AI시대의 패러다임 전환과 사이버보안강국의 길

2025. 7.

법무법인 태평양 이상직 변호사

1. AI 시대

2. 사이버보안의 위기

3. 패러다임의 전환

4. 사이버보안 강국의 길

1. AI 시대

과학기술이 미래로 가는 고속도로라면
AI는 고속도로를 수천, 수만, 수조 개를 만들고
국도와 다른 길은 모두 없애는 것과 같아서

AI를 알든 모르든 살기 위해선 AI 고속도로에 오르지 않을 수 없는 시대

AI를 이용할 수 있는 비즈니스

1. 정보 검색, 통역, 번역, 추론 결과 제공

2. 문서, 이미지, 동영상, 창작 지원

(업무를 위한 보고서 등 서류 작성, 영화, 그림, 소설, 작곡, 작사)

*AI Hallucination(환각) 현상의 역할과 한계

3. AI 에이전트(비서 등 무형의 일꾼)

(고객을 대신해 사실, 법률행위)

4. 피지컬 AI (물리적 형태를 갖춘 일꾼)

(휴머노이드는 왜 만드는가?)

5. 시스템 운용

(운송, 제조, 교통, 에너지, 경영 등)

<AI에서 벗어날 수 있는 서비스 영역은 없다>

AI 시대와 과학기술 발전 4방향

O 인간 "신체" 기관의 외연 확장

- 석기, 청동기, 철기 등 도구는 손의 확장. 마차와 철도, 자동차는 발의 확장.

  증기기관, 도시망, 통신망, 교통망 등 기계와 시스템은 혈액망, 신경망의 확장.

O 인간 "정신" 기관의 외연 확장

- **AI** (2024년 제프리 힌튼 등 노벨물리학상)

O 약화된 "신체"에 대한 지원 및 보강 (2024년 데미스 하사비스 등 **AI**연구가 노벨화학상)

- 인간은 악어, 표범 등 근육, 이빨을 발전시키는 동물과 다른 진화 경로를 선택
- 신체는 약화되어 의료, 건강(바이오), 운동 등 보조적 추가 활동을 통해 유지
- 휠체어, 의족, 인공심장 등 다양한 하드웨어, 장비, 소프트웨어의 지원
- 뉴럴링크 등 중증 장애인, 초고령 노인의 뇌와 컴퓨터를 연결하여 활동 지원

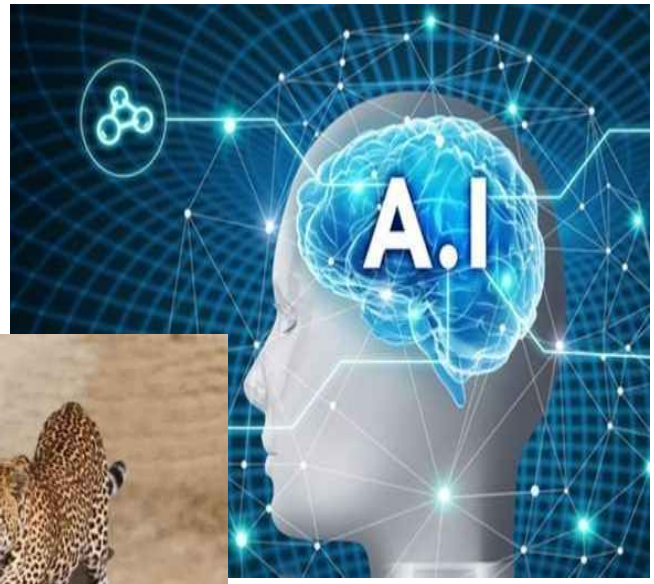
O 약화된 "정신" 지원 및 보강 (미래의 노벨상?)

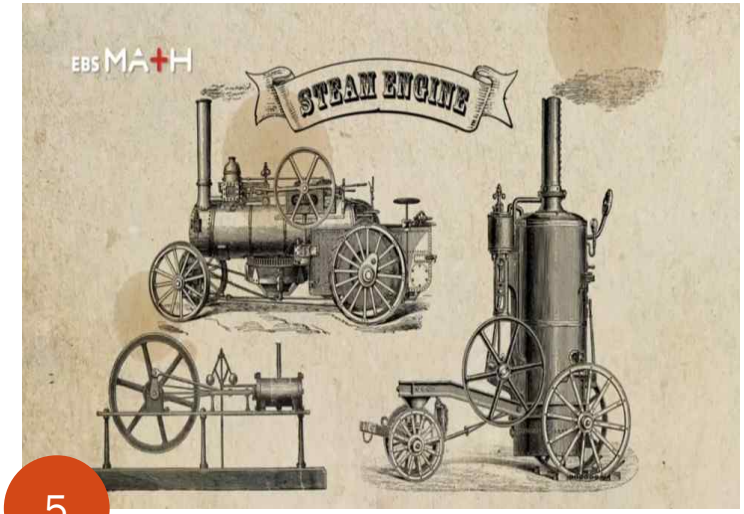
- 물질과 기계, 시스템, AI 의존도 증가는 소외, 불안, 우울, 공포, 정신질환을 야기
- 심리 안정과 정신 강화 기술 발전(뇌과학은 **AI**연구를 통해 뇌 질환치료 및 개선을 연구)

*AI의 특이점이 아니라 인간의 특이점을 고민해야 하는 시대.

<4가지 기술방향의 확장과 연결고리가 AI>

참고: 과학기술 발전 4방향의 생태계

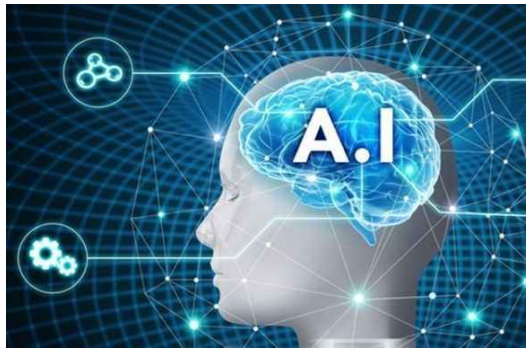




기술 존재형태의 발전에 따른 사이버 보안 위험 증가의 필연성

노동의존도가 높음. 완성도는 제작자가 결정. 외관상 용도가 명확. 위험 파악이 용이하고 대응도 쉬움. 완성된 형태로 시장에 나옴. 운용시스템 없음. (사이버보안 위험도 최하 단계)

자본의존도가 높음. 완성도는 외관상 알 수 없고 회사, 규제, 시장이 결정. 위험 파악이 어렵고 대응도 어려움. 완성된 형태로 시장에 나오지만, 운용시스템을 통해 서비스 지속 강화.



자본의존도가 매우 높음. 완성도는 외관상 알 수 없고 회사, 규제, 시장이 결정하나 시장에 나와 완성도를 높이는 과정이 존재. 소비자는 인터랙션을 통해 서비스 성장에 기여. 위험이 일상화되고 운용 및 위험 통제시스템이 매우 중요.

자본의존도가 가장 높음. 외관상 서비스 완성도를 알 수 없음. 규제 장벽도 높음.
최상위 안전이 요구됨. 소비자의 서비스 이용 과정이 중요. 위험 통제 및 운용시스템이 매우 중요. (사이버보안 위험도 최상 단계)

AI는 앞으로도 계속 성장할 것인가

O 성장하지 못하는 자본주의 시장경제는 갈등과 분쟁만 야기

- 미소 냉전 등 공산주의와의 싸움에서 승리
- 인터넷으로 연결해 세계를 시장화하고 글로벌 상생('기술과 노동 분업')
- 성장이 정체되면서 미중 갈등, 국지전(러시아-우크라이나, 이스라엘-이란) 발생

O 자본주의 시장경제는 발전할 수 있는가('진짜를 능가하는 가짜의 시대')

사회비평가 발터 벤야민은 "기술적 복제를 거듭하며 진짜의 아우라가 사라진다"고 했다. **가짜는 진짜를 능가할 수 있는 아우라를 창출할 수 없는가?**

- 온라인, 모바일, 메타버스
- 생쥐와 미키마우스
- 메타버스에서 아바타에게 구찌 가방과 버버리 원피스를!!!
- 블록체인의 발명: 암호화폐, 그리고 NFT(Non Fungible Token)
- **AI는 정보검색을 넘어 이미지, 동영상, 소설, 음악 등 콘텐츠 생성을 통한 창작 도구화 등 사업의 필수 동반자 역할**

<자본주의는 성장을 위해 AI를 활용할 수밖에 없고, 그에 따라 보안 위협도 지속적으로 증가>

AI가 뒷받침하는 창작의 세계

2. 사이버보안의 위기

사각지대 없는 사이버 공간의 확장은
사이버위협의 일상화, 다양화, 피해의 대규모와 회복 불가능성을 높임

최근 사이버 보안 위협의 특징

O 북한 등 암호화폐 탈취와 범죄집단의 사이버 공격 등 침해 공격의 일상화

O AI를 도입한 서비스, 보안시스템 증가와 범죄집단의 AI활용으로 피해 수준과 범위를 확대

O 침해방법과 경로의 다양화, 고도화 및 원인 불명 사례 증가

O 피해기업의 자체 보안력으론 방어에 한계

- 중소기업 뿐 아니라 대기업도 뚫리는 상황(AI등 과학기술의 급속한 발전으로 보안 수준이 높다고 안심할 수 없다).
- 당해 기업만 아니라 비즈니스 관련 기업, 고객에 연쇄 피해 등 파급효과가 크고, 다른 범죄 등의 수단화 현상 가속화.
- 범죄 전략 고도화로 침해 이후 발각 위험을 줄이고 상당한 기간이 경과한 후에 집중 공격을 통해 정보, 재산 유출 등 피해를 높이는 등 지능화 추세.

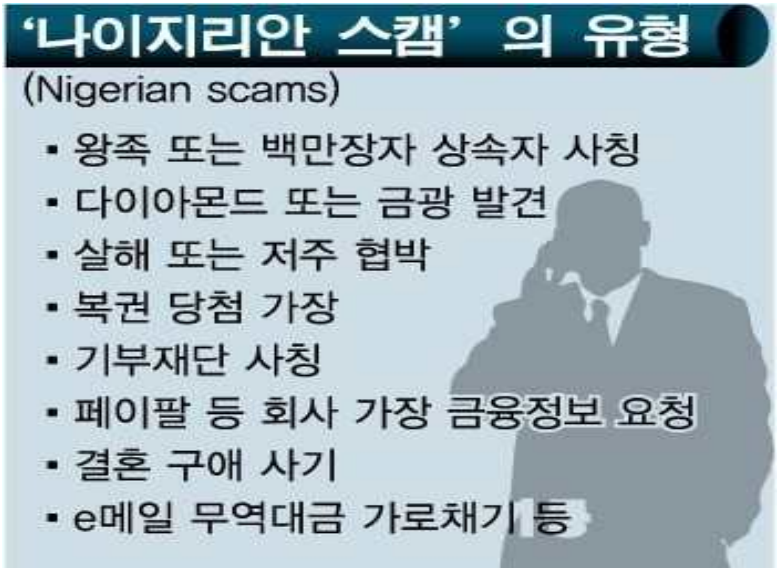
생성형 AI 등을 이용한 기업에 대한 사이버 위협

O AI를 이용해 악성코드 생성 및 투입, 피싱메일 제조 활용, 범죄지식 습득, 허위 또는 대량 데이터 투입, 이용자가 입력한 기밀 등 데이터 수집

O AI시스템을 이용하는 기업에 대해선 허위 데이터 투입 또는 생성, 서비스 중단 또는 결과조작, 시스템파괴, 재산탈취, 저작권침해, 산업기밀 탈취, 개인정보 등 데이터 해킹

*홍콩 글로벌 금융기관 직원의 약 340억 송금 사기 사건(AI 페이크 영상 활용)
*생성형AI를 통해 개인정보 과다 또는 동의 없는 수집 논란
*회의정보를 입력해 회의록 작성하고 프로그램 오류 해결 과정에서 소스코드 입력실수
*사이버안보 위협, 암호화폐 탈취(코로나판데믹 중 해외 취업 및 원격근무 기회 활용)

기업보안 공격을 통해 획득한 정보의 피싱 범죄 등 활용



기존 범죄의 특징:
경기침체기, 투망식, 노약자, 엉성함.

신형 범죄의 특징:
범죄를 위한 데이터 수집(해킹 등) 및 분석 중요.
AI 딥페이크, 정교함, 일상성, 피해자의 다양화.

대응:
AI기반 보이스피싱 등 음성, 이미지, 영상 및 패턴 분석 모델 도입(경찰)
은행의 AI패턴 예측, 창구 및 온라인 대응, 30분 등 시간 지연 출금(은행)
범죄 프로세스의 유형별 다양한 이해관계자가 참여하는 대응 생태계 구축

3. 패러다임의 전환

전통적인 보안만으로는 극복할 수 없는 예측불허의 사이버 공격과 침해 일상화 시대,

사이버 보안의 패러다임이 바뀐다.

AI 위험의 특성 ("핵발전소와 AI중 무엇이 더 위험할까")

1. 딥러닝을 하는 블랙박스 구간의 존재
2. 정상적 작동과정에서 사고 위험 증가
3. 행위와 위험의 인과관계 불확실성
4. 피해의 전염성, 연쇄성
5. 피해 회복의 어려움

*위험통제는 비용이 아니라 AI서비스의 핵심요소, 위험통제는 강력한 보안을 요구.

*보안은 외부에 대해서만 아니라 AI의 자율적 특성으로 인해 내부에 대해서도 요구.

*보안은 기존에 확인된 위협만이 아니라 새로운 형태의 위협도 대응가능해야 한다.

*스페이스 오디세이 2001

과학기술 발전은 살아 '움직이는 생물로서의 보안' 요구

디지털 사회는 AI등 기술을 이용해 리좀*식 혁신을 통해 발전
(*리좀: 땅속에서 장애를 뚫거나 우회하며 사방팔방으로 자라는 식물로서 철학자 질 들뢰즈가 사회현상을 설명하기위해 고안. 도시, 인터넷, 기업 등 성장과 유사한 모델)

하이데거의 실존주의 철학을 빌려오면
피투(彼投): 아무런 잘못없이 내가 어쩔 수 없는 상황 속에 내던짐을 당한 상태.
기투(企投): 피투의 상태에 굴복 않고 이성과 과학을 통해 미래를 개척해 나가는 것

사이버 공간은 인간이 시장경제 발전과 생존을 위해 의도적으로 만든 '적극적 기투'의 공간이므로 핵심인프라이므로 사이버보안은 선택이나 비용이 아니라 필수이면서 책임

끊임없이 변화하는 AI등 디지털 환경에서의 보안을 어떻게 강화할 것인가.

- Protection by Design의 한계(끊임없이 성장하는 보안 요구)
- 데이터 AI 혁신과 함께 하는 보안기술의 지속적 혁신 요구
- 다른 기관과 연결된 사례의 증가로 제3자 보안 협력 등 보안 생태계 중요

전통보안과 AI 보안

<전통 보안>

O 오랜 기간 검증되고 신뢰성과 안정성이 확인된 보안시스템으로서 방화벽, 소프트웨어, 암호화, 침입탐지시스템 등 사전적으로 정의되고 알려진 공격패턴을 확인하고 방어하는데 최적화

O 전통적인 보안 시스템을 우회하거나 새로운 형태의 공격방법, 변종 악성코드에 취약하고, 공격이 있을 경우 자동적이 아니라 전문가의 인적 판단을 거쳐 대응조치를 하므로 골든타임을 놓칠 위험

＊"생존자 편향의 오류" 위험

<AI 보안>

O 대용량 트래픽의 학습과 추론 알고리즘을 통해 대용량 로그, 네트워크 트래픽, 행동데이터와 패턴 등을 실시간 분석해 비정상 징후, 새로운 형태의 위협을 실시간 탐지해 선제적, 즉각적 대응 가능

O 충분한 데이터와 추론 알고리즘을 확보하지 못할 경우 오작동 위험이 있고, AI보안시스템을 타겟팅하는 공격(악성 데이터 투입, 알고리즘 혼란 초래, 결과값 수정 등)이 진화할 경우 여전히 침해 위험. 추론과정의 설명과 해석이 어려울 경우엔 설명가능성 부족으로 신뢰성 악화 위험.

참고: AI 보안 활용의 장점

- O 프로그램 또는 파일의 실행 전에 그 특징을 분석해 신종 악성 코드 포함여부를 예측하여 이상 징후가 있을 경우에 선제적으로 차단

- O 평소 상태의 트래픽의 통계적 특징을 학습하고 비정상적으로 많은 데이터의 전송이나 평소와 다른 현상을 찾아 실시간 경고

- O 임직원들의 시스템 활동 패턴을 학습해 평소와 다른 이상 행동패턴이 있을 경우에 경고(법위반, 권한 남용 예방)

- O 보안관제시스템을 효과적으로 적용하여 수많은 경보 데이터에서 의미없는 데이터를 제외하고 공격 또는 침해 위험이 높은 데이터 중심으로 대응해 효율성 제고 가능

- O 키워드 중심이 아니라 문맥, 발신형태와 패턴을 학습하여 스팸 또는 피싱메일을 효과적으로 점검해 의심 패턴을 포착해 침해 또는 피해 방지

*하인리히 법칙: 큰 재해 1건 발생 전에는 작은 재해 29건과 사소한 사고 300건이 발생한다. (*그렇다면 AI보안은 데이터 학습과 추론을 통해 보안 침해 경고 및 방어시스템 고도화 가능)

참고: AI 보안 활용의 단점과 대응

O 임직원들이 생성형 AI를 업무에 이용하는 과정에서 영업 기밀 유출, 고객 정보 침해 등 위험 요인 발생

O 공격자들이 생성형 AI를 이용해 공격대상의 취약점 탐지, 피싱 이메일의 정교한 작성, 데이터 오염, 결과물 오류 등 유인하여 보안 침해사고 야기

O AI 보안시스템에 대해서도 AI의 수준 차이를 악용하여 AI간 커뮤니케이션을 통해 보안시스템의 AI를 조정해 혼란에 빠트리는 등 침해사고를 야기하고 침해 정도를 극대화할 위험

<해결책>

전통 보안과 AI 보안의 효과적인 융복합, 방어시스템과 법제도의 유기적 연계를 통한 대응 생태계와 거버넌스 확립

4. 사이버보안 강국의 길

전통적인 보안과 AI 보안의 동태적 융복합화, 메가보안기업 육성,
전국민의 보안 생활화를 통해 사이버 보안 강국이 되는 것이

디지털, 온라인시대, 세계 경제 강국으로 거듭나는 유일한 방안이다.

사이버 보안에 관한 인식 대전환이 필요하다

*과학기술, 특히 AI가 주도하는 자본주의 경제질서에서는 세계적인 AI강국 중심으로 경제 쏠림 현상이 불가피하고
세계화, 온라인화 되어 기업거래 만이 아니라 개인 거래도 글로벌화하고 있는 상황이므로 미국 중심 경제에 휘둘리는 상황
(미국 대통령이 누구인지, 미국 연방준비제도 이사회의 금리인하가 어떻게 되는지, 미국 증권시장이 어떤지, 미국의 경제정책이 어떻게 되는지 등)

*AI 도입으로 땀 흘려 시간 써서 일하는 노동의 시대가 저물고 있다.

*기존의 과학기술과 달리 AI는 범용의 예측불허함을 가지므로 위험의 성격이 다르다.
(작을 수 있고 클 수 있다. 하나일수 있고 여러 개이거나 융복합적일 수 있다.)

<모두가 온라인에서 살아가고 사이버공격에서 자유로운 곳이 없는 시대에, 사이버보안은 비용이 아니라 AI서비스의 핵심>

사이버 보안시스템 강화 방향

o 사이버 위기 일상화에 대응하는 동적, 통합적 보안 역량 강화

- 데이터 처리와 학습, 추론 등 지속적인 성장과정을 고려하여 살아 움직이는 생물로서의 보안 기능 강화 (설명가능, 지속가능한 보안)

o 메가 보안기업을 만들어야 한다

- 기존 시스템은 기업의 자체 보안력을 중심으로 외부 보안기업의 지원을 받는 형태가 일반적이나,
- 피해 기업의 보안력에만 의존하면 경기침체, 사업 상황에 따라 보안이 비용절감 대상이 되고 보안 공백 야기
- 보안서비스를 메인 사업으로 하는 메가 보안기업 추진 필요(인수합병 등)

o '정보통신 보안 기본법' 제정하자

- 정보통신망법의 개인정보 분야는 개인정보보호법으로 이미 이관됐고
- 정보통신망 확충은 상당부분 목적을 달성했으니
- AI시대 보안 프레임 중심의 '정보통신 보안 기본법'으로 개편

o 사이버 보안 거버넌스를 구축하고 강화하자

- 개별 기관의 노력만으로 효과적인 사이버 침해 방어 한계
- 정부(과기정통부, 국가사이버안보센터)와 산업, 학계 등 연계시스템 구축

사이버 보안시스템 강화 수단

O 레거시 시스템의 인증, 접근 권한 통제, 암호화, 개인정보 보호, 모니터링 강화 (설명가능한 보안)

O 성장하는 AI 침해 기법 등 분석과 관련 기관 정보 공유 및 협업체계 강화

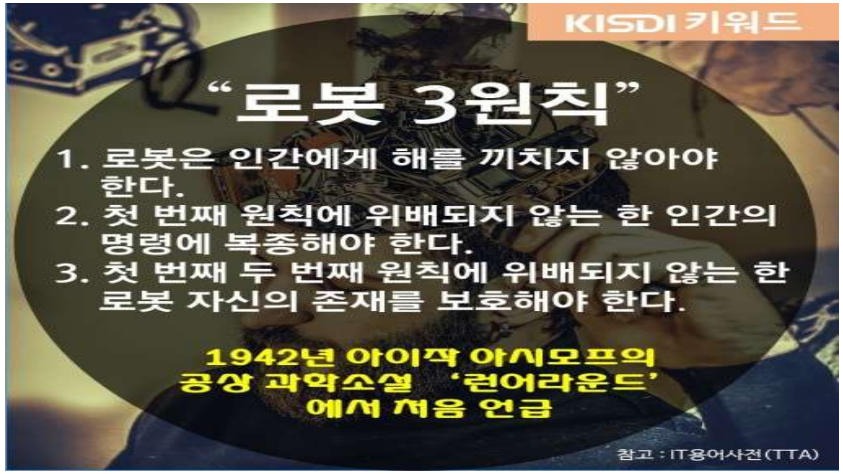
O AI시대 보안은 비용 요소가 아닌 사업의 핵심요소로 보고 인력 개발, 투자 집행 중요

O 보안기술은 사업(서비스)의 핵심기술과 연계하면 서비스 고도화를 겸해 보안 강화 용이

O 임직원의 성과 평가에 보안 실적 여부를 추가하는 것도 필요 (보안KPI개발)

O 사이버 위협 일상화에 맞게 전 국민 대상의 보안 교육 및 보안 생활화

AI 윤리기준은 사이버보안에서 어떤 의미가 있을까
(문제점: 추상적이어서 가이드 역할 한계, 법령상 의무와 중복되기도)



<해결책>

'사이버보안기업의 아이덴티티' 정립이 정답

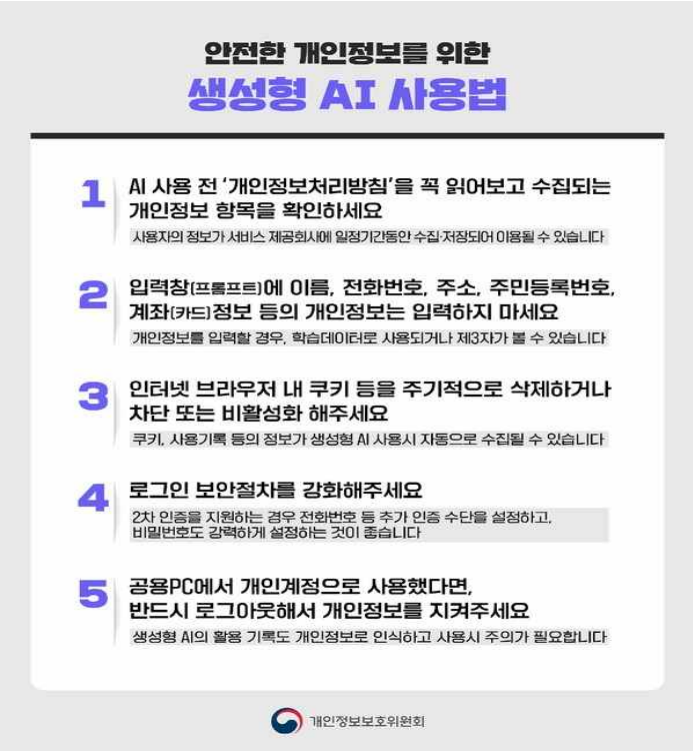
(무엇을 위해, 왜 존재하는가)

<참고>

스마트폰업체A: "To lift humanity and enrich people's lives in all the ways people want experience it"

SNS업체B: "To give people the power to build community and bring the world closer together"

기업을 넘어 '전 국민의 사이버 보안 생활화'



AI 시대엔 고객이 기업과 함께 서비스 제공 프로세스를 구성하는 주요 요소가 됨.
(사생활, 개인정보, 사업, 취향, 계획 등 데이터 입력과 콘텐츠 이용 및 생성 관여)
서비스 보안 공격, 침해 위험은 고객의 서비스 이용 과정과 결과를 수단으로 악용 가능.

모든 사안에 통일된 보안은 없다.
각 기업의 특성과 구조, 비즈니스에 맞는 문제 해결 중심의 보안 중요.
그에 따라 고객, 임직원의 보안수칙도 달라져야 한다.
(AI시대 사이버 보안은 움직이는 과녁을 맞힐 수 있는 활과 화살이 되야)

AI시대도 사람이 우선이다.
AI특이점이 오기 전에 '인간의 특이점'을 찾아야 한다.
(과학기술 시대의 위기와 기회를 조율하는 오케스트라의 지휘자 역할)

보안은 AI 뉴노멀, 패러다임 전환의 시대를 뒷받침하는 핵심 인프라다.

경청해 주셔서 감사합니다.