ISSN : 1976-5304
https://kdfs.jams.or.kr

PGP 공개키 단서를 활용한 다크웹 범죄수사 방안

김 재 진
경찰청 (경감)

Dark Web Crime Investigation Using PGP Public Keys Cues

Jaejin Kim
Korean National Police Agency (Senior Inspector)

요 약

은밀화된 범죄의 온상지인 다크웹 사용자는 매년 급격히 늘어나나, 일반적인 사이버범죄에서 범죄자를 추적하는데 이용되는 아이피, 아이디, 전화번호 등의 단서들을 이용하여 다크웹 사용자를 추적하기는 어렵다. 본 논문에서는 다크웹에서 범죄거래를 위해 빈번히 사용 중인 정형화된 PGP 공개키를 활용하여 범죄단서 간 연관성을 파악해 보았다. 그 결과 PGP 공개키를 중심으로 총 1,631쌍 중 349쌍의 단서가 서로 연관되어 있음을 확인하였다. 앞으로 다크웹에서 신분을 감추기 위해 암호화 프로그램인 PGP를 이용한 범죄에 대해서는 PGP 공개키를 중심으로 연관된 단서를 파악하여 다크웹 범죄자를 추적하고, 동일 범죄자에 의한 사건임을 특정하여 수사력을 집중할 수 있을 것이다.

주제어 : 다크웹, 범죄 단서, PGP 공개키, 연관 분석

ABSTRACT

Dark Web users, who are the habitat of hidden crime, increase rapidly every year, but the clues such as IP, ID, and telephone numbers used to track offenders in general cyber crimes are difficult to use in dark web using encrypted network. In this paper, I used the PGP public key that is frequently used for criminal transactions on the dark web, to find out the relationship between the criminal cues. As a result, it was confirmed that 349 pairs of clues among 1,631 pairs are related to PGP public key. In the future, for crimes that use PGP, an encryption program, to hide identity on the Dark Web, it is possible to focus on the investigation by identifying the relevant clues centered on the PGP public key and tracking the Dark Web criminals.

Key Words : Dark Web, Criminal Cues, PGP Public Key, Associative Analysis

Ⅰ. 서 론

현대 정보통신기술은 과거의 점진적인 3차 산업혁명과는 달리 하루가 다르게 급속히 발전하고 있다. 정보통신기술의 발전을 선도하는 우리나라는 세계 최초로 5G를 상용화 하였으며, 첨단 네트워크 구축 등 사이버 강국이라는 평을 듣고 있다. 하지만, 기술의 발전에 비례해 사이버범죄도 점점 일상화되어 국민의 안전과 재산에 대한 위협 수준도 커지고 있다.

현재 해킹, 악성코드 등을 이용한 랜섬웨어 등 새로운 유형의 범죄가 계속 등장하여 사회적인 문제가 되고 있으며, 최근에는 익명화된 정보보안 프로그램을 이용한 사이버범죄가 급속히 증가 중이다. 구글, 네이버와 같은 일반 표면웹(Surface Web)상 검색엔진에서 검색되지 않는 다크웹(Dark Web)상 불법행위라는 새로운 범죄의 등장에 따라 수사기관의 적극적인 대응 및 예방이 필요하나, 전문성 및 기술지원 등이 미흡한 바 새로운 수사기법의 발굴이 필요하다.

선행 연구에서는 다크웹과 관련된 현황 조사와 국제공조를 위한 유럽의 사이버범죄협약 가입 필요성[1], 온라인 수색 및 잠입수사관 제도도입과 관련된 형사법적 대응 방안[2]이 중점적으로 논의되었다. 본 연구에서는 선행 연구에 이어 다크웹 범죄에서 사용 중인 단서를 크롤링한 데이터를 분석하여 단서 간의 연관성을 찾아내고, 동일 범죄여부를 특정하고자 한다. 마지막으로 확보된 데이터를 기반으로 연관된 범죄 단서를 실제 수사에 활용할 수 있는 방안에 대해서도 제시하고자 한다.

▪ Received 03 November 2019, Revised 24 November 2019, Accepted 17 December 2019
▪ 제1저자(First Author) : Jaejin Kim (Email : kjiny0411@gmail.com)

Ⅱ. 다크웹상의 범죄 특징 및 규모

2.1 의의 및 특징

월드와이드웹을 사용하여 정보를 게재하고, 검색할 수 있는 웹을 표면웹(Surface Web)이라 부르고, 일반적인 웹브라우저로는 검색되지 않는 월드와이드웹 컨텐츠를 딥웹(Deep web)이라 말한다[3]. 그리고 딥웹의 일부로서 검색 엔진에 의도적으로 숨겨져 있고, 숨겨진 IP 주소를 사용하며, 특수 웹 브라우저를 통해서만 접속할 수 있는 인터넷을 다크웹이라 부른다[4]. 다크웹은 주로 범죄조직 또는 개인이 개설하여 불법행위에 악용하고 있으며, 대표적인 접속 방법으로는 '토르(TOR : The Onion Router) 브라우저', I2P, 프리넷(Freenet)이 있고, 그중 토르 브라우저가 세계적으로 많이 사용되고 있다.

다크웹은 토르와 같은 특정 프로그램을 이용해야만 접속이 가능하며, 다크웹 URL 주소를 모른다면 관련 범죄정보에 접근하기조차 어려워 이를 수사하기 위해선 고도의 전문지식이 필요하다. 반면에 접속 프로그램만 있으면 어느 나라, 어느 시간에도 공간적인 제약 없이 접속이 가능하다. 다크웹에서는 마치 오프라인 공간의 암시장처럼 온갖 개인정보, 해킹 툴, 악성코드, 아동음란물, 불법 촬영물, 마약, 총기, 심지어 청부살인과 같은 불법 거래가 이루어지고 있고, 거래대금은 주로 가상통화, 그 중에서도 비트코인을 통해서 대부분 이루어진다. 이는 가상통화에 대한 금융관리가 취약하다는 점, 익명성이 보장된다는 점, 추적이 어렵다는 점을 악용하고 있는 것이다. 최근에는 비트코인 거래주소 추적을 위한 트랜젝션(Transaction) 클러스터링(Clustering) 기술이 개발되자 이를 회피하기 위해 믹싱(Mixing) 서비스를 제공해주는 사이트들이 등장하여 범죄수익 추적이 어려워지고 있다.[1] 그 뿐만 아니라 모네로, 지캐시, 대시 같은 익명성을 목적으로 만들어진 가상통화들도 등장하여 범죄수익 추적의 어려움은 더욱 가중되고 있다.

2.2 규모 및 유형

2017년 초 보안업체 트렌드마이크로는 다크웹에 있는 데이터가 일반 인터넷에 있는 데이터보다 550배 더 많다고 발표하였다[5]. 토르를 분석하는 업체인 토르 매트릭스에서는 한국에서 매일 다크웹에 접속하는 인원이 2016년 말 하루 평균 5,156명에서 2019년 7월 11일 기준으로 1만 5,951명으로 세배 이상 급증하였고, 같은 기간 글로벌 접속자도 151만 794명에서 290만 955명으로 늘었다고 발표하였다[6].

다크웹에서는 위조지폐, 마약, 해킹 툴, 무기 및 여권·주민등록번호·전화번호·생체정보 등의 개인정보, 아동음란물·고어물과 같은 변태물 등이 거래되고 있으며, 심지어 청부살인 요청도 있다. 경찰청과 과학기술정보통신부에서는 다크웹 내 범죄 실태를 파악하기 위해 정부 과제를 추진하였는데, 다크웹 내 3,000개 범죄 사이트 현황을 도출해냈다[그림 1]. 범죄 사이트는 금융사기 관련 사이트가 655개로 가장 많았고, 이어서 불법 정보제공 401개, 마약류 337개, 해킹 관련 298개 순이었다[7].

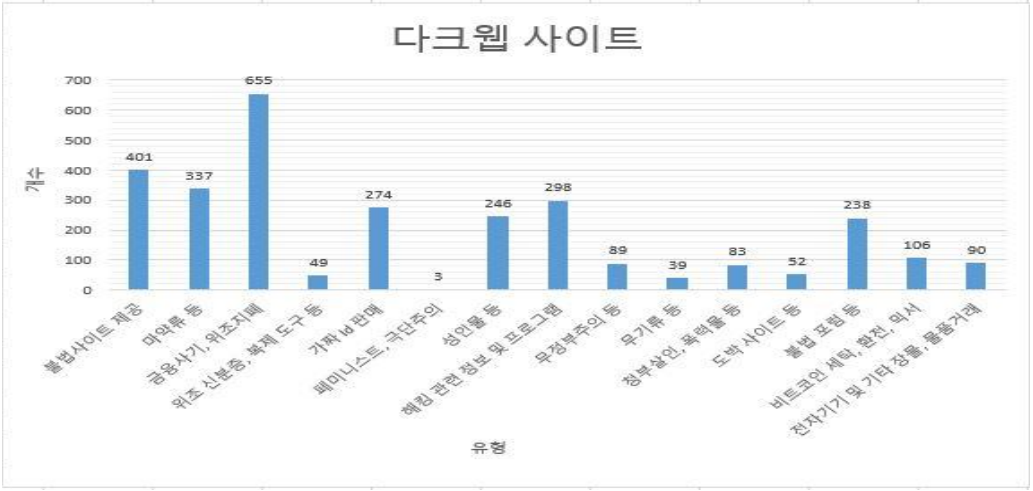

그림 1. 다크웹 내 범죄유형별 사이트 현황(2017~2018, 연구용역 자료 각색)
Fig. 1. Site Status by Type of Crime in Dark Web (2017~2018, Based on research data)

1) 믹싱 서비스는 익명성을 보장하는 것을 넘어 자금세탁에 이용되는 경우가 많다. 2019년 5월 22일(현지시간) 네덜란드 금융범죄수사부(FIOD)가 유로폴(Europol) 및 룩셈부르크 규제당국, 보안회사 맥아피(McAfee)와 협력해 가상통화 믹싱서비스 웹사이트 '베스트믹서(Bestmixer)를' 단속하였다. 이 사건은 유로폴이 가상통화 믹싱사이트 서버를 단속한 첫 번째 사례이다[8].

Ⅲ. 국내외 다크웹 범죄 대응현황

3.1 해외 대응현황

미국 및 독일, 유로폴, 인터폴 등 다크웹 범죄 대응에 있어 선진화된 체제를 갖춘 국가 및 국제기구에서는 다크웹 범죄에 관해 언더커버(Undercover) 수사 등 효과적인 수단을 사용하고, 국가 간 공동 대응하는 등 다크웹상의 범죄 해결을 위해 노력하고 있다. 미국 및 유럽평의회에 소속된 대부분의 나라가 사이버범죄협약(Cybercrime convention)에 가입하여 국제적인 사이버범죄에 공동으로 대응하기 위한 체제를 갖추고 자료보전, 온라인 수색[2] 및 역외 압수수색[3] 제도 등을 운영하고 있으며, 일본도 형사소송법을 개정하여 사이버범죄협약을 이행할 수 있는 근거를 마련해 두고 있다.

실제 다크웹 수사사례를 살펴보면, 언더커버 활동과 관련하여 미국에서는 다크웹 내 대규모 아동음란물 사이트를 직접 운영하여 아동성애자를 검거하였고(Playpen), 독일과 네덜란드에서는 다크웹 내 한사마켓 운영자 검거 시, 서버 운영권한을 획득하여 1개월간 서버에 접속한 약 2만명 가량의 판매자 정보를 획득한 일이 있다[9]. 유로폴은 최근 The Giftbox Exchange라는 아동 포르노 사이트를 수색하기 위하여 온라인 수색의 일종인 NIT(Network Investigative Techniques) 수사를 사용하였고, 호주 정부도 The Love Zone이라고 불리는 아동포르노 사이트를 해킹하기 위하여 피싱 공격을 사용한 사례가 있다[10]. 2019년 4월 미국과 독일, 유로폴이 공조해 세계에서 두 번째로 큰 규모의 다크웹인 월스트릿 마켓 운영자를 검거하고, 사이트 운영을 정지시키기도 하였다[11].

표 1. 국가별 다크웹상의 범죄수사를 위한 효율적인 지원 제도[2][10][12]
Table 1. Efficient Support System for Dark Web Crime Investigation by Country

국가	국내 법률 근거				유럽 사이버범죄 협약 가입
	전기통신 감청	온라인 수색	역외 압수수색	위장 수사	
독일	○	○	○	○	○
미국	○	△ (판례)	△ (규칙)	△ (지침)	○
일본	○	-	○	-	○

3.2 국내 대응현황

다크웹상의 범죄도 일반 사이버범죄 수사와 같이 형법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 같은 개별법에 근거하여 수사를 하고 있으나, 사이버범죄 수사를 위해 효율적인 방법으로 논의되고 있는 방안인 온라인 수색과 역외 압수수색, 감청[4] 등의 수단이 현재 우리나라에서는 개인정보보호법 및 통신비밀보호법 등에서 허용하지 않거나 엄격히 제한하고 있다. 현재 다크웹상의 정보는 정보통신망에서 유통되는 정보라는 점에서 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제44조의7 제2항과 제3항에 근거하여 방송통신심의위원회의 심의를 거쳐 다크웹에 유통되는 불법 정보의 삭제 및 접속 차단을 명령할 수 있다. 그러나 방송통신위원회의 경우 주로 표면웹에 대한 불법정보 차단에 집중하고 있으며, 다크웹에 유통되는 불법정보에 대해서는 다크웹의 정보가 표면웹에 노출되는 경우에만 해당 정보를 표면웹에서 차단하고 있다[13].

다크웹상의 범죄 수사를 위해선 수사 인력의 전문성 외에도 대용량 파일 및 추적경로 분석을 위한 고성능 장비와 수사시스템의 지원이 필수적이다. 그런데, 대부분의 수사를 담당하는 경찰청의 경우 사이버테러・음란물(아동 성착취물)・다크웹 범죄 등에 대해 지방청 일제 지시를 통한 테마성 집중단속 외에는 사이버안전국 사이버수사과 내 1개 수사팀(6명 이내)에서만 다크웹 수사를 전담하고 있고, 대용량 파일을 분석하기 위한 기본 장비만 있는 실정이다(2019년 11월 기준). 수사지원을 위한 시스템을 개발하고는 있으나, 예산 및 기술의 한계로 충분한 기능을 갖추기에는 많은 시간이 소요될 것으로 보인다. 현재 우리나라는 해외 수사기관에 비해 제도, 인적 구성, 장비, 시스템 구축 등 모든 부분에서 열악하다.

2) 온라인 수색이란 수사기관이 여러 가지 기술적 수단을 이용하여 당사자의 IT 시스템에 비밀리에 접근하여 대상시스템의 이용을 비밀리에 감시하거나 절차상 중요한 저장매체의 내용을 열람하기 위해 거기에 저장된 데이터를 수사기관이 비밀리에 전달하는 것을 말한다[14].

3) 디지털 증거에 대한 역외 압수수색이란 수사기관이 수사상 필요성에 의해 역외에 존재하는 컴퓨터 데이터 및 관련 디지털 증거에 대해 집행하는 압수수색 방법이다. 하지만 이와 관련하여 아직까지 일관된 정의는 존재하지 않으며, 각 나라에서 집행하고 있는 실무상의 역외 압수수색 또한 그 범주를 달리하고 있는 실정이다[15].

4) 우리나라에서 감청 등과 관련된 내용은 통신비밀보호법 제4조에서 불법검열과 불법감청 증거사용 금지를, 제5조에서 허가요건을 규정하고 있고, 전기통신 감청 중 패킷(Packet)감청은 위헌 판결(헌재 2018. 8. 30. 2016헌마263)이 났다.

3.3 소 결

다크웹상의 범죄는 일반인들이 쉽게 접근하고 사용할 수 있는 토르 브라우저가 있어 이미 일상 속으로 깊숙이 침투하고 있다. 다크웹상에서 한글로 운영되는 사이트의 수는 2017년 기준 세계 5위 수준으로[16], 마약판매, 위조 등 명백히 범죄에 이용할 목적으로 개설된 사이트가 다수 존재한다. 하지만 현재 국내에서 다크웹을 이용해 일어난 범죄에 대한 검거는 우연한 기회에 시민의 제보에 의해 드러나거나 사이버상에서의 언더커버 수사활동으로 인해 이루어진 것이 대부분이며, 국내에서 다크웹을 이용하여 일어난 것으로 추정되는 범죄 건수에 비하여 현격히 낮은 것이 사실이다[1]. 신종 범죄수단인 다크웹의 등장으로 점점 은밀화・지능화되는 범죄를 수사하기 위한 전문성은 더욱 높게 요구되는 반면, 현재 우리 수사기관의 대응 수단은 미약하며, 이에 대한 대책이 필요하다. 한때 다크웹상에서 유명했던 실크로드 2.0의 운영자인 블레이크 벤달은 토르 내 실크로드 2.0 서버를 등록하면서 본인이 실제 사용하는 이메일 계정을 사용하는 운영상의 실수를 범하여 FBI에 체포되었다[17]. 판매자가 실수하는 운영 보안상의 취약점 또는 응용 프로그램 단계에서의 취약점 등을 이용한[18] 수사기법은 다크웹 범죄 검거에 큰 역할을 할 것이다.

Ⅳ. 다크웹 범죄 추적 및 수사 방안

4.1 다크웹 범죄 추적단서 분석방법

4.1.1 다크웹 범죄 추적단서 유형

일반적인 사이버범죄에서는 범인을 추적하기 위해 아이피, 아이디, 닉네임, 이메일 및 계좌번호, 전화번호 등을 단서로써 주로 활용한다. 반면, 토르 네트워크를 이용한 다크웹 범죄는 세계 여러 나라의 수많은 노드를 거쳐 접속하는 특성상 아이피 추적이 불가능하기 때문에 일반적인 사이버범죄에서 범인을 추적하기 위해 가장 많이 활용하는 아이피는 추적 단서로서 큰 의미가 없다. 보통 다크웹에서는 [그림 2]의 게시물과 같이 수사기관의 추적을 피하기 위해 비트코인과 같은 가상통화를 이용하는 경우가 대부분이다. 이때 가상통화 지갑주소가 드러난다면 범인을 추적하기 위한 실마리가 제공되는 셈이다. 다만, 실질적으로 비트코인 지갑주소를 직접적으로 노출하는 경우는 거의 없다. 다크웹 게시물을 보면 거래내용과 장소, 비트코인 지갑주소 노출을 피하기 위해 암호화하고 복호화하는 프로그램인 PGP(Pretty Good Privacy)를 이용하는 경우가 대부분이다. 이 경우 한 사람이 여러 다크웹 사이트에서 여러 아이디(ID)를 사용하여 게시하는 경우 동일한 PGP 키를 사용하는 아이디들이 동일한 사람에게 속하는 것을 보여주는 결정적인 증거가 될 수 있다[19].

그림 2. 다크웹에서 비트코인을 이용한 총기 판매
Fig. 2. Sale of guns using Bitcoin on Dark Web

4.1.2 다크웹 범죄단서 연관분석 필요성

다크웹상의 범죄 역시 사이버범죄로써 그 특성상 동일 범죄자에 의한 다중 범죄가 발생하는 경우가 많다. 예를 들어 판매자가 A라는 다크웹에서 A-a라는 아이디와 C라는 PGP 공개키를 쓰고, B 다크웹에서 B-a라는 아이디와 C라는 PGP 공개키를 쓸 경우 동일 범죄자일 가능성이 높다. 특히 가상통화 지갑주소 같은 다른 단서들이 계속 연결된다면 그 가능성은 더욱 높아진다.

따라서 다크웹상 범죄에 대해 향후 수사 단서로써 활용할 범죄첩보 수집 및 중복수사 방지를 위해 다크웹 게시물 내 범죄 단서를 군집화하여 단서들을 연관 분석하는 기법의 활용이 필요하다. 하나의 범죄단서와 연결된 또 다른 범죄단서 간의 군집화를 통해 동일 범죄자에 의한 범행임을 특정하면 범죄자의 여죄 파악 및 수사기관 간 동일 범죄자 수사로 인한 시간 및 인력, 예산 낭비를 막을 수 있다.

4.1.3 범죄단서 연관분석 방법 (인터넷사기: 계좌번호-전화번호 분석)

일반적으로 표면웹상 사이버범죄 중 가장 많이 발생하는 것은 인터넷 사기(2018년 경찰청 통계 기준 전체 사이버범죄의 약 75%)이다. 인터넷사기 사건의 경우 유전자와 같이 각 사건(객체)은 다양한 수사단서(속성)를 포함하고 있으며, 수사단서가 100% 일치하는 사건은 극히 일부에 불과하지만, 바이클러스터링 군집화 기법을 적용하여 중복된 수사단서가 있는 경우 동일 범죄로 판단할 수 있다[20].

〔표 2〕와 〔표 3〕은 계좌번호와 전화번호 단서를 활용한 사이버범죄 수사단서 분석 행렬구조(Matrix)로 사건(Case), 계좌번호(Account Number), 전화번호(Telephone Number), 기타 단서(아이피, 이메일, 아이디 등)로 구성해 보았다. 방법은 다음과 같다. ① 사건 C1에서 사용된 계좌번호 'A100'을 가지고 있는 사건을 검색하고 ② 추출된 사건 'C1・C3・C4' 중, 'C1'에서 사용된 전화번호 'T100'을 가지고 있는 사건을 검색한 다음 ③ 추출된 'C6・C8'의 계좌번호 'A700・A900'을 ①과 같은 방법으로 추출하여 그룹화하고 동일 사건으로 선정(연관된 'T700' 확인)한다. 상기 2차 분석에서 추가 발견된 전화번호 'T700'을 같은 방법으로 연관 분석하여 동일 사건으로 판명 시, 이를 분류・군집화하고 피의자(범죄조직)를 추적하여 사건 간 연관성을 확인할 수 있다. 이러한 연관분석 방식을 다크웹 수사단서 분석에도 유사하게 적용할 수 있다.

표 2. 1차 분석, 계좌번호 중심
Table 2. Primary analysis, centered on account number

사건	수사 단서			동일 사건
	#1 계좌번호	#1 전화번호	기타	
C1	A100	T100	?	○
C2	A200	?	?	
C3	A100	?	?	○
C4	A100	?	?	○
C5	A300	?	?	

표 3. 2차 분석, 연관된 전화번호 중심
Table 3. Secondary analysis, centered phone number associated

사건	수사 단서				동일 사건
	#1 전화번호	#1 계좌번호	#2 전화번호	기타	
C1	T100	?	?	?	○
C6	T100	A700	T700	?	○
C7	T200	?	?	?	
C8	T100	A900	T700	?	○
C9	T500	?	?	?	

4.2 다크웹 범죄단서 분석

4.2.1 다크웹 게시판 및 거래 특징

다크웹 내 게시판에서는 마약 및 개인정보 등 다양한 불법 거래를 위해 판매자와 구매자의 PGP 공개키와 아이디를 활용해 거래 내역을 암호화하여 사용 중인 경우가 많다. PGP는 개인정보보호를 목적으로 만들어진 통신방법으로, 이메일 내용을 암호화하면 인터넷서비스제공사업자(ISP)도 그 내용을 확인할 수 없다. 다만, 발신자와 수신자가 누구인지는 확인이 가능하나, 다크웹에서는 토르 브라우저에서 IP 추적이 어렵다는 점을 이용하여 발신자 및 수신자와 관련된 정보를 암호화하는 방법으로 수사기관의 추적을 피해 불법 거래에 이용하고 있다.

다크웹에서의 물품 판매는 사이트 운영자가 직접 판매하는 경우와 개인 간 직거래를 하는 방식으로 크게 운영되고 있다. 그 중 직거래 방식인 다크웹 한글 마약사이트 '0000 KOREA'는 게시글을 올리기 위해 필수적으로 등급 업그레이드(이하 등업)를 요구하고 있고, 등업을 위해선 PGP 공개키와 연결된 아이디가 필요하다. 게시글은 게시자의 PGP 아이디와 공개키가 공개된다[그림 3]. 또한 등업 후 가입자 개인이 아이디를 변경하는 것은 불가능하다(다른 한글 마약 사이트 'Mi0's 00 shop'도 운영 방식이 동일하다). 거래방법은 다른 사람의 아이디를 친구 등록한 후 개인 메세지 전송 기능[그림 4]을 활용해 〔그림 5〕와 같이 메시지를 암호화 후 전송하여 약속을 정하고, 판매자가 마약을 임의의 장소에 떨어뜨려 구매자가 가져가는 방식을 이용한다. 이러한 방식은 다크웹 서버를 압수하지 않는 한 연락을 주고받는 당사자의 정보를 ISP도 알 수가 없고, 설사 서버가 압수되더라도 메시지 내용을 알 수 없다. 똑같은 이유로 메시지를 암호화하여 텔레그램으로 거래하기도 한다.

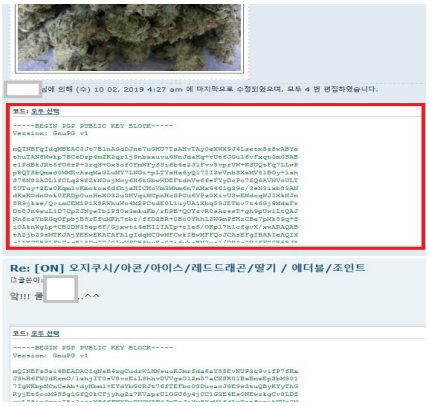

그림 3. 다크웹 게시판 아이디, 공개키 게시 상태
Fig. 3. Dark Web Bulletin ID, Public Key Posting Status

그림 4. 다크웹 내 메시지 전송 기능
Fig. 4. Message transmission function in dark web

그림 5. 메시지 암호화
Fig. 5. Message encryption

4.2.2 GnuPG 프로그램 기능

PGP 오픈소스 프로그램인 'Gpg4win'과 'gpg4usb'를 사용하여 한쌍의 공개키와 개인키를 생성할 수 있는데, 'Gpg4win'을 사용하여 동일한 아이디를 가진 다수의 공개키 생성이 가능하다[표 4]. 반대로 동일한 공개키를 가진 다수의 아이디 및 이메일 생성도 가능하다[그림 6](GnuPG에서 제공하는 맥 OS용 프로그램 'GPG Suite'와 시만텍에서 제공하는 유료버전 'Encryption Desktop' 프로그램을 사용해서도 동일한 아이디를 가진 다수의 공개키, 동일한 공개키를 가진 다수의 아이디 생성이 가능하다).

표 4. 동일한 아이디를 가진 다수 PGP 공개키 생성
Table 4. Generate multiple pgp public keys with the same id

-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: User-ID: mr.tester Comment: Created: 2019-10-17 오후 4:30 Comment: Expires: 2021-10-17 오후 12:00 Comment: Type: 4096-bit RSA (secret key available) Comment: Usage: Signing, Encryption, Certifying User-IDs Comment: Fingerprint: 596BD1885AFA09B47D0B60F3C8E5665EE4EF0034 mQINBF2oGJgBEADD3+Y/gROAr8eI30Siqd7MGjjN1+6CDBSygrapxWIAgW3YyZzc pPJj1rZJXPtn4+wmpH/0Txf1juJvFEidLIRE+Dm3JCbkIvAlSFKGFlKz1Z5BpU// b319q7Ns2bt7yOqVPX3wUuVUWKCOdp/k6rH2ZKb4aYlUSzpMpFOKNZkR4Vs+9xpf SfOxe6i4k1QoFDUCR2GMEtFpK1hvPMsS7z+jEIKMJ7htzL8ivFEbFXHeVqg4OeEh..... ..... -----END PGP PUBLIC KEY BLOCK-----	-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: User-ID: mr.tester Comment: Created: 2019-10-17 오후 4:29 Comment: Expires: 2021-10-17 오후 12:00 Comment: Type: 2048-bit RSA (secret key available) Comment: Usage: Signing, Encryption, Certifying User-IDs Comment: Fingerprint: 78B274686400A54F0685D55646038B3B9859F0EF mQENBF2oGHMBCADn2xhtD2qcvXi9lpOlTzm KjJlGVy6ZDq+fybBclSxKpr6lNoe8 C4rLZaEjrTxcsOPeXxd9Z7NZXv2MLgrWyMKI /JNfgCcJCPm20pGXlrOmkq+M5zwO puFo7rRpgQcNarty2MuvFeOSbtvRLB9fP0yW uMF+glxJGdbqBi/S34uQWWaLLsqT buXQPIKrcPjlLLjC0kmsDFCbP3MtgUOpkaWe prcPlUbtTllt9jf+ZNQ37yltA4xU KjMeyWg8NxhJnxCqptQ6Dlu8dz1argr9kf5qnuS..... -----END PGP PUBLIC KEY BLOCK-----	-----BEGIN PGP PUBLIC KEY BLOCK----- Comment: User-ID: mr.tester Comment: Created: 2019-10-17 오후 4:28 Comment: Expires: 2021-10-17 오후 12:00 Comment: Type: 4096-bit RSA (secret key available) Comment: Usage: Signing, Encryption, Certifying User-IDs Comment: Fingerprint: 2BF07D8A7C10DBEB646A4AED8803FE57F724EED0 mQINBF2oGAkBEAD7mC16qU4Q8SKeloM+hk aYuLM5ZvYfOciqZAVpp6phZ73Zzrwg qHVH/o2KM+ZFXkJbospZNCj0kF1UJlfLO8Ple zUXdwUR3sQhId0ofB0AqzSG1dBV uhiPEZ38oDrSXhWQdFQ2MSToeXpnIT05/up ZBcIlte1/LBzzb8kYyegDSVOFeTsA ut19V6xkx/7QS/TVTKm7/4qcehZqk03yuzQ7 vSyS+CVJJUA6son42ALuSRABMP5PpSGunzrk hB1BSEMfqzG/rY5aLph3Xf9rV0Zt..... ..... -----END PGP PUBLIC KEY BLOCK-----

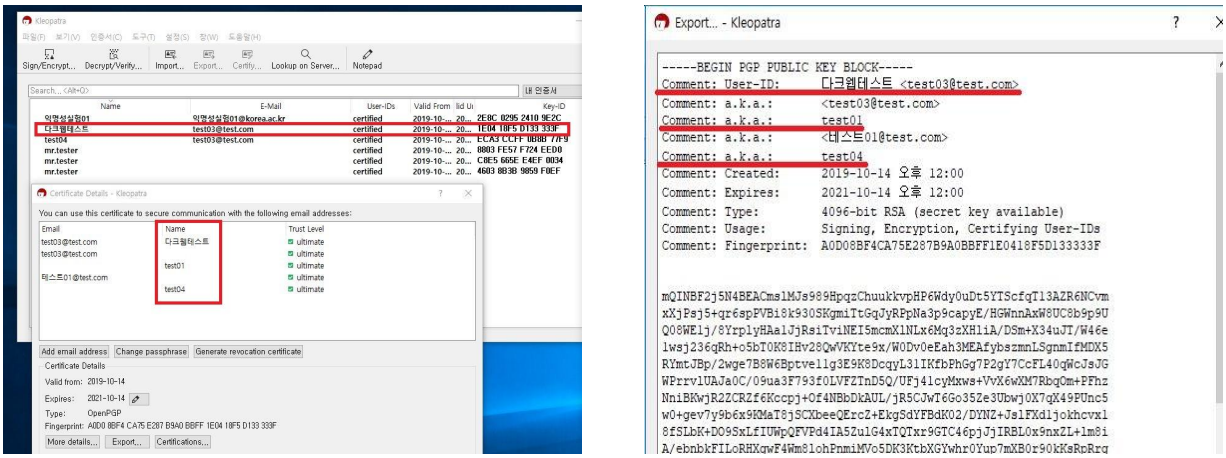

그림 6. 동일한 pgp공개키를 가진 다수 아이디 생성
Fig. 6. Generate multiple IDs on the same pgp public key

4.2.3 PGP 키 연관분석 결과

본 연구는 다크웹에서 한글로 서비스하는 최대사이트 중 한 곳인 '0000 KOREA' 게시판에서 크롤링 된 데이터(2017년 7월 기준)[7]에서 추출한 PGP 공개키와 아이디 1,631쌍을 분석해 보았다. 연관성 분석에 앞서 PGP 공개키(숫자00 표기)와 아이디(ID00 표기)에 고유번호를 부여하였고, 중복값을 가진 데이터를 파악하기 위해 ① PGP 공개키별 연관된 아이디[그림 7]와 ② 아이디별 연관된 PGP 공개키[그림 8]로 분류하여 군집화 하였다. 시각화는 군집된 수가 많을수록 큰 원으로 표현된다. 가장 많은 수의 아이디와 연관된 상위 10개의 PGP 키 번호와 가장 많은 PGP키 개수와 연관된 상위 10개의 아이디는 [그림 7]과 [그림 8]에서 색을 진하게 하고 글자를 삽입하여 표현하였다.

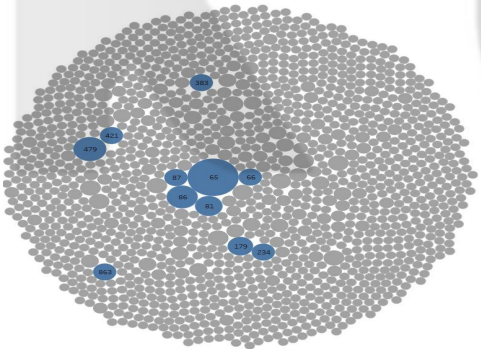

그림 7. PGP 키 기준 군집도
Fig. 7. PGP key cluster

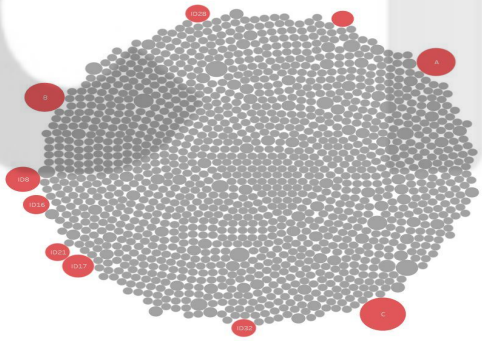

그림 8. 아이디 기준 군집도
Fig. 8. ID cluster

PGP 공개키와 아이디 간의 연결을 구체적으로 확인하기 위해 ① 상위 10개의 단서들 중에서 연관된 PGP 키 개수를 가장 많이 보유한 상위 3개의 아이디와, ② 연관된 아이디 개수를 가장 많이 가진 상위 3개의 PGP 키를 표본으로 추출하여 상호 간의 연관성을 분석해 보았다. 상위 3개의 아이디는 'A', 'B', 'C'로 표기하였다. 그리고 'A'와 연관된 공개키 14개 중 상위 3개 순위 공개키 번호 '65번', '86번', '479번'이 있는지 확인하였다. 마찬가지 방법으로 기준 아이디 'B', 'C'도 상위 3개 순위 공개키와 연관된 것이 있는지를 확인하고, 상위 공개키와 연관된 아이디까지 함께 정렬하였다. 상위 공개키와 연관된 아이디에도 ID 1~8번(86번 PGP 키와 연관), ID 10~18번(479번 PGP 키와 연관), ID 20~41번(65번 PGP 키와 연관)으로 고유번호를 각각 부여하였다. 다만 PGP 공개키가 동일하면 아이디 간의 연관성은 확실하나, 일반적으로 아이디가 동일하다고 공개키가 다른 동일한 아이디를 가진 사람이 모두 동일인이라고 단정할 수 없다는 위험성은 있을 수 있다. 하지만 분석한 사이트에서는 탈퇴하지 않는 한 같은 아이디로 다른 사람이 가입 할 수 없게 되어 있어, 동일한 아이디에 연결된 공개키가 모두 같은 사람의 것일 확률이 굉장히 높다. 실제로 상위 3개 다크웹 아이디 게시글을 읽어보면 어휘나 문법, 행동 양상이 비슷해 동일한 인물로 보였고, 사이트에서 공개키 변경은 프로필 편집의 서명 등록기능을 활용해 쉽게 할 수 있다. 또한 사이버범죄 중 실제 표면웹상 물품판매 관련 범죄에서 인터넷 계좌번호가 다르지만 아이디가 동일한 경우, 검거해보면 동일인물인 사건도 있다.

통계 분석 프로그램 RStudio를 사용[그림 9]하여 시각화한 결과는 [그림 10]과 같다. [그림 10]을 보면 모든 단서들이 전부 연결되어 있는 것이 한눈에 파악된다. 기준 아이디 'A'는 PGP 키 '234 ·488·554번'을 통해 기준 아이디 'B'와 1단

계 건너 연결된다. 또한 기준 아이디 'A'는 PGP 키 '86번'과 연관된 'ID 8번'과 연결되고, PGP 키 '65번'을 통해서 기준 아이디 'C'까지 4단계를 거쳐 연결점을 찾을 수 있다. 기준 아이디 'B' 또한 PGP 키 '479번'과 연관된 'ID 8번', 'ID 13번'과 연결되고, PGP 키 '65번'을 통해서 기준 아이디 'C'까지 4단계를 거쳐 연결되어 있음을 확인할 수 있다. 이는 판매자가 하나의 조직으로 체계적으로 운영되거나 또는 개인이 지능적으로 수사기관을 속이기 위해 아이디와 PGP 공개키를 바꾸어 가며 사용 중이라는 점을 알 수 있다. 또한 PGP 공개키를 활용한 연관성 분석을 통해 기준 아이디 'A'로부터 총 86개의 연관된 다른 단서를 확보할 수 있음을 의미한다.

```
1  library(readxl)
2  exam <- read_excel("C:/graduate/darkweb db/exam.xlsx",
3  sheet = "Sheet1")
4  View(exam)
5  library(tidygraph)
6  library(ggraph)
7  dark <-as_tbl_graph(exam)
8  class(dark)
9  plot(dark)
10 exam %>% as_tbl_graph() %>% ggraph(layout='kk') + geom_node_text(aes
   (label=name)) + geom_edge_link(aes(start_cap = label_rect(node1.name),
   end_cap = label_rect(node2.name)))
```

그림 9. RStudio 시각화 코드

Fig. 9. RStudio visualization code

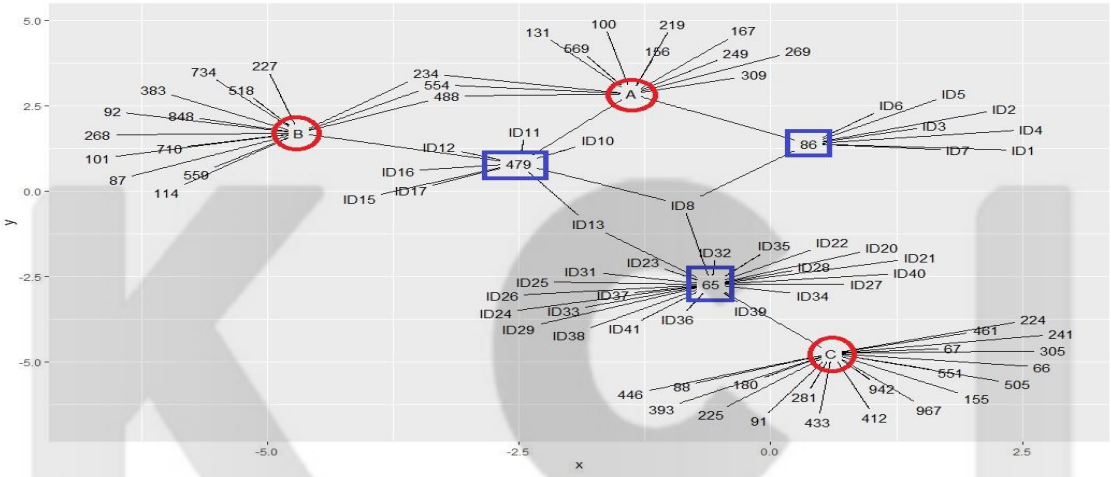

그림 10. 다크웹 ID ↔ PGP 공개키 연관분석 시각화 결과(상위 3개)

Fig. 10. Dark Web ID ↔ PGP public key association analysis visualization result(Top 3)

매트릭스 구조를 이용하여 PGP 공개키와 아이디 1,631쌍 전체의 연관성을 분석한 결과는 〔그림 11〕과 같다. 1,631쌍 중 1개 이상의 중복된 PGP 공개키를 가진 단서는 총 349쌍이고, 모두 17개의 그룹으로 분류되었다. 그 중 PGP 공개키를 중심으로 가장 많은 연관성을 가진 1개의 그룹은 총 307쌍이나 되는 공개키, 아이디 각각의 노드(node)들이 한 쌍의 공개키와 아이디에서, 다른 쌍의 공개키와 아이디로 계속 연결되어 있다.

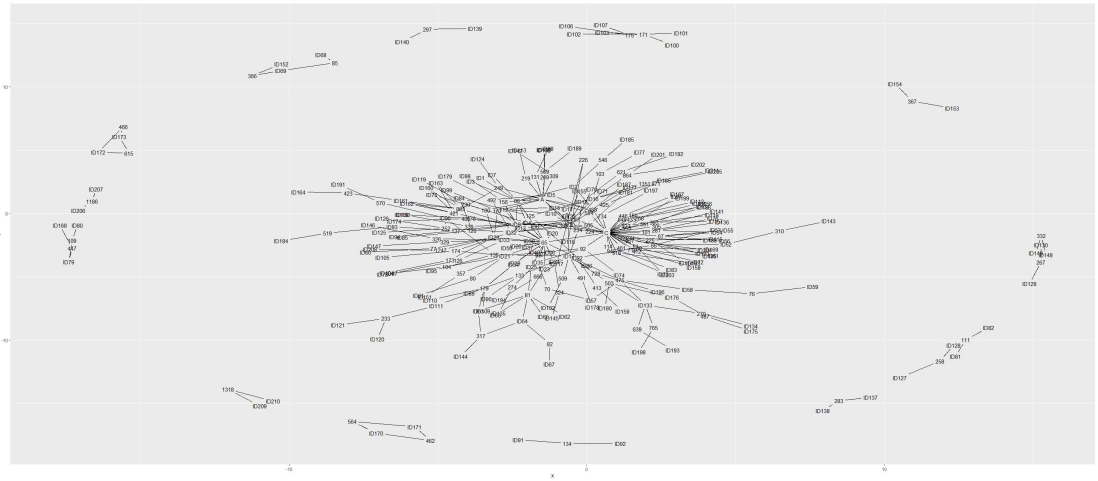

그림 11. 다크웹 ID ↔ PGP 공개키 연관분석 시각화 결과(전체)

Fig. 11. Dark Web ID ↔ PGP public key association analysis visualization result(all)

표 5. 다크웹 ID ↔ PGP 공개키 연관분석 결과(그룹별)
Table 5. Dark Web ID ↔ PGP public key association analysis result(By group)

구분 (그룹)	개수		개수(중복제거)		변경 횟수(평균)		활동 유형 (주요 특성)	분류 (추정)
	PGP 키	아이디	PGP 키	아이디	PGP 키	아이디		
A그룹 (소그룹 1개)	307쌍		103개	161개	102회	160회	사이트 운영 및 마약 판매, 지식 공유	조직화된 집단
B그룹 (소그룹 4개)	16쌍		8개	10개	1회	1.5회	마약 판매 및 지식 공유	지능범
C그룹 (소그룹 12개)	26쌍		12개	26개	없음	1회	마약 거래, 지식 공유	개인 사용자
소계	349쌍							
기타	1,282쌍		1,282개	1,282개	없음	없음	지식 요청, 댓글 게재	개인 사용자 (단순 호기심)
총계	1,631쌍		1,405개	1,479개				

DDOS나 APT 공격에서 프로파일링을 통해 범죄조직을 분류하여 수사역량을 집중하듯이, 다크웹상의 범죄도 단순한 호기심에 의해 접속한 경우와 수사망을 피하기 위해 지능적으로 정보를 은닉하는 경우, 조직적인 범죄로 판단되는 경우 등 몇 개의 그룹으로 분류해 대응 방법을 달리할 필요가 있다. 그룹 특성에 따른 대응 방안 수립을 위해 〔그림 10〕에서 분류한 PGP 공개키 데이터 변경횟수를 기준으로 17개의 소그룹을 크게 4개의 그룹으로 나누었다〔표 5〕. A그룹은 공개키 변경을 1회 이상, B그룹은 1회, C그룹은 공개키 변경 없이 아이디만 변경하였고, 기타 그룹은 사이트 가입 후 아이디와 공개키를 변경한 연관성을 찾을 수 없었다. A그룹은 총 307쌍이 서로 연결되어 있는데 공개키와 아이디 각각의 중복값을 제외한 고유값은 총 103개의 공개키와 161개의 아이디로 이루어져 있다. 2014년 사이트가 생성된 이후 데이터가 크롤링 될 때까지 최초 공개키와 아이디를 생성한 후 공개키는 102회, 아이디는 160회나 변경한 것으로 추정되어, 개인의 은닉 활동이라기보다는 조직적인 개입이 있었을 것으로 판단된다. 실제로 해당 사이트 운영진의 아이디와 공개키도 포함되어 있다. B그룹의 경우 공개키를 1회 변경한 이력을 가진 4개의 소그룹으로 이루어져 있고 중복값을 제외한 고유값만 계산하면 총 8개의 공개키와 10개의 아이디로 구성되어 있다. B 그룹은 공개키를 평균 1회, 아이디를 평균 1.5회 변경하였는데, 신분을 위장하기 위해 개인이 지능적으로 공개키와 아이디를 번갈아 변경한 것으로 보인다. C그룹의 경우 공개키 변경 없이 13개의 소그룹이 평균 1회의 아이디 변경만 하였다. 다만 C그룹의 경우 아이디 변경 사유는 신분 은닉 목적이 있었을 수도 있고, 아이디의 비밀번호를 잃어버려 기존 공개키로 아이디를 변경하여 새로 가입하였을 가능성도 있다.

데이터가 크롤링된 기간을 포함해 2019년 10월까지의 게시글을 통해 그룹별 사이트 활동 내용을 분석해보면 기타 그룹은 단순히 게시글을 읽거나, 댓글을 다는 정도로 호기심으로 사이트에 접속하는 표면웹상 일반적인 사용자와 같은 양상을 보인다. B그룹과 C그룹은 마약 관련 전문지식 공유와 실제 거래를 해본 경험도 있는 것으로 보인다. A그룹에 속한 아이디 중 활동이 많은 아이디를 선정하여 게시글을 읽어보면 여론 조성 행위, 마약 관련 정보공유, 대마 재배방법 교육 등 전문지식이 필요한 글이 다수이고, 사이트 이용 방법 등에 대한 교육도 있다. 운영진 공개키 및 아이디와의 연관성, 공개키와 아이디 변경횟수, 사이트 게시글을 분석했을 때 그룹A는 체계적으로 활동하는 범죄조직으로 보이며, 그룹B는 지능범, 그룹 C와 기타 그룹은 사이트 활동에 목적을 둔 개인 사용자로 판단된다(다만, 1,631쌍에 속하는 아이디의 게시글 중 연구자가 접근할 수 없는 게시글도 있어 성향 분석에 한계가 있음을 밝힌다). 수사기관은 그룹B와 같은 지능적이고 실제 범죄를 저질렀을 가능성이 높은 경우는 집중 관리대상으로 선정하고, 그룹A와 같이 범죄조직으로 의심될 경우 수사력을 집중하여 장기적으로 추적하여야 할 것이다.

4.3 다크웹 수사 적용 가능성

4.3.1 PGP 공개키를 활용한 수사

PGP 공개키를 중심으로 관련된 아이디, 닉네임, 이메일 주소, 비트코인 지갑주소 등 정형화된 단서들을 추가로 확보하여 범인을 추적하는데 활용할 수 있다. 조직화·지능화된 범죄자의 경우 의도적으로 다크웹에서 사용한 공개키와 연결된 개인정보 단서를 남기지 않으려고 노력하겠으나, 일부 판매자의 경우 실수로 PGP 키 서버에 공개키를 올리거나, 실크로드

2.0 사례와 같이 본인도 모르게 공개키 정보와 관련된 개인정보 흔적을 표면웹상에 남겼다면, IP 추적이나 표면웹 검색 등을 통해 공개키와 연관된 범죄자 단서를 찾을 수 있을 것이다. 또한 향후 피의자를 특정하여 개인 PC 등을 확보한다면 공개키 저장내역 또는 대칭되는 개인키 저장 내역 등을 비교해 범죄 입증 증거로써 사용이 가능하다.

4.3.2 동일사건 군집화를 통한 중복수사 방지

범죄단서 간 연관분석을 통해 동일 범죄자에 대해 다수의 경찰관서에서 수사(내사) 중이라면 사건 관할 규정에 따라 담당관서를 지정하여 중복수사를 방지하고 업무의 효율성을 제고할 수 있다. 예를 들어 다수의 대포통장 및 전화번호를 사용하는 표면웹 인터넷 사기와 같이, 다크웹에서 마약 판매자가 PGP 공개키와 아이디를 변경해가며 범죄행위 시 각 관서에서 파편적으로 사건을 접수하여 동일 범죄자에 의한 사건임에도 개별 사건으로 각각 수사하는 것을 예방할 수 있다. 이는 한정된 인력과 시간제한이라는 수사기관의 한계를 극복하고, 수사력이 집중되는 효과를 발휘할 것이다.

4.4. 소 결

범죄단서 정보란 경찰이 독자적으로 범죄를 예방하거나, 수사 절차상 내사와 수사에 진입하기 위한 단초, 즉 수사 단서를 확보하고 경찰인지 사건으로 수사하기 위해 수집하는 범죄정보를 말한다[21]. 본 연구에서는 정형화된 단서, 그 중에서도 PGP 공개키를 기준으로 단서 간의 연관성을 파악하고 다크웹 범죄 단서를 활용하는 방안을 제안하였다. 향후 다크웹 수사 시 PGP 공개키를 기반으로 상호 연관성을 분석한다면 범죄자가 신분을 은닉하며 저지른 범행 간의 관계를 밝혀낼 수 있을 것이다. 또한 다크웹에서의 범죄와 유사한 범죄가 오프라인이나 표면웹상에서 발생하여 검거되었을 때 다크웹상의 범죄와 연관성이 있는지 확인할 필요가 있다.

본 연구에서는 다크웹상의 범죄 단서간의 연관성만 분석하였으나, 표면웹상의 단서와의 연관성에 대한 연구도 차후에 필요할 것으로 보인다. 표면웹상의 단서도 다크웹상의 범죄 수사에 활용 가능하다면, 범인을 추적하고 특정할 수 있는 폭을 보다 더 넓힐 수 있을 것이다. 또한 다크웹에서 수집된 단서를 표면웹에서 발생한 사이버범죄 수사에도 활용할 수 있다면, 다크웹 범죄의 해결뿐만 아니라 표면웹의 사이버범죄 해결을 위해서도 큰 도움이 될 것으로 기대된다. 현재 표면웹 수사시스템에는 PGP 공개키 정보가 없어, 향후 사이버범죄 첩보 ·단서 입력 시 공개키 정보도 입력하도록 현재의 범죄정보 입력 체계를 개선할 필요도 있다.

Ⅴ. 결 론

다크웹이라는 용어가 일반인들에게는 생소하였던 것이 이제는 국내에서만 하루 1.6만명(19년 7월 기준) 가깝게 접속할 정도로 보편화 되고, 접속 인원은 해가 갈수록 급격히 증가하고 있다. 마약, 아동음란물, 인신매매 등 물리적 공간에서 중대하게 처벌되는 범죄가 암호화된 네트워크를 통해서 이루어지고 있어, 다크웹상의 범죄는 세계적으로도 커다란 문제로 인식되고 있다. 이에 미국·독일 등의 국가와 유로폴 등의 국제기구는 수사력을 강화하기 위해 다크웹 취약점을 파악하기 위한 여러 가지 시도를 해 왔고, 온라인 수색, 잠입수사관 제도 등이 다크웹 범죄를 해결하기 위한 방안으로 제시되고 있다.

본 논문에서는 현 법률체계·기술환경에서 다크웹 범죄를 수사하기 위한 하나의 기법을 연구하였고, 암호화된 프로그램을 이용하여 거래하는 다크웹 범죄자에 대한 단서가 PGP 공개키를 중심으로 서로 연관되어 있음을 확인하였다. 다만, 범죄와 관련된 단서 데이터를 활용하기 위해선 전제 조건으로 개인정보보호를 위한 엄격한 조치가 필요하고, 나아가 내사 및 수사에 이용한 범죄 단서를 향후 다크웹 수사에 활용하기 위해선 개인정보에 대한 자기 결정권과 프라이버시에 대한 기본권 침해라는 논쟁을 불식하기 위해 관련 법규에 대한 개정도 필요하다.

또한 수사관의 업무 효율성 제고 및 수사력 강화를 위해 다크웹 범죄를 검색하고, 단서를 자동수집·분석하며, 범죄수익을 추적할 수 있는 시스템 개발도 이루어져야 할 것이다. 특히 범죄 단서에 대한 연관분석은 정형화된 단서뿐만 아니라 비정형화된 구문 등의 행동 패턴을 분석함으로써 동일 범죄자임을 특정하는 기술 도입도 필요하다.

향후 지속적으로 새로운 수사기법 발굴 및 취약점 분석이 이루어져 범죄자 검거가 증가한다면, 다크웹에서 일어나는 사이버범죄도 감소될 것이다.

참 고 문 헌 (References)

〔1〕 Taejin Chung and Guangmeen Rhee, "Criminal activities in the darkweb : International cooperation and countermeasure". Korean Police Studies Review, 17(1), 213-234, 2018.

〔2〕 Park, Woong Shin and Lee, Kyung Lyul, "A Study on the Darknet Crime Phenomenon and Criminal", New Trends in Criminal Law, 219-256, 2018.

〔3〕 Hamilton Nigel, "The Mechanics of a Deep Net Metasearch Engine", DBLP, 57 Reads, January 2003.

〔4〕 Solomon Jane, https://www.dictionary.com/e/dark-web/ (2015. 5. 6.)

〔5〕 다크웹의 사이버 범죄자들, 모바일로 흩어지고 있다. (보안뉴스, 2017. 10. 27.) https://www.boannews.com/media/view.asp?idx=57728&kind=1

〔6〕 인터넷범죄 온상 된 '다크웹'…韓 접속자 하루 1만6000명 (한국경제, 2019. 7. 30.) https://www.hankyung.com/it/article/2019072984951

〔7〕 다크넷 스캐닝 기술 기반의 정보 수집·분석 발표자료(경찰청 제안, 과기정통부 주관 정부 연구개발(R&D) 과제), 2019.2.20.

〔8〕 유로폴, '비트코인 믹서' 첫 차단…자금세탁방지 속도 붙이나, https://blockinpress.com/archives/17470

〔9〕 한국형사정책연구원 국외출장보고서, "독일 노르트라인베스트팔렌주 경찰청 초청, 사이버범죄 전문가 세미나 참석" P23, 2018. 7. 21. ~ 29.

〔10〕 Orin S. Kerr, Sean D. Murphy, GOVERNMENT HACKING TO LIGHT THE DARK WEB: WHAT RISKS TO INTERNATIONAL RELATIONS AND INTERNATIONAL LAW, 70 Stan. L. Rev. Online 58, 2017.

〔11〕 다크웹에서 가장 큰 시장, '월 스트리트 마켓' 폐쇄하는 데 성공 (보안뉴스, 2019. 5. 6.) https://www.boannews.com/media/view.asp?idx=79263&kind=

〔12〕 Dae Yong Jeong, "A study on the Acceptability of Online Search for Collecting Digital Evidence", Journal of Digital Forensics 12(1), 67-76(10 pages), 2018.6.

〔13〕 최진응, "다크웹상 사이버범죄 정보 유통 현황 및 대응 방안", 「이슈와 논점」, 제1386호, 2017. https://www.nars.go.kr/brdView.do?cmsCd=CM0018&brd_Seq=22024

〔14〕 Hee-Young Park, Zulässigkeit und Grenzen der Online-Durchsuchung zum präventiven Zweck und zur Strafverfolgung, Journal of Law research, Vol 28, P154, 2012.

〔15〕 Soyeon Jeong, "Study on Extra-territorial Seizure of Digital Evidence from Legal Perspective", Journal of Digital Forensics 11(1), 61-71(11 pages), 2017.06.

〔16〕 https://www.darkowl.com/blog/2017/demystifying-the-darknet

〔17〕 https://krebsonsecurity.com/2014/11/feds-arrest-alleged-silk-road-2-admin-seize-servers/

〔18〕 Gyungbin Lee. "A Study on Tor -Hidden Service Server For ensic Case and Tracking Technique", Journal of Digital Forensics 12(1), 37-47(11 pages), 2018.6.

〔19〕 Jinhee Lee, Younggee Hong, Hyunsoo Kwon and JunBeom Hur, "Shedding Light on Dark Korea: An In-depth Analysis and Profiling of the Dark Web in Korea", P28, The 20th World Conference on Information Security Application.

〔20〕 Ju Hee Kim, "Technique for Indentifying Cyber Crime Using Clue", Journal of the Korea Institute of Information Security & Cryptology 25(4), 767-780(14pages), 2015.8.

〔21〕 Lee Dong-Hwan and Pyo Chang-Won, "A Systematic Plan to Collect and Analyze Criminal Intelligence by Police", Korean Institute of Criminology, 7-138(134 pages), p23, 2005.12.

저 자 소 개

김 재 진 (Jaejin Kim)

2010년 8월 : 동국대학교 경찰행정학과 졸업
2016년 1월~현재 : 경찰청 사이버안전과 재직 (경감)
2018년 9월~현재 : 고려대학교 정보보호대학원 석사과정
관심분야 : 사이버수사, 디지털포렌식 등