방통융합정책연구 KCC-2020-14

인터넷 기술 환경 변화에 따른 불법정보 유통 대응 방안 연구

A Study on Emerging Encryption Technologies and Future Threats to Preventive Measures for Illegal Content on the Internet

천혜선/신혜인/이찬구/전주혜/김용희/김유석

2020. 12

연구기관 : (사)미디어미래연구소

방송통신위원회
Korea Communications Commission

이 보고서는 2020년도 방송통신위원회 방송통신발전기금 방송통신 융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**인터넷 기술 환경 변화에 따른 불법정보 유통 대응 방안 연구**』의 연구결과보고서로 제출합니다.

2020년 12월

연구 기관: 미디어미래연구소
총괄책임자: 천혜선
참여연구원: 신혜인
이찬구
전주혜
김용희
김유석

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

인터넷 기술 환경 변화에 따른 불법정보 유통 대응 방안 연구

2. 연구 목적 및 필요성

SNI필드정보를 활용한 접속차단조치의 도입('19. 2. 11.)와 관련하여, 불법정보에 대한 실효적인 유통방지 방안 마련에 대한 국민적 요구와 더불어 인터넷이용자의 정보접근권 및 통신보안에 대한 우려도 제기되었다. 이에 따라 방송통신위원회는 국민정서를 반영한 인터넷규제개선 방안 도출을 위해, 각계각층의 전문가와 시민단체가 참여하는 '인터넷규제개선 공론화 협의회'를 운용하였다. 이 협의회는 약 6.5개월 동안의 긴 논의를 통해, 현재의 접속차단 조치를 무력화할 수 있는 기술동향에 대응할 것과 더불어 접속차단 조치를 보완하기 위해 이용자의 개인정보보호제도 검토, 민간 자율규제 활성화, 국제공조수사 강화 등의 비기술적 조치방안을 검토할 것을 권고했다.

이에 본 연구는 '인터넷규제개선 공론화 협의회'의 후속조치로, ① 기술 환경 변화에 대응한 불법정보(사이트) 차단 조치의 개선과제를 도출하고, ② 기술적 조치에 대응한 이용자 보호 강화를 위한 제도적 보완방안을 검토했다.

3. 연구의 구성 및 범위

본 연구는 불법유해정보의 유통방지를 위한 기술적 조치의 기술적· 제도적 개선과제의 도출을 위해 제2장은 기술 대응에 초점을 두었으며, 제3장은 제도보완에 초점을 두어 진행했다.

제2장은 불법정보 유통방지를 위한 기술 이슈와 대응에 대해 다루었으며, 통신 보안접속 기술의 표준화 동향과 주요 정보통신사업자들의 보안접속 기술의 적용현황을 분석하여 불법정보

유통방지를 위한 기술과제들을 도출했다. 이를 위해 본 과제는 국제표준화기구와 민간 통신 기술 개발 그룹들의 인터넷 전송계층 보안 프로토콜 표준 및 주소암호화 기술 개발 동향을 분석했으며, DNS통신부문에서 운영체제, 웹브라우저, DNS 서버 등 분야별 주요사업자들의 암호화 기술 채택 동향을 분석하고, 전송계층 보안프로토콜 표준인 TLS 1.3과 ESNI채택 동향을 분석하여 현 시점에서 접속차단의 우회가능성을 평가했다. 본 연구에서는 상기의 동향분석 결과들을 토대로 암호화 기술 개발에 따른 차단 실효성 평가와 기술 대응 방향에 대해 제언하고, 현 시점에서 가능한 우회접속기술에 대한 대응방안을 제시했다. 또한 정보통신서비스제공사업자의 서비스 단에서 불법영상물의 업로드와 다운로드를 제한하는 필터링 기술의 성능평가를 위해 성능평가의 도입 필요성과 도입방안도 검토하였다.

제 3장은 불법정보 유통방지를 위한 제도개선 이슈와 대응에 대해 다루며, 이용자 보호 제도 현황 분석을 통해 제도개선방안을 도출하고, 불법정보 유통방지를 위한 비기술적 대응 방안으로 자율규제 활성화 방안과 국제 공조 강화 방안 등을 검토했다. 본 연구에서는 개인정보보호와 관련한 현행의 법제도들을 검토하여 네트워크 상에서의 접속차단 과정에서 이용자들이 우려하는 개인정보의 유출 등을 미연에 방지하는 법률적 근거들을 확인했다. 또한 불법영상물 유통방지와 관련하여 인터넷접속역무제공자들이 현행 법률과 제도에 근거하여 충실하게 이용자에게 접속차단을 위한 고지의무를 시행하고 있는지를 검토했다. 이 외에도 HTTPS 접속차단의 과정에서 제기되었던 업무처리의 투명성 개선을 위해 기존 '해외 불법정보 차단 업무 처리지침'을 분석하고 HTTPS 차단조치의 포섭을 위한 개정방안을 제시했으며, 불법정보 유통방지를 위한 비기술적 대응방안 강화를 위해 해외의 불법정보 심의 및 삭제·차단과 관련한 자율규제 기구의 사례들을 소개하고, 사이버범죄 수사의 국제공조 강화를 위한 방안으로 유럽 사이버범죄 협약 가입 필요성과 우려사항 및 법률개정 필요성 등을 검토했다.

4. 연구 내용 및 결과

제2장은 불법정보 유통방지를 위한 기술 이슈와 대응과 관련해서, 본 연구는 통신보안접속 기술 표준화와 주요 사업자의 보안접속 기술 적용 동향을 분석하고, 불법정보 유통 방지를 위한 기술과제를 도출했다. 보안접속 기술의 표준화 및 적용현황을 분석한 결과, 주소정보

암호화 기술 및 전송계층 보안 프로토콜 표준의 개발 등이 이뤄지고 있는 것은 사실이나 현행의 접속차단 조치가 무력화될 수준은 아닌 것으로 판단했다. 따라서 현 시점에서 보안통신기술 자체를 제한하거나 새로운 기술적 조치를 도입하는 것은 개인정보침해 및 과잉차단의 우려가 있다고 판단했다. 다만, 주요 사업자들의 새로운 보안접속 기술의 채택여부와 확산 추세를 지속적으로 모니터링 하는 것을 바람직하다고 판단했다.

이 외에도 제 2장에서는 VPN이나 TCP Fragmentation을 이용한 차단조치 우회가능성을 평가했다. 평가결과 VPN이나 TCP Fragmentation을 이용한 우회가 특정 조건에서 기술적으로는 가능하나, 해당 기술이 우회접속만을 목적으로 사용되는 기술이 아니고 네트워크의 국제망 특수성을 고려할 때 기술자체를 제한하는 것은 바람직하지 않다는 결론에 도달했다. 다만, VPN에 대해서는 가입자에게 인터넷접속역무를 제공하는 하위계층 ISP사업자에게 불법사이트 차단의무 이행을 강화하고, VPN의 불법적 이용을 조장하는 광고물에 대한 심의·제재를 강화하는 비기술적 대응을 통해 규제하는 것이 가능하다고 판단했다. TCP Fragmentation에 대해서는 기존 네트워크 장비 단에서 TCP 복호화(reassemble) 기능을 구현을 해서 쪼개진 URL정보를 탐지하는 방식과 같은 기술들을 개발하는 것이 가능하다고 판단했다.

제3장은 이용자 보호제도 현황 분석을 통해 제도개선방안을 도출하고, 불법정보 유통방지를 위한 비기술적 대응방안으로 자율규제 활성화 방안과 국제 공조 강화 방안 등을 검토했다. 검토결과, 현행 개인정보보호 관련 법제들은 ISP가 개인의 인터넷이용정보를 수집하거나 제공하는 데에 엄격한 제한을 두고 있는 것으로 확인되었으며 법률 제·개정은 필요하지 않은 것으로 판단했다. 또한 인터넷접속역무사업자의 이용약관에서도 불법정보의 접속제한에 대한 고지가 대체적으로 이뤄지고 있는 것으로 확인됐다. 다만, 일부 사업자의 이용약관은 근거법 개정 및 정부조직개편에도 불구하고 예전의 약관을 그대로 사용하고 있어, 시정이 필요한 것으로 판단됐다. 또한 현행 '해외불법정보 차단업무 처리지침'이 URL차단 기준으로 작성되어 있어, 일부 조항의 문구 수정이 필요하다고 판단했다.

이 외에도 본 연구에서는 불법정보 유통방지를 위한 비기술적 대응방안 강화를 위해 해외의 불법정보 심의 및 삭제·차단과 관련한 자율규제 기구의 사례들을 소개했다. 일반적으로 해외의 자율규제기구들은 자문기관의 역할과 불법정보의 신고접수 등을 수행하고 있으며, 영국의 IWF는 불법정보의 신고접수부터 통신내용의 심의, 삭제권고까지 일부 기능을 위임받아 수행하는 형태로 운영되고 있는 것을 확인했다. 우리나라도 이번 전기통신사업법 제

22조의5 1항과 시행령 제30조의5의 개정으로 성폭력피해상담소, 한국여성인권진흥원, 그 밖에 방송통신위원회가 정하여 고시하는 기관 및 단체 등이 불법촬영물 등을 신고할 수 있는 법률적 근거가 마련됨에 따라 민간기관과 정부간의 협력체계가 구축되었다.

마지막으로 본 연구는 아동성범죄 영상에 대한 국제공조수사 강화를 위한 방안으로 유럽 사이버범죄 협약 가입 필요성과 우려사항 등을 검토했다. 사이버범죄협약의 절차법 규정들은 수사기관의 신속한 정보보전 요청, 압수・수색, 감청 등을 허용하고 있기 때문에, 개인정보의 자기결정권과 수사기관의 정보수집에 대한 제한을 두고 있는 국내의 개인정보보호법과 통신비밀보호법과 상당한 상충이 있다고 판단했다. 특히 협약 제32조는 우리나라 정부의 승인 없이도 회원국들이 통신사나 인터넷서비스 제공자에게 직접 트래픽 데이터에 대한 접근과 제출을 요구할 수 있다는 우려가 있다.

5. 정책적 활용 내용

본 연구는 불법유해정보의 유통방지를 위한 기술적 차단조치의 실효성을 점검하고, 향후 인터넷통신기술 개발동향에 대응한 불법사이트 차단의 제도적 보완 및 필터링 성능평가 도입방안을 제언하였기에, 관련 정책 수립 시 참고 자료로 활용이 가능하다. 또한 해외불법정보 차단업무 처리지침의 개선안과 불법정보 유통방지를 위한 국제적 협력 강화 등비기술적 규제 대안들을 검토하여, 현행 기술적 조치의 한계를 보완하는 제도 개선안 도출에 활용이 가능하다.

6. 기대효과

본 연구의 결과는 불법유해정보의 유통방지를 위한 기술적 차단조치의 제도적, 기술적 개선을 위한 정책수립의 기초자료로 활용될 것으로 기대된다.

제 1 장 서 론

제1절 연구의 목적

○ (기술대응) 인터넷주소 전송을 암호화하는 보안통신기술과 인터넷 전송계층 보안 프로토콜 표준의 기술발전으로 인해 현행 불법사이트 접속차단 조치가 무력화된다는 우려가 제기되고 있어 기술 환경 변화에 대한 정확한 분석이 필요함

- 현행 접속차단 조치는 인터넷접속과정에서 암호화되지 않은 '서버네임인디케이션 정보(이하 SNI필드 정보)'를 이용하여 불법사이트 접속을 차단하는 방식으로, SNI필드정보까지 암호화하는 기술이 개발·적용 될 경우, 접속차단조치가 무력화될 것이라는 우려가 제기됨(한국경제, 2019. 12. 8)

- 이에 대해「인터넷규제개선공론화 협의회(2019년도)」의 검토결과, 인터넷주소 정보를 암호화하는 기술(DoH도입, ESNI, TLS 1.3 표준화 등)이 현 시점에서 불법정보의 접속차단 조치를 무력화하지는 않지만, 관련기술의 개발과 채택이 빠르게 이뤄질 가능성이 있어 관련기술에 대한 지속적인 동향분석과 대응과제 도출을 위해 노력할 것을 권고함

  ※ '19년도 운영된 '인터넷규제개선 공론화협의회' 의 「인터넷 규제개선을 위한 권고」는 인터넷 보안통신기술 표준의 개발 동향을 분석하여 기술적 조치의 실효성을 지속 점검할 것을 권고했으며, 기술적 수단에 의존하지 않고 디지털성범죄물과 불법음란물 등에 대한 국제공조 강화 등의 비기술적 수단 사용을 위해 노력할 것을 권고함

- 이에 따라 인터넷주소 전송을 암호화하는 보안통신기술과 인터넷 전송계층 보안 프로토콜 표준의 기술발전에 따른 최신 보안통신 기술표준의 개발 및 채택현황을 파악하고 기술환경 변화에 대응한 과제 발굴이 요구됨

- 또한 전기통신사업법과 정보통신망법의 개정으로 특수유형부가통신사업자와 부가통신사업자 등에게 불법영상의 업로드와 다운로드를 막는 필터링 기술 적용이 의무화됨에 따라, 필터링의 성능평가를 위한 제도 도입방안 연구가 필요함

○ (제도보완) 접속차단의 기술적 조치 도입과정에서 이용자 이익침해, 도입절차의 투명성, 대안적 규제수단 필요성 등이 제기되었기에, 이용자보호제도 보완방안, 기술적 조치의 투명성 강화 방안, 불법정보 유통방지를 위한 국제적 협력 강화(예: 사이버범죄협약

가입) 등 비기술적 규제 대안들을 검토할 필요가 있음

- SNI필드정보를 활용한 접속차단조치의 도입('19. 2. 11.)에 대해 인터넷이용자의 정보접근권 및 통신보안에 대한 우려가 제기되었으며, 이에 대해 '인터넷규제개선 공론화 협의회'는 이용자 보호 방안을 마련하고, 국제적 협력 강화 등의 비기술적 조치를 발굴할 것을 권고한 바 있음
- 이에 따라 기술적 조치 관련 이용자 보호제도 보완방안으로써 기술적 조치의 투명성을 위해 절차· 운용에 관한 지침이나 고시를 검토할 필요가 있음
- 또한 불법정보유통의 주요 경로가 되고 있는 글로벌CP(content providers)나 해외사이트에 효과적으로 대응하기 위해, 협약당사국 간의 통일적인 또는 상호 합의한 사이버범죄 수사 및 기소 관련협정 등을 규정한 유럽 사이버범죄방지협약(일명 부다페스트 협약) 가입을 검토할 필요도 제기되고 있어 이를 대비한 법률개정 필요성 등의 검토가 필요함

○ (연구목적) 2019년 2월에 도입된 HTTPS 차단조치와 관련하여, 기술적 조치의 실효성 개선과 제도적 보안의 필요성이 제기됨에 따라, 본 연구는 ① 기술 환경 변화에 대응한 불법정보(사이트) 차단 조치의 개선과제를 도출하고, ② 기술적 조치에 대응한 이용자 보호강화를 위한 제도적 보완방안을 검토하고자 함

제2절 연구의 방법과 구성

○ (연구구성) 본 과제는 불법유해정보의 유통방지를 위한 기술적 조치의 기술적· 제도적 개선과제의 도출을 위해 제2장은 기술 대응에 초점을 두었으며, 제3장은 제도보완에 초점을 두어 진행함

- 제2장은 불법정보 유통방지를 위한 기술 이슈와 대응에 대해 다루며, 통신 보안접속 기술의 표준화 동향과 주요 정보통신사업자들의 보안접속 기술의 적용현황을 분석하여 불법정보 유통방지를 위한 기술과제들을 도출함
  - ▸ 이를 위해 본 과제에서는 국제표준화기구와 민간 통신기술 개발 그룹들의 인터넷 전송계층 보안 프로토콜 표준 및 주소암호화 기술 개발 동향을 분석함
  - ▸ 또한 DNS통신부문에서 운영체제, 웹브라우저, DNS 서버 등 분야별 주요사업자들의 암호화

기술 채택 동향을 분석하고, 전송계층 보안프로토콜 표준인 TLS 1.3과 ESNI채택 동향을 분석하여 현 시점에서 접속차단의 우회가능성을 평가함

- ▸ 상기의 동향분석 결과들을 토대로 암호화 기술 개발에 따른 차단 실효성 평가와 기술 대응 방향에 대해 제언하고, 현 시점에서 가능한 우회접속기술에 대한 대응방안을 제시함
- ▸ 또한 정보통신서비스제공사업자의 서비스 단에서 불법영상물의 업로드와 다운로드를 제한하는 필터링 기술의 성능평가를 위해 성능평가의 도입 필요성과 도입방안을 검토함

- 제 3장은 불법정보 유통방지를 위한 제도개선 이슈와 대응에 대해 다루며, 이용자 보호 제도 현황 분석을 통해 제도개선방안을 도출하고, 불법정보 유통방지를 위한 비기술적 대응방안으로 자율규제 활성화 방안과 국제 공조 강화 방안 등을 검토함

- ▸ 본 과제는 개인정보보호와 관련한 현행의 법제도들을 검토하여 네트워크 상에서의 접속차단 과정에서 이용자들이 우려하는 개인정보의 유출 등을 미연에 방지하는 법률적 근거들을 확인함
- ▸ 또한 불법영상물 유통방지와 관련하여 인터넷접속역무제공자들이 현행 법률과 제도에 근거하여 충실하게 이용자에게 접속차단을 위한 고지의무를 시행하고 있는지를 검토함
- ▸ HTTPS접속차단의 과정에서 제기되었던 업무처리의 투명성 개선을 위해 기존 '해외 불법정보 차단업무 처리지침'을 분석하고 HTTPS 차단조치의 포섭을 위한 개정방안을 제시함
- ▸ 불법정보 유통방지를 위한 비기술적 대응방안 강화를 위해 해외의 불법정보 심의 및 삭제·차단과 관련한 자율규제 기구의 사례들을 소개하고, 사이버범죄 수사의 국제공조 강화를 위한 방안으로 유럽 사이버범죄 협약 가입 필요성과 우려사항 및 법률개정 필요성 등을 검토함

제2장 불법정보 유통방지를 위한 기술 이슈와 대응

제1절 통신 보안접속 기술 표준화 동향

1. 접속차단 기술방식

가. 데이터 통신의 구조

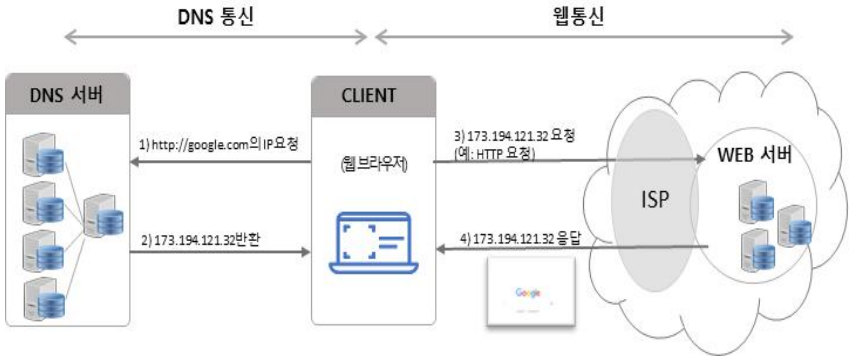
○ (접속원리) 인터넷 통신은 이용자가 ① 웹서버의 주소를 확인하는 DNS통신과 ② 웹서버로부터 데이터를 전송받는 실제 웹통신으로 구성

- ① DNS† 통신: 사람이 기억하기 쉽고 의미를 갖도록 만들어진 문자 형태의 도메인(https://google.com 등)을 컴퓨터가 처리하기 쉬운 숫자형태의 IP주소로 매칭하여 이용자에게 제공하는 통신

† DNS(도메인네임 서버, Domain Name System): 인터넷에 연결된 모든 컴퓨터는 32비트의 숫자로 구성된 고유의 IP주소를 가지고 있으며, DNS는 이 숫자로 된 IP주소를 사람들이 기억하기 쉽도록 문자로 된 호스트 이름을 부여하고 관리하는 시스템

- ② 웹통신: 이 IP주소에 해당하는 웹서버로부터 데이터 전송을 요청하여 인터넷서비스를 이용

[그림 2-1] 데이터통신의 구조



- (DNS통신) 인터넷 이용자가 웹브라우저에 접속하고자 하는 웹사이트의 URL(Uniform Resource Locator)주소(www.kcc.go.kr 등)를 입력하면, 분산된 서버들로부터 해당 URL

주소에 부합하는 웹서버의 IP주소(127.255.255.255 등)를 반환하는 과정

- (웹통신) DNS서버로부터 얻은 IP를 이용해서 웹서버를 호출하여 원하는 데이터를 전송받는 과정([그림 2-1]의 3 ~ 4단계)

○ (DNS통신) 인터넷에서 특정 웹사이트에 연결하기 위해 해당 사이트의 IP주소를 확인하는 절차

- 도메인네임서버† 는 인터넷이용자가 사용하는 친숙한 영문주소 이름(www.kcc.go.kr 등)을 컴퓨터가 이해할 수 있는 IP주소(127.255.255.255 등)로 변환하여 매칭하는 역할을 수행

† 도메인네임(Domain Name)은 인터넷의 실제 IP주소와 연결된 기억하기 쉬운 영문주소이름이며, 도메인네임서버(DNS: Domain Name Server)는 분산구조화된 트리 구조를 이용하여 하나의 영문주소 이름에 여러 개의 IP주소를 집합시켜 관리하는 서버를 의미함

- IP주소와 서버호스트이름은 상호통신이 가능한 여러 개의 DNS서버에 분산되어 있어, 분산된 서버간의 계층적 통신과정을 통해서 URL주소를 IP주소로 매칭하여 알려줌

* 2017년 기준, 약 3억 3,200만개 이상의 도메인이 등록(Shaw, 2018)

○ (주소매칭과정) 클라이언트가 접속하고자 하는 사이트의 IP주소정보를 DNS에 확인하는 과정

- ① 사용자가 접속하고자 하는 사이트(예: www.kcc.go.kr)의 URL을 웹브라우저에 입력하면 웹브라우저는 로컬 DNS서버에 IP 주소를 알려달라는 요청을 전송
- ② DNS 서버는 www.kcc.go.kr의 IP 주소인 127.255.255.255를 찾기 위해 데이터베이스를 확인
- ③ DNS서버는 확인한 IP 주소를 사용자의 웹브라우저에 반환

나. 인터넷 접속 차단의 기술 개요

○ (접속차단) 글로벌한 인터넷의 특성으로 인해 불법정보에 대한 국가별 통제가 어렵기 때문에 불법성이 확인된 특정 사이트나 게시물로의 접속을 네트워크에서 제한하는 기술적 방식

- 이용자의 특정 사이트나 게시물로의 접속요청(IP주소, 도메인 네임, URL 등)을 확인하여 접속을 차단하는 방식

▸ (IP차단) 불법성이 확인된 특정사이트의 IP주소를 ISP의 라우터에서 직접 차단하는 IP차단방식

▸ (DNS차단) 이용자가 불법성이 확인된 특정 사이트나 게시물의 IP주소를 확인하기 위해 DNS에 접속할 때, 해당 요청을 확인하여 다른 IP주소(접속차단페이지)를 반환하는 방식

▸ (URL차단) 불법성이 확인된 특정사이트 뿐만 아니라 하위경로까지 지정해 불법정보로의 접속을 차단하는 URL차단 방식

(1) IP차단방식

○ (개념) 불법사이트 차단을 위해 설치된 라우터 장비에서 불법사이트의 IP주소를 차단하는 방식

- 과거에는 도메인 이름과 연결된 IP 주소를 인터넷사업자의 라우터에서 원천적으로 차단하는 IP차단이 실시됨
- 이용자가 URL이 아닌 IP주소를 알고 입력하더라도 불법사이트의 IP목록과 매칭하여 차단할 수 있음
- IP주소는 URL주소보다 쉽게 바꿀 수 있기 때문에 차단목록에 포함될 경우, 불법사이트 제공자가 IP주소를 변경하여 우회 제공이 가능함
- 또한 하나의 IP주소에 여러 개의 도메인 명을 매핑하는 웹호스팅 업체들이 등장함에 따라, 동일한 IP주소로 연결되는 공용서버의 합법적 사이트도 차단될 수 있다는 한계가 있어 현재는 거의 사용되지 않음

(2) DNS 차단방식

○ (개념) 접속하고자하는 사이트의 IP주소를 확인하는 DNS통신과정에서 차단리스트에 있는 도메인 네임이 일치하는 접속요청이 올 경우 접속을 차단하거나 차단 안내페이지의 IP주소를 반환하는 방식

○ (기술 개요) DNS 서버에서 특정 도메인 네임의 검색을 차단하고 브라우저가 검색하려는 IP주소 대신에 다른 IP주소(예:warning.or.kr)를 전달

- 인터넷 주소를 IP주소로 변환하는 DNS서버(DNS의 리졸버(resolver))에서 차단
- 클라이언트가 DNS서버에 요청한 URL정보를 IP주소로 변환하는 DNS통신과정에서, ISP에

라우터(router)를 설치하여 차단리스트에 있는 도메인 네임이 일치하면 접속하려고 하는 클라이언트에게 다른 IP주소를 반환하거나 접속을 차단

○ (특징) 도메인 네임으로 제공되는 모든 콘텐츠를 차단할 수 있음

- 인터넷이용자에게 차단 안내페이지(www.warning.or.kr)를 제공할 수 있음
- 도메인 네임은 IP보다 관리하기 쉽고 더 정확하기 때문에 IP 기반 차단방식보다 좀 더 효율적임

○ (실효성) 인터넷이용자나 CP가 해외 DNS 서버를 사용하거나 접속방식을 변경하는 방식으로 접속차단을 우회하기 쉬움

- 이용자의 네트워크 연결을 완전하게 통제할 때 유효하므로, 이용자가 타 DNS서버 세트를 이용하거나 다른 접속방식을 선택한다면 DNS 차단이 이루어지지 않음
- 또한 불법사이트 제공자가 도메인 네임을 바꾸는 것이 IP 주소를 바꾸는 것보다 쉽기 때문에 우회가 쉬움

  예) sex.com과 같은 사이트라면, www.sex.com 이라는 이름은 서버 이외에도 ww2.playboy.com이나 ww3.playboy.com과 같이 도메인 이름을 가진 추가적인 서버들을 사용하여 실제 콘텐츠를 공급할 수 있음

○ (과차단 우려) 도메인 네임만 일치하면 차단하기 때문에 과차단의 우려가 있음

- 도메인 네임(예:google.com)은 복수의 하위도메인(예: mail.google.com, docs.google.com 등)을 포함하여 계층적으로 관리할 수 있음
- 따라서 같은 서버에서 같은 도메인 네임을 이용하는 경우, IP기반 차단방식과 마찬가지로 DNS 차단도 합법 콘텐츠까지 차단할 우려가 있음

(3) URL 차단(HTTP차단)

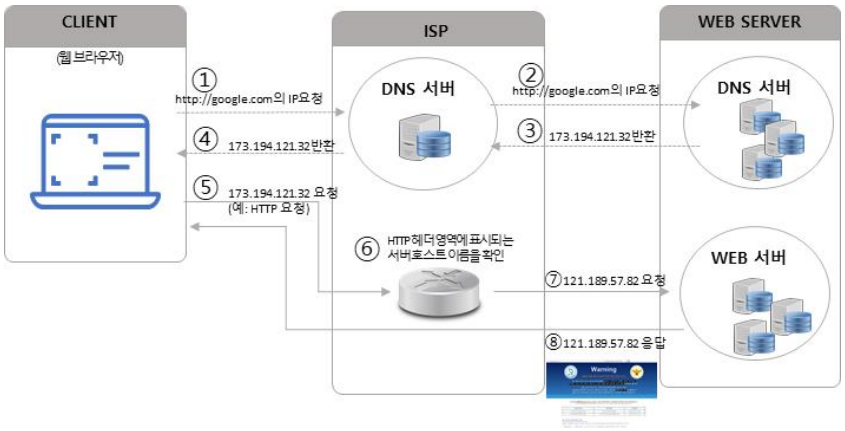
○ (개념) 이용자의 요청 패킷 중 HTTP헤더에 들어가는 호스트 정보를 ISP에서 식별해 불법사이트나 불법정보의 URL목록과 매칭하여 차단하는 방식

- 해외관문국에 해당하는 ISP에 전용라우터를 설치하여 방심위에서 심의한 불법사이트의 목록과 접속요청을 매칭하여 불법성이 확인된 URL로의 접속시도를 차단하는 방식

○ (기술 개요) HTTP헤더 영역에 표시되는 서버호스트 이름을 확인하여 해당 서버 사이트를 차단

- 필터가 웹(HTTP) 트래픽의 흐름을 가로 채서 HTTP 요청에 나타나는 URL을 로컬 데이터베이스 또는 온라인 서비스와 비교하여 확인하여 연결을 허용하거나 차단
- 필터링 장치가 이용자와 인터넷을 연결하는 선상에 위치해야 하고, 합당한 성능을 위해서 높은 수준의 리소스가 필요하기 때문에 차단 비용 높다는 한계가 있음

[그림 2-2] URL차단의 개요도



○ (특징) 하위디렉토리 및 페이지 단위까지 정교하게 차단이 가능하고 차단안내페이지를 제공할 수 있음

- 웹페이지를 리다이렉트(redirect)해 이용자를 다른 페이지로 연결시켜 차단 안내페이지를 제공할 수 있음
- URL 필터링은 차단을 수행하는 필터의 품질에 따라 성능이 좌우되며, 잘못 설계되거나 광범위한 필터로 인해 트래픽의 전반적인 속도와 신뢰도가 하향될 수 있음

○ (실효성) 정보의 전체 카테고리에 대해 전면적인 차단을 실시할 때 유효하나, 암호화된 웹서버와 마찬가지로 새로운 페이지와 소형 사이트는 쉽게 빠져나갈 수 있음

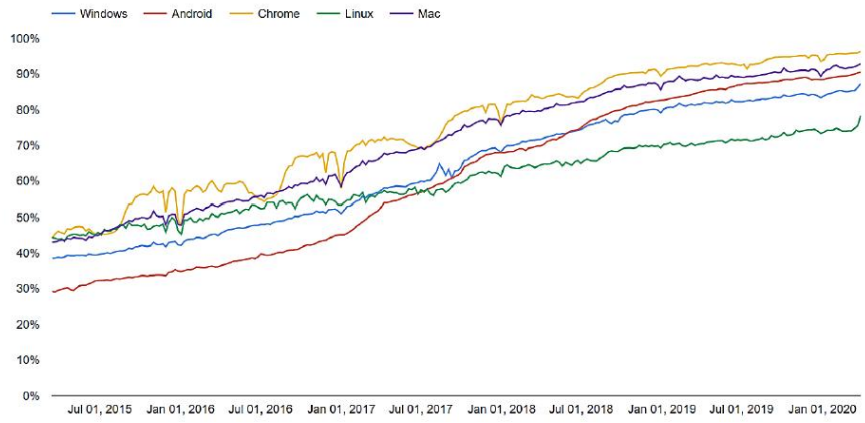
- 고수준(high-level) URL에서는 차단이 용이하나, 딥링크 차단이 어려움
- TLS를 통해 암호화되는 보안접속(HTTPS†)의 경우 해당호스트 이름을 확인할 수 없기 때문에 차단이 불가능함

† HyperText Transfer Protocol over Secure Socket Layer의 약어로, 인터넷에서 감청 위협으로부터 데이터를 안전하게 보호하기 위해 전송되는 데이터를 암호화하여 송수신하는 프로토콜임.

- IP주소를 암호화하는 보안접속 통신을 사용할 경우, 불법사이트로의 접속시도임에도 불구하고 주소정보를 확인할 수 없다는 한계가 있음
- 최근 보안접속을 활용한 인터넷통신이 증가함에 따라 기존의 IP주소와 URL주소를 확인하여 차단하는 방식의 실효성이 낮아짐

※ 구글 크롬이나 모질라 파이어폭스와 같은 특정 브라우저의 경우 전체 웹 트래픽 중 보안접속을 사용한 트래픽의 비중이 OS별로 78~96%에 이르는 등 보안접속의 비중이 높음('20. 4. 기준)

[그림 2-3] OS별 구글 크롬 이용자의 HTTPS 트래픽 비중



출처: European Union Agency for Cybersecurity(2010. 4. 23).

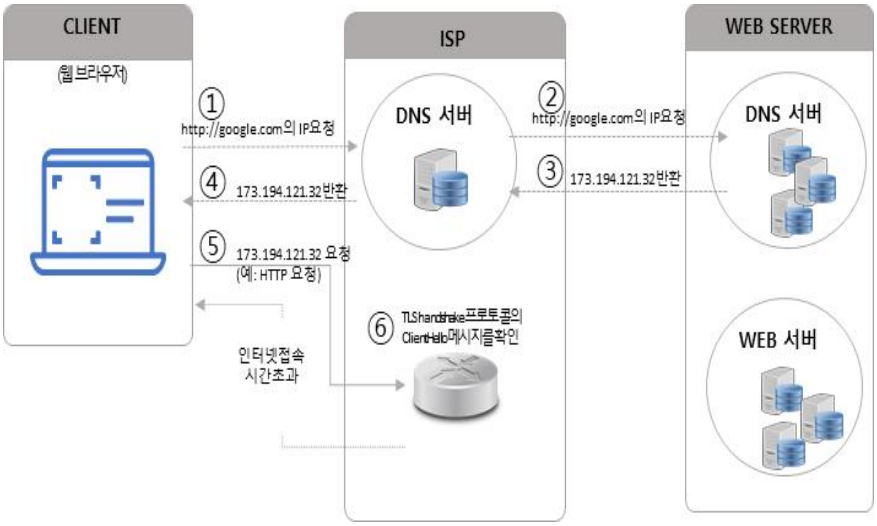
○ (과차단 우려) IP차단이나 DNS차단 방식과 달리 하위디렉토리 및 페이지 단위까지 차단이 가능하기 때문에 비교적 과잉차단의 우려가 낮음

(4) HTTPS 차단(SNI필드 차단)

○ (개념) 보안접속시에도 암호화되지 않는 영역인 SNI필드에서 서버네임을 특정하여 차단하는 방식

- 보안접속을 활용하는 사이트에 대해서도 접속여부를 확인하여 차단할 수 있는 방식으로 SNI필드정보를 확인하여 차단하는 HTTPS 차단방식을 방송통신위원회가 도입('19. 2.)

[그림 2-4] HTTPS 차단의 개요도



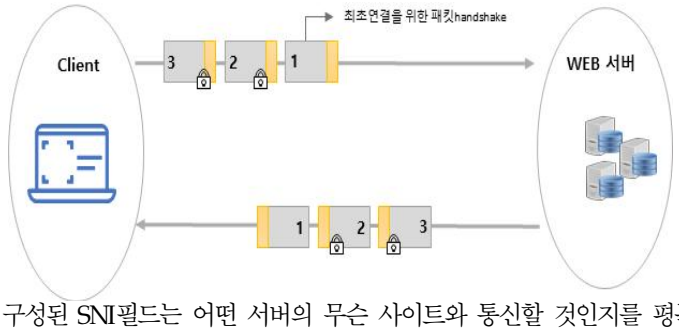
○ (기술방식) TLS handshake 프로토콜의 ClientHello 메시지를 확인하여 해당 서버의 접속을 차단하는 방식

- HTTPS 방식은 브라우저와 웹서버가 암호를 풀수 있는 공개키 인증서(PKI) 정보를 주고받아 접속을 체결한 뒤 이후 통신내용을 암호화하여 전송하게 됨

- 공개키(PKI) 인증서 정보를 주고받는 핸드쉐이킹(handshaking)과정은 보안이 적용되지 않은 평문으로 통신이 이뤄짐

  * PKI(공개키, public key infrastructure) 인증서를 교환하는 핸드쉐이킹 과정은 웹브라우저와 서버간의 보안통신을 시작하기 전에 서로 암호화된 통신내용을 해독할 수 있는 키를 교환하는 과정으로서, 이 단계에서 전달되는 통신에서 서버명이 포함된 SNI필드를 확인할 수 있음

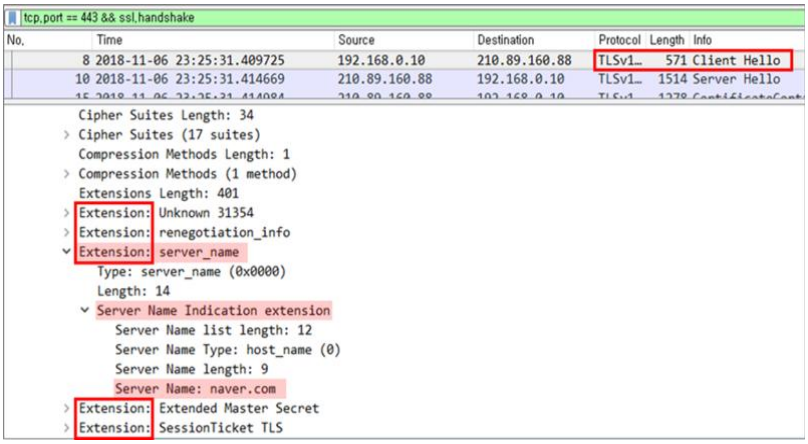
[그림 2-5] TLS 핸드쉐이크 과정의 헤더 개념도



- 평문으로 구성된 SNI필드는 어떤 서버의 무슨 사이트와 통신할 것인지를 평문으로 전달되기 때문에, 이 부분을 분석하여 불법사이트의 웹서버 접속 요청을 확인하여 차단할 수 있음

  * SNI(Server Name Indication: 서버네임표시자)는 클라이언트와 서버가 키정보를 교환하는 과정인 핸드쉐이크(handshake)를 거치는 과정에서 노출되는 평문화된 정보를 의미함. HTTPS의 경우 HTTP의 헤더정보를 비롯한 모든 메시지가 암호화되기 때문에 목적지인 호스트의 정보를 알 수 없으나, 이 경우에도 SNI필드 정보는 암호화가 적용되기 이전 단계의 정보이기 때문에, 아래의 그림에서 보듯이 서버네임이 평문형태로 노출

[그림 2-6] SNI필드 정보의 예시



○ (특징) 보안접속에 대해서도 불법성 여부를 확인해 접속차단을 할 수 있다는 장점이

있으나, 웹페이지를 리다이렉트(redirect)할 수 없기 때문에 이용자에게 차단안내메시지 제공이 불가능함

○ (실효성) DNS 차단이나 URL 차단 방식에 비해 우회접속이 어려움

- 기존 URL차단 방식으로는 차단할 수 없었던 보안접속 기반 불법사이트도 효과적으로 차단할 수 있으며, 그로 인해 그동안 DNS차단이나 URL차단을 우회하여 제공하던 불법사이트들이 상당수 차단됨
- 다만 향후 SNI필드 정보를 암호화하는 ESNI기술이 개발되어 TLS1.3에 적용될 경우, 실효성이 낮아질 수 있어 이에 대한 지속적인 모니터링이 필요하다는 지적이 있음

○ (과차단 우려) URL차단과 달리 하위디렉토리 및 페이지 단위까지 차단할 수는 없어 과차단 우려가 있음

- 서비스(mail,news등) 단위별로는 차단이 가능하나 개별 게시물 단위로 차단하는 것은 불가능하기 때문에, 불법게시물과 합법게시물이 혼재되어 있을 경우에는 과차단의 우려가 발생할 수 있음
- 따라서 통신심의 과정에서 현저한 수준의 불법게시물이 있는 사이트를 불법사이트로 판단하여 차단하는 방식이 적용되고 있음

2. 보안접속 기술 표준 동향

가. 기술발전에 따른 우회 우려

○ (실효성 약화 우려) 이론적으로는 ① DNS통신과정이 암호화되고, ② HTTPS에서 헤더정보까지 암호화되면 접속차단의 실효성이 약화될 수 있음

- 현재까지 개발 및 적용된 접속차단 시스템은 DNS쿼리를 확인하여 차단하는 DNS차단과 HTTP/HTTPS로 접속정보를 확인하여 차단하는 방식을 모두 포함하기 때문에, DNS통신과 웹통신 중 하나만 암호화된다고 하더라도 불법사이트로의 접속을 차단하는 것이 불가능하지 않은 상황임
- 따라서 새로운 통신기술의 개발이 현재의 접속차단 조치를 무력화하는 단계에 이르기

위해서는 ① DNS통신부문 암호화와 ② 웹통신 암호화가 동시에 이뤄져야 함

- 즉, 클라이언트(웹브라우저), DNS서버, 웹서버 모두에서 DoT 또는 DoH, ESNI, TLS1.3를 지원해야함

  ① DNS 쿼리를 암호화하는 기술: DoH(DNS over HTTPS), DoT(DNS over TLS)

  ② HTTPS에서 헤더정보를 암호화하는 기술: ESNI(Encrypted SNI)

○ (DNS암호화) 이전에는 암호화되지 않았던 DNS통신을 암호화하는 기술이 일반화되면 DNS차단의 실효성이 낮아짐

- 원래 DNS통신은 보안문제를 고려하지 않고 개발된 통신으로 DNS쿼리는 암호화되어 있지 않기 때문에 DNS서버에서 IP주소를 묻는 요청이 들어오면 차단사이트(warning.co.kr)의 IP주소를 알려주어 차단할 수 있었음
- 그러나, 만약 DNS통신까지 암호화되는 기술이 개발·확산될 경우 클라이언트와 DNS서버 간의 통신에서 접속하고자 하는 도메인네임을 확인할 수 없기 때문에 불법사이트로의 접속여부를 알 수 없음
- 현재 IETF의 워킹그룹에서 DNS통신을 암호화하는 기술표준으로 DoH(DSN over HTTPS: DNS 통신을 HTTPS 암호화를 적용하는 방식)와 DoT(DNS over TLS: DNS 통신에 전송계층 암호화(TLS)를 적용하는 방식)을 개발하는 연구가 이루어지고 있음
- IETF의 홈페이지에 공개된 바에 따르면, DoH의 제안표준(RFC 8484)은 2018년 10월에, DoT의 기술표준(RFC 7858)은 2016년 5월에 제정되어 업데이트 중에 있음
- IETF의 워킹그룹에서 제안표준(Proposed Standard)이 제정되었다 함은 바로 기술을 상용적으로 사용하고 확산될 수 있음을 의미하는 것은 아니며, 표준 또는 표준의 일부가 되는 초안(internet draft)으로 시작되어 여러 번의 개정을 통해서 RFC(Request for Comments)로 받아들여지면 제안표준(Proposed Standard)이 되며, 이후 초안표준(Draft Standard)를 거쳐 인터넷표준(Internet Standard)로 확정됨
- 일반적으로 초안표준은 다수의 구현체가 있고 이 표준이 시장에서 이미 널리 받아들여지면 인터넷표준(Internet Standard)으로 요청할 수 있음. 인터넷 표준이 되기까지 소요되는 시간은 표준마다 각기 다름

○ (웹통신 암호화) SNI필드까지 암호화하는 암호화된 SNI(ESNI: encrypted SNI) 표준이

제정되어 적용되면 SNI필드 정보의 확인이 어려워져 HTTPS 차단의 실효성이 낮아진다는 우려

- 기존의 보안접속(HTTPS)에서도 초기에 클라이언트와 서버간의 통신을 시작하기 위해 공개키를 전달하는 과정인 핸드쉐이킹 과정에서 SNI필드 정보는 평문으로 전달되었고, 이 SNI필드 정보에서 접속하고자 하는 서버네임을 확인하여 접속차단이 실시되었음
- 그러나 최근 TLS1.3의 확장프로그램(extensions)으로써 SNI 필드 정보까지 암호화하려는 기술연구가 진행되고 있으며, 이 기술이 도입될 경우 평문화된 SNI필드 정보까지 암호화하여 접속하고자 하는 주소 정보를 확인할 수 없게 변환되어 현행의 접속차단 조치가 무력화될 것이라는 우려가 제기되고 있음

나. 암호화 기반 DNS 통신 표준기술 개발 동향

○ (개념) 암호화기술이 적용되지 않은 DNS통신의 약점을 악용하는 해킹이나 하이재킹 등의 사이버 공격을 방어하기 위해, DNS 통신 전체를 암호화하기 위한 기술 표준이 IETF에서 진행되어옴

<국제 인터넷 표준화 기구(Internet Engineering Task Force, IETF)>
- 인터넷의 운영, 관리, 개발에 대해 협의하고 프로토콜과 구조적인 사안들을 분석하는 인터넷 표준화 작업기구
- 인터넷 아키텍처 위원회(IAB)의 산하기구로 인터넷의 운영, 관리 및 기술적인 쟁점 등을 해결하는 것을 목적으로 망 설계자, 관리자, 연구자, 망 사업자 등으로 구성된 개방된 공동체
- 주로 자발적인 참여와 논의 과정을 통하여 인터넷 관련 기술표준을 마련하고 있어, 기술표준이 제안되었다고 해도 강제성이 있지는 않음
- 정보보호기술의 표준화는 IETF의 보안영역의 워킹그룹에서 진행하고 있고, 현재 25개의 워킹그룹이 정보보호기술(security area)의 표준화를 담당하고 있음

○ (개발동향) 클라이언트가 DNS서버에 특정 사이트의 주소정보를 확인하는 DNS통신 프로토콜에 HTTPS 암호화를 적용(DoH)하거나 전송계층 암호화(TLS)를 적용(DoT)하여 DNS통신을 암호화할 수 있다는 원리에 기반하여 해당 표준이 개발된 상황

- (공통점) DNS서버와 클라이언트 사이의 통신을 암호화하여 서버에게 보내는 DNS요청에 대한 정보를 확인할 수 없게 하는 것은 공통적임

- (차이) DoH와 DoT는 DNS 통신을 암호화한다는 목적은 같으나, 각각 사용하는 네트워크 계층이 다르기 때문에 사용하는 포트가 다르다는 점이 가장 큰 차이

  * 현재 DNS통신은 53번 포트를 통해서 평문으로 전송

  ▸ DoH: 기존 DNS 프로토콜에 HTTPS 암호화를 적용하여 DNS 쿼리를 HTTP요청인 것처럼 위장하는 방식으로, 기존 HTTP통신이 사용하는 포트(Port)† 443을 사용함

  † Port란 TCP/IP통신에서 프로토콜의 데이터가 컴퓨터 내부에서 전송되는 논리적 통로로써, 데이터의 처리프로세스를 구분하기 위해 사용함

  ▸ DoT: 기존 DNS 프로토콜에 전송계층 암호화(TLS)를 적용한 방식(Port 853)

(1) DNS over HTTPS 개발 동향

○ (개념) 클라이언트가 DNS서버에 특정 사이트의 주소정보를 확인하는 DNS통신 프로토콜에 HTTPS 암호화를 적용하는 방식

- 개인정보보호 및 보안을 위해 DNS통신을 HTPPS로 캡슐화한 통신프로토콜로 표준안이 2018년 10월에 제안됨

○ (기술방식) HTTP GET 명령내부에 DNS요청을 삽입하여 HTTPS 암호통신으로 DNS쿼리를 보내는 방식

- 즉, DNS 요청 메시지를 HTTP 요청인 것처럼 위장하여 DNS 통신에 대한 조작, 검열, 도청 등을 방지하고 보안성을 확보하는 방식

- 모든 DoH 트래픽이 HTTPS이기 때문에 DoH 요청은 암호화되어 일반 웹트래픽에 숨어져 있으며, DoH서버의 해석기에 전송되어 도메인 이름의 IP주소를 반환할 때에도 암호화된 HTTPS로 응답하게 됨

- DNS통신이 HTTP요청인 것으로 위장되고 DoH가 적용된 DNS서버(클라우드 플레어, 쿼드9등)를 지정하여 사용하기 때문에, DNS차단방식으로 불법사이트의 도메인 주소를 IP주소로 반환하는 과정을 확인할 수 없음

- 따라서 평문화된 DNS통신 내용을 확인하고 도메인 주소를 IP주소로 반환하는 과정을 차단하는 방식인 DNS차단방식을 적용할 수 없음

○ (기술적 제약) DoH가 적용되더라도 네임서버를 직접 쿼리하지 않기 때문에 이용자가 네임서버를 지정해야하는 등 현시점에서 DoH 적용을 하는 과정이 쉽지 않고, 이 경우에도 현재의 HTTPS 차단은 그대로 적용이 가능하기 때문에 접속차단을 우회할 수 없음

- DNS통신은 분산된 DNS서버시스템을 통해 IP주소정보를 확인하는 과정으로 여러 개의 서버 간 통신이 발생하는데 DNS통신이 HTTPS로 암호화되어 전송된다고 하더라도 도메인네임을 IP주소로 반환하는 과정에서는 운영체계(OS)가 DoH를 지원하는 리졸버를 설정하고 분산되어 있는 DNS서버들 간의 통신도 통제되어야 함
- 이 과정에서 DNS통신이 암호화하기 위해서는 이용자가 직접 DoH가 적용되는 네임서버를 지정하고 클라이언트의 운영체제와 브라우저, DNS서버 모두 DoH를 지원해야함
- DoH는 홉대홉(hop-to-hop[†]) 암호화로써 통신의 시작과 끝(end-to-end)까지 암호화하는 기술이 아니기 때문에, DoH적용만으로 전체 통신이 모두 암호화되지는 않음

[†] 홉은 컴퓨터 네트워크의 한 부분으로 통신 시작점과 통신 목적지 사이에 위치한 경로 내에서 다음 네트워크 장비까지 패킷이 이동하는 절사이의 통신 단위를 의미함

○ (탐지방법) 패킷의 목적지가 클라우드플레어(1.1.1.1), Google Public DNS (8.8.8.8) 등이라면 DoH 사용일수도 있다고 추정은 할 수 있으나, 이를 통해 특정 HTTPS 통신이 DNS통신 목적으로 발생한 것인지를 확실하게 알 수는 없음

- DoH는 기존 HTTPS 트래픽의 표준 포트인 443을 기반으로 HTTPS 및 HTTP/2를 사용하여 연결하기 때문에 일반 HTTP통신과 구분이 어려움
- 다만, DoH가 적용되는 네임서버(클라우드플레어(1.1.1.1), Google Public DNS (8.8.8.8) 등)가 패킷의 최종목적지라면 이를 통해 DoH를 사용한다고 추정할 수는 있음

○ (개발일정) DoH 는 표준화 작업이 현재 진행중인 상태로서 아직까지 최적의 구현방법이 결정된 확정표준은 아니며, IETF의 DoH WG에서 지속적인 업그레이드 중에 있음

- DoH 표준기술개발은 2017년 IETF DoH WG에서 시작되었으며 2018년 10월에 RFC 8484(DNS Queries over HTTPS, Oct 2018) 작성
- IETF는 DoH를 수행하고 합의된 승인 표준을 개발하기 위해서 ADD(Adaptive DNS Discovery) 워킹그룹을 설정하여 지속적인 업그레이드를 준비 중에 있음

(2) DNS over TLS 개발 동향

○ (개념) DNS-over-TLS(DoT)는 기존 DNS 프로토콜에 전송계층 암호화인 TLS(Transport Layer Security)를 적용하여 암호화하는 방식

※ 전송계층 보안(SSL/TLS)기술은 인터넷 접속과정에서 웹서버와 웹브라우저 사이의 정보를 암호화하는 정보보호기술로서, SSL/TLS는 컴퓨터 통신망을 통해 전달되는 데이터의 위변조를 막기 위해 개발되었으나 결과적으로 주소(179.194.121.32등)를 확인하는 과정에서 전달되는 메시지를 암호화할 수 있어 전송계층 보안기술의 발전 동향에 따라 현행 접속차단 기술의 실효성이 영향을 받을 수 있음

- DNS통신에 TLS를 적용하여 암호화하면 DNS요청에서 불법사이트로의 접속시도 여부를 확인할 수 없기 때문에 접속차단의 실효성이 낮아진다는 주장이 있음

○ (기술적 제약) DoH와 마찬가지로 DoT가 적용되더라도 네임서버를 직접 쿼리하지 않기 때문에 이용자가 네임서버를 지정해야하는 등 제약이 있음

- DNS통신은 분산된 DNS서버시스템을 통해 IP주소정보를 확인하는 과정으로 여러 개의 서버간 통신이 발생하는데, DNS통신이 암호화되어 전송된다고 하더라도 도메인네임을 IP주소로 반환하는 과정에서는 운영체계(OS)와 브라우저 등이 DoT를 지원해야함

○ (탐지방법) DoT는 전용포트 853을 사용하기 때문에 다른 트래픽과는 구별이 가능하기 때문에 모니터링 및 접속 차단이 가능함

- 현재 DNS요청은 53번 포트를 통해 평문으로 전송되는데 TLS프로토콜을 통해 DNS 쿼리를 전송할 경우 자체 전용 포트인 853을 기반으로 TCP 연결 프로토콜로 사용하고 TLS 암호화 및 인증을 통해 연결하게 됨

- 전용포트를 사용하면 트래픽 관리가 가능하다는 장점이 있으나, DNS통신 암호화는 DNS통신을 암호화해서 보호하겠다는 것이 목적이기 때문에 웹서버나 브라우저를 중심으로 빠르게 확산될 것으로 예상되지 않음

- 따라서 DoT가 상용화되더라도 현재의 불법사이트 접속차단의 실효성에 큰 영향을 미칠 것으로 예상되지 않으며, 전용포트의 트래픽을 대상으로 한 불법사이트 접속시도에 대한 차단도 기술적으로는 가능할 것으로 예상함

○ (개발일정) DoT 표준화는 2015년 IETF DPRIVE WG에서 논의가 시작되었으며 첫 번째 제안표준(RFC 7858)은 2016년 5월에 제안되었고, 이후 2018년 3월에 새로운 업데이트 표준(RFC 8310)이 제정됨

다. 전송계층 표준화 동향

○ (전송계층 보안기술) SSL/TLS통신은 HTTPS라는 통신채널을 사용하며 서버인증(server authentication), 클라이언트 인증(client authentication), 데이터암호화(data encryption) 기능을 제공하는 기술

- 초기 협상단계(핸드쉐이킹 단계)와 인증단계를 거쳐 통신암호화가 시작됨

① 초기 협상단계: 클라이언트와 서버간에 ClientHello, ServerHello 메시지를 교환하는 단계로서, 클라이언트가 서버에게 서버 인증서를 요구하는 단계

② 인증단계: 서버에서 공개키, 서버명, 인증기관 주소 등을 포함한 인증서를 클라이언트에게 반환하는 단계로서, 이때 서버는 클라이언트가 제시한 것 중 자신이 선택한 암호화 방식

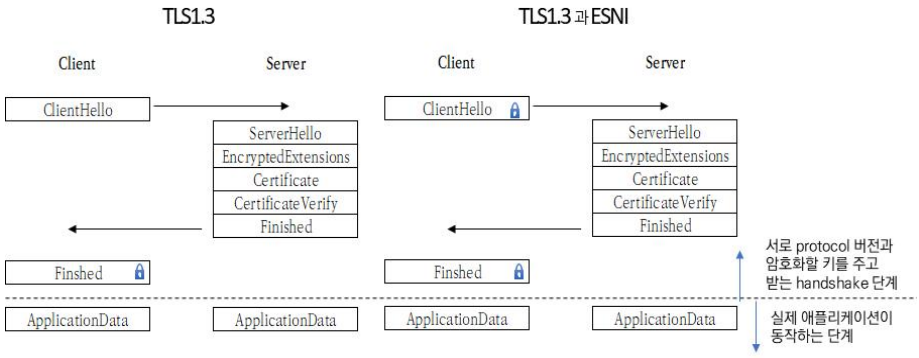
- 현재 접속차단 조치는 초기협상단계에서 평문 통신을 확인하고 접속을 차단하는 방식임

○ (ESNI개념) ESNI기술은 전송계층보안표준인 TLS1.3에 적용하기 위한 확장표준으로, 클라이언트에서 서버로 가는 초기메시지(Client Hello)정보까지 암호화하는 방식

- ESNI는 클라이언트가 서버에 통신을 시작하기 위해 전달하는 클라이언트 헬로 메시지를 암호화하여 접속정보의 비밀을 유지하는 방식

- 아래의 그림에서 보듯이 TLS 1.3에 ESNI가 적용되지 않을 경우 클라이언트가 서버에 접속할 때 접속하고자 하는 서버네임이 노출되게 되나, ESNI가 적용되면 클라이언트 헬로 메시지까지 암호화되어 접속정보를 확인할 수 없음

[그림 2-7] TLS1.3과 ESNI적용할 경우 암호화되는 범위



○ (기술방식) 클라이언트와 서버간의 공개키 전달을 DNS통신단계에서 실시하고, HTTP 통신의 헤더부분인 SNI는 암호화하여 서버에 송신하는 방식

- 클라이어트와 서버가 모두 암호를 해독할 수 있는 키를 공유하고 있는 경우에만 정상적인 통신이 가능하기 때문에, 클라이언트와 웹서버간의 헬로메시지가 전달되기 이전에 상호간의 공개키 공유과정이 필요함

- TLS에서는 암호화하는 방법을 표준으로 특정하지 않고 핸드쉐이크 과정*에서 클라이언트와 웹서버가 대칭암호키(encryption keys)를 공유

  * 핸드쉐이크 과정은 서버와 클라이언트 통신이 시작되는 지점으로 키교환이 아직 이뤄지지 않은 상황이기 때문에 암호화되어 있지 않은 평문으로 구성되며, 이 과정에서 클라이언트와 웹서버가 이후의 암호통신에서 통신내용을 해독할 수 있는 대칭암호키를 공유하게 됨

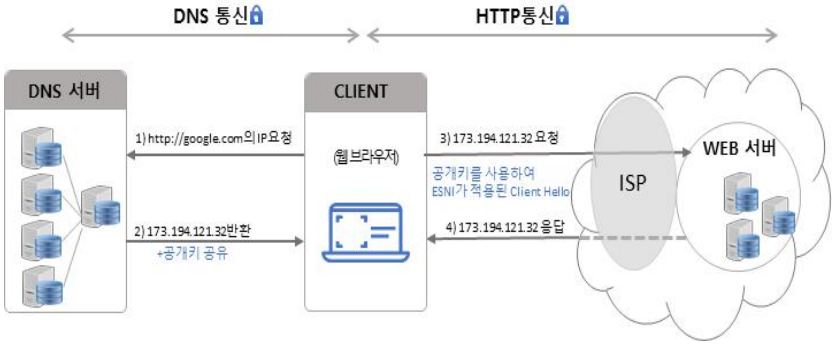
- 현재 평문으로 전송되는 handshake단계의 SNI에서 서버네임이 노출되기 때문에, ESNI는 SNI를 암호화함

- 단, 클라이언트와 서버가 TLS 암호화 키를 협상하기 전에 클라이언트 hello 메시지가 전송되므로 ESNI 암호화 키는 DNS통신에서 전달되어야 함

○ (공개키공유) 암호화된 DNS통신(DoH나 DoT)에서 키교환이 이뤄진 상태에서 SNI까지 암호화되면 접속하려는 주소나 도메인 정보를 숨길 수 있음

- DoH나 DoT를 이용해서 웹서버가 해외 공개 DNS서버(클라우드 플레어, 구글 Public DNS)의 레코드에 자신의 공개키를 올려놓아 DNS쿼리 전송단계에서 클라이언트가 웹서버에 접속하기 전에 공개키 정보를 공유할 수 있음

[그림 2-8] DNS암호화기술과 ESNI의 연동



- DNS통신 암호화만으로는 현재의 접속차단 조치를 우회하기는 어렵고, DNS통신 암호화(DoH 또는 DoT적용)와 HTTP통신에서 TLS핸드쉐이크의 SNI부분을 암호화하는 ESNI(암호화된 SNI)가 함께 사용될 경우 우회가능성이 있다는 지적이 있음

  * ESNI나 DoH 모두 개별적으로는 우회접속 가능성이 없음

○ (개발일정) 현재 ENSI기술은 TLS 1.3 표준에 포함되지 않았으며, 별도의 문서로 분리되어 IETF에서 논의 중에 있음

- 2018년 8월에 제정된 IETF의 TLS 1.3표준(RFC 8446)에 대한 확장표준 중 하나로서 SNI필드 정보를 암호화하는 ESNI가 제안되었으나, ESNI 기술은 가시성(Visibility)† 문제로 TLS 1.3에 포함되지 못함

  † 가시성이란 네트워크 트래픽을 운영·관리하기 위해서는 네트워크의 모든 구성요소들을 눈으로 확인하고, 발생할 수 있는 잠재적 병목 현상을 식별할 수 있어야 함을 의미하는데, SNI필드 정보가 암호화되면 네트워크 트래픽 모니터링 및 장애 문제 해결과 같은 네트워크 관리차원에서 정보확인이 어려울 수 있어 통신안정성을 위해 TLS1.3에서 제외함

- 현재는 IETF의 TLS WG에서 RFC 8446과는 별도로 분리되어 표준화를 위한 논의를 진행하고 있음

  * 2020년 6월 기준으로 일곱 번째 버전이 작성되어 있음

제 2 절 주요사업자의 보안접속 기술 적용동향

1. 보안접속 기술 적용 동향

가. DNS통신 암호화기술(DoH, DoT) 채택 동향

(1) 운영체제

○ (개념) 운영체제(Operating System)는 컴퓨터 사용자와 컴퓨터 하드웨어 간의 인터페이스로서 컴퓨터 시스템의 자원들을 관리하는 역할을 수행

- 대표적인 OS는 마이크로소프트, 애플 등이 공급하고 있어 이들의 보안통신 기술 채택 여부가 접속차단의 실효성에 영향을 미칠 수 있음
- 국내 데스크톱PC OS의 시장은 마이크로소프트 윈도우(88.8%), 애플 맥OS(8.2%), 리눅스(0.6%), 구글크롬OS(0,03%)의 점유율을 보이고 있어, 마이크로소프트 윈도우의 보안기술채택 여부가 중요(statcounter.com, '20. 8월 기준)
- 국내 모바일과 태블릿 OS시장은 안드로이드(74.6%), iOS(25.4%)기 차지하고 있음(statcounter.com, '20. 8월 기준)

○ (마이크로소프트) 2020 년 5 월 DoH를 활성화할 수 있는 Windows 10 Insider Preview Build 19628을 출시

- 2019 년 11 월, Microsoft 는 자사의 기업블로그에서 DoH를 시작으로 Microsoft Windows 에서 암호화 된 DNS 프로토콜 지원을 구현할 계획을 발표(Gallager, 2019)
- DoH를 활성화하기 위해서는 윈도우10 이상을 사용해야하며 최신버전으로 업데이트를 실시한 후, 사용자가 직접 DoH를 활성화하는 설정변경이 필요함
- 이전 운영체제를 사용할 경우 HTTPS를 통한 DNS통신은 불가능함

  ※ 국내 데스크탑PC에서 사용하는 윈도우의 버전별 점유율은 윈도우10이 83.07%, 윈도우7이 12.8%, 윈도우8.1이 2.7%, 윈도우8이 0.57%, 윈도우 XP가 0.82%를 차지함

- Windows 10을 보유하고 있다고 하더라도, DoH를 활성화하여 보안통신을 하려면 운영 체제

레지스트리를 변경하고 DNS서버를 수동 편집해야하는 불편함이 있음

○ (애플) 암호화된 DNS 통신을 위한 기술 지원 계획을 발표하고 일부 적용

- 개발자 컨퍼런스인 '세계 개발자 컨퍼런스(WWDC) 2020(2020년 6월22일)'에서 애플은 ios와 macOS 운영체제에서 암호화된 DNS 통신을 위한 기술 지원 계획을 발표
- 2020년 10월에 발표한 iOS 14 와 macOS 11 은 HTTPS를 통한 DNS(DoH)와 TLS를 통한 DNS(DoT)를 모두 지원
- 그러나 DoH와 DoT 모두 자동으로 적용되는 것은 아니고, 이용자가 설정앱에서 DNS 암호화를 직접 설정해야함
- 또한 기업내 WI-FI을 사용하거나 카페나 기차 등에서 WI-FI에 접속하는 캡티브 네트워크에서는 DNS암호화 기능이 자동으로 해제됨

(2) 웹브라우저

○ (모질라) 구글과 함께 DoH의 개발과 확산을 주도하고 있는 대표적인 브라우저 사업자

- 2018년 3월부터 클라우드플레어와 함께 자사의 파이어폭스 브라우저에 DoH를 적용할 수 있는 테스트를 실시
- DoH적용과 관련해서 영국ISP사업자 연합회인 ISPA(Internet Service Providers Association) 및 인터넷감시재단(IWF)의 문제제기가 있어, 2019년 9월25일에 영국에서 DoH를 기본으로 제공하지 않을 것을 확인함(ISP review, 2019. 9. 25)

  ※ 영국 ISPA는 DoH개발과 확산이 불법콘텐츠 등을 필터링 할 수 없게 만들어 인터넷 환경의 건전성을 저해한다고 지적하고, 모질라를 2019년에 인터넷 악당(Internet Villian) 어워드에 후보를 지명

- 2020년 2월부터 미국 이용자를 대상으로 DoH를 기본설정으로 제공

<표 2-1> 모질라 파이어폭스의 DNS암호화 지원 동향

일정	주요 내용
2018년 3월	클라우드플레어와 파트너쉽을 통해 파이어폭스 사용자를 위한 DoH를 제공하는 테스트를 실시

2019년 9월	영국 파이어폭스 사용자에게는 DoH를 기본 설정으로 제공하지 않을 것임을 공표
2020년 2월 25일	미국에 있는 모든 파이어폭스 사용자에게 DoH를 기본설정으로 제공
2020년 6월 25일	파이어폭스의 신뢰할 수 있는 리졸버 프로그램(TRR: Firefox's Trusted Recursive Resolver)에 미국 컴캐스트 참여 * Cloudflare, Comcast, NextDNS가 현재 파이어폭스의 Trusted Recursive Resolver (TRR) program에 참여중

- 2020년 6월에 미국 컴캐스트가 ISP사업자로서 최초로 파이어폭스의 Trusted Recursive Resolver (TRR) program에 참여함

  * Comcast와 Mozilla는 2019 년 이후 DNS 암호화에 관해 논의 해 왔으며 2020 년 3 월 Comcast 네트워크의 Firefox 사용자에게 DoH를 베타버전으로 배포하기로 합의함. 즉, 컴캐스트의 Xfinity 사용자가 모질라 파이어폭스에서 DoH를 사용할 경우, Xfinity의 리졸버에서 이용자의 웹브라우징 히스토리를 트래킹하지 않는다는 것을 의미함

○ (구글크롬) 구글 브라우저인 크롬에서 DoH를 적용하고 있으나 기본설정으로 제공하고 있지는 않음

- 모질라와 함께 DoH확산을 주도하고 있는 사업자인 구글은 2018년 3월부터 DoH를 제공하는 테스트를 시작하고, 2019년 6월부터 크롬버전84부터 이용자가 수동으로 DoH를 적용할 수 있도록 변경
- 즉, 사용자 인터페이스 내에서 사용할 사전 설정 또는 사용자 지정 DoH 서버를 수동으로 지정하는 방식으로 디폴트(default)방식은 아님
- DoH를 기본으로 설정하는 시기에 대해서는 명확하게 밝히지 않고 있음

○ 이 외에도 오페라와 네이버 웨일 등이 DoH 기능을 지원하는 베타버전을 제공하고 있음

- 오페라는 2020년 1월부터 베타버전에서 DNS-over-HTTPS 기능을 지원함
- 네이버는 2020년 2월 27일 '네이버 웨일'브라우저의 베타버전(v2.7.95.6)에서 DNS-over-HTTPS 기능을 지원함
- 그러나 두 브라우저 모두 베타버전에서만 DoH를 제공하고 있고, DoH가 기본설정은 아니며 이용자가 설정변경을 하고 클라우드플레어(1.1.1.1)의 DoH 리졸버를 지정해야함

(3) DNS 서버

○ 현 시점에서 국내 주요 ISP의 DNS들은 DoT와 DoH 모두를 지원하지 않음

<표 2-2> 국내 주요 DNS서버의 DoT와 DoH지원 현황

서버명		DOT	DoH
국내	KT DNS	X	X
	SKBroadband	X	X
	LGU+	X	X
	LG Hellovision DNS	X	X
	C&M	X	X
	온세통신(신비로)	X	X
	티브로드	X	X
글로벌	Cloudflare DNS	O	O
	Google Public DNS	O	O
	IBM Quad9	O	O

○ 현재는 해외 DNS 서버에서 클라우드플레어, 구글 퍼블릭 DNS, IBM 쿼드9만이 DoH와 DoT를 지원하고 있음

(4) 웹서버

○ 최종적으로 웹에서 정보를 제공하는 웹사이트(서버)가 암호화된 통신을 지원해야 접속 차단을 우회할 수 있으나, 웹서버 중에 DoH나 DoT를 지원하는 현황을 명확하게 파악할 수 없음

- 주요 인터넷서비스 사업자 중에서는 페이스북이 2018년 12월에 클라우드플레어 DNS와 공동으로 DoT의 파일럿 테스트를 실시한 바 있었음

나. TLS1.3과 ESNI 채택 동향

○ 전 세계 브라우저 시장을 주도하는 구글이 TLS1.3으로의 전환을 추진하고 있어 중장기적으로는

TLS 1.3으로 전환될 예정

- 전세계 웹브라우저 시장에서 점유율이 70%에 이르는 구글 크롬이 HTTPS (TLS1.2이상)으로의 전환을 주도하고 있어 보안접속 트래픽의 비중이 높아질 전망

  ※ 시장조사기관 스탯카운터(https://gs.statcounter.com/) 에 따르면 2020년3월 기준 전 세계 웹브라우저 점유율은 크롬이 69.35%로 1위고 파이어폭스 9.54%, 사파리 8.51%, 엣지 4.64%, IE는 3.47%. 한국에서는 크롬이 71.56%, IE 13.76%, 엣지 4.73%, 웨일 3.93%, 사파리 3.34%, 파이어폭스 1.61% 순

- Chrome, Firefox, Edge 및 Safari 등 주요 브라우저는 이전 TLS에 대한 지원을 중단함으로써 다음세대의 TLS 1.3으로의 전환에 가속도를 붙이려는 계획을 발표한 바 있음

  ※ 2018년 10월에 주요 브라우저 개발사들이 2020년 3월부터 TLS 1.0(개발후 20년)과 1.1(개발후 12년)에 대한 지원을 중단한다고 발표

○ 암호화된 SNI(ESNI)가 확산되기 위해서는 TLS 1.3기반의 HTTPS통신이 전제되어야 하나, 아직도 이전 버전인 TLS 1.1과 1.2의 통신 비중이 높음

- 주요브라우저의 주도로 HTTP 트래픽이 HTTPS 트래픽으로 대체되고 있는 것은 사실이나 TLS1.3으로의 전환이 빠르게 진행되고 있다고 보기는 어려움
- '18년도 3사분기 기준 BuitWith의 조사에 따르면 상위 트래픽을 차지하는 10만개의 웹사이트의 약 21% 정도가 여전히 HTTPS를 사용하고 있지 않고, 약 68개의 웹사이트가 여전히 TLS1.0을 지원하고 있음(Hostingtribunal, 2020)
- 95.2%의 웹사이트들이 TLS 1.1과 TLS 1.2를 지원하고 있어, 여전히 TLS 1.2가 인터넷보안 표준으로 사용되고 있는 상황
- 2019년 5월 기준으로 단지 14.2% 의 웹사이트만이 TLS 1.3을 지원
- 아직까지 TLS 1.3구현과 관련하여 운영상의 애로사항이 있다고 생각하는 IT관련 직무 담당자 비중이 93%, 보안상의 우려가 있다고 응답한 비중은 91%로 TLS1.3을 적용한 웹서버가 빠르게 확대될 것으로 보기는 어려움

○ 웹서버들의 TLS 1.3으로의 전환속도가 더디고 코로나 확산으로 인해 최근 구글, 마이크로소프트, 모질라 등도 TLS 1.0과 1.1의 비활성화 계획을 철회함

- (크롬) 금년도 5월부터 크롬 83부터 TLS 1.0과 1.1 버전의 지원을 중단시킬 예정이었으나,

연기되어 일정이 명확하지 않음

- (모질라) 2020년 3월 10일에 출시한 파이어폭스 74.0부터 TLS 1.0과 1.1에 대한 지원 기능을 비활성화했으나 이를 취소하고 다시 TLS 1.0과 1.1에 대한 지원을 시작함
- (마이크로소프트) 에지 브라우저 84 버전(2020년 7월)과 익스플로러11버전(2020년9월)부터 TLS 1.0과 1.1에 대한 지원을 중단할 계획이었으나 코로나 19의 확산으로 일정 지연
- (네이버) 네이버의 브라우저인 네이버웨일은 현재까지 ESNI 적용 계획이 없는 것으로 확인됨
- 따라서, ESNI의 전제조건인 TLS 1.3의 채택속도는 더뎌질 것으로 전망됨

○ 특히 기술표준화 방식이 TLS 1.3 이후로 적극적 표준화 방식으로 변화됨에 따라, 한동안은 현재의 기술적 조치가 완전히 무력화되지는 않을 것으로 예상됨

- IETF가 2018년 8월28일 TLS 1.3(RFC8446)발표했으나 최종안이 승인되었다는 의미가 표준이 완결되었다는 의미는 아님
- TLS의 표준화 방식이 TLS 1.2까지는 선배포 후 패치를 추가하여 기술을 개선(design-release-break-patch)하는 반응적 표준화(reactive standardization) 방식이었다면, TLS 1.3부터는 잠재적 위협과 기술결함을 수정한 후에 배포(design-break-fix-release)하는 적극적 표준화(proactive standardization) 방식으로 변화
- 따라서 SNI필드 정보를 확인하고 차단하는 기술적 조치가 완전하게 무력화되는 기술이 개발되는 데까지는 오랜 시간이 걸릴 것으로 예상됨

2. 기술동향에 따른 접속차단 실효성 이슈

○ 일부 사업자들 중심으로 DNS 암호화 기술이 채택되었다 하더라도, 우회접속을 위해서는 웹브라우저와 DNS서버 모두 DoH나 DoT를 사용하여야 하기 때문에, DNS암호화만으로는 우회접속이 불가능함

- 불법사이트 소유자의 웹서버, 인터넷이용자의 OS와 웹브라우저, 인터넷이용자의 DNS쿼리를 처리하는 DNS서버가 모두 ① DoH나 DoT를 지원해야하며, ② TLS1.3과 ESNI를 지원해야하는 전제조건에서만 현재의 접속차단을 우회할 수 있음

○ 트래픽을 관리하기 위해서는 가시성(visibility)*이 필요하기 때문에, 가시성이 낮은 DoH가 기존의 DNS통신을 완전히 대체하는 상황은 빠르게 진전되지 않을 것으로 예상함

○ TLS1.3 기술표준에서 ESNI가 포함되지 않았기 때문에 ESNI기술이 개발되어 상당한 수준으로 채택될 때까지는 상당한 시간이 걸릴 것으로 현재의 HTTPS 차단이 유효함

- 또한 ESNI를 실제 구현하고 확산하기 위해서는 연동이 필요한 기술들이 있기 때문에 ESNI 단독으로 동작이 불가능하며 적용이 쉽지 않아, 접속차단의 기술적 조치를 변경할 만큼 시급한 상황으로 판단하지 않음

○ 현 시점에서는 기술자체에 대한 대응은 시기상조이며 무리한 기술적 대응은 오히려 개인정보침해 및 과잉차단의 우려가 있음

- 현 시점에서는 주요 사업자들의 새로운 보안접속 기술의 채택여부와 확산 추세를 계속 지켜보는 것이 필요

제 3 절 불법정보 유통방지를 위한 기술과제

1. 암호화기술 개발에 따른 접속차단 실효성 평가와 기술대응 방향

○ 주요 웹서버 및 브라우저를 중심으로 DNS암호화기술 채택이 점차 증가할 전망

- 파이어폭스, 크롬 등에서 DoH를'정식 기능'으로 배포한 상황이며, 점점 더 많은 웹 브라우저들이 DoH기능을 탑재할 계획을 가지고 있어 DoH는 채택이 점차 증가할 것으로 예상됨
- DoH의 경우 HTTPS표준 포트인 443을 사용하기 때문에 DoH 사용여부를 확인하거나 불법사이트 접속시도 여부를 확인할 수 없다는 한계
- ISP가 사용자의 동의를 얻어 별도의 모니터링 프로그램을 사용자 단말(PC, 태블릿, 스마트폰)에 설치를 한다면 DoH 사용 여부 설정을 확인할 수 있으나, 이 경우에는 DoH를 사용해 통신을 암호화하고자 하는 목적과 상치되기 때문에 사용자 동의를 얻기 어려울 것으로 예상

○ 다만, 현재 DNS차단, URL차단, HTTPS 차단이 모두 적용되고 있기 때문에, DNS통신 암호화 기술이 적용될 경우에도 접속차단이 가능함

- DNS통신이 암호화되더라도 클라이언트가 웹서버에 접속요청을 할 때에 URL차단이나 HTTPS 차단이 가능
- 불법사이트 소유자의 웹서버, 인터넷이용자의 OS와 웹브라우저, 인터넷이용자의 DNS쿼리를 처리하는 DNS서버가 모두 ① DoH나 DoT를 지원해야하며, ② TLS1.3과 ESNI를 지원해야하는 전제조건에서만 현재의 접속차단을 우회할 수 있음

○ 또한 일부 사업자들 중심으로 DNS 암호화 기술이 채택되었다 하더라도, 우회접속을 위해서는 웹브라우저와 DNS서버 모두 DoH나 DoT를 사용하기 때문에 우회접속이 쉽지 않음

- 현재 DoH를 지원하는 DNS는 Cloudflare, Google public DNS, Quad9 등으로 국내에서 대중적으로 사용되고 있지 않음
- DoH를 지원한다고 해서 DoH가 반드시 기본(default)으로 제공되는 것을 의미하지 않으며, 대부분의 경우 이용자가 직접 DoH를 설정해야하기 때문에 한계가 있음

- DoH를 설정한다고 해서 Encrypted SNI(ESNI)를 지원하지는 않으면, 사실상 현재의 접속차단 조치를 완전하게 우회할 수 없음

○ 트래픽을 관리하기 위해서는 가시성(visibility)† 이 필요하기 때문에, 가시성이 낮은 DoH가 기존의 DNS통신을 완전히 대체하는 상황은 빠르게 진전되지 않을 것으로 예상함

† 가시성이란 네트워크의 모든 구성요소들을 눈으로 확인하고, 발생할 수 있는 잠재적 병목현상을 식별·해소하는 것으로써, 운영·관리에 있어서 의미 있는 통계를 산출함으로써 네트워크에 대한 보다 심도 있는 관리가 가능하도록 함을 의미함(차종환, 2016. 7. 8.)

- 암호화기술은 이용자의 접속정보를 암호화하기 때문에 사이버 보안에 도움이 될 수도 있으나, 다른 한편으로는 네트워크 트래픽의 분석 및 모니터링을 방해하기 때문에 관리상의 어려움이 발생
- 실재로 도메인네임시스템(DNS)의 통신 내용을 암호화해주는 DoH 기능을 해킹에 악용하는 사례가 발생하고 있음

※ 이란 지능형지속위협(APT) 그룹으로 알려진 '오일리그'가 DoH프로토콜을 사용해 데이터를 암호화한 뒤 정보를 유출하는 해킹을 시도한 바 있으며(ZDNET, 2020. 8. 6), DoH를 사용하여 트래픽 모니터링을 회피해 DDos공격을 시도하는 고들루아(Godlua) 공격시도도 발견됨(데일리시큐, 2020.8.5.)

- 특정 포트를 통해 들어오는 DoT의 경우는 DNS 요청을 차단하거나 관리하는 것이 가능하기 때문에 DNS통신 암호화를 추진하는 측에서도 채택 속도가 상대적으로 더딜 것으로 예상되며, DoT적용 후에도 기술적 방법을 통해 불법사이트 접속차단이 가능할 것으로 예상함

○ TLS1.3 기술표준에서 ESNI가 포함되지 않았기 때문에 ESNI기술이 개발되어 상당한 수준으로 채택될 때까지는 상당한 시간이 걸릴 것으로 상당기간 동안 현재의 HTTPS 차단이 유효함

- 현행 TLS1.3 기술표준에서도 서버네임이 포함된 클라이언트헬로 메시지는 암호화되지 않았기 때문에 현재의 HTTPS차단은 유효함
- 웹서버와 데이터 센터가 TLS1.3규격을 적용하는 데 많은 시간이 걸릴 것으로 전망됨
- 아직도 TLS 1.2보다 더 오래된 버전을 사용하는 서버들이 있으며, 경험적으로도 TLS

1.2 표준이 2008년에 발표되어 현재까지 12년간 최신표준인 것을 고려할 때 ESNI가 적용된 TLS1.3이 더 낮은 버전의 트래픽을 모두 대체하기에는 많은 시간이 걸릴 것으로 예상됨

- ESNI 기술은 DNS 서버에서 키 교환을 하는 것이 선행되어야 가능한 기술이기 때문에 DNS 서버와 웹서버를 함께 운영하는 회사(예: 클라우드플레어) 외에는 구현하기가 쉽지 않은 상황

○ DoH와 ESNI가 모두 사용될 경우에도 IP주소 기반 차단은 가능

- DoH와 ESNI가 모두 사용되면 DNS통신과 웹통신 모두 서버네임을 암호화하기 때문에 기존의 HTTPS차단은 상당히 어려워질 수 있음
- 다만 DoH와 ESNI를 사용하면 우리가 접속하는 사이트의 서버네임은 암호화되지만 그 사이트의 'IP주소'는 ISP에 노출
- 따라서 DoH와 ESNI가 차단을 어렵게 하는 기술이지만 접속차단 자체가 100% 무력화된다고 볼 수 없음

○ 현 시점에서는 기술자체에 대한 대응은 시기상조이며 무리한 기술적 대응은 오히려 개인정보침해 및 과잉차단의 우려가 있음

- 기술적 측면에만 한정할 경우 ① DoH 패킷과 ESNI 필드의 복호화 기술, ② HTTPS 패킷 내 접속하려는 서버의 IP 주소 확인을 통한 웹사이트 매핑 기술 정도가 가능한 대안

  ※ 복호화(decoding)란 암호화의 역과정으로써, 평문에 암호기술을 적용하여 변환된 암호문을 다시 평문으로 복원하는 과정을 의미함.

- 그러나 복호화 기술을 적용하면 분명히 웹브라우저에서 경고를 띄우거나 차단하는 기능이 적용될 것이기 때문에 이론적으로는 가능하나 실제적으로 적용이 어렵다는 의견이 있음

○ 현 시점에서는 주요 사업자들의 새로운 보안접속 기술의 채택여부와 확산 추세를 지켜보는 것이 필요

- ESNI기술은 SNI필드 정보까지 암호화하기 때문에 현재의 HTTPS차단과는 배치되는 기술이나, TLS 1.3의 확장판일 뿐 모든 TLS1.3 통신에 적용되지는 않기 때문에' 현 시점이나 단기적으로 HTTPS차단을 무력화할만큼 확산되지 않았다고 보는 것이 바람직함
- 또한 ESNI를 실제 구현하고 확산하기 위해서는 연동이 필요한 기술들이 있기 때문에 ESNI 단독으로 동작이 불가능하며 적용이 쉽지 않아, 접속차단의 기술적 조치를 변경할 만큼 시급한 상황으로 판단하지 않음
- 일반적으로 보안 기술표준들은 기술을 만들어 배포하면서 표준화를 추진하는 전략을 많이 쓰기 때문에 표준화 완료 시점과 기술의 확산 시점의 관계는 크게 중요하지 않음
- 따라서 표준이 제안되었다 하더라도 기술이 확산되는 것과는 시기적인 차이가 있음
- 현 시점에서 클라우드플레어 외에는 웹서버 업체들의 DoH와 ESNI채택 비율이 높지 않기 때문에 확산추세를 지켜보는 것이 필요하며, 모든 암호화기술이 불법사이트 접속만을 위해 사용되는 것이 아니기 때문에 기술자체에 대한 시급한 대응은 적절하지 않음

2. 우회접속에 따른 접속차단 실효성 평가와 기술대응 방향

가. VPN방식의 우회접속과 접속차단 실효성 평가

(1) VPN방식의 우회접속

○ (개념) VPN(가상 사설망, Virtual Private Network)은 인터넷과 같은 공중망(Public Network) 환경에서 전용회선을 이용하는 효과를 위해 공중망을 가상화하여 암호화된 보안 네트워크를 구축하는 기술방식

- 보다 저렴한 비용으로 보안이 강화된 전용회선의 효과를 누리기 위해 기업이나 공공기관의 원격업무관리 등에 광범위하게 사용됨

  예) 특정기업이 자사만을 위한 보안이 강화된 네트워크를 구성할 때 전용망을 구축하게 되는데, 이러한 사설망을 물리적으로 구성할 경우 많은 설치비용과 운영비용이 요구됨. 따라서 KT망처럼 공중망(public network)에 가상으로 이를 구축하는 기술이 VPN이라고 할 수 있음.

- 이러한 사설망 기술에서 중요한 것은 다른 망으로부터 분리되어 있어서 보안적인 측면에서 우수하고 다른 망의 트래픽으로부터 독립적이라는 측면에서 QoS등이 유지된다는 측면에서 장점

○ (우회 우려) VPN을 적용한'차단 우회앱'이나 '우회프로그램'을 이용하여 접속차단 조치를 우회할 수 있다는 우려가 제기되고 있음

- VPN이 불법사이트 차단조치를 우회하기 위해 만들어진 기술이 아님에도 불구하고 차단조치가 우회된다고 하는 이유는, VPN을 이용할 경우 터널링 기법이 사용되어 원래 IP 패킷에 있던 데이터가 암호화되어 목적지 IP주소를 확인하여 차단하는 방식이 적용되기 어려울 수 있기 때문임

- 터널링(tunneling)기술이란, 라우터와 라우터 사이에 가상화된 전용고속도로를 연결하는 사용하는 방식으로 터널링 과정에서 원래 IP주소가 감춰짐

  ▸ 예를 들어 물리적으로 A와 C사이의 연결을 위하여 A-B-C라는 물리적인 경로가 필요하다고 할 때 A-C사이를 논리적 연결을 통해서 가상화하여 연결하는 방식

  ▸ 이를 터널링 기법† 이라고 부르는데, 터널링 기법을 사용하게 되면 기본적으로 원래 IP packet의 데이터를 캡슐화(encapsulation)‡ 하여 사용하면서 원래 IP주소는 감춰지고 새로운 IP주소를 사용하게 됨

  † 터널링은 데이터 스트림을 인터넷 상에서 가상의 파이프를 통해 전달시키는 기술(정보통신기술용어해설)로, 터널링에 사용되는 프로토콜은 다양한 방법이 있는데 2계층(데이터링크계층)에서 사용되는 터널링 기법들은 PPTP, L2TP, L2F가 있고 3계층(네트워크 계층) 프로토콜에서는 IPSec, MPLS, GRE, 7계층에서는 SSL 등의 다양한 기법들이 존재함.

  ‡ 캡슐화는 OSI 계층모델에서 데이터가 각 계층을 지나면서, 상위 계층으로부터 온 정보에 자신의 계층 특성을 담은 제어정보를 헤더로 붙여서 안의 구현내용을 은닉하는 과정(정보통신기술용어해설, 캡슐화). 아래의 그림과 같이 OSI의 각 계층에서 정보가 응용계층에서 물리계층까지 전달될 때 상위계층에서 전달된 데이터에 각 계층의 특징제어정보(헤더, header)를 추가하는 과정이 캡슐화 과정이라고 할 수 있음.

[그림 2-9] 통신계층의 캡슐화 과정

출처: 정보통신기술용어해설

- VPN의 터널링 과정에서 원래 목적지 IP주소가 캡슐화되어 전송되기 때문에, 목적지 IP주소를 식별하여 접속을 차단하는 필터링 기법들이 무력화될 수 있음

(2) VPN우회로 인한 접속차단의 실효성 평가

○ (기술적 특성) 국내 인터넷 이용자가 불법사이트가 불법이 아닌 국가의 IP를 경유해서 해외 VPN에 접속할 경우 VPN을 경유한 이후의 통신내용을 탐지할 수 없음

- 국내 ISP의 차단장치는 국내 인터넷이용자가 해외불법사이트를 접속하지 않도록 차단하는 장치이기 때문에 불법사이트로 지정되지 않은 해외 VPN으로 접속하고자 하는 접속요청을 차단하지 않음
- 일단 국내 인터넷이용자가 차단대상이 아닌 해외VPN서버로 접속 요청을 하여 국내 ISP의 차단장치를 통과한 후, 해외VPN서버를 경유하여 국내에서 차단된 웹서버에 접속요청을 하게 되어 정보를 반환받을 경우, 국내 ISP의 차단장치는 이를 확인할 수 없음
- 기술적으로는 ISP의 차단장치에서 특정 VPN으로의 접속시도 여부를 확인할 수 있거나 또는 해외 웹서버가 특정VPN의 접속요청을 확인할 수는 있지만, 해당 VPN서버를 경유하여 접속하는 통신의 내용을 ISP의 차단장치가 탐지할 수 없음

○ (제공현황) VPN은 불법적인 용도를 위해 개발된 보안네트워크 기술이 아니기 때문에 프로그램 개발·배포 및 VPN서비스 제공에 법적이 제한을 둘 수 없고, 이로 인해 국내외 다수의 사업자가

제공 중에 있음

- 안정적이고 보안수준이 높아 QoS가 보장이 되는 VPN의 경우(예:MPLS VPN*)는 일정 규모 이상의 기간통신사업자(예: KT Cloud VPN, KT Biz VPN, SK브로드밴드 VPN 등)와 부가통신사업자(예: 시스코 VPN, NTT 코리아 VPN 등)에 의해서 제공되고 있으며, 이들 서비스는 불법사이트 접속용도로 사용될 가능성이 매우 낮음

  ※ 공용의 인터넷 상에서 가상의 VPN (IP-VPN)을 구성하는 기술로, 망사업자(ISP등)가 전용의 라우팅테이블을 별도로 구축하여 공용망과 분리하여 VPN을 제공하는 방식

- 다만 인터넷이용자들 사이에서 차단우회 프로그램이나 우회어플 (Intra, 유니콘)로 알려진 프로그램을 제공하는 사업자들은 대체로 신고면제대상인 소규모 부가통신사업자들에 의해서 제공되고 있는 것으로 파악됨

  ※ 차단우회앱, 차단우회프로그램 등은 명칭은 각기 달라도 기술적으로는 VPN방식을 사용하고 있는 것으로 확인됨

<표 2-3> 주요 앱 또는 웹스토어의 VPN 프로그램 제공현황

구분(운영체제)	VPN 프로그램 동향
구글 웹스토어(windows)	VPN unlimited,Touch VPN, ZenMate, uVPN, Hotspot Shield 등
구글 플레이스토어(안드로이드)	Touch VPN, Browsec VPN, NordVPN, 유니콘, ASPEAR, 미어캣, Express VPN, Turbo VPN, Ultra Surf Security 등
애플 앱스토어(iOS)	유니콘, VPN master, Turbo VPN, Express VPN 등
원스토어(안드로이드)	터보VPN, Ghost VPN, Fast VPN, 슈퍼VPN 등

○ (실효성 평가) VPN을 이용한 우회접속이 기술적으로 가능하나 유료VPN의 비용적 부담, 무료 VPN의 속도와 용량제한, 개인정보유출 등의 문제가 있어 일반인이 불법정보 접속 등의 개인적 용도로 사용하는 경우는 제한적임

- VPN은 프로그램 개발·판매만으로 사설망 제공업무가 끝나는 것이 아니라 지속적인 서버 관리· 운영이 요구되는 사업이기 때문에, 속도가 보장되는 VPN의 경우는 대부분 유료로 제공되고 있음

- 유료 VPN의 경우 업무용으로 장기약정으로 계약하는 경우가 일반적으로 일반인이 불법정보 접속 등의 개인적 용도로 사용하는 경우는 제한적임. 또한 차단 우회를 위해서 유료 해외 VPN을 사용할 경우 비용부담이 있어 청소년 대상으로 활성화되기

어려움

- 무료로 알려진 VPN의 경우 용량, 기간, 속도가 제한되는 일종의 체험판 형태로써 지속적으로 사용할 수 없으며, 용량과 속도 제한으로 스트리밍 영상을 시청하는 데 적절하지 않은 것으로 생각됨

- 시중에 제공되는 VPN프로그램을 다운받아 사용할 경우 동영상을 시청하기에는 적합하지 않는 수준으로 인터넷 속도가 저하되어 활성화 가능성이 낮다는 주장도 있음

  ※ VPN 서비스를 이용할 경우 사용자의 위치정보를 암호화 하기 위해 VPN 서버라는 중간 거점을 거치기 때문에 이용자가 늘 경우 인터넷속도가 저하될 수밖에 없으며, 이로 인해 대용량의 동영상물의 전송이 증가할 경우 유료가 아닌 무료로 서비스를 제공하는 데에 한계가 있음

- VPN을 이용한 불법사이트 접속이 가능하기는 하나 불법홍보 등으로 인해 실제보다 우회가능성이 과대하게 오해되는 부분이 있다는 지적이 있음

  ▸ 특히 일부 개발자들이 홍보용으로 VPN프로그램을 SNI차단 우회가능 프로그램 등으로 안내하고 있고, 체험판에서 인터넷 속도를 보장하기 때문에 SNI차단을 우회하여 불법영상물 시청이 가능한 것처럼 오인되는 사례들이 있음

- 특히 무료VPN의 경우 위치정보, 접속기록 등 개인정보 유출 가능성이 높고 개인의 인터넷 보안이 취약해질 우려가 있어 이용자들의 VPN사용이 일상화되기에는 한계가 있음

  ▸ 개인정보보호 규정이 약한 해외에서 제공되는 VPN프로그램을 사용할 경우 개인정보(접속기록 및 비밀번호 등을 포함)가 해킹될 우려가 높고, 포르노사이트를 포함한 콘텐츠 서비스 업체, 인터넷 회선을 제공하는 해외통신사업자 등에게 사용자의 온라인 행동정보가 제공될 우려가 있음

  ▸ VPN운용은 비용이 들어가기 때문에 무료로 VPN을 제공할 경우 그에 상응하는 다른 수익모델이 있어야 하는데, 일상적인 동영상 시청을 저해하는 광고가 과다하게 포함될 수도 있고 또는 해킹 등의 불법적 용도로 사용될 우려도 있음

  ※ VPN해킹관련보도: 연합뉴스(2020. 1. 7). 동영상 더 싸게 보려 가상사설망 썼다가…해킹위험 노출 , 비즈한국(2019. 12. 3). 유튜브 프리미엄을 2천원에? VPN 쓰다 '좀비폰' 될라 , 전자신문(2020. 9. 22). 美 "이란 해킹조직, VPN 취약점 악용해 정보 유출" 등

  ▸ 이런 이유로 인터넷 사용자들 사이에서도 VPN을 통한 우회방법에 대해서 개인정보 유출, 유료결제 전환 강제, 과도한 광고 제공, 우회기능이 미작동, 접속장애 등에 대한 피해 사례들이 공유되고 있음

- 따라서 비용과 보안 등을 고려할 때 우회 프로그램이나 어플 등을 통한 우회 접속 행위가 확대될 가능성은 제한적으로 평가하고 있으나, 불법이용 목적으로 VPN을 광고·홍보하는 행위에 대해서는 제재가 필요함

(3) 기술대응 방향과 과제

가. VPN 이용실태 파악 및 대응방향

○ (탐지원리) VPN은 IP접속지역 정보를 암호화를 하고 있고 서버 주소가 계속적으로 변동할 수 있기 때문에, VPN의 사용실태나 VPN을 이용한 불법사이트 우회접속 실태를 탐지하는 것은 기술적으로 어려움

- 특정 VPN의 서버주소를 안다면, ISP의 차단장치에서 특정 VPN으로의 접속시도 여부를 확인하는 것은 기술적으로 가능하고, 해외 웹서버가 특정VPN의 접속요청을 확인하는 것도 가능함
- 그러나 이용자가 VPN서버를 경유하여 접속차단지로 접속하는지 여부를 ISP나 제3자가 탐지하는 것은 어려움
- VPN을 통한 불법사이트 접속여부를 확인하기 위해서는 VPN을 통과한 트래픽의 암호화(encapsulation)된 패킷들을 다시 복호화(decapsulation)해서 최종 접속지를 확인하는 과정이 필요
- 그러나 복호화과정은 통신비밀 침해의 문제가 있을 수 있고, 기술적으로도 상당히 어려움

  ※ 예를 들어, VPN의 경우 패킷의 목적지 주소를 기준으로 보내는 곳과 받을 곳을 계산하여, 해당 포트로 1:1로 연결하는 스위칭 과정에서 전체 접속 중에 L2(MAC주소[1])와 L3(프로토콜 주소) 패킷의 크기를 파악하는 것은 표본조사 등을 통해서 가능할 수는 있음. 그러나 L2, L3패킷 중 접속차단지로 전달되는 패킷을 추적하는 것은 현실적으로 가능성이 낮음

○ (VPN 이용실태 파악) 특정 VPN의 서버주소를 확보하여 표본조사를 시행할 경우, 해당

1) 컴퓨터의 물리적 주소로, 네트워크 인터페이스 카드에 할당된 고유 식별자

VPN을 통해 접속되는 트래픽의 양과 추이를 대략적으로 확인할 수 있음

- 우회접속용으로 사용될 것으로 추정되는 VPN의 서버주소 목록을 확보할 수 있다면, VPN이용실태를 파악할 수 있음
- 차단우회앱으로 홍보한 VPN일지라도 앱마켓 등록을 위해서는 통신판매업 등록이 필요하고, 이를 위해 호스트서버소재지와 사업자의 등록 정보가 공개되므로, 이들 VPN서버의 주소를 확인하여 해당 VPN으로 접속하는 트래픽의 양을 조사할 수 있음
- 그러나 해외 VPN서비스와 웹브라우저의 확장기능(browser extension)을 이용하여 VPN을 설치하는 방식의 서비스(e.g., expressvpn.com, cyberghostvpn.com, 등) 는 서버주소를 확보하기가 어렵고, 서버주소가 자주 변경되어 조사가 어려움

○ (VPN을 이용한 우회접속 실태 파악) VPN으로 유입되는 트래픽이 모두 불법사이트 접속을 목적으로 하는 것은 아니기 때문에 VPN을 경유하여 접속차단지로 접속하는 트래픽 조사가 필요함

- 앞서 설명한 바와 같이 VPN을 경유하여 접속차단지로의 접속여부를 제3자가 확인하는 것은 기술적으로 가능하지 않음
- 웹서버에서 특정 VPN의 IP주소를 탐지하여 특정 VPN을 경유하여 유입되는 접속시도를 확인하는 것은 가능하나, 제3자가 이를 확인하기는 어려움
- 따라서 VPN을 경유해서 접속차단지로의 접속여부를 확인하려면 VPN사업자의 협조가 필요한데, VPN사업자들을 (트래픽 양 또는 매출의) 규모에 따라 몇 개의 그룹으로 나눈 후에, 각 그룹에서 협조가 가능한 VPN 업체들을 표본으로 선정하여 불법사이트 접속의 비율을 파악하는 형태의 표본조사를 실시 할 수 있음
- 그러나 현실적으로 접속지 정보가 공개되면, 보안통신을 위한 VPN 이용 목적이 달성되지 않기 때문에 VPN의 협조를 얻어 최종접속지 정보까지 확인하는 것은 쉽지 않을 수 있음
- 대안적 방법으로는 국내 인터넷이용자들을 대상으로 주로 사용하는 VPN 서비스와 불법사이트 이용빈도를 설문조사하고, 해당 VPN 서버들로의 통계적인 트래픽 자료를 보완적으로 사용하여 대략적인 추정을 시도할 수도 있음

[유사사례: 한국저작권위원회 저작권보호 연차보고서의 '불법복제물 조사']

▸조사목적: 온・오프라인상의 불법복제물 이용량과 이용률, 그리고 기타 이용실태와 저작권 보호 인식 수준 등 실태 파악

▸조사항목:

- 콘텐츠(합법저작물 ・ 불법복제물) 분야별 이용경로별 이용량
- 콘텐츠 분야별 온・오프라인 불법복제물 이용률
- 성, 연령, 지역 등 응답자 특성에 따른 콘텐츠 분야별 불법복제물 이용실태
- 콘텐츠 분야별 저작권 보호 인식

▸조사체계:

- 조사대상 : 전국의 만 13세~69세의 일반국민 2만명
- 조사방법 : 응답자 자기기입식 온라인 조사

○ (접속차단 적용방안) 보안목적으로 도입된 VPN의 특수성을 고려할 때, 기술적으로 VPN 통신을 ISP나 제3자가 복호화하여 접속차단지를 확인한 후 접속차단을 실시하는 것은 실현가능하지 않음

- VPN은 공중망(public network)에서도 전용망과 같이 보안이 강화된 통신을 이용하기 위해 도입된 서비스로, 통신비밀의 보장이 필요함
- 현행법상 VPN은 부가통신사업에 해당하고 망설비를 보유하고 있지 않고 부가통신사업자이기 때문에 VPN서비스 제공자에게 인터넷접속사업자에 부과되는 차단의무를 부과할 법적 근거가 없음
- 네트워크의 국제망 특수성과 우회접속 차단의 실효성을 고려할 때, 인터넷접속 자체를 막지 않는 이상 해외 VPN 이용을 완전히 차단하는 것은 불가능

  ※ 일례로 중국의 경우, 금순공정(金盾工程) 혹은 황금방패(黃金防牌)라는 인터넷검열시스템이 VPN사용으로 우회되자 이에 대한 대응을 위해 PC에 인터넷 검열 소프트웨어인 그린댐(綠-花季航:GreenDam-YouthEscort)을 제작 배포함. 이를 통해 모든 인터넷 사용에 대한 기록을 로그 파일(LogFile)로 남겨 확인할 수 있게 하는 방식으로 VPN을 차단하고 있음(박정훈 외, 2020). 그러나 글로벌네트워크의 특성을 이용하여 중국인터넷이용자들이 대안적인 다양한 해외 VPN을 이용할 수 있기 때문에 접속을 완전하게 차단하지 못함(모정훈, 2020)

- 즉, VPN서버 주소를 다 알고 있다는 가정 하에, VPN서버로 가는 총 접속 트래픽을 알 수 있다고 해도, 암호화된 패킷을 복호화하지 않고는 접속차단지로 가는 트래픽을 변별해내는 것은 가능하지 않기 때문에 VPN을 경유한 트래픽의 최종접속지를 확인하여 차단하는 것은 쉽지 않음

○ (제도적 대응) 가입자에게 인터넷접속역무를 제공하는 하위계위 ISP사업자에게 불법사이트 차단의무 이행을 강화하고, VPN의 불법적 이용을 조장하는 광고물에 대한 심의·제재를 강화하는 비기술적 대응 필요

- VPN의 경우 기술적 조치가 어렵고 복호화로 인해 통신비밀 침해의 문제 등이 있어 비기술적 조치의 강화를 통해 해결해야함
- 하위계위 ISP사업자가 망임대사업자와 계약시 불법사이트의 차단조치를 위한 장비설치 및 차단실시 등을 요청하는 것을 의무화하고, 차단의무 이행여부에 대해 점검을 강화함으로써 우회행위를 관리할 수 있음
- 또한 경제적 목적을 위해 불법사이트에 접속할 수 있다거나 우회접속이 가능하다는 상품정보를 제공하면서 VPN앱 광고를 판매하는 경우는 앱마켓의 개발자 정책에 근거한 자율규제나 법령에 근거한 시정 등이 가능할 수 있음

나. 하위계위 ISP사업자의 접속차단 조치 이행 강화

○ 접속차단의 기술적 조치의 의무는 모든 ISP에게 부과되어 있으나, 기술적으로는 해외관문국을 보유한 상위ISP사업자와 IX에 탐지와 차단장치를 설치하여 시행되었음

- '해외불법정보 차단업무 처리지침'은 인터넷접속사업자에게 해외 불법정보의 국내 유입을 차단하는 의무를 부여함
- 해외 불법정보가 국내에 유입되는 관문인 해외관문국을 차단할 경우 국내 이용자가 해외 불법정보에 접속할 수 없기 때문에, 그동안 해외관문국을 보유한 상위 ISP사업자에게 장비 설치와 운용의 의무를 명령함

<표 2-4> 국내 인터넷접속사업자 계층 구분 및 현황

분류			사업자
IX & 트랜짓			KINX, SKB, KT, LG U+, 세종텔레콤, 드림라인
ISP	상위 계위		KT, SKB, LGU+
	하위 계위	망중계사	세종, 드림라인,
		종합유선 방송(MSO)	LGH, T-Broad, DLive, HCN (다수 SO 포함)

- 하위계위사업자들도 불법정보 차단의 의무가 부과되어 있으나, 기술적 조치는 해외

관문국에 설치한 차단장비 설치 사업자에게 위임한 것으로 간주해왔음

- 따라서 하위계위사업자들은 차단 장비 등을 설치하거나 해외 불법정보의 처리 거부를 위한 별도의 기술적 조치를 취하지는 않았으나, 차단 장비의 설치비용을 협의하여 분담해왔음
- 또한 하위계위사업자도 차단사실에 대한 안내를 이용자에게 제공할 의무가 있으며, 이로 인한 민원 및 법적 분쟁에 대하여는 해당 민원 및 법적 분쟁을 제기한 자에게 인터넷 접속역무를 제공하는 인터넷접속사업자의 책임으로 인정되어옴
- 즉, 하위계위사업자가 차단 업무를 위임하여 URL차단장비를 설치할 의무는 없으나 해외불법정보로의 접속차단을 위한 책임을 위임한 것으로 보기는 어려우며, 상위계층 사업자와 하위계위 사업자 모두 불법정보의 차단에 대한 책임이 있다고 해석됨
- 하위계위 ISP사업자가 보안이 적용된 전용회선이나 클라우드 기반 VPN(MPLS VPN)을 제공하는 망임대사업자를 사용할 경우, 최종 인터넷이용자가 직접 VPN을 사용해서 우회접속을 하는 것과 유사한 현상이 발생할 가능성이 있음

  ※ 예를 들어 하위계위 ISP사업자가 해외에 서버를 둔 클라우드 기반 VPN(MPLS VPN)을 제공하는 망임대사업자에게 트래픽 관리 등의 업무를 일부 위임할 경우, 해외관문국의 탐지장비에서 인터넷가입자들의 접속IP주소를 확인하기 어려움
- 따라서, '해외불법정보 차단업무 처리지침'의 개정을 통해 하위계위 ISP사업자가 망임대사업자와 계약시 불법사이트의 차단조치를 위한 장비설치 및 차단실시 등을 요청하는 것을 의무화하고, 차단의무 이행여부에 대해 점검을 강화함으로써 우회행위를 관리할 수 있음

다. VPN을 우회접속용으로 홍보하고 판매하는 행위에 대해 제재 가능성 검토

○ 실재 우회여부와 상관없이 불법적인 우회접속용도로 VPN을 광고하는 사례가 확인되고 있으며, 이로 인해 VPN을 통한 우회접속 시도가 있음

- 비용 및 속도, 보안 등을 고려할 때 VPN을 이용한 우회접속이 대중적으로 사용되기에 여러 가지 한계가 있음에도 불구하고, 앱명칭이나 앱정보에 접속차단 우회를 주된 용도로 기재하여 인터넷이용자들을 기만하는 행위가 발생
- 앱마켓에 등록할 때, 앱명칭이나 앱정보에 "HTTPS 차단", "HTTPS 우회", "SNI 차단 우회", "DNS 차단 우회"등의 용어를 사용한 사례들이 발견됨

<표 2-5> VPN 앱에 대한 불법광고 현황

앱 명칭에 불법우회접속 홍보	앱정보에 불법우회접속 홍보
 [redacted]PS 우회앱 - 안전하고 빠른 HTTPS/SNI 차단 우회앱 [redacted] HTTPS 우회앱. 속도 저하없는 HTTPS,SNI 우회 [redacted]	대표 기능 • warning.or.kr 사이트 우회 • HTTPS 차단 우회 • DNS 차단 우회 • SNI 차단 우회 • 속도 저하 없음 • 모든 브라우저 지원

○ 현행법상 접속차단 우회행위방법을 공유하는 행위는 명백한 불법정보로 보기에는 어려우나, 경제적 이익을 목적으로 우회행위의 수단을 제공하는 행위는 제재할 수도 있음

- 현행법상 불법정보를 유통하는 행위는 불법으로 보지만, 불법정보에 접속하는 행위가 명백하게 불법인지는 명확하지 않음

- 정보통신심의에 관한 규정 제7조(범죄 기타법령 위반)는 기타 범죄 및 법령에 위반되는 위법행위를 조장하여 건전한 법질서를 현저히 해할 우려가 있는 정보는 심의의 대상이 되도록 규정하고 있으며,

제7조(범죄 기타 법령 위반) 범죄 기타 법령에 위반되는 행위에 관련된 다음 각 호의 정보는 유통이 적합하지 아니한 것으로 본다.
1. 범죄를 목적으로 하거나 예비・음모・교사・방조할 우려가 현저한 정보
2. 범죄의 수단이나 방법 또는 범죄에 이르는 과정이나 결과를 구체적으로 묘사하여 범죄를 조장할 우려가 있는 정보
3. 범죄, 범죄인 또는 범죄단체 등을 미화하여 범죄를 정당하다고 보이게 할 우려가 있는 정보
4. 기타 범죄 및 법령에 위반되는 위법행위를 조장하여 건전한 법질서를 현저히 해할 우려가 있는 정보

- 동 규정 제9조는 해당 정보를 배포, 판매, 임대 하거나 광고, 선전 하는 행위에 대해서는 시정요구를 할 수 있다고 규정

제9조(광고・선전 등의 제한) 위원회는 제5조 내지 제8조에 위배되는 정보를 배포・판매・임대 등을 하거나 공연히 전시 또는 전송을 할 목적으로 매개・광고・선전 등을 하는 내용의 정보에 대하여 시정요구 할 수 있다.

- 따라서 ① VPN을 사용하여 우회접속하는 행위 또는 ② 우회접속용으로 VPN을 판매하는 행위가 제7조제1호, 제2호 또는 제7조제4호† 에 관한 판단된다면, 앱마켓이나 커뮤니티 사이트, 또는 인터넷 게시글에서 우회접속 프로그램에 대한 홍보나 상세한 절차에 대한 게시글도 법령위반을 조장하는 행위로 판단되어 제재의 근거가 있음

  † 접속이 차단되는 불법사이트의 종류, 내용(즉, 불법사이트로 분류하는 이유와 근거)을 고려할 때, 청소년성보호법에 따른 아동·청소년 성착취물 사이트 접속 및 시청할 개연성이 상당히 높거나 현저하다고 해석될 여지가 있음. 이러한 해석적 접근을 하는 경우 심의규정 제7조 제1호, 제2호, 제4호(밑줄 친 부분 참조)에 해당하는 행위로 해석될 가능성이 농후하며, 그 결과 제9조에 따른 시정요구가 가능할 것으로 판단됨

- 그러나 ①과 ② 모두에서 현행법상 명백한 위법행위로 보기 어려울 소지가 있음

① VPN을 사용하여 우회접속하는 행위

- ①의 경우 정보통신망법 제44조의 7은 불법정보를 유통하는 행위만을 위법행위로 규정할 뿐, 시청하는 행위에 대는 위법행위로 규정하지 않음

- 단, 청소년성보호법 제11조의5에 따라 아동·청소년 성착취물을 시청한 행위만 법령에 위반되는 위법행위로 판단할 수 있음

[아동·청소년의 성보호에 관한 법률 (약칭: 청소년성보호법)]

제11조(아동·청소년성착취물의 제작·배포 등) ① 아동·청소년성착취물을 제작·수입 또는 수출한 자는 무기징역 또는 5년 이상의 유기징역에 처한다.
② 영리를 목적으로 아동·청소년성착취물을 판매·대여·배포·제공하거나 이를 목적으로 소지·운반·광고·소개하거나 공연히 전시 또는 상영한 자는 5년 이상의 징역에 처한다.
③ 아동·청소년성착취물을 배포·제공하거나 이를 목적으로 광고·소개하거나 공연히 전시 또는 상영한 자는 3년 이상의 징역에 처한다.
④ 아동·청소년성착취물을 제작할 것이라는 정황을 알면서 아동·청소년을 아동·청소년성착취물의 제작자에게 알선한 자는 3년 이상의 징역에 처한다.
⑤ 아동·청소년성착취물을 구입하거나 아동·청소년성착취물임을 알면서 이를 소지·시청한 자는 1년 이상의 징역에 처한다.
⑥ 제1항의 미수범은 처벌한다
⑦ 상습적으로 제1항의 죄를 범한 자는 그 죄에 대하여 정하는 형의 2분의 1까지 가중한다.

- 그러나 이 경우에도 VPN을 이용하여 어떤 사이트나 영상물에 접속했다는 것을 확인할

수 없고, VPN을 이용하는 행위만으로 불법을 저질렀다고 판단할 수 없음

* 예를 들어 위장형 카메라와 만능키 등은 불법행위에 이용될 가능성이 있으나, 합법적 용도로 사용될 가능성도 있기 때문에 해당 상품을 구매하거나 이용하는 행위를 위법행위로 간주할 수 없음. 따라서 해당 상품을 이용하여 실제 범죄가 발생한 경우에 대해 사후에 행위자에 대해 민·형사상 책임을 묻고 있을 뿐, 판매자(통신판매업 포함)나 통신판매중개업자에게 책임을 묻지 않고 있음

- 게재자가 특정 VPN을 언급하여 불법사이트 접속방법을 상세히 게재한 경우에도 불법사이트 접속행위 자체가 명백한 불법행위로 규정된 것이 아니기 때문에, 특정 VPN을 이용하여 HTTPS차단을 우회하거나 warning.or.kr을 우회할 수 있다는 정보를 게재하는 행위가 망법 제44조의7과 심의규정 제7조의2를 위반한다고 볼 수 없음
- 게재자가 VPN을 이용하여 불법사이트에 접속할 수 있음을 인지하고 해당 VPN앱을 다운받을 수 있는 링크를 단순 제공했을 경우에도, 불법성은 인지했으나 경제적 수익 추구의 조건은 충족하지 못함
- 따라서 게재자나 플랫폼 사업자 모두 당해 행위로 인한 제재가 가능하지 않은 것으로 판단됨

② 우회접속용으로 VPN을 홍보하거나 판매하는 행위

- ②의 경우, VPN 판매자가 불법정보의 유통행위를 방조·조장한 행위로 판단할 여지가 없지는 않으나, 그동안의 판례들이나 통신심의 심결 등을 고려할 때 최소규제의 원칙이 적용되어 해당 행위가 법률에 따라 제재되지 않아왔음
- 예를 들어 불법영상을 주소연결방식(URL게재)으로 게재한 사이트에 대해서 저작권 침해로 보고 정보통신망법 제44조의7의 불법정보로 판단하여 사이트를 차단한 경우도 있으나, 이 경우에도 현저한 수준의 불법정보 유통행위를 조장했다고 판단할 근거가 필요함

※ 한국저작권위원회의 유권해석에 따르면 단순링크(simple link), 직접 링크(deep link)는 불법으로 보지 않고, 프레이밍 링크(framing link)[2], 임베디드 링크(embedded link)[3] 등은 불법으로 해석함.

---

2) 외부의 웹페이지 일부를 자신의 웹페이지에 그대로 구현하여 이용자가 클릭시 재생되는 방식의 링크

3) 링크된 정보를 호출하기 위해 이용자가 클릭을 할 필요 없이 링크제공 정보를 포함한 웹페이지에 접속하면 자동으로 링크된 정보가 바로 재생되는 방식의 링크

단순링크나 직접링크의 경우 연결된 불법정보가 최초 접속한 웹페이지에서 제공되지 않고, 웹페이지 밖으로 나가 해당 불법정보나 불법사이트에 직접 접속되기 때문에 링크를 제공한 웹페이지 제공자의 책임이 현저하다고 볼 수 없음. 반면, 프레이밍 링크나 임베디드 링크의 경우 최초 접속한 웹페이지 내에서 불법정보나 불법정보가 담긴 웹페이지가 전시되기 때문에 링크를 제공한 웹페이지 제공자의 서비스 안에서 구현된다고 볼 수 있고, 그로 인해 링크를 제공한 웹페이지와 웹사이트 제공자는 접속자를 자신의 웹페이지와 웹사이트로 유인하는 이익을 얻을 수 있어 책임이 현저하다고 볼 수 있음

- 한국저작권위원회의 유권해석에도 불구하고 불법저작물의 주소를 제공하는 행위에 대해서는 상이한 판례가 존재하기는 하나, 이때는 ①불법의 인식, ②경제적 수익 여부가 링크의 불법성 판단에 중요한 기준으로 작용하고 있음

판례) 저작권법위반방조(인터넷 링크 사건) [대법원 2015. 3. 12., 선고, 2012도13748, 판결]

【판시사항】
[1] 웹사이트 회원들이 게시판에 불법저작물을 링크하는 행위가 저작권법상 복제 및 전송에 해당하는지 여부
[2] 사이트 운영자가 인지하지 못한 불법저작물 링크가 저작재산권 침해행위의 방조행위에 해당하는지 여부

【판결요지】
[1] 인터넷 링크(Internet link)는 인터넷에서 링크하고자 하는 웹페이지나, 웹사이트 등의 서버에 저장된 개개의 저작물 등의 웹 위치 정보나 경로를 나타낸 것에 불과하여, 비록 인터넷 이용자가 링크 부분을 클릭함으로써 링크된 웹페이지나 개개의 저작물에 직접 연결된다 하더라도 링크를 하는 행위는 저작권법이 규정하는 복제 및 전송에 해당하지 아니한다.
[2] 링크를 하는 행위 자체는 인터넷에서 링크하고자 하는 웹페이지 등의 위치 정보나 경로를 나타낸 것에 불과하여, 침해행위의 실행 자체를 용이하게 한다고 할 수는 없으므로 이러한 링크 행위만으로는 저작재산권 침해행위의 방조행위에 해당한다고 볼 수 없다.

판례) 손해배상(기) [서울고법 2017. 3. 30., 선고, 2016나2087313, 판결 : 상고]

【판시사항】
[1] 인터넷 사이트를 개설한 후 해외 동영상사이트의 저작권위반 영상물에 대한 임베디드 링크(embedded link)를 게재하여 이용자들이 무료로 시청할 수 있도록 한 사안

【판결요지】
[1] 甲의 링크행위는 실질적으로 해외 동영상 공유 사이트 게시자의 공중에의 이용제공의 여지를 더욱 확대시키는 행위로서 해외 동영상 공유 사이트 게시자의 공중송신권(전송권) 침해행위에 대한 방조에는 해당한다고 한 사례

- 이를 토대로 볼 때에 우회접속용으로 VPN을 홍보하거나 제공하는 행위가 불법정보 유통행위를 방조·조장한 행위로 판단하기 위해서는 ①불법의 인식, ②경제적 수익이라는 두가지 조건을 충족해야함

- 유사사례 판례들을 토대로 볼 때, 단순히 불법사이트 접속을 위해 VPN을 이용하는 방법이나 VPN을 이용하면 접속차단조치를 회피할 수 있다는 정보를 블로그나 커뮤니티 사이트에 게시하는 행위, 우회접속 방법을 안내하고 VPN다운로드 방법을 링크하는 행위는 현저하게 불법정보 유통행위를 조장했다고 보기 어려울 것으로 보임

- 그러나 통신판매업으로 등록한 VPN개발사와 판매자가 앱마켓에 유료결제, 앱내 구매, 광고, 유료구독 등이 포함된 VPN을 제공하면서 앱마켓이나 자사홈페이지와 블로그, 기타 자사와 관련된 SNS사이트 등에 불법사이트에 접속할 수 있다고 기재하거나, 접속차단을 우회할 수 있다고 홍보하는 행위는 ① '불법의 인식', ②'경제적 수익'등의 조건이 충족되어 불법성이 현저하다고 판단할 수 있음

- 요약하자면, 차단우회앱개발자 또는 판매자가 경제적 수익을 목적으로 불법우회접속 가능성을 홍보하거나 상세한 우회방법을 설명하거나 암시할 경우, ① '불법의 인식', ②'경제적 수익'등의 조건이 충족되어 위법하다고 판단할 여지가 있음

- 통신판매업으로 등록한 차단우회앱개발자 또는 판매자가 ① 앱마켓이나 자사홈페이지와 블로그, 기타 자사와 관련된 SNS사이트 등에 불법사이트에 접속할 수 있다고 기재하면서, ② 앱마켓에 유료결제, 앱내 구매, 광고, 유료구독 등이 포함된 VPN을 제공하는 행위

  예) 프로텍트 HTTPS: 홈페이지에 차단우회앱으로 기재되어 앱마켓 다운로드 페이지로 링크되어 있고, 앱은 무료로 다운받을 수 있으나 광고가 포함되어 수익이 발생함. 또한 앱마켓에서 SNI필드 차단 우회라 명기되어 있음

- 상기와 같은 행위자는 망법 제44조의 7과 심의규정 제7조4호를 위반한 것으로 판단되어, 앱마켓사업자에게 시정요구가 필요함

  ※ 참조: '차단사이트 우회접속 조장'과 관련하여 차단된 해외서버 사이트에 대해 불특정 다수의

이용자들이 우회적으로 접속할 수 있도록 하기 위한 목적으로 우회접속 방법 등을 구체적으로 제공하는 것과 관련하여, 방송통신심의위원회는 시정요구를 의결한 바 있으며(제88차 통신심의소위원회 심결, 2020.11.30.), 이에 따라 위법행위 조장이 현저하다고 판단된 경우는 시정이 이뤄짐

○ 타법 위반 여부 검토

- 앱마켓에 경제적 목적(유료다운로드, 앱내 결제, 광고, 유료구독 등)으로 앱을 등록하는 사업자들은 부가통신사업자이나 대체로 영세하기 때문에 신고 의무는 면제되지만, 앱마켓 등록과 유료결제를 위해서 통신판매업자로 등록해야하며, 이에 따라 VPN앱 개발자와 사업자는 전자상거래법, 표시광고법 등을 적용받게 됨

  ▸ 차단우회앱이나 프로그램 제공자들은 망설비를 보유하지 않은 부가통신사업자로, 정보통신망법에 근거한 등록 등의 의무가 없고 불법사이트 차단조치의 의무가 없음

  ▸ 부가통신사업자도 전기통신사업법 제5조와 시행령 제29조에 따라 신고의 의무가 있으나, 자본금 1억 이하의 소규모 사업자들은 신고 면제(시행령 제30조)에 해당하여, 광고우회앱 또는 차단우회앱으로 홍보하고 VPN서비스를 제공하는 일부 군소 사업자들은 대체로 신고면제사업자에 해당함

  ▸ 신고면제 사업자에 해당할 경우 중앙전파관리소에 신고 및 등록[4]을 하지 않기 때문에 전기통신사업법에 근거한 신고 및 관리 적용이 어려움

  ※ 부가통신사업자는 전기통신사업법 제 22조에 근거한 신고사업자로 지정되어 있어, 신고한 사업자의 경우 중앙전파관리소에 등록되어 있음. 그러나 소규모 사업자의 경우(자본금 1억 이하)는 신고면제사업자로 되어 있어 불법 앱개발 유포의 경우는 중앙전파관리소에도 등록이 되어 있지 않음

[전기통신사업법 및 동법시행령 상 부가통신사업자의 지위와 신고]

전기통신사업법 제5조(전기통신사업의 구분 등) ① 전기통신사업은 기간통신사업 및 부가통신사업으로 구분한다.

② 기간통신사업은 전기통신회선설비를 설치하거나 이용하여 기간통신역무를 제공하는 사업으로 한다.

③ 부가통신사업은 부가통신역무를 제공하는 사업으로 한다.

제22조(부가통신사업의 신고 등) ① 부가통신사업을 경영하려는 자는 대통령령으로 정하는 요건 및 절차에 따라 과학기술정보통신부장관에게 신고(정보통신망에 의한

4) 2020년 10월 기준, 15,015개의 부가통신사업자가 등록.

신고를 포함한다)하여야 한다.
④ 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 자는 부가통신사업을 신고한 것으로 본다.
1. 자본금 등이 대통령령으로 정하는 기준에 해당하는 소규모 부가통신사업을 경영하려는 자

동법 시행령 제29조(부가통신사업의 신고절차 등) ① 법 제22조제1항 전단에 따라 부가통신사업을 신고하려는 자는 부가통신사업 신고서(전자문서로 된 신고서를 포함한다)와 다음 각 호의 서류(전자문서를 포함한다)를 과학기술정보통신부장관에게 제출하여야 한다.
1. 통신망구성도(새로운 유형의 부가통신역무를 신고하는 경우로서 과학기술정보통신부장관이 필요하다고 인정하여 요구하는 경우만 해당한다)
2. 개인정보보호조치 구축 명세서(개인정보를 취급하는 경우만 해당한다)
<이하생략>

제30조(부가통신사업자 신고의 면제) ① 법 제22조제4항제1호에서 "대통령령으로 정하는 기준에 해당하는 소규모 부가통신사업"이란 인터넷을 이용하여 부가통신역무를 제공하는 자본금 1억원 이하인 부가통신사업자를 말한다.
② 제1항에 따라 신고가 면제된 부가통신사업자는 자본금이 1억원을 초과하게 된 경우에는 그 사유가 발생한 날부터 1개월 이내에 법 제22조제1항에 따라 과학기술정보통신부장관에게 신고하여야 한다.

- VPN제공은 비용이 들어가기 때문에 앱마켓 등록시에 유료다운로드, 앱내 결제, 광고, 유료구독 등을 적용하는 것이 일반적이며, 이로 인해 통신판매업 신고가 필요함

- 따라서, VPN사업자들은 구글 플레이스토어나 애플 앱스토어 등 앱결제 플랫폼에서 유료앱이나 인앱구매가 포함된 앱을 배포하기 위해 사업자 등록 및 통신판매[†]업 신고를 완료한 후, ①사업자등록번호, ②통신판매신고번호, ③통신판매업 신고를 받은 기관 이름(시/군/구청)을 제출하고 있음

  [†] 전자상거래소비자보호법 제2조(정의)의 2. "통신판매"란 우편·전기통신, 그 밖에 총리령으로 정하는 방법으로 재화 또는 용역(일정한 시설을 이용하거나 용역을 제공받을 수 있는 권리를 포함한다. 이하 같다)의 판매에 관한 정보를 제공하고 소비자의 청약을 받아 재화 또는 용역(이하 "재화등"이라 한다)을 판매하는 것을 말한다.

- 통신판매업자는 신고의무(법 제12조), 표시광고에 신원정보 포함 의무, 거래기록 보존 의무 등이 부과되며, 이를 위반할 경우 시정권고, 시정조치 및 영업정지, 과징금 등의 행정적 제재가 있음

- 통신판매업자는 전자상거래소비자보호법 제12조에 따라 주된 사업장 소재지 관할 지자체에 사업자 신고의무가 있음

  * 단, 이 경우에도 최근 6개월 동안 거래횟수가 20회 미만이거나, 매출액 1,200만원 미만의 사업자는 신고가 면제되나, 이러한 조건의 사업자가 제공하는 VPN서비스에 의한 우회접속 가능성은 그 영향이 크지 않을 것으로 판단됨

  ** 통신판매업자의 신고내역에는 상호, 주소, 전화번호, 대표자 성명, 주민등록번호, 사업자 등록번호, 법인등록번호, 전자우편주소, 인터넷도메인이름, 호스트서버 소재지, 참고사항 (판매방식, 취급품목 등)이 포함.

[전자상거래 등에서의 소비자보호에 관한 법률 (약칭: 전자상거래법)]
제12조(통신판매업자의 신고 등) ① 통신판매업자는 대통령령으로 정하는 바에 따라 다음 각 호의 사항을 공정거래위원회 또는
특별자치시장·특별자치도지사·시장·군수·구청장에게 신고하여야 한다. 다만, 통신판매의 거래횟수, 거래규모 등이 공정거래위원회가 고시로 정하는 기준 이하인 경우에는 그러하지 아니하다.
1. 상호(법인인 경우에는 대표자의 성명 및 주민등록번호를 포함한다), 주소, 전화번호
2. 전자우편주소, 인터넷도메인 이름, 호스트서버의 소재지
3. 그 밖에 사업자의 신원 확인을 위하여 필요한 사항으로서 대통령령으로 정하는 사항
② 통신판매업자가 제1항에 따라 신고한 사항을 변경하려면 대통령령으로 정하는 바에 따라 신고하여야 한다.
③ 제1항에 따라 신고한 통신판매업자는 그 영업을 휴업 또는 폐업하거나 휴업한 후 영업을 다시 시작할 때에는 대통령령으로 정하는 바에 따라 신고하여야 한다.
④ 공정거래위원회는 제1항에 따라 신고한 통신판매업자의 정보를 대통령령으로 정하는 바에 따라 공개할 수 있다.

- 그러나 전자상거래법은 상품의 위법성이나 위법하게 사용될 여지가 있는지에 대해 다루지 않기 때문에, 위법의 소지가 있는 상품을 판매하더라도 직접적으로 규제할 수 없음

- 다만 판매자가 불법행위를 할 수 있는 기능이 있다고 광고하여 해당 상품을 구매한 소비자가 실재로 해당 기능을 이용할 수 없었다고 소비자 피해를 접수할 경우, 표시광고법 제3조(부당한 표시광고행위)의 기만광고와 허위·과대광고 등으로도 판단할 수 있어 제재가 가능하다고 볼 수는 있음

- 이를 종합할 때, 접속차단을 우회하는 행위를 조장하는 상품 판매를 전자상거래법에 근거하여 제재하기는 어려울 것으로 판단됨

○ (자율규제 요청) 경제적 수익을 목적으로 상품을 판매하는 경우 불법행위를 조장할 수 있거나 사회적 통념에 부합하지 않는 경우에는 플랫폼사업자들(예: 포털이나 오픈마켓 등)의 자율규제가 시행된 유사사례들도 있어, 앱마켓 사업자들에게도 유사한 수준의 자율적 정화노력을 요청할 필요가 있음

- 법령상의 명백한 불법행위가 아니어도 사회적 통념에 부합하지 않는 정보의 게재나 상품의 판매에 대해서는 플랫폼사업자(통신판매업자 또는 통신판매중개업자)가 자율적으로 삭제나 정정 등을 요청하고 있음
- 명백한 불법상품은 아니지만 범죄에 악용될 수 있는 상품(예: 몰래카메라, 만능키를 불법행위에 연동해서 광고하는 경우)을 판매하는 행위는 불법으로 보기 어렵고, 불법행위를 할 수 있다는 암시가 있는 광고나 홍보를 한 경우에도 현행법(정보통신망법, 전자상거래법, 표시광고법 등)상 명백한 금지 조항은 존재하지 않으나,
- 주요 상거래 플랫폼들(예: 네이버쇼핑, 이베이코리아, 쿠팡 등) 은 불법행위를 조장할 수 있는 상품정보를 제공하는 상품에 대해서 범죄에 악용될 수 있는 상품으로 판단되는 경우(예: 몰래카메라, 만능키 등)나 관할기관이 삭제 요청한 상품에 대해 자발적인 고지, 삭제, 정정, 등록 거부 등을 시행하고 있음

예) 네이버쇼핑은 클린프로그램이라는 자체적인 상품판매관리기준을 운용하여, 법령에 위배되거나 법령에 위배되지 않더라도 사회적으로 문제가 될 수 있는 상품 판매의 등록을 거부하고 있음

[네이버쇼핑 클린프로그램의 클린기준]

◆ 상품취급기준

법령에 위배되거나, 온라인 판매가 부적절한 상품에 대해 기준을 정하고, 상품군에 따라 각종 인증이나 판매 자격요건을 갖춰 판매하도록 기준을 운영하고 있습니다

◆ 네이버쇼핑 미취급 상품에 대한 기준

<생략>

2. 각종 법령에 위배되거나, 법 기준위반이 아니더라도 사회적으로 문제가 될수 있는 상품에 대해서는 판매를 금하고 있습니다.

ex)・만능키, 몰카, 어뷰징 프로그램, 사행성 상품 등 부정적인 목적으로 사용될 우려가 있는 상품

・이용자 안전사고 위험이 높은 상품

<이하 생략>

예) 쿠팡은 사업자용 서비스이용약관에 법령에 위배되지 않더라도 사회통념상 판매하기에 부적합한 상품에 대해서는 인지했을 경우 노출을 제한하거나 판매를 금지하는 조치를 취하고 있음. 예를

들어 쿠팡은 2019년 7월 불법촬영에 악용될 소지가 있는 초소형 카메라 제품 판매게시물에 여성의 신체부위를 부각한 사진이 포함되어 불법행위를 조장할 수 있다는 지적이 제기되자, 해당 게시물의 노출과 판매를 중단(2019. 7. 7)함. 즉, 초소형 카메라는 법령상 위법한 상품은 아니기 때문에 판매자체를 제한할 수 없으나, 위법한 행위 또는 사회통념에 부합하지 않는 행위를 암시하는 경우에 대해서는 자율규제를 적용하고 있음

[쿠팡 서비스 이용 약관-사업자용]

◆ 상품판매자의 금지행위 기준

① 판매자는 다음의 행위를 직접 하거나 제3자로 하여금 하도록 하여서는 안됩니다.

제14조 (금지행위)

21. 사회통념상 판매하기에 부적합한 상품의 판매 또는 합리적인 이유로 회사에 의해 판매가 제한된 상품의 판매.

23. 관련 법령 및 규정 위반.

② 판매자는 상기 제1항에 언급된 금지 행위의 위반에 대하여 전적으로 책임을 부담합니다.

③ 회사는 상기 제1항에 명시된 금지된 위법행위를 발견한 경우, 마켓플레이스에서 상품의 판매를 제한 또는 금지하거나 상품이 고객들에게 노출되는 것을 제한할 수 있으며, 사전 통지 없이 기타 필요한 조치를 취할 수 있습니다. 상품이 이미 판매된 경우에는 해당 거래는 취소될 수 있습니다. 이러한 경우, 상품이 허위 상품(모조품)인 경우에는, 회사는 해당 구매자에게 구매 가격 및 구매자가 입은 정신적 고통에 대한 손해를 직접 배상할 수 있습니다.

④ 회사는 상기 제1항을 위반한 판매자에 대하여 서비스 이용 제한, 판매자 자격 정지 및 본 약관 및 서비스 T&C의 해지를 포함하여 조치를 취할 수 있으며, 그로 인해 발생한 손해에 대하여 판매자에게 손해배상을 청구할 수 있습니다.

- 현재 앱스토어, 구글플레이 등 앱마켓의 자율규제 기준에도 불법활동을 위한 앱광고를 게재하거나 불법활동을 위한 앱을 배포는 개발자 정책 위반에 해당되며, 고지, 삭제, 검색 제한 등이 가능함

- 따라서 차단우회 홍보 앱에 대해서 “HTTPS 차단 우회”, “HTTPS 우회”, “SNI 차단 우회”, “DNS 차단 우회”, “검열 우회”등의 메타데이터 등록 금지 요청 필요

[구글 개발자 정책]

▸ 구글의 콘텐츠 정책은 개발자의 앱이 사용자에게 표시하는 광고, 앱이 호스팅하거나 링크를 제공하는 사용자 제작 콘텐츠와 같이 앱이 표시하거나 링크를 제공하는 모든 콘텐츠에 적용됨

▸ 구글플레이 정책은 아동학대, 부적절한 콘텐츠, 불법적인 금융서비스, 불법도박・게임

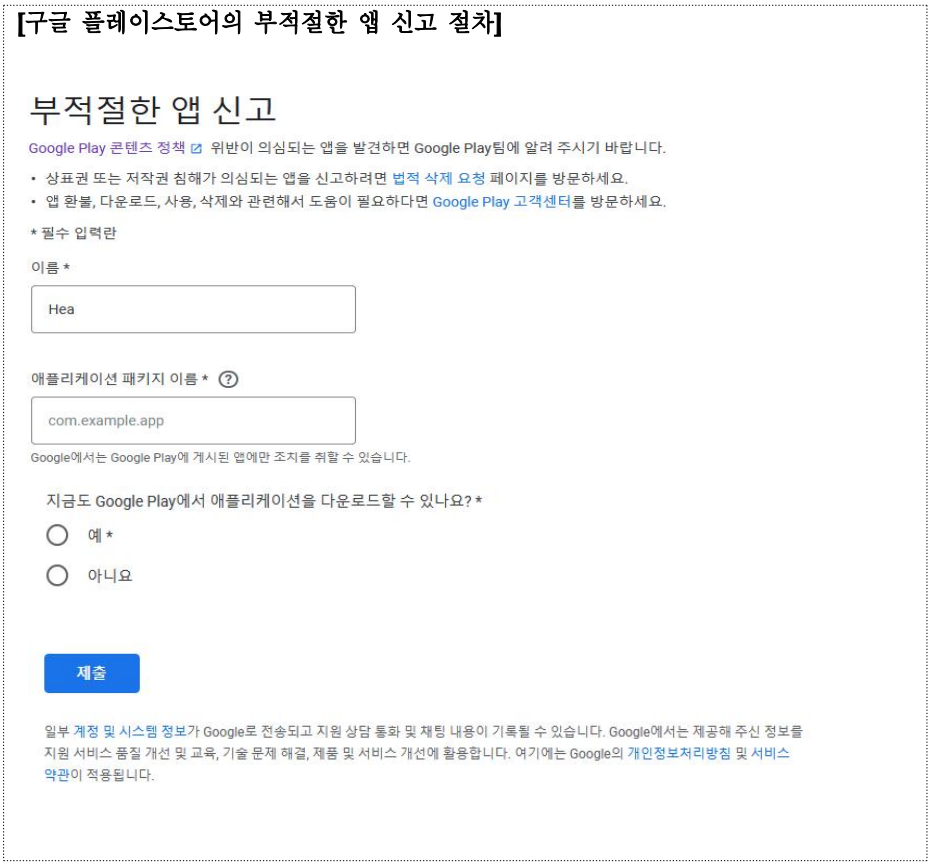
앱, 불법활동, 불법약물, 지적재산 침해 콘텐츠, 개인정보침해와 사기 및 기기 악용 등과 관련된 앱에 대해서, 고지, 삭제, 계정정지, 검색제한, 계정해지 등이 가능함

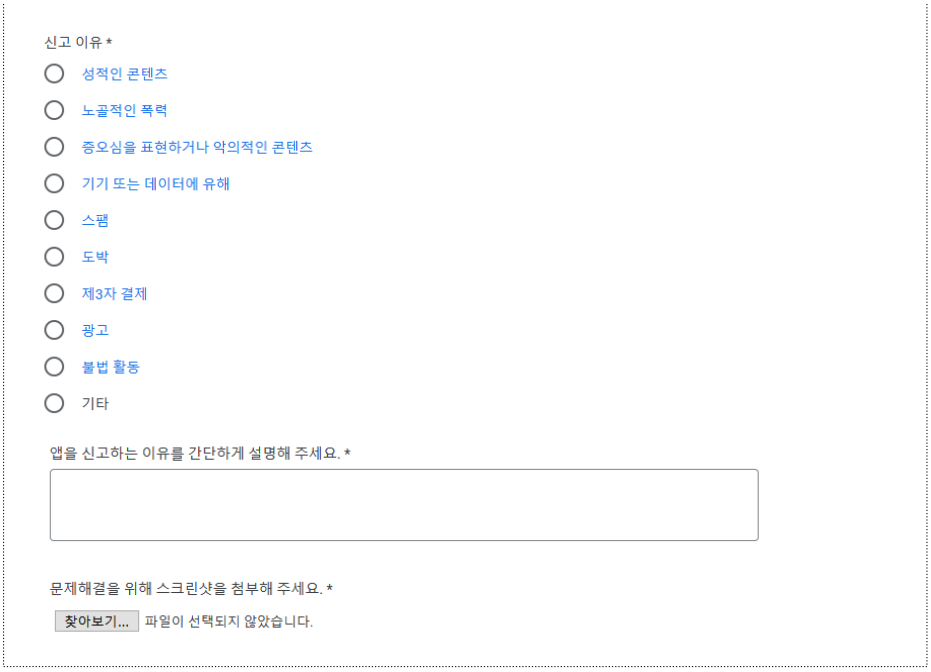
- ▸ 또한 성적인 콘텐츠, 증오성 콘텐츠, 명의 도용을 포함하여 개발자 배포 계약을 위반한 앱이나 댓글의 경우 "부적절한 콘텐츠 신고"가 가능함
- ▸ 규제당국 또는 법집행기관이 불법정보나 불법정보와 연관된 것으로 의심되는 앱에 대해서 구글에 삭제 등을 요청할 수 있음
- ▸ 구글은 6개월 단위로 투명성보고(Transparency Report)를 통해 국가별・사안별 콘텐츠 삭제 요청에 대해서 공개하고 있음

[애플 앱스토어 정책]

- ▸ 규제당국 또는 법집행기관이 불법정보나 불법정보와 연관된 것으로 의심되는 앱에 대해서 앱스토어에서 삭제할 것을 요청할 수 있음
- ▸ 애플은 매달 투명성보고(Transparency Report)를 통해 국가별・사안별 앱 삭제 요청에 대해서 공개하고 있음

[구글 플레이스토어의 부적절한 앱 신고 절차]





나. TCP Fragmentation 방식의 우회접속과 접속차단 실효성 평가

(1) TCP Fragmentation 방식의 우회접속

○ (명칭) TCP fragmentation(TCP단편화), MTU 분할 등으로 불림

- MTU 값†을 조정하는 MTU분할로 통칭되나, '인터넷규제개선 공론화협의회(2019년)'의 기술소위는 TCP통신을 분할한다는 의미로 TCP fragmentation으로 명명함

  † MTU(Maximum Transmission Unit)는 한 번에 전송되는 패킷의 최대단위를 의미함.

- MTU의 기본 취지는 다양한 망마다 적정한 패킷사이즈가 있기 때문에 최대 패킷사이즈를 망의 특성에 따라서 조절하는 것

- 모든 패킷을 분할하지 않고 클라이언트헬로 메시지만 분할하는 앱† 이나 프로그램 등도 가능하기 때문에, 클라이언트헬로 패킷 단편화(ClientHello packet fragmentation)라는 명칭도 가능함

  † 예: https://aspear.io나 https://github.com/ValdikSS/GoodbyeDPI

○ (접속차단) 현행 접속차단 방식은 ClientHello 패킷 내부의 SNI(실제 서버의 이름)을 탐지하여 차단하는 방식

- 클라이언트(웹브라우저)가 서버(웹서버)와 암호 통신(TLS)을 할 때 TCP 연결이 되고 나서 제일 처음 클라이언트가 ClientHello를 서버에 보내게 되며, ClientHello 패킷 내부에 평문으로 공개된 SNI필드 정보를 확인
- 네트워크 탐지 장비는 in-path가 아닌 out-of-path로 작동을 하고 있으며 차단을 해야 할 때 패킷을 누락(drop)시키는 방식이 아니라 연결을 끊는 RST 패킷을 클라이언트와 서버에 전송하는 것으로 연결을 끊는 방식

○ (개념) 탐지를 우회하기 위해서는 ClientHello 메세지를 한꺼번에 보내지 않고 2개(혹은 그 이상)으로 쪼개어 보내는 방식

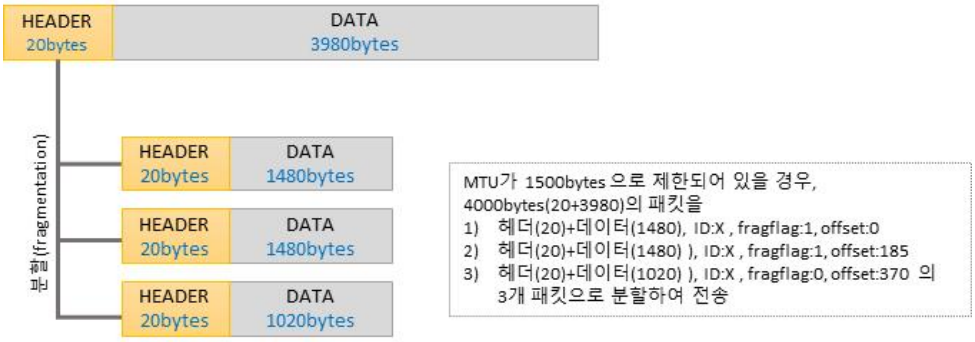
- 패킷의 최대 전송단위인 MTU*를 조정하여 클라이언트에서 쿼리를 분할 전송하고 서버에서 다시 결합하는 방식
- MTU분할과 복호화(fragmentation/reassembly)는 다양한 망 (유선/무선)을 지나는 패킷들을 망의 환경에 따라서 자동적으로 쪼개고 붙여주는 IP의 기본적인 기능으로, 인터넷의 특성자체가 다양한 망으로 연결되어 있기 때문에 이에 대한 호환성을 보장해주기 위한 방법
- 큰 IP 패킷들이 적은 MTU를 갖는 링크를 통하여 전송되려면 여러개의 작은 패킷으로 쪼개어/조각화 되어 전송되어야 함

  ※ MTU는 유선망의 경우 1.5Kbyte, 무선망의 경우 이보다 작은 값으로 설정되는 것이 일반적임. 이 크기보다 큰 사이즈의 패킷은 현시점에서 실제 네트워크 환경에서 처리(라우팅)가 되지 않음. 따라서 MTU보다 큰 크기의 패킷은 컴퓨터가 알아서 여러개로 쪼개어 네트워크로 전송하게 되는데, 이 MTU 값은 시스템의 설정 값을 바꾸어 변경할 수 있음

- 이렇게 조각화되어 전송되는 패킷을 최종수신단에서 재조립(Reassembly)하면 원본의 데이터로 환원할 수 있음

  ※ IP 헤더에서 단편화-재결합을 위해 식별자, 플래그, 단편화 오프셋을 전달. 모두 같은 식별자(ID)를 가지고 있어야 하고, 마지막 단편화 데이터그램의 플래그는 0, 나머지 데이터그램의 플래그는 1, 오프셋 필드는 첫번째 단편화된 데이터그램의 페이로드를 8로 나눈 값으로 연속하여 할당함으로써, 단편화된 각각의 데이터그램의 순서를 알려주기 때문에 이를 활용해서 재결합할 수 있음

[그림 2-10] TCP Fragmentation의 개념



- 통신속도가 느린 환경에서 안정적인 통신을 위해서 MTU값을 낮게 설정함

※ 일반적으로 알려진 표준 MTU값은 케이블 모뎀이 1500, ADSL이 1454, 모뎀이 576 수준

○ (우회방법) 네트워크탐지장비에서 탐지 및 차단할 수 없도록 클라이언트에서 MTU를 조정하여 ClientHello 메시지를 분할 전송

- 일반적으로 ClientHello 메시지의 용량이 500bytes가 넘기 때문에 MTU를 465, 또는 400bytes 이하로 조정하여 전송하면 접속차단을 우회할 수 있다는 정보가 인터넷에 공유되고 있음

- 실제 사용자들은 시스템의 MTU를 직접 조절하는 방법보다 전용 앱(ASPEAR, GoodbyeDPI 등)을 사용

- MTU값을 작게 설정하면 한 번에 전송할 수 있는 패킷의 크기가 제한되기 때문에, 용량이 큰 데이터 전송이 필요한 통신(예: 게임 등)환경에서는 라우터에서 패킷을 쪼개서 전송하는 과정에서 통신장비에 부하† 가 가중되고 속도가 느려지는 문제가 발생할 수 있음

† MTU 조절방식은 ClientHello만 쪼개어 지는 것이 아니라 모든packet들이 쪼개어지기 때문에 시스템 차원에서 불필요한 자원이 낭비될 수 있으며 네트워크의 속도의 저하가 나타남

- 따라서 우회목적으로 MTU를 작게 조정했다면 다른 시스템으로부터 연결을 시도하기 위해 MTU를 재조정해야하는 번거로움이 있을 수 있음

- 또한 공유기를 사용할 경우 클라이언트 단말과 공유기 모두에서 MTU크기를 조정해야 하는 번거로움이 있음 등이 지적됨

(2) 기술대응 방향과 과제

○ (기술적 과제) 이론적으로는 기존 네트워크 장비 단에서 TCP 복호화(reassemble) 기능을 구현해서 쪼개진 URL정보를 탐지를 할 수 있음

- 패킷을 쪼개기(fragment) 전에는 접속차단 대상인 불법사이트의 URL이 쪼개지지 않았기 때문에 하나의 패킷에서 URL주소를 확인할 수 있음
- 그러나 접속단의 주소정보가 나뉘어져 여러 개의 패킷에 분산되게 되면, 이 쪼개진 패킷들이 재조합(reassembly)되기 전까지는 네트워크 사업자가 이를 파악하기 어려움
- TCP 단편화와 복호화 작업은 네트워크가 아니라 인터넷접속의 끝인 호스트와 서버 단에서 발생하기 때문에 네트워크 사업자가 통신의 중간에서 이를 파악하는 것이 쉽지 않음
- 네트워크 사업자가 이러한 연결들을 접속차단하기 위해서는 복호화(reassembly)를 라우터에서 실행해야 하는데, 만약 in-path방식으로 탐지·차단이 이뤄질 경우 IP 망의 특성에 따라서 거의 불가능에 가깝다는 주장도 있음

  ※ 초당 수백만 이상의 패킷을 처리해야 하는 고속의 라우터에서, in-path방식으로 동일한 접속을 판별하고 여러 개의 패킷을 재조립하기 위해서 저장하고 다시 복호화과정(reassembly operation)을 수행한다는 것은 저장 메모리(memory) 부하, cpu부하 등이 커져서 불가능에 가깝다는 의견이 있음

- 따라서 In-path방식의 탐지·차단은 모든 패킷을 다 검색하는 것이 아니라 부분적 sampling을 통해서 실태파악을 하는 수준에 머물 것이라는 주장이 있음
- 그러나 실제 유해사이트 접속 트래픽 탐지의 경우, 모든 패킷을 처리하지 않고 패킷에 클라이언트 헬로 메시지가 포함되어 있는지 여부를 확인한 후, 해당 패킷에 단편화된 TCP를 복호화하는 방식으로 탐지할 수 있어 처리용량 및 속도 등의 문제를 해결하고 있음

  ▸ 차단장비는 데이터의 시작에 “16 03 01”로 시작되는 패턴이 있는지를 탐지하여 클라이언트 헬로 메시지가 있는지를 확인한 후, 서버네임정보와 차단목록을 비교하여 차단하는 단계적

방식으로 차단 실시

1) 패킷이 클라이언트 헬로인지 파악(데이터의 시작이160301로 시작하는지 여부)하고, 클라이언트 헬로가 아니면 무시

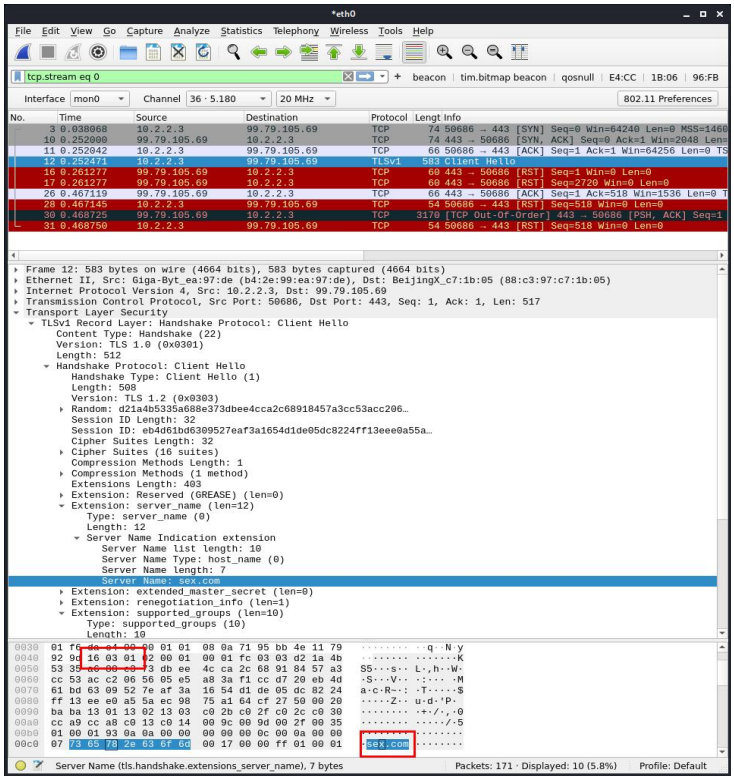
2) 패킷에SNI 정보가 있는지 파악하고 SNI가 없으면 무시

3) 추출한SNI 정보가 유해사이트DB에 포함되어 있나? 포함되어 있지 않으면 무시

4) 차단 패킷을 클라이언트와 서버 측에 보내어 차단을 함

▸ ClientHello packet을 2개로 쪼개어서 보내면 1번과 2번의 조건이 만족하지 않으므로 차단을 우회할 수 있음

[그림 2-11] 클라이언트헬로 패킷 예시



❍ (탐지 방식) 이론적으로는 기존 네트워크 장비 단에서 TCP 복호화(reassemble) 기능을 구현을 해서 탐지를 할 수 있음

- TCP단편화의 실태를 파악하기 위해서는 작은 패킷들이 얼마나 증가했는지 추이를 파악하여 간접적으로 파악할 수 있음

※ 이 때 TCP ACK 패킷등 기본적으로 작은 사이즈의 패킷을 제외하고 패킷이 분할 되어 있음을 표시해주는 IP header의 Fragment offset 필드를 참조하여 하나의 패킷의 일부분임을 나타내주는 패킷을 모니터링하면 이러한 패킷들이 얼마나 되는지 파악할 수 있음

- 네트워크 장비에서 탐지 및 차단 SW가 탑재된 형태로 운영되고 있으며, 이론적으로는 해당 탐지 및 차단 SW를 업그레이드를 하면 대응이 가능함

- 현재 유해사이트 탐지 및 차단 장비에서는 이러한 복호화 기능이 부재함

※ 전송패킷을 보고 패킷의 목적지 주소를 기준으로 보내는 곳과 받을 곳을 계산하여 해당포트로 연결하는 웹방화벽(firewall)이나 보안스위치(L7 switch) 등에서는 이러한 기능이 일부 탑재되어 있으나, 현재 유해사이트 탐지 및 차단 장비에서는 이러한 기능이 구현되어 있지 않음

- 따라서, 유해사이트 탐지 및 차단장비에서 TCP 복호화 기능을 추가할 경우, MTU조정을 통한 접속여부를 확인할 수 있음

- 인터넷 프로토콜(IP)에서는 하나의 IP 패킷에서 분할된 패킷들이 서로 다른 경로를 가지는 것이 가능해서 탐지가 어렵다는 주장도 있으나, 현재 인터넷 접속에서 다른 경로를 선택하는 경우는 많이 발생하지 않아, 네트워크 장비 단에서 TCP 복호화를 통해, URL 정보를 탐지하는 것이 가능함

- 현재 네트워크에서 MTU 값이 작은 네트워크 (1500 바이트 이하)는 많지 않으므로, 분할된 IP 패킷의 경우, 의도적으로 패킷이 분할되었을 가능성이 높아, 분할된 패킷의 현황 파악을 통해 우회접속의 현황을 간접적으로 파악할 수 있을 것으로 예상됨

○ (네트워크 속도에 미치는 영향) 현재 유해사이트 탐지 및 차단장비가 out-of-path방식으로 이뤄지고 있어 TCP복호화 기능을 추가할 경우에도 네트워크 흐름에 영향을 주지 않는다고 판단되나, 이를 검증하기 위한 테스트가 필요함

- 일반적으로 out-of-path로 작동하는 유해사이트 탐지·차단 장비는 기존 트래픽에 큰 영향을 주지 않음

- out-of-path 방식은 패킷의 변경이나 차단이 불가능하므로 기존 패킷을 제어하는 것이 아닌 TCP 연결을 끊을 수 있도록 RST 패킷 인젝션(RST packet injection)† 을 실시하는 방식

† TCP통신의 헤더(header)에 논리적 TCP연결회선 제어 및 데이터 관리용 필드(control flag field)가 존재하는데, 그 중 RST는 송신자가 유효하지 않은 연결을 시도할 때 양 끝단(클라이언트와 서버)에

동시에 리셋신호를 보내서 일시적으로 세션을 끊는 방식

<표 2-6> In-path방식과 out-of-path방식의 비교

구분	in-path(또는 in-line) 방식	out-of-path (또는 mirroring)방식
분석 범위	▪ packet의 분석, 변경, 폐기가 가능	▪ packet의 분석만 가능
장비	▪ 네트워크의 흐름에 지장을 준다.	▪ 네트워크 흐름에 지장을 주지 않는다.
예(H/W)	▪ router, switch, nat, backbone	▪ tap, switch mirror
예(S/W)	▪ iptable, arp spoofing	▪ pcap live, pcap file
특성	▪ 네트워크 탐지 모듈은 packet 전송 구간의 중간에 위치하게 된다. ▪ 패킷의 분석, 변경, 폐기 등이 가능하다. ▪ 장비에 이상이 있는 경우 네트워크가 끊기는 단점이 존재한다. ▪ 이를 위해 bypass NIC card를 사용하는 경우도 있다.	▪ 네트워크 탐지 모듈은 packet 전송을 복사하여 분석을 하게 된다. ▪ 패킷의 분석만이 가능하다. ▪ 장비에 이상이 있어도 네트워크가 끊기지 않는 장점이 존재한다. ▪ 기존의 네트워크 흐름에 지장을 주지 않는다.
개요도		

- 유해사이트 접속정보에 대한 탐지 및 차단은 in-path방식이 아닌 out-of-path방식으로 실시하고 유해사이트를 차단하는 별도의 전용장비에서 작동하기 때문에 TCP복호화 기능을 탑재했다고 해도 기존 네트워크 흐름에 영향을 주거나 실질적으로 고가의 장비나 속도 저하와 같은 우려가 크지 않을 것으로 예상함

- 또한 2000년대 초반부터 패킷 단편화(packet fragmentation)을 이용한 다양한 네트워크 공격방식이 유행을 하였고 이러한 공격방식을 대응하기 위해 대부분 네트워크 장비 개발업체들은 대부분 복호화 기술을 보유하고 있어, 복호화 기술을 적용하는 데에 있어 기술적 장벽도 높지 않다고 판단함

○ (요구사항) TCP 단편화 대응을 위한 기술 요구사항

- (기술조건) 차단SW에 TCP 복호화(Reassemble) 기능을 추가하는 SW업데이트와, TCP 복호화 기능 구현을 위해 CPU사용 증가에 대응하기 위한 장비 사양 개선(HW 업데이트)

- (예산) SW/HW 업데이트 및 업그레이드 비용
- (기간) 실제 ISP에 도입된 장비의 SW를 업데이트하게 되면 평균 6개월 정도 소요 예상(개발 및 테스트 포함)
- (고려사항) 기술적 대응을 적용함에 있어, SW 업데이트 비용(장비개발업체의 SW를 업데이트하고 테스트를 하는데 드는 경비)과 늘어난 CPU를 처리하기 위한 HW가 필요함

○ (기타 고려사항) out-of-path 방식의 우회접속방지 기술의 효과성에 대한 검증이 필요함

- out-of-path 방식으로 URL을 탐지하여 TCP RST 패킷을 전송함으로써 세션을 끊는 방식의 우회접속방지에 대한 무력화 방법도 개발되고 있어, TCP RST 패킷을 무시하는 기능에 대한 대응력을 시범적으로 테스트 해야함
- 또한 이러한 복호화를 통한 탐지가 보편화되었을 경우에, 이를 무력화시키는 방안도 어렵지 않게 구현이 가능할 것으로 예상됨
- 예를 들면, 현재의 스마트폰은 Wi-fi와 LTE/5G의 셀룰라 네트워크를 동시에 사용하는데, 분할된 패킷들을 강제로 각각 다른 네트워크 통해서 전송할 경우, 패킷들이 경로가 겹치지 않아서 복호화를 통한 탐지가 무력화 될 수 있음

3. 불법영상물 유통방지를 위한 필터링 조치와 관리

3-1. 불법영상물 필터링 기술 현황

○ 불법영상물의 유통을 제한하는 기술적 방법으로 네트워크에서는 차단(blocking 또는 drop-down) 조치가 가능하며, 정보통신서비스에서는 삭제 이외에도 검색, 업로드, 다운로드 등을 제한하는 필터링(filtering) 조치가 가능함

- 필터링이란, 콘텐츠의 내용을 확인할 수 있는 식별기술(Identification Techniques)이 포함된 필터를 설치하여 내용물의 적합·부적합을 판단하는 방식임
- 접근가능한 정보의 수준에 따라 필터링은 소극적필터링(Exclusion Filtering)과 적극적 필터링(Inclusion Filtering)으로 구분(진정남 외, 2016)되며, 웹하드, P2P, 소셜미디어와 같이 개방형 온라인 플랫폼에서는 소극적 필터링이 일반적으로 사용되고 있음
  - ▸ 소극적 필터링: 특정 정보의 검색을 제한하는 배타적 필터링 방식으로 사용자의 자유로운

업로드와 다운로드를 허용하는 개방형 온라인 플랫폼에서 특정정보로의 접근을 제한하는 방식임

- ▸ 적극적 필터링: 이용허락을 받은 콘텐츠1에 대해서만 검색과 접근을 허용하는 방식으로 서비스 제공 정보의 내용을 식별하고 온전히 통제할 수 있는 온라인 플랫폼에서 적용가능한 방식임

※ 권리자들과 공급계약을 체결하거나 이용허락을 받는 등 콘텐츠에 대한 접근이 허용되는 콘텐츠만을 의미(윤종수, 2009)

- 영상물의 필터링을 위해 식별하는 정보의 형식에 따라 필터링은 ①키워드 필터링, ②해시값(Hash) 필터링, ③핑거프린팅(finger-printing) 필터링† 으로 구분되며, 핑거프린팅 필터링은 다시 사용하는 방식에 따라 워터마크 기반의 핑거프린팅과 특징점 기반의 핑거프린팅으로 분류됨

† 지문을 통해 사람의 신원을 확인하듯이, 콘텐츠의 고유한 특징점을 찾아내 콘텐츠를 식별하기 때문에 핑거프린팅으로 지칭함(김동균, 2008)

- ▸ 키워드 필터링: 콘텐츠와 함께 제공되는 문자 정보(제목, 파일명, 게시글 등)를 사전에 목록화된 특정 금칙어(가슴, 음모, 자위, sex 등) 목록과 대조하여 콘텐츠의 적합· 부적합을 판단하는 방식으로, 콘텐츠의 내용이 아닌 부가정보만을 식별함
- ▸ 해시값 필터링: 해시함수를 이용하여 임의의 콘텐츠에 대한 요약 정보(해시값)를 생성하고 생성된 해시값을 차단 또는 허용하고자 하는 원본 콘텐츠의 해시값과 대조하여 콘텐츠 내용의 적합· 부적합을 판단하는 방식(한지연 외, 2015)
- ▸ 핑거프린팅 필터링: 콘텐츠를 식별하기 위해 고안된 특정 정보를(워터마크) 삽입하거나, 콘텐츠 자체의 고유한 특성인 주파수나 화면정보 등(특징점)을 분석· 대조하여 콘텐츠의 내용의 적합· 부적합을 판단하는 방식(이진태, 2009)으로 디지털성범죄 촬영물 등에서는 특징기반 필터링이 사용됨

<표 2-7> 핑거프린팅 필터링의 분류

유형	특성
워터마크 기반 필터링	▪ 워터마크(Watermark) 기술은 멀티미디어 콘텐츠에 사람이 인지할 수 없는 정보를 삽입하고, 검출기를 통해 삽입 정보를 식별하는 기술(알앤디비즈, 2010) ▪ 워터마크는 영상제작이나 배포 전(前) 단계에서 삽입되어야 하므로 저작권자 또는 판매권자가 명확한 저작물 등에 적용 가능
특징(DNA) 기반 필터링	▪ 차단하고자하는 영상물 고유의 특징(오디오 주파수, 색상 정보, 모션 정보, 장면전환 정보, 화면 내 특징 등)을 추출하여 데이터베이스를 구축하고, 임의 콘텐츠의 특징(DNA)을 추출하여 대조하는 방식(한승완 외, 2012)

	▪ 사전에 워터마크 등의 정보삽입 없이도 적용이 가능하기 때문에 디지털성범죄영상 등에 적용가능

○ (적용현황) 국내에서는 2012년부터 '웹하드 등록제'가 도입돼 각종 문제가 있는 영상의 업로드와 다운로드를 막는 필터링 기술이 의무화되어 특수유형부가통신사업자에게 적용되고 있음

- 2015년에 개정된 전기통신사업법 제22조의3(법률 제13011)은 특수유형부가통신사업자에게 불법음란정보 유통방지를 위한 의무조치 사항으로 '불법정보의 유통 방지를 위하여 대통령령으로 정하는 기술적 조치'를 취하도록 규정함

전기통신사업법 제22조의3(특수유형부가통신사업자의 기술적 조치 등) ① 제22조제2항에 따라 특수한 유형의 부가통신사업을 등록한 자(이하 이 조에서 "특수유형부가통신사업자"라 한다) 중 제2조제13호가목에 해당하는 자는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7제1항제1호에 따른 불법정보의 유통 방지를 위하여 대통령령으로 정하는 기술적 조치를 하여야 한다.
(이하 생략).

- 이때 기술적 조치는 동법 시행령 제30조의3에 규정되어 있는데, 제1호인 '정보의 제목, 특징 등을 비교하여 해당정보가 불법정보임을 인식할 수 있는 조치'와 제2호인 '해당 정보를 이용자가 검색하거나 송수신하는 것을 제한하는 조치'가 필터링을 의미함

전기통신사업법 시행령 제30조의3(불법음란정보의 유통 방지를 위한 기술적 조치 등)
① 법 제22조의3제1항에서 "대통령령으로 정하는 기술적 조치"란 다음 각 호의 모두에 해당하는 조치를 말한다.
1. 법 제22조제2항에 따라 특수한 유형의 부가통신사업을 등록한 자 중 법 제2조제13호가목에 해당하는 역무를 제공하는 자(이하 이 조에서 "사업자"라 한다)가 정보의 제목, 특징 등을 비교하여 해당 정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7제1항제1호에 따른 불법정보(이하 "불법음란정보"라 한다)임을 인식할 수 있는 조치
2. 사업자가 제1호에 따라 인식한 불법음란정보의 유통을 방지하기 위하여 해당 정보를 이용자가 검색하거나 송수신하는 것을 제한하는 조치
3. 사업자가 제1호의 조치에도 불구하고 불법음란정보를 인식하지 못하여 해당 정보가 유통되는 것을 발견하는 경우 해당 정보를 이용자가 검색하거나 송수신하는 것을 제한하는 조치
4. 사업자가 불법음란정보 전송자에게 불법음란정보의 유통 금지 등에 관한 경고문구를 발송하는 조치
(이하생략)

- 현시점에 특수유형부가통신사업자에게 적용되고 있는 필터링은 총 3단계(키워드 필터링, 해시값 필터링, 특징기반 필터링)로, 콘텐츠의 유형(불법저작물과 불법촬영물)에 따라

적용되는 단계가 다름

- 불법저작물 필터링 분야에서는 키워드 필터링, 해시값 필터링, 특징기반 필터링이 모두 적용된 반면, 반면 불법촬영물 필터링 분야에서는 핑거프린팅(워터마크나 특징DNA 등) 생성이나 분석이 용이하지 않아, 불법영상물 필터링 분야에서는 금칙어 기반, 해시 기반 필터링만 적용되어 왔음(한지연 외, 2015)

<표 2-8> 필터링 방식별 적용현황과 장·단점

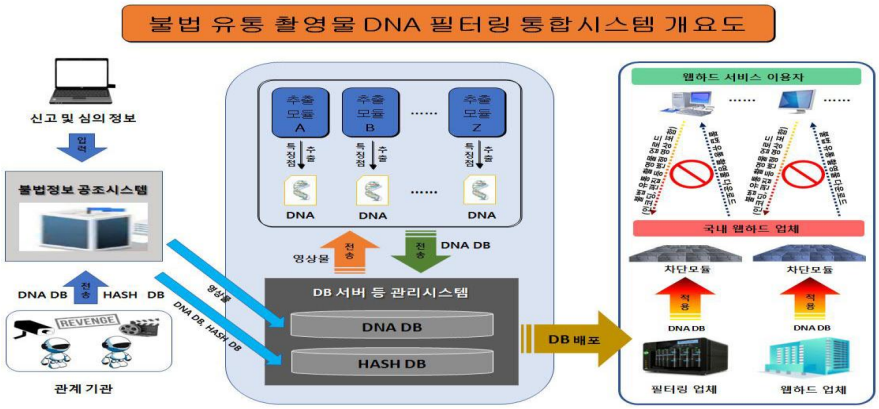
유형	비고	차단 수준	적용 난이도
키워드 기반 필터링	● 적용현황: 불법음란물과 저작물 모두에 적용되고 있으나, p2p업체에 따라 제목, 문자열, 파일 필터링이 각기 다르게 적용되고 있음 ● 장점: 처리부하가 적고 실시간 고속처리가 가능하며 광범위한 적용이 가능함 ● 단점: 파자(破字) 등의 변형을 통해 제목과 문자열 필터링을 우회할 수 있으며, 파일명 변경을 통해 파일 필터링을 우회할 수 있음	▲ 낮음	▲ 낮음
해시 목록 기반 필터링	● 적용현황: 불법음란물과 저작물 모두에 적용되고 있음 ● 장점: 해시정보 생성이 간단하고 처리속도가 빨라 광범위하게 적용할 수 있고, 해시목록을 범주화해서 구성하면 범주에 따라 차단이 가능함 ● 단점: 코덱 및 해상도를 변경하거나 약간의 편집을 가할 경우 식별이 어려움		
특징정보 기반 필터링	● 적용현황: 현시점에서 불법유해음란물에 대한 특징정보 데이터베이스가 구축되어 있지 않아 저작물에만 제한적으로 적용되고 있음 ● 장점: 파일명이나 코덱 등을 변경해도 콘텐츠의 내용을 판단할 수 있어 타 필터링 방법에 비해 타당성이 높음 ● 단점: 영상변형의 정도가 심한 불법·유해음란물의 경우 특징값이 무력화될 우려가 있어 지속적인 기술개발이 필요	높음 ▼	높음 ▼

- 해시 목록 기반 필터링은 해시정보의 생성이 간단하고 처리 속도가 빨라 광범위하게 적용할 수 있다는 장점도 있으나, 코덱이나 해상도 변경과 같은 작은 변형에도 쉽게 무력화된다는 단점으로 인해 불법영상물 필터링의 실효성이 낮다는 지적이 있어왔음

- 이에 범정부 합동'디지털 성범죄 피해 방지 종합대책('17.9.26)'에 따라, 방송통신심의

위원회는 불법영상물의 특징정보 추출시스템과 필터링 DB의 구축을 추진해옴

[그림 2-12] 웹하드/P2P의 불법유통촬영물 필터링을 위한 특징기반 DNA DB 개요도



출처: 여성가족부 · 과학기술정보통신부 · 법무부 · 방송통신위원회 · 경찰청 · 방송통신심의위원회(2018.11.28.)

○ (특징정보 기반 필터링의 절차) 콘텐츠 필터링은 임의콘텐츠의 특징을 추출하고, 추출한 특징정보를 기존에 구축된 불법촬영물 등에 대한 DNA DB와 매칭하여 불법성 여부를 식별· 차단하는 과정이 필요함

- 따라서 임의콘텐츠를 필터링 하기 위해서는 ① 불법정보에 대한 고유한 특징정보를 저장한 특징DNA DB가 있어야 하며, ② 조치의무사업자(필터링 기술업체 포함)가 임의 콘텐츠의 특징을 추출하여 DNA와 매칭하여 불법성을 식별하고 차단하는 기술이 필요함

- (특징DNA DB) 영상물의 고유한 특징정보(DNA)를 추출하여 메타정보와 함께 저장한 DB로, 불법촬영물 여부를 판단하기 위한 준거 정보를 제공함

- (콘텐츠 식별) 임의 콘텐츠로부터 특징정보를 추출하고, 해당 특징정보를 특징DNA DB와 매칭하여, 불법성여부를 판단하고 처리하는 과정을 의미함

○ (특징DNA DB) 불법촬영물 등 불법영상물로부터 추출한 특징정보를 저장한 저장소

- 불법촬영물 원본은 피해자에 대한 심각한 인권 침해 및 개인정보 침해 우려가 있어

원본영상물의 불법적 유출이나 유포로 인한 피해 방지를 위해서 엄격한 관리가 필요함

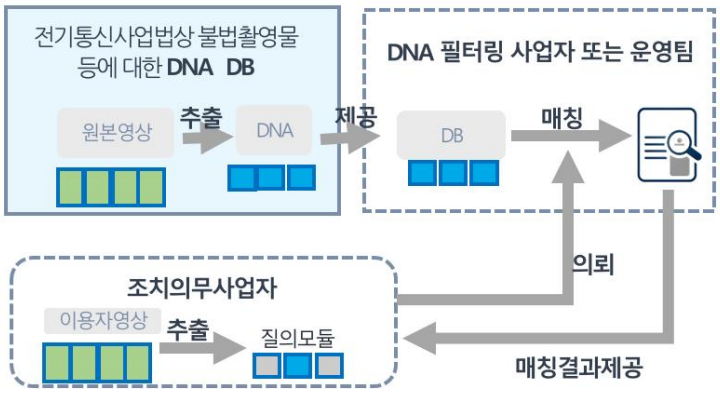
- 따라서 불법영상물에 대한 관리권한이 있는 주체의 관리 하에서 관리주체가 인정한 자가 특징정보를 추출하여 DNA DB를 구축하고 원본영상물이 아닌 DNA DB를 배포하는 것이 필요함
- 새로운 불법영상물이 확인될 때마다 해당 영상물의 DNA를 추출하여 DNA DB에 지속적으로 업데이트하기 위해서는 불법영상물에 대한 관리권한이 있는 주체(방송통신심의위원회)가 DNA DB를 보유 및 운영할 필요가 있음
- 현재 경찰청, 여가부는 수사 또는 피해자 지원 과정에서 각각 수집한 불법촬영물을 방송통신심의위원회로 전달하고, 방송통신심위원회는 경찰청과 여가부가 수사 및 피해자 지원 과정에서 확보한 불법촬영물과 심의결과에 따른 불법촬영물을 취합하여 관리하고 있음
- 이 취합된 불법촬영물 영상들로부터 특징점을 추출하여 DB를 구축하고, 새로운 불법촬영물 영상들이 추가될 경우 지속적인 업데이트를 실시해야함

○ (콘텐츠식별) 불법영상물의 유포방지를 위해서는 기술업체가 보유하고 있는 특징정보 추출 및 인식의 기술 수준에 대하여 평가하여 일관성 있는 성능을 보장할 수 있는 관리시스템 구축이 필요함

- 콘텐츠 식별기술이란, 웹하드나 온라인서비스 등에 게재하려고 하는 임의콘텐츠로부터 특징정보들을 추출하는 '검출기술'과 추출한 특징정보를 불법영상물DNA DB를 검색·매칭하여 불법여부를 판단하는'인식 및 차단기술'로 구성됨
- 콘텐츠 식별 시스템은 1) 핑거프린트(특징을 추출하는 부분)과 2) 인식을 위해 특징을 관리하고 매칭하는 부분으로 나뉨
- 추출부에서는 콘텐츠로부터 특징을 추출하기 위해 콘텐츠의 포맷을 분석하고 특징을 추출할 수 있는 정규화된 데이터를 생성하는 전처리(front-end) 과정이 필요
- 매칭부에서는 기존의 특징들을 관리해주는 DB와 인식 속도를 빠르게 하기 위한 검색 구조 및 특징들 사이의 유사도를 평가할 수 있는 척도가 필요함
- 임의콘텐츠를 식별하는 기술은 개별 기술업체(필터링사업자 등)들이 개발하여 사용하게 되는데, 기술업체마다 임의콘텐츠를 식별하는 기술 방식과 기술수준이 달라 필터링

성능의 최소요구수준 마련과 객관적·신뢰성 있는 계량화된 평가기준과 수단 등이 포함된 성능평가 관리체계가 필요함

[그림 2-14] 특징정보 기반 필터링 절차



3-2. 필터링 성능평가제도 도입방안

가. 도입필요성

○ (배경) 최근 개정된 전기통신사업법(법률 제16019호)의 제22조의5에 따라, 부가통신사업자와 특수유형부가통신사업자에게 불법촬영물 등의 유포·확산을 방지하기 위한 특징기반 필터링 조치의무가 부과됨

> **전기통신사업법 제22조의5(부가통신사업자의 불법촬영물 등 유통방지)** ① 제22조제1항에 따라 부가통신사업을 신고한 자(제22조제4항 각 호의 어느 하나에 해당하는 자를 포함한다) 및 특수유형부가통신사업자 중 제2조제14호가목에 해당하는 자(이하 "조치의무사업자"라 한다)는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 중 다음 각 호의 정보(이하 "불법촬영물등"이라 한다)가 유통되는 사정을 신고, 삭제요청 또는 대통령령으로 정하는 기관·단체의 요청 등을 통하여 인식한 경우에는 지체 없이 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취하여야 한다. (이하 생략)

- 개정된 동법 시행령 제30조6는 기술적· 관리적 조치의무대상사업자로 「저작권법」

제104조에 따른 특수한 유형의 온라인서비스제공자와 전년도 매출액이 10억원 이상이고 하루 평균 이용자 수가 10만 명 이상인 부가통신사업자로 지정함

- 이에 따라 웹하드, P2P 사업자(36개)와 일정 규모 이상 부가통신사업자(60~70여개 추정) 등이 조치의무사업자에 포함될 예정

<표 2-9> 기술적·관리적 조치의무사업자(시행령 제30조의6제1항)

구분	대상 규모
o 특수유형부가통신사업자 중 공중이 저작물 등을 공유할 수 있도록 하는 온라인서비스제공자(웹하드, P2P) 전체(사업법 제2조제14호가목)	36개 ('20년 8월 기준)
o 부가통신사업자 중 다음 각 호의 어느 하나에 해당하는 자로써, 불특정 다수의 이용자가 서로 정보를 공유하는 것을 목적으로 하는 SNS 및 커뮤니티, 인터넷개인방송, 검색서비스 등 - 정보통신서비스 부문 전년도 매출액 10억원 이상 또는 전년도 4/4분기 일일평균 이용자수 10만 명 이상 - 정보통신망을 이용하여 일반에게 공개되어 유통되는 정보를 이용자가 게재·공유할 수 있는 서비스 중 각 목*의 어느 하나에 해당하는 서비스를 제공하는 자(단, 재화의 판매나 용역의 제공을 주로 하거나, 국가, 지방자치단체, 공공기관, 법인운영서비스 제외)	60~70여개 추정

- 또한 조치의무대상사업자들은 이용자가 게재하려는 정보의 특징을 분석하여 방심위에서 불법촬영물등으로 심의·의결한 정보에 해당하는지 여부를 비교·식별 후 그 정보의 게재를 제한하는 조치(이하 '특징정보 기반 필터링 조치)를 2020년 12월10일까지 시행해야함

- 이때, 조치의무사업자는 특징정보 기반 필터링 조치를 적용함에 있어 ① 국가기관이 개발하여 제공하는 기술을 사용하거나 ② 방송통신위원회가 정하여 고시하는 기관이나 단체의 성능평가를 통과하고 평가 유효기간 내에 있는 기술을 적용해야함

<표 2-10> 전기통신사업법 시행령상 조치의무사업자의 기술적관리적 조치 내용

구분	기술적관리적 조치 내용
기술적· 관리적 조치 내용 (시행령 제30조의6)	▸신고·삭제 요청 등을 할 수 있는 기능 마련 ▸이용자가 입력한 검색어로 제목·명칭 등을 비교하는 방식으로 식별하여 검색결과 삭제 등 검색결과 송출 제한 ▸이용자가 게재하려는 정보의 특징을 분석하여 방심위에서 불법촬영물등으로 심의·의결한 정보에 해당하는지 여부를 비

구분	기술적관리적 조치 내용
	교・식별 후 그 정보의 게재를 제한하는 조치 < 조치 기술 선택 사항 > 가. 국가기관이 개발하여 제공하는 기술 나. 방통위가 정하여 고시하는 기관・단체가 최근 2년 이내에 시행한 성능평가를 통과한 기술 ▸불법촬영물등을 유통할 경우 관련 법률에 따라 처벌 받을 수 있다는 내용을 이용자에게 미리 알리는 조치 ▸ 로그기록 보관(3년)
위반 시 제재규정 (법 제95조의2와 법제 104조)	▸과태료 5천만원 / 등록취소 ▸벌칙(3년 이하의 징역 또는 1억원 이하의 벌금)

○ (제도적 필요성) 개정된 전기통신사업법 시행(12.10.)으로 인해 부가통신사업자에 대한 불법촬영물 등의 유통방지를 위한 기술적・관리적 조치에 대한 세부기준 및 이행평가 체계 수립 필요

- 시행령 제30조의6에 정의된 성능평가는 송수신을 제한(필터링)하는 기술 중 특징기반(DNA) 필터링 기술의 성능을 객관적인 평가 지표로 정량화하여 제시하는 평가를 의미함
- 특징기반 필터링기술은 필터링 기술업체마다 콘텐츠 식별・ 차단하는 기술방식과 기술수준이 각기 달라, 필터링 성능의 최소요구기준을 지정하여 적합성 여부를 평가하는 성능평가 제도 도입이 필요함

○ (성능평가의 기대효과) 표준규격에 따른 적합성 평가 및 성능 인증을 통해 민간상용기술 및 사업자 자체 기술에 대한 신뢰성을 확보하고, 불법촬영물 유통 방지의 실효성을 제고할 수 있으며, 계량적 지표를 활용한 객관적인 관리가 가능함

- (신뢰성) 민간 상용 필터링 업체가 보유한 기술과 조치의무사업자가 자체적으로 개발・운영하는 필터링 기술 등의 불법촬영물 필터링 성능을 평가・ 인증하여 조치의무사업자의 기술적 조치의 신뢰성 보장
- (실효성) 자체 필터링 시스템을 사용할 수 없는 조치의무사업자들에게 신뢰할 수 있는 필터링 시스템을 제공하여 불법촬영물 등의 유통방지 실효성 확대
- (객관성) 불법촬영물 등의 특징정보를 담은 표준 DNA DB 개발과 필터링 인증제도 도입으로, 계량적이고 객관적인 민간 상용필터링 시스템 기술수준 관리가 가능함

나. 유사사례

○ (유사제도) 저작권법 및 동법 시행령에 근거하여 불법저작물 등의 유통방지를 위해 특수유형 부가통신사업자(웹하드)를 대상으로 성능평가를 통과한 필터링 기술의 적용이 의무화되어 있음

- 전기통신사업법 제29조 제9항에 따른 시행령 별표3. 특수한 유형의 부가통신사업자 등록요건은 「저작권법」 제104조 및 법 제22조의3에 따른 기술적 조치를 취하도록 하고 있음
- 이때 「저작권법」제104조에 따른 기술(DNA필터링)과 관련하여, 특수유형부가통신사업자는 한국저작권위원회의 성능평가를 통과하고 평가 유효기간 내에 있는 기술을 사용하도록 하고 있음
- 저작권법 제104조는 필터링 등의 기술적 조치를 다른 사람들 상호 간에 컴퓨터 등의 기기를 이용하여 저작물을 복제하거나 전송하도록 하는 것을 주된 목적으로 하는 온라인 서비스 제공자로, 특수한 유형의 온라인 서비스 제공자에 한정하여 적용하고 있음
- 또한 저작권법 시행령 제66조의 4는 한국저작권위원회의 저작권정보센터가 기술적 보호조치 표준이행에 대한 평가 및 이를 위한 표준 평가 도구 개발업무를 수행하도록 위임

<표 2-11> 저작권법 및 동법 시행령 상 필터링 관련 조항

저작권법	저작권법 시행령
제104조(특수한 유형의 온라인 서비스제공자의 의무 등) ①다른 사람들 상호 간에 컴퓨터를 이용하여 저작물등을 전송하도록 하는 것을 주된 목적으로 하는 온라인서비스제공자(이하 "특수한 유형의 온라인서비스제공자"라 한다)는 권리자의 요청이 있는 경우 해당 저작물등의 불법적인 전송을 차단하는 기술적인 조치 등 필요한 조치를 하여야 한다. 이 경우 권리자의 요청 및 필요한 조치에 관한 사항은 대통령령으로 정한다. ② 문화체육관광부장관은 제1항의 규정에 따른 특수한 유형의 온라인서비스제공자의 범위를 정하여 고시할 수 있다. ③ 문화체육관광부장관은 제1항에 따른 기술적인 조치 등 필요한 조치의 이행 여	저작권법 제66조(저작권정보센터 조직 및 운영 등) ① 법 제120조에 따른 저작권정보센터에는 저작권 정보제공 등을 위한 저작권거래소와 권리관리정보, 저작권 보호 및 유통지원을 위한 기술위원회를 둘 수 있다. ② 저작권정보센터는 다음 각 호의 업무를 수행한다. 1. 저작물 권리관리정보의 체계적인 수립·관리·활용을 위한 통합관리체계 구축 및 운영 2. 저작물 및 권리자를 식별할 수 있는 통합저작권번호체계의 개발, 관리 및 보급 3. 기술적 보호조치의 표준화에 관한 연구 4. 기술적 보호조치 표준이행에 대한 평가

부를 정보통신망을 통하여 확인하여야 한다. ④ 문화체육관광부장관은 제3항에 따른 업무를 대통령령으로 정하는 기관 또는 단체에 위탁할 수 있다.	및 이를 위한 표준 평가 도구 개발 5. 저작권 정보 기술에 관한 조사・연구

○ (성능평가체계) 한국저작권위원회가 성능평가 제도 시행 및 정책 수립, 불법저작물 DB관리, 성능평가 홈페이지 관리

- 한국저작권위원회의 저작권기술팀이 성능평가 사업계획을 수립하여 성능평가를 실시할 수 있는 역량을 가진 위탁사업자와 사업을 관리하는 감리업체를 선정하여 관리

※ 저작물의 경우, TTA가 기술적보호조치의 표준규격을 개발하고, 한국저작권위원회가 기술적보호조치의 성능기준을 수립하여 민간 상용 필터링 기술에 대해 평가・인증

- 선정된 성능평가 주관사업자가 테스트베드 고도화 및 성능평가 업무를 수행하게 되며, 감리업체는 성능평가 운영을 감리함

<표 2-12> 저작권 성능평가의 운용체계

구 분	역 할	비 고
한국저작권위원회 (주관기관)	o 사업 추진 - 사업 기획 및 예산운영 - 조달입찰 의뢰 및 공고 - 시스템 요구사항 제시, 문제 해결 지원 - 사업 총괄 관리, 최종 검사 수행 등 - 감리업체 관리 - 성능평가 안내 및 접수 포털 운영	사업 주관
감리업체	o 사업 수행 관련 기술감리 실시 o 개선 사항 도출・권고	기술감리
주관사업자	o 사업 수행 o 사업 산출물 작성 등	사업수행

자료: 한국저작권위원회(2020).

○ (절차) 필터링을 이용한 불법저작물의 검색 및 송신제한 조치는 저작권법 시행령 제45조에 따른 권리자의 요청에 의해 개시되며, 요청을 접수 받은 특수유형부가통신사업자는 령 제46조에 따라 검색 및 송신제한을 위한 기술적 조치를 실시해야함

- 권리자는 기술조치 등 요청서, 권리자임을 소명할 수 있는 자료, 차단을 요청하는 저작물을 인식할 수 있는 자료 등을 구비하여 특수유형부가통신사업자에게 기술적 조치 등을

요청할 수 있음(저작권법시행령 제45조)

- 이때, 권리자임을 소명할 수 있는 자료로는 저작물 등의 권리자로 표시된 저작권 등의 등록증 사본 또는 그에 상당하는 자료, 자신의 성명 등이나 이명으로서 널리 알려진 것이 표시되어 있는 저작물 등의 사본 또는 그에 상당하는 자료 등이 해당됨

저작권법시행령 제45조(권리자의 요청)

법 제104조제1항에 따라 권리자가 해당 저작물 등의 불법적인 전송을 차단하는 기술적인 조치 등 필요한 조치를 요청하려면 문화체육관광부령으로 정하는 요청서(전자문서로 된 요청서를 포함한다)에 다음 각 호의 자료(전자문서를 포함한다)를 첨부하여 특수한 유형의 온라인서비스제공자에게 제출하여야 한다. 다만, 권리자가 저작권신탁관리업자이거나 최근 1년 이내에 반복적인 침해행위에 대하여 권리자임을 소명할 수 있는 자료를 이미 제출한 사실이 있는 경우에는 제1호의 자료를 제출하지 아니할 수 있다.

1. 권리자임을 소명할 수 있는 다음 각 목 중 어느 하나에 해당하는 자료

가. 자신이 그 저작물등의 권리자로 표시된 저작권 등의 등록증 사본 또는 그에 상당하는 자료

나. 자신의 성명등이나 이명으로서 널리 알려진 것이 표시되어 있는 저작물등의 사본 또는 그에 상당하는 자료

2. 차단을 요청하는 저작물등을 인식할 수 있는 저작물의 제호, 그에 상당하는 문자나 부호(이하 "제호등"이라 한다) 또는 복제물 등의 자료

- 권리자의 요청을 접수한 특수유형부가통신사업자는 저작물 등의 제호 등과 게시물의 특징(DNA)을 비교하여 불법저작물을 특정하고 이에 대한 검색 및 송신제한을 위한 기술적 조치를 실시해야함(저작권법시행령 제46조)

- 만약 특수유형부가통신사업자가 이를 이행하지 않은 경우 3천만 원 이하의 과태료가 부가될 수 있음

○ (기술적 조치) 특수유형부가통신사업자가 취해야 하는 기술적 조치는 저작물의 불법적인 복제와 전송을 차단하기 위한 저작물 인식조치, 검색제한 조치, 송신제한조치 및 경고문구 발송임(저작권법시행령 제46조)

- 기술적 조치 등 필요한 조치를 하지 않을 경우, 당해 특수유형부가통신사업자는 저작권법 제142조와 동법 시행령 제77조에 근거해 3천만원이하의 과태료 부과

저작권법시행령 제46조(불법적인 전송을 차단하는 기술적인 조치 등 필요한 조치) ①법 제104조제1항 전단에서 "해당 저작물등의 불법적인 전송을 차단하는 기술적인 조치 등 필요한 조치"란 다음 각 호의 모든 조치를 말한다.

1. 저작물등의 제호등과 특징을 비교하여 저작물등을 인식할 수 있는 기술적인 조치
2. 제1호에 따라 인지한 저작물등의 불법적인 송신을 차단하기 위한 검색제한 조치 및 송신제한 조치
3. 해당 저작물등의 불법적인 전송자를 확인할 수 있는 경우에는 그 저작물등의 전송자에게 저작권침해금지 등을 요청하는 경고문구의 발송

②제1항제1호 및 제2호의 조치는 권리자가 요청하면 즉시 이행하여야 한다.

- 반면 저작권법 제102조는 특수유형부가통신사업자가 저작권 침해행위를 인지하고 방지 및 중단을 시킨 경우, 저작권법에 따라 보호되는 권리가 침해되더라도 그 책임을 감경 또는 면제하고 있음

저작권법 제102조(온라인서비스제공자의 책임 제한)

① 온라인서비스제공자는 다음 각 호의 행위와 관련하여 저작권, 그 밖에 이 법에 따라 보호되는 권리가 침해되더라도 그 호의 분류에 따라 각 목의 요건을 모두 갖춘 경우에는 그 침해에 대하여 책임을 지지 아니한다.

1. 내용의 수정 없이 저작물등을 송신하거나 경로를 지정하거나 연결을 제공하는 행위 또는 그 과정에서 저작물등을 그 송신을 위하여 합리적으로 필요한 기간 내에서 자동적·중개적·일시적으로 저장하는 행위

가. 온라인서비스제공자가 저작물등의 송신을 시작하지 아니한 경우

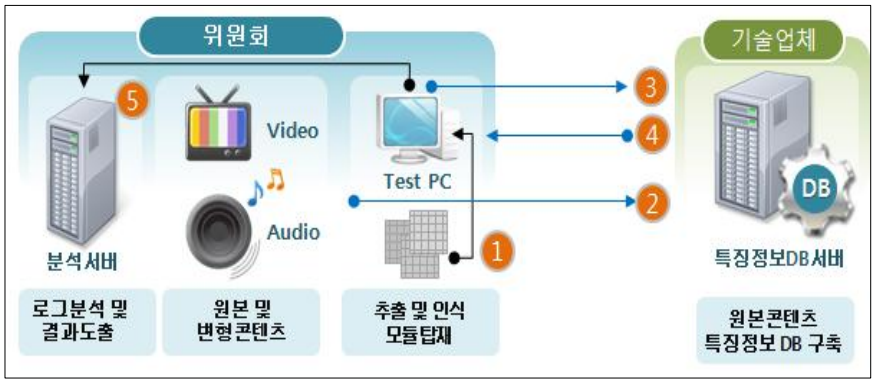
<생략>

라. 저작물등을 식별하고 보호하기 위한 기술조치로서 대통령령으로 정하는 조건을 충족하는 표준적인 기술조치를 권리자가 이용한 때에는 이를 수용하고 방해하지 아니한 경우

○ (성능평가대상) 특수유형부가통신사업자가 적용해야하는 기술적 조치 중에, 영상물의 특징을 분석하여 필터링하는 기술에 대해서는 성능평가를 실시해야함

- (평가범위) 특수유형부가통신사업자가 시행해야하는 기술적 조치 중에서 특징기반 필터링 기술만 평가대상으로 하며, 한국저작권위원회의 시험용 PC와 기술업체의 서버간 네트워크 통신을 통해 필터링 기술의 알고리즘에 대해 평가하고 기준 부합시 확인서를 발급하는 방식으로 운영됨

[그림 2-15] 특징(DNA)기반 필터링 알고리즘 평가 방법



출처: 한국저작권위원회(2011).

- (신청대상) 특수유형부가통신사업자가 신청하는 것이 아니라 특수유형부가통신사업자에게 필터링 시스템을 제공할 필터링 제품 개발사가 신청하도록 하고 있음
- (검증대상) 기술평가는 서비스가 아닌 특징기반 필터링 제품을 대상으로 검증하게 되며, 기술업체가 보유하고 있는 특징정보 추출 및 인식에 대한 기술(알고리즘) 수준에서 이뤄짐
- (평가방식) 한국저작권위원회 평가 PC와 기술업체의 서버 간 네트워크 통신(상호운영)을 통해 평가 항목을 측정하게 됨

○ (평가항목) TTA가 개발한 단체표준규격인'비디오 콘텐츠 필터링 성능평가 표준(TTAK.KO-12.0161/R1)(2013년 12월 18일 개정)' 준용

- 강인성, 일관성, 시스템사용률, 특징정보량, 고속추출, 추출 및 검색· 비교속도, 부분매칭, 인식정보량 등 8가지 항목을 측정

<표 2-13> TTA의 비디오콘텐츠 필터링 성능평가표준의 품질평가 항목

평가항목	내 용
강인성	o 변형콘텐츠의 특징정보가 원본콘텐츠의 특징정보를 정확하게 인식하는 정도
일관성	o 반복적으로 수행된 특징정보 추출 및 인식에 대한 일관성 유지 정도

평가항목	내 용
추출 및 검색·비교 속도	o 변형(왜곡) 콘텐츠가 원본콘텐츠의 특징정보를 인식하는데 소요되는 변형콘텐츠 특징정보 추출 및 검색/비교 시간
시스템 사용률	o 특징정보 추출 및 인식 결과 회신 등에 사용한 시스템 자원 사용률
특징 정보량	o 원본콘텐츠 특징정보의 크기
고속 추출	o 원본콘텐츠 특징정보를 추출하는데 소요되는 시간
부분 매칭	o 콘텐츠 중간부문의 특징정보에 대한 인식 정도(믹스된 콘텐츠의 인식 정도)
인식정보량	o 특징정보 인식을 위해 필요한 콘텐츠의 최소 크기

○ (성능평가기준) 성능평가를 통과하고 확인서를 발급받기 위해서는 강인성, 일관성, 추출 및 검색/비교속도의 3가지 측면에서 기준통과가 필요함

- 강인성의 경우 3초 이내의 다양한 변형에도 인식이 가능한지의 여부와 오인식률을 평가하게 되며, 일관성은 100%, 추출 및 검색/비교속도는 3초 이하로 설정되어 있음
- 단, 콘텐츠 특성을 고려하여 성능평가의 대상인 저작물이 오디오, 비디오, 북스캔/만화인지에 따라서 강인성의 평가기준이 다소 달라짐
- 3초 이내의 강인성 기준이 오디오의 경우 97%, 비디오의 경우 95%, 북스캔/만화의 경우 95% 이상으로 설정되어 있음

<표 2-14> 한국저작권위원회 특징기반 필터링기술 성능평가기준

평가대상	평가기준(PC)	
오디오	강인성	3초이내 강인성 97%이상 인식, 오인식률 1%미만
	일관성	100%
	추출 및 검색/비교속도	3초이하
비디오	강인성	3초이내 강인성 95%이상 인식, 오인식률 1%미만
	일관성	100%
	추출 및 검색/비교속도	3초이하
북스캔 만화	강인성	3초이내 강인성 95%이상 인식, 오인식률 1%미만
	일관성	100%
	추출 및 검색/비교속도	3초이하

○ (적용여부 점검) 성능평가 확인을 받은 기술이 실재로 특수유형부가통신 서비스에 적용되었는

지의 여부는 과학기술정보통신부 주관 웹하드 등록요건 준수 실태점검에서 확인하며, 점검결과는 한국저작권위원회에 통보하게 됨

- (공지) 성능평가 결과 및 제한조치 대상기관 등을 한국저작권위원회 홈페이지에 공지
- (통보) 위원회의 시정요청 누적 횟수가 3회 초과될 경우 과학기술정보통신부(중앙전파관리소) 및 문화체육관광부 등 소관부처에 통보

다. 도입방안

○ (절차)사업법 제22조의 5 및 동법 시행령 제30조6에 따른 필터링 조치와 성능평가를 도입하기 위해서는 특징정보를 추출하여 필터링하는 '표준DNA DB'기술 개발 및 제공, 불법촬영물로부터 추출한 DNA DB의 구축과 배포, 자체기술을 사용하는 조치의무사업자를 대상으로 한 성능평가 실시가 필요함

- ① 표준 필터링 기술 개발·배포: 영상특징정보의 추출기술, 추출 DNA 정보와 원본 DNA 정보를 비교분석하는 식별기술, 실 서비스에 필터링을 적용하기 위한 공개API 기술의 개발과 개발된 기술을 조치의무사업자에게 배포하는 것을 포함함
- ② 표준DNA DB 구축· 배포: 방송통신심의위원회가 여가부와 경찰청 등으로부터 수집한 불법촬영물로부터 고유한 영상특징정보(DNA)를 추출하여 표준 DNA DB를 구축· 운영하고 하고, 해당 DB를 조치의무사업자에게 배포하는 것을 포함함
- ③ 조치의무사업자 대상 필터링 성능평가: 불법촬영물의 변형한 성능평가용 데이터셋 DB를 구축하고 사전에 지정한 성능평가 항목과 기준에 따라 특징정보 기반 필터링 기술의 성능을 평가하는 것을 의미함

<표 2-15> 표준 DNA DB 시스템 구축 및 필터링 성능평가의 절차

단계	업무	업무
STEP1. 표준필터링 기술개발	1. 표준 DNA 추출·식별기술 및 API개발	• (내용)불법촬영물 등에서 DNA를 추출하거나 서버에 업로드하려는 영상에서 DNA를 추출하는 기술, 추출한 DNA를 표준DNA DB와 매칭하는 기술, 공개 API기술을 포함함 • (주체)정부의 관리 하에 있는 과학기술분야 정부출연 연구기관이 개발

STEP2. 표준DNA DB구축・운영	2. 불법촬영물 DNA 추출 및 DNA DB구축	• (내용)정부가 개발한 DNA 추출기술을 이용하여 불법촬영물 원본영상에서 DNA를 추출하여 DB를 구축 및 업데이트를 실시하는 업무가 포함됨 • (주체)불법촬영물의 불법유출 방지를 위해 불법촬영물의 관리책임이 있는 방송통신심의위원회가 운용
	3. 표준DNA DB 및 공개 API제공 운영	• (내용)조치의무사업자에게 표준DNA DB와 공개API를 배포 • (주체) 표준DNA DB의 관리권한이 있는 방송통신심의위원회가 DNA DB와 공개API를 배포할 수 있는 시스템을 운영
STEP3. 필터링 성능평가	4. 성능평가 표준 개발	• (업무)필터링의 성능을 객관적으로 평가할 수 있는 표준(평가항목, 기준 등) 개발 • (주체) 정부가 개발한 기술수준에 맞는 성능평가 표준이 개발되어야 하므로 기술개발기관이 성능평가의 기준을 제정
	5. 시험용데이터셋 개발/업데이트	• (업무) 필터링의 성능평가 실시를 위한 시험용 데이터셋 (불법촬영물 원본 및 변형본 등)개발 • (주체) 표준DNA DB구축과정에서 정부가 개발한 추출기술을 사용해서 시험용데이터셋을 개발
	6. 성능평가 실시	• (업무) 성능평가의 시스템을 구축하여 자체기술을 사용하는 조치의무사업자를 대상으로 필터링 기술의 성능평가를 실시하고 인증서 발급 • (주체) 성능평가운용의 기술적 능력이 있고, 방송통신위원회의 관리가 가능한 평가기관을 선정하여 운용

○ (표준 필터링 기술 개발·배포) 임의의 콘텐츠로부터 고유한 특징값(DNA)을 추출하여 표준 DNA DB와 비교·분석을 통해 불법촬영물 등의 유통을 차단할 수 있는 기술로써, 추출기술, 식별기술, 공개 API 등을 포함함

- 추출기술이란 추출모듈을 통해 임의의 콘텐츠로부터 특징점을 추출하여 식별가능한 DNA 파일을 구성하는 기술임
- 식별기술이란, 추출된 DNA 파일과 불법촬영물의 DNA 파일을 비교하여 임의콘텐츠의 불법 여부를 식별하는 기술임
- 공개API(Application Programming Interface)란, 필터링사업자나 조치의무사업자가 개발한 필터링 제품이 방송통신심의위원회가 구축한 '표준DNA DB'와 연동하여 사용할 수 있도록 미리 개발된 인터페이스를 의미함

- 시행령 제30조의6은 자체기술을 사용하지 않는 조치의무사업자에게 국가기관이 표준 필터링 기술을 개발하여 제공하도록 하고 있어, 정부의 관리 하에 있는 과학기술분야 정부출연 연구기관(예: ETRI)이 표준필터링 기술의 개발을 수행하는 것이 적절함

- 또한, DNA추출기술 개발 과정에서 일반 성인영상물(예: 프로덕션이 제작한 영상물)을 토대로 불법촬영물의 원본영상이 없어 추출기술을 개발할 경우 불법촬영물의 효과적인 식별이 어려울 수 있기 때문에, 추출기술 개발과정에서 방심위의 협조 하에 불법촬영물의 원본영상을 대상으로 한 표준 필터링 기술 개발이 필요함

- 표준필터링 기술의 배포는 표준DNA DB와 연동되어 배포되어야 하며, 이에 따라 방송통신심의위원회의 '공공 DNA DB 등 통합 관리·공조 시스템'에 R&D기관이 개발 완료하여 제공한 "표준 DNA 추출 시스템"을 탑재하여 배포하는 것이 바람직함

○ (표준DNA DB 구축· 배포) 국가기관이 개발한 표준 필터링 기술을 사용하여 불법촬영물 영상으로부터 DNA를 추출하고, 추출한 DNA를 데이터베이스로 구축하여 조치의무사업자에게 배포하는 것을 포함함

- 방송통신심의위원회는 정보통신망에서 유통되는 불법·유해 정보에 대한 내용심의 기관으로써, 위원회가 심의·의결한 불법촬영물에 대해 암호화·수치화된 형태의 DNA를 추출하여 데이터베이스를 구축함

- 또한 표준 DNA DB 등 배포용 홈페이지(웹페이지, API 연동 프로그램 등)를 도입하여, 표준 DNA DB 및 표준 DNA 검출 시스템, 사업자 자체 DNA DB 등을 정보통신서비스 제공자의 요청에 따라 배포함

- 불법촬영물의 효과적인 유통 방지를 위해서 지속적인 업데이트와 관리가 필요함

○ (조치의무사업자 대상 필터링 성능평가) 자체기술을 사용하는 조치의무사업자를 대상으로 필터링 기술의 성능을 계량적으로 평가하는 것으로, 성능평가지표와 성능평가기준의 개발, 성능평가를 위한 시험도구(데이터셋 및 시험환경)의 개발 등이 필요함

- (성능평가범위) 영상식별기술을 평가하고 인증할 수 있는 체계 구축을 위해서 ① 성능평가 기준, ② 성능평가 도구(시스템) 개발, ③ 평가 데이터 셋 구축이 필요함

- (평가항목) 기 개발되어 있는 TTA의 단체표준† 인 '비디오 콘텐츠 필터링 성능평가

표준(TTAK.KO-12.016/R1)'을 일부 준용하여, 강인성 등 총 8개 항목으로 운용이 가능함

† TTA의 성능평가 표준은 영상콘텐츠의 특징정보를 추출 및 인식하고 특징정보 DB와 매칭하여 콘텐츠의 불법성을 식별하는 필터링 절차를 평가하고 있어, 불법영상물의 식별에도 적용이 가능함

- (평가기준) 객관적인 성능평가를 위해서 기술요구사항, 평가항목, 파라미터, 항목속성, 측정단위, 가중치 등 성능평가의 결과를 계량화하고 최소 요구수준의 기준 마련 필요

  ▸ 불법촬영물은 방송용 콘텐츠나 영화와 다른 영상 특징을 보유하고 있어, 이를 고려한 강인성 등 평가기준에 대한 세부방안 마련이 필요함

  ▸ 성범죄 피해동영상 등 불법영상물은 상대적으로 해상도와 조도가 낮은 저화질 화면의 롱테이크 영상으로 촬영되며, 인물이나 신체 일부에 초점을 두어 영상이 제작되는 특징이 있음

  ▸ 또한 불법저작물은 원본 영상의 변형이 높을 경우 확산이 일어나지 않을 가능성이 높은 반면, 불법촬영물은 특정 부분만 발췌편집하거나 화면에 광고자막을 삽입하거나 자르기, 붙이기 등 변형의 정도가 높아도 복제와 확산이 지속되는 특성이 있음

  ▸ 이와 같이 동영상 배경 이미지가 일정한 특징으로 인해 적은 수의 대표프레임 만으로도 동영상 요약이 가능한 반면, 압축, 자르기, 붙이기 등의 변형의 정도가 높아, 강인성과 추출 및 검색·비교 속도 등에 있어 기존의 불법저작물에 적용하던 기준보다는 다소 완화된 기준을 적용한 후 기술의 발전 속도에 따라 기준을 단계적으로 높이는 방향이 필요할 것으로 예상됨

  ▸ 이에 따라 TTA의 성능평가 표준을 준용하되, 콘텐츠의 변형정도에 대한 인식률과 처리 속도 등 불법촬영물의 특성에 부합하는 별도의 최소요구기준 수립이 필요함

<표 2-16> 불법촬영물과 불법저작물 왜곡(변형)의 차이 >

구 분	불법촬영물	불법저작물
촬영 방식	해상도와 조도가 낮고 흔들림이 많은 저화질 화면 원격고정카메라(스마트폰 등) 의 촬영장소가 변화없고 촬영구도가 제한적임 복잡한 편집기능이 사용되지 않은 롱테이크 영상(30초이상) 상대적으로 짧은 영상	해상도와 조도가 높고 고화질의 안정적인 화면 다수의 카메라로 시점변환이 자유롭고, 촬영구도가 다양함 편집점이 많은 숏테이크영상 (2~20초) 상대적으로 긴 영상
촬영 대상	인물 및 신체 위주	인물, 소품, 건물, 배경 등 다양함
주요 변형방법	자막추가(불법도박사이트 광고 등), 압축, 자르기, 붙이기 등	회전, 좌우반전, 인코딩 등 ※ 영상물이 구분 가능하도록

	변형의 정도가 높음 ※ 홍보 또는 주요장면 추출 변형	변형의 정도가 낮음

자료: 낭종호(2020), KAIT(2020). 재구성.

- (평가도구) 차단기술의 사양, 정확성, 강인성, 속도 등 기술요구사항과 기준을 정하고 기준 충족여부(성능)를 평가하는 시스템(HW/SW) 구축이 필요함
- (데이터셋) 비디오콘텐츠필터링 성능평가를 위해 테스트 데이터(원본 및 변환)의 구축과 테스트 원본의 권장규격, 변환의 유형과 강도 등에 대한 기준 수립 필요함

○ (신청대상) 성능평가는 자체적인 필터링기술을 사용하는 조치의무사업자를 대상으로 함

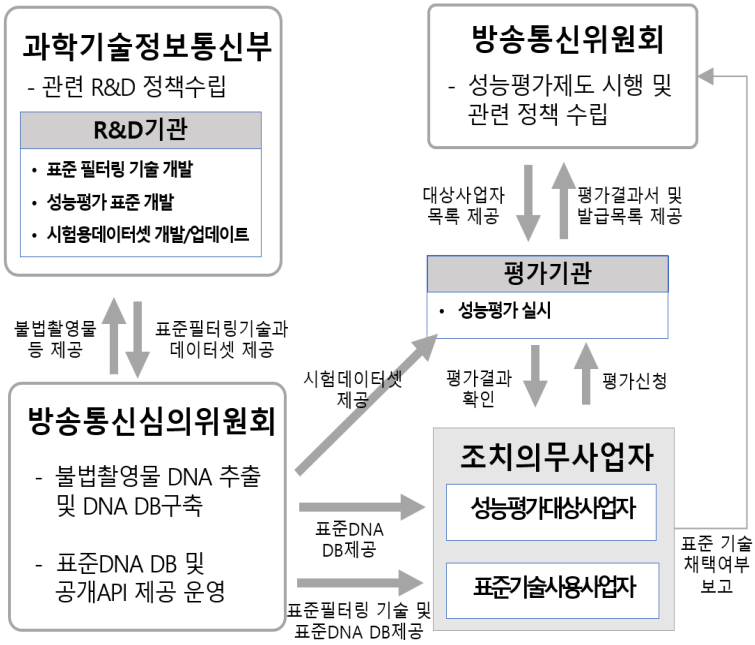
- 모든 조치의무사업자가 성능평가를 통과할 기술을 적용해야하나, 정부가 불법영상물의 특징정보 DNA DB와 필터링 기술을 개발할 뿐만 아니라 정부가 시험 데이터셋과 성능평가기준을 수립하기 때문에 정부가 개발한 표준DNA DB와 API를 사용하는 사업자에 한하여 성능평가 통과의무를 면하는 것이 바람직함

○ (지정・통보) 방송통신위원회가 조치의무대상사업자를 지정하고, 지정된 조치의무대상사업자는 자체필터링 기술을 사용할 것인지의 여부를 방송통신위원회에 고지한 후, 평가기관에 성능평가를 신청하여야 함

- 1단계: 방송통신위원회는 불법촬영물등의 유통가능성, 서비스 목적·유형 등을 고려하여 매년 5월말까지 지정하여 조치의무사업자에게 통보함
- 2단계: 조치의무사업자는 자체필터링 기술을 도입할 것인지 또는 표준 필터링 기술을 도입할 것인지를 결정하여 방송통신위원회에 고지하고 평가기관에 성능평가를 신청해야함
- 3단계: 평가기관은 성능평가를 실시하여 시험결과서를 성능평가대상자에게 제공하고, 시험결과서 및 평가결과보고서를 방송통신위원회에 제출해야함
- 이 때 자체 필터링 기술을 도입한 조치의무사업자가 많을 경우, 평가관리기관이 평가일정 관리 등을 위해 성능평가대상자에게 성능평가 실시와 관련한 제반사항을 통보 및 독촉을 할 수 있도록 해야 함

○ (성능평가체계) 성능평가 제도 시행 시 혼돈을 최소화하기 위해 성능평가절차에 따라, 대상 사업자를 포함하여 관련 기관(방송통신위원회, 방송통신심의위원회, 과학기술정보통신부, R&D기관, 평가기관)들 간의 관계를 명확히 정의하는 역할정립이 필요함

[그림 2-16] 성능평가 추진체계



제3장 불법정보 유통방지를 위한 제도개선 이슈와 대응

제1절 이용자 보호 제도 현황 및 분석

1. 개인정보보호 관련 법제 현황

1-1. 검토 배경

○ HTTPS 차단 방식은 인터넷 사용자의 개인정보나 통신비밀을 침해할 가능성이 높지 않다는 것이 전문가들의 견해(이찬구 외, 2019)이나, HTTPS 차단방식 도입으로 인해 개인의 프라이버시 염려(privacy concern)가 환기되었음

- HTTPS 접속차단과 관련한 국민여론 분석결과에 따르면, ISP의 상시적 트래픽 관리 과정에서 ISP가 개별 인터넷이용자의 인터넷접속기록(IP주소)을 실시간으로 수집·저장하거나 저장한 정보를 개인정보와 결합하여 다른 목적으로 사용할 수도 있을 것이라는 우려가 제기됨

○ 인터넷이용자의 IP주소[5]가 그 자체로써 개인정보를 식별할 수 있는 정보라기보다는 다른 개인식별정보와 결합되어 동의없이 임의로 외부에 공개되거나 제3자에게 전달될 때에 개인정보의 침해 우려가 발생함

- IP주소는 특정한 시점에 ISP가 인터넷 접속기기에 부여하는 자동생성정보로, 그 자체로써 이용자 개인을 식별할 수 있는 정보로 보기는 어렵고, 일반적으로 서비스 이용 시간대나 해당 IP 주소를 할당받은 기기에 접근할 수 있는 자, 유동 및 고정 여부 등에 대한 다른 요소들을 고려하여 다른 정보와 결합될 때에 개인을 특정할 수 있는 식별가능성이 발생함(임규철, 2018)

---

5) IP주소(Internet Protocol address)는 인터넷 네트워크에서 ISP가 송신원과 송신선을 식별하기 위해 배정하는 주소로, 유동IP는 특정 이용고객에 대해 IP주소가 고정적으로 배정되는 것이 아니라 이용고객이 네트워크에 접속할 때마다 새롭게 할당되는 형태임

- 이로 인해 개인식별정보로 명백히 분류되는 정보들(예: 주민등록번호, 개인 위치정보 등)과 달리 이용자의 동의 수집 대상이 아님
- 따라서 ISP가 인터넷 접속기록을 수집하거나 저장함으로써 발생하는 프라이버시 침해를 방지하기 위해서는 IP주소 기록 자체에 대한 관리보다는 IP주소가 이용자의 동의없이 다른 식별가능한 개인정보와 결합되지 않도록 하는 규정과 결합된 정보를 제3자에게 위법하게 제공하지 않도록 하는 규정이 필요함

※ 예: IP 주소가 확인되고 이용자의 ID가 이용된 서비스를 확인할 수 있다는 전제 하에, 서비스 제공자가 수집 및 저장한 ID 정보와 ISP가 확인한 IP를 결합할 경우 개인을 식별할 수 있음. ISP는 회선가입자 정보를 회원가입 등을 통해 동의에 의해 수집하고 사전에 알고 있기 때문에 IP주소와 접속시간을 조합하면 접속한 단말을 통해 개인을 식별할 수 있음

○ (근거법률) ISP의 IP주소의 수집· 제공에 관한 사항은 통신비밀보호법에 의해서 제한되며, 인터넷이용자를 식별할 수 있는 개인정보의 수집과 활용은 개인정보보호법*에 의해서 제한됨

※ 정보통신망법 상 개인정보 보호와 관련된 규정들(제4장 및 제재규정 등)이 특례 또는 기존 「개인정보 보호법」 규정에의 반영을 통해 개정 「개인정보 보호법」으로 이관되어, 2020년 2월4일에 공포됨

- 이에 본 장에서는 통신비밀보호법과 개인정보보호법을 분석하여 인터넷이용자의 접속기록 수집· 저장행위의 방지 및 수집된 정보의 무단 사용에 대한 제한과 제재에 관한 규제 현황을 파악함

1-2. 통신비밀보호법상의 관련규정 현황

○ ISP가 수집하는 IP주소 정보는 국내법에서는 통신비밀보호법 제2조의 11의'통신사실확인자료'사목에 명시되어 있으며, 이에 따라 통신비밀보호법에 의해 통신 및 대화 비밀의 보호(제3조)에 따라 보호됨

- IP정보는 통신사실확인자료 중"컴퓨터 통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료"에 해당함

통신비밀보호법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
사. 컴퓨터 통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

- 이 통신사실확인자료에는 정보통신망에 접속된 이용자의 접속지 자료만 포함될 뿐 이용자가 접속하고자하는 통신의 착신지 자료는 포함되어 있지 않음
- 따라서 현행 법체계 상 통신사실확인자료 제도는 접속차단 조치와 관련하여 개인이 특정사이트에 접속을 시도하였는지의 여부를 수집하거나 저장하여 제공하는 것과는 무관함
- 또한 통신비밀법 제3조(통신 및 대화비밀의 보호)에 따라 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 통신사실확인자료를 제공하지 못하고, 이를 위반할 경우 제16조에 따라 1년 이상 10년 이하의 징역과 5년 이하의 자격정지에 처함

통신비밀보호법 제3조(통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다.
1.~2. (생략)
3. 구속 또는 복역중인 사람에 대한 통신 : 형사소송법 제91조, 군사법원법 제131조, 「형의 집행 및 수용자의 처우에 관한 법률」 제41조·제43조·제44조 및 「군에서의 형의 집행 및 군수용자의 처우에 관한 법률」 제42조·제44조 및 제45조에 따른 구속 또는 복역중인 사람에 대한 통신의 관리
4. 파산선고를 받은 자에 대한 통신 : 「채무자 회생 및 파산에 관한 법률」 제484조의 규정에 의하여 파산선고를 받은 자에게 보내온 통신을 파산관재인이 수령하는 경우
(이하 생략)
제16조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 1년 이상 10년 이하의 징역과 5년 이하의 자격정지에 처한다.
1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자
2. 제1호에 따라 알게 된 통신 또는 대화의 내용을 공개하거나 누설한 자

○ 통신비밀보호법 제13조는 통신사실확인자료를 요청하여 제공받을 수 있는 기관과 절차에 대해 법원의 통제에 따라 운영되도록 규정하고 있음

- 또한 개인의 통신사실 확인자료의 협조요청기관으로는 검사, 사업경찰관, 법원, 정보수사기관의 장과 같이 형사소송법에 근거한 법률적 권한을 가진 자에 한하고 있으며, 이에 따라 법원의 통제에 따라 운영되고 있으며 불법정보의 차단을 위한 시정명령을 내린 방송통신위원회나 방송통신심의위원회가 통신사실 확인자료를 제공받지 않음
- 절차적으로도 통신사실확인자료 제공을 요청하기 위해서는 i)검사 또는 사법경찰관이 수사 또는 형의 집행을 위항 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원의 허가를 받거나, ii) 법원이 재판상 필요한 경우로서 민사소송법 제294조 또는 형사소송법 제272조의 규정에 의하여 전기통신사업자에게 통신사실확인자료를 요청하거나, iii) 정보수사기관의 장이 국가안전보장에 대한 위해를 방지하기 위해 정보수집이 필요한 경우로서 전기통신사업자에게 통신사실확인자료 제공을 요청하는 경우에 한정되어 있음

통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차) ①검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다.

② 검사 또는 사법경찰관은 제1항에도 불구하고 수사를 위하여 통신사실확인자료 중 다음 각 호의 어느 하나에 해당하는 자료가 필요한 경우에는 다른 방법으로는 범죄의 실행을 저지하기 어렵거나 범인의 발견・확보 또는 증거의 수집・보전이 어려운 경우에만 전기통신사업자에게 해당 자료의 열람이나 제출을 요청할 수 있다. 다만, 제5조제1항 각 호의 어느 하나에 해당하는 범죄 또는 전기통신을 수단으로 하는 범죄에 대한 통신사실확인자료가 필요한 경우에는 제1항에 따라 열람이나 제출을 요청할 수 있다.

1. 제2조제11호바목・사목 중 실시간 추적자료
2. 특정한 기지국에 대한 통신사실확인자료

③제1항 및 제2항에 따라 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.

④제3항 단서에 따라 긴급한 사유로 통신사실확인자료를 제공받았으나 지방법원 또는 지원의 허가를 받지 못한 경우에는 지체 없이 제공받은 통신사실확인자료를 폐기하여야 한다.

⑤검사 또는 사법경찰관은 제3항에 따라 통신사실 확인자료제공을 받은 때에는 해당 통신사실 확인자료제공요청사실 등 필요한 사항을 기재한 대장과 통신사실

확인자료제공요청서 등 관련자료를 소속기관에 비치하여야 한다.
⑥지방법원 또는 지원은 제3항에 따라 통신사실 확인자료제공 요청허가청구를 받은 현황, 이를 허가한 현황 및 관련된 자료를 보존하여야 한다.
⑦전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연 2회 과학기술정보통신부장관에게 보고하고, 해당 통신사실 확인자료 제공사실등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서등 관련자료를 통신사실확인자료를 제공한 날부터 7년간 비치하여야 한다.
⑧과학기술정보통신부장관은 전기통신사업자가 제7항에 따라 보고한 내용의 사실여부 및 비치하여야 하는 대장등 관련자료의 관리실태를 점검할 수 있다.
⑨이 조에서 규정된 사항 외에 범죄수사를 위한 통신사실 확인자료제공과 관련된 사항에 관하여는 제6조(제7항 및 제8항은 제외한다)를 준용한다.
제13조의2(법원에의 통신사실확인자료제공) 법원은 재판상 필요한 경우에는 민사소송법 제294조 또는 형사소송법 제272조의 규정에 의하여 전기통신사업자에게 통신사실확인자료제공을 요청할 수 있다.

1-3. 개인정보보호법상의 관련규정 현황

○ (수집과 이용) 일반적으로 인터넷이용자의 개인정보보호는 개인정보보호법에 의해서 보호되고 있으며, 정보주체의 자기결정권 보호를 위해 정보주체의 동의없이 수집되거나 이용되는 것을 제한하고 있음

- 제15조는 개인정보의 수집과 이용의 범위에 대해 정보주체의 사전 동의를 받도록 규정하여 정보주체의 자기결정권을 보호하고 있음

개인정보보호법 제15조(개인정보의 수집ㆍ이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을

정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

- 정보주체의 사전동의를 받지 않고 개인정보를 수집할 수 있는 경우는 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우와 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우로 한정되어 있음
- 이에 따라, ISP는 가입자 정보를 취득할 시에 가입자의 사전 동의를 받고 있으며, 가입자의 사전동의 없이 가입자 정보를 타인에게 누설 또는 배포할 수 없고 사전에 이용고객에게 고지 또는 이용약관에 명시하여 동의를 얻은 목적 이외의 목적으로 사용하지 않음을 기재하고 있음

○ (정보제공) 법 제17조는 개인정보를 제3자에게 제공할 수 있는 경우로 정보주체의 동의를 받거나, 법률에 특별한 규정이 있거나, 공공기관이 법령 등에서 정하는 소관업무의 수행이 불가피한 경우 등으로 한정하고 있음

- 정보주체의 동의를 받지 않고 제3자에게 개인정보를 제공하거나 제공받은 자는 법 제71조(벌칙)에 따라 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처함
- 다만 ISP의 이용약관에는 관계법령에 의한 수사상의 목적으로 관계기관으로부터 요구받은 경우 이외에도 방송통신심의위원회의 요청이 있는 경우에 이용자의 이용정보를 제공할 수 있다고 기재되어 있으나, 이는 망법 제44조의 6에 따른 인터넷명예훼손과 관련한 '이용자 정보 제공청구'제도에 의한 것으로 접속차단과는 무관함

※ 이용자정보 제공청구란 특정한 이용자에 의한 정보의 게재나 유통으로 명예훼손 등 권리를 침해당한 자가 민·형사상의 소(訴)를 제기하기 위하여 침해사실을 소명할 경우, 방송통신심의

위원회의 명예훼손 분쟁조정부가 해당 정보통신서비스 제공자에게 보유하고 있는 이용자에 관한 정보(성명, 주소, 그밖에 민형사상의 소제기를 위해 필요하다고 인정하는 해당 이용자의 연락처 등의 정보)를 제공하도록 청구하는 제도

개인정보보호법 제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호・제3호・제5호 및 제39조의3제2항제2호・제3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

2. 불법영상물 유통 방지 관련 이용약관 실태

2-1. 불법정보 접속 차단의 제도적 근거

○ (법적 근거) 인터넷접속사업자의 접속차단은 「망중립성 및 인터넷 트래픽 관리에 관한 가이드라인(2011)」에 근거하여 시행

- 방송통신위원회의 접속차단 명령은 정보통신망법 제44조의7에 의거하여 이뤄지나, 인터넷접속역무 사업자의 접속차단은 「망중립성 및 인터넷 트래픽 관리에 관한 가이드라인(2011)」에 근거한 합리적 트래픽 관리기준에 근거를 두고 시행하고 있음

※ 방통위 접속차단 요청의 이행은 “국가기관의 법령에 따른 요청이 있거나 타법의 집행을 위해 필요한 경우”에 해당됨

<표 2-17> 망중립성 및 인터넷 트래픽 관리에 관한 가이드라인(2011)

구분	내용
망중립성 가이드라인 (2011)	합리적인 트래픽 관리 6. 합리적인 트래픽 관리의 필요성이 인정되는 경우는 아래의 경우를 포함하며, 이에 한하지 않는다. 그 밖에 합리적인 트래픽 관리의 범위, 조건, 절차, 방법 및 트래픽 관리의 합리성 여부에 대한 판단 기준 등은 방송통신위원회가 별도로 정한다. 이 경우 해당 망의 유형(유무선 등)과 기술 특성에 따라 다르게 정할 수 있다. ① 망의 보안성 및 안정성 확보를 위해 필요한 경우 ② 일시적 과부하 등에 따른 망 혼잡으로부터 다수 이용자의 이익을 보호하기 위해 필요한 경우 ③ 국가기관의 법령에 따른 요청이 있거나 타 법의 집행을 위해 필요한 경우 등
사업자 이용약관	・약관내 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인', '통신망의 합리적 관리・이용과 트래픽 관리의 투명성에 관한 기준'에 따라 트래픽 관리를 시행할 수 있음을 기재하고 있음 ・구체적인 트래픽 관리 기준은 별표로 적용조건, 적용대상, 적용방식, 적용 후 영향, 적용기간 등을 포함함

○ (이용약관 상의 근거) 최종 인터넷 이용자에게 인터넷 접속서비스를 제공하는 초고속 인터넷(가입자망)사업자들은 트래픽이나 서비스의 전부, 또는 일부 제공을 중단할 수 있음을 명시하고 있음

- 불법정보의 접속차단 행위는 상시트래픽 관리 행위(망 위해 트래픽, 불법/유해콘텐츠, 이용자의 요청이 있는 경우)에 해당되어 통신사업자의 정상적・합리적인 트래픽 관리의 대상으로 약관에 규정
- 적용조건: 불법정보 뿐만 아니라 유해정보와 기타 비정상적 정보

① 음란물, 도박, 불법선거운동, 지적재산권 침해 등 정부나 유관기관 등이 불법 또는 유해한 것으로 지정한 경우

② 스팸메일, 감염의도 메일 등 통신망에 비 정상적인 정보를 전송하는 경우

- 적용대상: 불법/유해 웹사이트 또는 불법/유해 콘텐츠를 유발 시키는 트래픽이나 서비스, 단말기 등
- 적용방식: 당해 웹 사이트, 트래픽, 서비스, 단말기의 차단, 이용 제한 등

- 적용 후 영향: 당해 트래픽, 서비스의 전부 또는 일부 제공 중단, 음란/불법사이트 접속 불가
- 적용기간: 불법/유해 콘텐츠로의 지정 해제, 비 정상적인 정보 전송이 중단 될 때까지로 규정

2-2. 현행 약관 내용 분석결과와 개선방향

○ (약관상의 불명확성) 대부분의 사업자가 불법유해정보도 트래픽 관리의 대상임을 기재하고 있으나, 이용자의 접속요청을 정지할 수 있음에 대해서는 명확하게 기재하지 않음

- 불명확성의 큰 원인은 불법·유해 트래픽 관리의 적용조건을 기재함에 있어, 불법정보의 접속차단과 광고성 정보 전송제한을 혼용하고 있기 때문임
- 불법사이트의 접속차단은 웹서버로부터 반환되는 트래픽이 이용자에게 전달되지 않도록 처리를 거부하는 경우와 이용자가 접속하고자 하는 사이트의 서버정보가 불법사이트에 해당할 경우 접속을 초기화하여 정보의 처리를 정지하는 형태도 포함됨
- 반면, 광고성 정보 전송제한은 불법스패머 등으로부터 이용자에게 전달되는 정보전송 역무를 거부하는 형태
- 불법정보의 접속차단은 망법 제44조7에 근거하여 정보통신서비스 제공자가 정보의 처리를 거부·정지할 수 있도록 하고 있음
- 반면 광고성 정보 전송 제한은 망법 제50조의4에 근거하여 정보전송의 역무를 거부하도록 하고 있음

<표 3-1> 현행 정보통신망법 제44조의 7, 제50조의 4 약관내용

구분	내용
불법정보의 차단	망법 제44조의7(불법정보의 유통금지) (생략) ② 방송통신위원회는 제1항제1호부터 제6호까지, 제6호의2 및 제6호의3의 정보에 대하여는 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다.(생략) ③ 방송통신위원회는 제1항제7호부터 제9호까지의 정보가 다음 각 호의 모두에 해당하는 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다. 1. 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 「성폭력범죄의

	처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것 2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정 요구를 하였을 것 3. 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니하였을 것
광고성 정보 전송제한	망법 제50조의4(정보 전송 역무 제공 등의 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에 해당 역무의 제공을 거부하는 조치를 할 수 있다. 1. 광고성 정보의 전송 또는 수신으로 역무의 제공에 장애가 일어나거나 일어날 우려가 있는 경우 2. 이용자가 광고성 정보의 수신을 원하지 아니하는 경우

- 일부 사업자의 경우 불법·유해트래픽 관리의 적용조건을 불법광고성 정보와 같이 웹서버로부터 최종이용자에게로 가는 패킷전달을 차단하는 행위로만 기재하고 있음

※ HCN, KT등은 불법유해트래픽에 대한 접속제한 또는 차단에 대한 적용방식은 명기하고 있으나, 적용조건에 대한 내용은 “제공정보 및 광고행위”로 기재하고 있어 이용자의 불법정보 접속 시도를 정지하는 것도 포함하는 지가 명확하게 기재하지 않음

<표 3-2> HCN, KT 약관상 적용조건

사업자	약관상 적용조건(원문)
HCN, KT	・적용조건(원문): ① 제공정보 및 광고행위가 음란, 도박 등으로 관련 법령을 위반하여 사법기관, 한국정보보호진흥원, 방송통신심의위원회 등 정부/유관기관으로부터 요청이 있는 경우 ② 비정상적 광고성 정보 및 관련 법령을 위반한 스팸성 트래픽 ・적용대상: - 불법스팸성 정보제공자 - 불법, 음란, 유해정보 트래픽

- 이 외에도 이용자 약관상에 부정확한 정보들이 많아 이용자가 망법 제44조의7에 의거하여 불법사이트로의 접속이 제한될 수 있음을 인지하지 못할 우려가 있음

※ 현재 가입자들에게 제공되는 이용약관들은 부정확하거나 잘못된 내용(예: 방송통신심의위원회의 명칭이 정보윤리위원회로 되어 있거나, 약관 신고를 방송통신위원회에 한다는 등)이 많아, 이에 대한 수정도 필요함

○ (약관상 고지 미비) 일부 사업자는 이용약관에 트래픽이나 서비스의 전부, 또는 일부 제공을 중단할 수 있음을 명시하고 있지 않음

- LGU+의 경우 불법정보나 광고성 정보의 전송은 처리를 거부·정지하고 있음을 명기하지 않음
- 따라서 불법정보의 차단에 대해 이용자에게 고지하고 있지 않음

<표 3-3> LGU+ 약관내용

미비사업자	약관 내용
LGU+ (미비)	· 서비스의 일부사용 제한 및 중단 대상을 DDos/바이러스/해킹 등 침해사고로만 한정함 · 적용조건(원문): ① DDos/바이러스/해킹 등 외부에서 발생한 침해사고로 인하여 회사에 심각한 장애 발생 우려가 클 경우 ② 이용고객의 정보시스템에 발생한 이상 현상으로 인하여 다른 이용고객 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있거나, 장애발생에 대한 원인파악을 위해 차단을 필요로 하는 경우

○ (적용조건 등) 불법정보 접속차단을 위해 정보의 처리를 거부하거나 정지할 수 있음을 명확히 기재하도록 표준문안 마련 필요

- 약관 본문에 기재된 합리적 트래픽 관리 기준에 "관련법령에 의한 불법, 유해 트래픽(예, 음란· 폭력 정보, 청소년 유해정보, 도박 등 사행행위) 관리는 고지 또는 공지 없이 시행될 수 있습니다[6]."를 기재할 필요가 있음
- 현행 트래픽 관리 기준에 "상시트래픽 관리기준"의 하나로 불법·유해트래픽을 포함하도록 권고하여, 상시적으로 불법사이트로의 접속시도에 대해서 차단안내페이지로 리다이렉트하거나 접속을 중단(drop)할 수 있음을 기재할 필요가 있음
- 적용조건, 적용대상, 적용방식, 적용 후 영향, 적용기간을 다음과 같이 기재하여 불법·유해사이트의 접속이 불가함을 기재할 필요가 있음

6) KT 이용약관

<표 3-4> 표준문안 마련(안)에 포함 내용

적용 조건	・정부/유관기관 등이 그 처리를 거부・정지 또는 제한 요청한 음란물, 도박 등 불법・유해 정보 및 스팸 메일 등 ・비정상적인 정보 전달에 대한 트래픽
적용 대상	・불법・유해 정보・스팸성 트래픽이나 서비스, 단말기 등
적용 방식	・해당 트래픽에 대한 접속제한 또는 차단
적용 후 영향	・침해 트래픽 중단 및 음란・불법사이트 접속 불가
적용 기간	・트래픽 제한・차단의 원인 해소시점까지

- 또한 트래픽 관리 시행 이전 '사전 고지 혹은 공지'가 원칙이나, 불법정보의 확산 방지를 위해 긴급성이 요구될 경우에는 사전 고지 혹은 공지가 적합하지 않을 수 있음
- 따라서, 이용자 고지와 관련하여 불법정보 확산을 방지하기 위해 긴급성이 요할 경우, 트래픽 관리 조치 시행 시 고지 방식에 부득이한 경우에는 고지 또는 공지 없이 시행 될 수 있음을 다음과 같이 기재하는 것을 권고함

※ 관련 법령에 의한 불법・유해 트래픽(예, 음란・청소년 유해정보, 도박 등 사행행위)관리는 고지 또는 공지 없이 시행 될 수 있음

3. 접속차단조치 도입절차 개선을 위한 지침 개선 방안

3-1. 배경

○ (개정의 필요성)접속차단 과정에서 차단대상이 되는 정보를 식별하는 방식이 변경되고, 관련 법률 개정 및 정부조직개편 등으로 인해 기존 "해외 불법정보 차단업무 처리지침"의 일부 규정들이 HTTPS 차단조치에 적합하지 않아, 일부 개정이 필요함

- 방송통신위원회는 '19년 2월에 HTTPS차단조치를 시행하면서 2008년에 마련한 "해외 불법정보 차단업무 처리지침"에 따라 상위계위 인터넷서비스제공사업자(ISP)와 IX, 망중계사를 대상으로 접속차단 요청했음
- 새로 도입된 HTTPS 차단은 기술적인 이유로 기존 HTTP차단과 달리 접속차단의 사유를 안내하는 페이지(warning.or.kr)로 리다이렉트(re-direct)되지 않아 불법사이트를 접속하고자 하는 이용자들에게 혼란이 있었음

- 또한 접속차단이 도입된 당일에 KT가 기존의 URL 방식 차단 요청 목록까지 HTTPS 차단목록 DB와 통합하면서 KT이용자에 한해서만 URL차단 목록의 도메인까지 차단하는 과잉차단이 발생했음
- 이에 대해 감사원은 새로운 불법 사이트 접속차단방식을 도입할 경우 인터넷접속사업자에게 차단장비의 설치를 요구할 근거, 차단장비 및 설치방법 등을 정한 업무지침이나 고시 등을 마련하여, 향후의 혼란을 방지할 필요성이 있음을 지적함
- 이에 따라 본 보고서에서는 기존 2008년도에 마련한"해외 불법정보 차단업무 처리지침"의 내용을 분석하고 HTTPS 차단조치의 포섭을 위한 개정안을 제시함

3-2. 현행 해외불법정보 차단을 위한 업무처리지침

○ (차단업무처리지침) 구(舊)정보통신부는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의 7, 제55조 및 동법 시행령 제22조의 12에 따라 해외불법정보를 차단하기 위한 업무처리지침을 마련한 바 있음

※ 2008년 정보통신부는 감사원의 지적에 따라 URL 차단방식 도입과 관련하여 인터넷접속사업자에게 URL 차단장비의 설치를 요구할 근거, 차단장비 및 설치방법 등을 정한 "해외 불법정보 차단업무 처리지침"을 마련·운용한 바 있음

- 해외불법사이트의 URL차단을 위해 '해외불법정보 차단업무 처리지침(이하 URL차단지침)'을 도입하고, 관문국에서 국내로 유입되는 해외불법정보의 차단을 위한 대상정보의 범위와 차단절차, 차단주체 및 차단장비 등 에 대한 처리기준을 설정한 바 있음
- '해외불법정보 차단업무 처리지침'은 취급거부명령 등 대상 인터넷접속사업자 및 차단대상정보 범위의 지정 등을 비롯하여 총 3장 13개 조항으로 구성되어 있음

<표 3-5> 해외불법정보 차단업무 처리지침의 구조

구분	내용
제1장 총칙	제1조(목적) 제2조(적용범위)
제2장 해외불법정보의 차단	제3조(취급거부명령 등 대상 인터넷 접속사업자 및 차단대상정보 범위의 지정) 제4조(인터넷접속사업자에 대한 해외 불법정보 URL 및 IP주소의 제공 등)

	제5조(인터넷접속사업자의 차단) 제6조(URL 차단장비 설치에 의한 차단) 제7조(URL 차단장비의 설치) 제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계) 제9조(차단사실의 안내 등) 제10조(차단의 실사 등) 제11조(해외 불법정보 차단책임자의 지정)
제3장 보칙	제12조(자료제출요구) 제13조(해외 불법정보 차단 지원)

○ (구성항목) 대상사업자(인터넷접속사업자)의 네트워크에 차단장비의 설치와 접속차단 이행에 대한 실사 등이 포함되어야 함으로, 차단업무 처리지침은 (1) 처리의 범위, (2) 차단의 체계, (3) 차단장비 및 장비의 설치· 운용에 대한 규정, (4) 접속차단이행에 대한 관리 등이 포함되었음

- 기존 '해외 불법정보 차단업무 처리지침'은 구(舊)정보통신윤리위원회(現 방송통신심의위원회)의 시정요구에 따라 구(舊)정보통신부(現 방송통신위원회)의 취급거부 등의 행정집행을 위한 범위와 절차를 명시

※ 2008년 2월 「방송통신위원회의 설치 및 운영에 관한 법률」에 따라 정보통신부는 방송통신위원회로, 정보통신윤리위원회는 방송통신심의위원회로 직무가 이관

<표 3-6> 주요항목별 해외불법정보 차단업무 처리지침 조항

구분	해당조항
(1) 처리의 범위	제2조(적용범위) 제3조(취급거부명령 등 대상 인터넷 접속사업자 및 차단대상정보 범위의 지정)
(2) 차단의 체계	제4조(인터넷접속사업자에 대한 해외 불법정보 URL 및 IP주소의 제공 등) 제5조(인터넷접속사업자의 차단)
(3) 차단장비 및 장비설치· 운용	제6조(URL 차단장비 설치에 의한 차단) 제7조(URL 차단장비의 설치) 제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계)
(4) 접속차단 이행에 대한 관리	제9조(차단사실의 안내 등) 제10조(차단의 실사 등) 제11조(해외 불법정보 차단책임자의 지정)

가. 처리의 범위

○ (차단대상정보) 해외에 서버를 두고 국내 이용자를 대상으로 제공하는 불법사이트를 제한하기 위한 목적으로 차단 대상이 되는 정보의 범위를 "해외에서 국내로 유입되는 한글로 제공되는 음란, 도박 등 불법정보"로 한정하여 기술하였음

- URL 차단지침 제3조2항에서는 "차단하여야할 해외불법정보의 범위를 정하고자 할 때에는 현재의 차단기술, 장비 또는 방법 등에 관하여 윤리위원회(現 방송통신심의위원회), 인터넷접속사업자 등으로부터 의견을 들을 수 있도록 정함

- 즉 지침 상에서는 한글로 제공되어 명백히 국내 인터넷이용자를 대상으로 하는 불법정보와 사이트만을 한정하여 정의하였으나, 실무적으로는 방송통신심의위원회가 심의하여 불법으로 판단한 차단대상 정보를 차단하고 있음

○ (대상사업자) URL 차단지침은 해외에서 국내로 유입되는 해외 불법정보에 대한 내국인의 접속차단을 방지하기 위해, 해외 관문국을 보유한 국내 인터넷접속사업자에게 처리업무 지침을 적용함

- 정보통신망을 통해 국내로 유입되는 트래픽이 모두 통신관문국을 거치기 때문에 불법유해정보의 기술적 차단 및 우회접속 대응과 관련해서는 전기통신사업자로서 정보통신서비스 제공자 가운데에서 주로 인터넷접속서비스와 관련해서 논의되어야 할 것이므로 설비를 보유하고 해외접속역무를 담당하는 기간통신사업자에 한정해왔음

- 이에 따라 지침 제2조(적용범위)는 차단업무를 수행해야 할 사업자를 해외인터넷 접속역무를 허가 받거나 등록하여 제공하는 정보통신서비스 제공자(인터넷접속사업자)로 정의하고 있음

  ※ 해외인터넷접속역무를 허가받거나 등록하여 제공하는 인터넷접속사업자는 국제회선 육양 및 비육양 해저 광케이블[7]의 설비를 보유한 기간통신사업자(KT, SK브로드밴드, LG유플러스, 드림라인)들로, 이들은 처리지침에 따라 해외관문국에 차단장치를 설치하여 해외 불법사이트 트래픽을 차단하고 있음

- 그러나 지침 제3조 1항은 "정보통신부장관(現 방송통신위원회)와 윤리위원회(現 방송통신심의위원회)는... 취급거부명령 등의 대상이 되는 인터넷 접속사업자를 적정하게

7) 해저광케이블의 전송망 회선설비에 관한 사항은 한국인터넷진흥원(KISA)가 보유함.

지정하여야 한다"로 규정되어 있어, 차단시점의 현재의 차단기술, 장비 또는 방법 등을 고려하여 취급거부명령 시에 지정할 수 있는 근거가 있음

- 다만 해외관문국을 보유하지 않은 사업자에게 취급거부명령을 하고자 할 때에는, 당해 사업자가 지침 제2조(적용범위)에서 해외인터넷접속역무를 허가받거나 등록하여 제공하는 정보통신서비스 제공자에 해당하지 않기 때문에 URL 차단지침의 범위를 벗어난다는 해석도 가능함

나. 차단의 체계

○ (취급거부명령) 해외불법정보의 차단을 위한 취급거부명령을 하고자 할 때에는 방송통신위원회나 방송통신심의위원회가 인터넷접속사업자에게 차단하여야할 해외 불법정보 URL과 해당 시점에서 알려진 IP주소를 제공하도록 함(제4조1항)

○ (취급거부명령의 철회 등) URL 차단지침은 불법정보를 제공하는 사이트나 페이지의 URL과 IP주소가 변경되거나 불법정보 차단 사유가 소멸될 경우에는 인터넷접속사업자의 신청을 받아 취급거부명령을 철회할 수 있도록 규정하고 있음

- 불법정보를 제공하는 사이트의 변경이나 폐쇄 등으로 인해 불법정보 차단 사유가 소멸된 경우에는 해당 URL에 대한 취급거부명령이 철회되어야 하나, 철회의 절차는 직권 또는 취급거부명령 등을 받은 인터넷접속사업자의 신청을 받아 방송통신위원회나 방송통신심의 위원회가 해당 해외불법정보의 차단을 위한 취급거부명령 등을 철회하도록 하고 있음(제4조2항)
- 불법정보의 IP주소가 변경된 경우에도 직권 또는 취급거부명령 등을 받은 인터넷접속사업자가 신청하여 방송통신위원회나 방송통신심의위원회가 변경된 IP주소를 제공해야함(제4조3항)
- 또한 취급거부명령 등을 받은 인터넷접속사업자는 방송통신위원회나 방송통신심의위원회에서 제공받은 IP주소가 변경된 것을 인지하였을 경우 이에 대해 통보할 의무가 있음(제4조4항)
- 이와 같이 현행 URL 차단지침은 주소변경 등으로 불법 사유가 해소된 IP나 URL의

정정이나 취급거부 철회를 인터넷접속사업자의 신청으로부터 시작되도록 하고 있기 때문에, 인터넷접속사업자가 단순히 차단사이트와 IP주소의 DB를 업데이트 하는 것을 넘어서 불법사유의 해소 여부 등에 대해 적극적인 행위를 전제하고 있는 상황임

- 그러나 실무적으로는 인터넷접속사업자는 차단장비를 설치하고 해당 URL과 IP주소가 차단되었는지 여부만을 확인할 수 있으며 해당 URL과 IP주소에서 제공되는 내용을 심의할 권한이 없기 때문에 사실상 취급거부명령의 철회를 신청하기가 쉽지 않은 상황임

○ (취급거부이행) 접속차단을 위한 취급거부 명령 등을 받은 인터넷 접속사업자들은 일괄적으로 신속하게 차단하도록 하고 있음(제5조)

- 접속차단을 명령을 받은 이후 5일 이내에, 모든 사업자가 동시에 일괄적으로 실시하도록 하고 있음
- 이는 불법정보 접속을 위해 이용자가 다른 인터넷접속사업자로의 이동 또는 이탈이 발생하지 않도록 하기 위함
- 차단의 철회는 해외불법정보의 차단 사유가 소멸된 경우에 정부·관계부처로부터 해당 해외 불법정보의 차단을 위한 취급거부명령 등을 철회하였음을 통보받은 후에 가능함

○ (하위계위 사업자) 타 인터넷접속사업자(하위계위사업자) 등은 URL차단장비 설치 사업자에게 해외 불법정보 차단을 위한 업무를 위임한 것으로 간주함(제8조)

- 따라서 하위계위 사업자들은 URL차단 장비 등을 설치하거나 해외 불법정보의 처리 거부를 위한 기술적 조치를 취할 필요성이 없음
- 단, URL차단 장비의 설치에 따라 발생하는 비용 중 타 인터넷 접속 사업자가 임차하여 사용하는 정보통신망에 해당하는 비용은 URL차단 장비 설치 사업자와 타 인터넷접속 사업자가 협의하여 분담하며 협의는 (사)한국인터넷기반진흥협회(現 한국인터넷진흥협회)가 위임받아 처리함(제8조3항 및 4항)
- 또한 민원 및 법적 분쟁에 대하여는 해당 민원 및 법적 분쟁을 제기한 자에게 인터넷 접속역무를 제공하는 인터넷접속사업자가 이를 책임지고 처리하도록 함(제8조5항)
- 또한 차단사실에 대한 안내를 이용자에게 제공할 의무도 부여됨(제9조)
- 즉, 하위계위사업자가 차단 업무를 위임하여 URL차단장비를 설치할 의무는 없으나

해외불법정보로의 접속차단을 위한 책임을 위임한 것으로 보기는 어려우며, 상위계층 사업자와 하위계위 사업자 모두 불법정보의 차단에 대한 책임이 있다고 해석됨

○ (차단의 실사) URL차단지침은 필요에 따라 정기 또는 수시로 차단여부에 대한 실사를 실시할 수 있도록 규정하고 있음

- 단, 긴급을 요하거나 증거인멸 등으로 실사의 목적을 달성할 수 없다고 인정하는 경우를 제외하고는, 실사를 하고자 하는 경우에는 실사 7일 전까지 통보해야함
- 실사계획을 통보할 경우 실사 사유, 일시, 대상, 방법 및 차단 이행기준 등을 실사를 받을 인터넷접속사업자에게 통지하도록 함
- 실사 후 실사결과 및 차단이행여부는 인터넷접속사업자에게 통보하고 인터넷접속사업자의 의견을 참조하여 법에 따른 조치가 가능함

○ (책임자 지정) 인터넷접속사업자는 해외불법정보의 차단을 효율적으로 수행하기 위해 관련 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 해외 불법정보 차단 책임자를 지정하여야 함(제11조)

- 차단책임자는 해외 불법정보의 차단을 수행하고 해외불법정보 차단계획, 인원 및 장비 등에 관한 자료를 매년 1월말까지 방송통신위원회에 제출해야함

○ (해외불법정보차단지원) 기존 지침은 해외불법정보의 효과적인 차단을 위하여 인터넷 접속사업자에 대하여 웹서버 운영, IP추출 프로그램의 개발· 보급 및 사후관리를 지원할 수 있도록 규정하고 있음(제13조)

다. 차단장비 및 장비설치·운용

○ (차단방식) 해외 관문국을 보유한 사업자에게 국제망 접속점의 최상위구간에 URL차단 방지를 설치하여 차단하도록 하고 있음(제6조와 제7조)

- URL차단 지침에는 방송통신위원회나 방송통신심의위원회가 해외 인터넷접속설비를 직접 설치한 사업자에 대하여 자신이 설치, 보유하는 해외 인터넷접속설비에 해외 불법정보의 차단을 위한 "URL차단 장비"를 설치하도록 명시되어 있음

  ※ 제6조는 방송통신위원회와 방송통신심의위원회가 ISP사업자에게 차단장비를 설치할 수 있도록 취급거부명령을 내릴 수 있는 근거를 명시하고, 제 7조는 ISP의 URL차단 장비 설치와 접속차단 업무의 범위를 명시함

- 비록 URL차단장비가 측정 차단장비나 차단의 기술을 의미하는 것은 아니고 차단장비에 차단대상인 URL 주소의 DB를 매칭하도록 하는 것을 지칭하지만, URL(예: http://www.naver.com)이 아닌 도메인(예: naver.com)의 DB를 매칭 할 경우 기존 URL차단 지침에서 벗어날 수 있는 것으로 해석될 여지도 있음

○ (차단의무의 범위) 국제망 접속점의 최상위구간에 URL차단장비를 설치한 사업자(이하, URL차단 장비 설치 사업자)는 우회접속방지를 위한 기술적 조치도 강구하도록 하고 있음(제7조)

- (차단주체) 실무적으로는 ISP가 보유한 국제망 접속점의 최상위 구간에 URL차단장비를 설치하는 사업자(차단장비 설치사업자)가 접속차단을 구현하나, ISP에게 최종적인 접속차단 책무가 부여되어 있기 때문에, 제7조는 해외관문국을 보유한 ISP를 URL차단장비 설치사업자로 명시

- (트래픽 관리) URL차단장비 설치사업자는 포워딩† 서버를 이용하거나 멀티도메인 웹호스팅‡으로 여러 도메인이 하나의 IP를 공유하는 경우 URL단위의 차단을 통하여 해외불법정보를 제공하지 않는 정상적인 사이트가 차단되지 않도록 노력하여야하며, 정상적인 사이트가 함께 차단된 경우에는 방통위·방송통신심의위원회의 직권 또는 URL차단장비 설치사업자의 신청에 의하여 해당 IP차단을 철회하도록 해야함

  † 포워딩(forwarding)서버: 고객의 웹사이트를 포워딩 업체가 등록한 간략하고 편리한 도메인 주소로 연결하는 서버

  ‡ 멀티도메인 웹호스팅: 웹호스팅 업체가 호스팅 서버에 한 개의 IP주소를 할당하고 복수의 URL을 연동하여 서비스 하는 방식

- (우회접속의 방지) 도메인 및 IP주소의 변경, DNS 우회, IP주소 직접 접속, 프록시(Proxy)서버, 아노마이져 등에 의한 우회 접속을 방지하기 위한 기술적 조치를 강구해야함
- (보고의 의무) URL차단장비설치사업자는 차단 조치 후 1개월 이내에 해외 불법정보의 차단을 증명하는 자료를 정부에 제출† 해야 하며, 우회접속 비율 및 정도 등 우회접속의 실태를 파악하고 정부가 이를 제출하도록 요청하는 경우 이에 응할 의무가 있음(제7조, 제12조)

† 단, 불법 해외정보 차단과 관련한 실사자료로 갈음할 수 있음

3-3. 도입절차 및 처리업무에 대한 법적 근거 마련

○ (개정필요성) 해외 불법정보 차단업무 처리지침 도입 이후, 근거법령 개정 및 정부조직 개편 등으로 인해 차단업무 처리 체계 등의 변경을 반영하고, 새롭게 도입된 HTTPS 차단방식에 부합하도록 일부 조문의 개정이 필요

- (근거조문수정) 기존 지침이 근거하고 있는 조항이 정보통신망법과 동법 시행령의 개정으로 인해 변경됨에 따라, 지침이 지시하는 근거조문 수정이 필요함(제2조)
- (기관명칭수정) 정부조직개편으로 인해 지침상의 정보통신부와 정보통신윤리위원회가 방송통신위원회와 방송통신심의위원회로 변경됨에 따라, 명칭 변경의 반영이 필요함(제2조~제4조, 제6조~8조, 제10조~제13조)
- (기술포섭) 2019년 2월부터 HTTPS 차단이 실시됨에 따라 접속차단 업무를 이행하는 인터넷접속역무사업자에게 공유하는 정보의 범위에 도메인을 포함하는 조문 변경(제4조)이 필요함
  - ▸ HTTPS 차단방식이 기존의 차단방식과 기술적으로 큰 변경이 있지 않고 기존의 HTTP차단과 HTTPS차단이 병행하여 운영되고 있어, HTTPS 차단을 위한 별도의 지침이 필요하기보다는 기존 지침의 내용일 일부 수정 및 업데이트하는 것이 바람직함
  - ▸ 새로 도입된 HTTPS 차단방식은 데이터를 읽는 영역이 서버네임(SNI)필드라는 점만 달라질 뿐 기존의 HTTP차단과 동일하게 불법사이트의 정보를 확인하여 차단하는 방식으로, 차단업무의 체계나 대상 등이 크게 변경되지 않음
  - ▸ 다만, 기존 지침은 불법정보를 식별하기 위한 정보로 URL과 IP만을 기재하고 있어, 도메인까지

차단대상정보로 포섭하는 방향으로 개정이 필요함

▸ 또한 차단장비의 명칭을 “URL차단장비”로 명기한 것을 “차단장비”로 변경이 필요함(제6조~제8조)

- (우회방지책무강화) 하위계위 인터넷접속사업자의 임대망 사용 및 트래픽 관리 과정에서 우회접속이 발생할 여지를 방지하기 위해, 하위계위 인터넷접속사업자의 우회접속 방지를 위한 책무를 명시하는 조항을 신설할 필요가 있음(제8조)

<표 3-7> 해외불법정보 차단업무 처리지침의 조항별 개정 필요성

구분	내용	개정필요성
제1장 총칙	제1조(목적)	· 근거 조문 업데이트
	제2조(적용범위)	· 기관 명칭 업데이트 · 차단대상의 범위확대
제2장 해외불법정보의 차단	제3조(취급거부명령 등 대상 인터넷 접속사업자 및 차단대상정보 범위의 지정)	· 기관 명칭 업데이트
	제4조(인터넷접속사업자에 대한 해외 불법정보 URL 및 IP주소의 제공 등)	· 기관 명칭 업데이트 · 정보범위 확대
	제5조(인터넷접속사업자의 차단)	-
	제6조(URL 차단장비 설치에 의한 차단)	· 기관 명칭 업데이트 · URL차단장비 명칭 변경
	제7조(URL 차단장비의 설치)	· 기관 명칭 업데이트 · URL차단장비 명칭 변경
	제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계)	· 기관 명칭 업데이트 · URL차단장비 명칭 변경 · 하위계위ISP의 관리 의무조항 신설
	제9조(차단사실의 안내 등)	· 안내책임 한계 범위 명시
	제10조(차단의 실사 등)	· 기관 명칭 업데이트
	제11조(해외 불법정보 차단책임자의 지정)	· 기관 명칭 업데이트
제3장 보칙	제12조(자료제출요구)	· 기관 명칭 업데이트
	제13조(해외 불법정보 차단 지원)	· 기관 명칭 업데이트

○ (근거조문수정) 정보통신망법과 동법 시행령의 개정으로 인해 접속차단을 위한 취급거부 명령의 근거 조항이 변경되어, 이에 대한 반영이 필요함

- URL차단지침 제정 당시의 불법정보 취급거부 명령과 관련한 근거조항은 정보통신망법 제44조의7, 제55조 및 동법 시행령 제22조의 12였으나, 현행 개정법은 망법 제44조의

7 및 제64조로 변경되어, 차단지침의 제1조(목적)의 근거조항의 변경이 필요함

<표 3-8> 정보통신망법 신구조문 대비표

정보통신망법(2007년도)	정보통신망법(2020년)
제44조의7 (불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다. (생략)	제44조의7(불법정보의 유통금지 등) ① ――. (생략)
② 정보통신부장관은 제1항제1호 내지 제6호의 규정에 따른 정보에 대하여는 제44조의8의 규정에 따른 정보통신윤리위원회의 심의를 거쳐 정보통신서비스제공자 또는 게시판 관리・운영자로 하여금 그 취급을 거부・정지 또는 제한하도록 명할 수 있다. 다만, 제1항제2호 및 제3호의 규정에 따른 정보의 경우에는 그러한 정보로 인하여 피해를 받은 자의 명시(明示)한 의사에 반하여 이를 명할 수 없다.	② 방송통신위원회는 ―――――――――――― 부터 ―――까지, 제6호의2 및 제6호의3의 ――――――――――――――――――――심의위원회의 ――처리를 ―――――――――――――――――――――――――――. 다만 ―――――――――――――――――――― 에 ――――――――――――――――――――――― 해당 ――――――――――――――――――――――― 가 구체적으로 밝힌――――――――그 처리의 거부・정지 또는 제한을 ―――――――――.
③ 정보통신부장관은 제1항제7호 내지 제9호의 규정에 따른 정보에 대하여는 관계 중앙행정기관의 장의 요청이 있는 경우에 한하여 요청을 받은 날부터 7일 이내에 정보통신윤리위원회의 심의를 거친 후 제44조의9제1항제3호의 규정에 따른 시정요구에도 불구하고 정보통신서비스제공자 또는 게시판 관리·운영자가 이에 응하지 아니하는 경우에는 그 취급의 거부·정지 또는 제한을 명하여야 한다. <신설>	③ 방송통신위원회는 ―――――――――――――부터 ――――――까지의 ―――가 다음 각 호의 모두에 해당하는 경우에는 ――에게 해당 정보의 처리를 ―――――――――――――――――― 하도록 ―――――――――――――――――――. 1. 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것 2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정 요구를 하였을 것 3. 정보통신서비스 제공자나 게시판 관리・운영자가 시정 요구에 따르지 아니하였을 것
④ 정보통신부장관은 제2항 및 제3항의	④방송통신위원회는 ――――――――――――――――

규정에 따른 명령의 대상이 되는 정보통신서비스제공자, 게시판 관리·운영자 또는 해당 이용자에게 사전에 의견제출의 기회를 주어야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.	에―――――――――――――――――――――― ―――――――――――――――――――――――― ――――――――――――――――――――미리 ――――――――――――――――――――――――. ―――――――――――――의견제출의 기회를 주지 아니할 수 있다.
제55조 (자료제출 등) ①정보통신부장관은 다음 각 호의 어느 하나에 해당하는 경우에는 정보통신서비스제공자등(이하 이 조에서 제58조의 규정에 따라 준용되는 경우에 해당되는 자를 포함한다)에게 관계 물품·서류 등을 제출하게 할 수 있다. 1. 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 인지한 경우 2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우 <신설> 3. 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령이 정하는 경우 ② (생략)	제64조(자료의 제출 등) ① 과학기술정보통신부장관 또는 방송통신위원회는 ―――――――――――――――――――――――― ―――――――――――(국내대리인을 포함한다. 이하 이 조에서 같다)―――――――――――――――――― ―――――――――――――――――――――――― ――――――――――――――――――――――――. 1 ――――――――――――――――――――――― ――――――――――――――――알게 된 경우 2 ――――――――――――――――――――――― ―――――――――― 2의2. 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우 3―――――――――――――――――――――――― ――――――――으로 정하는 경우 ②(생략)
③ 정보통신부장관은 정보통신서비스제공자등이 제1항 및 제2항의 규정에 의한 자료를 제출하지 아니하거나 이 법의 규정을 위반한 사실이 있다고 인정되는 경우에는 소속공무원으로 하여금 정보통신서비스제공자등의 사업장에 출입하여 업무상황·장부 또는 서류 등을 검사하게 할 수 있다.	③ 과학기술정보통신부장관 또는 방송통신위원회는 ――――――가―――――― 따른 ―――――――――――――――――――――――― ――을 ―――――――――――――――――――――― ―――――인정되면 ――――――――――――――――― ―에게 ―――――――――――――――――――――― , 해당 법 위반 사실과 관련한 관계인의 ―――――――――――――――――――――――하도록 ―――――――――――――――.
④ 정보통신부장관은 이 법에 위반한 정보통신서비스제공자등에 대하여 필요한 시정조치를 명할 수 있다. ⑤ 정보통신부장관은 제4항의 규정에 따라 필요한 시정조치를 명한 경우에	④ 과학기술정보통신부장관 또는 방송통신위원회는 ――을 ――――――――――에게 해당 위반행위의 중지나 시정을 위하여 ―――――――――――――――――― 있고, 시정조치의 명령을 받은 정보통신서비스 제공자에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다. 이 경우 공표의 방법·기준 및 절차 등에 필요한 사항은 대통령령으로 정한다. ⑤ 과학기술정보통신부장관 또는 방송통신위원회는 ――――에 ――――――――――――

는 그 사실을 공개할 수 있다. 이 경우 공개의 방법·기준 및 절차 등에 관하여 필요한 사항은 정보통신부령으로 정한다.	---------- ---시정조치를 명한 ---------- 등에 ---------- 대통령령 ---------.
⑥ 정보통신부장관이 제1항 및 제2항의 규정에 따라 자료 등의 제출 또는 열람을 요구할 때에는 요구사유, 법적근거, 제출시한 또는 열람일시, 제출 또는 열람하여야 할 자료의 내용 등을 명시하여 서면(전자문서를 포함한다)으로 통지하여야 한다.	⑥ 과학기술정보통신부장관 또는 방송통신위원회가 ---------에 ---------- ----------제출열람할---------- 구체적으로 밝혀 ---------- ----------알려야 ----.
⑦ 제3항의 규정에 따른 검사를 하는 경우에는 검사개시 7일 전까지 검사일시, 검사이유 및 검사내용 등에 대한 검사계획을 해당 정보통신서비스제공자등에게 통지하여야 한다. 다만 긴급을 요하거나 사전통지의 경우 증거인멸 등으로 검사목적을 달성할 수 없다고 인정하는 경우에는 그러하지 아니하다.	⑦---------에 ---------- ----시작 ---------- ---------- ----------에게 알려야 -----. ----------한 경우나 ----------를 하면 ---------- -- 그 검사계획을 알리지 ---한--.
⑧ 제3항의 규정에 의하여 검사를 하는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 하며, 출입시 성명·출입시간·출입목적 등이 표시된 문서를 관계인에게 교부하여야 한다.	⑧---------에따라---------- ---------- ---------- ---------- ----------내주어야 한다.
⑨ 정보통신부장관은 제1항 내지 제3항의 규정에 따라 자료 등을 제출받거나 열람 또는 검사한 경우에는 그 결과(조사결과 시정조치명령 등의 처분을 하고자 하는 경우에는 그 처분의 내용을 포함한다)를 해당 정보통신서비스제공자등에 대하여 서면으로 통지하여야 한다.	⑨ 과학기술정보통신부장관 또는 방송통신위원회는 ---부터 ---까지 ---------- ---------- ----------하려는 ---------- ---------- ----------에게 ---------- -------- 알려야 한다.
(이하생략)	(이하생략)

<표 3-9> 정보통신망법 시행령 신구조문 대비표

정보통신망법 시행령(2007년도)	정보통신망법 시행령(2020년)
제22조의12(시정요구 등) ①윤리위원회는 법 제44조의9제1항제3호에 따라 정보를 심의하여 정보통신서비스제공자 또는 게시판 관리·운영자에게 다음 각 호의 시정요구를 할 수 있다. 1. 해당 정보의 삭제 또는 접속차단 2. 이용자에 대한 이용정지 또는 이용해지 3. 청소년유해정보의 표시의무 이행 또는 표시방법 변경 등 그 밖에 필요하다고 인정하는 사항 ② 정보통신서비스제공자 또는 게시판 관리·운영자는 제1항에 따른 시정요구를 받은 경우에는 그 조치결과를 윤리위원회에 지체 없이 통보하여야 한다.	<삭제>

③ 윤리위원회는 정보통신서비스제공자 또는 게시판 관리·운영자가 제1항에 따른 시정요구에 응하지 아니하는 경우로서 당해 정보가 법 제44조의7제1항 제1호부터 제6호까지에 따른 불법정보인 때에는 정보통신부장관에게 정보통신서비스제공자 또는 게시판 관리·운영자로 하여금 그 취급거부·정지 또는 제한을 하도록 하는 명령을 하여 줄 것을 요청할 수 있다. ④ 정보통신부장관이 제3항에 따라 요청을 받아 정보통신서비스제공자 또는 게시판 관리·운영자로 하여금 해당 정보의 취급거부·정지 또는 제한을 하도록 명령하는 경우에는 법 제44조의7제2항 및 제3항에 따른 윤리위원회의 심의를 거치지 아니할 수 있다.	

- 이에 따라 법률개정 현황을 반영하여 현행 지침의 제1조(목적)를 다음과 같이 개정하여 처리지침의 법률적 근거를 제44조의 7과 제64조에 두고 있음을 명시함

<표 3-10> 지침 상 근거조문수정을 위한 신구조문 대비표

현행	개정안
제1장 총칙 제1조(목적) 이 지침은 정보통신망이용촉진 및 정보보호등에 관한 법률(이하 "법"이라 함) 제44조의 7, 제55조 및 동법 시행령(이하"영"이라 함) 제22조의 12에 따라 해외불법정보를 차단하기 위한 업무처리 절차를 정함을 목적으로 한다.	제1장 총칙 제1조(목적) ---------- ---------- ---------- ----- 제44조의 7, 제64조에 따라 ---- ------ ---------- ---------- ---------- ----------.

○ (적용범위) 전기통신사업법 개정[8]으로 기간통신사업이 허가제에서 등록제로 변경됨에 따라 차단업무 처리지침 대상사업자를 허가에서 등록 사업자로 변경하는 등 제3조의 개정이 필요함

- 전기통신사업법 개정으로 기간통신사업자의 인허가제도가 허가에서 등록 및 신고제로 전환(전기통신사업법 제6조)됨에 따라, 제2조의 "해외인터넷 접속역무를 허가 받거나 등록하여 제공하는 정보통신서비스 제공자(인터넷접속사업자)"를 등록 또는 신고하여 제공하는 정보통신서비스 제공자로 변경이 필요함

8) 전기통신사업법 제6조(기간통신사업의 등록 등)의 개정으로 별정통신사업자가 기간통신사업의 신고대상사업자로 포섭이 되고 기존 기간통신사업자는 등록대상사업자로 변경됨. 이에 따라 해외관문국을 보유한 인터넷접속역무사업자들이 모두 등록대상 사업자로 변경됨.

- 해외서버나 사이트를 통해서 국내로 유입되는 불법정보의 차단을 위한 처리지침이기 때문에 취급거부명령 이행을 위한 업무처리지침의 적용범위를 해외관문국을 보유한 사업자에 한정하는 것은 여전히 적절하다고 판단할 수 있음
- 다만 차단 대상이 되는 정보의 범위를 "해외에서 국내로 유입되는 한글로 제공되는 음란, 도박 등 불법정보"로 한정했던 기존 지침이 언어와 상관없이 불법 해외사이트(예: pornhub.com)에 접속하는 현실과 맞지 않기 때문에 "해외에서 국내로 유입되는 음란, 도박 등 불법정보"로 변경이 필요함

<표 3-11> 처리지침 적용범위 확대를 위한 신구조문 대비표

현행	개정안
제2조(적용범위) 이 지침은 정보통신부장관의 취급거부 등 명령, 시정조치명령 또는 정보통신윤리위원회(이하 "윤리위원회"라 한다)의 시정요구(이하 "취급거부명령 등"이라 함)에 따라 해외 인터넷 접속역무를 허가를 받거나 등록하여 제공하는 정보통신서비스제공자(이하 "인터넷접속사업자"라 함)가 자신이 운영하는 정보통신망을 통하여 해외에서 국내로 유입되는 한글로 제공되는 음란, 도박 등 불법정보(이하 "해외 불법정보"라 함)에 대한 국내에서의 접속을 차단하는데 적용한다.	제2조(적용범위)---------- 방송통신위원회 위원장의 취급거부 등 ---,----------또는 방송통신심의위원회--------- ---------- ----------해외 인터넷 접속역무를 등록하여---------- ---------- ---------- ---------- ---------- ---------- 음란, 도박 등 불법정보 ---------- ----------.

○ (대상정보확대) 도메인까지 차단대상정보로 포섭하는 방향으로 개정이 필요함
- HTTP차단에서는 불법정보를 식별하기 위한 정보로 URL과 IP 정보의 공유가 필요하나, HTTPS 차단에서는 도메인의 공유가 필요함에 따라, 지침 제4조에서 인터넷접속사업자에게 제공해야할 정보의 범위를 "불법정보 식별정보(도메인, URL 및 해당시점에 알려진 IP주소)"로 변경이 필요함
- 실무적으로 방송통신위원회가 취급거부 명령을 내릴 때, 불법정보 식별정보만을 제공하는 것이 아니라 제3조 2항[9]에 따라 현재의 차단기술, 장비 또는 방법 등에 대해 인터넷접속사업자의 의견을 청취하고 차단방법에 대해 고지하고 있음

9) 정보통신부장관은 제1항에 따른 차단하여야할 해외불법정보의 범위를 정하고자 할 때에는 현재의 차단기술, 장비 또는 방법 등에 관하여 윤리위원회, 인터넷접속사업자 등으로부터 의견을 들을 수 있다.

- 그러나 HTTPS 도입당시 KT가 HTTP차단목록 DB와 HTTPS 차단목록DB를 합쳐서 과잉차단한 것과 같은 상황을 방지하기 위해, 해외불법정보의 식별정보와 함께 식별정보 목록(DB)의 관리방법을 함께 제공하도록 제4조 1항에 명시하는 것도 검토가 필요함
  ※ 방송통신위원회 위원장 또는 방송통신심의위원회는 인터넷접속사업자에 대하여 해외불법정보의 차단을 위한 취급거부명령 등을 하고자 하는 경우 해외 불법정보의 식별정보(도메인, URL 및 해당 시점에 알려진 IP주소)와 식별정보 목록(DB)의 관리방법을 함께 제공하여야 한다.

<표 3-12> 기술포섭을 위한 신구조문 대비표

현행	개정안
제4조(인터넷접속사업자에 대한 해외 불법정보 URL 및 IP주소의 제공 등) ① 정보통신부장관 또는 윤리위원회는 인터넷접속사업자에 대하여 해외불법정보의 차단을 위한 취급거부명령 등을 하고자 하는 경우 해당 인터넷접속사업자에게 차단하여야 할 해외 불법정보의 URL과 해당 시점에 알려진 IP주소를 제공하여야 한다. ② 정보통신부장관 또는 윤리위원회는 제1항에 의한 해외 불법정보의 URL의 제공 이후 해외 불법정보를 제공하는 사이트의 변경·폐쇄 등으로 인하여 해외 불법정보의 차단 사유가 소멸된 경우에는 직권 또는 취급거부명령 등을 받은 인터넷접속사업자의 신청으로 해당 해외 불법정보의 차단을 위한 취급거부명령 등을 철회하여야 한다.	제4조(인터넷접속사업자에 대한 해외 불법정보 식별정보의 제공 등) ① 방송통신위원회 위원장 또는 방송통신심의위원회는 --------- ------------ ----------- ---------------------- ------------------------- ------- -- ------------------------ 해외 불법정보의 식별정보(도메인, URL 및 해당 시점에 알려진 IP주소)와 식별정보의 관리 방법을 제공하여야 한다. ② 정보통신부장관 또는 윤리위원회는 ------------ 해외 불법정보의 URL과 도메인의 제공 이후 ---- ----------------------------- --- --------------------------- ----------------------- ------- ------------------------------ ------------ -- -- ------------.
제13조(해외 불법정보 차단 지원) 정보통신부장관 또는 윤리위원회는 해외 불법정보의 효과적인 차단을 위하여 인터넷접속사업자에 대하여 웹서버 운영, IP 추출 프로그램의 개발·보급 및 사후관리를 지원할 수 있다.	제13조(해외 불법정보 차단 지원) 방송통신위원회 위원장 또는 방송통신심의위원회는 --------------------------------- ----------- -------------------------------, IP와 도메인 추출 프로그램의 --------------------------- ---------------.

○ (차단장비) "URL차단장비"를 "차단장비"로 변경하여 도메인 DB를 포괄

- HTTPS 차단이나 기존 차단 모두 국제망 접속점의 최상위 구간에 접속차단을 위한

장비를 설치하고 불법정보의 주소목록 DB(URL DB 및 도메인 DB)와 매칭하여 차단하는 방식을 취하고 있음

- 따라서 인터넷접속사업자가 설치해야하는 차단장비가 URL DB 및 도메인 DB를 모두 포괄하기 때문에 기존 지침의 "URL 차단장비"를 "차단장비"로 명기하는 수정이 필요함

<표 3-13> 차단장비 명칭 변경을 위한 신구조문 대비표

현행	개정안
제6조(URL 차단장비 설치에 의한 차단) 정보통신부장관 또는 윤리위원회는 해외 불법정보의 효율적 차단을 위하여 인터넷접속사업자 중 해외 인터넷접속설비를 직접 설치한 사업자에 대하여 자신이 설치·보유하는 해외 인터넷접속설비에 해외 불법정보의 차단을 위한 URL 차단장비를 설치하도록 취급거부명령 등을 내릴 수 있다.	제6조(차단장비 설치에 의한 차단) ① 방송통신위원회와 방송통신심의위원회는 ----------차단장비를 ----------.
제7조(URL 차단장비의 설치) ① 제6조의 취급거부명령을 받은 인터넷접속사업자(이하 "URL 차단장비 설치 사업자"라 함)는 국제망 접속점의 최상위 구간 등에 URL 차단장비를 설치하여야 한다. ② URL 차단장비 설치 사업자는 포워딩(Forwarding)서버를 사용하거나 멀티도메인 웹호스팅으로 여러 도메인이 하나의 IP를 공유하는 경우 URL 단위의 차단을 통하여 해외 불법정보를 제공하지 않는 정상적인 사이트가 차단되지 않도록 노력하여야 하며, 정상적인 사이트가 함께 차단된 경우에는 정보통신부장관 또는 윤리위원회는 직권 또는 URL 차단장비 설치 사업자의 신청에 의하여 해당IP 차단을 철회할 수 있다. ③ URL 차단장비 설치 사업자는 차단장비의 설치 등을 통하여 도메인 및 IP주소의 변경, DNS(Domain Name System)우회(DNS-free 사용 등), IP주소 직접 접속, 프록시(Proxy)서버, 아노마이져(Anonymizer) 등에 의한 우회접속방지를 위하여 기술적 조치를 강구해야 한다.	제7조(차단장비의 설치) ① ----------인터넷접속사업자(이하 "차단장비 설치 사업자"라 함)는 ----------차단장비를 ----------. ② 차단장비 설치 사업자는 ----------방송통신위원회 위원장 또는 방송통신심의위원회는--------차단장비 설치 사업자의 신청에 의하여 ----------. ③ 차단장비 설치 사업자는 ---------- . ④ 차단장비 설치 사업자는----------

④ URL 차단장비 설치 사업자는 자신의 정보통신망을 통한 우회접속비율 및 정도 등 우회접속의 실태를 파악하고, 정보통신부장관이 이에 관한 자료의 제출을 요청하는 경우 이에 응하여야 한다. ⑤ URL 차단장비 설치 사업자는 차단목록 입력 등 차단 조치 후 1개월 이내에 해외 불법정보의 차단을 증명하는 자료를 정보통신부 장관에게 제출하여야 한다. 다만, 불법 해외정보의 차단과 관련한 실사 자료가 있는 경우 이로써 갈음할 수 있다.	----------,방송통신위원회위원장이 ----------. ⑤ 차단장비 설치 사업자는---------- 방송통신위원회 위원장에게----------.
제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계) ① URL 차단장비의 설치를 통한 해외 불법정보의 차단의 경우 URL 차단장비 설치사업자로부터 정보통신망을 임차하여 운영하는 인터넷접속사업자(이하 “타 인터넷접속사업자”라 함)는 해당 해외 불법정보의 차단을 URL 차단장비 설치사업자에게 위임한 것으로 본다. ② URL 차단장비 설치 사업자는 URL 차단장비를 설치한 경우 정보통신부장관 또는 윤리위원회로부터 취급거부명령 등을 받은 사실 및 차단한 해외 불법정보의 목록을 타 인터넷접속사업자에게 지체없이 통지하여야 한다. ③ URL 차단장비의 설치에 따라 발생하는 비용 중 타 인터넷접속사업자가 임차하여 사용하는 정보통신망에 해당하는 비용은 URL 차단장비 설치사업자와 타 인터넷접속사업자가 협의하여 분담한다. ④ 제3항에 따른 비용 분담의 원활한 협의를 위하여 (사) 한국인터넷기반진흥협회는 URL 차단장비 설치 사업자로부터 이를 위임받아 처리한다. ⑤ URL 차단장비 설치를 통한 해외 불법정보의 차단과 관련하여 발생하는 민원 및 법적 분쟁에 대하여는 해당 민원 및 법적 분쟁을 제기한 자에게 인터넷접속역무를 제공하는 인터넷접속사업자가 이를 책임지고 처리하여야 한다.	제8조(차단장비 설치 사업자와 타 인터넷접속사업자와의 관계) ① 차단장비의 ---------- 차단장비 설치 사업자로부터---------- ----------차단장비 설치사업자에게 ----------. ② 차단장비 설치 사업자는 ----------방송통신위원회위원장 또는 방송통신심의위원회로부터----------. ③ 차단장비의 설치에 ----------차단장비 설치사업자와 ----------. ④ ---------- ---------- (사) 한국인터넷진흥협회는 차단장비 설치 사업자로부터 ----------. ⑤ 차단장비 설치를 ----------

○ (우회방지책무강화) 하위계위 인터넷접속사업자의 우회접속 방지 책무를 명시하고 우회

실태파악을 위한 인터넷접속사업자의 협조의무를 구체화할 필요가 있음

- 기존 지침은 모든 인터넷접속사업자에게 접속차단의 의무가 부여되어 있으나 접속차단 업무의 운용과 책임을 해외관문국을 보유한 상위계층사업자에게 위임한 것으로 간주(제8조1항)했음

<표 3-14> 정부 계위평가방식에 따른 국내 ISP사업자 분류

분류	사업자
상위 계위 ISP	KT, SKB 및 LGU+
망중계사업자	세종, 드림라인 및 KINX
하위계위 ISP	LG헬로, T-Broad, DLive, HCN, CMB

출처: 권오상 외(2019)

- 하위계위 ISP 사업자의 책임은 URL차단장비 설치의 비용을 분담(제8조3항과 4항)하고, 해외 불법정보의 차단과 관련하여 발생하는 민원 및 법적 분쟁에 대하여 책임을 지고 처리(제8조5항)하는 데에 있는 것으로 규정되었으며, 이에 따라 하위계위사업자는 이용약관에 불법정보 차단을 위해 인터넷접속이 제한될 수 있음을 명기하고 이용자의 접속 관련 민원을 접수 및 처리해왔음
- HTTPS 차단에서도 해외불법정보의 국내유입을 해외관문국에 설치한 차단장비로 차단하기 때문에 차단장비의 설치 및 운용은 상위계층 ISP사업자에게 부과하고, 하위계위 사업자는 차단장비 설치의 비용을 분담하고 민원 및 법적 분쟁을 처리하는 현행 체계를 유지할 수 있음
- 다만 하위계위 ISP사업자가 망이용의 효율성을 위해 보안이 적용된 전용회선이나 클라우드 기반 VPN(MPLS VPN)을 이용하는 경우에 접속자의 IP주소까지 암호화되어 해외관문국에 설치된 차단장비에서 접속차단이 무력화되지 않도록, 하위계위ISP사업자의 책임을 명기할 필요가 있음
- 하위계위 ISP사업자는 자신의 정보통신망에 별도의 차단장비를 설치할 필요는 없으나 망설비를 임차하여 사용할 경우 망설비를 제공하는 사업자에게 불법사이트의 차단조치를 위한 장비설치 및 차단실시 등이 이행하는지 여부를 확인하고, 제3항에서 차단장비 설치사업자로부터 받은 해외불법정보 목록이 차단되는지 여부를 확인할 필요가 있음

- 이에 따라, 하위계위 ISP사업자가 망설비를 임차하여 사용할 경우, 자신의 인터넷가입자 접속에서 해외불법정보가 차단될 수 있도록 확인하고 관리하는 규정이 신설되어야 함 (제8조 6항)

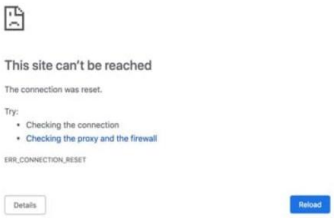
<표 3-15> 타 인터넷사업자의 관계를 위한 신구조문 대비표

현행	개정안
제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계)	제8조(차단장비 설치 사업자와 타 인터넷접속사업자와의 관계)
①~⑤ (생략)	①~⑤ (생략)
<신설>	⑥ 인터넷접속사업자가 최종이용자에게 인터넷망에 접속할 수 있도록 물리적 또는 가상의 회선(동선, HFC, 광케이블, 가상사설망 등)을 사용할 경우, 제3항에서 제공받은 해외불법정보의 차단이 이뤄지도록 적절한 조치를 취하여야 한다.

○ (차단사실의 안내) 현행 지침은 해외 불법정보를 차단한 인터넷 사업자(상위계층 ISP 사업자)가 안내하도록 하고 있어, 접속차단 시 이용자에게 접속차단의 사유를 안내하는 안내페이지로 리다이렉트(re-direct) 해야 하는 것으로 해석될 수 있음

- 그러나 HTTP차단과 달리 HTTPS차단은 접속이 차단된 불법사이트에 접속하고자 할 때, 접속차단 여부와 이유를 고지할 수 있는 웹페이지(warning.or.kr)등으로 리다이렉트 할 수 없는 기술적 한계가 있음
- HTTPS 차단은 SNI에서 도메인 명을 찾아서 접속을 끊는(drop) 방식으로, 접속하고자 하는 이용자에게 빈 페이지만 제시됨

<표 3-16> 불법정보 차단 시 이용자 화면 비교

HTTP 차단 시 안내페이지	HTTPS 차단시 화면
	

- HTTPS차단으로 빈페이지를 확인한 인터넷이용자들은 해당 사이트로의 접속이 불가능한 이유가 불법사이트 접속차단으로 인한 것인지 또는 단순한 인터넷 접속차단인지를 확인할 수 없음
- 따라서 HTTPS차단으로 인해 접속하고자 한 사이트에 접속하지 못한 인터넷이용자는 해외 불법정보를 차단한 인터넷 사업자가 아니라 자신이 가입한 인터넷 사업자에게 민원을 접수하게 되며, 이러한 민원에 대한 대응은 제8조5항에 해당 민원 및 법적 분쟁을 제기한 자에게 인터넷접속역무를 제공하는 인터넷접속사업자가 처리하도록 규정되어 있음
- 따라서 제9조의 차단사실 안내 의무는 HTTP차단 시 안내페이지(warning.or.kr)로 리다이렉트하는 의무에 한정됨을 명시해야함

<표 3-17> 차단사실의 안내를 위한 신구조문 대비표

현행	개정안
제9조(차단사실의 안내 등) 해외 불법정보를 차단한 인터넷사업자는 이용자의 인터넷접속역무 이용 상의 혼란을 방지할 수 있도록 차단사실을 자신의 이용자에게 안내하여야 한다.	제9조(차단사실의 ---------- ---------- ---------- URL 차단사실을 ---- ----------.

제 2 절 불법정보 유통방지를 위한 비기술적 대응방안

1. 자율규제 활성화 방안

1-1. 인터넷 불법정보 심의의 자율규제 모형

○ (정의) 인터넷 콘텐츠의 자율규제는 인터넷이 가지는 국제성을 극복하고(황승흠·황성기, 2003) 표현의 자유를 확보하기 위한 방안으로, 정부가 사업자, 기관 등의 민간 영역에 규제 권한을 부여하는 것이나, 산업 내부의 필요성에 의해 자발적으로 규제하는 경우도 포함
- 자율규제의 필요성은 산업계의 내부에서 자생적으로 발생할 수 있으나, 정부가 규제 필요성을 인식하여 해당 권한을 위임하여 발생하기도 함

○ (규제 주체) 인터넷 콘텐츠의 자율규제 주체를 정부, 인터넷 사용자, 인터넷 서비스 제공자로 세 그룹으로 구분(Machill, Hart & Kaltenhäuser, 2002; 김유승, 2005에서 재인용)

○ (책임) 인터넷 콘텐츠 관리에 있어 ISP의 책임이 강조되는 의견도 있는데, 이는 해당 콘텐츠에 대한 접속을 규제하는 게이트 키퍼(gate keeper)로의 역할을 효율적으로 수행할 수 있기 때문으로 해석됨(Edwards, 2000. 김유승, 2005에서 재인용)
- EU "전자상거래에 대한 지침(Directive on electronic commerce)"에서 ISP는 불법정보의 존재를 인지하면(notice) 즉각 해당 정보에 대해 접속 차단 또는 삭제 조치를 취해야 한다(take down)는 의무를 부여하여, 콘텐츠 규제에 대한 ISP의 자율적 조치를 실시하도록 함
- 한편으로 CP(Content Provider)의 역할이 강조되기도 하는데, 이는 콘텐츠를 생산하고 유통하는 당사자에 대한 직접적인 규제 필요성을 강조하는 맥락에서 실시됨 (Akdeniz, 2001, 김유승, 2005에서 재인용)

○ (유형) 자율규제의 모델은 책무성 관점에서 자발적 자율규제, 위임형 자율규제의 세 가지

로 구분됨(황용석, 이동훈, 김준교., 2009)

- 자발적 자율규제는 정부개입 및 법률적 근거가 없이 규칙의 제정과 집행이 모두 민간에 의해서 제정되고 운영되는 경우로 미국이 대표적임
- 위임형 자율규제는 규칙의 제정과 집행이 민간에 의해서 이뤄지지만 민간에 의한 자율규제의 시행이 정부의 인허가 등에 따라 관리되거나 일정정도의 자율성이 제약되는 경우로, 영국, 프랑스, 독일, 일본 등이 이에 해당함
- 이론적으로는 정부의 역할범위에 따라 자율규제모델을 자발적 자율규제, 부분위임 자율규제, 완전위임 자율규제로 구분해왔으나(황용석 외, 2009, 송순영, 2011, 김유향, 2016)
- 현실적으로는 위임의 범위를 명확히 분류하기가 어려울 뿐만 아니라 프랑스의 FDI가 2011년 해산함에 따라, 정부가 자율규제기구의 재정을 지원하고 관리감독하는 부문 위임형 자율규제를 시행하는 사례가 없음

<표 3-18> 인터넷 자율규제 모델 유형

구분	자발적 자율규제	위임형 자율규제
정부의 위임방식	없음	정책적 승인
자율규제의 형식	독립형	협력형
담당 자율기구 수	복수	단수 또는 복수
자율기구의 주요 기능	교육/핫라인/정책연대	교육/핫라인/정책연대/분쟁조정
자율기구의 재정	기금, 기부, 회비 등 다양	기금, 기부, 회비 등 다양

자료: Gunningham & Rees(1997), 황용석, 이동훈, 김준교(2009), 송순영(2011), 김유향(2016), 재구성

1-2. 주요국의 자율규제 현황

가. 유럽위원회(EC)의 불법정보 관리를 위한 권고

○ (개요) 유럽위원회는 인터넷 불법정보의 효과적 관리를 위한 권고안을 채택('18.3.1)

- (배경) 불법정보를 단순히 제거하는 기존 조치만으로는 테러유인, 혐오표현, 아동성착취물,

지적재산권 침해, 온라인 소비자 보호와 같은 국경을 넘는 인터넷 불법정보를 효과적으로 관리할 수 없다는 판단에 따라, EU전반에 걸친 규제개선 필요성 대두

- (목적) 인터넷불법정보† 의 효과적 관리를 위해 온라인 플랫폼에 대해 콘텐츠 관리에 대한 책임을 부여하고, 신속하게 사전에 감지, 제거 및 재유통을 방지하는 일반적인 방법론을 제안함

† EC에서 규정하는 불법정보(illegal content)는 테러조장, 인종차별 또는 외국인 혐오, 불법적 혐오 발언, 아동 성착취물, 불법 상업관행, 지적재산권과 상품안전 침해와 같이 유럽연합법 또는 회원국의 법을 준수하지 않는 모든 정보를 의미함.

○ (제안사항) 인터넷불법정보 유통방지 조치의 수립에 있어서 ① 명확한 '통지 및 조치' 절차, ② 효율적·능동적 대처, ③ 강력한 기본권 보장, ④ 소규모플랫폼 배려, ⑤ 당국과의 긴밀한 협력 등이 반영되어야 함

① 명확한 '통지 및 조치' 절차 : 온라인 플랫폼은 '신뢰할 수 있는 신고자'에 대한 빠른 추적 절차를 포함하여 불법 콘텐츠를 알리는 쉽고 투명한 규칙을 설정할 의무가 있으며, 콘텐츠 제공업체에게는 반론권이 보장되어야 함

② 효율적·능동적 대처: 테러 콘텐츠나 아동성착취물과 같이 명확한 불법정보에 대해서는 능동적으로 찾아내고 삭제·방지하는 시스템을 구축해야 함

③ 강력한 기본권 보호: 표현의 자유 및 데이터 보호 규칙 등과 같이 기본권한과 관련하여 효과적이고 적절한 보호수단 마련 필요

④ 소규모 플랫폼 배려: 업계는 자발적인 합의를 통해 경험, 모범 사례 및 자동 탐지가 가능한 도구를 포함한 기술 솔루션을 공유·협력할 필요가 있음

⑤ 당국과의 긴밀한 협력: 심각한 범죄 행위 또는 불법 콘텐츠가 생명이나 안전에 위협이 된다는 의혹이 있는 경우, 즉시 신고할 의무를 부여해야함

○ (면책) 유럽연합법은 전자상거래에 관한 유럽지침에서 ISP나 인터넷 중개업자(intermediaries)의 면책(liability)의 범위를 정하고 있음

- 전자상거래에 관한 유럽지침 제46조에 따라 불법정보에 대한 인지 또는 실질적인 지득에 따라 ISP나 호스팅 사업자 등이 불법정보의 접속을 제한하는 행위를 할 수 있도록 하고

있으며, 이는 국가수준에서 정한 절차에 따르도록 정하고 있음

<전자상거래에 관한 유럽지침>

"내부 시장에서의 정보사회 서비스, 특히 전자상거래에서의 법적 측면에 대한 2000년 7월 8 일 유럽의회 및 위원회 지침 2000/31/EC"

(40) 서비스 제공자의 행위책임, 특히 국경 간에 서비스나 경쟁의 발전을 저하시키는 행위에 대한 회원국의 법률 및 판례법; 서비스 제공자가 특정상황 하에서 불법행위를 하지 않도록 할 의무를 제공하고; 본 지침은 불법 정보에의 접근을 차단하는 신속하고 신뢰할 수 있는 절차의 개발을 정하며; 이 메커니즘은 회원국 국가들 간의 자발적인 동의 하에 이루어 져야 하며; 정보사회서비스 규정에서의 모든 당사자의 권리를 위한 절차를 채택하며; 책임과 관련한 본 지침 규정은 지침 95/46/EC 과 지침 97/66/EC에서 정하는 디지털 테크놀로지 기술로서 가능한 기술적인 감독의 효율적인 작동 및 보호 개발을 방해하지 않아야 한다.

(45) 본 지침에서 설립한 서비스제공자의 책임 제한은 다른 종류의 금지사항에 영향을 미치지는 않으며; 이러한 금지사항으로는 불법정보의 삭제 및 접근 불가 등이 있다.

(46) 책임 제한을 적용받기 위해서, 정보를 저장하는 정보사회서비스 제공자는 불법행위에 대한 인지 또는 실질적인 지득에 따라 관련된 정보로의 접속을 막거나 제거하는 행위를 신속하게 실시해야하며; 정보에의 접근 제한 및 금지는 표현의 자유에 관한 국가 수준에서 정한 절차에 따라야 하며; 본 지침은 회원국이 정보의 제거 및 이용불가의 조치를 취하기 이전에 신속하게 행해야 하도록 국가수준에서 정한 특정 요건에 영향을 미치지 않는다.

- (책임) ISP는 수동적으로 전송하는 정보에 대해서 민법 또는 형사법에 대해 책임을 지지 않으며, 콘텐츠를 모니터링할 의무가 없음. 그러나 법원이나 행정부가 각 국가의 법적 체계에 따라 내용의 불법성을 판단하여 ISP에게 차단을 명령할 수 있음

○ (자율규제 적용정도) 불법정보의 접속차단과 관련한 규제체계는 각국의 법체계와 상황에 따라 차이가 있으나 대체로 행정부나 사법부의 영역에서 이뤄져왔으며, 예외적으로 영국의 경우 자율규제의 비중이 높은 경향

- 판례의 구속력이 있는 영미법/보통법 계통의 국가들(영국, 미국 등)은 사적영역의 자율규제의 비중이 높은 경향이 있으며, 인터넷 전체에 적용되는 법체계 수립보다는 사안별로 일반법과 판례를 적용하는 경향
- 대표적으로 영국의 경우는 공공기관이나 경찰에 대한 ISP의 자발적인 협조, 인터넷매개자

(intermediaries)의 이용자약관 등을 통해서 불법정보의 차단, 삭제, 필터링 등을 실시하며, 법적 근거는 테러방지법, 명예훼손 관련 법 등의 일반법에 따라 이뤄지고 있음

나. 유럽위원회(EC)의 디지털서비스법(Digital Services Act)에서의 플랫폼 책무

○ (개요) '20년 12월 EU는 디지털서비스법(Digital Servicies Act)과 디지털시장법(Digital Markets Act)를 통해 온라인 플랫폼의 불법 정보에 대한 규제안을 제시함

- 디지털 서비스의 중요성이 증대됨에 따라 온라인 플랫폼은 소비자에게 혜택을 주고, 유럽연합 내외의 거래를 촉진했으나, 동시에 불법콘텐츠 유포 및 불법 상품 및 서비스 판매의 창구로 기능
- 온라인에서 이용자의 기본권에 대한 포괄적 보호 뿐 아니라 불법콘텐츠의 신속한 제거를 위한 새로운 절차를 포함하여 소비자를 재화, 서비스 또는 콘텐츠에 연결하는 모든 디지털서비스에 EU 회원국 전체의 의무를 구속력 있게 규율하고자 함
- 사용자, 중개플랫폼 및 규제기관의 권리와 책임을 재조정할 것이며, 인권, 자유, 민주주의, 평등, 법치 존중 등 유럽적 가치에 기반을 두고 있음

※ 디지털서비스법은 온라인상 서비스와 오프라인 서비스의 불법 정도를 달리보는 규제를 조정하는 것이 주 내용, 혐오표현 규제 등이나 온라인 서비스 알고리즘 투명성 등을 내용으로 함

○ (적용 대상) 디지털서비스법의 특징은 적용 대상 사업자의 유형에 따라 의무를 달리 규정하였다는 점이며, 특히 대규모 온라인 플랫폼의 경우 대다수의 의무가 부여된 것이 특징적임

- 중개서비스, 호스팅서비스, 온라인 플랫폼, 대규모 온라인 플랫폼으로 분류된 사업자 유형에 따라 의무가 부여됨
- 디지털 서비스를 제공하는 사업자 간의 역할, 규모, 온라인 생태계에 미치는 영향력을 고려하여 의무를 부여하였으며, 중개서비스→ 호스팅서비스→ 온라인플랫폼→ 대규모 온라인 플랫폼 순으로 의무가 누적됨

<표 3-19> EU 디지털서비스법 적용 대상 구분

구분	설명
중개서비스 (Intermediary services)	네트워크 인프라를 제공하는 사업자 인터넷 접속 사업자, 도메인 네임 등록사업자
호스팅 서비스 (Hosting services)	클라우드, 웹호스팅 서비스
온라인 플랫폼 (Online platforms)	판매자와 소비자가 함께 이용하는 플랫폼 온라인 마켓, 앱스토어, 집합적 경제 플랫폼, 소셜미디어플랫폼
대규모 온라인 플랫폼 (Very large online platforms)	불법 콘텐츠의 유포와 사회적 피해를 야기할 위험이 큰 사업자 유럽 소비자 중 10% 이상에 도달하는 사업자(약 4천 500만명)

자료: EC의 The Digital Services Act.

- 모든 사업자에 공통적으로 적용되는 의무는 투명성 보고, 기본권을 충분히 고려한 서비스 이용조건, 명령에 따른 회원국 규제당국과의 협력, 컨택트 포인트(필요시 법적 대리인)의 4가지로 이루어져 있음

○ (주요 의무) 디지털서비스법안에서는 불법 온라인 콘텐츠에 대한 각 사업자별 유형에 따라 의무를 부여하고 있으며 조치 방법, 절차, 정보제공 등으로 이루어짐

- 이중 불법콘텐츠 삭제와 관련한 의무는 신뢰 기반 신고자 제도 등 불법재화나 서비스 또는 불법 콘텐츠 유통방지를 위한 조치의무가 포함됨
- 신뢰기반 신고자(Trusted flaggers) 프로그램은, 커뮤니티가이드를 위반하는 콘텐츠를 정보통신서비스제공사업자에게 신고할 수 있도록 사전에 인증된 개인, 정부기관, NGO등에게 신고프로그램을 제공하는 제도로, 일반적으로 일괄신고도구, 신고된 콘텐츠에 대한 조치 결과의 공개, 관련 교육 등이 포함됨

○ (사업자 면책) 서비스 제공자의 유형에 따라 불법 콘텐츠를 인식하지 못하였으나 적절한 조치를 취한 경우 면책을 받을 수 있음

[EU 디지털서비스법 중개서비스 제공자의 면책]

※ 제2장: 중개서비스 제공자의 책임 면제

(제3조, 단순전달자) ① 전송을 시작하지 않은 경우, ② 수신자를 선택하지 않은 경우, ③ 전송에 포함된 정보를 선택하거나 수정하지 않은 경우에 전송된 정보에 대한 책임 면제

(제4조, 캐싱) ① 정보를 수정하지 않은 경우, ② 정보에 대한 접근 조건을 준수한 경우, ③ 업계의 보편적인 방식으로 정보 업데이트 규칙을 준수한 경우 정보의 일시적 자동 저장에 대해 책임 면제

(제5조, 호스팅) ① 불법 행위·콘텐츠를 실제로 인지하지 못하고, ② 손해 배상 청구와 관련하여 불법 행위·콘텐츠가 명백한 사실관계 또는 정황을 인지하지 못한 경우, ③인지한 즉시 불법 콘텐츠를 삭제하거나 접근을 차단하기 위해 노력한 경우에 책임 면제

(제6조, 자율적인 조사 및 법 준수) 자발적으로 불법 콘텐츠의 탐지·식별·삭제·접근 차단을 위해 조사 및 활동을 수행하거나 EU법을 준수하기 위해 필요한 조치를 취한 것만으로 제3조~제5조에 따른 면책이 적용되지 않는 것으로 간주되지 않음

(제7조, 일반적 모니터링 또는 적극적 사실 확인 의무 부존재) 중개서비스 제공자가 정보를 모니터링할 일반적 의무 또는 불법행위를 암시하는 사실관계나 상황을 적극적으로 찾아야 할 의무는 없음

(제8조, 불법 콘텐츠에 대한 조치 명령) 사법기관 또는 행정당국 으로부터 특정 불법 콘텐츠에 대해 조치를 취할 것을 명령받으면 지체없이 조치를 취하고 취한 조치 및 조치를 취한 시각을 보고

- 명령의 요건 : ① 위반한 법조문, URL, 중개서비스 제공자와 해당 콘텐츠를 제공한 이용자에 대한 구제절차를 포함한 명령문 ② 명령의 지리적 범위가 그 목적을 달성하기 위해 필요한 정도를 초과하지 않을 것 ③ 중개서비스 제공자가 신고한 언어로 작성되고 지정한 컨택트 포인트에 전달될 것

(제9조, 정보제공 명령) 규제당국은 서비스 제공자에게 이용자에 관한 정보제공을 명령할 수 있음

- 명령문에는 정보가 요청되는 목적, 정보 요청이 이용자의 규정 준수여부를 판단하기 위해 필요하고 비례적이라는 점, 서비스 제공자와 해당 이용자가 이용할 수 있는 구제절차에 대한 정보가 포함되어야 함

출처: 김현수, 전성호 (2020).

○ (미준수 조치사항) 사업자 규모에 따라 조치사항을 차등적으로 적용함

- 대규모 온라인 플랫폼이 규정을 미준수하는 경우(제58조) 집행위원회는 '규정 미준수(non-compliance)' 결정을 내릴 수 있음
- 제58조의 규정미준수 결정을 결정을 받으면, 제59조에 따라 집행위원회는 대규모 온라인 플랫폼에 과징금을 부과할 수 있고, 이는 전년도 전체 매출액의 6%를 넘지 않는 수준에서

결정됨

- 이외에도, 당 플랫폼이 제52조에 해당하는 요청에 대해 정보 제공을 성실히 하지 않는 경우 등에 한해서도 전년도 전체 매출액의 1% 미만의 과징금 부과가 가능함
- 제60조에 따른 이행 강제금은 ① 제52조 정보제공, ②제54조 현장조사, ③제55조제1항 임시조치, ④제56조제1항 구속력 있는 시정안 준수를 위한 강제금으로, 이행강제검을 정기적으로 부과할 수 있고, 이는 전년도 일평균 매출액의 5% 미만으로 부과되도록 규정하고 있음

다. 영국

○ (법적 근거) 인터넷 특화 규제가 없는 대신 ISP의 이용약관의 적용이나 경찰-ISP-저작권자-관련부처 간의 자발적인 협력, 또는 ISP/DNS-사적 규제기관 간 파트너십에 근거를 둔 사적 규제를 적용하고 있음

- 일반적으로 저작권, 명예 훼손 및 테러 활동을 다루는 의회 법 및 2차 입법[10]에는 ISP가 온라인 자료를 삭제하는 것과 관련된 일부 조항이 포함되어 있으며, 이에 따라 잉글랜드, 웨일즈 지역에서는 고등법원(High Court)이 명예훼손과 저작권 침해에 대해 ISP에게 삭제/차단 명령을 내릴 수 있음
- 테러 법과 기타 명예 훼손 법의 다른 조항들은 통지 및 게시 중단 규칙에 따라 행동하는 ISP에 대한 책임이 면제됨

---

10) 영국 제정법률은 크게 의회에서 제정되는 법인 1차 입법(Primary Legislation)과 Codes, Orders, Regulations, Rules 등이 해당하는 하위 또는 위임입법인 2차 입법(Secondary Legislation, Statutory Instruments)으로 나뉜다. 1차 법률은 다시 UK의회에서 통과된 Public General Acts와 특정 지역, 단체 또는 개인에게만 적용되는 소수의 Private Acts(Local and Personal Acts)로 구분된다. UK의회에서 통과된 Public General Acts는 영국 전역(잉글랜드, 웨일스, 스코틀랜드, 북아일랜드)에 적용된다. 그러나 스코틀랜드, 웨일스, 북아일랜드도 또한 위임된 사항에 관련해서는 독자적인 법률과 법체계를 갖는다. 2차 법률은 1차 법률의 세부적인 내용을 규율하기 위하여 의회법으로 주어진 권한에 따라 장관이나 기타 기관에서 제정한다. 영국 정부가 체결한 국제조약은 자동적으로 국내법이 되는 것이 아니라 의회의 비준과 동의를 얻어 국내법으로 편입되는 이원론이 적용된다.

- 사이버 범죄에 관한 유럽 평의회 협약은 2011년 5월 영국에 의해 비준되었지만, 영국 정부가 이미 충족한 절차적 요구 사항을 포함하여 기존의 국내 입법 조항을 통해 영국 정부가 대부분의 요구 사항을 충족한 상황
- 테러 예방 협약 및 성 착취 및 성 학대에 대한 아동 보호 협약과 같은 다른 유럽 협의회 협약에 서명을 했으나 아직 영국 정부에 의해 비준되지 않음

○ (규제 기관) 영국은 민간기구인 IWF(Internet Watch Foundation)을 주축으로 불법정보의 신고 접수 및 삭제 조치를 시행하고 있음
- IWF는 잠재적으로 불법적인 콘텐츠가 영국에서 호스팅 되는 경우 ISP 및 영국 법 집행기관과 협력하여 콘텐츠를 삭제하고 필요한 경우 콘텐츠 제작자(또는 배포자)의 처벌이 가능하도록 지원하는 단체

○ (IWF 연혁) 1996년 불법아동성착취 제작 콘텐츠 사건에서 촉발된 '안전한 네트워크 재단'을 시초로 하여, 현재의 '인터넷 감시재단(Internet Watch Foundation: IWF)'로 명칭을 변경하여 이어짐
- 1996년, 영국 런던 경찰청은 '인터넷 서비스 제공자 협회'(Internet Service Providers Association)에게 일부 유즈넷뉴스그룹의 콘텐츠가 불법아동성착취로 제작된 자료임을 통보하고, 조사로 수집된 132개의 사이트에 접속을 제한할 것을 공개적으로 요청
- 해당 사건에 대해 콘텐츠 검열이라는 비난 여론이 있었으나, 런던 경찰청이 강력한 법적 행동에 나서며 ISPA와 런던경찰, 영국내무부 및 경제·산업부 및 일부ISP가 참여하여 유사 사건의 재발 방지를 마련하기 위한 해결책으로 'R3 안전한 네트워크 협약(R3 Safety Net Agreement)을 체결, '안전한 네트워크 재단'(Safety net Foundation)의 운영기조를 마련
- 현재는 영국뿐만 아니라 '인호프(INHOPE)'로 불리는 네트워크를 통해 해외 41여개 국가와 협력으로 불법아동성착취물에 대한 접근차단활동을 진행함

○ (협력 체계) 영국은 아동성착취물 등의 유통 방지 및 자율규제를 위해 영국내의 각계부처와 시민단체 뿐만 아니라, 유럽평의회, 유엔 등 국제적 협력 시스템을 구축함

- 영국정부와는 내무부, 디지털·문화·미디어 및 스포츠부, 법무부, 교육부 등과 협력하며, 영국의회에서는 온라인아동성착취에 대한 전문단체로서 활동함
- 유럽평의회와 유엔, 기타 온라인 거버넌스 기관과 협력하여 활동하는 국제적 협력 시스템을 갖춤

※ 이외에도 유럽연합은 영국의 온라인 어린이 보호기관 '영국의 더 안전한 인터넷을 위한 센터'(UK Safer Internet Center)에 운영기금을 지원하는데, IWF는 이 센터의 일환이자 온라인 안전 프로그램 운영 측면에서 10%의 기금을 지원받고 있음(IWF는 2004년 비영리회사에서 자선단체로 전환)

○ (회원사) IWF의 회원사는 140개 이상으로('20년 기준)

- IWF는 회원사에게서 연간 멤버십 요금을 받고 있으며, 사업자의 사업 영역 및 회사 규모에 따라 1,110 파운드~82,810 파운드(약 164만원~1억 2천만원[11])으로 책정됨

<표 3-20> IWF 회원사 중 납부 멤버십 비용 규모별 예시 (2020년 기준)

£81,185+	£54,125+	£27,060+	£21,660+	£16,245+
Amazon	Atlassian	Avast	Barracuda	Adobe
Apple	CA Inc	BAE Systems	Networks Ltd	Allot
Aspiegel Ltd	(Symantec)	Applied	Sandvine	BlackBerry
New BT	McAfee	Intelligence	SonicWall	Jagex
Cisco	Palo Alto	Ltd	Stackpath LLC	NetSTAR ALSI
Facebook	PayPal	Coinbase	the FA	Zoom
Google	Safaricom	Dropbox	Watchguard	
Microsoft	Tata	Forcepoint	Technology	
MTN	Communicatio-	ship	Inc.	
Sky	ns	Fortinet	Webroot	
TalkTalk	Trend Micro	Hutchison 3G	Zscaler Inc.	
Telefonica	Verizon Media	UK Ltd (Three		
Tik Tok		UK)		
Verisign		LINX ship		
Virgin Media		Roblox		
Vodafone		Snap		

11) 원화-파운드 환율 약 1481원 적용(2020년 12월 1일 기준)

		Sophos The Walt Disney Company Twitter Yandex		

출처: IWF 홈페이지.

○ (운영 목표) '온라인에서의 불법 아동성착취 콘텐츠 제거'를 운영 기조로 활동

- 이와 같은 운영 기조에 따른 세부 목표는 아래 4가지로 구성됨

① 온라인에서 불법아동성착취 이미지의 제거

② 불법아동성착취 이미지 삭제를 통한 피해자 구제

③ 모든 사람이 이용할 수 있는 온라인 환경 조성

④ 회원사들의 서비스와 브랜드의 가치 보호 등

○ (활동 내용) IWF의 활동은 불법 콘텐츠에 대한 식별과 삭제 조치부터 국제 협력과 전문 지식 공유까지 이어지는 불법 콘텐츠 유통 방지를 통한 자율규제로 이루어짐

- 주요 활동은 아래 다섯가지로 이루어짐

① 불법 아동성착취 이미지의 식별, 평가, 신고, 삭제

② 익명의 핫라인 제공

③ 공개온라인에서 불법 아동성착취 이미지와 동영상 검색

④ 전 세계의 협력사와 공동으로 불법 아동성착취 이미지를 제거, 확산 저지

⑤ 전문지식 공유

- 자체 검색과 신고접수, 협력사의 신고 등으로 수집된 불법아동성착취 콘텐츠들은 IWF 내부 전문가들을 통해 개별적으로 평가되고, 콘텐츠가 공유되는 사이트를 추적한 후 관련 지역기관, 경찰에 위치정보를 제공하거나 불법콘텐츠가 유통되는 ISP에 통보하여 내부 조치를 취할 수 있도록 지원함

○ (평가 기준) 영국을 포함한 전세계 기준과 영국을 제외한 해외 호스팅콘텐츠의 두 가지 수준에서 평가를 실시하고 있음

- ① 전 세계 기준

  ▸ 수집된 콘텐츠의 불법 여부 판단 기준은 영국의 국내법 기준에 따르고 있으며, 이는 '1978년의 아동보호법'(Protection of Children Act 1978, 잉글랜드와 웨일즈), '1982년의 시민정부법'(Civic Government Act, 1982, 스코틀랜드), '2003년의 성범죄 법'(Sexual Offences Act 2003. 잉글랜드와 웨일즈), '2006년의 경찰 및 사법'(Police and Justice Act 2006), '2008년의 형법 및 이민법'(Criminal Justice and Immigration Act 2008) 등에 따름

  ▸ 불법아동성착취 콘텐츠와 관련하여 모든 규정의 근간이 되는 아동보호법은 '배포하거나 보여주기 위한 목적으로 아동의 음란한 사진이나 이와 유사한 이미지를 만든 행위'를 범죄로 규정하고 있으며, 여타 법률의 경우 세부 내용을 다루고 있음

  ▸ 특히 영국 내 콘텐츠의 경우 '1988년의 형법'(The Criminal Justice Act of 1988)에서는 불법아동성착취 콘텐츠 소유 자체를 위법행위로 정하고 있기 때문에 영국 내 ISP들은 관련 규정을 더 엄격한 적용을 받음

<표 3-21> IWF의 불법아동성착취물 구분에 적용기준

법령	내용
1978년의 아동보호법	· 아동의 음란한 사진이나 의사(pseudo)사진의 제작, 배포, 광고게시 · 16세 미만 기혼자의 경우 사진표시 제한(배우자, 배포금지 등)
1982년의 시민정부법	· 18세 미만 아동의 음란한 사진 또는 의사(pseudo)사진의 제작과 배포, 소유, 의향이 있음을 알리는 광고의 게시, 18세미만 아동의 음란한 사진 또는 의사(pseudo)사진 소유에 대한 범죄규정(제52A)
2003년의 성범죄 법	· 아동연령변경(16세→18세)
2006년의 경찰 및 사법	· 압수된 불법아동성착취물의 몰수권
2008년의 형법 및 이민법	· 사진뿐만 아니라 아동을 성적대상으로 표현한 콘텐츠도 포함(예술작품 제외)

출처: IWF 홈페이지.

  ▸ IWF는 콘텐츠 분석에 영국 양형위원회(Sentencing Council)의 '성범죄 결정 가이드라인(Sexual Offences Definitive Guideline)'의 '아동의 음란한 사진(The Indecent Photographs of Children)'을 참조하여 직접 평가를 실시

※ 성범죄 가이드라인의 불법아동성착취 콘텐츠 내용을 ① A등급: 아동/동물/가학적 성행위로 성적 접촉이 포함된 것 ② B등급: 성적접촉이 없는 것 ③ C등급: 성적접촉과 관련 없는 다른 음란한 부분 등 세 가지로 구분

- ② 전 세계 기준+영국 내 적용 추가 기준
  - ▸ '사진이 아닌 아동성적학대 이미지'(non-photographic child sexual abuse imagery)[12]도 불법유해정보에 포함
  - ▸ '1959년 음란물출판법'(Obscene Publications Act 1959)에 따라 허용되지 않는 서비스에 콘텐츠를 공유 또는 배포했을 경우에만 적용되며 ① 시각적 콘텐츠가 음란물이고 ② 심하게 모욕적, 혐오감 조성, 외설적인 인물묘사일 경우 ③ 아동의 신체주요부위에 초점을 맞추거나 기타행위(아동과 성관계, 아동참여 자위행위 등의 성적학대 및 직접적인 가해 등)를 묘사하는 경우 음란물로 규정
  - ▸ 이 개념은 영국을 포함한 소수의 국가들에서만 적용되므로 IWF는 관련 자료를 수집하여 영국 내와 해외사건으로 이를 분류하고, 영국 내에서 발생한 사건들에 대해서만 조치를 취하고 있음
  - ▸ 이 과정에서 IWF는 조사과정에 참여하는 것이 아니라 콘텐츠 내용을 영국경찰에 알리고, ISP 업체들에게 이를 제거할 것을 알리는 역할만 수행함

○ (불법 콘텐츠 조치) 불법 콘텐츠에 대해 기술적 조치와 비기술적 조치를 혼합 시행하고 있으며, 기술적 조치는 콘텐츠 차단을, 비기술적 조치는 사업자 및 국제기구 협조를 주 내용으로 함

○ (기술적 조치) 온라인 콘텐츠 차단을 위한 기술적 조치로 해시 차단, 통보조치, URL 및 키워드 목록 제공 조치를 실시하고 있음

① IWF 해시(Hash) : IWF가 발견한 불법아동성착취 이미지와 비디오는 일종의 디지털 지문(Microsoft PhotoDNA사용)인 고유코드(해시)로 변환하는 방식으로, 해당 데이터가 업로드되면 콘텐츠 업로드, 공유, 호스팅 등의 활동이 중단됨

② 게시 중단 알림(Take down Notices): ISP 업체의 서버에 불법콘텐츠가 업로드되면 관련 IWF는 관련 정보를 바로 해당 업체에 이를 통보 조치함. 게시 중단 알림은 온라인 상에서 불법아동성착취물 콘텐츠 제거 뿐만 아니라 정보를 보존토록 하여 향후 조사를 위한 자료로 활용하기 위한 목적으로도 이용됨

12) 만화 또는 컴퓨터 제작 이미지(cartoon or computer generated image)

※ 해당 서비스는 회원사를 대상으로 실시하고 있는데, 비회원사가 점차 늘어난다는 한계도 존재함 ('19년 영국 내에서 접수된 불법아동성착취 콘텐츠와 관련한 ISP는 21개였으나, 이 중 IWF의 회원사는 2개에 불과하였음)

③ URL 목록(URL list) : 불법아동성착취 콘텐츠가 게시된 웹페이지 목록을 제공 사업으로, 회원사들과 영국정부부서, 공공와이파이 등에서 인터넷을 이용할 때 URL목록에 있는 웹페이지 접속 및 정보습득을 자동으로 차단하는 방식

※ 역시 회원사들을 대상으로 제공되기 때문에 비회원 ISP의 경우 통제나 접속제한이 불가능

④ 키워드 목록 (Keyword list): 특별검색단어들에 대한 필터링을 위한 목록을 제공하여, 검색엔진뿐만 아니라 게임 및 소셜미디어 플랫폼의 대화 필터링, 조사 중인 파일 및 도메인 확인 등의 과정에 적용

○ (비기술적 조치) 사업자 및 국제기구 협조를 통한 서비스 차단 등으로, 도메인 서비스 통보, 콘텐츠 구매 불가 조치, 국제 공조를 통한 접근 제한 절차 및 수사 지원이 포함됨

- 합법적인 도메인 서비스에서 호스팅 되는 불법아동성착취물 서비스를 파악하여 도메인 서비스에 통보하여 이를 폐쇄하도록 함
- 불법아동성착취물 콘텐츠 구매를 불가능하게 하도록 가상화폐 및 결제서비스에 관련 정보를 제공하여 구매를 제한함
- IWF는 국제 불법아동성착취 콘텐츠 활동기관인 INHOPE와 협력으로 회원국 내의 ISP에서 불법콘텐츠가 발견되면 절차에 따라 접근제한절차를 실시함

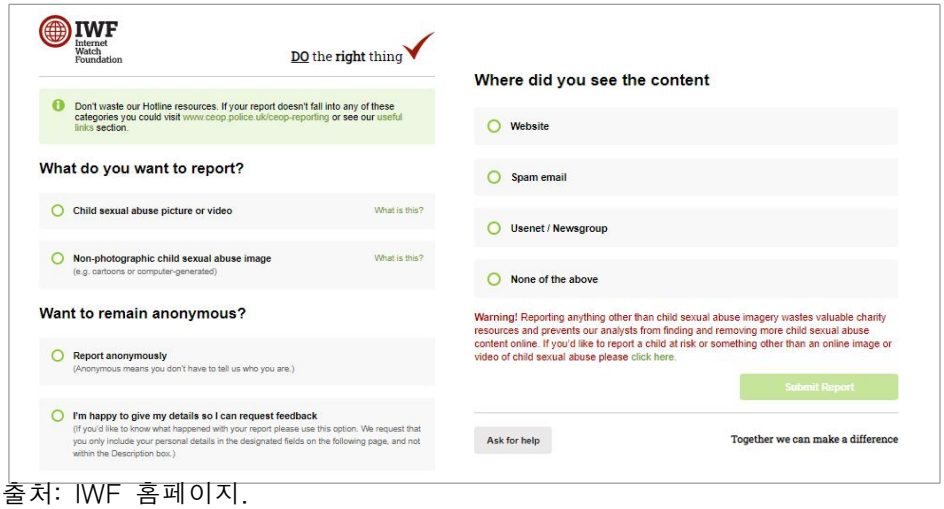
※ 미국의 ISP에서 발견되는 경우 미국의 민간 비영리단체인 '실종 및 아동학대센터'(The National Center for Missing & Exploited Children, NCMEC)에 통지하고, 동시에 즉각적인 경고조치(Simultaneous Alerts)를 내림

※ IWF와 협력을 맺지 않은 국가들의 ISP에서 불법아동성착취 콘텐츠가 발견되는 경우엔 그 사례를 영국범죄국(National Crime Agency)에 제공하여 인터폴에서 공식적으로 수사할 수 있도록 조치를 취함

○ (조치 절차) IWF는 불법 콘텐츠에 대한 절차는 4개 단계로 이루어지며, 이는 접수(Report), 평가(Assessment), 분석(Analysis), IWF 조치방식으로 이루어짐

- ① 접수(Report)는 자체 검색, 대중신고접수, 경찰접수, 회원접수 등의 채널로 이루어지며, IWF의 자체 검색이 전체 접수의 절반 이상을 차지('19년 기준, 56.62%)(IWF, 2020)

[그림 3-1] IWF 불법콘텐츠 신고 화면



출처: IWF 홈페이지.

- ② 평가(Assessment)에서 (1) 이 콘텐츠가 아동을 성적으로 학대하는 사진이나 비디오인지 (2) 영국 법에 저촉되는지 (3) 어떤 유형의 학대에 포함되는지 (4) 영국 내에서 호스팅 된 사진이 아닌 아동을 성적으로 학대하는 이미지 또는 동영상인지(그래픽, 그림 등)를 기준으로 분류

  ▸ 평가에서 혐의가 없는 콘텐츠에 대해 (1) 접수자에게 관련 근거에 대한 정보와 판단규칙에 대한 정보를 제공하거나 (2) 다른 서비스에 해당 사안이 회부될 수 있는지에 대한 정보를 제공한 후 사건을 종료하고, 반대로 평가에서 혐의가 발생했을 경우엔 어떤 위반인지에 대해서 더 조사하고 처리방향을 결정

③ 분석(Analysis)은 해당 사건이 어느 지역에서 발생했는가에 대해 조사하며, 불법으로 판정된 사례를 처리하기 위한 방법을 선택하기 위함으로서 사건이 발생한 장소(영국 내/영국 외를 구분)에 따라 처리방식을 결정함

④ IWF의 조치방식은 3단계 분석을 거쳐 영국 자국 내와 국제 사건 구분에 따라 다음과 같은 절차를 거침

  ▸ 자국의 사건으로 분류된 경우 (1) 조사 및 허가를 위해 영국범죄국과 지역경찰대(Regional

Police Force)에 공지 → (2) 호스팅업체(ISP)에 증거보존과 콘텐츠제거 공지 → (3) 수집·등급·해시코드처리 된 이미지를 CAID(Child Abuse Image Database)에 추가→ (4) 웹페이지에 콘텐츠가 삭제될 때까지 감시, 삭제조치 후 사건을 종료함

▸ 국제적으로 발생한 사건은 협력으로 조치하여 (1) INHOPE/국제핫라인/관련기관에 보고→ (2) 수집·등급·해시코드처리 된 이미지를 CAID에 등록→ (3) 콘텐츠가 제거되기 이전까지 해당사이트에 접근하지 못하도록 IWF의 접근금지 목록에 추가→ (4) 웹페이지에 콘텐츠가 삭제될 때까지 감시, 처리되었어야 할 콘텐츠에 대한 IWF팀의 직접 추적→ (5) 콘텐츠가 제거된 경우 IWF의 접근금지 목록에서 제외함

라. 프랑스

○ (자율규제 현황) 프랑스는 정부의 법률적 승인에 의해 자율규제기구인 FDI[13]를 만들고 정부가 콘텐츠 규제의 일부 권한을 법률에 의거하여 위임하는 부분위임자율규제의 대표적인 사례(김유향, 2018, 황용석 외, 2009)로 국내에 알려져 있으나, 사실은 2011년에 정부의 재정지원이 끊겨 FDI가 해산결정을 내린 이후 활동을 하고 있지 않음

- 현재는 인터넷 제공협회(L'Association Francaisedes Prestataires de l'Internet, AFPI)와 민관 협치형 기구인 인터넷권리포럼(Forum des Droit sur L'internet, FDI)이 신고사이트(Point de Contact.net)를 통해 불법정보를 익명으로 신고하면 차단하는 형태 수준의 자율규제를 시행하고 있음(최진응, 2017)
- FDI는 ①인터넷과 관련하여 정부에 입법규제권고안을 제출하는 자문기관의 역할, ② 일반 인터넷 이용자에게 관련정보를 제공하는 역할, ③ 인터넷이용자와 기업간의 분쟁을 중재하는 역할 등을 수행했으나, 정부의 재정보조가 끊기면서 해산함

마. 독일

(1) FSM(Freiwillige Selbstkontrolle Multimedia-Diensteanbieter)

○ (법적 근거) 독일의 청소년 유해 콘텐츠와 관련한 법령은 '청소년보호법'

13) 국가의 재정보조를 받는 협치기구로써, 정부재정보조가 약 80%에 달했기 때문에 2011년 재정보조가 중단되며 해산함

(Jugendschutzgesetz: JuSchG)과 '청소년미디어보호주간협약'(Jugendmedienschutz-Staatsvertrag, JMStV)을 기준으로 함

- 청소년보호법(JuSchG)은 휴대용미디어에 관한 콘텐츠를 규제한다면 청소년미디어보호주간협약(JMStV)은 텔레미디어(전자미디어, Telemedien)에 대한 조항들로 구성
- 이 외에도 미디어주간협약과 형법 등을 통해서 미디어사업자들에게 청소년 미디어보호를 위한 조치를 취하도록 명하고 있지만 일반적으로 청소년미디어보호 정책을 다룰 땐 JMStV를 근거로 함

○ (FSM 설립 근거) FSM은 청소년미디어보호주간협약(JMStV) 제19조에 따라 자율규제기관으로 설립됨

- 2003년 청소년미디어보호주간협약(JMStV)는 방송매체와 텔레미디어로 제공되는 유해정보로부터 어린이와 청소년을 보호하기 위한 목적으로 신설되었으며, 제19조(19, 19a, 19b)에 따라 방송 및 미디어분야에서 자율규제기관의 설립과 역할을 명시
- 청소년미디어보호주간협약(JMStV)의 제19조는 '자율규제기관' (Einrichtun-gen der Freiwilligen Selbstkontrolle) 조항으로서 방송 및 텔레미디어서비스사업자들의 자율규제기관 설립을 허용

  ※ 자율규제기관 인증 요건: 조직구성에 있어 ① 청소년보호분야 사회단체의 대표인 등이 참여하는 등의 감사인(Prüfer)의 독립성과 전문성이 보장되고 ② 여러 사업자들이 참여하여 기관운영에 필요한 자재를 제공해야하고 ③ 감사인의 결정에 관한 지침이 어린이와 청소년 보호를 위한 효과적인 보장을 근거로 하고 ④ 주 정부에서 법적으로 운영되는 청소년기관의 요청에 따라 자율규제기관의 결정을 검토할 수 있는 요구조건들에 대한 가능성과 절차규칙을 갖고 있으며 ⑤ 결정 이전 관련 사업자의 의견청취 과정보장, 서면으로 결정내용 전달 등을 거치며 ⑥ 불만접수처리창구를 운영하는 등의 기본 조건을 충족해야 함

- 각 주의 미디어청(Medienanstalten)은 청소년미디어보호위원회(Kommission für Jugend mediens-chutz: KJM)를 통해 자율규제기관의 결정에 대한 결정철회, 의무이행요구도 가능하다(제19b조)

○ (업무내용) FSM('멀티미디어사업자들의 자율규제 협회'Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V: FSM)은 정관에 따라 멀티미디어분야에서 소비자보호와 청소년보호, 청소년의 교육 및 양육을 촉진하는 것을 목표로 조직된 자율규제기관

- 주요 활동 내용으로는 ① 협회의 활동을 텔레미디어 사업자들과 대중에게 홍보하고 ② 회원들을 위한 이익단체로서 독일 내와 국제기관에서 활동하며 ③ 회원사들의 FSM-행동규칙(FSM-Verhaltenkodexes) 준수를 지원하고 조언을 제공하는 등의 활동이 있음
- 법령위반이나 불만접수와 관련하여 FSM은 규제기관인 KJM과 회원사 중간에서 활동하는 일종의 중간단체로서 청소년보호 관련 위반이 발생했을 시 사안처리 및 처벌근거를 KJM에 전달하고 조절하는 역할을 수행하지만, FSM을 통한 불만처리가 법적조치를 대체하는 것은 아님
- 즉, JMStV의 제20조에 따라 KJM은 FSM의 정회원인 텔레미디어 사업자가 청소년미디어보호 위반사항을 발견하게 되더라도, 위반에 대한 판단은 FSM의 위원회에 우선 회부시키며, FSM이 조치가 결정되지 않거나 제재내용이 자체규정의 범주를 벗어나 공법위반에 해당하는 경우엔 KJM이 직접 처벌기준을 마련하게 되는 방식
- 그렇기 때문에 FSM의 회원이 아닐 경우엔 중재자가 존재하지 않기에 더 강한 처벌의 가능성도 있음

○ (FSM-행동규칙준수) FSM은 회원사들에 FSM-행동규칙을 제정하고 회원사들에 이를 준수할 것을 요구하고 있으며, 해당 규정의 미준수는 탈퇴 조치로 이어짐

- 회원사들이 자사의 콘텐츠와 연령 제한을 변경하는 경우, 회원사들은 그 내용을 FSM 측에 제출한 후에 행동규칙 위배 여부를 평가받음 (FSM, 2018)
- 회원사 중에서 행동규칙을 여러 차례 위반하거나, 행동규칙 위반에 따라 법적으로 2만 유로 이상의 벌금처벌을 받았을 경우엔 더 이상 회원으로서 활동하지 못함
- FSM-행동규칙은 JMStV와 기타 관련법들에서 근거하는 청소년미디어보호 기준에 준하고 있으며, 해당내용은 FSM의 접수된 불만을 처리하기 위한 평가기준해설인 'FSM의 평가기본규칙'(Prüfgrundsätze der FSM) 및 실제 적용기준인 'FSM의 평가가이드라인' (Prüfrichtlinie der Freiwilligen Selbstkontrolle Multimedia- Diensteanbieter)과 동일한 기준을 적용

- FSM-행동규칙은 3개의 장, 13개의 항목으로 구성된 내부규칙으로서 기본적으로 JMStV에서 구분하는 온라인 콘텐츠분류기준을 따르고 있음

<표 3-22> FSM-행동규칙 항목별 주요내용

항목		주요내용
1	적용범위	· FSM회원가입과 동시에 행동규칙을 준수해야 함.
2	불법아동성착취 콘텐츠와 에로토그래피(erotografie)금지	· 불법아동성착취 콘텐츠 금지 · 에로토그래피(성적목적으로 제작된 그래픽) 금지. · 발견 시 즉각적으로 담당관정에 신고.
3	절대적 불법콘텐츠	· JMStV외의 기타 법률에서 금지하는 표현이 담긴 콘텐츠 유포 금지.
4	상대적으로 허용되지 않는 콘텐츠	· 성인콘텐츠에 대한 접근 연령제한조치.
5	성장에 영향을 미치는 콘텐츠	· 연령표시에 따라 연령 별 선택적 콘텐츠 접근허용조치.
6	광고	· JMStV 제6조에 따라 미성년자를 현혹시키는 광고방식 금지. · 주류광고/ 식단에 부정적 영향을 미치는 광고금지 · 콘텐츠 위에 표시되는 광고방식 금지.
7	저널리즘-편집 콘텐츠	· 정보전달에 있어서 저널리즘-편집원칙 준수. · 정보 확인, 사실과 의견분리원칙, 여론조사의 명확한 표기.
8	청소년보호 소프트웨어와 기술적 수단	· FSM의 청소년보호 소프트웨어와 기술적 수단의 홍보. · 청소년보호 소프트웨어와 기술적 수단에 대한 정기적 적합성 평가(3년)
9	연령분류등급표시	· JMStV 제9조에 따른 연령표시의무. · 텍스트, 이미지, 영화, 게임 등 모든 유형의 콘텐츠에 해당.
10	사업자표시, 청소년미디어보호담당자표시*	· FSM 회원표시의무. · JMStV 제7조에 따라 청소년미디어보호담당자 관련 필수정보표시.
11	미디어능력프로젝트 지원	· 부모와 청소년 대상 미디어능력프로젝트 촉진.
12	정보청구	· 접수된 불만에 대해 FSM회원들의 정보접근 자유보장
13	콘텐츠 검토의무	· 청소년미디어보호담당자가 없는 회원사 콘텐츠에 대한 예비검사 시행.

출처: FSM, 2016.

※ JMStV 제7조에 따라 라이선스발급대상 방송사업자, 무료상업방송사업자, 청소년유해콘텐츠가 포함된 텔레미디어 및 검색엔진사업자는 자사에 청소년미디어보호 관련 전문지식을 갖춘 독립권한의 청소년보호담당자를 임명해야 함. 소규모 기업(월평균 1천만 건 이하 이용, 직원 50명 이하, 지역방송 등)은 자율규제기관이 청소년보호담당자를 대신할 수 있음.

○ (평가 가이드라인) FSM 행동규칙의 내용을 기반으로 FSM의 불만처리위원회(Beschwerdeausschuss)가 접수 불만에 대해 처리하는 '평가 가이드라인'에 의거하여 각 항목에 대한 검토사항을 마련함

- 가이드라인의 평가 대상은 제4조에서 규정되며 각 불법정보의 범주에 따른 조사 범위를 규정하고 있음

<표 3-23> FSM 불만처리위원회의 불만처리를 위한 텔레미디어서비스 평가단위

평가단위	주요내용
도메인 및 하위 디렉터리	· 불만신고 된 특정 온라인페이지를 중심으로 구성. · 불만이 전체 웹사이트에 관한 것이거나 웹 사이트의 특정상황을 해석하는데 중요할 경우 전체 도메인이 평가단위로 분류되어 심사를 받게 됨.
개별요소와 전체느낌	· 개별요소가 전체느낌에 미치는 상호작용을 고려하여 판단. · 개별요소에 초점을 맞출 경우 전체이미지를 왜곡할 수 있기 때문에 전체느낌을 고려.
광고, (특히) 배너	· 온라인에서 운영되는 모든 형태의 광고. · 광고서버에 의해 자동으로 웹사이트에 노출되는 광고에 대해 운영자는 광고에 관한 정보를 갖고 있어야 함.
팝업광고, 팝언더광고	· 웹사이트 접속에서 나타나는 팝업광고와 팝언더광고. · 제3자에 의한 광고노출일 때 광고가 노출된 웹사이트에 대한 정보가 있을 경우에만 광고 집행 가능.
브라우저에서 감지하지 못하는 코드	· HTML코드는 평가단위에 포함되지 않음.
링크: 첫 번째 링크 단계	· 원칙적으로 평가단위는 하이퍼링크를 선택하면 연결되는 콘텐츠까지 포함 가능함. · 하지만 제공자가 링크의 내용을 알고 있거나 특정 표시기준에 따라 링크를 통해 제공되는 콘텐츠의 확인의무가 존재할 경우에만 불법성판단이 가능함.
추가 링크 단계	· 두 번째 이상 링크된 웹페이지는 평가단위에 포함되지 않음. · 하지만 첫 번째 링크가 연령표기기준 대상이고, 이 링크가 두 번째 링크로 접속하기 위한 통로역할만 행하는 것이 확실한 경우

	평가단위에 포함 가능함.
링크된 콘텐츠와 거리두기	· 제공한 링크가 편집정보 또는 의견제공의 일부일 경우, 제공자가 구체적으로 링크된 정보와 거리를 두는 경우 평가단위로 포함되지 않음.
콘텐츠분리 위반	· 콘텐츠와 광고를 시각적으로 분리하지 않은 경우 링크를 통해 제공된 콘텐츠는 평가단위에 포함 가능함.
하이퍼링크가 없는 참조	· 평가단위에는 하이퍼링크로 텍스트형식으로만 참조하거나, 참조내용 없이 URL만 나열되어 있는 경우엔 포함되지 않음.

출처: FSM, 2013.

- 절대적인 불법 콘텐츠에 대한 불만사항은 FSM이나 KJM의 절차로 처리되지 않고, 관련 형법 및 기본법 위반 등으로 처리됨

○ 가이드라인 제3조에서는 제기된 불만사항에 대한 평가에 있어 불만처리위원회가 자율규제 기관으로서의 역할을 넘어서지 않기 위해 지침을 정하고 있음

- 지침은 ① 불만처리에 따른 행정절차오류는 허가되지 않고, ② 불만에 제기된 내용이 사실이라고 가정해야 하며, ③ 해석에 대한 해당 법률을 제시하여, ④ 일반적인 법률이나 JMStV의 평가기준에 따른 법령 및 지침을 위반하지 않도록 해야 하고, ⑤ 감사인이 불만처리와 관련 없는 요인들로 판결에 영향을 받아선 안 된다는 원칙으로 이루어짐

○ (자율규제기관) 자율규제 실시를 위한 규제기관의 조건을 부여하고, 이에 따라 인가를 내어주는 '자율규제 인가'를 명시하고 있으며 인가 요건과 인가 관청을 규정함

- 연방법무소비자부(BWJV)는 소셜미디어 플랫폼 사업자에게 자율규제기관으로서의 권한을 부여하여 유통되는 정보에 대한 조치 의무 및 권한을 부여
- JMStV 7조 1절은 청소년 보호를 위해 각 사업자[14]는 자사에 청소년보호담당자를 임명하도록 규정하고 있으며, 소규모 기업*의 경우 자율규제기관이 이 이를 대체할 수 있도록 함

* 월평균 이용건 1천만 건 이하, 직원 50명 이하, 지역방송 등

14) 라이선스발급대상 방송사업자, 무료방송사업자, 청소년유해콘텐츠가 포함된 텔레미디어 및 검색엔진사업자

- JMStV는 이러한 조항으로 소규모 사업자의 콘텐츠 관리 부담을 자율규제기관이 대신할 수 있도록 하였음. 특히 JMStV에서 규정하는 청소년보호담당자는 청소년미디어보호 관련 전문지식을 갖춰야 한다는 요건을 포함하기 때문
- 따라서 관련 사업자를 대상으로 청소년보호담당자를 지정하도록 하면서도 소규모 사업자에 대해 해당 지정 부담 및 업무 부담을 경감하고 있음

(2) 네트워크 시행법[15](NetzDG)

○ (개요) 소셜미디어의 가짜뉴스 유통을 방지하기 위한 목적으로, 사용자 200만명 이상의 소셜미디어 콘텐츠 서비스 제공자에 대한 콘텐츠 관리 의무를 둠
- '17년 10월 1일 시행된 네트워크 시행법(NetzDG, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken)은 소셜 미디어에서의 가짜뉴스를 방지하기 위한 목적으로 제정됨
- 네트워크 시행법은 독일 내의 사용자가 200만명 이상인 소셜 미디어에서는 콘텐츠의 불법성이 명백하게 드러날 경우 24시간 이내에 게시를 중단할 의무를 부여함
- 소셜미디어 사업자는 네트워크 시행법 제3조에 의거하여 불법콘텐츠에 관한 이용자의 불만을 처리하기 위해 행정당국이 위임한 기관이나 인증된 자율규제기관을 설립해야 하며, 관련 업무를 빠르게 진행해야 함
- 네트워크 시행법에서 명시하는 명백한 불법 콘텐츠는 21개의 형법을 위반하는 콘텐츠이며, 불법콘텐츠로 분류되는 경우 즉시 조치를 취해야 함

<표 3-24> Google의 독일 네트워크 시행법(NetzDG) 불법 정보 분류 기준

Google 분류	독일 형법 분류
증오심 표현 또는 정치 극단주의	▪ § 130 StGB: 증오 조장 ▪ § 166 StGB: 종교, 종교적 단체 및 이념 단체에 대한 명예 훼손
테러리스트 또는 위법 콘텐츠	▪ § 86 StGB: 위법 단체의 홍보 자료 배포 ▪ § 86a StGB: 위법 조직의 상징 사용

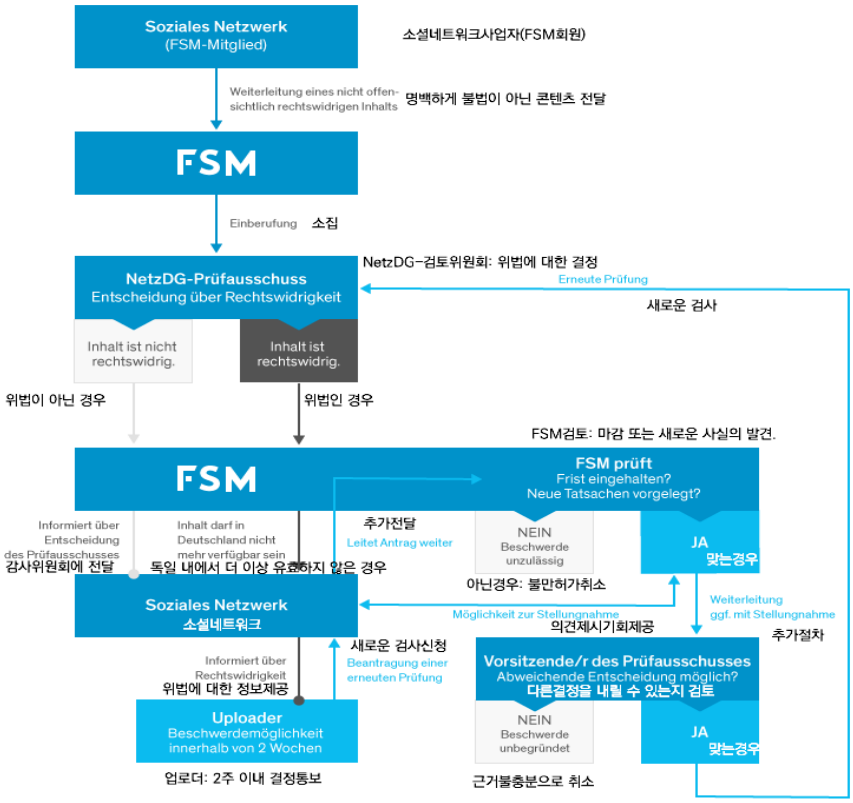
15) '네트워크 시행법' 또는 '망 집행법'으로 번역 (NetzDG, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken)

	▪ § 89a StGB: 국가를 위험에 빠뜨리는 심각한 폭력 범죄 준비 ▪ § 91 StGB: 국가를 위험에 빠뜨리는 심각한 폭력 범죄 조장 ▪ § 100a StGB: 위조 방조 ▪ § 129 StGB: 범죄 조직 형성 ▪ § 129a StGB: 테러리스트 조직 형성 ▪ § 129b StGB: 해외 범죄 및 테러리스트 조직 - 확장된 몰수 및 박탈 ▪ § 138 I StGB와 관련된 § 140 StGB: § 138 I StGB에 나열된 특정 범죄 행위에 대한 보상 및 인정 ▪ § 269 StGB: 증거 제공을 위한 데이터 위조
폭력	▪ § 131 StGB: 폭력적인 자료 유포
유해하거나 위험한 행위	▪ § 111 StGB: 공개적인 범죄 조장 ▪ § 126 StGB: 범죄 실행 위협으로 치안 방해 ▪ § 126 I StGB와 관련된 § 140 StGB: § 126 I StGB에 나열된 범죄 행위에 대한 보상 및 인정 ▪ § 241 StGB: 중죄 위원회 위협
명예 훼손 또는 모욕	▪ §185 StGB: 모욕 ▪ § 186 StGB: 명예 훼손 ▪ §187 StGB: 의도적인 명예 훼손
개인정보 보호	▪ § 201a StGB: 사진 촬영에 의한 사생활 침해
성적인 콘텐츠	▪ § 184d StGB: 방송, 미디어 서비스 또는 통신 서비스에 의한 음란물 배포와 관련된 § 184b StGB: 아동 음란물 배포, 습득 및 소지 ▪ §§ 176~178과 관련된 § 140: §§ 176~178에 나열된 특정 범죄 행위에 대한 보상 및 인정

○ (조치사항) 불법 콘텐츠에 대한 조치는 보고된 사항을 즉시 조사하여 삭제 또는 차단조치에 관한 결정을 내리는 것으로 불법성 정도에 따라 최대 24시간 이내 또는 7일 이내 조치되어야 함

- 명백하게 불법적인 콘텐츠는 24시간 이내에 차단 및 삭제조치를 해야하며, 일반적인 불법콘텐츠는 7일 이내에 삭제하거나 접근을 막아야 함

[그림 3-2] FSM의 소셜미디어 불만처리절차



출처: FSM 홈페이지

바. 일본

○ (개요) 일본은 세이퍼인터넷협회(SIA, Safer Internet Association)라는 사업자협회에 경찰청 위탁사업인 인터넷 핫라인(IHC)를 운영하여 온라인 상의 불법·유해정보에 대응하고 있음

- 2013년 설립되었으며, 가입 사업자로는 Yahoo! Japan, ALSI, PIT CREW, mixi, Amazon, CyberAgent 등
- 2016년부터 경찰청 위탁사업으로 인터넷핫라인(IHC)을 운영하며, 국제공조를 위한

INHOPE 가맹 회원으로 업무 협조를 시행하고 있음

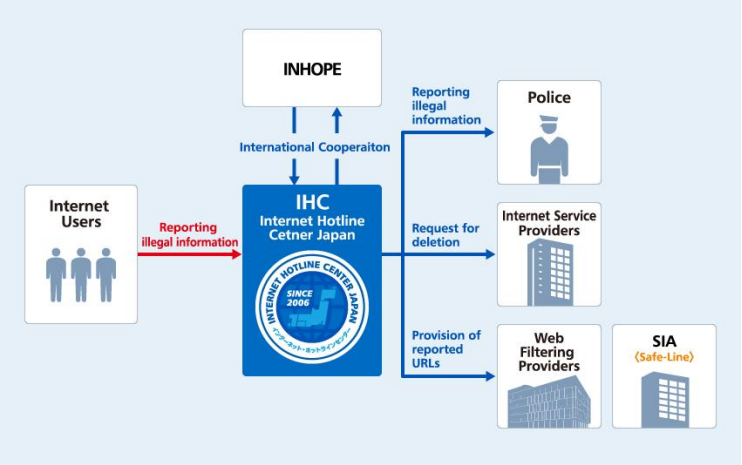
○ (인터넷핫라인센터) 일본의 인터넷핫라인센터(IHC)는 INHOPE의 회원으로 익명 제보를 받아 경찰에 수사 정보를 제공하거나 웹사이트 관리자나 ISP 등에 불법유해정보를 삭제할 것을 요청함

- 사단법인 '세이퍼인터넷협회'는 '16년 4월부터 경찰청에서 '인터넷 핫라인 센터' 운영 업무를 위탁받아 인터넷 불법정보와 관련한 신고 접수 및 게시판 관리자 등 콘텐츠 공급자에 삭제 요청을 실시하고 있음
- 처리하는 불법정보의 종류로는 음란정보, 아동 포르노, 성매매, 데이트 규제법 위반 금지 유인 행위, 마약범죄 또는 약물 남용, 규제약물, 지정약물 등 비허가 의약품 광고, 통장, 휴대전화 등의 무산 양도 권유·유인, 휴대전화식별부호입력 부정 행위, 부정 액세스 조장 행위 등
- 다만 운영 지침 중 명예 훼손, 비방, 살인 및 폭파 예고, 지적 재산권 침해 정보, 포르노 데이트 사이트 등 정보에 대해서는 처리하지 않음
- 해외 정보에 대해서는 외국 핫라인과 연계를 통해 정보의 대응하고 있으며 '20년 상반기에 해외 핫라인을 통해 처리한 불법정보는 통보 1,295건, 신고접수 343건

○ (처리 절차) 인터넷핫라인센터의 불법유해정보는 인터넷 이용자의 불법 정보 신고에 따라 경찰에 불법 정보 보고, ISP에 정보 삭제 요청, 웹 필터링 제공자 및 SIA(Safe-Line)에 해당 정보의 URL 제공으로 처리

- 해외 불법 정보의 경우 INHOPE와의 공조로 정보를 교환하고 있으며 일본 내에 유통되는 해외 정보에 대한 신고 및 처리를 요청

[그림 3-3] 일본 인터넷핫라인센터(IHC)의 불법유해정보 처리 절차



출처: IHC 홈페이지.

○ (프로바이더 책임제한법) 프로바이더[16] 권리 침해 정보에 대해 삭제 조치를 실시하거나, 실시하지 않은 경우 손해배상 책임 면책 요건을 규정한 법

- 2002년에 시행된 프로바이더책임제한법[17]은 프로바이더가 권리침해정보를 삭제하지 않거나 삭제했을 경우에 손해배상책임 면책요건을 규정함
- 해당 법안의 목적은 프로바이더의 책임을 명확히 하여 프로바이더의 자율적인 대응을 촉구하기 위한 것
- 프로바이더가 보유한 발신자 정보공개를 청구할 수 있는 권리도 규정하고 있다. ISP가 권리침해정보의 유통을 방치한 경우에는 부작위로 인한 책임을 물어야 할 가능성이 있으며, 반대로 권리침해라고 판단해 정보를 삭제한 경우에는 불법행위로 책임을 지게 됨
- 프로바이더 책임제한법에서는 ISP의 손해배상책임을 일정 정도 제한해 자율적으로 대응하도록 함
- '발신자 정보공개 청구권'을 통해 권리침해정보가 익명인 경우 피해자가 가해자를 특정해 손해배상을 청구할 수 있도록 프로바이더에게 기해자를 특정할 수 있는 정보공개를

16) 인터넷을 이용하여 서비스를 제공하는 사업자, OSP

17) 「특정전기통신역무제공자의 손해배상책임의 제한 및 발신자정보의 공개에 관한 법률」

청구할 권리를 규정

※ 시행령에 명시된 발신자 정보공개 대상이 되는 정보는 ①발신자 이름 또는 명칭, ②발신자 주소, ③발신자 메일주소, ④침해정보 관련 IP주소, ⑤휴대전화단말 등의 이용자식별부호, ⑥SIM카드 식별번호, ⑦타임스탬프(침해정보가 송신된 연월일 및 시각) 등

사. 시사점

○ 온라인 서비스를 제공하는 사업자의 자율규제를 활성화하기 위한 방안으로 (1) 플랫폼 사업자의 책임 범위와 한계를 명확히 명시, (2) 소규모 사업자의 의무 경감 지원, (3) 자율규제 기관의 권한 토대 마련을 제시할 수 있음

○ 플랫폼 사업자의 책임범위와 한계를 명시하여 자율적인 규제권한을 부여하는 방안에 대한 검토도 가능함

- 일부 국가에서는 불법정보 유통과 관련하여 플랫폼 사업자의 조치 의무가 부여되면서도 해당 사업자의 적극적 조치가 이루어지는 경우 일정정도의 면책 요건을 부여하는 방식으로 사업자들에게 자율규제에 대한 동기를 부여하고 있음
- EU의 디지털서비스법안은 대형 플랫폼 사업자에 대해 의무를 부여하고, 미준수 결정이 내려지면 과징금을 부여받을 수 있어 강화된 조치를 요구하는 동시에 면책요건을 설정하여 사업자의 자율규제 범위 및 책임에 대한 법적 명확성을 제공
- 일본 프로바이더책임제한법은 온라인 플랫폼 상의 정보로 발생한 피해에 대해 서비스 제공자에 손해배상을 청구하더라도, 해당 서비스 사업자가 정보 게시자에 대한 정보를 제공하는 등 피해자의 손해배상 절차에 대한 부담을 경감하는 경우 서비스 제공자의 책임을 면제하고 있음
- 면책조항은 이용자에 대한 침해를 발생시키거나 불법정보 유통방조에 악용될 소지도 있기 때문에 매우 조심스러운 검토가 필요하나, 사업자의 적극적인 자율규제 활동에 대한 동인을 부여하기 위해 면책의 범위를 확대하는 검토가 필요함

○ 소규모 사업자의 콘텐츠 관리 의무 위탁으로 콘텐츠 모니터링 및 관리 조치 인력이 충분하지 않은 사업자의 자율규제를 활성화 할 수 있음

- 독일은 콘텐츠 자율규제에 대한 기관 인가제를 통해 소규모 사업자에게 콘텐츠 관리 의무를 부여하면서도 인가 기관에 업무 위탁을 시행할 것을 권고
- 국내의 경우 정보통신망법 시행령 제25조를 통해 청소년보호책임자 지정의무자를 규정하고 있으나 일정 규모의 이용자 및 매출액 이상에 대해서만 규정하고 있기 때문에 소규모 사업의 경우 의무에서 제외됨
- 따라서 전체 온라인 서비스 사업자를 대상으로 일정 자격 이상의 청소년보호담당자를 지정하도록 하면서도 소규모 사업자에 대해 해당 지정 부담 및 업무 부담을 경감하는 독일 사례에서 시사점을 얻을 수 있음
- 영국의 IWF는 회원사에 대한 회원료 부담을 사업자 규모별로 설정하고 해당 금액 범위를 투명하게 공개하여 중소규모 사업자가 적정한 수준에서 부과할 수 있도록 함

○ 자율규제 활성화를 위한 기관 및 사업자의 권한 확대 필요성

- 영국, 독일 및 일본에서 불법 게시물에 대한 신고 및 삭제 책임을 자율규제기관 및 사이트 운영 기업에 부과하여 효율적인 콘텐츠 관리 기능 및 책무를 부여(손형섭, 2020)하고 있는데, 이는 이번 전기통신사업법 제22조의5 1항과 시행령 제30조의5의 개정으로 국내에서도 성폭력피해상담소, 한국여성인권진흥원, 그 밖에 방송통신위원회가 정하여 고시하는 기관 및 단체 등이 불법촬영물 등을 신고할 수 있는 법률적 근거가 마련됨

시행령 제30조의5(불법촬영물 등의 신고 및 삭제요청 등) ① 법 제22조의5제1항에서 "대통령령으로 정하는 기관·단체"란 다음 각 호의 기관·단체를 말한다.
1. 「성폭력방지 및 피해자보호 등에 관한 법률」 제10조제1항에 따른 성폭력피해상담소
2. 「양성평등기본법」 제46조의2제1항에 따른 한국여성인권진흥원
3. 그 밖에 국가 또는 특별시·광역시·특별자치시·도·특별자치도로부터 법 제22조의5제1항에 따른 불법촬영물등(이하 "불법촬영물등"이라 한다)의 삭제 지원 등에 관한 사업 수행에 필요한 비용을 보조받아 그 사업을 수행하는 기관·단체로서 방송통신위원회가 정하여 고시하는 기관·단체

② 법 제22조의5제1항에 따라 불법촬영물등의 신고 또는 삭제요청(이하 "신고·삭제요청"이라 한다)을 하려는 자는 별지 서식의 불법촬영물등 유통 신고·삭제요청서 또는 같은 서식의 내용이 포함되도록 작성한 문서를 조치의무사업자에게 제출해야 한다.

③ 조치의무사업자는 불법촬영물등으로 의심되는 정보에 대하여 신고·삭제요청을 받은 경우로서 해당 정보가 불법촬영물등에 해당하는지를 판단하기 어려운 경우에는 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조제1항에 따른 방송통신심의위원회(이하 "방송통신심의위원회"라 한다)에 심의를 요청할 수 있다.
④ 방송통신심의위원회는 제3항에 따른 심의 요청을 받은 경우 그 정보가 불법촬영물등에 해당하는지를 심의·의결한 후 심의를 요청한 조치의무사업자에게 그 결과를 통보해야 한다.
⑤ 조치의무사업자는 제4항에 따라 불법촬영물등에 해당한다는 통보를 받은 경우에는 지체 없이 법 제22조의5제1항에 따라 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취해야 한다.

- 민간영역의 자율성 확대를 위해서 각 콘텐츠 가이드라인의 제정을 자율규제기관이나 사업자 협회에서 규정하여 불법 여부에 대한 심사 기준 및 범위, 주체 등을 자체적으로 설정하고, 이 과정에서 소비자단체나 시민단체, 정부의 협력적 관계 구축을 통해 법률 준수를 유도하는 노력이 필요함
- 특히 민간사업자의 자율규제 시행과정에서 사업자가 불법정보를 적극적으로 제한하기 위해서는 자율규제 기관의 성격과 책임 영역 확립을 위한 법률적 근거 마련이 필요하며, 이러한 권한은 신속한 콘텐츠 처리와 정보 제공자(또는 게시자)에 대한 효율적 대처를 가능하게 함
- 동시에 삭제통지(Notice and Take Down) 절차에 대한 콘텐츠 게시자의 권익 보호를 위한 항변 절차 마련 등을 의무화하는 등 자율규제 방식과 절차에 대한 제도적 근거와 가이드가 마련되어야 함

2. 국제공조 강화 방안

2-1. 불법영상물의 국제공조 필요성

○ (유통양상) 불법정보는 그 불법성으로 인해 유통실태가 명확하게 파악되지는 않지만, 해외사이트 등을 통한 불법저작물 및 불법영상물의 국내 유입은 지속적인 문제로 지적
- 불법저작물의 경우 2018년 기준 약 20억 건 정도가 유통되는 것으로 추정됨(한국저작권보호원, 2019. p.141)

- 방송통신심의위원회의 불법·유해정보 시정요구건수도 2019년 기준 20만여 건에 이름 (방송통신심의위원회, 2020)

<표 3-25> 방송통신심의위원회의 불법유해정보 시정요구건수 동향(2020년)

구분	이용해지/정지	접속차단	삭제	합계
시정요구건수 (비중, %)	1만656건 (5.2%)	16만803건 (77.8%)	3만4천995건 (16.9%)	20만6천759건 (100%)

자료: 방송통신심의위원회(2020)

- 불법복제물의 주 유통경로였던 토렌트·웹하드·포탈·P2P 등에 대한 국내 규제가 강화되자, 국내 단속을 피하기 위해 해외로 서버를 이전하여 유통하는 비중이 증가
- 접속차단 조치에 대응하여 불법사이트들이 서버를 이전하여 대체 사이트를 생성하는 주기†도 점차 짧아지고 있는 반면, 해외 서버와 사이트에 대한 수사가 어려워 이를 단속하고 수사하는 속도가 그에 비례해서 짧아지지 못하고 있음

† 불법저작물의 경우 대체사이트의 생성 주기를 평균 2주정도로 추정(문화체육관광부, 2018.7.10.)하는 반면, 현행 국가 간 형사사법공조는 공조를 요청한 시점으로부터 외국 수사 및 사법 기관으로부터 근거 자료를 받기까지 평균 4~6개월 이상 시간이 소요됨

- 이에 점차 국제화되는 불법정보 유통 양상에 효율적으로 대응하기 위해 수사의 속도를 높이는 것이 중요하고 관련국들과의 신속한 국제공조가 필요하다는 의견이 대두되고 있음

※ 여성가족부의 「제1차 여성폭력방지정책 기본계획 (2020. 2. 20)」 중 하나로 '국제공조 강화'를 제시함

○ (인터넷 특수성) 컴퓨터 자료의 일시성, 확산성, 접근성 등의 문제로 디지털 범죄기록의 추적, 증거 보전 등이 어렵다는 문제가 있음

- (확산성) 특정 매체나 지역에 물리적으로 고정되지 않아 전 세계 각 국 및 각 서버로 이동이 가능함
- (일시성) 디지털성착취물 등 사이버범죄와 관련된 증거는 대체로 누구나 디지털 정보의 삭제 및 훼손이 가능하여 보존이 어렵기 때문에 신속한 대응이 필수적임
- (접근성) 디지털 증거의 저장 형태나 방식이 빠르게 변하고 암호화 및 IP변동 등 추적을

피하는 방법도 고도화되고 있어, 수사기관의 디지털 증거에 대한 접근이 점차 어려워지고 있음

<표 3-26> 아동음란물 URL주소의 지리적 분포

구분	유럽	북미	아시아	아프리카	남미	호주	다크웹	합계
건수	51,344	25,395	1,627	20	10	149	44	78,589

출처: 영국 인터넷감시재단(IWF), 유민종(2019. 2, 재인용.)

○ (국제공조 필요성) 글로벌 네트워크를 통해 유통되는 불법정보는 여러 국가의 관할권이 관계되므로 한 나라의 수사력만으로 해결이 어렵기 때문에, 국가간 사법공조의 필요성이 제기되고 있음

- 국내에서도 해외서버를 경유하거나 해외사이트를 통해서 국내로 유통되는 아동포르노 등 불법정보의 피해가 심각해짐에 따라, 국제화되는 불법정보 유통 방지를 위해서 효율적인 국제· 국가간 공조방안 마련의 필요성이 제기
- 인터넷 공간 자체가 초국가적 성격을 가지고 IP주소를 여러차례 우회하여 여러국가를 경유하여 제공되는 다크웹이나 불법사이트 등의 규제에 있어 관할권의 문제가 발생하기 쉽고 국내적 규제수단 만으로는 초국가적으로 발생하는 불법행위를 대처하는 데에 한계가 있음

※ 국제공조수사 요청 건수는 2015년 284건에서 2019년 858건으로 4년 만에 약 3배 증가했으며, 동기간 국내 사이버범죄는 14만4679건에서 18만499건으로 24.8% 증가함(경찰청, 2020, 뉴스핌(2020. 6. 24), 재인용)

- 특히 텔레그램 'N번방', 다크웹 '코챈(kor chan)' 등의 사건[†] 을 계기로, IT 기술의 발달과 함께 성범죄의 형태가 점점 더 복잡해지고 있고 서버를 해외에 둔다든지 하는 방식으로 검거가 쉽지 않은 디지털성범죄물의 유통 방지를 위해 사이버범죄방지협약 가입 필요성이 제기되고 있음

† 다크웹(Dark Web)은 암호화된 네트워크에 존재하는 웹사이트로 일반적인 검색 엔진이나 일반적인 브라우저에서 검색되지 않는 인터넷 부분을 포괄적으로 지칭하는 용어임. 텔레그램 'N번방'사건은 2018년 하반기부터 2020년 3월까지 클라우드 기반 인터넷 메신저에서 회원제로 성착취물 영상을 공유한 사건이며, 코챈(Kor Chan)은 다크웹에 존재하는 한국어 커뮤니티로

소위 텔레그램 상의 'N번방'사건과 관련된 성착취물 영상 공유에 관한 정보 등이 공유되었음

- 불법정보의 인터넷 유통에 대한 입법적 대응 노력 중의 하나가 바로 유럽의 사이버범죄방지협약으로, 다국가를 경유하는 불법정보의 유통에 대해서 전자증거의 압수수색 절차와 관할권 규정을 포함한 절차를 포괄하고 있음
- 이에 유럽평의회가 2001년에 제정한 사이버범죄협약[†] 가입에 대한 검토 논의가 필요함

[†] 사이버범죄협약(Convention on Cybercrime)은 국내에서'사이버범죄방지협약', '사이버범죄조약', '사이버범죄방지조약', '유럽사이버범죄조약' 등으로 번역되고 있음 (2001년 11월 23일 헝가리 부다페스트에서 위 협약의 서명식이 개최되었기 때문에 일명 '부다페스트협약'으로 불리기도 함)

2-2. 불법영상물 유통방지를 위한 국제공조 해외사례

가. 유럽사이버범죄협약 가입현황

○ (가입현황) 유럽평의회가 제정한 사이버범죄협약은 2001년에 제정하여 2020년 11월 기준 총 78개국이 협약에 서명하였으나 그 중 65개국이 협약에 비준한 상태

- 전체 47개 회원국 중 44개국, 31개 비회원국 중 21개국 총 65개국이 사이버범죄협약에 비준한 상태

<표 3-27> 유럽 사이버범죄협약 가입국 현황

구분	서명국	비준국
회원국	47	44
비회원국	31	21
전체	78	65

출처: 유럽사이버범죄협약 공식홈페이지

- 2001년 협약 초기 가입국들은 대부분 유럽 권역이었지만, 최근 미국·남아프리카공화국·캐나다·일본 등 유럽평의회 소속이 아닌 비회원국 가입이 증가함에 따라 지역 협약이라는 성격에서 탈피하여 국제적 협약으로 속성이 변화되고 있음
- 국내에서는 디지털관련 범죄 증가로 인해 협약 가입 필요에 대한 논의가 있었으나, 개인정보의 국외이전 및 수사과과정에서 통신비밀보호 침해 등의 우려가 있어 현재에는

미 가입 상태

나. 유럽사이버범죄협약 개관

○ (정의) 국경을 초월하여 행해지는 사이버범죄행위에 대해 개별 국가 간 동일하거나 유사 규정 마련을 통해 국제공조체계 구축한 세계 최초 유럽평의회 사이버범죄협약

○ (의의) 사이버범죄협약은 컴퓨터 및 인터넷범죄를 방지·처벌할 수 있도록 제안한 최초의 국제적 협약

- 사이버범죄와 관련하여 가입국이 기본적으로 갖추어야 할 실체법과 절차법을 규정하고 효율적인 국제협력체계 구성 체계 마련
- 글로벌 네트워크의 특성을 갖는 인터넷 상에서의 불법정보 유통은 한 국가만으로 해결될 수 있는 문제가 아니라 모든 국가에 걸쳐 문제가 되는 네트워크 범죄이기 때문에 다국간의 수사공조 필요성이 증가함에 따라, 양자간 사법공조를 넘어서 다자간 사법공조를 위한 국제적 합의가 이루어졌다는 점에서 의의가 있음

○ (목적) 정보통신기술환경에 적합한 수사상 권한에 대한 공통된 규정을 정립함으로써, 가입국간의 형사절차의 상호적인 조정과 조화를 도모하는 데에 있음

<표 3-28> 사이버범죄방지협약의 목적

구분	주요 내용
1	• 컴퓨터시스템·네트워크 및 정보의 오용뿐만 아니라 이에 대한 기밀성, 무결성, 유용성을 침해하는 행위를 범죄화하여 사어버범죄로부터 사회의 안전 도모
2	• 사이버범죄에 관한 국가 간·기업 간 상호협력 제고
3	• 사이버범죄에 대한 효과적 처벌을 위해 신속하고 원활한 국제공조방안 마련
4	• 국내적·국제적 차원에서 사이버범죄행위에 대한 수사 및 기소를 지원하는 동시에 신속하고 공정한 국제협력을 의무화함으로써 범죄행위에 효과적 대응
5	• 컴퓨터시스템이나 데이터 관련된 범죄의 효과적인 수사 및 기소를 위

	하여 기존 형사사법 공조협약이나 범죄인인도협약을 보충하고, 사이버 범죄의 전자증거 수집에 필요한 근거 마련

출처: 대검찰청(2009)

○ (구조) 사이버범죄방지협약은 전문(Preamble)과 4장, 48개의 조문으로 구성되어져 있고, 실체법 절차법, 공조절차, 협약가입 및 적용범위 등을 규정하고 있음

- 제1장은 협약에서 사용되는 용어의 정의, 제2장은 가입국이 갖추어야할 실체법 및 절차법, 제3장은 국제협력 절차, 제4장은 협약의 가입·발효·유보 등 운영 규정을 다룸

<표 3-29> 사이버범죄방지협약 구조

편제	주제	주요내용		관련조항
제1장	용어의 정의	• ‘컴퓨터 시스템’, ‘컴퓨터 데이터’, ‘서비스 제공자’, 트래픽 데이터‘에 대한 개념 정의		• 제1조
제2장	실체법 규정	1절	• 사이버범죄유형과 구성요건	• 제2조~ 제13조
		2절	• 디지털 증거확보를 위해 가입국들이 자국법에 갖추어야할 절차 규정	• 제14조~ 제22조
제3장	절차법 규정	1절	• 국제공조의 일반원칙 규정	• 제23조~ 제28조
		2절	• 가입국 간 협약 제2장에 규정된 절차 공조하는데 필요한 절차 • 공조 업무 담당하기 위해 가입국에 설치하는 24/7 네트워크 규정	• 제29조~ 제34조
제4장	국제 공조 절차	• 협약의 서명·발효절차		• 제36조
		• 비회원국의 가입절차		• 제37조
		• 협약의 효력		• 제38조~ 제41조
		• 유보조항		• 제42조~ 제43조
		• 개정 절차		• 제45조
		• 협약의 해석·적용에 관한 분쟁해결		• 제46~ 제48조

○ (유형) 사이버범죄협약에서 국제수사공조의 대상이 되는 사이버범죄는 불법접속(제2조), 불법감청(제3조), 데이터 침해(제4조), 시스템 방해(제5조), 장치 남용(제6조), 컴퓨터 관련

위조(제7조), 컴퓨터 관련사기(제8조), 아동음란물(제9조), 저작권 침해 범죄(제10조) 총 9가지로 분류함

- 각국마다 정의하는 사이버범죄의 유형과 범위가 다르지만, 사이버범죄협약에서는 협약 당시 회원국의 합의에 따라 폐해가 심각하고 국제공조가 시급한 범죄를 우선적으로 선정함
- 이에 따라 국내에서 규정하고 있는 온라인 명예훼손· 모욕 등은 협약에서 규정한 사이버범죄에 포함되지 않음

<표 3-30> 사이버범죄방지 협약 상 사이버범죄 유형

범죄유형	해당범죄
정보 및 컴퓨터시스템의 비밀, 완결성, 활용성을 침해하는 범죄	• 제2조 불법접근 • 제3조 불법감청 • 제4조 데이터침해 • 제5조 시스템방해 • 제6조 장치의 오용
컴퓨터관련 범죄	• 제7조 컴퓨터관련위조 • 제8조 컴퓨터관련사기
콘텐츠관련 범죄	• 제9조 아동포르노그래피
지적재산권침해관련 범죄	• 제10조 저작권침해

출처: 대검찰청(2008)

- 사이버범죄방지 협약에 따른 사이버범죄의 유형은 각각 다음과 같이 정의함
  - ▸ 불법접근: 권한 없는 자가 컴퓨터 시스템의 일부 또는 전부에 고의적으로 접속하는 행위, 컴퓨터 데이터를 획득할 의도로 또는 기타 부정한 의도로 보호조치를 침해하는 행위로 정의되며, 대표적으로 해킹†, 크래킹‡ 등을 포함
    - † 해킹: 허가되지 않은 방법 등으로 시스템관리자의 권한을 획득하는 것
    - ‡ 크래킹: 시스템 및 네트워크에 접근할 수 있도록 패스워드를 알아내는 보안공격
  - ▸ 불법감청: 컴퓨터시스템에서 데이터를 비공개 전송하는 것을 기술적 수단을 이용하여 권한 없이 고의로 감청하는 행위로 정의
  - ▸ 데이터침해: 권한 없이 컴퓨터 데이터를 고의로 훼소, 삭제, 가치저하, 변경, 은폐하는 행위로

정의

- ▸ 시스템 방해: 권한 없이 고의로 컴퓨터데이터를 입력, 전송, 훼손, 삭제, 가치저하, 변경 또는 은폐하여 컴퓨터시스템의 작동을 심각하게 방해하는 행위로 정의
- ▸ 장치의 오용: 컴퓨터시스템이나 데이터의 기밀성, 무결성, 가용성에 대해 범죄에 악용될 수 있는 장치를 사용하여 취득, 수입, 배포, 이용하게 하는 행위로 정의
- ▸ 컴퓨터 관련 위조: 권한 없이 고의로 컴퓨터 자료를 입력, 변경, 삭제 또는 은폐하는 행위로 정의
- ▸ 컴퓨터 관련 사기: 경제적 이익을 목적으로 권한없이 고의로 데이터를 입력, 변경, 삭제 및 은폐하거나, 컴퓨터시스템의 정상적인 작동을 방해하는 행위로 정의
- ▸ 아동포르노그래피: 컴퓨터 시스템을 통하여 배포할 목적으로 아동을 대상으로 한 성착취물을 제작, 제공, 전송, 배포, 획득, 소유하는 행위로 정의
- ▸ 저작권침해: 문예저작물의 지적재산권을 침해하여 권한 없이 복제, 유포하는 행위로 정의

<표 3-31> 사이버범죄방지협약의 아동포르노물 관련 범죄와 아동포르노물 정의

구분	정의
아동포르노물 관련범죄(offences related to child pornography)	① 컴퓨터 시스템을 통하여 아동포르노물을 배포할 목적으로 이를 제작하는 행위, ② 컴퓨터 시스템을 통하여 아동포르노물을 이용하도록 하거나 제공하는 행위, ③ 컴퓨터 시스템을 통하여 아동포르노물을 전송 또는 배포하는 행위, ④ 본인이나 타인을 위해 컴퓨터 시스템을 통하여 아동 포르노를 획득하는 행위, ⑤ 컴퓨터 데이터 저장매체 또는 컴퓨터 시스템 내에 아동포르노물을 소유하는 행위를 권한없이 고의적으로 저지르는 것으로 정의함(제9조).
아동포르노물(child pornography)	① 성적으로 노골적인 행위를 하는 미성년자, ② 미성년자가 성적으로 노골적인 행위를 한다고 표시하는 성인, ③ 성적으로 노골적인 행위를 미성년자가 한다는 것을 표시하는 사실적인 영상을 시각적으로 묘사하는 포르노물

- 유럽사이버범죄방지협약에서 불법정보 유통과 관련된 조항은 제9조 아동포르노물에 해당함

○ (유보가능조항) 협약 제42조에 의거하여, 협약 당사국은 서명하거나 비준·수락·승인 또는

가입단계에서 유럽평의회 사무총장에게 보내는 서면통지에서 협약의 일정한 조항에 대해 유보를 허용

- 유보가능 조항은 데이터 침입(제4조 제2항), 장치의 남용(제6조 제3항), 아동포르노그래피 관련 범죄(제9조 제5항), 저작권 관련 권리의 침해(제10조 제3항), 고의 미수(제11조 제3항), 컴퓨터데이터의 실시간 수집에 있어서 유보(제14조 제3항), 관할권에 대한 유보(제22조 제2항), 쌍방가벌성을 요건으로 한 공조요청 거부(제29조 제4항), 연방조항(제41조 제1항)이 해당함

다. 주요국의 입법례 사례 분석

○ 협약은 가입국들이 수사 초기에 필요한 데이터 보전 수단의 최소한의 기준 또는 기본적인 형태만을 규정하고 있을 뿐, 가입국마다 보전조치의 구현방식, 요건 등 법체계가 상이함

- 사이버범죄방지협약은 절차법규정으로서 적용범위와 요건, 컴퓨터데이터의 신속한 보존조치, 컴퓨터데이터의 제출명령, 실시간 수집 등에 대해 특별한 규정을 마련하도록 요구하고 있음

<표 3-32> 해외 주요국의 비교

사이버범죄협약		독일	일본	미국
전자기록의 신속한 보전	제16조 제17조	• 형사소송법 제94·95·98·100조g	• 형사소송법 제197조 제3항·4항	• 형법 제2703조f
전자기록의 수색과 압수	제18조	• 형사소송법제95조	• 형사소송법 제99조의2	• 형법 제2703조
데이터의 실시간 수집 및 감청	제20조 제21조	• 형사소송법 제100a·b조	• 통신감청법 제5·6·7조	• 형법 제2704·2511조

① 전자기록의 신속한 보전

- 디지털 증거를 사전에 보전하기 위한 장치로, 협약 제16조(저장된 컴퓨터데이터의 신속한 보존), 협약제17조(트래픽데이터의 신속한 보존과 일부제출) 조항을 두고 있음

[유럽사이버범죄협약 제16조와 제17조]

제16조 (저장된 컴퓨터데이터의 신속한 보존) 1. 컴퓨터시스템에 의해서 저장되어 있는 통신데이터를 포함한 특정한 컴퓨터데이터가 특히 손실되거나 변경될 수 있다고 믿을 만한 근거가 있는 경우에는 가입국은 이러한 데이터의 신속한 보존을 자국의 권한 있는 기관이 명령하거나 이와 유사한 방법으로 획득할 수 있도록 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. (이하생략)

제17조 (트래픽데이터의 신속한 보존과 일부 제출) 1. 각 가입국은 제16조에 의하여 보존될 통신데이터와 관련하여, a) 하나 또는 그 이상의 서비스제공자가 이 통신의 중개에 참여하고 있는지에 관계없이 통신데이터의 신속한 보존이 가능하고, b) 가입국이 서비스제공자 및 통신의 전송 경로를 확정할 수 있도록 충분한 량의 통신데이터가 가입국의 관할기관이나 이 기관으로부터 지명받은 자에게 즉시 제출(공개)되도록 필요한 입법적 조치와 그 밖의 조치를 취해야 한다.

- 협약가입국들의 관련 입법 사례를 살펴보면, 독일은 형사소송법 제94~98조 근거하여, 일본은 형사소송법 제197조 제3항에 근거하여, 미국은 18 U.S.C 2703(f) 조항에 근거하여 전자기록 등의 보존 및 비밀유지 요청을 통해 범죄의 증거를 사전에 보존하도록 함

② 전자기록의 수색과 압수

- 통신내역을 알거나 이를 보전하기 위해 통신내역이 기록된 통신사업자의 컴퓨터나 기록매체에 대하여 압수·수색이나 검증하는 장치로, 협약 제18조(제출명령) 조항을 두고 있음
- 외국의 입법례를 살펴보면, 독일은 형사소송법제95조(제출 및 인도의무), 일본은 형사소송법 제99조의2항, 미국은 18 U.S.C. §2703(이용자통신내용 및 통신기록의 공개의무) 조항에 근거하여 제출명령을 규정하고 있음
- 국내의 경우, 전기통신사업자가 보관하고 있는 서버 전체를 압수·수색하는 방법은 범죄사실과 관계없는 사람의 권리나 이익의 침해가 우려되므로 '기록 후 제출명령제도†'가 우선적으로 강구되어야함

† 기록 후 제출 명령제도란 전자기록 등을 보관하는 자 또는 기타 전자기록 등을 이용하는 권한을 가지고 있는 자에게 필요한 전자기록만을 기록매체에 기록하게하거나 인쇄하게 한 다음, 당해 기록매체를 압수하는 제도

[유럽사이버범죄협약 제18조]

► 제18조 (제출명령) 1. 각 가입국은 a) 어떤 자가 자국의 영토 내에서 소유하고 있거나 지배하고 있고 컴퓨터시스템 내에 또는 컴퓨터데이터저장매체에 저장되어 있는 특정한 컴퓨터데이터를 제출하고, b) 서비스제공자가 가입국의 영토 내에서 그의 서비스와 관련하여 소유하고 있거나 지배하고 있는 가입자정보를 제출하도록 명령할 권한을 관할 기관에게 부여하도록 필요한 입법적 조치 및 그 밖의 조치를 취해야 한다.

③ 실시간 데이터 수집 및 감청

- 범죄의 증거인 통신데이터의 실시간 통신로그 등을 수집하기 위한 제도적 장치로, 협약 제20조(트래픽데이터의 실시간수집), 협약제21조(통신내용데이터의 실시간수집) 조항을 두고 있음
- 범죄의 관점에서 트래픽데이터[18]의 실시간수집(협약제20조)과 통신내용데이터[19]의 실시간수집(협약제21조)을 구분하고 있으며(대검찰청, 2015), 통신내용데이터의 실시간 수집은 실시간 감청을 의미함
- 실시간 수집이나 감청은 사생활 침해 가능성이 크기 때문에 각 당사국의 국내법에서 정한 엄격한 요건과 절차에 따르도록 하고 있는 것이 일반적임

  ※ 외국의 입법례 사례를 살펴보면, 독일은 통신감청 제100조a,b(통신감청), 일본은 형사소송법 제99조의2항, 미국은 18 U.S.C. §2704(백업의 보존)·18 U.S.C. §2511(유선·음성·전자통신의 감청과 공개의 금지)조항에 근거하여 실시간데이터수집 및 감청을 규정하고 있음
- 협약에 따르면 데이터 수집 및 제출 시 서비스제공자가 정상적 사법절차에 따라 데이터 수집을 가능하도록 규정하고 있으나, 실제로 데이터 수집할 기술적 능력을 국내법적으로 갖춘 나라는 독일정도 뿐인 것으로 평가되고 있음

[유럽사이버범죄협약 제20조와 제21조]

► 제20조 (트래픽데이터 실시간 수집) 1. 각 가입국은 자국의 권한 있는 기관이 a) 자국의 영토 내에서 컴퓨터시스템을 수단으로 중계되는 특정한 통신과 관련 있는

---

18) 트래픽데이터란 협약 제1조d호에서 정의한, 컴퓨터 시스템에 의해 행해지는 통신과 관련된 모든 컴퓨터 데이터를 의미 ex)통신의 발신지, 수신지, 경로, 시간, 날짜, 크기 그리고 서비스의 지속시간 또는 유형

19) 통신내용데이터란 내용데이터로 협약에 정의되지 않지만 통신의 내용을 의미함 ex) 트래픽데이터를 제외한 통신에 의해서 전달되고 있는 메시지 또는 정보를 의미

통신데이터를 자국의 영토 내에서 기술적인 수단을 사용하여 실시간으로 수집하거나 기록하고, b) 서비스제공자에게, ⅰ) 자국의 영토 내에 있는 기술적 수단을 사용하여 그러한 통신데이터를 실시간으로 수집하거나 기록하고, ⅱ) 그러한 통신데이터의 실시간 수집과 기록에 있어서 권한 있는 기관과 협력하고 이를 지원할 수 있는 기존의 기술적 능력 내에서, 서비스제공자에게 의무를 부과하도록 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다. (이하생략)

► 제21조 (통신내용데이터의 실시간 수집) 1. 각 가입국은, 자국의 권한있는 기관에 대해서, 자국의 국내법에 의해서 규정되는 중대한 범죄의 범위 내에서, a) 자국의 영토 내에 있는 컴퓨터시스템을 이용하여 전달되는 특정한 통신의 내용데이터를 자국의 영토 내에서 기술적 수단을 사용하여 실시간으로 수집하거나 기록하고, b) 서비스제공자의 기술적 가능성과 관련하여 ⅰ) 자국의 영토 내에서 기술적인 수단을 사용하여 그러한 내용데이터를 실시간으로 수집하거나 기록하고 또는 ⅱ) 그러한 내용관련 데이터의 실시간 수집 및 기록의 경우에 권한 있는 기관과 협력하고 이를 지원할 의무를 서비스제공자에게 부여하도록 필요한 입법적 조치와 그 밖의 조치를 취해야 한다.

(1) 독일

○ (협약가입) 독일은 2001년 11월에 유럽이사회의 26개 가입국과 함께 사이버범죄방지협약에 서명한 후 약 8년 동안 관련 법률의 개정을 거쳐 2009년 3월에 유럽평의회에 협약을 비준

- 형사소송법과 통신감청법의 개정을 통해 ① 전자기록의 보전요청에 관한 규정의 정비(형사소송법 제94·95·100조g), ② 전자기록의 수색과 압류제도의 신설(형사소송법 제95조), ③ 통신데이터수집 및 감청(통신감청법 제100조 a,b)의 근거조항 마련 등을 실시함

<표 3-33> 사이버범죄협약 절차규정 관련 독일의 대응법규

협약		관련조항
전자기록의 신속한 보전	제16조(저장된 컴퓨터데이터의 신속한 보존)	• 형사소송법 제94조(증거대상의 보전) • 형사소송법 제95조(제출 및 인도의무) • 형사소송법 제98조(압수명령)
	제17조(통신데이터의 신속한 보존과 일부제출)	• 형사소송법제100조g(교신데이터조사)
전자기록의 수색과 압수	제18조(제출명령)	• 형사소송법 제95조(제출의무)

데이터의 실시간 수집 및 감청	제20조(통신데이터의 실시간 수집) 제 21조(통신내용 데이터의 실시간 수집)	• 형사소송법 제100a조(통신의 감청에 관한 조건) • 형사소송법 제100b조(통신감청 명령 및 이행)

① 전자기록의 신속한 보전

- 독일 형사소송법 제94조(증거대상의 보전)과 제95조(제출 및 인도 의무)는 범죄와 관련된 수사를 위해 증거대상을 보전하고, 증거를 제출 받을 수 있는 법적 근거를 제공하고 있음
- 형사소송법 제94조와 제95조는 컴퓨터데이터에 대해 명시적으로 언급하고 있지 않지만, 컴퓨터데이터에도 상응하게 적용되어(박희영 외, 2015), 형사소추기관이 컴퓨터데이터에 직접 접근하는 것을 허용하고 컴퓨터 데이터를 확보할 수 있도록 하고 있음
- 트래픽 데이터의 보전과 제출의무에 대해서는 별도의 조항이 적용될 수 있는데, 형사소송법 제100조g에 따라 범죄의 수사 목적으로 당사자의 동의 없이도 교신데이터(통신데이터)를 포괄적인 수집할 수 있는 권한이 수사기관에 부여되었음
- 또한 전기통신사업자에게 데이터의 보전 및 제출 협조 의무는 전기통신법 제 113a조(데이터 보관의무)와 제113b조(통신정보의 저장의무)에 규정하고, 전기통신사업자가 수집하고 보전하는 통신정보의 범위는 제96조 제1항(통신정보의 수집)와 제113b조3항에 규정함

[전자기록의 신속한 보전과 관련한 독일의 법률 조항]

►형사소송법 제94조(증거대상의 보전)

① 심리에 중요한 증거는 유치하거나 다른 방법으로 보전해야 한다.

② 위 대상을 개인이 소지하고 있고 자발적으로 인도하지 않는 때에는 압수한다.

③ 제1항과 제2항은 증거로 사용될 운전면허증에도 적용한다.

►형사소송법 제95조(제출 및 인도의무)

①전술한 종류의 대상을 소지하고 있는 자는 요구가 있으면 이를 제출하고 인도할 의무가 있다.

②전항의 의무이행을 거부하는 경우에는 제70조에 규정된 질서유지수단 및 강제수단을 부과할 수 있다. 단 증언거부권이 있는 자에게는 적용되지 않는다.

►형사소송법 제100g조(교신데이터 조사)

① 특정한 사실에 근거하여 누군가가 정범 또는 공범으로서 다음 각 호에 해당하는 범죄를 행했다는 혐의가 있을 때에는, 사안의 조사 및 피의자의 소재지 수사에 필요한 한, 당사자가 이를 알지 못하더라도 교신데이터(통신법 제96조 제1항, 제113조a)를

조사할 수 있다.
1. 구체적인 사례에 비추어 중대한 의미가 있는 범행, 특히 제100조a 제2항에 규정된 범행을 행했거나 미수의 가벌성이 있는 행위의 착수 또는 별도의 범행을 통해 예비한 때
2. 통신을 수단으로 행한 범죄 (이하생략)
►전기통신법 제96조 제1항(통신정보의 수집) ① 서비스 제공자는 본 절에 정한 목적을 위해서 필요한 경우 다음 통신정보를 수집할 수 있다.
1. 가입한 접속 및 단말기의 번호 및 표지, 개인관련 권리자 표지, 고객카드 이용의 경우 카드번호, 모바일 접속의 경우 위치정보,
2. 개별접속의 시작 및 종료 후의 날짜와 시간, 유료요금제의 경우 전달된 데이터의 량
3. 이용자가 이용한 전기통신서비스
4. 비교환 회선의 경우 목적지, 이의 시작과 종료후의 날짜 및 시간
5. 전기통신의 구축 및 유지 그리고 요금 산정을 위해서 필요한 그 밖의 통신정보
② 제1항의 범위를 넘어서는 트래픽 데이터의 수집과 이용은 허용되지 않는다.
(이하 생략)
►전기통신법 제113a조(데이터 보관의무)
① 공중이 접근 가능한 전기통신서비스를 이용자를 위해서 제공하는 자는 서비스의 이용에 있어서 그가 생성하거나 처리한 트래픽 데이터를 제 2항내지 제5항의 기준에 따라 6개월간 독일 또는 유럽공동체 회원국 안에서 보관할 의무가 있다. (이하생략)
►전기통신법 제113b조(통신정보의 저장의무)
① 제113조a에 언급된 자는 제2항 및 제3항의 데이터는 10주간, 제4항의 위치데이터는 4주간 국내에 저장할 의무가 있다.
(생략)
③ 공중접근 인터넷접속서비스 제공자는 다음 각호에 정한 데이터를 저장한다.
1. 인터넷접속을 위해 가입자에게 부여되는 IP주소
2.인터넷이용으로 생성되는 회선의 명확한 표지 및 할당된 이용자 표지
3. 표준시간대의 정보가 포함되어 있는 할당된 IP주소로 인터넷이용시작과 종료날짜 및 시간
(이하생략)

② 전자기록의 수색과 압수

- 독일 형사소송법 제95조에 근거하여 데이터를 포함한 압수목적물을 소지하는 자는 수사기관의 요구에 의하여 해당 자료를 제출·인도하도록 규정
- 독일은 특히 형사소송법 제110조 제3항에 근거하여 전자적 데이터 저장매체의 열람을 공간적으로 떨어져 있는 저장매체로 확장하여 포괄적인 전자기록의 수색을 허용함

[전자기록의 수색과 압수에 관련한 독일 법률 조항]

► 제110조(문건 및 전자 저장매체의 검열) ③ 수색대상인 자의 전자 저장매체에 대한 검열은 검열대상인 데이터가 상실될 우려가 있다면 저장매체로부터 도달될 수 있는 한, 당해 저장매체와 공간적으로 분리되어 있는 전자매체들에까지 확대될 수 있다. 조사에 중요한 의미가 있을 수 있는 데이터는 이를 압수할 수 있다. (이하 생략)

③ 데이터의 실시간 수집 및 감청

- 협약 제20조에 규정된 트래픽 데이터의 실시간 수집에 대응하기 위해, 독일 형사소송법 제 100조a,b의 요건 하에서 수사기관의 전기통신의 감시와 녹취를 허용하여 통신(내용) 데이터의 실시간 수집이 가능함

[데이터의 실시간 수집 및 감청과 관련한 독일 법률 조항]

► 형사소송법 제100조a(통신감청) ① 다음 각 호의 하나에 해당하는 경우 당사자가 이를 알지 못하더라도 통신을 감청 및 녹음을 할 수 있다.

1. 제2항에 열거된 중범죄의 정범 또는 공범으로서 수행했다는 혐의 및 미수를 처벌하는 사례에서 실행에 착수하였거나 다른 범죄행위를 통해 이를 예비하였다는 혐의의 근거가 되는 사실이 있는 경우
2. 개별사례에 비추어 범행의 중대성이 인정되는 경우
3. 사실관계의 조사나 피의자의 소재에 대한 수 (이하생략)

►형사소송법 제100조b(명령 및 이행) ① 제100조a에 따른 처분은 검사의 신청에 기하여 법원만이 행할 수 있다. 긴급을 요하는 경우에는 검사도 당해 처분을 명할 수 있다. 검사의 명령이 3일 이내에 법원의 추인을 받지 못한 경우에는 검사의 명령은 효력을 상실한다. 감청명령은 최장 3개월의 기간에 한정된다. 획득된 수사결과를 고려하여 명령의 요건이 존속하는 때에는 3개월 이하의 연장이 허용된다. (이하생략)

나. 일본

○ (협약가입) 유럽평의회 비회원국인 일본은 유럽이사회의 26개 가입국과 함께 2001년 11월 사이버범죄방지협약에 서명했으며 2004년 7월에 비준하였으며, 2012년 7월에 사이버 범죄에 관한 협약을 공포 및 고시하여 2012년 11월부터 효력이 발생

- 일본은 2004년 4월 동 협약에 비준했으나 심의과정에서 협약이 요구하는 수사권이 내국인의 프라이버시 침해 가능성, 국가의 정보자산에 대한 자주권 침해 우려, 정보통신사업자의 부담 등을 이유로 관련 법안의 개정안이 통과되지 못하다가 2011월 6월

법률안이 공포되어 2012년부터 시행됨

- 협약 반영을 위해 일본은 형법을 일부 개정하여 ①보전요청에 관한 규정의 정비(형사소송법 제197조 제3항,제4항) ②기록명령부 압류의 신설(형사소송법 제99조의2, 제218조 제1항), ③데이터수집 및 감청(통신감청법 제5조·6조·7조) 등의 절차적 근거를 마련함

<표 3-34> 사이버범죄협약 절차규정 관련 일본의 대응법규

협약		관련조항
전자기록의 신속한 보전	제16조(저장된 컴퓨터데이터의 신속한 보존)	• 형사소송법 제197조 제3항,제4항
	제17조(통신데이터의 신속한 보존과 일부제출)	
전자기록의 수색과 압수	제18조(제출명령)	• 형사소송법 제99조의2
데이터의 실시간 수집 및 감청	제20조(통신데이터의 실시간 수집)	• 통신감청법 제5조, 제6조, 제7조
	제 21조(통신내용데이터의 실시간 수집)	

① 전자기록의 신속한 보전

- 협약 제16조와 제17조에 대해서는 일본 형사소송법 제197조 제3항(보전요청)이 대응하여, 수사기관이 전기통신사업자에 대해 수사와 관련한 전자기록에 대한 보전요청을 할 수 있는 권한의 근거를 마련함
- 트래픽 데이터의 보전 요청은 압수 및 수색과 달리 영장없이 서면요청을 통해서도 가능하며, 트래픽 데이터이외의 컴퓨터 데이터의 보전은 압수영장이 필요함

[전자기록의 신속한 보전과 관련한 일본의 법률 조항]

►제197조 ③ 수사에 관해서는 전기통신을 하기 위한 설비를 통신용도에 제공하는 사업을 영위하는 자 또는 자기의 업무를 위하여 불특정 혹은 다수자의 통신을 매개할 수 있는 전기통신을 하기 위한 설비를 설치하고 있는 자에 대하여 그 업무상 기록하거나 기록해야 할 전기통신의 송신처, 수신처, 통신일시 기타의 통신이력에 관한 전자기록 등의 내용 중 필요한 것을 특정하고 90일을 넘지 않는 기간을 정하여 이를 삭제하지 않도록 서면으로 요구할 수 있다

④ 제2항 또는 제3항에 따른 요청을 하는 경우 필요한 때에는 이를 함부로 누설하지 않을 것을 요청할 수 있다.

② 전자기록의 수색과 압수

- 협약 일본 형사소송법 제 218조(압수 및 수색)와 형사소송법 제99조2에 따르면 법원은

필요한 경우에 한해 전자적 기록의 보관자 등에게 필요한 전자적 기록을 기록매체에 기록하게 한 후 압수가 가능함

[전자기록의 수색과 압수에 관련한 일본의 법률 조항

►제99조의2(기록복사명령) 법원은, 필요한 경우에는, 기록명령부 압수(전자적 기록을 보관하는 자 그 밖에 전자적 기록을 이용할 수 있는 권한을 가진 자에게 명하여 필요한 전자적 기록을 기록매체에 기록하게 하거나 인쇄하게 하여, 당해 기록매체를 압수하는 것을 말한다. 이하 같다)를 할 수 있다.

►제218조 ① 검찰관, 검찰사무관 또는 사법경찰관은 범죄의 수사를 함에 있어서 필요한 때에는 재판관이 발부하는 영장에 의하여 압수, 기록명령부 압수, 수색 또는 검증을 할 수 있다.

② 압수해야할 물건이 컴퓨터인 때에는 당해 컴퓨터에 전기통신회선으로 접속하고 있는 기록매체로서 당해 컴퓨터로 작성했거나 변경한 전자적 기록 또는 당해 컴퓨터에서 변경할 수 있거나 삭제할 수 있는 전자기록을 보관하기 위해 사용되고 있다고 인정할 만한 충분한 사유가 있을 때에는 그 전자적 기록을 당해 컴퓨터 또는 다른 기록매체에 복하한 다음 당해 컴퓨터 또는 그 다른 매체를 압수할 수 있다.

③ 데이터의 실시간 수집 및 감청

- 일본은 '범죄수사를 위한 통신감청에 관한법률(이하, '통신감청법')'을 제정하여 데이터 수집 및 통신감청에 관한 사항을 해당 법률로써 규율함(한국법제연구원, 2017)

※ 일본의 현행 통신감청법(犯罪捜査のための通信傍受に関する法律)은 통신내용의 감청에 관한 것이며 통신기록의 실시간 추적·수집에 해당하는 규정은 부재함

[데이터의 실시간 수집 및 감청과 관련한 일본 법률 조항]

►제5조·7조(통신감청기간 및 연장)통신 감청기간은 10일 이내로 하고 있으며, 10일 이상의 기간을 정하여 감청 기간을 연장할 수 있으나 전체 감청 기간은 전체 30일을 초과할 수 없도록 하고 있다. 또한 이는 검찰관 또는 사법경찰원의 청구에 의해 지방법원의 재판관이 발부한 영장에 의하여야 한다.

►제6조·7조(통신감청에 관한 규칙) 감청 기간 연장의 청구는 서면으로 하여야 하며, 연장을 필요로 하는 사유 및 연장을 요구하는 기간을 기재하여야 하며, 연장 사유에 대한 자료를 제공하여야 한다

► 제11조(통신사업자의 협력의무) 검사 또는 사법 경찰 직원은 통신 사업자 등에 대하여 도청의 실시에 관하여 도청 장비의 연결 기타 필요한 협조를 요청할 수있다. 이 경우에는 통신 사업자 등은 정당한 이유없이이를 거부 하여서는 아니된다

다. 미국

○ (협약가입) 유럽평의회 비회원국인 미국은 유럽이사회의 26개 가입국과 함께 2001년

11월 사이버범죄방지협약에 서명한 후, 약 5년의 국내법 개정과정을 거쳐 2006년 9월에 비준함

- ①보전요청에 관한 규정의 정비(형법 제2703조f)②기록명령부 압수제도(형법 제2703조), ③데이터수집 및 감청(형법 제2704조·2511조) 등에서 협약에 상응하는 대응법규 정비가 이뤄짐

<표 3-35> 사이버범죄협약 절차규정 관련 미국의 대응법규

협약		관련조항
전자기록의 신속한 보전	제16조(저장된 컴퓨터데이터의 신속한 보존)	• 형법 제2703조f(이용자 통신내용 및 통신기록의 공개의무)
	제17조(통신데이터의 신속한 보존과 일부제출)	
전자기록의 수색과 압수	제18조(제출명령)	• 형법 제2703조(이용자 통신내용 및 통신기록의 공개의무)
데이터의 실시간 수집 및 감청	제20조(통신데이터의 실시간 수집)	• 형법 제2704조(백업의 보존) • 형법 제2511조(유선·음성·전자통신의 감청과 공개의 금지)
	제 21조(통신내용 데이터의 실시간 수집)	

① 전자기록의 신속한 보전

- 협약 제16조와 제17조에 근거한 컴퓨터데이터와 트래픽데이터의 신속한 보전은 미국 형법 제2703(f)조항의 저장된 유선 및 전자통신과 거래기록에 대한 접근이 대응함
- 제2703(f)조항에 근거하여 법관의 영장이 발부될 때까지 네트워크 서비스 공급자는 가입자정보, 통신내역 및 통신내용정보에 대하여 수사기관이 보존 요청할 수 있도록 입법적 조치 마련
- 그러나 협약 제16조가 컴퓨터데이터를 포괄적으로 정의하여 통신내용도 포함할 수 있다고 해석될 수 있는 반면에, 미국 형법 제2703조는 가입자 정보와 트래픽 정보만 명시하고 있음

[전자기록의 신속한 보전과 관련한 미국의 법률 조항]

►제2703조f (이용자통신내용 및 통신기록의 공개의무)

1. 총칙. 통신서비스 제공자가 정부기관의 청구를 받은 경우 법원의 명령이나 그 밖의 절차가 교부될 때까지 자신이 소유한 기록과 그 밖의 증거를 보존하기 위해 필요한 모든 조치를 하여야 한다.
2. 보관 기간. 제1호에서 말하는 기록은 90일 기간 동안 보관하여야 하며, 정부 기관의 재요청이 있는 때에는 그 기간을 90일 더 연장하여야 한다.

② 전자기록의 수색과 압수

- 미국 형법 제121장 제2703조에 근거하여 정부는 관할법원이 발부한 영장, 법원명령, 가입자 또는 고객의 동의 확보, 통신판매사기에 대한 고객이나 가입자의 서면 청구 제출 등을 근거로 전기통신사업자에게 전자식으로 저장된 유선 또는 전자통신의 내용에 대한 공개를 요청할 수 있음

[전자기록의 수색·압수와 관련한 미국의 법률 조항]

►제2703조(이용자 통신내용 및 통신기록의 공개의무)

(a) 전자스토리지에 보관된 유선/전자통신내용에 대하여 영장을 받아 최대 180일동안 제출을 명령

(b) 원격 컴퓨팅 서비스의 유선/전기통신내용에 대하여, 영장 발부시 그 이용자에게 통지하지 않고 그 제출을 명령하고, 법원명령이나 대배심의 행정소환장(administrative subpoena)이 있는 경우 그 이용자에게 통지하고 제출을 명령함(법에 정한 사유에 의하여 통지의 연기 가능)

(c) 전자통신서비스 또는 원격컴퓨터서비스에 대하여 영장을 발부받았을 때, 법원명령이 있을 때, 당사자의 동의가 있을 때, 텔레마케팅 사기와 관련하여 서비스이용자의 이름, 주소, 사업장을 제출할 것을 서면으로 요청할 때, 법령이나 대배심에 의한 행정소환장을 제시할 때에 한하여 기록 등의 제출을 명령할 수 있다.

(d) 법원명령의 요건으로는 일단 관할권이 있는 법원에서 이를 명령하여야 하며 정부기관은 이러한 명령을 받기 위해 구체적인 근거를 제시하여야 한다.

(e) 서비스 프로바이더에 대한 면책

(f) 정부기관의 이러한 요청을 받게 되면 증거보존을 위하여 필요한 모든 절차를 수행하여야 하며 그 기간은 기본적으로 90일, 수사기관의 요청에 따라 최대 90일을 더 연장할 수 있다.

③ 데이터의 실시간 수집 및 감청

- 미국 형법 제2704조(백업의 보존) 및 제2511조(유선·음성·전자통신의 감청과 공개의 금지)에 근거하여 인터넷서비스제공자는 백업본을 생성하도록 강제할 수 있으며, 연방통신위원회의 대리인이 직무수행의 범위 내에서 적법하게 감청할 수 있음
- 추적장치의 설치 및 사용은 원칙적으로 금지되지만 아래와 같이 이용자의 이익보호를

위한 목적으로 사용하는 경우 당사자의 동의가 있는 경우에는 예외적으로 허용됨

- 단, 정보의 통신내용은 수집불가하며 다이얼링 정보, 경로추적정보, 신호정보만 수집이 가능함

[데이터의 실시간 수집 및 감청과 관련한 미국 법률 조항]

►형법 제2704조(백업의 보존)

(a) 정부기관은 행정소환장이나 법원명령을 통해 2영업일 이내에 서비스 프로바이더로 하여금 백업본을 생성하도록 강제할 수 있다. 당사자에게는 2영업일까지 통지하지 않으며 정부기관에 백업 생성 완료를 통지한 후 3영업일에 이를 통지한다. 생성된 백업본은 요청이 있은 날로부터 14일 이전까지는 제출하지 아니한다.

(b) 정부기관의 요청이 있은 날로부터 14일 이내에 당사자는 이에 불복할 수 있다.

►형법 제2511조(유선·음성·전자통신의 감청과 공개의 금지)

(1) 원칙적으로 유선, 구두, 전자통신의 감청과 누설 및 감청장비의 사용행위, 감청(형사사건의 수사 과정에서 합법적으로 이루어진 감청을 포함한다)으로 취득한 정보임을 알거나 알 수 있었음에도 이러한 정보를 사용하는 행위는 금지된다. 미수범은 처벌한다

(2) 유선 및 전자통신서비스 프로바이더의 교환수, 직원, 대리인이 일상적인 업무활동으로 서비스의 정상적인 제공 또는 보호를 위하여 행하는 경우는 제외한다. (이하생략)

2-3. 불법정보 유통 관련 국내법 대응 현황 및 개정 필요성 검토

가. 아동포르노그래피의 구성요건

(1) 협약상의 구성요건

○ (정의) 사이버범죄협약은 아동이 실연하거나 아동이 실연하는 것으로 보여질 수 있는 포르노물의 제작, 제공, 전송과 배포, 획득과 소지 등을 모두 포괄하여 범죄로 정의

- 협약 제9조 1항에서 정의한 아동포르노물 관련 범죄란 고의로 범해진 행위에 따라 아동포르노물의 전자적 제조, 소지 및 배포에 관한 다양한 행위를 범죄로서 처벌하도록 규정하고 있음

[유럽사이버범죄협약 제9조]

1. 각 당사국은 권한 없이 고의로 범해진 다음의 행위를 국내법상 범죄로 하는데 필요한 입법 및 그 밖의 조치를 취해야 한다

a 컴퓨터 시스템을 통하여 아동포르노를 제작하는 행위
b. 컴퓨터 시스템을 통하여 아동포르노를 이용하도록 하거나 제공하는 행위
c. 컴퓨터 시스템을 통하여 아동포르노를 배포 또는 전송하는 행위
d. 본인이나 타인을 위하여 컴퓨터 시스템을 통하여 아동포르노를 획득하는 행위
e. 컴퓨터데이터 저장매체 또는 컴퓨터시스템에서 아동포르노를 소지하는 행위

2. 제1항의 아동포르노에는 다음 행위를 시각적으로 묘사하는 포르노물을 포함시켜야 한다

a. 성적으로 노골적인 행위를 실연하는 미성년자
b. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 행위하는 사람
c. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 보여주는 사실적인 이미지

3. 제2항의 미성년자에는 18세 이하의 사람이 모두 포함되어야 한다. 당사국은 연령을 낮출 수 있으나, 최저 16세 이상이어야 한다

- 다만 제2조·제8조와 마찬가지로 고의로 행위한 경우만을 처벌하기에, 아동음란물의 취득 또는 소지, 미성년자로 보이는 자 또는 사실적 이미지로서 미성년자의 성적 행위를 대상으로 한 여러 행위들은 처벌받지 않음
- 대표적인 범죄로는 아동음란물, 협박 또는 복수 목적으로 몰래 촬영한 성관계 사진 또는 영상물을 유포하거나 영리 목적으로 제공하는 디지털 성범죄, 인터넷 도박 범죄 등이 이에 해당됨

○ (행위태양설명) 협약에서 규정한 5가지 행위태양은 각각 다음의 세부적 행위를 포섭함

<표 3-36> 협약 제9조의 주석서에 따른 행위태양 설명

행위태양	주석서 내용
a. 제작하는 행위	아동포르노그래피의 제작
b. 이용하도록 하거나 제공하는 행위	이용하도록 하는 행위는 타인의 사용을 위해 온라인 상에 업로드하거나 하이퍼링크를 설정하거나 편집하는 행위를 의미하며, 제공은 타인이 아동포르노그래피를 얻을 수 있도록 권유하는 행위를 포함하여, 타인에게 아동포르노그래피를 제공하는 행위를 의미
c. 배포 또는 전송하는 행위	배포는 적극적인 유포행위를 의미하며 전송은 타인에게 아동포르노그래피를 컴퓨터네트워크를 통해 전달하는 행위를 의미

d. 획득하는 행위	다운로드와 같이 아동포르노그래피를 적극적으로 획득하는 행위
e. 소지하는 행위	컴퓨터시스템이나 디스켓, 시디롬과 같은 저장매체에 저장해서 보유하는 행위

○ (유보가능조항) 획득과 소지 행위와, 성인이 미성년자가 실연하는 것처럼 행위하거나 보여주는 포르노물에 대해서 유보가능

- 제9조4항에 따라, 제9조제1항제d호, 제e호, 제2항 제b호, 제c호의 일부 또는 전체를 적용하지 아니할 권리를 유보할 수 있다고 규정

[협약 제9조에서 유보가능한 조항]
1. 각 당사국은 권한 없이 고의로 범해진 다음의 행위를 국내법상 범죄로 하는데 필요한 입법 및 그 밖의 조치를 취해야 한다
d. 본인이나 타인을 위하여 컴퓨터 시스템을 통하여 아동포르노를 획득하는 행위
e. 컴퓨터데이터 저장매체 또는 컴퓨터시스템에서 아동포르노를 소지하는 행위
2. 제1항의 아동포르노에는 다음 행위를 시각적으로 묘사하는 포르노물을 포함시켜야 한다
b. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 행위하는 사람
c. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 보여주는 사실적인 이미지
4. 각 당사국은 제9조 제1항 제d호, 제1항 제e호, 제2항 제b호, 제2항 제c호의 일부 또는 전체를 적용하지 아니할 권리를 유보할 수 있다

(2) 국내법 대응 법규 검토

○ (대응법규) 협약 제9조는 국내의 아동청소년보호법(이하 청소년성보호법), 형법, 정보통신망법, 성폭력범죄의 처벌 등에 관한 특례법, 청소년보호법에 대응

- '아동청소년의 성보호에 관한 법률(이하 청소년보호법)'개정(법률 제17352호, 2020. 6. 9)으로 협약 제9조의 내용이 대체로 대응됨

<표 3-37> 협약 제9조에 대응하는 국내 대응 법규 현황

협약 제9조		대응법규
제1항	제a호	• 청소년성보호법 제11조 제1항과 제2항
	제b호	• 청소년성보호법 제11조 제2항과 제 3항 • 정보통신망법 제44조 제1항 제1호와 제 74조 제1항 제2호
	제c호	• 청소년성보호법 제11조 제 2항과 제 3항 • 정보통신망법 제44조 제1항 제1호와 제 74조 제1항 제2호

		• 성폭력범죄의 처벌 등에 관한 특례법 제13조
	제d호	• 청소년성보호법 제11조 제2항과 제 5항
	제e호	• 청소년성보호법 제11조 제2항과 제 5항
제2항		• 청소년성보호법 제2조 제5항
제3항		• 청소년보호법 제2조 제1항

○ (아동청소년보호법) 협약 제1항 제a호~제e호는 아동포르노그래피 관련 행위태양을 규정하고 있으며 우리나라의 경우 이와 관련된 범죄는 '아동청소년의 성보호에 관한 법률(이하 청소년보호법)'에서 규정하고 있음

- 형법 제243조(음화반포), 형법 제244조(음화제조)를 통한 처벌도 고려할 수 있으나 아동포르노그래피와 관련된 범죄는 청소년성보호법에서 규정하고 있으므로 이를 적용하는 것이 적합함
- 개정된 청소년성보호법 (법률 제17352호, 2020. 6. 9)은 사이버범죄협약의 아동포르노그래피 관련 행위태양을 반영하는 형태로 개정됨
  - ▸ 컴퓨터 시스템을 통하여 아동포르노를 제작하는 행위(제1항 a)는 제11조제1항1호에 해당
  - ▸ 컴퓨터 시스템을 통하여 아동포르노를 제공하는 행위(제1항 b)와 배포· 전송하는 행위(제1항 c)는 제11조 제2항과 제3항에 해당
  - ▸ 컴퓨터 시스템을 통하여 아동포르노를 획득하는 행위(제1항 d)와 소지하는 행위(제1항 e)는 제11조 제2항과 제5항에 해당

<표 3-38> 협약 제9조 제1항 대응법규-청소년 성보호법

사이버범죄협약 제9조	청소년성보호법 제11조
a 컴퓨터 시스템을 통하여 아동포르노를 제작하는 행위	① 아동·청소년성착취물을 제작·수입 또는 수출한 자는 무기징역 또는 5년 이상의 유기징역에 처한다. ④ 아동·청소년성착취물을 제작할 것이라는 정황을 알면서 아동·청소년을 아동·청소년성착취물의 제작자에게 알선한 자는 3년 이상의 징역에 처한다.
b. 컴퓨터 시스템을 통하여 아동포르노를 이용하도록 하거나 제공하는 행위	② 영리를 목적으로 아동·청소년성착취물을 판매·대여·배포·제공하거나 이를 목적으로 소지·운반·광고·소개하거나 공연히 전시 또

c. 컴퓨터 시스템을 통하여 아동포르노를 배포 또는 전송하는 행위	는 상영한 자는 5년 이상의 징역에 처한다. ③ 아동・청소년성착취물을 배포・제공하거나 이를 목적으로 광고・소개하거나 공연히 전시 또는 상영한 자는 3년 이상의 징역에 처한다.
d. 본인이나 타인을 위하여 컴퓨터 시스템을 통하여 아동포르노를 획득하는 행위	② 영리를 목적으로 아동・청소년성착취물을 판매・대여・배포・제공하거나 이를 목적으로 소지・운반・광고・소개하거나 공연히 전시 또는 상영한 자는 5년 이상의 징역에 처한다. ⑤ 아동・청소년성착취물을 구입하거나 아동・청소년성착취물임을 알면서 이를 소지・시청한 자는 1년 이상의 징역에 처한다.
e. 컴퓨터데이터 저장매체 또는 컴퓨터시스템에서 아동포르노를 소지하는 행위	

- 개정된 청소년성보호법은 사이버범죄협약에서 정의한 아동포르노그래피보다 포괄하는 행위태양이 보다 넓음
  - ▸ 국내 청소년성보호법은 컴퓨터 시스템 등 사용수단에 대한 규정이 없고, 사이버범죄협약에서 명기하지 않은 수입, 수출, 운반, 광고, 소개, 제작알선, 시청 등을 포괄하고 있어 행위태양의 범위가 보다 넓음
- 국내 청소년성보호법은 아동・ 청소년이 직접 등장하거나 성인이 아동・ 청소년으로 오인될 수 있도록 실연하는 포르노그래피를 모두 아동・ 청소년성착취물로 포섭하여 협약 제9조제2항에 대응함
  - ▸ 국내 청소년성보호법상 "아동・청소년성착취물"이란 "아동・청소년 또는 아동・청소년으로 명백하게 인식될 수 있는 사람이나 표현물이 등장하여 제4호의 어느 하나에 해당하는 행위를 하거나 그 밖의 성적 행위를 하는 내용을 표현하는 것으로서 필름・비디오물・게임물 또는 컴퓨터나 그 밖의 통신매체를 통한 화상・영상 등의 형태로 된 것을 말한다"로 규정하고 있어, 협약의 9조2항을 모두 반영함

<표 3-39> 협약 제9조 제2항 대응법규

사이버범죄협약 제9조	청소년성보호법 제2조
2. 제1항의 아동포르노에는 다음 행위를 시각적으로 묘사하는 포르노물을 포함시켜야 한다 a. 성적으로 노골적인 행위를 실연하는 미성년자 b. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 행위하는 사람 c. 성적으로 노골적인 행위를 미성년자가 실연하는 것처럼 보여주는 사실적인 이미지	제2조(정의) 5. "아동·청소년성착취물"이란 아동·청소년 또는 아동·청소년으로 명백하게 인식될 수 있는 사람이나 표현물이 등장하여 제4호의 어느 하나에 해당하는 행위를 하거나 그 밖의 성적 행위를 하는 내용을 표현하는 것으로서 필름·비디오물·게임물 또는 컴퓨터나 그 밖의 통신매체를 통한 화상·영상 등의 형태로 된 것을 말한다.아동·청소년 이용음란물의 개념

- 협약 제9조 제3항는 아동포르노그래피 관련 미성년자 나이를 규정하고 있으며 이는 국내 청소년성보호법 제2조 제5호가 대응

<표 3-40> 협약 제9조 제3항 대응법규

사이버범죄협약 제9조	**청소년성보호법 제2조**
3. 제2항의 미성년자에는 18세 이하의 사람이 모두 포함되어야 한다. 당사국은 연령을 낮출 수 있으나, 최저 16세 이상이어야 한다	제2조(정의) 1. "청소년"이란 만 19세 미만인 사람을 말한다. 다만, 만 19세가 되는 해의 1월 1일을 맞이한 사람은 제외한다.

- 다만 협약은 “고의성” 여부에 중점을 둔 반면, 국내 청소년성보호법은 고의성보다 “인지” 여부에 중점을 두고 있으며, 고의성(영리목적) 여부는 배포· 제공과 이를 목적으로 광고·소개 · 전시· 상영하는 행위에서 양형기준으로 적용되고 있어 차이가 있으며, 보다 포괄적임

○ (정보통신망법) 사이버범죄협약에서 정의하고 있는 기술수단(컴퓨터시스템 등)과 관련된 규정은 국내 정보통신망법의 불법정보 유통에 관한 규정이 대응할 수 있음

- 협약 제9조 제1항 제b호는 컴퓨터시스템을 통한 아동포르노그래피를 이용가능하게 하거나 제공하는 행위는 아동포르노그래피가 컴퓨터 시스템에 업로드된 형태를 전제로 하고 있기 때문에, 컴퓨터 시스템으로 전송될 수 있는 형태로 변환되거나 제조되어야

협약에서 정의한 처벌대상으로 규정됨

- 국내 정보통신망법 제 44조의7은 정보통신망을 통하여 유통하는 행위만을 규제하기 때문에, 협약 제9조 제1항 b에 근거한 제공하는 행위, 제9조 제1항 c에 근거한 배포·전송하는 행위에 해당함
- 이 때 배포는 컴퓨터 시스템을 통해 다수의 타인에게 적극적 유포행위를 의미하며 전송은 컴퓨터 시스템을 통해 타인에게 전송하는 것을 의미하는데, 이때 망 법 제44조의7제1항제1호를 받은 처벌 규정인 제 74조제1항제2호에서 "배포·판매·임대하거나 공공연하게 전시한 자"로 정의하고 있어, 협약 제9조 제1항c에서 정의한 배포·전송 중 배포만이 망법에 포섭된다고 할 수 있음

<표 3-41> 협약 제9조 제1항 대응법규-정보통신망법

사이버범죄협약 제9조	정보통신망법
1. 각 당사국은 권한 없이 고의로 범해진 다음의 행위를 국내법상 범죄로 하는데 필요한 입법 및 그 밖의 조치를 취해야 한다 b. 컴퓨터 시스템을 통하여 아동포르노를 이용하도록 하거나 제공하는 행위 c. 컴퓨터 시스템을 통하여 아동포르노를 배포 또는 전송하는 행위	제44조의7(불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다. 1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보 제74조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 2. 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자

○ (성폭력처벌법) 협약 제9조 제1항 b와 c가 정의하고 있는 전송행위는 국내 성폭력처벌법 제 14조도 일부 대응함

- 협약 제9조 제1항 제c호의 '배포'는 적극적으로 포르노 유포하는 것으로 정보통신망법 제74조 제1항 제2호가 적용 가능하지만, '전송'의 경우 성폭력범죄의 처벌 등에 관한 특례법 제14조 통신매체이용음란죄가 대응한다고 볼 수도 있음

- 그러나 성폭력처벌법은 '자기 또는 다른 사람의 성적욕망 유발·만족시킬' 목적을 지닐 경우로 한정하고 있어, 성적 욕망과의 연계성을 고려하지 않고 '고의성'을 기준으로 삼는 협약과는 범위가 좁음

※ 통신매체이용음란죄의 경우 '자기 또는 다른 사람의 성적욕망을 유발하거나 만족시킬 목적'을 가져야하는데, 해당 목적 없이 컴퓨터 시스템을 통하여 아동포르노 전송하는 행위는 동법에 포섭되지 아니함

<표 3-42> 협약 제9조 제1항 대응법규- 정보통신망법 및 성폭력처벌법 비교

사이버범죄협약 제9조	국내 대응법규
1. 각 당사국은 권한 없이 고의로 범해진 다음의 행위를 국내법상 범죄로 하는데 필요한 입법 및 그 밖의 조치를 취해야 한다 c. 컴퓨터 시스템을 통하여 아동포르노를 배포 또는 전송하는 행위	• (배포) 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자(정보통신망법 제74조 제1항 제2호) • (전송) 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 2년 이하의 징역 또는 200만원 이하의 벌금에 처한다(성폭력범죄의 처벌 등에 관한 특례법 제13조 통신매체이용음란죄)

○ 개정된 청소년성보호법은 기술적 수단의 사용여부와 상관없이 아동청소년 성착취물의 제작, 전송, 배포, 소지, 시청 등을 포괄적으로 포함하고 있어 사이버범죄협약 제9조의 행위태양을 대체로 포섭한다고 보는 것이 타당하며, 정보통신망법이나 성폭력처벌법의 타법보다는 개정된 청소년성보호법의 법규가 대응한다고 보는 것이 바람직함

나. 형사절차와 국제공조의 규정

(1) 협약상의 형사절차와 국제공조 규정

○ (수단과 절차) 사이버범죄협약은 수사를 위해 전자적 증거수집에 필요한 절차와 수단을

규정하고 있으며, 협약 당사국도 이를 위한 국내 입법 조치를 요구하고 있음

- 수사절차상 도구로써, 전자기록의 신속한 보전(제16조~제17조), 수색과 압수(제18조~제19조), 데이터의 실시간 수집과 감청(제20조~제21조) 등에 관한 내용이 포함되어 있음
- 또한 이를 위한 국제공조에 관한 사항으로 전자기록의 신속한 보전(제29조~제30조), 상호법률지원을 위한 컴퓨터 접속허용(제31조~제32조), 상호법률지원을 위한 감청허용(제33조~제34조), 24시간 연락망 가동(제35조) 등이 규정되어 있음

<표 3-43> 디지털증거확보를 위해 가입국들이 자국법에 갖추어야할 절차규정

구분		내용
전자기록의 신속한 보전	제16조(저장된 컴퓨터 데이터의 신속한 보전)	1. 컴퓨터시스템에 의해서 저장되어 있는 통신데이터를 포함한 특정한 컴퓨터데이터가 특히 손실되거나 변경될 수 있다고 믿을 만한 근거가 있는 경우에는 이러한 자국의 권한 있는 기관이 데이터의 신속한 보존을 명령하거나 이와 유사한 방법으로 획득할 수 있도록 가입국은 필요한 입법적 조치와 그 밖의 조치를 취하여야 한다.
	제17조(트래픽 데이터의 신속한 보전 및 제출)	1. 각 가입국은 제16조에 의하여 보존될 통신데이터와 관련하여, a) 하나 또는 그 이상의 서비스제공자가 이 통신의 중개에 참여하고 있는지에 관계없이 통신데이터의 신속한 보존이 가능하고, b) 가입국이 서비스제공자 및 통신의 전송 경로를 확정할 수 있도록 충분한 양의 통신데이터가 가입국의 관할기관이나 이 기관으로부터 지명받은 자에게 즉시 제출(공개)되도록 필요한 입법적 조치와 그 밖의 조치를 취해야 한다.
전자기록의 수색과 압수	제18조(컴퓨터 데이터 제출명령)	1. 각 당사국은 a. 어떤 자가 자국의 영토 내에서 컴퓨터 시스템 또는 컴퓨터 데이터 저장매체에 저장되어 있는 특정한 컴퓨터 데이터를 보유하고 있거나 관리하고 있는 경우 이를 제출하고, b. 서비스 제공자가 당사국의 영토 내에서 보유하고 있거나 관리하고 있는 자신의 서비스와 관련한 가입자 정보를 제출하도록 명령할 권한을 관할 기관에게 부여하도록 필요한 입법적 조치와 그 밖의 조치를 취해야 한다. (생략) 3. 이 종에서 의미하는 가입자 정보란, 서비스 제공자가 보유하고 있는 서비스 이용자에 관한 정보 중 트래

		픽 데이터 또는 내용 데이터를 제외한 컴퓨터데이터의 형태로 되어 있거나 이와 다른 형태로 되어 있는 모든 정보로서 다음을 확인할 수 있는 정보를 말한다. a. 이용 중인 통신서비스의 종류, 이 통신서비스를 위해서 기술적 조치 및 서비스의 이용기간 b. 가입자의 신원, 주소, 전화번호 및 그밖의 접속번호, 통신서비스와 관련한 계약이나 협약에 근거해서 이용될 수 있는 요금의 청구 및 지급에 관한 정보 c. 서비스 계약 또는 협약에 근거한 통신기기의 설치장소에 관한 그 밖의 정보
	제19조(저장되어 있는 컴퓨터데이터의 수색과 압수)	1. 각 당사국은 관할기관에게 다음 각호에 대하여 자국의 영토 내에서 수색하거나 이와 유사한 방식으로 거기에 접근할 권한을 부여하기 위해서 필요한 입법적 조치 및 그밖의 조치를 해야한다. a. 컴퓨터시스템 또는 그 일부 및 거기에 저장되어 있는 컴퓨터 데이터 b. 컴퓨터데이터가 저장될 수 있는 컴퓨터 데이터 저장매체. (생략) 3. 각 당사국은 관할기관에게 제1항과 제2항에 의해서 접근한 컴퓨터 데이터를 압수하거나 이와 유사한 방법으로 확보하기 위한 권한을 부여하기 위해서 다음과 같은 필요한 입법적 조치와 그 밖의 조치를 취해야한다. a. 컴퓨터 시스템 또는 그 일부 혹은 컴퓨터 저장매체를 압수하거나 이와 유사한 방법으로 확보할 권한 b. 컴퓨터데이터를 복제하여 보유할 권한 c. 저장되어 있는 해당 컴퓨터데이터의 완전성을 보전할 권한 d. 접근한 컴퓨터시스템에 있는 컴퓨터데이터에 접근을 불가능하게 하거니 이로부터 분리할 권한 (생략)
데이터의 실시간 수집 및 감청	제20조(트래픽 데이터의 실시간 보전)	1. 당사국은 자국의 관할기관이 자국의 영토내에서 컴퓨터시스템을 통하여 전송되는 특정한 통신과 관련한 트래픽데이터를 실시간으로, a. 자국의 영토 내에서 기술적 수단을 사용하여 수집하거나 기록하고, b. 서비스 제공자에게 현재의 기술적 능력내에서, i. 자국의 영토내에 있는 기술적 수단을 사용하여 수집하거나 기록하고, ii. 수집하거나 기록하는 경우 관할 기관과 협력하고 지원하도록 입법적 조치와 그 밖의 조치를 취하여야 한다. (생략)

	제21조(통신내용데이터의 실시간 수집)	1. 당사국은 관할기관에 대해서 자국의 국내법에서 정한 중대한 범죄 범위내에서 a. 자국의 영역 내에 있는 컴퓨터 시스템을 이용하여 전달되는 특정한 통신의 내용데이터를 자국의 영역내에서 기술적 수단을 사용하여 실시간으로 수집하거나 기록하고, b. 서비스 제공자의 기술적 가능성과 관련하여, I. 자국의 영역내에서 기술적인 수단을 사용하여 그러한 내용데이터를 실시간으로 수집하거나 기록하고, 또는 ii. 그러한 내용관련 데이터의 실시간 수집 및 기록의 경우에 권한있는 기관과 협력하고 이를 지원할 의무를 서비스제공자에게 부여하도록 필요한 입법적 조치와 그밖의 조치를 위해야 한다. 2. 당사국이 제1항 제a호에서 언급한 조치를 자국의 국내법질서에서 확정된 원칙들에 의해서 취할 수 없는 경우에는, 당사국은 그 대신 자국의 영역 내에서 특정한 통신의 내용데이터가 자국의 영역내에서 기술적인 수단을 사용하여 실시간으로 수집되고 기록되도록 할 수 있는 필요한 입법적 조치와 그밖의 조치를 취해야한다. (생략)

○ (전자기록의 신속한 보전) 협약은 ISP나 인터넷서비스제공자에 의해서 수집되었거나 획득된 데이터의 보전과 제출받을 수 있는 권한에 관한 규정(제16조와 제17조)을 요구

- 저장된 컴퓨터가 손괴 또는 변경될 수 있다고 판단될 경우 이를 보존하도록 강제할 수 있도록 수시기관(법집행기관)에 권한을 부여하도록 하고 있음(협약 제16조)
- 또한 수사시간이 통신경로를 확인하기 위해 ISP에게 접속기록 등의 통신데이터에 대해 신속한 보존명령을 내리고 제출받을 수 있는 권한을 부여하도록 하고 있음(협약 제17조)
- 이 두 조항은 실시간 또는 새롭게 데이터를 수집하거나 획득하는 행위와 관련된 것은 아니고, 제 14조에 의해서 협약에 규정된 모든 권한과 절차는 '특별한 형사법상의 수사 또는 절차의 목적을 위한 것'으로 한정되며, 이러한 목적에 따라 이미 컴퓨터 시스템에 의해 저장되어 있는 데이터를 보전하는 것과 관련되어 있음
- 물론 보전의 방법과 상세한 절차는 당사국에 위임되어 있으나, 통신과정의 중계에 관계된 다수의 서비스제공자가 '충분한 양의 통신데이터'를 관할기관에 즉시 공개하도록 하기 위해서는 보전명령을 받는 사업자의 범위와 공개방식, 공개되는 데이터의 범위 등에

대한 상세한 절차규정이 입법조치 되어야 함

○ (전자기록의 수색과 압수) 협약은 전기통신서비스 제공자 등이 보유한 가입자 정보에 접근할 권한(제18조와 제19조)에 관해 회원국에게 입법할 것을 요구하고 있음

- 제18조와 제19조는 이미 수집되어 있는 전자기록의 수색과 압수 등에 관한 사항
- 제18조는 자국 내의 전자기록을 보유 또는 관리하는 자, 또는 전기통신 서비스 제공자에게 가입자 정보와 전자기록에 대해 관할기관이 제출명령을 내릴 수 있도록 하는 조항을 입법할 것을 요구하고 있으며, 제출자료에 포함되는 가입자 정보는 이용 중인 통신서비스 내역, 가입자를 식별할 수 있는 인적정보(신원, 주소, 전화번호 등), 그 밖의 통신기기 설치장소에 관한 정보 등이 포함됨
- 제19조는 컴퓨터데이터가 저장될 수 있는 컴퓨터시스템 또는 저장매체에 대한 수색과 압수를 위한 절차규정을 입법할 것을 요구함

○ (데이터의 실시간 수집 및 감청) 협약은 회원국의 관할기관이 트래픽데이터(제20조)와 통신데이터(제21조)를 실시간으로 수집· 기록하거나 이와 관련하여 서비스제공자가 협조할 의무를 부여하는 입법적 조치를 요구함

- 제20조는 회원국이 자국의 영토 내에서 특정한 통신과 관련한 트래픽 데이터를 실시간으로 수집하거나 기록하고, 서비스제공자에게 수집하거나 기록할 경우 관할기관에 협조하도록 하는 입법적 조치를 요구함
- 제21조는 중대한 범죄와 관련하여 통신의 내용데이터를 실시간으로 수집하거나 기록하고, 서비스제공자에게 수집하거나 기록할 경우 관할기관에 협조하도록 하는 입법적 조치를 요구함

○ (국제공조 절차법 규정) 저장된 컴퓨터데이터 접근에 관한 공조(제31조), 저장된 컴퓨터데이터 초국경적 접근(제32조), 트래픽 데이터 실시간 수집에 관한 상호공조(제33조)를 위해 당사국의 일정한 권리와 의무 요구하고 있음

- 제31조는 협약에 가입한 국가 간에 데이터의 수색, 접속, 압수 및 획득을 요청할 권한과 그에 공조할 의무를 규정하고 있음

[유럽 사이버범죄협약 제31조]

제31조(저장된 컴퓨터 데이터의 접근에 관한 공조) 1. 당사국은 제 29조에 따라 보전되어 있는 데이터를 포함하여 피요청국의 영역 내에 위치한 컴퓨터 시스템을 통해서 저장된 데이터의 수색 및 유사한 접속, 압수 및 유사한 획득 또는 공개를 피요청국에 요청할 수 있다.

2. 피요청국은 제 24조에 의한 국제합의, 협정 및 법률의 적용을 통하여 그리고 제 3장의 다른 규정에 따라서 요청에 회신하여야 한다.

3. 공조는 a. 관련 데이터가 특히 손상 또는 변경되기 쉽다고 믿을만한 근거가 있거나, b. 신속한 공조제공 또는 제 2항의 합의, 협정 및 법률이 있는 경우에는 신속한 공조제공 원칙에 따라 회신되어야 한다.

- 제32조는 접근하고자 하는 데이터가 지리적 위치에 관계없이 공개접근이 가능한 경우와, 당사국이 자신의 영역 내에 있는 컴퓨터 시스템을 통해서 자신의 영역 외부에 있는 데이터에 접근하거나 또는 자신의 영역 내에 있으면서 다른 당사국에 저장되어 있는 컴퓨터 데이터를 공개할 정당한 권한이 있는 자로부터 자발적 동의를 받아서 정보를 공개할 경우 접근할 권한이 있다고 정의하고 있음
- 예를 들어서 국내에서 미국 구글 서버에 저장된 데이터에 접근할 때에, 우리정부가 미국정부의 승인을 득하지 않고도 구글의 국내 대리인으로부터 자발적인 동의를 얻어서 미국 서버에 저장된 데이터에 접근하거나 획득하는 경우에 해당함

[유럽 사이버범죄협약 제32조]

제32조(동의에 의해서 또는 공개 접근이 가능한 경우 저장된 컴퓨터 데이터의 초국경적 접근) 당사국은 다른 당사국으로부터 권한을 부여받지 아니한 상태에서

a. 데이터의 지리적 위치에 관계없이 공개접근이 가능한 저장된 컴퓨터 데이터(오픈소스)에 접근할 수 있고 또한

b. 만일 당사국이 당사국에 있는 컴퓨터 시스템을 통해서 당사국에게 데이터를 공개할 정당한 권한을 가진 자의 자발적인 동의를 얻은 경우에는 다른 당사국에 저장되어 있는 컴퓨터 데이터에 접근하거나 수신할 수 있다

- 제33조는 당사국의 수사기관이 다른 당사국에 있는 컴퓨터 시스템을 통과하는 통신과 관련하여 실시간으로 트래픽을 획득할 수 있도록 상호공조를 제공할 의무에 대해서 규정하고 있음

[유럽 사이버범죄협약 제33조]

제33조(트래픽 데이터의 실시간 수집에 관한 상호공조) 1. 당사국은 컴퓨터

시스템으로 전송되는 자국의 영역 내의 특정 통신과 관계있는 트래픽 데이터의 실시간 수집에 관한 상호공조를 제공해야 한다. 제 2항에 따른 공조는 자국법이 규정한 요건과 절차를 준수해야 한다.
2. 각 당사국은 최소한 트래픽 데이터의 실시간 수집이 자국의 유사한 사건에 적용될 수 있는 범죄에 관해서는 공조를 제공해야 한다.

○ (절차) 협약 가입은 유럽회의 회원국의 만장일치의 동의가 필요함

- 절차적으로는 유럽회의 각료위원회가 협약 가입국의 협의를 거쳐 만장일치의 동의를 얻는 과정이 필요하며, 가입서를 기탁한 날로부터 3개월이 경과한 후에 발표되도록 해야 함

[유럽 사이버범죄협약 제37조]

제37조 (협약의 가입) 1. 동 협약의 발효 이후에 유럽회의 각료위원회는 동 협약 가입국의 협의 및 만장일치의 동의를 얻은 후에 유럽회의 회원국이 아닌 또는 협약의 검토·제정에 참여하지 아니한 일체의 국가에게 동 협약의 가입을 요청할 수 있다.
2. 제1항에 따라서 동 협약에 가입하는 국가의 경우 동 협약은 유럽회의 사무총장에게 가입서를 기탁한 날로부터 3개월을 경과한 후 그 다음 달의 첫째 일에 발효되도록 해야 한다.

(2) 국내법 대응 법규 검토

○ (국내 대응법규) 전자기록의 신속한 보전, 수색, 압수, 실시간 수집 및 감청과 관련하여 협약이 요구하는 요건들은 국내 통신비밀보호법, 형사소송법, 전기통신사업법에 일부 대응하는 내용이 존재

- 전자기록의 신속한 보전: 통신비밀보호법상의 통신사실 확인자료의 제공과 관련한 조항들(제13조, 제15조의 2, 시행령 제41조)가 관련되나 제공되는 자료의 범위와 전기통신사업자의 협조의 범위에 차이가 있으며, 보전명령을 위한 근거조항이 부재함
- 전자기록의 수색과 압수: 형사소송법 제 106조 제3항에 수색과 압수에 관한 근거 조항을 적용할 수 있음
- 데이터의 실시간 수집 및 감청: 통신비밀보호법상 범죄수사를 위한 통신제한조치의 허가요건이 일부 관련되나, 회원국에게 실시간 수집 및 감청 데이터에 접근할 수 있는

권한을 광범위하게 요구하는 협약과는 상충됨

<표 3-44> 사이버범죄협약의 절차법 규정에 대한 국내 대응법규

구분	사이버범죄협약	대응법규
전자기록의 신속한 보전	제16조(저장된 컴퓨터 데이터의 신속한 보전)	• 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차) • 통신비밀보호법 제15조의2(전기통신사업자의 협조의무) • 동법 시행령 제41조(전기통신사업자의 협조의무 등)
	제17조(트래픽데이터의 신속한 보전 및 제출)	
전자기록의 수색과 압수	제18조(컴퓨터데이터 제출명령)	• 형사소송법 제 106조 제3항 • 전기통신사업법 제83조 제3항
	제19조(저장되어 있는 컴퓨터데이터의 수색과 압수)	
데이터의 실시간 수집 및 감청	제20조(트래픽데이터의 실시간 보전)	• 통신비밀보호법 제5조(범죄수사를 위한 통신제한조치의 허가요건)
	제21조(통신내용데이터의 실시간 수집)	

- 협약에서 규정하고 있는 데이터의 신속한 보전· 수색· 압수 및 트래픽데이터와 통신내용데이터의 실시간 수집 등은 개인정보보호법, 통신비밀보호법, 전기통신사업법 등에서 보호하는 권익을 침해할 여지가 있어 관련조항의 일부개정 내지는 관련 법률의 신설이 필요함

<표 3-45> 사이버범죄협약의 절차법 규정과 국내법규 상충우려

구분	사이버범죄협약	국내법 상충우려
전자기록의 신속한 보전	제16조(저장된 컴퓨터 데이터의 신속한 보전)	<개인정보보호법> • 개인정보보호법상 이용자의 동의가 요구되며, 데이터보전, 수색, 압수, 감청은 정보의 자기결정권 침해 우려가 있음 <통신비밀보호법> • 통신비밀보호법에 보존대상이 되는 컴퓨터데이터에 대한 정의조항이 없음 • 통신비밀보호법상 통신경로, 통신크기 등 트래픽데이터의 범위가 명시되지 않음 • 통신비밀보호법상 전기통신사업자의 자료제출의 범위는 통신사실확인자료에만 제한
	제17조(트래픽데이터의 신속한 보전 및 제출)	
전자기록의 수색과 압수	제18조(컴퓨터데이터 제출명령)	
	제19조(저장되어 있는 컴퓨터데이터의 수색과 압수)	

데이터의 실시간 수집 및 감청	제20조(트래픽데이터의 실시간 보전)	• 통신비밀보호법상 범죄수사를 위한 통신제한조치(감청)의 허가요건에 사이버범죄가 포함되어 있지 않음 <전기통신사업법> • 전기통신사업법상 법원, 수사기관, 정보기관의 요청에 따른 통신자료제출이 의무사항이 아님
	제21조(통신내용데이터의 실시간 수집)	

□ 개인정보보호법

○ (자기결정권 침해우려) 현행 법률상 개인정보 국외 이전 시 목적이나 형태 불문하고 사전 동의를 요구하고 있으므로, 협약에 따라 회원국에게 저장된 전자기록을 제공하거나 접근을 허용할 경우 개인정보보호법에서 보호하는 개인정보의 자기결정권을 침해할 우려가 있음

- 국내법은 개인정보의 국외 이전에 대해서 엄격하게 제한하고 있는데, 개인정보보호법 제17조와 제39조의 12는 개인정보 국외 제공 시 정보주체의 사전 동의를 요구하고 있음
- 2020년 8월 5일부터 시행되는 개정된 개인정보법은 이미 국외로 이전된 개인정보도 제 3국으로 재이전할 경우 국외 이전 규정을 준용하도록 하는 조항이 신설되어, 원칙적으로 국외이전과 동일하게 정보주체로부터 동의를 받도록 하고 있어 이전보다 엄격해짐
- 국외이전을 위해 정보주체에게 고지해야 하는 사항은 이전되는 개인정보의 항목, 개인정보가 이전되는 국가, 이전일시, 이전방법, 개인정보를 이전받은 자의 성명, 개인정보를 이전받은 자의 이용목적, 보유, 이용기간 등으로, 사실상 협약 제31~33조에 따라 해외 국가의 수사당국이 데이터의 수색, 접속, 압수 및 획득을 하는 것이 어렵다고 볼 수 있음

개인정보보호법 제17조(개인정보의제공) 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

개인정보보호법 제39조의 12(국외 이전 개인정보의 보호)[20] ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결해서는 아니 된다.

② 제17조제3항에도 불구하고 정보통신서비스 제공자등은 이용자의 개인정보를

국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 제3항 각 호의 사항 모두를 제30조제2항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.

③ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

⑤ 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제1항부터 제4항까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자등"은 "개인정보를 이전받는 자"로, "개인정보를 이전받는 자"는 "제3국에서 개인정보를 이전받는 자"로 본다.

□ 통신비밀보호법

○ (보존명령 근거조항 부재) 통신사업자에게 자료제출 협조요청의 근거는 있으나 자료를 보전하도록 명령할 근거 조항은 부재하여 자료보존명령을 위한 근거조항 신설이 필요함

- 협약 제16조와 제17조는 디지털 증거를 사전에 보전하기 위해 전기통신사업자에게 신속하게 데이터를 보전하도록 명령을 내리거나 일정기간 컴퓨터데이터와 트래픽데이터를 보존하도록 하는 규정을 마련할 것을 요구하고 있으나,
- 통신비밀보호법 제15조의2와 시행령 제41조 제2항은 통신사실확인자료의 보관과 제공에 대해서만 규정하고 있을 뿐, 협약 제16조와 제17조가 규정한 증거 확보를 위한 전자기록의 신속한 보전 명령에 해당한다고 보기 어려움

통신비밀보호법 제15조의2(전기통신사업자의 협조의무)

① 전기통신사업자는 검사·사법경찰관 또는 정보수사기관의 장이 이 법에 따라

---

20) 데이터3법 개정에 따라 국외 이전 개인정보의 보호 법률은 「정보통신망법」에서 「개인정보보호법」으로 이관됨

집행하는 통신제한조치 및 통신사실 확인자료제공의 요청에 협조하여야 한다.
② 제1항의 규정에 따라 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항, 통신사실확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정한다.
「통신비밀보호법 시행령 제41조(전기통신사업자의 협조의무)」
① 법 제15조의2에 따라 전기통신사업자는 살인·인질강도 등 개인의 생명·신체에 급박한 위험이 현존하는 경우에는 통신제한조치 또는 통신사실 확인자료제공 요청이 지체없이 이루어질 수 있도록 협조하여야 한다.
② 법 제15조의2제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다. 1. 법 제2조제11호가목부터 라목까지 및 바목에 따른 통신사실확인자료 : 12개월. 다만, 시외·시내전화역무와 관련된 자료인 경우에는 6개월로 한다. 2. 법 제2조제11호마목 및 사목에 따른 통신사실확인자료 : 3개월

- 따라서 협약 제16조와 제17조에 대응하기 위해서는 수사기관이나 관할기관이 특정요건을 충족할 경우 전기통신사업자에게 수사와 관련한 전자기록에 대한 보전을 명령할 수 있는 근거 조항이 신설되어야하며,
- 통신비밀보호법 제15조의 2나 시행령 제41조에 협조요청을 받은 전기통신사업자가 일정기간 동안 컴퓨터데이터를 손실이나 변경 없이 보관할 의무를 명시하고 해당 의무를 강제하도록 개정해야함

○ (전자기록의 범위) 협약에 의해서 신속한 보존 및 제출을 요구할 수 있는 자료의 범위가 국내 통신비밀보호법상 전기통신사업자의 협조의무의 자료범위와의 상충이 있고,
- 협약 제 16조와 제17조는 컴퓨터시스템에 의해 저장되어 있는 '컴퓨터 데이터'와 '트래픽 데이터' 모두를 보존하도록 하는 포괄적인 규정으로 전기통신사업자에게 광범위한 자료의 보전과 제출의무가 부과되나, 국내 통신비밀보호법에서 제출의무가 부과되는 자료의 범위는 "통신사실 확인자료" 만을 다루고 있음
- 협약 제1조(정의)에 따른 컴퓨터 데이터는 컴퓨터 시스템을 통하여 기능을 수행하기에 적합한 프로그램뿐만 아니라, 컴퓨터 시스템에서 처리하는 데 적합한 형태로 되어 있는 일체의 사실, 정보, 개념을 표현한 것으로 정의되어 있어 상당히 광범위하고 포괄적인 디지털정보자산을 의미함

▸ 협약 제1조에 따른 트래픽 데이터는 컴퓨터 시스템을 이용한 통신과 관련된 모든 컴퓨터 데이터로서 통신망의 일부를 구성하는 컴퓨터 시스템에 의해서 생성되고 통신의 발신지, 수신지, 경로, 일시, 크기, 지속시간, 또는 이용된 서비스의 유형을 나타내는 데이터를 의미함

- 국내의 경우 통신비밀보호법에 의해 수사기관의 요청에 따라 전기통신사업자가 통신사실확인자료를 3개월에서 12개월 보관하도록 규정하고 있으나, 통신비밀보호법 제2조(정의)에 따른 통신사실 확인자료는 가입자의 전기통신일시, 전기통신개시 및 종료시간, 사용도수 등 통신여부와 통신대상에 대한 정보로 한정

통신비밀보호법 제2조(정의)
11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
가. 가입자의 전기통신일시
나. 전기통신개시·종료시간
다. 발·착신 통신번호 등 상대방의 가입자번호
라. 사용도수
마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료
사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

- 따라서 통신비밀보호법 제2조에 통신사실확인자료의 수집정보의 범위를 확대하는 개정을 실시하거나, 이와는 별도로 신속한 보존을 적용할 수 있는 컴퓨터· 트래픽 데이터의 범위를 정의하는 조항을 신설하고 제15조의2의 개정을 통해 해당 데이터자료를 통신사업자가 제출해야하는 자료의 범위에 포섭해야함

<전자기록의 수색과 압수>

○ 컴퓨터데이터 수색과 압수는 현행법에서도 통신비밀보호법 제13조 통신사실확인자료 제공 절차와 형사소송법 제106조 제3항을 적용하면 일정부분 가능한 것으로 해석되나, 원격수색이나 수색과 압수의 절차에 관한 세부적인 사항들을 보완하는 법률개정이 필요함

- 협약 제19조 제1항은 수색과 압수의 대상물로 유형물인 컴퓨터와 저장매체 뿐만 아니라 무형물이 컴퓨터데이터까지 포섭하고 있으나, 우리의 형사소송법 제106조제3항은 컴퓨터용 디스크, 정보저장매체 등을 압수의 대상으로 명시하고 있으나 협약에서 요구하고 있는 컴퓨터데이터를 포섭하고 있지 않아, 이를 포섭하기 위한 개정이 필요함

형사소송법 제106조(압수) (생략)
③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.
④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18.>

- 또한 협약 제19조 제2항은 "자국 영토내의 다른 컴퓨터 시스템 또는 그 시스템의 일부에 저장되어 있을 때, ...(생략)..... 다른 시스템으로 신속하게 수색 또는 유사한 접근을 확대할 수 있도록 입법적 조치"를 취하도록 하고 있어, 원격수색을 허용하는 조항이 통신비밀보호법과 형사소송법에 신설되어야 한다는 견해가 있음(박희영 외, 2015)
- 최근 대법원 판례(2017도9747)에서는 적합한 압수・수색영장에 따라 이뤄진 것이라면 저장매체가 국외에 있는 경우라 하더라도 전자정보에 대한 원격수색이 적법하다고 판시한 바가 있음

[대법원 2017. 11. 29., 선고, 2017도9747, 판결]
【판결요지】 피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수·수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려받거나 현출된 전자정보를 대상으로 하여 범죄 혐의사실과 관련된 부분에 대하여 압수·수색하는 것은, 압수·수색영장의 집행을 원활하고 적정하게 행하기 위하여 필요한 최소한도의 범위 내에서 이루어지며 그 수단과 목적에 비추어 사회통념상 타당하다고 인정되는 대물적 강제처분 행위로서 허용되며, 형사소송법 제120조 제1항에서 정한 압수·수색영장의 집행에 필요한 처분에 해당한다. 그리고 이러한 법리는 원격지의 저장매체가 국외에 있는 경우라 하더라도 그 사정만으로 달리 볼 것은 아니다.

<데이터의 실시간 수집 및 감청>

○ 통신데이터 실시간 수집·기록(협약 제20·제21조)과 관련하여 통신비밀보호법 제5조에서 열거하고 있는 통신감청대상 범죄에 협약 제9조에 규정된 아동포르노 관련 항목을 포함시킬 필요가 있음

- 국내의 경우 통신비밀보호법 제15조의 2와 동법 시행령 제41조에 근거하여 개인의 생명·신체에 급박한 위험이 현존하는 경우 통신제한조치 또는 통신사실확인자료제공 요청을 지체 없이 이루어질 수 있도록 협조하여야 한다고 규정되어 있으나, 협약 제20조와 제21조가 요구하는 통신감청의 허용범위에 비해 협소함
- 또한 국내법에서 사이버범죄는 중대범죄에 해당하지 않기 때문에, 통신비밀보호법 제5조(범죄수사를 위한 통신제한조치 허가요건)에서 열거한 통신감청대상범죄는 주로 국가·기밀안보 등 국가적 차원의 범죄를 다루고 있어, 사이버범죄는 배제되어 있음

□ 전기통신사업법

○ (전기통신사업자의 협조의무) 제출명령(협약제18조)과 관련하여 국내 전기통신사업법상 제83조 제3항에서 수사기관이 수사를 위해 통신자료를 요청하면 '따를 수 있다'고 규정하지만 사업자가 응하지 않더라도 제재할 규정이 없음

- 국가기관의 통신자료 취득은 헌법상 기본권인 개인정보 자기결정권을 중대하게 침해할 수 있으므로 전기통신사업자가 법원이나 수사기관, 정보기관의 요청(전기통신사업법 제83조 3·4항)에 따른 통신자료 집행도 위헌(법률신문, 2016. 5. 18)

전기통신사업법 제83조(통신비밀의 보호)③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범 처벌법」 제10조제1항·제3항·제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청하면 그 요청에 따를 수 있다.

- 전기통신사업법 제83조제3항은 전자적 정보의 열람이나 제출요청에 대해 전기통신사업자가 “따를 수 있다”는 비강제적 협조 요청만을 명시하고 있고, 협조하지 않았을 경우에 대한 제재 조항이 없음
- 이는 협약 제18조 등의 가입자정보 제출 명령과 관련해서 강제성이 요구되기 때문에 협약에 상응하지 않는 면이 있음

다. 협약 가입 관련 검토

○ (현재의 공조수사체계) 우리는 이미 2011년 말에 유럽평의회 형사사법공조협약에도 가입되어 있고 원칙적으로 국제 형사사법공조는 국가간의 조약과 국내법인 국제형사사법공조법에 의해 진행되나, 조약이 체결되지 않은 경우에도 상대방 국가의 청구에 응한다는 보증을 하는 경우 상호주의에 따라 형사사법공조를 청구할 수 있음

- 사이버범죄협약에 가입하지 않고도 현재의 공조체계로도 아동성착취물 유통 등의 강력범죄에 대한 국제 공조수사가 불가능하지는 않음
- 현재 우리나라는 73 개국과 국제 형사 사법 공조조약, 77 개국과 죄인 인도 조약, 69 개국과 수감자 이송제도, 23 개국 또는 전 대륙 26 개 단체와 상호 협력 MOU를 체결한 상황(2020. 3월 기준)
  - ▸ ‘국제형사사법공조’는 형사사건의 수사·재판에 필요한 증거자료를 국가 상호 간에 수집·제공하는 절차를 의미하며, 2020. 3. 현재 우리나라는 전 세계 74개국과 국제형사사법공조조약이 체결되어 있음
- 또한 디지털증거의 신속한 보존과 공조를 위해 G7 24/7 High-tech Crime Network (이하 ‘G7 24/7 Network’)에 2000년 12월부터 가입한 상황으로, 미국, 영국, 일본, 호주 등 86개 국가와 디지털증거의 신속한 보존 조치와 첨단범죄 관련 범죄 정보, 법률자문 교환 등이 가능함(대검찰청 과학수사부 사이버수사과, 2020).
- 다만, G7 24/7 Network는 각국의 법이 허용하는 범위 내에서 최선의 협력을 제공하는 비공식적 네트워크로 체결국간 상호 협력의무가 발생하는 형사사법공조협약에 비해 강제성이 약하기 때문에 공조수사의 신속성과 실효성이 약하다는 한계가 있음
  - ▸ “G7 24/7 네트워크’는 ’97년 G7 국가 주도로 결성된 국제공조 네크워크로서 디지털증거의 신속한

보존요청 및 수사정보를 교환하기 위하여 운영되고 있고, '20. 3. 현재 전세계 86개국이 가입되어 있음(우리나라는 '00. 12.에 가입)

- 성범죄 해외도피처에 대한 수사기관의 주요 국제수사공조 사례

① '16년도. 아동음란물 사이트인 '소라넷' 관련하여 네덜란드와의 국제공조를 통하여 관련 서버를 폐쇄한 사례

② '19년도. 미국, 한국 등 전세계 32개국 수사기관은 다크웹 아동음란물 사이트에 대한 공조수사를 진행한 사례. 아동성착취물 등을 유포한 웰컴투비디오 웹사이트의 경우, 국내 경찰청, 미국 국토안보수사국(HSI)·국세청(IRS)·연방검찰청, 영국 국가범죄청(NCA), 독일 연방경찰청 등을 포함한 약 32개국의 수사기관이 공조하여 총 38개국 337명의 운영자와 아동음란물 소지자를 검거함.

- 그러나 국제형사사법공조나 G7 24/7 네트워크 등은 사이버범죄가 자국의 이해관계나 큰 관련성이 없는 경우 타국 수사기관의 적극적 공조가 어려우며 많은 시간이 소요되는 것이 현실임
- 따라서 협약 가입을 통해서 사이버범죄와 관련해서 전 세계 71개국과의 국제공조가 보다 원활해지기 때문에 수사 등이 보다 유리하다는 장점이 있다는 주장이 있음

○ (가입효과) 유럽사이버범죄협약은 다수의 국가들이 가입하고 있고 사이버범죄에 대해 국내법상의 조치에 상응하는 국제적 차원의 조치들을 규정하고 있어, 특정유형의 사이버범죄에 대한 국가공조의 효율성이 제고될 것으로 여겨짐

- 현재 우리나라와 뉴질랜드를 제외한 34개 OECD회원국 전부가 해당 협약에 가입하고 있기에 사이버범죄협약은 대표적인 국제협약으로, 전 세계 71개국과의 국제공조 체계 구축 마련이 가능하다는 장점이 있음
- 특히 협약에서 디지털 증거 확보를 위한 컴퓨터데이터의 신속한 보전(제 16조), 트래픽 데이터의 신속한 보전 및 제공(제 17조), 긴급시 공조 방식의 간이화 (제25조 제3항), 24/7 네트워크 운영(제35조)가 명시되어 있어, 긴급사안에 대한 신속한 대응이 가능할 것이라는 기대가 있음

○ (개정필요사항) 협약의 절차규정에 상응하기 위해서는 통신비밀보호법의 개정을 통해 전자기록의 신속한 보존, 전가기록의 수색과 압수, 데이터의 실시간 수집과 감청의 법률적 근거조항을 마련하고, 전기통신사업법상의 전기통신사업자의 협조의무를 강화하는 개정이 필요함

- (전자기록의 신속한 보존) 협약 제16조와 제17조가 요구하는 전자기록의 신속한 보존을 위해서는 수사기관이나 관할기관이 특정요건을 충족할 경우 전기통신사업자에게 수사와 관련한 전자기록에 대한 보전을 명령할 수 있는 근거 규정을 신설해야하며, 통신비밀보호법 제2조에 통신사실확인자료의 수집정보의 범위를 확대하는 개정이 필요함
- (전자기록의 수색과 압수) 형사소송법 제106조제3항의 압수의 대상을 확대하기 위해 컴퓨터용디스크, 정보저장매체 이외에 컴퓨터데이터를 추가하는 개정이 필요하고, 네트워크를 통해 접근하여 전자기록을 수색하는 원격수색을 허용하기 위한 조항이 신설되어야 함
- (데이터의 실시간 수집과 감청) 협약 제20조와 제21조에서 요구하는 데이터의 실시간 수집과 감청을 허용하기 위해서는, 통신비밀보호법 제5조(범죄수사를 위한 통신제한조치 허가요건)에 청소년성보호법 제2조의 5에 따른 아동· 청소년성착취물을 비롯한 협약에서 요구한 사이버범죄를 포섭하는 형태의 개정이 필요함
- (전기통신사업자의 협조의무) 협약 제18조에 따른 가입자정보 제출 명령과 관련해서 전기통신사업자의 협조의무 강화를 위해 전기통신사업법 제83조제3항(통신비밀의 보호) 3호에 전기통신사업자가 자료열람이나 제출 요청에 대해 “따를 수 있다”는 현재의 조항을 “따라야 한다”로 개정해야하며, 그에 따른 벌칙조항을 신설해야함

○ (우려사항) 인터넷망을 통한 불법정보의 유통의 글로벌적인 특성으로 인해 수사에 있어 국제공조의 필요성이 높아지고 있어 국내에서도 협약가입의 필요성이 제기되고 있으나, 국내법에서 중요시하는 통신비밀의 보장과 개인정보의 자기결정권 침해, 그리고 전기통신사업자의 부담 증가 등의 부작용이 있을 수 있음

- 사이버범죄협약은 수사기관의 신속한 정보보전 요청, 압수· 수색, 감청 등을 허용하고 있기 때문에, 수사기관의 자의적 판단으로 영장을 청구하고 실시간으로 트래픽데이터나

통신내용데이터를 수집할 경우 많은 개인정보들이 과도하게 수집될 수 있다는 우려가 있음

- 따라서 국내의 개인정보보호법과 통신비밀보호법은 개인정보의 자기결정권과 수사기관의 정보수집에 대한 제한을 두고 있으며, 이로 인해 협약에서 요구하는 수준으로 개인정보와 통신데이터에 대한 신속한 보존· 수집· 제출이 허용될 경우 해당법률 위반의 소지가 상당함
- 특히 협약 제32조에 근거하여 회원국들이 우리나라 정부의 승인 없이도 통신사나 인터넷서비스 제공자에게 직접 트래픽 데이터에 대한 접근과 제출을 요구할 수 있기 때문에, 내국인의 정보적 자기결정권과 통신비밀을 보호할 수 있는 수단이 마땅하지 않다는 우려가 있음
- 아울러 협약에 따라 회원국이나 수사기관이 국내의 통신사와 인터넷서비스 제공자에게 광범위한 정보수집과 보관, 감청과 자료 제출을 요청할 경우 정보저장시설 및 관리인력 증가가 필요하기 때문에, 인터넷서비스제공자의 경제적 부담이 증가한다는 지적이 있음

참 고 문 헌

국내 문헌

경찰청(2020)[단독] 경찰, 사이버범죄 국제공조 강화한다…'부다페스트협약' 가입 시동, 뉴스핌. (뉴스핌(2020. 6. 24), 재인용), Retrieved from https://m.newspim.com/news/view/20200623000783

김동균(2008). 문화의 향상 발전을 위한 저작권 보호기술 연구보고서, 저작권보호센터 (이진태(2009), 재인용.)

김민정(2020). 가짜뉴스(fake news)에서 허위조작정보(disinformation)로 - 가짜뉴스 규제 관련 국내 법안과 해외 대응책에 나타난 용어 및 개념정의 비교 - , 미디어와 인격권, 5(2), 43-81.

김유향(2019). 허위정보 해외법제 현황-독일·프랑스·싱가포르 법률의 주요내용 및 시사점. 외국입법 동향과 분석, 20호

김유향(2016). 해외 인터넷 자율규제의 동향 및 시사점. KISO 저널, (23), 44-49.

김유승(2005). 인터넷 콘텐츠 공동규제 연구. 사이버커뮤니케이션학보(16), 83-117

김윤희(2020. 8. 6). 해커, 'DoH' 악용해 데이터 훔쳤다. -카스퍼스키, 이란 APT 그룹 활동 포착…"코로나19 관련도메인 공격", ZDNET Korea, retrieved from https://zdnet.co.kr/view/?no=20200806160007

김한균, 김성은, 이승현(2009). 사이버범죄방지를 위한 국제공조방안 연구, 대검찰청

김현수, 전성호(2020). 유럽연합 디지털서비스법안(Digital Services Act)의 주요 내용 및 시사점. KISDI Premium Report, 20-11

낭종호(2020). 디지털 성범죄 피해확산 방지를 위한 근-복사 동영상 검출 기술.

뉴스핌(2020. 6. 24.). [단독] 경찰, 사이버범죄 국제공조 강화한다…'부다페스트협약' 가입 시동, Retrieved from https://m.newspim.com/news/view/20200623000783

대검찰청(2008). 「사이버범죄 방지를 위한 국제공조방안연구」

대검찰청(2015). 「사이버범죄협약 이행입법연구」

대검찰청(2020). 과학수사부 사이버수사과 홈페이지

데일리시큐(2020.8.5.). 이란해킹그룹, DoH를 정보유출 채널로 사용해 탐지 무력화 시켜

라광현·윤해성(2019). 유럽평의회 사이버방지협약 성과에 대한 실증적 검토, 범죄수사학연구, 통권 제8호, pp.49-73.

박정훈, 정원치, 오상익, 박남제. (2020). SNI 차단 기법 기반의 불법 웹 차단 기술적 정책 개선. 멀티미디어학회논문지, 23(3), 430-439.

박희영·최호진·최성진(2015). 사이버범죄협약 이행입법 연구, 대검찰청

방송통신심의위원회(2020). 2019년 불법·유해정보 심의·의결 결과.

법률신문(2016. 5. 18.). "수사·정보기관에 통신자료제공 전기통신사업법 제83조 3항은 위헌" , 대법원・법원행정처, Retrieved from https://m.lawtimes.co.kr/Content/Article? serial=100584

비즈한국(2019. 12. 3). 유튜브 프리미엄을 2천원에? VPN 쓰다 '좀비폰' 될라, Retrieved from http://www.bizhankook.com/bk/article/19061

손형섭 (2020). 일본에서의 온·오프라인 혐오표현과 그 규제에 관한 연구. KISO

연합뉴스(2020. 1. 7). 동영상 더 싸게 보려 가상사설망 썼다가…해킹위험 노출, Retrieved from https://www.yonhapnewstv.co.kr/news/MYH20200107002300038

유민종(2019. 2), 사이버범죄협약과 국내 법제의 양립가능성 연구, 서울대학교 융합과학기술대학원 석사학위논문

임규철(2018). 유럽연합과 독일의 개인정보보호법의 비판적 수용을 통한 우리나라의 개인정보보호법의 입법개선을 위한 소고. 법학논고, 61, 81-115.

전자신문(2020. 9. 22). 美 "이란 해킹조직, VPN 취약점 악용해 정보 유출", Retrieved from https://m.etnews.com/20200922000229) 등

정태진(2018. 11. 14). 유럽사이버범죄협약과 사이버 범죄대응을 위한 국제 공조, 서울대학교 국제문제연구소, 통권 98호

진정남, 지경준, 김래봉, 최희재(2016). 정보통신망법상 불법음란정보의 기술적 차단

을 위한 정책방안 연구, 한국정보통신진흥협회, 방통융합정책연구 KCC-2016-24.

여성가족부· 과학기술정보통신부· 법무부· 방송통신위원회· 경찰청· 방송통신심의위원회(2018.11.28.) 「주요 현안 보고-디지털 성범죄 대응 관련-」, 제364회 국회(정기회) 여성가족위원회

윤종수(2009) 온라인서비스제공자의 책임제한과 특수한 유형의 온라인서비스제공자의 기술조치의무-서울 고등법원의 소리바다 결정을 중심으로, 인권과 정의, vol., no. 395, 통권395호 pp. 30-53(24pages)

이진태(2009) 유튜브의 비디오 저작권 보호기술, SW 지적재산권 동향, 「SW IPReport 제6호」, 2009. 2. 20.

차진아(2013) 사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀 보장. 공법학연구, 14권 1호, pp.39-70.

최진응(2020). 불법촬영물 규제에 대한 해외 입법례와 시사점. NARS 외국입법 동향과 분석, 49호.

하주용(2015). 인터넷 미디어 공동규제(co-regulation)의 한국식 모델을 위한 제언. 언론중재위원회. 2015. 겨울호

한국경제(2019. 12. 8.). 인터넷 주소 암호화 기술 확산…'유해 사이트 차단' 무력화되나, 한국경제, Retrieved from https://www.hankyung.com/society/article/201912089367Y

한국법제연구원(2017) 「일본의 통신감청기간 및 연장에 관한 법제의 주요내용」

한국저작권보호원(2019). 「저작권 보호 연차보고서」, p.141.

한국저작권위원회(2011). 「웹하드 등록요건에 포함된 특징기반 필터링기술 성능평가 실시 안내」

한국저작권위원회(2020). 제안요청서-저작권기술 및 성능평가 시스템 기능개선 및 운영

한승완, 최병철, 임재덕(2012). 유해멀티미디어 분석 및 차단 기술 동향, 정보보호학회지 제22권 제3호, 2012. 5

한지연, 지경준, 김래봉, 곽정원(2015). 특수유형부가통신사업자의 불법정보 유통방지를

위한 개선방안 연구, 한국정보통신진흥협회, 방통융합정책연구 KCC-2015-24.
황용석, 이동훈, 김준교 (2009). 미디어 책무성 관점에서의 인터넷 자율규제제도 비교 연구. 언론과 사회, 17(1), 102-134
황승흠, 황성기. (2003). 「인터넷은 자유공간인가?」. 서울: 커뮤니케이션북스.

해외 문헌

Akdeniz, Y. (2001). Internet content regulation: UK government and the control of Internet content. *Computer Law & Security Review*, 17(5), 303-317.(김유승, 2005, 재인용)

European Commission, *The Digital Services Act*, Retrieved from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Commission. Ileigal Content on online platforms. URL:https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms

Facebook Engineering(2018.12.21.). DNS over TLS:Encypting DNS end-to-end, retrieved from https://engineering.fb.com/security/dns-over-tls/

FMS (2017). Übersicht über positiv bewertete Konzepte für geschlossene Benutzergruppen, Retrieved from https://www.kjm-online.de/fileadmin/user_upload/KJM/ Aufsicht/Technischer_Jugendmedienschutz/AVS_Uebersicht.pdf

FSM (2011). Prüfgrundsätze der FSM, Retrieved from https://www.fsm.de/sites/default/files/Pruefgrundsaetze_2.Auflage.pdf

FSM (2013). Prüfrichtlinie der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter. Retrieved from https://www.fsm.de/sites/default/files/FSM_Pruefrichtlinie_27-08-2013.pdf

FSM (2014). Beschwerdeordnung Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., Retrieved from https://www.fsm.de/sites/default/files/FSM_Beschwerdeordnung_

2014-11-03.pdf

FSM (2016). Verhaltenskodex Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.. Retrieved from https://www.fsm.de/sites/default/files/fsm_verhaltenskodex_2016-11-15.pdf

FSM (2018). Satzung Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.. Retrieved from https://www.fsm.de/sites/default/files/fsm_satzung_2018-11-07-final.pdf

FSM (2020). FSM-Jahresbericht 2019. Retrieved from https://www.fsm.de/sites/default/files/2020-06-03_jahresbericht_2019-web-final.pdf

FSM 홈페이지(https://www.fsm.de/)

Gallager, S. (2019. 11. 20). Microsoft says yes to future encrypted DNS requests in Windows, arsTecnnica, Retreived from https://arstechnica.com/information-technology/2019/11/ microsoft-announces-plans-to-support-encrypted-dns-requests-eventually/

Gunningham, N., & Rees, J. (1997). Industry self regulation: an institutional perspective. Law & Policy, 19(4), 363-414.

Hostingtribunal(2020). 21+ SSL Statistics that Show Why Security Matters so Much, Retrieved from https://hostingtribunal.com/blog/ssl-stats/#gref/

IHC 홈페이지

ISP Review(2019. 9. 25) Firefox says- No DNS over HTTPS(DoH) By default for UK, https://www.ispreview.co.uk/index.php/2019/09/firefox-says-no-dns-over-https-DoH-by-default-for-uk.html

IWF 홈페이지(https://www.iwf.org.uk/)

IWF(2019). 아동음란물 URL주소의 지리적 분포, (유민종(2019. 2), 재인용.)

IWF (2020) Annual Report 2019.

JMStV. [url] https://www.gesetze-bayern.de/Content/Document/JMStV

Machill, M.,Hart, T. and Kaltenhäuser, B. (2002), "Structural development of Internet

self regulation: Case study of the Internet Content Rating Association (ICRA)", info, Vol. 4 No. 5, pp. 39-55. (김유승, 2005, 재인용)

Memorandum of Understanding between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003, Retrieved from https://www.cps.gov.uk/publication/memorandum-understanding-between-crown-prosecution-service-cps-and-association-chief

NetzDG. [url] https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

Sentencing Council (2014). Sexual Offences Definitive Guideline. Retrieved from https://www.sentencingcouncil.org.uk/wp-content/uploads/Aug-2015-Sexual-Offences-Definitive-Guideline-web.pdf

스탯카운터, https://gs.statcounter.com/

부 록

<해외 불법정보 차단업무 처리지침 신구조문 대비표>

현행	개정안
제1장 총칙 제1조(목적) 이 지침은 정보통신망이용촉진 및 정보보호등에 관한 법률(이하 “법”이라 함) 제44조의 7, 제55조 및 동법 시행령(이하“영”이라 함) 제 22조의 12에 따라 해외불법정보를 차단하기 위한 업무처리 절차를 정함을 목적으로 한다.	제1장 총칙 제1조(목적)---------- ---------- ----------제44조의 7, 제64조에 따라 ---------- ---------- ----------.
제2조(적용범위) 이 지침은 정보통신부장관의 취급거부 등 명령, 시정조치명령 또는 정보통신윤리위원회(이하 “윤리위원회”라 한다)의 시정요구(이하 “취급거부명령 등”이라 함)에 따라 해외 인터넷 접속역무를 허가를 받거나 등록하여 제공하는 정보통신서비스제공자(이하 “인터넷접속사업자”라 함)가 자신이 운영하는 정보통신망을 통하여 해외에서 국내로 유입되는 한글로 제공되는 음란, 도박 등 불법정보(이하 “해외 불법정보”라 함)에 대한 국내에서의 접속을 차단하는데 적용한다.	제2조(적용범위)----- 방송통신위원회 위원장의 취급거부 등 ---,---------또는 방송통신심의위원회---------- ---------- ----------외 인터넷 접속역무를 등록하여---------- ---------- ---------- ---------- ------ 음란, 도박 등 불법정보---------- ---------- ----------.
제3조(취급거부명령 등 대상 인터넷 접속사업자 및 차단대상정보 범위의 지정) ① 정보통신부장관 또는 윤리위원회는 인터넷접속사업자에 대하여 해외 불법정보의 차단을 위한 취급거부명령 등을 하고자 하는 경우 차단하여야 할 해외 불법정보 차단의 범위 및 효율성 등을 고려하여 취급거부명령 등의 대상이 되는 인터넷접속사업자를 적정하게 지정하여야 한다. ② 정보통신부장관은 제1항에 따른 차단하여야할 해외불법정보의 범위를 정하고자 할 때에는 현재의 차단기술, 장비 또는 방법 등에 관하여 윤리위원회, 인터넷접속사업자 등으로부터 의견을 들을 수 있다.	제3조(취급거부명령 등 대상 인터넷 접속사업자 및 차단대상정보 범위의 지정) ① 방송통신위원회 위원장 또는 방송통신심의위원회는 ---------- ---------- ---------- -------- ---------- ---------- ---------- ----------. ② 방송통신위원회 위원장은 -------- ---------- ---------- ---------- ---------- 방송통신심의위원회, --------- ----------.
제4조(인터넷접속사업자에 대한 해외 불법정보 URL 및 IP주소의 제공 등) ① 정보통신부장관 또는 윤리위원회는 인터	제4조(인터넷접속사업자에 대한 해외 불법정보 식별정보의 제공 등) ① 방송통신위원회 위원장 또는 방송통신심

넷접속사업자에 대하여 해외불법정보의 차단을 위한 취급거부명령 등을 하고자 하는 경우 해당 인터넷접속사업자에게 차단하여야 할 해외 불법정보의 URL과 해당 시점에 알려진 IP주소를 제공하여야 한다. ② 정보통신부장관 또는 윤리위원회는 제 1항에 의한 해외 불법정보의 URL의 제공 이후 해외 불법정보를 제공하는 사이트의 변경·폐쇄 등으로 인하여 해외 불법정보의 차단 사유가 소멸된 경우에는 직권 또는 취급거부명령 등을 받은 인터넷접속사업자의 신청으로 해당 해외 불법정보의 차단을 위한 취급거부명령 등을 철회하여야 한다.	의위원회는 ---------- 해외 불법정보의 식별정보(도메인, URL 및 해당 시점에 알려진 IP주소)와 식별정보의 관리방법을 제공하여야 한다. ② 정보통신부장관 또는 윤리위원회는 ---------- 해외 불법정보의 URL과 도메인의 제공 이후 ----------.
제5조(인터넷접속사업자의 차단) 해외 불법정보의 차단을 위한 취급거부명령 등을 받은 인터넷접속사업자는 해당 해외 불법정보를 5일 이내에 신속하게 차단하여야 하며, 해당 인터넷접속사업자들이 일괄적으로 해외 불법정보를 차단함으로써 인터넷접속사업자간에 이용자의 이동 또는 이탈 등이 발생하지 않도록 노력하여야 한다.	제5조 (현행과 같음)
제6조(URL 차단장비 설치에 의한 차단) 정보통신부장관 또는 윤리위원회는 해외 불법정보의 효율적 차단을 위하여 인터넷접속사업자중 해외 인터넷접속설비를 직접 설치한 사업자에 대하여 자신이 설치·보유하는 해외 인터넷접속설비에 해외 불법정보의 차단을 위한 URL 차단장비를 설치하도록 취급거부명령 등을 내릴 수 있다.	제6조(차단장비 설치에 의한 차단) 방송통신위원회와 방송통신심의위원회는 ---------- 차단장비를 ----------.
제7조(URL 차단장비의 설치) ① 제6조의 취급거부명령을 받은 인터넷접속사업자(이하 “URL 차단장비 설치 사업자”라 함)는 국제망 접속점의 최상위 구간 등에 URL 차단장비를 설치하여야 한다. ② URL 차단장비 설치 사업자는 포워딩(Forwarding)서버를 사용하거나 멀티도메인 웹호스팅으로 여러 도메인이 하나의 IP를 공유하는 경우 URL 단위의 차단을 통하여 해외 불법정보를 제공하지 않는	제7조(차단장비의 설치) ① ----------인터넷접속사업자(이하 “차단장비 설치 사업자”라 함)는 ---------- 차단장비를----------. ② 차단장비 설치 사업자는 ----------

정상적인 사이트가 차단되지 않도록 노력하여야 하며, 정상적인 사이트가 함께 차단된 경우에는 정보통신부장관 또는 윤리위원회는 직권 또는 URL 차단장비 설치 사업자의 신청에 의하여 해당IP 차단을 철회할 수 있다. ③ URL 차단장비 설치 사업자는 차단장비의 설치 등을 통하여 도메인 및 IP주소의 변경, DNS(Domain Name System)우회(DNS-free 사용 등), IP주소 직접 접속, 프록시(Proxy)서버, 아노마이져(Anonymizer) 등에 의한 우회접속방지를 위하여 기술적 조치를 강구해야 한다. ④ URL 차단장비 설치 사업자는 자신의 정보통신망을 통한 우회접속비율 및 정도 등 우회접속의 실태를 파악하고, 정보통신부장관이 이에 관한 자료의 제출을 요청하는 경우 이에 응하여야 한다. ⑤ URL 차단장비 설치 사업자는 차단목록 입력 등 차단 조치 후 1개월 이내에 해외 불법정보의 차단을 증명하는 자료를 정보통신부 장관에게 제출하여야 한다. 다만, 불법 해외정보의 차단과 관련한 실사자료가 있는 경우 이로써 갈음할 수 있다.	----------, ---------- 방송통신위원회 위원장 또는 방송통신심의위원회는---------- 차단장비 설치 사업자의 신청에 의하여 ----------. ③ 차단장비 설치 사업자는 ---------- . ④ 차단장비 설치 사업자는 ----------, 방송통신위원회 위원장이 ----------. ⑤ 차단장비 설치 사업자는 ---------- 방송통신위원회 위원장에게----------.
제8조(URL 차단장비 설치 사업자와 타 인터넷접속사업자와의 관계) ① URL 차단장비의 설치를 통한 해외 불법정보의 차단의 경우 URL 차단장비 설치 사업자로부터 정보통신망을 임차하여 운영하는 인터넷접속사업자(이하 “타 인터넷접속사업자”라 함)는 해당 해외 불법정보의 차단을 URL 차단장비 설치사업자에게 위임한 것으로 본다. ② URL 차단장비 설치 사업자는 URL 차단장비를 설치한 경우 정보통신부장관 또는 윤리위원회로부터 취급거부명령 등을 받은 사실 및 차단한 해외 불법정보의 목록을 타 인터넷접속사업자에게 지체없이 통지하여야 한다. ③ URL 차단장비의 설치에 따라 발생하는 비용 중 타 인터넷접속사업자가 임차하여 사용하는 정보통신망에 해당하는 비용은	제8조(차단장비 설치 사업자와 타 인터넷접속사업자와의 관계) ① 차단장비의 ---------- 차단장비 설치 사업자로부터 ----------차단장비 설치사업자에게 ----------. ② 차단장비 설치 사업자는 ---------- 방송통신위원회 위원장 또는 방송통신심의위원회로부터---------- ----------. ③ 차단장비의 설치에 ----------

URL 차단장비 설치사업자와 타 인터넷접속사업자가 협의하여 분담한다. ④ 제3항에 따른 비용 분담의 원활한 협의를 위하여 (사) 한국인터넷기반진흥협회는 URL 차단장비 설치 사업자로부터 이를 위임받아 처리한다. ⑤ URL 차단장비 설치를 통한 해외 불법정보의 차단과 관련하여 발생하는 민원 및 법적 분쟁에 대하여는 해당 민원 및 법적 분쟁을 제기한 자에게 인터넷접속역무를 제공하는 인터넷접속사업자가 이를 책임지고 처리하여야 한다.	차단장비 설치사업자와 ----------. ④ ---------- (사) 한국인터넷진흥협회는 차단장비 설치 사업자로부터 ----------. ⑤ 차단장비 설치를 ----------
제9조(차단사실의 안내 등) 해외 불법정보를 차단한 인터넷사업자는 이용자의 인터넷 접속역무 이용 상의 혼란을 방지할 수 있도록 차단사실을 자신의 이용자에게 안내하여야 한다.	제9조(URL 차단사실의 안내 등) ---------- URL 차단사실을 ----------.
제10조(차단의 실사 등) ① 정보통신부장관 또는 윤리위원회는 우회여부 등 해외불법정보에 대한 차단이 이뤄지고 있는지에 대하여 첨부 1에 따라 정기 또는 수시로 차단에 대한 실사를 할 수 있다. ② 정보통신부장관 또는 윤리위원회는 제 1항에 따른 차단에 대한 실사를 하고자 하는 경우 실사 7일 전까지 실사 사유, 일시, 대상, 방법 및 차단 이행기준 등을 실사를 받을 인터넷접속사업자에게 통지하여야 한다. 다만, 긴급을 요하거나 증거인멸 등으로 실사의 목적을 달성할 수 없다고 인정하는 경우에는 그러하지 아니하다. ③ 정보통신부장관 또는 윤리위원회는 차단에 대한 실사 후 실사결과 및 차단이행 여부를 실사를 받은 인터넷접속사업자에게 통보하여야 하며, 인터넷접속사업자는 통보받은 사실에 대하여 의견을 제출할 수 있다. ④ 정보통신부장관 또는 윤리위원회는 차단 실사결과 및 차단불이행 여부와 이에 대한 인터넷접속사업자의 의견을 참조하여 법에 따른 조치를 취할 수 있다.	제10조(차단의 실사 등) ① 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------. ② 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------. ③ 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------. ④ 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------
제11조(해외 불법정보 차단책임자의 지정)	제11조(해외 불법정보 차단책임자의 지정)

① 인터넷접속사업자는 해외 불법정보의 차단을 효율적으로 수행하기 위하여 관련업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 해외 불법정보 차단 책임자를 지정하여야 한다. ② 제1항에 따른 차단책임자는 해외 불법정보의 차단을 수행하고 해외 불법정보 차단 계획, 인원 및 장비 등에 관한 자료를 매년 월말까지 정보통신부장관에게 제출하여야 한다.	① ----------. ② ----------방송통신위원회 위원장에게 ----------.
제12조(자료제출요구) 정보통신부 장관 또는 윤리위원회는 해외 불법정보의 효과적인 차단을 위하여 인터넷접속사업자에게 필요한 자료의 제출을 요구할 수 있다.	제12조(자료제출요구) 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------.
제13조(해외 불법정보 차단 지원) 정보통신부 장관 또는 윤리위원회는 해외 불법정보의 효과적인 차단을 위하여 인터넷접속사업자에 대하여 웹서버 운영, IP추출 프로그램의 개발·보급 및 사후관리를 지원할 수 있다.	제13조(해외 불법정보 차단 지원) 방송통신위원회 위원장 또는 방송통신심의위원회는 ----------, IP와 도메인 추출 프로그램의 ----------.

저 자 소 개

천 혜 선

- 이화여대 신문방송학과 졸업
- 이화여대 신문방송학과 석사
- 뉴욕주립대 커뮤니케이션학과 박사
- 현 미디어미래연구소 미디어경영센터 센터장

신 혜 인

- 한국외대 언론정보학과 졸업
- 현 미디어미래연구소 연구원

이 찬 구

- 한국외국어대 신문방송학과 졸업
- 한국외국어대학교 신문방송학과 석사
- 한양대학교 경영학과 박사
- 현 미디어미래연구소 미디어경영센터 부센터장

전 주 혜

- 고려대 사회학과 졸업
- 고려대 언론학과 석사
- 고려대 언론학과 박사
- 현 미디어미래연구소 연구위원

김 용 희

- 숭실대 경영학과 졸업
- 숭실대 경영학과 석사
- 숭실대 경영학과 박사
- 현 숭실대 경영학과 조교수

김 유 석

- 한림대 언론정보학부 졸업
- 고려대 언론학과 석사
- 고려대 언론학과 박사수료
- 현 오픈루트 실장

방송융합정책연구 KCC-2020-14

인터넷 기술 환경 변화에 따른 불법정보 유통 대응 방안 연구

2020년 12월 31일 인쇄
2020년 12월 31일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
경기도 과천시 관문로 47
정부과천청사
TEL: 02-2110-1323
Homepage: www.kcc.go.kr