이학석사 학위논문

클라우드에 저장된 전자정보의 압수·수색 방법에 관한 연구

2023년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

안 상 현

클라우드에 저장된 전자정보의 압수·수색 방법에 관한 연구

지도교수 이 상 원

이 논문을 이학석사 학위논문으로 제출함
2022년 12월

서울대학교 융합과학기술대학원
수리정보과학과 정보보호 및 디지털포렌식학 전공
안 상 현

안 상 현의 석사 학위논문을 인준함
2023년 1월

위 원 장 국 웅 (인)

부위원장 이 상 원 (인)

위 원 엄 현 상 (인)

국문초록

클라우드 컴퓨팅이란, 실시간 통신 네트워크로 연결된 다수의 컴퓨터가 관여된 다양한 컴퓨팅 개념을 표현하는 일반적·통칭적 개념이다. 클라우드 컴퓨팅 서비스는 2010년경부터 보급되기 시작하였는데 현재는 아마존, 구글, 마이크로소프트 등 다양한 서비스제공자가 클라우드 서비스를 제공하고 있고, 서비스의 범위도 점차 넓어지고 있다.

오늘날 클라우드 컴퓨팅 서비스 환경은 대중화되어 개인 사용자는 물론 기업에 이르기까지 다양한 분야에서 폭넓게 사용되고 있다. 이와 같은 클라우드 컴퓨팅 서비스의 확산에 따라 기업 또는 개인 사용자들의 데이터는 스마트폰, PC 내의 로컬 저장소에서 클라우드 저장소로 옮겨가고 있고 그 양도 방대하다. 그러므로 수사기관의 사건 관련 증거 수집의 대상도 클라우드 저장소의 데이터들까지 포함하는 것으로 범위가 확장되어야 한다.

개인 사용자들은 스마트폰, PC 등을 사용하면서 클라우드 컴퓨팅 서비스를 이용하여 수시로 스마트폰, PC 등을 통해 생성한 정보를 동기화하므로 클라우드 저장소에는 특정한 개인에 대한 자세하고 많은 정보가 존재하게 된다. 그리고 이와 같이 스마트폰, PC 등을 사용하는 과정에서 메타데이터가 해당 디바이스에 존재하게 된다.

한편, 클라우드 컴퓨팅 서비스는 전자정보가 원격지 서버 등 컴퓨터와 네트워크로 연결되어 있는 외부 저장매체에 저장되어 있는 경우가 많다. 이러한 경우 압수·수색 장소를 어떤 방식으로 특정할

것인지 문제가 될 수 있는데, 이것이 원격 압수·수색 및 역외 압수·수색의 문제이다. 이것이 현행 형사소송법상 허용되는지에 관하여 긍정·부정의 견해가 나뉘고 대법원은 모두 허용되는 취지로 판시한 바 있다. 그러나 보다 근본적으로는 법령을 개정하거나 사이버범죄 협약에 가입하는 방안을 검토해야 할 것이다.

클라우드에 대한 디지털포렌식은 수사기관이 법정 증거로 사용하기 위한 디지털 증거를 클라우드에서 찾아내는 포렌식 절차이다. 클라우드에 대한 디지털포렌식은 클라우드 서비스에 접속한 디바이스를 대상으로 디지털 아티팩트를 찾기 위해 실시되는데, 네트워크, 물리적 하드웨어, 호스트 운영시스템, 하이퍼바이저, 게스트 운영체제, 게스트 응용프로그램 등 각각의 단계에서 기술적인 어려움이 존재한다.

클라우드에 대한 디지털포렌식 방법에 관하여, 이 논문에서는 메타데이터 기반 파일을 수집하는 방법, 클라우드의 사용 및 삭제 흔적을 추적하는 방법을 검토하였는데, 사용자의 스마트폰, PC 등 디바이스에 저장되어 있는 메타데이터 등을 확보하여 증거를 수집하거나 서드파티앱을 통해 인증 토큰을 받아 클라우드 계정에 접속한 다음 클라우드 내 파일리스트, 메타데이터 및 컨텐츠를 획득할 수 있다.

주요어 : 클라우드 컴퓨팅, 원격 압수·수색, 역외 압수·수색, 클라우드 포렌식, 메타데이터

학 번 : 2021-27970

목 차

그 림 목 차

제1장 서론

1. 압수·수색 환경의 변화

가. 스마트폰 등에 대한 기존 압수·수색 방식

실무상 스마트폰·태블릿 등 모바일기기, 컴퓨터와 같은 디지털 증거에 대한 압수·수색은 모바일기기 등을 임의제출 받거나 법원으로부터 압수·수색 영장을 발부받아 피압수자로부터 모바일기기 등을 압수하여 이를 봉인한 후 검찰, 경찰의 포렌식 부서로 가져와 복제본을 획득하는 방식으로 하고 있다.

법원은 위와 같은 디지털 증거에 대한 압수·수색 영장을 발부할 때 영장에 '압수 대상 및 방법의 제한'이라는 제목의 별지를 첨부함으로써 디지털 증거에 대한 압수·수색 방법을 제한하고 있고, 검찰 및 경찰은 위 별지의 기재 내용과 같은 방식으로 압수·수색 영장을 집행하고 있다. 위 별지의 기재 내용에 의하면, 컴퓨터용 디스크 등 정보저장매체(휴대전화 포함)에 저장된 전자정보에 대한 압수·수색·검증은 원칙적으로 저장매체의 소재지에서 수색·검증 후 혐의사실과 관련된 전자정보만을 범위를 정하여 문서로 출력하거나 수사기관이 휴대한 저장매체에 복사하는 방법으로 압수할 수 있고, 예외적으로 집행현장에서 저장매체의 복제본 획득이 불가능하거나 현저히 곤란할 때에 한하여 피압수자 등의 참여 하에 저장매체 원본을 봉인하여 저장매체의 소재지 이외의 장소로 반출할 수 있다.

나. 스마트폰 기술의 변화

최근 출시되는 스마트폰은 데이터를 기기에 내장된 플래시 메모리에 저장하기 때문에 사용자가 스마트폰에서 파일을 삭제할 경우 기존의 디지털포렌식 방식으로는 삭제된 데이터를 복구하기가 매우 어렵다. 그리고 스마트폰 제조사는 새로운 기종을 출시할 때마다 개인정보 보호를 개선된 사항으로 홍보하면서 보안을 강화하는 추세이고, 사용자 이외의 사람의 내부 데이터 접근을 허용하지 않기 때문에 피압수자의 협조가 없이는 원하는 데이터를 획득하는 것이 어렵다. 게다가 최근 출시되는 스마트폰은 저장매체 자체를 암호화하는 방식을 채택하고 있기 때문에 이를 복호화하기 전까지는 타인이 데이터에 접근하기가 어렵다. 한편, 스마트폰 제조사뿐만 아니라 안드로이드, iOS 등 운영체제 개발사나 개별 애플리케이션의 서비스제공자도 사후적으로 보안 등에 취약점이 발견되면 신속하게 업데이트를 실시하기 때문에 보안에 관한 결점이 빠르게 개선되고 있다.

2. 스마트폰의 클라우드 동기화

스마트폰에는 사용자의 문자메시지, 통화내용, 메모 등 많은 정보가 보관되어 있고, 카메라등이용촬영, 성착취물제작 등 스마트폰을 이용한 범죄와 관련된 사진, 동영상 등 핵심적인 증거가 보관되어 있기도 하다. 그럼에도 위와 같은 스마트폰 기술의 변화로 인해 스마트폰에서 사진, 동영상, 문자메시지 등 정보가 삭제될 경우 범죄사실을 입증할 수 있는 중요한 증거를 확보하지 못하는 등의 문제가 발생하게 된다.

한편, 스마트폰 사용자들은 스마트폰 기기 자체의 저장용량의 한계 등으로 인해 문자메시지, 사진, 동영상 등의 정보를 스마트폰 내부 저장소에만 저장하지 않고, 애플의 iCLOUD, 네이버 클라우드 등 별도의 클라우드 서비스 저장소에 동기화하는 방법으로 저장하기도 한다. 그리고 가령, PC 등으로 구글 이메일, 캘린더 등을 사용할 경우 본문 내용 및 수발신 내용이 구글의 데이터센터에도 저장되고, 사용자의 접속기록 등이 PC, 스마트폰 등이나 브라우저에 저장되기도 한다.

이와 같은 이유로 스마트폰, PC 등에 대한 압수·수색의 한계를 스마트폰, PC 등과 연동되어 있는 사용자의 클라우드 저장소 계정이나 구글 이메일 등 서비스 제공자의 데이터센터에 저장되어 있는 사용자의 계정에 대한 압수·수색을 통해 극복할 수 있고, 사용자가 스마트폰, PC 등 클라우드 서비스에 접속하여 사용한 내용에 관한 메타데이터에서 간접적인 정보를 획득할 수 있을 것으로 보인다.

아래에서는 클라우드 컴퓨팅의 개념을 살펴보고, 클라우드 압수·수색에 관하여 현행 형사소송법상 원격 압수·수색 및 역외 압수·수색이 허용되는지 여부를 검토한 후 클라우드 포렌식의 방법으로서 클라우드 등에 저장되어 있는 전자정보를 압수·수색하는 구체적인 방안에 관하여 살펴볼 것이다.

제2장 클라우드 컴퓨팅

1. 클라우드 컴퓨팅의 개념

가. 클라우드 컴퓨팅의 개요

클라우드 컴퓨팅(Cloud Computing)이란 컴퓨터를 사용한 정보처리를 사용자가 보유한 PC로 하지 않고 클라우드 사업자의 데이터센터 안의 시스템에서 처리하는 것으로서, 클라우드 사용자가 인터넷에 접속한 후 웹브라우저 또는 클라우드 서비스 전용 소프트웨어를 통해 서비스를 이용하는 방식이다. 클라우드 컴퓨팅은 인공지능(AI), 사물인터넷(IoT), 빅데이터와 함께 4차 산업혁명 시대의 핵심기술이자 가장 주목해야 할 컴퓨팅 기술로 인정받고 있다. 이에 글로벌 IT자문기관인 가트너(Gartner)는 클라우드 관련 기술을 미래의 유망 기술로 선정하기도 하였다.

이와 같은 클라우드 컴퓨팅은 그 등장 이전에 사업자가 서비스를 제공하기 위해 자체적으로 데이터센터를 구축하여 IT 리소스를 보유, 운용 및 관리하는 방식인 '온프레미스 시스템(On-Premise System)'과 대비되는 개념으로서, IT 리소스[1]를 소유하지 않고 네트워크를 통해 서비스의 형태로 시·공간의 제약 없이 사용할 수 있기 때문에 제조, 유통, 게임, 미디어, 엔터테인먼트 등 다양한 분야에서 사용되고 있다.

클라우드 컴퓨팅 서비스의 사용 패턴은 크게 4가지로 구분되는데, ① EC(Electronic Commerce) 사이트와 동영상, 이미지 등 전송의 웹 사이트를 기반으로 이용하는 'B to C 분야', ② 제조, 유통, 오피스 등 기업 내부 시스템의 기반으로 이용하는 '엔터프라이즈 분야', ③ 정보, 지자체와 교육 등 공공이용을 기반으로 하는 '공공 분야', ④ 사물인터넷(IoT)과 인공지능(AI), 빅데이터 분석이 이용하는 '신사업 분야'가 그것이다. 초창기

1) IT 리소스(resource)는 하드웨어(물리서버, CPU, 메모리, 네트워크 장비, 저장장치 등)뿐만 아니라 소프트웨어(운영체제, 플랫폼, 유틸리티, 애플리케이션, 그룹웨어 등) 등 IT 관련 기기를 포괄하는 개념이다.

클라우드 서비스가 제공될 때에는 주로 웹 사이트나 애플리케이션 개발 환경으로 이용되었으나 VPN망, 전용선 등 네트워크 서비스와 데이터베이스 등 기능이 정비되고 서비스의 안정성 · 신뢰성이 높아져 최근에는 기업의 내부 정보 시스템 기반으로도 채택되기 시작하였다.

클라우드 컴퓨팅 서비스 환경은 대중화되어 다양한 분야에서 사용되고 있는데, 저장 장소 역시 기존의 개인 저장매체에서 클라우드 스토리지로 옮겨가는 추세이다. Spiceworks에 따르면, 현재 약 39%의 기업에서 클라우드 기반 스토리지를 사용하고 있는데, 2022년까지 약 59%까지 증가할 것으로 예상하였다. 또한, IDC(International Data Corporation)에 따르면 현재 40ZB의 데이터가 존재하는데 2025년까지 175ZB의 데이터가 존재할 것으로 예상되고, 이러한 데이터 중 약 49%가 클라우드 스토리지에 위치할 것으로 보았다[2].

그리고 가트너(Gartner)는 세계의 클라우드 서비스 매출이 2020년 2,498달러에서 2022년 약 3,312억 달러로 급증하고, 국내의 클라우드 시장은 2020년 2조 7,818억 원에서 2022년 3조 7,238억 원으로 급성장할 것이라고 전망하였다. 2019년을 기준으로 글로벌 클라우드 시장 점유율 1위는 아마존의 AWS(32.3%)이며, 마이크로소프트의 애저(16.9%), 구글 클라우드(5.8%), 알리바바 클라우드(4.9%)가 그 뒤를 잇고 있다. 또한, 클라우드 시장의 성장률은 구글 87.8%, 마이크로소프트 63.8%, 알리바바 63.8%, AWS 36%를 기록하였는데, 위 4대 클라우드 사업자는 2018년부터 2019년까지 모두 1.5배 이상의 성장세를 보였다. 특히 AWS의 2020년 1분기 매출은 전년 대비 약 33%가 증가한 102억 달러였는데, 코로나19로 인해 화상회의, 화상수업 등의 사용량이 증가하였기 때문인 것으로 보인다[3].

---

2) 한중수 외 5인, “클라우드 스토리지 서비스에 대한 메타데이터 기반 파일선별 수집 방법 및 구현”, 디지털포렌식 연구 제14권 제3호(2020. 9.), 2.

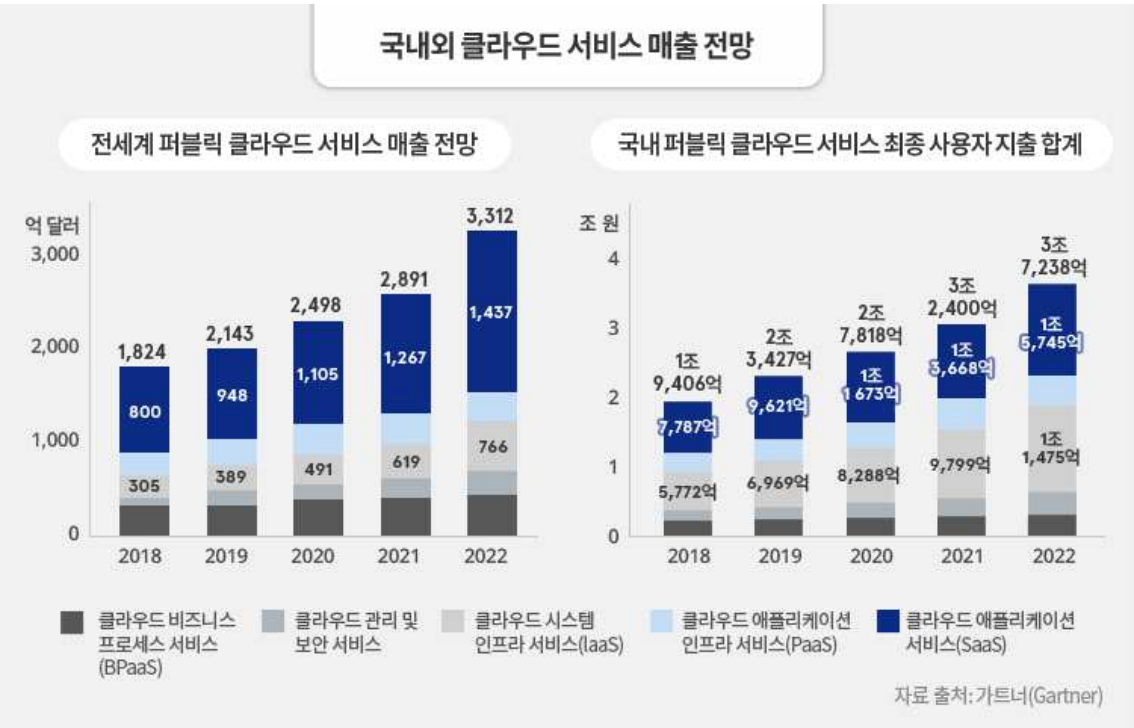

그림 1. 국내외 클라우드 서비스 전망

나. 클라우드 컴퓨팅의 등장 배경

1980년대에는 모든 데이터 등을 대형 범용 컴퓨터를 통해 집중적으로 처리했던 '메인 프레임' 시대였고, 1990년대에는 PC의 대중화로 인해 중앙 컴퓨터가 PC에 데이터 처리를 일부 맡기는 분산형 처리 방식인 '클라이언트 서버' 모델이었다가, 2000년대에는 유무선 네트워크 기술의 대중화로 기업 내 시스템이 구축되어 데이터 처리가 서버에 집중되었다. 그 후 2010년경부터 클라우드 컴퓨팅 모델이 등장하여 급속도로 보급되었는데, 이처럼 클라우드 컴퓨팅이 급속도로 보급된 이유는 첫째, CPU 처리 속도의 고속화, 가상화 기술과 분산처리 기술이 발전하는 등 다양한 기술

3) https://enterprise.kt.com/bt/P_BT_TI_VW_001.do?bbsId=657&bbsTp=A(클라우드 컴퓨팅 산업의 글로벌 및 국내 시장 동향)

이 발전하여 클라우드 컴퓨팅을 받아들일 환경이 갖추어졌고, 둘째, 개별 서버의 리소스 사용률은 평균 10~15% 정도에 불과한데, 클라우드 컴퓨팅을 통해 사용하지 않는 유휴 컴퓨팅 리소스를 다른 사용자들과 공유함으로써 컴퓨팅 리소스를 효율적으로 활용함과 동시에 그 비용을 절감할 수 있게 되었기 때문이다. 그리고 셋째, 맞춤형 서비스 등 사회 트렌드의 변화로 새로운 서비스는 신속하게 개시하고 불필요한 서비스는 선제적으로 제거하는 등 유연한 IT 서비스가 요구되는데, 클라우드 컴퓨팅을 통해 IT 투자비용을 절감하고 유연하게 서비스를 설계·구축 및 운용할 수 있기 때문이다.

이에 비하여 '클라우드 컴퓨팅'과 대비되는 '온프레미스 시스템'은 데이터센터 구축부터 운영·확장까지 초기에 많은 비용이 필요할 뿐만 아니라 데이터센터 구축 후 변경이 어려워 초기에 정확하게 예측하지 못할 경우 큰 손실을 입을 수 있다.

다. 클라우드 컴퓨팅의 정의

클라우드 컴퓨팅의 정의는 1961년 스탠포드 대학의 존 맥카시(John McCarthy) 박사가 제안한 '유틸리티 컴퓨팅(utility computing)'에서 시작되는 것으로 보인다. 존 맥카시 박사는 미래의 컴퓨팅 환경은 전화 시스템과 같은 공공 유틸리티 시설로 구성될 것이고, 이때의 유틸리티 컴퓨팅 환경은 주요 산업의 기반이 될 수 있다고 언급한 바 있다[4]. 이후 가트너(Gartner)는 클라우드 컴퓨팅을 확장 가능하고 탄력적인 IT 기능이 인터넷을 사용하는 외부 고객들에게 서비스 형태로 제공되는 컴퓨터 방식이라

4) 토마스 얼·자이엄 마흐무드·리카르도 푸티니, 클라우드 컴퓨팅 - 개념에서 설계 아키텍처까지, 에이콘 출판사, 2018, 61.

고 정의하였고, 포레스터(Forrester) 리서치는 클라우드 컴퓨팅을 인터넷 기술을 통해 사용량에 따라 과금하거나 셀프 서비스하는 방식으로 제공되는 표준화된 IT 기능(서비스, 소프트웨어 혹은 인프라)이라고 정의하였으며, IBM은 웹 기반 어플리케이션을 활용하여 대용량 데이터베이스를 인터넷 가상 공간에서 분산처리하고 이 데이터를 PC, 휴대전화, 노트북 PC 등 다양한 단말기에서 불러오거나 가공할 수 있게 하는 환경이라고 정의하였다[5].

한편, 우리나라의 『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』(법률 제13234호, 2015. 3. 27. 제정, 2022. 1. 11. 일부 개정) 제2조에서는 '클라우드 컴퓨팅'을 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계라고 정의하고, '클라우드 컴퓨팅 기술'을 클라우드 컴퓨팅의 구축 및 이용에 관한 정보통신기술로서 가상화 기술, 분산처리 기술 등이라고 정의하며, '클라우드 컴퓨팅 서비스'를 클라우드 컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스라고 정의하였다.

위와 같이 클라우드 컴퓨팅에 관하여 다양한 정의가 제안되고 있으나 가장 많이 인용되는 정의인 미국국립표준기술연구소(NIST, National Institute of Standards and Technology)의 것이 클라우드 컴퓨팅을 체계적으로 정의한 것으로 보인다. NIST는 2011년 9월 클라우드 컴퓨팅에 대하여 "공유 구성이 가능한 컴퓨팅 리소스(네트워크, 서버, 스토리지, 애플리케이션 서비스)의 통합을 통해 어디서나 간편하게, 요청에 따라 네트워

5) 토마스 얼·자이엄 마흐무드·리카르도 푸티니, 위의 책, 62-63.

크를 통해 접근하는 것을 가능하게 하는 모델로서 최소한의 이용 절차 또는 서비스 공급자의 상호 작용을 통해 신속히 할당되어 제공되는 것"이라고 정의하였다[6].

위 NIST가 2011년 9월에 내린 클라우드 컴퓨팅에 관한 정의는 현재까지도 클라우드 컴퓨팅을 정의하는 자료로 사용되며 여전히 유효한데, 위 정의에 따른 클라우드 모델은 아래와 같이 다섯 가지의 필수 특성과 세 가지의 서비스 모델 그리고 네 가지의 배포 모델로 구성된다[7][8].

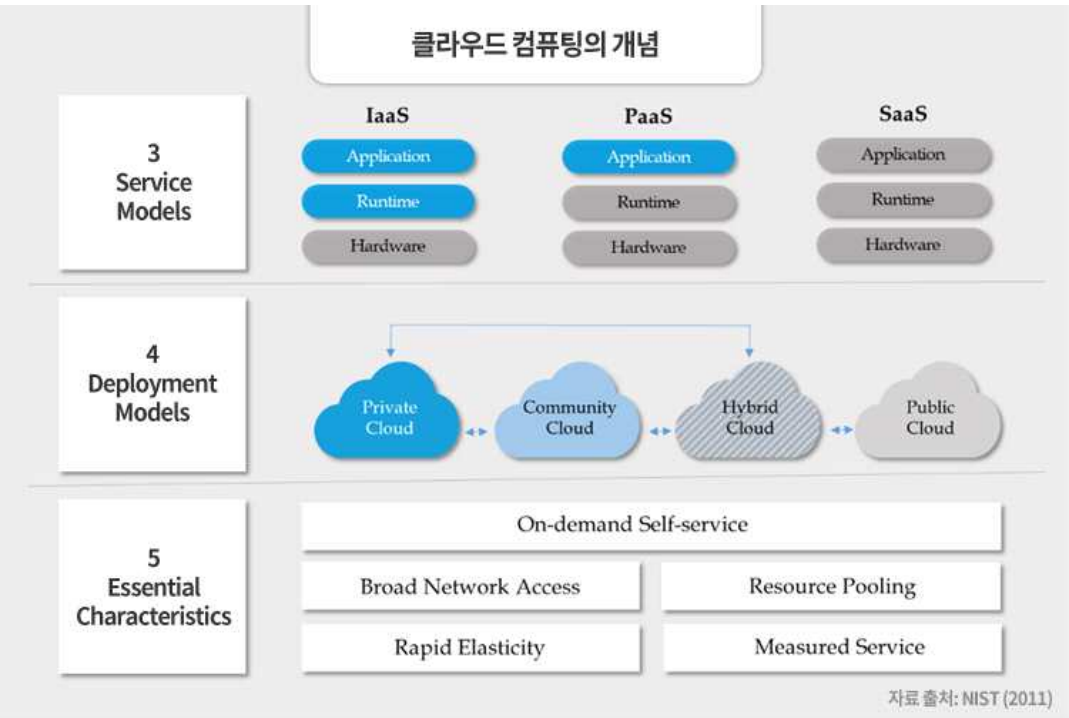

그림 2. NIST 클라우드 컴퓨팅 개념[9]

6) Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145(2011. 9.)
7) Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud https://www.nist.gov/speech-testimony/cloud-computing-benefits-and-risks-moving-federal-it-cloud
8) ttps://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
9) https://enterprise.kt.com/bt/P_BT_TI_VW_001.do?bbsId=657&bbsTp=A

라. 클라우드 컴퓨팅의 특성

클라우드 컴퓨팅은 다음의 특성을 갖는다. 첫째, '주문형 셀프서비스(On-demand self service)'이다. 클라우드 컴퓨팅은 사용자가 서버, 네트워크 장치, 저장장치 등의 IT 리소스를 전문가의 개입 없이 필요한 만큼 자동적으로 확보하여 사용한다. 즉, 서비스 제공자와의 직접적인 상호작용이나 의사소통 없이 자율적으로 클라우드 포털 관리 화면을 통해 서버, 네트워크 저장소와 같은 리소스를 요청하면 즉시 리소스를 할당받아 사용할 수 있다.

둘째, '광범위한 네트워크 접속(Broad network access)'이다. 클라우드 컴퓨팅은 서버가 원격지에 가상으로 존재하여 네트워크로 연결되는 클라이언트-서버[10] 구조의 한 형태로, 팻 클라이언트[11]와 씬 클라이언트[12] 모두 네트워크에 접속하여 대량의 데이터를 처리할 수 있는 환경을 제공한다. 즉, 클라우드 서비스 제공자는 모바일, PC 등 기종에 상관없이 웹 인터페이스를 통하여 서비스에 접근할 수 있는 환경을 제공한다.

셋째, '리소스 풀링(Resource pooling[13])'이다. 클라우드 컴퓨팅은 멀

---

10) 클라이언트-서버(client-server) 모델은 서비스 요청자인 클라이언트와 서비스 제공자인 서버 간에 작업을 분리해주는 분산 애플리케이션 구조이나 네트워크 아키텍처이다.

11) 팻 클라이언트(fat client)는 중앙 서버와 독립하여 풍부한 컴퓨팅 기능을 보유한 클라이언트-서버 구조나 네트워크의 클라이언트를 의미한다.

12) 씬 클라이언트(thin client)는 자신의 컴퓨팅 역할을 충족시키기 위해 다른 컴퓨터(서버)에 크게 의존하는 컴퓨터나 네트워크의 클라이언트를 의미한다.

13) 풀링(pooling)은 객체를 사용자가 지속적으로 소유하거나 점유하지 않고 공유 저장소인 풀(pool)에서 객체를 관리하면서 필요한 사용자에게 할당하고, 사용

티 테넌트[14](multi-tenant) 모델을 기반으로 하며, 사용자는 요구에 따라 스토리지, 프로세싱, 메모리, 네트워크 대역폭 및 가상 머신 등 리소스를 할당받을 수 있다. '멀티 테넌트'란 다중소유 모델이라고도 불리며, 논리적으로 분리된 영역에서 다중의 사용자에게 개별 프로그램 인스턴스를 제공하여 각 사용자가 독립적으로 사용하게 하는 것을 말한다. 클라우드 컴퓨팅에서 리소스 풀링이 중요한 이유는 여러 컴퓨터 기능을 단일 서버에서 하나의 시스템으로 통합할 경우 더 적은 리소스로 더 많은 작업을 수행할 수 있는데, 이로 인해 리소스 인프라를 단순화할 수 있어 리소스 관리 및 운영 비용을 절감할 수 있기 때문이다.

넷째, '신속한 확장성(Rapid elasticity)'이다. 클라우드 제공자는 사용자에게 미리 협의한 IT 리소스를 기본적으로 제공하고, 추가 사용량에 따라 IT 리소스를 확장 및 축소할 수 있는 탄력성을 지원한다. 즉, 클라우드 컴퓨팅은 사용자의 요구에 따라 IT 리소스를 무한대로 확장할 수 있고 필요한 수준으로 언제든지 축소할 수 있어 리소스와 요금 등 측면에서 탄력적이다.

다섯째, '서비스 사용량 측정(Measured Service)'이다. 클라우드 컴퓨팅은 저장장치, CPU, 네트워크 대역폭 등 리소스 사용량을 모니터링하여 사용자에게 보고함으로써 투명성을 제공하고, 리소스를 자동으로 제어하고 최적화한다. 그 결과 사용자는 자신의 서비스 사용량에 대하여만 비용을 지불하게 된다. 예를 들어, 마이크로소프트 Azure의 경우, 가상 서버에 대해 시간당 사용료를 책정하고, 사용하려는 서버의 CPU 코어 개수,

---

후에 다시 풀에 반환하는 기법을 말한다.

14) '테넌트'는 클라우드 컴퓨팅 환경에서 단위화 할 수 있는 한 조직의 인프라 또는 서비스를 나타낸다.

메모리 및 저장장치의 용량, 종류 등에 따라 사용료를 달리 한다.

마. 클라우드 컴퓨팅의 서비스 모델

클라우드 컴퓨팅은 다양한 사용자의 요구에 따라 여러 클라우드 서비스 모델이 제공되고 있으므로 클라우드상 컴퓨터 리소스의 구성 요소와 사용자, 제공자의 관리 영역에 따라 클라우드 서비스가 달라진다. NIST에서는 아래와 같이 SaaS, PaaS, IaaS의 3가지 모델을 제시하였다.

첫째, '서비스로서의 클라우드 소프트웨어(SaaS; Cloud Software as a Service)'이다. 사용자에게 제공되는 기능은 클라우드 인프라[15]에서 실행되는 서비스 제공자의 애플리케이션을 사용하는 것이고, 사용자가 별도의 다운로드나 설치를 하지 않아도 된다. 서비스 제공자는 데이터 센터, 네트워킹 방화벽, 보안, 서버 및 저장소, 운영체제, 개발도구, DB 관리, 호스팅된 응용프로그램이나 앱을 제공한다. 사용자는 제한된 사용자별 애플리케이션 구성 설정을 제외하고 네트워크, 서버, 운영 체제, 스토리지 또는 개별 애플리케이션 기능을 포함한 기본적인 클라우드 인프라를 관리하거나 제어하지 않는다. SaaS의 예로는 구글 앱스(메일, 드라이브 등), 드롭박스(drop box) 등이 있다.

둘째, '서비스로서의 클라우드 플랫폼(PaaS; Cloud Platform as a

15) 클라우드 인프라는 클라우드 컴퓨팅의 5가지 주요 특성을 만들어주는 하드웨어와 소프트웨어의 모음으로서 물리 계층과 추상 계층을 모두 포함한다. 물리 계층은 제공받는 클라우드 서비스를 지원하는데 필요한 하드웨어 자원으로 구성되는데 일반적으로 서버, 스토리지, 네트워크 같은 요소를 포함하고, 추상 계층은 클라우드의 핵심 특성을 잘 나타내는 물리 계층을 통해 배포된 소프트웨어로 구성되어 있고 물리 계층의 위에 놓여 있다.

Service)’이다. 이 모델은 사용자에게 프로그래밍 언어로 만들어진 애플리케이션, 라이브러리, 서비스, 서비스 제공자에 의해 제공되는 도구 등을 제공한다. 즉, 클라우드 사용자는 특정 소프트웨어나 자체 개발 애플리케이션을 위해 클라우드 서비스 제공자로부터 기반 환경인 플랫폼을 제공받는 것이다. 서비스 제공자는 데이터 센터, 네트워킹 방화벽, 보안, 서버 및 저장소, 운영체제, 개발도구, DB 관리 등을 제공하고, 사용자는 스스로 도입한 애플리케이션을 위 플랫폼 위에서 구동하여 직접 데이터를 관리 및 처리한다. 사용자는 네트워크, 서버, 운영 체제 또는 스토리지를 포함한 기본 클라우드 인프라를 관리하거나 제어하지 않지만 배포된 애플리케이션 및 애플리케이션 호스팅 환경 구성 설정을 제어할 수 있다. PaaS의 예로는 스노우파이프사가 있는데, 스노우파이프사는 마이크로소프트의 Azure를 사용하여 게임 서비스를 제공한다.

셋째, ‘서비스로서의 클라우드 인프라(IaaS; Cloud Infrastructure as a Servic)이다. 이 모델은 사용자가 운영 체제 및 애플리케이션과 같은 임의의 소프트웨어를 임의로 배포하고 실행할 수 있는 프로세싱, 스토리지, 네트워크 및 기타 기본 컴퓨팅 자원을 즉시 사용할 수 있는 기능을 제공한다. 사용자는 기본 클라우드 인프라를 관리하거나 제어하지 않지만 운영 체제, 스토리지, 배포된 애플리케이션을 관리하고, 일부 네트워킹 구성 요소(예를 들어 호스트 방화벽)에 대한 제한된 제어 권한을 가질 수 있다. IaaS의 예로는 넷플릭스(Netflix)가 있는데, 넷플릭스는 아마존의 AWS를 이용하여 서비스를 제공하고 있다.

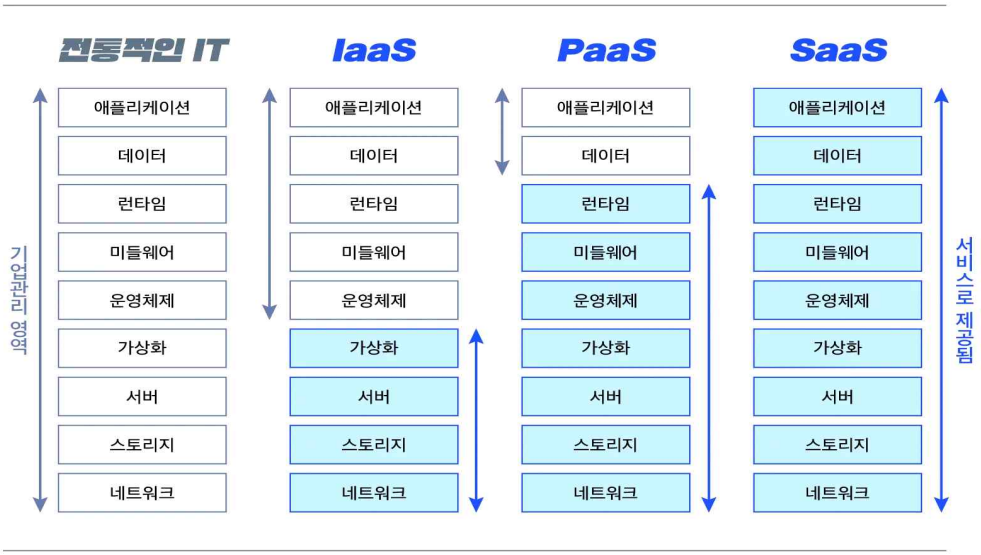

그림 3. 클라우드 컴퓨팅 서비스 모델16)

바. 클라우드 컴퓨팅의 배포 모델

클라우드 컴퓨팅에는 다양한 형태의 배포 모델이 있다. 첫째, '프라이빗 클라우드(Private cloud)'이다. 이는 단일 조직이 독점적으로 데이터센터를 구축하고 독점적으로 사용하는 컴퓨터 환경을 의미한다. 온프레미스 시스템과 유사하지만 데이터센터의 IT 리소스를 가상화하여 사용하는 방식이다. 특정 조직 내에서만 운영되고 접근 가능한 폐쇄적인 클라우드이다.

둘째, '커뮤니티 클라우드(Community cloud)'이다. 이는 금융권과 같이 여러 조직의 업무와 기능이 유사한 경우 파트너쉽을 맺고 연합된 조직 또는 커뮤니티가 퍼블릭 클라우드와 유사하게 공동으로 데이터센터를 구축하고 공유된 접근을 허용하는 방식이다.

16) https://www.whatap.io/ko/blog/9/img/iaas_paas_saas3.webp

셋째, ‘퍼블릭 클라우드(Public cloud)’이다. 이는 다수의 사용자가 클라우드 서비스 제공자가 공급하는 서버 및 저장소와 같은 IT 리소스를 공유하여 사용하는 모델을 말한다. 사용자는 원격으로 접속하여 부여된 계정을 통해 서비스에 접근한다. 대표적으로 마이크로소프트 Azure, 아마존 AWS, 네이버 클라우드 등이 이 모델에 속한다.

넷째, ‘하이브리드 클라우드(Hybrid cloud)’이다. 이는 둘 이상의 호환되는 여러 클라우드 제공자의 퍼블릭 클라우드의 인프라와 조직 내 구성된 프라이빗 클라우드 인프라가 결합되어 사용되는 방식이다. 일반적으로 프라이빗 클라우드의 용량이 부족한 경우 퍼블릭 클라우드에서 IT 리소스를 할당 받아 사용한다.

2. 클라우드 컴퓨팅 기술

클라우드 컴퓨팅 환경을 구축하고 운용하기 위해서 다양한 기술들이 필요하다. 그 기술에는 가상화 기술, 컨테이너 기술, 분산 처리 기술, 데이터베이스 기술, 저장 기술 등이 있다.

첫째, ‘가상화’ 기술이다. 가상화란 하나의 물리적 서버 리소스(CPU, 메모리, 스토리지)에 여러 개의 서버 환경을 할당하고 각각의 환경에 OS와 애플리케이션을 실행할 수 있게 함으로써 논리적으로 다룰 수 있게 만드는 기술이다. 가상화 기술을 사용하면 하나의 물리 서버 리소스를 여러 개로 나누어 여러 개의 서버 환경을 구축할 수도 있고 여러 대의 물리적

서버 리소스를 하나의 서버 환경으로 통합할 수도 있다. 그리고 시스템 구성을 빠르고 유연하게 변경하거나 리소스가 부족해지면 자동으로 리소스를 추가하는 등의 작업이 가능하다. 가상화 기술에는 서버 가상화, 네트워크 가상화, 스토리지 가상화가 있다.

둘째, '컨테이너' 기술이다. 하나의 OS 환경에서 애플리케이션을 실행하기 위한 영역(유저 스페이스)을 여러 개로 나누어 사용할 수 있는데 이렇게 나눈 각각의 유저 스페이스를 컨테이너라고 한다. 각각의 컨테이너는 다른 컨테이너에 영향을 주지 않으며 별도의 애플리케이션을 실행할 수 있다. 서버 가상화가 하드웨어 환경을 가상화하는 것이라면 컨테이너는 애플리케이션 실행 환경을 가상화하는 것이다.

셋째, '분산 처리' 기술이다. 이는 대량의 데이터를 여러 서버에 분산시켜 동시에 병렬적으로 처리하는 기술이다. 가령, 빅데이터 분석 등 다량의 다양한 데이터를 처리할 때 클라우드 컴퓨팅 서비스를 이용한다면 경제적인 비용으로 빠르게 데이터를 처리할 수 있게 된다. 이를 위해 여러 개의 서버를 결합하여 하나의 컴퓨터로 보이게 만드는 클러스터링 장치가 활용되기도 한다.

넷째, '데이터베이스' 기술이다. 각 클라우드 사업자들은 대량의 데이터 분석 처리 및 트랜잭션(상거래와 같은 일련의 처리) 등 사용자의 이용 목적에 맞는 다양한 데이터베이스 서비스를 제공하고 있다. 주요 데이터 베이스 기술에는 RDB(Relational Database)와 NoSQL(Not Only SQL)이 있다. 'RDB'는 여러 개의 데이터베이스를 행과 열이 있는 표 형식으로 표현하여 복잡한 데이터의 관계를 처리할 수 있도록 만든 데이터베이스로

서 데이터 조작 언어로 SQL을 사용한다. RDB에서 데이터베이스 처리 능력을 향상 시키려면 하드웨어의 기능 강화가 필수적이다. 다음으로 'NoSQL'은 RDB와 같은 관계형 데이터베이스가 아닌 것을 가리키는 용어로서, 구체적인 제품마다 데이터베이스를 저장하는 방식이나 데이터 조작 언어가 다르지만, 대량의 데이터를 분산시켜 고속으로 처리하는 분산형 데이터베이스를 의미한다. NoSQL은 분산시켜 처리한다는 특성 때문에 클라우드 컴퓨팅 서비스 구현에 적합하고, 주로 빅데이터 분석 등에 사용된다. NoSQL에서 데이터베이스 처리 능력을 향상 시키려면 서버 증가가 필수적이다.

다섯째, '스토리지' 기술이다. 스토리지는 데이터와 프로그램을 저장하는 기록 장치이다. 클라우드 컴퓨팅 서비스에는 블록 스토리지, 파일 스토리지, 오브젝트 스토리지 총 3가지의 엑세스 방식을 제공한다. 먼저, 블록 스토리지는 일정한 크기의 블록으로 나뉜 스토리지의 논리 볼륨을 블록 단위로 액세스할 수 있는 스토리지로서, 서버와 스토리지가 데이터를 교환할 때의 오버헤드가 적어 빠르게 데이터를 전송할 수 있다. 그리고 파일 스토리지는 파일을 그대로 읽고 쓰고 공유할 수 있는 스토리지로서, 데이터 처리가 Windows OS에서 사용하는 SMB(Server Message Block), CIFS(Common Internet FileSystem)와 Linux OS에서 사용하는 NFS(Network FileSystem) 등의 파일 공유 프로토콜을 사용하여 파일 단위로 이루어진다. 이는 주로 파일 서버로 이용되며 파일의 접근을 제어하거나 파일의 속성 정보를 관리하기 쉽다는 장점이 있다. 끝으로 오브젝트 스토리지는 데이터를 객체 단위로 처리하는 스토리지로서, 데이터 및 관련 메타데이터로 구성된 오브젝트에 고유한 ID(URI)가 부여된다. 오브젝트 스토리지는 OS나 파일 시스템에 의존하지 않으면서도 데이터를 저장

하고 오브젝트에 엑세스할 수 있는데, 이때 HTTP 프로토콜 기반의 REST(REpresentational State Transfer) 형식의 API[17]를 사용한다. 오브젝트 스토리지는 쉽게 용량을 늘릴 수 있고 데이터의 크기 및 저장할 수 있는 데이터의 수에 제한이 없다는 장점이 있다.

3. 클라우드 컴퓨팅의 장점 및 단점

가. 클라우드 컴퓨팅의 장점

클라우드 컴퓨팅은 온프레미스 시스템과의 관계에서 다음과 같은 장점을 갖는다.

첫째, 클라우드 컴퓨팅은 경제적이다. 자체 시스템을 구축할 경우 피크 이용량을 계산하여 하드웨어 및 소프트웨어를 갖추어야 하지만 클라우드 컴퓨팅은 하드웨어와 소프트웨어를 소유하지 않고 사용하고자 하는 기능을 사용하고자 하는 기간 동안만 서비스로서 사용할 수 있어 데이터 유지 보수의 효율성을 높이고 비용을 절약할 수 있다.

---

17) API(Application Programming Interface)란, 응용 프로그램이 운영체제나 데이터베이스 관리 시스템과 같은 시스템 프로그램과 통신할 때 사용되는 언어나 메시지 형식이다. 즉, 프로그램이 가진 기능이나 리소스를 외부의 다른 프로그램이 호출하여 이용하기 위한 명령, 함수, 데이터 형식 등을 정한 것이다. 클라우드 컴퓨팅에서 가상 서버에 마련된 API를 사용하여 프로그램을 작성하면 가상 서버의 생성, 정지 같은 조작이 사람의 손을 거치지 않고 프로그램으로 직접 제어할 수 있게 되어 가상 서버와 스토리지, 데이터베이스 등 다양한 서비스에 이용된다.

둘째, 클라우드 컴퓨팅은 유연성이 있다. 자체 시스템을 구축할 경우 서버의 증축 및 시스템 확장에 많은 비용이 들지만 클라우드 컴퓨팅은 컴퓨팅 리소스를 필요로 할 때 필요한 만큼만 확장하였다가 필요하지 않을 때 축소하는 등 유연하게 활용할 수 있다.

셋째, 클라우드 컴퓨팅은 가용성이 높다. 자체 시스템을 구축할 경우 서버 장애에 대처하기 위해 백업 등 조치를 취해두어야 하지만 클라우드 컴퓨팅은 재해에 강한 데이터센터를 갖추어 하드웨어에 장애가 발생하더라도 서비스를 계속해서 사용할 수 있다.

넷째, 클라우드 컴퓨팅은 신속하게 구축할 수 있다. 자체적으로 시스템을 구축할 경우 설계 및 하드웨어, 소프트웨어 배치까지 시간이 걸리지만 클라우드 컴퓨팅은 클라우드가 제공하는 하드웨어, 소프트웨어를 이용하여 시스템을 신속하게 구축할 수 있다.

나. 클라우드 컴퓨팅의 단점

클라우드 컴퓨팅은 온프레미스 시스템과의 관계에서 안전하고 경제적인 컴퓨팅 환경을 제공하지만 항상 우수한 것은 아니다. 클라우드 컴퓨팅에는 아래와 같은 단점이 있다.

첫째, 보안의 취약성이 증가한다. 기업의 데이터가 클라우드에 저장된다는 것은 데이터 보안의 책임이 클라우드 사업자와 공유된다는 것을 의미한다. 그 결과 보안 아키텍처를 구축하는 것이 더욱 어려워져서 클라우드와 사용자를 연결하는 네트워크의 다운, 악의적인 공격자의 도청, 중

간자 공격, 데이터 도용 또는 손상 등을 당할 위험이 높아진다. 사용자가 아무리 관리를 철저히 한다고 하더라도 데이터가 사라지거나 제3자에게 유출되거나 공개되는 등 위험성이 있다.

둘째, 사용자가 제한된 관리 권한을 갖는다. 클라우드 사업자는 비용을 절감하고 관리가 편한 지리적 장소에 데이터센터를 구축하기 때문에 사용자는 자신의 데이터가 저장되고 처리되는 장소를 알지 못하는 상황이 된다. 또한 공권력의 요청, 해킹 등에 의해 사용자의 데이터가 열람 및 제공될 수 있다는 점에서 사용자가 데이터에 대하여 완전하고 개별적인 통제권을 갖기 어렵다. 결국 클라우드 사용자는 온프레미스 IT 리소스보다 낮은 수준의 관리 제어 권한을 갖게 된다.

셋째, 산업 표준 또는 국제 표준이 없다. 클라우드 서비스는 일반적으로 클라우드 사업자에 의해 독점적으로 제공된다. 그 결과 기업은 이미 도입된 클라우드 서비스에 종속되어 솔루션을 구축할 수밖에 없게 되므로 다른 사업자로 이동하는 것은 불가능에 가까워지게 된다.

넷째, 과도한 비용을 지출할 우려를 배제할 수 없다. 클라우드가 경제적인 측면에서 항상 온프레미스보다 우위에 있는 것은 아니다. 가령 기업 사용자가 장기간에 걸쳐 시스템을 계속 사용하거나 또는 대규모 시스템을 구축하고 운영할 경우에는 클라우드보다 온프레미스방식이 더 경제적일 수도 있다.

4. 클라우드 컴퓨팅 서비스

가. 개요

클라우드 컴퓨팅 서비스가 대중화됨에 따라 전 세계적으로 다양한 클라우드 컴퓨팅 서비스가 제공되고 있다. 클라우드 컴퓨팅 시장은 아마존이 최초로 성공하여 지금까지 시장을 선도하고 있으며, 후발 주자로 마이크로소프트, 구글 등이 뒤를 잇고 있다. 국내에서도 아마존 등 글로벌 클라우드 컴퓨팅 서비스가 약 80% 이상을 점유하고 있고, 위 글로벌 업체들은 이미 기술력과 가격 경쟁력 등을 모두 확보하였다. 그 결과 삼성 SDS, LG CNS, SK C&C 등 국내 IT기업들은 위 글로벌 업체들과 경쟁하는 것이 아닌 협력사에 그친 상황이다. 예를 들어, 삼성전자는 아마존과 구글의 클라우드 컴퓨팅 서비스를 사용하고 있고, LG전자는 아마존, 구글, 마이크로소프트 등의 서비스를 이용하여 클라우드 전환에 나섰다. 현재 국내 IT업체 중에서는 네이버, 카카오, KT 등이 클라우드 컴퓨팅 서비스를 제공하고 있다.[18]

나. 아마존의 AWS(Amazon Web Services)

아마존은 2006년부터 Amazon Web Services라는 클라우드 서비스를 제공하기 시작하였는데, 현재 세계에서 가장 많이 이용되는 퍼블릭 클라우드 서비스이고, 전 세계 20개 이상의 리전을 운영하고 있다. 아마존은 다양한 서비스를 제공하고 있고 매년 새로운 서비스와 기능이 추가되고 있는데, 대표적으로 Amazon EC2(가상 서버), Amazon S3(클라우드 스토리지), Amazon RDS(관계형 데이터베이스 서비스), Elastic Container

18) 정재화, 클라우드 컴퓨팅, 한국방송통신대학교출판문화원, 2021, 174-178.

Service(컨테이너 실행 관리 서비스), AWS IoT(디바이스와 클라우드의 사물인터넷), Amazon Machine Learning(머신러닝 딥러닝), AWS RoboMaker(로봇 관련 애플리케이션 개발), VMware Cloud on AWS(기업 사용자의 사내 시스템) 등이 있다[19].

다. 구글의 클라우드 플랫폼

구글은 퍼블릭 클라우드 서비스인 Google Cloud Platform을 통해 검색엔진, Gmail, Youtube 등의 서비스를 제공하고 있다. Google Cloud Platform의 주요 사용용도는 게임 배포 플랫폼, 빅 데이터의 분석 플랫폼, 애플리케이션 개발인데, Google Cloud Platform의 모든 서비스는 Cloud Console이라는 웹 인터페이스와 명령줄 REST API로 제어할 수 있다.

구글은 현재 전 세계 21개 존 64개 리전을 운영하면서 Compute Engine(가상 서버), App Engine(애플리케이션 실행 환경), Kubernetes Engine(컨테이너 관리), Cloud SQL(관계형 데이터베이스), Cloud Datastore(NoSQL 데이터베이스), Cloud Storage(오브젝트 스토리지) 등을 서비스로 제공하고 있고, 빅데이터 분석을 위한 클라우드 기반 데이터 웨어 하우스인 BigQuery, 대량 데이터의 취합·변환·분석·분류 등 다양한 데이터 처리가 가능한 Cloud Data flow, 오픈 소스 머신러닝 라이브러리인 TensorFlow, 머신러닝 환경인 Cloud Machine Learning Engine, 이미지·음성·비디오 데이터를 분석할 수 있는 학습된 머신러닝 모델 Vision API, Speech API, Cloud Video Intelligence API 등 서비스를 제공하고 있다[20].

---

19) 정재화, 위의 책, 182-184.
20) 정재화, 위의 책, 180-182.

라. 마이크로소프트의 클라우드 서비스

마이크로소프트는 B2B에 노하우가 많은 기업으로서 이미 세계의 많은 기업이 마이크로소프트의 윈도우, 오피스 등 소프트웨어를 사용하고 있다는 이점을 이용하여 클라우드 컴퓨팅 시장에서 빠르게 성장하고 있다. 실제 마이크로소프트는 최근 인프라 구축에 약 150억 달러를 투자하는 등 클라우드 컴퓨팅 시장을 빠르게 확장해 나가고 있다. 마이크로소프트는 2017년에는 약 60여개의 서비스를 제공하였지만, 2020년에는 약 250여개에 달하는 서비스를 제공하고 있다.

마이크로소프트는 'Microsoft Office 365', 'Microsoft Dynamics 365' 등 SaaS형 서비스뿐만 아니라 Microsoft Azure를 통해 IaaS/PaaS형 서비스도 제공한다. 그 중에서 IaaS형 서비스에는 가상 서버(Virtual Machines), 파일 스토리지(Azure Files), 가상 네트워크(Virtual Network) 등이 있고, PaaS형 서비스에는 컴퓨팅, 애플리케이션 플랫폼, 개발자 서비스, 통합, 미디어, 분석, 데이터, AI, 사물인터넷 등이 있다.

그 중 일반적으로 많이 사용되는 것이 컴퓨팅 중 가상머신 서비스가 있는데, 이는 가상화된 디스크 및 스토리지를 제공받을 수 있고 스냅샷(snapshot) 기능을 사용하여 가상화된 디스크의 스냅샷을 만들어 백업용으로 관리까지 할 수 있다[21].

5. 클라우드에 대한 디지털포렌식

가. 클라우드 포렌식의 정의

21) 정재화, 위의 책, 174-180.

디지털포렌식은 수사기관이 법정에서 증거로 사용하기 위한 디지털 증거를 찾는 절차이다. 그 중 클라우드 포렌식은 디지털포렌식의 하위 분야로서 클라우드 컴퓨팅 환경에서 포렌식 원리와 원칙에 근거하여 디지털 수사를 하기 위해 마련되었다. NIST는 클라우드 컴퓨팅 포렌식에 대하여, 지나간 클라우드 컴퓨팅 이벤트들을 재구성하는 것을 용이하게 하려는 목적으로 디지털 데이터를 식별하고, 수집하고, 보존하고, 조사하고, 리포트하는 과정을 통하여 지나간 컴퓨팅 이벤트들을 처리하기 위해 과학적인 원리, 기술적인 지침, 도출된/증명된 방법들을 응용하는 것이라고 정의하였다[22].

나. 클라우드 포렌식의 특성

클라우드 컴퓨팅이 빠르게 성장하고 있어 다양한 사이버 범죄에 노출될 수 있는 위험성이 높아졌음에도 클라우드 컴퓨팅에 대한 디지털 포렌식은 아직 미비한 상황이다. 특히, 클라우드 컴퓨팅 서비스의 가용성 문제로 인해 물리적인 장비에 대한 압수가 현실적으로 불가능하고 클라우드 플랫폼 및 가상화 기술에 따라 다양하고 복잡한 형태를 가지고 있지만, 수사기관이 접근할 수 있는 영역은 관리 시스템 정도로 제한될 수밖에 없다. 그리고 사용자들의 데이터들이 대부분 가상화된 영역에 저장되어 있기 때문에 이를 획득하는 절차 등에 대한 신뢰성 문제도 대두하게 된다[23].

---

22) Stavros Simou1 et al., “A survey on cloud forensics challenges and solutions”, SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2016), Published online in Wiley Online Library(wileyonlinelibrary.com). DOI: 10.1002/sec.1688, 3-4.

23) 이재윤, “클라우드 환경에서 역외 압수·수색에 관한 연구”, 박사학위논문, 성

NIST는 클라우드 컴퓨팅 포렌식의 어려움에 관하여 법적, 기술적, 구조적인 부분을 구분하였는데, 대부분의 문제는 기술적인 부분에 관한 것이다[24]. 클라우드 컴퓨팅 포렌식은 원격이든, 가상이든, 네트워크이든, 라이브이든, 규모가 크든, 정보가 많든 적든지 디지털 아티팩트를 찾아내기 위하여 클라우드 서비스에 접속한 기기를 사용한다. 클라우드 컴퓨팅 구조는 물리 영역, 관리 영역, 가상화 영역, 서비스 영역으로 나누어지고, 추상화된 클라우드 계층은 네트워크, 물리적 하드웨어, 호스트 운영시스템, 하이퍼바이저, 게스트 운영체제, 게스트 응용프로그램으로 나누어지는데, 클라우드 계층마다 다른 내용의 포렌식 수집 활동이 이루어져 각 계층별로 포렌식의 어려움의 내용이 상이하다[25].

첫째, '네트워크' 단계에서는 다양한 목적을 가진 사용자들이 참여하고 있으므로, 특정 사용자에 의해 이용되는 네트워크 리소스를 모니터링할 수 있어야 하는데 기존의 네트워크 장치 또는 모니터링 솔루션은 멀티 테넌트 환경에서 증거를 획득하는 것이 어렵다[26].

둘째, '물리적 하드웨어' 단계에서는 원본 하드디스크 확보 또는 복제를 통해 저장된 데이터의 복구 및 분석이 필요하고 원본을 보존할 필

균관대학교, 24-25.

24) Martin Herman et al,. "NIST Cloud Computing Forensic Science Challenges", https://www.nist.gov/publications/nist-cloud-computing-forensic-science-challenges

25) J. Dykstra, A. T. Sherman, "Acquiring Forensic Evidence from Infrastructure-as-a-Service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques", Digital Investigation, Vol 9, 2012, 90-98.

26) 한수빈·이태림·신상욱, "클라우드 컴퓨팅 플랫폼에서 디지털 증거 수집 절차", 2014년 춘계학술발표대회 논문집 제21권 제1호(2014. 4), 2-3.

요가 있을 때 수행된다. 이때 획득할 수 있는 데이터에는 파일시스템의 메타정보, 시스템과 응용 프로그램의 로그 기록 등이 있다[27]. 그러나 아마존, 구글 등 국외 클라우드 서비스 제공자에 대한 압수·수색영장을 발부받는다고 하더라도 국가관할권의 문제로 인하여 이를 집행하는 것이 불가능하다.

셋째, '호스트 운영체제' 단계에는 중앙제어에 관한 구성요소, 클라우드 서비스 사용, 액세스 권한, 사용자 로그인 등의 정보를 제공하는 클라우드 플랫폼이 포함되어 있다. 그러나 공용 클라우드는 라이브 포렌식 및 휘발성 데이터에 대한 액세스를 허용하지 않고 클라우드 플랫폼에 따라 로그 파일 및 리소스가 분산되어 있다[28].

넷째, '하이퍼바이저' 단계에서 데이터의 사용은 IDS(Intrusion Detection System)의 동작을 통해 증거를 획득할 수 있는데, 이러한 조사는 하이퍼바이저에 대한 액세스 권한이 필요하기 때문에 IaaS 클라우드 조사에 적합하다. 문제는 서비스 이용자에 대한 압수·수색으로는 이러한 정보를 얻을 수 없고 종류에 따라 데이터에 대한 보존과 형식이 다양하다는 점이다[29].

다섯째, '게스트 운영체제, 게스트 응용프로그램' 단계에서 게스트 운영체제는 저장된 이미지와 스냅샷을 통해 내부 정보를 얻을 수 있지만, 서비스 제공자가 영구저장소를 제공하지 않으면 인스턴스의 종료와 함께 사라질 수 있다. 그리고 사용자가 악의적으로 강제 종료하거나 간단한 명

27) 이상진, 디지털 포렌식 개론, 이룬, 2010, 105-137.
28) 한수빈·이태림·신상욱, 앞의 논문, 3.
29) 한수빈·이태림·신상욱, 앞의 논문, 3.

령어로 스냅샷을 삭제할 수 있기 때문에 이러한 경우 수집이 어렵다. 응용 프로그램의 경우 데이터가 휘발성이고, 사용자 이벤트가 서비스 제공자 측에 위치하고 있기 때문에 수집할 수 있는 경우가 제한적이고, 서비스 제공자와 응용 프로그램을 신뢰해야 한다는 문제가 있다[30].

다. 클라우드 포렌식을 통해 획득할 수 있는 정보

클라우드 포렌식을 통하여는 클라우드 서비스 이용자가 통상적인 방법으로 접속하여 접근할 수 있는 클라우드 계정 내에 저장된 전자정보를 획득할 수 있고 그 이상의 전자정보를 수집하기 위한 것은 허용되지 않는다. 그리고 클라우드 서비스 이용자에 대하여 획득할 수 있는 전자정보의 범위는 클라우드 컴퓨팅의 서비스 모델에 따라 그 내용이 다른데, SaaS와 PaaS의 경우에는 서비스 이용자들이 하드웨어를 관리하지 않기 때문에 로그 정보 등을 수집할 수 없는 반면, IaaS의 경우에는 로그 정보를 수집할 수 있다.

제3장 원격 압수·수색과 역외 압수·수색의 문제

1. 전자정보에 대한 압수·수색

가. 전자정보와 압수·수색 목적물

30) 한수빈·이태림·신상욱, 앞의 논문, 3.

전자정보는 전기적·자기적 방식에 의하여 저장·전송되는 무형적 정보로서 정보의 표기·저장·전달의 형태가 0과 1의 조합인 이진수 방식으로 이루어지는 정보를 말한다. 전자정보는 저장된 매체와 독립하여 동일한 정보의 자유로운 복제와 네트워크를 통한 전송이 가능하고, 오감으로 인식이 불가능하여 컴퓨터 등 일정한 판독장치를 통해서만 인식할 수 있으므로 판독장치로 해당 파일을 열기 전에는 그 내용을 알 수 없다. 압수목적물이 전자정보라 하더라도 형사소송법상 영장주의가 적용되므로 일반적인 압수 요건, 집행 및 사후절차 등의 규정은 그대로 적용된다. 다만, 위와 같은 전자정보의 특성으로 말미암아 대물적 강제처분이 그대로 적용될 수 없으므로 형사소송법에 전자정보의 압수·수색에 관한 특칙이 마련되어 있다.

형사소송법 제106조 제3항은 '법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다.'라고 규정하고 있다. 즉, 전자정보를 압수하는 경우에도 압수 목적물은 전자정보를 저장한 정보저장매체이고, 다만 압수하는 방법을 달리 정하는 방식을 취하고 있어 명시적으로 전자정보를 압수의 목적물로 인정하고 있지는 않다. 다시 말하면, 압수의 목적물이 정보저장매체인 경우에는 정보저장매체 자체가 아니라 그 정보저장매체에 저장된 정보가 증거로서의 가치를 지닐 것이므로, 압수·수색의 방법으로서 정보저장매체에 저장된 데이터를 출력하거나 복제하는 방식으로 하도록 하고 있는 것이다.

그러나 위 형사소송법 규정에 대하여 대법원은 “전자정보에 대한 압수·수색영장을 집행할 때에는 원칙적으로 영장 발부의 사유인 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 위 방법이 예외적으로 허용될 수 있을 뿐이다. (중략) 따라서 그러한 경우 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이다.” 라고 판시하여, 2011년부터 줄곧 전자정보 자체가 압수의 목적물이라는 취지의 판시를 하는 것으로 보인다[31](대법원 2011. 5. 26. 결정, 2009모1190호 등 참조).

나. 전자정보에 대한 압수·수색 영장 집행 방법

---

31) 이에 대하여, 미국 실무례는 전자정보의 압수에 관하여 저장매체 자체를 압수하는 것을 원칙으로 하는데 반해, 우리나라 법원 실무는 정보저장매체 등의 압수를 거의 인정하지 않고 전자정보만을 압수의 대상으로 인정하며 원래 소재지에서의 반출도 제한적으로 인정하는 것으로 운용되고 있다고 평가하면서, 디지털 정보는 바로 눈으로 보는 것이 아니고 전자기적으로 저장된 것이므로 확장자의 변경, 비할당 영역의 이용, 비어의 사용 등으로 정보를 저장매체 내에 은닉하였을 경우 이를 찾는 것은 손쉬운 일이 아니고, 압수 초기에 필요한 정보라고 판단하지 못했더라도 수사나 재판 과정에서 필요한 정보가 될 가능성도 있어 일부 정보만을 압수할 경우 중요한 증거를 놓칠 가능성도 있다는 이유로 비판적으로 보는 견해도 있다(안성수, 주석 형사소송법(제5판), 2017. 11., 564-567).

검사 또는 사법경찰관은 형사소송법 제219조, 제118조에 따라 압수·수색영장을 처분을 받는 자에게 반드시 제시하여야 하고, 처분을 받는 자가 피의자인 경우에는 그 사본을 교부하여야 한다. 그리고 공무소, 군사용 항공기 또는 선박·차량 안에서 압수·수색영장을 집행하려면 그 책임자에게 참여할 것을 통지하여야 하고, 그 외에 타인의 주거, 간수자 있는 가옥, 건조물(建造物), 항공기 또는 선박·차량 안에서 압수·수색영장을 집행할 때에는 주거주(住居主), 간수자 또는 이에 준하는 사람을 참여하게 하여야 한다(형사소송법 제123조 제1항, 제2항).

형사소송법 제219조, 제106조 제3항에 따라 정보저장매체등에 기억된 전자정보를 압수하는 경우에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 하고, 그 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 압수·수색 또는 검증 현장에서 정보저장매체등에 들어 있는 전자정보 전부를 복제하여 그 복제본을 정보저장매체등의 소재지 외의 장소로 반출할 수 있으며, 그에 따른 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 피압수자 또는 형사소송법 제123조에 따라 압수·수색영장을 집행할 때 참여하게 해야 하는 사람이 참여한 상태에서 정보저장매체등의 원본을 봉인하여 정보저장매체등의 소재지 외의 장소로 반출할 수 있다[검사와 사법경찰관의 상호협력과 일반적 수사준칙(이하 '수사준칙'이라 한다)에 관한 규정 제41조]. 그리고 검사 또는 사법경찰관은 압수·수색 또는 검증의 전 과정에 걸쳐 피압수자등이나 변호인의 참여권을 보장해야 하며, 피압수자등과 변호인이 참여를 거부하는

경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수·수색 또는 검증을 해야 한다(수사준칙 제42조 제4항).

수사기관이 전자정보의 탐색·복제·출력을 완료한 경우에는 지체 없이 피압수자등에게 압수한 전자정보의 목록을 교부해야 하고, 그 목록에 포함되지 않은 전자정보가 있는 경우에는 해당 전자정보를 지체 없이 삭제 또는 폐기하거나 반환해야 한다(수사준칙 제42조 제1항, 제2항). 이때 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 한다(대법원 2018. 2. 8. 선고 2017도13263호 판결).

실무상 형사소송법 및 위 수사준칙 규정에 따른 검찰의 전자정보에 대한 압수수색은 '디지털 증거의 수집·분석 및 관리 규정'(개정 대검예규 제1285호, 2022. 5. 18. 시행)에 따라 이루어지고, 경찰의 압수수색은 '디지털 증거의 처리 등에 관한 규칙(개정 경찰청훈령 제1030호, 2021. 8. 30. 시행)'에 따라 이루어지고 있다.

2. 원격 압수·수색

가. 원격 압수·수색의 정의

원격 압수·수색은 전자정보가 원격지 서버 등 컴퓨터와 네트워크로 연결되어 있는 외부 저장매체에 저장되어 있는 경우에 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수·수색 영장에 의하여 원격지의 저장매체에 통상적인 방법으로 적법하게 접속하여 전자정보를 수

색 장소의 정보처리장치로 내려받거나 화면에 현출시켜 압수·수색할 수 있는지 여부에 관한 것이다.

전자정보에 대한 압수·수색 장소는 원칙적으로 전자정보가 저장되어 있는 서버 등의 소재지이다. 그러나 형사소송법 제106조 제3항은 디지털 정보가 저장된 정보저장매체등을 압수 대상물로 하고 있을 뿐 컴퓨터 네트워크를 이용하여 서버 등 정보저장매체등에 접근하는 방식으로 압수하는 원격 압수·수색이 허용되는지 여부에 관하여는 명시적으로 규정하고 있지 않다[32)33)].

---

32) 국회는 형사소송법 제106조 제3항을 개정하면서, 압수 목적물에 관한 위 규정 외에 실무적으로 이에 필연적으로 부대될 수밖에 없는 수색의 장소적, 논리적 범위나 수색할 장소에 대해서는 디지털 증거의 무형성과 정보성을 반영한 규정을 신설하지 않았다(정대용·김기범·권헌영·이상진, “디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 - 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로 -” 법조(2016. 12.), 45).
그리고 형사소송법 제106조 제3항은 기기 자체에 저장된 정보에 대한 확보만을 규정하고 있을 뿐 해당 기기가 네트워크를 통해서 독점적 · 배타적으로 접근할 수 있는 데이터에 대한 확보에 대하여 별도로 규정하고 있지 않다(조아라, “이용자 디바이스를 통한 클라우드 데이터의 압수·수색에 관한 고찰”, 사법연수원(2017), 117).
형사소송법 제106조 제3항은 유형물에 대한 압수·수색을 전제로 한 전통적인 압수·수색에 기반한 것으로서 전자정보가 압수·수색의 대상이 되는지 여부에 대해서 명시적으로 규정하지 않고 있다. 즉, ‘정보저장매체’에 대한 압수·수색과 정보저장매체에 저장되어 있는 ‘전자정보’에 대한 압수·수색은 구별됨에도 위 조항은 ‘전자정보’에 대한 압수·수색에 관하여는 명시적으로 규정하지 않고 있다. 나아가 위 규정은 이메일, SNS, 클라우드와 같이 서비스 제공자가 존재하고 서비스 제공자와 서비스이용계약을 체결한 서비스 제공자가 소유 또는 소지하는 각종 전자정보가 서비스 제공자가 관리하는 서버에 저장되어 있는 경우 흔히 문제 되는 원격 압수에 대한 해답을 주지 못한다(권경선, 권경선, “국외 클라우드 컴퓨팅 서비스 이용자에 대한 압수·수색”, 이학석사 학위논문, 서울대학교, 28).

나. 원격 압수·수색에 관한 학설

서비스 사용자의 계정에 접속한 다음 서비스 제공자가 제공하는 클라우드에 저장되어 있는 전자정보를 압수·수색하는 것은 피압수자가 아닌 제3자가 관리하는 제3의 장소에 있는 서버에 저장되어 있는 전자정보를 압수·수색하는 것인데, 학계에서는 이와 같은 원격 압수·수색이 현행 형사소송법상 허용되는지 여부에 관한 논의가 있다.

(1) 적극설

현행 형사소송법 규정만으로도 원격 압수·수색이 허용된다는 견해이다. 네트워크를 통해 원격지에 있는 시스템에 접속하는 것은 형사소송법 제120조 제1항의 '압수·수색영장을 집행함에 있어서 필요한 처분'에 포함되는 것으로 해석할 수 있기 때문이라고 한다. 원격 압수·수색을 하는 경우 영장에 기재된 수색장소에서 PC 등을 이용하여 해당 서버에 접속한 후 범죄와 관련된 전자정보를 수색장소에 있는 PC 등에 다운로드하거나

33) 2021. 1. 1.부터 시행되고 있는 대검찰청 예규인 『디지털 증거의 수집·분석 및 관리 규정』 제31조에서는 원격지에 저장된 전자정보의 압수·수색·검증이라는 제목으로 "압수·수색·검증의 대상인 정보저장매체와 정보통신망으로 연결되어 있고 압수 대상인 전자정보를 저장하고 있다고 인정되는 원격지의 정보저장매체에 대하여는 압수·수색·검증 대상인 정보저장매체의 시스템을 통해 접속하여 압수·수색·검증을 할 수 있다. 이 경우 피압수자 등이 정보통신망으로 정보저장매체에 접속하여 기억된 정보를 임의로 삭제할 우려가 있을 경우에는 정보통신망 연결을 차단할 수 있다."고 규정함으로써, 원격 압수·수색이 허용된다고 보고 있다. 그러나 대검찰청 예규는 행정규칙이므로 대외적 구속력이 없고, 수사절차 단계에서 증거의 수집과 보존에 관해서만 적용된다는 점이 한계이다(권경선, 앞의 논문, 28).

출력하면 해당 전자정보가 수색장소에 존재하게 되므로 영장에서 허용한 집행의 범위를 초과하는 문제는 발생하지 않는다는 점을 근거로 든다[34].

(2) 소극설

현행 형사소송법으로는 원격 압수·수색이 허용될 수 없다는 입장이다. 영장의 장소적 범위를 벗어난 장소에 있는 컴퓨터에 대하여 영장의 효력이 미친다고 볼 수 없고, 강제처분의 대상을 저장매체로 보는 이상 다른 저장매체에 접속하여 그 내용을 인식하는 것은 허용되지 않는다고 본다. 그리고 형사소송법 제120조 제1항의 '압수·수색영장을 집행함에 있어서 필요한 처분'이 장소적 범위까지 확장하는 것은 아니고, 접속권한은 개인에 귀속되는 권한이지 컴퓨터라는 물건에 주어진 것이 아니므로 접속권한을 컴퓨터 관리권의 일부로 볼 수 없다는 점 등을 근거로 든다[35].

(3) 제한적 적극설

현행 형사소송법의 해석상 일정한 조건을 갖춘 경우에는 원격 압수·수색이 허용된다는 견해이다. 즉, 전송이 용이한 전자증거의 특성으로 인해 입력장치와 저장장치가 분리되어 있고 수사기관이 압수·수색영장 청구

34) 양근원, "형사절차상 디지털 증거의 수집과 증거능력에 관한 연구", 박사학위논문, 경희대학교(2006), 152~153; 박봉진・김상균, "디지털 증거 압수·수색에 관한 연구", 법과 정책 19집 1호, 제주대학교 법학연구소(2013. 2.), 717; 이숙연, "디지털증거의 압수·수색", 재판자료(123), 664; 압수·수색영장실무 집필위원회, 압수·수색영장실무(개정판 2010), 76; 김상우, "미국에서의 컴퓨터에 대한 압수·수색 개관", 해외연수검사연구논문집(Ⅱ), 제12집 261.

35) 전승수, 앞의 논문, 197-198; 정대용 등, 앞의 논문, 67; 노명선, 사단법인 한국포렌식학회, 한국저작권위원회 개최 국회 디지털증거 압수·수색에 관한 개정 법률안 공청회 발표문(2012. 11.) 29.

단계에서 이를 사전에 확인할 수 없거나 원격의 저장장치를 특정할 수 없는 경우에는 영장 청구시 입력장치를 특정하는 방법의 원격 압수·수색이 허용되고, 정보저장 서버까지 특정하지 않더라도 해당 정보가 그로부터 합법적으로 접속 가능한 시스템 안에 존재하는 한 영장 기재의 특정성을 위반한 것은 아니라고 한다[36].

다. 외국의 입법례

(1) 미국의 연방형사소송규칙

미국은 개정 연방형사소송규칙 §41(b)(6)30)(2016. 4. 28. 개정, 2016. 12. 1. 시행)에서, “치안판사는 일정한 상황에서 원격 접속을 통해 전자적 저장매체를 수색하거나 전자적으로 저장된 정보를 압수하는 영장을 발부할 수 있다.”라는 규정을 두어 명시적으로 원격 압수수색을 허용하고 있다[37].

(2) 유럽평의회의 사이버범죄협약

유럽평의회 사이버범죄협약(Convention on Cybercrime, 일명 ‘부다페스트 협약’)은 사이버범죄 대응에 관한 국제협약으로서, 신속한 국제공조수사 체계 구축을 위해 각 당사국에 일정한 범죄에 대하여 실체법적으로 범

36) 탁희성, “전자증거의 압수·수색에 관한 일고찰”, 형사정책연구 제15권 제1호, 한국형사정책연구원(2004), 32; 오기두, “전자정보의 수색·검증, 압수에 관한 개정형사소송법의 함의”, 형사소송 이론과 실무 4권 1호(2012. 6.), 한국형사소송법학회, 159.

37) 정문경, “원격지 저장매체에 저장된 전자정보에 대한 압수·수색”, 대법원판례해설 제114호(2017년 하), 법원도서관, 7.

죄화하여 형사처벌을 하도록 요구하고, 증거수집에 대한 절차법적인 입법 및 협약 가입국 간 국제협력 절차 수립 등을 규정하고 있다[38]. 위 협약은 2001년 11월 유럽평의회에서 채택되고, 헝가리 수도 부다페스트에서 30개국이 서명에 참가하여 2004년 7월 발효된 조약으로서 현재 미국, 일본, 호주 등 총 67개국이 가입되어 있다.

위 협약 제19조 제2항에서는 가입국의 법집행기관이 특정한 컴퓨터 시스템이나 그 일부를 수색 또는 접근함에 있어 찾는 자료가 해당 가입국의 영토 내에 있는 다른 컴퓨터시스템 또는 그 시스템의 일부에 저장되어 있고, 최초의 시스템을 통해 합법적으로 접근 또는 이용가능하다고 믿을 만한 근거가 있는 경우 다른 컴퓨터시스템이나 그 일부에 대한 수색 또는 그와 유사한 접근을 신속히 확대할 수 있도록 하는 데 필요한 입법적 조치나 방법을 취해야 한다고 규정하여 원격 압수·수색을 허용하고 있다.[39]

라. 판례

(1) 사실관계

---

38) 노명선, 사이버범죄 대처를 위한 EU 사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안, 법무부, 163.

39) EU사이버범죄 방지조약 제19조 (저장되어 있는 컴퓨터데이터의 수색과 압수) 2. 각 가입국은 그의 기관이 제1항 a)에 의한 특정 컴퓨터 또는 그것의 일부를 수색하거나 이와 유사한 방법으로 이에 접근하여 발견한 데이터가 자국 영토 내의 다른 컴퓨터시스템 또는 이 시스템의 일부에 저장되어 있고, 이 데이터가 첫 번째 시스템으로부터 정당하게 접근 가능하고 이용할 수 있다고 추측할만한 근거를 가지는 경우에는, 수색 또는 유사한 접근을 다른 시스템으로 신속하게 확대할 수 있는 것을 확보하기 위해서 필요한 입법적 또는 그 밖의 조치를 취해야 한다.

수사기관이 압수·수색영장에 따라 피의자와 변호인에게 영장을 제시하여 참여의 기회를 부여하고, 압수·수색영장에 기재된 수색장소인 한국인터넷진흥원에 설치된 인터넷용 컴퓨터에서 한국인터넷진흥원 소속 직원인 전문가와 일반인 포렌식 전문가가 참여·입회한 가운데 외국계 이메일 홈페이지인 시나닷컴(sina.com)의 로그인 입력창에 사전에 적법하게 취득한 아이디와 비밀번호를 입력하여 피의자가 이용하는 외국계 이메일 계정에 접속한 후 위 컴퓨터 화면에 현출된 이메일 본문 및 첨부문서 중 범죄 혐의사실과 관련된 부분인 총 15건을 출력하거나 캡처·저장하는 등의 방법으로 선별 압수·수색하였다.

(2) 서울고등법원 2017. 6. 13. 선고 2017노23 판결

이와 같은 압수·수색 영장의 집행에 대하여, 위 서울고등법원 판결은 적법하지 않다고 보았는데 재판부는 아래와 같은 근거를 제시하였다.

① 형사소송법에서 정하고 있는 압수·수색은 압수할 물건을 상대로 이루어지는 대물적 강제처분이라고 할 것이다. 만약 수사기관이 특정 이메일서비스 이용자로부터 이메일 계정에 관한 접근권한에 관한 자료(ID, 비밀번호)를 확보하였음을 기화로, 외국에 위치한 서버에서 해당 디지털 정보 자체를 보관하고 있는 이메일 서비스 제공자에 대한 강제처분이 아닌 그 밖의 방법에 의하여 해당 이메일 계정에 접근하여 관련 전기통신 등에 관한 자료를 확보하는 것은 형사소송법이 상정하고 있는 압수·수색의 방법은 아닌 것으로 보인다.

② 이러한 압수·수색은 형사소송법이 정하고 있는 압수·수색의 집행

방식에도 부합하지 아니한다. 압수·수색은 해당 대상물을 소지하고 있는 소유자, 소지자 또는 보관자를 상대로, 전기통신의 경우에는 해당 전기통신을 소지 또는 보관하고 있는 기관 등을 상대로 해당 물건이나 전기통신에 대하여 이루어질 것을 정하고 있는 형사소송법 제106조와 제107조의 규정과 저촉된다.

③ 그와 같은 방식의 압수·수색을 허용한다면, 처분을 받는 자에게 해당 압수·수색영장을 반드시 제시하도록 정하고 있는 형사소송법 제118조와 압수·수색이 피고인 또는 피의자의 주거지 외에서 이루어질 경우 해당 주거주 또는 간수자 등을 참여하도록 정하고 있는 형사소송법 제123조의 규정을 실질적으로 회피하게 되는 것으로 볼 수 있다.

④ 이메일 서비스 이용자의 접근수단을 이용하여 임의의 장소에서 해당 이메일 계정에 접근하여 관련 전기통신 등을 수집하는 방식의 압수·수색을 허용할 경우, 이메일 서비스 제공자의 참여를 배제한 채 이루어지게 됨으로써, 수집된 증거의 원본성과 무결성을 실질적으로 담보할 수 없게 된다.

⑤ 형사소송법 제120조 제1항에서 '압수·수색영장의 집행에 있어서는 건정(자물쇠)을 열거나 개봉 기타 필요한 처분을 할 수 있다'고 규정하고 있으나, 대상물이 해외에 존재하여 대한민국의 사법관할권이 미치지 아니하는 해외 이메일 서비스 제공자의 해외 서버 및 그 해외 서버에 소재하는 저장매체 속 디지털 정보에 대하여까지 압수·수색·검증영장의 효력이 미친다고 보기는 어렵다(이메일 서비스 제공자가 외국 기업으로 서버가 해외에 존재하는 경우 대한민국의 사법관할권이 적용되지 아니하므로

수사기관이 정보저장매체에 물리적으로 접근할 수 있는 방법이 없고, 따라서 현재로서는 형사사법공조 절차를 거치거나 개별 이메일 서비스 제공자의 협조를 얻어 디지털 정보를 제공받아야 할 것으로 보이고, 궁극적으로는 관련 법령의 개정이나 관련 외국과의 조약 체결의 방법으로 해결할 문제이다.)

(3) 서울고등법원 2017. 7. 5. 선고 2017노146 판결

한편 이와 같은 압수·수색 영장의 집행에 대하여, 다른 서울고등법원 판결은 적법하다고 보았는데 재판부는 아래와 같은 근거를 제시하였다.

① 압수·수색이 필요한 이메일 계정을 외국계 서비스제공자가 운영하고 그 관리 서버도 외국에 있는 경우에는 형사사법공조 절차를 거치거나 개별 서비스제공자의 협조를 얻지 않는 한 해당 이메일 계정에 대한 압수·수색은 사실상 곤란하게 된다. 그러나 이메일 송·수신자인 피의자가 자신의 아이디와 비밀번호로 외국 인터넷 서비스 제공자의 해외 서버에 접속하여 해당 이메일 계정에 있는 이메일 등 전자정보를 취득(통상적으로 다운로드, 출력, 화면 캡처 등의 방식에 의한다)한 후 이를 수사기관에 임의로 제출하는 것은 법적으로 아무런 하자가 없는바, 적법하게 피의자의 아이디와 비밀번호를 지득한 수사기관이, 피의자가 이메일 계정에 있는 자료의 임의제출을 거부하는 상황에서, 이에 갈음하여 법관으로부터 압수·수색영장을 발부받아 국내에서 전문가의 참여하에 해당 이메일 계정의 아이디와 비밀번호를 입력하는 방식으로 외국 인터넷 서비스 제공자의 해외 서버에 접속한 후 송·수신이 완료된 이메일 등 전자정보를 무결한 방법으로 취득하여 이를 압수·수색하는 것은 적법하다.

② 적법하게 지득한 피의자의 아이디와 비밀번호를 이용한 외국 서비스제공자 운영 이메일 계정의 압수·수색이 허용된다면, 외국의 형사 사법권을 침해한다는 우려가 제기될 여지도 있으나, 실제 압수·수색영장의 집행과정에서는 영장에 기재된 국내의 수색장소에서 온라인을 통해 해당 해외 서버에 접속하여 범죄와 관련된 이메일 등 전자정보를 국내의 수색장소에 있는 컴퓨터를 이용하여 다운로드, 출력, 화면 캡처 등의 방식으로 취득함으로써 해당 전자정보에 대한 수색에서부터 압수에 이르는 전 과정이 사실상 국내에 있는 수색장소에서 이루어지므로, 그로 인해 외국 사법권의 침해나 국제 관할위반 등의 문제가 발생한다고 보기 어렵다.

③ 위와 같은 방식의 압수·수색 과정에서 수사기관이 해외 서버 접속을 위해 기존에 적법하게 확보한 피의자의 아이디와 비밀번호를 이용하여 송·수신된 전자정보를 취득하는 것은 압수·수색영장 집행의 목적을 달성하기 위한 필요 최소한의 조치로서 그 수단과 목적에 비추어 사회통념상 상당하다고 인정되므로, 형사소송법 제120조 제1항의 '압수·수색영장의 집행에 필요한 처분'에 해당한다고 볼 수 있다.

④ 해외 서버 접속을 위해 입력한 이메일 사용자의 아이디와 비밀번호가 사전에 등록된 것과 일치한다면, 외국계 서비스제공자는 실제 해당 이메일 계정의 등록사용자 본인이 직접 접속한 것인지 여부를 식별하는 절차를 별도로 거치지 않고, 즉시 서버에의 접속을 허용하는 것이 일반적이다. 따라서 법관의 압수·수색영장 발부를 통해 정당한 접근 권한을 부여받은 제3자인 수사기관이 기존에 적법하게 입수한 피의자의 아이디와 비밀번호로 외국 서버에 접속하는 것이 위법하다고 단정할 수 없다.

⑤ 해외 서버에 접속하여 취득한 이메일 등 전자정보의 압수 과정에서 피압수자 및 전문가 등의 참여 하에 봉인, 암호 설정, 원본과 복제본의 각 해시값 산출 및 확인, 압수·수색과정의 녹화 등의 방법을 통해 전자정보의 동일성과 무결성을 충분히 확보할 수 있다.

(4) 대법원 2017. 11. 29. 선고 2017도9747 판결

위와 같은 사안에서 원격 압수·수색이 허용되는지 여부에 관하여 서울고등법원은 비슷한 시기에 상반된 판결을 각각 선고하였는데, 대법원은 원격 압수·수색이 적법하지 않다고 본 서울고등법원 2017노23호 판결의 상고심인 2017도9747호 판결에서 원심판결을 파기환송하고, 원격 압수·수색이 허용된다고 본 서울고등법원 2017노146호 판결의 상고심인 대법원 2017도11502호 사건에서 상고기각 판결을 선고함으로써, 원격 압수·수색이 적법하다는 입장을 취한 것으로 해석된다.

즉, 대법원은 수사기관이 인터넷 서비스 이용자인 피의자를 상대로 피의자의 컴퓨터 등 정보처리장치 내에 저장되어 있는 이메일 등 전자정보를 압수・수색하는 것은 전자정보의 소유자 내지 소지자를 상대로 해당 전자정보를 압수・수색하는 대물적 강제처분으로 형사소송법의 해석상 허용된다. 나아가 압수・수색할 전자정보가 압수・수색영장에 기재된 수색장소에 있는 컴퓨터 등 정보처리장치 내에 있지 아니하고 그 정보처리장치와 정보통신망으로 연결되어 제3자가 관리하는 원격지의 서버 등 저장매체에 저장되어 있는 경우에도, 수사기관이 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 영장에 따라 영장 기재 수색장소에 있

는 컴퓨터 등 정보처리장치를 이용하여 적법하게 취득한 피의자의 이메일 계정 아이디와 비밀번호를 입력하는 등 피의자가 접근하는 통상적인 방법에 따라 원격지의 저장매체에 접속하고 그곳에 저장되어 있는 피의자의 이메일 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시키는 것 역시 피의자의 소유에 속하거나 소지하는 전자정보를 대상으로 이루어지는 것이므로 그 전자정보에 대한 압수·수색을 위와 달리 볼 필요가 없다고 판시하였다.

그리고 대법원은 피의자로부터 휴대폰을 임의제출 받은 다음 네이버 클라우드에 저장된 범죄혐의사실 관련 전자정보가 있는 것을 발견하여 피의자로부터 클라우드 서비스의 아이디와 비밀번호를 임의제출의 방식으로 제공받은 다음, 수사기관이 이와 같이 알아낸 아이디와 비밀번호를 입력하여 네이버 클라우드에 저장된 범죄혐의 사실 관련 전자정보를 확보한 사안에서, 압수·수색이 적법하다고 판시[40]하여 원격 압수·수색이 허용된다고 한 위 대법원 판결을 다시 한 번 확인하였다.

---

40) 압수·수색할 전자정보가 압수·수색영장에 기재된 수색장소에 있는 컴퓨터 등 정보처리장치 내에 있지 아니하고 그 정보처리장치와 정보통신망으로 연결되어 제3자가 관리하는 원격지의 서버 등 저장매체에 저장되어 있는 경우에도, 수사기관이 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 영장에 따라 영장 기재 수색장소에 있는 컴퓨터 등 정보처리장치를 이용하여 적법하게 취득한 피의자의 이메일 계정 아이디와 비밀번호를 입력하는 등 피의자가 접근하는 통상적인 방법에 따라 그 원격지의 저장매체에 접속하고 그곳에 저장되어 있는 피의자의 이메일 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시키는 것 역시 피의자의 소유에 속하거나 소지하는 전자정보를 대상으로 이루어지는 것이므로 그 전자정보에 대한 압수·수색을 위와 달리 볼 필요가 없다(대법원 2017. 11. 29. 선고 2017도9747 판결).

다만, 대법원은 이러한 경우에도 원격지 서버에 저장된 전자정보가 특정되어야 한다고 판시하였다. 즉, 수사기관이 압수·수색영장에 적힌 수색할 장소에 있는 컴퓨터 등 정보처리장치에 저장된 전자정보 외에 원격지 서버에 저장된 전자정보를 압수·수색하기 위해서는 압수·수색영장에 적힌 압수할 물건에 별도로 원격지 서버 저장 전자정보가 특정되어 있어야 한다. 압수·수색영장에 적힌 압수할 물건에 컴퓨터 등 정보처리장치 저장 전자정보만 기재되어 있다면 컴퓨터 등 정보처리장치를 이용하여 원격지 서버 저장 전자정보를 압수할 수는 없다(대법원 2022. 6. 30 자 2020모735 결정).

마. 검토

오늘날 개인의 사진, 동영상, 위치정보, 금융거래정보 등 대부분의 전자정보는 개인의 스마트폰 등 정보처리장치보다 클라우드 서비스 제공자 등의 서버에 저장되어 있는 경우가 많고, 기업의 경우에도 업무 자료 등 정보가 클라우드 서비스 제공자가 제공하는 클라우드의 서버에 저장되는 빈도나 용량이 늘어가고 있는 추세이다.

그런데 네이버 등 국내 서비스 제공자의 경우라고 하더라도 실제 피압수자에 대한 전자정보가 어느 지역에 있는 서버에 저장되어 있는지 그 장소를 특정하기 어렵고, 구글, 아마존, 마이크로소프트 등 외국의 서비스 제공자는 여러 나라에 수십개의 대규모 서버 저장소를 운영하고 있어 전자정보가 지역적으로 다수의 공간에 분산 저장되어 있을 수 있다.

이와 같은 상황에서 원격 압수·수색을 허용하지 않는다면 압수·수색

영장 청구서의 '압수할 장소'를 특정하는 것에 상당한 시간과 비용을 들일 수 밖에 없게 되고, 위 '압수할 장소'를 특정하기 위해 별도의 압수·수색 영장을 받아야 할 경우도 생길 수 있어 압수·수색의 밀행성 및 신속성을 저해하게 된다. 그리고 구글, 아마존, 마이크로소프트 등 외국 서비스 제공자에 대한 압수·수색 영장의 청구 및 집행에 장기간이 소요되는 불합리함이 발생한다.

그리고 전자정보의 압수할 장소는 한 번 저장된 장소에 계속 저장되어 있다고 단정할 수 없고, 서비스 제공자의 서버 운영 정책에 따라 그 저장 장소가 수시로 바뀔 수 있어, 압수·수색 영장을 청구 및 집행할 때마다 전자정보의 저장 장소를 확인하여야 한다는 문제가 있다. 즉, 압수·수색 영장을 청구할 당시의 전자정보의 저장 장소와 압수·수색 영장을 집행할 당시의 전자정보의 저장 장소가 달라진다면, 위 압수·수색 영장은 적법하게 발부받은 것임에도 사후적인 사정에 의해 집행 불능 상태가 되는 것이다.

이와 같은 이유로 원격 압수·수색은 허용된다고 보아야 할 것이다. 그리고 영장 실무상 원격 압수·수색은 큰 논란 없이 그동안 허용되어 왔고, 법원도 소위 '종근당 사건'에 대한 대법원 전원합의체 결정에서 방론 형식으로 그 영장 집행의 허용성을 인정하기도 하였다[41]. 그러므로 위 대법원 판례 사안과 같은 방식의 원격 압수·수색은 현행 형사소송법상 허용

41) 원격지 서버에 저장되어 있는 정보라도 영장에 기재된 수색장소에서 해당 서버 또는 웹사이트에 접속하여 범죄와 관련된 이메일 등 전자정보를 복제하거나 출력하는 방법으로 하는 압수수색도 가능하다(대법원 2015. 7. 16.자 2011모1839 전원합의체 결정 중 다수의견에 대한 대법관 이인복, 대법관 이상훈, 대법관 김소영의 보충의견).

된다고 해석하여야 한다.

입법론의 관점에서, 앞서 언급한 유럽평의회의 사이버범죄협약에 가입하는 것을 검토할 필요가 있다. 위 협약은 67개 국가가 이미 가입하였고, 그 중 일본[42], 독일[43], 프랑스[44]는 원격 압수·수색에 관한 규정을 두고 있다. 그런데 위 협약 가입국 중 우리나라와 유사한 법체계를 가지고 있는 일본이 IT에 관한 각종 법률 정비 작업을 서둘러 진행하면서 위 협약에 가입하였다는 점은 우리에게 시사하는 바가 크다고 생각된다[45].

---

42) 일본 형사소송법 제218조 제2항 압수해야 할 물이 전자계산기인 때에는 당해 전자계산기에 전기통신회선으로 접속하고 있는 기록매체로서 당해 전자계산기로 처리하여 전자적 기록으로 보관하기 위해 사용되고 있다고 인정할 만한 충분한 사유가 있는 때에는 그 전자적 기록을 당해 전자계산기 또는 다른 기록매체에 복사한 다음 당해 전자계산기 또는 그 다른 매체를 압수할 수 있다.

43) 독일 형사소송법 제110조(문건 및 전자 저장매체의 검열) ③수색대상인 자의 전자 저장매체에 대한 검열은 검열대상인 데이터가 상실될 우려가 있다면 저장매체로부터 도달될 수 있는 한, 당해 저장매체와 공간적으로 분리되어 있는 저장매체들에까지 확대될 수 있다. 조사에 중요한 의미가 있을 수 있는 데이터는 이를 압수할 수 있다. 이에 대해서는 제98조 제2항을 준용한다.

44) 프랑스 형사소송법 제57-1조 ① 사법경찰관 또는 그의 감독 하에 있는 사법경찰리는 본법에 규정된 바에 따라 수색을 함에 있어 그 수색장소에 설치된 정보장치에 대해서도 진행 중인 수사와 관련된 정보 수색을 할 수 있다. 그 정보가 다른 정보장치에서 시동되었거나 혹은 다른 정보장치에 접근하여 압수·수색할 수 있는 경우에는 그 다른 정보장치에 대하여도 수색할 수 있다.
② 다른 정보장치로부터 접근가능하거나 다른 정보장치로부터 취득 가능한 것으로 확인된 전자정보가 국외에 설치된 경우, 현행 국제협약에 정한 접근 조건에 따라 사법경찰관이 그 전자정보에 접근할 수 있다.
③ 본조의 규정에 따라 접근 가능한 전자정보는 모든 정보매체 저장수단으로 복사할 수 있고, 정보매체 저장수단은 본법에 정한 바에 따라 봉인되고 압수된다.

45) 노명선, 앞의 책, 165.

위 협약은 서명국에 ① 컴퓨터범죄 영역에서 특정한 범죄에 대한 처벌 규정을 신설하도록 요구하고, ② 조약당사국으로 하여금 컴퓨터범죄를 수사할 절차적인 제도를 도입할 것을 요구하며, ③ 컴퓨터시스템을 통해 범해진 범죄에 국제적으로 협력·공조할 것을 제시하고 있다.

그러므로 우리나라가 위 협약에 가입하기 위해서는 위 협약의 규정에 맞도록 실체법 및 절차법을 개정하여야 한다. 먼저, 실체법적인 처벌규정 측면에서는 우리나라의 형법 및 특별법 등에서 이미 대부분 규정하고 있거나 위 협약에 맞도록 구성요건을 일부 수정하는 수준에 그쳐 크게 어려움이 없을 것으로 보인다. 그렇지만 절차법적인 측면에서는 기록명령부 제출명령,[46] 전자기록 등을 다른 매체에 복사, 인쇄, 이전 후 압수,[47] 피처

---

46) 위 협약 제18조 (제출명령) 1. 각 가입국은 a) 어떤 자가 자국의 영토 내에서 소유하고 있거나 지배하고 있고 컴퓨터시스템 내에 또는 컴퓨터데이터저장매체에 저장되어 있는 특정한 컴퓨터데이터를 제출하고, b) 서비스제공자가 가입국의 영토 내에서 그의 서비스와 관련하여 소유하고 있거나 지배하고 있는 가입자정보(subscriber information; donnés relatives aux abonnés; Bestanddaten)를 제출하도록 명령할 권한을 관할 기관에게 부여하도록 필요한 입법적 조치 및 그 밖의 조치를 취해야 한다.
2. 이 조에 의한 권한과 절차는 제14조와 제15조를 기초로 하여야 한다.
3. 이 조에서 의미하는 가입자정보란 컴퓨터데이터의 형태로 또는 그 밖의 다른 형태로 포함되어 있는 모든 정보로써, 통신데이터나 내용관련 데이터를 제외한, 서비스제공자의 서비스 이용자에 관한 것으로써 서비스제공자에게 보관되어 있고, a) 이용 중인 통신서비스의 종류, 이 서비스에 관련되는 기술적 조치 및 서비스의 기간; b) 가입자의 신원, 주소, 전화와 그 밖의 접속번호, 통신서비스와 관련한 계약이나 협약에 근거해서 이용될 수 있는 요금의 청구 및 지급에 관한 정보; c) 통신서비스와 관련한 계약 또는 협정에 근거하여 존재하는 전기통신시설이 있는 장소에 관한 그 밖의 정보를 통해서 확정될 수 있는 모든 정보를 의미한다.

47) 위 협약 제19조 (저장되어 있는 컴퓨터데이터의 수색과 압수) 3. 각 가입국은 권한 있는 기관에게 제1항과 제2항에 의해 접근한 컴퓨터데이터를 압수하거나 이와 유사한 방법으로 보전할 권한을 부여하기 위해서 필요한 입법적 조

분자에 대한 작동 기타 필요한 협력 요청[48] 등 기존 우리 절차법에서 정하지 않은 새로운 제도를 도입하여야 하므로 형사소송법 및 특별법 등에 대한 상당 수준의 입법이 필요하다는 지적이 있다[49].

이에 우리나라는 수년 간 위 사이버범죄협약에 가입하기 위한 이행입법 필요성 등을 분석한 결과, 2022. 10. 위 사이버범죄협약 가입을 위한 첫 단계로 유럽평의회에 협약 가입의향서를 제출하였다[50]. 향후 유럽평의회의 심의 및 가입 초청 절차와 국내 이행입법 절차가 남아있지만, 조속히 우리나라도 위 사이버범죄협약의 당사국이 될 것으로 기대한다.

3. 역외 압수·수색

가. 역외 압수·수색의 정의

치와 그 밖의 조치를 취해야 한다. 이러한 조치는 다음의 권한을 포함한다: a) 컴퓨터시스템 또는 그 일부 또는 컴퓨터저장매체를 압수하거나 이와 유사한 방법으로 보존할 권한, b) 컴퓨터데이터를 복제하고 반환할 권한, c) 관련된 저장컴퓨데이터의 무결성을 유지할 권한, d) 접근한 컴퓨터시스템의 컴퓨터데이터에 접근을 불가능하게 하거나 이로부터 차단할 권한.

48) 위 협약 제19조 (저장되어 있는 컴퓨터데이터의 수색과 압수) 4. 각 가입국은 컴퓨터시스템의 기능이나 거기에 포함되어 있는 데이터의 보호조치에 관하여 지식을 가진 자에게 제1항과 제2항에 언급하고 있는 조치의 수행이 가능하도록 하기 위해서 합리적인 기준에 따라서 필요한 정보를 제공하도록 명령할 수 있는 권한을 부여하기 위해 필요한 입법적 조치 및 그 밖의 조치를 취해야 한다.

49) 노명선, 앞의 책, 164-165.

50) https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=372854(외교부 보도자료 사이버범죄협약(일명 '부다페스트협약') 가입의향서 제출)

디지털 증거는 스마트폰에 저장될 수도 있지만 스마트폰과 연결된 네트워크에 존재할 수도 있다. 네트워크에 저장된 디지털 증거는 이용자가 스마트폰을 통해 클라우드에 접속하는 장소와 해당 클라우드 서비스 제공자의 소재지 및 실제 데이터가 보관되어 있는 장소가 다른 경우가 대부분이어서 클라우드 서비스 제공자의 소재지만을 압수·수색 장소로 한다면 디지털 증거를 확보하기 어려운 경우가 생기게 된다. 그리고 압수·수색영장을 청구할 때 데이터의 소재지 자체를 특정하기 어려운 경우도 많다.

특히, 구글(Google)과 같이 외국에 법인 소재지를 두고 전세계적으로 광범한 서비스를 제공하는 사업자의 경우, 이용자의 서비스 이용지역이나 서비스 가입 시점에 따라 데이터의 저장장소가 정해지는 것이 아니라 이용자의 데이터가 나뉘어져 여러 나라에 분산 저장될 수도 있고, 서버 운영 정책에 따라 한 지점으로부터 다른 지점으로 자동적으로 데이터가 이동되어 보관될 수도 있다.

이처럼 클라우드 등 전자정보를 저장한 서버가 압수·수색의 당사자국이 아닌 제3국에 존재하는 것을 역외 압수·수색이라고 한다. 역외 압수·수색에서는 수사기관이 피압수자에 대한 디지털 증거를 압수·수색하려고 할 때 당사자국이 아닌 제3국에 존재하는 데이터 서버에 저장된 디지털 증거를 당사자국 법원에서 발부한 영장으로 집행할 수 있는지가 문제의 핵심이다.

나. 역외 압수·수색에 관한 학설

(1) 긍정설

해외기업이 디지털 정보를 임의로 제공하는 경우 이를 압수하는 것은 문제가 없으므로 임의로 제공하지 않을 경우 압수·수색영장의 집행에 필요한 처분(형사소송법 제120조)에 의하여 아이디와 비밀번호를 얻어 외국 서버에 접속하는 것은 가능하다는 견해[51]와 형사소송법의 해석상 송수신이 완료되어 서버에 보관된 이메일에 대한 압수·수색의 상대방을 서버의 유지관리 책임자인 인터넷 서비스 제공자로 한정해야 한다는 제한이 있다고 보기 어렵고, 국외 소재 서버에 대한 접근은 인터넷 서비스 제공자가 서비스이용약관에 따라 메일 서버에 보관하는 이메일 정보를 로그인한 컴퓨터로 현출시켜 열람할 수 있고, 서버의 소재지를 특정하기 어려운 전자정보의 특성에 비추어 장소적으로도 문제가 없으며, 실체적, 절차적 요건도 충족하므로 허용된다는 견해가 있다[52].

(2) 부정설

역외 압수·수색의 전제가 되는 네트워크를 통한 원격 압수·수색이 현행 형사소송법의 해석상 영장의 장소적 범위를 벗어난 것으로 위법하므로 역외 압수·수색도 영장의 장소적 범위를 벗어난 것으로 위법하다고 보는 견해이다[53]. 이 입장에 따르면 해외 서버에 대한 압수수색은 다른 나라의 관할권을 침해하는 것이므로, 조약 체결의 대상이 될 뿐이다.[54]

---

51) 이숙연, 앞의 논문, 36.
52) 정문경, “원격지 저장매체에 저장된 전자정보에 대한 압수·수색”, 대법원판례해설 제114호(2017년 하), 법원도서관(2017)
53) 전승수, 앞의 논문, 197-198.
54) 오기두, 사단법인 한국포렌식학회·한국저작권위원회 개최 국회 디지털 증거 압수수색에 관한 개정법률안 공청회 토론문(주제발표 : 노명선, “디지털증거

다. 외국의 입법례

(1) 미국의 클라우드법

미국 클라우드 법은 소위 '마이크로소프트 사건'에서 비롯되었다. 이 사건은 미국 수사기관이 2013년 12월경 마약밀매 수사를 하던 중 저장통신법[the Stored Communications Act of 1986 (SCA)][55]에 근거하여 영장을 발부받았는데, 이는 마이크로소프트社에 대하여 특정 계정에 대한 이메일과 정보들을 제출하도록 요구하는 내용이었다. 이에 마이크로소프트社는 미국 내에 위치한 서버에 담겨진 정보의 제출에는 응하였지만, 아일랜드 더블린에 위치한 서버에 담겨진 정보의 제출에는 응하지 않으면서 미국 치안판사가 외국에 저장되어 있는 정보에 대하여 영장을 발부할 권한이 없다는 이유를 들었다.

이에 대하여 치안판사와 연방지방법원판사는 미국 정부의 손을 들어주었으나, 연방 제2항소법원은 하급심 판결을 뒤집고 위 영장을 무효화하였다. 이에 미국 정부가 연방 대법원에 상고하여 연방 대법원이 위 사건을 심리하는 동안, 미국 의회는 클라우드 법[the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)]을 발의하였다. 이 법은 서버가 국내외 어디에 있는지와 상관 없이 통신제공자(communication providers)들의 저장 공간에 저장통신법(SCA)이 적용되도록 개정하는 내

압수수색에 관한 법률의 문제점과 개선방안"), (2012. 11.), 44.

55) 위 저장통신법 중 핵심적인 부분은 정부기관이 전기통신서비스 제공자에게 송신자와 수신자 관련 기록들 및 통신 내용 등 전기통신서비스 제공자의 서버에 저장된 전기통신들을 제공해달라고 요청할 수 있음을 규정한 제2,703조이다.

용이었다. 이 클라우드 법은 2018년 3월 미국 의회를 통과하였고 2018년 3월 22일 대통령이 서명하여 법률이 되었다.

클라우드 법의 주요 내용은 ① 저장통신법(SCA)의 역외 적용을 명문화, ② 통신서비스제공자의 영장에 대한 이의절차 규정 신설, ③ 예양(comity) 분석 및 고려에 대한 규정, ④ 외국 기관에 대한 통신자료 제출에 관한 규정의 도입이다.

그 중 역외 압수·수색에 관한 조항으로 클라우드법 제103조는 저장통신법 제2713조(Section 2713)를 추가하였다. 이는「통신서비스제공자는 해당 통신, 기록 또는 기타 정보가 미국 내 또는 미국 밖에 저장되어 있는지 여부와 관계없이 해당 제공자가 보유, 보관 또는 통제하고 있는 유선 또는 전자통신의 내용 및 기타 기록 또는 고객 또는 가입자의 정보를 보존, 백업, 또는 공개할 법적 의무를 준수하여야 한다.」라고 규정하고 있다. 이 조항은 저장통신법이 역외 적용된다는 것으로, 통신서비스제공자는 그들이 보관하는 고객의 정보가 미국 밖에 위치하여 있더라도 해당 정보를 제출하여야 하는 것이다.

그리고 클라우드법 제105조는 저장통신법 제2,523조(Section 2,523)라는 새로운 조항을 도입하였다. 이는 미국 정부가 외국 정부와 행정협정(executive agreement)을 맺는 것과 관련된 것인데, 이러한 행정협정은 전기통신서비스 제공자들이 저장통신법을 위반하지 않으면서도 해당 협정에 근거하여 요청하는 외국 정부의 요청에 응하는 방식을 규정하고 있다. 즉, 저장통신법 제2,523조는 미국의 전자 통신 서비스 제공자가 행정협정에 따라 외국 정부의 정보 제공요청에 응할 수 있도록 법적 근거를 제공하는

규정으로, 특정 외국 정부의 국내법 및 그 실행이 데이터 수집과 관련하여 프라이버시 및 자유권을 실체적·절차적으로 강력하게 보장하는 등 법률에서 정한 요건을 충족하는 경우, 미국 법무장관에게 해당 정부와 행정협정을 체결할 수 있는 권한을 부여하고 있다[56].

(2) 유럽평의회의 사이버범죄협약

유럽평의회 사이버범죄협약(Convention on Cybercrime) 제32조[57]는 "당사국은 다른 당사국으로부터 권한을 수여 받지 아니한 상태에서 다른 당사국에게 컴퓨터 시스템을 통하여 자료를 공개할 수 있는 법적 권한을 가진 개인으로부터 합법적이고 자발적인 동의를 얻었다면 다른 당사국에 위치한 저장된 컴퓨터데이터를 당사국의 컴퓨터 시스템을 통하여 접속 및 수령할 수 있다."라고 규정하여 가입국들 사이의 상호 협조 없이도 사용자의 권한에 근거하여 컴퓨터 데이터에 대한 초국경적인 접근이 가능하도록 정하고 있다.

라. 판례

---

56) 김미영, "스마트폰 접속을 통한 역외 서버 데이터 압수방법에 관한 연구", 이학석사 학위논문, 서울대학교, 16.

57) 제32조 (공식적으로 또는 동의에 의한 저장된 컴퓨터 데이터의 초국경적 접속) 당사국은 다른 당사국으로부터 권한을 수여받지 아니한 상태에서
a. 데이터의 지리적 위치에 관계없이 (공개된) 저장된 컴퓨터 자료를 공식적으로 이용하기 위해 접속할 수 있으며 또한
b. 만약 당사국이 다른 당사국에게 컴퓨터 시스템을 통하여 자료를 공개할 수 있는 법적 권한을 가진 개인으로부터 합법적이고 자발적인 동의를 얻었다면 다른 당사국에 위치한 저장된 컴퓨터데이터를 당사국의 컴퓨터 시스템을 통하여 접속 및 수령할 수 있다.

서울고등법원 2017. 7. 5. 선고 2017노146 판결은 “적법하게 지득한 피의자의 아이디와 비밀번호를 이용한 외국 서비스제공자 운영 이메일 계정의 압수·수색이 허용된다면, 이는 해당 전자정보가 해외에 있는 관리 서버에 존재함에도 압수·수색을 허용하는 결과가 되어 서버가 소재하는 외국의 형사 사법권을 침해한다는 우려가 제기될 여지도 있으나, 실제 압수·수색영장의 집행 과정에서는 영장에 기재된 국내의 수색장소에서 온라인을 통해 해당 해외 서버에 접속하여 범죄와 관련된 이메일 등 전자정보를 국내의 수색장소에 있는 컴퓨터를 이용하여 다운로드, 출력, 화면 캡처 등의 방식으로 취득함으로써 해당 전자정보에 대한 수색에서부터 압수에 이르는 전 과정이 사실상 국내에 있는 수색장소에서 이루어지므로, 그로 인해 외국 사법권의 침해나 국제 관할위반 등의 문제가 발생한다고 보기 어렵다.”라고 판시하였다[58].

대법원은 앞서 본 원격 압수·수색에 관한 판결에서 “피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수・수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려받거나 현출된 전자정보를 대상으로 하여 범죄 혐의사실과 관련된 부분에 대하여 압수・수색하는 것은, 압수・수색영장의 집행을 원활하고 적정하게 행하기 위하여 필요한 최소한도의 범위 내에서 이루어지며 그 수단과 목적에 비추어 사회통념상 타

58) 한편, 원격 압수·수색이 적법하지 않다고 본 서울고등법원 2017. 6. 13. 선고 2017노23호 판결은 역외 압수·수색도 허용되지 않는다고 보았다. 즉, 이메일 서비스 제공자가 외국 기업으로 서버가 해외에 존재하는 경우 대한민국의 사법관할권이 적용되지 아니하므로 수사기관이 정보저장매체에 물리적으로 접근할 수 있는 방법이 없고, 따라서 현재로서는 형사사법공조절차를 거치거나 개별 이메일 서비스 제공자의 협조를 얻어 디지털 정보를 제공받아야 할 것으로 보이고, 궁극적으로는 관련 법령의 개정이나 관련 외국과의 조약 체결의 방법으로 해결할 문제라는 것이다.

당하다고 인정되는 대물적 강제처분 행위로서 허용되며, 형사소송법 제120조 제1항에서 정한 압수·수색영장의 집행에 필요한 처분에 해당한다. 그리고 이러한 법리는 원격지의 저장매체가 국외에 있는 경우라 하더라도 그 사정만으로 달리 볼 것은 아니다[59].”라고 판시하여 역외 압수·수색도 원격 압수·수색과 마찬가지로 허용된다는 입장이다.

마. 검토

구글, 아마존, 마이크로소프트 등 외국의 클라우드 서비스 제공자는 세계적으로 광범하게 클라우드 컴퓨팅 서비스를 제공하고 있고 점유율도 매우 높은 편이다. 위 사업자는 미국 외의 여러 나라에 수십개의 대규모 서버 저장소를 운영하고 있으며 구체적으로 특정하기 어려울 정도로 점차 그 수가 늘고 있다. 그리고 최근 온라인 게임을 통한 범죄도 적지 않게 발생하는 추세인데, 세계적인 온라인 게임을 제공하는 사업자도 한국 외의 중국, 미국 등 외국에 소재지를 두거나, 별도의 서버를 제3국에 두는 경우가 적지 않다. 그래서 대한민국 국민 또는 대한민국에 거주하는 외국인의 범죄에 대하여 그들이 대한민국 내에서 접속하여 사용하는 클라우드에 있는 전자정보를 압수·수색하기 위해서는 외국의 클라우드 서비스 제공자를 상대로 압수·수색 영장을 청구 및 집행할 수 있다고 해석할 필요성이 매우 크다.

이와 같은 상황에서 역외 압수·수색을 허용하지 않는다면 외국의 클라우드 서비스 제공자에 대한 압수·수색 영장의 청구 및 집행에 장기간이 소요되거나, 이에 관한 별도의 조약이 체결되어 있지 않은 현 상황에서는

59) 대법원 2017. 11. 29 선고 2017도9747 판결

외국의 클라우드 서비스 제공자에 대한 압수·수색 영장의 집행은 불가능하다는 결과가 된다.

디지털 증거인 전자정보에 대한 압수·수색은 유체물에 대한 압수·수색과는 달리 압수·수색을 위하여 우리나라의 수사기관이 국외에 위치한 서버 소재지에 갈 필요 없이 네트워크로만 이루어지므로 서버가 소재한 국가의 국가관할권을 침해한다고 보기 어렵다. 그러므로 역외 압수·수색은 현행 형사소송법상 허용된다고 해석하는 것이 타당하다.

제4장 클라우드 서비스 이용자에 대한 압수·수색

1. 클라우드 서비스 이용자에 대한 압수·수색 방식

클라우드 서비스 이용자에 대한 압수·수색은 클라우드 서비스 이용자를 피압수자로 하여 압수·수색영장을 발부받아 집행하거나 클라우드 서비스 이용자로부터 계정에 관한 아이디·비밀번호의 정보를 임의제출 받는 방식으로 이루어진다.

그 중 임의제출 방식은 이용자의 자발적인 의사에 따라 수사기관에 클라우드에 저장되어 있는 정보를 제출하는 것이므로 문제 되지 않지만 압수·수색 영장을 발부받아 집행하는 방식의 경우에는 헌법 및 형사소송법적인 문제가 발생한다. 즉, 클라우드 서비스 이용자를 상대로 계정에 대한 아아디·비밀번호 등을 제출하도록 강제할 수 있는지에 관하여 진술거

부권 침해 여부의 문제가 있다. 한편, 우리 법원은 전자정보 또는 그 출력물을 증거로 사용하기 위하여 동일성 및 무결성을 요구하고 있는데, 클라우드에서 수집한 전자정보에 대하여 동일성 및 무결성을 어떻게 확보할 것인지도 살펴볼 필요가 있다.

2. 클라우드 서비스 이용자의 아이디·비밀번호 확보와 진술거부권

가. 클라우드에 대한 압수·수색 영장 집행의 문제

클라우드 서비스 이용자에 대한 압수·수색 영장을 발부받아 이를 집행할 때에는 서비스 이용자의 클라우드 서비스 계정에 대한 아이디와 비밀번호를 입력하여 해당 계정에 접속하여야 한다. 이때 서비스 이용자인 피압수자가 자발적으로 수사기관에 클라우드 서비스 계정의 아이디와 비밀번호를 제출하면 수사기관이 이를 토대로 피압수자의 계정 접속과 마찬가지 방식으로 접속하여 해당 계정에 있는 전자정보에 대하여 수색 및 압수를 할 수 있을 것이다. 문제는 피압수자가 클라우드에 대하여 발부된 압수·수색 영장에도 불구하고 계정에 대한 아이디와 비밀번호를 제출하지 않는 경우이다. 이러한 경우 피압수자에게 클라우드 서비스 계정의 아이디와 비밀번호를 강제로 제출하도록 할 수 있는지 문제되는데, 헌법상 진술거부권의 침해와 관련된다.

나. 진술거부권 침해 여부

헌법 제12조 제2항은 “모든 국민은 고문을 받지 아니하며, 형사상 자기에게 불리한 진술을 강요당하지 아니한다.”라고 규정하여 진술거부권을 정하고 있다. 헌법재판소는 「진술거부권은 자기부죄거부의 특권(自己負罪拒否의 特權, privilege against self - incrimination)에서 유래하는 권리로서, 피고인 또는 피의자가 공판절차나 수사절차에서 법원 또는 수사기관의 신문에 대하여 형사상 자신에게 불리한 진술을 거부할 수 있는 권리로 묵비권(默秘權, right of silence)이라고도 하는바, 헌법이 진술거부권을 기본적 권리로 보장하는 것은 형사피의자나 피고인의 인권을 형사소송의 목적인 실체적 진실발견이나 구체적 사회정의의 실현이라는 국가적 이익보다 우선적으로 보호함으로써 인간의 존엄성과 생존가치를 보장하고 나아가 비인간적인 자백의 강요와 고문을 근절하려는데 있고, 이러한 진술거부권은 형사절차에서만 보장되는 것은 아니고 행정절차이거나 국회에서의 질문 등 어디에서나 그 진술이 자기에게 형사상 불리한 경우에는 묵비권을 가지고 이를 강요받지 아니할 국민의 기본권으로 보장되며, 이는 고문 등 폭력에 의한 강요는 물론 법률에 의하여서도 진술을 강요당하지 아니함을 의미한다(헌재 1998. 7. 16. 96헌바35, 헌재 1990. 8. 27. 89헌가118). 이때 "진술"이라 함은 언어적 표출 즉, 생각이나 지식, 경험사실을 정신작용의 일환인 언어를 통하여 표출하는 것을 의미한다(헌재 1997. 3. 27 96헌가11)[60].

60) 헌법재판소는, 위 결정에서, 진술거부권의 진술을 정의한 다음, ‘호흡측정’은 신체의 물리적, 사실적 상태를 그대로 드러내는 행위에 불과하고, 진술서와 같은 진술의 등가물(등가물)로도 평가될 수 없는 것이고 신체의 상태를 객관적으로 밝히는데 그 초점이 있을 뿐, 신체의 상태에 관한 당사자의 의식, 사고, 지식 등과는 아무런 관련이 없는 것이어서 호흡측정행위는 진술이 아니므로 호흡측정에 응하도록 요구하고 이를 거부할 경우 처벌한다고 하여도 ‘진술강요’에 해당한다고 할 수는 없다고 하였다.

법원 또는 수사기관이 피압수자에게 클라우드 서비스 계정의 아이디와 비밀번호를 강제로 제출하도록 할 경우 법원 또는 수사기관은 용이하게 피압수자에 대한 클라우드 서비스 계정의 아이디와 비밀번호를 획득하게 되고, 수색 및 압수 절차를 거쳐 해당 계정 안에 저장되어 있는 전자정보를 취득하게 된다. 이는 반대로 피압수자에게는 형사상 불리한 자신의 전자정보를 강제로 법원 또는 수사기관에 제출하도록 하는 결과를 초래하게 된다. 그리고 피압수자가 법원 또는 수사기관에 클라우드 계정에 대한 아이디와 비밀번호를 제출하는 행위는 생각 또는 경험사실인 아이디와 비밀번호를 정신작용의 일환인 언어를 통하여 표출하는 것이므로 진술에 해당한다.

한편, 이 문제에 대하여 미국에서는 연방 수정헌법 제5조의 자기부죄 거부 특권과 관련하여 논의되고 있다. 자기부죄 거부 특권에 따르면 피의자는 자기에게 불리한 '진술'만 거부할 수 있으므로, 혈액이나 필적의 샘플을 제공하는 등 '행위'를 강요받는 것은 수정헌법 제5조를 들어 거부할 수 없게 된다. 이에 따르면 비밀번호는 인간 내면의 정보에 해당하므로 수정헌법 제5조로 보호받는 '진술'에 해당하여 이를 근거로 진술을 거부할 수 있고, 다수의 미국 판결도 같은 논리로 수사기관이 피의자에게 비밀번호 제출을 강제하는 것은 수정헌법 제5조 위반이라고 보았다[61].

다. 검토

앞서 본 것처럼 피압수자의 클라우드 계정에 대하여 압수·수색 영장을 발부받았다고 하더라도 피압수자가 자신의 계정에 대한 아이디와 비

61) 권경선, 앞의 논문 74-77.

밀번호를 제출을 거부하는 경우 이를 강제하는 것은 피압수자의 진술거부권을 침해하는 위법한 것에 해당한다. 그리고 이를 우회하는 다른 방식(가령, 피압수자에게 스스로 아이디와 비밀번호를 입력하도록 하거나 잠금을 해제한 후 수사기관 등에 제출하도록 하는 것, 피압수자의 지문·홍채 등 생체정보를 입력하도록 하는 것 등)도 실질적으로 피압수자에게 형사상 불리한 결과를 초래하여 진술거부권을 침해하는 것으로 평가할 수 있으므로 허용되지 않는다고 볼 것이다.

만약, 피압수자에게 클라우드 서비스 계정에 대한 아이디와 비밀번호를 강제로 제출하게 하여 해당 계정에 접속하였다면 위 아이디와 비밀번호는 위법수집증거로 증거능력이 없고, 위와 같은 방식으로 접속하여 취득한 클라우드 계정 내의 전자정보 역시 위법수집증거를 토대로 획득한 2차적 증거로 유죄 인정의 증거로 삼을 수 없을 것이다.

3. 클라우드에서 수집한 전자정보의 동일성·무결성

가. 동일성 및 무결성의 의의

형사소송법 제106조 제3항은 전자정보를 압수하는 경우 압수 목적물은 전자정보를 저장한 정보저장매체이고, 다만 압수하는 방법을 달리 정하여 정보저장매체에 저장된 데이터를 출력하거나 복제하는 방식으로 하도록 정하고 있다. 그러나 클라우드에 대한 압수·수색의 경우 전자정보가 저장된 정보저장매체는 서버가 될 것이므로, 전자정보가 저장된 정보저장매체 자체를 압수하는 것은 사실상 불가능하다.

전자정보는 원본 매체에 저장된 전자정보가 다른 매체에 복사되는 등의 방식으로 이전되어 증거로 제출되고, 전체 또는 일부에 대한 수정·삭제 등 조작이 용이하며 수집·보존·분석 과정에서 인위적 조작이나 실수로 변형될 가능성이 있기 때문에 압수·수색 절차에서 전자정보의 동일성 및 무결성을 보장하기 위한 조치가 필요하다.

대법원은 전자정보 또는 그 출력물을 증거로 사용하기 위하여 동일성 및 무결성을 요구하고 있는데, 그 취지는 다음과 같다. 즉, "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 입력하여 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다." (대법원 2013. 7. 26 선고 2013도2511 판결)[62]

62) 위 판결에서 대법원은 동일성 및 무결성을 증명하는 방법에 관하여, "출력문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, 피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(hash)값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 의해 정보저장

그리고 수사준칙은 “수사기관은 전자정보의 복제본을 취득하거나 전자정보를 복제할 때에는 해시값을 확인하거나 압수·수색 또는 검증의 과정을 촬영하는 등 전자적 증거의 동일성과 무결성을 보장할 수 있는 적절한 방법과 조치를 취해야 한다(수사준칙 제42조 제3항).”라고 규정하고 있다.

나. 동일성 및 무결성에 관한 문제점

클라우드 서비스 이용자에 대한 압수·수색은 수색장소의 컴퓨터 등 정보처리장치를 이용하여 서비스 제공자의 서버에 접속한 다음 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 화면에 현출시킨 다음 이를 압수하는 방식으로 이루어진다[63]. 클라우드 서비스의 정보처리장치는 주로 외국에 존재하는 서비스 제공자의 서버가 될 것이므로 위 대법원 입장에 따르면 서비스 제공자의 서버가 정보처리장치로서 원본으로 될 것이고, 이로부터 복제된 것을 복제본으로 보게 될 것이다. 그러나 서비스 제공자의 정보처리장치를 원본으로 본다면 동일성을 증명하기가 매우 어려워진다.

매체 원본과 ‘하드카피’ 또는 ‘이미징’한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있으며, 반드시 압수·수색 과정을 촬영한 영상 녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다.”라고 판시하였다.

63) 앞에서 본 대법원 2017. 11. 29 선고 2017도9747 판결의 사실관계도 이와 같은 방식으로 압수수색 영장을 집행하였다.

한편, 휴대폰, PC, 태블릿 등 디바이스에 대한 포렌식 절차에서 쓰기 방지 등 조치를 취함으로써 압수·수색 대상에 변경이 가해지는 것을 막을 수 있는 것과 달리 클라우드에 대한 포렌식 절차에서는 이러한 조치를 할 수 없다. 오히려 클라우드 서비스 이용자는 자신의 클라우드 서비스 계정에 대한 포렌식 절차가 이루어지고 있다는 사실을 알았을 경우, 자신 스스로 또는 다른 사람을 통해, 다양한 디바이스를 이용하여 언제 어디에서든지 자신의 클라우드 서비스 계정에 접속하여 전자정보를 삭제하거나 변경·은닉할 수 있고, 수사기관이 이를 막을 뾰족한 방법은 없다. 이와 같은 이유로 무결성을 증명하는 것도 결코 쉬운 일이 아니다.

다. 판례 및 규정

앞에서 본 대법원 2017. 11. 29 선고 2017도9747 판결은 “수사기관이 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 영장에 따라 영장 기재 수색장소에 있는 컴퓨터 등 정보처리장치를 이용하여 적법하게 취득한 피의자의 이메일 계정 아이디와 비밀번호를 입력하는 등 피의자가 접근하는 통상적인 방법에 따라 원격지의 저장매체에 접속하고 그곳에 저장되어 있는 피의자의 이메일 관련 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시키는 것 역시 피의자의 소유에 속하거나 소지하는 전자정보를 대상으로 이루어지는 것이므로 그 전자정보에 대한 압수・수색을 위와 달리 볼 필요가 없다.”라고 판시하여, 전자정보를 수색장소의 정보처리장치로 내려받거나 그 화면에 현출시킨 것을 원본으로 보는 것으로 해석된다.

대검찰청 예규인 「디지털 증거의 수집·분석 및 관리 규정(2022. 5.

18. 시행)」은 원분과 복제본에 관한 명확한 정의 규정을 두고 있지 않으나, 제20조 제3항에서 '정보저장매체등의 원본'이라는 표현을 사용하고, 제29조에서 표제어로 '정보저장매체등 원본 반출 시 조치'라고 규정하고 있는 것으로 보아, '원본'이란 전자정보 압수·수색·검증을 목적으로 반출 대상이 된 정보저장매체 등을 의미하고, '복제본'이란 정보저장매체등에 저장된 전자정보 전부를 하드카피 또는 이미징 등의 기술적 방법으로 별도의 다른 정보저장매체에 저장한 것을 의미하는 것으로 해석된다. 이는 정보저장매체에 저장된 정보를 원본으로 보는 대법원과 동일한 입장으로 보인다[64].

라. 검토

위 대법원 판례의 원칙적인 입장 및 대검찰청 예규에 따르면, 정보저장매체등의 원본은 클라우드 서비스 제공자의 서버가 되므로 클라우드 서비스 이용자에 대한 압수·수색의 방식으로 전자정보를 압수하였을 경우 전자정보의 동일성 및 무결성을 입증하기 어려운 문제가 생긴다. 그리고 형사소송법 제106조 제3항 단서는 "범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다."라고 규정하고 있는데, 클라우드에 대한 압수·수색 영장의 집행에 대하여는 이 규정을 매끄럽게 적용하기 어렵게 된다.

그렇다면, 압수의 목적물에 따라 '원본'의 개념이 상대적일 수 있다는 점을 인정함으로써 동일성 및 무결성을 증명할 수 있다고 생각된다.

64) 권경선, 앞의 논문, 124-127.

즉, 휴대폰, PC, 태블릿 등 디바이스에 대한 포렌식의 경우에는 전자정보를 저장한 정보저장매체를 원본으로 보고, 클라우드 서버 등 원격지에 있거나 규모가 방대하여 사실상 정보저장매체를 압수할 수 없는 목적물에 대한 포렌식의 경우에는 위 대법원 2017도9747 판결과 같이 전자정보를 수색장소의 정보처리장치로 그대로 내려받거나 그 화면에 현출시킨 것을 원본으로 봄으로써 동일성 및 무결성 문제를 해결할 수 있다고 생각된다.[65]

제5장 클라우드에 대한 기술적 압수·수색 방법

1. 메타데이터 기반 파일 수집

가. PC에 존재하는 메타데이터 분석

윈도우즈 데스크톱 PC 클라이언트를 대상으로 웹 브라우저를 통해 클라우드 스토리지에 접근한 경우, 싱크 및 파일이 관리되는 메타데이터를 분석하여 캐시된 파일, 클라우드 서비스 인증정보 등 PC에 남아 있는 흔적을 분석할 수 있다. 이를 통해 데이터가 삭제된 경우에도 사용자를 특정하는데 필요한 데이터를 발견할 수 있다. 이는 클라우드 인스턴스에서 직접 데이터를 수집하거나 타임스탬프와 같은 파일 메타데이터를 사용하여 클라우드 컴퓨팅 환경에 저장된 데이터와 사용자 작업과의 연관성을 연결하는 데 사용될 수 있다.[66]

---

65) 같은 취지로 권경선, 앞의 논문, 128.
66) Ben Martini and Kim-Kwang Raymond Choo, “Cloud storage forensics:

그리고 스마트폰에 저장된 데이터를 백업하면서 스마트폰을 컴퓨터에 연결하게 되면 윈도우즈 시스템에도 그 흔적을 남기게 되는데 PC의 윈도우 이벤트 로그를 분석하면 사용자가 스마트폰을 컴퓨터에 연결했는지 여부 및 시간을 알 수 있다. 즉, AXIOM 프로그램을 이용하여 PC를 분석하면, 'Microsoft-Wnidows-MTPClassDriver'를 통해 스마트폰과 PC의 연결시간 등을 알 수 있고, Autoplayhandlers를 이용하여 스마트폰이 윈도우 시스템에 연결된 최초 및 마지막 시간을 알 수 있으며, Amcache.hve를 이용하여 스마트폰 연결의 흔적을 발견할 수 있다[67].

나. 스마트폰에 존재하는 메타데이터 분석

안드로이드(Android) 및 iOS 플랫폼 환경에서 스마트 기기에 존재하는 흔적을 분석하는 방법도 있다. 즉, 모바일 앱을 사용하면 형사 또는 민사 소송에서 잠재적으로 유용한 정보를 남길 수 있는데, 구체적으로 로그인, 업로드, 다운로드, 삭제 및 파일 공유와 같은 사용자 활동에서 발생하는 다양한 인공물과 포렌식으로 복구할 수 있는 파일의 타임스탬프 수정과 같은 결과를 식별할 수 있다.[68] 그리고 네트워크 PCAP 캡처 파일을 조사하면, 애플리케이션에서 사용하는 URL 및 IP 주소는 물론 로그인 및 데이터 트랜잭션에서 클라우드 스토리지 서비스에서 사용하는 타임스탬

---

ownCloud as a case study", Digital Investigation, Vol. 10, Issue 4, pp.287-299, Dec. 2013.

67) 이승무, 윈도우 디지털 포렌식 완벽 활용서, 비제이퍼블릭, 2022, 230-241.

68) Android 및 iOS 기기 모두에서 업로드 및 다운로드 활동은 원본 및 다운로드 파일의 해시값이 동일하게 유지되었으나 다운로드한 파일의 타임스탬프는 원본 샘플 파일의 타임스탬프와 달랐는데, 다운로드된 파일의 생성 및 수정 시간이 클라이언트 장치에 설정된 시간으로 변경되었다.

프, 서버 이름 및 인증 제공자를 확인할 수 있다.[69] 이에 대한 구체적인 내용은 2.항에서 살펴보도록 한다.

다. 가상 컴퓨터 생성을 통한 파일 분석

가상 포렌식 컴퓨팅 소프트웨어를 사용하는 방법도 있다. 즉, 이전에 Google 드라이브 클라이언트 소프트웨어를 설치하고 계정과 동기화한 포렌식 이미지에서 가상 컴퓨터를 생성함으로써 사용자 이름이나 비밀번호를 모르더라도 Google 드라이브 계정에 액세스할 수 있다. 구체적으로 포렌식 이미지를 가상 컴퓨터로 실행하고 클라이언트 소프트웨어에서 '웹에서 Google 드라이브 방문' 옵션을 선택하면 사용자 이름이나 비밀번호를 입력하지 않고도 계정에 연결할 수 있다.

이를 통해 구글 드라이브에서 클라이언트 애플리케이션에 대해 디렉토리 리스팅, 계정 인증정보 및 주요 파일들을 획득하고 이를 카빙할 수 있다. 이와 같은 방법을 이용하여 Apple iPhone 3G에 클라우드 스토리지를 사용한 후 남아 있을 가능성이 있는 인공물(사용자 이름, 액세스한 파일의 파일 이름)을 식별한 사례가 있다.[70]

라. 서드파티앱을 통한 메타데이터 획득 및 분석

클라우드 스토리지 내의 파일들은 파일 리스트, 파일 메타데이터 및

69) Farid Daryabar and Ali Dehghantanha, "Cloud storage forensics: MEGA as a case study", Australian Journal of Forensic Sciences, Vol. 49, Issue 3, pp.344-357, Apr. 2016.

70) Darren Quick, "Google Drive: Forensic analysis of data remnants", Journal of Network and Computer Applications, 40, pp.179-193, Apr. 2014.

파일 컨텐츠들이 모두 원격지의 저장소에 위치해 있고 각각의 클라우드 컴퓨팅 서비스마다 메타데이터의 종류 및 획득 방법이 다르며 사용자 인증 또는 파일 정보 획득에 다른 형식의 API를 지원한다.[71]

가령, 마이크로소프트의 '원드라이브'의 경우, 써드파티의 앱에서 이 클라우드 컴퓨팅 서비스를 사용할 권한을 획득하는 사용자 인증방법으로 'OAuth 2.0[72]'을 사용하는데, 포렌식 도구로 OAuth 2.0의 인증을 위임받고 원드라이브에서 제공하는 API를 통해 저장소 내의 파일들에 대한 리스트, 메타데이터, 컨텐츠를 획득할 수 있다.

이 과정을 구체적으로 살펴보면, 먼저, OAuth 클라이언트를 통해 서버와 연결하여 인증과정을 거친다. 인증이 허가되면 OAuth 클라이언트는 서버로부터 '인증코드'를 토큰으로 교환하여 서버의 자원들에 접근할 수 있다. 즉, 포렌식 도구에서 제공하는 인증 URL에 접속하여 로그인 정보를 입력하고 인증코드를 포함한 페이지를 응답으로 받은 후 인증코드를 이용하여 인증 서버로부터 인증 토큰을 받는다.

다음으로, 원드라이브 서비스가 제공하는 자원에 접근하기 위해서 저장소에 대한 접근 권한 획득이 필요하다. 마이크로소프트社의 경우에는 마이크로소프트 Graph API를 통해 원드라이브를 포함한 마이크로소프트社의 클라우드 컴퓨팅 서비스에 통합적으로 접근할 수 있다. 이때 읽기 및 쓰기 권한 외에 리프레시 토큰 발급을 위한 offline_access 권한 및 읽기 전용 접근을 위한 onedrive.readonly 권한이 필요하다.

---

71) 한중수 외 5인, 앞의 논문, 3.
72) The OAuth 2.0 Authorization Framework. Available: http://tools.ietf.org/html/rfc6749, The OAuth 2.0 Autorization Framework.

그리고 ① 파일 리스트 획득에 관하여, 원드라이브는 각각 'file'과 'folder'라는 최상위 항목으로 구분되고 각각 다른 메타데이터 값을 가지는데 파일, 폴더들은 각 아이템들의 ID, 경로 등의 식별값을 이용하여 정보를 획득할 수 있다. 구체적으로 원드라이브 저장소의 폴더 내 파일 리스트를 획득하는 API URL은 'https://graph.microsoft.com/v1.0'이고, Get URL은 "/drive/root:/path/to/folder:/children' 등 4개로 구성되며, Header는 'Authorization: Bearer <Authentication Token> Content-Type: application/json'이다.

② 파일 메타데이터 획득에 관하여, 파일 리스트를 획득할 때 JSON 형식의 응답은 파일 및 폴더에 대한 메타데이터를 포함하게 된다. 이때 획득된 메타데이터들은 파일에 대한 오브젝트 자료 구조에 저장되어 추후 분석 또는 선별에 사용될 수 있다. 원드라이브의 경우, id, createdBy, createdDateTime, lastModifiedBy, lastModifiedDateTime, description, name, webUrl 등의 메타데이터를 제공한다.

③ 파일 컨텐츠 획득은 원드라이브 서비스에서 제공하는 파일 컨텐츠 다운로드 API를 이용한다. 원드라이브는 파일 다운로드시 해당 파일 리소스가 존재하는 URL(https://graph.microsoft.com/v1.0)로 리다이렉트 시키는데, 위에서 획득한 메타데이터 중 ID 필드값을 이용하여 파일 컨텐츠 내려받기를 진행한다.

④ 선별 수집 방법 및 절차는, 원드라이브 서비스의 API를 활용하여 클라우드 저장소 내 파일들의 리스트 및 메타데이터를 획득한 후 이를 메

모리로 내려받아 기존 로컬 저장소의 파일을 분석하는 것과 동일하게 논리 이미징 방식으로 분석할 수 있다. 이때 파일 선별은 파일 이름, 크기, 수정시간 등의 메타데이터만을 사용하여 이루어질 수 있는데, 구체적으로 범행기간의 파일을 필터링하거나, 확장자(*.hwp, *.pdf 등)로 선별하거나, 클라우드 저장소 내의 경로 정보를 이용하여 선별할 수 있다.

2. 클라우드의 사용 및 삭제 흔적 추적

가. 아마존의 AWS

(1) 주요 특징

아마존 웹서비스(Amazon S3)는 안전하고 쉬운 관리 기능을 제공하는 객체 스토리지 서비스로서 사용자가 원하는 만큼 데이터를 저장하고 관리할 수 있다. 이는 버킷을 통해 객체(파일)에 대한 접근 제어를 관리하고, 버전 관리 기능을 이용하여 파일을 복원할 수 있다.

(2) 사용 흔적 추적 방법

첫째, 사용자의 PC에서 Amazon S3를 실행할 때 링크파일[73](.aws.lnk)이 생성되고 Amazon S3를 삭제하더라도 위 링크파일이 남아 있기 때문에 사용자의 PC에서 Amazon S3의 사용 유무를 판단할 수 있다. 링크파일의 경로는 아래와 같다.

C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Recent

73) 윈도우 운영체제에서 응용프로그램, 디렉터리, 파일 등 객체를 참조하는 파일

둘째, S3Browser 경로에 있는 accounts.xml, queue.v3.xml, sync-jobx.xml 파일과 로그(log) 파일을 분석하면 사용자 정보, 작업 정보 등을 확인할 수 있다. 즉, ‘accounts.xml’의 내용을 통해 사용자 이름, 버킷 이름, 마지막 사용된 액세스 키, 시크릿 키를 확인할 수 있고, ‘queue.v3.xml’의 내용을 통해 아마존 웹브라우저를 통해 작업 중인 내용을 확인할 수 있으며 아마존 웹브라우저를 통해 파일을 업로드하면 바탕화면의 임시폴더(*.tmp)에 생성된다. 그리고 ‘sync-jobx.xml’의 내용을 통해 아마존 웹 서비스와 사용자 PC간의 동기화되는 폴더와 버킷 정보를 확인할 수 있고 로그(log) 폴더의 내용을 통해 업로드 되는 파일과 마지막 동기화되는 시간 정보를 알 수 있다. S3Browser 경로는 아래와 같다.

C:\Users\<User Name>\AppData\Roaming\S3Browser

셋째, FTK Imager를 이용하여 History 파일을 추출하여 Amazon S3에 접속한 인터넷 기록을 확인할 수 있다. 즉, History 파일의 url테이블을 통해 접속 사이트, 접속 시간을 확인할 수 있고, 접속 URL을 통해 사용자 계정에 있는 버킷 이름과 폴더 이름을 알 수 있다. 그리고 History 파일의 downloads 테이블의 필드를 확인하면 다운로드 받은 파일명, 받은 시간, 받은 사이트를 알 수 있다. History 파일이 저장된 경로는 아래와 같다.

C:\Users\<User Name>\AppData\Local\Google\Chrome\User Data\Defalut

넷째, 사용자는 AWS에서 제공하는 AWS CLI를 이용하여 클라이언트에서 AWS 서버를 다룰 수 있으므로, 만약 사용자의 PC에 AWS CLI가 설치되어 있다면 AWS 사용 흔적을 더 찾을 수 있다. 이때 AWS CLI를 사용하기 위하여는 액세스 키가 필요한데, 이는 로그인 후 http://

console.aws.amazon.com/iam/home#/home에서 사용자 추가 후 생성하면 발급받을 수 있다. 액세스 키를 생성하면 액세스 키와 그 비밀번호가 저장된 액셀파일인 credential.csv를 다운받을 수 있는데 그 후 AWS CLI를 설치한 다음 'aws configure'라는 명령어를 입력하면 액세스 키를 이용하여 사용자의 AWS 계정에 접근하여 버킷 생성, 객체(파일) 업로드 및 다운로드 등 다양한 명령어를 사용할 수 있다. 해당 파일 경로는 아래와 같다[74].

C:\Users\<User Name>\.aws\credentials

(3) 삭제 흔적 추적 방법

첫째, 사용자의 PC에서 Amazon S3를 실행할 때 링크파일(.aws.lnk)이 생성되는데, 이는 Amazon S3를 삭제하더라도 남아 있기 때문에 아래 경로로 이동하면 링크 파일을 확인할 수 있다.

C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Recent

둘째, FTK Imager를 이용하여 위 경로를 통해 History 파일을 추출하였는데, 이를 'DB Browser for SQLite'라는 도구를 이용하면 Amazon S3를 삭제하더라도 Amazon S3에 접속한 인터넷 기록을 확인할 수 있다[75].

나. 구글의 드라이브

(1) 사용 흔적 추적 방법

74) 이별·장윤선·김광훈, 클라우드 포렌식, 브이메이커스, 2019, 101-112.
75) 이별·장윤선·김광훈, 앞의 책, 113-116.

첫째, 구글 드라이브 내에 업로드 및 동기화되어 있는 파일의 위치는 C:\Users\<User Name>\GoogleDrive이므로 이 경로 안에서 파일을 찾을 수 있다.

둘째, 아래 경로에 저장되어 있는 'sync_log.log'에는 동기화 세션에 대한 정보를 저장하고 있다. 즉, 업로드 및 다운로드된 파일의 정보, 구글 드라이브에서 삭제된 파일의 정보, 사용자의 계정이 연결된 시간, 사용자의 시스템이 연결된 시간에 대한 정보 등이 담겨 있다. 즉, 'Direction.UPLOAD', 'Direction.DOWNLOAD', 'Action CREATE', 'MOVE', 'RENAME', 'DELETE'를 통해 정보를 얻을 수 있는데, 가령, 'Direction.UPLOAD Action CREATE'라고 하면 구글 드라이브 서버에 파일을 업로드 및 동기화시 파일이 서버에 없다면 생성을 의미하고, 'Direction.DOWNLOAD Action CREATE'라고 하면 파일이 로컬에 다운로드되었다는 것을 알 수 있고, 다운로드 시간, 파일 이름, 다운로드한 파일이 위치한 폴더 정보를 알 수 있다.

C:\Users\<User Name>\AppData\Local\Google\Drive\user_default

셋째, 위 경로에 저장되어 있는 'snapshot.db'에 업로드(동기화)한 파일 목록과 그 외 정보들이 담겨 있는데, DB분석도구를 통해 업로드(동기화)한 파일 이름, 생성시간, 수정시간, 해쉬값, 크기, 공유된 횟수 등을 확인할 수 있다. 그리고 같은 경로에 저장되어 있는 'sync_config.db'에 구글 드라이브 정보가 담겨 있는데, DB 분석도구를 통해 설치된 구글 드라이브 버전, 동기화 경로, 구글 계정(user email), 동기화 허용 폴더 목록 등을 확인할 수 있다. 또한, 'global.db'에는 구글 드라이브 사용자 정보가 담겨 있는데, DB 분석도구를 통해 사용자 계정 정보를 확인할 수 있다

넷째, 사용자의 PC에서 구글 드라이브를 실행할 때 링크파일(*.lnk)이 생성되고 구글 드라이브를 삭제하더라도 위 링크파일이 남아 있기 때문에 사용자의 PC에서 구글 드라이브의 사용 유무를 판단할 수 있다. 링크파일의 경로는 아래와 같다[76].

```
C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Recent
```

다섯째, AWS의 경우와 마찬가지로 FTK Imager를 이용하여 History 파일을 추출하여 구글 드라이브 로그인, 드라이브 접근, 문서 접근 등의 정보를 확인할 수 있다.

여섯째, 'pagefile.sys'는 램(RAM)의 부하를 덜어주기 위해 램 공간을 하드디스크를 이용하여 처리하는 영역으로 PC에서 사용한 흔적들이 저장되고 여기에 로드되었던 것들은 시스템이 재부팅되어도 흔적이 계속 남는다. 그러므로 'FTK-Imager'와 같은 포렌식 도구를 이용하여 아래 경로에 있는 파일을 추출하면, 구글 드라이브의 흔적, 로그인한 계정, 계정의 이름을 확인할 수 있다.

```
C:\Users\jang>strings pagefile.sys >> pagefile.txt
```

(2) 삭제 흔적 추적 방법

첫째, 사용자의 PC에서 구글 드라이브를 삭제하더라도 생성된 폴더가 완전히 삭제되지 않기 때문에 사용자 PC에 있는 동기화 폴더를 통해 파일을 확인할 수 있다.

---

76) 이별·장윤선·김광훈, 앞의 책, 17-34.

둘째, 사용자의 PC에서 구글 드라이브를 실행할 때 링크파일이 생성되는데 이는 구글 드라이브를 삭제하더라도 남아 있고 구글 드라이브 동기화 폴더를 삭제하여도 남아 있기 때문에 아래 경로로 이동하면 링크파일을 확인할 수 있다.

C:\Users\<User Name>\AppData\Roaming\Microsoft\Windows\Recent

셋째, FTK Imager를 이용하여 위 경로를 통해 History 파일을 추출하였는데, 이를 'DB Browser for SQLite' 도구를 이용하면 구글 드라이브를 삭제하더라도 그 흔적을 발견할 수 있다[77].

제6장 결론

오늘날 클라우드 컴퓨팅 서비스 환경은 대중화되어 개인 사용자는 물론 기업에 이르기까지 다양한 분야에서 폭넓게 사용되고 있다. 이와 같은 클라우드 컴퓨팅 서비스의 확산에 따라 기업 또는 개인 사용자들의 데이터는 스마트폰, PC 내의 로컬 저장소에서 클라우드 저장소로 옮겨가고 있는 추세이고 그 양도 방대하다. 특히 개인 사용자들은 스마트폰, PC 등을 사용하면서 수시로 생성된 정보를 클라우드에 동기화를 하므로 클라우드에는 특정한 개인에 대한 자세하고 많은 정보가 존재하게 되고, 그와 같이 스마트폰, PC 등을 사용한 흔적에 관한 메타데이터가 해당 디바이스나 브라우저 등에 존재하게 된다.

한편, 클라우드 컴퓨팅 서비스에서는 전자정보가 원격지 서버 등 컴

77) 이별·장윤선·김광훈, 앞의 책, 35-42.

퓨터와 네트워크로 연결되어 있는 외부 저장매체에 저장되어 있는 경우가 많다. 이러한 경우 압수·수색 장소를 어떤 방식으로 특정할 것인지 문제가 될 수 있는데, 이것이 곧 원격 압수·수색 및 역외 압수·수색의 문제이다. 현행 우리 형사소송법의 규정은 이에 대하여 명시적으로 규정하고 있지 않아 해석상 견해가 나뉘지만, 대법원 판례에 의하면 허용되는 것으로 해석된다. 그렇지만 보다 근본적으로는 법령을 개정하거나 EU 사이버범죄협약에 조속히 가입하여야 할 것이다.

클라우드에 대한 디지털포렌식은 수사기관이 클라우드에서 증거로 사용하기 위한 디지털 증거를 찾는 포렌식 절차이다. 이 논문에서는 메타데이터 기반 파일을 수집하는 방법, 클라우드의 사용 및 삭제 흔적을 추적하는 방법을 검토하였다. 사용자가 클라우드 컴퓨팅 서비스에 접속한 스마트폰, PC 등 디바이스에 저장되는 메타데이터 등을 통해 증거를 획득하거나, 서드파티앱을 통해 인증 토큰을 받아 사용자의 클라우드 서비스에 직접 접속한 다음 스토리지 내 파일리스트, 메타데이터 및 컨텐츠를 획득하여 수사기관에서 증거로 활용할 수 있을 것이다.

참 고 문 헌

[국내문헌]

□ 단행본

이재상·조균석·이창온, 형사소송법(14판), 박영사, 2022

김희옥·박일환 등, 주석 형사소송법(제5판), 한국사법행정학회, 2017

오기두, 전자증거법, 박영사, 2015

토마스 얼·자이엄 마흐무드·리카르도 푸티니, 클라우드 컴퓨팅 - 개념에서 설계, 아키텍처까지, 에이콘 출판사, 2018

정재화, 클라우드 컴퓨팅, 한국방송통신대학교출판문화원, 2021

이승무, 윈도우 디지털 포렌식 완벽 활용서, 비제이퍼블릭, 2022

이별·장윤선·김광훈, 클라우드 포렌식, 브이메이커스, 2019

노명선, 사이버범죄 대처를 위한 EU 사이버범죄협약 가입 필요성과 가입에 따른 협약이행 방안, 법무부, 2011

박병민·서용성, 디지털 증거 압수수색 개선방안에 관한 연구, 사법정책연구원, 2021

이상진, 디지털 포렌식 개론, 이룬, 2010

□ 논문

김미영, “스마트폰 접속을 통한 역외 서버 데이터 압수방법에 관한 연구”, 이학석사 학위논문, 서울대학교(2020. 2.)

권경선, “국외 클라우드 컴퓨팅 서비스 이용자에 대한 압수·수색”, 이학석사 학위논문, 서울대학교(2022. 2.)

김남용·박종혁, “클라우드 컴퓨팅의 기술 및 보안서비스 연구”, 춘계학술발표대회 논문집 제24권 제1호(2017. 4.)

김동호·이상진, “구글 클라우드 데이터의 수사활용 방안에 관한 연구(스마트폰 사용자 중심)”, 디지털포렌식 연구 제12권 제3호(2018. 12.)

전승수, “형사절차상 디지털 증거의 압수·수색 및 증거능력에 관한 연구”, 법학박사학위논문, 서울대학교(2011.)

한중수 외 5인, “클라우드 스토리지 서비스에 대한 메타데이터 기반 파일 선별 수집 방법 및 구현”, 디지털포렌식 연구 제14권 제3호(2020. 9.)

이인곤, “클라우드 컴퓨팅 환경에서 전자정보 압수수색에 관한 입법적 개선방안 - 선행연구 결과에 대한 입법론적 접근 -”, 형사법의 신동향 통권 제58호(2018. 3.)

신도욱, “원격 압수·수색의 적법성 - 해외에 존재한 서버에 저장된 이메일 압수·수색을 중심으로 -”, 법조(2018. 6.)

정대용·김기범·권헌영·이상진, “디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 - 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로 -” 법조(2016. 12.)

이순옥, “디지털 증거의 역외 압수·수색”, 중앙법학 제20권 제1호(2018. 3.)

전치홍, “디지털 증거의 역외 압수수색에 관한 최신 쟁점 - 미국의 사례 및 법제를 중심으로 -”, 형사소송 이론과 실무 제10권 제2호(2018. 12.)

송영진, 미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점, 형사정책연구 제29권 제2호(통권 제114호)(2018. 6.)

한수빈·이태림·신상욱, “클라우드 컴퓨팅 플랫폼에서 디지털 증거 수집 절차”, 2014년 춘계학술발표대회 논문집 제21권 제1호(2014. 4.)

조아라, “이용자 디바이스를 통한 클라우드 데이터의 압수·수색에 관한 고찰”, 사법연수원(2017.)

양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위논문, 경희대학교(2006.)

박봉진 · 김상균, “디지털 증거 압수·수색에 관한 연구”, 법과 정책 19집 1호, 제주대학교 법학연구소(2013. 2.)

김상우, “미국에서의 컴퓨터에 대한 압수·수색 개관”, 해외연수검사연구논문집(Ⅱ), 제12집

탁희성, “전자증거의 압수·수색에 관한 일고찰”, 형사정책연구 제15권 제1호

오기두, “전자정보의 수색·검증, 압수에 관한 개정형사소송법의 함의”, 형사소송 이론과 실무 4권 1호(2012. 6.)

양종모, “클라우드 컴퓨팅 환경에서의 전자적 증거 압수·수색에 대한 고찰”, 홍익법학 제15권 제3호(2014. 9.)

정완, “클라우드컴퓨팅 서비스의 이용자 정보 압수·수색에 관한 고찰”, 법조 제70권 제3호(2021. 6.)

이재윤, “클라우드 환경에서 역외 압수·수색에 관한 연구”, 박사학위논문, 성균관대학교(2020.)

[외국문헌]

□ 단행본

Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145(2011. 9.)

□ 논문

Ben Martini and Kim-Kwang Raymond Choo, “Cloud storage forensics: ownCloud as a case study”, Digital Investigation, Vol. 10, Issue

4, pp.287-299, Dec. 2013.

Farid Daryabar and Ali Dehghantanha, “Cloud storage forensics: MEGA as a case study”, Australian Journal of Forensic Sciences, Vol. 49, Issue 3, pp.344-357, Apr. 2016.

Darren Quick, “Google Drive: Forensic analysis of data remnants”, Journal of Network and Computer Applications, 40, pp.179-193, Apr. 2014.

Hyunji Chung, Jungheum Park, and Sangjin Lee, “Digital forensic investigation of cloud storage services”, Digital Investigation, 9, pp.81-95, Nov. 2012.

Darren Quick, “Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?”, Digital Investigation, 10, pp.266-277, Oct. 2013.

Vassil Roussev, Irfan Ahmed, Andres Barreto, Shane McCulley, and Vivek Shanmug han, “Cloud forensics-Tool development studies & future outlook”, Digital Investigation, 18, pp.79-95, Sep. 2016.

Corrado Federici, “Cloud Data Imager: A unified answer to remote acquisition of cloud storage areas”, Digital Investigation, Vol. 11, Issue 1, pp.30-42, Mar. 2014.

Abstract

A Study on Search and Seizure Measures of Digital Evidence for the Cloud

An Sanghyeon
Department of Mathematical Information Science
The Graduate School
of Convergence Science and Technology
Seoul National University

Cloud computing is a general and collective concept expressing various computing concepts involving a large number of computers connected by a real-time communication network. Cloud computing services began to spread around 2010, but now various service providers such as Amazon, Google, and Microsoft are providing cloud services, and the range of services is gradually expanding.

Today, the cloud computing service environment has become popular and is widely used in various fields ranging from individual users to companies. With the spread of such cloud computing services, data of companies or individual users is moving from local storage in smartphones and PCs to cloud storage, and the amount is enormous. Therefore, the scope of the investigation agency's case-related evidence collection must also be expanded to include data in the cloud storage.

Individual users use cloud computing services while using smartphones and PCs to synchronize information generated through smartphones and PCs from time to time, so detailed and large amounts of information about specific individuals exist in cloud storage. In this way, in the process of using a smartphone, PC, etc., metadata exists in the corresponding device.

Meanwhile, in cloud computing services, electronic

information is often stored in an external storage medium connected to a computer through a network, such as a remote server. In this case, it can be a problem how to specify the seizure/search location, which is the problem of remote seizure/search and offshore seizure/search. Positive and negative opinions are divided as to whether this is permitted under the current Criminal Procedure Act, and the Supreme Court has ruled that both are permitted. However, more fundamentally, it will be necessary to review ways to revise the law or join the Cybercrime Convention.

Digital forensics for the cloud is a forensic procedure in which an investigative agency finds digital evidence in the cloud for use as forensic evidence. Digital forensics for the cloud is conducted to find digital artifacts for devices connected to cloud services. Technical difficulties arise at each stage, such as network, physical hardware, host operating system, hypervisor, guest operating system, and guest application. exist.

Regarding the digital forensic method for the cloud, this paper reviewed a method for collecting metadata-based files and a method for tracking usage and deletion traces of the cloud. to collect evidence, or obtain an authentication token through a third-party app to access your cloud account and obtain filelists, metadata, and content in cloud.

keywords : **Cloud Computing, Remote Seizure, Extra-Territorial Seizure, Cloud Forensics, Metadata**

Student Number : **2021-27970**