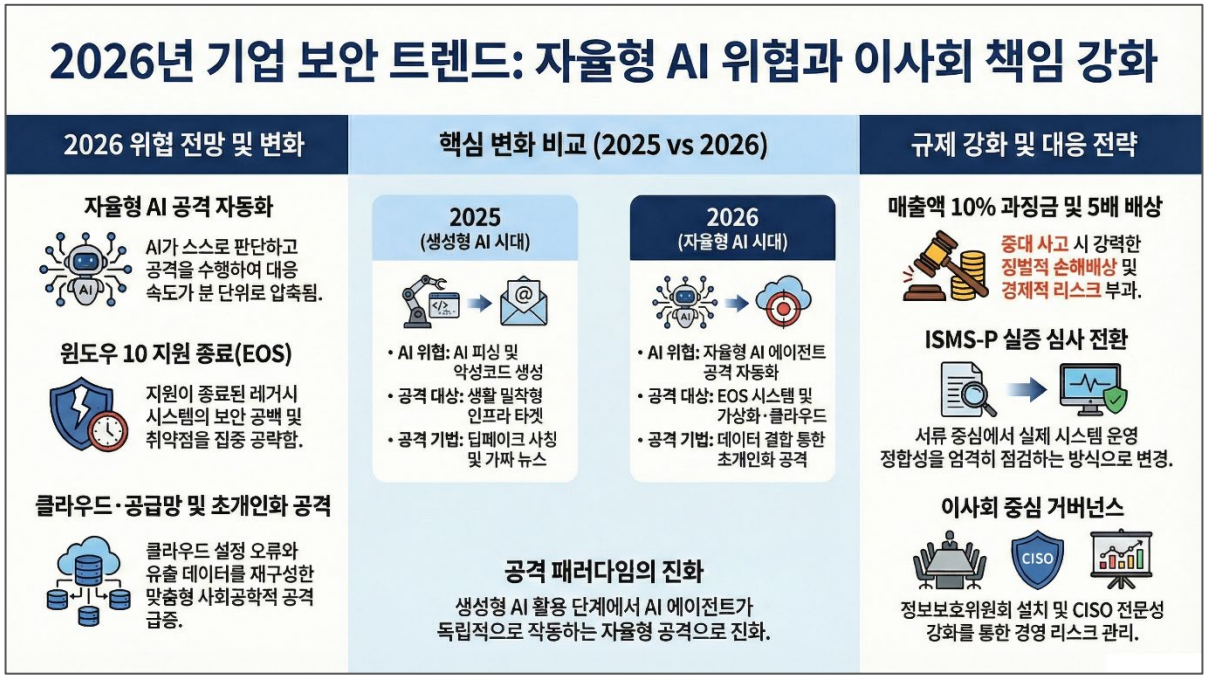
LEGAL UPDATE

정보보호센터

Feb. 2026

2026년 기업 보안의 핵심 키워드는 '자율형 AI 대응'과 '이사회 책임 강화'

과학기술정보통신부와 한국인터넷진흥원(KISA)은 최근 '2025년 사이버 위협 동향 및 2026년 전망'을 발표하며, 인공지능(AI) 기반 공격의 본격화를 예고했습니다. 2025년 침해사고 신고가 사상 최고치를 기록한 가운데, 2026년은 AI가 스스로 판단하고 실행하는 '자율형 에이전트' 위협이 기업 보안의 핵심 쟁점이 될 것으로 보입니다. 정부가 중대 사고 시 매출액의 최대 10%에 달하는 과징금 부과와 실증 중심의 심사 전환 등 전례 없는 강력한 규제를 예고한 만큼, 기업은 기술적 방어와 이사회 차원의 법적 대응 체계를 점검해야 합니다.



1. 2025년 사이버 위협
2. 2025년 주요 동향 및 2026년 위협 전망 분석
3. 규제 변화 전망 및 실무 영향
4. 시사점

1. 2025년 사이버 위협

2025년은 사이버 위협이 단순한 기술적 침해를 넘어 우리 사회의 핵심 기반 시설과 일상생활에 실질적인 타격을 입힌 기록적인 해였습니다. 공격의 표적이 단순한 데이터 탈취를 넘어 대형 통신사, 온라인 유통 플랫폼, 금융기관 등 국민 생활과 직결된 핵심 서비스, 인프라 등 전방위로 확산되었습니다. 이로 인해 발생한 대규모 서비스 장애와 개인정보 유출 사고는 사회 전반에 깊은 불안감을 조성하였고, 기업들에게는 높은 과징금과 정보보호 수준 강화를 위한 확실한 노력을 요구하고 있습니다. 이제 사이버 보안은 단순한 IT 부서의 업무가 아니라, 기업의 생존과 직결된 최우선 경영 리스크로 관리되어야 합니다.

2. 2025년 주요 동향 및 2026년 위협 전망 분석

가. 2025년 주요 동향

과학기술정보통신부가 발표한 **'2025년 사이버 위협 동향 및 2026년 전망'**에 따르면, 2025년 국내 침해사고 신고는 전년 대비 26.3% 증가한 2,383건으로 사상 최고치를 기록하여, 매년 증가 추세를 보이고 있습니다. 특히 2025년에는 통신·유통·금융 등 국민 생활 밀접 인프라가 연달아 피해를 입어 전례없는 수준의 개인정보가 유출되었고, 개발자들이 신뢰하는 오픈소스 플랫폼(NPM, PyPI)과 IoT 생태계가 공급망 공격의 주요 경로로 악용되었습니다. 나아가 랜섬웨어 공격이 교육·의료·혈액공급 같은 생명 관련 분야 및 산업 전반으로 확대되는 양상을 보였습니다.

나. 2026년 위협 전망 분석

2026년은 자율형 AI 에이전트 기반의 공격이 본격화될 것으로 보입니다. 공격자들이 대량 정보 수집을 통해 새로운 공격 기법을 개발·자동화하면서, 유출된 개인정보를 AI로 재구성하여 고도화된 맞춤형 피싱, 스미싱을 비롯해 사회공학적 공격을 수행할 것으로 예상됩니다. 또한 Windows 10 지원 종료로 인한 보안 공백과 방치된 레거시 시스템이 해킹 통로로 악용될 우려가 높으며, 클라우드 이용 가속화에 따라 AI를 활용한 자동화된 취약점 탐지와 여러 취약점의 연계 공격이 현실화될 것으로 전망됩니다. 나아가 AI 서비스 모델 자체를 공격 대상으로 삼는 위협도 본격화되어, 챗봇이나 보안 AI 등에 악의적 내용을 주입하거나 학습 데이터를 조작해 오작동을 유도하는 공격이 증가할 것으로 보입니다.

구분	2025년 (과거 전망 및 실제)	2026년 (새로운 전망)	변화의 핵심
AI 위협	생성형 AI를 활용한 정교한 피싱 메일, 악성코드 생성 지원	자율형 AI 에이전트의 공격 자동화 및 프롬프트 주입을 통한 AI 조작	공격 주체가 '사람'에서 '자율형 AI'로 전환되며 공격 속도 가속화
공격 대상	통신·금융 등 생활 밀착형 인프라 및 오픈소스 공급망	지원 종료(EOS) 시스템 및 기업용 가상화·클라우드 환경	윈도우 10 지원 종료 등에 따른 보안 공백 및 클라우드 설정 오류 집중 공략
사회공학	딥페이크를 이용한 단순 사칭 및 가짜 뉴스 유포	유출 정보를 결합한 초개인화 2차 공격 및 실시간 비싱(Vishing)	이미 유출된 대규모 데이터를 AI로 재구성하여 맞춤형 사기 발생전망

3. 규제 변화 전망 및 실무 영향

가. 규제 변화 전망

정부는 사이버 위협의 고도화에 대응하기 위해 기업의 책임을 대폭 강화하는 방향으로 제도를 정비하고 있습니다.

우선, 침해사고를 은폐하거나 고의로 신고를 지연할 경우 매출액의 최대 3%에 달하는 과징금을 부과하며, 정보유출 중대사고 발생일 경우 매출액 10%의 과징금과 사고로 인한 피해에 대해 최대 5배의 징벌적 손해배상 책임을 묻는 등 제재 수위를 높이고 있습니다.

특히 2026년부터는 정보보호 관리체계(ISMS-P) 심사가 기존의 서류 중심에서 실제 시스템을 점검하는 실증 심사로 전환되어, 보안 정책과 실제 운영 간의 정합성을 더욱 엄격하게 평가할 예정입니다. 또한 정보보호 공시 의무를 상장사 전체로 확대 추진 중으로, 기업의 보안 수준이 시장과 투자자에게 투명하게 공개되어 정보보호 투자 및 운영 수준이 기업에 대한 평가로 이어질 것으로 보입니다.

나. 기업 실무 영향

강화된 규제 환경에서 보안은 IT 부서의 기술적 문제를 넘어 이사회 차원의 핵심 리스크 관리 사안으로 격상되었습니다.

경영 측면에서는 정보보호위원회를 설치하고 CISO/CPO의 전문성을 강화하는 등 전사적 거버넌스를 체계화하여, 보안 투자를 지속 가능한 경영을 위한 필수 자산으로 인식하는 인식의 전환이 필요합니다.

실무적으로 기업은 사고 발생 시 즉각적으로 가동할 수 있는 법률·기술·컨설팅 통합 대응 매뉴얼을 수립해야 하며, 외부 전문 협력사(법무법인, 포렌식, 침해사고 분석기업 등)와의 사전 계약 체계를 구축하여 신속한 대응력을 확보해야 합니다. Windows 10 지원 종료(EOS) 등에 따른 보안 공백이 해킹 통로로 악용될 경우 법적 과실이 가중될 수 있으므로, 전사 IT 자산 관리와 패치 관리의 자동화가 필수적입니다.

4. 시사점

글로벌 보안 기업들(Google Cloud/Mandiant, Palo Alto Networks, Fortinet) 또한 2026년에는 자율형 AI 에이전트(Agentic AI)가 공격과 방어 양측을 주도하여 공격 대상이 확대되고, 그 방법은 더욱 고도화될 것으로 전망하고 있습니다. 인간 감독 없이 독립적으로 작동하는 AI 범죄 에이전트의 부상과 다크웹내 데이터 거래 시장이 현실의 전자상거래 수준으로 활성화될 것으로 전망하였고, 공격 속도는 수 시간에서 수 분 단위로 압축되어, 인공지능을 활용한 사이버 공격이 급증할 것으로 보이며, 기업 전반의 리스크 관리 측면에서 노력을 요구하고 있습니다.

2026년의 이러한 예상에서 알 수 있듯, 공격자가 AI를 활용하여 공격 과정 절차를 단축하는 만큼, 기업도 방어의 자동화를 통해 대응 속도를 맞춰야 하며, 강화되는 규제와 과징금 제도를 고려하여 보안 투자가 더 이상 비용이 아닌 지속 가능한 경영을 위한 필수 자산으로 인식해야 합니다. 기업은 이러한 변화 속에서 법률·기술·컨설팅을 통합한 침해사고 대응 매뉴얼 수립, 정보보호위원회 및 CISO 운영 체계 설계, ISMS-P 실증 심사 대비 정책-실제 운영 정합성 점검, 정보보호 공시 항목 작성 가이드 등 실질적인 보안 체계에 대해 누락되거나 부족한 부분이 없도록 정보보안 체계 검토가 필요합니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우
센터장/파트너변호사
T. (+82) 2 6003 7558
E. klee@yoonyang.com

정한근
고문
T. (+82) 2 6003 7781
E. hkjung@yoonyang.com

이광욱
파트너변호사
T. (+82) 2 6003 7535
E. kwlee@yoonyang.com

이수경
파트너변호사
T. (+82) 2 6182 8132
E. sgyi@yoonyang.com

박수정
파트너변호사
T. (+82) 2 6182 8388
E. parksj@yoonyang.com

지재원
연구위원
T. (+82) 2 6003 7568
E. jwji@yoonyang.com