Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1129

포털 전자메일 압수수색을 위한 메일헤더기반 디지털포렌식*

이 해 진,† 손 태 식‡
아주대학교

E-mail Header-Based Search and Seizure for Internet Portal Digital Forensics*

Hae-Jin Lee,† Tae-Shik Shon‡
Ajou University

요 약

인터넷의 보급과 다양한 디지털기기의 발달에 따라 전자정보의 양은 급격하게 증가하고 있다. 전자정보 중에서 본인이 직접 소지하지 않는 포털사 전자메일과 같은 제3자 보관 전자정보 압수수색은 지속해서 증가하고 있으며 재판에 증거로도 사용되고 있다. 그러나 현행 압수수색 방식은 압수 기간만 산정한 뒤 전체 전자메일에 대하여 무분별하게 압수수색을 진행하고 있으며 압수수색 결과에 대한 통보 부재와 같은 많은 문제점이 있어 압수수색 절차를 살펴보고 그 개선점에 대해 제시하였다.

ABSTRACT

In accordance with the spread of the Internet and the development of various digital devices, the amount of electronic information is rapidly increasing. Selection of electronic information seizure searches continues to increase for third parties, such as portal sites e-mails that persons do not possess directly from the electronic information, and it is also used as evidence in court. However, the current method of searching for houses has many problems such as the absence of notice of seizure search result, seizure searches are proceeded indiscriminately against whole e-mail after calculating only during the seizure period, and seizure search procedure And presented the improvement points.

Keywords: Digital forensics, e-mail seizure search, infringement of privacy

I. 서 론

인터넷의 보급과 다양한 디지털기기의 발달에 따라 디지털 정보의 양은 빅데이터 시대라 부를 만큼 빠른 속도로 늘어나고 있다. 이에 따라 수사기관에서 압수하는 디지털기기와 정보의 양도 증가하고 있다. 이는 모든 분야의 범죄 수사에서 디지털 흔적 즉, 전자정보[1]를 얼마나 잘 찾아내어 복구, 분석하는가에 따라 수사의 성패가 달려 있다고 해도 과언이 아닐 만큼 중요한 하나의 수사 형태로 자리 잡았다.

이러한 전자정보는 일반 유체물 형태의 압수물과 다르게 별도의 장치를 통하여 인식하여야 하고, 작성

Received(06. 05. 2018), Modified(07. 23. 2018), Accepted(07. 30. 2018)
* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-01000, 디지털 포렌식 통합 플랫폼 개발)
† 주저자, luckyhaejin@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

1) 학계에서는 디지털 증거, 디지털 기록 등 다양한 용어를 사용하고 있지만, 본 논문에서는 최근 대법원에서 사용하는 '전자정보'라는 용어로 통일한다.

자의 의도와 관계없이 시스템에 의해 자동 생성·저장되는 정보가 있으며, 양이 일반 종이와 같은 전통적인 매체와 비교할 수 없을 만큼 방대하며, 통신망을 통해 전송되는 등 기존의 일반 유체물 압수와는 다른 특성을 보이고 있다.

전자정보의 경우 대량성, 네트워크성, 비가독성 등의 특성으로 인하여 압수한 전자정보의 내용이나 송·수신이 완료된 전자메일을 직접 열람하기 전까지는 해당 사건과 연관성을 확인하기 어렵다.

이러한 특수성으로 인하여 지금까지 전자정보의 압수수색에 있어 과도한 기본권, 사생활 등을 침해한다는 우려가 많이 있었다. 법률에서도 이러한 부분을 엄격히 규율할 필요가 생겼고, 2011. 7. 18. 신설된 「형사소송법」 제106조 제3항, 제4항, 제14조 제1항 단서 등 이에 관한 규정이 새로이 도입되었다[1].

전자정보는 본인이 직접 소지하고 있는 컴퓨터, 모바일 기기 등에 저장된 정보의 형태도 있지만, ①로그형태, ②메시지형태, ③가상공간 저장형태는 정보통신 서비스제공자[2]와 같은 사건관계인이 아닌 제3자가 보관하고 있는 전자정보도 존재한다. 이러한 제3자 보관 전자정보[3]의 경우 압수수색에 관하여 규정된 바가 없어, 수사기관별로 방법과 절차가 다르고 압수수색의 주체인 수사기관이 직접 참여할 수 없는 등 많은 문제점이 있다.

따라서 본 논문에서는 포털사 전자메일 압수수색에 대한 현행 절차와 그에 대한 문제점과 개선 방안에 대해 모색하였다. 본 논문의 2장에서는 국내에서 연구되고 있는 포털사 압수수색에 관한 연구사례를 살펴본다. 3장에서는 현행 인터넷포털 전자메일 압수수색 절차에 대해 분석하고 그에 따른 문제점에 대해 살펴본다. 4장에서는 3장에서 도출된 문제점을 개선하기 위하여 법제도 기반과 기술적 기반으로 나누어 새로운 압수수색 방식을 제안한다. 5장에서는 새롭게 제안한 압수수색 방식에 대한 검증을 위하여 실제 시나리오 기반으로 검증하고 토의를 진행한다. 마지막 6장에서는 본 논문에 대한 결론과 향후 추가 연구 방향에 대해 논의하고 논문을 마무리한다.

2) 정보통신서비스제공자란 「전기통신사업법」 제2조 제8호의 규정에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신 역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. LGU+와 같은 전기통신사업자와 네이버, 카카오와 같은 포털 사이트 운영자가 대표적이다.

3) 피의자 등 사건관계인이 아닌 은행이나 포털 사이트 업체가 보관하고 있는 전자정보로 금융계좌정보, 전자메일, 통신기록, 가입자 정보, 접속 Log, 게시글 등 특정 서비스 제공업체의 서버에 보관되는 정보이다.

II. 국내 전자메일 압수수색 관련 연구 동향

2.1 전자메일 압수수색 기간선정 부분

현재는 수사기관들이 수사상의 필요를 이유로 서버 전체에 대해 또는 전자메일계정 전체에 대해 영장을 청구하고 있고 법원은 기간을 한정하거나 여타의 방식으로 제한을 하고 있으나 검찰은 이에 대해 '월권행위'라고 비난하고 있다고 기술하고 있다[2]. 전자메일계정의 기간선정에 대한 제한의 문제점에만 초점을 맞추어 범죄와 연관된 기간을 명시하려는 방법은 제시되지 못한 한계가 있다.

2.2 전자메일 압수수색 기간선정 부분

압수수색을 위하여 정보통신서비스제공업체에게 영장 집행 시, 수사기관이 아닌 업체의 업무 담당자가 압수할 물건에 해당하는 자료를 수사기관 담당자 기관 메일로 회신한다.

자료를 수집하여 제공할 때 수사기관이나 피압수자가 전자정보 증거수집 시 참여하지 않았기 때문에 수집된 데이터에 대한 출처, 내용에 대한 검증 절차 없이 제3자가 제공한 데이터를 그대로 신뢰할 수 밖에 없다.

이러한 문제점 개선을 위하여 ①수사기관에 부여된 권한을 통해 직접 포털사 자료에 접근하여 수색하는 방안[3] ②제3자에 의한 필터링 제도 도입[4] ③온라인 수색제도의 도입[5] 이와 같은 개선안을 제시하였다. 위 3가지 개선안은 개념적인 측면에서는 좋다고 할 수 있겠지만, 실제적인 구현을 위한 제시가 부족하다는 한계점이 있다.

2.3 압수수색 결과 통지 부분

압수수색이 침해하는 기본권이 프라이버시이며 압수수색에 따른 영장 제시가 기본권 침해에 대한 적법절차로써 이루어지는 이상 헌법이 요구하는 적법절차의 원리를 충족시키기 위해서는 전자메일 압수수색도 압수수색이 이루어지는 시점에서 그 전자메일의 계정 소유자에게 압수수색 집행과 동시에 영장 제시나 통

지가 이루어져야 한다고 기술하고 있다.

제3자 보관 전자정보에서 참여권은 제3자 보관 전자정보의 압수 이후 피압수자에게 이를 구체적으로 통지함으로써 참여권을 대신할 수 있다. 이때, 어떤 정보가 압수되었는지 구체적으로 명시하여 피압수자가 자신의 전자정보가 언제 어떠한 이유로 압수되었는지 알 수 있게 해야 한다. 따라서, 압수 후 며칠 이내, 혹은 사건 송치 후 며칠 이내 등 구체적으로 통지해야 하는 기간과 통지 사유를 정하여 압수한 후 정해진 기간 내에 구체적으로 압수한 데이터를 명시하여 피압수자에게 압수가 이루어졌음을 통지해야 한다고 기술하고 있다[6]. 피압수자에게 통보되지 못하는 문제점만 언급 후 통보를 위한 구체적인 개선안이 제시되지 못한 한계점이 있다.

III. 현행 인터넷 포털 전자메일 압수수색 분석

3.1 압수수색 절차 및 과정의 문제점

수사기관에서 포털사 전자메일 압수수색을 위한 단계별 절차에 대해 세부적으로 살펴보고 단계별 문제점과 최근 판례를 통하여 개선안을 찾아본다.

가. 영장청구 단계

형사소송법 제215조 제1항[4]에서 볼 수 있듯이 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 영장을 청구해야 하지만, 전자메일 압수수색의 경우 기간만 산정한 뒤 기간에 해당하는 전체 자료에 대해 압수하는 영장을 청구하고 있다. 범죄와 연관된 것으로 추정하는 모든 기간에 송·수신된 전자메일에 대해 영장을 청구한다는 것이 문제이다.

아래 항목은 현행 검찰에서 청구하는 영장에서 압수할 물건의 예시이다.

〔별지1〕

압수할 물건

○ 피의자 허OO 관련

1. 피의자 허OO(70OOOO-1OOOOOO)이 사용하고 있는 LGU+ 휴대전화 010-2OOO-OOO와 관련된 LGU+ 제공 클라우드서비스(유박스등 명칭 불문)에 **2013. 6. 1. ~ 2017. 9. 24. 동안 저장된** 본건과 관련된 문서, 녹음파일, 사진 영상 등 자료 일체
2. 피의자 허OO(70OOOO-1OOOOOO)의 주민등록번호 또는 아래 본인인증 정보(CI, DI)와 연계된 네이버 등 포털사 또는 네이트등 통신사에서 제공하는 클라우드 서비스 서버에 **2013. 6. 1. ~ 2017. 9. 24. 동안 저장된** 본건 관련 문서, 녹음파일, 사진 영상 등 자료

나. 영장 집행 단계

압수수색 현장에서 피처분자에게 직접 영장 원본을 제시하도록 헌법 제12조 제3항[5]에 명시되어 있으나 금융계좌추적이나 제3자 보관 전자정보의 경우 FAX(모사전송)를 이용하여 영장을 집행하고 있다. 이러한 영장 집행 방법에 많은 논란이 있었으나 2017. 9. 7. 2015도10648[6] 대법원 판례에서는 FAX(모사전송)를 통한 영장 집행은 위법하지 않다고 판결하였다.

다. 포털사 회신 단계

전자정보의 관리 주체인 업무 담당자는 영장에서 압수할 물건에 해당하는 자료를 일반적으로 포털사 A, B는 3~5일, 포털사 C는 1~3일(파일 용량에 따라 달라 질 수 있음) 후에 담당 수사관 전자메일로 파일과 해시값을 함께 회신하고 있다. 수사기관에서 직접 선별하여 압수할 수 없어 사건과 관련 없는 모든 자료를 회신하는 문제점과 포털사 별로 회신 기간이 다르고, 회신자료에 대한 문서 비밀번호가 모든 영장이 동일한 점은 한 번이라도 특정 포털사에 영장을 집행한 사람이면 누구나 쉽게 파일을 열어 볼 수 있다는 문제점이 있다.

4) 검사는 범죄 수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원 판사에게 청구하여 발부받은 영장에 의하여 압수수색을 할 수 있다.

5) 체포·구속·압수 또는 수색을 할 때는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다.

6) 대법원 2017. 9. 7. 선고, 2010도 10648 판결
압수수색 검증영장에 집행 초기 FAX(모사전송)를 통한 송부는 위법하지 않으나, 전자메일 수령단계에서 영장 원본을 제시하지 아니하고, 압수목록이 작성되거나 교부하지 않은 이상 영장 집행 절차가 위법하며, 압수한 전자메일의 증거능력도 부정하였다.

라. 영장 원본 제시 및 압수물 수령단계

담당 수사관이 집행장소에서 업무 담당자에게 영장 「원본」을 제시하고 기관 전자메일로 회신 받았던 전자정보를 CD, DVD와 같은 저장장치에 저장하여 봉인·수령 한다. 전국의 경찰, 검찰 등 사법경찰권이 부여된 기관에서 직접 각 포털사로 직접 방문하여 업무를 처리하기 위해서 인적, 물적 처리 비용이 상당하다는 문제점이 있다.

마. 압수목록교부서 교부

유체물과 포털사 전자메일 외 전자정보의 경우 압수목록교부서의 내용을 피압수자에게 확인받고 목록을 교부하지만, 포털사 전자메일의 경우 그동안 압수목록을 교부하지 않고 있었다.

2017. 9. 7. 대법원 2015도10648 판례의 취지로 인하여 포털사 전자메일도 압수목록 교부를 시작하게 되었다. 위법수집증거로 증거능력이 부정되어 「원본」 제시 및 압수목록 교부가 필요하지만, 적법절차의 준수와 업무의 효율성을 모두 고려하는 개선안이 필요할 것이다.

바. 압수물 분석

최종 압수된 전자정보의 내용을 확인하여 어느 것이 범죄와 연관된 사항인지 어느 것이 범죄와 연관되지 않은 것인지 분석 후 관련된 사항만 수사기록에 첨부한다.

영장에 대한 압수물 분석 시 회신 받은 자료에서 실제 사건과 연관된 자료는 극히 일부분이고, 대부분 개인적인 자료가 많아 개인의 프라이버시 침해가 상당하다는 문제점이 있다.

3.2 개인정보보호 침해의 문제점

아래 표 1 「형사소송법 개정 전·후 비교표」에서 보듯이 개정 이전에는 '필요성'만을 규정하고 있었으나, 개정 이후에서는 해당 사건과의 '관련성'을 강조하고 있다[7].

컴퓨터, 모바일 기기 등 압수수색 시에는 피압수자의 참여와 추출 파일에 대하여 개별 해시값을 교부하며 확인받는 절차로 법정에서 증거 사용되는데 문제가 되지 않는다. 하지만 제3자 보관 전자정보의 경우 수사기관에서 직접 압수수색 하지 않고 해당 전자정보의 관리 주체인 업무 담당자를 통하여 대리 압수하는 형태를 취하고 있다. 그리하여 사건과 관련 있는

Table 1. Comparative chart before and after revision of criminal procedure law

Before Criminal Procedure Act Revision
Article 106 (Seizure) (1)When it is necesary, a court may seize any articles which, it believes, may be used as evidence, or liable to confiscation: Provided, That the same shal not apply to the cases where there exist other provisions in Acts.
Article 109 (Search) (1)A court may, if necessary, search the person, effects or dwelling or any other place of the defendant.
Article 215 (Seizure, Search and Inspection of Evidence) (1)If necessary for investigation of crimes, public prosecutors may seize, search or inspect evidence according to the warrant issued by a judge of the competent district court upon request by the public prosecutors.
After Criminal Procedure Act Revision
Article 106 (Seizure) (1)If necessary, a court may seize any articles thought to be used as evidence or liable to confiscation, only when such articles are deemed to be connected with the accused case: Provided, That the same shall not apply where otherwise provided in Act.
Article 109 (Search) (1)If necessary, a court may search the body of the criminal defendant, or articles, dwelling, or any other place of the defendant, only when they are deemed to be connected with the accused case.
Article 215 (Seizure, Search and, Inspection)(1)If necessary for the investigation of crimes, prosecutors may seize, search, or inspect articles or persons according to the warrant issued by a judge of the competent district court upon request of the prosecutors, only when there are circumstances where a criminal suspect is suspected of having committed a crime and the articles or persons to be seized, searched, or inspected are deemed to be connected with the relevant case.

전자정보에 대한 확인 없이 압수 기간만 선정하여 전체 전자정보에 대한 압수수색이 이루어져 피압수자에 대한 개인정보침해가 상당하다.

실제로 2010가단407243[7] 서울중앙지법 판례에 의

7) 서울중앙지방법원 2012. 9. 11. 선고, 2010가단

하면 주경복 건국대 교수가 '불법적으로 전자메일 압수·수색을 당했다'라며 국가를 상대로 낸 손해배상청구 소송에서 '주 교수에게 700만원을 배상하라'라는 원고일부승소 판결을 했다. 판례의 취지는 전자메일의 경우 사생활에 관한 정보가 집약되어 있고, 범죄혐의와 무관한 개인정보가 포함된 경우가 많은데, 검찰이 수사 목적 범위와 무관하게 과도한 기간 동안 이메일을 압수·수색했다면 국가가 손해배상을 해야 한다고 판결하였다.[8)]

3.3 압수수색 결과 통보의 부재

금융계좌에 대한 압수수색의 경우 금융실명거래 및 비밀보장에 관한 법률에 따라 명의인에게 거래정보 등을 제공한 사실을 각 금융기관이 피압수자에게 통보하는데 반해, 전자메일 압수수색의 경우 통신비밀보호법에 명확한 규정이 없어서 형사소송법에 의한 압수수색영장에 의하고 있었고, 압수수색의 결과에 대한 통보가 이루어지지 않았다. 이에 대한 보완책으로 2009. 5. 28. 신설된 통신비밀보호법 제9조의3[9)]에 의거하여 개인에게 통보되도록 규정하고 있다.

407243 판결
유체물 압수수색과 달리 전자정보, 특히 전자메일의 경우 사생활에 관한 정보가 집약되어 있고, 범죄혐의와 무관한 개인정보가 포함된 경우가 많으며, 전자메일 사용자의 사생활 보호에 대한 기대수준이 높아 그 보호 가치가 높기 때문에 압수할 전자메일의 적정한 송수신 기간을 정하여 범죄혐의와 무관함이 명백한 전자메일을 압수하지 않도록 할 의무가 있는데, 그러한 조치 없이 위 교육감 선거일로부터 7년 전에 송수신한 전자메일까지 구분하지 않고 모두 압수한 것은 위법하고, 검사에게 직무상 과실이 있으며, 나아가 그로 인하여 원고가 정신적 고통을 입었을 것임은 경험칙상 충분히 인정할 수 있으므로 피고가 국가배상법에 따라 손해배상책임이 있다.

8) 검찰은 2009년 주경복 전 서울시 교육감 후보의 정치자금법 위반 사건 수사 시 수사대상자 100여 명에 대하여 7년간의 송수신이 완료된 전자메일을 압수수색을 하였다.

9) 제9조의3(압수·수색·검증의 집행에 관한 통지)
① 검사는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다.

Fig. 1. As a result of NAVER privacy center search, the reason for the seizure report

압수수색 통보를 위하여 개정된 법률조항에도 불구하고 현재까지 포털사 전자메일 압수수색에 대한 통지는 이루어지고 있지 않다. 법원은 피의사실과 무관하게 수집된 증거의 적법성 여부와 이에 대한 위법수집증거 배제법칙의 적용상 예외 인정 여부에 관해 엄격하게 판단하고 있지만, 통지의무 위반 등의 경우 위법수집증거 배제법칙 적용상의 예외를 관대하게 인정하는 경향이 있다.[10)][8].

각 포털사 중 네이버의 경우 그림 1과 같이 NAVER 프라이버시센터의 「투명성 보고서 FAQ」[11)]자료에 "현행 통신비밀보호법 및 형사사소법의 취지상 금지(비밀준수의무의 부담)된다는 것이 대법원 판례의 입장"이라는 모호한 표현으로 압수수색 결과를 통지하지 않는다고 명시하고 있다.

또한, 2012년도 국가인권위원회에서 연구과제로 진행한 「사이버 수사 및 디지털 증거수집 실태조사」에 의하면, 전자메일이 압수되었다는 사실을 언제 알았는지에 대한 질문에서 ①'수사과정에서 우연히 알게 되었다'라고 응답한 비율이 55.6%, ②'수사기관이 서면으로 통지해 주어서 알게 되었다'고 응답한 비율은 22.2%, ③'법원공판과정에서 알게 되었다'고 응답한 비율도 22.2%로 조사되었다[9].

IV. 제안하는 압수수색 방안

위에서 살펴본 인터넷포털 전자메일 압수수색 분석과정의 문제점은 어떠한 메일이 범죄 연관된 것인지 압수 전까지는 파악이 불가능 하고, 압수수색 결과를 피압수자에게 통보하지 않는다는 것이다.

압수수색 기간으로 명시된 시점에 생성된 모든 전

10) 대법원 2012. 7. 26. 선고 2011도12407 판결, 2015. 1. 22. 선고 2014도10978 판결 등.

11) [네이버 홈페이지] 2018. 4. 11. 검색 https://privacy.naver.com/transparency/transparency_report_faq?menu=transparency_faq

자정보가 압수됨에 따라 개인정보 침해가 발생할 수 밖에 없다. 이러한 문제점 개선을 위하여 ①수·발신 전자메일의 ID ②수·발신 시간 ③전자메일 제목의 정보가 포함된 메일헤더[12]를 사전에 확인하여 범죄와 연관된 전자메일만 압수하는 방안을 추진한다면 수개월 또는 수년씩의 전자메일 전체를 압수하는 현행 방식보다 개인정보침해를 최소화할 수 있을 것이다. 그리고 각 수사기관이 사건정보를 공유하는 형사사법정보시스템(KICS)을 이용할 경우, 포털사와 수사기관 간의 메일헤더 송·수신과 압수수색 결과 통보 부재에 대한 개선을 동시에 해결할 수 있다. 그러나 현행 법률상 수사기관이 메일헤더 정보를 확보하기 위해서 압수수색 영장으로만 가능하다는 한계점이 있다.

자칫 개인의 기본권 침해가 우려되어 메일헤더 압수수색 영장과 본문·첨부 파일에 대한 압수수색 영장을 별개로 진행할 경우 수사의 속도가 느려질 뿐만 아니라, 압수수색 사실이 노출되었을 때 피압수자가 전자메일을 삭제하게 된다면 범죄와 관련된 중요 증거가 사라져 실체적 진실을 밝히기 어려워지는 문제가 발생할 수 있다.

본 논문에서는 메일헤더 정보를 압수수색이 아닌 통신자료제공요청을 통해 확보함으로써 1~2일 안에 신속히 메일헤더를 확인하여 영장을 청구하는 방안에 대해 자세히 살펴보고자 한다.

4.1 법제도 기반 제안방안 구현

전기통신사업법 제83조 3항 법률에 의하여 '전기통신사업자는 법원, 검사 또는 수사관서의 장, 정보수사기관의 장이 재판, 수사(「조세범 처벌법」 제10조 제1항·제3항·제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 '다음 각 호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청하면 그 요청에 따를 수 있다.'에 의하여 자료를 요구할 수 있다.

아래 표 2와 같이 같은 법 제83조 3항에 전기통신의 결과물인 전자메일의 헤더정보를 추가하는 형태로 법을 개정하여 통신자료제공요청을 통해 포털사에서 메일헤더를 제공 받고, 범죄와 연관성이 있다고 판단되는 전자메일 본문과 첨부 파일만 압수수색을 하여 개인정보침해를 최소화하며 신속하게 수사를 진행하는 것이 가능하다.

12) 여러 가지 제어 정보가 기록된 전자메일의 앞부분으로써 본문 앞에 기입된 정보로 수·발신자의 이름, 전자메일 주소, 제목, 송신 일시, 첨부 파일의 마지막 코드 방식 등이 기입된다. 〔네이버 지식백과〕 (한국정보통신기술협회) 2018. 4. 6. 검색 http://terms.naver.com/entry.nhn?docId=846272&cid=42346&categoryId=42346, 2018. 4. 6.

Table 2. TELECOMMUNICATIONS BUSINESS ACT Article 83, item 3 revised bill

Current Law
A telecommunications business operator may comply with a request for the perusal or provision of any of the following data (hereinafter referred to as "provision of communications data") from a court, a prosecutor, the head of an investigative agency (including the head of a military investigative agency, the Commissioner of the National Tax Service and the Commissioner of a Regional Tax Office; hereinafter the same shall apply) or the head of an intelligence and investigation agency, who intends to collect information or intelligence in order to prevent any threat to a trial, an investigation (including the investigation of a violation committed by means of a telephone, the Internet, etc. among the offenses prescribed in Article 10 (1), (3) and (4) of the Punishment of Tax Offenses Act), the execution of a sentence or the guarantee of the national security: 1. Names of users; 2. Resident registration numbers of users; 3. Addresses of users; 4. Phone numbers of users; 5. User identification word (referring to the identification codes of users used to identify the rightful users of computer systems or communications networks);

6. Dates on which users subscribe or terminate their subscriptions.
Revised bill of Author
A telecommunications business operator may comply with a request for the perusal or provision of any of the following data (hereinafter referred to as "provision of communications data") from a court, a prosecutor, the head of an investigative agency (including the head of a military investigative agency, the Commissioner of the National Tax Service and the Commissioner of a Regional Tax Office; hereinafter the same shall apply) or the head of an intelligence and investigation agency, who intends to collect information or intelligence in order to prevent any threat to a trial, an investigation (including the investigation of a violation committed by means of a telephone, the Internet, etc. among the offenses prescribed in Article 10 (1), (3) and (4) of the Punishment of Tax Offenses Act), the execution of a sentence or the guarantee of the national security: 1. Names of users; 2. Resident registration numbers of users; 3. Addresses of users; 4. Phone numbers of users; 5. User identification word (referring to the identification codes of users used to identify the rightful users of computer systems or communications networks); 6. Dates on which users subscribe or terminate their subscriptions. **7. E-mail Header Information**

이러한 방식의 개인정보침해 최소화를 위한 입법화는 꼭 필요할 것이다. 입법화가 된다면 전자메일과 같은 전자정보에 대한 선별압수가 가능할 것이다. 이는 법원의 영장 발부 취지와도 일치하게 될 것이고, 업무영역까지 살펴볼 경우 수사기관은 신속히 범죄와 연관된 전자메일을 선별할 수 있고, 각 포털사는 영장별로 전체 기간이 아닌 개별 전자메일에 대해서만 자료를 제공하여 업무 부담을 완화할 수 있을 것이다.

실제로 2017년 서울중앙지방검찰청에서 청구한 2017-243** 영장은 「압수할 물건 청구내용 서술」에 대하여 압수하고자 하였으나, 법원에서 메일헤더로 제한 발부하였다. 일부 기각의 취지는 「전자메일 본문 등은 메일헤더 정보 압수 후 그 분석에 따라 청구함이 타당하므로 기각」이었다. 이는 개인정보침해를 막고자 하는 법원의 입장이라고 해석할 수 있을 것이다.

아래 그림 2는 2017-243** 영장을 통하여 확보한 포털 3사의 메일헤더 회신 내용이다.

또한, 익명의 공간인 인터넷상에서 불법행위를 행한 자를 특정하거나 피해자를 구제하기 위해서 통신기록을 보전하는 것은 꼭 필요하다. 사이버범죄방지조약은 가입국으로 하여금 서비스 제공자 등 제3자에게 보전명령을 내릴 수 있는 제도를 입법화할 의무를 부과하였다(제16조, 제17조). 그러나, 우리나라에서는 보전명령제도가 소개되어 제18대, 제19대 국회에서 이를 도입하기 위한 형사소송법 개정안이 제출되었으나, 아직 입법화가 되지 않고 있다.

디지털 증거의 수집에 관한 법 제도를 선도해 온 국가 중 하나인 독일이나 우리나라와 유사한 형사소송 체계를 갖추고 있는 일본의 경우, 디지털 증거의 보전명령제도와 유사한 제도를 이미 마련하였거나 사이버범죄방지조약의 의무이행으로 입법화한 디지털 증거의 보전 명령 제도를 운영하고 있다[10].

메일헤더를 통해 범죄 연관성을 확인 후 해당 전자메일 본문과 첨부 파일에 대한 영장 발부에 소요되

NAVER

dl @naver.com(이OO) - 991개

Date	Time	Send E-MAIL	Receive E-MAIL	Subject
2016-02-14	PM 8:48:33	@gmail.com	@naver.com	Gaesung industrial complex corporation association public statement
2016-02-14	PM 8:48:33	@gmail.com	@naver.com	Gaesung industrial complex corporation association public statement
2016-02-15	PM 7:47:48	@onefreekorea.kr	@naver.com	#Aggie Award candidate#""
2016-02-15	PM 7:47:48	@onefreekorea.kr	@naver.com	#Aggie Award candidate#""
2016-02-15	AM 11:06:32	@hanmail.net	@naver.com	4th press release
2016-02-15	AM 11:06:32	@hanmail.net	@naver.com	4th press release
2016-02-15	PM 12:48:26	@naver.com	@naver.com	160215 4th press release .hwp

KAKAO

j @hanmail.net(장OO) - 38개

Folder ID	Mail ID	Subject	From	Send Time	Receive Time
INBOX	900000000GnCfY	FW::::	@naver.com	2016-08-02 5:00	2016-08-03 17:00
INBOX	900000000GnCfX	FW::::	@naver.com	2016-08-02 5:03	2016-08-03 5:03
INBOX	900000000GnCfQ	[U+BOX] Personal Information use breakdown	@imory.co.kr	2016-08-02 23:40	2016-08-02 23:40

NATE

Date	Send E-MAIL	Receive E-MAIL	Subject
2016-04-20 17:03	@korea.kr>	<@nate.com>	Smartworkcenter reservation information
2016-04-20 5:04	@korea.kr>	<@nate.com>	Smartworkcenter reservation information
2016-04-19 17:33	@korea.kr>	<@nate.com>	Smartworkcenter reservation information
2016-04-20 10:38	@korea.kr>	<@nate.com>	KHIDI News Letter Vol.52(2016. 04.)

Fig 2. Header seizure of e-mails reply from 3 portal companies Electronic information

는 시간 동안 전자메일이 삭제될 우려가 있다. 디지털 증거의 보전명령은 이러한 시간적 지체에 따른 전자정보를 보존하는 효과를 거둘 수 있다.

실제로 2017-259** 영장에 「압수수색 영장 집행 시점을 기준으로 대상 전자메일 관련 자료에 대한 백업 및 보전조치」 문구에 대하여 영장을 발부받아 포털 3사에 협력을 요청하였으나 협력할 수 없다는 답변을 받은 적이 있으므로, 메일헤더를 통한 선별압수수색의 보완 조치로 디지털 증거자료에 대한 자료보존 명령을 꼭 필요할 것이다.

4.2 기술적 제안 방안 구현

현행 포털사 전자메일 압수수색 집행은 FAX(모사전송)으로 이루어지고, 자료 회신은 담당 수사관의 기관 전자메일을 이용하고 있다.

전자메일을 통한 회신과정은 데이터의 유출 등 보안에 취약하므로 별도의 독립적인 시스템을 통해 메일헤더 송·수신과 압수수색결과 통보를 위한 방안이 필요하다.

형사사법정보시스템(KICS)은 경찰·검찰·법무부 각 수사기관이 사건정보를 공유하고 사건접수, 영장청구·발부, 송치 등과 관련된 모든 업무 처리할 수 있는 통합 시스템이다. 그림 3은 현재 SKT, LGU+, KT 전기통신사업자가 연계된 통신자료제공 요청 시스템에 대한 화면이다. 추가로 포털사와 시스템 연계 구성 시 메일헤더를 1~2일 이내로 단축 가능하며 안전하고 독립적인 시스템을 사용할 필요가 있다.

피압수자는 압수수색 결과에 대한 통보를 받을 권리가 있고, 수사기관은 결과를 통보할 의무가 있음에도 불구하고 제대로 시행되고 있지 않다. 해당 문제점 개선을 위하여 형사사법정보시스템(KICS)를 통한 압수수색결과 통보를 구현하여 수사기관으로써 의무를 다해야 할 것이다. 더 나아가 현행 법률에서 통보사실에 대하여 서면으로 제한하고 있는 부분을 서면 또는 전자우편으로 유연하게 확대할 경우, 압수수색 결과 통보를 현행방식 보다 쉽고 빠르게 처리할 수 있을 것이다.

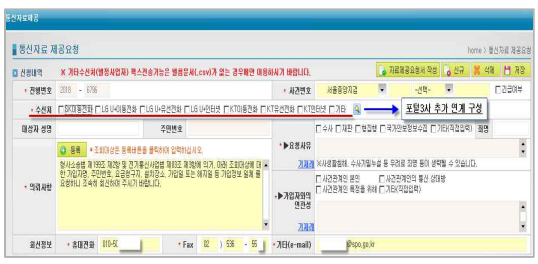

Fig. 3. Communication via existing KICS Three companies communication data provision

4.3 포털3사 형사사법정보시스템(KICS) 연계방안

현행 형사사법정보시스템(KICS)의 통신자료제공시스템 개념도를 기반으로 각 포털사와 연계가 필요한 구성에 대해 알아보고 단계별 흐름도를 살펴본다.

아래 그림 4는 형사사법정보시스템과 통신 3사간 통신자료제공시스템 구성 개념도이다. 기존 VPN을 통해 통신망을 연결하여 자료연계가 가능하도록 구성했다. 이처럼 포털3사도 VPN을 통해 저비용으로 메일헤더 시스템 자료 연계 구성이 필요할 것이다.

수사기관이 포털사에 메일헤더 자료를 요청 후 수신까지는 그림 5와 같이 총 4단계의 절차를 거치는 과정이 필요하다. 내부 결재 등 프로세스만 신속하게 진행된다면 1~2일 이내에 해당 계정의 메일헤더 정

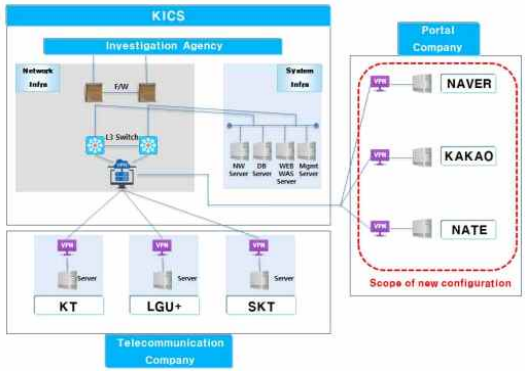

Fig. 4. Conceptual diagram of cooperative topology

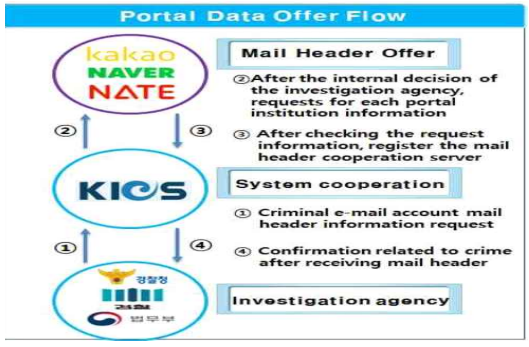

Fig. 5. Mail header Provide flow

보를 확보하여 범죄와 관련성을 신속히 파악 할 수 있을 것이다.

V. 제안방안 검증

수사기관의 전자메일 압수수색은 모든 수사에서 꼭 필요한 부분이 되었고, 대부분의 IT 수사관들은 전자메일 영장에 대한 집행을 경험하였다. 본 논문에서 필자가 제시한 포털사 전자메일 압수·수색 전 메일헤더를 통하여 범죄와 연관성을 확인한 후 관련된 전자메일 본문과 첨부자료에 대해서만 영장을 청구하는 방안에 대한 개선안의 타당성 확인을 위하여 실제 영장 청구 시나리오와 관련 내용에 대해 담당 수사관들과 토의를 통해 검증하였다.

5.1 실제 시나리오 기반 검증

형사소송법 제215조 '검사는 범죄 수사에 필요한 경우 지방법원 판사에게 압수·수색영장을 청구할 수 있다. 사법경찰관이 범죄 수사에 필요한 때에는 검사에게 신청하여 검사의 청구로 판사가 발부한 영장에 의하여 압수·수색 또는 검증을 할 수 있다.'에 의하여 영장을 청구하고, 형사소송법 제219조, 제114조 제1항 '지방법원판사는 검사의 영장청구에 대하여 그 요건을 심사하여 압수수색 영장을 발부한다. 압수수색 영장에는 피의자의 성명, 죄명, 압수할 물건, 수색장소, 신체, 물건, 발부일자 그리고 유효기간과 그 기간을 경과하면 집행에 착여하지 못하며 영장을 반환해야 한다는 취지, 압수·수색의 사유 등을 기재하고 판사가 서명·날인해야 한다.'에 의해 영장을 발부하게 된다.

검찰에서 실제로 청구하는 현행 전자메일 압수수색을 위한 영장청구 사례를 바탕으로 개선안이 적용된 영장 청구 작성례를 살펴본다.

5.1.1 기존 청구 방식에서 압수할 대상

표3, 4는 현행 압수수색 청구 방식에서 압수할 대상 소유자 인적사항과 이메일 계정의 예시이다.

Table 3. Personal information of current method

No	Name	Resident Registration No	Hold Office Period
1	김OO	39OOOO - 104OOOO	13. 8. 5.~ 15. 2. 23.
(중략)			
16	이OO	48OOOO - 204OOOO	14. 4.~

Table 4. E-Mail address of current method

No	E-Mail ID	Note
1	ysch*****@hanmail.net	
(중략)		
6	dlg***@naver.com	

□ 압수할 물건

- 각 포털사(전자메일 운영사 포함)를 상대로,

① 위 대상자들의 인적사항 및 본인확인기관의 본인 인증정보(CI·DI 조회결과) 및 인증결과 값(휴대전화 인증 값 포함)으로 가입된 계정 정보(ID, 전자메일 주소 포함), 결제내역(결제수단 포함, 결제계좌, 결제방법, 결제자 인적사항, 결제일시 포함)

② 위 특정 전자메일 계정의 사용자 정보(성명, 생년월일, 주소, 연락처, CI·DI값, 가입시 IP 포함), 결제내역(결제수단 포함, 결제계좌, 결제방법, 결제자 인적사항, 결제일시 포함)

③ 본건 범죄사실과 관련된 위 각 계정의 자료요청기간 동안의 송수신이 완료된(실시간 아님) 전자메일 내용(첨부자료 포함) 및 쪽지함(개인함, 휴지통, 헤더 포함)

④ 메신저 대화내용〔네이트 메신저 및 위 계정으로 가입된 모바일 메신저(카카오톡 포함)〕, 클라우드 서비스(N드라이브 포함)에 보관 중인 자료, 주소록 내용, 친구목록 및 내용, 주소록 및 친구목록 내 계정(ID)의 가입자정보(전화번호, IMEI, 전자기기 고유번호, 프로필 내용 포함)

⑤ 위 각 계정을 사용하여 아래 자료 요청 기간 동안 접속한 로그 자료(접속 IP 포함)

- 자료요청기간 :
  2013. 3. 10.부터 2017. 8. 31.까지
- 압수수색 장소
  . 주요 포털사 및 본인확인기관 등 관련
  ① 서울 서대문구 통일로 87 임광빌딩 신관 (SK커뮤니케이션즈 실 사무실 포함)

② 경기 성남시 분당구 불정로 6
(NAVER 그린팩토리 실사무실 포함)
③ 서울 용산구 한남대로 98
(카카오 각 실사무실 포함)

5.1.2 기존 청구 방식에서 압수할 대상

표5, 6는 개정된 압수수색 청구 방식에서 압수할 대상 소유자 인적사항과 이메일 계정의 예시이다.

Table 5. Personal information of author revision method

No	Name	Resident Registration No	Hold Office Period
1	김OO	39OOOO - 104OOOO	13. 8. 5.~ 15. 2. 23.
(중략)			
16	이OO	48OOOO - 204OOOO	14. 4.~

Table 6. E-Mail address of author revision method

No	E-Mail ID	Note
1	ysch*****@hanmail.net	
(중략)		
6	dlg***@naver.com	

□ 압수할 물건
- 각 포털사(전자메일 운영사 포함)를 상대로,
① 네이버·카카오·네이트의 2. 특정 전자메일 계정에 대하여 「메일헤더로 선별된 범죄와 연관된 사항 〔별첨〕」 자료에 해당하는 전자메일 본문 및 첨부자료 및 쪽지함(개인함, 휴지통 등), 송수신 IP자료(맥어드레스 등 기기 식별 정보 포함)
② 2. 특정 전자메일 계정에 대하여 「〔별첨〕 메일헤더의 연월일과 일치하는 시기」에 클라우드 서비스(N드라이브 포함) 보관 중인 저장된 문서, 녹음파일, 사진 영상 등 자료, 주소록, 친구목록, 네이버페이등 결제 내역 자료
③ 2. 특정 전자메일 계정에 대하여 「〔별첨〕 메일헤더의 연월일과 일치하는 시기」에 해당하는 메신저 대화내용〔네이트 메신저 및 위 계정으로 가입된 모바일 메신저(카카오톡 포함)〕, 클라우드 서비스(N드라이브 포함)에 보관 중인 자료, 주소록 내용, 친구목록 및 내용, 주소록 및 친구목록 내 계정(ID)의 가입자정보(전화번호, IMEI, 전자기기 고유번호, 프로필 내용 포함)

- 자료 요청 기간 : 범죄와 연관된 메일헤더 송수신 일시로 확인된 〔별첨〕의 일자에 해당하는 전자메일 본문 및 첨부자료

5.1.3 압수수색 장소에 대한 청구 주소 변화

정보통신의 발달과 인터넷의 보급으로 인하여 물리적인 공간적 제약을 뛰어넘어 통신망을 통해 국경을 초월하여 실시간으로 전세계 어디든 실시간으로 자료가 유통되고 있다. 이에 따라 압수수색영장에서 압수수색 장소의 개념을 변경할 필요가 있다. 「금융계좌 추적용」 압수수색 영장의 압수수색 장소는 「금융실명거래 및 비밀보장에 관한 법률 제2조 제1호에서 정하는 기관」으로 법령에서 정하는 기관으로 특정하여 청구하고 있다.

대형 포털사의 경우 서버가 여러 데이터 센터에 저장될 수 있고, 수사기관에 통보 없이 이전할 수 있음에도 압수수색 장소를 도로명 혹은 지번 주소까지 특정하여 청구하고 있는 실정이다. 본 논문에서는 아래와 「전기통신사업법」과 같은 제3자 전자정보 보관을 위한 법령에서 정하는 기관으로 영장의 특성에 맞게 변경할 필요가 있을 것이다.

□ 기존 청구방식
- 포털사(전자메일 운영사 포함)
① 서울 용산구 한남대로 98
(카카오 각 실사무실 포함)
② 제주 제주시 첨단로 242
(카카오 각 실사무실 포함)
③ 경기 성남시 분당구 불정로 6
(NAVER 그린팩토리 실사무실 포함)
④ 서울 서대문구 통일로 87 임광빌딩 신관
(SK커뮤니케이션즈 실사무실 포함)
⑤ 위 각 업체의 게시글, 전자메일, 메신져, 쪽

지, 클라우드 관리 서버 소재지 포함

□ 필자 개정 청구방식
- 압수수색 대상 전기통신사업자
① 「전기통신사업법 제2조 제1항제 1호」의 규정에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 기관
② 「전기통신사업법 제2조」에 해당하는 전기통신회선설비를 이용하여 기간통신역무를 제공하는 기간통신사업자에 해당하는 기관
③ 「전기통신사업법 제3조」에 해당하는 별정통신사업자에 해당하는 기관
④ 「전기통신사업법 시행령 제3조」에 해당하는 보편적 역무를 제공하는 전기통신사업자로 지정된 기관

5.2 검증토의

실제 영장청구 시나리오를 통해 기존 포털사 전자메일 압수수색 방식과 제시한 개선 압수수색 방식에 대해 토의한 결과, 기간만 산정하여 전체 전자메일 본문과 첨부자료를 압수하는 방식보다 메일헤더로 범죄와 연관된 것을 확인한 후 자료 요청 기간을 '범죄와 연관된 메일헤더 송수신 일시로 확인된 〔별첨〕의 일자에 해당하는 전자메일 본문 및 첨부자료'로 변경하는 압수수색 방안에 대해 동의하였다.

기존 영장관련 업무에 대해서 포털사의 입장은 어떠한지와 개선안이 적용된 영장 청구 방식의 변화에 대해 포털사의 입장은 어떠한지 사전 협의가 필요하다는 의견도 상당히 많았다. 마지막으로 압수수색 장소에 대한 청구 주소 변화에 대해서는 모두 적극 찬성한다는 입장이었다. 기존 포털사에 대한 실제 주소지로 영장을 청구하였으나 해당 전자정보는 자회사 혹은 백업 데이터 센터에 있는 등 각 수사기관에서 사전에 확인하기 어려운 점들이 많이 있었다.

VI. 결 론

포털사 전자메일 압수수색에서 개인정보 침해 최소화를 위해서는 명시된 기간내에 생성된 전자메일 본문 및 첨부자료 일체에 대한 압수수색 방식은 신속히 개선되어야 할 것이다. 이와 같은 점에서 개선되어야 함 점을 요약해 보면 다음과 같다.

첫째, 전기통신사업법 제83조 3항 개정을 통해 「메일헤더」를 통신자료에 포함하여 영장청구 이전 범죄와의 연관성을 선별할 수 있는 방안이 필요하다. 또한 담당 수사관의 기관 전자메일을 통해 자료 회신하는 보안의 문제점 해소를 위해 이미 구축된 형사사법정보시스템(KICS)를 통해 포털사와 수사기관 간의 자료 송수신 연계 방안이 필요하다.

둘째, 메일헤더를 통해 범죄 연관성을 확인 후 선별된 전자메일 본문에 대한 압수수색 시점까지 자료보전명령제도 시행을 통해 전자메일을 보존하는 것이 꼭 필요할 것이다.

셋째, 압수수색 결과 통보를 위하여 개정된 법률조항에도 불구하고 현재까지 포털사 전자메일 압수수색에 대한 통지는 이루어지고 않는 문제점도 형사사법정보시스템(KICS)를 통해 구현한다면 통보의 편리함과 개인의 알권리를 모두 충족할 수 있을 것이다.

넷째, 기술적 제안 방안 구현에서 제시된 형사사법정보시스템(KICS)에서 통신자료제공 요청 시스템을 통하여 SKT, LGU+, KT 전기통신사업자와 같이 연계하여 업무의 편리성과 보안의 강화를 이루는 효과를 모두 달성할 수 있을 것이다.

포털사 전자메일 압수수색은 범죄와 연관된 것으로 추정하는 기간의 모든 전자정보를 압수수색하는 문제점이 있었다. 이러한 문제점 개선을 위하여 '법제도 기반 제안방안 구현'과 '기술적 제안방안 구현' 2가지 측면에 대한 개선안 제시와 검증을 진행하였다. 이를 통해 개인정보 침해를 최소화 하고 수사기관과 포털사측 모두에게 효율적인 업무 개선안 제시를 통해 앞으로 지속적으로 증가할 수사기관의 포털사 전자메일 압수수색에 대한 나아갈 방향을 제시하였다. 향후 포털사 전자메일 외에도 모바일 메신저, 클라우드 서비스 등에 대한 압수수색 시 사전 선별에 대한 방안도 추가적인 연구가 필요할 것이다.

References

〔1〕 Ji-Young Son/Ju-Seok Kim, "Research on the Improvement of the Search and Seizure Procedure", Judicial Policy Research Institute, pp.40, July. 2016.
〔2〕 Kyungsin Park, "Problems of and Legislative Solutions to Searching

and Seizing Electronic Mails", The Institute of Legal Studies Inha University, pp 8, August. 2010.
〔3〕 Jung Dae-hee/Lee Sang-mi, "The question of relevancy in searches and seizures of digital evidence", Korean Criminological review 26(2), pp 99, June. 2015.
〔4〕 Joung-Hee Lee/Ji-Hyun Kim, "A Study on a Problem and Improvement Method In Selzing Digital Evidence Stored on a Third Party", Journal of Digital Forensics 8(1),pp 94, June. 2014.
〔5〕 Kuack Byong-Sun, "Survey on cyber investigation and digital evidence collection, National Human Rights Commission Of The Republic Of Korea, pp xxii, December. 2012.
〔6〕 Joung-Hee Lee/Ji-Hyun Kim, "A Study on a Problem and Improvement Method In Selzing Digital Evidence Stored on a Third Party", Journal of Digital Forensics 8(1),pp 95, June. 2014.
〔7〕 Jung Dae-hee/Lee Sang-mi, "The question of relevancy in searches and seizures of digital evidence", Korean Institute of Criminology Korean Criminological Review 26(2), pp99, June. 2015.
〔8〕 Kuack Byong-Sun, "Survey on cyber investigation and digital evidence collection, National Human Rights Commission Of The Republic Of Korea, pp 11, December. 2012.
〔9〕 Ji-Young Son/Ju-Seok Kim, "Research on the Improvement of the Search and Seizure Procedure", Judicial Policy Research Institute, pp.39, July. 2016.
〔10〕 Kuack Byong-Sun, "Survey on cyber investigation and digital evidence collection, National Human Rights Commission Of The Republic Of Korea, pp 94, December. 2012.

〈저자소개〉

이 해 진(Hae-Jin Lee) 학생회원
2018년: 아주대학교 정보통신대학원 졸업
2015년 12월~2017년1월: 대검찰청 정보통신과
2017년 1월~2018 7월: 서울중앙지방검찰청 첨단범죄수사제1부
2018년 7월~현재: 대검찰청 대변인실
〈관심분야〉 디지털포렌식, 빅데이터 분석, 정보보호

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신· DMC 연구소 책임연구원
2017년~2018년: Illinois Institute of Technology 방문교수
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 교수
〈관심분야〉 ICS/SCADA, DFIR, Anomaly Detection