석사 학위논문

제3자 보관 정보 서비스 플랫폼을 통한 증거 수집 방안

2023년 2월

서울대학교 융합과학기술대학원
수리정보과학과 정보보호 및 디지털포렌식학 전공
전 수 진

제3자 보관 정보 서비스 플랫폼을 통한 증거 수집 방안

지도교수 이 병 영

이 논문을 석사 학위논문으로 제출함

2022년 11월

서울대학교 융합과학기술대학원

수리정보과학과 정보보호 및 디지털포렌식학 전공

전 수 진

전 수 진의 석사 학위논문을 인준함

2023년 1월

위 원 장 이 광 근 (인)

부 위 원 장 이 병 영 (인)

위 원 박 상 철 (인)

국문초록

전 세계적으로 온라인 서비스가 일상화되면서 사이버공간에서의 활동에 따른 범죄가 증가하고 있다. 글로벌 IT 서비스 기업의 온라인 서비스 점유율의 성장에 비례하여 사이버범죄의 초국경성으로 인해 국외 피해 규모가 급증하는 추세다. 범죄 행위가 글로벌 IT 서비스 기업을 이용한 경우 국외 서비스 제공자의 협조가 중요하다.

사이버범죄 수사에 있어 전자증거가 글로벌 IT 서비스 기업의 데이터센터에 분산되어 있는 경우에는 국제공조 방법이 필수다. 국제공조에는 공식적으로 법적 근거인 “형사사법공조 조약”, 유럽 “사이버범죄 협약”, 미국 “클라우드법 행정협정”에 의한 요청이 있다. 비공식적으로는 해외 수사기관을 통하거나 국외 서비스 제공자에 직접 요청한다.

공식 국제조약에 의거한 형사사법공조는 요청 시 협조 의무가 있지만, 요청부터 회신까지의 시간이 오래 걸려 수사의 단서가 되는 제3자 보관 정보의 신속한 확보 방법으로는 비효율적이다. 또한, 공식적인 국제공조 방법 중 “사이버범죄 협약”, “클라우드법 행정협정”의 경우 우리나라는 아직 체결하지 않아서 이러한 법적 근거에 의한 도움을 받기 어렵다.

비공식적인 국제공조 방법의 경우에는 G7 24/7 첨단범죄 네트워크, 인터폴, 해외 수사기관과 MOU를 활용하여 해외 수사기관을 통하거나 글로벌 IT 서비스 기업에 직접 협조 요청한다. 수사기관의 필요에 따라 개별적으로 국외 서비스 제공자의 제3자 보관 정보를 수집하는데, 증거 수집 절차의 부재와 기술의 미비로 인해 수사의 지연, 정보 유출 문제가 우려된다.

현재 주요 글로벌 IT 서비스 기업에는 법집행 요청 포털을 이용하여 국외 서비스 제공자가 보관하고 있는 가입자정보를 직접 요청하고 있다. 이 기업들은 법집행 요청 포털에 영장이나 허가서를 업로드하고 가입자정보를 제공받아 다운로드하는 형태다. 가입자정보는 수사를

하는데 기초가 되는 정보로, 이를 토대로 2차 추적을 실시하여 피의자 특정 및 범죄 행위 입증이 가능하다.

본고에서는 제3자 보관 정보를 수집하는 법제도적, 기술적 조치 마련을 통해 적시에 효과적으로 전자증거를 확보하도록 한다. 국외 서비스 제공자에 직접 협조 요청하는 방법을 토대로 공개키 기반 구조의 전자서명 적용 서비스를 구현하여 제3자 보관 정보 수집 과정에서 전자서명, 전자봉투, 인증서를 이용하도록 제안한다.

'제3자 보관 정보 서비스 플랫폼'을 도입하는데, 법제도적으로 뒷받침해 줄 수 있는 프로세스와 기술적으로 '공개키 기반 구조의 전자서명 암호화'를 활용하는 방식이 플랫폼 구축의 핵심이다. 법제도 및 기술적 요소를 체계화하여 수사기관이 요청하면 국제공조 전담부서에서 절차에 따라 신속하게 제3자 보관 정보를 수집할 수 있다.

국외 서비스 제공자에 협조 요청이 증가하고 있는 상황에서 전자서명 적용 서비스 플랫폼을 구현하면 수사의 효율성을 높이고 사회적 비용이 감소하여 경제적 실익이 클 것이다. 전자서명 암호화 기술로 보안성을 유지하고 수사 및 개인정보 유출의 가능성을 최소화하여 신뢰성을 확보하면서 형사소송절차에서 실체적 진실을 발견할 수 있을 것으로 기대한다.

주요어 : 제3자 보관 정보 서비스 플랫폼, 전자서명, 공개키 기반 구조, 국외 서비스 제공자, 전자증거, 사이버범죄

학번 : 2021-27350

목 차

표 목 차

그 림 목 차

제1장 서론

제1절 연구의 배경 및 목적

정보통신기술의 발달로 컴퓨터, 인터넷에 이어 모바일과 클라우드 컴퓨팅 등 새로운 기술이 진화를 계속하고 있다. 첨단기술의 발전에 따라 삶의 질 향상 이면에는 사이버범죄의 횡행으로 인한 문제도 증가하고 있다. 사이버범죄로 인한 문제가 단순히 금전적 피해를 넘어 사람의 생명과 국가의 안보를 위협하는 형태로 이동하여 심각한 현실이다.

코로나 유행의 영향으로 인해 재택근무 및 온라인 모임의 증가로 인터넷을 이용한 사이버공간에서의 활동이 활발해지면서 사이버범죄가 급증하였다. 해커가 원격 시스템을 배포한 후 보안 취약성을 이용하여 데이터를 도용하고 업무를 중단시키는 경우가 많아지고 있다. 매년 사이버범죄의 증가와 더불어 그 대상도 개인, 중소기업에서 대기업, 정부 및 주요 인프라시설로 점차 확대되고 있다.

사이버공간에서 국경을 뛰어넘어 공간을 초월하며 발생하는 범죄의 증가는 사이버범죄에 대한 경각심을 더욱 높이고 있다. 각국 수사기관은 사이버공간상 범죄의 위험성에 초국가적 범죄를 척결하기 위한 국제공조의 중요성에 대해 공감하고 있다. 사이버범죄의 경우 인터넷 특성상 초국경적이며, 범죄 특성상 전자증거 수집에서 국제공조는 필수 요소다.

사이버범죄 수사 시 증거 수집에 있어 글로벌 IT 서비스 기업이 보관하는 가입자정보, 통신내용, 트래픽데이터 등 제3자 보관 정보가 관건이 되는 경우가 많다. 전 세계가 네트워크로 연결되어 있는 상황에서 사이버범죄 수사에 필요한 제3자 보관 정보 수집을 위해 국외 서비스 제공자에 직접 요청하는 사례가 증가하고 있다. 현재 우리나라 수사기관에서도 글로벌 IT 서비스 기업의 제3자 보관 정보에 대한 증거를 수집하기 위해 노력을 기울이고 있다.

국외 서비스 제공자의 제3자 보관 정보는 국내 서비스 제공자가 보관하는 경우와 수집 절차 및 방법에 차이가 있다. 일반적으로 국내 서비스 제공자는 제3자 보관 정보 중 가입자정보의 경우 통신자료제공요청이나 압수수색영장을 통해 제공한다. 국외 서비스 제공자의 경우에는 기업 정책에 의해 정해지며 해당 국가별 설립 준거법이나 본사 소재지법에 따라 상이하다.

국외 서비스 제공자에 직접 제3자 보관 정보를 요청하는 사례는 증가하지만, 사이버공간에서 일어나는 범죄에 대응하는 정도는 기업의 규모나 지침에 따라 다르게 시행되어 어려움이 있다. 제3자 보관 정보 확보에 절차가 통일되어 있지 않아서 시간이 오래 소요되거나 기술상의 미비로 확보한 정보를 실제 수사에서 활용하지 못하는 경우가 있다. 제3자 보관 정보를 대상으로 하는 국제공조 방법 중 국외 서비스 제공자에 직접 요청하는 경우 절차의 부재로 표준화된 수집 방법에 대한 연구의 필요성이 있다.

한편, 제3자 보관 정보 수집 과정에서 개별적으로 가입자정보를 확보한 후 보관 및 관리하는 과정에서 수사정보와 개인정보 유출로 악용될 우려가 있다. 사이버공간에서 이동·삭제가 쉬운 전자증거를 확보하기 위해서는 적시성과 보안성이 요구되므로 국제공조를 통해 초국경적인 제3자 보관 정보를 효율적으로 확보하는 방안이 마련되어야 한다. 이에 따라 국외 서비스 제공자의 가입자정보를 중심으로 신속하고 안전하게 증거를 수집하기 위한 방안에 대해 모색한다.

본고에서는 제3자 보관 정보 수집 시 전자문서에 공개키 기반 구조의 암호화를 통해 전자서명한 후 전자봉투를 적용하여 '제3자 보관 정보 서비스 플랫폼'으로 전송하고자 한다. 이를 위한 법제도적, 기술적 문제를 해결할 수 있는 방안을 제시하는 것을 목표로 하여 수사의 효율성과 개인정보 보호를 보장하면서 제3자 보관 정보를 수집할 수 있도록 한다.

제2절 연구의 내용과 방법

본고는 다음과 같은 내용에 대해 연구하고자 한다.

우선 사이버범죄 개요를 통해 사이버범죄의 정의 및 유형을 살펴보고 사이버범죄 사례를 통해 국제공조의 필요성에 대해 알아본다. 다음으로 사이버범죄의 국제공조를 통한 제3자 보관 정보 확보 방법을 법적 근거에 의한 요청, 해외 수사기관을 통한 요청, 국외 서비스 제공자에 직접 요청으로 구분하여 각 방법의 특징을 비교해본다. 법적 근거에 의한 요청에는 “형사사법공조 조약”, 유럽 “사이버범죄 협약”, 미국 “클라우드법 행정협정”이 있다. 해외 수사기관을 통한 요청은 G7 24/7 첨단범죄 네트워크, 인터폴, 해외 수사기관과 MOU에 대해 다룬다.

국외 서비스 제공자의 협조는 사람들이 많이 이용하는 글로벌 IT 서비스 기업인 마이크로소프트, 구글, 트위터, 페이스북(인스타그램)의 요청 방법에 대해 알아본다. 이 기업들의 본사가 있어 직접 요청하는 빈도가 높은 미국과의 직접 협조 요청 현황에 대해 살펴본다. 현행 국외 서비스 제공자 협조 요청의 경우 절차가 통일되어 있지 않고 개별적으로 가입자정보를 수집하는 과정에서 업무의 비효율성 및 기술적 요소의 미비로 인한 정보 유출 문제가 있다. 이러한 문제점을 해결할 수 있는 법제도적, 기술적 방안을 고찰해본다. 현행 직접 협조 요청의 대안으로 공개키 기반 구조의 전자서명 적용 서비스 플랫폼인 ‘제3자 보관 정보 서비스 플랫폼’을 제안한다.

앞서 제안한 제3자 보관 정보 서비스 플랫폼의 핵심인 공개키 기반 구조의 전자서명에 대해 구체적으로 소개한다. 전자서명의 전제조건이 되는 공개키 기반 구조의 의의를 중심으로 공개키 기반 구조의 형태 및 구성 요소, 관리 대상 순으로 다룬다. 전자서명의 이해를 돕기 위해 전자서명의 개념, 전자서명의 방식, 특수 전자서명의 유형을 자세히 살펴본다. 현행법상 공개키 기반 구조의 전자서명의 내용을 기술하고 공개키 기반 구조의 전자서명을 활용한 전자서명 적용 서비스 플랫폼의 암호화에 대한 설명을 추가한다.

마지막으로 전자서명 적용 서비스 플랫폼의 구현 관련해서 전자서명의 적용, 제3자 보관 정보 서비스 플랫폼의 도입 및 효과를 연구한다. 전자서명의 과정, 전자서명 적용 서비스, 전자봉투로 전송, 전자서명 서비스의 특징을 통해 전자서명의 적용에 대해 살펴본다. 제3자 보관 정보 서비스 플랫폼은 기존 형사사법정보시스템을 개선하고 '공개키 기반 구조의 전자서명 암호화' 기술을 적용하여 구현한다. 제3자 보관 정보 서비스 플랫폼 절차를 토대로 '접속 포털'은 서명 및 관리, '내부 시스템'은 저장과 보관 기능이 가능하도록 구성한다. 접속 포털과 내부 시스템의 유기적 연결을 통해 사이버범죄에 이용된 제3자 보관 정보 수집이 원활하게 이루어지도록 설계한다. 제3자 보관 정보 서비스 플랫폼 도입을 통해 제3자 보관 정보 수집 과정에서 전자서명 적용 서비스 플랫폼의 보안성 및 효율성 향상으로 인한 기대 효과에 대해 기술하면서 논의를 마무리한다.

제2장 사이버범죄 개요

제1절 사이버범죄의 정의

온라인상에서의 사이버범죄 발생이 전 세계적으로 증가하고 있다. 현재 사이버범죄에 대해 명확하게 확립된 정의는 없지만 일반적으로 사이버공간에서 일어난 범죄를 나타낸다. 사이버범죄는 크게 사이버공간의 등장으로 컴퓨터 시스템과 네트워크 자체를 범죄의 대상(target)으로 삼아 컴퓨터 시스템의 원활한 작동을 방해하는 형태와 전통적인 범죄가 사이버공간에서 정보통신기술을 활용하여 컴퓨터 시스템과 네트워크를 범죄의 도구(tool)로 이용하는 형태로 구분된다.

사이버공간의 등장으로 새롭게 발생한 사이버범죄 형태는 사이버공간이라는 새로운 공간이 등장하면서 나타난 불법 행위다. 정보통신망 침해 범죄는 정당한 접근 권한이 없거나 접근 권한을 넘어

정보통신망에 침입 또는 시스템, 데이터 프로그램을 훼손·변경하여 컴퓨터 시스템에 성능 저하, 사용 불능 등 장애를 유발한다. 고도의 기술적 요소에 해당하며, 컴퓨터와 정보통신망 자체에 대한 공격을 수반하는 범죄로 정보통신망을 매개로 하지 않은 경우도 포함한다. 기존의 규정으로는 규제하기 어려운 범죄 행위로 해킹, 악성코드 유포, 디도스 공격 등이 이에 해당한다.

사이버공간을 이용한 전통적인 범죄는 기존에 존재해온 불법 행위가 사이버공간이라는 새로운 공간에서 행해지는 형태다. 정보통신망 이용 범죄는 범죄의 본질적인 구성 요건에 해당하는 행위를 하는 주요 수단으로 정보통신망을 이용한 경우에 해당한다. 전통적인 범죄를 행하기 위해 컴퓨터 시스템을 이용하는 인터넷 사용자 간 범죄로 사기, 도박, 개인·위치정보 침해, 저작권 침해, 성착취물 유포, 명예훼손·모욕, 스토킹 등이 있다. 한편, 불법 콘텐츠 범죄는 정보통신망을 통해 유통되는 콘텐츠 자체가 불법적인 경우로, 법률에서 금지하는 재화, 서비스나 정보를 정보통신망으로 배포·판매·임대·전시하는 경우다.[1)]

사이버범죄를 다루는 사이버범죄 협약에서는 범죄의 폐해가 심각하고 국제공조가 시급한 범죄를 나누어 규정하고 있다. 협약에서 규정하는 9개의 사이버범죄 범위에는 불법접속, 불법감청, 데이터 침해, 시스템 방해, 장치 남용, 컴퓨터 관련 위조, 컴퓨터 관련 사기, 아동음란물, 저작권 침해 범죄가 포함된다. 전통적인 범죄에 비해 사이버공간에서 일어나는 범죄는 피의자를 특정하기 어려워 증거의 역할이 커지고 있다. 사이버범죄 수사를 하는데 필요한 전자증거는 휘발성이 강해 신속한 확보가 중요하다.

제2절 사이버범죄의 유형

사이버공간이 등장하면서 나타난 해킹, 악성코드 유포, 디도스 공격,

1) 사이버범죄 신고시스템 웹사이트 “사이버 범죄 분류” <https://ecrm.police.go.kr/minwon/crs/quick/cyber1> (2022. 11. 30. 방문).

피싱·파밍·스피어피싱 등 불법 행위는 신종 범죄 유형이다. 사이버범죄는 기술의 발달에 따라 다양한 형태로 진화하며 발생하고 있다.

1. 해킹

최근 가상자산 거래가 활발해지면서 해킹을 통한 거래소, 개인지갑의 가상자산 탈취가 빈번하게 일어나고 있다. 가상자산이 네트워크 기반이므로 해킹의 위험이 높고, 이를 방지하고 보안을 강화하기 위해 블록체인 방식을 도입했지만 해킹 발생률은 여전히 높다. 대표적인 가상자산인 비트코인은 해킹, 횡령 등 범죄의 대상이 되고 있다. 가상자산 해킹 관련 범죄는 범죄대상이 가상자산 거래소가 보유하고 있는 가상자산으로, 거래소에 있는 가상자산 지갑이 보안의 취약점이다. 가상자산은 보안성이 높지만 이를 거래하는 가상자산 거래소는 블록체인기술과 연관이 없어 보안에 취약한 허점을 노린 범죄가 발생하는 것이다.

최초의 가상자산 거래소 해킹은 2014년 2월 마운트곡스 해킹 사건으로, 비트코인 약 85만개를 분실하면서 사이트는 폐쇄되고 마운트곡스는 파산에 이르렀다. 이 사건을 계기로 가상자산이 해킹에 안전하지 않다는 인식이 확산되어 비트코인 가치가 폭락하였다. 한편, 2018년 4월에는 우리나라 최초로 가상자산 거래소 야피존이 해킹당했다. 이후 유빗이 영업을 승계하였지만 한 차례 더 해킹을 당한 후 코인빈이 인수하였고, 두 차례 해킹으로 225억원 규모의 가상자산을 탈취당한 회사는 결국 파산하였다.

가상자산 거래소 해킹은 4가지 유형으로 구분할 수 있다. 워터링홀을 이용한 침투는 가상자산 거래소 직원이 가상자산 커뮤니티 게시글에 심어진 공격코드에 접근하면 해커들은 가상자산 거래소 내부시스템을 감염시키고 지갑을 해킹해서 가상자산을 탈취한다. 스피어피싱은 해커가 가상자산 거래소 직원에게 피싱 이메일을 보내 첨부파일을 내려받은 직원의 컴퓨터에 악성코드를 심고 관리자계정, 지갑 등을 탈취한다.

가상자산 거래소 개인정보 탈취는 해커가 거래소 홈페이지 관리자 전용 페이지를 해킹해서 회원정보를 탈취하고 거래소를 사칭하여 악성 이메일을 보내 가상자산 송금을 유도하는 방식으로 이루어진다. 공급망 공격은 가상자산 거래소가 주기적으로 업데이트하는 것을 이용하여 해커가 서버 설정 파일을 해킹하고 내부망을 장악해서 가상자산을 탈취한다.

2. 악성코드 유포

악성코드(Malware)란 Malicious(악의적인)와 Software(소프트웨어)의 합성어로 사용자가 원하지 않는 일을 몰래하는 소프트웨어다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제2항에는 “누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하여서는 아니 된다.”라고 규정하고 있다.

사이버공간에서 해커는 사람이 직접 행하는 범죄 행위들을 악성코드가 대신하도록 프로그램을 만들고, 원격에서 조종해서 원하는 목적을 이루므로 악성코드는 사이버범죄의 필수 도구다. 악성코드 감염대상 기기로 기존에는 윈도우를 사용하는 컴퓨터에서 스마트폰, 태블릿 기기 등을 목표로 유포되는 경우가 점점 증가하는 추세다. 이러한 악성코드는 개인을 대상으로 금융 및 개인정보 유출, 광고 노출, 가짜 프로그램 사기, 협박 등 정치적·금전적 목적으로 유포된다. 한편, 국가기관 및 기업을 대상으로는 내부망 침투, 사이버테러, 기밀정보 유출, 데이터 조작, 이메일 사기, 네트워크 감청 등을 위해서 광범위하게 유포되고 있다.

악성코드 종류에는 기밀자료 및 정보 유출형, 협박 및 금전 요구형, 개인 금융정보 탈취형이 있다. 기밀자료 및 정보 유출형은 악성코드 관리 도구인 원격 접속 트로이목마(Remote Access Trojan, RAT)를 이용하여 악성코드 파일을 쉽게 생성하고, 감염된 좀비 컴퓨터를 원격제어 기능으로 관리한다. 협박 및 금전 요구형의 대표적 형태인

랜섬웨어(Ransomware)는 몸값(Ransom)과 제품(Ware)의 합성어로 사용자의 컴퓨터나 문서를 인질로 삼아 금전을 요구하는 수법이다. 악성 이메일 첨부파일, 웹 취약점 등을 악용하여 유포되며, 추적을 피하기 위해 비트코인과 같은 가상자산을 요구한다. 개인 금융정보 탈취형은 컴퓨터에 저장된 인증서를 유출하고 도메인 정보를 변조하여, 은행 사이트 접속 시 피싱 사이트로 유도해 컴퓨터 사용자 인터넷뱅킹 정보를 탈취한다.

악성코드는 주로 이메일, 웹사이트, 정상 프로그램 위장 등을 통해 유포되고 있다. 이메일을 통한 유포는 이메일 원문, 이메일 시스템의 수발신 로그를 수집한 후 발신자 주소, 발신 IP, 수신자 주소, 수신 일자, 악성 첨부파일, 악성 링크 등을 분석한다. 분석 결과를 토대로 발신 IP의 서비스 제공자 가입자정보, 발신자 이메일 가입자정보, 악성코드 제어서버를 추적한다. 웹사이트를 통한 유포는 우선 악성코드 감염 컴퓨터, 악성코드 유포 다운로드 사이트 및 웹소스 채증, 악성코드 발췌, 유포 사이트 운영사 확인, 사이트 웹로그를 확보한다. 이를 통해 유포에 악용된 취약점, 유포 경로, 유포 사이트 해킹 경위, 악성코드를 분석한 후 유포 사이트 침해 IP, 악성코드 제어서버 등을 추적한다. 정상 프로그램 위장은 악성코드 감염 컴퓨터, 감염경로 확인 후 업데이트 서버를 수집한다. 감염 컴퓨터에서 윈도우 아티팩트[2] 분석으로 감염경로 확인, 업데이트 서버 로그에서 감염 컴퓨터 확인, 악성코드 분석을 통해 제어서버 확인을 하여 업데이트 서버 침해 IP, 악성코드 제어서버를 추적한다.

3. 디도스 공격

디도스(Distributed Denial of Service, DDoS)[3]는 악성 프로그램에 감염된 다수의 컴퓨터를 이용하여 특정 인터넷 서버에 대량의 트래픽을 전송하여 서버의 정상적인 서비스 이용을 방해하는 사이버 공격이다.[4]

---

2) 컴퓨팅 환경에서 시스템이 운영되면서 사용자 또는 운영체제에 의해 남게 되는 모든 흔적.

3) 분산서비스 거부 공격.

이용자 컴퓨터가 좀비 컴퓨터로 변하고, 해커로부터 공격명령을 받으면 공격이 실행된다. 2009년 7월 7.7 디도스 대란, 2011년 4월 농협 전상망 마비 사태 등 대형 사이버범죄에 가정 및 회사에서 사용하고 있는 컴퓨터가 주요 국가기관과 금융기관 등을 공격하는 좀비 컴퓨터로 악용되었다.

디도스 공격이 이루어지는 과정은 크게 4단계로 나누어 볼 수 있다. 우선 해커는 컴퓨터에 보안 취약점이 있는 홈페이지를 해킹해 홈페이지에 악성프로그램을 숨긴다. 악성프로그램이 숨겨진 사실을 모르는 인터넷 이용자가 홈페이지를 방문하여 게시물을 열람하면 컴퓨터는 악성프로그램에 감염된다. 이때 설치되는 프로그램이 디도스 공격의 범행도구로, 이용자 컴퓨터는 좀비 컴퓨터가 되는 것이다. 이 악성프로그램은 트래픽 유발 및 다른 기능이 포함되도록 해커가 프로그램을 추가하거나 변경할 수 있다. 좀비 컴퓨터는 해커에게 감염사실을 알리고 대기하고 있다가 명령을 전달하는 좀비 컴퓨터가 다수의 좀비 컴퓨터에 디도스 공격명령을 전달한다. 공격명령에 따라 다수의 좀비 컴퓨터가 자동으로 공격 도구를 실행하여 특정 사이트를 공격한다.

4. 피싱·파밍·스피어피싱

피싱(Phishing)은 수사기관, 금융기관 등에서 보낸 이메일, 메시지로 위장하여 사용자가 가짜 사이트에 접속하도록 유도한 뒤 개인정보, 금융정보를 탈취하는 방식이다. 이메일에 포함된 웹페이지 주소(Uniform Resource Locator, URL)를 누르는 순간 공격자가 미리 개설해 놓은 피싱 사이트로 연결되고, 사용자가 입력하는 계정정보가 공격자에게 전송되도록 설계되어 있다.

파밍(Pharming)은 악성코드로 사용자의 컴퓨터를 감염시켜 도메인 서버 주소를 변조함으로써 사용자가 정상적인 사이트 주소를

---

4) 전완근, “디도스 공격증거와 법적 책임”, 대검찰청, 형사법의 신동향 제32호 (2011), 112면.

입력하더라도 가짜 사이트로 자동 접속되도록 유도하는 수법이다. 피싱의 경우에는 사용자가 웹페이지 주소를 유심히 살펴보면 가짜임을 알아차릴 수 있지만, 파밍은 평소에 사용자가 이용하는 사이트로 알고 의심 없이 접속한다. 피싱에 비해 파밍의 경우 계정이나 금융정보를 노출시킬 위험성이 더 크다.

스피어피싱(Spear Phishing)의 경우 불특정 다수를 대상으로 하는 피싱과 달리, 특정기관의 내부직원을 표적으로 삼는다. 지능형 지속 위협(Advanced Persistent Threats, APT) 공격[5]의 시발점으로, 계정 정보를 탈취하거나 악성코드를 감염시키기 위한 피싱 시도로 많이 사용된다. 스피어피싱은 특정인의 계정을 탈취함으로써 계정에 보관된 중요 정보를 수집하거나 특정인의 컴퓨터를 악성코드에 감염시켜 소속 기관의 내부시스템에 잠입하기 위한 수단이다.

제3절 국제공조 필요성

오늘날 사이버공간에서 자유로운 의견 교환으로 표현의 자유가 촉진되는 반면, 온라인 활동 증가에 따라 사이버범죄가 폭증하고 있다. 사이버범죄 수사에서 중요한 전자증거는 디지털매체에 보관되거나 디지털매체를 통해 전송되는 정보로 쉽게 사라지고 있다. 국외 서비스 제공자로부터 제공받는 제3자 보관 정보도 디지털매체에 보관하고 있는 정보를 전송받는 것으로 전자증거로 볼 수 있다.[6]

사이버공간상 일어나는 범죄는 수사 단서의 범위가 확대되어 외국에 제3자 보관 정보를 요청하는 경우가 증가하고 있다. 유럽연합 집행위원회(European Commission)의 보고서에 따르면 전 세계 형사사건 중 85%가 전자증거와 관련있고, 이 중 2/3가 해외 소재 서비스 제공자로부터 제공받아야 한다. 정보통신기술의 발전으로 수사의

---

5) 사전조사, 제로데이 공격, 사회공학, 은닉, 적응, 지속의 6단계 과정.

6) 김윤섭·박상용, “형사증거법상 디지털 증거의 증거능력”, 형사정책연구 26(2), (2015), 168면.

50% 이상에서 전자증거에 대한 초국경적 접근 요청이 필요하다.[7] 즉, 형사사건 중 절반 이상이 외국과의 수사공조가 요구됨에 따라 국제공조의 필요성은 더욱 커지고 있다.[8]

초국가적 사이버범죄를 척결하기 위해서 국제공조는 필수적이며, 사이버공간상 전자증거는 휘발성이 강해 소멸되기 쉬워서 증거 확보에 어려움이 크다. 사이버범죄의 증가로 제3자 보관 정보가 중요해짐에 따라 국제공조를 통해 요청하는 사례가 늘면서 그 필요성이 부각되고 있다. 사이버범죄에 있어 국제공조는 중요하며 국외 서비스 제공자가 관리하고 있는 제3자 보관 정보를 직접 요청해 제공받아 활용하면 신속한 수사에 도움이 될 것이다.

온라인을 통한 사이버범죄가 횡행하는 상황에서 국경을 넘나드는 사이버범죄에 대한 심각성이 더욱 높아지고 있다. 사이버공간을 이용한 사기의 경우 소개팅 사이트를 개설하고 보증금을 편취하거나 랜덤채팅 앱에 접속하여 성매매를 하겠다고 유도한 다음 선입금을 받아 취득하는 방식으로 수십억원을 편취하였다. 사이버 도박 사건은 해외 결제 대행 업체를 통해 도박자금을 충전한 후 해외 인터넷 도박 사이트에서 상습적으로 도박하는 방식으로 이루어졌다. 사이버공간을 이용한 범죄 중 성착취물 유포의 경우 'N번방 사건' 이전부터 큰 비중을 차지하였는데, 그 기간이 수년에 걸쳐 이루어지는 특징이 있다.

2013년 6월에서 2016년 12월까지 성매매업소 광고를 목적으로 해외에서 음란 사이트를 개설하고 아동음란물, 불법촬영물 등을 게시하여 성매매업소로부터 광고대금을 지급받은 사례가 있다. 또한,

---

7) Michael Plachta, "European Commission Recommends Negotiating a Treaty with U.S. on Access to Electronic Evidence", 35 No. 3 Int'l Enforcement L. Rep. 78 (2019), 1면.

8) European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules of the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings" (2018), 14면.

2013년 12월부터 2017년 4월 사이에 미국에 음란 사이트를 개설한 후 상품권이나 비트코인 결제를 통해 회원들로부터 아동음란물 등 46만여편을 게시하도록 하였다. 등급별 회원을 관리하는 방법으로 사이트 이용요금 및 광고대금을 통해 부당이득을 취득하였다. 베트남에서는 2015년 9월에서 2017년 1월 사이 미국, 일본에 서버를 두고 음란 사이트를 운영하며, 아동음란물을 게시하여 광고비로 비트코인을 지급받았다.[9)]

2017년 전 세계에 퍼진 'NotPetya' 랜섬웨어, 2019년 코로나를 악용한 위조 의료용품 온라인 판매와 인터넷을 통한 사기 등 신종 사이버범죄가 지속적으로 발생하고 있다. 2022년 1월에는 웹사이트가 훼손되고 여러 정부기관에 속한 데이터가 지워지는 사건이 있었다. 지난 2월 우크라이나에 대한 러시아의 침략이 시작된 이후 우크라이나의 발전소와 인프라시설, 정보 기술 자원에 대한 공격이 계속되고 있다.

기술의 발달과 법제도 사이의 간극을 줄이고 사이버범죄 퇴치를 향해 다음 단계로 전진하는 것이 필요한 시점이다. 사이버범죄를 엄단하고 사이버공간에서 자유롭게 활동하기 위해 범죄 관련 증거를 신속하게 확보할 수 있는 환경이 요구된다. 사이버범죄는 현실과 가상 공간을 넘나들며 첨단화·국제화·가상화되는 양상을 띠고 있으므로 제3자 보관 정보 수집을 위해서는 효율적인 국제공조체계를 정립해야 한다.

제3장 국제공조 방법

제1절 법적 근거에 의한 요청

사이버범죄는 주요 증거가 정보통신기술과 관련되며, 이러한 전자증거의 경우 외국에 존재하는 경우가 많다. 대부분 국가의 영장

9) 최훈제, "가상화폐 압수수색 표준절차 및 정족수다중서명을 이용한 압수물관리방안 제안", 석사학위논문, 서울대학교 (2019), 2면.

범위는 각국의 영토 내에 해당하므로 범죄에 대한 중요한 증거가 해외 서버에 존재할 경우 영장에 의한 집행이 불가능하다. 각국 수사기관은 관련 전자증거를 획득하기 위해 소재지 국가에 법적 근거인 형사사법공조 조약, 유럽 사이버범죄 협약, 미국 클라우드법 행정협정에 의해 요청한다.

1. 형사사법공조 조약

외국에 있는 증거를 확보하기 위해서 공식적으로 형사사법공조 조약(Mutual Legal Assistance Treaty, MLAT)을 활용하는 방법이 대표적이다. 이는 국가 간 체결한 조약에 의해 사건의 수사·기소·재판에 따른 소재 수사, 증거 수집, 압수수색 등을 위해서 협조를 제공하거나 받는 형태로 이루어진다.

우리나라의 형사사법공조 범위와 절차 등은 국제형사사법 공조법으로 정하고 있다. 국제형사사법 공조법 제3조에 “공조에 관하여 공조조약에 이 법과 다른 규정이 있는 경우에는 그 규정에 따른다.”라고 명시하고 있는 점을 볼 때 형사사법공조 조약이 국제형사사법 공조법보다 우선한다.

현재 우리나라는 형사사법공조 조약이 77개국과 체결(발효 77개국)[10] 되어 있다. 조약 미체결국도 상호주의 원칙에 따라 동일한 사항에 관해 요청국이 한국의 공조 요청에 따른다는 보증이 있으면 공조를 진행할 수 있다. 2021년 기준으로 우리나라가 형사사법공조를 요청한 경우는 741건, 외국에서 형사사법공조를 요청받은 경우는 285건으로 2020년 각각 420건, 202건에 비해 급증하였으며 매년 증가하고 있는 추세다.[11]

형사사법공조는 공식적인 공조 국제조약을 통한 요청이므로 체결국 간 강제력이 있고 절차가 표준화되어 있으며, 진행절차는 개인의 권리를 보호하기 위한 법적 요건을 충족한다. 형사사법공조 요청을 통해 확보한 증거는 형사 절차상 증거로 사용할 수 있다. 한편, 형사사법공조 조약을

10) 법무부, 『2021년 법무연감』 (2022), 310면.
11) 법무부, 앞의 자료, 311면.

활용하는 방안은 미체결국의 경우 새로운 조약을 맺어야 하고, 기체결국의 경우에는 데이터를 확보하는데 시간이 오래 걸린다. 형사사법공조의 경우 요청 절차가 복잡하고 시간이 많이 소요되는 비효율성으로 인해 실제 다수의 사이버범죄 수사가 방치되고 있다.

형사사법공조는 외교절차를 거치며, 법무부가 중앙기관으로 수사기관에서 법무부, 외교부를 거쳐 상대국에 절차를 진행하는데 요청부터 회신까지 수개월이 걸린다.[12] 이는 휘발성이 강해 신속성을 요구하는 사이버공간에서 일어나는 범죄의 증거 수집 방법으로는 비효율적이다. 글로벌 IT 서비스 기업의 데이터 보관 기간은 대부분 90일이므로 형사사법공조를 통해 증거를 확보하려고 할 경우 이미 삭제되어 존재하지 않을 가능성이 크다.[13] 신속한 증거 수집을 요구하는 사이버범죄에서 절차가 복잡하고 시간이 많이 소요되는 형사사법공조를 진행하기에는 어려움이 있다.

클라우드 컴퓨팅 기술이 발전함에 따라 글로벌 IT 서비스 기업이 데이터를 전 세계 데이터센터에 분산 보관하여 수사기관에서 필요한 데이터의 소재를 파악하지 못하는 경우가 있다. 형사사법공조는 당사국 간 상호협의에 의해 이루어지는데, 여러 국가의 관할에 서버가 있어 데이터 위치 확인 불가로 영토주의를 적용할 수 없을 경우에는 공조를 할 수 없다. 미국의 경우 수사의 효율성을 위해 통신내용, 트래픽데이터 등 민감한 자료는 형사사법공조를 통하고, 가입자정보는 국내 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 전제로 직접 제공한다.

2. 유럽 사이버범죄 협약

사이버범죄 협약(Convention on Cybercrime, 일명 “부다페스트 협약”)은 2001년 유럽평의회가 주도하여 만든 사이버범죄를 다룬 최초의 구속력 있는 다자간 협약이다. 2022년 11월 기준 전 세계 67개국[14]이

12) 박재성, “사이버범죄 국제조약의 동향”, 저스티스 통권 제185호 (2021), 266면.
13) 박다온, “외국의 정보통신 서비스 제공자에 대한 통신 자료 요청 방법과 형사법적 문제”, 형사정책연구 통권 제125호 (2021), 170면.

가입하였으며, 전자증거의 특성인 휘발성을 고려할 때 중요한 부분인 데이터의 신속한 보전, 제출명령 등에 관해 다룬다.[15] 협약은 가입국이 필수적으로 범죄화해야 하는 사이버범죄 유형을 제시하고, 사이버범죄 수사를 원활하게 하기 위한 절차, 국가 간 수사공조를 신속하게 하기 위한 규정을 두고 있다.

사이버범죄 협약은 사이버범죄의 실체법, 절차법적 기준을 제시하여 서로 다른 법체계를 가지고 있는 국가 간 사이버범죄 수사 협력을 위한 토대를 만들고자 한다. 실체법적으로는 컴퓨터 시스템에 불법접속, 아동포르노 유포, 저작권 침해와 같이 각국이 범죄로 규정해야 하는 행위를 다루고 있다. 절차법적으로는 이 행위를 수사하기 위해 필요한 권한을 수사기관에 부여하고 그 한계에 대해 규정하며, 원활한 국제공조를 위해 필요한 절차를 다룬다.

유럽평의회는 2022년 5월 사이버범죄 협약을 보충하는 내용의 제2 추가의정서(Second Additional Protocol)를 비준하였다. 이는 시대의 흐름에 따라 변화한 사회상을 반영하여 사이버범죄 수사공조를 효율적으로 하기 위한 결정이다. 제2 추가의정서는 전자증거의 강화된 협력 및 공개를 국가 간, 국가 및 민간 부분 간으로 확대하고 있다. 또한, 효율적인 협력의 필요성에 대응하여 서비스 제공자가 보유한 데이터를 외국에 직접 제공할 수 있는 경우를 명시하고 있다. 사이버범죄 협약 제18조는 가입자정보 등에 대한 제출명령을 인정하고, 제2 추가의정서 제7조는 일정 요건 하에 정보 제출명령이 형사사법공조 절차를 거치지 않고 직접 국외 서비스 제공자에 이루어지도록 규정한다.

구체적으로 사이버범죄 협약 제18조 제1항 b호에 의하면 당사국의 관할관청은 자국 영토에서 서비스를 제공하는 서비스 제공자를 대상으로 가입자정보를 제출할 것을 명령할 수 있다. 협약 해석과 적용에 관한

---

14) 유럽평의회 웹사이트 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> (2022. 11. 30. 방문).

15) 유민종, “사이버범죄협약과 국내 법제의 양립 가능성 연구”, 석사학위논문, 서울대학교 (2019), 10면.

당사국 간 공통적 이해를 반영하는 주해서에는 서비스 제공자의 자국 내 서비스 제공 부분을 넓게 해석하여 제18조 제1항 b호의 적용 범위를 확장하고 있다. 협약 주해서에 의하면 서비스 제공자가 당사국 영토 내 소재하지 않지만 자국 영토에서 서비스를 제공하는 경우 당사국 관할관청은 직접 서비스 제공자에게 제출명령을 할 수 있다.

한편, 사이버범죄 협약 제2 추가의정서에서도 가입자정보 관련 국외 서비스 제공자의 직접 협력, 법집행기관의 초국경적인 전자증거 확보 문제를 다룬다.[16] 제2 추가의정서 제7조에 의하면 관할관청은 직접 국외 서비스 제공자가 가입자정보를 제출하도록 명령할 수 있다. 해당 서비스 제공자가 30일 이내에 공개하지 않으면 다른 형태로 명령을 집행할 수 있다. 이에 따라 협약 제18조는 가입자정보와 관련해서 서비스 제공자가 서비스를 제공하는 외국의 법집행기관에 데이터를 공개하는 법적 근거가 된다.

사이버공간상의 범죄 수사 시 요구되는 신속한 국제공조를 위해 사이버범죄 협약, 나아가 제2 추가의정서에 가입하는 방안이 있다. 2022년 10월 우리나라는 사이버범죄 대응을 위해 장기간 논의 및 연구한 사이버범죄 협약 가입을 위해 가입의향서를 제출하였다. 협약에 가입하기 위해 국내에서는 입법논의를 거쳐 데이터 보전명령제도 도입, 상시 연락거점인 접촉창구(Point of contact) 설치 등을 해야 한다. 현시점에서 통신비밀보호법 및 형사소송법 개정, 협약 24/7 네트워크 접촉창구 지정 등 협약 비준을 위한 국내 절차를 완료하고 최종 가입하기까지 상당한 시간이 소요될 것이다.

기존 사이버범죄 협약은 각국이 공조를 위한 상시 접촉창구를 마련해 협약 당사국에 효율적인 증거 보전 및 확보를 하도록 규정한다. 형사사법공조 절차가 요청부터 회신까지 평균적으로 3-12개월 소요되는

16) Jennifer Daskal and Debrae Kennedy-Mayo, “Budapest Convention: What is it and How is it Being Updated?” <https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1#_edn27> (2022. 11. 30. 방문).

것과 비교하여, 사이버범죄 협약에 따른 공조의 경우 6-24개월 걸리므로 협약에 의한 국제공조가 더 신속하다고 단정할 수 없다. 지난 5월 채택된 제2 추가의정서의 내용을 포함하지 않고 논의한 후 국내법을 정비하여 협약에 가입하면, 사회의 변화를 반영하지 않은 것이므로 가입의 의미가 퇴색될 것이다.[17] 이행입법 할 때 제2 추가의정서의 국외 서비스 제공자에 직접 요청, 외국의 제출명령에 강제력 부여 등 신속한 국제공조를 추구하는 내용을 참고하여 논의하면 효과적일 것이다.

사이버범죄 협약 제2 추가의정서에는 가입국이 국외 서비스 제공자에 직접 데이터 요청하는 것을 허용하여 수사의 효율성을 높이는 조항을 포함하고 있다. 신속하고 긴밀한 수사 공조를 추구하면서도 제도 남용 및 기본권 침해 등 부작용을 방지하여 사이버공간에서 자유로운 정보 교환이 이루어지도록 한다. 사이버범죄 협약 가입을 통해 신속한 공조 절차를 확보하여 사이버범죄에 대응하는 수사기관의 역량을 강화하고 남용방지 규정을 통해 개인정보를 보호한다. 협약과 관련하여 국내에서 인권 침해의 소지가 있는 부분은 엄격하게 검토해야 한다.[18] 수사 시 필요한 데이터 제공의 경우 효율성을 추구하는 과정에서 기본권 보장을 위한 장치 마련이 필요하다.

3. 미국 클라우드법 행정협정

클라우드법(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)은 합법적인 해외 데이터 활용의 명확화 법률로 2018년부터 시행되고 있다. 동 법률은 마이크로소프트 사건에서 미국에 본사를 둔 기업의 해외에 저장된 데이터에 대한 접근 가능성 여부를 두고 미국 정부와 마이크로소프트 사이의 소송을 계기로 제정되었다. 클라우드법에 따라 행정협정을 체결하면 해외 소재 서버에 범죄 수사에 필요한 데이터가 저장되어 있을 경우에도 데이터를 안정적으로 확보할 수 있다.

글로벌 IT 서비스 기업의 해외 서버에 저장된 데이터는 자국의

17) 박재성, 앞의 논문, 278면.
18) 정명현, “유엔 사이버범죄 대응 국제조약의 논의동향과 전망”, 외교부, 국제법 동향과 실무 통권 제62호 (2021), 18면.

개인정보 보호법의 적용을 받으므로, 그동안 수사기관은 해당 국가에서 압수수색영장을 발부받거나 행정협정을 통해 외교적 절차를 거쳤다. 미국은 클라우드법으로 자국 글로벌 IT 서비스 기업의 해외 서버에 저장된 가입자정보, 통신내용, 트래픽데이터 등을 열람할 수 있는 역외 데이터 접근에 대한 명시적 근거를 마련하였다.[19] 클라우드법에 의하면 미국의 법집행기관은 영장을 발부받지 않고 전 세계에 저장된 데이터에 대한 법집행이 가능하다.

미국 클라우드법은 개인정보 보호와 외국의 주권을 존중하면서 공공의 안전을 보호하기 위해 필요한 제3자 보관 정보를 위치에 관계 없이 서비스 제공자에게 요구할 수 있는 법적 근거를 갖는다. 클라우드법 행정협정을 체결한 국가는 서비스 제공자에 직접 정보를 요구할 수 있도록 허용하여 신속하게 전자증거에 접근하고 활용하는 방안을 제시한다. 이는 마이크로소프트, 구글 등 글로벌 IT 서비스 기업을 통해 수집한 정보의 가치 및 국가안보 차원의 중요성을 고려하여 미국법과 상충하는 문제를 해결하기 위한 방법이다.

클라우드법에 의해 미국 내 글로벌 IT 서비스 기업은 저장통신법을 위반하지 않고 외국의 정보 제공 요청에 응할 수 있다. 글로벌 IT 서비스 기업이 이용자의 개인정보를 보호해야 할 의무와 법집행기관에 협조할 의무 사이에서 상반된 요구를 받을 경우 클라우드법으로 법적, 윤리적 딜레마에서 벗어날 수 있다.[20] 외국의 데이터 제출 요청과 반출을 금지하는 각국의 국내법 준수 의무 사이 충돌의 경우 클라우드법의 시행으로 법적 의무의 해결이 가능하다.

미국 클라우드법의 의의는 데이터의 관리, 공개 등의 의무 준수에 대한 역외 적용의 법률적 근거[21] 신설에 있다. 법집행을 목적으로 서비스 제공자에 데이터를 요구할 수 있도록 규정하여 법집행기관의 요청에

19) 송영진, “미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점”, 형사정책연구 통권 제114호 (2018), 151면.
20) 한국인터넷진흥원, “미국 클라우드법(CLOUD ACT)의 주요 내용 및 전망” (2018), 181면.
21) 18. U.S.C. §2713.

따라 해외에 저장된 데이터에 대해서도 공개 가능하도록 한다. 초국경적인 데이터에 대한 접근 및 교환을 촉진하기 위해 다른 국가와 행정협정을 체결할 수 있도록 권한을 부여한다. 미국이 외국과 행정협정을 체결함으로써 범죄의 수사와 기소를 위해 법집행기관이 상대국에서 보유한 데이터에 상호 접근할 수 있도록 한다. 또한, 행정협정이 체결된 경우에는 해외에 저장된 이용자의 정보 요구에 대해 서비스 제공자가 이의를 신청[22]할 수 있도록 허용한다.

클라우드법에 따르면 행정협정을 맺기 위해서는 사이버범죄 협약 당사국이거나 협약에 명시된 정의 및 요건이 국내법과 일치해야 한다.[23] 우리나라는 사이범죄협약 가입국이 아니며 협정 당사국으로 적합성을 위해서는 국내법의 면밀한 검토가 필요하다. 국내법상 데이터의 수집·보유·활용에 대해서는 통신비밀보호법, 형사소송법, 전기통신사업법, 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등에 허가 요건, 절차, 통지의 의무를 명시하고 있다. 국외로 데이터를 이전할 경우에 대해서 현행법을 보완할 필요가 있는지, 클라우드법 행정협정 요건에 해당 규정이 적합한지 검토를 위해서는 시간이 오래 걸릴 것이다.[24]

4차 산업혁명 시대에 데이터의 국외 이전이 빈번한 상황에서 데이터의 양적·질적 확보 및 개인정보 보호에 높은 가치를 부여하고 있다. 미국 클라우드법, 해당 법률에 따른 행정협정이 수사기관에는 필요하지만, 기업이나 개인정보 주체에게는 권리침해적 요소가 존재한다. 클라우드법 행정협정 시행 시 외국 법집행기관이 국내 서비스 제공자의 데이터에 접근할 수 있도록 권한을 부여하는 것에 대해 우려가 있다.

클라우드법 행정협정 체결 시 상호주의 원칙에 따라 국내 기업이 보유·관리하는 데이터도 제공해야 하므로 외국 법집행기관의 요청에

---

22) 18. U.S.C. §2703(h).
23) 18. U.S.C. §2523.
24) 김나정, “미국 「CLOUD Act」의 주요 내용과 시사점”, 국회입법조사처, 외국입법 동향과 분석 제55호 (2020), 7면.

대비해야 한다.[25] 국내에서 데이터 주권과 충돌하는 부분은 행정협정 체결을 위해서 관련 조치가 필요하며, 궁극적으로 개인의 권리를 보호하는 방안 마련을 선행해야 한다. 즉, 데이터 주권 및 개인정보 자기결정권의 보장 조치가 필요하므로 개인정보의 국외 이전 등에 대한 기술적·관리적 보호 방안을 강화해야 한다.

유럽연합의 GDPR(General Data Protection Regulation)은 유럽연합 내에 저장된 데이터를 유럽연합 외부로 이전할 경우 형사사법공조 조약과 같은 국제협정만 인정한다. 이에 미국 클라우드법 행정협정은 해당하지 않아 GDPR과 충돌 가능성이 있다.[26] IT 강국인 우리나라가 미국과 행정협정을 맺어 클라우드법을 따르면 실효성이 있지만, 다수 국가가 참여하는 공식적인 조약을 대체하기에는 한계가 있다.

제2절 해외 수사기관을 통한 요청

외국에 저장된 전자증거가 수사의 성패를 좌우할 만큼 중요하므로 수사기관은 효율적으로 증거를 확보할 수 있는 방안 마련의 필요성이 점점 커지고 있다. 공식적인 법적 근거에 의한 요청 외에 비공식적인 국제공조 중 해외 수사기관을 통한 요청에는 G7 24/7 첨단범죄 네트워크, 인터폴, 해외 수사기관과 MOU를 활용하는 방법이 있다.

1. G7 24/7 첨단범죄 네트워크

G7 24/7 첨단범죄 네트워크(G7 24/7 High-Tech Crime Network)는 1997년 G7 국가 주도로 결성된 국제공조 네트워크다. 우리나라의 경우 2000년에 가입하였고 2022년 11월 기준으로 90개국이 가입한 상태다. 우리나라는 대검찰청 사이버수사과가 컨택포인트(접촉창구)로 이 네트워크를 통해 증거 보전, 정보 교환 및 법률·기술 자문 등 외국과 협력을 하고 있다. 컨택포인트는 검찰, 경찰, 특별사법경찰 등 각

25) 이근우, “클라우드컴퓨팅법과 CLOUD Act는 다르다” <https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=163869> (2022. 11. 30. 방문).
26) Jennifer Daskal, “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0”, Stanford Law Review Online, Vol. 71 (2018), 12면.

수사기관의 요청을 받아 해당 국가에 협력을 요청하거나 회원국들의 협력 요청을 받아 처리하는 접촉창구 역할을 하고 있다.

G7 24/7 첨단범죄 네트워크는 수사기관 간 자발적인 협력으로 범죄 예방 및 수사를 위해 상호 협력한다. 수사 과정에서 해외 소재 데이터에 대한 증거 보전 조치 필요 시 요청을 하는데, 이때 요청 대상 범죄는 사이버범죄를 포함하여 증거 보전이 필요한 모든 범죄가 해당한다. G7 24/7 첨단범죄 네트워크를 통해 회원국 컨택포인트에 보전 요청서를 발송하고, 보전 조치 결과를 요청기관에 회신한다.

구체적으로 살펴보면, 해외로 하는 요청은 우선 증거 보전 요청기관에서 해당 데이터의 가입국 여부를 확인한 후 요청기관에서 대검찰청으로 공문을 송부한다. 이를 대검찰청 접촉창구가 접수하여 G7 24/7 첨단범죄 네트워크 회원국 컨택포인트에 보전 요청 이메일을 발송한다. 이후 회원국 컨택포인트로부터 보전 조치 완료 이메일을 수신하면 대검찰청 접촉창구인 사이버수사과에서 증거 보전 요청기관에 보전 조치 완료 결과를 회신한다.

반대로 해외에서 받은 요청의 경우 G7 24/7 첨단범죄 네트워크 회원국 컨택포인트에서 우리나라 접촉창구에 이메일로 요청하면 요청 대상 데이터 소재 기업에 연락해 증거 보전 및 송부 요청을 한다. 우리나라 접촉창구인 대검찰청 사이버수사과는 요청 대상 보전 조치 후 데이터를 보관하고, 회원국 컨택포인트에 보전 조치 완료 이메일을 회신한다.

일본 온라인 서비스 제공자는 자국 법원이 발부한 압수수색영장만 인정하고 해외 법집행기관에서 영장을 제시할 경우 데이터를 제공하지 않는다. 이로 인해 시간이 오래 걸리는 형사사법공조 진행 과정에서 중요한 증거가 삭제될 우려가 있는데, G7 24/7 첨단범죄 네트워크를 통해 사전에 증거 보전 요청을 하면 유용하다. 메신저 앱을 기반으로 다양한 모바일 서비스를 제공하는 기업인 라인의 경우 형사사법공조를 전제로 한 증거 보전은 하고 있다. 일본에 본사가 있는 기업의 경우 증거 보전 조치 후 형사사법공조 절차를 거쳐 최종적으로 데이터를

확보한다.

G7 24/7 첨단범죄 네트워크를 통한 증거 보전 요청은 형사사법공조 요청 전 소멸하기 쉬운 증거의 신속한 보전(freezing)을 목적으로 운영되고 실제 증거 확보는 형사사법공조 절차에 따라 진행된다. 형사사법공조 요청 시 사전 증거 보전 요청 사실을 기재하면 신속한 공조 절차 진행이 가능하다. G7 24/7 첨단범죄 네트워크는 회원국들이 자국의 법률이 허용하는 범위 내에서 최대한 협조한다. 다만, 공식 협약이 아니므로 협력을 강제할 수 없고, 회신내용 및 범위도 한정적이어서 적극적인 수사 공조에는 제약이 있다.

2. 인터폴

인터폴(International Criminal Police Organization, Interpol)[27]은 우리나라를 포함하여 195개국[28]이 가입한 세계 최대의 형사경찰 간 협력기구다. 인터폴 헌장과 회원국의 국내법이 허용하는 범위 내에서 국제범죄에 관한 정보를 교환하고 범죄 예방 및 진압을 위해 상호 협력한다. 국제형사사법 공조법 제38조에는 국제범죄의 정보 및 자료 교환, 동일증명 및 전과 조회, 사실 확인 및 그 조사 등 형사사건 수사에 대하여 인터폴과 상호 협력을 규정하고 있다.

인터폴은 가입국별 국가 중앙 사무국(National Central Bureau, NCB)을 지정하고, I-24/7 네트워크를 통해 국가 중앙 사무국이 직접 통신하는 시스템을 구축하였다. 우리나라는 경찰청 외사국 내 국가 중앙 사무국을 설치하여 각 수사기관의 요청을 받으면 대상국에 협력을 요청하는 전문을 발송한다.[29] 수사기관 간 직접 요청을 주고받으므로 외교경로를 거치는 형사사법공조보다 상대적으로 빠르게 회신받을 수 있다. 그러나 인터폴은 국제법상 강제성에 대한 근거가 없고 협력의 범위가

27) 국제형사경찰기구.
28) 인터폴 웹사이트 <https://www.interpol.int/Who-we-are/Member-countries> (2022. 11. 30. 방문).
29) 정대용·김성훈·김기범·이상진, “국제협력을 통한 디지털 증거의 수집과 증거능력”, 형사정책연구 28(1) (2017), 53면.

제한적이므로 압수수색이나 체포가 필요한 수사 공조를 할 수 없다.[30]

3. 해외 수사기관과 MOU

G7 24/7 첨단범죄 네트워크, 인터폴을 통한 자발적인 협력의 한계를 극복하고자 UNODC, 유로폴 등 다양한 국제기구와 긴밀한 교류를 이어나가고 있다. 또한, 미국·영국·프랑스·독일·네덜란드 등 주요 협력국의 수사기관과 MOU(Memorandum Of Understanding)[31]를 체결하여 사이버범죄 대응 및 수사를 위해 국제공조를 하고 있다.

국제적으로 특정 사건에 여러 국가가 참여하여 정보를 교류하고 피의자를 검거하는 형태의 공조수사가 활발히 이루어지고 있다. 'N번방 사건'에서 피의자는 미국의 메신저 앱인 디스코드를 통해 성착취물을 유통하였다. 이 사건에서 피의자를 특정하고 검거하는데, 미 연방수사국(Federal Bureau of Investigation, FBI)과 국토안보수사국(Homeland Security Investigations, HSI)의 협조를 받았다.

리플[32] 가상자산 탈취 사건의 경우 한·미 수사기관이 공조하여 리플 피싱 사기를 당한 피해자들을 구제하였다. 미국이 첩보 자료를 제공하였으며, 국제공조를 통해 가상자산 사기 범죄의 수사단계에서부터 피해 회복까지 원스톱으로 진행하여 성공한 대표적인 사례다. 피의자들은 2017년 6월부터 2018년 1월까지 미국에 리플 가상자산 피싱 사이트를 개설하여 피해자들을 유인한 뒤 피해자가 피싱 사이트에 입력한 ID와 비밀번호로 실제 사이트의 접속 정보를 탈취하였다. 이후 실제 가상자산 사이트의 피해자 계정에 접속하여 국내외 피해자 61명으로부터 9억원[33] 상당의 리플을 빼돌렸다.

2019년 3월 FBI는 미국 가상자산 거래소에 은닉된 한국인 피의자의 가상자산을 발견하고 동결 및 압류에 성공하였다. 같은 해 4월 한국

---

30) 오세연·송혜진, "초국가적 범죄의 대응강화를 위한 인터폴의 효율적 활용방안에 관한 연구", 한국재난정보학회논문집 10(4) (2014), 562면.
31) 당사국 사이의 외교교섭 결과에 따라 서로 양해된 사항을 확인·기록하는 양해각서.
32) 리플은 비트코인, 이더리움에 이어 다섯 번째로 규모가 큰 블록체인 기반의 가상자산.
33) 2021. 12. '리플' 시세인 1XRP = 973원으로 환산한 피해금액은 23억 5,000만원 상당.

검찰은 FBI와 일본 경찰청을 방문하여 일본인 피의자의 검거를 위해 사건을 설명하고 정보를 공유하였다. 2019년 6월 FBI는 압류 가상자산과 관련성이 있는 피해자를 선별하여 한국 검찰에 통보하였다. 대검찰청은 연락이 닿은 피해자를 만나 환부 과정을 설명하고 환부에 필요한 동의서를 받아 FBI에 전달하였다. FBI가 2021년 8월 대검찰청으로 환부승인 통지서를 보내고, 11월에 미국이 피해자의 계좌로 환부금을 송금하며 마무리되었다. 한·미 양국은 수사뿐만 아니라 피해자들의 피해 회복을 위한 절차에 있어서도 상호 긴밀한 공조를 통해 성과를 냈다.

국가 간 공조가 증가하면서 사이버범죄에 대응하기 위해 해외 수사기관과의 교류 협력도 활성화되고 있다. 사이버범죄의 초국가적 특성으로 인해 국제회의, 컨퍼런스, 심포지엄 등을 개최하여 국제협력의 중요성에 대한 국제적 공감대를 형성하고 있다. 사이버범죄에서 국제공조는 필수불가결한 요소로 각국 수사기관 사이의 협력을 통해 사이버범죄 관련 정보 교환, 증거 보전 요청, 데이터 제공 등을 하고 있다.[34]

제3절 국외 서비스 제공자에 직접 요청

신속하고 효율적인 공조체제를 통해 해외에 소재한 제3자 보관 정보를 확보하고자 국외 서비스 제공자에 직접 요청한다. 국외 서비스 제공자의 제3자 보관 정보는 글로벌 IT 서비스 기업이 보관하는 정보를 대상으로 한다. 수사기관이 범죄 수사 시 필요한 제3자 보관 정보에는 가입자정보, 통신내용, 트래픽데이터 등이 있다. 글로벌 IT 서비스 기업에 직접 요청을 하면 대부분의 경우 가입자정보를 회신받으며, 통신내용과 트래픽데이터는 형사사법공조 절차가 필요하다.

글로벌 IT 서비스 기업은 제3자 보관 정보 요청 대상으로 저작권법상 온라인 서비스 제공자(Online Service Provider, OSP)에 해당한다. 제3자

34) 정대용·김성훈·김기범·이상진, 앞의 논문, 55면.

보관 정보를 제공하는 피압수자인 온라인 서비스 제공자는 초기에는 인터넷을 대상으로 인터넷 접속 서비스를 제공하는 기업을 의미하였다. 인터넷 산업이 발전하면서 그 의미가 점차 확장되어 인터넷 접속 서비스를 통해 다양한 콘텐츠 및 콘텐츠 서비스를 제공하는 회사들이 주를 이루고 있다.[35] 대표적인 온라인 서비스 제공자에는 포털, 소셜미디어, 메신저 등 글로벌 IT 서비스 기업이 있다.

글로벌 IT 서비스 기업을 이용하기 위해서는 해당 서비스에 회원으로 가입해야 한다. 회원가입은 신분 확인을 위해 필요한 절차로, 가입자의 인적사항을 저장하는 방식은 서비스 제공자마다 다르지만 가입자정보의 형태는 비슷하게 보관하고 있다. 국외 서비스 제공자는 서비스의 운영 및 유지 관리를 위해서 가입자로부터 동의를 얻어 가입자의 인적사항과 활동 정보를 서버에 저장 및 보관하여 활용하고 있다. 가입자정보는 전화번호, 이메일 주소 등을 포함하며, 이를 토대로 2차 추적을 실시하여 피의자 특정 및 범죄 행위를 입증하는데 이용된다.

사이버공간에서 가입자의 활동으로 생성한 정보의 소유자는 가입자지만, 가입자의 동의를 받아 글로벌 IT 서비스 기업이 보관하고 활용하므로 국외 서비스 제공자는 제3자 보관자가 된다.[36] 국외 서비스 제공자는 24시간 서비스를 제공하며 가입자들이 생성한 정보를 저장하므로 데이터센터의 서버에 저장된 정보는 실시간 변한다. 그 대상이 대형 포털사, 소셜미디어 등 글로벌 IT 서비스 기업의 경우에는 저장하는 데이터의 양이 방대하다. 사이버공간상 글로벌 IT 서비스 기업이 생성하고 저장하는 정보가 많아지면서 제3자 보관 정보의 중요성이 강조되고 있다. 사이버범죄 수사에 있어서도 국외 서비스 제공자의 빅데이터를 통한 정보를 이용하는 경우가 증가하고 있다.

글로벌 IT 서비스 기업의 이용 증가로 제3자 보관 정보 요청에 대한 수요도 점점 늘어나고 있는 추세다. 이메일, SNS(Social Networking

35) 김지만, “일본의 온라인 서비스 프로바이더의 책임”, 콘텐츠재산연구 3, (2012), 31면.
36) 김종빈, “전자정보를 대상으로 한 압수수색검증영장의 효율적인 집행방법에 대한 연구”, 석사학위논문, 서울대학교 (2020), 35면.

Service)의 사용이 일상화되면서 국외 서비스 제공자에 가장 많이 직접 요청하고 있는 제3자 보관 정보는 가입자정보다. 가입자정보에 대한 형사사법공조 요청이 많아 업무 부담이 가중되면 통신내용, 트래픽데이터 등 형사사법공조를 통해서만 제공받을 수 있는 정보에 대한 공조 요청은 제대로 이행되지 못한다. 또한, 형사사법공조의 경우 요청부터 회신까지 절차가 복잡하고 시간이 오래 걸려 휘발성이 강한 사이버범죄의 증거를 신속하게 획득하는데 어려움이 있다.

일부 국가에서는 수사 시 통신내용, 트래픽데이터에 비해 개인정보 침해 요소가 적은 가입자정보의 접근 요건을 완화하고 있다. 이 국가들의 서비스 제공자는 서비스를 제공하는 외국의 수사기관이 가입자정보를 요청하는 경우 기업 내 가이드라인을 충족하면 형사사법공조 절차를 거치지 않고 바로 회신한다. 미국의 경우 수사의 효율성 측면에서 수사기관이 제3자 보관 정보를 신속하게 확보하기에 용이한 방향으로 절차를 처리하는 추세다. 마이크로소프트, 구글, 트위터, 페이스북(인스타그램) 등 글로벌 IT 서비스 기업은 사이버범죄 협약 가입국이 보내는 제3자 보관 정보 요청 중 60% 정도의 데이터를 공개하였다.[37]

국외 서비스 제공자의 경우 요청 방법과 회신 기준을 명시하는 기업, 요청서 양식에 맞춰 요청하도록 요구하는 기업 등 기업에 따라 그 기준은 다르다. 데이터 제공 정책과 절차가 일관되지 않고 변경이 빈번하여 예측하기가 어렵지만, 자국법이 허용하는 범위 내에서 해당 기업의 요청 요건을 만족하면 정보를 빠르게 확보할 수 있다. 여러 단계를 거치지 않고 직접 데이터 관리자에게 필요한 정보를 요청하고 회신받는 방식으로 절차가 간소화되어 효율적이다. 이러한 협조 요청에는 평균 2-5주(긴급사안의 경우 48시간 내)가 소요되어 신속성을 요구하는 사이버범죄 수사의 제3자 보관 정보 확보에 유용하다.

---

37) Jan Kleijssen and Pierluigi Perri, 『Cybercrime, Evidence and Territoriality: Issues and Options』, Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser (2017), 164면.

사이버범죄 관련 제3자 보관 정보 중 서비스 사용자의 가입자정보의 경우 이메일이나 법집행 요청 포털을 통해 국외 서비스 제공자에 직접 요청하고 있다. 마이크로소프트, 구글, 트위터, 페이스북(인스타그램) 등 국외 서비스 제공자의 경우 가입자정보는 국내 압수수색영장 또는 통신사실확인자료 제공요청 허가서의 스캔본을 제출하고 제공받는다. 실제 국외 서비스 제공자를 통해 직접 요청하여 회신받은 가입자정보로 사건에 결정적인 수사 단서를 확보하여 수사에 도움이 된 다수의 사례가 있다.

글로벌 IT 서비스 기업	요청 수단	요청 시 제출서류	회신율 (2021년 하반기)
마이크로소프트	법집행 요청 포털	압수수색영장 또는 통신사실확인자료 제공요청 허가서	72%
구글			86%
트위터			59%
페이스북(인스타그램)			80%

[표 1] 글로벌 IT 서비스 기업별 직접 요청 방법

제4장 국외 서비스 제공자 협조 현황 및 대안

제1절 국외 서비스 제공자의 협조

1. 마이크로소프트

미국에 본사를 두고 있으며, OneDrive, Xbox, Outlook 등 마이크로소프트가 제공하는 서비스에 대한 가입자정보 및 접속로그를 제공하고 있다. 일반적으로 가입자정보 요청은 마이크로소프트 법집행기관 포털에 접속해 국내 법원에서 발부한 압수수색영장 또는 통신사실확인자료 제공요청 허가서 한글 원본을 스캔하여 첨부한 후 제출하는 방식이다. 긴급 정보 요청은 마이크로소프트 긴급요청서 작성 후 영장이나 허가서의 스캔본을 수사기관 이메일을 이용하여 송부한다.

법집행기관 포털에 온라인 접속 시 초기화면의 “공인된 법집행기관 또는 공무원이거나 마이크로소프트로부터 접근 권한을 부여받았으며 이는 공식 요청임”에 해당하는 항목을 체크한 후 해당 페이지에 접속한다. 로그인하여 요청사항을 입력하고 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 스캔하여 업로드한다. 영장, 허가서에 장소는 마이크로소프트 본사 소재지인 ‘1 Microsoft Way, Redmond, WA 98052, USA’로 기재하여 발부받는다.

요청 정보 수신은 다운로드 안내 이메일의 링크를 통해 마이크로소프트 법집행기관 포털에 접속하여 다운로드하는 방식이다. 구체적으로 살펴보면 각 링크에 대한 다운로드는 3회 가능하며, 다운로드 횟수를 초과한 경우에는 해당 정보에 대한 재전송 요청을 해야 한다. 한편, 이메일을 수신한 날로부터 14일이 경과되면 정보가 삭제된다. 데이터는 압축 폴더 형식으로 제공되며, 압축 풀기 과정에서 필요한 비밀번호는 마이크로소프트 법집행기관 포털에서 확인이 가능하다.

마이크로소프트는 반기마다 전 세계 법집행기관 데이터 제공 요청 관련 통계를 보고하는데, 한국은 2021년 하반기에 요청한 105건에 대해 198개의 계정 정보 요청 중 72%의 데이터를 회신받았다.[38] 마이크로소프트는 제3자 보관 정보 중 가입자정보, 접속로그에 대해 회신하고 통신내용은 형사사법공조를 통해 제공한다.

2. 구글

전 세계 대부분의 국가에서 구글 검색, 지메일, 유튜브, 구글 드라이브 등 구글 서비스를 이용하고 있다. 구글은 미국에 본사를 두고 글로벌 이용자에게 다양한 서비스를 제공한다. 구글의 법집행기관 가이드라인에 의하면 구글이 제공하는 서비스 계정에 대한 가입자정보, 접속로그를 받기 위해서는 국내 법원이 발부한 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 제출해야 한다. 이때 영장, 허가서에 기재할 장소는

38) 마이크로소프트 웹사이트 <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report> (2022. 11. 30. 방문).

구글 본사 소재지인 '1600 Amphitheatre Parkway, Mountain View, CA 94043, USA'로 한다.

수사기관은 법원에서 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 발부받고, 법집행기관 요청 시스템을 통해 제3자 보관 정보 제공을 요청한다. 해당 사이트에서 법집행기관 소속 인증을 받은 후 요청사항을 입력하며 영장 또는 허가서 스캔본을 첨부하여 제출하고, 요청 시 입력한 이메일을 통해 데이터를 회신받는다. 구글은 반기마다 전 세계 법집행기관 데이터 제공 요청 관련 보고서를 발간하는데, 이에 따르면 한국은 2021년 하반기에 요청한 4,149건에 대해 25,386개의 계정 정보 요청 중 86%의 데이터 회신을 받았다.[39]

구글은 접속로그 중 관련성이 확인되면 해외 IP도 제공하지만, 영장이나 허가서에 장소를 잘못 기재하거나 유효기간이 지난 경우에는 회신하지 않는다. 데이터 제공 요건 충족 시에는 성명, 이메일 주소, 휴대전화번호, 가입일시 등 가입자정보 및 접속로그를 회신한다. 회신 데이터에 포함된 국내 전화번호, 이메일 주소, IP 주소 등에 대한 2차 추적을 실시하여 피의자 특정 및 범죄 행위 입증이 가능하다.

3. 트위터

트위터는 글로벌 메시지 기반 소셜 미디어 기업으로 본사가 미국에 있다. 트위터의 경우 가입자정보 및 접속로그 제공 요청은 트위터 온라인 법적 요청 접수 사이트를 통해 할 수 있다. 해당 사이트에서 법집행기관 소속 인증을 받은 후 요청사항을 입력하고, 국내 법원이 발부한 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 스캔하여 제출한다.

영장, 허가서는 트위터 본사 소재지인 '1355 Market Street, Suite 900, San Francisco, CA 94103, USA'로 장소를 기재하여 발부받아야 한다. 트위터가 전 세계 법집행기관 데이터 제공 요청과 관련해 발간한

39) 구글 웹사이트 <https://transparencyreport.google.com/user-data/overview?user_requests_rep%20ort_period=series:requests,accounts;authority:KR;time:&lu=legal_process_breakdown&user_requests_report_period> (2022. 11. 30. 방문).

보고서에 따르면, 한국은 2021년 하반기에 요청한 288건에 대해 460개의 계정 정보를 요청하였고, 이 중 59%의 데이터를 회신받았다.[40]

트위터는 기업 정책에 따라 정보 요청 사실을 사용자에게 통지할 수 있으므로 사용자에게 정보 요청 내용이 통지되는 것을 원하지 않을 경우 그 사유와 기간을 명시하여 통지유예 항목을 작성해야 한다. 회신 데이터는 요청 시 입력한 이메일로 오며, 계정에 대한 가입자정보, 접속로그는 회신하지만 통신내용은 형사사법공조를 통해서만 제공한다.

4. 페이스북(인스타그램)

소셜 미디어 이용자들은 대부분 페이스북, 인스타그램을 사용하고 있다. 페이스북 본사는 미국에 있으며 인스타그램을 인수하여 동일한 데이터 제공 정책을 적용하고 있다. 페이스북은 해외 수사기관의 데이터 요청에 대해 미국 외 지역 관할권에 법적 요청이 수반되며, 그 지역 내 사용자들에게 영향을 미치고 국제적으로 용인되는 기준에 부합할 때 제공한다.

페이스북은 가입자정보, 접속로그 요청 시 법집행기관 온라인 요청 시스템을 통해서 한다. 법집행기관 소속 인증을 받은 후 국내 법원에서 발부한 압수수색영장 또는 통신사실확인자료 제공요청 허가서와 영문 번역본을 스캔하여 업로드한다. 이때 영장, 허가서에 기재할 장소는 페이스북 본사 소재지인 '1601 Willow Road, Menlo Park, CA 94025, USA'로 해야 한다.

온라인 접속 시 초기화면의 "공인된 법집행기관 또는 긴급 수사를 하는 공무원으로서 공식 요청임"에 해당하는 항목을 체크한 후 수사기관의 이메일 주소를 입력한다. 입력한 이메일 주소로 인증페이지에 접속할 수 있는 링크를 포함한 이메일이 전송되며, 이 인증페이지에서 개인정보를 입력한 후 요청서를 작성하고 처리 내역을 확인할 수 있다. 회신할 때는 정보 요청 시 입력한 이메일 주소로 URL을 전송하여 데이터를

40) 트위터 웹사이트 <https://transparency.twitter.com/en/reports/information-requests.html#2021-jul-dec> (2022. 11. 30. 방문).

다운로드한 후 확인할 수 있다.

페이스북 가이드라인 충족 시 성명, 이메일 주소, 휴대전화번호, 가입일시 등 가입자정보 및 접속로그를 회신하며, 통신내용은 형사사법공조를 통해서만 제공한다. 페이스북 투명성 센터의 통계에 따르면 한국 수사기관은 2021년 하반기에 요청한 1,158건에 대해 1,604개의 계정 정보를 요청하였고, 이 중 80%의 데이터 회신을 받았다.[41]

제2절 직접 협조 요청 현황

1. 우리나라

한국인터넷투명성보고서의 통신자료제공요청 현황에 따르면 통신자료 제공요청의 경우 대부분 가입자 신원정보 확인을 위한 것이다.[42] 국내 서비스 제공자는 개인정보 보호법에 따라 가입자정보를 수집하고 사용할 수 있으며, 범죄 수사와 공소의 제기 및 유지를 위해 필요한 경우에는 가입자정보를 제공할 수 있다.

한편, 개인정보 보호법 제18조 제1항에 의하면 국내 서비스 제공자는 개인정보의 제3자 제공이 제한된다. 동조 제2항 제6호의 예외규정에도 “조약, 그 밖의 국제협정의 이행을 위해 외국정부 또는 국제기구에 제공하기 위해 필요한 경우”라고 한정하고 있어 형사사법공조에 의하지 않고서는 개인정보를 제공할 수 없다.

‘회피연아 사건’ 이후 네이버, 카카오는 통신자료제공요청이 임의수사로, 반드시 이에 응할 의무는 없다고 판단하여 수사기관의 통신자료 제공요청에 응하지 않고 있다.[43] 양대 포털은 전기통신사업법 제83조 제3항을 근거로 수사기관의 통신자료제공요청으로 가입자정보를 제공하지 않고 압수수색영장을 통해서만 제공한다.[44]

---

41) 페이스북 웹사이트 <https://transparency.fb.com/data/government-data-requests/country/KR/> (2022. 11. 30. 방문).
42) 고려대학교 법학전문대학원 공익법률상담소, “한국인터넷투명성보고서” (2021), 11면.
43) 서울고법 2012. 10. 18. 선고 2011나19012 판결.

2. 미국

우리나라는 국외 서비스 제공자 중 주로 미국 서비스 제공자에 제3자 보관 정보를 직접 요청하고 있다. 미국 서비스 제공자의 통신 데이터 제공은 저장통신법(Stored Communications Act, SCA)[45]에 근거하여 이루어진다. 18. U.S.C. §2702는 전자 통신 서비스 제공자 및 원격 컴퓨팅 서비스 제공자의 자발적 정보 공개, §2703은 의무적 정보 공개를 규정하고 있다.

18. U.S.C. §2703(a),(b)에 의해 정부기관이 서비스 제공자에게 통신내용의 공개를 강제할 때 저장기간이 180일 이하인 경우에는 영장, 180일 이상이거나 저장 목적인 경우에는 영장(warrant) 또는 제출명령(subpoena)이나 법원명령(court order)에 의해야 한다. 동법 §2703(c)에 의해 영장, 법원명령, 가입자 동의, 텔레마케팅 사기 수사 시 법집행기관의 서면 요청 등으로 가입자나 고객 관련 기록 및 기타 정보(통신내용 제외)의 공개를 강제하는 방법이 있다. 이때 권한있는 관할의 법원이 영장, 제출명령, 법원명령을 발부하도록 명시하고 있다.

우리나라 수사기관이 미국 서비스 제공자에 직접 요청 시 제시하는 국내 법원이 발부한 압수수색영장, 통신사실확인자료 제공요청 허가서 등은 18. U.S.C. §2703에 해당하지 않으므로 적용되지 않는다. 즉, 국내 수사기관이 미국 서비스 제공자에 직접 요청해서 제3자 보관 정보를 제공받는 것은 18. U.S.C. §2702에 의한 자발적 정보 공개에 적용된다. 동법 §2702(a)에 서비스 제공자는 통신내용을 누구에게도 누설할 수 없고, 가입자나 고객 관련 기록 및 기타 정보(통신내용 제외)는 정부기관에 누설할 수 없다고 명시하고 있다. 동법 §2702(b),(c)는 (a)의 예외규정인데, 이 중 §2702(c)(6)에서 통신내용이 아닌 가입자나 고객 관련 정보는 정부기관 이외에 제공할 수 있다고 규정한다.

18. U.S.C. §2702에서 정부기관의 개념은 미 연방의 부처나 주 또는

---

44) 이은빈, “제3자 보관 개인정보에 대한 증거수집과정에서의 동형암호 활용방안”, 석사학위논문, 서울대학교 (2022), 10면.

45) 18. U.S.C. Chapter 121 §2701-2712.

정치적 구획을 의미[46]하므로 외국 정부는 포함되지 않는다. 따라서 동법 §2702(c)(6)을 근거로 하여 미국 서비스 제공자는 외국 수사기관에 통신내용을 제외한 가입자정보 관련 요청에 협조하고 있다. 미국 서비스 제공자가 외국 정부에 가입자정보를 공개하는 것은 18. U.S.C. §2702(c)(6)에 근거한 자발적 공개에 해당한다. 기업별 정책과 개인정보 처리지침에 따라 요청 시 개별적으로 검토한 후 결정하므로 미국 내에서도 기업마다 제3자 보관 정보 요청에 대한 협조의 정도가 다르다.

국내 수사기관이 미국 서비스 제공자에 직접 요청 시 영장이나 허가서 제출은 요청국에서 적법한 수사를 위해 요청하는 정보가 필요하고, 이에 대한 법원의 허가를 공식 문서를 통해 확인하기 위한 절차로 판단된다. 한편, 유럽 온라인 서비스 제공자들은 GDPR 시행 이후 개인정보 보호정책이 강화됨에 따라 유럽연합 회원국이 아닌 국가의 법집행기관에 직접 데이터를 제공하지 않는다. GDPR 제48조에 따르면 유럽연합 회원국과 외국 정부 간 체결된 형사사법공조 조약과 같은 공식적인 국제협정에 의한 경우에만 외국의 영장 또는 법원명령을 인정한다. 국외 서비스 제공자가 제3자 보관 정보 제공 요청에 비협조적일수록 수사에 어려움이 크고, 이러한 점을 악용한 범죄가 사이버공간에서 일어나고 있다.

제3절 현행 협조 요청의 대안

1. 현행 직접 협조 요청의 문제점

국외 서비스 제공자의 제3자 보관 정보 요청 시 글로벌 IT 서비스 기업의 정책상 법원의 허가를 요구하므로 국내 수사기관은 범죄 수사를 위해 법원에서 허가받은 문서를 제출한다. 미국 서비스 제공자의 경우 저장통신법에 의한 규정에 따라 통신내용을 제외한 정보에 대해서는 외국의 직접 요청에 정보를 제공하므로 상당수의 제3자 보관 정보

46) 18. U.S.C. §2711(4).

수집이 가능하다. 그러나 수사기관에서 개별적으로 직접 정보를 요청하여 제공받는 경우 절차의 부재로 업무 처리가 비효율적이고, 기술의 미비로 수사정보 및 개인정보가 유출될 가능성이 농후하다.

일반적으로 서비스 제공자의 제3자 보관 정보에 대한 압수수색은 현장에서 수색해서 압수하는 것이 아니라 피압수자의 협조를 통해 제공받는 형태로 이루어진다. 국내 서비스 제공자의 경우에는 압수수색 시 전문가인 피압수 서비스 제공자의 서버 관리자의 협조를 받아 데이터베이스에서 대상 정보를 추출하는 방식으로 비대면으로 제3자 보관 정보를 확보하고 있다. 국외 서비스 제공자의 제3자 보관 정보에 대한 압수수색은 글로벌 IT 서비스 기업의 경우 이메일이나 법집행 요청 포털을 통해 집행하고 기록에 첨부하고 있는 현황이다.

현재 국외 서비스 제공자의 제3자 보관 정보에 대한 압수수색은 다음과 같은 과정으로 이루어진다. 수사기관은 법원에서 국외 서비스 제공자를 대상으로 압수수색영장 또는 통신사실확인자료 제공요청 허가서를 발부받는다. 그리고 국외 서비스 제공자의 이메일이나 법집행 요청 포털로 영장이나 허가서를 제출하고 제3자 보관 정보 제공을 요청한다. 이후 국외 서비스 제공자의 법집행 담당자가 수사기관에서 요청한 제3자 보관 정보를 기관 이메일이나 법집행 요청 포털을 통해 제공하면 다운로드받아 분석하고 기록에 첨부하는 것으로 절차는 종료된다.

제3자 보관 정보 제공 시 글로벌 IT 서비스 기업의 정책과 개인정보 처리지침에 따라 해외 법집행기관에 자발적으로 협조하므로 서비스 제공자마다 제공하는 정보의 형태가 다르다. 동일한 분야일지라도 기업별로 저장하는 데이터 방식과 사용하는 양식이 다르고, 정책이 자주 바뀌므로 처음 해보거나 자주 해보지 않으면 시행착오를 겪는다. 신속한 압수수색영장 집행이 사이버공간상 범죄의 증거인멸을 방지할 수 있는 최선의 방법인데, 이러한 압수수색절차에서는 신속성을 기대하기 어렵다. 제3자 보관 정보 수집 과정에서 불필요하게 낭비되는 시간을 단축시키고 업무의 효율성을 향상시키는 시스템 및 제도가 필요하다.

한편, 압수수색영장 집행 후 피압수회사의 법집행 담당자로부터 기관 이메일이나 법집행 요청 포털로 제공받는 과정에서 해킹의 위험이 있다. 제3자 보관 정보 수신 후 해당 정보를 컴퓨터에 저장한 채 방치하는 경우 정보 유출의 문제에서도 자유로울 수 없다. 국외 서비스 제공자에 개별적으로 제3자 보관 정보를 요청하여 제공받는 과정에서 드러난 한계로 인해 사건 처리가 지체되거나 유출된 정보를 이용하여 2차 피해를 입게 되는 결과로 이어질 수 있다.

인권을 보장하는 수사환경으로의 변화 속에서 이러한 방법으로 국외 서비스 제공자가 보관하는 제3자 보관 정보를 수집하는 것은 심각한 문제다. 사이버범죄 수사에 필요한 제3자 보관 정보 수집과 관련하여 보다 안정적이고 효율적인 방향으로 증거 확보 방법의 변화가 요구된다. 현행 직접 요청 방법의 불확실성을 제거하고 개인정보를 보호하면서 신속한 수사를 통해 경제적 효과를 얻을 수 있는 대안에 대해 모색할 필요가 있다.

2. 직접 협조 요청 문제의 해결방안

사이버범죄의 증거는 클라우드 컴퓨팅 환경에서 장소를 바꿔가며 존재한다. 제3자 보관 정보를 확보하기 위해 이를 관리하고 있는 외국과 수사공조는 필수다. 국내에서 사이버범죄를 대상으로 하는 국제공조 방법 중 국외 서비스 제공자에 직접 요청은 증가하는 반면, 정형화된 체계 없이 개별적으로 이루어지고 있어 표준화된 절차가 필요하다.

제3자 보관 정보의 수집은 개인정보 침해의 소지가 있는 조치이므로 비례원칙에 따라 필요한 최소한도에서 요건을 규정하고 관련 근거를 마련할 필요가 있다. 국외 서비스 제공자에 직접 국내에서 발부된 압수수색영장을 집행할 때는 가입자정보에 한정한다. 가입자정보는 사용자가 서비스 이용을 위해 가입할 때 기재하는 인적사항으로, 개인을 특정할 수 있는 개인정보를 포함하고 있다. 사이버범죄 수사에 있어 기초가 되어 빈번하게 요구되는 가입자정보는 통신내용, 트래픽데이터에 비해서 개인정보 침해의 소지가 적다. 우리나라의 경우 가입자정보는

개인정보 보호법에 따라 수집하고 사용할 수 있으며, 국내 서비스 제공자의 경우 수사기관이 가입자정보를 요구하면 제공하고 있다.

한편, 현행 형사사법정보시스템의 기술을 활용하여 유사한 형태의 전자서명 적용 서비스 플랫폼을 구축해 제3자 보관 정보 수집 과정에서 정보 유출 없이 수집한다. 국내 형사사법정보시스템은 가상사설망(Virtual Private Network, VPN)을 통해 각 통신사와 연결되어 있다. VPN은 가상사설망 전용 회선을 통해 네트워크를 연결하고 보안 단계를 거쳐서 정보를 송수신한다. 우리나라 기간통신사업자인 SKT, KT, LGU+의 경우에는 형사사법정보시스템과 연계하여 통신자료제공요청을 집행하면 당일에 회신하고 있다. 국제공조 전담부서에서 통합하여 절차대로 국외 서비스 제공자에 제3자 보관 정보를 직접 요청하고 회신받는 기간을 단축하면 업무의 효율성을 충분히 높일 수 있다.

국외 서비스 제공자가 저장하는 제3자 보관 정보는 기간통신사업자들이 저장하는 정보의 형태와 차이가 있으므로 서비스 제공자의 특성에 맞게 형사사법정보시스템 구조를 보완한다. 제3자 보관 정보 서비스 플랫폼은 구현하는데 소요되는 비용과 시스템 활용도를 고려하여 구현 시 우선순위를 정한다. 수사기관과 국제공조 전담부서에서 국외 서비스 제공자의 가입자정보를 요청하거나 제공하는 방식, 시스템 연결에 적용되는 기술 등을 협의하여 구축한다.

3. 전자서명 적용 서비스 플랫폼

국외 서비스 제공자에 직접 요청하여 제공받는 제3자 보관 정보는 국내법상 형사사법정보시스템을 통해 통신자료제공요청 시 회신받는 가입자정보에 해당한다. 형사사법정보시스템의 기술을 활용하여 국외 서비스 제공자의 제3자 보관 정보 수집 시 전자서명 적용 서비스 플랫폼인 제3자 보관 정보 서비스 플랫폼을 통해 송수신하도록 한다. 수사기관이 내부 시스템을 통해 국제공조 전담부서로부터 전송받은 정보의 경우 통신자료의 보관기간과 동일하게 적용한다. 해당 정보를 전송받은 시점부터 7일 보관 후 시스템상에서 자동으로 삭제되도록

설정한다.

전자서명 적용 서비스 플랫폼을 통해 수사기관에서부터 국제공조 전담부서를 거쳐 국외 서비스 제공자까지 이어지는 제3자 보관 정보 수집은 여러 가지 이점이 있다. 전자서명으로 전자문서의 공개키 기반 구조를 활용한 암호화 기술을 통해 송수신 과정에서 정보가 외부로 유출될 위험을 줄여 개인정보를 보호하고 기본권을 보장할 수 있다. 또한, 제3자 보관 정보 요청 및 제공 송수신 여부, 전자서명을 한 전자문서의 전송 등은 국제공조 전담부서에서 통합 관리하고 시스템적으로 처리하여 인력 유지에 대한 비용이 줄어든다. 즉, 제3자 보관 정보 서비스 플랫폼을 통해 전자문서의 전송체계를 변경하면, 제3자 보관 정보의 전송 중에 발생할 수 있는 손망실을 최소화하고 행정비용을 낮추는 효과가 있다.[47]

4. 공개키 기반 구조의 전자서명

전자서명으로 전자문서에 대한 인증과 손상·훼손되지 않았다는 것을 증명할 수 있다. 공개키 기반 구조의 전자서명은 전자서명 이후에 변경되는 법제도적 규정을 반영하여 수정 및 보완을 통해 발전적인 방향으로 나아가도록 한다. 전자서명 사용기간 도과로 폐지 시에도 이전에 한 전자서명의 서명자를 확인하여 검증할 수 있도록 서비스를 구현해야 한다.

기본적인 구조는 송신자의 공개키/개인키를 생성하고, 전자문서를 해시함수에 통과시켜 해시값으로 변환한다. 이 해시값을 송신자의 개인키로 암호화하여 전자서명을 생성한 후 수신자에게 전자문서, 전자서명, 송신자의 공개키가 포함된 인증서를 함께 전송한다. 전자서명의 검증을 위해서는 우선 인증기관의 개인키로 서명한 인증서를 인증기관의 공개키로 복호화하여 인증기관의 서명을 검증한다. 인증서의 유효성이 인증되면 송신자의 공개키로 전자서명을 검증하여 송신자가 전자문서에 서명한 사실을 확인할 수 있다.

---

47) 김종빈, 앞의 논문, 78면.

제5장 공개키 기반 구조의 전자서명 소개

제1절 공개키 기반 구조의 의의

1. 전자서명의 전제조건[48)]

전자서명을 이용하기 위해서는 수신자가 서명을 검증할 때 이용하는 공개키가 송신자의 공개키라는 전제조건이 있다. 이렇게 검증된 공개키를 확보하기 위해 고안된 인증서는 공개키를 메시지로 간주하고, 인증기관(제3의 신뢰기관)이 서명을 해서 받은 형태다. 공개키 암호 및 전자서명 기술이 인증서 발급과 사용을 위한 키의 생성, 인증 과정을 안전하게 관리할 수 있는 체계가 공개키 기반 구조(Public-Key Infrastructure, PKI)다.

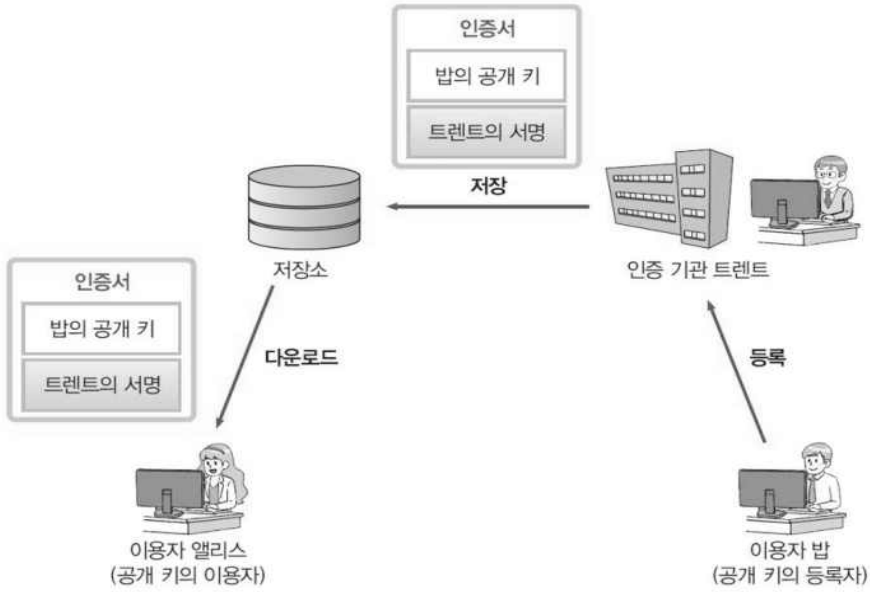
공개키 알고리즘을 위한 키 관리 구조인 공개키 기반 구조의 경우 공개키 알고리즘을 사용하는 응용 방식은 디렉터리에 공개키를 공개한다. RFC 2822[49)]에서 공개키 기반 구조는 비대칭키 암호시스템에 기초하여 디지털 인증서를 생성·관리·저장·분배·폐지하는데 필요한 하드웨어, 소프트웨어, 사람, 정책, 절차로 정의한다. 공개키 기반 구조에는 인증기관, 검증기관, 등록기관, 사용자, 저장소 등이 포함된다.

공개키 기반 구조는 인터넷상에서 신분증을 검증해주는 구조로 인증기관은 동사무소, 인증서는 신분증에 해당한다. 신분증 검증의 경우 동사무소, 구청, 시청 순으로 최상위에는 정부가 있다. 현실에서 다른 지역의 동사무소에서 자신의 신분증을 제시하고 주민등록등본 발급이 가능하듯이 공개키 기반 구조에서 사용자는 어디에서든지 인증기관에서 받은 인증서를 통해 증명이 가능하다.

---

48) 조현준, 『2022 알기사 정보보안기사(산업기사) 필기』, 도서출판 탑스팟 (2022), 107-108면.

49) IETF(Internet Engineering Task Force) 공식표준문서.



[그림 1] 공개키 기반 구조의 구성도[50]

2. 공개키 기반 구조의 형태[51]

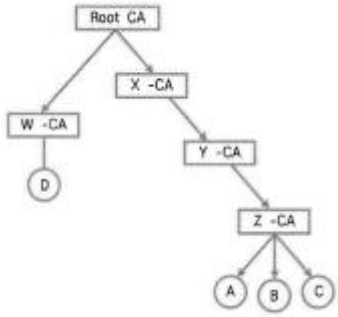
가. 계층 구조

최상위의 루트 CA 아래에 계층적으로 하위의 인증기관이 존재하는 트리 형태다. 상위 인증기관이 하위 인증기관에 CA 인증서를 발급하고, 상위 인증기관의 인증정책에 하위 인증기관은 영향을 받는다. 루트 CA 간의 상호 인증은 허용하는 반면에 하위 인증기관 간 상호 인증은 배제한다. 최상위 인증기관 간 상호 인증을 통해 외국과 상호 연동을 원활하게 한다.

---

50) 박종혁, "2022-1st 정보보호론-제11장 인증서", SeoulTech UCS Lab, 27면 <http://www.parkjonghyuk.net/lecture/2022-1st-lecture/information-protect/chap11.pdf> (2022. 11. 30. 방문).

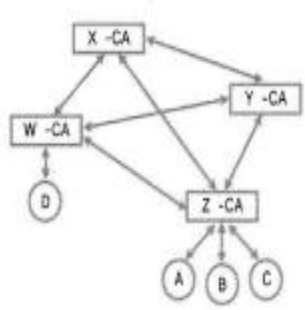
51) 조현준, 앞의 책, 110-111면.



[그림 2] 공개키 기반 구조의 계층 구조[52)]

나. 네트워크 구조

상위 인증기관의 영향 없이 각 인증기관의 인증정책에 따라 독립적으로 존재한다. 인증기관 간 인증을 위해 상호 인증서를 발급하여 인증 서비스를 하며, 상호 인증이 모두 허용될 경우 상호 인증 수는 폭증하게 된다.



[그림 3] 공개키 기반 구조의 네트워크 구조[53)]

다. 혼합형 구조

계층 구조와 네트워크 구조의 장점을 혼합하여 도메인별 신뢰관계에 적합한 구조다. 각 도메인의 독립적 구성을 허용하면서 서로 효율적인 상호 연동을 보장한다.

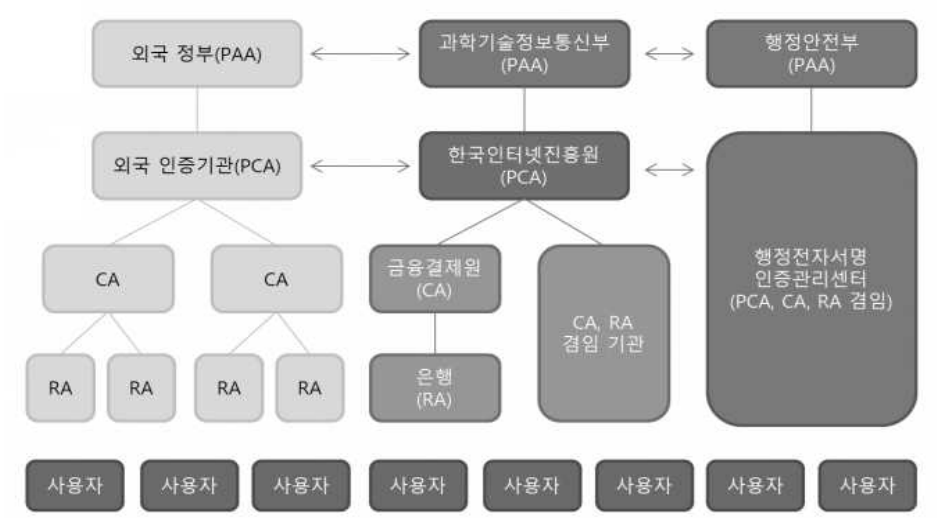
---

52) 조현준, 앞의 책, 111면.
53) 조현준, 앞의 책, 111면.

3. 공개키 기반 구조의 구성[54]

가. 인증기관

인증기관(Certification Authority, CA)은 인증정책 수립, 인증서 인증 및 효력 정지, 폐지 목록 관리를 하며 다른 인증기관과 상호 인증을 제공한다. 우리나라의 경우 정부 최상위 인증기관인 행정전자서명 인증관리센터와 금융결제원, 한국지능정보사회진흥원, 한국정보인증, 한국전자인증, 코스콤, 한국무역정보통신 등의 공동인증기관이 있다.



[그림 4] 공개키 기반 구조의 구성 요소[55]

(1) 정책 승인기관

정책 승인기관(Policy Approving Authority, PAA)은 '루트 CA'로 인증서 운영을 위한 최상위 계층에 위치하며, 공개키 기반 구조 전반에 사용되는 정책과 절차를 수립한다. 공개키 기반 구조의 최상위 인증기관으로서 하위 기관들의 정책 준수 상태 및 적정성을 감사하는 역할을 한다. 정부 공개키 기반 구조의 경우 정책 승인기관은 외국의 정책 승인기관들과 상호 연동을 위한 협정을 체결한다.

---

54) 조현준, 앞의 책, 108-110면.
55) "공개키 기반 구조" <https://itwiki.kr> (2022. 11. 30. 방문).

(2) 정책 인증기관

정책 인증기관(Policy Certification Authority, PCA)은 정책 승인기관 아래 계층으로 자신의 도메인 내 사용자와 인증기관이 따라야 할 정책을 수립한다. 인증기관의 공개키를 인증하고 인증서 및 인증서 폐지 목록 등을 관리한다.

(3) 인증기관

인증기관(Certification Authority, CA)은 정책 인증기관 아래 계층으로 등록기관의 요청에 의해 사용자의 공개키 인증서를 발급하고, 필요에 따라 폐지해 인증서 폐지 목록을 발급한다. 인증서 발급은 인증기관에서 하는데, 인증기관별 등록대행기관에서도 인증서를 발급받아 사용할 수 있다. 인증기관은 사용자에게 자신의 공개키 및 상위 기관의 공개키를 전달하고, 인증서 사용자를 대신하여 공개키/개인키 쌍을 생성할 수 있으며 안전한 방법으로 전달한다. 인증기관의 업무 중 공개키 등록과 본인에 대한 인증은 등록기관이 하는 경우도 있다.

나. 검증기관

검증기관(Validation Authority, VA)은 인증서와 관련된 거래의 유효성을 확인하고, 인증서의 유효성 여부와 인증서가 적절한 개체로 발급된 사실을 신뢰 당사자에게 확인해주는 역할을 한다. 검증기관 없이 인증기관만 존재할 수 있지만, 인증서 검증이 없을 경우 보안 측면에서 인증서 기반 응용은 불완전하다. 검증기관은 인증기관이 통합적으로 직접 운영하거나 독립해서 외주로 운영한다.

다. 등록기관

등록기관(Registration Authority, RA)은 사용자와 인증기관이 원거리에 있는 경우, 사용자와 인증기관 사이에서 사용자가 인증서를 신청할 때 인증기관 대신 사용자의 신분을 확인한다. 등록기관은 사용자의 신분과 소속을 확인하고 인증서 요청에 서명한 후 인증기관에 제출한다. 등록기관의 서명을 확인한 인증기관은 사용자의 인증서를 발급하여 등록기관이나 사용자에게 전달한다. 등록기관은 선택 요소로 등록기관이

없을 때 인증기관이 등록기관의 기능을 수행한다.

라. 사용자 및 최종 개체

공개키 기반 구조 내 사용자는 사람, 사람이 이용하는 시스템을 모두 의미한다. 공개키/개인키 쌍 생성, 공개키 인증서를 요청하여 획득, 전자서명의 생성 및 검증이 가능하다. 개인키의 분실·손상, 조직의 탈퇴 등으로 사용자의 정보가 변경되면 인증서 폐지 요청을 수행한다.

마. 저장소

저장소(Directory)는 사용자의 인증서를 저장하는 데이터베이스로 인증기관이 인증서를 발급하면 디렉터리에 저장하며, 사용자는 상대방의 인증서 검색이 가능하다. 저장소에 사용자 정보가 포괄적으로 관리되고 상황에 따라 접근 제한을 한다. 현재 디렉터리 표준형식은 ITU-T에서 정의한 X.500과 이것을 개선한 LDAP(Lightweight Directory Access Protocol) 등이 있다.

4. 공개키 기반 구조의 대상[56)]

가. 인증서

인증서(Public-Key Certificate, PKC)는 공개키 기반 구조의 주요 관리 대상이며, 인증기관(제3의 신뢰기관)이 표준화된 형식으로 발급한다.

(1) 인증서 표준 규격

인증서는 인증기관에서 발급하고 사용자가 검증하는데, 인증서의 형식은 표준 규격으로 정해져 있다. ITU, ISO에서 정하고 있는 X.509는 가장 많이 사용되는 인증서 표준 규격이다. X.509는 인증서를 작성하고 교환할 때 표준 규격으로 다수의 응용 방식에서 지원된다. X.509 인증서는 IP 보안(Internet Protocol Security), 보안 소켓 계층(Secure Sockets Layer, SSL), 안전한 전자 거래(Secure Electronic Transaction, SET), 보안/다목적 인터넷 메일 확장(Secure/Multipurpose Internet Mail Extension, S/MIME) 등 네트워크 보안 응용에서 주로 사용되고 있다.

---

56) 조현준, 앞의 책, 111-115면.

(2) 인증서 구조

인증서에는 이름, 전자서명 검증정보, 인증기관이 이용하는 전자서명 방식, 인증서의 일련번호 등이 포함되어 있다. 인증서 내부에는 버전, 일련번호, 서명 알고리즘, 발급자, 유효기간(시작), 유효기간(끝), 주체, 공개키 등이 있다. 이 중 버전은 인증서의 버전을 의미하며 우리나라의 경우 X.509 V3 표준을 사용하고, 서명 알고리즘은 sha256RSA를 이용한다. 일련번호는 인증서의 고유번호를 나타내며, 유효기간(시작)과 유효기간(끝)은 인증서의 유효기간 시작일과 종료일을 의미한다. 그 밖에도 기관 키 식별자, 주체 키 식별자, 주체 대체 이름, CRL 배포 지점, 기관 정보 액세스 등 다양한 정보가 있다.

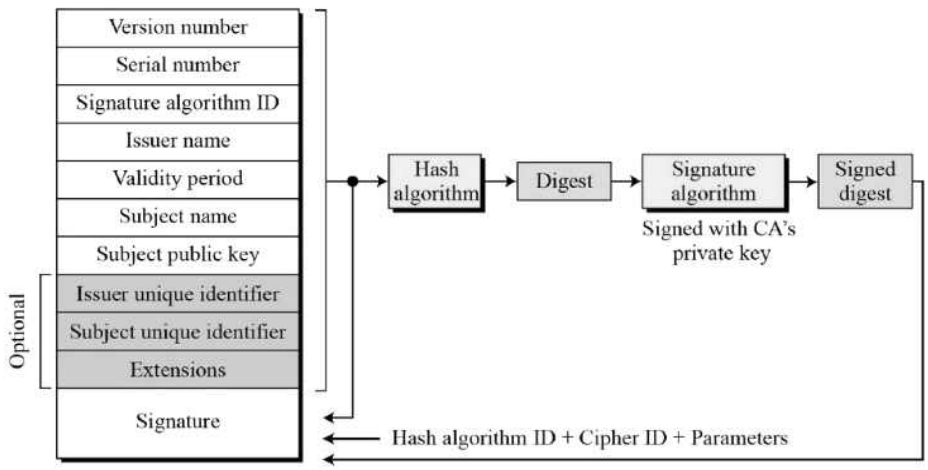
공개키 인증서에는 이름, 소속, 이메일 주소 등 개인정보와 그 사람의 공개키가 기재되어 있고, 인증기관의 개인키로 전자서명 되어 있다. 공개키/개인키 한 쌍과 특정 사람/기관을 연결시켜 해당키가 특정인의 것이라는 사실을 보증한다. 또한, 전자서명에 사용된 개인키에 대응하는 공개키를 제공하여 그 공개키가 특정인의 것이라는 사실을 확신할 수 있는 증거의 기능을 한다. 인증서가 저장되는 경로에는 NPKI와 GPKI 폴더가 있다. NPKI(National Public-Key Infrastructure)는 일반 국민을 대상으로 하는 개인용 인증서, GPKI(Government Public-Key Infrastructure)는 정부기관에서 사용하는 인증서를 의미한다.

요소	구분	설명
버전번호 (Version number)	필수	인증서의 X.509 버전 정의
일련번호 (Serial number)	필수	인증기관에 의해 부여되는 번호(인증기관에서 발급한 인증서에 대해서는 유일)
서명 알고리즘 식별자 (Signature algorithm ID)	필수	인증기관이 인증서에 서명하기 위한 알고리즘, 알고리즘 식별자를 포함(인증서 끝부분에 있는 서명 필드에도 포함)
발급자 이름 (Issuer name)	필수	인증서 발급자(인증기관)의 이름

유효기간 (Validity period)	필수	인증서 유효기간의 시작일, 종료일
주체 이름 (Subject name)	필수	인증서에 대한 사용자의 이름(상위 인증기관이 하위 인증기관에 인증서를 발급하는 경우 사용자는 인증기관)
주체의 공개키 정보 (Subject public key)	필수	사용자의 공개키 정보(공개키, 관련 알고리즘)
발급자 유일 식별자 (Issuer unique identifier)	선택	발급자, 사용자의 이름이 중복되는 경우 구별하기 위한 수단
주체 유일 식별자 (Subject unique identifier)	선택	다른 개체가 X.509 이름을 재사용할 경우 사용자를 유일하게 구별하는데 사용
확장 (Extensions)	선택	발급자가 인증서에 사적인 정보를 추가할 수 있는 필드(V3에서 추가)
서명 (Signature)	필수	다른 필드 전체에 해시함수를 적용하여 얻은 해시값을 인증기관의 개인키로 암호화한 서명값(인증서의 나머지 필드 전체를 보호)

[표 2] X.509 인증서 프로파일[57]

(3) 인증서 형식



[그림 5] X.509 인증서 형식[58]

57) 조현준, 앞의 책, 113면.

나. 인증서 확장 영역

X.509 V3 인증서 확장 영역은 사용자의 공개키 정보와 연관된 추가 정보 및 인증서의 계층 구조 관리 방법을 제공한다.

(1) 키 및 정책 정보

인증서와 관련된 키와 키의 용도, 인증서 정책에 관한 부가적인 정보를 포함한다. 기관키 식별자는 인증서에 서명하기 위해 사용되는 개인키에 대응하는 공개키를 구분한다. 주체키 식별자는 최종 개체가 여러 인증서를 획득한 경우 특정 공개키를 포함하는 인증서의 집합을 빠르게 구분할 수 있다. 키 용도는 인증서에 포함된 암호화, 서명, 인증서 서명 등 키의 용도를 정의한다. 인증서 정책은 인증기관이 발급한 인증서에 대한 정책으로 인증서 내에 표기한다.

(2) 주체 및 발급자 속성

주체, 인증서 발급자에 대해 다양한 형식의 대체 이름을 지원한다. 주체 대체 이름은 추가 신분이 인증서의 사용자와 결합할 수 있도록 한다. 정의된 선택 사항에는 인터넷 메일 주소, DNS(Domain Name System) 이름, IP 주소, URI(Uniform Resource Identifier)가 포함된다. 발급자 대체 이름은 여러 형식으로 된 다른 대체 이름을 포함한다.

(3) 인증 경로 제약조건

다른 인증기관이 발급한 인증기관의 인증서에 포함될 제약조건을 제공한다. 기본 제약조건은 인증서의 사용자가 인증기관인지 여부를 구분한다. 이름 제약조건은 특정 이름의 형태가 나타날 때 사용자 고유 이름, 사용자 대체 이름을 제한한다. 정책 제약조건은 인증기관에 발급된 인증서 내 정책 제약을 확장할 수 있다.

다. 인증서 폐지

인증서에는 유효기간이 있는데, 인증서에 문제가 있으면 인증기관은 사용 중인 인증서의 유효기간이 끝나기 전에도 폐지한다.

---

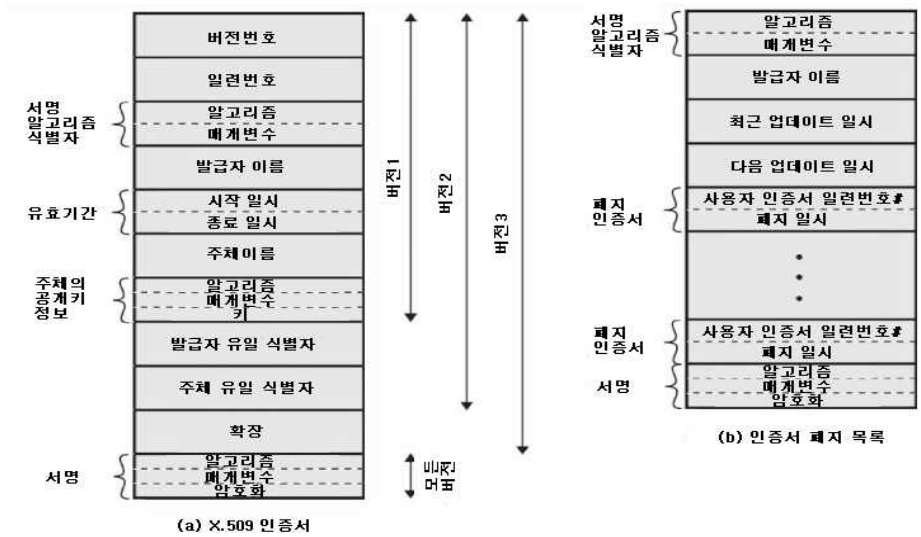
58) Behrouz A. Forouzan, 이재광·신상욱·임종인·전태일 공역, 『암호학과 네트워크 보안』, 한티에듀 (2021), 488면.

(1) 인증서 폐지 사유

사용자의 개인키가 침해당하였거나 인증기관이 사용자를 더 이상 인증하지 않을 때 그 기관과 관련해 발급된 사용자의 인증서는 유효기간이 끝나기 전이라도 폐지해야 한다. 또한, 인증서를 검증하는데 필요한 인증기관의 개인키가 침해받았을 때는 유효기간이 남아있어도 인증기관은 모든 인증서를 폐지해야 한다.

(2) 인증서 폐지 목록

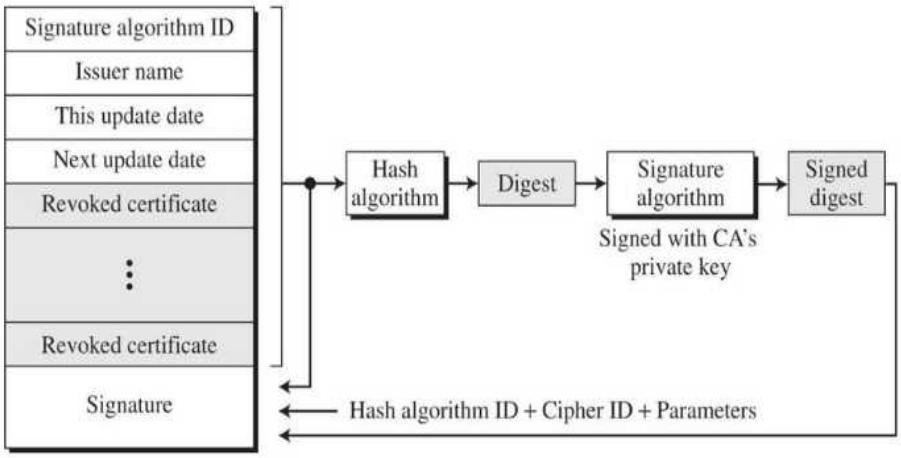
인증서 폐지 목록(Certificate Revocation List, CRL)은 폐지된 인증서들의 목록이며, 인증기관의 디렉터리 시스템에 포함하여 신뢰 당사자가 언제든지 이 목록을 검색할 수 있도록 한다. 폐지된 인증서의 경우 사용자에게 발급한 것과 다른 인증기관에 발급한 것을 모두 포함한다. 인증서 폐지 목록에는 인증서 폐지 목록의 버전, 서명 알고리즘 및 발급자 이름, 인증서 발급일, 다음 업데이트일, 폐지된 인증서에 대한 정보[59]가 포함되어 있고, 폐지된 인증서는 일련번호로 확인 가능하다.



[그림 6] X.509 인증서 및 인증서 폐지 목록[60]

59) 인증서 일련번호, 폐지일, 폐지 사유 등.

(3) 인증서 폐지 형식



[그림 7] X.509 인증서 폐지 형식[61]

라. 인증서 운영 프로토콜

온라인 인증서 상태 검증 프로토콜(Online Certificate Status Protocol, OCSP)은 IETF의 PKIX[62] 워킹그룹에서 1997년 처음 제안한 이후 개정을 거쳐 RFC 2560(Proposed Standard : 1999)으로 발표되었다. 온라인 인증서 상태 검증 프로토콜은 인증서의 상태 정보를 실시간으로 확인 가능한 서비스이며, OCSP 클라이언트, OCSP 서버, 인증기관 서버로 구성된다.

온라인 인증서 상태 검증 프로토콜은 인증기관이 관리하는 인증서 폐지 목록을 검사하는데, 온라인 인증서 상태 검증 프로토콜이 구현되면 백그라운드에서 자동으로 작업이 수행된다. 즉, 인증서 검증 과정을 통해서 인증서 폐지 목록을 확인할 수 있는 프로토콜을 가지게 되는 구조다.

---

60) 김호원, "인증서 및 OpenID Connect OAuth2 기술", 부산대학교 정보보호 및 사물지능 연구실, 8면 <http://infosec.pusan.ac.kr/wp-content/uploads/2019/09/3.-%EC%9D%B8%EC%A6%9D%EC%84%9C-%EB%B0%8F-OpenID-Connect-OAuth2%EA%B8%B0%EC%88%A0.pdf> (2022. 11. 30. 방문).

61) Behrouz A. Forouzan, 이재광·신상욱·임종인·전태일 공역, 앞의 책, 490면.

62) Public-Key Infrastructure X.509.

한편, 인증서 관리 프로토콜(Certificate Management Protocol, CMP)은 공개키 기반 구조에서 인증서 관리 서비스를 제공하기 위한 공개키 기반 구조의 사용자, 인증기관, 등록기관, 저장소 사이의 통신 프로토콜이다.

[그림 8] 온라인 인증서 상태 검증 프로토콜의 구성도[63]

제2절 전자서명의 이해

1. 전자서명의 개념

전자서명(Electronic signature)은 일반적으로 컴퓨터를 매개로 하여 전자적 형태의 자료로 서명자의 신원을 확인하고 자료의 내용에 대한 당사자의 승인을 의미한다. 본고에서는 구체적으로 전자기술을 통해 구현된 공개키 암호 방식을 이용한 전자서명(Digital signature)의 의미를 나타낸다.

전자서명법상 전자서명은 “서명자의 신원, 서명자가 해당 전자문서에 서명하였다는 사실을 나타내는데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보”로 정의한다. 한편, 전자문서는 “정보처리시스템에 의해 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보”라고 규정하고 있다.

전자서명 중 비밀키 암호화 서명은 서명의 생성과 검증을 제3자가 중재하며, 서명할 때마다 인증기관(제3의 신뢰기관)이 참여해야 한다.

63) 한국전자인증 웹사이트 <https://www.crosscert.com/solution/03_1_05.jsp> (2022. 11. 30. 방문).

과거부터 널리 사용되어 온 비밀키 암호화의 경우 암호화와 복호화에 동일한 키를 이용하는 대칭키 암호 방식이다. 암호화와 복호화에 동일한 암호키(대칭키)를 사용하여 비밀키 암호 방식에서는 암호화하는 자와 복호화하는 자가 사전에 키를 공유해야 한다. 또한, 암호화가 많아지거나 암호화에 참여하는 사람의 증가에 비례하여 관리해야 하는 키의 수가 증가하는 어려움이 존재한다.

공개키 암호화 서명의 경우 서명자의 검증정보를 공개해 누구나 검증 가능하며, 비밀키 암호화 서명에 비해 서명의 생성과 검증이 편리하다. 키 공유 문제를 해결하기 위해 고안된 공개키 암호화는 비대칭키 암호 방식이다. 1970년대에 등장한 공개키 암호 방식은 단방향 함수의 특성을 활용한다. 단방향 함수란 일방향에서는 계산이 용이하나 역으로는 계산이 어려운 함수로, 대표적으로 소인수분해가 있다. 공개키 암호 방식인 RSA 암호에서는 이러한 소인수분해의 어려움을 이용하고 있다.[64]

공개키 암호화의 경우 효율성 제고를 위해 비밀키 암호화와 함께 하이브리드 암호 방식의 형태로 사용한다. 시간과 데이터양의 측면에서 보면 비밀키 암호화가 공개키 암호화보다 효율적이므로 대량의 정보를 암호화할 때는 비밀키 암호 방식, 키 공유와 같은 중요한 전달에는 공개키 암호 방식을 사용하는 것이다.[65]

2. 전자서명의 방식

가. 메시지 복원형 전자서명

서명자는 공개키/개인키를 생성한 후 자신의 개인키를 이용하여 메시지를 암호화해 전송하고, 검증자는 서명자의 공개키를 이용해 서명된 암호문을 복호화한다. 검증 결과 일정한 규칙을 만족하여 유의미한 메시지가 확인되면 서명이 검증된다.

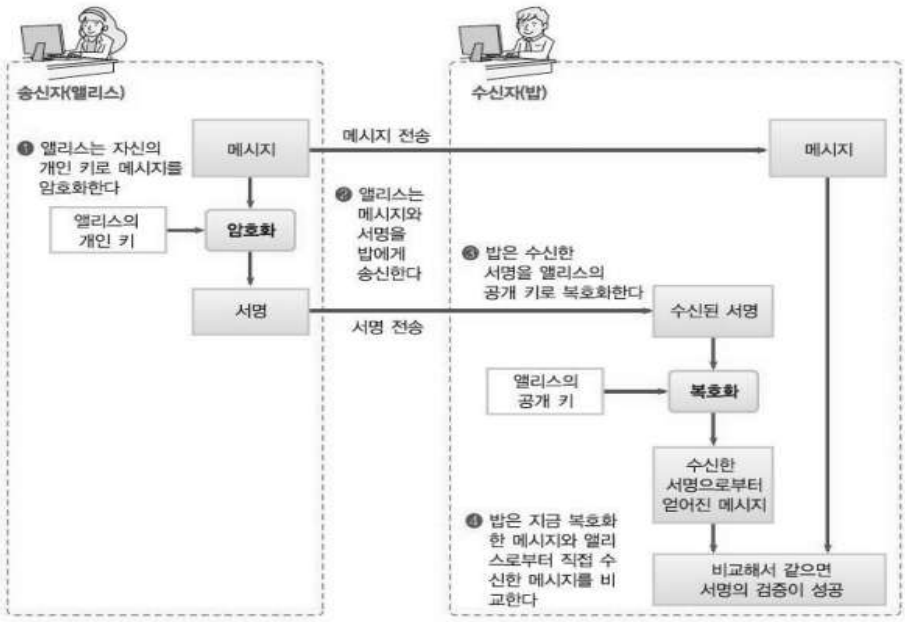
---

64) 마이크로소프트 학습 웹사이트 “공개 키 암호화 이해” <https://technet.microsoft.com/ko-kr/library/aa998077(v=exchg.65).aspx> (2022. 11. 30. 방문).

65) 남성우, “공개키 암호를 이용한 전자정보 보전처분에 관한 연구”, 석사학위논문, 서울대학교 (2021), 34면.

메시지 복원형 전자서명 방식은 기존 공개키 암호 방식을 이용하므로 별도의 전자서명 프로토콜이 필요하지 않다. 그러나 메시지를 일정한 크기의 블록으로 나누어 각 블록에 서명해야 하므로 시간이 오래 걸려 실제로는 사용하지 않는다.

송신자가 메시지에 서명을 생성하고, 수신자는 서명을 검증한다. 사전에 송신자는 공개키/개인키의 키 쌍을 만들고, 수신자는 서명을 검증하기 위해 송신자의 공개키를 확보해둔다.



[그림 9] 메시지 복원형 전자서명 방식[66]

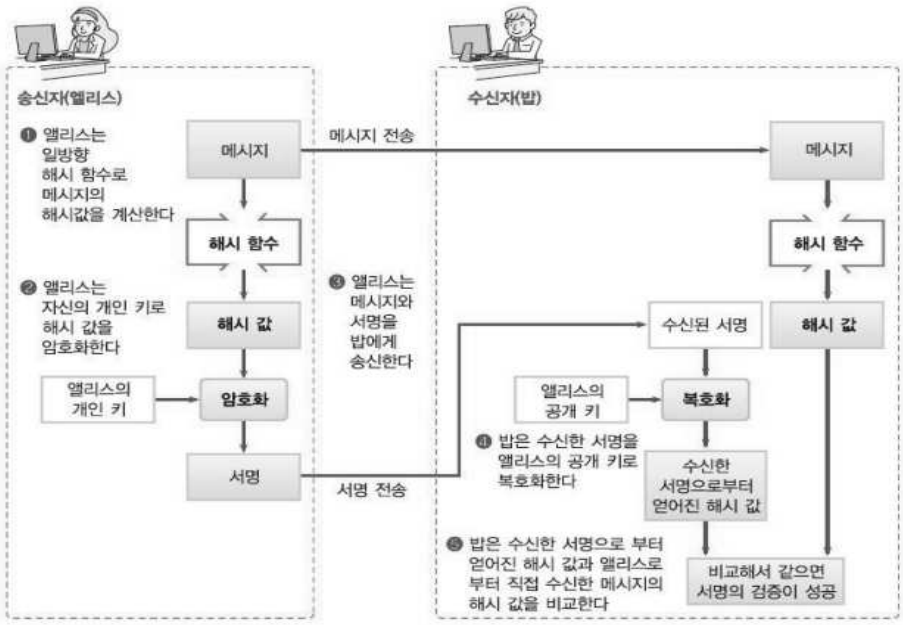
66) 박종혁, “2019-2nd 정보보호론-제10장 디지털서명”, SeoulTech UCS Lab, 19면 <http://www.parkjonghyuk.net/lecture/2019-2nd-lecture/informationsecurity/chap10.pdf> (2022. 11. 30. 방문).

나. 메시지 부가형 전자서명

임의의 길이로 주어진 메시지를 해시함수를 이용하여 일정한 길이로 압축하고, 그 해시값에 서명자의 개인키를 이용하여 전자서명을 생성한 후 메시지에 부가한 형태로 전송한다. 전자서명의 검증은 수신한 메시지의 해시값과 공개키를 이용하여 전자서명을 복호화한 값을 비교한다.

메시지 부가형 전자서명 방식은 메시지와 전자서명을 전송해야 하므로 전송량이 증가하지만, 메시지의 길이에 상관 없이 서명 생성 과정을 한 번만 거쳐 효율적이므로 실제로 많이 사용된다.

송신자가 메시지의 해시값에 서명하고, 수신자는 서명을 검증한다. 메시지 전체를 암호화하는 대신 일방향 해시함수를 사용하여 메시지의 해시값을 구하고, 그 해시값에 서명하여 암호화한다. 메시지가 길어도 해시값은 짧으므로 암호화하기에 용이하다.



[그림 10] 메시지 부가형 전자서명 방식[67]

67) 박종혁, 앞의 자료, 21면.

3. 특수 전자서명의 유형[68]

가. 부인방지 서명

전자서명은 검증자가 누구든지 검증할 수 있으며, 임의로 검증이 가능한 자체 인증 특성이 있다. 한편, D.Chaum에 의해 제안된 부인방지 서명은 자체 인증하는 기능을 배제시켜 서명을 검증할 때 서명자가 있어야 검증 가능한 서명 방식이다.

나. 의뢰 부인방지 서명

부인방지 서명은 자신의 서명을 부인하지 못하게 하므로 거짓말 탐지기 기능을 제공한다. 이러한 방식은 검증을 원하는 검증자가 누구든지 부인 과정을 수행할 수 있어 문제가 된다. 부인방지 서명의 거짓말 탐지기 기능 문제를 해결하기 위해 임의의 검증자가 부인 과정을 수행하지 못하고 특정 검증자만 부인 과정을 수행할 수 있도록 한다.

다. 수신자 지정 서명

전자서명의 검증 시 특정 검증자만 서명을 확인할 수 있고, 그 서명이 문제가 있는 경우에도 검증자의 비밀서명 생성정보를 노출시키지 않고 제3자에게 서명의 출처를 증명한다. 지정된 수신자만 서명을 확인할 수 있고, 필요 시 제3자에게 그 서명이 서명자에 의해 수신자에게 발행된 서명임을 증명할 수 있어 검증자가 서명의 남용을 통제할 수 있다.

라. 은닉 서명

은닉 서명은 D.Chaum이 제안한 방식으로, 서명 용지 위에 묵지를 놓고 봉투에 넣어 서명자가 서명문을 모르는 상태에서 서명하도록 한다. 이러한 방식은 서명문의 내용을 숨기는 서명으로 서명을 받는 사람의 신원과 서명문을 연결시킬 수 없어 익명성을 유지할 수 있다.[69]

서명자인 은행이 화폐에 은닉 서명을 하면 화폐의 소유자에 대한 익명성 유지가 가능하다. 은행은 추적 불가능한 화폐의 특성을 통해 고객에 대한 익명성을 보장한다. 고객이 묵지가 내장된 봉투에 서명받을

---

68) 조현준, 앞의 책, 104-105면.

69) Behrouz A. Forouzan, 이재광·신상욱·임종인·전태일 공역, 앞의 책, 439면.

화폐를 동봉해 은행에 보내면, 은행은 해당 고객의 예금 계좌에서 해당 금액을 인출하고 고객이 보낸 봉투 위에 서명한다. 이 경우 묵지에 의해 봉투 안에 있는 서명 용지에도 동일하게 서명된다. 은행이 서명된 봉투를 고객에게 보내면, 고객은 봉투를 제거하고 그 안에 있는 용지 위의 서명을 확인한다.

마. 위임 서명

M. Mambo는 본인을 대신하여 서명할 수 있는 위임 서명 방식을 최초로 제안하였다. 위임 서명은 위임 서명자(proxy signer)가 원래 서명자(original signer)를 대신하여 대리로 서명이 가능하도록 하는 기법이다. 이때 서명 권한을 위임받은 서명자가 또 다른 위임 서명자에게 서명 권한을 위임할 수 있다. 이러한 방식은 위임 서명의 확장된 형태로 S. Araki가 제안한 다단계 위임 서명이다.[70]

바. 다중 서명

대부분의 전자서명은 문서에 한 사람이 서명하는 단순 서명(single signature) 방식으로 개발되었다. 한편, 탄원서, 성명서 등에 서명할 때 여러 명이 각자 자신의 서명을 한 번씩 하는데 이를 반복해서 적용하면 서명의 길이가 늘어난다. 서명 검증의 경우도 서명자의 수만큼 검증해야 하므로 서명자가 많은 경우 검증 시간이 오래 걸린다. 다중 서명(multi-signature)은 이러한 단순 서명의 문제를 해결하기 위해 동일한 문서에 여러 사람이 서명할 수 있도록 고안한 방식이다.

다중 서명 방식은 정족수 스킴(Threshold Scheme)에 이론적 기반을 두고 있다. $t \leq k$를 만족하는 두 양의 정수 t, k에 대하여, (t,k)-정족수 스킴이란 다음의 조건을 만족하도록 비밀 정보 S의 부분들을 k명에게 나누어 주는 기법이다.[71]

---

70) 남기희·이여진·김성열·정일용, “위임 인증서를 기반으로 한 대리 서명 방식 프로토콜의 설계”, 한국정보과학회 30(1) (2003), 431면.

71) 김명환, 『수리암호개론』, 경문사 (2019), 284면.

(조건)

t명 이상이 모이면 각자가 가진 부분들을 결합하여 S를 복원할 수 있지만, t명 미만이 모이면 S를 복원할 수 없다.

다중 서명은 $M-of-N$의 형태로 N개의 키를 생성하고 M개의 서명이 있어야 거래가 가능하도록 N개의 키를 분배하여 보관한다. M개의 키를 모두 분실·유출하지 않는 이상 보안은 유지되고 M명의 동의가 있어야 관리 권한이 생기므로 관리의 투명성도 보장될 수 있다.[72]

이러한 방식은 여러 개의 개인키 사본을 두어 유출이나 1개의 키만 생성하여 유일한 키가 훼손될 가능성 있는 기존의 방법과 다르게 최대 M개의 키가 유출되거나 훼손되지 않으면 안전한 장점이 있다. 또한, M개의 키 중 1개를 제3의 신뢰기관에 위탁·보관하면 관리상의 보안뿐만 아니라 신뢰성도 보장할 수 있다.[73]

공개키 방식을 이용한 전자서명은 검증키를 공개하고 있어 누구든지 서명의 진위를 검증할 수 있다. 그러나 전자서명의 사용에 제한이 필요한 경우에는 제한하기 곤란하여 사생활 침해의 우려가 있다. 이러한 문제를 해결하기 위해 서명자의 동의가 있어야 검증 가능하거나 서명문을 모르게 서명하도록 하는 다양한 형태의 특수 전자서명을 사용한다.

제3절 공개키 기반 구조의 전자서명 활용

1. 현행법상 공개키 기반 구조의 전자서명

공개키 기반 구조에서 개인키는 전자서명법상 전자서명을 생성하기 위해 사용하는 전자서명생성정보에 해당하며, 전자서명인증은 공개키로 전자서명생성정보가 서명자에게 속하는 사실을 검증하는 행위다. 또한, 인증서는 전자서명생성정보가 서명자에게 속하는 사실을 확인하고

72) 최훈제, 앞의 논문, 11면.
73) 최훈제, 앞의 논문, 35면.

증명하는 전자적 정보로, 공개키가 서명자에게 해당하는 것을 검증하는 수단이다. 공개키 기반 구조의 경우 다른 사람이 공개키를 도용하거나 위조하지 못하도록 하고, 개인키에 해당하는 전자서명생성정보를 부정하게 발급받거나 행사하면 형사처벌 받는다.

공개키 기반 구조는 인증서의 발급·사용·폐지를 통해 인증, 기밀성, 무결성, 부인방지, 접근제어 서비스를 제공한다. 인증서를 통해 사용자에 대한 인증으로 신원 확인이 가능하고, 암호화로 기밀성을 확보하여 송·수신자 외에는 전송 내용을 알 수 없으며, 해시함수를 통해 송신 내용이 변경되지 않았다는 무결성을 보장한다. 전자서명으로 송·수신자 간 송·수신 사실 부인을 방지하며, 인증기관은 키 생성·등록·분배·폐지 등 키 관리를 통해 접근을 제어한다.

한편, 전자서명법 제3조 제1항 “전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.”, 동조 제2항 “법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.”는 전자서명의 효력에 대해 규정하고 있는 법조항이다.

전자문서 및 전자거래 기본법에서는 제4조 제1항 “전자문서는 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니한다.”, 동법 제11조 “전자거래 중에서 전자서명에 관한 사항은 「전자서명법」에서 정하는 바에 따른다.”라고 규정한다. 즉, 전자서명법에 따라 전자서명을 통해 전자문서에 서명, 서명날인 또는 기명날인하더라도 법적 효력을 가진다는 의미로 해석된다.

2. 전자서명 적용 서비스 플랫폼의 암호화

국외 서비스 제공자를 대상으로 제3자 보관 정보 수집 시 공개키 기반 구조의 암호화를 통해 개인키로 서명하고 공개키로 검증한다. 국외 서비스 제공자의 제3자 보관 정보 확보를 위해 수사기관은 국내 법원이 발부한 문서를 첨부하고 전자서명하여 국제공조 전담부서에 전송한다.

수사기관이 국제공조 전담부서에 제3자 보관 정보를 요청하면 국제공조 전담부서에서 국외 서비스 제공자에 직접 요청한다. 이후 국외 서비스 제공자로부터 가입자정보를 수신하면 국제공조 전담부서는 요청 수사기관에 제3자 보관 정보를 제공한다.

이러한 제3자 보관 정보 수집 과정에서 수사기관, 국제공조 전담부서, 국외 서비스 제공자를 연결하는 제3자 보관 정보 서비스 플랫폼을 이용한다. 공개키 기반 구조의 암호화 기술을 활용한 전자서명 적용 서비스 플랫폼을 구현하여 보다 안전하게 제3자 보관 정보를 송수신하는 체계를 마련한다. 위·변조 및 정보유출을 방지하기 위해서는 공개키 기반 구조의 전자서명을 적용하고, 기밀성을 확보하기 위해 전자서명 후 전자봉투로 전송하도록 한다. 전자문서를 송수신할 때 전자서명을 통해 신원을 확인하고 전자봉투로 보내면 송수신 과정에서 해킹 시에도 암호화된 전자문서는 쉽게 노출되지 않을 것이다.

제6장 제3자 보관 정보 서비스 플랫폼 구현

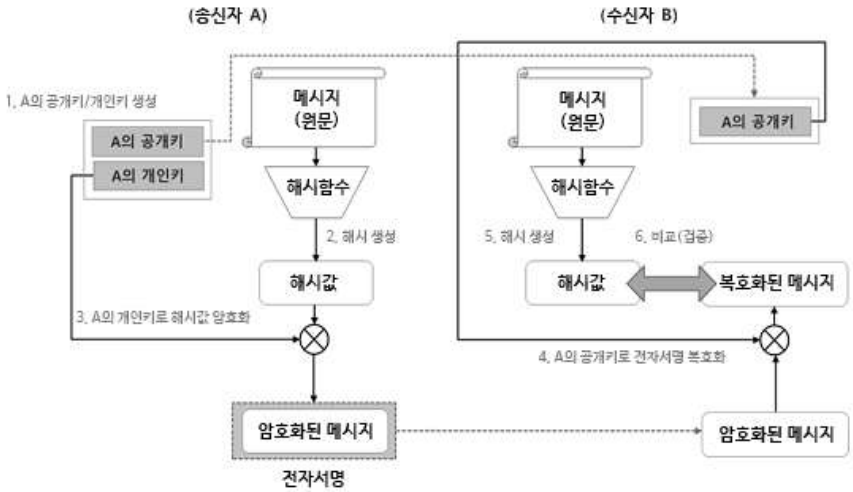
제1절 전자서명의 적용

1. 전자서명의 과정

송신자는 서명 알고리즘을 이용하여 메시지에 서명해 수신자에게 메시지와 서명을 전송한다. 수신자는 메시지와 서명을 받으면 검증 알고리즘을 적용한다. 검증 결과가 일치하면 메시지를 받아들이고, 일치하지 않으면 받아들이지 않는다.

전자서명의 생성을 위해 송신자는 공개키/개인키 한 쌍을 생성한다. 메시지(원문)를 해시함수에 통과시켜 해시값(메시지 다이제스트)으로 변환한다. 이 해시값을 송신자의 개인키로 암호화한다. 즉, 송신자의 개인키로 해시값에 서명하는데, 송신자가 가지고 있는 개인키에 의해 암호화된 메시지가 전자서명이다.

전자서명 검증의 경우 수신자는 송신자의 공개키를 이용하여 송신자의 전자서명을 복호화한다. 이후 전자서명의 생성과 마찬가지로 메시지(원문)를 해시함수에 통과시켜 해시값(메시지 다이제스트)으로 변환한다. 이 해시값이 복호화한 전자서명과 일치하는지 비교하여 검증한다.



[그림 11] 전자서명 과정[74]

2. 전자서명 적용 서비스[75]

가. 전자서명을 통한 정보 요청

[K=Key(키), M=Message(메시지), S=Signature(서명), C=Certificate(인증서), V=Verification(검증)]

(1) 정보요청자는 메시지(전자문서)[M]를 해시함수[H]에 통과시킨 후 정보요청자의 개인키($K_{요}^{개}$)로 서명[S]해서 전자문서와 전자서명(암호화된 메시지)을 정보제공자에게 전송한다. 이때 정보제공자가 전송된 전자서명이 정보요청자의 서명이 맞는지 검증을 할 수 있도록 전송 시

74) AI IMPACTS, "[보안구현기술] 전자서명의 이해(전자서명의 생성 및 검증과정)" <https://blog.naver.com/jvioonpe/221384924295> (2022. 11. 30. 방문).

75) 김승일, "전자서명 기반 전자영장을 활용한 압수·수색영장의 원격 집행 방안에 대한 연구", 석사학위논문, 서울대학교 (2022), 156면.

정보요청자는 전자문서, 전자서명, 정보요청자의 공개키($K_{요}^{공}$)가 포함된 인증서를 함께 전송한다.

$[M(\text{전자문서}) + S_{요}(K_{요}^{개}, H(M)) + C(K_{요}^{공}, S_{인}(K_{인}^{개}, K_{요}^{공}))]$

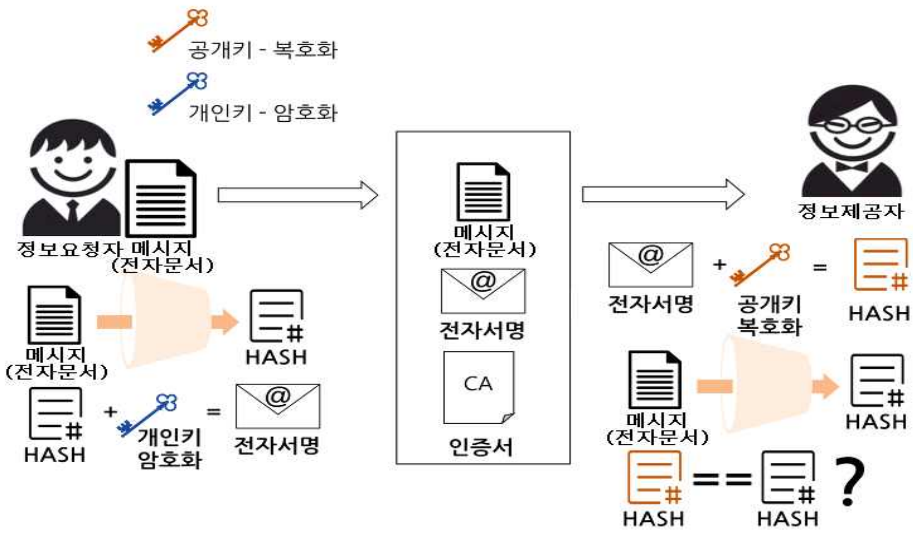
(2) 전자문서를 수신한 정보제공자는 전자서명의 검증을 위해서 인증서의 유효성을 확인한다. 인증기관의 공개키를 이용해 인증기관의 개인키로 암호화된 서명을 풀어서 인증기관의 서명이 검증되면 정보요청자의 공개키라는 것이 확인된다.

$[V_{인}(K_{인}^{공}, S_{인}) \rightarrow K_{요}^{공}]$

(3) 정보제공자는 인증서를 통해 확인된 정보요청자의 공개키를 이용해 정보요청자의 개인키로 암호화된 정보요청자의 서명을 검증한다.

$[V_{요}(K_{요}^{공}, S_{요}) \rightarrow M]$

(4) 따라서 정보제공자는 정보요청자가 메시지(전자문서)[M]를 서명[S]한 것이라는 사실을 신뢰할 수 있다.



[그림 12] 전자서명을 통한 정보 요청[76]

76) IT, I Think, “공인인증서와 블록체인을 이용한 공동인증 [1]” <https://cholol.tistory.com/426> (2022. 11. 30. 방문).

나. 전자서명을 통한 정보 제공

[K=Key(키), M=Message(메시지), S=Signature(서명), C=Certificate(인증서), V=Verification(검증)]

(1) 정보제공자는 메시지(가입자정보)[M]를 해시함수[H]에 통과시킨 후 정보제공자의 개인키($K_{제}^{개}$)로 서명[S]해서 가입자정보와 전자서명(암호화된 메시지)을 정보요청자에게 전송한다. 이때 정보요청자가 전송된 전자서명이 정보제공자의 서명이 맞는지 검증을 할 수 있도록 전송 시 정보제공자는 가입자정보, 전자서명, 정보제공자의 공개키($K_{제}^{공}$)가 포함된 인증서를 함께 전송한다.

$[M(\text{가입자정보}) + S_{제}(K_{제}^{개}, H(M)) + C(K_{제}^{공}, S_{인}(K_{인}^{개}, K_{제}^{공}))]$

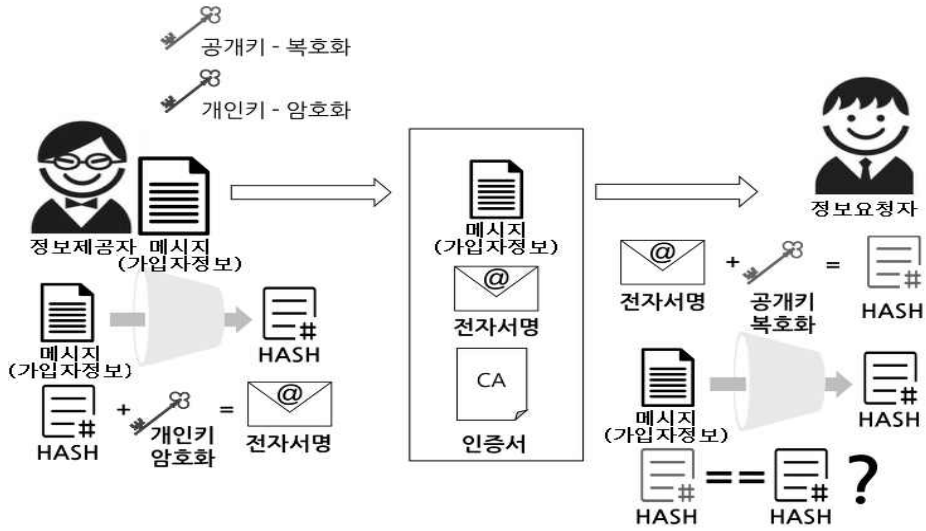
(2) 가입자정보를 수신한 정보요청자는 전자서명의 검증을 위해서 인증서의 유효성을 확인한다. 인증기관의 공개키를 이용해 인증기관의 개인키로 암호화된 서명을 풀어서 인증기관의 서명이 검증되면 정보제공자의 공개키라는 것이 확인된다.

$[V_{인}(K_{인}^{공}, S_{인}) \rightarrow K_{제}^{공}]$

(3) 정보요청자는 인증서를 통해 확인된 정보제공자의 공개키를 이용해 정보제공자의 개인키로 암호화된 정보제공자의 서명을 검증한다.

$[V_{제}(K_{제}^{공}, S_{제}) \rightarrow M]$

(4) 따라서 정보요청자는 정보제공자가 메시지(가입자정보)[M]를 서명[S]한 것이라는 사실을 신뢰할 수 있다.



[그림 13] 전자서명을 통한 정보 제공[77]

3. 전자봉투로 전송

가. 전자봉투의 개념

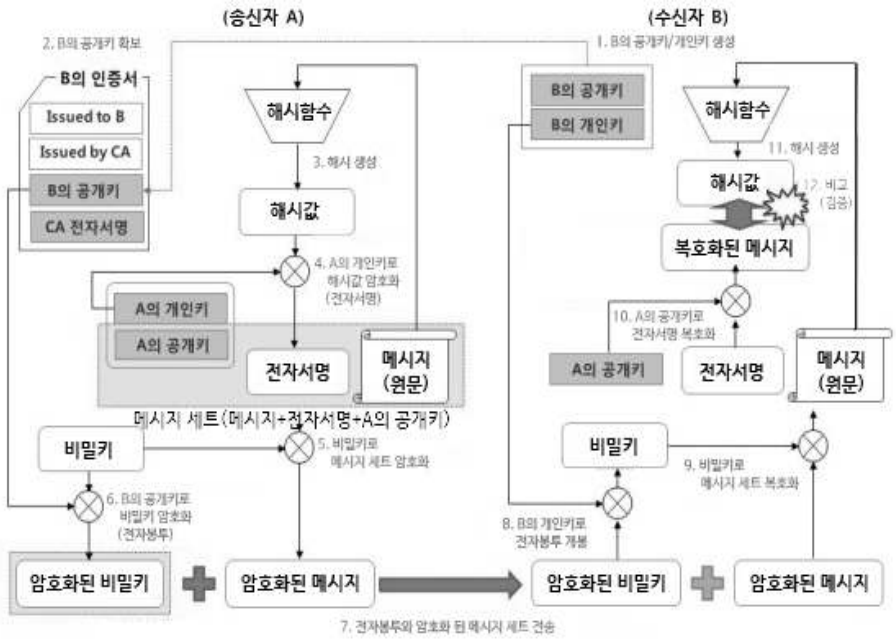
전자봉투(Digital envelope)는 비밀키(대칭키) 암호화와 공개키(비대칭키) 암호화의 하이브리드 암호 방식으로 효과적인 전송 방법이다. 비밀키 암호 방식은 속도가 빠르지만 키를 1개만 사용하므로 키 공유의 문제가 있고, 공개키 암호 방식은 비밀키 암호 방식에 비해 속도는 느리지만 키를 공개적으로 전달하므로 키 공유 문제는 해결된다. 이 두 가지 암호 방식의 장점을 혼합하여 메시지를 비밀키로 암호화한 후 비밀키를 수신자의 공개키로 한번 더 암호화하여 전달하는 방식이 나왔고, 이때 비밀키를 봉투에 담아서 보내 전자봉투라고 한다.

전자봉투의 구성을 위해 우선 수신자는 공개키/개인키 한 쌍을 생성한다. 송신자는 수신자의 공개키를 확보하기 위해 수신자의 인증서를 요청한다. 수신자의 인증서 유효성을 인증하는 인증기관을 신뢰할 수 있는지 검증하기 위해 인증기관의 인증도 요청한다.

77) IT, I Think, 앞의 자료.

인증기관의 서명 검증을 통해 인증서의 유효성을 확인하고 수신자의 공개키를 확보한다.

메시지(원문)를 해시함수에 통과시켜 해시값으로 변환하고, 송신자의 개인키로 해시값에 전자서명한다. 메시지, 전자서명, 송신자의 공개키를 비밀키로 암호화하고, 이 비밀키를 송신자가 확보한 수신자의 공개키를 이용하여 암호화하여 전자봉투에 담아 전송한다. 수신자는 자신의 개인키로 전자봉투를 개봉하여 비밀키를 획득하고, 암호화된 메시지를 비밀키로 복호화한다. 송신자의 공개키로 전자서명을 복호화하여 전자봉투 구성 시와 같은 방식으로 메시지(원문)로부터 해시값을 생성해서 비교 검증한다.



[그림 14] 전자봉투 개념도[78]

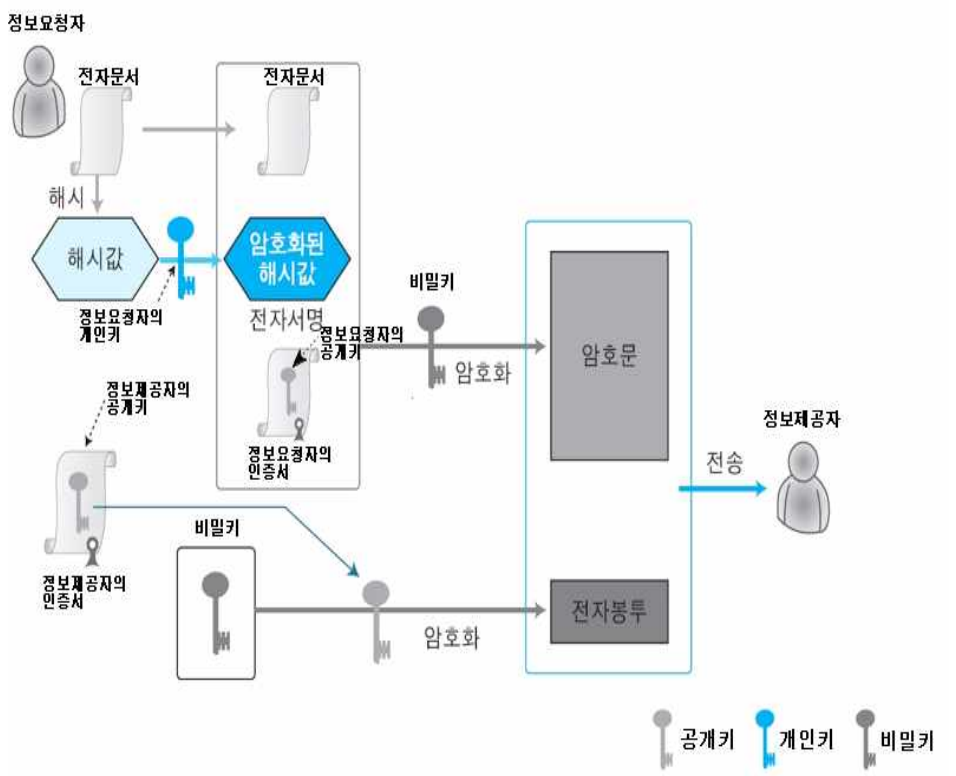
78) AI IMPACTS, “[보안구현기술] 전자봉투(Digital Envelope)의 이해(생성 및 개봉 동작원리)” <https://blog.naver.com/jvioonpe/221388172751> (2022. 11. 30. 방문).

나. 전자봉투를 이용한 전송

전자봉투로 전송 시 전자서명을 통해 전자문서, 가입자정보를 암호화하고 복호화하는 과정이 있다.

(1) 전자문서의 암호화 및 복호화

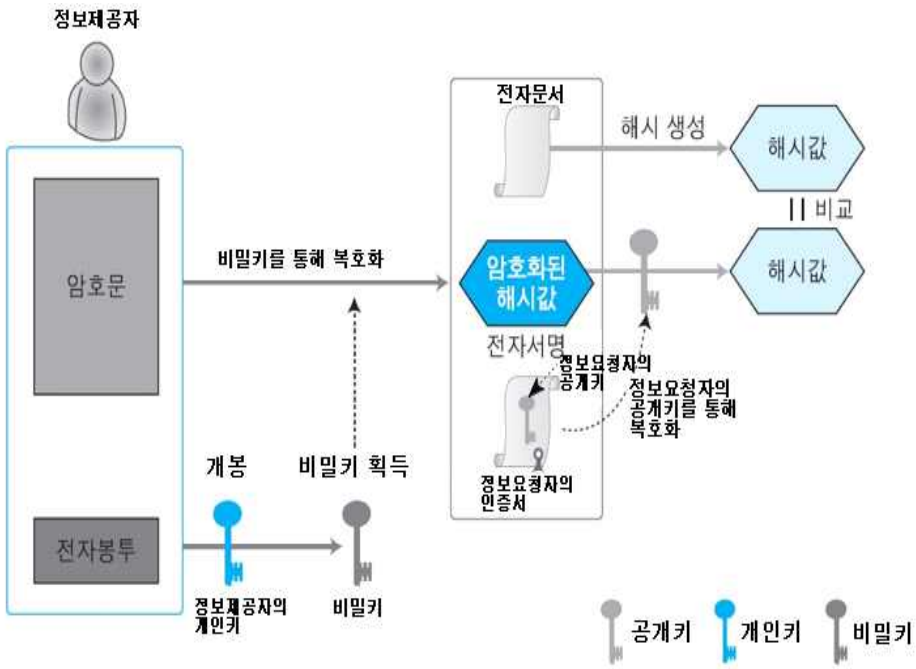
정보요청자는 전자문서를 암호화하여 전송하기 위해 전자서명을 생성한 후 전자문서, 전자서명, 인증서(정보요청자의 공개키 포함)를 비밀키로 암호화하는 절차를 거친다. 전자문서, 전자서명, 인증서 전체를 암호화한 상태의 암호문과 비밀키를 정보제공자의 공개키로 한번 더 암호화하여 전자봉투를 이용해 보낸다.



[그림 15] 전자문서의 암호화[79]

79) 이창기, “정보시스템 보안 강의자료-ch09_암호를 이용한 전자상거래.ppt”, 강원대학교 컴퓨터공학과, 17면 <https://cs.kangwon.ac.kr/~leeck/IS/ch09.pdf> (2022. 11. 30. 방문).

전자봉투를 통해 정보요청자로부터 정보제공자의 공개키로 암호화된 비밀키를 받은 정보제공자는 자신의 개인키로 전자봉투를 개봉하여 비밀키를 획득한다. 획득한 비밀키를 이용해 전자문서, 전자서명, 인증서를 복호화한다. 인증서에서 정보요청자의 공개키를 확보하여 전자서명을 복호화한 후 서명이 검증되면 정보요청자가 보낸 전자문서로 증명되는 것이다.

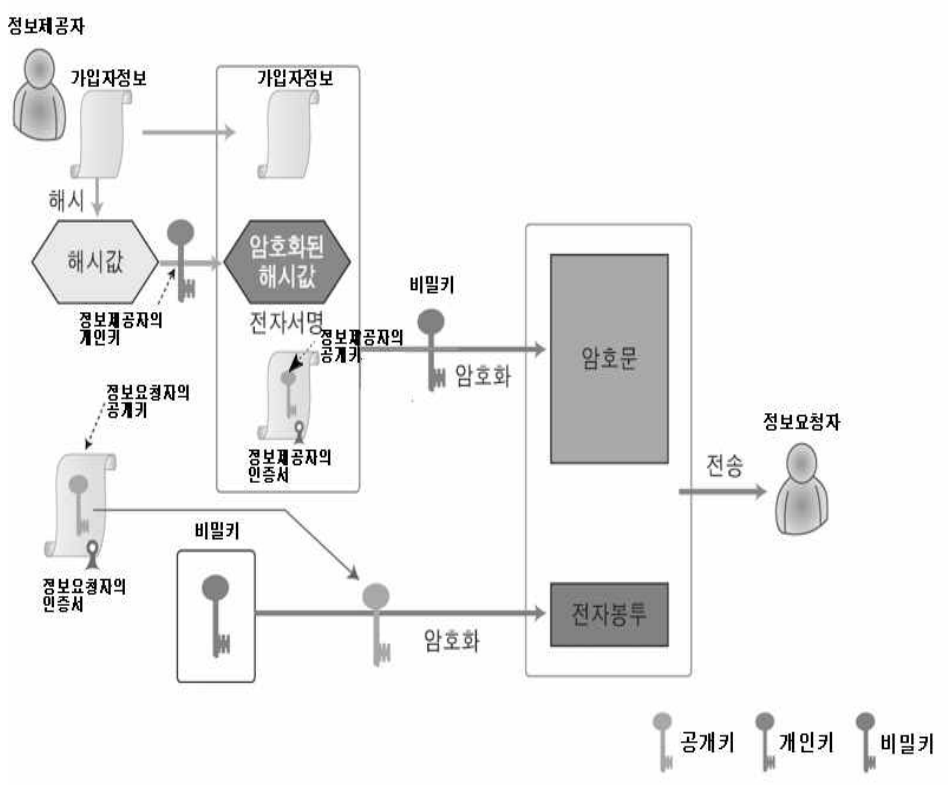


[그림 16] 전자문서의 복호화[80]

(2) 가입자정보의 암호화 및 복호화

정보제공자는 가입자정보를 암호화하여 전송하기 위해 전자서명을 생성한 후 가입자정보, 전자서명, 인증서(정보제공자의 공개키 포함)를 비밀키로 암호화한다. 이 암호화한 가입자정보, 전자서명, 인증서와 정보요청자의 공개키로 한번 더 암호화한 비밀키를 전자봉투를 통해 정보요청자에게 전송한다.

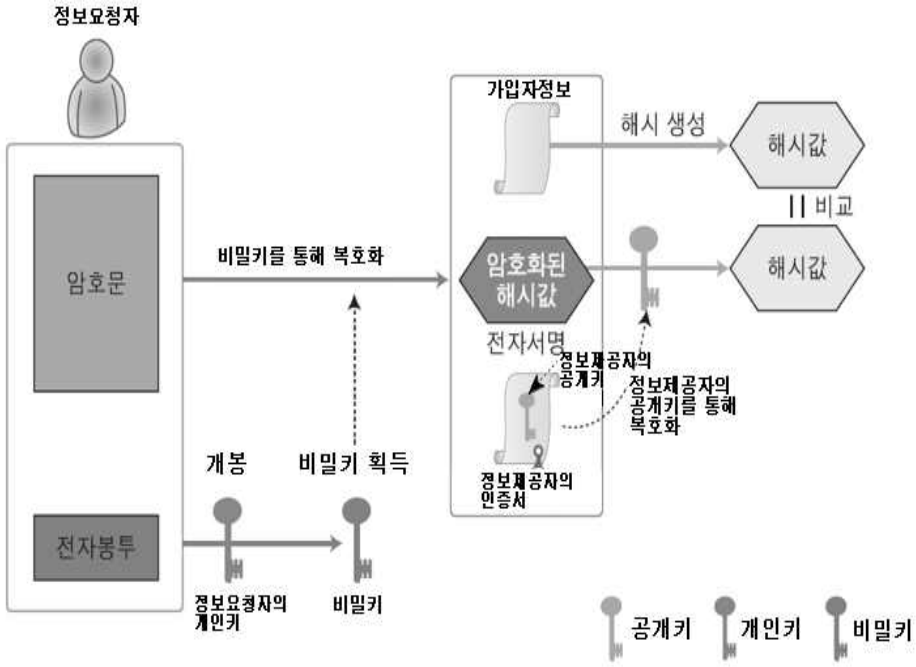
80) 이창기, 앞의 자료, 18면.



[그림 17] 가입자정보의 암호화[81]

정보제공자로부터 전자봉투를 통해 정보요청자의 공개키로 암호화된 비밀키를 전송받은 정보요청자는 자신의 개인키로 전자봉투를 개봉해 비밀키를 획득한다. 그 비밀키를 이용하여 가입자정보, 전자서명, 인증서를 복호화한다. 인증서에서 정보제공자의 공개키를 확보해 전자서명을 복호화한 후 서명이 검증되면 정보제공자가 전송한 가입자정보로 증명된다.

81) 이창기, 앞의 자료, 17면.



[그림 18] 가입자정보의 복호화[82]

가입자정보, 전자서명, 인증서를 비밀키로 암호화하고, 비밀키를 정보요청자의 인증서에서 확보한 공개키로 암호화하여 전자봉투로 보내면 기밀성도 충족해 보안상 안전하다. 가입자정보의 경우 전자서명이 가능한 기술을 활용하여 서명하고, 전자서명된 가입자정보를 암호문의 형태로 전송하면 가입자정보가 노출되지 않을 것이다.

4. 전자서명 서비스의 특징[83]

가. 메시지 인증

전자서명은 메시지 인증을 통해 수신자가 받은 메시지가 송신자로부터 온 것을 확신한다. 제3자 보관 정보 수집 과정에서 전자서명으로 전자문서의 인증이 된다.

---

82) 이창기, 앞의 자료, 18면.
83) Behrouz A. Forouzan, 이재광·신상욱·임종인·전태일 공역, 앞의 책, 420-422면.

나. 메시지 무결성

현재 사용되는 전자서명 시스템은 해시함수를 사용하여 서명 및 검증 알고리즘을 만들어서 메시지의 무결성을 유지한다. 메시지 무결성은 메시지가 변경되면 전자서명(암호화된 해시값)이 달라지므로 전체 메시지에 서명을 할 경우에도 보장된다. 따라서 제3자 보관 정보 수집 과정에서 전자문서가 변경되면 전자서명이 바뀌므로 전자문서의 무결성이 확보되는 것이다.

다. 부인방지

메시지를 보낸 송신자가 해당 메시지를 보낸 사실을 부인할 경우 제3의 신뢰기관은 저장하고 있는 메시지를 제시한다. 이때 수신자의 메시지가 제3의 신뢰기관이 보관하고 있는 메시지의 복사본과 같으면 송신자는 메시지를 보낸 것을 부인할 수 없다. 한편, 수신자가 메시지를 받은 사실을 부인할 경우 수신자의 메시지가 제3의 신뢰기관이 보관하고 있는 메시지의 복사본과 같으면 수신자는 메시지를 받은 것으로 수신을 부인할 수 없다. 제3자 보관 정보 수집 과정에서는 전자서명으로 전자문서의 송수신 부인방지가 가능하다.

라. 기밀성

메시지에 전자서명을 하면 메시지 자체는 원문으로 암호화되지 않고 그대로 전송되므로 기밀성이 보장되는 것은 아니다. 전자서명을 할 경우 기밀성이 필요하면 메시지와 서명에 비밀키, 공개키를 이용하여 암호화를 해야 한다. 전자봉투를 이용하면 기밀성이 확보되어 안전하게 전송할 수 있다. 제3자 보관 정보 수집 과정에서 전자서명 및 전자봉투를 통해 암호화하여 전송하면 메시지 인증, 무결성, 부인방지, 기밀성을 확보하면서 증거 수집이 가능하다.

제2절 제3자 보관 정보 서비스 플랫폼의 도입

1. 기존 형사사법정보시스템의 개선

형사사법절차 전자화 촉진법 및 약식절차 등에서의 전자문서 이용 등에

관한 법률에 의거하여, 형사사법정보를 생성, 저장, 처리하기 위해 2010년 7월부터 형사사법정보시스템을 운영하고 있다. 형사사법정보시스템은 형사사법절차를 전자화하여 형사사법기관이 표준화된 정보처리시스템에서 수사·기소·재판·집행 업무를 하고, 그 결과 생성된 문서 및 정보를 활용하는 전자적 업무 관리 체계다.

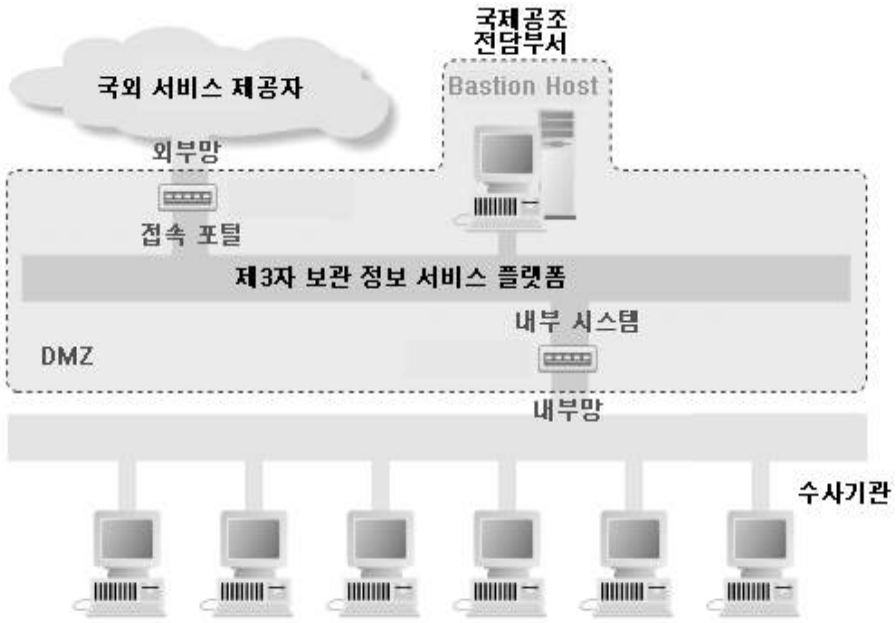
기관별 업무 특성을 고려하여 법원, 법무부, 검찰청, 경찰청 등 형사사법기관은 각각 독립된 시스템을 운영하고 있다. 각 기관에서 생성한 정보의 경우 전자결재, 문서관리 등이 형사사법정보 공통시스템으로 연계되어 공동으로 활용한다. 현재 수사기관은 형사사법정보시스템을 운영하고 있지만 국내 서비스 제공자의 정보 전송에만 제한적으로 사용한다. 국외 서비스 제공자에 직접 요청하는 경우 개별적으로 이메일이나 법집행 요청 포털을 통해 정보 전송이 이루어지고 있다.

국외 서비스 제공자의 정보 전송에 이용하도록 형사사법정보시스템에 공개키 기반 구조의 전자서명 암호화 기술 부분을 추가한 형태의 제3자 보관 정보 서비스 플랫폼을 구축한다. 기존 형사사법정보시스템을 개선하고 국외 서비스 제공자에 대한 증거 수집의 특성을 고려해서 제3자 보관 정보의 전송을 위한 내부 시스템과 접속 포털을 만든다. 수사기관 내부의 업무를 처리하기 위해 사용하는 내부 시스템에 전자문서 완전 전자화를 위한 기능을 추가하고, 접속 포털에 연결하는 방식으로 구현한다.

한편, 수사기관이 국외 서비스 제공자로부터 증거를 수집하는 과정에서 제3자 보관 정보를 안전하게 전송받을 수 있도록 DMZ(Demilitarized Zone)를 설정한다. DMZ는 인터넷과 내부망 또는 인터넷 구간 사이에 위치한 중간 지점으로, 국외 서비스 제공자와 국제공조 전담부서 사이의 보안 구역이다. 인터넷 구간에서 접근이 가능하고 내부망은 접근통제 시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역이다. 국외 서비스 제공자가 내부 시스템에 직접 접속하는 것은 보안상

위험하므로 외부에 보안성이 높은 접속 포털을 만들고, DMZ 내 배스천 호스트를 거쳐 간접적으로 접속하도록 구성한다.[84]

네트워크 보안상 중요한 방화벽 역할을 하는 배스천 호스트(Bastion Host)는 외부와 내부 네트워크 사이에 위치하는 게이트웨이다. 배스천 호스트는 보안 방어를 위해 사용하는데, 외부에서 내부로의 네트워크 공격을 방어하도록 설계한다. 네트워크 구성과 밀집도에 따라 다르지만 배스천 호스트 자체로도 방어가 가능하고, 다른 방어계층과 함께 보안시스템을 구성하여 보안을 강화할 수도 있다. 외부 해커의 공격에 대비해 공격 위험 가능성이 높은 시스템에 설치하여 침입하기 어려운 구조로 만든다.



[그림 19] 제3자 보관 정보 서비스 플랫폼 구조[85]

84) 개인정보보호위원회·한국인터넷진흥원, “개인정보의 안전성 확보조치 기준 해설서”, 제2020-2호 (2020), 63면.

85) Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman, “Building Internet Fire walls” <https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch06_03.htm> (2022. 11. 30. 방문).

2. 제3자 보관 정보 서비스 플랫폼의 절차

수사기관의 필요에 따라 개별적으로 수집하는 제3자 보관 정보 요청 및 제공 방법을 통일시키고, 제3자 보관 정보 서비스 플랫폼을 활용하여 표준화된 절차로 처리하도록 한다. 제3자 보관 정보 수집 과정에서 국외 서비스 제공자와 국제공조 전담부서 간에는 접속 포털, 국제공조 전담부서와 수사기관 사이는 내부 시스템을 통해 서비스를 제공한다. 접속 포털은 내부망과 외부망을 연결하여 제3자 보관 정보의 요청 및 제공, 내부 시스템은 전자문서의 저장·보관 등을 위해서 필요하다.

수사기관이 국제공조 전담부서를 통해 제3자 보관 정보 요청 전자문서를 국외 서비스 제공자에 전송하면, 국외 서비스 제공자로부터 전자적 형태로 제공받을 수 있도록 프로세스를 설계한다. 전자문서 확인 시 해당 수신 내역이 전자적인 형태로 생성되어 내부 시스템에서 제3자 보관 정보 서비스 플랫폼으로 연계 전송된다. 제3자 보관 정보의 요청 및 제공 절차 전반에서 모든 전자문서의 생성·유통·보관되는 과정을 관리하는 것을 목표로 제3자 보관 정보 서비스 플랫폼을 구현한다.

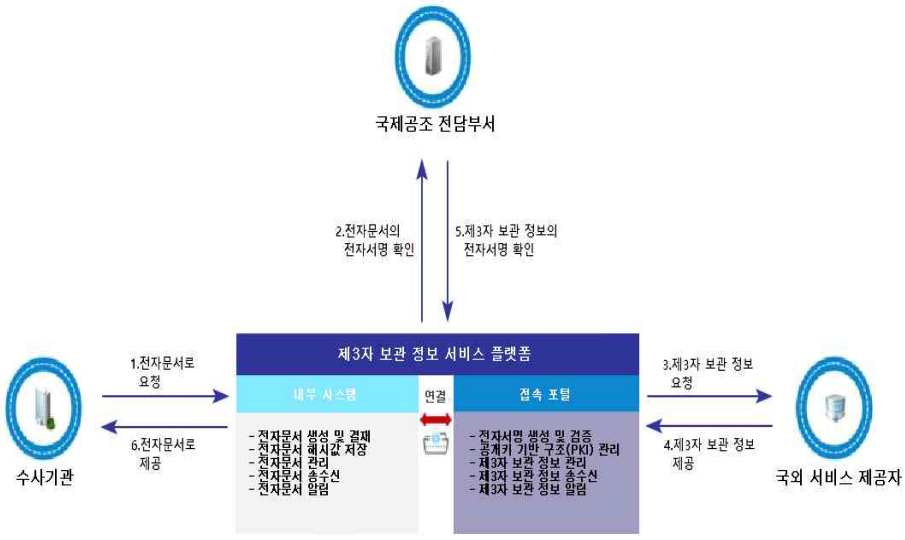
내부 시스템을 이용하여 수사기관이 제3자 보관 정보 요청 전자문서를 전송하면, 국제공조 전담부서는 알림을 통해서 전자문서 접수 사실을 통지받는다. 제3자 보관 정보 서비스 플랫폼에 접속하여 인증절차를 거친 후 전자문서를 열람하고, 해당 국외 서비스 제공자에 제3자 보관 정보를 요청한다. 국외 서비스 제공자는 요청 대상이 되는 제3자 보관 정보를 선별한 후 기술적 조치를 거쳐 국제공조 전담부서를 통해 수사기관에 가입자정보를 회신한다.

제3자 보관 정보 제공 시에도 수사기관이 가입자정보를 수신하면, 제3자 보관 정보 서비스 플랫폼을 통해서 자동적으로 국제공조 전담부서에 통지되도록 알림 기능을 설정한다. 접속 포털에 연결되어 있는 내부 시스템을 통해 수사기관은 요청한 제3자 보관 정보의 수신을 확인하고 다운로드할 수 있다. 이러한 절차를 거쳐 수사기관의 국외 서비스 제공자에 대한 제3자 보관 정보 요청과 해당 제3자 보관 정보의

제공이 전자적으로 완성된다.

제3자 보관 정보 서비스 플랫폼에 따른 시스템 관리자 및 장소를 정한다. 가장 현실적인 방법은 국제공조 전담부서를 별도로 만들고 국외 서비스 제공자에 직접 제3자 보관 정보를 요청하는 담당자를 모집해 운영하는 것이다. 국제공조 전담부서에서 업무 특성을 고려하여 제3자 보관 정보 서비스 플랫폼을 통합적으로 관리하고 유지·보수를 통해 개선해 나간다.

시스템의 경우 한 곳에 두면 효율적인 관리가 가능하지만 보안에 취약하고, 여러 곳에 분산해 운영하면 보안상 안전하지만 상대적으로 관리하기가 힘들다. 이 두 가지를 절충하여 접촉창구로 국제공조 전담부서를 구성하고, 해당 부서의 소재지에 통합시스템을 구축하는 방식이 있다.[86] 표준화된 절차에 의한 수사기관의 시스템 활용도 및 예산을 고려하고, 국제공조 전담부서의 의견을 종합해서 결정한다.



[그림 20] 제3자 보관 정보 서비스 플랫폼 절차

86) 김승일, 앞의 논문, 108면.

3. 제3자 보관 정보 서비스 플랫폼의 구성

가. 접속 포털

제3자 보관 정보 수집을 위해 국제공조 전담부서와 국외 서비스 제공자를 연계하여 서비스를 제공하는 접속 포털을 구성한다. 접속 포털은 국제공조 전담부서가 수사기관 내부 업무망과 국외 서비스 제공자와 통신할 외부 인터넷망 사이에서 정보의 이동을 위해 필요하다. 즉, 국제공조 전담부서가 국외 서비스 제공자에 제3자 보관 정보를 요청하고 제공받기 위해서 접속하는 허브 역할이다.

접속 포털을 통한 정보 수집 시 송신자는 전자문서를 해시하여 해시값을 형성한다. 이 해시값을 송신자의 개인키로 암호화하여 전자서명을 생성한 후 전자문서에 서명을 첨부해서 인증서와 함께 전송한다. 수신자는 인증서에 포함된 송신자의 공개키로 전자서명을 복호화하여 송신자가 전자문서에 서명한 사실을 검증하는 구조다. 이 과정에서 전자문서, 전자서명, 인증서를 비밀키로 암호화하고, 비밀키를 수신자의 공개키로 암호화한 후 전자봉투로 전송하는 시스템을 구현한다.

접속 포털 이용 시 제3자 보관 정보 수집 기반 기술로 전자서명 암호화를 통해 전자문서가 노출되지 않도록 한다. 접속 포털을 통한 제3자 보관 정보 수집 과정에서 전자서명이 사용된 전자문서의 보안을 강화하기 위해 최신 기술을 활용한다. 기술적 조치로는 제3의 신뢰기관[87] 증명을 통한 타임스탬프, 블록체인, NFT(Non-Fungible Token) 등이 있다.[88]

접속 포털은 웹페이지 형태로 설계하여 향후 기술의 발전에도 지속적으로 이용할 수 있어야 한다. 접속 포털에서 관리하는 제3자 보관 정보는 법제도의 변경 내용을 반영하여 보관 및 삭제하며, 증거의 특성을 고려하여 적절한 절차에 따라 처리한다. 이 과정에서 제3자 보관

87) 전자문서의 진본 및 시점 확인을 위해 타임스탬프를 발급하는 행정안전부 전자문서 진본 확인센터.

88) 김승일, 앞의 논문, 172면.

정보 요청 및 제공, 제3자 보관 정보 내역·진행 절차·송수신 여부 조회 등이 적시에 정확하게 이루어지도록 한다.

나. 내부 시스템

수사기관은 내부 시스템에 접속해서 제3자 보관 정보 수집과 관련된 문서를 전자적으로 생성하여 국제공조 전담부서에 요청한다. 국제공조 전담부서의 경우 실제 수사기관에서 요청을 보냈다는 것을 확인한 후 제3자 보관 정보 서비스 플랫폼을 통해 대상 국외 서비스 제공자에 요청한다.

동일한 방식으로 국제공조 전담부서가 국외 서비스 제공자로부터 수신한 제3자 보관 정보를 수사기관에 내부 시스템을 통해 제공하면, 해당 수사기관은 국제공조 전담부서에서 보냈다는 것을 확인한다. 수사기관의 수신 확인이 완료되면 제3자 보관 정보 서비스 플랫폼에 수신 내역이 연계 전송되고, 국외 서비스 제공자에 대한 제3자 보관 정보 수집 절차가 마무리되는 구조다.

내부 시스템의 경우 수사기관 간 연계를 고려해 종이문서 방식에서 벗어나 전자문서를 이용하여 수집하는 절차에 맞게 설계한다. 국제공조 전담부서는 제3자 보관 정보 수집 시 전자문서 파일 포맷으로 요청하여 수집한다. 내부 시스템을 통해 전자문서로 받거나 수신 시점에 전자화하여 궁극적으로 완전한 전자화를 달성한다.

내부 시스템은 필요에 따라 전자문서에 관련 정보를 첨부파일로 추가할 수 있고, 첨부파일은 전자문서 내에서 확인할 수 있도록 구성한다. 기존 제3자 보관 정보 수집에서 사용하고 있는 업무 체계를 활용해 표준화된 절차 및 통일된 기준을 수립하여 전자문서를 처리한다. 또한, 전자서명이 가능한 전자기기를 활용하여 서명된 전자문서를 최종 저장하여 보관한다.

다. 전자서명

국외 서비스 제공자의 제3자 보관 정보 수집 시 전자서명에 사용되는 공개키/개인키는 구글 인증서 등 글로벌 IT 서비스 기업이 가지고 있는

RSA 암호 방식의 공개키 기반 구조 시스템을 활용한다. 공개키 기반 구조의 인증서를 통해 국외 서비스 제공자가 공개키를 전달하고, 국제공조 전담부서는 인증서의 공개키로 서명을 검증하는 구조로 이루어진다.

한편, 적법한 범죄 수사를 위해 수사기관에서 제3자 보관 정보를 요청한다는 인증과 보낸 전자문서가 위·변조되지 않았다는 무결성을 증명하려면 전자서명의 검증이 필요하다. 이를 위해 국제공조 전담부서로 전자문서 전송 시 전자서명의 해시값을 생성해서 수신한 전자문서가 수사기관에서 요청한 것인지 확인한다. 수사기관에서 생성한 해시값과 국제공조 전담부서가 전자문서를 수신한 후 검증한 해시값을 비교하여 같으면 해당 전자문서를 국외 서비스 제공자에 전송하여 제3자 보관 정보를 요청한다.

국외 서비스 제공자는 제3자 보관 정보를 요청받은 후 선별하여 가입자정보에 대해 전자서명한 다음 국제공조 전담부서로 안전하게 전송한다. 가입자정보 전송 시에도 전자서명의 해시값을 생성하여 국외 서비스 제공자가 보낸 것인지, 제3자 보관 정보 수집 과정에서 손상이나 훼손이 없는지 국제공조 전담부서에서 확인한다. 국외 서비스 제공자가 생성한 해시값과 국제공조 전담부서에서 검증한 해시값이 일치하면 수사기관에 해당 제3자 보관 정보를 전달한다.

제3자 보관 정보 서비스 플랫폼의 전자서명 암호화는 해시값을 비교하는 검증으로 전자문서에 위·변조가 없었다는 것을 확신할 수 있다. 전송 시 전자봉투를 이용하면 보안성을 확보하여 기밀성도 충족한다. 전자서명 적용 서비스 플랫폼을 거쳐 전자서명한 전자문서를 전송하는 방법은 정보 유출로 인한 정보 주체에 대한 권리 침해의 가능성을 낮출 수 있어서 유용하다.

라. 전자문서변환 애플리케이션

제3자 보관 정보 서비스 플랫폼의 전자문서 관리에서 국외 서비스 제공자가 제공한 비정형 데이터의 경우 기술적 조치를 거쳐 시스템에서

관리 가능한 형태로 변환하여 등록한다. 제3자 보관 정보가 비정형 데이터인 경우에는 전자문서변환 애플리케이션을 이용하여 전자문서를 생성한다. 일부가 비정형 데이터인 경우에도 전자화 과정을 거쳐 전체 데이터를 전자문서의 형태로 만들어 보관할 수 있도록 처리한다.

전자화의 경우 전자문서변환 애플리케이션을 설계하여 전자문서의 생성·보관·전송 등을 관리하고, 각 기관의 협조를 통해 전자문서 규격에 맞는 형식으로 수집한다. 부득이한 사정으로 협조가 어려운 상황에는 자체적으로 애플리케이션을 통해 전자화하도록 한다. 전자화 과정은 사용자의 접근통제, 전자문서변환 애플리케이션의 관리, 전자화 문서의 작성 및 보안, 색인정보의 생성 및 수정 기능을 갖춘 애플리케이션을 활용하도록 한다.

마. 전자문서뷰어 프로그램

전자문서를 보기 위해 필요한 전자문서뷰어 프로그램은 수사기관에서 공통적으로 사용하도록 구축한다. 각종 전자문서를 편리하게 볼 수 있도록 문서 인식률이 높아야 한다. 기본적으로 전자문서 원본은 유지하면서 기관 내부적으로 변경 내용을 공유할 수 있다. 전자문서뷰어에서 변경된 내용은 별도의 저장 공간에 보존하여 확인이 가능하다.

전자문서뷰어 프로그램은 내부 시스템과 접속 포털을 연결하여 E-Book 형태의 화면 넘기기, 책갈피, 북마크, 최근문서 기록, 상세정보 조회가 가능하도록 한다. 추가로 검색결과 보기, 결과 내 재검색, 검색결과 더보기, 검색결과 저장 등의 기능도 구현하면 업무의 효율성 향상으로 경제적 실익도 발생할 것이다.

4. 제3자 보관 정보 서비스 플랫폼의 설계

가. 전자문서의 생성 및 결재

제3자 보관 정보 수집 관련 문서는 PDF/A-1[89] 파일 포맷으로

89) 강일용, “[칼럼] PDF라고 다 같은 PDF가 아니다, 보관용은 따로 있다” <https://it.donga.com/25481/> (2022. 11. 30. 방문).

생성하고, 해당 포맷을 표준 문서 형식으로 설정한다. PDF/A는 국제표준화기구(ISO)에서 정의한 PDF 포맷 버전으로, PDF/A-1는 공공기관에서 발생하는 문서의 장기보존을 위한 전자문서 파일 규격이다. PDF/A-1 문서는 문서 생성 당시 애플리케이션 없이도 해당 문서의 내용을 그대로 재현해 볼 수 있다. 전자정부에 따른 호환성을 고려해보면 공공기관의 전자기록물을 영구적으로 보존하기 위해서는 문서보존 표준 포맷인 PDF/A-1이 효과적이다.

제3자 보관 정보의 요청에 따라 내부 시스템에서 생성한 전자문서는 전자서명을 포함한 기술적 조치를 한 표준 문서 형식으로 송수신한다. 내부 시스템을 이용하여 작성한 전자문서는 정해진 결재선을 거쳐 상신하도록 한다. 전자결재 단계에서 결재자가 수정할 수 있으며 원문에 수정한 내용을 표시한다. 수정 사유 및 이력 등을 기록해 작성자는 수정 전후 내용을 비교하며 확인할 수 있다. 설계 시 결재 과정에서 문서 수정 등 세부적인 기능은 수사의 특성을 반영해서 구체화하여 추가하도록 한다.

나. 전자문서의 관리

제3자 보관 정보 서비스 플랫폼에서 전자문서의 경우 접속포털에서 관리하고 전자문서뷰어 프로그램을 통해 조회 가능하도록 한다. 제3자 보관 정보 수집 과정에서 전자문서는 전자결재 방식을 이용하여 전자적으로 완결한다. 시스템 점검, 셧다운 등의 문제로 인해 시스템 이용이 불가능한 경우 전자문서의 다운로드 사유 입력 후 승인을 받아 이전의 방법대로 처리 가능하도록 허용한다. 기존 방식으로 처리를 해야 하는 불가피한 상황에서는 적법 절차를 지키면서 제3자 보관 정보를 관리할 수 있는 장치를 마련한다.

전자결재 프로세스를 통해 전자문서의 검토 및 결재 관리를 할 수 있고, 내부결재를 완료하면 국외 서비스 제공자로 전송 가능하도록 설계한다. 수사기관에서 요청, 제공하는 전자화된 전자문서는 제3자 보관 정보 서비스 플랫폼을 통해 효율적으로 관리하도록 한다. 제3자 보관

정보 서비스 플랫폼에서 관리되는 전자문서 및 제3자 보관 정보의 보관 및 삭제는 향후 변경되는 법제도적 내용을 반영한다. 구체적인 규정이 없는 경우에는 수사의 특성에 맞는 절차를 통해 처리하도록 한다. 이는 분석 및 설계 과정에서 구성원들과 논의하고 법제도를 적용해서 실질적으로 정비하여 구현한다.

다. 전자문서의 전송

수사기관은 내부 시스템을 통해 국제공조 전담부서로 전자문서를 전송한다. 알림을 통해서 국제공조 전담부서는 전자문서의 수신을 알 수 있다. 제3자 보관 정보 서비스 플랫폼에서 해당 전자문서의 열람이 가능하며, 열람하는 순간 전자문서 전송이 확인된 것이다. 국제공조 전담부서는 수신 확인 후 국외 서비스 제공자에 전자문서를 발송한다. 알림을 설정하여 전자문서의 발송이 완료되면 전자문서의 요청 완료 상태를 나타내도록 한다.

국제공조 전담부서의 경우 국외 서비스 제공자로부터 제3자 보관 정보를 전송받으면 요청한 가입자정보인지 확인한다. 가입자정보는 제3자 보관 정보 서비스 플랫폼을 통해 열람할 수 있다. 국제공조 전담부서는 접속 포털과 연결되어 있는 내부 시스템을 통해서 요청 수사기관에 가입자정보를 전송한다. 가입자정보의 전송이 완료되면 알림을 통해 제3자 보관 정보의 제공 완료 상태를 표시한다. 제3자 보관 정보 서비스 플랫폼을 통해서 국외 서비스 제공자에 직접 제3자 보관 정보 수집이 가능하도록 프로세스를 설계한다.

제3절 제3자 보관 정보 서비스 플랫폼의 효과

1. 전자서명 적용 서비스 플랫폼의 보안성

전자서명을 적용하여 전송할 경우 인증은 송신자의 공개키로 복호화함으로써 확인된다. 부인방지는 공개키 암호 방식의 경우 송신자의 개인키로 메시지의 해시값을 암호화(서명 생성)한 후 수신자에게 전송하고, 수신자는 송신자의 공개키로 복호화(서명

검증)함으로써 확보된다. 비밀키 암호 방식에서는 신뢰할 수 있는 인증기관(제3의 신뢰기관)을 통해 해결된다. 또한, 해시값 비교로 무결성이 확인되며, 전자봉투를 통한 암호화로 기밀성이 보장된다.

전자서명에는 위조 불가, 서명자 인증, 부인방지, 변경 불가, 재사용 불가 기능이 있다. 이 중 서명 재사용의 경우 전자서명이 메시지를 기반으로 하므로 불가능하다. 서로 다른 메시지 M과 M'에 대한 전자서명(암호화된 해시값)을 각각 $Sig(M)$, $Sig(M')$라고 하면, 암호화된 해시값이 서로 다르므로 $[Sig(M) \neq Sig(M')]$ 메시지 M에 대한 서명을 메시지 M'의 서명으로 사용할 수 없다.

한편, 제3자 보관 정보 서비스 플랫폼의 예상되는 취약점으로 시스템상 유효한 메시지를 골라 복사한 후 재전송함으로써 정당한 사용자로 가장하는 재전송 공격(Replay attack)[90]이 있다. 이를 방어하기 위해 시간·순서에 따른 유효성을 알 수 있도록 타임스탬프, 시퀀스넘버, 시도-응답 (Challenge-Response) 인증, 난스(Nonce) 등을 전자서명 시 활용하면 효과적일 것이다.

2. 제3자 보관 정보 서비스 플랫폼의 기대 효과

글로벌 IT 서비스 기업은 제3자 보관 정보 제공에 관한 정책과 절차를 임의로 변경해서 증거 수집에 어려움이 있다. 기업별로 개인정보 처리지침이 상이하고, 국외 서비스 제공자의 자발적인 협조에 중요한 증거의 확보를 의존해야만 한다. 제3자 보관 정보 서비스 플랫폼을 통해 국제공조 전담부서에서 통합하여 처리하면, 수사기관에서 개별적으로 절차를 진행하는 것에 비해서 증거 수집 시간 단축이 가능하다.

전자문서를 암호화한 전자서명, 전자봉투를 적용한 제3자 보관 정보 서비스 플랫폼은 적시에 정확한 수사를 위해 중요한 법제도적 인프라가 될 것이다. 접속 포털을 중심으로 보안 통제된 환경에서 내부 시스템을 통해 업무를 처리하는 절차의 마련으로 엄격하게 관리하도록 한다. 이를

90) 한국정보통신기술협회, IT용어사전 <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=054296-2> (2022. 11. 30. 방문).

위해 공개키 기반 구조의 전자서명과 전자서명 적용 서비스 플랫폼이 동반되어야 한다.

제3자 보관 정보 서비스 플랫폼의 경우 전자서명의 전제조건이 되는 공개키 기반 구조의 암호화를 키 관리에 활용하도록 한다. 공개키 기반 구조를 이용하면 제3자 보관 정보 수집 과정에서 사용되는 인증서를 통해 비대면상에서 상대방을 신뢰하면서 키를 안전하게 전달할 수 있다. 공개키 기반 구조의 전자서명 적용 서비스를 통해 전자서명, 전자봉투, 인증서로 신뢰성을 유지하면서 전자증거를 수집할 수 있다.

전자서명으로 법적 효력을 가진 전자문서가 제3자 보관 정보 서비스 플랫폼을 통해 전송되므로 효과적인 증거 수집이 가능하다. 법제도의 정비를 통해 제3자 보관 정보의 수집 절차 마련으로 신속하게 수집할 수 있다. 또한, 암호화 기술로 전자서명을 하면 국외 서비스 제공자의 제3자 보관 정보를 안전하게 수집할 수 있다. 전자서명 적용 서비스 플랫폼을 이용한 제3자 보관 정보 수집을 통해 개인정보를 보호하면서 효율적으로 수사를 진행할 수 있다.

제7장 결론

현대사회의 사이버범죄는 첨단화·국제화·가상화되어 국경을 뛰어넘어서 공간을 초월하는 양상을 띠고 있다. 그동안 빠르게 증가하는 사이버범죄의 형태에 비해 수사기관은 새로운 환경으로의 전환 및 적응이 늦어 범죄에 대응하는 속도가 떨어지게 되었다. 나날이 진화하는 사이버범죄에 신속하게 대응하기 위해 인터넷, 네트워크, 시스템 등 첨단기술의 유기적인 연결이 요구된다.

한편, 사이버범죄의 수사 패러다임 전환에 따라 국제공조는 필수 불가결하다. 지금까지 다양한 유형의 사이버범죄, 국제공조, 국외 서비스 제공자 협조, 공개키 기반 구조의 전자서명, 제3자 보관 정보 서비스

플랫폼 순으로 제3자 보관 정보에 대한 증거 수집 방법을 알아보았다. 사이버공간에서의 범죄 특성을 고려할 때 원활한 국제공조를 위해서는 법제도의 정비, 시스템의 개발, 수사기관 간 협업, 업무 담당자의 인식 변화가 필요하다.

본고에서는 '제3자 보관 정보 서비스 플랫폼'을 통한 증거 수집 방안에 대해 연구하였다. 현행 국외 서비스 제공자에 제3자 보관 정보 협조 요청 시 문제점을 토대로 미비점을 보완하고 대안을 모색하였다. 기존의 절차 및 시스템을 살펴보고 국외 서비스 제공자에 직접 협조 요청으로 제3자 보관 정보에 대한 증거를 수집하는 문제의 해결방안에 대해 고찰해보았다.

국제공조를 통한 제3자 보관 정보 수집 방법 중 국외 서비스 제공자에 직접 요청하는 경우 절차의 부재로 업무의 비효율성, 기술적 요소의 미비로 인한 수사와 개인정보 유출 문제가 있다. 실제로 수사가 지체되거나 유출된 정보를 이용하여 2차 피해가 발생한 사건이 상당수 존재한다. 이러한 문제점으로 인한 피해를 줄이고 수사의 효율성을 높일 수 있는 해결책을 법제도적, 기술적 방안을 중심으로 제시하였다.

법제도적으로는 절차의 마련, 기술적으로는 시스템의 구축을 통해 해결하도록 한다. 구체적으로 법적 효력이 있는 전자서명을 활용하여 제3자 보관 정보 서비스 플랫폼 절차를 수립한다. 플랫폼은 '공개키 기반 구조의 전자서명 암호화' 기술을 적용하여 수사기관과 국제공조 전담부서 사이는 '내부 시스템', 국제공조 전담부서와 국외 서비스 제공자 간에는 '접속 포털'로 연결하도록 구성한다.

제3자 보관 정보의 수집 절차를 통해 수사기관, 국제공조 전담부서, 국외 서비스 제공자의 체계적인 협조로 수사의 신속성, 밀행성을 확보할 수 있다. 전자서명 적용 서비스 플랫폼의 시스템을 통한 전자서명 암호화로 보안상 안전성을 보장하고 정보 유출의 가능성을 최소화할 수 있다. 이를 통해 신속한 수사와 인권 보호 사이에서 균형을 찾아 중요한 역할을 할 것이다.

앞서 논의한 법제도, 기술적 구현으로 제3자 보관 정보 서비스 플랫폼을 이용하면 증거 수집 과정의 유기적인 연결을 통해 적시에 효과적으로 증거를 확보할 수 있다. 국제공조 방법 중 국외 서비스 제공자에 직접 협조 요청이 증가하고 있는 상황에서 실체적 진실의 규명을 위한 형사사법 절차에서의 효율성 향상이 있을 것이다. 사회 전반에 걸친 법제도 및 기술적 부분의 사회적 비용 감소로 경제적 효과로 이어지는 것을 고려하면 시너지 효과가 상당할 것으로 기대한다.

참고문헌

1. 단행본

김명환, 『수리암호개론』, 경문사 (2019).

법무부, 『2021년 법무연감』 (2022).

조현준, 『2022 알기사 정보보안기사(산업기사) 필기』, 도서출판 탑스팟 (2022).

Behrouz A. Forouzan, 이재광·신상욱·임종인·전태일 공역, 『암호학과 네트워크 보안』, 한티에듀 (2021).

Jan Kleijssen and Pierluigi Perri, 『Cybercrime, Evidence and Territoriality: Issues and Options』, Netherlands Yearbook of International Law 2016. The Hague: T.M.C. Asser (2017).

2. 논문

김나정, “미국 「CLOUD Act」의 주요 내용과 시사점”, 국회입법조사처, 외국입법 동향과 분석 제55호 (2020).

김승일, “전자서명 기반 전자영장을 활용한 압수·수색영장의 원격 집행 방안에 대한 연구”, 석사학위논문, 서울대학교 (2022).

김윤섭·박상용, “형사증거법상 디지털 증거의 증거능력”, 형사정책연구 26(2), (2015).

김종빈, “전자정보를 대상으로 한 압수수색검증영장의 효율적인 집행방법에 대한 연구”, 석사학위논문, 서울대학교 (2020).

김지만, “일본의 온라인 서비스 프로바이더의 책임”, 콘텐츠재산연구 3, (2012).

남기희·이여진·김성열·정일용, “위임 인증서를 기반으로 한 대리 서명 방식 프로토콜의 설계”, 한국정보과학회 30(1) (2003).

남성우, “공개키 암호를 이용한 전자정보 보전처분에 관한 연구”, 석사학위논문, 서울대학교 (2021).
박다온, “외국의 정보통신 서비스 제공자에 대한 통신 자료 요청 방법과 형사법적 문제”, 형사정책연구 통권 제125호 (2021).
박재성, “사이버범죄 국제조약의 동향”, 저스티스 통권 제185호 (2021).
송영진, “미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점”, 형사정책연구 통권 제114호 (2018).
오세연·송혜진, “초국가적 범죄의 대응강화를 위한 인터폴의 효율적 활용방안에 관한 연구”, 한국재난정보학회논문집 10(4) (2014).
유민종, “사이버범죄협약과 국내 법제의 양립 가능성 연구”, 석사학위논문, 서울대학교 (2019).
이은빈, “제3자 보관 개인정보에 대한 증거수집과정에서의 동형암호 활용방안”, 석사학위논문, 서울대학교 (2022).
전완근, “디도스 공격증거와 법적 책임”, 대검찰청, 형사법의 신동향 제32호 (2011).
정대용·김성훈·김기범·이상진, “국제협력을 통한 디지털 증거의 수집과 증거능력”, 형사정책연구 28(1) (2017).
정명현, “유엔 사이버범죄 대응 국제조약의 논의동향과 전망”, 외교부, 국제법 동향과 실무 통권 제62호 (2021).
최훈제, “가상화폐 압수수색 표준절차 및 정족수다중서명을 이용한 압수물관리방안 제안”, 석사학위논문, 서울대학교 (2019).
Michael Plachta, “European Commission Recommends Negotiating a Treaty with U.S. on Access to Electronic Evidence”, 35 No. 3 Int'l Enforcement L. Rep. 78 (2019).
Jennifer Daskal, “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0”, Stanford Law Review Online, Vol. 71 (2018).

3. 웹문서

강일용, “[칼럼] PDF라고 다 같은 PDF가 아니다, 보관용은 따로 있다” <https://it.donga.com/25481/> (2022. 11. 30. 방문).

“공개키 기반 구조” <https://itwiki.kr> (2022. 11. 30. 방문).

구글 웹사이트 <https://transparencyreport.google.com/user-data/overview?user_requests_rep%20ort_period=series:requests,accounts;authority:KR;time:&lu=legal_process_breakdown&user_requests_report_period> (2022. 11. 30. 방문).

김호원, “인증서 및 OpenID Connect OAuth2 기술”, 부산대학교 정보보호 및 사물지능 연구실 <http://infosec.pusan.ac.kr/wp-content/uploads/2019/09/3.-%EC%9D%B8%EC%A6%9D%EC%84%9C-%EB%B0%8F-OpenID-Connect-OAuth2%EA%B8%B0%EC%88%A0.pdf> (2022. 11. 30. 방문).

마이크로소프트 웹사이트 <https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report> (2022. 11. 30. 방문).

마이크로소프트 학습 웹사이트 “공개 키 암호화 이해” <https://technet.microsoft.com/ko-kr/library/aa998077(v=exchg.65).aspx> (2022. 11. 30. 방문).

박종혁, “2019-2nd 정보보호론-제10장 디지털서명”, SeoulTech UCS Lab <http://www.parkjonghyuk.net/lecture/2019-2nd-lecture/informationsecurity/chap10.pdf> (2022. 11. 30. 방문).

_____, “2022-1st 정보보호론-제11장 인증서”, SeoulTech UCS Lab <http://www.parkjonghyuk.net/lecture/2022-1st-lecture/information-protect/chap11.pdf> (2022. 11. 30. 방문).

사이버범죄 신고시스템 웹사이트 “사이버 범죄 분류” <https://ecrm.police.go.kr/minwon/crs/quick/cyber1> (2022. 11. 30. 방문).

유럽평의회 웹사이트 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> (2022. 11. 30. 방문).

이근우, “클라우드컴퓨팅법과 CLOUD Act는 다르다” <https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=163869> (2022. 11. 30. 방문).
이창기, “정보시스템 보안 강의자료-ch09_암호를 이용한 전자상거래.ppt”, 강원대학교 컴퓨터공학과 <https://cs.kangwon.ac.kr/~leeck/IS/ch09.pdf> (2022. 11. 30. 방문).
인터폴 웹사이트 <https://www.interpol.int/Who-we-are/Member-countries> (2022. 11. 30. 방문).
트위터 웹사이트 <https://transparency.twitter.com/en/reports/information-requests.html#2021-jul-dec> (2022. 11. 30. 방문).
페이스북 웹사이트 <https://transparency.fb.com/data/government-data-requests/country/KR/> (2022. 11. 30. 방문).
한국정보통신기술협회, IT용어사전 <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=054296-2> (2022. 11. 30. 방문).
한국전자인증 웹사이트 <https://www.crosscert.com/solution/03_1_05.jsp> (2022. 11. 30. 방문).
AI IMPACTS, “[보안구현기술] 전자봉투(Digital Envelope)의 이해(생성 및 개봉 동작원리)” <https://blog.naver.com/jvioonpe/221388172751> (2022. 11. 30. 방문).
_____, “[보안구현기술] 전자서명의 이해(전자서명의 생성 및 검증과정)” <https://blog.naver.com/jvioonpe/221384924295> (2022. 11. 30. 방문).
Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman, “Building Internet Firewalls” <https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch06_03.htm> (2022. 11. 30. 방문).
IT, I Think, “공인인증서와 블록체인을 이용한 공동인증 [1]” <https://cholol.tistory.com/426> (2022. 11. 30. 방문).

Jennifer Daskal and Debrae Kennedy-Mayo, “Budapest Convention: What is it and How is it Being Updated?” <https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/?cn-reloaded=1#_edn27> (2022. 11. 30. 방문).

4. 기타

개인정보보호위원회·한국인터넷진흥원, “개인정보의 안전성 확보조치 기준 해설서”, 제2020-2호 (2020).

고려대학교 법학전문대학원 공익법률상담소, “한국인터넷투명성보고서” (2021).

한국인터넷진흥원, “미국 클라우드법(CLOUD ACT)의 주요 내용 및 전망” (2018).

European Commission, “Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules of the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings” (2018).

Abstract

Methods of evidence collection via a service platform for third-party stored information

JEON Sujin
Department of Mathematical Information Science
Graduate School of Convergence Science and Technology
Seoul National University

As online service has become common across the world, there has been a surge in cybercrimes. Given the borderless nature of cybercrimes, their overseas damage has increased at a large scale, in proportion to the growth in the online share of global IT service companies. If a crime occurs via global IT service companies, it is imperative to ask foreign service providers to cooperate.

If electronic evidence for cybercrime investigations is distributed across data centers of global IT service companies, international cooperation is necessary. Legal grounds for formal international cooperation requests include the “Mutual Legal Assistance Treaty,” “Convention on Cybercrime” in Europe, and “CLOUD Act Executive

Agreement" in the U.S. It can also be informally requested via overseas investigative agencies or directly from foreign service providers.

While the Mutual Legal Assistance requires parties to cooperate, it can take a long time for a party to respond after the initial request. This approach is thus considered inefficient, since that information stored by a third party—the key evidence for investigation—needs to be swiftly secured. Moreover, South Korea has not signed onto the "Convention on Cybercrime" or "CLOUD Act Executive Agreement" and may therefore face difficulties in receiving help on such legal grounds.

In the case of informal international cooperation methods, it can be requested via the G7 24/7 High-Tech Crime Network, Interpol, or a Memorandum Of Understanding (MOU) with overseas investigative agencies. Alternatively, an investigative agency can make a direct request to global IT service companies. Information stored by foreign service providers is collected on a case-by-case basis, according to the needs of the investigative agency. This may breed concerns about the investigation being delayed or information being leaked, given the lack of evidence collection procedures and technology.

Currently, investigative agencies directly request the subscriber information stored by foreign service providers through Law Enforcement Request Portals from global IT service companies. The investigative agencies upload a warrant or a court order through the portal and then download the subscriber information. Subscriber information provides the basis for investigation because it enables secondary tracking for the identification of suspects and evidence of their criminal acts.

In this paper, it is shown that electronic evidence can be effectively secured in a timely manner by providing legal and technical measures to collect information stored by a third party. The paper proposes a method in which an investigative agency can request cooperation directly from foreign service providers and gather information stored by a third party by implementing a digital signature service with Public-Key Infrastructure (PKI) and using digital signatures, digital envelopes, and certificates.

The building blocks for the implementation of a 'service platform for third-party stored information' include a process that legally supports this platform and a 'digital signature encryption technology with PKI'. The systemization of legal and technical elements will enable an international cooperation department to collect information stored by a third party promptly and in accordance with the procedure, should an investigative agency request it.

Given that investigative agencies have seen an increase in requests to cooperate from foreign service providers, the implementation of a digital signature service platform will enhance the efficiency of investigations and reduce social costs, resulting in significant economic benefits. It is expected that the digital signature encryption technology will place investigative agencies a step closer to finding the substantive truth in criminal proceedings while maintaining security, minimizing the risks of disclosure of investigative and personal information, and securing reliability in their work.

Keywords : service platform for third-party stored information, digital signature, Public-Key Infrastructure, foreign service provider, electronic evidence, cybercrime

Student Number : 2021-27350