사이버범죄 트렌드(2023)

2022년 사이버범죄 통계 분석

2022년 주요 사이버범죄 유형별 분석

2023년 사이버범죄 트렌드

국가수사본부
사이버수사국

목 차

수록된 2022년 통계자료는
잠정치로서 추후 수정될 수 있습니다.

I

2022년
사이버범죄 통계 분석

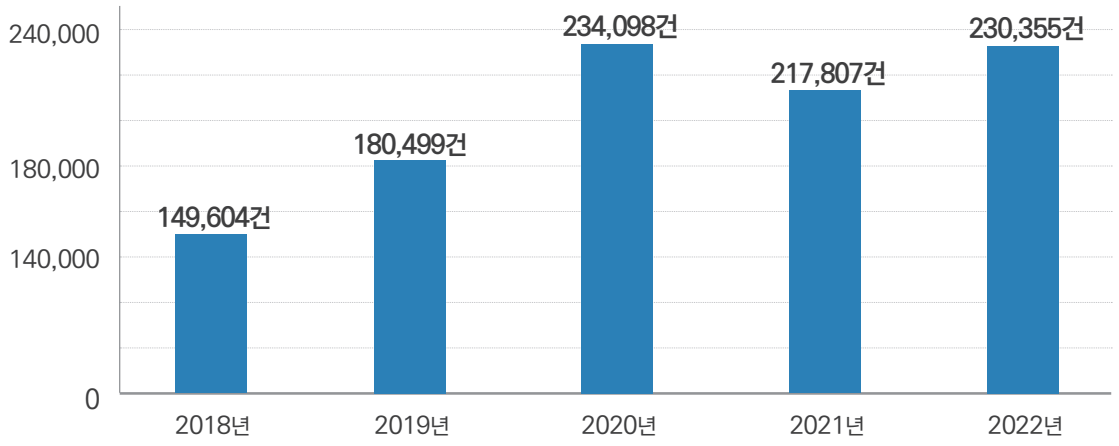
1. 발생 현황

2. 2022년 통계 분석

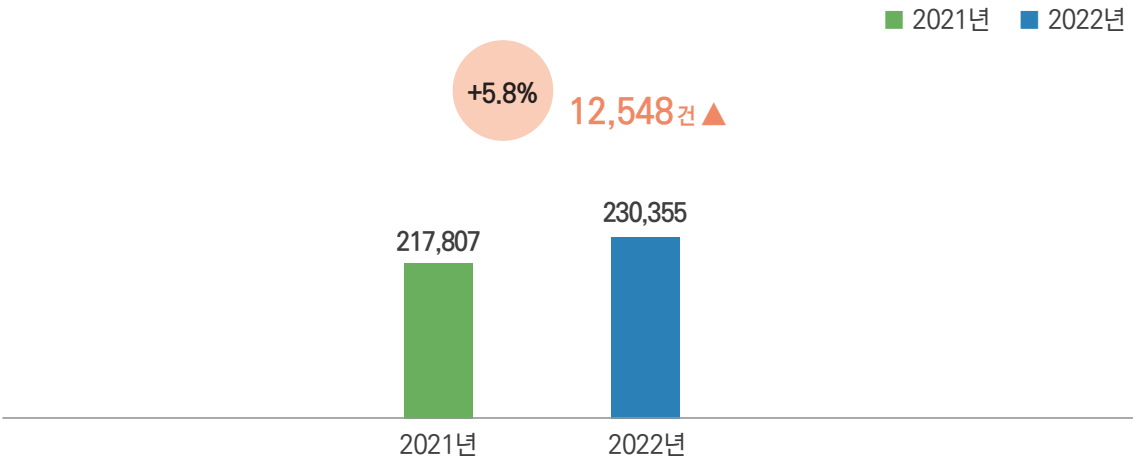
발생 현황

2022년 전체 사이버범죄는 230,355건 발생하였으며, 2021년 217,807건 대비 소폭 (5.8%) 증가하였다.

5년 간 사이버범죄 전체 발생건수 추이

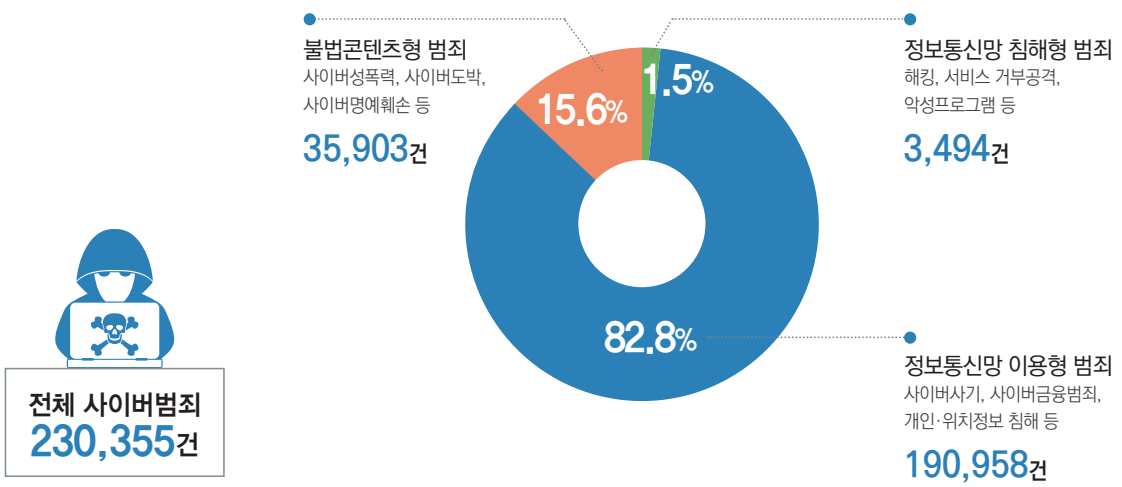


전체 사이버범죄 발생건수 증가율

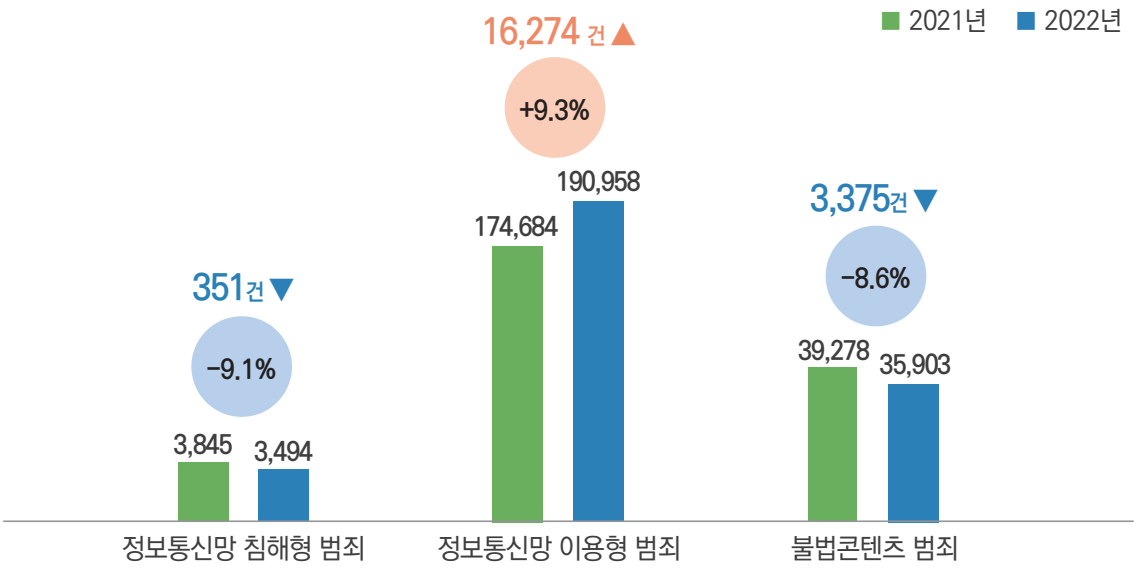


대분류로 살펴보면, 정보통신망 침해범죄(해킹, 악성프로그램 유포 등 정보통신망에 불법적으로 침입하는 방식으로 저지른 범죄)는 9.1% 감소하였으며, 정보통신망 이용범죄(사이버사기, 사이버금융범죄 등 정보통신망을 이용해 저지른 범죄)는 9.3% 증가했다. 반면 불법콘텐츠 범죄(불법성영상물, 사이버도박 등 법이 금지하는 정보 등을 생산 유포하는 범죄)는 8.6% 감소하였다.

사이버범죄 유형별 발생 비율(대분류)

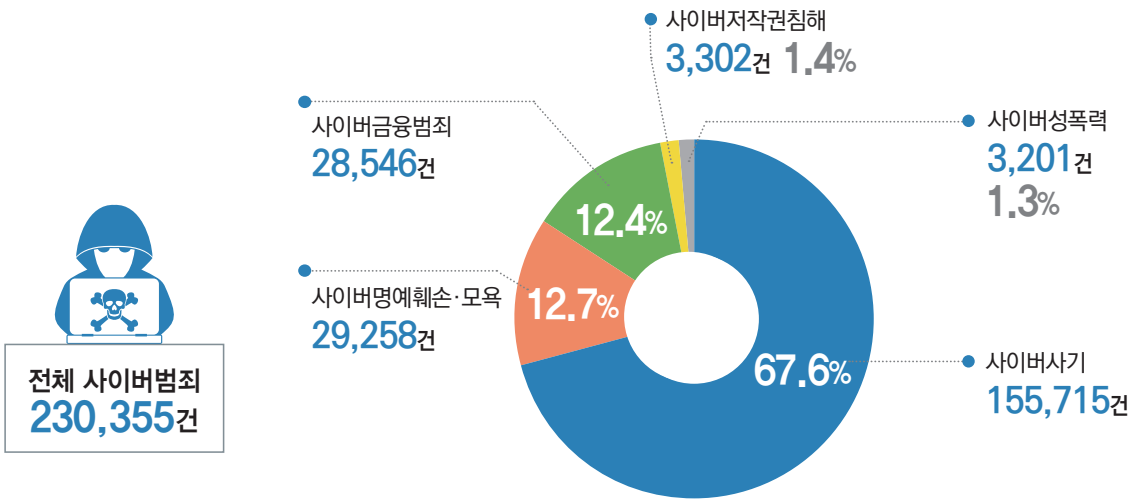


사이버범죄 유형별 발생건수 증가율(대분류)

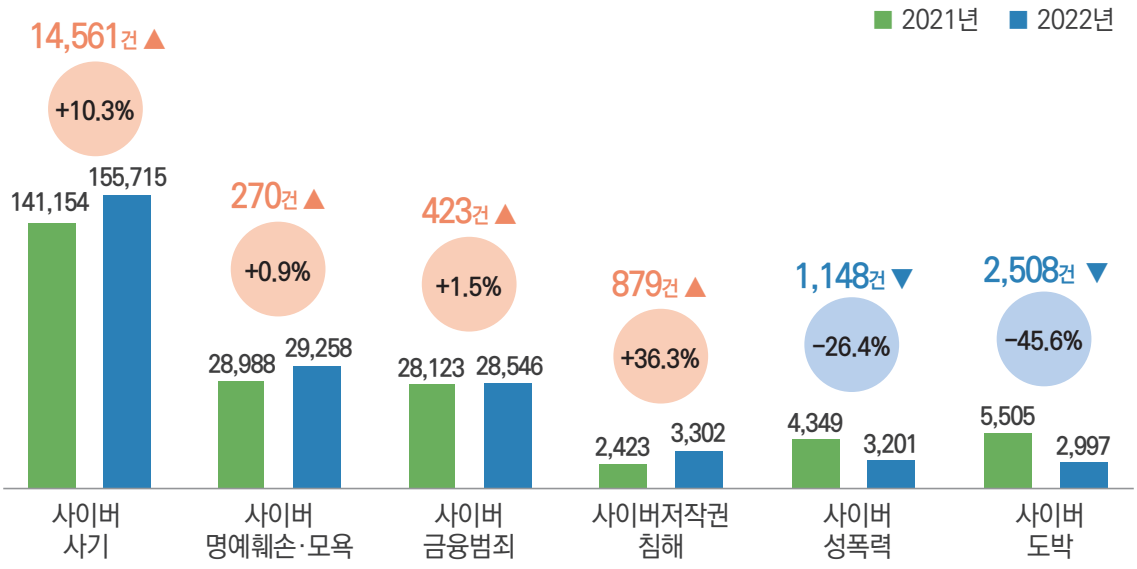


유형별 비중을 보면, 사이버사기(155,715건)가 전체 사이버범죄(230,355건) 발생건수의 67.6%로 가장 큰 비중을 차지하였다. 다음으로 사이버명예훼손·모욕(29,258건)이 12.7%, 사이버금융범죄(28,546건)가 12.4%를 차지하였으며, 그 외에 사이버저작권침해(3,302건) 1.4%, 사이버성폭력(3,201건) 1.3%가 그 뒤를 이었다.

사이버범죄 유형별 발생 비율(중분류)



사이버범죄 유형별 발생건수 비교(중분류)



사이버범죄의 특성상 수사 회피 목적으로 해외기업·해외 가상자산거래소 등을 악용하는 사례가 늘어남에 따라, 경찰은 효율적인 국제공조 수사를 위하여 인터폴·해외 법집행기관 공조, 글로벌 IT 기업 직접공조 등 다양한 유형의 국제 네트워크를 형성하고 있다.

2021년 해외기업을 통한 사이버사기가 증가하였으나 범죄수익금 세탁 수단 및 범죄유형의 변화(해외기프트카드→국내상품권·대포통장·가상통화거래소 등)로 국제공조요청 건수가 20.4% 감소 하였다.

※ 경찰청을 통해 요청한 건수만 집계(개별수사관이 요청한 건수는 제외)

국제공조 현황

	합계	사이버사기	사이버성폭력	사이버테러	기타*
2020년	7,560	6,273	767	112	408
2021년	12,771	10,708	1,166	231	666
2022년	10,167	6,431	1,468	881	1,387
전년대비	20.4%▼	39.9%▼	25.9%▲	281.4%▲	108.3%▲

*기타 : 사이버도박, 정통망법, 저작권법위반, 총포·마약 등

2022년 통계 분석

2022년에는 코로나 장기화로 인한 비대면 활동의 증가와 일상생활의 사이버化로 인해 사이버범죄 발생건수가 전년 대비 5.8% 소폭 증가하였다.

세부 유형별 범죄통계를 살펴보면, 사이버사기는 예년과 마찬가지로 사이버범죄 발생건수 중 가장 큰 부분(67.6%)을 차지하였다. 사이버사기는 전통적으로 중고거래 카페·앱, 인스타그램·페이스북 등 SNS 플랫폼, 쇼핑몰 등 다양한 경로를 통해 이뤄지고 있으며, 범죄 발생건수도 지속적으로 증가(10.3% ▲)하고 있다.

두 번째로 사이버명예훼손·모욕 범죄는 전년 대비 0.9% 증가한 것으로 나타났다. 일상생활이 사이버 공간으로 확대됨에 따라 인터넷상의 뉴스전파, SNS, 온라인 커뮤니티의 참여, 인터넷 구매 후기 등 다양한 활동이 많아지며 이에 관련한 분쟁도 증가하였다. 이에 따라 유튜버·연예인 등 사회 유명인에 대한 무분별한 악성 댓글과 인터넷을 이용한 가짜뉴스 등의

피해사건이 늘어나면서 사이버명예훼손·모욕 범죄도 증가한 것으로 판단된다.

세 번째로 사이버금융범죄 발생건수는 소폭 증가(1.5%▲)하는 경향을 보였다. 특히 몸캠피싱[1](3,026건→4,313건, 42.5%↑)·피싱[2](2,731건→3,028건, 10.9%↑) 등은 범죄 건수가 전년 대비 증가하였으나, 스미싱[3](1,336건→799건, 40.2%↓)은 큰 폭으로 하락한 모습을 보여주었다. 그러나 스미싱 발생건수 자체가 줄어들었다고는 볼 수 없다. 범죄자들은 스미싱을 통해 획득한 정보를 바탕으로 피싱이나 사이버사기 등을 저지르기 때문에, 범죄피해자는 최종 범죄인 피싱이나 사이버사기로 신고한다. 스미싱은 최종 범죄의 수단으로서 포함되기 때문에, 통계상 스미싱 자체 발생건수가 하락한 것으로 판단된다.

네 번째로 사이버저작권침해(2,423건→3,302건, 36.3%↑)는 급격하게 증가하였다. 대한민국의 웹툰·웹소설 같은 K-콘텐츠의 열풍으로, 헤비업로더들이 웹툰·드라마·영화 등을 대량으로 불법 유통시키면서 그에 따른 저작권법 위반 사례도 다양한 형태로 이어지고 있다. 저작권물을 유통하는 네이버나 카카오 등 플랫폼 업체에서도 이러한 불법 유통을 막기 위해 집중 모니터링 조직을 구성하여 경찰과 함께 적극 대응하였다. 또한 국민들의 저작권 인식 향상으로 인해 저작권 등록과 저작권 침해 고소가 늘어나면서 발생건수가 증가한 것으로 판단된다.

1) 음란화상채팅(몸캠) 후, 영상을 유포하겠다고 협박하여 금전을 갈취하는 행위
2) 개인정보(Private data)와 낚시(Fishing)의 합성어, 가짜 이메일 등을 발송하여 금융정보를 탈취하는 행위
3) 문자메세지(SMS)와 낚시(Fishing)의 합성어, 문자메세지를 발송 후 악성코드를 설치하여 정보를 탈취하는 행위

II

2022년
주요 사이버범죄 유형별 분석

1. 사이버사기

2. 사이버성범죄

3. 사이버도박

경찰은 지속적으로 주요 사이버범죄들에 대해 집중단속을 실시하고, 사이버 국제공조 협력도 계속 확대하고 있다. 또한 범죄피해 방지를 위해 사이버범죄 전문강사를 통해 예방교육도 실시하고 있다.

이러한 노력에도 불구하고, 스마트폰 등 최첨단 기기가 널리 보급되고 국민들이 보다 많은 시간을 사이버 공간에서 보냄에 따라 사이버범죄 발생건수는 계속 증가하는 경향을 보이고 있다. 이에 사이버범죄에 대한 유형 분석 및 최신 범죄 동향을 확인하여 지속적으로 대비할 필요가 있다.

본 보고서에서는 앞서 통계 분석한 내용을 바탕으로 국민 치안과 밀접하게 관련된 사이버범죄 중 가장 많은 발생건수를 보여준 사이버사기와 도박으로 인해 국민에게 큰 피해를 주는 사이버도박에 대해 분석하였다.

또한 피해자에게 큰 심적 고통과 깊은 상처를 남기는 사이버성폭력 범죄에 대해 살펴보고, 작년에 도입된 위장수사가 어떠한 영향을 끼쳤는지 확인하고자 한다.

1. 사이버사기

사이버사기는 정보통신망을 이용하여 물품이나 용역을 제공할 것처럼 속여 피해자로부터 금품을 교부받는 범죄로서, 전체 사이버범죄 총 건수에서 가장 큰 비중을 차지하고 있다.

현 황

사이버사기는 2022년 총 155,715건이 발생하여 2021년 141,154건 대비 10.3% 증가하였다.

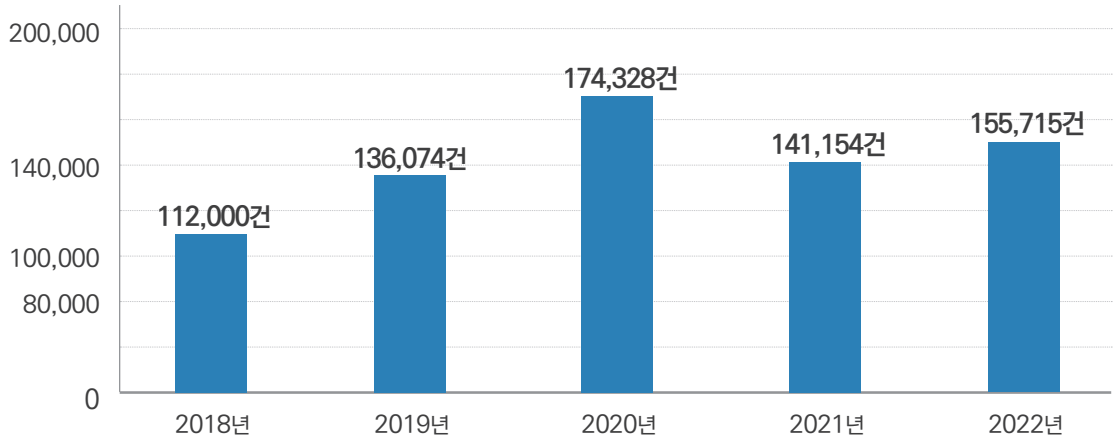
사이버사기는 직거래 사기, 쇼핑몰 사기, 게임 사기와 이에 해당하지 않은 기타 사기[4]로 분류된다. 특히 기타 사기는 2022년 65,570건으로 2021년 47,087건 대비 39.3% 상승하여 그 증가폭이 두드러졌다. 이는 기존에는 오프라인에서 진행되던 투자 사업설명회가

4) 직거래, 쇼핑몰, 게임사기에 해당하지 않고 정보통신망(컴퓨터 시스템)을 통한 기망행위를 통해 재산적 행위를 편취한 사기

가상자산 등 신종 투자 아이템을 빙자하면서 온라인으로 그 공간을 옮김에 따라, 사이버사기[5]로 분류되며 통계상 발생건수가 증가한 것으로 판단된다.

2020년 발생건수에 비해 2021년 발생건수는 다소 감소하였으나, 2022년의 발생건수는 다시 증가하여 여전히 증가하고 있는 추세이다.

전체 발생건수 중 사이버사기 발생건수 추이



주요 범행 수법

사이버사기의 가장 대표적인 수법은 중고거래 카페·앱에서 개인 간 거래를 빙자하여 이뤄지는 '직거래 사기'이다. 최근에는 해외 사무실을 두고 체계적 조직을 구성하여 치밀하게 범행을 저지르기도 한다.

주요 검거 사례

▶ 2018년~2020년 베트남에 사무실을 두고 총책, 콜직원, 인출책 등으로 역할을 나눠 중고거래 사이트에 전자제품 등 물품을 판매한다고 허위 글을 게시하여 피해자 1,465명으로부터 약 7억 2천만 원을 편취한 사기조직 총책 등 15명 검거(구속 7)

5) 온라인을 이용해 금품을 편취한 경우 사이버사기 통계에 반영

또한 재테크 등 투자에 대한 관심이 과열됨에 따라, 주식·가상자산 투자를 미끼로 한 소위 '리딩방' 사기 피해사례가 속출하고 있다. 특히 기존 투자사기가 오프라인에서 오픈 채팅 등 온라인으로 그 공간이 변화함에 따라 기존 경제범죄에서 사이버사기로 진화하고 있다.

주요 검거 사례

▶ 2021년 오픈 채팅방에서 피해자들에게 "가상자산 파생상품으로 고수익을 낼 수 있다"고 속여 주식거래소를 사칭한 가짜사이트에 회원 가입을 유도, 피해자 306명으로부터 투자금·수수료 명목으로 147억 원을 편취한 사기조직 총책 등 18명 검거(구속 9)

그뿐만 아니라 가짜 사이트나 악성 프로그램을 이용하는 신종 사기 범죄도 다수 발생하고 있다.

주요 검거 사례

▶ 2012년~2022년까지 가짜 사이트에 위조 당첨 복권, 당첨 사례·후기 등을 게시, 복권 당첨번호를 예측할 수 있을 것처럼 속여 피해자 64,104명으로부터 약 607억 원을 편취한 사기조직 총책 등 52명 검거(구속 4), 기소 전 추징보전 380억 원 인용, 범행사이트 38개 삭제·차단

경찰의 대응

경찰은 사이버사기에 대한 집중단속을 실시해 2022년 3월부터 10월까지 총 25,616명을 검거하고 1,391명을 구속하였다.

특히 동일 계좌가 사용된 다수 피해사건은 '사이버범죄 신고시스템(ECRM[6], ecrm.police.go.kr)'을 통해 접수 초기 신속하게 사건을 병합하여 수사하고 있으며, 피해 규모가 큰 사기범죄는 시·도경찰청으로 이관하여 집중수사하는 등 조직화·악성화되는 사이버범죄에 대응하고 있다.

6) Electronic Cybercrime Report & Management system의 약자로 사이버범죄 관련 신고를 접수하고 처리하는 시스템

예방수칙

경찰청은 최근 3개월 동안 3회 이상 사이버범죄 신고시스템에 신고된 사이버사기 의심 전화·계좌번호·이메일 주소를 조회할 수 있는 서비스인 '사이버캅'을 제공 중이다. 거래 전 사이버캅에서 상대방의 정보를 조회하여 사기 피해를 사전에 차단할 수 있다. 또한 중고나라·번개장터·당근마켓과 같은 개인간 거래 업체(Consumer-to-consumer, C2C 플랫폼)와도 협력하고 있다. 경찰청은 사이버범죄 신고시스템으로 접수된 사기 의심 게시물 웹주소를 C2C 플랫폼 업체에 실시간으로 전송하여 업체에서 즉시 해당 게시물 및 작성자를 검증하는 시스템을 운용하고있다.

※ 경찰청 홈페이지(police.go.kr) 또는 앱스토어에서 '사이버캅'을 검색하여 설치 후 이용

2. 사이버성폭력

현황

일상생활의 많은 부분을 사이버 공간에서 보내면서, 디지털을 통해 대화하며 자신을 표현하는 시대로 변화해가고 있다. 특히 아동·청소년들에게는 대면으로 소통하는 것보다 페이스북, 트위터, 인스타그램 등 SNS를 이용해 사이버 공간에서 비대면으로 소통하는 것이 훨씬 더 편하게 느껴진다. 이와 같이 사이버 공간에서의 활동이 늘어감에 따라 2022년 전체 사이버범죄 발생건수도 2021년 대비 증가[7]한 것으로 나타났다.

특히 눈에 띄는 점은 사이버성폭력 범죄는 2022년 총 3,201건이 발생하여 2021년 4,831건 대비 26.4% 감소하였다는 것이다. 이는 아동·청소년 대상 사이버성폭력에 대한 적극적인 위장수사와 집중단속으로 발생건수가 줄어든 것으로 분석된다.

2021년 9월 24일부터 위장수사 제도를 도입하여 2022년 10월 31일까지 약 1년간 총 183건의 위장수사를 실시, 433명(구속 30)을 검거했다. 경찰의 위장수사는 성폭력범죄의 예방과 검거라는 두 축에 확실한 영향을 끼친 것으로 보인다.

- 영리 목적으로 피의자들(남3, 여4)이 직접 출연한 불법성영상물 628개 제작, 해외 유료 구독형 SNS 내 불법성영상물을 유포한 피의자 7명 검거(구속 2)
- SNS를 이용, 돈을 준다고 속여 알몸사진을 받은 후 이를 유포하겠다며 협박하여 피해자가 스스로 촬영한 알몸사진을 전송받아 아동성착취물 648개 제작 및 배포·판매한 피의자 검거

최근 동향

과거에는 사이버성폭력 범죄분야에서 불법성착취물 구매·소지·시청 행위가 가장 많이 발생하는 범죄 유형이었다. 그러나 최근에는 불법성착취물을 구매하여 시청·소비하는 단순 수요적 행위를 넘어, 아동성착취물 제작·판매 등과 같은 공급적 행위가 큰 비중을 차지하는

7) 본 보고서 "2022 사이버범죄 통계 분석(2page)" 참조

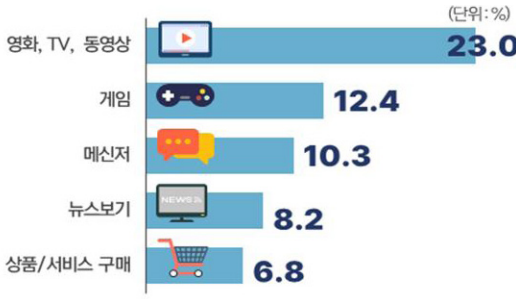
모습을 볼 수 있다. 또한 사이버성폭력 아동·청소년 피해자가 증가한 것뿐만 아니라 가해자 또한 10대가 가장 많은 비중을 차지하는 등 관련자들의 연령이 낮아지고 있는 추세이다.

이는 코로나19 이후 비대면·온라인 중심의 일상생활로 변화되면서 인터넷·스마트폰 사용 시작 연령은 점점 낮아지고, 동영상·게임 등 온라인 콘텐츠 이용이 급증[8]한 영향도 크다고 볼 수 있다.

스마트폰 이용률 및 이용시간

('19~'21방송매체이용행태조사, 방통위)

코로나19 이후 이용량 증가율



('21 스마트폰 과의존 실태조사, 과기정통부)

- 초등 4학년 96% 스마트폰 쓴다. 16%는 인터넷·폰 '과의존 위험' (2022. 5. 26. 연합뉴스)
- "특히, 최근 3년간 과의존 위험군 수가 가장 크게 증가하는 등 인터넷·스마트폰 과의존 저연령화 추세가 지속" 2022년 청소년 인터넷·스마트폰 이용습관 진단조사 결과 발표 (2022. 5. 26. 여성가족부)

최근에는 IT기술의 발전으로 현실과 가상이 결합한 메타버스[9] 내에서 아바타를 이용한 성범죄 문제가 발생하여 이에 대한 대비책이 필요하다.

- 메타버스서 초등생~고교생 11명 성착취 30대 남성 구속 (2022. 4. 14. 연합뉴스)
- "오빠랑 음성 채팅하자"…청소년들 성범죄 위험에 노출된 메타버스 (2022. 8. 5. 뉴시스)
- 10대의 아바타도 성추행…'온라인 그루밍'으로 성범죄까지 (2022. 9. 20. KBS)

8) 과학기술정보통신부, 제5차 스마트폰 인터넷 과의존 예방 및 해소 기본 계획(2022~2024), 2022. 6. 14.

9) '가공, 추상'을 의미하는 'Meta(메타)'와 현실세계를 의미하는 'Universe(유니버스)'의 합성어로 디지털 공간의 가상세계를 의미

문제는 메타버스 내 성인을 대상으로 한 범죄는 '통신매체이용음란'으로, 아동·청소년 대상으로 한 범죄는 '통신매체이용음란'·'온라인그루밍' 등으로 처벌이 가능하나 아바타(가상 캐릭터)를 대상으로 한 성범죄는 아바타의 인격권이 인정되지 않아 법적으로 처벌이 곤란하다는 것이다. 이에 언론·시민단체에서는 아바타에 대한 성범죄 처벌을 위해 성적 인격권 부여 등 적극적인 사회적·법적 규제를 촉구하고 있다.

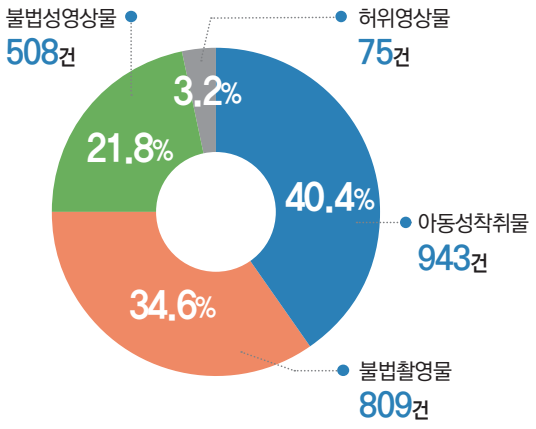
- ▶ 2022.5월 민형배 의원실(무소속, 교육위원회)에서 성폭력처벌법 개정안(유사성교 처벌) 발의
- ▶ 2022.7월 윤영덕 의원실(더불어민주당, 정무위원회)에서 정통망법 개정안(스토킹 처벌) 발의
  ⇨ 현재 상임위원회(여성가족위원회, 과학기술정보방송통신위원회) 심사 중

경찰의 대응

경찰청 국가수사본부(사이버수사국)에서는 2022년 한 해 동안 사이버성폭력 단속을 통해 불법촬영물 · 아동성착취물 관련 범죄 등 총 2,471명을 검거하였고, 이 중 139명을 구속하였다.

사이버성폭력 범죄 단속 현황 (기간: 2022.1.1.~12.31. / 킥스(KICS) 통계)

구분	총계	아동 성착취물	불법 촬영물	불법 성영상물	허위 영상물
검거 건수	2,335건	943건	809건	508건	75건
검거 인원 (구속)	2,471명 (139)	986명 (62)	855명 (43)	552명 (30)	78명 (4)



사이버성폭력 범죄의 경우 검거와 더불어 피해자에 대한 2차 피해가 발생하지 않도록 피해영상물(불법촬영물, 성영상물 등)의 확산 방지도 중요하다. 이를 위해 경찰에서는 여성가족부, 방송통신위원회, 방송통신심의위원회 등 관련 부처와 협업하여 불법 영상물을 신속히 삭제·차단할 수 있는 시스템을 구축·운영 중이다. 더불어 해외 수사기관 및 글로벌 IT 기업과 공조를 통해 해외에 소재한 수사자료를 확보하는 등 국제협력 강화에 많은 노력을 기울이고 있다.

앞으로도 경찰청 국가수사본부는 아동·청소년 대상 사이버성폭력 범죄에 대한 위장수사 제도를 적극 활용하여 범인 검거는 물론 범죄 예방 효과를 높이고, 피해자 보호에 최선을 다하는 등 사이버성폭력 범죄 근절을 위해 전방위적으로 대응해 나갈 방침이다.

3. 사이버도박

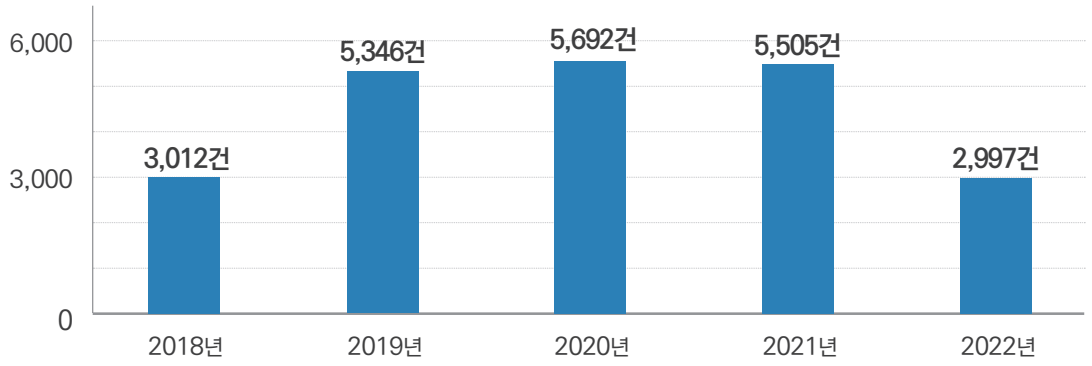
현 황

사이버도박은 국민경제의 건전성을 저해하고 가정의 경제적 파탄과 해체를 유발하는 가장 치명적인 범죄이다. 하지만 사이버도박은 이미 사이버 공간 곳곳 깊숙이 파고들어 성행하고 있으며, 심지어 합법을 가장한 교묘한 수법까지 동원하고 있어 더욱 큰 문제가 되고 있다.

불법 도박사이트의 경우 회원가입시 무료가입 포인트와 높은 환급률로 홍보하나, 사이트 폐쇄 이후 잠적하거나 강제로 회원을 탈퇴시키는 등의 방법으로 금전을 지급하지 않는 피해사례도 다수 존재한다. 또한 불법 사이트의 경우 도박 횟수 및 최대금액이 제한되어 있지 않아 도박 중독으로 인한 금전적 피해가 확산될 수 있다.

사이버도박 발생건수는 경찰청에서 운영 중인 누리캅스 신고 등이 예방효과를 발휘하여 2021년 5,505건에서 2022년 2,997건으로 줄었으나, 도박금액 규모는 커지고 매 순간 새로운 사이트들이 생겨나고 있다.

사이버도박 발생건수 추이



검거사례

사이버도박은 추적과 검거를 피하기 위해 해외에 사무실과 서버를 두고, 철저한 회원 관리와 함께 통장관리팀장·인출책·홍보팀장 등의 역할을 분담하여 점점 체계적으로 이뤄지는 양상이다.

1) 중국과 국내에 각각 본사를 두고 입금액 5조 7천억 원대 규모의 불법 도박사이트를 조직적으로 운영해 650억 원 상당의 범죄수익금을 챙긴 피의자 총 191명 검거(구속 20)
2) 미국에 서버를 두고 베트남에 사무실을 차린 후 입금액 1천억 원대 규모의 불법 도박사이트를 개설·운영한 피의자 9명 검거(구속 8)
3) 국내 외국인을 상대로 입금액 1천억 원대 규모의 외국인 전용 불법 도박사이트 '스포츠도박', '슬롯머신' 등을 개설·운영한 태국 국적의 불법 체류자 등 피의자 총 17명 검거(구속 11)
4) 국내 및 중국에 콜센터를 차린 후 입금액 1조 2천억 원대 규모의 불법 스포츠도박사이트 24개를 운영해 570억 원 상당의 범죄 수익금을 챙긴 피의자 22명 검거(구속 4)

검거된 피의자들에는 도박사이트 운영자뿐 아니라, 도박사이트 운영에 협력한 자, 도박행위자까지 포함되어 있다. 도박프로그램 개발자, 통장을 빌려주거나 도박수익금 인출에

협조한 자, 해외 현지에서 통역을 담당한 자 역시 도박사이트 운영에 협력한 자로 처벌받게 된다. 무엇보다도, 호기심으로 도박을 한 행위자도 처벌받을 수 있다는 점에 각별한 주의가 필요하다.

경찰의 대응

경찰은 2022년 9개월 간('22. 3. 1.~12. 31.) 전국적으로 특별단속을 실시하였다. 그 결과 대규모 불법 도박을 운영하는 조직을 검거하는 등 2,916명(구속 163)을 검거하는 성과를 거두었다.

앞으로도 수사력을 집중시키는 전담 단속체제를 유지하고 인터폴, 해외 수사기관과의 적극적인 공조를 통해 해외 피의자를 추적·검거하여 국내 송환할 수 있도록 노력할 것이다. 이러한 국제공조 수사 강화를 통해 불법 온라인 도박을 근절하고 건전한 사이버 공간 조성에 최선을 다할 것이다.

신고방법

우리나라에서는 공식 인터넷 사이트인 '배트맨(betman.co.kr)', 혹은 허가받은 판매점 스포츠토토 홈페이지(sportstoto.co.kr)'에서만 합법적으로 체육진흥투표권을 구매할 수 있다.

해외에서 합법적으로 운영되는 스포츠 베팅 사이트라고 할지라도 국내인이 이용하는 것은 불법이며, 청소년의 경우에는 합법 경로를 포함한 모든 스포츠 토토가 금지되므로 가정 및 학교에서 지도가 필요하다.

인터넷상 불법 사이트 발견 시 사행성감시위원회 불법사행산업 감시 신고센터 및 국민체육진흥공단 불법스포츠토토 신고센터 또는 경찰청 사이버범죄신고시스템 등을 통해 신고 가능하다. 도박으로 인해 대인관계, 재정적 문제 등이 발생하여 도박 중독이 의심된다면 한국도박문제관리센터 홈페이지(www.kcgp.or.kr) 또는 상담전화(1336)를 통해 본인이나 가족을 위한 전문상담과 도박문제 관련 정보도 받을 수 있다.

▲ 사행산업통합감독위위원회 불법사행산업감시 신고센터

- 1855-0112
- www.ngcc.go.kr

▲ 국민체육진흥공단 불법스포츠토토 신고센터

- 1899-1119
- cleansports.kspo.or.kr

▲ 경찰청 사이버범죄 신고시스템(ECRM) 제보 (첩보 등 수사자료로 활용)

- ecrm.police.go.kr

▲ 한국도박문제관리센터

- 1336
- www.kcgp.or.kr

III

2023년
사이버범죄 트렌드

1. 사이버전
2. 사이버테러 위협의 증가
3. 가상자산
4. 플랫폼 마비로 인한 재난 대비
5. 마이데이터

사이버범죄는 그 특성상 IT 신기술과 접목되어 매년 범행 수법이 고도화·정교화되고 범죄트렌드 역시 빠르게 변화하고 있다. 사이버범죄는 국민 개개인뿐 아니라, 불특정 다수 및 국가 자체에도 큰 위협이 되고 있다.

본 보고서에서는 2022년 사이버범죄 분석결과, 2023년 사회적 이슈, 국내외 사이버보안 전망 리포트, 경찰에 신고된 주요 피해사례를 종합하여 새롭게 등장하는 사이버범죄 동향을 전망해보고자 한다.

먼저 러시아-우크라이나에서 등장한 사이버전과 사이버테러가 국가 단위에서 실행될 경우 어떠한 파급력을 갖게 되는지 알아보고 날로 증가하는 사이버테러의 위협을 살펴보고자 한다.

다음으로 지속적으로 이슈화되고 있는 가상자산 관련 범죄를 알아보고, 가상자산을 이용한 범죄·가상자산을 대상으로 한 범죄를 구체적으로 살펴보겠다.

마지막으로 사회적으로 많은 영향을 끼치는 플랫폼, 그리고 개인정보 등 민감한 정보를 갖고 있는 마이데이터를 살펴보고자 한다.

1. 사이버전(戰)

최근 동향

IT기술의 급속한 발전은 사회·경제·문화 등 우리 생활 전 분야뿐 아니라 군사 분야에도 적용되어 적국의 주요 시스템 마비를 일으키는 사이버 공격 비중이 높아지고 있다.

2022년 초에 시작되어 현재까지 진행되고 있는 러시아와 우크라이나의 전쟁으로 두 국가뿐 아니라 경제, 사회적으로 전 세계가 큰 혼란에 빠지게 되었다. 특히 이번 전쟁은 러시아가 우크라이나를 본격적으로 물리적 침공하기 이전에 이미 사이버상에서 공격이 이루어졌다는 점이 크게 주목된다.

국립외교원 외교안보연구소에 따르면 이번 발발된 러시아우크라이나 전쟁은 사이버전이 현대 전면전(a full-fledged war)에서 실제로 어떻게 전개되고 어떤 비중의 역할을 차지

하는지 관찰할 수 있는 보기 드문 역사상 첫 번째의 사례이며, 사이버전이 얼마만큼의 파괴력을 발휘하며 전세에 영향을 끼치는지 혹은 그러한 영향력이 어떤 한계를 갖는지 보여주는 사례로 의미가 있다고 하였다.[10)]

위협 전망

사이버전(cyber戰)은 학자들마다 여러 가지 의미로 정의되고 있다. 다만 국가 또는 국가에 준하는 정치집단이 정치적 의지를 달성하기 위해 사이버 공간에서 상대방의 시스템을 파괴하거나 정보를 탈취하는 등의 공격을 하는 행위라는 것이 공통적인 견해이다.

즉, 컴퓨터 네트워크를 통하여 디지털 정보가 유통되는 가상 공간에서 다양한 사이버 공격 수단을 사용하여 적의 정보 체계를 교란·거부·통제·파괴하고 이를 방어하는 활동[11)]이다.

사이버전은 DDoS, 랜섬웨어 등과 같은 최신 사이버 공격기법을 이용하여 국가의 주요 전력과 통신 시설을 마비시키고, 정부기관·금융기관 등 국가의 핵심 인프라를 공격하여 실제 물리적 전쟁을 수행하기 어렵게 한다. 이뿐 아니라 허위 정보를 유포하여 여론을 분열시키는 등 국민들에게 불안감을 조성해 저항 의지를 무력화시킬 수 있다. 이는 미사일, 핵무기 등을 사용하는 전쟁의 공격 방법에 비해 비교적 손쉬운 방법이지만, 실제 물리적 전쟁의 피해만큼이나 큰 파괴력을 가지고 있다

과학기술정보통신부에서는 러시아-우크라이나 사태가 장기화됨에 따라 2023년에도 국제 해킹 조직의 활동은 증가할 것이며, 주요 기반시설이나 국제 기업을 대상으로 대규모 사이버 공격 시도가 지속될 것으로 예측하고 있다.[12)]

사이버전은 공격자의 식별이 어려워 공격의 목적이 정치적 목적인지 여부를 확인할 수 없기에 민간이 행위 주체인 사이버범죄와 구분이 어렵다. 따라서 국가의 주요 시설이나 주요기관·기업 등에서는 민간에서의 사이버공격뿐 만아니라 적대국으로부터의 사이버공격에 대비하여 정상적인 업무 및 서비스가 가능하도록 △공격 트래픽 차단 △공격 방어 △백업과 신속한 복구 등에 대한 사전 훈련 및 체계적인 대응 전략을 갖추고 있어야 한다.

---

10) 송태은, 국립외교원 외교안보연구소 주요국제문제분석, 「러시아-우크라이나 전쟁의 사이버전 : 평가와 함의」, 2022. 5.10.

11) 국방과학기술용어사전, dtims.dtaq.re.kr

12) 과학기술정보통신부, '22년 사이버 보안 위협 분석 및 '23년 전망 발표, 2022. 12. 26.

경찰의 대응

최근 사이버 공격은 랜섬웨어, 다크웹 등 다양한 방법과 경로로 조직화·지능화되는 추세이며, 익명성이 보장되는 가상화폐, 익명 네트워크 등 첨단 기술을 이용하여 공격의 근원지 추적과 분석을 어렵게 하고 있다.

이에 경찰청 국가수사본부(사이버수사국)에서는 과학기술정보통신부와 협력하여 랜섬웨어에 대한 다차원 분석을 통해 증거를 수집하고 취약점을 찾아 공격자를 식별하고 분석하는 연구[13]에 참여하는 등 고도화된 첨단 IT기술을 악용한 사이버범죄에 적극 대처하고 있다.

이뿐 아니라 △사이버테러 초동대응 모의 훈련 실시 △첨단 사이버 기술 및 추적기법 관련 사이버범죄 전문교육 확대 △인터넷진흥원 등 유관기관과의 사이버훈련 협력을 추진하고 있다. 또한 사이버수사역량강화를 위한 연구·교육·훈련 및 국내외 협력체계를 구축하여 다각적인 방면으로 사이버테러 위협에 대비하고 있다.

2. 사이버테러 위협의 증가

최근 동향

디지털정보와 이를 관리·운영하는 정보시스템은 현대사회에서 쓰이지 않는 곳이 없다고 할 수 없을 정도로 사회 전반에서 활용되고 있다. 이에 따라 디지털정보와 시스템을 대상으로 한 사이버공격·위협(이하 사이버테러로 지칭)도 급격히 증가하고 있다.

13) 과학기술정보통신부 주관 R&D, '사이버공격 대응을 위한 Life-cycle 기반 공격그룹 식별 및 유형 분석기술개발', '랜섬웨어 공격 근원지 식별 및 분석 기술 개발'

사이버안보업무규정 제2조

▶ “사이버공격·위협”이란 해킹, 컴퓨터바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다.

사이버테러범죄자들은 다양한 전자적 방법과 수단을 통하여 사이버공간을 공격하고 있다. 최근 발생한 주요 사이버테러 사건을 살펴보면 전국 PC방 DDoS 공격[14], 국회의원실·기자 사칭 악성 이메일 유포, 대기업 계정 해킹, 가상자산 거래소 해킹, 아파트 월패드 해킹 등 각종 정보시스템을 공격하는 형태가 기승을 부렸다.

2022년 사이버테러 관련 주요 언론보도

▶ 전국 19개 PC방을 대상으로 총 59회에 걸쳐 ‘해외 IP’에서 ‘국내IP’로 대량의 트래픽을 전송하는 방식으로 공격 (2022. 5. 17. YTN)

▶ 국회의원실 등을 사칭하며 악성이메일 발송, 외교·안보·통일 등 북한 관련 전문가의 전자우편을 실시간 감시 (2022. 12. 25. MBC)

▶ ‘영상 편집도구로 위장한 악성프로그램’을 유포하여 문화체육관광부 등 정부기관에서 운영하는 유튜브 채널 3개의 관리자 권한을 탈취하여 가상자산 사기사이트를 홍보하는 영상 게시 (2022. 9. 3. 연합뉴스)

▶ 아파트 40만 가구 월패드 해킹해 영상 유출, 보안전문가 체포 (2022. 12. 20. 동아일보)

위협 전망

국내외 2023년 사이버 보안 위협 전망[15]에서는 사이버테러에 대한 대비를 특히 강조하고

14) 디도스 공격은 분산서비스거부공격(Distributed denial of service attack) 약자로 대량의 통신을 발생시켜 인터넷서비스를 마비시키는 범죄이다.

15) 안랩, 2023년 5대 사이버 보안 위협 전망, KISA(한국인터넷진흥원), 2023 사이버 보안 위협 전망. 체크포인트(美), 2023 사이버 보안 예측

있다. 특히 랜섬웨어 공격과 같은 사이버범죄를 저지르는 조직의 활동이 기승을 부릴 것으로 전망하고 있다.

사이버테러범죄 조직의 공격은 점점 익명화·점조직화[16] 되고 있다. 사이버테러범들은 익명의 사람들과 비대면 메신저를 통해 역할을 분담하며 범죄를 저지른다. 익명화된 네트워크 서비스인 다크웹[17]을 통해 서버와 접속자 IP를 노출 시키지 않으면서 랜섬웨어[18]와 같은 악성 프로그램 등을 공유한다. 또한, 범죄대상을 '직접 공격'하지 않고 '국내·외 대행서비스'를 이용하여 공격함으로써 범죄 수단을 외주화[19] 시키기도 한다. 이처럼 익명화·점조직화됨에 따라 이러한 범죄조직을 검거·추적하는 일은 점점 더 어려워지고 있다.

한편 가상자산과 다크웹의 사용이 보편화 되어감에 따라, 사이버테러 범죄자들은 가상자산을 다크웹을 통해 범죄에 자주 이용한다. 가상자산은 흔히 추적이 불가능할 것이라고 생각하기 때문에 범행에 이용되며, 이를 통해 사이버테러범죄의 수익금이 취득·세탁·배분된다. 앞으로 사이버테러범죄에서 가상자산의 이용은 더욱더 늘어날 전망이다.

다크웹 이용자 통계 (출처: http://torproject.org)

연도		2018	2019	2020	2021	2022
다크웹 주소(개)		92,405	82,130	150,730	143,819	760,033
사용자 (명)	전체	2,401,258	2,063,963	2,124,776	2,207,942	2,525,546
	한국	**8,825**	**12,337**	**15,379**	**14,183**	**17,889**

가상자산 불법행위 피해금액 (출처 :국회의원 양경숙 홈페이지, 경찰청 보도자료)

연도	2018	2019	2020	2021	2022
피해금액	1천693억원	7천638억원	2천136억원	3조1천282억원	1조192억원

16) 서로 연결되지 않는 조직으로, 특정 구성원이 검거되더라도 연계 추적이 거의 불가하여 꼬리 자르기에 용이

17) 전용 프로그램으로만 접속가능한 익명화 사이트로, 마약·아동성착취물 등 다양한 범죄의 온상이 되고 있음

18) 몸값(Ransom)과 소프트웨어(Software)의 합성어로, 사용자의 PC를 암호화하여 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램

19) 2021년 12월부터 SNS상 '해킹 의뢰' 채널을 운영하며 웹사이트를 해킹한 피의자 12명 검거(구속 7)

아울러, 사이버테러범죄의 대표적인 유형으로 디도스(DDoS) 공격을 들 수 있다. 최근에는 대량의 데이터를 전송하면서 공격지의 IP주소까지 위조하는 '익명화 공격 수법'까지 등장하여 추적을 어렵게 하고 있다. 경찰의 추적을 방해하는 사이버 공격 기법이 고도화됨에 따라 이에 대한 대비책도 필요한 상황이다.

경찰의 대응

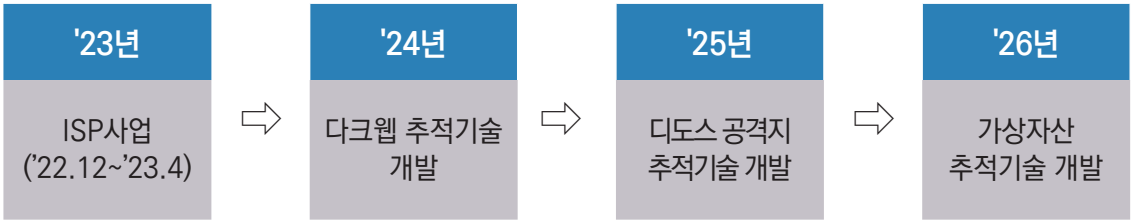
경찰은 파급력이 큰 사이버테러범죄를 대비하기 위하여 2016년 7개 시도경찰청에 사이버테러수사팀 신설을 시작으로, 현재는 전국 시도경찰청 사이버테러수사대 내에 사이버테러수사팀을 설치 운영 중이다. 2022년에는 경찰청 사이버수사국 산하에 사이버테러대응과를 신설하여 전국 사이버테러 수사에 대한 컨트롤타워 역할을 수행하고 있다.

경찰청 국가수사본부(사이버수사국)는 2023년 3월 다크웹·가상자산·디도스(DDoS) 공격을 시급하게 해결해야 할 '3대 사이버테러수사 역점과제'로 선정하고, 관련 대응기술 및 수사기법을 고도화하기 위하여 '사이버 범죄플랫폼 대응 TF'를 구성·운영하여 다크웹·디도스 근원지 추적기술을 우선 확보하기로 하였다. '사이버 범죄플랫폼 대응 TF'는 민간 IT업체에서 네트워크·시스템·소프트웨어 개발 전문가 경력을 인정받아 채용되거나 차세대 정보보안 리더로 선발된 국내 최고의 IT 기술을 보유한 수사관들로 구성하였다.

경찰청은 기재부로부터 다크웹·디도스·가상자산 추적기술 개발의 필요성·시급성을 인정받아 ISP 사업예산을 확보하고 이를 위한 사업을 진행 중으로, 향후 3년간 추적플랫폼 구축사업을 진행할 계획이다.

* ISP(Information Strategy Plan) : 시스템구축사업의 내실화를 위해 사전에 예산·인력·기간·기능 등을 세부적으로 준비하는 정보화전략계획 사업

연차별 개발 계획



앞으로 경찰은 한국인터넷진흥원, FBI 등 국내외 기관과도 긴밀한 협조 관계를 유지하며 △다크웹 추적, △가상통화 분석, △디도스(DDoS) 공격 추적기술 등을 고도화하여 웰컴투비디오 사건[20], 클롭 랜섬웨어 사건[21]과 같은 초국경적 대형·중대범죄에 대응할 예정이다.

3. 가상자산

최근 동향

2022년 한해 가상자산의 가격은 테라·루나 사태, 글로벌 거래소 FTX의 파산, 위믹스 상장폐지 등 예상하기 어려운 변수로 많은 급등락을 반복했다. 2021년 11월까지만 해도 3조 달러(약 3,780조 원)에 달하던 가상자산 시가총액은 어느새 3분의 1수준에도 미치지 못할 만큼 줄어들었다.

가상자산 가격의 폭락과는 별개로 가상자산에 대한 제도권의 관심은 더욱더 높아가고 있다. 부산시가 디지털자산 거래소를 설립하겠다고 나선 데 이어 금융투자협회도 대체거래소를

20) 다크웹 상에서 운영된 불법사이트 '웰컴투비디오' 관련, 아동성착취영상을 유포한 운영자 및 성착취영상 공유자(한국, 미국 등) 300여명 검거

21) 국내 대학·기업을 포함 전세계에 랜섬웨어를 유포하고 가상자산을 갈취한 국제 범죄조직 관련, 한국·인터폴 등 전세계 18개 법집행기관이 합동 수사하여 우크라이나 현지에서 조직원 6명 검거

준비하면서 가상자산을 제도권으로 끌어들이기 위한 노력은 가속화될 것으로 보인다. 금융위원회가 발표한 2022년 상반기 가상자산사업자 실태조사 결과에 따르면, 2022년 상반기 가상자산 일평균 거래대금은 5.3조 원으로 2021년 하반기 11.3조 원 대비 53% 감소하였다. 그럼에도 불구하고 가상자산 거래대금은 같은 기간 코스피 일평균 거래대금 10.4조원의 50.9%에 달할 만큼 상당한 규모로 확인되었다. 거래가능 이용자(신원확인이 된 이용자) 계정은 690만개로 2021년도 대비 132만개(+24%)가 증가하였다. 평균 거래대금의 규모와 거래 계정 숫자의 증가는 가상자산이 일부 투자자에게만 투자대상이었던 것을 넘어 일반 대중들에게도 투자의 대상으로 고려된다는 것을 의미한다. 이처럼 가상자산이 하나의 재산적 가치를 지닌 대상으로 인식됨에 따라 범죄에도 그 사용 사례가 빈번해 지고 있다.

최근 수사사례 및 전망

투자 열풍에 편승해 고수익 보장 등으로 피해자를 속여 가상자산을 편취는 유형, 피해자의 계정 등에 권한 없이 침입하여 가상자산을 탈취하는 유형, 불법적인 자금을 가상자산으로 세탁하는 유형이 대표적인 가상자산 관련 범죄이다.

① 투자전문가를 사칭하면서 허위 투자사이트 회원가입을 유도하고, 사이트에 접속한 회원들을 상대로 3억 원을 가로챈 사기 피의자 3명 검거(구속 1)

② 가상자산 투자리딩방을 개설하면서 피해자 130명으로부터 투자금 및 수수료 약 70억 원을 편취한 사기조직 피의자 16명 검거(구속 8)

③ 국내 가상자산 거래소를 사칭하여 “해외 아이피 로그인 알람” 등의 피싱 문자 메시지를 유포, 접속을 유도한 후 보관중이던 가상자산을 탈취(약 4억 원 상당)한 피의자 1명 구속

④ 가족을 사칭해 휴대폰을 조작할 수 있는 악성앱을 설치한 후, 가상자산 거래소에서 직접 송금하는 방식으로 보이스피싱 피해금을 세탁한 보이스피싱·폭력단체 20명 검거(구속 8)

또한 가상자산을 채굴한다는 명목으로 투자자를 모집하거나, 비자금을 만들기 위해 가상자산을 발행하는 업체가 등장하는 등 기존 범죄에 가상자산이 활용되는 일도 급격히 증가하고 있다.

① 국내외 각지에 채굴기를 두고 00코인을 채굴해 수익을 창출한다면서 투자자를 모집하였으나, 투자금을 반환하지 못한 대표 고소

② 소프트웨어 업체인 00사의 대표는 가상자산을 이용하여 비자금을 조성했다는 의혹과 관련하여, 수사중

가상자산이 대중화됨에 따라, 가상자산을 대상으로 하는 범죄뿐만 아니라 가상자산을 수단으로 하는 범죄도 늘어날 전망이다. 제도권의 통제를 받지 않는 일부 거래소에서는 해킹, 횡령의 문제가 발생할 소지가 매우 높고, 기존 사기·유사수신 등에 가상자산이 결합되어 실제로는 가치가 없는 가상자산을 판매 및 투자 권유하는 등의 범죄도 더 늘어날 전망이다.

경찰의 대응

경찰청은 가상자산 활용 범죄에 대응하기 위해 계속 가상자산 추적 프로그램을 확대 도입하는 한편, 2022년 4월 19일 국내 주요 가상자산 거래소인 고팍스, 빗썸, 업비트, 코빗, 코인원과 경찰 전용 직통 회선을 구축하였다. 이어 2022년 10월 13일에는 위 거래소들과 '가상자산 관련 범죄 수사 공조 및 피해 예방을 위한 업무협약'을 체결했다. 이 협약은 국내 가상자산 거래 규모와 이용자 수가 꾸준히 증가하여, 경찰-거래소 간의 협조가 매우 중요해짐에 따라 이루어진 것이다.

경찰청은 국내 가상자산 거래소뿐만 아니라 해외 거래소와의 협조도 계속 추진할 계획이다. 특히 공조 및 피해 예방을 위한 협력과 범죄 동향, 범죄수익 환수, 자금세탁 방지 등에 대한 정보를 교류할 예정이다.

4. 플랫폼 마비로 인한 재난 대비

'플랫폼(Platform)'이란 경계가 없던 땅이 구획되면서 계획에 따라 집이 지어지고, 건물이 생기고, 도로가 생기듯이 '용도에 따라 다양한 형태로 활용될 수 있는 공간'을 상징적으로 표현한 단어이다.[22]

최근 동향

모바일 메신저, OTT[23], 배달 애플리케이션, 장보기 서비스 등 다양한 플랫폼 기업의 서비스는 편리함을 넘어서 필수재로 자리 잡고 있다. 플랫폼의 영향력이 커짐에 따라 재난 상황 및 사이버위협 발생 시 일상생활을 마비시킬 수 있는 우려 역시 더욱 커지고 있다.

2022년 10월 판교 데이터센터에서 화재가 발생하여 플랫폼 기업인 카카오·네이버의 일부 서비스에 장애가 발생하였다. 특히 카카오 플랫폼의 경우 메시지 앱뿐만 아니라 플랫폼과 결합된 결제·대중교통·은행 앱과 같은 계열사 서비스, 카카오 계정 인증방식을 사용하는 가상자산 거래 앱 서비스 등의 작동이 중단되었다.

2022년 판교 데이터센터 화재 관련 주요 언론보도

- ▶ 카카오·네이버 동시다발 장애, 원인은 판교 데이터센터 화재 (2022. 10. 15. 한국일보)
- ▶ 카카오 '먹통' 5일 7시간반 만에 '복구 완료'(2022. 10. 26. 매일일보)
- ▶ 카카오 멈추자 일상이 멈췄다 "거대 플랫폼 의존 사회 돌아봐야"(2022. 10. 16. 경향신문)

카카오톡 이용자 수는 약 4,700만 명으로 국내 모바일 메신저 시장점유율 95% 이상을 차지하고 있어 그 피해가 더욱 컸다. 특히 카카오모빌리티를 통해 승객을 태우는 택시나 카카오 유통채널을 이용하여 물건을 판매하는 상인 등 카카오 서비스를 활용해 영업을 하던 이들이 타격을 입었다.

22) 신동희(2014). 인간과 컴퓨터의 어울림. 커뮤니티케이션북스.

23) OTT란 'Over The Top'의 약자로 인터넷으로 영화, 드라마 등 각종 영상을 제공하는 서비스로, 대표적인 OTT 업체로는 넷플릭스, 유튜브 등이 있다(출처 : 네이버 시사상식사전).

카카오에 따르면 위 화재 사건으로 인해 접수된 피해사례는 87,195건에 달하였으며, 그중 유료 서비스 관련 피해 접수는 14,918건(17.1%), 무료 서비스 중 금전 피해 접수는 13,195건(15.1%), 기타 문의·의견은 59,082건(67.8%)이었다.[24] 이에 대해 카카오와 계열사들은 유료 서비스 이용자에게 화재 사건 직후 보상하는 한편 무료 이용자·카카오 서비스를 이용한 소상공인을 상대로도 보상안을 마련해 시행하였다.

위협 전망

피해의 직접적인 원인은 화재 사건이었으나, 화재로 인한 서비스 복구 시간이 지연되면서 화재와 같은 위기상황에 대비한 백업·이원화 미비, 비상 대응체계 부족 등 위기관리 대응능력 부족이 근본적인 문제점으로 지적되었다.

문제는 일부 대기업에 의한 플랫폼의 독과점으로 인해, 다양한 서비스가 과도하게 특정 플랫폼에 결합하게 되며 이에 대한 의존도가 심화되고 있다는 점이다. 이는 특정 플랫폼 내부에 다량의 정보기술자원 및 사용자들의 정보가 과도하게 집적되는 결과를 만들었다.

이 플랫폼 안에서 처리되는 정보들은 동일한 기술 인프라 및 도구가 사용될 가능성이 매우 높아 이에 대한 침입·결함이 전체 서비스의 마비로 이어질 수 있다는 점이 큰 문제점으로 부각되고 있다.

플랫폼을 구성하는 네트워크나 소프트웨어는 태생적으로 취약점이 존재하기 때문에, 이 취약점을 이용한 해킹, 디도스 공격의 표적이 된다. 이 경우 서비스를 이용하는 다양한 분야에 걸친 대규모 피해가 예상되고 심각한 위험 요소가 될 수 있는 만큼 위기 상황에 대한 대비 필요성 역시 더욱 강조되고 있다.

경찰의 대응

판교 데이터센터 화재로 인한 장애 사태를 계기로 국가안보실 주관으로 경찰청 ·

24) '카카오, 1015 피해지원 협의체와 함께 피해지원 방안 발표' 참조(http://kakaocorp.com/page/detail/9863?lang=KOR)

과학기술정보통신부 · 국방부 · 국가정보원 · 대검찰청 · 사이버작전사령부 등이 참여하는 범정부 사이버안보 태스크포스(TF)가 구성되었다.
이에 경찰은 디지털 재난이 안보 위협상황으로 전개될 것을 대비하여 주요 정보통신기반시설에 대한 전담 시도청을 지정하고 핫라인을 구축하여 피해 발생 시 신속하게 대응하는 시스템을 구축하는 등 정보통신망·시설에 대한 대비 태세를 점검하였다.
또한 정보통신 기반시설에 대한 공격을 대비하여 경찰청과 전국 시도청에 사이버테러 수사인력을 확충하여 사이버테러 전문 수사체계를 구축하였다. 그 밖에도 사건 발생 시 신속하게 초동대응을 하고 추가 피해를 막기 위해 '사이버테러 초동대응 모의훈련'을 정기적으로 실시하는 등 디지털 재난에 효과적으로 대응하기 위해 만전을 기하고 있다.

5. 마이데이터

4차 산업혁명[25]의 핵심 분야인 빅데이터·사물인터넷·인공지능 등의 기술이 발전함에 따라 그 기반이 되는 데이터들도 함께 축적되고 있다. 현대사회는 대부분의 사람들이 스마트폰을 휴대하며, 이를 이용해 소셜네트워크서비스도 많이 사용한다. 이에 따라 스마트폰과 SNS 상에 저장된 개인의 데이터들이 많아지면서 그 데이터들의 활용에도 많은 관심을 가지게 되었다. 다수의 기업들도 이러한 데이터의 활용가치를 높이 평가해 산업 촉진과 신사업 모델의 구심점으로 삼았다. 이는 전 세계 상위 10개 기업 중 90% 이상이 데이터 기반 기업으로 이루어진 것만 보아도 알 수 있다.[26]

문제는 이러한 데이터의 주체가 개인임에도 불구하고 지금까지 데이터 활용이 사업자(예컨대, 은행, 보험회사 등) 주도로 이루어져 데이터가 어디에 저장되어 있는지, 어떻게

25) 4차 산업혁명은 빅데이터, 사물인터넷(IoT), 로봇공학, 가상현실(VR) 및 인공지능(AI)과 같은 혁신적인 기술이 우리가 살고 일하는 방식을 변화시키는 현재 및 미래를 의미

26) 전세계 기업 시총 top10 (2023.02.08. 기준) 1.애플, 2.마이크로소프트, 3.아람코, 4.구글, 5.아마존, 6.버크셔해셔웨이, 7.테슬라, 8.엔비디아, 9.메타(舊 페이스북), 10.비자카드 순으로 대부분의 기업이 디지털 산업군에 포함된다. http://top.hibuz.com

이용되고 있는지 개인이 알기 어려웠다는 점이다. 이러한 상황을 변화시키고자 정부는 데이터 권리의 핵심인 관리권과 이동권을 소비 주체인 개인들에게 부여하였다.

마이데이터란, 이렇게 개인이 생성한 자신의 정보를 적극적으로 관리 및 통제할 수 있는 것을 말한다. 개인은 축적된 데이터를 바탕으로 자신의 정보를 적극적으로 관리 및 통제하여 이를 신용관리, 자산관리 등에 능동적으로 활용할 수 있다. 개인은 데이터의 이동권을 토대로 마이데이터 보유 사업자로 하여금 자신의 데이터를 관리하게 하거나 제3자에게 이동하도록 요청할 수 있다. 또한 데이터를 제공 받은 마이데이터 사업자는 데이터 분석을 통해 개인 맞춤형 서비스를 제공함으로써 수익을 창출할 수 있다. 이렇게 개인은 데이터의 주체인 자신의 권리를 강화할 수 있고, 데이터사업자는 데이터 경제의 활성화를 통해 이익을 도모할 수 있기 때문에 금융분야를 중심으로 '마이데이터'가 도입된 것이다.[27)]

우리나라 역시 2018년 6월, 4차산업혁명위원회에서 '데이터 산업 활성화 전략'에 따라 개인의 주권을 보장하는 핵심 실행과제로 마이데이터 사업을 추진한다고 발표하였다. 같은 해 11월 '데이터 경제3법' 개정안 발의에 이어 2020년 8월 '데이터 3법'이 시행되면서 "내 데이터의 주인은 나"라는 마이데이터 개념이 주목받았다. 데이터 3법이란, 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭:정보통신망법), 신용정보의 이용 및 보호에 관한 법률(약칭:신용정보법) 3가지 법률을 말한다.

27) 한국소비자원, '마이데이터 서비스 소비자 보호 방안 연구' 정책연구 21-09 참조, 2021. 12.

데이터 3법의 주요 내용

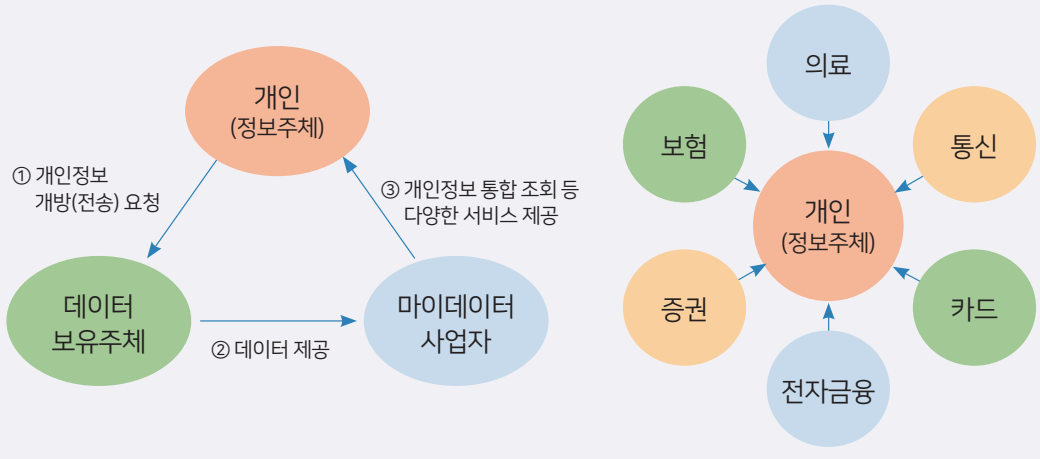
△ 개인정보보호법 개정안
- 개인정보의 개념을 개인정보, 가명정보, 익명정보로 구분하여, 안전하게 데이터를 활용하기 위한 방법과 기준 등을 마련하고 분산된 감독기관을 개인정보보호위원회로 일원화

△ 정보통신망법 개정안
- 개인정보 관련 법령이 다수의 법과 관리기관이 나눠져 있어 개인정보보호 관련 사항은 개인정보보호법으로 이관하고 온라인상 개인정보보호 관련 규제와 감독 주체를 개인정보보호위원회로 변경하는 등 혼란을 해결하기 위해 마련

△ 신용정보보호법 개정안
- 금융분야에 축적된 빅데이터 분석 및 이용의 법적 근거를 명확히 마련하고, 가명정보는 통계작성, 연구, 공익적 기록보존 등을 위해 동의 없이 활용 가능하도록 개정

정부는 분산된 개인데이터를 통합·관리·활용 및 제3자에게 제공할 수 있는 플랫폼 구축·운영사업을 추진하고 있다. 이 플랫폼은 의료, 금융, 통신 등 개인 일상과 밀접한 다양한 분야를 지원할 수 있다.

마이데이터 개요



각 분야의 진행 상황을 살펴보면, 의료분야에서는 건강검진 결과를 스마트폰 앱으로 확인하고, 걸음수·심박수 등 각종 건강정보 통합관리를 통해 실시간 건강관리를 할 수 있다. 금융분야에서는 기관들이 계좌거래, 카드내역 등을 Open API(Application Programming Interface) 형태로 제공받아 빠르게 자산조회 및 맞춤형 상품추천으로 안정적 재테크를 지원한다. 통신분야에서는 통신사가 보유한 이용자의 음성 및 데이터 사용량을 활용하여 최적의 맞춤형 요금제를 추천하는 등 통신비 절감에 일조한다.

마이데이터 사업이 활성화되었을 경우, 위와 같은 다양한 분야에서 개인과 사업자 모두 긍정적인 결과를 얻을 수 있다. 그러나 마이데이터의 보안상 문제가 발생한다면 방대한 데이터와 정보의 민감성으로 인해 많은 피해가 발생할 수 있다. 구체적으로 마이데이터에 대한 보안위협을 살펴보면 다음과 같다. 개인 금융 정보, 의료 데이터 등 민감한 개인정보가 있는 저장소에 보안 취약점을 이용한 디도스 공격, 개인정보 유출 등의 사이버 공격이 발생할 수 있으며, 공격으로 유출된 개인정보가 암호화되지 않았을 경우 유출된 개인정보로 인해 개인적 나아가서는 사회적으로 큰 피해를 입을 수 있다. 또한, 피싱이나 스미싱 등의 지능적인 범죄에 노출될 수 있다. 예를 들면, 마이데이터 서비스를 가장한 웹 또는 모바일 앱을 이용하여 정보를 가로채는 등의 사이버범죄에 악용될 수 있다.

이러한 문제에 대응하기 위해 사업자는 보안 취약점 점검을 의무적으로 이행하고 나아가 디도스 공격, 악성프로그램 설치, 랜섬웨어 등의 범죄에 대비하기 위해 데이터를 하나의 서버에 집중하기보다는 여러 개의 서버에 분산 저장할 수 있는 주기적인 백업도 필요하다. 또한 개인정보 전송 과정에서의 인증절차 강화 및 데이터의 암호화를 통해 보안 위협에 대비해야 한다. 개인 사용자는 보안 수칙을 준수하고 꾸준한 보안 교육을 통한 보안의식을 가져야 하며 정기적인 검사와 함께 의심스러운 메시지나 링크 접속은 피해야 한다. 마이데이터를 잘 활용하면 개인과 마이데이터 사업자 모두에게 이익이 된다. 그러나 정당한 권리를 지니지 않은 자에게 데이터가 넘어갔을 경우, 범죄의 타깃이 되거나 개인의 데이터가 원치 않게 공개될 수 있는 등 많은 피해가 예상된다. 따라서 사업자와 개인 모두 보안의식을 강화하고 보안 수칙을 철저히 지켜 안전한 마이데이터 환경을 구축해야 할 것이다.

Ⅳ

맺음말

경찰청은 최신 사이버범죄 트렌드와 주요 사이버범죄에 대한 정보를 제공하기 위해, 주요 사이버범죄 예방수칙과 전망을 소개하는 '사이버범죄 트렌드'를 발간 중이다.

이번 호에서는 2022년 사이버범죄 발생현황에 대한 분석을 바탕으로 사이버사기, 사이버성폭력, 사이버도박 등 주요 사이버범죄 유형 및 주목할 만한 사례를 살펴보았다.

그리고 러시아-우크라이나 전쟁에서 등장한 사이버전, 날로 증가하는 사이버테러의 위협, 지속적으로 이슈화되고 있는 가상자산에 대해서 살펴보았고, 필수재가 된 플랫폼 산업, 개인정보 등 민감한 정보를 갖고 있는 마이데이터에 대해서도 알아보았다.

사이버범죄는 특히 첨단 IT 기술과 사회공학적 기법이 접목되며 어떠한 범죄보다도 새로운 형태의 범죄 수법이 많이 등장한다. 또한 사이버범죄는 피해 발생시 회복이 쉽지 않아 범죄 예방 수칙을 철저히 준수하여 피해 예방을 하는것이 무엇보다 중요하다.

이에 사이버범죄 동향과 트렌드에 꾸준히 관심을 갖고 최신 예방수칙을 숙지함으로써 사이버범죄에 대해 대응하여야 한다.