중장기 전략

현재 정부는 '창조경제'라는 키워드를 바탕으로 "창조경제는 국민 개개인의 상상력과 창의성을 과학 기술과 ICT에 접목해 산업과 산업, 산업과 문화 콘텐츠와의 융합과 창업을 통해 지금까지 없었던 새로운 산업과 시장, 새로운 일자리를 만드는 것" 이라 설명하고 있다[4]. 또한 창의와 혁신으로 반드시 정보통신(ICT) 최강국을 만들겠다"는 목표하에 IT분야 공약을 발표하여, 건강한 정보통신 생태계 조성을 통한 창조경제 기반 구축, 콘텐츠산업의 집중 육성, 방송의 공공성 강화 및 미디어 산업의 핵심으로 육성, 통신비 부담 완화, 전담 부처 신설 적극 검토 등을 공약으로 제시하였다(2012. 10월 정보통신 최강국 실현을 위한 5대 전략 발표)[5].

미래창조과학부는 2013년 10월 23일 열린 제23차 경제관계 장관회의에서 이 같은 내용을 담은 '정보통신기술(ICT) 연구개발(R&D) 중장기 전략(일명 ICT WAVE 전략)'을 확정했다고 밝혔다. 미래부는 'ICT WAVE 전략'으로 창조경제 성장잠재력을 확충할 수 있도록 (W)세계 최고의 ICT 경쟁력 확보(World best ICT), (A)연구 환경의 획기적 개선(Activating R&D ecology), (V)산업적 성과창출(Vitalizing industry), (E)국민 삶의 질 개선(Enhancing life)이라는 4대 비전을 제시하고 향후 5년내 기술 상용화율 35%(현재 18%), ICT R&D 투자생산성 7%(현재 3.42%), 국제 표준특허 보유 세계 4위(현재 6위) 달성을 목표로 설정하였다.

이 전략은 미래부는 향후 5년간 ICT분야 R&D 중점개발 분야와 향후 서비스 추진 방향을 제시한 것으로 세계 최고 경쟁력 유지와 연구환경 개선, 산업적인 성과창출, 삶의 질 개선 등 4가지 목표를 담고 있다. 이 전략에 따르면 정부는 향후 5년내 기술 상용화율 35%(현재 18%), ICT R&D 투자생산성 7%(현재 3.42%), 국제 표준특허 보유 세계 4위(현재 6위) 달성을 목표로 설정했다.

이를 위해 콘텐츠(C), 플랫폼(P), 네크워트(N), 디바이스(D), 정보보호(S) 등 5개 분야에서 10대 핵심기술을 개발해 신성장동력으로 육성하고 글로벌 시장을 선점해 나갈 방침이다. 향후 5년내 기술 상용화율 35%(현재 18%), ICT R&D 투자생산성 7%(현재 3.42%), 국제 표준특허 보유 세계 4위(현재 6위) 달성을 목표로 설정했다. 이를 위해 콘텐츠(C), 플랫폼(P), 네크워트(N), 디바이스(D), 정보보호(S) 등 5개 분야에서 10대 핵심기술을 개발해 신성장 동력으로 육성하고 글로벌 시장을 선점해 나갈 방침이다.

이를 기반으로 하는 15가지 대표 미래 서비스를 중점 구현할 계획이다. 특히 모든 산업 고부가가치화, 신산업 창출, 소통/협업 등에 기여할 수 있는 창조경제 실현 도구(Enabler)로서 SW를 집중 육성할 계획이다. SW R&D 투자를 확대하고 공개 연구강화, 기초원천 SW분야 연구확대 등 특성에 부합되는 R&D 전략을 추진한다고 제시하였다. 또한 ICT 특별법에 근거하여 총리실에 설치('14.2월)되는 정보통신전략위원회 산하에 '정보통신융합 전문위원회'를 구성하여 범부처 과제 발굴 및 의견 조율을 추진하고, ICT R&D 정책→기획・평가・관리→사업화의 R&D 全주기 지원체계를 확립하기 위해 정보통신기술진흥원(전담기관)을 재구성하는 방안 등을 기재부 등과 협의하여 추진하기로 하였다.

표 5. 정부의 ICT R&D 중장기 전략의 5대 분야 10대 핵심기술 개념[5]
Table. 5 5 Categories and 10 core technologies of government leading ICT R&D mid-Long term strategy

Field	Technology	Concept	Ripple effect
Contents	hologram	The technology that enables full dimensional 3D media to produce, compressive transport, and diplay into the huge screen	-Lead media content new paradigm -Respond $4billion world market in 2022
	content 2.0	Collaborative production technique based on cloud for creating and distributing open type·participatory contents	-Promote collaborate works between small scale developers -$2.1trillion world market in 2016
Platform	intelligent SW	Software technology that can recognize, decide, and express(conversation or gesture) as a human	-Utilize native language education -Respond $245.5billion world market in 2020
	Internet of Everything (IoT) Platform	Super-connected service platform inter-connected various devices by internet	-Rear creative small scale service industry -Respond $1.9trillion world market in 2020
	big data·cloud	Information generating and service supporting technologies based on massive data	-Utilize for solving various social issues -Respond $300billion world market in 2017
Network	5th generation (5G) mobile telecommunication	Mobile communication original technology that is 1000 times faster than present technology and radio propagation applied technology	-Lead mobile communication new technology·market -Respond $7.64billion world market in 2017
	smart network	100Gbps optimized network service support technology based on software	-Future high qualified service infrastructure -Respond $2.1billion world market in 2017
Device	emotional device technology	Context-aware mobile using technology utilized user's five senses	-Lead new concept smart device development -Respond $235.1billion world market in 2020
	intelligent ICT convergence module	Core sensing technology for realizing ICT convergence new technology	-Secure core technology of convergence of other industries -Respond $120billion world market in 2017
Data secure	cyber attack reaction technique	New cyber security threat detecting and real time acting technologies	-Minimize cyber attack damage -Respond $44.2billion world market in 2017

또한 융합형 R&D 기획강화로 타부터 연계형 R&D 강화전략, 과학기술-ICT 융합, 협업 R&D 확대 등의 전략을 수립하였다. 즉, 총리실 정보통신잔략위원회 산하에 '(가칭)정보통신융합전문위원회'를 설치하여 부처간 의견 조율 및 과제 기획 추진할 계획으로 수요조사, 기획, 사업계획 검토 등 과제운영 과정에 수요부처 추천 전문가 및 관련기관이 참여하고, 미래서비스 조기구현을 위한 '범부처 협업 R&D 프로그램'을 추진할 계획이다. 즉, 정부의 ICT R&D 중장기 전략을 분석하여 보면, 정부는 창조경제의 근본적인 개념인 '국민 개개인의 상상력과 창의성을 과학 기술과 ICT에 접목해 산업과 산업, 산업과 문화 콘텐츠와의 융합과 창업'이라는

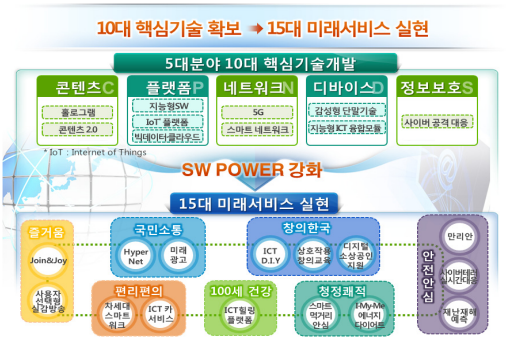

그림 2. 정부의 ICT R&D 중장기 전략[5]
Fig. 2 Government leading ICT R&D Mid-Long term Strategy

의미에 부합하는 ICT가 근간의 'ICT융합 전략'이라고 할 수 있다. 따라서 본 논문에서는 정부의 ICT WAVE 전략과 부합하는 ICT융합 전략을 고려하여 ICT기술의 발전방향과 정책의 변화 흐름을 반영하고, ICT 패러다임의 변화를 반영하는 디지털 포렌식 기술-정책 통합 프로세스의 프레임워크를 제안한다.

3.2. ICT패러다임변화와 ICT R&D 중장기 정책변화

현재 정부는 '창조경제'라는 키워드를 바탕으로 "창조경제는 국민 개개인의 상상력과 창의성을 과학 기술과 ICT에 접목해 산업과 산업, 산업과 문화 콘텐츠와의 융합과 창업을 통해 지금까지 없었던 새로운 산업과 시장, 새로운 일자리를 만드는 것" 이라 설명하고 있다[6]. 또한 창의와 혁신으로 반드시 정보통신(ICT) 최강국을 만들겠다"는 목표하에 IT분야 공약을 발표하여, 건강한 정보통신 생태계 조성을 통한 창조경제 기반 구축, 콘텐츠산업의 집중 육성, 방송의 공공성 강화 및 미디어 산업의 핵심으로 육성, 통신비 부담 완화, 전담 부처 신설 적극 검토 등을 공약으로 제시하였다(2012. 10월 정보통신 최강국 실현을 위한 5대 전략 발표)[6]. 또한 미래부에서는 ICT 중장기 전략을 확정 발표하였다.

그림 3. 7대 미래국가사회 수요와 15대 미래서비스 선정현황[5]
Fig. 3 7 Future society needs and 15 Future services

또한 창조경제를 구현하기 위한 큰 축이 바로 과학기술과 ICT라고 강조하고 있으며, 창조경제 실현을 위한 국정과제로 'IT · SW 융합을 통한 주력산업 구조 고도화', '세계 최고의 인터넷 생태계 조성', '정보통신 최강국 건설', '창업 · 벤처 활성화를 통한 일자리 창출' 등을 제시하고 있다[7].

이러한 정부의 ICT R&D 중장기 전략은 인터넷의 급속한 확산과 웹의 플랫폼화 진전과 다양한 OS, 서비스 플랫폼 사업자의 등장으로 기존에 비해 ICT산업의 서비스 경쟁력과 SW 기술력의 중요성이 증대되고 있는 상황을 반영한 정책수립이라고 볼 수 있다. 특히 이러한 인터넷 호나경의 변화는 SW산업의 서비스 산업화로의 확대를 야기하여 XaaS(~as a Service)개념이 확산되고 있어, SW산업정책과 서비스산업정책 및 규제간의 경계가 와해되고 있다. 이러한 변화는 기존의 제조 및 HW중심적인 전략/정책에서 SW중심 전략/정책으로 이동하고 있는 추세이고, SW산업의 다양성과 융복합화를 반영할 수 있는 통섭적인 시각의 필요성이 증대하고 있음을 반영한다.

현재 정부의 ICT R&D 중장기 전략은 기존의 ICT정책 현황은 지난 2~3년간 인터넷의 급격한 변화에 의한 다양한 ICT 패러다임의 변화에 따른 정책적 변화의 필요성을 반영한 결과이다. 이러한 결과는 정보통신정책연구원에서 제시하는 ICT 패러다임의 변화(인터넷이라는 네트워크를 통하여 통신, 방송, 미디어를 흡수함을 물론이고, 글로벌 ICT 기업들의 자체 플랫폼을 통하여 시장을 선점하려는 상황으로 이에 대한 기존의 법, 제도, 규제의 변화가 불가피함)를 반영한 것으로 분석된다[7].

3.2.1. 인터넷에 의한 SW, 네트워크 패러다임변화에 의한 전략 정책의 변화

스마트 산업생태환경은 인터넷/웹이 핵심적인 요소인데, 이는 클라우딩 컴퓨팅의 이용의 확대되면서 SW 부문에서의 구조적인 변화가 진행되고 있다. 특히 클라우딩 컴퓨팅환경의 도래와 SNS(소셜네트워크서비스)의 활성화로 기존의 프로세스로는 해결할 수 없는 많은 문제들이 산재해 있다. 클라우드 컴퓨팅은 인터넷을 이용하여 가상의 IT 자원을 제공하여 다양한 단말기기(PC, 노트북, 태블릿PC, 스마트폰 등)를 통해 정보에 접근할 수 있는 환경이기 때문에, 클라우드 컴퓨팅은 범죄의 객체, 주체가 될 수도 있고, 범죄의 수단으로 이용될 수도 있다. 해커가 CSP(Cloude Service Provider)를 대상으로 DDOS 공격을 행한 경우나, 타인의 클라우드에 존재하는 데이터를 삭제, 저작권 파일공유 등 다양한 범죄의 주체가 될 수 있다. 이러한 클라우드 컴퓨팅 서비스 유형은 IaaS(Infrastructure as a Service), Paas (Platform as a Service), 및 SaaS(Software as a Service)

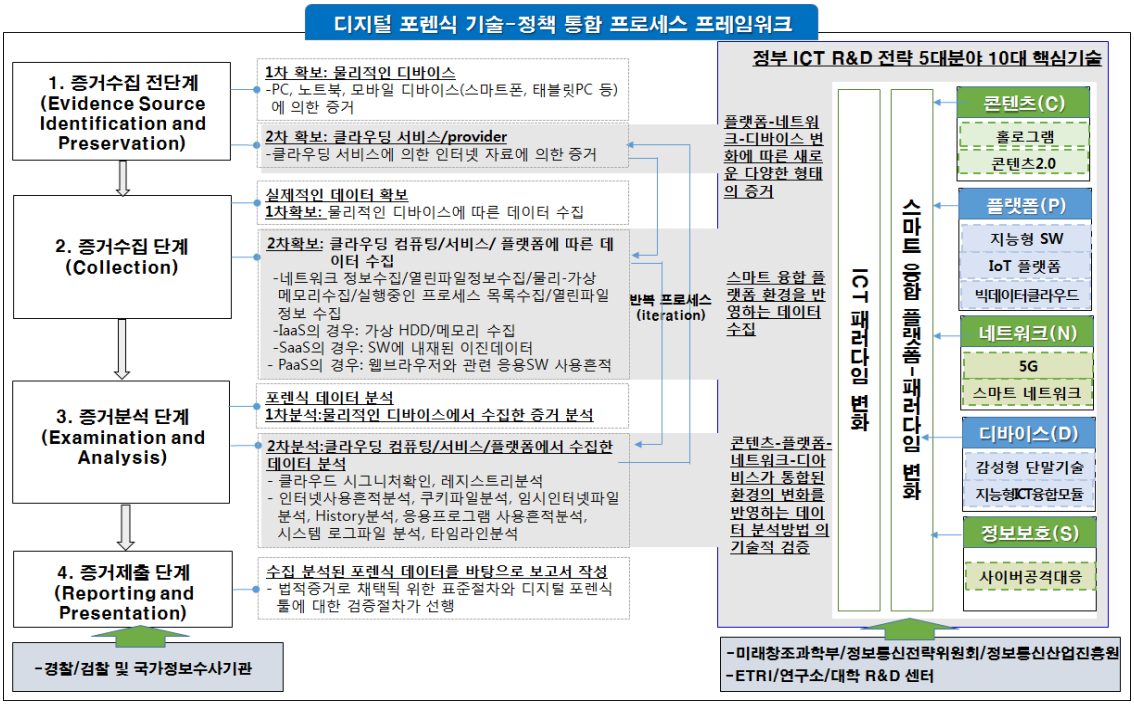

그림 4. 제안하는 국내의 IT융합기술의 발전방향 및 정책에 부합하는 기술-정책 통합프로세스 프레임워크
Fig. 4 Proposed technology-strategy integrated process framework complying IT-conversion technology trend and strategy

로 구분할 수 있고, 배치모델에 따라 사설 클라우드와 공공 클라우드로 분류할 수 있다.

특히 SW 부문의 패러다임의 변화는 기존의 네트워크 서비스, 콘텐츠, 어플리케이션 등 스마트 산업생태환경의 핵심적인 요소가 SW를 중심으로 통합되는 방향으로 전개되고 있고, 이에 따라 전략적, 정책적인 결정이 필요하다. 현행 '소프트웨어산업 진흥법'은 클라우딩 컴퓨팅, 인터넷/웹의 SW 플랫폼화, 새로운 SW 변화 등의 SW 패러다임 변화를 반영하지 못하고 있어서 클라우드 컴퓨팅 환경의 특징에 적합한 새로운 SW 패러다임 변화를 반영한 IT기술이 융합된 기술-정책 프로세스의 정립이 필요하다.

3.2.2. C-P-N-D가 연계된 디지털 스마트 융합플랫폼에 의한 패러다임 변화

최근 인터넷을 기반으로 콘텐츠(C)-플랫폼(P)-네트워크(N)-기기(D)를 밀접하게 연계시키는 글로벌 비지니스 모델이 성공하면서 콘텐츠 산업의 새로운 생태계 등장이 가속화되고 있다. 그렇지만 국내는 온라인/모바일 콘텐츠 유통 플랫폼 구축을 위하여 노력하고 있지만, 여전히 플랫폼과 응용 SW의 기술수준이 취약하고 불공정 콘텐츠의 유통 등으로 스마트 융합시대에 적극적으로 대처하지 못하고 있다. 이를 해결하기 위해서 정부에서 제시한 ICT R&D 중장기 전략에서와 같이 C-P-N-D가 연계된 디지털 ICT 스마트 융합플랫폼에 의한 패러다임의 전환을 반영한 기술적/정책적 전략수립이 필요하다.

3.3. 정부의 ICT R&D 중장기 전략에 부합하는 디지털 포렌식 기술-정책 프로세스 프레임워크

본 논문에서는 정부의 ICT R&D 중장기 전략과 ICT 패러다임의 변화를 반영하여 국내의 IT융합기술의 발전 방향 및 정책에 부합하는 디지털 포렌식 기술-정책 통합프로세스 프레임워크를 제안한다. 그림 4에 제시한 바와 같이 참고문헌 [8]에서 정립한 디지털 포렌식 절차를 바탕으로 하여 국내환경과 정부의 정책을 반영하고

미래 ICT기술을 반영한 프레임워크 모델을 제안한다.

제안하는 국내의 IT융합기술의 발전 방향 및 정책에 부합하는 디지털 포렌식 기술-정책 통합프로세스 프레임워크에서 알 수 있듯이, 기존에 물리적인 디바이스에 의한 포렌식 증거수집에서 클라우딩 컴퓨팅환경과 나아가서는 콘텐츠(C)-플랫폼(P)-네트워크(N)-디바이스(D)-정보보호(S)가 연계된 스마트 융합 플랫폼의 변화를 반영할 수 있는 방안을 제시하였다. 그림 4에서는 클라우딩 컴퓨팅/서비스/플랫폼에 따른 단계별 세부 고려사항만을 제시하였지만, 향후 기술발전과 스마트 융합 플랫폼의 변화에 따라 변화하는 각 포렌식 단계별로 정책방향을 제시하였다.

예를 들면, 그림 4의 증거수집단계에서는 현재 2차 데이터 확보를 위하여 클라우딩 컴퓨팅/서비스/플랫폼에 따른 데이터 수집을 기존의 방식인 물리적인 디바이스에 의한 데이터 수집방법에 추가하여 제시하였다. 그렇지만, 향후에는 콘텐츠-플랫폼-네트워크-디바이스의 통합 플랫폼의 변화와 같은 ICT 기술발전을 반영하여 데이터 수집형태, 수집종류, 수집방법에 대한 기술적 해결방안과 정책적 해결방안을 제시하는 것이다. 이러한 과정은 정부와 관련기관 및 대학/연구소의 R&D 결과와 정책결정에 의하여 신속하게 반영될 수 있도록 해야 할 것이다.

또한 증거분석 단계나 증거제출 단계에 있어서도 클라우딩 컴퓨팅/서비스/플랫폼 환경은 물론이고 지속적으로 변화하고 있는 스마트 융합 플랫폼을 반영할 수 있도록 정부와 R&D 연구센터 및 관계기관의 다각적인 융합협조체제를 구축할 필요가 있다. 현재에도 이러한 시도는 ICT R&D 중장기 전략에서 제시하였지만, 디지털 포렌식 표준정립을 위한 체계적인 분석이 더욱 요구된다. 따라서 본 논문에서 제안한 디지털 포렌식 기술-정책 통합프로세스 프레임워크를 기반으로 기술과 정책이 융합되어 효율적이며 신속한 디지털 포렌식 법제체제와 표준정립에 기여할 것이다.

또한, 정부에서는 2013년 5월부터 디지털 포렌식 기술을 범죄 수사에 직접 활용할 수 있도록 국민 복지·안전 수요해결형 연구개발 사업(공공복지안전연구사업)의 일환으로 '디지털 기반 첨단 과학수사 요소기술 개발 과제'를 마련하여 추진하고 있다. 따라서, 본 논문에서 제안한 기술-정책 통합프로세스 프레임워크와 연계한다면, 미래 ICT 패러다임 변화와 기술변화에 능동적으로 반영하는 디지털 포렌식 프로세스를 정립하는 데 기여할 것으로 예상된다.

Ⅳ. 결 론

본 논문에서는 디지털 포렌식 기술이 객관적으로 증명되어 법제 요구사항을 충족시킬 수 있도록 체계적인 디지털 포렌식 시스템 구축을 위한 기술적, 정책적 통합 프로세스 프레임워크를 제안하였다. 특히 정부의 ICT R&D 중장기 전략과 스마트 융합플랫폼 패러다임 변화를 반영하여 급변하는 ICT 기술과 정책이 연계되어 융합되는 기술-정책 통합프로세스 프레임워크의 방안을 제시하였다. 특히 클라우딩 컴퓨팅환경을 고려한 디지털 포렌식 프로세스를 한 일례로 제시하였고, 이를 바탕으로 콘텐츠(C)-플랫폼(P)-네트워크(N)-디바이스(D)-정보보호(S)가 연계된 스마트 융합 플랫폼의 변화를 반영할 수 있는 방안을 제시하였다. 본 논문에서 제시한 프레임워크를 기반으로 미래 ICT 패러다임 변화와 기술변화에 능동적으로 반영하는 디지털 포렌식 프로세스를 정립하는 데 기여할 것이다.

감사의 글

본 연구는 2012년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2012S1A5A2A01014422)

REFERENCES

[1] S. D. Jeon, D. S. Hong, G. J. Han, "Technologies prospect and Trends of Digital Forensics," National Information Society Agency, *Informatization policy,* Vol. 13, No. 4, pp. 3-19, 2006.

[2] I.R. Jeong, D.W. Hong and K.I. Chung "Technologies and Trends of Digital Forensics," Electronics and telecommunications, Vol. 22, No. 1, pp. 97-104, 2007. 2.

[3] S. J. Baek, M. N. Shim and J. I. Lim, "National Digital Forensics legal system and Digital Forensics law of Domestic and Foreign," *Journal of the Korea Institute of*

Information Security and Cryptology, Vol. 18, No. 1, pp. 49-61, 2008. 2.

[4] Available on http://www.korea.kr/policy/economyView.do?newsId=148759211&call_from=koreagov

[5] "ICT R&D mid & long-term Policy," Ministry of Science, ICT and Future Planning , 2013. 10.

[6] Available on http://incheon.saenuriparty.kr/xe/index.php?document_srl=422840&mid=subSnrpP3_6

[7] G. Y. Choi and etc., "The change of ICT paradigm and mid & long-term political subject," KISDI Premium Report, 2012.

[8] Ben Martini, Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing", Digital Investigation, 2012.

신준우(Jun Woo Shin)

1996년 2월 : 숭실대학교 경영학과 학사
2002년 2월 : 성균관대학교 정보통신공학과 공학석사
2010년 2월 : 고려대학교 정보관리 공학박사
1996년 2월 ~ 현재 : 정보통신산업진흥원
※관심분야 : 디지털 포렌식, 인력양성, ICT R&D