과학기술정보통신부	보도자료

보도 시점 2026. 1. 27.(화) 12:00 (2026. 1. 28.(수) 조간) **배포** 2026. 1. 27.(화) 09:00

2025년 사이버 위협 동향 및 2026년 전망 발표

- 인공지능 기반 사이버 위협 및 인공지능 서비스에 대한 사이버 공격 증가 전망 -

과학기술정보통신부(부총리 겸 과기정통부 장관 배경훈, 이하 '과기정통부')와 **한국인터넷진흥원**(원장 이상중)은 2025년 한 해 **사이버 침해사고 통계**를 종합하고, 국내외 **정보보안 전문가 관계망(네트워크)***과 함께 사이버 위협에 대한 **선제적 예방 및 대응체계 강화**를 위해 「**2025년 사이버 위협 동향과 2026년 사이버 위협 전망 보고서**」를 발표하였다.

* (국내) 안랩, 지니언스, 이글루코퍼레이션, NSHC, S2W, SK쉴더스, 플레인비트, (해외) Cisco Talos, Google, Microsoft, Trend Micro, Zscaler 12개 기업이 참여 중

< 2025년 사이버 위협 동향 및 2026년 전망 보고서 구성>

침해사고 통계	2025년 한국 인터넷진흥원에 접수된 기업 침해사고 신고 통계
'25년 사이버 위협 사례	① 일상을 위협하는 **생활 밀접 기반 시설(인프라)**에 대한 **침해사고**
	② **공개 소프트웨어(오픈소스)** 및 **저가형 사물인터넷 생태계**를 악용한 **공급망 공격**
	③ **금품요구 악성 프로그램(랜섬웨어)** 공격 대상 확대와 기업-고객 연계 공격 강화
'26년 사이버 위협 전망	① **인공지능 기반** 사이버 **위협** 및 **인공지능 서비스**에 대한 사이버 **공격** 증가
	② **기술지원 종료(EOS)**와 **방치된 미사용 시스템**이 해킹 통로로 악용
	③ **인터넷 기반 자원 공유(클라우드)** 환경의 **취약 요소 공격** 증가
	④ 유출된 개인정보를 악용한 **2차 사이버 위협**
전문가 기고	① 2025년 사이버 위협이 바꾼 한국의 인공지능 보안 지형
	② 대규모 침해사고 발생과 침해사고 대응체계 개선
	③ 범부처 정보보호 종합대책 제도개선 방향과 과제
	④ 인공지능 전환(AX) 시대, '지능형 스택' 보호를 위한 보안 아키텍처의 진화
	⑤ 양자컴퓨터가 오기 전에, 해킹은 이미 시작됐다

※ 보고서 원문은 1월27일(화) 12:00 시 기준 보호나라(www.boho.or.kr) 게시

< 침해사고 통계 >

2025년도 침해사고 신고 통계를 살펴보면, 2024년도 1,887건에서 **2025년 2,383건으로 신고 건수가 약 26.3% 증가**하였다. 반기별로 살펴보면 24년도 상반기 899건에서 25년 상반기 1,034건으로 약 15% 증가, 24년 하반기 988건에서 **25년 하반기 1,349건으로 약 36.5% 증가하여, 작년 하반기 침해사고가 심하게 증**가한 것을 알 수 있다.

올해 금품요구 악성 프로그램(랜섬웨어) 감염은 온라인 도서 판매점 등 **국민 생활 밀접 서비스 장애로 국민에게 크게 인식**되었으나 **전체 침해사고 중 비중은** 11.5%(274건)로 높은 수준은 아니며, **전년도(10.3%, 192건)에 비해 증가하며 감소세**에서 **증가 추세로 전환**된 것으로 나타났다.

< 최근 3년간 침해사고 신고접수 현황 >

구 분 \ 연도		2023년			2024년			2025년		
		상반기	하반기	종합	상반기	하반기	종합	상반기	하반기	종합
침해사고 신고	분산 서비스 거부 공격(DDoS)	124(18.7%)	89(14.5)	213(16.7%)	153(17.0%)	132(13.4%)	285(15.1%)	238(23.0%)	350(25.9%)	588(24.7%)
	악성코드	156(23.5%)	144(23.5)	300(23.5%)	106(11.8%)	123(12.4%)	229(12.1%)	115(11.1%)	239(17.7%)	354(14.9%)
	(금품요구 악성 프로그램 <랜섬웨어>)	(134, 0.2%)	(124, 20.2)	(258, 20.2%)	(92, 10.2%)	(103, 10.4%)	(195, 10.3%)	(82, 7.9%)	(192, 14.2%)	(274, 11.5%)
	서버 해킹	320(48.2%)	263(42.9)	583(45.6%)	504(56.1%)	553(56.0%)	1,057(56.0%)	531(51.4%)	522(38.7%)	1,053(44.2%)
	기타	64(9.6%)	117(19.1)	181(14.1%)	136(15.1%)	180(18.2%)	316(16.7%)	150 (14.5%)	238(17.6%)	388(16.3%)
합계		664	613	1,277	899	988	1,887	1,034	1,349	2,383

< 2025년도 국내외 사이버 위협 사례분석 >

과기정통부(한국 인터넷진흥원<KISA>)는 **국내 및 해외 기업 12개 사도 전문가들과 함께** 올 한 해 발생했던 사이버 침해사고를 3가지 주제(국민 생활, 공급망 보안, 금품요구 악성 프로그램<랜섬웨어>)를 중심으로 분류하여 분석하고, **3가지 주제를 대표**할 수 있는 국내외 주요 사고 사례를 제시하였다.

① 일상을 위협하는 생활 밀접 기반 시설(인프라)에 대한 침해사고

o **통신, 유통, 금융 등 국민 생활 밀접 분야**에서 연달아 침해사고가 발생하면서 금전적 피해뿐만 아니라 많은 **국민을 불안**하게 하였다.

< 주요 사고 사례 >

☞ 'SKT 해킹' 3년 전부터 시작...유심 정보 2,700만 건 털렸다(4월)

☞ '금품요구 악성 프로그램(랜섬웨어) 해킹' 예스24, 두 달 만에 또 먹통(6월, 8월)

☞ SK텔레콤 이어 KT·롯데카드까지...'해킹 공포(해킹 포비아)' 대한민국(8월)

② 공개 소프트웨어(오픈소스) 및 저가형 사물인터넷 생태계를 악용한 공급망 공격

o 소프트웨어 개발자들이 신뢰하는 공개 소프트웨어 이음터(**오픈소스 플랫폼**)**가 주요 공격 경로로 악용되었고,** 특히, 본격적으로 시장에 출시되기 전부터 악성코드에 감염된 사물인터넷 **기기가 대규모로 시장에 유입되는 사례**도 발생하였다.

< 주요 사고 사례 >

☞ FBI, BADBOX 2.0 악성코드로 100만 대 이상 감염 경고(6월)

☞ NPM*, PyPI** 공급망 악성코드 공격 피해 심각...공개 소프트웨어(오픈소스) 생태계 위협 급증(6월)

* 전 세계 개발자들이 JavaScript 공개 소프트웨어 꾸러미(오픈소스 패키지)를 공유·관리하는 대표 이음터(플랫폼)

** 전 세계 개발자들이 다양한 공개 소프트웨어 파이썬 꾸러미(오픈소스 파이썬 패키지)를 등록·배포하는 대표 이음터(플랫폼)

☞ 북한 해커, NPM 악성 꾸러미(패키지) 197개 추가..개발자 목표 대규모 악성코드 공격 확인(12월)

③ 금품요구 악성 프로그램(랜섬웨어) 공격 대상 확대와 기업-고객 연계 공격 강화

o 해커들의 **공격 대상**이 연구·제조·에너지 분야를 넘어 **교육·의료 등으로 확대되**고, **해킹 수법 또한 인공지능 기반 자동화나 연계형 공격**으로 고도화되고 있다.

< 주요 사고 사례 >

☞ 미국 신장 치료 전문 기업 다비타, Interlock 금품요구 악성 프로그램(랜섬웨어)에 의한 침해 발생(4월)

☞ 미국 병원 연결망(네트워크)이 금품요구 악성 프로그램(랜섬웨어) 공격으로 전산 시스템 대거 중단(5월~6월)

☞ Qilin 금품요구 악성 프로그램(랜섬웨어) 집단에 의한 다수의 국내 자산운용사 침해사고 발생(8월)

☞ 혈액 공급기관 상태 초유의 금품요구 악성 프로그램(랜섬웨어) 공격.."정보를 쥐고 있으니 협상하자"(11월)

< 2026년도 사이버 위협 전망 >

과기정통부(KISA)는 국내 및 해외 기업 12개 사 전문가들과 함께 인공지능 확산, 사이버 보안 관련 기술 및 정책 변화 등을 고려하여 2026년에 예상되는 사이버 위협 4가지 주제(인공지능, 자산관리, 인터넷 기반 자원 공유 <클라우드>, 개인 침해) 를 선정하였다.

특히, 국내 정부·공공 기관 및 기업 등이 사이버 위협 대응에 참고할 수 있는 사이버 위협에 대해 세부적으로 분석·제시하였다.

① 인공지능 기반 사이버 위협 및 인공지능 서비스에 대한 사이버 공격 증가

o **사이버 공격자들의 인공지능 활용이 본격**화하면서 2026년에는 **인공지능을 활용한 사이버 공격이 더욱 정교하고 다양화될 것으로 전망**된다. 특히, **인공지능 조작 영상(딥페이크) 음성·영상 기반 전자 금융 사기(피싱)가 실시간 음성 통화 및 화상회의에까지 확대되어, 신뢰를 기반으로 한 소통 체계를 직접적으로 위협**할 가능성이 높다.

아울러, **인공지능 서비스 모델 자체를 공격 대상으로 삼는 공격도 본격화**될 것으로 보인다. **공격자들은 챗봇, 자동 분석 시스템, 보안 인공지능 등에 악의적인 내용을 주입하거나 학습 데이터를 조작해 의도하지 않은 오작동이나 정보 노출을 유도**할 수 있다.

② 서비스 종료(EOS, End Of Service,)와 방치된 미사용 시스템이 해킹 통로로 악용

o **'관리의 빈틈'을 노린 정교한 공격들이 반복적으로 발생**할 것으로 보인다. 특히, 2026년에는 방치된 '서비스 종료(EOS) 기존 체계(**레거시 시스템)를 겨냥한 공격이 크게 증가할 것으로 예상**되며, Windows 10 지원 종료는 보안 갱신(업데이트) 공백을 노린 공격을 확산시키는 사이버 위협의 기폭제가 될 수 있다는 전망이다.

③ 인터넷 기반 자원 공유(클라우드) 환경의 취약 요소 공격 증가

o **인터넷 기반 자원 공유(클라우드) 서비스 이용이 가속화되면서 정보자산의 위치와 상태변화를 파악할 수 있는 가시성은 높아졌으나, 이에 따른 관리·통제의 복잡성도 급격히 증가하고 있어 인터넷 기반 자원 공유(클라우드) 환경에 대한 보안 위협이 증가할 것으로 예상된다.**

특히, 2026년에는 단순한 **설정 오류나 권한 남용을 넘어, 인공지능을 활용한 인터넷 기반 자원 공유(클라우드) 보안 취약점 탐지와 권한 탈취가 자동화되고, 개별 취약점을 단순히 공격하는 방식이 아닌 여러 취약점을 종합·연계하는 공격이** 인터넷 기반 자원 공유 최적화(클라우드 네이티브) 환경에서 현실화될 가능성 높다는 전망이다.

④ **유출된 개인정보를 악용한 2차 사이버 위협**

o 2025년에는 **4월 SKT, 9월 KT, 11월에는 쿠팡 등에서 대규모 개인정보 유출 사고가** 발생하였다. 이와 같은 **대규모 개인정보 유출 사고**가 반복되면서 국민 사이에서는 **'이미 털릴 만큼 털렸다'**, **'개인정보는 공공재가 됐다'** 등의 무력감이 확산하고 있다. 그러나 **유출된 개인정보를 악용한 2차 피해 위협에 대한 면밀한 주의가 필요하다.**

유출된 개인정보가 **다양한 경로를 통해 수집·결합**될 경우, 사기전화(보이스피싱)이나 문자 결제 사기(스미싱) 등 보다 지**능화된 공격에 활용되어 피해자를 추가로 위협할 수 있다.**

과기정통부 **최우혁 정보보호 네트워크정책실**장은 **"향후 인공지능을 활용한 공격이 현실화하고, 인터넷 기반 자원 공유(클라우드) 환경 취약점을 악용한 공격 등 사이버 위협이 더욱 지능화·고도화될 것으로 전망된다."** 라며,

"이에 대비할 수 있도록 기업의 책임 있는 정보보호 강화를 당부하는 한편, **정부 또한 인공지능 기반의 예방·대응체계를 운영하고, 보안 사각지대를 선제적으로 관리하여 국민이 안심할 수 있는 사이버 환경을 조성해 나가겠다"** 라고 밝혔다.

붙임 : '26년 위협 전망 및 '25년 주요 사고사례 포스터 1부. 끝.

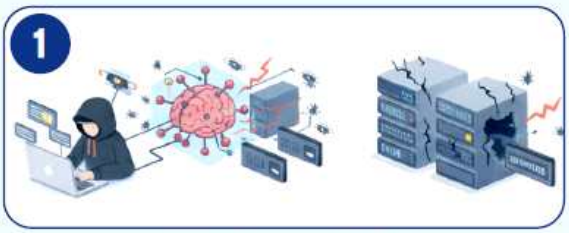
담당 부서	정보보호네트워크정책관실 사이버 침해조사팀	책임자	팀장	김우철 (044-202-6490)
		담당자	사무관	김성환 (044-202-6491)
관련 기관	한국인터넷진흥원 위협분 석단	책임자	단장	박용규 (02-405-4800)
		담당자	팀장	김광연 (02-405-4810)

내일을 만드는 과학기술
내삶을 채우는 디지털·AI
대한민국 정책브리핑
OPEN 출처표시
공공누리 공공저작물 자유이용허락

붙임1 `26년 위협 전망 및 `25년 주요 사고사례 (포스터)

과학기술정보통신부 KISA 한국인터넷진흥원

2026년 사이버 위협 전망



AI활용 위협의 일상화,
AI 서비스에 대한 위협 증가



기술지원종료,
쉐도우 시스템에 대한 위협 증가



취약한 클라우드 보안
환경의 공격 증가



유출된 개인정보를 악용한
2차 사이버 위협 증가

2025년 사이버 위협 분석



국민 생활과 밀접한
다수 침해사고 사례



오픈소스 및 IoT 생태계를
악용한 공급망 사고사례



다수 고객망 운영기업 대상,
랜섬웨어 사고사례

AhnLab Genians IGLOO NSHC S2W PLAINBIT
SK 쉴더스 CISCO TALOS Google Microsoft TREND zscaler