JDFR
Journal of Data Forensics Research
데이터포렌식연구, 2권 2호, 2025년 12월, 227-245면
Journal of Data Forensics Research, Volume 2, Issue 2, December 2025, Pages 227-245.
https://doi.org/10.12972/JDFR.2025.2.2.6
Print ISSN 3058-9460
Online ISSN 3058-9479

원저

익명네트워크에서 국내 마약 유통구조 분석 및 대응방안

최민영[1], 오소정[2], 김순욱[1], 이정훈[1], 김기범[3]

[1]성균관대학교 과학수사학과 디지털포렌식전공 석사과정
[2]성균관대학교 과학수사학과 디지털포렌식전공 박사과정
[3]성균관대학교 과학수사학과 교수

교신저자: 김기범, freekgb02@gmail.com

요약

다크웹은 마약, 성착취물, 개인정보 등 불법 콘텐츠의 주요 거래 공간이나 익명 통신 구조로 인해 수사기관이 추적하는데 구조적 한계가 존재한다. 특히 한국에서는 다크웹·텔레그램·가상자산이 결합된 마약 유통이 확대되고 있으나, 한국어 기반 다크웹 생태계에 대한 실증 분석은 부족하다. 본 논문은 한국어 다크웹 마약 시장을 대상으로 유통 구조와 조직 네트워크를 분석하고 대응 방안을 제시한다. 분석을 위해 Tor 기반 포럼·마켓에서 한국어 게시판 14개를 식별하고, 마약 판매글·거래 지역·상품명·시세·SNS 계정 등을 자동·수동으로 수집하였다. 이를 I2를 활용하여 네트워크를 분석한 결과, 국내 판매자들은 해외 포럼의 한국어 게시판을 홍보 창구로 활용한 뒤 텔레그램 등 익명 메신저로 구매자를 이동시키는 구조를 보였으며, 343개 텔레그램 계정에서는 대마 중심, 합성마약 중심, 혼합형 조직으로 역할이 분화되고 소수의 허브 계정이 핵심 노드로 기능하는 것이 확인되었다. 이를 바탕으로 국내 마약 유통 구조를 실증적으로 규명하고 수사에 적용 가능한 동일인 식별 및 기술적·정책적 대응 프레임워크를 제안한다.

주제어

다크웹, 범죄수사, 조직범죄, 사회연결망분석, 마약

Open Access

Received: December 11, 2025
Revised: December 31, 2025
Accepted: December 31, 2025
Published: December 31, 2025

Original Article

Empirical analysis of domestic drug distribution structures in anonymous networks and countermeasures

Minyoung Choi[1], Sojung Oh[2], Soonwook Kim[1], Junghun Lee[1], Gibum Kim[3]

[1]Digital Forensic Master's Course, Department of Forensic Science, Sungkyunkwan University, Republic of Korea
[2]Digital Forensic PhD Course, Department of Forensic Science, Sungkyunkwan University, Republic of Korea
[3]Professor, Department of Forensic Science, Sungkyunkwan University, Republic of Korea

Corresponding Author: Gibum Kim, freekgb02@gmail.com

ABSTRACT

The dark web serves as a primary marketplace for illegal content such as drugs, child sexual exploitation materials, and personal information. However, its anonymous communication structure poses structural limitations for investigative agencies attempting to track it. Particularly in South Korea, the drug distribution network combining the dark web, Telegram, and virtual assets is expanding; however, an empirical analysis of the Korean-language dark web ecosystem remains insufficient. This study analyzes the distribution structure and organizational networks of the Korean-language dark web drug market and proposes countermeasures. For analysis, 14 Korean-language boards were identified on Tor-based forums and markets, and data such as drug sales posts, transaction locations, product names, market prices, and SNS accounts were automatically and manually collected. The network analysis using I2 revealed that domestic sellers used Korean-language boards on overseas forums as promotional channels before redirecting buyers to anonymous messengers such as Telegram. Among 343 Telegram accounts, roles were differentiated into cannabis-focused, synthetic drug-focused, and mixed-type organizations, with a small number of hub accounts functioning as core nodes. Based on this, the study empirically identifies the domestic drug distribution structure and proposes an identity resolution and technical–policy response framework applicable to criminal investigations.

KEYWORDS

dark web, criminal investigation, organized crime, social network analysis, drugs

I. 서론

익명네트워크는 IP주소를 은폐하고 다중 경로를 우회하여 통신함으로써 트래픽 경로 추적이 구조적으로 어렵도록 설계된 네트워크 서비스를 의미한다. 이용자의 신원(Identity), 위치(IP), 통신 내용을 추적하기 어렵게 설계된 네트워크 구조가 특징이다[1]. 대표적으로 Tor, I2P, Freenet 등이 있고, 특수한 브라우저를 통해서만 접속이 가능하다. 주소는 일반 웹과 달리 56자 base32 문자열로 구성된 주소체계를 알아야 접속할 수 있다. 이러한 익명성 보장 메커니즘은 표현의 자유를 보호하는 긍정적 효과를 갖는 동시에, 추적 회피를 가능하게 하여 다양한 불법행위의 온상이 되고 있다.

당면적으로 Tor Metric에서 공개한 데이터에 따르면, 한국은 하루 평균 약 4만명이 꾸준히 Tor를 사용하고 있고, 전 세계적으로 4위에 올랐다[2]. 익명네트워크의 특성을 이용하여 정치적 목적이나 이념적 발언이 다수 게시되고, 동시에 마약, 아동성착취물, 분실 신용카드, 여권위조, 살해청부 등 불법정보도 유통되고 있다. 유럽 약물 및 약물 중독 모니터링 센터에 의하면, 설문 응답자의 약 20%가 다크웹을 통한 구매 경험이 있다고 밝혔고, 주요 다크웹 마켓에 등록된 약물의 수는 44,000개 이상에 달하며 다크웹이 마약 밀매의 주요한 플랫폼이 되었다고 발표했다[3]. 최근 서울중앙지검은 국제 다크웹 단속작전는 방법을 활용한 전문판매 다크웹 활동자 4,000여명을 검거하였다[4]. 그 외에도 '랩터(Operation Raptor)'의 일환으로 마약을 재배하는 방법을 공유하고, 판매하에도 2010년 비트코인이 배포되기 시작한 시기부터 다크웹의 범죄활동이 급격하게 증가하면서 수사기관의 검거사례도 계속해서 증가하는 추세이다. 또한 2025년 3월 정부가 발표한 "마약류 관리 시행계획"에 따르면, 전담조직 보강·AI 기술 활용 등 온라인 마약유통에 대한 대응체계 강화한다고 밝혔고, 다크웹 및 가상자산 등 비대면 온라인 유통망이 포함되어 있다[5]. 특히, 경찰은 시도경찰청 마약수사대 전담팀을 확대하여 다크웹 수사 전종 체제를 구축할 정도로 다크웹에서 유통되는 마약 단속에 집중하고 있다[6]. 그러나 다크웹에서 마약범죄는 대부분 익명 SNS, 가상자산 등 비식별 신원체계로 유입되면서 추적에 한계가 있으며, 판매-홍보-조달하는 유통체계, 범죄수익 관리책, 상선 등 전형적인 조직범죄 구조로 운용되면서 결과적으로 상선(Top-Level)을 검거하지 못하면 끊임없이 유통되는 구조이다.

본 연구는 익명네트워크를 기반으로 운영되는 한국어로 운영하고 있는 다크웹 마약 시장의 구조적 특징과 현황을 실증적으로 분석하고, 기술적·정책적 대응방안을 제시하고자 한다. 먼저, 제 2장에서는 다크웹의 개념과 기술적 운용구조를 분석하여 추적수사 한계에 대한 구조적 어려움을 증명하고, 제 3장에서는 한국어 다크웹에서 발생하는 마약범죄를 추적하기 위해서 연계 분석할 수 있는 노드별 유통현황을 살펴본다. 제 4장에서는 분석한 유통현황을 바탕으로 다크웹에서 발생하는 마약범죄 대응방안을 제시한다. 기본적으로 본 연구가 국가·언어 특화형 다크웹 마약 생태계의 실증 데이터를 확보하고, 수사기관이 직면하는 기술적 한계와 구조적 취약성을 극복하기 위한 자료로 활용되기 기대한다.

II. 익명네트워크의 종류와 구동원리 및 주요기술

2.1. 익명네트워크 개념과 추적 한계

2.1.1. 월드와이드웹과 다크웹의 개념

월드 와이드 웹(World Wide Web, WWW)은 접근 방식과 가시성에 따라 크게 표면웹(Surface Web), 딥웹(Deep Web), 다크웹(Dark Web)의 3계층으로 구분된다. 표면웹은 '가시적인 웹(Visible Web)' 또는 '색인화된 웹(Indexed Web)'으로도 불린다. 웹 크롤러에 의해 색인화되어 일반 웹 검색 엔진으로 쉽게 접근할 수 있는 공개 웹페이지를 의미한다. 표면 웹 접근은 데에는 로그인 자격 증명이나 특수 소프트웨어가 필요하지 않다[7]. 대부분의 YouTube 웹사이트, 소셜 미디어 게시물 등이 여기에 해당한다. 그러나 표면 웹은 전체 웹의 약 4% 정도에 불과하다[8]. 딥웹은 '보이지 않는 웹(Invisible Web)' 또는 '숨겨진 웹(Hidden Web)'이라고도 불리며, 검색 엔진에 의해 색인화되지 않는 웹사이트와 데이터를 포함한다[7]. 즉, 딥웹에 접속하기 위해서는 회원가입이나 자격증명을 요구하고, 방문자에 따라 콘텐츠가 동적으로 변화하거나, 유료 결제로 보호되거나, 다른 페이지와 연결되지 않아 고립되어 있다[9]. 딥웹의 대표적인 예시로는 Netflix와 같은 유료 스트리밍 서비스, 온라인 뱅킹, 웹 메일, 회원제 사이트, 그리고 각종 데이터베이스 등이 있다. 또한 의료 기록, 정부 자원, 기업 인트라넷과 같은 사설 네트워크도 포함된다. 다크웹은 일반적인 브라우저로 접근할 수 없으며, 특수 소프트웨어를 통해서만 접근 가능한 익명 네트워크 영역이다[7]. 가장 널리 사용되는 도구는 Tor(The Onion Router) 브라우저로, 일반적인 웹 도메인 대신 .onion 도메인을 사용하여 숨겨진 서비스를 제공한다. 다크웹은 익명네트워크(Anonymous Network)로서 이용자의 신원, 접속 위치, 트래픽을 은폐하기 위해 특수한 라우팅 기법과 암호화 기술을 사용하는 통신 인프라이다[10]. 일반적으로 정보 통제 회피, 프라이버시 보호, 검열 우회 등의 목적으로 활용되며, 구조적 특성상 네트워크 경로가 외부에서 관찰되기 어렵도록 설계되었다[11]. 대표적인 익명네트워크에는 Tor(The Onion Router), I2P(Invisible Internet Project), Freenet 등이 있고, 각각 고유한 아키텍처와 암호화 방식, 라우팅 기술을 기반으로 동작한다[12]. 다크웹은 다중 홉 라우팅(Multi-hop Routing), 계층적 암호화(Layered Encryption), 분산형 인프라(Distributed Architecture), 트래픽 난독화(Obfuscation) 등의 기술을 사용하여 익명성을 보장한다[13].

2.1.2. 다크웹 트래픽 특성

2.1.2.1. 다중 홉 라우팅(Multi-hop Routing)

다중 홉 라우팅(Multi-hop Routing)은 단일 중계 노드가 통신의 전체 경로 정보를 보유하지 못하도록 엔트리(Entry)-중간(Relay)-목적지 구조로 3~6개의 노드를 경유하여 트래픽을 전달하는 방식이다. 각 국의 Entry는 클라이언트 IP주소만 알 수 있고 목적지에 대한 정보는 알 수 없다[14]. 이때, 클라이언트는 무작위 위치에 존재하는 Relay 노드를 말한다. 특정 노드를 식별하여 장악한다고 해도 다크웹 네트워크에 모든 노드를 한번에 장악하지 않는 이상 추적은 어렵다[15].

2.1.2.2. 계층적 암호화(Layered Encryption)

계층적 암호화(Layered Encryption)는 송신자가 다중 홉 라우팅 경로에 포함된 각 중계 노드의 공개키를 이용하여 패킷에 여러 겹의 암호화 계층을 씌운 뒤, 네트워크를 통과하면서 홉마

다 한 층씩 복호화되도록 설계된 방식이다[16]. 클라이언트는 통신을 시작할 때 미리 정의된 수의 중계 노드를 선택하여 경로(Circuit)를 구성하고, 각 홉 사이에는 독립적인 암호화 채널을 설정하여, 어느 하나의 노드도 송신자와 수신자를 동시에 인지하지 못하게 한다[15]. 즉, 송신자는 최종 목적지에서 가장 가까운 노드부터 역순으로 각 노드의 공개키로 암호화를 반복하여 '어니언(onion)' 형태의 계층 구조를 생성한다[17]. 각 노드는 자신에게 해당하는 계층만 복호화하여 다음 홉의 주소와 전달해야 할 암호화된 페이로드(Payload)만을 획득한다. 그 결과, 어떠한 Relay도 경로 상 모든 노드 목록이나 최종 목적지, 송신자의 실제 IP주소, 원본 페이로드 내용을 동시에 식별할 수 없다[15].

2.1.2.3. 분산 인프라(Distributed Architecture)

다크웹에서 운용하는 트래픽은 구조적으로 폐쇄성을 확보하기 위해 분산형 인프라(Distributed Architecture)에 기반하여 운영되며, 네트워크 참여자가 자원을 자발적으로 제공하는 방식으로 유지된다[18]. 분산 구조는 특정 노드나 서버에 의존하지 않기 때문에 서비스 중단 위험을 최소화하고, 동시에 외부로 부터 추적을 회피한다[19]. 대표적으로 Tor의 OnionBalance는 다중 미러링 서비스로 하나의 .onion 주소 뒤에 여러 개의 백엔드 서비스를 병렬로 배치한다. 하나의 공동 서비스로 묶어 이용자에게는 항상 동일한 주소로 접속하게 하지만 실제로는 분산된 여러 서버 중 하나로 연결된다. 서버 트래픽을 분산시키고 단일 서버를 식별하거나 차단하더라도 전체 서비스가 중단되지 않는다. 또한 Ephemeral Onion Service는 주소가 영구적으로 유지되지 않고, 메모리 기반으로 짧은 주기마다 새로 생성된다[20]. 주소가 계속 변하기 때문에 외부에서 식별하거나 블랙리스트 등록과 지속적인 감시가 어렵다. 결과적으로 분산 인프라는 다크웹 네트워크 전체를 단일 대상으로 파악하기 어렵게 만들어 추적은 물론 식별조차도 어렵게 한다.

2.1.2.4. 트래픽 난독화(Obfuscation)

트래픽 난독화(Obfuscation)는 외부 관찰자가 패킷의 목적지, 타이밍, 패턴 등을 기반으로 통신 내용을 추론하거나 송·수신자를 특정하는 것을 방지하기 위한 기술이다[21]. 대표적인 난독화 방식으로는 트래픽 패딩(Traffic Padding), 지연 삽입(Timing Perturbation), 경로 무작위화(Path Randomization), 트래픽 모방(Protocol Mimicking) 등이 있다[22]. I2P와 같이 일부 네트워크의 경우 트래픽을 묶음 단위로 전달하거나 라우팅 경로를 예측 불가능한 방식으로 선택하여 네트워크 흐름에 대한 외부 분석의 정확도를 낮추는 구조를 활용하고 있다. 난독화 계층은 네트워크 상에서 관찰될 수 있는 패킷 특성을 의도적으로 변형하여 사용자 행동을 식별하기 어렵게 한다[23].

2.2. 다크웹 범죄의 역사 및 활용 사례

미 국방부 고등연구계획국(DARPA)이 1969년 세계 최초의 패킷 스위칭 네트워크인 ARPANET을 구축하며 현대 인터넷의 기초를 마련하였다. 1971년에는 스탠퍼드와 MIT 학생들 사이에서 이메일을 통한 마리화나 거래가 이루어지며 온라인 거래가 등장하였다[24]. 1983년에는 ARPANET이 민간 연구용 네트워크인 Internet으로 전환되었고, 같은해 군사용 독립 네트워크로써 MILNET이 분리되었다. 1990년대 중반 미 해군 연구소에서 정보기관의 안전한 통신을 위해 MILNET에 '어니언 라우팅' 개념을 도입했고, 다크웹의 기원이 되었다. 겹층 암호화를 기술적으로 구현하여 통신내용을 보호함으로써 전체 경로를 파악할 수 없도록 설계하였

다[9]. 2002년, Tor 프로젝트가 시작되었고, 2004년에는 오픈소스로 공개되면서 일반 사용자도 접근할 수 있게 되었다. 2006년에는 Tor Project가 비영리 단체로 설립되어 표현의 자유와 프라이버시 보호를 목표로 네트워크를 운영하기 시작했다[25]. 2010년 전후 아랍의 봄 당시에는 정부 검열을 우회하려는 시민들이 익명 네트워크를 적극 활용하면서 다크웹은 정치적 표현의 자유와 망명소로 부상하였고, 접속자 수가 대폭 증가하였다[26].

<Table 1> 아랍의 봄 당시 국가별 인터넷 보급률 및 성장률

국가	2012년 6월 기준 보급률(%)	인터넷 사용자 수(명)
바레인	77.0	961,200
이집트	35.6	29,809,700
요르단	38.1	2,481,900
리비아	17.0	954,300
시리아	22.5	5,069,400
튀니지	39.1	4,196,600
예멘	14.9	3,691,000

초기에 권위주의 국가에서의 검열 회피, 내부 고발자 보호, 언론인의 안전한 취재 활동 등 일명 '표현의 자유'라는 슬로건으로 운영되었다. 그러나 완전한 익명성을 악용하면서 범죄자들에 효과적인 범죄수단으로 활용되었고, 비트코인이 등장한 2010년 이후에는 불법 플랫폼으로 변질되었다. 대표적으로 2011년, Silk Road라는 다크웹 사이트가 개설되어 세계 최초 대규모 다크웹 마약 시장이 되었고, 국제공조 논의를 본격화시키는 계기가 되었다. 2013년 Silk Road가 폐쇄된 이후에도 다양한 후속 시장들이 연이어 등장했으며, 현재는 텔레그램, 시그널 등 보안메신저 기반 유입과 믹싱(Mixing)기술 등 고도화된 익명성 보장 기술과 결합하여 추적을 회피하고 있다.

2.3. 다크웹 범죄 동향

다크웹에서는 크게 불법 물품, 불법 영상물, 서비스형 범죄가 있다. 먼저, 불법 물품 거래는 마켓플레이스에서 마약·무기·위조지폐·신분증 등 각종 금지 물품을 홍보, 판매하고 있다. 불법 영상물은 보통 지인능욕 영상물을 공유하면서 모욕적인 말을 포함하고, 텔레그램 등 보안메신저의 비밀채팅방(일명, 노리방, 성례지방 등)을 통해서 공유되고 있는 불법영상물을 비식별화 없이 업로드하는 형태이다. 서비스형 범죄는 RaaS(Ransomeware-as-a-Service) 형태의 랜섬웨어 제작 및 판매, 해킹 의뢰와 해커 고용 등이 있다. 또한 해킹을 통해 얻은 불법정보를 판매하기도 한다. 다크웹 범죄는 대부분 텔레그램, 왓츠앱 등 또 다른 폐쇄공간에 연계하고 있다. 유입되면서 최종적으로 범죄정보를 소비하는 형태이다. 비트코인이나 모네로와 같은 암호화폐는 믹싱기술을 사용한다. 범죄수익은 암호화폐로 인하여 추적이 어렵고, 다크웹과 보안 메신저는 수사기관의 추적이 원활하지 않다. 특히, 한국어 다크웹은 마약과 아동성착취물, 개인정보 판매 등의 유형이 있고, 보통 유료 회원제로 회원 등급별로 콘텐츠를 제공한다. 또한 포럼에서 활동하는 홍보책, 폐쇄공간으로 인증하여 유입하는 회원 모집책, 인증된 회원들만 관리하는 운영책, 판매책, 자금책 등 전형적인 조직범죄 형태를 이루고 있다.

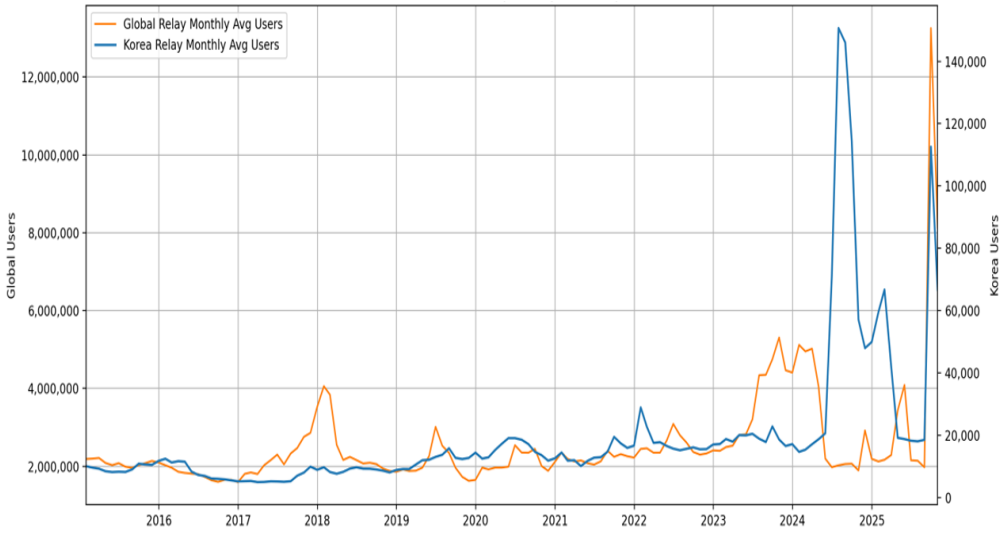
한국어 다크웹은 공유되고 있는 불법 영상물은 아동을 대상으로 하거나 지인을 대상으로 불법 영상물을 촬영하게 하거나 협박, 공갈을 동반한 범죄로 발생하고 있다. 특히, 아동을 대상으

로 하는 불법 영상물 거래는 간단한 인증을 통해 회원이 된 상태에서 사이트에 콘텐츠를 공유하는 방식으로 이루어진다. 지인을 대상으로 하는 경우, 포럼형태로 자연스럽게 대화를 게시글을 올리고, 답글을 다는 형식으로 이미지나 영상물을 공유하고, 보안메신저에 비밀채팅방의 정보를 공유해주는 방식이다. 최근에는 딥페이크 기술을 활용한 허위영상물 또한 증가 추세다.

2.4. 다크웹 사용 현황

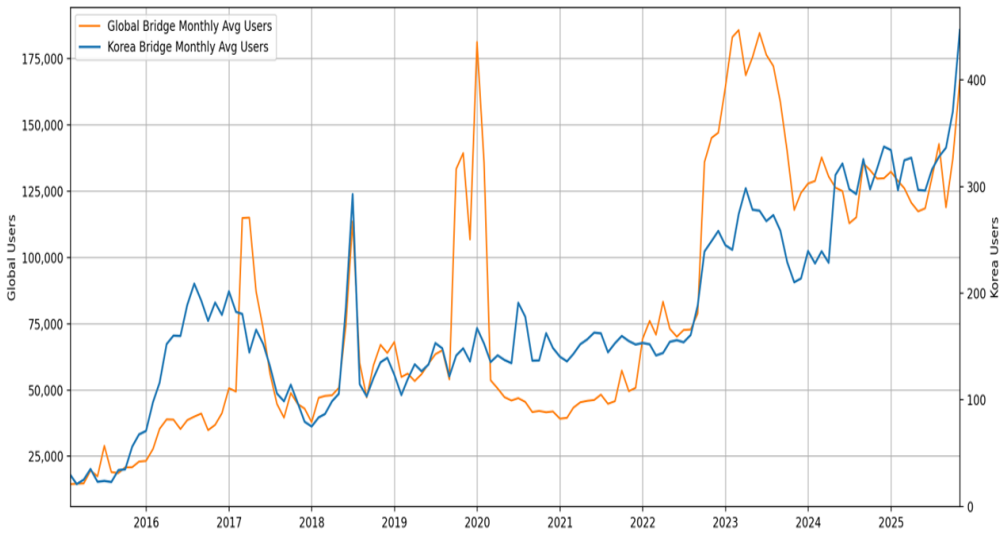
2.4.1. 네트워크 규모 및 접속자 수

Tor 네트워크는 사용자의 인프라를 자원받아 운용하고, 일반 공개 노드를 통해 접속하는 Relay 사용자층과 검열 회피용 비공개 노드에 접속하는 Bridge 사용자층으로 구분된다. 전 세계 Relay 이용자 수는 지난 10년간 연평균 약 255만 명이고, 2025년 기준 월 평균 417만 명으로 증가했다. 2015년 일일 평균 약 209만 명에서 2025년 418만 명으로 두 배 가까이 늘었다. 한국의 Relay 이용자도 2015년 약 9,568명에서 2025년 43,985명으로 약 4.6배 증가했으며, 전 세계 점유율도 0.5%에서 1.3%로 확대되었다.



<Figure 1> 전세계 및 국내 릴레이 접속자 현황(2025년 10월 기준)

Bridge 이용자는 전 세계적으로 2015년 일일 평균 1만 9,642명에서 2025년 13만 809명으로 약 6.7배 증가했고, 한국도 같은 기간 37명에서 334명으로 약 9배 늘어 점유율도 0.19%에서 0.25%로 상승했다. 특히 2018년 obfs4 도입과 2022년 Snowflake 적용 시기에 Bridge 접속 증가가 두드러져 기술 변화가 국내 이용 패턴에도 영향을 미친 것으로 보인다.



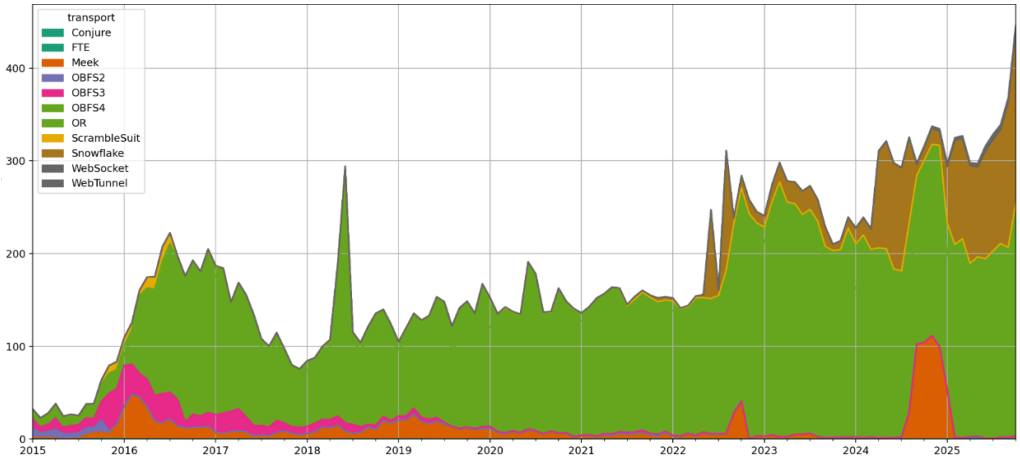
<Figure 2> 전세계 및 국내 브릿지 접속자 현황(2025년 10월 기준)

2.4.2. 사이트 개설 현황

2021년 Tor는 보안 취약점이 드러난 v2 onion 주소 지원을 공식 중단하고, 더 강력한 암호화 알고리즘을 적용한 v3 주소 체계로 전환하였다. 주소 길이도 기존 16자에서 52자로 확대했다. 2021년 11월, Darkow의 자체 플랫폼 조사에서 약 104,095개의 활성 .onion 서비스 중 62%가 여전히 v2 주소였다는 보고가 있었으나, 이후 v3로의 전환이 빠르게 진행되었다[27]. Buitrago López et al. (2024)에 따르면 전체 onion 주소의 약 67%는 주로 활성화된 상태이며, 7%는 간헐적, 나머지는 대부분 비활성이라고 분류하였다[28]. 전체 주소 중 38%는 단 한 번만 관측된 것으로 나타나 일시적 개설과 빠른 이탈 현상이 관찰되었다[29]. Tor Metric에 따르면, .onion 주소 규모는 2021년 연평균 64만 6,474개에서 2025년 85만 9,830개로 약 33% 증가했다[30]. 또한 2025년 하루 평균 약 86만 개의 v3 onion 주소가 존재하고, 2025년 11월 22일 기준 102만 개를 기록하는 등 꾸준히 증가하고 있다.

2.4.3. 한국 사설 서버 이용 현황

국내에서 사설 서버를 경유하여 Tor 접속한 경우, 2015년 일 평균 약 42명에서 2025년 334명으로 증가하며 10년간 약 8배 성장하였다[31]. 초기에는 OBFS2, OBFS3, Meek 등 구형 플러그인 전송(PT)이 주로 사용되었으나 2016년부터 OBFS4가 급격히 확산되었고, 2017~2020년 사이 구형 PT가 사실상 폐기되면서 OBFS4가 전체의 80% 이상을 차지하였다[32]. 이후, 2025년에는 Snowflake가 35.8%까지 성장해 OBFS4(49.6%)와 함께 양강 체제를 형성했다. 다만, 이 수치는 한국 이용자가 다크웹 접속을 위해서 사설 서버를 이용하는 수가 증가한 것이 아니라, 전 세계적으로 검열 심화로 인해 해외 이용자가 한국 서버를 우회 경유지로 활용한 것으로 해석할 수 있다. 한국에 위치한 서버가 우회경로로 활용되는 것은 인터넷 안정성이 높고, 트래픽 처리에 유리하며, Tor 릴레이 운영이 합법적이고 ISP의 간섭도 크지 않기 때문이다. 특히, 한국에서 VPN 서버 운영에 대한 정책적인 제약이 거의 없다는 점도 무시할 수 없다.

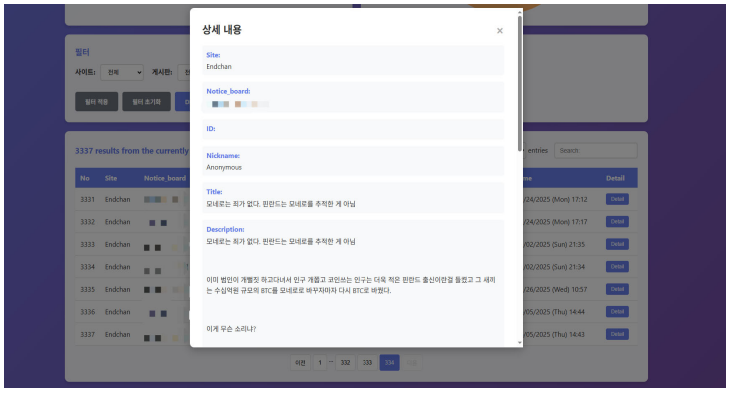


<Figure 3> 프로토콜별 한국 사설 서버 사용 접속 현황(2025년 10월 기준)

III. 한글 다크웹의 마약 유통 실태 분석

3.1. 데이터 수집 및 분석 방법

이 실험은 한국어로 운영되는 다크웹(이하 한글 다크웹)에서 유통되는 마약 실태와 구조를 분석하고, 수사기관의 정보기반 의사결정 체계를 지원하는데 목적이 있다. 다크웹은 구조적인 특성으로 인하여 표면 웹 조사 방식보다는 체계적 · 수동적으로 탐색하는 접근법이 요구된다[33]. 데이터는 2025. 3. 5. ~ 2025. 10. 5. 기간 동안 한국어로 운영되는 마약 다크웹 16개를 사용하였다. 이 중 현재 서버가 비활성화되어 있는 사이트 1개와 포럼 2개는 제외하여 총 13개 사이트를 설정하고 크롤링 기술을 통해 데이터를 수집하였다. 데이터는 텍스트만 총 3,337개 라인을 수집하였고, 용량은 10.9MB에 이른다. 마약 유통 체계는 수집 기간 동안 게시물 모니터링을 통해서 확인하였고, 연관성 분석을 위해 시각화 도구(I2 10.1 버전)로 수집한 데이터로부터 조직을 식별하거나 각 사용자들간 연계 분석이 가능한 요소로써 마약 홍보글로부터 지역 정보, 텔레그램 계정, 업로드 닉네임 등을 추출하였다.



<Figure 4> 수집한 데이터 데이터베이스 화면

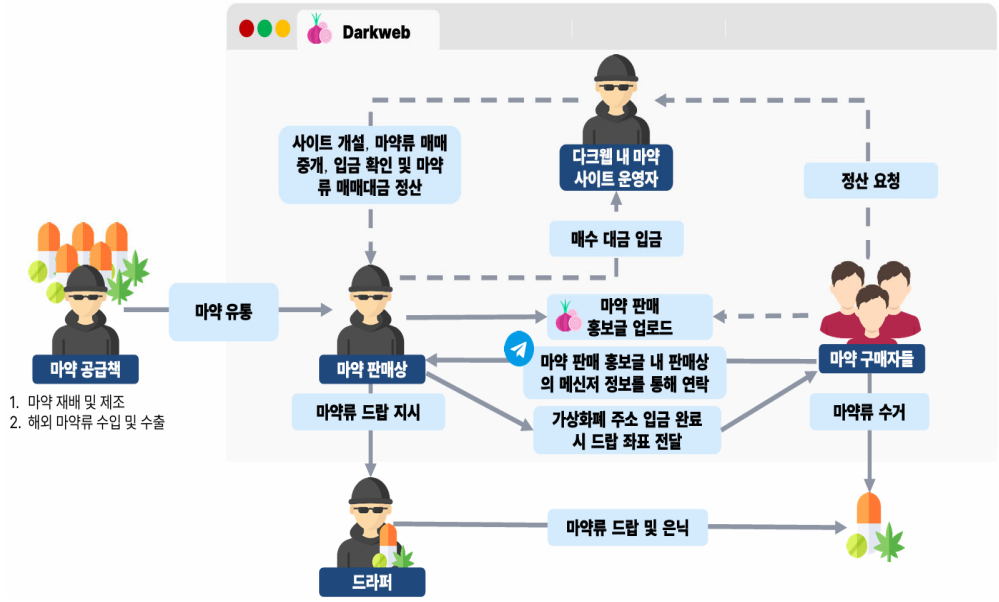
3.2. 다크웹 마약 데이터 유통 체계 분석

3.2.1. 사이트 운영 형태

한글 다크웹은 독자 사이트를 개설하는 것이 아니라 국내·외 운영자들이 개설한 대형 포럼에서 일부 사용료나 협력사항을 정하여 하위에서 게시판 형태로 운영한다. 이 구조는 유럽, 미국 등의 해외정부에서 다크웹 마켓을 운영하는 형태와도 일치한다[3]. 한글 다크웹은 활동 규칙이 존재하였고, 게시하는 형태나 공유하는 정보는 제한이 없었다. 일부 게시판은 “정치적 내용, 불법 저작권 자료 공유, 마약 판매 홍보는 허용하되 아동 성착취물은 공유를 금지”하는 정책을 갖고 운영하고 있다. 대형 다크웹 포럼이 자율 규제적 운영 규칙을 채택해 불법성 수준을 운영자가 판단해 차별화한다는 의미이며, 해외와 유사한 형태를 보인다[34]. 예상컨대, 국내에서 대규모 암시장을 구축할 때 발생하는 위험성과 기술적인 부담을 해외 서버 등에 배분함으로써 회피하기 위한 전략으로 보인다.

3.2.2. 유통 조직 구조

국내 마약 유통은 상선이 해외 등지에서 마약을 반입하여 모집-유통-자금관리-홍보 등의 철저한 역할 분담과 피라미드 구조로 움직인다. 플랫폼 운영자(관리자·모더레이터)가 시장 질서를 관리하면서 지시한다. 상위 벤더(Vender)는 지시에 따라 마약 판매 및 홍보를 담당하고, 다수의 구매자를 상대한다. 이후 마약은 운반책 및 드랍퍼(Dropper)를 통해 지정된 장소에 전달되며, 구매자는 가상화폐로 거래 대금을 지급한다. 물류·에스크로·암호화폐 세탁이 외부 인프라를 통해 수행된다[3].



<Figure 5> 한국 마약 유통 체계

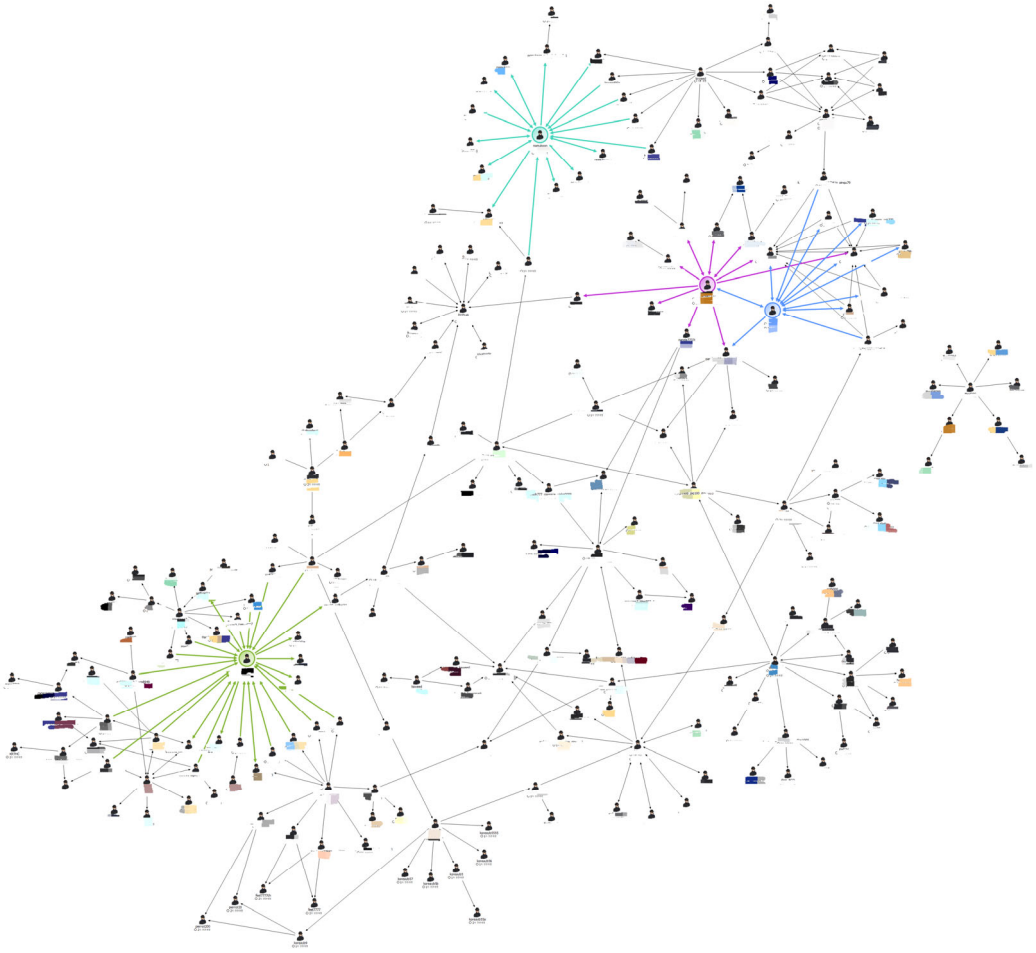
다만, 해외 마약 전문 판매 다크웹은 애스크로를 도입한 반면 한글 다크웹은 게시판 형태로 소규모로 홍보하고 텔레그램, 시그널 등의 보안 메신저로 유입된다. 보안메신저에서 또 다시 홍보방, 공지방, 인증방, 사기제보방, 1:1 비밀대화방 등의 형태로 분담화된 채널들을 관리하면서 조직 형태로 운용하고 있다.

3.3. 유통 마약 데이터간 연관성 분석

3.3.1. 계정간 연관성 분석

한글 다크웹 판매 게시글에서 1차적으로 식별한 텔레그램 ID는 7개이다. 이를 출발점(seed)로 설정한 후 텔레그램 플랫폼의 검색엔진을 이용해 결과로 나온 계정을 1차적으로 수집하고, 연결된 계정을 2차적으로 수집하여 총 343개의 계정을 확보하였다. 각 계정의 관계도를 시각화하기 위해 수집된 출발점 계정과 1차·2차 연관계정을 모두 엔티티로 설정한 후 계정 간 연결관계를 엣지로 구성하여 연관성 네트워크를 생성하였다.

분석결과, 마약 판매 네트워크는 소수 핵심 계정(허브)을 중심으로 다수의 주변 계정에 연결되는 구조를 보여주었다. 이때, 파란색 허브와 보라색 허브는 서로 연결되어 있는데, 두 계정 모두 주변에 대규모의 1차 노드(홍보, 모집 계정)를 보유하고 있었다. 이러한 구조는 동일 조직의 상위 운영 계정이거나 서로 다른 범죄 운영 채널을 연결하는 조정 계정임을 시사한다. 또한 네트워크 하부에 특정 허브와 연결된 일회성·저신뢰도의 소규모 계정(leaf accounts)이 광범위하게 분포하고 있었고 대부분 홍보 또는 유입 유도 기능을 수행하는 것으로 해석된다. 일부 계정은 다른 판매자를 사기로 지목하거나('사기꾼 박제방') 경쟁자를 공격하는 메시지를 발송하는 등 평판 경쟁(reputation warfare) 형태의 행동도 관찰되었다.



<Figure 6> 다크웹-텔레그램 연관성 분석

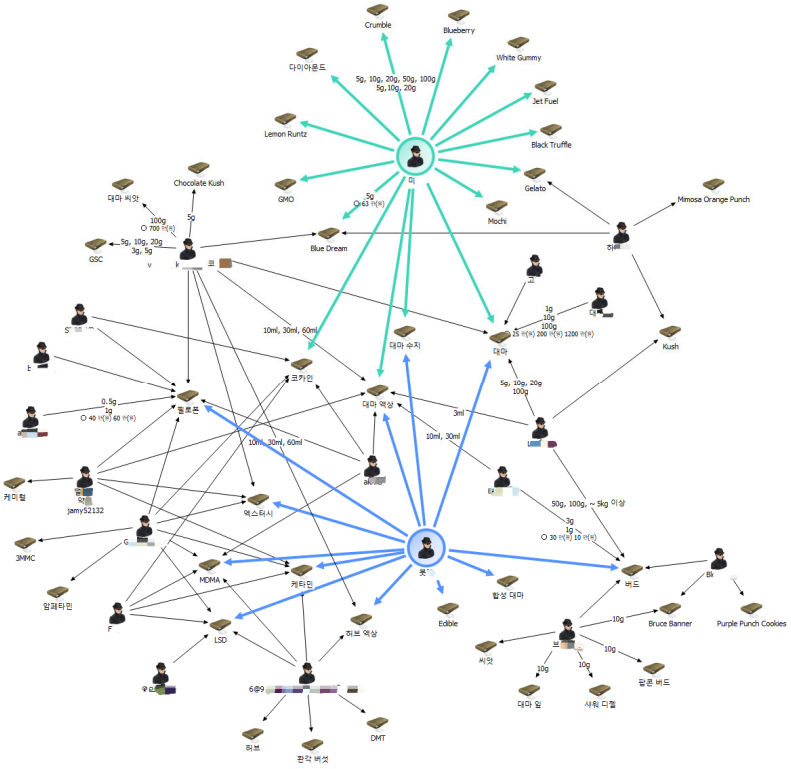
전체 계정 중 소수의 핵심 허브 계정이 네트워크 중심적 연결 구조를 형성하고 있는 점은 조직의 통제권이 다수의 주변 계정이 아닌 극소수의 상위 운영 계정에 집중되어 있음을 보여준다. 허브 계정을 식별·무력화하면 조직 전체의 붕괴를 가져올 수 있을 것이다.

3.3.2. 마약 판매 시세 및 용어 연관성

다크웹 판매 홍보 게시글 전체를 대상으로 사용자 닉네임, 메신저 ID, 상품명, 용량 단위, 품종명, 판매 시세와 약물의 종류, 용량 구조, 게시글에서 사용된 마약 은어를 1차적으로 분류하였다. I2에서 시각화를 진행하기 위해 사용자 정보와 취급 마약 종류를 엔티티로 설정하고, 판매 용량을 링크 속성으로 부여하여 계정과 약물간 연관성 네트워크를 구성하고 계정별 취급 약물군의 전문성 및 도·소매 여부와 용어 사용 패턴의 유사성을 분석하였다.

분석결과, 주요 계정간 대마 등 마약류 전문 조직(초록색), 합성마약 중심 조직(파란색), 양쪽을 연결하는 혼합 취급 계정으로 구분되는 조직적 패턴이 확인되었다. 이 중, 계정명 '미O'는 Blueberry, White Gummy, Jet Fuel, Crumble, Gelato, GMO 등 대마 품종 중심의 상품군이 집중적으로 연결되어 있었다. 또한 이 계정이 취급하는 거래 용량은 5g, 10g, 20g, 50g, 100g 등 도·소매를 모두 포함하고 있었다.

해석컨대, '미O'가 다수의 대마 품종을 국내에 안정적으로 공급할 수 있는 도매책 혹은 총판급 판매자 역할을 수행하고 있다고 할 수 있다. 계정 '붓O'는 LSD, MDMA, 케타민 등 주로 합성마약 및 정신작용제 중심의 약물군과 연결되어 있다. 이는 다크웹 내 합성마약 전문 판매 조직의 핵심 허브로 기능하고 있음을 보여준다. '코OD'의 경우, 대마류와 합성류가 모두 언급되었고, 마약 유통 네트워크에서 마약류 전문 조직과 합성마약 중심 조직의 허브로서 역할한다고 할 수 있다.

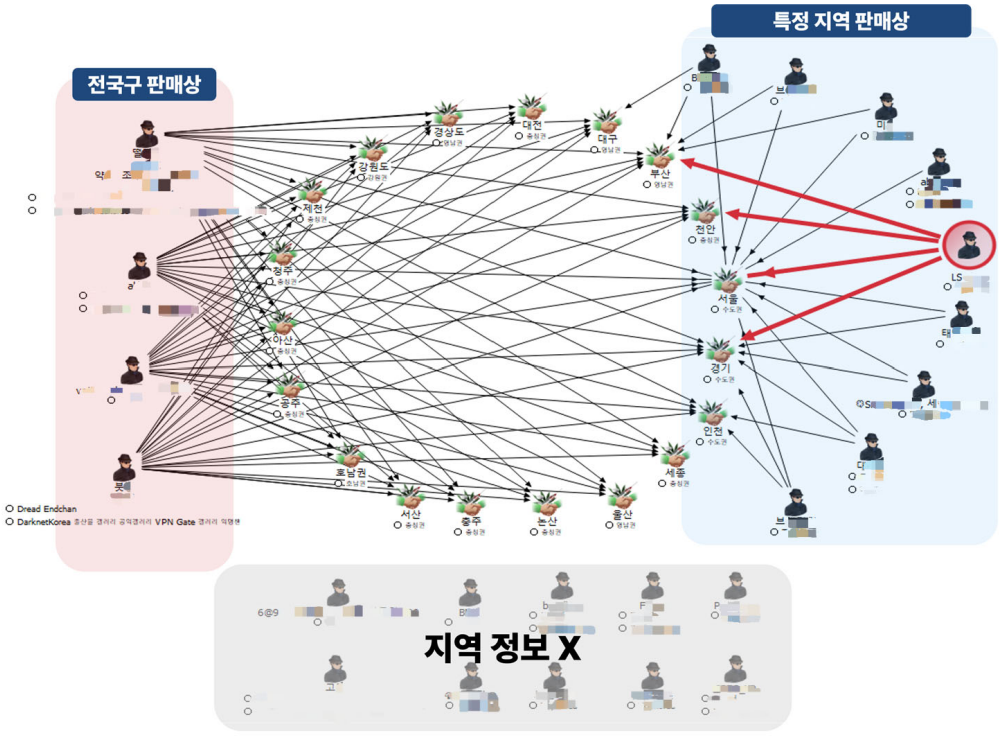


<Figure 7> 취급 마약류 및 시세 연관성 분석

3.3.3. 거래 지역 연관성

한글 다크웹에서 수집된 마약 판매 데이터 간 구조적 연관성을 분석하기 위해서 데이터 전처리, 엔티티 정의, 관계 설정의 3단계 분석 절차를 적용하였다. 먼저 판매 홍보 게시글을 전체 수집한 뒤 텍스트를 분석하여, 판매자가 배송 또는 거래 가능 지역을 명시한 게시글을 분류하였다. 이 과정에서 게시글에 포함된 닉네임, 메신저 ID를 기준으로 동일 사용자를 식별하였고 사용자 정보와 판매 지역을 각 엔티티로 정의하여 네트워크를 구성하였다.

분석결과, 제주를 제외하고 전국 거래가 가능한 게시자는 전체 23명 중 4명이었으며, 이중에서도 '약사'와 '붓다' 계정은 가장 넓은 활동 범위와 가장 높은 게시 빈도를 보였다. 수도권(서울, 경기, 인천)을 제외한 지역 중 가장 많이 언급된 지역은 부산으로 나타났다. 부산은 물류 중심지로서 마약 판매자들이 직접 마약을 반입하기에 유리한 지역적 특성을 갖고 있다. 이러한 특성은 불법 정보 판매자들이 물리적 위험을 분산하기 위해 물류 접근성이 좋은 지역을 중심으로 활동 범위를 설정하는 전형적인 마약 유통 패턴과 유사하다[35].



<Figure 8> 지역정보 연관성 분석

3.4. 시사점 및 한계

다크웹은 표현의 자유를 보장하고 검열 회피를 목적으로 설계된 익명 네트워크이나 기술적 특성이 범죄자에게 구조적으로 유리한 환경을 제공하게 되었다. 표면웹에서는 정상적인 콘텐츠를 위장한 취업 사기, 로맨스 스캠 등 미끼형 게시글 중심의 범죄 양상이 나타나지만, 다크웹은 게시된 정보 자체가 불법 거래를 전제로 생성되는 경우가 대부분이다. 특히, 개인정보, 불법 영상물, 마약 등 불법정보가 거래되고 역할 분담과 기능적 분화를 전제로 하는 전형적인 조직형·네트워크형 범죄 양상을 띄고 있다. 해외에서는 에스크로 시스템을 도입하여 온라인 쇼핑몰 형태를 갖추고 있지만 국내의 경우, 전문적인 판매 사이트보다는 포럼형 사이트에서 단일 게시

글에서 SNS 링크로 유입하는 다단계 형태를 보인다. 다단계 유입 방식은 거래 과정에서의 접점을 분산시키고 플랫폼 간 이동을 반복하게 하여 행위자에 대한 신원 추적을 어렵게 만드는 요인으로 작용한다. 따라서 다크웹 상에서 확보할 수 있는 데이터를 활용하여 추적 단서로 정의해야 한다. 마약범죄에서 확보할 수 있는 데이터는 조직(계정)마다 차이를 보이는 마약의 시세, 종류, 용어, 거래지역이 될 수 있고, 각 단서들을 연관분석하면 계정간의 연관성도 확인할 수 있다. 다크웹에서 활동하는 사람들의 익명성을 해제하기 위해서는 계속해서 추적할 수 있는 단서로 대입하여 범죄추적에 활용하는 노력이 필요하다.

IV. 다크웹 마약 유통에 대한 기술적·정책적 대응방안

4.1. 허브 계정 중심의 수사 전략

국내에서 다크웹을 통한 마약 유통은 보통 SNS 링크로 유인한 후, 홍보방으로 유입되면 또 다른 계정들이 식별되며 본격적인 판매, 구입이 이루어진다. 즉, 다크웹에서 활동은 조직에서 홍보를 담당하는 소수의 핵심 계정만 발생한다. 다크웹의 허브계정과 sns에서 식별되는 다수의 주변계정들간의 연관성을 파악하면 영향력이 파악되어 조직관계가 식별된다. 이것은 홍보·모집 기능을 수행하는 다수의 주변 계정과 실제 통제 기능을 수행하는 상위 운영 계정이 분리되는 구조를 식별할 수 있다. 특히, 조직의 실질적 통제권은 극소수의 허브 계정에 집중되어 있다. 하위 판매자나 홍보 계정이 반복적으로 생성·소멸되는 반면 허브 계정은 다수의 연결 관계를 유지하며 조직의 지속성을 보장하는 역할을 수행하기 때문이다. 따라서 다크웹 마약 범죄에 대한 효과적인 대응을 위해서는 단편적 사건 처리 중심의 수사 방식에서 벗어나 네트워크 구조 분석을 통해 핵심 허브 계정을 선별적으로 식별 및 무력화하는 전략이 필요하다. 다크웹 게시판, 보안 메신저, 가상자산 주소 등 다양한 플랫폼에 분산된 정보를 통합적으로 분석할 수 있는 체계를 구축할 필요가 있다. 허브 계정은 다수의 계정과 반복적으로 연결되므로 연관성 분석을 기반으로 한 표적 수사는 조직 전체 식별을 기대할 수 있다.

4.2. 활동 조직별 은어 사전(Dictionary) 구축

다크웹 마약 범죄는 온라인 공간에서 이루어지지만 실제 범죄 행위는 특정 지역을 기반으로 한 오프라인 유통·전달 과정과 밀접하게 연결되어 있다. 판매 게시글에 포함된 거래 가능 지역, 배송 방식, 은어로 표현된 장소 정보 등은 사이버 공간상의 활동이 물리적 공간과 연계되어 있음을 보여준다. 지리적 정보와 계정 활동을 결합한 공간 연관성 분석은 조직의 활동 범위와 거점 지역을 식별하는 데 기여할 수 있으며 특정 계정이나 조직이 반복적으로 언급하는 지역이나 유사한 배송·거래 패턴이 나타나는 공간적 범위는 조직의 물류 동선이나 활동 거점을 추정할 수 있는 단서로 작용한다. 이는 다크웹 마약 범죄를 단순한 온라인 거래가 아닌 온라인과 오프라인이 결합된 복합적 범죄 구조로 인식하고 대응 전략을 설계하는 데 중요한 기반이 된다.

다크웹과 보안 메신저 환경에서는 마약 거래를 은폐하기 위해 조직별·약물별로 상이한 은어와 변형어가 지속적으로 사용된다. 이러한 은어는 일반적인 키워드 차단이나 단순 검색 기반 수사 기법을 우회하기 위한 수단으로 활용되며 동일 조직 내부에서는 비교적 일관된 용어 체계를 유지하는 경향을 보인다. 따라서 조직별로 사용되는 은어와 그 변형 양상을 체계적으로 정리한 사전(Dictionary) 구축은 다크웹 마약 범죄 탐지와 분석의 정확도를 높이는 데 필수적이다. 기존 연구에서도 마약 범죄자들이 단속을 회피하기 위해 일반어, 은어, 그리고 은어의 변형어를 혼합하여 사용하는 경향이 확인되었으며, 이러한 키워드를 체계적으로 수집·분류하는 것이 마

약 범죄 추적에 효과적이라는 점이 제시된 바 있다 [36]. 특히 은어는 플랫폼과 조직에 따라 빠르게 변화하므로 고정된 키워드 목록이 아닌 지속적으로 갱신 가능한 은어 사전의 구축이 필요하다. 지리적 연관성 분석과 조직별 은어 사전을 결합할 경우 특정 지역에서 활동하는 조직의 언어적 특성과 활동 패턴을 함께 분석할 수 있다. 이는 단순히 게시글을 식별하는 수준을 넘어, 조직 간 구분과 역할 분화, 활동 영역의 중첩 여부를 파악하는 데에도 활용될 수 있다. 결과적으로 이러한 분석 체계는 다크웹 마약 범죄를 보다 입체적으로 이해하고, 조직 단위의 대응 전략을 수립하는 데 기초 자료로 기능할 수 있다.

4.3. 자동화기반 다크웹 추적노드 발굴 체계 구축

다크웹 마약 범죄는 단일 계정이나 특정 플랫폼에 고정되지 않고 다수의 사이트와 보안 메신저, 가상자산을 활용한다. 이는 장기간에 걸쳐 운영되는 특성을 가지기 때문에 단기간 관찰만으로는 전체 조직 구조를 파악하는데 한계가 존재한다. 특히 텔레그램 계정, 가상자산 지갑 주소, 게시글 간 링크 구조와 같이 핵심 요소는 여러 플랫폼에 분산되어 있어 이들 간의 연관성을 파악하기 위해서는 지속적인 데이터 수집은 필수적이다. 그러나 이러한 작업을 사건 단위의 수작업에 의존할 경우 시간적·인적 자원의 제약으로 인해 전체 네트워크를 포괄적으로 분석할 때 어려움을 가진다. 때문에 자동화 된 방식으로 추적 노드를 지속적으로 발굴·관리할 수 있는 체계가 구축되어야 한다. 자동화된 크롤링과 상시 데이터 수집을 통해 다크웹 게시글, 계정 정보, 외부 플랫폼 연계 정보를 확보하고 이를 기반으로 연관성 분석을 수행할 경우, 조직 구조의 변화와 확장을 장기적으로 추적하는 것이 가능해진다. 이러한 접근은 단기적인 검거 성과보다는 범죄 네트워크의 해체를 목표로 하는 전략적 수사에 적합하다. 또한 다크웹 데이터는 접근성과 안정성이 낮고, 전체 네트워크 구조를 파악하기 위한 연계 정보 확보에 상당한 시간이 소요되는 특성을 가진다. 따라서 다크웹 환경에 대한 이해를 전제로 장기간 동일 영역을 추적할 수 있는 전담 분석 조직의 필요성도 함께 고려되어야 한다. 전담 조직이 지속적으로 데이터를 수집·정제·분석하는 구조가 마련될 경우, 일회성 대응이 아닌 상시적 감시와 누적 분석이 가능해진다. 결과적으로 자동화된 추적 노드 발굴 체계와 이를 전담하는 분석 조직이 구축될 경우 수사기관은 다크웹 마약 범죄를 개별 사건이 아닌 지속적으로 진화하는 조직 범죄 현상으로 인식하고 대응할 수 있다.

V. 결론

다크웹 마약 범죄는 익명 네트워크 기반의 IP 은폐와 비식별 주소체계, 보안 메신저와 가상자산의 결합으로 인해 전통적인 수사 방식만으로는 범죄 구조를 파악하는 데 한계가 있다. 이러한 환경에서는 개별 판매자나 단일 사건 중심의 대응이 반복되는 범죄를 근본적으로 차단하기 어렵고 범죄를 지속시키는 조직 구조 자체를 분석 대상으로 삼을 필요가 있다.

한글 사용 다크웹을 중심으로 관찰한 결과 마약 거래는 독립적인 개인 행위라기보다 역할이 분화된 조직 구조를 통해 운영되고 있었다. 판매, 홍보, 의사소통, 자금 관리가 분리되어 이루어지며 소수의 핵심 계정이 다수의 주변 계정과 연결되는 네트워크형 구조가 확인되었다. 이러한 구조에서는 하위 계정이 빈번히 교체되더라도 조직의 통제 기능은 유지되는 경향을 보였으며 개별 판매자 단속 중심 접근의 한계를 뚜렷하게 보여준다. 연관성 분석을 통해 다크웹 마약 범죄 조직은 약물군별 전문화, 유통 구조, 시세 형성 방식에 따라 기능적으로 분화된 네트워크형 조직임이 확인되었다. 일부 조직은 전통적 범죄조직이 온라인 환경에 적응한 형태를 보이는 반

면, 다른 조직은 느슨하게 결합된 네트워크 구조로 운영되며 플랫폼 이동과 계정 변경을 통해 지속성을 확보하고 있었다. 이러한 특성은 범죄 대응 전략이 개별 행위자 식별을 넘어 조직 구조 전체를 대상으로 설계되어야 함을 시사한다. 이에 따라 다크웹 마약 범죄 대응은 허브 계정을 중심으로 한 구조적 수사 전략으로 전환될 필요가 있다. 지갑 주소, PGP 키, 보안 메신저 계정과 같이 변경이 어려운 식별 노드를 지속적으로 발굴하고 이를 연계 분석함으로써 조직의 운영 구조와 책임 주체를 규명하는 접근이 요구된다. 또한 비정형 데이터와 은어 중심의 표현이 지배적인 다크웹 환경의 특성을 고려할 때, 자연어 처리(NLP)와 자동화된 분석 기법을 활용한 데이터 세분화와 구조화는 수사의 효율성과 지속성을 제고하는 핵심 요소가 된다.

다만 이러한 분석은 특정 시점에 수집된 한글 다크웹 데이터를 중심으로 이루어졌다는 점에서, 조직 구조의 장기적 변화와 진화 양상을 충분히 반영하지 못한 한계를 가진다. 또한 공개적으로 접근 가능한 정보에 기반한 분석에 한정되어 폐쇄형 커뮤니티나 비공개 보안 메신저 내부의 의사소통과 자금 흐름까지 포괄적으로 규명하는 데에는 제약이 존재한다. 다크웹 데이터의 비정형성과 은어 사용 특성으로 인해 일부 해석 과정에서 분석자의 판단이 개입될 가능성 역시 배제할 수 없다.

향후 분석 대상을 한글 사용 다크웹에 국한하지 않고 한국인이 활동하는 해외 다크웹 마켓과 다국어 플랫폼까지 확장함으로써 국제적 연계 구조를 보다 입체적으로 분석할 필요가 있다. 마약조직의 실체를 보다 체계적으로 규명하고 효과적인 수사전략·기술·정책 개발에 기초자료로 활용되기 기대한다.

참고문헌 (References)

[1] Meng X, Liang M. 2023. Port-based anonymous communication network: an efficient and secure anonymous communication network. Sensors, 23(21), 8810. https://doi.org/10.3390/s23218810

[2] TorMetric. [n.d.]. Users. TorMetrics. Available at: https://metrics.torproject.org/ accessed on 2025. 12. 10.

[3] European Monitoring Centre for Drugs and Drug Addiction, Europol. 2017. Drugs and the darknet: Perspectives for enforcement, research and policy. Publications Office of the European Union, Luxembourg. pp.1-90. https://doi.org/10.2810/783427

[4] Suk GM. 2025. Whole family involved in marijuana sales: Drug platform with 4,000 members busted [온가족이 대마 장사…가입 4000명 마약플랫폼 일망타진]. The JoongAng. Available at: https://www.joongang.co.kr/article/25339394 accessed on 2025. 12. 10.

[5] Office for Government Policy Coordination. 2025. 2025 implementation plan for narcotics management (press release) ['25년도 마약류 관리 시행계획 보도자료]. Korea Policy Briefing. Available at: https://www.korea.kr/briefing/pressReleaseView.do?newsId=156677587 accessed on 2025. 12. 10.

[6] Lee DH. Police launch online narcotics investigation task force to break distribution chains [경찰, 온라인 마약 수사전담팀 출범…유통 고리 깬다]. Yonhap News Agency. Available at: https://www.yna.co.kr/view/AKR20250329047300004 accessed on 2025. 12. 10.

[7] Kaur S, Randhawa S. 2020. Dark web: A web of crimes. Wireless Personal Communications, 112(4), 2131-2158. https://doi.org/10.1007/s11277-020-07143-2

[8] Elangovan R. 2020. The dark web: Hidden access to internet today. In: Khosrow-Pour M, editor. Encyclopedia of criminal activities and the deep web, 3rd ed, pp. 129-139. IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-5225-9715-5.ch008

[9] Tubaishat A, Maramara AR. 2023. Security issues in the deep and dark web: What to know? Proceedings of the 2023 12th International Conference on Software and Information Engineering (ICSIE 2023), Sharm El-Sheikh, Egypt, pp. 93-96. https://doi.org/10.1145/3634848.3634849

[10] Park H, Yun W, Park J. 2023. A study on traces of I2P anonymous network usage in windows. Journal of Digital Forensics, (17)4, 95-107. http://doi.org/10.22798/KDFS.2023.17.4.95

[11] Shen T, Jiang J, Jiang Y, et al. 2022. DAENet: Making strong anonymity scale in a fully decentralized network. IEEE Transactions on Dependable and Secure Computing, (19)4, 2286-2303. https://doi.org/10.1109/TDSC.2021.3052831

[12] Shirvani MH, Akbarifar A. 2021. A comparative study on anonymizing networks: TOR, I2P, and Riffle networks comparison. Journal of Electrical and Computer Engineering Innovations, 10(2), 259-272. https://doi.org/10.22061/JECEI.2021.8027.466

[13] Aminuddin MAIM, Zaaba ZF, Singh MKM, et al. 2018. A survey on Tor encrypted traffic monitoring. International Journal of Advanced Computer Science and Applications, 9(8), 113-120. https://doi.org/10.14569/IJACSA.2018.090815

[14] Mccoy D, Bauer K, Grunwald D, et al. 2008. Shining light in dark places: Understanding the Tor network. Proceedings of the 8th International Symposium on Privacy Enhancing Technologies, Berlin, Heidelberg, Germany, pp. 63-67. https://doi.org/10.1007/978-3-540-70630-4_5

[15] Dingledine R, Mathewson N, Syverson P. 2004. Tor: The second-generation onion router. Proceedings of the 13th USENIX Security Symposium, San Diego, USA, pp. 1-18.

[16] Kelen DM, Seres IA, Béres F, et al. 2023. Integrated onion routing for peer-to-peer validator privacy in the ethereum network. MTA SZTAKI ILAB, pp. 1-11.

[17] Reed MG, Syverson PF, Goldschlag DM. 1998. Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 16(4), 482-494. https://doi.org/10.1109/49.668972

[18] Johnson A, Wacek C, Jansen R, et al. 2013. Users get routed: Traffic correlation on Tor by realistic adversaries. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, pp. 337-348. https://doi.org/10.1145/2508859.2516651

[19] Sucu C. 2015. Tor: Hidden service scaling. Master's thesis. University College London, London, UK.

[20] Höller T, Roland M, Mayrhofer R. 2022. Evaluating dynamic Tor onion services for privacy preserving distributed digital identity systems. Journal of Cyber Security and Mobility, 11(2), 141-164. https://doi.org/10.13052/jcsm2245-1439.1122

[21] Raymond JF. 2001. Traffic analysis: Protocols, attacks, design issues, and open problems. In: Federrath H, editor. Designing privacy enhancing technologies. Lecture notes in computer science, vol 2009. pp, 10-29. Springer. https://doi.org/10.1007/3-540-44702-4_2

[22] Cai X, Nithyanand R, Wang T, et al. 2014. A systematic approach to developing and evaluating website fingerprinting defenses. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, USA, pp. 227-238. https://doi.org/10.1145/2660267.2660362

[23] Egger C, Schlumberger J, Kruegel C, et al. 2013. Practical attacks against the I2P network. Proceedings of the 16th International Symposium on Research in Attacks, Intrusions, and Defenses - Volume 8145, Rodney Bay, St. Lucia, pp. 432-451. https://doi.org/10.1007/978-3-642-41284-4_22

[24] Markoff J. 2006. What the dormouse said: How the sixties counterculture shaped the personal computer industry. Penguin Books.

[25] Sultana J, Jilani AK. 2021. Exploring and analysing surface, deep, dark web and attacks. In: Bhardwaj A, Sapra V, editors. Security incidents & response against cyber attacks, pp. 97-108. EAI/Springer Innovations in Communication and Computing, Springer. https://doi.org/10.1007/978-3-030-69174-5_5

[26] Fekete E, Warf B. 2013. Information technology and the "Arab Spring". Arab World Geographer, 16(2), 210-227.

[27] Dark Owl. [n.d.]. Tor v2 deprecation shifts darknet landscape. Dark Owl. Available at: https://www.darkowl.com/blog-content/tor-v2-depreciation-shifts-darknet-landscape/ accessed on 2025. 12. 10.

[28] Buitrago López A, Pastor-Galindo J, Gómez Mármol F. 2024. Updated exploration of the Tor network: Advertising, availability and protocols of onion services. Wireless Networks, 30, 7527-7541. https://doi.org/10.1007/s11276-024-03679-4

[29] Höller T. 2021. V3 onion service usage. Tor Blog. Available at: https://blog.torproject.org/v3-onion-services-usage/ accessed on 2025. 12. 10.

[30] Tor Metrics. 2026. Users. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2021-01-01&end=2025-12-31&country=kr&events=off accessed on 2025. 12. 10.

[31] Tor Metrics. 2026. Users. Available at: https://metrics.torproject.org/userstats-relay-country.html?start=2021-01-01&end=2025-01-12&country=kr&events=off accessed on 2025. 12. 10.

[32] Tor Metrics. 2026. Unblocking Tor. Available at: https://support.torproject.org/tor-browser/circumvention/unblocking-tor/?utm_source accessed on 2025. 12. 10.

[33] Décary-Hétu D, Giommoni L. 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change, 67, 55-75. https://doi.org/10.1007/s10611-016-9644-4

[34] Barratt MJ, Lenton S, Allen M. 2013. Internet content regulation, public drug websites and the growth in hidden Internet services. Drugs: Education, Prevention and Policy, 20(3), 195-202. https://doi.org/10.3109/09687637.2012.745828

[35] Demant J, Munksgaard R, Décary-Hétu D, et al. 2018. Going local on a global platform: A critical

analysis of the transformative potential of cryptomarkets for organized illicit drug crime. International Criminal Justice Review, 28(3), 255-274. https://doi.org/10.1177/1057567718769719

[36] Lee Y, Lee S, Kim G, et al. 2023. Analysis of the relationship between cybercrime incidence and space - Using spatial regression analysis, a case for Seoul, Korea -. Journal of Digital Forensics, 17(4), 128-145. http://doi.org/10.22798/KDFS.2023.17.4.128