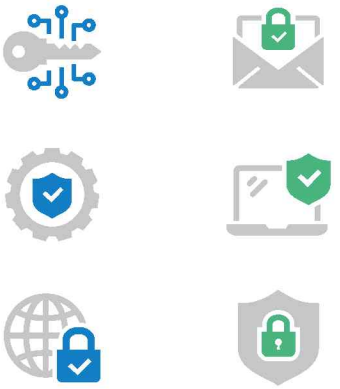
2025 VOL. 03
2025. 12

KISA INSIGHT



리더들이 전망하는 2026년 사이버보안 이슈

1. 인터넷법제도포럼 이상직 회장

2. 한국정보보호산업협회 조영철 회장

3. 한국정보보호학회 김호원 수석부회장

한국인터넷진흥원 김인섭 수석연구원 | 김다혜 주임연구원 | 김성훈 팀장

DIGITAL &
SECURITY
POLICY

KISA 한국인터넷진흥원

CONTENTS

KISA INSIGHT

2025 VOL. 03

DIGITAL & SECURITY POLICY

리더들이 전망하는 2026년 사이버보안 이슈

인터넷법제도포럼 이상직 회장 | 한국정보보호산업협회 조영철 회장 |
한국정보보호학회 김호원 수석부회장

I 리더들이 전망하는 2026년 사이버보안 이슈 I

I-1. (25년 평가) 사이버보안에 전방위적 위기가 닥쳤다. 1

I-2. (26년 전망) AI 대전환 시대, 반드시 선행되어야 할 필수 인프라는 사이버보안이다. 3

II 리더들이 전망하는 2026년 사이버보안 이슈 II

II-1. (25년 평가) 사이버보안 산업, 2025년 위기 속의 성장 모멘텀 확보 5

II-2. (26년 전망) 위기를 기회로 : 사이버보안 산업, AI시대의 기반 산업으로 도약 7

III 리더들이 전망하는 2026년 사이버보안 이슈 III

III-1. (25년 평가) 사이버 공격 관련하여, 공격자 우위의 시대가 본격화 및 연이은 대형 침해 사고로 확인된 구조적 한계 10

III-2. (26년 전망) "사이버보안 체질 개선"과 "AI 기반 위협 심화" 동시에 전개 13

IV 2026년 글로벌 사이버보안 이슈 전망

IV-1. 가트너 - 2026년 10대 전략 기술 트렌드 21

IV-2. 팔로알토 네트웍스 - AI 경제에 대한 6가지 예측 : 2026년의 새로운 사이버보안 규칙 22

IV-3. 포브스 - 사이버보안 2026: 6가지 전망과 청사진 23

IV-4. 구글위협인텔리전스그룹 - 2026년 사이버보안 전망 보고서 25

『KISA Insight』는
디지털·정보보호 관련 글로벌 트렌드 및 주요 이슈를
분석하여 정책 자료로 활용하기 위해
한국인터넷진흥원에서 기획, 발간하는 심층 보고서입니다.

이번 보고서는 12월을 맞이하여
올 한해를 평가하고 2026년을 전망하는
특집으로 준비하였으며
사이버보안 정책 포럼에 참여하고 계신 3인의 리더들이
집필에 참여해 주셨습니다.
이 자리를 통해 감사 인사를 드립니다.

작성

한국인터넷진흥원 정책연구실 정책연구팀

김인섭 수석연구원	061-820-1513	iskim07@kisa.or.kr
김다혜 주임연구원	061-820-1518	dahyekim@kisa.or.kr
김성훈 팀장	061-820-1510	shkim@kisa.or.kr

발간일 2025년 12월 02일

기획·발간처 한국인터넷진흥원 정책연구실 정책연구팀

I

리더들이 전망하는 2026년 사이버보안 이슈 I

이상직 인터넷법제도포럼 회장

- (現) 법무법인(유한) 태평양
- (現) 인터넷법제도포럼 회장
- (前) 국가지식재산위원회 인공지능 지식재산 특별위원장
- (前) 한국인터넷진흥원 비상임이사

I-1. 2025년 평가
사이버보안에 전방위적 위기가 닥쳤다.

▌사이버보안 침해 사고가 정교화, 일상화되고 있다.

- 인류의 삶이 디지털과 밀접성을 높이고 있는 가운데, 2025년은 사이버 공격과 침해사고가 유독 빈번했다. SK텔레콤, 케이티 등 대형 통신사뿐만 아니라 롯데카드 등 금융기관, 온라인 쇼핑몰도 예외가 아니었다.

- 해킹 세력은 끊임없는 침해경험과 전문성을 높이는 등 침해기술을 발전시켰고, 공격 접점을 넓혀가면서 기업의 인적, 물적 실수나 오류를 찾아내고 악용하기도 했다. 기업 내부 상황에 밝은 사람의 범죄 관여가 있다면 침해사고 피해가 현저히 커진다.

- 과거엔 기업이 충분한 보안 투자를 통해 방어시스템을 갖추면 사이버 공격을 막아낼 수 있었지만, 최근 상황은 대기업조차 사이버 공격에 침해 사고가 발생하고 있다. 피해기업의 자체 보안만으로 방어할 수 있는 한계에 직면했다.

• 중소기업의 경우, 침해 사고가 발생하면 성장이 중단될 뿐 아니라 즉각 경영 위기에 봉착하기도 한다. 정부, 기업, 보안업체, 고객 등 다양한 이해관계를 가진 보안 생태계를 굳건하게 갖춰 체계적인 공동 대응이 절실하다.

▌사이버 공격과 범죄에 인공지능(AI)을 활용하기 시작했다.

• 해킹 세력은 AI를 이용해 범죄 전략을 수립하기 시작했다. AI를 활용해 랜섬웨어, 악성 코드를 개발, 생성하여 기업의 시스템에 투입하고, 침해 이메일, 페이크 영상, 음성을 정교하게 작성한다. 허위 또는 대량의 데이터를 기업 시스템에 투입하는 등 피해기업의 허점을 찾아내 오류를 일으키거나 정보 유출, 작동 혼란 등 무력화하는 단계에까지 이르렀다. 사이버 공격은 날이 갈수록 지능화 수준을 높이고 있다.

• 피해기업의 보안시스템을 우회하거나 새로운 형태의 공격 방법, 변종 악성 코드를 통해 피해기업이 대응할 수 있는 여유를 주지 않고 즉각 침해 사고를 일으키는 위험이 증가하고 있다. 경우에 따라선 악성 코드를 심어두고 정보 유출까지 오랜 기간 기다리는 인내심을 보이기도 한다.

• 기업의 AI 전환도 증가하고 있는데, 사이버보안 시스템에 AI를 도입하는 과도기에 충분한 데이터와 알고리즘을 확보하지 못한다면 해킹 세력이 AI 오작동 등을 유도, 악용하고 방어시스템의 AI를 속이는 커뮤니케이션 수단까지 등장할 것으로 우려되고 있다.

▌동남아시아에서 조직적인 사이버 범죄 조직이 발각됐다.

• 캄보디아, 미얀마 국경 지역의 사이버 범죄 조직이 국내 피해자를 대상으로 보이스피싱 등 범죄를 조직적으로 저지르다가 발각됐다. 우리 청년들에게 고수익을 보장하겠다고 속여 유인, 감금하여 피싱 범죄를 저지르도록 강요하고 응하지 않으면 무자비한 폭력을 행사했다. 피해자가 가해자가 되는 악순환이 반복됐다.

• 현재 우리 정부와 현지 당국의 협력으로 사이버 범죄 조직을 소탕하고 있으나 많은 범죄자는 다른 국경 지역으로 이동하여 사이버 범죄조직을 재건할 위험이 있다. 또한 이들이 막강한 자금력으로 AI 활용이나 범죄 기술을 고도화 할 경우에는 또 다른 사이버 위협 요인이 될 것으로 보인다. 또한 이들 범죄조직이 다른 해킹 세력과 연계할 경우엔 침해 사고의 양적, 질적 위험이 더욱 증가할 것으로 우려된다.

• 사이버 범죄 예방과 대응에 국제적 협력이 쉽지 않다는 점 등을 고려한다면 기존의 사이버 방어시스템의 보완, 개선만으로는 근본적 해결이 어려운 상황이므로 사이버보안 패러다임의 근본적 변화와 새로운 보안 생태계, 거버넌스 구축이 요구된다.

I-2. 2026년 전망

AI 대전환 시대, 반드시 선행되어야 할 필수 인프라는 사이버보안이다.

▌AI 신기술을 사이버보안에 도입, 활용해 동적 보안 역량을 강화해 나간다.

- 끊임없이 진화하는 새로운 형태의 사이버 공격, 침해의 동적 환경에 대응하려면 인적, 물적 투자를 집중해 통합적 보안 역량 강화가 중요해진다.
- AI 등 신기술을 통해 대용량 데이터를 학습하고 추론하여 대용량 로그, 네트워크 트래픽, 공격 데이터와 패턴을 실시간 분석하여 비정상 징후, 새로운 형태의 위협을 실시간 탐지해 선제적, 즉각적 대응이 가능하도록 방어 전략을 갖추고 시스템화해야 한다.
- 물론 해킹 세력도 AI 신기술을 활용하여 기업의 방어시스템을 타겟팅하여 악성 데이터를 투입하고, 알고리즘 혼란을 야기하거나 결과값 수정 등 새로운 침해위협을 가할 수 있으므로 효과적인 대응 체계를 갖추어야 한다.

▌대기업 규모의 보안기업이 등장할 수 있도록 지원하고 보안산업 생태계를 육성, 강화한다.

- 현재 사이버 공격과 침해 사고 대응을 보면, 대기업은 계열사 지위에 있는 보안 기업이나 외부 보안 기업을 활용하는 경우가 많다. 이 경우 해당 보안 기업의 지위가 대기업에 비하여 영세하거나 열악하여 효과적인 보안시스템을 갖추지 못할 수 있다. 기업의 사이버보안 의식이 높아지고 있기는 하나 아직도 보안 투자를 매출 등 성과를 줄이는 비용 요소로 인식하는 폐단이 남아 있어 보안 산업 생태계가 발전할 수 없는 한계로 작용하고 있다.
- 사이버 공격과 침해 기술의 고도화로 피해기업 혼자 또는 계열사나 소규모 보안 기업의 지원을 받아서는 사이버 공격과 침해를 막기 어렵다. 보안 산업을 대규모로 성장시키고 보안 생태계 차원에서 사이버 공격과 침해를 막는 시스템을 갖춰야 한다. 인수 합병 등 다양한 방법을 통해 대기업 규모의 보안 기업이 등장할 수 있도록 지원해야 한다.

▌사이버보안 관계 법령을 재정비하고, 보안 거버넌스 확립을 추진한다.

- 사이버보안 관련 법령은 지능 정보화 기본법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률('정보통신망법'), 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률, 정보보호산업 진흥에 관한 법률, 인공지능 발전 및 신뢰 기반 조성 등에 관한 기본법, 개인정보 보호법, 신용정보의 보호 및 이용에 관한 법률 등으로 나뉘어 있다. 주무관청도 달라 칸막이식으로 분절되어 있어 날로 고도화되고 있는 사이버 공격과 침해에 대응해 유기적인 협력, 운영이 효과적으로 이루어지지 않을 수 있다.

- 정보통신망법은 개인정보 부분이 개인정보보호법으로 오래전 이관되었고 정보통신망 이용 촉진은 그 목적을 상당히 달성했으므로 정보통신망 이용 활성화보다는 사이버보안 중심으로 새롭게 프레임을 갖출 필요가 있다. AI 대전환과 사이버보안 패러다임 변화에 맞게 정보보호산업 진흥에 관한 법률 등과 함께 통폐합 또는 체계 정합성을 갖춰 '정보통신 보안 기본법' 등 새롭게 프레임을 구축하고 효과적인 보안을 위한 기반조성과 보안 산업 육성에 집중할 필요가 있다. 아울러, 침해위협 모니터링, 조기 신고와 체계적 대응, 인증 등 제도 효율화를 통한 법제 개선을 통해 기업의 방어력 강화가 이뤄질 것을 기대한다.

▌사이버보안 기본사회를 준비해야 한다.

- 사이버 위협 일상화, 전방위화, 대규모화, 피해의 회복 불가능성, 후속 피해 위험 증가와 이로 인해 국민 생활에 위해요소가 급격히 증가할 것이므로 통합적 보안 역량 강화와 방어시스템이 논의될 것으로 보인다. 물론, 국민에게 설명할 수 있고 납득할 수 있으며 지속 가능한 보안시스템의 구축이어야 한다.

- AI 시대는 사이버보안 없이 불가능하다. 사이버보안 기본사회는 디지털, AI 대전환 시대에 사이버보안이 국민 생활을 구성하는 기본적인 요소가 되는 사회다.

- 비밀번호의 수시 변경, 지문, 홍채 등 생체정보 활용, 단계별 보안 강화 등 방어력을 높여야 한다. 사이버보안의 생활화, 정기 및 수시 보안 생활교육과 보안 수칙 준수, 보안 수준 또는 품질평가, 적절한 시기와 방법으로 보안 교육을 받을 기회를 제공하는 등 다양한 방안이 강구되어야 할 것으로 기대한다.

II

리더들이 전망하는 2026년 사이버보안 이슈 II

조영철 한국정보보호산업협회 회장

- (現) 한국정보보호산업협회 회장
- (現) ㈜파이오링크 대표이사
- (前) 서울대학교 자동화시스템 공동연구소 전문연구원
- (前) Boston University Visiting Scholar
- (前) 서울대학교 제어계측학 학사, 석사, 전기공학 박사

II-1. 2025년 평가
사이버보안 산업, 2025년 위기 속의 성장 모멘텀 확보

▌정보보호 산업 현황 (KISIA, 2025년 정보보호산업실태조사 결과)

- 2024년 기준 국내 정보보호 시장 규모는 18.6조 원(10.5% ↑, +1조 8천억원)으로 국내 ICT 산업 전체 성장률(9.5% ↑)을 상회

※ 전년 대비 기업 수(4.2% ↑), 매출(10.5% ↑), 수출(11.4% ↑), 인력(+10.0% ↑)

〈표〉 ICT산업 및 정보보호산업 성장률 비교

구분	매출			수출		
	2023	2024	성장률	2023	2024	성장률
정보보호산업	16조 8,310억 원	18조 5,945억 원	+10.5%	1조 6,800억 원	1조 8,722억 원	+11.4%
ICT산업*	509.4조 원	557.7조 원	+9.5%	280조 원 (2,051억 달러)	345조 원 (2,532억 달러)	+23.5%

* 매출/수출: ICT 주요품목 동향 조사('24.12월호, '25.3월호)

• 국내 정보보호 영위 기업은 전체 1,780개(정보보안 876개, 물리보안 904개)이며, 중소기업 비중은 93.7%(1,668개)로 전년 대비 4.2% 증가

- 지역별로는 수도권에 1,383개, 비수도권 지역에 397개로 약 78%의 정보보호 기업이 수도권에 위치
- 2024년 매출액은 약 18조 6천억 원으로 전년 대비 10.5% 증가(+1조 8천억 원)하였으며, 이중 정보보안은 약 7조 1천억 원(15.9% ↑, +9천 8백억 원), 물리보안은 약 11조 5천억 원(7.3% ↑, +7천 8백억 원)으로 나타남
- 2024년 수출액은 약 1.9조 원으로 전년대비 11.4% 증가(+1,922억 원)했으며, 정보보안은 0.12조 원(15.9% ↓, △235억 원)으로 하락하였으나, 물리보안은 1.75조원(14.1% ↑, +2,157억 원)으로 수출액 상승 견인
- 정보보호 산업의 종사자 수는 총 66,367명으로 전년 대비 10%(+6,059명) 증가하였으며, 그 중 정보보안 인력은 23,987명(0.2% ↑, +40명), 물리보안 인력은 42,380명(16.6% ↑, +6,019명)으로 나타남

(현실이 된 위기) 광범위한 대형 사이버 침해 사고 발생

• 국민의 삶과 밀접한 통신사, 카드사, 인터넷 서점 등 광범위한 업종에서 심각한 사이버보안 사고가 연쇄적으로 발생

• 결과적으로 사이버보안 사고의 결과로 랜섬웨어 감염에 따른 서비스 중단, 개인정보 유출 및 무단 소액 결제 피해까지 심각한 피해 초래

• 이에, 산업계는 민관합동 조사단 등을 통해 대규모 사이버보안 사고에 대응하고 피해 수습에 적극적으로 참여

〈표〉 2025년 주요 사이버 침해 사고

연번	사고 발생 기업	피해 유형	피해 규모
1	**롯데 카드**	개인정보 유출	**297만 명**
2	KT	불법 소액 결제	**362명**
3	**예스24**	시스템 마비	**약 7시간 접속 불가**
4	**SGI 서울보증**	보증정보 유출	**약 13TB(조사 중)**
9	SKT	개인정보 유출	**2,324만 건**

(시장개척) 제로트러스트, N2SF 등 신규 보안 이슈 및 패러다임 대응

• 새로운 보안 패러다임으로 제시되는 제로트러스트, N2SF 등 실증 사업에 적극적으로 참여하여 새로운 시장을 개척

- 그 외 제로트러스트, AI, 서비스(컨설팅, 관제), 랜섬웨어 대응, 자율보안, 클라우드보안, CPS보안 등 다양한 이슈에 대해 산업계 차원의 협의체를 조직하여 의견을 개진하고 공동으로 대응

(정책제안) 사이버보안 산업계 차원의 정보보호 관련 정책 제안 활동

- 지난 대선 시 '사이버보안 없이 AI시대 없다.'라는 슬로건 아래 사이버보안 산업투자, 인식 제고 및 기반 조성, 인력양성, R&D, 수출 활성화 등의 정책 공략을 정당별로 제안하며 교류 확대
- 또한, 지속되는 해킹 사고에 대응하여 '범부처 정보보호 종합대책' 설계 시 정보보호 투자 확대, CISO 권한 강화, 인력양성 등의 의견을 개진

II-2. 2026년 전망
위기를 기회로: 사이버보안 산업, AI시대의 기반 산업으로 도약

(변화의 시작) C-level의 사이버 위기 대응 리더십 강화와 문화 정착

- 2025년의 연이은 대형 해킹과 정보 유출 사고는 사이버보안이 더 이상 IT 부서의 전담 영역이 아님을 명확히 보여주었다. 이제 보안은 기업 경영의 생존 전략이며, CEO와 경영진이 직접 관리해야 하는 핵심 영역으로 인식되고 있다. 정부는 2025년 「범부처 정보보호 종합대책」을 통해 CEO의 보안책임 원칙을 법령에 명문화하고, CISO·CPO에게 실질적인 권한을 부여하는 제도적 전환을 추진했다. 이에 따라 IT자산 통제권, 이사회 정기 보고 의무화, 정보보호 투자기준 마련 등이 구체적 조치로 이어지며, 2026년은 이러한 변화가 기업 경영 문화 전반에 뿌리내리는 「리더십의 원년」이 될 것으로 예측된다.
- 앞으로 기업들은 보안을 "위기 대응 부서의 역할"이 아니라 조직의 DNA로 내재화해야 하는 문화적 요소로 인식하는 방향으로 변화할 것이다. CEO가 직접 보안회의를 주재하고, 이사회가 보안투자를 주요 의사결정 안건으로 다루는 것이 보편화될 전망이다. 이러한 보안 리더십 강화는 단기적 규제 대응을 넘어, 기업이 스스로 신뢰를 설계하고 지배구조 속에 보안을 포함시키는 변화로 이어질 것으로 예상된다.

(전략적 투자) 사이버보안 투자 확대 및 새로운 보안 체계 도입의 시작

- 2025년 대형 해킹 사고들은 기존의 경계형 보안 체계가 한계에 도달했음을 증명했다. 이제 정보보호 산업계는 단순히 방화벽과 탐지시스템에 의존하는 수동적 방어에서 벗어나, 데이터 흐름과 접근 권한 전반을 통제하는 제로트러스트(Zero-Trust) 기반으로의 전환을 가속화하고 있다.

- 정부가 발표한 N2SF(Next National Security Framework) 가이드라인은 민간 기업들이 이러한 개념의 보안 체계를 설계·도입할 수 있도록 구체적 표준을 제시하고 있으며, 2026년은 이를 토대로 산업별 보안 아키텍처 전환 사업이 본격화될 것으로 예상된다. 이러한 변화는 단순한 기술 업그레이드가 아니라, 전략적 투자로서의 변화를 의미한다. 앞으로 보안 예산은 AI, 클라우드, 데이터산업 등 신성장 분야의 기반 요소로 인식될 것이다. 따라서 기업들은 향후 「보안을 위한 투자」에서 「투자를 보호하기 위한 보안」으로 관점을 전환하며, 보안 투자를 비용이 아닌 생존자산으로 평가할 것으로 예측된다.

(당면과제) AI기반 위협의 부상과 지능형 방어 시대의 개막

- 2026년 사이버 위협의 양상은 인공지능의 확산과 함께 근본적으로 변화하고 있다. AI는 보안의 도구이자 위협이 되고 있으며, 생성형 AI의 보급으로 공격자는 더욱 정교하고 개인화된 공격을 수행할 수 있게 되었다. 맞춤형 피싱, 딥페이크, 승인받지 않은 AI 도구의 무단 사용 등, AI가 만들어 내는 공격 방식은 인간의 감각으로 식별하기 어려운 수준으로 발전하고 있다.

- 그러나 동시에 정보보호 전문 기업들도 AI를 활용한 지능형 방어체계(Intelligent Defense)를 고도화하고 있다. AI 탐지 엔진은 실시간으로 비정상 패턴을 학습하며, 인간 분석가가 인지하지 못하는 위협의 징후를 조기에 포착한다. 이로써 방어체계는 단순히 「탐지」 중심에서 「예측·대응」 중심으로 진화하고 있으며, AI가 사람 대신 방어 결정을 내리는 시대가 열리고 있다.

- 따라서 2026년은 공격과 방어의 경계가 모두 AI에 의해 재편되는 「AI 대 AI의 사이버전(戰)」이 본격화되는 해가 될 것이다.

(미래 대응) AI 시대의 사이버보안: 신뢰 기반 위에 지능을 더하다.

- AI가 모든 산업의 경쟁력을 좌우하는 시대에, AI의 신뢰성과 투명성을 보장하는 핵심 요소는 바로 「보안의 내재화(Secure by Design)」이다. AI가 아무리 발전하더라도 데이터가 변조되거나 학습 과정이 조작되면, 그 결과는 더 이상 신뢰할 수 없다. 따라서 AI 산업의 성장은 보안이 보장될 때에만 가능하며, AI 보안은 이제 기술 선택이 아니라 AI 강국으로 가는 필수 조건으로 자리 잡고 있다.

- 특히 AI 보안은 단순한 기술 보호가 아닌 윤리적 신뢰 확보의 문제다. AI 모델의 투명성, 데이터 무결성, 개인정보 보호는 글로벌 시장 진출의 기본 요건이자 기업의 평판자산이 될 것이다.

- 결국 2026년 이후의 보안 패러다임은 「지능」의 경쟁이 아니라 「신뢰」의 경쟁으로 이동하게 될 것이다. 이러한 변화에서 C-level 리더십과 전략적 투자, 그리고 AI 중심의 새로운 보안체계가 결합될 때, 대한민국은 안전한 AI 시대의 토대를 구축하고 글로벌 기술 강국으로의 도약을 실현할 수 있다.

(결론) 위기를 넘어, 국가 전략 산업으로의 도약

- 2026년은 사이버보안 산업이 위기관리 산업에서 성장 산업으로 전환되는 해가 될 것이다. C-level의 리더십 강화는 보안의 조직 내 위상을 높이고, 전략적 투자는 산업 전반의 보안 체질을 혁신할 것이다. 또한 AI 시대의 지능형 위협에 대응하기 위한 기술적 고도화와 신뢰 기반의 관리체계는 정보보호 산업을 AI 혁신을 뒷받침하는 기반 산업으로 격상시킬 것이다.

- 이제 정보보호는 기업의 방패가 아니라 전 산업의 핵심 축이 되었다. 향후 정보보호 산업은 위기 속에서도 신뢰를 축적하고, AI의 발전 위에서 새로운 성장의 지평을 여는 산업으로 도약할 것이다.

III

리더들이 전망하는 2026년 사이버보안 이슈 III

김호원 한국정보보호학회 수석부회장

- (現) 한국정보보호학회 수석부회장
- (現) 부산대 컴퓨터공학과 정교수
- (現) ㈜스마트엠투엠 대표이사
- (現) 부산대 블록체인 플랫폼연구센터, 지능형 사물인터넷 연구센터 센터장
- (前) 한국전자통신연구원 선임연구원/팀장
- (前) 경북대 전자공학과 학사, 포항공대 전기전자 석사/박사

III-1. 2025년 평가

사이버 공격 관련하여, 공격자 우위의 시대가 본격화 및 연이은 대형 침해 사고로 확인된 구조적 한계

▌공격자 우세의 현실화

- 2025년은 국내외 전방위적 침해 사고가 동시다발적으로 발생하며, 공격자가 방어자보다 앞서 있는 시대가 본격화된 해로 볼 수 있음
- 즉, 생성형 AI, 자동화 공격도구, RaaS(Ransomware-as-a-Service)의 확산은 물론, 다크웹을 통한 전문 공격 툴과 익스플로잇의 손쉬운 구매 및 확산으로 공격자는 더 빠르고 정교하게 공격이 가능해짐
- 반면 피해기업과 기관은 레거시 시스템의 보안 이슈, 탐지 체계 미성숙, 조직적 거버넌스 부재 등, 구조적 한계를 해결하지 못해 방어와 대응 모두 공격의 속도와 질적 변화를 따라가지 못하는 상황이 발생함

- 비록 ISMS 등 제도적 장치는 있었으나 실제 보안 성숙도를 끌어올리기엔 부족했고, 공격자는 동일한 취약점 패턴을 여러 산업에서 반복적으로 악용하며 공격 효과를 극대화하고 있음
- 이처럼, 2025년은 한국 ICT 인프라 전반에서 사이버보안 분야에서"공격자 우위"가 확인된 해로 볼 수 있음

생활밀착형 서비스 전반에서 사이버 공격 피해가 확산

- 통신 분야와 금융 분야, 전자상거래 분야 등, 국민 생활과 밀접한 업종에서 대형 사이버 공격 사고가 연속적으로 발생함
- 서비스 중단과 고객정보·결제정보 유출, 무단 결제, 랜섬웨어 암호화 등 복합적 피해가 광범위하게 나타나 사회적 및 기술적 신뢰가 크게 흔들림

레거시 시스템의 사용과 패치 지연, 취약한 IT 인프라 누적

- 오래된 시스템과 신규 서비스가 혼합된 구조에서, 권한 분리나 암호화, 접근통제 등, 기본 보안 설계가 일관되지 못해 다수의 취약 지점이 동시에 드러남
- 또한, 보안 패치 지연, 구성 오류, 노출된 API, 취약한 인증 체계가 한꺼번에 악용되며 공격자에게 '대량 침투'를 허용하게 됨

공격 탐지 및 관제 체계의 실전성 부족

- 공격자의 장기 잠복과 수평이동을 감지하지 못하고 침해 사실 인지까지 수 주~수 개월이 소요되는 사례가 반복됨
- 백업과 복구 체계의 미흡으로 동일 기업이 두 번 연속 감염되는 사례도 발생함
- 위협 헌팅, 행위 기반 탐지, 클라우드/OT 통합 관제 역량 부족이 공통적으로 확인됨

사이버보안 정책과 제도의 실효성 한계

- ISMS 등 인증제도가 존재했음에도 사고가 잇따르며, 서류 기반 평가 중심 구조의 근본적 한계가 드러남. 즉, 기업과 기관이 이러한 인증 제도를 적극적으로 수용하고자 하는 의지가 약했음

- 또한, 제도는 산업별 위험도 차이를 충분히 반영하지 못해, 대형 통신·금융기관과 중소 온라인몰이 동일 기준을 적용받는 불균형이 지속되고 있음

피해자, 공격자 및 당국 관점에서 본 2025년의 주요 사이버 침해 사고의 특성

(피해자 관점) 왜 이러한 공격을 막지 못했는가?

- 기술 및 시스템, 서비스의 취약성과 조직/문화적 취약성이 존재한 것으로 보임
- 즉, 레거시 인프라, 패치 지연, 권한관리 실패, 중요데이터 암호화 부재 등 구조적 약점이 누적되어 있었으며, 탐지체계 성숙도 부족으로 초기 침입 및 내부 확산을 조기에 식별하지 못함
- 또한, 일부 기업은 백업 및 복구 전략이 미흡해, 동일 공격 그룹에 재감염되는 사례까지 발생함
- 그 외에 조직 및 문화 관점에서도 취약성도 존재함
- 즉, 보안보다 기능·서비스 출시를 최우선하는 내부 문화와 사이버보안을 바라보는 배타적인 시각, 그리고 사이버보안 전문 인력 부족과 예산 제약으로 공격자의 AI 기반 자동화 속도를 따라가지 못함

(공격자 관점) 어떻게 이러한 공격을 성공시킬 수 있었을까?

- 공격자 관점에서는 고도화 및 자동화된 공격 수단을 가지고 있었으며, 또한, 소위 말하는 공격 파이프라인을 갖추기 용이했음
- 예를 들어, APT 공격과, eBPF 기반 백도어, 클라우드 자격증명 탈취 공격 등, 고급 공격 기법을 비교적 쉽게 사용할 수 있는 환경이 됨
- 생성형 AI를 활용한 피싱과 스캐닝, 취약점 weaponizing 속도와 효율성도 증가한 것으로 보임
- 이를 통해, 쉽게 공격 파이프라인 및 생태계 구축이 용이했음. 즉, RaaS나 Initial Access Broker를 초보 공격자들도 사용할 수 있는 상황이 되었음
- 또한, 공격자들은 한국의 대형 IT 플랫폼이나 통신 기업들에 대해, 한번 공격에 성공하게 되면, 막대한 이익을 얻을 수 있을 것으로 판단하여, 전략적으로 공격 목표를 정한 후, 지속적 표적 공격을 수행한 것으로 보임

▌(사이버보안을 책임지는 기관과 당국자 관점) 어떤 어려움이 있었을까?

- 예를 들어, ISMS가 있었는데도 왜 사이버보안 공격을 막는 것이 어려웠을까? 이는 제도적인 한계와 현장에서의 감독 권한 부재, 그리고 분산된 거버넌스 때문이었을 것으로 보임
- 즉, ISMS는 체크리스트·서류 검증 중심으로, 실제 운영 보안 수준과 실전 대응 역량을 지속해서 평가하는 것이 어려움
- 또한, 위험 기반 감독이 부족했을 것으로 보임. 산업별 위험도나 보유 데이터 민감도 차이가 충분히 반영되지 않아 고위험군 사업자의 취약점이 그대로 노출됨
- 분산된 거버넌스도 체계적인 대응을 어렵게 함. 예를 들어, 과기정통부–KISA–금융보안원–국정원 등, 관계 기관 간 역할 분산으로 인해 신속한 일원화 대응이 어려웠을 것으로 보임
- 또한, 기술과 전문 인력, 예산 지원 측면에서도 현장 중심의 사이버보안 역량 강화가 충분히 이루어지지 못한 것으로 보임

III-2. 2026년 전망
"사이버보안 체질 개선"과 "AI 기반 위협 심화" 동시에 전개

▌사이버보안 재구축 출발점으로서의 2026년

- 2025년의 연속된 대형 사이버 공격 침해 사고는 기존 보안 체계의 구조적 한계를 명확하게 드러내며, 2026년은 그 한계를 개선하기 위한 변화가 본격화되는 해
- 즉, 기업과 기관은 더 이상 기존의 경계형·패치 중심 보안 체계만으로는 AI·자동화 기반 공격의 속도와 복잡성을 방어할 수 없음을 인식해야 함
- 특히 CEO와 이사회 중심의 보안 리더십 강화와 CISO 권한 확대, 보안을 경영의 핵심축으로 통합하는 움직임이 조직문화 전반에 정착되기 시작할 것으로 보임
- 이에 따라 2026년은 단순한 보안투자 확대가 아니라, 기업이 시스템·프로세스·조직 전반에 신뢰 구조(Trust Architecture)를 내재화해야 하는 재구축의 출발시점이 되어야 함

AI 기반 공격의 고도화와 AI 기반 방어의 본격적 확산 : AI 확산이 만든 새로운 위협 환경

- 생성형 AI와 자동화된 취약성 스캐너, 딥페이크 등은 공격자에게 더 낮은 비용으로 더 높은 성공률을 제공하며, 2026년에는 공격이 더욱 정밀·대규모·다층화될 것으로 볼 수 있음
- RaaS 생태계에 AI 기능이 결합 되면서, 전문성이 낮은 공격자조차 고급 공격을 손쉽게 수행할 수 있게 되고, 이는 조직이 직면하는 위협의 양과 질을 모두 증가시키는 요인이 될 것으로 보임
- 반면 방어측에서도 AI 기반 탐지·행위 분석·예측 모델을 활용한 지능형 방어체계가 확산되며, 탐지를 넘어 선제적 대응까지 가능한 AI 기반 자율 방어 시대가 본격화될 것으로 볼 수 있음
- 이처럼 2026년은 공격자와 방어자 모두가 AI를 핵심 도구로 삼는 대대적 기술 전환의 해가 될 것으로 보임

제도와 감독 체계의 실질적 개선 시작 : 제도적 한계가 드러난 이후의 조정 방향

- 2025년의 사고는 여러 가지 사이버보안 관련 제도가 존재함에도 불구하고 해킹 사고가 반복됨. 이는 제도적 한계와 감독 체계 부재에 있었음을 보여주었고, 2026년은 이를 개선하기 위한 노력이 본격적으로 진행될 것으로 보임
- 예를 들어, ISMS는 체크리스트·서류 중심 심사로 인해 실제 운영 보안 수준이나 탐지·대응 역량을 충분히 반영하지 못했고, 산업별 위험도를 고려한 차등 감독도 부족했다는 점이 핵심 한계로 지적됨
- 또한 과기정통부–KISA–금융보안원–국정원 등 여러 부처·기관 간 역할이 분산되어 있어 신속한 일원화 대응이 어려웠으며, 현장 중심의 기술·인력·예산 지원이 충분하지 않았던 점도 문제로 제시됨
- 이에 따라 2026년에는 운영 보안 중심의 실질 인증 강화, 산업별 위험 기반 차등 감독, 사고 발생 시 재평가·교정 명령 도입 등 보다 현실적인 제도적 보완 과제가 핵심적으로 다뤄져야 함

기업·정부·산업 전반에서 실질적 보안 생태계 구축 필요

- 2026년은 공격자 우위가 지속되는 환경 속에서, 기업·정부·산업계가 기존의 “형식적 보안 관리 체계”에서 벗어나 실제 운영 보안과 지능형 방어 중심의 생태계로 전환하는 출발점이 될 것으로 보임
- AI 기반 위협이 빠르게 고도화될수록, 보안은 선택적 기능이 아니라 AI 시대의 신뢰·안정성·경쟁력을 결정하는 국가적 기반 요소로 확고히 자리매김할 것으로 예상됨

참고 1 사이버보안 정책 포럼 소개

❙ 개요

• 민간 분야 사이버보안 정책 방향 논의와 협력 기반 강화를 위해 사이버보안 분야 리더, 전문가 등이 참여하는 「사이버보안 정책 포럼」을 운영

❙ 연혁

• ('21.11월) 사이버보안 정책 포럼 창립 총회 개최
• ('22.12월) 사이버보안 정책 포럼 정기 총회 개최
• ('23. 7월) 2023년 제1회 사이버보안 정책 포럼 공개 워크숍 개최
• ('23.12월) 2023년 제2회 사이버보안 정책 포럼 정기 총회 및 워크숍 개최
• ('24.11월) 2024년 사이버보안 정책 포럼 정기 총회 및 워크숍 개최
• ('25. 7월) 2025년 정보보호 주간 사이버보안 정책 포럼 세미나 개최
• ('25.12월) 2025년 사이버보안 정책 포럼 정기 총회 및 워크숍 개최

❙ 회원 현황

구분		소속	이름	직위
의장		한국인터넷진흥원	이상중	원장
		한국정보보호학회	박영호	회장
운영위원	협단체	한국CISO협의회	이기주	회장
		한국CPO포럼	정태명	회장
		한국정보보호산업협회	조영철	회장
		한국침해사고대응팀협의회	원유재	회장
		인터넷법제도포럼	이상직	회장
		5G보안협의회	염흥열	위원장
		한국정보보호학회	김호원	수석부회장
	정부·기관	과학기술정보통신부	임정규	국장
		AI안전연구소	김명주	소장
		정보통신기획평가원	김창오	정보보안PM
		국가기술보안연구소	오형근	부소장
		한국전자통신연구원	김정녀	본부장
		한국인터넷진흥원	이익섭	실장
	학계	상명대학교	유진호	교수
회원	정부·기관	국가사이버위기관리단	이현호	단장
		과학기술정보통신부	김연진	과장
		과학기술정보통신부	심재환	사무관
		한국인터넷진흥원	이동근	본부장
	산업계	한국정보보호산업협회	배환국	수석부회장
		한국정보보호산업협회	김진수	수석부회장
		스틸리언	박찬암	대표
		티오리	박세준	대표
		법무법인 세종	최광희	고문
	학계	숭실대학교	이정현	교수
		중앙대학교	최명길	교수

참고 2 2025년 사이버보안 정책 포럼 세미나 개최 현황

[제1회]

NO.	주제	발표자	일시 / 장소
1	**AI에서의 안전 그리고 보안**	AI안전연구소 김명주 소장	3.26(수) / 달개비

〈주요 내용〉

- 챗GPT 등장 이후 구글과 마이크로소프트 간 글로벌 AI 경쟁이 심화되었으며 GPT-4, Bard 등 생성형 AI 공개에 따른 보안 취약점, 데이터 유출 문제 발생
  - 제프리 힌튼 등 딥러닝 분야 전문가들이 AI의 위험성을 경고하였으며 Hallucination, Jail break와 같은 예상치 못한 부작용 발생
- 안전한 AI 개발 요구가 급증하였으며 윤리와 규제 등 AI 거버넌스가 본격화됨
  - 미국 AI 행정 명령과 EU 등 주요 국가들이 AI의 윤리적 사용과 보안 강화를 위한 정책을 마련했으며 AI의 악용, 개인정보 유출 방지를 위한 법적 기술적 대응 필요
- 딥시크 AI를 비롯한 일부 오픈소스 AI는 보안 취약점으로 인해 악용될 가능성이 높으며 특히 Jailbreak와 데이터 조작 위험이 존재하여 강력한 보안 검토가 요구됨
- AI RISK(위험)영역은 정치, 경제, 사회, 안보 등 범위가 매우 넓으며 SAFETY 라는 개념은 AI의 윤리적 측면부터 SECURITY를 모두 포함
- 소프트웨어에서 개발자의 검사(Verification) 및 수요자의 검증(Validation)이 핵심이 되듯 AI에서의 Security에서는 신뢰성 보장(Trustworthy)이 핵심
  - AI 신뢰성을 보장하는 기술적·사회적 대응이 필요하며 AI 윤리 및 규제 프레임워크 정비 필요성 증가
  - AI기술 때문에 생기는 문제에 대한 허브 역할을 AI 안전연구소가 하고 있지만 해결을 위한 정책이나 기술은 부처·조직별 전문성을 고려하여 협업해야 함

[제2회]

NO.	주제	발표자	일시 / 장소
2	**RSAC 2025 시사점과 글로벌 동향**	한국정보보호산업협회 조영철 회장	5.28(수) / 달개비

〈주요 내용〉

- 키노트에서 AI가 실질적인 활용과 협업의 도구로 활용됨에 따라 AI를 활용한 강력한 방어체계 확보가 급선무임을 강조
  - AI가 공격도 방어도 주도하고 있으며 인간 중심의 통제가 필수적
- 국가 간의 사이버 분쟁이 눈에 가시적으로 보일 정도로 구체화 되었으며 사이버 분쟁은 전쟁과 동일해지고 있어서 이에 대한 대비 필요
  - 국가와 민간의 협력, AI에 대한 신뢰 구축 등이 필요하고 매년 새로운 공격 유형*의 등장에 대비해야 함
    * 클라우드 환경, ICS 시스템 위협, AI 규제 위협 등
- 기술 10대 키워드로 AI, LLM, SBOM, 윤리 등 사이버보안 전반의 기술적, 정책적, 문화적 이슈를 다각도로 조명하였으며 AI 기반 위협의 인식, 보안에 대한 정체성, 윤리적 규제, 양자 위협 등이 핵심적으로 논의됨
- 주요 국가들은 사이버보안 산업 국제 경쟁력 강화를 위해 차세대 핵심 기술을 활용한 통합 연구개발 및 해외 신시장 진출 등 다양한 지원 정책 추진 중
  - 현재 한국은 IT 예산 대비 기업의 정보보호 투자 비중은 선진국에 비해 다소 저조한 편으로 기업의 보안 역량 확보를 위한 투자 필요
  - 민간 중심의 AI 보안 테스트베드 확대가 필요하며 AI 보안 인재 양성 등이 요구됨
- AI 보안 기술의 중요성과 함께, 국가 차원의 전략 수립과 민관 협업을 통한 글로벌 경쟁력 확보 필요
  - AI 시대의 사이버 위협은 단순한 기술 문제가 아닌 거버넌스와 생태계 전반의 문제로 인식해야 하며, 이를 해결하기 위한 다층적 대응 체계 구축 필요
  - 내수시장 규모 확대, 보안 투자 확보, 정부와 기업의 글로벌 시장 진출 협력 체계 확보, M&A 활성화 장려 및 정보보호 펀드 확대 등을 통한 산업 성장 기대

[제3회]

NO.	주제	발표자	일시 / 장소
3	**국내·외 AI 보안 동향 및 향후 정책 방향**	한국인터넷진흥원 정현철 연구위원	9.24(수) / 달개비

〈주요 내용〉

- 챗GPT 등장 전후 공격자와 방어자 모두 많은 부분이 바뀌었으며 보안 시장에서도 AI 보안이 하나의 메가트렌드로 자리를 잡음
- AI 기반 피싱공격 자동화 문제가 심각한 수준이며 범죄자들은 대규모 언어모델 챗봇을 사용하여 고도로 표적화된 피싱 공격을 다발적으로 실행
- AI는 기존 시스템에 비해 불명확성의 특징을 가지고 있으며 이제는 챗GPT 같은 대화형 AI를 넘어 스스로 판단하고 실행하는 AI 시스템(AGENTIC AI), 물리 장치에서 작동하는 AI(PHYSICAL AI)로 진화할 전망
- 최근 주요국들은 AI 보안을 '안전·신뢰성'에서 '국가 안보' 관점으로 변화하는 추세
  - AI를 악용한 사회 문제들을 해결하고 기술 패권을 주도하기 위한 AI 시큐리티를 강조
- 미국은 AI 기반 산업혁명, 정보혁명 등 다발적 혁신과 AI 글로벌 주도권 확보 유지를 위한 AI 액션플랜을 발표하였으며 Security 키워드를 반복하여 강조함
- 우리나라도 AI 관련 내용들이 포함된 123대 국정운영을 발표하였으나 사이버보안 및 AI보안 관련 내용은 강조되지 않은 아쉬운 점이 존재
  - 하지만 최근 전략위원회에서 보안 TF를 만들어 보안 관련 중요한 부분이 정책에 반영될 수 있는 기대감 상승
- AI 보안 정책 포럼 운영 추진, AI 보안 기준 마련, AI 레드팀 구성, AI 취약점 발굴 및 공유, AI 보안 인증 추진, AI 기반 탐지·대응체계 고도화 등 추진 필요
- 정부가 AI 보안 시장의 마중물 역할을 할 수 있는 투자 및 R&D 사업 등을 통해 AI 보안을 미래 성장 산업으로 육성할 필요성 존재
  - 자주적인 AI 모델 개발에 보안은 필수적이며 우리 자체적인 보안 기술을 소버린 AI에 탑재하는 등 AI 보안 기술 확보가 중요함

[제4회]

NO.	주제	발표자	일시 / 장소
4	**최신 AI보안 이슈와 대응방안**	이로운앤컴퍼니 윤두식 대표	11.5(수) / 달개비

〈주요 내용〉

1. 최신 AI보안 이슈와 대응방안

- 생성형 AI 발전과 확산으로 딥페이크, 보이스피싱 등 현실적 피해가 증가하고 기업 내부에서는 데이터 유출과 쉐도우 AI 문제 등 보안 위험이 심화되고 있음

- 도입 방식에는 직접 도입 방식, API 통합 방식, 온프레미스 방식, 클라우드 방식 등이 있으며 AI 거버넌스 강화와 보안 게이트웨이 구축 등 통제 기반의 안전한 활용 체계 마련 필요성이 대두됨

  – 최근 클라우드와 온프레미스를 적절히 섞어 쓰는 하이브리드 방식을 많이 사용하고 있으며 각 방식의 장단점을 잘 살펴 기업에 맞는 방식을 도입시켜야 함

- AI 보안 대응 방향이 기존 사후 대응에서 선제적 보안으로 패러다임 전환되고 있으며 AI 모델을 활용한 동적 방어 메커니즘 구축이 확대되고 있음

  – 또한, AI를 활용해서 AI를 공격을 방어하는 'AI 대 AI' 대응 기술을 연구 중이며 제로트러스트 아키텍처, AI공급망 보안 강화 등 기술적 접근이 병행되고 있음

- 프롬프트 인젝션 방어를 위해서는 다중 레이어 방어체계와 AI 기반 프롬프트 분석을 결합한 하이브리드 접근법이 효과적임

- AI보안 프레임워크는 ① AI 위험 평가 ② AI 자산 분류 ③ 접근 제어 및 인증 ④ 모니터링 및 감사 사이클로 구현

- 미국은 규제 완화 중심의 AI 확산 전략, 유럽은 위험 기반의 안정적 발전 모델, 중국은 오픈소스 중심 저변 확대 전략을 추진 중

  – 반면 국내는 보안 인력 부족(전체 6만 명 중 실무인력 2.4만 명), 중소기업의 투자 회의론 확산 등으로 인해 AI보안 역량 격차가 심화되고 있음

- AI 전문인력 수요는 증가하나 경력 중심 채용 확대와 인건비 부담으로 신규 인력 진입이 어려운 구조가 지속되고 있음

  – 이에 따라 내부 재교육 및 정부 차원의 AI 보안 인재 양성, 민관 협력 강화 및 R&D 투자 확대, AI 보안이 포함된 국가 전략 재정립 필요함

IV

2026년 글로벌 사이버보안 이슈 전망

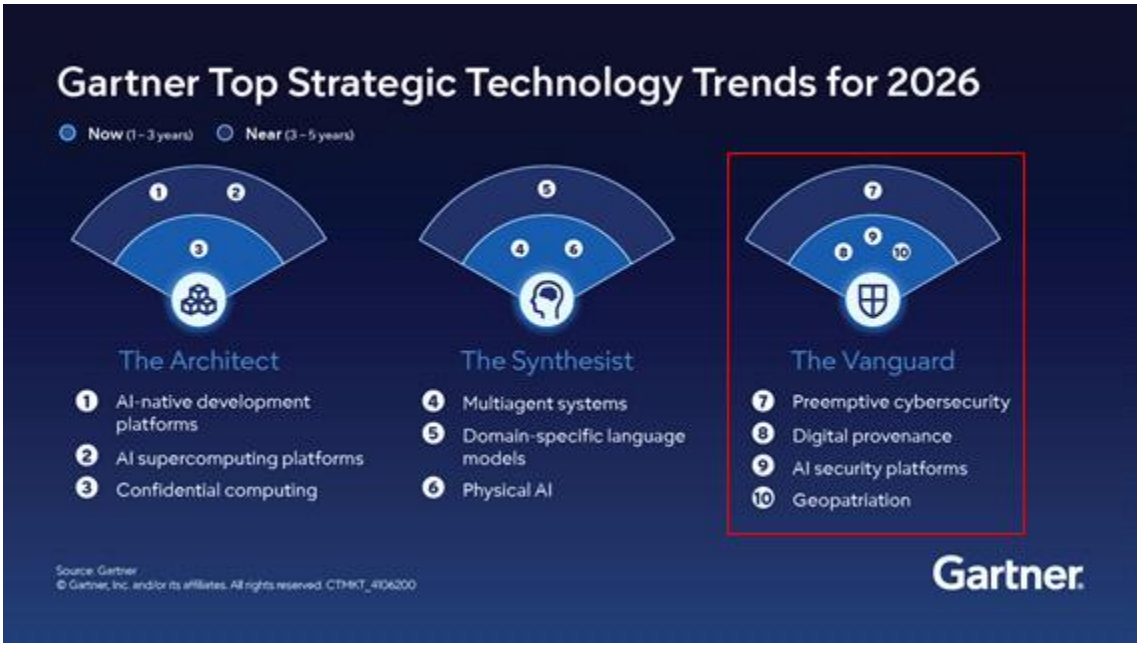
AI 기술 발전은 다양한 산업에 중대한 영향을 미치고 있으며 사이버보안은 그 대표적인 분야로 AI 기술의 발전 속도가 공격과 방어 양쪽 모두를 가속화시키고 있습니다. 물리적 세계와 디지털 세계의 경계는 사라지고 공격자들은 이러한 변화를 또 다른 기회로 이용하게 될 것입니다. AI 기술 발전으로 빠르게 변모해 가는 사이버 환경과 진화하는 위협은 다가올 2026년에도 지속 확대될 것으로 예상하고 있습니다. 글로벌 주요 기관에서 다음과 같이 2026년 사이버보안 이슈와 트렌드를 전망하고 있습니다.

〈표〉 글로벌 2026년 사이버보안 전망 요약

<table>
<tr><th>가트너
(2026년 10대 전략기술 트렌드)</th><th>팔로 알토 네트워스
(AI 경제에 대한 6가지 예측:
2026년의 새로운 사이버보안 규칙)</th><th>포브스
(사이버보안 2026:
6가지 전망과 청사진)</th><th colspan="2">구글위협인텔리전스그룹
(2026년 사이버보안 전망 보고서)</th></tr>
<tr><td rowspan="2">선제적 사이버보안</td><td>새로운 기만의 시대:
AI 신원의 위협</td><td>에이전트 AI, 새로운 공격 및
방어의 최전선</td><td rowspan="5">① 인공지능</td><td>공격자, AI 전면 도입</td></tr>
<tr><td rowspan="2">새로운 내부 위협:
AI 에이전트 보안</td><td rowspan="2">포스트 양자 암호화로의 전환</td><td>프롬프트 주입으로 AI 조작</td></tr>
<tr><td rowspan="2">디지털 출처</td><td>AI 기반 사회공학</td></tr>
<tr><td>새로운 기회:
데이터 신뢰 문제 해결</td><td>딥페이크, 합성 미디어, 신원
사기 증가</td><td>AI 에이전트 패러다임 전환</td></tr>
<tr><td rowspan="2">AI 보안 플랫폼</td><td>새로운 망치:
AI 위험과 임원 책임</td><td>IoT, 엣지, 기기 증가에 따라
공격 표면 확대</td><td rowspan="5">② 사이버범죄</td><td>강력한 보안 분석가</td></tr>
<tr><td rowspan="2">새로운 카운트다운:
양자적 필수성</td><td rowspan="2">사이버 범죄,
기업형 사업으로 성장</td><td>섀도우 에이전트 위험</td></tr>
<tr><td rowspan="2">지리적 이동</td><td>랜섬웨어 및 데이터
유출/강탈</td></tr>
<tr><td>새로운 연결:
새로운 작업 공간으로서의
브라우저</td><td>사이버보안,
전체 비즈니스의 전략적 기둥</td><td>온체인 사이버범죄 경제</td></tr>
<tr><td></td><td></td><td></td><td></td><td>위협받는
엔터프라이즈 가상화</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ICS 및 OT 공격</td></tr>
</table>

IV-1. 가트너 - 2026년 10대 전략 기술 트렌드

〈그림〉 가트너 2026년 10대 전략 기술 트렌드



출처) 가트너, https://www.gartner.com/en/articles/top-technology-trends-2026

가트너(Gartner)는 지난 10월 2026년 10대 전략 기술 트렌드를 발표하였습니다. 가트너는 2026년에 혁신은 가속화되고 AI는 더 이상 선택 사항이 아니며, 10대 기술 트렌드는 서로 긴밀하게 연관되고 디지털 신뢰를 추구해야 하는 AI 기반 초연결 사회의 현실을 반영하고 있음을 강조합니다.

특히, 3대 분류 체계(설계, 통합, 전위)에서 사이버보안 관련 축을 포함하고 있어 향후 사이버보안의 중요성이 더욱 부각되고 있음을 엿볼 수 있습니다.

사이버보안 관련 전략 기술		주요 내용
⑦	**Preemptive cybersecurity (선제적 사이버보안)**	• 네트워크, 데이터, 연결 시스템 겨냥 위협 급증으로 기업은 선제적 사이버보안에 주목 • 사후 대응 중심의 방어 전략에서 사전 예방 중심의 전략으로 전환 • 2030년까지 선제적 보안 솔루션이 전체 보안 지출의 절반을 차지
⑧	**Digital Provenance (디지털 출처)**	• 오픈소스 코드, AI 생성 콘텐츠 활용 증가에 따라 디지털 출처 검증 중요성 높아짐 • 2029년까지 디지털 출처 관리 역량이 부족한 기업들은 수십억 달러 규모의 제재 리스크에 노출될 것으로 예측

사이버보안 관련 전략 기술		주요 내용
⑨	AI security platforms (AI 보안 플랫폼)	• AI 보안 플랫폼은 프롬프트 주입 ,데이터 유출, 악성 에이전트 활동 등 AI 관련 보안 위협으로부터 조직을 방어 • 2028년까지 기업의 절반 이상이 AI투자 보호를 위해 AI 보안 플랫폼 도입 전망
⑩	Geopatriation (지리적 이동)	• 지정학적 리스크 대응을 위해 기업 데이터와 애플리케이션을 글로벌 퍼블릭 클라우드에서 소버린 클라우드, 지역 클라우드 공급업체 자체 데이터 센터로 이전하는 전략 • 2030년까지 유럽과 중동 기업의 75% 이상이 지정학적 위험을 줄이기 위해 가상 워크로드를 해외로 이전 예상

출처) 가트너, https://www.gartner.com/en/articles/top-technology-trends-2026

IV-2. 팔로알토 네트웍스 - AI 경제에 대한 6가지 예측: 2026년의 새로운 사이버보안 규칙

미국 사이버보안 기업 팔로알토 네트웍스(Palo Alto Networks)는 “AI 경제에 대한 6가지 예측: 2026년의 새로운 사이버보안 규칙”을 발표하였습니다. 2026년 세계 경제는 ‘AI 전환’에서 ‘AI 네이티브’로 전환하는 변곡점이 될 것이며 추론, 행동과 기억 능력을 갖춘 자율 AI 에이전트가 새로운 시대를 정의하리라 예측하였습니다.

새로운 경제는 새로운 전략을 요구하며 승리하려면 보안은 후방 방어에서 선제적이고 공격적인 전력으로 진화해야 한다고 강조합니다.

〈표〉 팔로알토 네트웍스, AI 경제에 대한 6가지 예측: 2026년 새로운 사이버보안 규칙

예측		주요 내용
1	새로운 기만의 시대: AI 신원의 위협	• 기업 신뢰의 기반 중 하나인 신원 개념 자체가 2026년 AI 경제의 주요 전장 • 공격 영역은 단순한 네트워크나 애플리케이션이 아니라 신원 그 자체 • AI가 실시간으로 기업을 지휘할 수 있는 리더의 완벽한 복제본을 만들어 냄 • 인간의 개입 없이 명령에 따라 행동하도록 프로그래밍된 자율 에이전트의 등장은 최종적이고 치명적인 취약점을 야기
2	새로운 내부 위협: AI 에이전트 보안	• 2026년에 기업들이 AI 에이전트를 대거 도입할 것으로 예상됨에 따라 사이버 격차는 근본적으로 바뀔 것 • 자율 에이전트는 지칠 줄 모르는 디지털 직원이지만, 동시에 강력한 “내부 위협”이 됨 • 기업이 에이전트를 배포하는 것만큼 보안에 주의를 기울이지 않는다면, 치명적인 취약점을 초래
3	새로운 기회: 데이터 신뢰 문제 해결	• 2026년에는 “데이터 포이즈닝”이라는 새로운 공격 영역 등장 • 공격자는 훈련 데이터를 출처부터 조작하여 숨겨진 백도어와 신뢰할 수 없는 “블랙박스” 모델을 생성 • 기업의 핵심 인텔리전스를 구축하는 데 사용되는 데이터에 공격이 내재되어 있다면 기존의 경계는 아무런 의미가 없음 • 기술적인 문제가 아니라 조직적인 문제 • 데이터 포이즈닝이 성공하는 방식은 문을 부수는 것이 아니라, “좋은 데이터”라는 위장을 하고 들어오는 것임

예측		주요 내용
4	**새로운 망치: AI 위험과 임원 책임**	• AI 기반 우위를 차지하기 위한 경쟁은 법적 현실에 부딪힐 것 • AI가 잘못될 경우 책임 문제는 법적 문제로 전환되고, AI 기업을 운영하는 데 있어 경영 책임에 대한 새로운 기준이 마련될 것 • AI 이니셔티브는 기술적 한계가 아닌 위험 관리가 제대로 이루어지고 있음을 입증하지 못해서 정체될 것임 • CIO는 기술적 수호자에서 전략적 조력자로 진화하거나, "최고 AI 리스크 책임자"(CAIRO)와 같은 새로운 부서와 협력해야 함
5	**새로운 카운트다운: 양자적 필수성**	• "지금 수확하고 나중에 복호화하라"는 위협은 AI로 인해 가속화 • 2026년까지 역사상 가장 크고 복잡한 암호화 마이그레이션을 촉발하고 중요 인프라와 공급망은 양자 암호(PQC)로의 전환이 시작됨 • PQC 마이그레이션에 대한 기한이 정해진 계획이 요구되고 공공 양자 컴퓨팅 전환점이 도래 • 기업들은 인증서 관리에서 성능 오버헤드로의 전환에 따른 엄청난 운영상의 복잡성에 직면
6	**새로운 연결: 새로운 작업 공간으로서의 브라우저**	• 브라우저는 정보 합성 도구에서 사용자를 대신하여 복잡한 작업을 실행하는 에이전트 플랫폼으로 진화하고 있음 • 기업들이 생산성 향상을 위해 브라우저를 도입하기 위해 경쟁하는 가운데, CIO와 CISO는 중대한 딜레마에 직면 • 브라우저의 새로운 에이전트 기능은 고유한 가시성 격차를 야기하여 고급 AI 상호작용으로부터 완벽하게 보호하기 위한 특수 보안 계층 필요 • 브라우저 기반 위협은 이미 폭발적으로 증가 • 에이전트적 상호작용을 관리해야 하는 필요성은 브라우저 자체의 진화를 요구하며, 새로운 제어 아키텍처로 자리매김 • 브라우저 내부의 상호작용 지점에서 일관된 제로 트러스트 보안을 구현하는 통합 클라우드 네이티브 보안 모델 필요

출처) https://www.paloaltonetworks.com/perspectives/2026-cyber-predictions#aipov-accordion

IV-3. 포브스 - 사이버보안 2026: 6가지 전망과 청사진

미국의 출판과 미디어 기업 포브스(forbes)는 "사이버보안 2026: 6가지 전망과 청사진"을 발표하였습니다. 포브스는 사이버보안 환경이 새로운 기술, 변화하는 위협 행위자, 그리고 변화하는 글로벌 역학 관계들이 결합되어 기업들은 그 어느 때보다 큰 압박을 받고 있는 단계에 접어들고 있다고 평가하였습니다.

〈표〉 포브스, 사이버보안 2026: 6가지 전망과 청사진

전망		주요 내용
1	**에이전트 AI, 새로운 공격 및 방어의 최전선**	• 2026년, AI는 단순한 도구가 아닌 그 자체로 전장이 될 것 • 공격자와 방어자 모두 최소한의 인간 통제만 받거나 아예 통제하지 않는 자율적인 AI 시스템을 점점 더 많이 활용 • 공격자는 AI 시스템을 탐색, 적응, 공격에 활용, 방어자는 위협을 모니터링, 탐지, 봉쇄에 활용

전망		주요 내용
2	**포스트 양자 암호화로의 전환**	• 양자 컴퓨팅은 오랫동안 위협으로 인식 및 2026년 전환점에 도달 • RSA 및 ECC와 같은 기존 암호화 방식에서 실질적인 위험이 나타나기 시작 • 규제 기관, 보험사, 그리고 적대국들은 기업들이 양자 복원력을 갖춘 표준을 채택하도록 압박
3	**딥페이크, 합성 미디어, 신원 사기 증가**	• 해커들이 믿을 수 없을 정도로 가짜 오디오, 비디오, 그리고 신원 구성을 무기로 사용하며, 일반적인 탐지 방법으로 발견 안 됨 • 생체 인식 및 신원 확인 시스템은 조작된 신원이나 복제된 생체 인식을 이용한 스푸핑에 취약 • 일회성 확인 대신 지속적인 신원 인증 사용 및 음성·비디오 인증 시스템에 이상 탐지 기능을 추가 필요
4	**IoT, 엣지, 기기 증가에 따라 공격 표면 확대**	• 엣지 컴퓨팅, 5G/6G 구축, 그리고 IoT 기기가 보편화됨에 따라, 주 데이터 센터가 아닌 가장 취약한 임베디드 기기에서 대규모 공격 발생 • 펌웨어를 쉽게 업그레이드할 수 없거나 취약한 기본 비밀번호를 사용하는 기기는 쉬운 표적이 될 것임 • 봇넷, DDoS 공격, 공급망 침투 활동은 분산된 기기들을 점점 더 많이 활용 • 프로비저닝, 패치 적용, 그리고 폐기를 포함하는 기기 수명 주기 관리는 2026년 최우선 보안 과제
5	**사이버 범죄, 기업형 사업으로 성장**	• 2026년 사이버 범죄 활동은 사업 단위에 더 가까울 것으로 예상 • 잘 조직되고 서비스 지향적이며 전 세계적으로 이루어질 것임 • 랜섬웨어와 갈취는 제휴 모델, 구독 서비스, 암호화된 자금 세탁과 같은 완전한 생태계로 성장 • 아웃소싱, 기업 식별, 마케팅, 심지어 "피해자 고객 지원"까지 일상화 • 회복력, 리더십, 문화가 중요한 전략적 차별화 요소가 될 것임
6	**사이버보안, 전체 비즈니스의 전략적 기둥**	• 사이버보안은 비즈니스 차원의 조율, 이사회의 참여 및 기업 문화 변화 필요 • 위협이 인간과 신원 벡터를 점점 더 노리고 직원들은 최전선 방어선이 됨 • 공공-민간 협력, 공급망 조정, 위협 정보 공유를 구조화

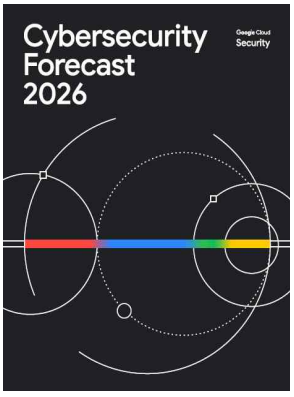
출처) https://www.forbes.com/sites/chuckbrooks/2025/11/10/cybersecurity-2026-6-forecasts-and-a-blueprint-for-the-year-ahead

IV-4. 구글위협인텔리전스그룹 - 2026년 사이버보안 전망 보고서

구글위협인텔리전스그룹(Google Threat Intelligence Group, GTIG)은 “2026년 사이버보안 전망 보고서”를 발표하였습니다. 2026년 사이버보안 전망 보고서는 1) 인공지능, 2) 사이버 범죄, 3) 국가 주도 공격 활동 세 가지 핵심 주제에 초점을 맞추고 있습니다.

GTIG는 2026년은 공격자와 방어자 모두에게 AI와 보안의 새로운 시대가 열릴 것이라 전망하며, 복잡하고 빠르게 변화하는 환경에서 기업은 선제적이고 다층적인 방어 전략 우선, AI 거버넌스 투자, 복원력 확보를 위한 보안 태세 지속 조정을 강조하고 있습니다.

〈표〉 구글위협인텔리전스그룹, 2026년 사이버보안 전망 보고서(①인공지능, ②사이버 범죄)



주요 내용
① 인공지능
①-1 공격자, AI 전면 도입
• 위협 행위자의 AI 활용 일반화 및 사이버 위협 환경 급변 • AI를 최대한 활용하여 작전의 속도, 범위, 효과를 향상 • 공격 자동화, 간소화, 확장위해 에이전트 시스템을 점점 더 많이 도입
①-2 프롬프트 주입으로 AI 조작
• AI 가장 중요한 위험 중 하나이며 2026년 크게 증가 • 기업 AI 시스템에 대한 표적 공격 증가
①-3 AI 기반 사회공학
• AI 기반 사회공학 사용을 가속화하여 심각한 위협으로 부상 • 보이스 피싱(비싱)은 AI 기반 음성 복제를 통합하여 매우 사실적으로 사칭 • 2026년 공격의 규모가 증가에 따른 여러 견제와 균형을 갖춘 프로세스 시급
①-4 AI 에이전트 패러다임 전환
• AI 에이전트의 빠른 도입으로 인해 새로운 과제 발생 • 보안 취약점을 평가하기 위해 포괄적인 방법론, 프레임워크 및 도구 개발 필요 • 새로운 보안 패러다임의 핵심은 AI 에이전트를 고유한 관리 ID를 가진 별개의 디지털 행위자로 취급
①-5 강력한 보안 분석가
• AI가 도입으로 인한 보안 분석가의 업무 영역이 근본적으로 재편 • 분석가는 AI 에이전트를 지휘하는 모델로 전환
①-6 섀도우 에이전트 위험
• 정교한 AI 에이전트의 확산으로 “섀도우 AI” 문제가 심각한 “섀도우 에이전트” 문제로 확대 • 직원들은 회사의 승인 여부와 관계없이 강력하고 자율적인 에이전트를 업무에 독립적으로 활용

② 사이버 범죄

②-1 랜섬웨어 및 데이터 유출/강탈

- 2026년 전 세계적으로 가장 큰 재정적 피해를 입히는 사이버 범죄 유형
- 사이버 범죄자들은 보이스 피싱 및 기타 표적형 사회 공학 기법 등 초기 접근 전략을 계속 활용
- 제로데이 취약점을 점점 더 많이 활용하고, 더욱 창의적인 방법 강구

②-2 온체인 사이버범죄 경제

- 암호화폐와 토큰 자산 등 글로벌 온체인 경제 전환에 따른, 위협 행위자들의 블록체인 특성 악용
- 탈중앙화 금융(DeFi) 플랫폼과 암호화폐 거래소 대상 대규모 공격, 디지털 자산 탈취와 결합된 공급망 공격 등 고부가가치 공격 지속 발생
- 미국, 동남아시아, 중동과 같이 규제 우호적이고 산업 입지 확대 지역에 대한 공격 지속

②-3 위협받는 엔터프라이즈 가상화

- 게스트 운영 체제 내 보안 제어가 발전함에 따라, 가상화 인프라에 대한 위협 집중도 증가
- 간과된 계층 보호를 위한 보안 전략 전환 및 인프라 수준에서 직접 대응할 수 있는 역량 개발 필요

②-4 ICS 및 OT 공격

- 산업 제어 시스템(ICS)과 운영 기술(OT)에 대한 사이버 범죄 지속
- 기업 소프트웨어에 특화된 랜섬웨어 공격이 OT 운영에 필수적인 데이터 공급망을 심각하게 교란

출처) https://cloud.google.com/security/resources/cybersecurity-forecast

www.kisa.or.kr

KISA INSIGHT

2025VOL. 03
2025. 12

KISA 한국인터넷진흥원