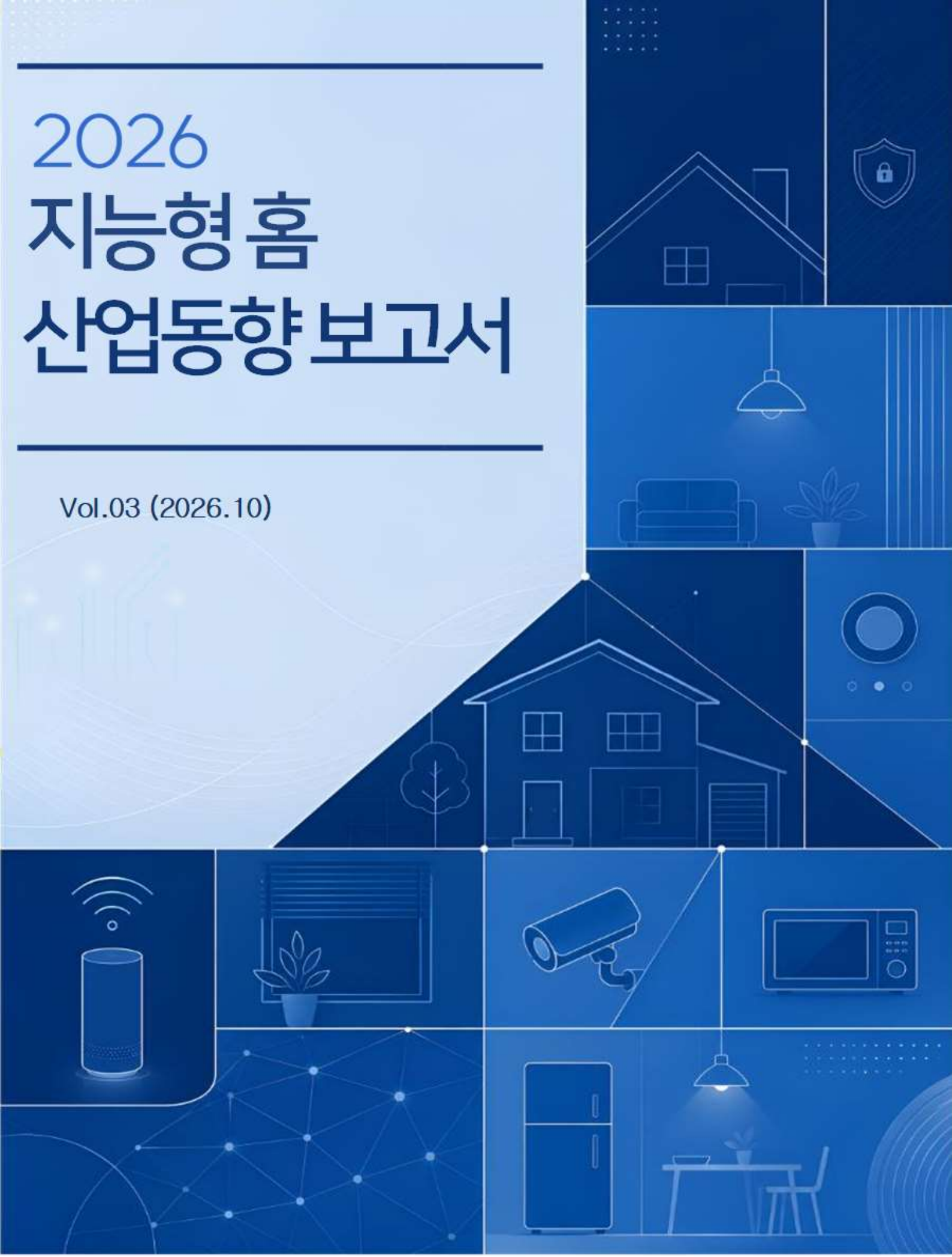
2026 지능형 홈 산업동향 보고서

Vol.03 (2026.10)



nipa 정보통신산업진흥원 National IT Industry Promotion Agency

KASH 한국AI스마트홈산업협회 Korea Association of AI Smart Home

지능형 홈(AI@Home) 얼라이언스

CONTENTS

지능형 홈 산업동향 보고서(2026. Vol. 03)

1. 지능형 홈 표준・특허 동향 ---- 01

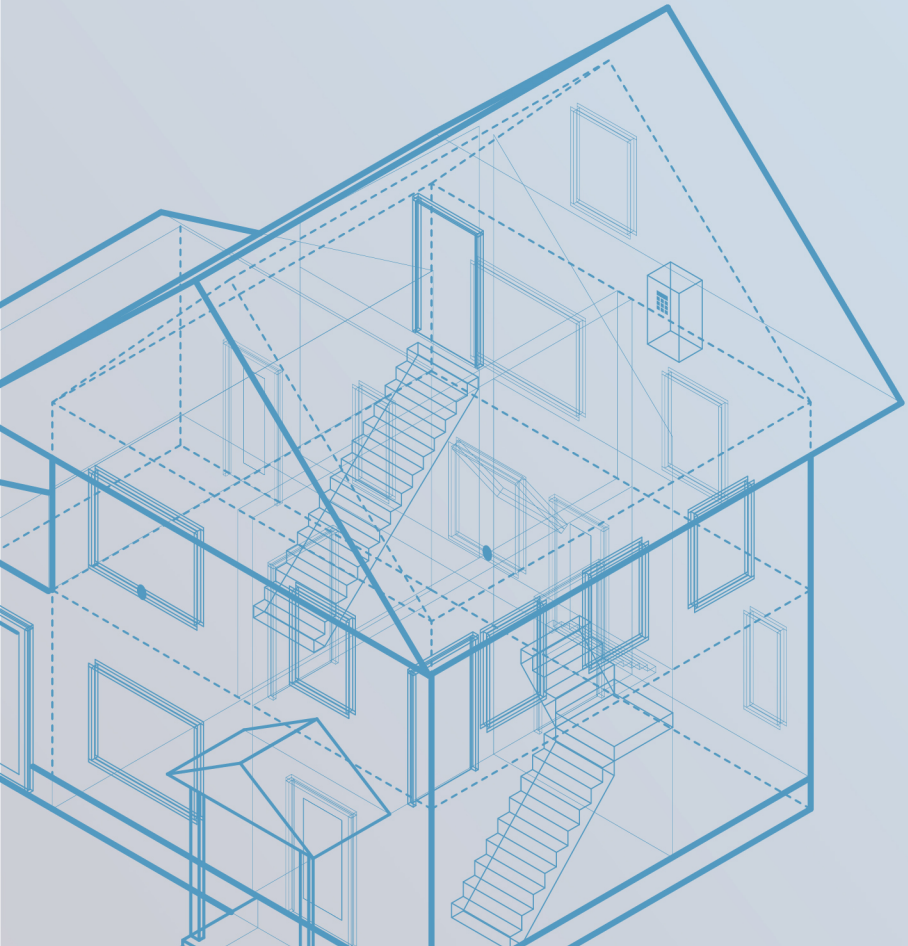
2. 지능형 홈 건설 동향 ---- 34

3. 지능형 홈 가전・디바이스 동향 ---- 48

4. 지능형 홈 인공지능 동향 ---- 62

5. 지능형 홈 보안 동향 ---- 78

6. 지능형 홈 에너지 동향 ---- 90



Ⅰ. 지능형 홈 표준 · 특허 동향

1 ETSI, Cyber Security (CYBER); CRA; Cybersecurity requirements for smart home general purpose virtual assistants(2026. 07. 20)

- ETSI가 2026년 7월 공개한 Draft ETSI EN 304 631 V1.0.0은 「EU 사이버복원력법(Cyber Resilience Act, CRA)」에 대응해 스마트홈용 범용 가상비서(Smart Home General Purpose Virtual Assistants, SHGPVA)가 갖춰야 할 사이버보안 요구사항과 적합성 평가기준을 구체화한 유럽표준 초안. 스마트 스피커뿐 아니라 자연어 명령을 받아 다른 서비스에 접근하거나 주거환경의 연결기기를 제어하는 범용 가상비서가 대상
- 현재 문서는 최종 확정 표준이 아니라 Draft/Enquiry 단계. ETSI는 EN 304 631을 포함한 CRA 지원 표준안을 2026년 여름 공개해 승인 절차를 진행하고 있으며, EN 304 631은 9월 17일 기준 EC 평가 단계. 향후, 유럽연합 관보(OJEU)에 조화표준으로 인용될 경우, 해당 규범적 요구사항을 충족한 제품은 적용 범위 내에서 CRA의 관련 필수 사이버보안 요건을 충족한 것으로 추정받을 수 있음

01 스마트홈 AI 비서를 CRA 규제체계 내에서 구체적인 보안 대상으로 규정

- EN 304 631은 인터넷에 직접 또는 다른 장치를 통해 연결되고, 음성·문자 등의 자연어 명령을 처리해 서비스에 접근하거나 스마트홈 기기를 제어하는 제품을 대상으로 함. 대표적으로 AI 기반 스마트 스피커와 독립형 가상비서 등이 포함될 수 있음. 표준은 이들 제품에 대해 CRA Annex I Part I의 필수 사이버보안 요구사항을 구현·검증하는 구체적 기준을 제시
- 즉, 기존의 일반적인 IoT 보안 원칙을 넘어 AI 비서가 음성·영상·개인일정·연락처 등의 개인정보를 상시 처리하고 다른 스마트홈 기기를 제어할 수 있다는 특성을 고려한 제품별 세부 보안기준이라고 볼 수 있음

02 Security by Default를 제품 기본 설계 원칙으로 요구

- 표준은 사용자가 별도의 보안 설정을 하지 않더라도 제품이 기본적으로 안전한 상태로 작동하도록 하는 Secure by Default를 핵심 원칙으로 채택
- 위험을 발생시킬 수 있는 기능의 기본 인증 설정, 자동 보안업데이트의 기본 활성화, 보안 관련 이벤트 처리, 안전한 초기화(factory reset), 암호기술 및 암호키·비밀번호 관리 등이 주요 요구사항으로 포함. 또한, 장기 암호키의 적절한 길이와 사용자가 설정하는 비밀번호의 복잡성에 관한 요구사항도 제시
- 이는 보안을 사용자의 선택적 설정에 맡기기보다 제조사가 제품 설계 단계부터 기본 보안수준을 확보해야 한다는 CRA의 'security by design/default' 방향을 제품 수준으로 구체화한 것으로 분석

03 취약점과 보안 업데이트를 제품 생애주기 관리 대상으로 규정

- 표준은 제품에 알려진 악용 가능 취약점(known exploitable vulnerabilities)이 없어야 하며, 최초 사용 전후 필요한 초기 보안 업데이트를 적용할 수 있도록 요구
- 또한, 안전한 소프트웨어 업데이트 메커니즘, 핵심 구성요소의 보안 업데이트 제공, 자동 업데이트, 업데이트 연기 또는 비활성화 옵션, 사용자 통지 등을 세부적으로 규정
- 따라서, 스마트홈 AI 제품의 보안책임이 출시 시점에서 끝나는 것이 아니라 출시 이후 취약점 발견 → 패치 → 배포 → 사용자 통지로 이어지는 지속적인 제품 생애주기 관리로 전환되고 있다는 점이 핵심

04 인증·접근통제와 최소권한 원칙 강화

- 가상비서는 단순 정보 제공을 넘어 도어록, 조명, 냉난방, 보안설비 등 다양한 스마트홈 장치를 제어할 수 있기 때문에 잘못된 명령이나 계정 탈취가 물리적 피해로 연결될 가능성이 있음
- 이에 따라, EN 304 631은 피해를 유발할 수 있는 기능에 대해 인증과 접근통제를 적용하고, 권한은 필요한 범위로 제한하는 최소권한(least privilege) 원칙을 적용함. 사용자가 부여한 권한을 철회할 수 있어야 한다는 요구도 포함

05 음성·영상 수집 여부를 이용자가 명확하게 알 수 있도록 요구

- 가상비서 특성상 특히 주목할 부분은 마이크와 카메라에 대한 투명성 요구. 표준은 하드웨어형 가상비서와 소프트웨어형 가상비서 모두에서 오디오 또는 비디오 캡처가 활성화된 경우, 이용자가 이를 인지할 수 있도록 표시해야 하며, 사용자가 캡처 기능을 비활성화할 수 있는 메커니즘도 요구
- 이는 AI 비서가 항상 주변환경을 듣거나 촬영할 수 있다는 우려에 대응해 '수집 중인지 알 수 있는 권리'와 '수집을 중지할 수 있는 통제권'을 기술적 보안요건으로 구현한 것으로 해석됨

06 데이터 최소화와 로컬 처리 원칙을 보안 요구사항에 포함

- 표준은 처리하는 데이터를 필요한 범위로 최소화하고, 음성·영상 데이터 처리에 관한 정보를 이용자에게 제공하도록 요구. 특히, 일부 이벤트 탐지는 로컬에서 수행하는 방식도 요구사항으로 제시
- 이는 민감한 음성·영상 데이터를 클라우드로 전송하기 전에 기기에서 처리하는 온디바이스·엣지 처리 방식이 단순 성능 최적화뿐 아니라 보안·개인정보 보호 수단으로 활용될 가능성이 커지고 있음을 의미

07 네트워크 장애 상황에서도 핵심 기능의 복원력 확보

- EN 304 631은 기밀성이나 무결성뿐만 아니라 가용성(availability)을 별도의 핵심 축으로 다루고 있음. 전원 손실 후 기능 복구, 네트워크 연결이 끊어진 상황에서의 로컬 동작, 네트워크 복구 후 정상상태 복귀, 서비스 제한 또는 중단에 대한 사용자 알림, DoS 대응을 위한 입력 속도 제한, 업데이트 일정 관리 등의 요구사항이 포함
- 특히, 스마트홈 시스템이 도어록·경보·안전설비 등과 연결될 경우 '클라우드가 끊겨도 기본 기능은 작동해야 한다'는 복원력 요구가 중요해지고 있음을 의미

08 공격표면 최소화 및 Secure Boot 요구

- 표준은 외부 입력값 검증과 sanitisation, 불필요한 물리·논리 인터페이스 비활성화, 기본 설치 앱 최소화, Secure Boot 등을 요구

- 이에 따라, AI 기능 자체뿐 아니라 운영체제·API·통신 프로토콜·앱·펌웨어 등을 포함하는 전체 제품 스택의 공격표면 관리가 CRA 대응의 핵심으로 자리잡음

09 위협 수준에 따라 모니터링·로그 관리 차등 적용

- 제품과 기능의 보안 위험을 Low·Medium·High 등으로 구분하고, 위험도가 높아질수록 더 높은 수준의 이벤트 기록과 로그 보존·시간동기화 등이 요구
- 표준은 보안 이벤트 로깅, 타임스탬프, 로그 저장, 로깅 설정뿐 아니라 개인정보와 관련된 로그에 이용자가 접근할 수 있는 기능도 요구
- 즉, 모든 기능에 동일한 통제를 적용하는 방식이 아니라 자산·기능의 영향도에 따라 보안수준을 차등화하는 risk-based approach를 채택

10 개인정보 성격에 따라 보호등급을 세분화

- 부속서에서는 가상비서가 처리할 수 있는 주요 데이터의 보안 영향도를 분류. 예를 들어, 건강정보는 기밀성과 무결성 모두 High, 개인 일정·연락처·개인 메모·비공개 음성·영상 등은 대체로 Medium 수준의 기밀성·무결성·가용성 영향도를 부여. 위치정보 역시 중간 수준 이상의 보호가 필요한 데이터로 다룸
- 이는, 향후 스마트홈 AI 제품의 보안 설계에서 모든 데이터를 동일하게 보호하는 것이 아니라 데이터 민감도 및 침해 시 피해 수준을 기준으로 보호조치를 차등화해야 함을 의미

11 시사점

- AI 가상비서 규제가 'AI 모델' 자체보다 이를 탑재한 제품 전체의 사이버보안과 생애주기 관리로 확대. EN 304 631은 AI 알고리즘의 정확도나 성능보다 인증·권한관리, 업데이트, 암호화, Secure Boot, 로그, 네트워크 복원력 등 제품 전체의 보안구조를 다룸. 따라서, 향후 AI 스마트홈 시장에서는 AI 모델 경쟁력뿐 아니라 제품 개발부터 유지보수까지 이어지는 Secure-by-Design 체계 구축 여부가 유럽시장 진입의 핵심 조건으로 작용할 가능성이 높음

- 음성·영상 AI 서비스에서는 개인정보 보호와 사이버보안의 경계가 더욱 밀접하게 결합될 전망. 카메라·마이크 작동 표시, 캡처 중지 기능, 데이터 최소화, 로컬 처리, 사용자 로그 접근 등이 보안표준 안에 포함되면서 개인정보 보호가 단순한 약관·동의 절차가 아니라 제품 설계 단계의 기술 요구사항으로 전환. 스마트 스피커, AI 글래스, 홈 로봇, 차량용 AI 에이전트 등 상시 센싱형 제품에서도 유사한 설계방식이 확산될 것으로 예상
- EU 수출 기업은 CRA 대응을 위해 제품별 보안자산 분류와 증적관리 체계를 조기에 구축할 필요가 있음. EN 304 631은 데이터·기능별 영향등급을 설정하고, 각 요구사항마다 별도의 적합성 평가기준을 제시하고 있어 단순한 체크리스트식 대응만으로는 충분하지 않음. 국내 스마트홈·AIoT 기업은 제품의 데이터 흐름, 권한구조, 업데이트 방식, 로그, 암호기술, 외부 인터페이스 등을 사전에 문서화하고 '요구사항 → 구현조치 → 시험·검증자료'로 연결되는 CRA 적합성 증적체계를 마련할 필요가 있음

2 ETSI, Cyber Security (CYBER); CRA; Cybersecurity requirements for smart home products with security functionalities; including smart door locks, security cameras, baby monitoring systems and alarm systems(2026. 07. 20)

- ETSI의 Draft EN 304 632 V1.0.0(2026-07)은 EU 「Cyber Resilience Act(CRA)」를 지원하기 위해 마련된 보안 기능을 갖춘 스마트홈 제품(Smart Home Products with Security Functionalities, SHPSF)의 사이버보안 요구사항과 적합성 평가기준을 규정한 유럽 조화표준 초안임. 적용 대상에는 스마트 도어록, 홈 보안 카메라, 베이비 모니터링 시스템, 침입·경보 시스템 등 주거환경의 물리적 보안을 보호하면서 원격 제어·관리가 가능한 디지털 제품이 포함
- 앞서 살펴본 EN 304 631이 스마트홈 범용 가상비서를 대상으로 했다면, EN 304 632는 도어록·카메라·화재·가스·침입감지·사회적 돌봄 경보 등 실제 물리적 안전·보안과 연결되는 스마트홈 제품에 초점을 맞춘다는 점이 핵심적인 차이

01 스마트홈 보안제품을 CRA의 구체적 사이버보안 대상으로 설정

- EN 304 632는 EU 집행규정 2025/2392의 중요 디지털제품 분류 중 Category 17에 해당하는 제품을 대상을 대상으로 함. 구체적으로 소비자의 주거환경에서 물리적 보안을 보호하고 다른 시스템을 통해 원격으로 제어 또는 관리되는 제품과 이를 중앙에서 관리하는 하드웨어·소프트웨어가 포함. 스마트 도어록, 베이비 모니터, 경보시스템, 홈 보안카메라 등이 대표적
- 표준은 CRA Annex I Part I의 필수 사이버보안 요구사항을 제품 수준에서 구체화하고 있으며, 향후 EU 관보에 조화표준으로 인용될 경우 해당 표준의 규범적 요구사항 충족은 적용 범위 내에서 CRA 준수 추정의 근거로 활용될 수 있음

02 물리적 안전과 사이버보안을 하나의 위험체계로 결합

- 표준의 가장 중요한 특징은 사이버공격이 단순한 정보유출에서 끝나는 것이 아니라 실제 주거환경의 물리적 피해로 이어질 수 있다는 점을 위험평가에 반영
- 표준은 기능이 잘못 사용됐을 때 발생할 수 있는 피해 수준을 별도로 평가하며, 이를 위해 도어록 제어, 화재·가스 경보, 침입·강도 경보, 외부 센싱, 긴급지원 기능 등을 독립적인 기능 자산(function asset)으로 정의. 예를 들어 도어록 계정이 탈취되면 주택에 무단 접근할 수 있고, 화재·가스 알람이 비활성화되거나 조작될 경우 직접적인 인명·재산 피해로 연결될 수 있기 때문에 일반 IoT 제품보다 높은 수준의 보호가 요구됨

03 제품별 위험을 '데이터·기능 자산'으로 세분화

- EN 304 632는 단순히 모든 제품에 동일한 보안조치를 적용하지 않고, 제품이 사용하는 데이터 자산과 기능 자산의 영향도(Impact Class)에 따라 요구되는 보호수준을 달리하는 위험기반 접근방식을 채택
- 위치정보·인증정보·연락처, 사적 음성·영상정보, 화재·가스 감지정보, 침입·강도 감지정보, 사람의 긴급상황 감지정보, 도어록 잠금상태 및 창·문 개폐정보, 기기 훼손(tamper) 감지정보, 건강정보, 로그, 소프트웨어 패키지 등의 정보가 주요 데이터에 포함
- 특히, 건강정보는 기밀성·무결성 모두 높은 영향등급으로 분류되며, 인증정책·화재감지·가스감지 등 안전 관련 정보는 무결성이 훼손될 경우 높은 위험이 발생할 수 있는 자산으로 다뤄짐

04 Secure by Default와 초기 보안업데이트 의무 강화

- 제품은 시장 출시 전에 원칙적으로 알려진 악용 가능 취약점(known exploitable vulnerabilities)이 없어야 하며, 예외적으로 존재하는 취약점은 공식 취약점 관리 프로세스의 적용을 받아야 함. 또한, 제품의 최초 사용 전 또는 최초 사용 과정에서 보안업데이트를 확인·알림·설치하도록 요구
- 한편, 위험을 초래할 수 있는 기능에는 초기 상태부터 적절한 인증 메커니즘을 적용하도록 하고, 가능한 경우 자동 보안업데이트를 기본 설정으로 활성화하도록 규정
- 즉, 사용자가 별도의 설정을 하지 않더라도 제품이 기본적으로 안전하게 구성돼 있어야 한다는 Secure-by-Default 원칙이 제품 설계단계에서부터 적용

05 도어록·경보 등 위험 기능에 인증·접근통제와 최소권한 원칙 적용

- 표준은 피해를 발생시킬 수 있는 기능에 대해 인증(authentication)과 접근통제(access control)를 적용하고, 이용자·서비스·앱에 부여하는 권한을 필요한 범위로 제한하는 최소권한(least privilege) 원칙을 요구함. 부여된 권한은 철회 가능해야 함
- 특히, 원격으로 출입문을 열거나 주요 보안설정을 변경하는 기능은 단순 사용자 편의기능이 아니라 물리적 안전과 직접 연결되는 고위험 기능으로 취급. 표준은 PIN·생체정보·OTP 등을 활용하는 단일 또는 다중 인증방식의 개념까지 세부적으로 정의

06 화재·가스·침입 경보는 '서비스 가용성' 자체가 보안 요건

- 도어록이나 경보시스템은 서버·인터넷·전원 장애 시 기능이 중단되면 안전문제로 이어질 수 있기 때문에 가용성(availability)이 가장 중요
- 전원 복구 후 신속한 기능·통신 복원, 네트워크가 없어도 가능한 기능은 로컬에서 계속 작동, 네트워크 복구 후 정상적인 재접속, 핵심 기능이 중단될 경우 이용자에게 알림, 배터리 부족 시 사전 경고, 중요한 기능에 네트워크·전력 자원 우선 배분, DoS 공격 등에 대응한 비정상 요청 제한, 중요기능에 영향을 줄 수 있는 업데이트는 적절한 시점에 수행 등의 요구사항을 제시
- 즉, 스마트홈 보안제품의 사이버보안은 해킹 방지 뿐만 아니라, 필요 시 반드시 작동하는 것까지 포함

07 클라우드·모바일 앱·게이트웨이를 포함한 전체 서비스 구조 규제

- 표준의 적용범위는 개별 하드웨어 기기만이 아니며, 스마트홈 제품은 제품 본체뿐 아니라 스마트폰 앱, 클라우드 원격처리시스템(RDPS), 게이트웨이, 다른 디지털 제품과의 연계 구조로 구성될 수 있으며, 전체 아키텍처에서 보안기능이 어떻게 분담되는지를 고려
- 따라서, 기업은 안전한 하드웨어만으로는 CRA 대응을 완료할 수 없으며, 앱–클라우드–게이트웨이–제품 간 통신과 권한 구조 전체를 하나의 보안경계로 관리해야 함

08 데이터 최소화 원칙을 스마트홈 영상·음성 수집에도 적용

- 제품이 처리하는 데이터는 목적에 적합하고 관련성이 있으며 필요한 범위로 제한되어야 함. 표준은 특히 오디오·영상 데이터를 언제 수집·저장·전송하는지 제품 문서에서 명확히 하고, 실제 처리도 그 범위에 제한하도록 요구
- 이는 보안카메라·베이비 모니터와 같이 주거공간의 민감한 음성·영상정보를 지속적으로 처리하는 제품에서 개인정보보호 원칙과 사이버보안 요구가 직접 결합되고 있음을 의미

09 공격 표면 최소화와 Secure Boot 등 제품 자체 보호 강화

- 외부에서 입력되는 데이터는 검증·정제해야 하며, 사용하지 않는 물리·논리 인터페이스와 앱은 기본적으로 비활성화하거나 제거하도록 요구. 또한, Secure Boot를 포함해 소프트웨어의 무결성을 보호하고, 중요 데이터·기능에 대한 특권 접근을 제한하도록 규정
- 이는 USB·JTAG·Wi-Fi·Bluetooth·웹 인터페이스·앱 API 등 다양한 경로를 통한 공격 가능성을 줄이기 위한 Attack Surface Minimisation을 제품 설계 원칙으로 설정

10 경보·인터컴 등 사용 사례별 위험등급을 별도로 적용

- 표준은 일반적인 스마트홈 보안제품 외에 BIS(Building Intercom System, 건물 인터컴·출입통제), FGS(Fire/Gas Detection System, 화재·가스 탐지), I&HAS(Intrusion and Hold-Up Alarm System, 침입·강도 경보), SAS(Social Alarm System, 고령자·취약계층 긴급지원 경보) 등 4개 사용사례를 별도로 구분
- 각 사용사례에서 데이터와 기능의 중요도를 다시 세분화하기 때문에 동일한 데이터라도 제품 용도에 따라 보안요구 수준이 달라질 수 있음. 예를 들어, 건물 인터컴의 위치·개인 연락처·음성·영상 데이터는 기밀성·무결성·손실가용성 측면에서 각각 별도 영향등급이 부여됨

11 시사점

- 스마트홈 보안 규제의 중심이 '정보보호'에서 '사이버-물리 안전(Cyber-Physical Security)'으로 확대. 스마트 도어록, 화재경보, 침입탐지 제품의 해킹은 개인정보 유출에 그치지 않고 출입통제 무력화, 경보 실패 등 실제 물리적 피해로 이어질 수 있음. 이에 따라, 향후 스마트홈·AIoT 제품은 기밀성·무결성뿐 아니라 안전·가용성까지 포함하는 통합 위험관리 체계를 갖추는 것이 중요해질 전망
- 클라우드 의존형 스마트홈 서비스에는 '로컬 복원력' 확보가 핵심 경쟁요소가 될 것으로 예상. EN 304 632는 인터넷 연결이 없어도 가능한 핵심기능은 로컬에서 지속적으로 작동하도록 요구. 따라서, 도어록·경보·안전센서 분야에서는 클라우드 연결이 끊겨도 최소 안전기능을 유지하는 온디바이스·엣지 구조, 배터리 백업, 장애 복구 설계가 단순 기술특성을 넘어 규제 대응요소가 될 것으로 예상됨
- 국내 스마트홈 기업은 개별 기기가 아니라 '제품 생태계 전체'를 기준으로 CRA 적합성을 준비할 필요가 있음. 표준은 하드웨어뿐 아니라 모바일 앱, 클라우드, 게이트웨이와 외부 서비스까지 제품 아키텍처에 포함. 따라서, 유럽시장 진출기업은 기기-앱-클라우드-API-게이트웨이 간 데이터 흐름과 인증·권한체계를 통합적으로 문서화하고, 각 요구사항에 대한 시험·검증 증적을 확보하는 방식으로 개발·인증체계를 전환할 필요가 있음
- 보안카메라·베이비모니터 등 상시센싱 제품에서는 개인정보보호와 CRA 대응을 별도로 추진하기 어려워질 전망. 음성·영상·위치·건강정보의 민감도를 별도로 평가하고 데이터 최소화를 요구하면서, GDPR식 개인정보보호 원칙과 CRA의 제품 사이버보안 요구가 실질적으로 결합되고 있음. 국내 기업도 향후 Privacy by Design+Security by Design을 통합한 제품개발 체계를 구축하는 것이 필요
- CRA 대응은 제품 출시 시점의 일회성 인증보다 지속적인 생애주기 관리 역량을 요구. 최초 사용 시 보안업데이트, 알려진 취약점 관리, 자동 업데이트, 로그, 복구 기능 등을 요구하는 만큼 제조사는 제품 출시 이후에도 취약점 탐지·패치·배포·공지·지원종료를 체계적으로 관리해야 함. PSIRT, SBOM, 취약점 관리, OTA 업데이트 등 제품보안 운영역량이 EU 시장 접근의 중요한 기반이 될 것으로 예상됨

3 ETSI, Cyber Security (CYBER); Cyber Security for Consumer Internet of Things; Requirements for Smart Voice-Controlled Devices(2026. 08. 18)

- ETSI의 ETSI TS 103 927 V2.1.1, 「Cyber Security for Consumer Internet of Things; Requirements for Smart Voice-Controlled Devices」는 스마트 스피커 등 음성 기반 가상비서가 탑재된 소비자용 IoT 기기(Smart Voice-Controlled Device, SVD)에 특화된 사이버보안·개인정보보호 요구사항을 규정한 기술규격
- 최신판은 소비자 IoT 보안 기준인 ETSI EN 303 645를 기본 틀로 삼으면서, 음성수집·AI 학습·스마트홈 기기 제어라는 SVD 특유의 위험을 추가로 다룸. 2026년 8월 18일 V2.1.1이 정식 발간

01 범용 IoT 보안에서 '음성 AI 기기 특화 보안'으로 확장

- ETSI는 SVD를 사용자의 음성 명령·질문에 반응하는 가상비서 로직을 탑재한 소비자 IoT 기기로 정의. 스마트 스피커 등이 대표적인 사례이며, 음악 재생이나 정보검색뿐 아니라 전화, 일정·연락처 이용, 스마트홈 기기 제어까지 수행이 가능. 산업용 음성제어기기와 자동차에 통합된 음성비서는 적용 대상에서 제외
- 일반 IoT와 달리 SVD는 ▲마이크를 통한 지속적인 환경 접근, ▲음성 및 개인데이터 처리, ▲클라우드 AI 서비스와의 연결, ▲ 다른 스마트홈 기기에 대한 제어권 등을 갖기 때문에 공격면이 더 넓음. 실제로 표준은 음성 명령이 위치·연락처 등의 개인정보와 연결되고, 스마트홈 기기 제어가 현실세계의 물리적 안전에도 영향을 미칠 수 있다고 명시

02 EN 303 645를 기본 보안 프레임으로 적용

- TS 103 927은 별도의 독립적인 보안체계를 새로 만드는 것이 아니라 ETSI EN 303 645의 소비자 IoT 보안 요구사항을 기본으로 채택함. 기본 요구사항을 SVD 특성에 따라 강화하거나 구체화하고, 필요한 경우 새로운 요구사항을 추가하는 방식

- 범용 기본 비밀번호 사용 금지, 취약점 신고·관리 체계 구축, 안전한 소프트웨어 업데이트, 중요 보안 매개변수의 안전한 저장, 안전한 통신, 공격표면 최소화, 소프트웨어 무결성 보호, 개인정보 보호, 장애·중단에 대한 복원력, 시스템 텔레메트리·로그 분석, 사용자 데이터 삭제 지원, 안전하고 쉬운 설치·유지관리, 입력 데이터 검증 등이 주요 영역이며, 기본적인 IoT 보안 + 음성 AI 특화 보안이라는 2단 구조를 가짐

03 초기 페어링부터 인증 보안 강화

- 스마트 스피커 등은 스마트폰 앱이나 다른 스마트홈 기기와 최초 페어링하는 과정이 중요한 공격지점이 될 수 있음. 표준은 QR코드나 페어링 코드 역시 사실상 인증 자격증명으로 간주하고, 가능하면 기기별 고유값이나 동적으로 생성된 값을 사용하도록 권고. 또한, 네트워크 인터페이스를 대상으로 한 무차별 대입(brute-force) 공격이 현실적으로 성공하기 어렵도록 인증 보호 메커니즘을 구현하도록 요구
- 따라서, SVD의 보안범위가 단순 계정 비밀번호에서 벗어나 초기설정·페어링·기기간 신뢰관계 형성 과정 전체로 확대됨

04 보안 업데이트를 자동화하고 OTA 전달경로까지 보호

- 최신판은 SVD가 안전하게 업데이트될 수 있도록 보안 업데이트 메커니즘을 의무적으로 제공하고, 적어도 하나의 안전한 업데이트 방식은 자동화할 수 있도록 규정. OTA(Over-The-Air) 방식으로 업데이트하는 경우 인증된 통신 상대와 안전한 통신채널을 사용할 것도 요구
- 또한, 기능 업데이트와 보안 업데이트를 가능하면 분리해 배포하도록 권고. 이는 사용자가 새로운 기능 도입을 원하지 않더라도 최신 보안패치는 계속 적용할 수 있도록 하기 위한 것으로 분석됨
- 특히, 제품 출시 시점에 운영체제와 사전설치 소프트웨어가 6개월 이상 공개된 CVE/NVD 취약점을 미완화 상태로 포함하지 않도록 요구하는 규정도 포함

05 공격표면을 적극적으로 축소

- SVD는 Wi-Fi·Bluetooth·앱·클라우드 API·스마트홈 프로토콜 등 다수의 인터페이스를 이용하기 때문에 공격면 관리가 핵심. 표준은 초기화된 제품에서 비정상적인 네트워크 패킷을 필터링하고, 고정 네트워크 포트에는 접근통제를 적용하도록 함. 또한, 기기에 연결되는 다른 장치의 수를 실제 필요한 수준으로 제한하고, 사용하지 않는 통신 세션을 적시에 종료하도록 권고
- 제조사 공식 앱스토어가 아닌 곳에서 앱을 설치하는 경우에는 보안 위험과 영향을 사용자에게 알리고 명시적 확인을 받도록 요구

06 음성 데이터를 일반 개인정보보다 민감한 보안자산으로 취급

- 이 규격의 가장 중요한 특징 중 하나는 음성정보를 SVD 특유의 핵심 개인정보로 다룬다는 점임. SVD가 음성을 AI 모델 개선에 활용하는 경우 사용자의 원본 음성뿐 아니라 모델 학습 과정에서 생성되는 중간 데이터까지 사용자 데이터로 간주. 따라서, AI 모델 개발·개선 과정 역시 개인정보 보호 범위에 포함됨
- 이는 단순히 녹음 파일만 삭제하면 개인정보 보호가 완료되는 것이 아니라, AI 학습 데이터와 파생 데이터까지 관리대상으로 봐야 한다는 방향을 명확히 제시

07 개인데이터 접근은 사용자 선택이 전제

- SVD가 연결된 스마트폰 등의 일정·연락처와 같은 개인정보에 접근할 수 있는 경우 이용자가 접근 허용 여부를 선택할 수 있도록 해야 함. 또한, 위치정보 등 특정 개인정보 제공을 거부하더라도 제품 전체가 사용 불가능해지는 구조보다는, 해당 데이터가 꼭 필요한 기능만 제한하고 나머지 기능은 계속 사용할 수 있도록 설계해야 함. 표준은 사용자가 데이터를 제공하지 않았을 때 어떤 기능이 제한되는지도 설명하도록 요구
- 이는 개인정보 제공을 제품 사용의 포괄적 전제조건으로 삼는 방식에서 벗어나 기능별 데이터 접근권한을 세분화하는 방향으로 분석됨

08 클라우드 전송 최소화와 로컬 처리 강화

- SVD는 가능한 한 사용자의 음성과 데이터를 외부로 업로드하지 않거나 최소화하는 방식으로 서비스를 제공하도록 권고. 제조사가 통제하는 외부 서비스와 데이터를 주고받는 경우에는 적절한 암호화로 기밀성을 보호해야 함
- 따라서, 음성인식·AI 추론 기능에서도 모든 데이터를 클라우드에 보내는 구조보다는 온디바이스 AI 또는 엣지 처리를 통해 전송량을 줄이는 설계가 개인정보보호 측면에서 더욱 중요해짐

09 AI 모델 개선 목적의 음성 수집에도 명시적 동의를 요구

- 사용자 음성이나 개인정보를 수집하는 경우에는 사용자의 명시적 동의를 확보하도록 규정. 특히, AI 모델 개선이나 통계목적으로 사용자 데이터를 사용하는 경우에는 개인을 식별하거나 개별 사용자의 정보가 추론되는 위험을 낮추기 위해 차등프라이버시(differential privacy) 적용을 권고
- 이는 스마트 음성기기의 개인정보 보호가 단순 암호화에 그치지 않고 AI 학습 데이터의 재식별·추론 위험까지 고려하는 단계로 확대됐음을 의미

10 시사점

- 소비자 IoT 보안의 범위가 '기기 자체'에서 'AI 서비스 전체 생태계'로 확대. 스마트 음성기기의 공격면은 하드웨어뿐 아니라 모바일 앱, 클라우드 서비스, AI 모델, 계정, 연결된 스마트홈 기기까지 이어짐. 따라서, 제조사는 향후 Device–App–Cloud–AI Model을 하나의 보안체계로 관리하는 End-to-End Security를 구축할 필요가 있음
- 음성 AI 서비스에서는 개인정보 최소수집과 온디바이스 AI의 중요성이 더욱 커질 전망. TS 103 927은 가능한 한 음성·사용자 데이터의 업로드를 최소화하도록 권고. 이는 온디바이스 음성인식·LLM·엣지 AI가 단순히 응답속도 개선이나 비용 절감 기술이 아니라 Privacy by Design을 구현하는 핵심 기술로 자리잡을 가능성을 나타냄

- AI 학습데이터 관리가 제품 사이버보안의 핵심 영역으로 편입. 사용자의 음성 원본뿐 아니라 모델 학습 과정에서 생성되는 중간 데이터까지 사용자 데이터로 간주하는 것은 매우 중요. 향후 생성형 AI 기반 음성비서에서는 수집 데이터 → 전처리 데이터 → 학습 데이터 → 모델 업데이트까지 데이터 생애주기 전반에 대한 개인정보 보호체계가 요구될 가능성이 높은 것으로 분석됨
- '동의 여부'보다 '사용자 통제권'이 더 중요한 설계 원칙으로 부상. 연락처·일정 등 데이터 접근 여부를 사용자가 선택할 수 있고, 특정 데이터 제공을 거부하더라도 해당 정보가 필요하지 않은 기능은 계속 이용할 수 있도록 한 것은 서비스 가입 단계의 일괄동의 방식에서 기능별·목적별 권한관리 방식으로의 전환을 의미
- AI·IoT 제품의 보안 업데이트와 취약점 관리가 제품 경쟁력의 필수요소. 자동 업데이트, 안전한 OTA, 출시 시 장기간 공개된 미완화 취약점 방지 등은 제조사가 제품 출시 이후에도 지속적으로 보안책임을 부담해야 한다는 의미. 국내 스마트 스피커·AI 홈기기 기업도 PSIRT, CVE 모니터링, OTA 업데이트, 지원기간 관리 등 제품 생애주기 보안체계를 갖춰야 할 것으로 분석됨

4 중국, GB/T 47777-2026「智能家用电器质量安全风险分类评价指南」(지능형 가전제품 품질·안전 위험 분류·평가 가이드라인 발표)(2026. 07. 02)

- 중국 국가시장감독관리총국(SAMR)·국가표준화관리위원회는 2026년 7월 2일 GB/T 47777-2026「智能家用电器质量安全风险分类评价指南」(스마트 가전제품 품질·안전 위험 분류·평가 가이드라인)을 발표
- 이 표준은 권고성 국가표준(GB/T)이며, 2027년 2월 1일부터 시행될 예정. 스마트 가전의 위험을 기존의 전기·기계적 안전뿐 아니라 기능안전, 사이버보안, 데이터·개인정보보호까지 통합해 평가한다는 점이 핵심

01 스마트 가전의 안전 개념을 '물리적 안전+디지털 안전'으로 확대

- GB/T 47777-2026은 스마트 가전이 기존 가전제품의 하드웨어 위험과 네트워크 연결·지능화에 따른 새로운 디지털 위험을 동시에 갖는다는 점이 전제. 이에 따라 품질·안전 위험을 전기안전, 기능안전, 정보안전, 데이터·개인정보보호의 4개 영역으로 구분해 평가
- 전기안전에는 누전·화재 등의 전통적 위험이, 기능 안전에는 기계적 끼임이나 온도제어 실패 등 오작동 위험이 포함. 여기에 네트워크 침입·시스템 취약점과 같은 정보보안 위험, 사용자 개인정보 유출·제3자의 무단 데이터 접근과 같은 데이터·프라이버시 위험을 추가함으로써 스마트 가전의 안전범위를 사이버-물리 영역 전체로 확장

02 단순 규격 시험이 아니라, 다양한 정보를 결합한 종합 위험평가 체계 도입

- 이번 표준은 제품의 기술적 시험결과만으로 안전성을 평가하지 않고, 제품 자체의 안전 특성, 규제·컴플라이언스 데이터, 소비자의 실제 사용 경험을 함께 반영하는 종합 평가방식을 도입
- 구체적으로 제품 하드웨어, 제어시스템, 네트워크 전송 등에 대한 시험·평가뿐 아니라 전자상거래 이용자 평가, 제품 안전 관련 여론·이슈 등의 외부 정보도 평가자료로 활용. 이는 실험실 시험만으로 발견하기 어려운 실제 사용환경의 위험을 위험평가에 반영하려는 접근

03 전기·제어시스템·네트워크·데이터를 하나의 평가 프레임으로 통합

- 스마트 가전은 기존 제품과 달리 센서, 소프트웨어, 네트워크, 클라우드 서비스 등이 결합돼 있어 하나의 취약점이 다른 영역의 사고로 확대될 수 있음
- 이에 따라 GB/T 47777-2026은 전통적인 전기·기계적 안전을 별도의 영역으로 분리하는 데 그치지 않고, 제어시스템과 네트워크 통신, 정보보안, 데이터 처리 위험을 함께 평가하는 통합 위험관리 구조를 제시
- 예를 들어, 네트워크 침해로 냉난방 제어시스템이 조작될 경우 이는 단순 정보보안 사고가 아니라 기능안전 문제로 전이될 수 있으며, 카메라·마이크 등이 탑재된 스마트 가전에서는 정보보안 취약점이 개인정보 유출로 연결될 수 있음

04 데이터·개인정보보호를 '제품 품질·안전'의 한 축으로 명시

- 데이터 및 개인정보보호(数据与隐私保护)를 별도의 안전위험 영역으로 명시했다는 점에서 주목. 표준은 스마트 가전의 연결성과 데이터 활용 특성에 따라 사용자 개인정보 유출, 제3자의 부적절한 데이터 접근·이용 등을 제품 품질·안전 측면에서 평가해야 할 위험으로 인식
- 이는 개인정보보호를 단순한 서비스 약관이나 법률준수 문제로만 보지 않고, 스마트 가전제품 자체의 품질·안전관리 영역으로 편입했다는 데 의미

05 위험을 A·B·C·D 4개 등급으로 분류

- 표준은 제품 위험평가 결과를 일정한 절차에 따라 A, B, C, D의 4개 위험등급으로 구분. 이를 위해 제품별 특성을 고려할 수 있는 다양한 평가방법과 공통 평가 프로세스를 제시
- 따라서, 기업은 위험 여부를 단순 '적합/부적합'으로 판단하는 것이 아니라 위험수준을 단계적으로 식별해, 상대적으로 위험이 높은 영역에 대해 우선 개선이 가능
- 이는 제품 설계 단계에서 위험을 사전에 발견하고 설계 개선, 소프트웨어·펌웨어 업그레이드, 보안조치 강화 등으로 연결하는 사전 예방적 위험관리를 지원하기 위한 구조

06 평가를 일회성 인증이 아닌 폐쇄형 위험관리 프로세스로 구성

- SAMR은 이 표준이 완전하고 실행 가능한 폐쇄형(closed-loop) 평가 프로세스를 구축했다고 설명. 위험을 식별하고 평가하는 데서 끝나지 않고, 평가결과를 제품설계 개선과 펌웨어 업데이트 등 후속조치로 연결하는 구조
- 따라서, 스마트 가전 제조사 입장에서는 제품 출시 전 시험만으로 안전관리가 끝나는 것이 아니라, 실제 시장에서 발생하는 취약점·고객불만·안전사고·온라인 평가 등을 지속적으로 모니터링하고 다시 제품 개선에 반영하는 제품 생애주기 기반 위험관리체계가 중요해지고 있음

07 시사점

- 중국의 스마트 가전 안전정책이 전통적인 제품안전에서 '사이버-물리 통합안전'으로 전환. 네트워크 연결과 AI·소프트웨어가 가전제품의 핵심 기능에 개입하면서, 전기·기계적 안전과 사이버보안을 별도로 관리하기 어렵다는 판단이 반영된 것으로 분석됨. 향후, 스마트 가전 기업은 Electrical Safety·Functional Safety·Cybersecurity·Privacy를 통합한 제품개발·품질관리 체계를 마련할 필요가 있음
- 개인정보보호가 스마트 가전의 '제품 품질' 평가요소로 편입됐다는 점이 중요. 스마트 가전에서 발생하는 위치·영상·음성·사용패턴 등의 데이터에 대한 침해가 단순 개인정보 컴플라이언스 문제를 넘어 제품 자체의 품질·안전 문제로 평가될 수 있다는 의미. 이는 향후 중국 스마트홈 시장에서 Privacy by Design과 Security by Design이 제품 경쟁력 및 품질평가의 기본요건으로 자리잡을 가능성이 높은 것으로 분석됨
- 제품 출시 전 시험 중심의 관리에서 '시장 데이터 기반의 지속적 위험평가'로 이동. 전자상거래 이용후기와 안전 관련 여론까지 위험평가에 활용한다는 것은 실제 사용환경에서 나타나는 이상현상이나 소비자 불만을 제품안전 관리에 직접 반영하려는 접근으로 분석됨. 따라서, 기업은 제품 출시 이후에도 취약점, 장애, 사용자 불만, 개인정보 이슈를 지속적으로 수집·분석하고 이를 OTA·펌웨어 업데이트 등으로 개선하는 체계를 갖춰야 할 필요성이 커지고 있음
- 중국에서도 스마트홈·AIoT 관련 국가표준 체계가 빠르게 세분화되고 있음. 2025~2026년에는 스마트홈 상호운용성, 스마트 가전 지능화 평가, 음성 인터랙션, 가정용 대규모 AI 모델 등 관련 국가표준이 연이어 마련되고 있음. GB/T 47777-2026도 이 가운데 제품 '안전·위험관리' 축을 담당하는 기본 표준으로 볼 수 있음

- 중국 시장에 진출하는 국내 가전·AIoT 기업은 물리적 시험성적뿐 아니라 디지털 위험관리 증적을 함께 준비하는 것이 바람직. GB/T 47777-2026 자체는 강제성 GB가 아닌 권고성 GB/T 표준이지만, 중국의 품질평가·시험·시장감독에서 활용될 가능성을 고려하면 네트워크 취약점, 개인정보 처리, 제어시스템 안전, 펌웨어 관리 등에 대한 위험평가 문서와 기술 증적을 제품 개발단계부터 관리하는 것이 중요해 질 것으로 예상됨

5 중국, 基于局域网的智能家居设备间计算服务调用技术要求 (근거리 통신망(LAN) 기반 스마트홈 기기 간 컴퓨팅 서비스 호출 기술 요구사항)(2026. 07. 10)

- 중국 국가표준정보공공서비스플랫폼에 등록된 국가표준화 지도성 기술문서(国家标准化指导性技术文件) 제정 프로젝트. 표준명은 「基于局域网的智能家居设备间计算服务调用技术要求」, 등록번호는 20263753-Z-339이며, 2026년 7월 10일 등록되어 현재 의견수렴(征求意见) 단계. 전국통신표준화기술위원회(TC485)가 관할하고 중국 공업정보화부가 주관
- 중국정보통신연구원(CAICT)을 비롯해 차이나모바일·차이나텔레콤·차이나유니콤, OPPO, vivo, Huawei, ZTE, Qualcomm China, Tuya 등 통신사·단말·칩·IoT 플랫폼 기업들이 공동 제정에 참여

01 스마트홈 연산을 '클라우드'에서 '가정 내 LAN'으로 분산시키기 위한 기술기반 마련

- "基于局域网(Local Area Network 기반)"과 "设备间计算服务调用(기기간 컴퓨팅 서비스 호출)"이 표준의 핵심 키워드. 즉, 스마트홈 기기가 필요한 연산을 항상 외부 클라우드에 요청하지 않고, 동일 가정 내 LAN에 연결된 다른 단말의 컴퓨팅 자원을 호출·활용할 수 있는 구조를 표준화하려는 것으로 해석할 수 있음. 표준이 통신서비스·응용 분야인 ICS 33.030으로 분류된 것도 이러한 기기간 서비스 호출·연결 구조와 관련된 것으로 분석됨
- 예를 들어, TV, 스마트폰, 홈게이트웨이, AI 스피커, 가전 등이 각자 연산을 수행하는 대신, 상대적으로 높은 AI 연산능력을 가진 기기가 가정 내 다른 기기의 영상·음성·AI 추론 등을 대신 처리하는 홈 엣지 컴퓨팅 구조로 발전할 수 있을 것으로 분석됨

02 스마트홈을 '개별 기기 연결'에서 '분산 컴퓨팅 시스템'으로 발전시키는 표준

- 기존 스마트홈 표준은 주로 기기 연결, 검색, 페어링, 제어 및 상호운용성에 초점을 맞춰왔으나, 이번 프로젝트는 한 단계 더 나아가 한 기기가 다른 기기의 '컴퓨팅 서비스'를 직접 이용하는 구조를 다룬다는 점에서 차이

- 중국은 이미 스마트홈 WLAN 단말의 신속한 네트워크 연결을 규정한 YD/T 6744-2026을 마련했으며, 별도로 스마트홈 기기 중계통신 및 상호운용성 관련 국가표준을 추진. SAMR 역시 이들 표준을 이번 프로젝트와 유사·관련 표준으로 연결하고 있는 것으로 분석됨
- 따라서, 중국의 스마트홈 표준화는 대체로 접속·페어링 → 기기간 통신 → 기기간 서비스 호출 → 분산 연산으로 범위가 확장되고 있는 것으로 분석됨

03 홈 엣지 컴퓨팅과 AI 연산자원의 공유를 위한 기반

- 표준 제정 참여기업에 Qualcomm, Huawei, ZTE 및 스마트폰 제조사인 OPPO·vivo 등이 포함되어 있다는 점도 주목
- 이는 스마트폰·TV·홈게이트웨이 등에 탑재된 CPU·GPU·NPU와 같은 연산자원을 다른 스마트홈 기기가 활용하는 가정 내 분산 AI 컴퓨팅과 밀접한 기술방향으로 해석할 수 있음
- 예를 들어, 향후에는 ▲ 저사양 카메라의 AI 영상분석을 홈 허브의 NPU에서 처리, ▲ 가전 음성인식을 스마트폰·스피커의 AI 프로세서에서 수행, ▲ 센서 데이터를 로컬 AI 모델에서 분석, ▲ 여러 기기의 연산부하를 가정 내 기기 사이에서 분산 등의 구조가 가능해질 수 있을 것으로 예상됨

04 클라우드 의존도를 줄이는 로컬 서비스 구조 확대

- 현재 상당수 스마트홈 서비스는 기기 명령이나 데이터를 인터넷을 통해 클라우드로 전송한 후 결과를 다시 내려받는 구조. 반면, LAN 기반 기기간 서비스 호출이 표준화되면 가정 내부에서 서비스 검색·요청·처리를 완료하는 구조가 확대될 수 있음
- 이에 따라, ▲ 네트워크 지연 감소, ▲ 클라우드 트래픽 및 비용 절감, ▲ 인터넷 장애 시에도 일부 스마트홈 기능 유지, ▲ 사용자 데이터의 외부전송 감소, ▲ 실시간성이 중요한 AI·자동화 기능 개선 등의 효과를 기대할 수 있을 것으로 예상됨
- 중국에는 이미 YD/T 4312-2023 「移动互联网+智能家居系统 家庭边缘计算总体技术要求」라는 가정용 엣지컴퓨팅 관련 표준이 존재하며, SAMR도 이를 이번 프로젝트와 연관된 표준체계로 제시

05 서로 다른 제조사 간 컴퓨팅 서비스 상호운용성 확보가 중요

- 스마트홈 시장은 제조사마다 별도의 생태계와 통신규격을 사용하기 때문에, 단순 기기 제어뿐 아니라 컴퓨팅 서비스까지 상호 호출하려면 공통 인터페이스와 서비스 표현방식이 필요
- 이번 표준에는 China Mobile·China Telecom·China Unicom뿐 아니라 Huawei, OPPO, vivo, ZTE, Tuya, Qualcomm 등이 참여하고 있어, 특정 제조사 내부에서만 사용되는 기술이 아니라 다기종·다브랜드 스마트홈 생태계의 연산자원 상호활용을 위한 공통 기준을 마련하려는 성격이 강한 것으로 분석됨

06 시사점

- 중국 스마트홈의 경쟁축이 '기기 연결'에서 '가정 내 AI 컴퓨팅 자원 공유'로 이동할 가능성이 있는 것으로 분석됨. 그동안 스마트홈 표준화가 연결성·페어링·제어 중심이었다면, 이번 표준은 기기간 컴퓨팅 서비스 활용을 대상으로 함. 향후, TV·스마트폰·라우터·AI 스피커·홈 허브 등이 가정 내 분산 AI 인프라 역할을 수행하는 방향으로 발전할 가능성이 있는 것으로 분석됨
- 온디바이스·엣지 AI 확산을 촉진할 수 있을 것으로 예상됨. 영상·음성·센서 데이터를 매번 클라우드로 전송하지 않고 LAN 내부의 AI 연산기기에서 처리할 수 있다면, 응답속도 향상뿐 아니라 데이터 외부전송도 줄어듦. 따라서, 스마트홈 분야에서도 Cloud AI → On-device/Edge AI → Distributed Home AI로 연산구조가 분산될 가능성이 커질 것으로 분석됨
- 스마트폰과 가전·홈IoT의 경계가 더욱 약해질 전망. Xiaomi·OPPO·vivo·Huawei 등 단말 제조사가 표준화에 참여하고 있다는 점은 스마트폰이 단순 리모컨이 아니라 NPU·CPU·메모리 등의 연산자원을 제공하는 스마트홈 컴퓨팅 노드로 진화할 수 있음을 의미
- 중국은 스마트홈 상호운용성 표준을 단계적으로 촘촘하게 구축. 신속한 WLAN 연결을 다루는 YD/T 6744-2026, 스마트홈 기기 중계통신 기술, 가정용 엣지컴퓨팅 표준과 이번 기기간 서비스 호출 기술문서가 연계되면서 연결-통신-컴퓨팅으로 이어지는 스마트홈 기술표준 체계가 형성되고 있음
- 국내 기업도 중국시장 대응 시 '프로토콜 호환'뿐 아니라 '컴퓨팅 서비스 호환성'을 고려할 필요가 있음. 향후, 이 기술문서가 실제 표준·산업생태계에 확산될 경우, 중국 스마트홈 시장에서 기기는 단순히 명령을 주고받는 수준을 넘어 다른 단말에 연산을 제공하거나 요청할 수 있어야 함. 국내 가전·스마트폰·AIoT 기업도 서비스 디스커버리, 연산능력 표현, 작업 분배, 데이터 전송, 권한·보안 인터페이스 등 분산 컴퓨팅 호환기술을 주시할 필요가 있음

6 중국, 人工智能 家居大模型技术要求(인공지능 가정용 대규모 모델 기술 요구사항)(2026. 08. 27)

- 국가시장감독관리총국·국가표준화관리위원회를 통해 GB/Z 228-2026 「人工智能家居大模型技术要求」(인공지능가정용 대규모 모델 기술요구)를 발표. 이 문서는 현재 유효한 국가표준화 지도성기술문서(指导性技术文件)이며, 전국정보기술표준화기술위원회(TC28)가 관할하고 AI 분과(TC28/SC42)가 수행. 즉, 강제인증 규격이라기보다 중국 스마트홈 기업의 홈 대모델 개발·설계·응용을 위한 국가 차원의 기술 프레임워크

01 스마트홈용 대규모 모델을 별도의 '산업 특화 AI모델'로 정의

- 표준은 가정용 대규모 모델(home large model)을 대규모 가정·스마트홈 분야 데이터를 이용해 학습되고, 다중모달 이해·추론·의사결정 능력을 갖춰 스마트홈 환경에 적용되는 AI 모델로 정의
- 따라서, 일반적인 범용 LLM을 단순히 스마트홈 서비스에 연결하는 것이 아니라, 가정 내 센서·가전·영상·음성·환경정보를 이해하고 이를 기반으로 실제 기기를 제어할 수 있는 도메인 특화 대규모 모델을 별도의 기술영역으로 규정

02 '기기-네트워크-모델-응용' 4계층 구조 제시

- 표준은 스마트홈 대규모 모델 시스템을 다음 4개 논리 계층으로 구성
  - 기기 계층(Device Layer): 스마트가전, 센서, 카메라, 스피커 등 물리적 단말
  - 네트워크 계층(Network Layer): 기기 간 연결 및 데이터·명령 전달
  - 모델 계층(Model Layer): 인지·이해·추론·의사결정 등 AI 핵심 능력
  - 응용 계층(Application Layer): 실제 스마트홈 서비스와 사용자 기능
- 표준의 직접 규정 대상은 네트워크·모델·응용 계층이며, 기기 계층 자체의 제품요건은 별도로 규정하지 않고 있음. 이는 중국이 스마트홈 AI를 개별 'AI 모델'로 보기보다 기기-통신-AI-서비스가 결합된 하나의 시스템 구조로 정의하고 있다는 점에서 의미

03 Home Intelligent Central System을 핵심 허브로 설정

- 표준은 家庭智能中枢系统(가정 지능형 중추 계통)이라는 개념을 별도로 정의. 이는 영상·음성 등 감각 데이터를 이해·추론·의사결정·언어 등의 인지정보로 변환하고, 가정 내부에 연결된 기기를 지능적으로 제어하며 엣지 컴퓨팅과 데이터 저장 기능까지 수행하는 시스템
- 즉, 스마트홈 대규모 모델은 단순 챗봇이 아니라, 사용자·환경 감지 → 상황 이해 → 추론·의사결정 → 가전·설비 제어까지 담당하는 '가정의 AI 두뇌' 역할을 전제로 하고 있음

04 음성 중심에서 '다중모달 스마트홈 AI'로 확대

- 중국이 표준화를 추진한 주요 배경 중 하나는 기존 스마트홈의 음성명령 중심 인터페이스가 복잡한 상황과 문맥을 이해하는 데 한계가 있다는 점으로 분석됨
- 공식 외국어판 제정 설명에서는 스마트홈 대규모 모델이 음성·영상·센서 등 다중모달 데이터의 융합분석, 문맥을 이어가는 연속 대화, 환경정보를 결합한 의도 이해 등을 지원해야 할 필요성을 명시. 예를 들어, 사용자가 "온도를 올려줘"라고 말한 뒤 "다시 2도 내려줘"라고 하면 이전 문맥을 유지해 이해하거나, "너무 어둡다"는 발화를 환경정보와 연결해 조명 제어로 해석할 수 있는 형태
- 따라서, 스마트홈 AI의 인터페이스가 명령어 기반 제어 → 상황·맥락 기반 자연어 및 멀티모달 상호작용으로 전환되는 방향을 보여주고 있는 것으로 분석됨

05 단일 기기 제어에서 '복수 기기 협업·상황 자동화'로 확대

- 가정용 대규모 모델은 개별 에어컨이나 조명을 제어하는 수준을 넘어 여러 기기를 동시에 이해하고 협업시키는 역할을 지향하고 있는 것으로 분석됨
- 공식 표준화 설명은 브랜드·프로토콜 차이로 서로 다른 기기가 연계되지 않는 문제를 주요 표준화 필요성으로 제시하고 있으며, 통일된 인터페이스·데이터 형식과 다중모달 데이터 분석이 필요하다고 설명
- 이에 따라, 향후 스마트홈은 "조명 켜기" → "귀가 상황을 판단해 조명·공조·커튼·AV 등을 일괄 제어"와 같이 모델이 사용자의 의도와 생활 상황을 파악하고 여러 기기를 자율적으로 조율하는 AI 에이전트형

스마트홈으로 발전할 가능성이 큰 것으로 분석됨

06 스마트홈의 AI 핵심 능력을 이해·추론·의사결정까지 확장

- 기존 스마트홈 AI는 음성인식이나 간단한 명령 해석이 중심이었지만, GB/Z 228-2026은 가정용 대규모 모델을 다중모달 이해·추론·의사결정 능력을 보유한 모델로 정의
- 관련 중국의 가정용 대규모 모델 표준체계에서도 음성 깨우기, 사용자 식별, 텍스트 생성뿐 아니라 스마트 보안, 스마트 AV, 스마트 조명 등 다양한 시나리오 지원 능력과 공격 방어·서비스 피드백 등이 평가 영역으로 다뤄져 왔음. 즉, 가정용 대규모 모델의 핵심 경쟁력이 "얼마나 말을 잘 알아듣는가"에서 "얼마나 상황을 정확히 이해하고 적절한 행동을 결정하는가"로 이동하고 있는 것으로 분석됨

07 개인정보·보안 문제를 스마트홈 대규모 모델의 핵심 요건으로 인식

- 가정용 AI는 음성·영상·센서·생활패턴과 같이 매우 민감한 데이터를 지속적으로 처리. GB/Z 228-2026은 규범적 인용표준으로 GB/T 41387-2022 「정보보안기술 스마트홈 일반 보안규범」을 포함
- 따라서, 가정용 대규모 모델의 도입은 AI 성능 문제만이 아니라 스마트홈 정보보안 체계와 연계해 구현해야 하는 기술 영역으로 설정됐다고 볼 수 있으며, 이는 대규모 모델이 집 안의 카메라·마이크·센서 및 가전 제어권을 동시에 보유하게 되면서 기존 스마트 가전보다 개인정보 및 사이버-물리보안 위험이 커지는 데 대응한 것으로 해석됨

08 시사점

- 중국 스마트홈의 중심이 '연결된 가전'에서 'AI가 의사결정하는 가정'으로 이동. 기존 스마트홈은 앱·음성으로 사용자가 직접 각 기기에 명령하는 구조였다면, 가정용 대규모 모델은 환경과 사용자 의도를 스스로 이해하고 복수 기기의 행동을 결정하는 구조를 전제로 함. 이에 따라, 스마트홈 경쟁의 핵심도 기기 연결 수 → AI의 상황 이해·추론·자율제어 능력으로 이동할 가능성이 높은 것으로 분석됨
- 가정용 AI 에이전트가 새로운 스마트홈 플랫폼의 핵심으로 부상할 가능성이 큰 것으로 분석됨. '가정

지능형 중추'가 음성·영상·센서 데이터를 통합하고 기기를 제어하는 구조는 사실상 AI Agent + Home Hub + Edge Computing의 결합으로 해석할 수 있음. 향후, TV·스마트폰·스피커·홈게이트웨이 가운데 어떤 기기가 이 중추 역할을 확보하느냐가 스마트홈 플랫폼 경쟁의 중요한 변수가 될 수 있는 것으로 분석됨

- 온디바이스·엣지 AI의 중요성이 더욱 높아질 전망. 가정에서는 영상·음성·생활패턴과 같은 민감한 정보를 처리하고 실시간으로 기기를 제어해야 하기 때문에, 모든 데이터를 클라우드로 보내기보다 홈 허브나 고성능 가전에서 일부 AI 추론을 수행하는 구조가 유리. 표준에서 가정 지능형 중추에 엣지 컴퓨팅·데이터 저장 능력을 포함한 것도 이러한 방향과 연결되는 것으로 분석됨
- 스마트홈 산업의 경쟁 범위가 가전 제조사에서 AI 모델·통신·보안 사업자로 확대되고 있음. 이번 표준 제정에는 Midea·Haier·Hisense뿐 아니라 China Mobile, iFlytek, Dahua 등 통신·AI·영상 기업도 참여. 이는 스마트홈 시장이 더 이상 가전제품 제조만의 영역이 아니라 AI 모델–네트워크–데이터–기기–서비스가 결합된 생태계 경쟁으로 전환되고 있음을 보여주고 있는 것으로 분석됨
- 국내 가전·AI 기업은 중국 시장에서 단순 기기 상호운용성뿐 아니라 'AI 모델 상호운용성'까지 주시할 필요가 있음. 중국은 이미 스마트홈 상호연결 표준 GB/T 46456 시리즈에 이어 가정용 대규모 모델 표준까지 마련하고 있음. 향후 중국 스마트홈 생태계에서는 기기가 다른 제조사의 AI 중추·대규모 모델과 연계될 수 있도록 공통 데이터 구조, 멀티모달 입력, 제어 API, 권한·보안 구조에 대응해야 할 가능성이 커질 수 있는 것으로 분석됨
- AI 성능과 개인정보·사이버보안이 동시에 제품 경쟁력의 기준이 될 가능성이 큰 것으로 분석됨. 대규모 모델이 카메라·마이크·생활 센서와 실제 가전 제어권까지 연결될 경우, 잘못된 추론이나 보안 침해가 단순 정보 오류를 넘어 프라이버시 침해나 물리적 피해로 이어질 수 있음. 따라서, 향후 스마트홈 AI 제품은 AI Safety + Cybersecurity + Privacy + Functional Safety를 통합적으로 설계하는 방향으로 진화할 가능성이 높은 것으로 분석됨. 이 표준이 스마트홈 일반 보안 규범인 GB/T 41387-2022를 직접 인용하고 있다는 점도 이런 방향을 뒷받침하고 있는 것으로 분석됨

7 Broadband Forum, New interface simplifies management of Matter-powered smart homes(새로운 인터페이스를 통해 Matter 기반 스마트홈 관리 간소화)(2026. 08. 18)

- Broadband Forum, 2026년 8월 18일 Matter 기반 스마트홈을 통합 관리하기 위한 새로운 표준 인터페이스인 'Matter Service API'를 공개. 이 인터페이스는 TR-517(MatterService Data Model for USP Enabled Devices)을 기반으로 하며, Broadband Forum의 USP(User Services Platform, TR-369)와 Matter 프로토콜을 결합해, 제조사와 생태계가 달라도 하나의 공통 인터페이스에서 Matter 기기를 관리할 수 있도록 하는 것이 핵심

01 Matter의 '기기 상호운용성'을 '서비스 상호운용성'으로 확장

- Matter는 Apple, Google, Amazon, Samsung 등 서로 다른 제조사의 스마트홈 기기가 같은 네트워크에서 상호작용할 수 있도록 만든 공통 연결 표준임. 그러나, 실제 서비스 운영 단계에서는 여전히 각 제조사의 클라우드, 모바일 앱, 독자 API에 의존하는 경우가 많아 서비스 제공자와 개발자가 제조사별로 별도의 연동을 구현해야 하는 문제가 있었음
- Broadband Forum의 Matter Service API는 이 문제를 해결하기 위해 Matter 기기를 제조사와 관계없이 하나의 표준화된 서비스 인터페이스로 노출. 이에 따라, 서비스 제공자는 각 생태계별로 서비스를 따로 개발하는 대신, 한 번 개발한 서비스를 여러 Matter 기기에 적용할 수 있음
- 즉, 기존 Matter가 Device ↔ Device 상호운용성을 중심으로 했다면, TR-517은 이를 Device↔Service↔Operator·Application 상호운용성으로 확대하는 역할을 수행

02 TR-517은 Matter와 USP/TR-369를 연결하는 브릿지 역할

- TR-517의 정식 명칭은 MatterService Data Model for USP Enabled Devices임. 이 데이터 모델은 Broadband Forum의 USP/TR-369 관리체계와 Matter 프로토콜을 결합해 스마트홈 게이트웨이, 라우터, 홈 허브가 Matter 기기를 일관된 방식으로 관리할 수 있도록 지원

- Matter 기기 → Matter Service API(TR-517) → USP/TR-369 → 사업자·애플리케이션 서비스의 구조를 가지며, 따라서, 통신사나 서비스 사업자는 기존에 광대역 단말·홈게이트웨이 관리에 활용해 온 USP 체계 안에서 Matter 기기까지 함께 관리할 수 있게 됨

03 제조사와 관계없이 전체 Matter 기기를 한눈에 관리

- Broadband Forum은 Matter Service API를 서비스 제공자가 스마트홈 네트워크 내 모든 Matter 기기를 제조사와 무관하게 전체적으로 볼 수 있게 하는 최초의 표준화 솔루션으로 설명
- 이를 통해 서비스 사업자는 ▲ 기기 상태 및 장애 진단, ▲ 스마트홈 자동화, ▲ 에너지관리, ▲ 고객지원, ▲ 원격 문제 해결, ▲ 기기 상태 모니터링 등의 기능을 통합적으로 제공할 수 있을 것으로 예상됨
- 특히, 장애나 설정 문제를 고객이 인지하기 전에 사업자가 탐지·조치하는 Proactive Customer Care 서비스 구현이 가능해질 수 있을 것으로 예상됨

04 스마트홈 게이트웨이·라우터가 서비스 플랫폼으로 변화

- TR-517의 중요한 의미는 가정 내 게이트웨이와 라우터의 역할 변화임. 기존에는 인터넷 접속과 Wi-Fi 연결이 주 기능이었다면, Matter Service API를 적용하면 게이트웨이와 스마트홈 허브가 여러 Matter 기기를 통합관리하고 새로운 서비스가 실행되는 플랫폼으로 기능할 수 있음
- Orange Innovation은 이 구조를 통해 게이트웨이와 스마트홈 허브가 안정적인 혁신 플랫폼이 되고, 서비스 사업자가 새로운 유료 서비스를 더 쉽게 출시할 수 있다고 설명. 즉, Broadband Gateway → Home Service Platform으로의 전환이 본격화되는 것으로 분석됨

05 Matter 기기 확장에 자동 대응하는 데이터 모델

- Matter는 초기 조명·플러그 중심에서 최근 카메라, 가전제품, 에너지관리 기기, 센서, 블라인드·차양 등으로 적용 분야를 넓히고 있음. TR-517은 Matter의 기기 정의 변화와 자동으로 정렬(aligned)되는 구조를 갖기 때문에 새로운 Matter 기기 유형이 등장할 때마다 사업자가 별도의 관리체계를 처음부터 다시 개발해야 하는 부담을 줄일 수 있음

- 따라서, 스마트홈 생태계가 확대돼도 장기간 활용 가능한 future-ready service framework를 지향한다고 볼 수 있음

06 클라우드 의존도를 줄이고, 홈 내부 처리를 확대

- Broadband Forum은 TR-517을 통해 게이트웨이와 스마트홈 허브가 가정 내 Matter 기기와 직접 통신할 수 있어 클라우드 서비스 의존도를 줄일 수 있다고 설명
- 이에 따라, ▲ 인터넷 장애 시에도 일부 스마트홈 기능 유지, ▲ 클라우드 왕복 지연 감소, ▲ 민감한 가정 데이터를 홈 네트워크 내부에서 처리, ▲ 외부 클라우드 서비스 장애 영향 감소, ▲ 서비스 응답속도 및 복원력 향상 등의 효과를 기대할 수 있을 것으로 예상됨
- 이는 스마트홈 구조가 Cloud-centric → Home Edge/Local-centric으로 일부 이동하는 흐름과 연결됨

07 시사점

- Matter의 경쟁 축이 '기기 연결'에서 '서비스 통합'으로 이동. Matter가 제조사 간 연결 문제를 상당 부분 해결했지만, 서비스·관리 계층은 여전히 Apple·Google·Amazon·Samsung 등 각 생태계에 분절되어 있었음. TR-517은 이 위에 공통 서비스계층을 추가함으로써 향후 스마트홈 경쟁의 중심을 Connectivity → Management & Service로 확장할 가능성이 있는 것으로 분석됨
- 통신사의 스마트홈 시장 역할이 커질 가능성이 있음. 통신사는 이미 가정 내 브로드밴드 게이트웨이와 라우터를 관리하고 있고 USP/TR-369를 활용하고 있음. 여기에 Matter 기기 관리가 결합되면 통신사는 인터넷 연결뿐 아니라 스마트홈 진단, 보안, 에너지관리, 자동화, 유지보수 서비스를 제공하는 홈 플랫폼 사업자로 확대될 수 있음. Broadband Forum도 TR-517을 새로운 수익화 서비스의 기반으로 제시하고 있음
- 홈게이트웨이가 스마트홈의 '로컬 컨트롤 플레인'으로 부상할 수 있음. Matter 기기를 클라우드가 아닌 가정 내 게이트웨이·허브에서 직접 관리하면 네트워크 장애 시에도 서비스 지속성을 확보할 수 있고 민감한 데이터를 외부로 보내지 않아도 됨. 이는 앞서 중국에서 추진되는 홈 엣지·분산 컴퓨팅 표준과도 방향성이 유사하며, 스마트홈 아키텍처가 클라우드 중심에서 Cloud + Home Edge의 하이브리드 구조로 전환되고 있음을 보여줌

- 스마트홈 사업자의 개발·운영비용을 크게 줄일 수 있음. 지금까지 여러 제조사·플랫폼의 스마트홈 기기를 지원하려면 각각의 API·클라우드·앱과 개별적으로 통합해야 했지만, TR-517이 확산되면 사업자는 한 번의 표준 인터페이스 개발로 복수 Matter 생태계를 지원할 수 있음. 따라서, 서비스 출시 기간 단축과 유지관리 비용 절감 효과가 기대됨
- 스마트홈의 새로운 수익모델이 '기기 판매'에서 '관리형 서비스'로 확대될 가능성이 있음. 통합 진단, 에너지 절감, 자동화, 예방적 장애관리, 원격 고객지원 등의 기능을 구독형·부가서비스로 제공할 수 있기 때문임. 특히, 통신사 입장에서는 기존 인터넷 회선과 Wi-Fi 관리 서비스에 Matter 기반 스마트홈 서비스를 결합해 Managed Smart Home 상품으로 확장할 가능성이 커짐
- 국내 통신사·홈 IoT 기업도 Matter 자체뿐 아니라 USP/TR-369와 TR-517의 결합을 주시할 필요가 있음. 앞으로 Matter 기기가 확대될수록 경쟁력은 단순히 "Matter를 지원하는가"보다 "다양한 Matter 기기를 얼마나 일관되게 진단·관리·자동화하고 서비스화할 수 있는가"로 이동할 가능성이 높음. 특히, 국내 통신사가 보유한 홈게이트웨이·Wi-Fi 관리 플랫폼을 TR-517과 연결한다면 스마트홈, 보안, 에너지관리, 돌봄 서비스 등으로 사업 범위를 확대할 수 있을 것으로 예상됨

8 日 ECHONET, ECHONET Lite Device Authentication 仕様向け認証局募集のご案内 (ECHONET Lite 기기 인증 사양용 인증기관 모집 안내)(2026. 08. 28)

- ECHONET Consortium은 2026년 8월 28일 「ECHONET Lite Device Authentication(DA) 사양용 인증기관 모집」을 공고. ECHONET Lite 기기 간 통신에 전자증명서 기반 기기 인증과 암호화를 도입하고, 이를 검증하는 'ECHONET Lite Secure' 제3자 인증제도를 2026년부터 본격 운영하기 위해 인증서 발급기관(CA)을 지정하는 것이 핵심

01 ECHONET Lite에 '기기 인증' 보안계층 추가

- ECHONET Lite는 다양한 전송매체에서 높은 상호운용성을 확보하는 데 강점이 있었지만, 연결된 기기끼리 상대방의 신원을 확인하고 통신 대상을 제한하는 기능은 별도의 보안 강화가 필요
- 새로운 Device Authentication(DA) 사양은 사용자가 연결을 승인한 기기를 식별하고, 기기 간에 서로를 인증한 뒤 안전하게 통신하도록 하는 구조를 도입. ECHONET Consortium은 DA를 통해 기기 인증과 통신 암호화를 활용할 수 있다고 설명
- 즉, 기존 구조가 ECHONET Lite 연결 → 기기 제어 중심에서 향후, 기기 식별 → 상호 인증 → 권한 있는 기기 간 암호화 통신 → 제어 구조로 강화될 것으로 예상됨

02 전자증명서 기반 신뢰체계(PKI) 구축

- DA 사양을 실제로 동작시키기 위해서는 각 기기에 사용할 전자증명서가 필요. 이에 따라, ECHONET Consortium은 해당 인증서를 발급하는 인증기관(Certificate Authority)을 직접 운영하는 대신, 일정 요건을 충족하는 외부 기관을 심사·인정하는 체계를 구축
- 이번 공고의 직접적인 목적도 바로 이 DA용 인증기관 모집임. 인증기관으로 인정받으려면 DA 사양에 대한 전문성을 보유하고 인증기관을 설치·운영할 수 있어야 하며, ECHONET Consortium 회원 또는 준회원 자격도 요구됨(신청 기한은 2026년 9월 25일로 제시)

- 이는 ECHONET Lite 보안이 단순한 암호화 알고리즘 적용을 넘어 기기 신원을 보증하는 PKI 기반 Trust Infrastructure로 발전하고 있다는 것을 의미

03 'ECHONET Lite Secure' 제3자 인증제도 도입

- ECHONET Consortium은 DA 사양을 탑재한 기기를 대상으로 ECHONET Lite Secure 제3자 인증제도를 2026년부터 시작한다고 밝힘. 기존 ECHONET Lite와 AIF의 적합성 인증제도가 주로 상호접속·기능 호환성을 검증했다면, 새 제도에서는 DA 사양의 적합성과 보안 기능까지 인증 대상으로 확대됨
- 컨소시엄은 DA 대응 제품을 각각 'ECHONET Lite Secure', AIF까지 지원하는 경우 'ECHONET Lite AIF Secure'로 구분할 계획이며, 2026년 가을 무렵을 목표로 인증 운영 개시를 추진

04 JC-STAR 스마트홈 보안요건과 연계

- DA 사양은 일본의 IoT 보안 적합성 평가·라벨링 제도인 JC-STAR의 스마트홈 분야 ★2 보안요건안을 고려해 개발. ECHONET Consortium은 과거 검토 사양을 기반으로 실제 운용을 염두에 두고 개선한 DA 사양을 마련했다고 밝힘
- 따라서, DA는 ECHONET 자체의 기술개선에 그치지 않고, 일본 정부 차원의 IoT 제품 보안 라벨링·인증 정책과 상호연계되는 산업표준으로 발전

05 상호운용성과 보안을 동시에 유지하는 구조

- 보안을 강화한다고 해서 기존 ECHONET Lite의 개방성과 상호운용성을 희생하지 않는 것이 DA의 중요한 설계 방향
- ECHONET Consortium은 기존 ECHONET Lite 프로토콜의 높은 상호접속성을 전제로 하면서, 그 위에 기기 인증 기능을 추가해 통신 상대를 적절하게 제한하는 방식이라고 설명. 즉, Interoperability + Authentication + Encryption을 동시에 확보하려는 구조임

06 시사점

- 일본 스마트홈 표준화의 중심이 '연결 가능성'에서 '신뢰 가능한 연결'로 이동. ECHONET Lite의 초기 강점은 제조사가 다른 가전·에너지 기기 간 상호운용성이었지만, 스마트홈 기기 수가 증가하면서 단순히 연결되는 것만으로는 부족해짐. DA 사양은 누가 연결됐는지 확인하고, 승인된 기기끼리만 통신하도록 하는 Zero Trust형 접근을 스마트홈에 도입하는 방향으로 이해
- 스마트홈에서도 PKI와 디지털 기기 신원이 핵심 인프라로 부상. 각 기기에 전자증명서를 부여하고 인증기관이 이를 보증하는 체계를 구축한다는 것은, 향후 스마트가전·HEMS·EV·태양광·배터리 등이 고유한 디지털 신원을 갖고 상호 인증하는 구조로 발전할 가능성을 의미. 이에 따라, 인증서 발급·갱신·폐기와 키 관리가 제품 생애주기 보안의 중요한 영역으로 확대될 것으로 예상됨
- 일본의 IoT 보안 라벨링 제도와 민간 스마트홈 표준이 본격적으로 결합되고 있음. DA 사양이 JC-STAR ★2 요구사항을 고려해 설계됐다는 점은, 향후 정부 보안정책과 ECHONET의 제품 인증체계가 서로 보완적으로 작동할 가능성을 보여줌. 제조사 입장에서는 통신규격 적합성뿐 아니라 제품보안 인증·라벨 대응까지 동시에 고려해야 하는 구조가 형성될 수 있는 것으로 분석됨
- 스마트홈 보안 경쟁이 개별 기기 보안에서 '생태계 신뢰관리'로 확대. 기기 자체에 보안칩이나 암호화를 적용하는 것만으로는 충분하지 않고, 어떤 제조사·기기가 신뢰되는지, 누가 인증서를 발급하고 폐기하는지까지 관리해야 함. 즉, 경쟁의 초점이 Device Security → Identity & Trust Management로 확대되고 있음
- 국내 스마트가전·HEMS 기업도 일본시장 대응 시 DA 인증체계를 확인할 필요가 있음. 향후, ECHONET Lite Secure가 실제 조달·HEMS·에너지관리 시장에서 활용될 경우 일본에 제품을 공급하는 기업은 기존 ECHONET Lite/AIF 적합성뿐 아니라 기기 인증서 탑재, 보안키 관리, 상호 인증, 암호화 통신 및 제3자 인증까지 준비해야 할 가능성이 있음. 특히, 장기간 사용하는 에어컨·급탕기·EV 충·방전기·ESS 등에서는 인증서의 장기 관리 정책까지 중요해질 수 있음

II. 지능형 홈 건설 동향



AI 홈 에이전트의 확산과 아파트의 지능형 주거 플랫폼 전환

01 지능형홈의 진화

- 지능형홈은 Connected Home→Automated Home→Intelligent Home→Agentic Home→Intelligent Residential Platform의 단계로 발전
- (Connected Home) 가전·센서·조명·도어록 등 각각의 기기를 네트워크에 연결하고, 스마트폰이나 음성으로 원격 모니터링·제어할 수 있는 단계로 '지능'보다 Connectivity와 Interoperability가 핵심
  - (CSA) Matter를 IP 기반의 공통 연결 표준으로 정의하고 있으며, 서로 다른 제조사와 생태계의 기기들이 함께 작동하도록 하는 것이 핵심 가치. 2026년 Matter 1.6에서도 다중 생태계 간 기기 관리와 상태·기능 표현 개선이 주요 과제로 다뤄짐
  - 사용자 → 앱·음성 → 개별 기기 제어가 일반적인 구조로, 예를 들어 외부에서 에어컨을 켜거나, 앱에서 도어록 상태를 확인하고, 하나의 앱에서 조명과 플러그를 제어하는 방식
  - "얼마나 많은 기기를 연결할 수 있는가", 그리고 "다른 제조사 기기와 얼마나 쉽게 연동되는가"가 핵심 경쟁력이며, '독립형 가전' → '네트워크에 연결된 가전'으로 전환되고 있음
- (Automated Home) 연결된 기기들을 사람이 하나씩 제어하지 않고, 사전에 정의된 조건·규칙에 따라 자동으로 동작하는 단계로, Trigger → Condition → Action이 전형적인 구조
  - Google Home의 자동화 구조도 기본적으로 starter–condition–action을 이용하며, 사용자가 정의한 조건이 충족되면 특정 기기나 서비스를 작동시키는 방식으로 사람의 반복행동을 규칙으로 전환하는 것이 핵심
  - Connected Home에서는 사람이 매번 명령하지만, Automated Home에서는 한번 규칙을 설정하면 시스템이 반복적으로 실행. 반면, 대부분의 자동화는 여전히 사람이 사전에 규칙을 만들어야 하는 한계도 존재. '직접 제어' → '조건 기반 자동제어'로 전환되고 있음
- (Intelligent Home) 단순히 규칙을 실행하는 것을 넘어, AI가 사용자·환경·기기의 상태를

종합적으로 이해하고 상황에 적합한 행동을 결정하는 단계로 'Sensor+Data+AI+Context Awareness'가 핵심 기술

- (Google) 기존 스마트홈이 단순 명령 중심의 "transactional" 경험에 머물렀다고 설명하며, Gemini for Home을 통해 자연어, 문맥, 복잡한 요구를 이해하는 Home Intelligence로 발전시키고 있음
- (삼성전자) AI Home을 연결된 기기와 ambient intelligence를 결합해 사용자의 필요를 이해하고 예측하는 환경으로 설명
- 예를 들면, "사용자가 평소보다 늦게 귀가했고 집이 어두우며 피로도가 높은 상태 → 조명을 낮은 색온도로 켜고 실내온도를 선호값으로 조정"하는 방식이며, AI가 상황을 해석하고, AI가 적절한 행동을 추천·결정한다는 점에서 Automated Home과 큰 차이를 가짐
- Rule-based Automation에서 Context-aware Intelligence로 전환되는 것이 핵심

- (Agentic Home) 사용자의 목표(Goal)를 이해하고 여러 단계의 일을 스스로 계획·실행하는 단계로, Observe → Reason → Plan → Act → Verify로 핵심 구조가 변화
  - Agentic Home에서는 명령(Command)이 아닌 목적(Goal)을 입력받는 구조
  - (Google) 2026년 Home MCP를 통해 개인 AI Agent가 실제 Google Home의 기기 구조 조회, 실시간 상태 확인, 기기 제어, 과거 이벤트 분석을 수행할 수 있도록 Early Access를 제공하기 시작. Google은 이를 명시적으로 "personal agents"가 스마트홈과 직접 상호작용하는 구조라고 설명
  - 기존 스마트홈에서는 사람이 판단 → 기기가 실행했지만, Agentic Home에서는 사람이 목적 제시 → AI가 판단·계획 → 여러 기기·서비스 실행으로 변화하며, Context-aware AI → Goal-oriented Autonomous Agent로 핵심이 전환되고 있음

- (Intelligent Residential Platform) 지능의 범위가 한 가구 내부를 넘어 건물·단지·커뮤니티·외부 서비스까지 확대되는 단계로, 지능형홈이 더 이상 '스마트한 집'이 아니라 주거생활을 통합 운영하는 디지털 플랫폼으로 변화. Home → Building → Complex → City / Service Ecosystem이 핵심 구조
  - (삼성물산) 홈닉은 세대 내부 스마트홈뿐 아니라, 커뮤니티 시설, 생활서비스 등을 통합한 Residential Platform으로 사업 영역을 확대. (현대건설) AI 기반 건강주거 서비스 추진을 발표하면서, 주거공간을 일상 건강관리 플랫폼으로 확대하는 방향을 제시

표 1. 지능형홈 발전 단계에 따른 특징 비교

구분	Connected	Automated	Intelligent	Agentic	Residential Platform
핵심 질문	연결?	자동 동작?	상황 이해?	자가 수행?	주거생활 전체 운영?
사용자 입력	명령	규칙 설정	자연어·행동	목표	생활·서비스 요구
판단 주체	사람	규칙·엔진	AI	AI Agent	AI+플랫폼
자동화 수준	낮음	중간	높음	매우 높음	시스템 수준
데이터	기기 상태	이벤트 데이터	생활·환경 데이터	장기 Context	세대·건물·서비스 데이터
대상	기기	기기군	집	집+서비스	세대·건물·단지
핵심 기술	IoT·Matter	Routine	AI·멀티모달	LLM·Agent·MCP	AI+IoT+Cloud+ Edge+Platform
사업모델	기기 판매	스마트홈 기능	AI서비스	Agent 구독	주거플랫폼· B2B2C

출처 : 한국AI스마트홈산업협회

02 AI홈 에이전트의 개념과 기술적 진화

- 기존 스마트홈은 사람이 앱이나 음성으로 특정 행동을 직접 지시하고, 자동화 기능이 있어도 대부분 사용자가 미리 설정한 규칙을 실행하는 구조였다면, AI 홈 에이전트는 사용자가 행동(Action)을 지정하는 대신 목표(Goal)를 제시하면 AI가 상황을 이해하고 필요한 행동을 스스로 조합하는 구조
- 따라서, AI 홈 에이전트는 거주자의 자연어 명령과 생활패턴, 공간·환경 및 기기 상태 등의 맥락정보를 지속적으로 인지하고, AI의 추론·계획 능력을 이용해 사용자의 목표를 해석한 뒤 복수의 스마트홈 기기와 서비스를 자율적으로 조율·실행하는 지능형 소프트웨어 시스템으로 정의할 수 있음
- AI 홈 에이전트의 핵심 기능은 Perception, Context Understanding, Reasoning, Planning, Action, Learning·Memory임
  - (Perception) 온도, 소리, 카메라, 움직임 등 공간·사람·환경에 대한 인지
  - (Context Understanding) 재실 여부, 취침·외출 등 상황·의도에 대한 이해
  - (Reasoning) 에너지·쾌적성·보안 등 복합 정보에 대한 종합 판단

- (Planning) 냉방→조명→커튼 순차 실행과 같은 목표 달성을 위한 행동 계획 수립
- (Action) 가전·도어록·HVAC·EV 제어 등 기기 및 서비스 실행
- (Learning·Memory) 개인별 온도·조명 등에 대한 선호와 행동에 대한 학습 및 기억

- AI 홈 에이전트의 핵심 기술은 하나의 LLM만으로 구현되는 것이 아니라, ▲Perception, ▲Connectivity & Device Abstraction, ▲ Home Context / Digital Twin, ▲ Intelligence (LLM·Multimodal Model), ▲Memory & Personalization, ▲Agent Planning & Orchestration, ▲ Action / Tool, ▲ Cloud + Edge Hybrid AI 등의 다층 구조로 구성됨
  - (Perception) 집·가정의 현실 상태를 디지털 데이터로 변환하는 센싱 계층(카메라·영상, 마이크·음성, 온도·습도·공기질, 조도, 움직임·재실센서, 전력사용량, 가전 작동상태, 도어록·보안센서 등)이 가장 아래에 위치. 과거 스마트홈에서는 센서가 단순 트리거 역할을 했다면 AI 홈에서는 이들을 결합해 멀티모달 상황정보(Context)를 생성
  - (Connectivity & Device Abstraction) AI가 집을 제어하기 위해서는 제조사마다 다른 수 많은 가전과 기기들을 공통 방식으로 이해해야 하며, Matter와 같은 기술은 AI 홈 에이전트에게 일조으이 공통 디바이스 API 역할을 수행
  - (Home Context / Digital Twin) AI 홈 에이전트는 단순 기기 목록만으로는 부족하며, Home → Room → Device → User → State → Event의 정보를 구조화하는 것이 필요. 즉, AI 에이전트에게 홈 구조, 영역·기기, 속성, 실시간 상태를 조회할 수 있는 기능을 제공하는 것이 중요
  - (Intelligence-LLM·멀티모달 Model) AI 홈 에이전트의 두뇌로, 기존 스마트홈에서는 Rule Engine이 작동했다면, AI 홈 에이전트에서는 LLM·멀티모달 모델이 추론을 수행
  - (Memory & Personalization) AI 홈 에이전트는 사용자의 선호와 생활 맥락(선호 온도, 취침 시간, TV 시청 습관, 조명 밝기, 가족 구성, 반복되는 생활 및 외출 패턴, 에너지 절감 선호 등)을 기억하고 장기적으로 학습함
  - (Agent Planning & Orchestration) AI 홈 에이전트의 핵심 기술 계층으로 사용자의 목표를 여러 개의 실행 가능한 작업(Observe → Reason → Plan → Act → Monitor → Replan 등)으로 분해하고 각 작업을 조율
  - (Action / Tool) AI 홈 에이전트는 LLM → Tool/API → Device의 과정을 통해 실제로 집을 작동시킴. Google의 Home MCP는 AI 에이전트가 MCP를 통해 홈 구조 조회, 기기 검색, 실시간 상태 조회, 기기 제어, 과거 이벤트 분석을 수행하는 구조를 명확하게 보여줌
  - (Cloud + Edge Hybrid AI) AI 홈 에이전트는 클라우드 기반으로 실행되기 보다는 Cloud+Home Edge+On-Device AI 구조로 발전. 실시간성과 프라이버시가 필요한 기능은 로컬에서, 음성 Wake-up, 사람 존재 감지, 보안 카메라 이벤트 분석, 긴급 기기 제어 등은 로컬에서, 복잡한 추론은 클라우드에서 처리하는 구조를 가짐

그림 1. AI 홈 에이전트의 기술 계층



출처 : 한국AI스마트홈산업협회

- (Next Move Strategy Consulting) 글로벌 스마트홈 AI 시장 규모는 2025년 162억 3천만 달러로 추산되며, 2026년에는 202억 6천만 달러로 예상됨. 연평균 24.8%씩 성장하여 2035년 1,487억 5천만 달러 규모에 이를 것으로 예상됨
  - ▲ 생성형 AI 기반 홈 어시스턴트 확산, ▲ Matter 확산에 따른 제조사 간 상호운용성 개선, ▲ AI 스마트 보안기기 보급 확대, ▲ 엣지 AI 발전으로 프라이버시·지연 문제 완화, ▲ 하드웨어 판매에서 구독형 AI 서비스로 수익모델 전환 등이 시장 성장 요인으로 분석됨
  - 이 중에서 생성형 AI 어시스턴트의 확산이 가장 큰 성장요인으로 분석되는데, 생성형 AI 부문은 현재 시장 규모는 작지만, 2026년~2035년 연평균 42.6%씩 성장하여 AI 기술 중 가장 빠르게 성장할 것으로 전망됨. 이는 스마트홈의 경쟁력이 단순 기기 제어에서 대화·이해·추론·실행이 가능한 AI 홈 에이전트로 이동하고 있음을 의미하는 것으로 분석됨

표 2. 기술별 AI in Smart Home 시장 규모 전망(단위: 10억 달러)

기술 구분	2025년	2035년	CAGR(2026~2035)
NLP	3.57	22.31	19.6%
Computer Vision	3.25	28.26	24.1%
Machine Learning	3.90	29.75	22.3%
Predictive Analytics	1.95	16.36	23.6%
Context Awareness	1.30	13.39	26.4%
Edge AI	1.46	20.83	31.1%
Generative AI	0.49	14.88	42.6%
Residual AI Technologies	0.31	2.97	25.4%
Total	16.23	148.75	24.8%

출처 : Next Move Strategy Consulting
https://www.nextmsc.com/report/ai-in-smart-home-market-ic5444

03 국내 주요 건설사들의 AI 홈 에이전트 사업 동향

- 국내 주요 건설사들은 AI 홈 에이전트를 단순 '세대 내 기기제어 시스템'에서 '세대·단지·생활서비스를 통합하는 지능형 주거 플랫폼'으로 전환시키는 핵심 요인으로 인식하고, 사업을 강화하고 있음
- (GS건설·LG전자) 2026년 7월 '차세대 AI홈 공동개발' MOU를 체결하고, LG전자 AI홈 허브 ThinQ ON과 GS건설 '자이(Xi)'의 공동주택 인프라를 통합. AI홈의 범위를 냉난방·조명·가전 등 세대 내부에서 엘리베이터·주차·방문객·커뮤니티 시설 등 단지 전체로 확대하는 것이 핵심

- 세대 내 가전과 조명·난방·환기·콘센트·가스밸브뿐 아니라 엘리베이터 호출, 차량 시동 및 주차 위치 확인, 방문 이력 확인, 커뮤니티 시설 예약까지 하나의 AI홈 시스템에서 연결하는 구상. LG전자의 AI홈은 사용자와 자연어로 대화하면서 생활 맥락과 패턴을 파악해 필요한 기능을 제안하거나 자동 실행하는 구조
- 양사는 2026년 4월 이미 홈로봇 LG CLOiD와 단지 배송·서빙 로봇을 활용하는 미래형 주거 로봇 서비스 협력도 시작. 즉 AI Home Agent + Robot + Apartment Infrastructure를 하나의 주거 시스템으로 묶는 방향

● (포스코이앤씨) 2026년 7월 하이엔드 브랜드 오티에르(HAUTERRE) 전용 스마트홈 플랫폼을 출시. 기존 스마트홈 앱처럼 단순 설비 제어를 제공하는 것이 아니라 입주민의 주거 경험 전체를 하나의 플랫폼에 통합하는 것이 핵심

- 플랫폼은 My Home(세대 기기 제어), Life(커뮤니티 예약·관리비·생활서비스), Social(입주민 소통) 등으로 구성되고, 여기에 자산관리, 홈스타일링 상담, 건강검진 예약 등 외부 제휴서비스까지 연계. 향후, 플랫폼에 AI Agent를 도입해 자연어 기반 대화와 생활환경에 맞춘 맞춤형 제안을 제공하고, 궁극적으로 초개인화 주거 서비스로 고도화를 목표

● (HDC랩스) AI 홈 에이전트를 생활패턴 학습, 주거환경 데이터 분석, 사용자의 의도·상황 이해, 필요한 서비스 선제 제안, 공간환경 자동 최적화 등을 수행하는 핵심 솔루션으로 정의하고, AI Model+Home Agent+Wallpad(베스틴)+Building OS를 하나의 구조에서 개발

- AI 홈 에이전트는 단순 제어 중심의 스마트홈에서 한 단계 더 나아가 AI 에이전트와 자연어 처리, 초개인화 AI 기술을 통해 거주자의 생활 맥락을 이해하고 필요한 서비스를 능동적으로 제공. 특히, 버튼을 누르거나 화면을 터치할 필요 없이 일상적인 대화만으로 사용자의 의도와 상황을 파악해 조명·난방·환기 등 주거환경을 제어하고 다양한 생활 서비스를 연계
- 생활 데이터 수집→AI 패턴 학습→공간 자동 최적화→건강·생활 케어→AI 비서로 이어지는 구조. 2026년 국가 독자 AI 파운데이션 모델 프로젝트에도 참여해 주거·빌딩 특화 LLM/VLM을 실증. AI 월패드와 스마트홈 앱·관제·시설관리 등에 이를 확대하고, AI Agent 월패드를 상용화할 계획

● (현대건설) 2026년 6월 발표한 AI 주거 혁신 로드맵에서 생성형 AI 분양상담사(분양이나 청약 관련 문의 실시간 해결), AI 홈 라이프 서비스(자체 통합 플랫폼 앱과 연동해 주거 공간 제어 및 편의성 극대화), 초개인화 비서 서비스(입주 후 축적되는 라이프스타일 데이터를 바탕으로 다양한 컨시어지 서비스와 연동) 등 총 3단계 구축을 목표

- AI 고도화가 완료되면, 입주민은 온라인 통합플랫폼을 통해 민원 처리, 아파트 관리, 에너지 관리, 이동 서비스, 구독형 홈서비스, 여가생활 큐레이션 등과 같은 맞춤형 서비스를 개인의 생활 패턴에 맞춰 경험
- 또한, 현대차·기아 로보틱스랩 및 슈프리마와 협력해 공동현관·엘리베이터와 로봇을 연계하고, 배송·안내·보안순찰·어린이 안전·응급상황 대응 등의 단지 로봇 서비스 인프라도 구축

- (삼성물산) 홈닉(Homeniq)은 아파트용 스마트홈을 독립 주거 플랫폼 사업으로 전환. 2026년 7월 기준 홈닉은 HJ중공업을 포함해 18개 건설사와 협력 관계를 확대
  - HJ중공업에는 '해모로 by 홈닉' 형태로 제공돼 홈IoT, 커뮤니티 예약, 관리비·공지, 주차·방문차량, 에너지 관리 등을 서비스. 2026년 5월에는 한샘과 협력해 인테리어·입주청소 등 입주 전 서비스까지 범위를 확대, 8월에는 세대 청소, 출장 세차, 의류 수거, 펫케어 등 생활편의 서비스를 추가
  - 고객 접점이 입주 후 아파트 제어에서 입주 전 → 입주 → 거주 → 생활서비스로 확대되고 있으며, AI 에이전트 자체보다는 AI 에이전트가 활용할 수 있는 Residential Service OS를 지향하는 것으로 분석됨

표 3. 주요 건설사들의 AI 홈 에이전트 사업 동향

기업명	주요 플랫폼	적용 범위	차별점	진화 방향
GS건설·LG전자	자이(Xi)+LG ThinQ ON	세대 → 단지	AI홈과 아파트 인프라, 홈·배송 로봇까지 통합	Agentic Home → 단지형 지능형 주거 플랫폼
포스코이앤씨	오티에르 스마트홈 플랫폼	세대 + 생활서비스	AI Agent 도입 전 주거 데이터·서비스 플랫폼을 먼저 구축	Residential Experience Platform → AI Agent 기반 초개인화
HDC 랩스	AI Wonder Home, AI Agent 월패드, AI Building OS	세대 → 건물 → 단지	AI 홈 에이전트를 가장 직접적으로 제품화, LLM·VLM과 월패드·빌딩OS까지 결합	AI Home Agent → AI Building OS → Autonomous Town
현대건설	AI Home Life Service, Hyper-personalized Assistant	분양 → 세대 → 단지 → 생활서비스	AI를 주거 전 생애주기에 적용	Home Agent → Residential Life Agent
삼성물산	홈닉(Homeniq)	세대 → 단지 → 외부 서비스	홈닉을 타 건설사에도 공급하며 범용 B2B 주거 플랫폼으로 확장	Smart Home Platform → Residential Service OS

출처 : 한국AI스마트홈산업협회

04 글로벌 AI 홈 에이전트 사업 동향

- 글로벌 시장에서 AI 홈 에이전트의 최근 흐름은 Connected Device 중심의 스마트홈에서 공간이 사용자를 이해하고 AI가 기기·서비스를 자율적으로 조율하는 Intelligent Residential Platform으로 이동하고 있는 것으로 분석됨
- (HOMMA) Built-in Intelligence(BII)는 일반적인 스마트홈처럼 입주 후 IoT 기기를 구입해 앱과 연결하는 방식이 아니라, 주택 설계 단계부터 센서·조명·블라인드·공조·스마트록 등의 위치와 시스템 구성을 건축에 통합하는 방식. HOMMA는 이를 단순 스마트홈보다 한 단계 높은 건축과 테크놀로지의 융합으로 설명
  - 사용자가 스마트홈을 조작하지 않아도 되는 환경을 지향. 실내 센서가 사람의 움직임과 재실 상태를 인식해 조명을 자동으로 작동하고, 자연광 변화에 맞춰 하루 5개 시간대로 조명을 조정하는 Circadian Lighting 등을 구현. 전용 앱이나 음성 명령을 매번 사용하지 않아도 주택이 상황을 인식해 자동으로 작동하는 hands-free·autonomous home을 지향
  - 2026년 HOMMA와 KLab의 UAE 합작법인 설립 발표에서는 Built-in Intelligence를 보다 명확하게 Autonomous, Agent-based Smart Home으로 정의. 천장에 내장된 센서, Edge Computing, AI를 활용해 거주자의 생활습관을 학습하고 집의 리듬에 맞춰 자동으로 대응하는 구조. 적용범위도 조명·냉난방 자동화에서 홈 보안, 고령자 모니터링, 낙상감지 등 홈 헬스케어로 확장(Built-in Sensor→Home Edge Computing→Occupancy / Context Recognition→AI 판단→조명·공조·블라인드·보안 자동제어와 같이 Space/Sensor → AI → Autonomous Action으로 전환)
  - 한편, BII를 소비자가 직접 구매하는 스마트홈 제품이 아니라 주택 개발사·건설사에 공급하는 B2B 플랫폼으로 사업화하고 있음. HOMMA는 자사를 Real Estate Developer+Smart Home Software Company로 설명하며, 고층 공동주택, 타운하우스 등 개발사업에 스마트홈 기술과 건축요소를 일괄적으로 적용하는 턴키 솔루션을 제공
- (Google) Gemini for Home+Home MCP와 같이 AI Agent가 실제 집을 직접 제어하는 가장 명확한 Agent-to-Home Interface를 구축
  - 2025년 공개된 Gemini for Home은 기존 Google Assistant를 생성형 AI 기반으로 고도화해 자연어·문맥을 이해하고 여러 홈 기기에 걸친 복잡한 작업을 수행하도록 설계됐으나, 2026년에는 여기에서 한 단계 더 나아가 Google Home MCP(Model Context Protocol) Server를 Early Access로 공개
  - Home MCP를 이용하면 AI Agent가 실제 Google Home 환경에서 집·공간 구조 조회, 기기·영역·기능 검색, 실시간 상태 확인, 기기 제어, 과거 상태·이벤트 분석 등을 수행
  - Reasoning(Gemini)+Context(Home Graph)+Action Interface(MCP)의 구조로, AI가 집에 대해 답변하는 수준에서 실제 물리적 공간을 읽고 행동하는 Agent로 이동

- (Amazon) Alexa+는 생성형 AI를 기반으로 한 차세대 개인 AI Assistant로, 스마트홈에서 외부 생활서비스까지 실행
  - 스마트홈에서 Philips Hue·Roborock 등 기기를 제어하는 동시에, OpenTable 예약, Uber Eats 주문, Amazon Fresh 쇼핑, 서비스업체 예약 등 외부서비스까지 연결. 특히, Alexa+에 Agentic Capability를 도입해, 예를 들어 오븐이 고장 났을 때 사용자를 대신해 웹에서 수리업체를 찾고 인증·예약까지 완료하는 시나리오를 제시
  - Home Agent ↔ Commerce / External Services까지 범위를 확대하고 있으며, AI 홈 에이전트가 주거 플랫폼의 서비스 거래 인터페이스로 진화하는 모델로 분석
- (Midea) 2026년 IFA에서 Midea는 SMART MASTER라는 AI 기반 Home Ecosystem을 공개. 핵심에는 AI Agent가 있으며 140개 언어, 최대 8m 음성인식, 0.4초 응답을 지원하고 지속적인 자연어 대화를 통해 사용자의 의도를 이해. 에어컨·냉장고·오븐뿐 아니라 앱·차량·스마트스피커 등 다양한 접점에서 접근
  - AI Agent 아래에 Comfort Agent(공조·습도·세탁 등 쾌적환경), Health Agent(식재료·메뉴·조리 연계), Efficiency Agent(태양광·전력·가전 에너지 최적화), Service Agent(유지보수·고장·AS 관리) 등 역할별 전문 Agent를 구성
  - 향후 AI 홈의 구조가 단일 Assistant보다 Master Home Agent→ Energy Agent / Health Agent /Comfort Agent / Service Agent와 같은 멀티-에이전트 Residential Platform으로 발전할 가능성을 보여줌
- (Haier) AWE 2026에서 기존 스마트홈의 앱·음성 명령 의존도를 줄이고 공간이 인간의 필요를 자연스럽게 인지하고 반응하는 주거환경을 강조. AI Vision 2.0은 단순 시각인식을 넘어 복잡한 상황을 이해하고 더 빠르게 반응하도록 발전
  - Voice Command→Visual Perception→Context Understanding→Autonomous Response의 흐름을 강조하고 있으며, 궁극적으로는 사용자가 집을 조작하지 않아도 되는 스마트홈을 지향
- (중국 국가시장감독관리총국·국가표준화관리위원회) 2026년 8월 27일 GB/Z 228-2026「人工智能家居大模型技术要求」을 발표
  - 중국전자기술표준화연구원(CESI)을 중심으로 Midea, Haier, Hisense, China Mobile, iFlytek, Dahua, 중산대학 등이 참여. 즉 가전·통신·AI·영상 사업자가 공동으로 가정용 AI 모델의 기술틀을 마련
  - 표준은 Home Large Model(家居大模型)을 대규모 가정·스마트홈 분야 데이터를 기반으로 학습하고, 멀티모달 이해·추론·의사결정 능력을 갖춰 스마트홈에 적용되는 AI 모델로 정의. Home Large Model은 가정 전체에서 발생하는 다양한 정보를 통합적으로 이해하는 Home Foundation Model / Home Intelligence에 가까운 개념

- 家庭智能中枢系统(Home Intelligent Central System)가 AI 홈 에이전트의 핵심 구조로, 표준에서는 이를 영상·음성 등 감각신호를 이해·추론·의사결정·언어 등의 인지정보로 변환하고, 가정 내 연결된 기기를 지능적으로 제어하며, Edge Computing과 Data Storage 능력까지 갖춘 시스템으로 정의(Multimodal Perception→Home Large Model→Understanding / Reasoning→Decision Making→Device Control)
- AI 홈 에이전트를 국가 차원의 기술 아키텍처로 표준화한 것으로, 가전·센서→가정 네트워크→Home Large Model→Home Intelligent Central System→Smart Home Applications이라는 산업 공통 아키텍처를 국가표준으로 정리

05 건설 산업의 사업모델 및 경쟁 구조 변화

- AI 홈 에이전트의 확산은 지능형 주거 플랫폼과 맞물려 건설 산업의 경쟁 구조를 공간을 만들어 판매하는 산업에서 공간 위에서 지속적으로 플랫폼과 서비스를 운영하고, AI 기반 거주 경험(UX)를 제공하는 사업으로 전환시키고 있음. 이는 건설사가 향후 단순 시공자가 아니라, 주거 플랫폼·서비스 생태계의 운영자가 될 수 있음을 보여주는 것으로 분석됨
- (건설사에서 플랫폼 사업자로의 전환) 기존 주택사업은 기본적으로 토지 확보→설계·시공→분양→입주를 중심으로 한 일회성 사업모델임. 그러나, AI 홈 에이전트가 확산되면 건설사가 공급하는 것은 물리적인 주택만이 아니라 입주 후에도 지속적으로 서비스가 제공·업데이트되는 지능형 주거 플랫폼으로 확대될 가능성이 높음
  - 이는 건설사의 역할이 건설·분양 사업자→주거 플랫폼 운영자→주거 서비스 생태계 사업자로 확장되는 변화로 볼 수 있으며, 향후 건설사의 경쟁 단위가 아파트 단지에서 주거 플랫폼의 가입자·생태계·서비스 규모로 확대될 것으로 예상됨. 또한, AI 기반 주거 플랫폼 자체가 별도의 B2B/B2C 사업으로 발전할 가능성도 매우 높은 것으로 분석됨
- (지능형 홈이 옵션에서 필수 인프라로 전환) 기존 지능형 홈은 월패드, 모바일 앱, 스마트 조명, 홈IoT 가전 등 선택형 옵션 또는 부가설비에 가까웠으나, AI홈 에이전트가 사용자의 행동을 인식하고 공간 전체를 제어하려면 단순 IoT 기기만으로는 부족. 주택 자체에 센서→네트워크→홈게이트웨이→AI 허브→각종 설비·가전의 연결이 필수적. 따라서, AI 홈 에이전트는 향후 전기·통신·냉난방처럼 주택 설계 단계부터 고려해야 하는 건축 인프라로 이동할 가능성이 높은 것으로 분석됨
  - 향후 AI 홈 에이전트의 적용 여부가 고급 옵션 선택 여부가 아니라 건축물의 기본적인 지능형 성능을 평가하는 요소가 될 수 있을 것으로 예상되며, 건설사의 설계·MEP·통신·홈네트워크 단계부터 AI 홈 에이전트가 반영될 필요가 있음

- (지능형 홈 경쟁에서 주거 서비스 경쟁으로 전환) 홈 IoT 기술 표준화, Matter와 같은 상호운용성 확대, AI 홈 에이전트의 확산으로 단순한 가전·기기의 작동 기능만으로는 차별화하기 어려워짐. 따라서, 경쟁의 중심이 기기 제어에서 AI 기반의 에너지→보안→주차→헬스케어→돌봄→커뮤니티→유지보수→생활 서비스 등으로 빠르게 확대될 것으로 예상됨
  - 지능형 홈의 경쟁이 기술 경쟁에서 서비스 포트폴리오 경쟁으로 전환될 것으로 예상되며, 가전·기기의 종류와 기능보다는 입주 후 제공되는 서비스의 종류, 지속성, 연계성이 중요해질 것으로 예상됨. 건설사·가전사·통신사·보안사·모빌리티·헬스케어 기업이 동일한 주거서비스 시장에서 경쟁·협력 하면서 산업 간 경계는 약화될 것으로 예상됨
- (AI 홈 에이전트가 지능형 아파트 경험을 결정) 현재는 사용자가 각각의 앱이나 월패드에서 서비스를 찾아 실행하지만, AI 홈 에이전트가 도입되면, 사용자→AI 홈 에이전트→홈 플랫폼·설비·서비스라는 구조로 변화. AI 홈 에이전트가 사용자의 생활패턴과 상황을 파악하고 필요한 서비스를 먼저 제안하거나 실행한다면, AI 홈 에이전트가 아파트 서비스를 경험하는 가장 중요한 접점이자 인터페이스가 됨
  - 따라서, 향후 래미안·자이·힐스테이트 등의 브랜드 경험도 건축물의 디자인뿐만 아니라 그 브랜드의 AI 홈 에이전트가 얼마나 똑똑하고 편리하게 생활을 관리해주는가에 의해 좌우될 가능성이 높음. AI 홈 에이전트는 단순 명령 수행을 넘어 사용자의 상황과 공간을 이해해 최적화된 서비스를 구성하여 제안하거나 자율적으로 실행하는 방향으로 진화
- 종합하면, AI 홈 에이전트의 확산으로 건설사들은 플랫폼 사업자로서 입지가 강화되며, 지능형 홈은 더 이상 옵션이 아니라 필수적인 건축 인프라로 자리잡게 될 것으로 예상됨. 또한, 가전·기기의 기능 중심 차별화에서 에너지·보안·헬스케어·주차·로봇·생활서비스 등 지속적 서비스 경쟁으로 변화하며, AI 홈 에이전트가 주거 브랜드의 핵심 인터페이스로 자리매김 할 것으로 예상됨

그림 2. AI 홈 에이전트로 인한 건설 산업 사업모델·경쟁환경 변화



출처 : 한국AI스마트홈산업협회

06 시사점

- AI 홈 에이전트의 확산으로 지능형 홈의 경쟁 축이 연결 자동화에서 자율적 판단·실행으로 이동할 것으로 예상됨. 따라서, AI 홈의 경쟁력은 연결성보다 상황 이해도와 자율 행동력으로 이동하고 있으며, AI 홈 에이전트가 지능형 홈의 새로운 운영체제 역할을 담당하게 될 것으로 분석됨
- AI 홈 에이전트는 가전·기기·IoT 제품을 넘어 건축물의 기본 인프라로 내재화될 것으로 예상됨. AI 홈 에이전트는 아파트에 추가하는 기능에서 AI를 전제로 설계하는 건축 인프라로 변화하고 있으며, 향후, 주택의 지능화 수준 자체가 건축물의 품질과 상품성을 평가하는 핵심 기준으로 자리잡을 것으로 분석됨
- 건설사의 사업모델이 주택 판매에서 지속적 주거 플랫폼·서비스 운영으로 전환될 것으로 예상됨. AI 홈 에이전트의 확산은 건설사를 집을 짓고 판매하는 기업에서 입주 이후에도 고객과 연결되는 주거 플랫폼 사업자로 전환시키고, 주거 플랫폼 자체가 새로운 B2B·B2C 수익모델로 발전할 것으로 분석됨

- AI 홈 에이전트가 아파트 브랜드의 핵심 고객접점이 되면서, 경쟁구조가 공간·상품에서 주거 경험 중심으로 재편될 것으로 예상됨. AI 홈 에이전트는 주거서비스를 이용하는 핵심 인터페이스로 부상하고 있으며, 향후, 아파트의 브랜드 경쟁 역시 물리적 주택 품질을 넘어 AI의 지능·개인화·서비스 연계 수준이 결정하는 주거 경험 경쟁으로 확대될 것으로 분석됨

Ⅲ. 지능형 홈 가전 · 디바이스 동향



Home LLM·SLM이 이끄는 지능형 홈의 진화

01 홈 LLM·SLM의 부상

- 지능형 홈에서 AI의 역할은 기존의 음성명령 인식 및 규칙 기반 자동화에서 벗어나, 사용자의 자연어와 생활 맥락을 이해하고 여러 가전·설비를 연계해 스스로 판단·실행하는 방향으로 빠르게 진화. 이에 따라, 범용 생성형 AI를 그대로 사용하는 방식보다는 가정이라는 특정 환경에 최적화된 Home LLM과 Home SLM이 지능형 홈의 핵심 AI 모델로 부상
- (음성비서·규칙 기반 자동화에서 맥락 이해형 AI로 진화) 생성형 AI와 LLM이 홈에 적용되면서 사용자의 입력 방식이 명령(Command)→의도(Intent)·목표(Goal) 중심으로 전환
  - 기존 스마트홈은 “거실 불 켜줘”, “에어컨 24도로 설정해줘”처럼 사용자가 정확한 명령을 입력하면 특정 기기가 반응하는 구조가 중심. 여러 기기를 동시에 작동시키는 경우에도 사용자가 미리 조건과 동작을 정의하는 Routine·Rule 기반 자동화가 일반적
  - LLM 기반 홈 AI는 사용자의 명령을 기반으로 실내 온도 조절→조명 설정→조리기기 준비→음악·엔터테인먼트 환경 구성 등 필요한 작업을 추론하고 여러 기기와 서비스를 연계
- (범용 LLM에서 가정 특화 Home LLM으로 진화) 범용 LLM을 그대로 적용하기보다는 가정이라는 Vertical Domain에 최적화한 Home LLM 개발이 확대
  - 지능형 홈에서는 일반적인 지식 질의응답 능력보다 가전 상태, 공간 구조, 사용자 행동, 생활패턴, 센서 데이터 등을 이해하는 능력이 중요
  - 일반 지식·대화 중심의 범용 LLM에서 사람·공간·가전·서비스·생활맥락을 이해하는 Home LLM으로 AI 모델의 전문화가 진행
- (Home SLM의 부상) AI 기반 지능형 홈의 기능을 클라우드 LLM에 의존하기는 어려움. 음성·영상·출입정보·생활패턴·가전 사용기록 등 민감한 개인 데이터가 지속적으로 생성되며, 조명·냉난방·도어락과 같은 기기 제어는 매우 빠른 응답도 요구되기 때문임

- 지능형 홈 AI에는 저지연(기기 제어를 클라우드 왕복 없이 빠르게 처리), 프라이버시(음성·생활패턴 등 민감 정보를 가정 내부에서 처리), 연결 안정성(인터넷이 끊겨도 기본적인 AI 기능 수행), 저비용(반복적인 단순 명령에 대규모 LLM 호출 최소화), 개인화(특정 가정과 사용자의 습관을 로컬에서 지속 학습) 등의 요구가 높아지고 있으며, 이에 따라, 경량화된 언어모델인 Home SLM을 홈허브·게이트웨이·가전 등에 배치하는 연구가 확대되고 있음
- 2025년 HomeLLaMA 연구에서는 로컬에서 구동되는 SLM 기반 개인화 스마트홈 어시스턴트를 제시[1]하고 있으며, 2026년 AdaHome 연구에서도 역시 로컬 SLM을 기반으로 스마트홈 명령을 처리하는 구조를 제안[2]

● (Home LLM과 Home SLM의 역할 분화) 향후, 지능형 홈은 하나의 거대한 LLM이 모든 작업을 처리하는 구조보다는 LLM과 SLM이 역할을 나눠 수행하는 구조로 발전할 것으로 예상

- 2026년 IoTGPT 연구에서는 LLM 기반 IoT 제어가 복잡한 자연어 명령을 처리하는 데 유용하지만, 반복적인 LLM 호출은 지연시간·비용·신뢰성 측면의 한계가 있다고 지적하고, 기존에 학습한 하위 작업을 재사용해 LLM 호출을 줄이는 방식을 제안[3]

02 Home LLM·SLM의 개념 및 차이

● Home LLM과 Home SLM은 모두 가정 내 AI 에이전트의 핵심 지능을 담당하지만, 모델 규모·배치 위치·처리 대상·응답 특성·개인정보 보호 수준에서 역할이 다름. 두 모델을 대체관계라기보다 Home LLM은 복잡한 판단과 조정, Home SLM은 빠른 로컬 실행과 개인정보 보호를 담당하는 상호보완 구조로 보는 것이 핵심

● (Home LLM) 가정에서의 복잡한 추론과 다양한 서비스 오케스트레이션을 담당. Home LLM은 범용 LLM을 가정·가전·주거환경이라는 특정 도메인에 맞게 특화한 대규모 언어모델. 자연어 이해→맥락 이해→복합 추론→작업 계획→다중 기기·서비스 오케스트레이션이 Home LLM의 핵심 역할

- 일반적인 LLM이 광범위한 지식과 자연어 대화를 처리한다면 Home LLM은 여기에 가전 상태, 실내환경, 가족의 생활패턴, 공간정보, 홈IoT 및 외부 서비스에 대한 이해를 결합
- (Haier HomeGPT) 가정 분야의 Vertical LLM으로 정의하고 있으며, 가정생활 데이터와 가전 운행정보를 바탕으로 사용자의 행동, 기기 상태, 환경 변화의 관계를 이해하도록 개발. (LG전자

1) Towards Privacy-Preserving and Personalized Smart Homes via Tailored Small Language Models(2025). https://arxiv.org/abs/2507.08878
2) AdaHome: An Adaptive Smart Home Assistant using Local Small Language Models(2026). https://arxiv.org/abs/2607.18034
3) Leveraging LLMs for Efficient and Personalized Smart Home Automation(2026). https://arxiv.org/abs/2601.04680

ThinQ Claw) 자연어를 통해 사용자의 의도와 상황을 이해하고 관련 기기와 서비스를 연결해 필요한 작업을 수행

- (Home SLM) 저지연·로컬 실행·개인정보보호 담당. 상대적으로 작은 규모의 언어모델을 홈허브, 게이트웨이, 가전 등의 로컬 또는 엣지 환경에서 직접 실행하는 구조. Home LLM에 비해 추론 범위는 제한적일 수 있지만, 모델이 작기 때문에 연산 요구량과 메모리 사용량이 적고 클라우드 서버를 거치지 않고 즉시 처리할 수 있다는 것이 장점
  - Home SLM은 음성, 영상, 출입기록, 위치, 생활패턴, 건강·수면 데이터 등 스마트홈이 다루는 정보는 민감도가 높기 때문에 가정 환경에서 매우 중요. 로컬 이해→빠른 판단→기기 직접 제어→개인화→민감정보 보호가 Home SLM의 핵심 역할

표 4. Home LLM과 Home SLM 비교

Home LLM	구분	Home SLM
복잡한 이해·추론·계획·대화·서비스 조정	핵심 역할	실시간 및 로컬 명령 실행·기기 제어·개인화
상대적으로 대규모	모델 규모	상대적으로 소규모·경량
주로 Cloud·Edge	처리 위치	Home Hub·Device·Edge
네트워크·클라우드 처리에 따라 지연 가능	응답 속도	로컬 처리로 상대적으로 빠름
높음	연산·전력 요구	상대적으로 낮음
복합 요청, 다중 서비스 연계, 장기 계획	적용 영역	반복적·단순 명령, 실시간 자동화
높은 추론력·범용성	강점	저지연·저비용·개인정보보호
외부 정보·다양한 서비스	주요 데이터	개인 생활패턴·가정 내부 데이터
사용자·외부 서비스 정보를 종합	개인화	가정 내부 생활패턴의 지속적 학습
클라우드 전송 시, 보호체계 필요	개인정보보호	로컬 처리를 통해 외부 전송 최소화
두뇌(Brain)·플래너(Planner)	홈에서의 역할	로컬 실행(Local Executor)·개인정보보호(Privacy)

출처 : 한국AI스마트홈산업협회

- Home LLM과 Home SLM은 적용 영역에서 서로 다르게 분화됨. Home LLM은 사용자의 추상적인 명령에 대해 일정, 사용자(방문자) 특성, 날씨, 실내환경, 조명, 냉난방, 가전, 일정 서비스 등을 종합하고 여러 행동의 순서를 계획하지만, Home SLM은 반복적이고 정확한 명령에 대해 로컬 자동화 계층에서 빠르고 효율적으로 실행
  - Home SLM은 단순히 상대적으로 작고 경량의 AI라는 점보다 가정의 민감한 데이터를 집 밖으로 보내지 않고 처리할 수 있다는 점에서 개인정보 보호에 특히 유리. 가정 내에서는 음성 및 대화 내용, 영상·센서 정보, 가족의 재실 여부와 생활패턴, 수면 및 건강정보, 출입·보안 기록, 가전 사용내역 및 에너지 소비, 개인별 선호도 등의 데이터가 지속적으로 생성되기 때문에, 사용자 프로필과 홈 구성을 로컬 SLM에서 지속적으로 관리하고 개인화하는 것이 중요

- 향후, 지능형 홈에서는 Home LLM과 Home SLM 두 모델이 경쟁하기 보다는 분산적으로 협력하는 방향으로 진화할 것으로 예상됨
  - Home LLM은 복잡한 자연어 이해→다단계 추론→여러 서비스 간 조정→외부 정보와 서비스 활용→새로운 행동계획 생성 등을 담당하고, Home SLM은 센서·가전·사용자 상태의 로컬 이해→반복적인 명령 및 자동화 처리→민감정보 로컬 처리→즉각적인 기기 실행을 담당할 것으로 예상됨
  - 로컬에서 충분히 해결되지 않는 일부 요청의 경우에는 개인정보를 최소화해 원격 LLM을 활용하는 하이브리드 구조도 고려해 볼 수 있음

03 Home LLM의 확산과 가정 특화 AI 모델의 등장

- 생성형 AI가 지능형 홈에 적용되기 시작하면서 초기에는 범용 LLM의 자연어 이해·질의응답 능력을 스마트홈 인터페이스에 접목하는 수준이 중심이었다면, 최근에는 가정이라는 특정 공간과 생활 맥락을 이해하도록 특화된 Vertical Home LLM으로 발전하는 흐름이 뚜렷해지고 있음
  - 일반적인 범용 LLM은 폭넓은 지식과 대화 능력에는 강점이 있지만, 실제 가정에서는 단순 대화 이상의 능력이 필요함. AI가 가전의 현재 상태, 사용자의 생활패턴, 공간별 환경정보, 가족 구성과 선호, 센서 데이터, 외부 서비스를 함께 이해해야 하기 때문임
  - 따라서, Home LLM은 범용 LLM(자연어 이해·일반지식·대화)→Domain-adapted LLM(가전·지능형 홈 관련 지식 강화)→Vertical Home LLM(사람+공간+기기+환경+생활서비스 이해 기반 홈 시나리오의 생성과 실행)으로 진화할 것으로 예상됨. 즉, LLM이 단순한 대화 인터페이스에서 집 전체를 이해하고 여러 기기와 서비스를 조정하는 홈 인텔리전스의 중심 엔진으로 이동한다는 의미
- (Haier Home GPT) 2024년 AWE에서 HomeGPT를 '가정 수직 영역 모델(家庭垂域模型)'로 공개. HomeGPT를 탑재한 'Smart Home Brain(智家大脑)'의 핵심 능력을 이해력·감지력·진화 능력으로 설명하고 있으며, HomeGPT를 통해 가정에서 보다 깊은 의미 이해와 자연스러운 상호작용을 구현한다고 밝힘
  - 단순히 ChatGPT와 같은 일반적인 질의응답 모델을 가전에 연결한 것이 아니라, 가정생활이라는 Vertical Domain에 특화했다는 점이 특징. 사용자의 요청에 대해 답변이나 설명을 알려주는 데에서 끝나지 않고, 최적화된 방법을 자동으로 매칭해 가전 실행까지 연결
  - 즉, 사용자의 의도 이해→주변 환경·상황 이해→적절한 가전·기기 설정 판단→실제 가전·기기 제어 및 실행·생활지원으로 확장한다는 점에서 Vertical Home LLM의 대표 사례로 분석됨
- (LG AI Home) LLM 자체보다 이를 활용해 사람의 생활 맥락을 이해하고 여러 기기와 서비스를 조정하는 AI Agent 구현에 초점. LG AI Home은 LLM 기반 자연어 인터페이스→Contextual Intelligence→Contextual AI Agent로 발전

- 사용자의 일정, 반복적인 생활 루틴, 주거환경 상태, 가전 사용정보, 개인별 선호, 연결된 외부 서비스 등의 정보를 분석하고, 이를 바탕으로 사용자가 직접 모든 명령을 내리기 전에 적절한 행동을 추천하고 여러 기기·서비스를 조정. 이는 명령 기반 구조에서 상황·맥락 기반 입력을 이해하고 필요한 행동을 AI가 판단하는 구조로바뀌는 것을 의미
- 2026년 공개한 ThinQ Claw는 Contextual Agent의 구체화된 형태. ThinQ Claw는 텍스트 기반 AI 에이전트로, 단순히 사용자의 문장을 이해하는 데 그치지 않고 의도(Intent)와 맥락(Context)을 파악한 후 필요한 기기와 서비스를 연결하고 작업을 수행. ThinQ Claw는 개별 사건을 따로 처리하지 않고 사용자 삶의 맥락 속에서 정보를 해석
- 특히, ThinQ Claw는 사용자 발화→의도·상황 이해→필요 작업 판단→관련 서비스 검색·연결→복수 기기 조정→행동 실행→사용자 선호 기억의 기능이 중요하며, 이러한 구조는 LLM이 단순한 자연어 번역기가 아니라 홈 에이전트의 추론·계획 엔진으로 발전하고 있음을 의미
- 한편, ThinQ ON은 AI가 실제 공간과 연결되는 허브임. ThinQ ON은 AI Home의 중앙 허브 역할을 하며, 다양한 가전, IoT 센서, 외부 플랫폼 및 서비스를 연결. ThinQ ON은 AI Home 생태계의 central node이며, Contextual Agent가 무엇을 해야 하는지 판단한다면, ThinQ ON은 실제 가전·기기·서비스와 연결하는 구조

- Haier HomeGPT와 LG AI Home은 경쟁적인 기술이라기 보다는 Home AI가 발전하는 두 개의 핵심 방향으로 분석됨. Haier가 AI 모델 자체를 가정에 특화시키는 방향이라면, LG AI Home은 AI 모델을 이용해 생활 맥락을 이해하는 에이전트 시스템을 구축하는 방향으로 분석됨

표 5. LG Home AI와 Haier HomeGPT 비교

LG AI Home	구분	Haier HomeGPT
Contextual AI Agent	핵심 개념	Vertical Home LLM
LLM·AI를 활용한 홈 에이전트	출발점	가정 도메인 특화 LLM
사용자 생활 맥락·상황 이해	중심 기능	가정 지식·가전·시나리오 이해
일정, 루틴, 환경, 기기 상태, 선호	주요 데이터	가정 지식, 가전 상태, 생활 시나리오
상황 판단·서비스 조정	AI 역할	홈 전문지능 제공
ThinQ ON·Homey·ThinQ 생태계	기기 연결	Smart Home Brain·Haier 생태계
LLM → Contextual Intelligence → Agent	발전 방향	Vertical LLM → Smart Home Brain

출처 : 한국AI스마트홈산업협회

04 Home SLM과 온디바이스·로컬 AI 확대

- 지능형 홈이 AI 에이전트 중심으로 발전하면서 모든 요청을 클라우드의 대규모 LLM에 의존하는 방식에는 한계가 커지고 있음. 가정에서는 음성·영상·출입·생활패턴·가전 사용정보 등 민감한 데이터가 지속적으로 발생하고, 조명·냉난방·도어락과 같은 제어는 빠른 응답과 높은 안정성이 요구되기 때문임. 이에 따라 가전·홈허브·게이트웨이 등 가정 내부에서 직접 구동되는 Home SLM과 로컬 AI의 중요성이 확대되고 있음
- (클라우드 중심에서 Cloud-Edge-Device 분산 구조) Cloud LLM(복잡한 추론·외부 지식·다중 서비스 연계)→Home Hub·Gateway SLM(사용자 의도 해석·상황 판단·로컬 오케스트레이션)→Device AI(센서 분석·실시간 제어·단순 자동화) 구조가 주목
  - 기존 LLM 기반 스마트홈은 사용자 명령과 홈 상태 정보를 클라우드로 전송한 뒤 결과를 받아오는 구조가 일반적이었으나, 이 방식은 네트워크 지연, 통신 장애, 지속적인 API 비용, 개인정보 외부 전송 등의 문제가 발생
  - 따라서, 모든 연산을 클라우드에 집중하기보다 처리 난이도와 데이터 민감도에 따라 AI 기능을 분산하는 구조로 발전하고 있으며, 실시간 응답, 네트워크 안정성, 개인정보보호, 비용·자원 효율성을 고려한 Home SLM이 부상
- (AdaHome) 2026년 발표된 연구로, 로컬 SLM을 활용해 지능형 홈 명령을 효율적으로 처리하면서 장기적인 개인화까지 구현하려는 시스템으로, 기존 LLM 기반 스마트홈 어시스턴트가 모든 요청에 복잡한 추론을 적용해 계산량과 지연이 커지는 문제에서 출발
  - 모든 명령에 동일한 추론을 적용하지 않는 구조로 Intent-aware Planning, 즉 사용자 명령의 난이도에 따라 처리 방식을 다르게 선택하는 것이 AdaHome의 핵심. 명령 입력→의도·난이도 판단→단순 명령(Fast Path)→복합·모호 명령(Reasoning Path)으로 구분하며, 연구에서는 이를 통해 모든 요청에 무거운 추론을 수행하는 방식보다 연산 효율을 높임

- 제한된 자원에서도 추론 가능하도록 최적화함. AdaHome은 복잡한 요청을 처리할 때도 긴 Chain-of-Thought 대신 Chain-of-Draft라는 경량 추론방식을 활용. 충분한 의사결정을 수행하되 불필요하게 긴 추론 토큰을 생성하지 않는 것이 핵심. 이러한 접근은 특히 홈허브나 엣지 기기처럼 GPU·메모리·전력이 제한된 환경에서 중요. 실험 결과 AdaHome은 직접적인 명령에서 86.7%의 정확도를 기록했고, 비교 시스템 대비 최대 3배 낮은 지연시간을 보임. 또한, 모호한 명령에서도 낮은 연산비용으로 경쟁력 있는 성능을 유지
- 사용자 피드백을 통한 장기 개인화가 특징. 단순 명령 수행이 아니라 사용자의 선호를 지속적으로 반영하는 적응형 구조로, 시스템이 사용자의 명령·선호에 대한 피드백을 축적해 향후 비슷한 상황에서 자동으로 적용. AdaHome은 이를 위해 매번 프롬프트에 사용자 이력을 길게 추가하거나 모델 전체를 재학습하는 대신 별도의 preference adaptation mechanism을 사용. 연구 결과 다중 턴 환경에서 AdaHome은 88%의 선호 일관성(preference consistency)을 기록한 반면, 단순 prompt augmentation 방식은 52.5%인 것으로 나타남
- AdaHome은 Home SLM이 단순한 작은 LLM이 아니라, 제한된 홈 엣지 환경에서도 사용자의 상황과 요청 난이도에 따라 연산량을 조절하고, 장기적인 개인화까지 제공할 수 있는 적응형 AI로 발전할 수 있음을 보여주는 사례로 분석됨

● (HomeLLaMA) 2025년 발표된 연구로, 지능형 홈에서 개인정보 보호와 개인화를 동시에 달성하기 위해 맞춤형 SLM을 온디바이스에서 운영하는 구조를 제시

- 기존 클라우드 LLM 구조의 개인정보 문제에 대해 정보(사용자 명령, 개인 프로필, 가정 내 기기 목록, 방·공간의 구성, 사용자 선호, 생활 패턴 등)가 원격 서버에 지속적으로 전달될 경우 개인정보 노출 위험이 존재한다고 지적. 핵심 데이터를 집 밖으로 보내지 않고 로컬 SLM이 직접 처리하는 방식을 제안
- 일반적인 SLM을 단순히 설치하는 것이 아니라, 각 가정에 맞게 특화된 tailored SLM을 활용하는 것이 특징. 대규모 LLM의 능력을 학습 단계에서 활용(높은 수준의 지식·능력 제공, Home SLM 학습·지식 이전)하되, 실제 서비스 단계에서는 가정 내부의 작은 모델이 주된 역할을 수행(사용자 프로필 저장, 홈 구성 이해, 사용자 선호 학습, 로컬에서 개인화된 응답 생성)하도록 하는 구조
- HomeLLaMA는 배포 이후에도 사용자 프로필과 로컬 SLM을 지속적으로 업데이트함. 이를 통해, 사용자 행동→피드백 축적→로컬 프로필 업데이트→개인화된 추천·제어의 루프를 형성. 이러한 개인화 과정이 가정 내부에서 이뤄진다는 것이 중요. 따라서, 기존의 강화된 개인화로 클라우드로 전송되는 개인정보가 많아지는 구조에서 HomeLLaMA는 강화된 개인화에도 불구하고, 클라우드로 전송되는 개인정보는 최소화하는 구조

- 한편, 모든 요청을 반드시 로컬에서만 처리하는 것이 아니라, 로컬 SLM의 답변이 충분하지 않을 경우를 대비해 PrivShield라는 구조를 함께 제안. 사용자가 원할 경우 덜 민감한 요청만 원격 LLM으로 전달하고, 민감한 정보는 로컬에 유지. 민감하고 일상적인 요청은 HomeLLaMA에서 로컬로 처리하고, 복잡하지만 상대적으로 비민감한 요청에 대해서는, 필요 시 PrivShield를 통해 Cloud LLM을 활용하는 하이브리드 모델을 제안. 이는 향후 Home LLM + Home SLM 구조에서도 중요한 설계 원칙이 될 수 있을 것으로 분석됨

표 6. AdaHome과 HomeLLaMA의 비교

AdaHome	구분	HomeLLaMA
2026	발표	2025
효율적인 로컬 추론·적응	핵심 목표	개인정보 보호·개인화
Intent-aware Planning	핵심 기술	Tailored Local SLM
요청 난이도별 처리경로 분리	특징	사용자·가정별 모델 특화
사용자 피드백 기반 선호 적응	개인화	로컬 사용자 프로필 지속 갱신
로컬 SLM 중심	클라우드 의존	로컬 중심 + 선택적 Cloud LLM
효율성·저지연	주요 가치	프라이버시·개인화
Home SLM의 실행 효율성 입증	의미	Home SLM의 개인정보 보호 가치 입증

출처 : 한국AI스마트홈산업협회

- Home SLM과 로컬 AI의 확대는 지능형 홈의 AI 구조가 Cloud-first에서 Local-first+ Cloud-assisted 구조로 변화할 가능성을 보여주는 것으로 분석됨. 향후, Device·Hub SLM에서는 실시간 제어·민감정보·개인화를 처리하고, Edge·Home Agent에서는 가정의 전체 상황을 조정하고, Cloud LLM에서는 복잡한 추론·외부 지식·다중 서비스 연계를 담당하는 계층적 구조로 발전할 것으로 예상됨

05 Home LLM과 Home SLM의 결합

- 향후, 지능형 홈의 AI 구조는 하나의 거대한 모델이 모든 기능을 처리하기보다, Home LLM과 Home SLM이 역할을 분담하는 계층형 구조로 발전할 것으로 예상됨. 이는 가정 내 AI가 동시에 요구하는 기능이 서로 상충하기 때문임. 복잡한 추론과 외부 서비스 연계에는 대규모 모델이 유리하지만, 실시간 기기 제어와 개인정보 보호에는 로컬에서 작동하는 경량 모델이 더 적합

- 클라우드 기반 LLM은 자연어 이해, 복합 추론, 계획 수립, 외부 서비스 연계에는 강점이 있지만, 모든 요청을 클라우드로 보내 처리할 경우 지연시간, 비용, 네트워크 의존성, 개인정보 전송 문제가 발생할 수 있기 때문에, 단일 거대모델보다 역할 분담형 구조가 필요
  - HomeLLaMA 연구는 기존 LLM 기반 스마트홈이 사용자 명령뿐 아니라 사용자 프로필과 홈 구성정보까지 원격 서버로 보내는 구조를 문제로 지적하고, 이를 보완하기 위해 로컬 SLM+선택적 원격 LLM 구조를 제안. 즉, 평상시에는 로컬 SLM이 개인화된 서비스를 처리하고, 로컬 응답으로 부족한 경우에만 덜 민감한 요청을 원격 LLM에 전송
  - AdaHome 역시 모든 스마트홈 명령에 동일한 무거운 추론 과정을 적용하는 것이 비효율적이라고 보고, 요청의 난이도에 따라 단순 명령은 가벼운 처리 경로로, 해석이 필요한 명령은 경량 추론 경로로 분기하는 방식을 제시. 이는 향후 지능형 홈에서 모든 문제를 하나의 큰 모델에 맡기지 않는다는 방향성을 보여줌
- Home LLM은 지능형 홈의 Brain·Planner·Orchestrator 역할을 담당하면서, 모호하거나 복합적인 사용자 의도 이해, 여러 단계가 필요한 작업의 계획 수립, 서로 다른 가전·설비·서비스 간 조정, 외부 캘린더·날씨·에너지·콘텐츠 등 서비스 연계, 새로운 상황에 대한 추론과 대응, 여러 로컬 AI·기기를 통합하는 상위 오케스트레이션 등과 같은 복잡한 이해·추론·계획을 담당하는 상위 지능 계층으로 작동
  - 사용자의 일정, 생활루틴, 주거환경, 가전 사용정보 등을 종합해 의도와 맥락을 이해하고 필요한 행동을 추천하며 여러 기기와 서비스를 조정. 단순 기기 제어보다 한 단계 높은 계획·오케스트레이션 기능에 초점
- Home SLM은 가정 내에서 실시간 실행을 담당하면서, 센서·환경정보의 로컬 해석, 조명·냉난방·가전 등의 실시간 제어, 반복적인 사용자 명령 처리, 사용자 취향·생활패턴의 지속적 개인화, 인터넷 연결 없이 기본 기능 수행, 음성·출입·행동패턴 등 민감정보 로컬 처리 등과 같은 센서·기기제어·개인화·민감정보를 담당하는 로컬 계층으로 작동
  - 사용자 프로필, 가정의 구성 정보를 로컬 SLM에 유지하고, 로컬에서 사용자 프로필과 모델을 지속적으로 업데이트해 개인화하고, 제한된 컴퓨팅 환경에서도 적응형 추론과 개인화를 수행
- Home LLM과 Home SLM의 결합을 지능형 홈 전체 아키텍처로 확장하면, Cloud-Edge-Device 계층형 AI 구조가 형성될 것으로 예상됨

표 7. Home LLM과 Home SLM이 결합된 지능형 홈 AI 구조

Cloud (Home LLM/Foundation Model)	Edge/Home Hub (Home SLM/Home Agent)	Device (On-device AI)
고난도 추론	사용자 의도 분류	영상·음성·센서 분석
새로운 작업계획 생성	가정 전체 상황 이해	가전·기기 상태 판단

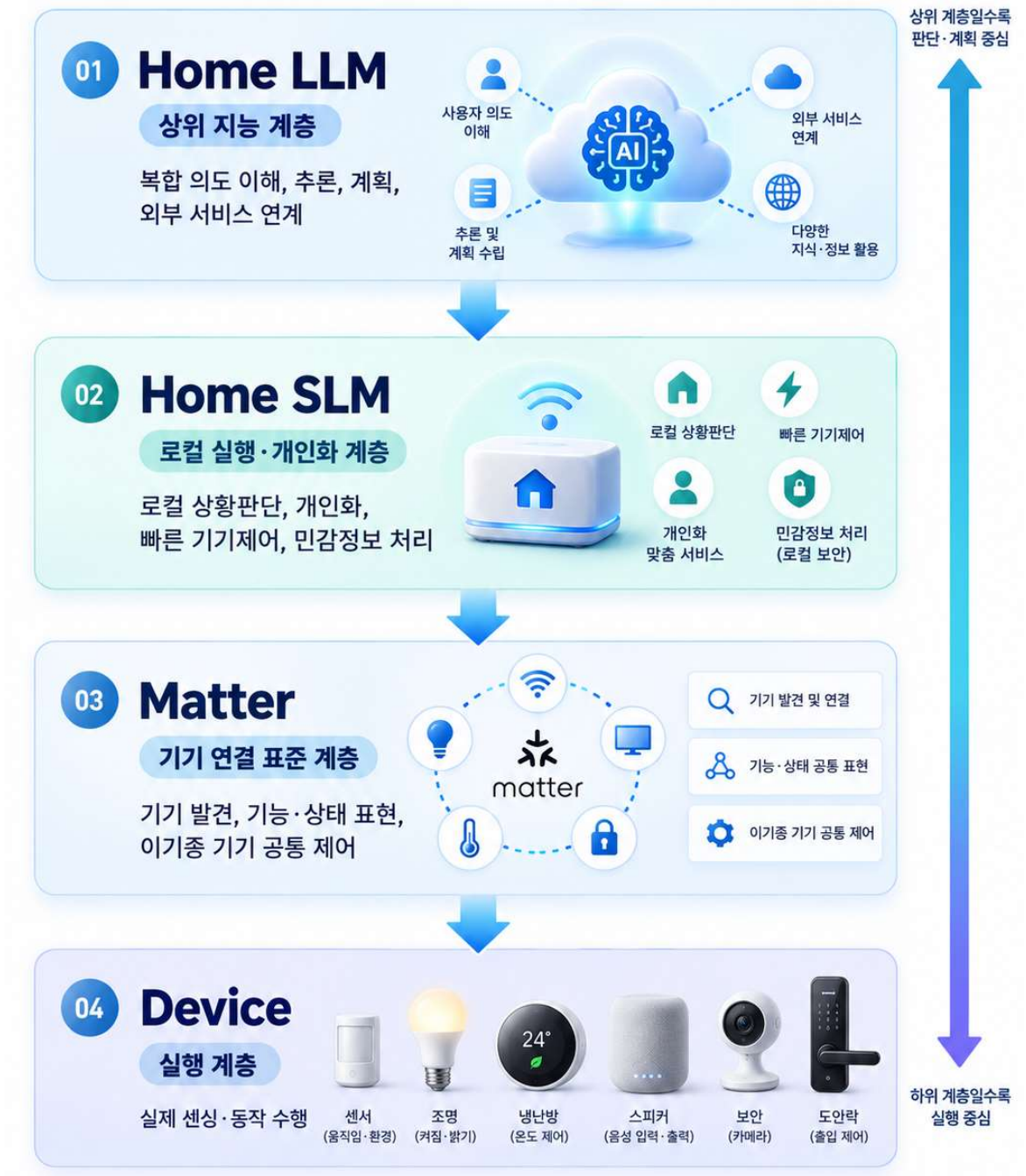
외부 지식 활용	개인화	실시간 자동화
서비스 검색·연계	여러 기기 조정	실시간 가전·기기 제어
멀티에이전트 조정	데이터 필터링·민감 정보 보호	

출처 : 한국AI스마트홈산업협회

06 Matter와 Home LLM·SLM의 결합

- Matter와 Home LLM·SLM의 결합은 향후 지능형 홈의 기본 아키텍처를 설명하는 핵심 구조가 될 것으로 예상됨. Matter가 서로 다른 제조사의 기기를 공통 방식으로 연결·식별·제어하는 표준 계층이라면, Home LLM·SLM은 그 위에서 사용자의 의도와 상황을 이해하고 어떤 기기를 어떻게 움직일지 판단하는 지능 계층을 담당하는 구조임
- Matter는 이기종 가전과 기기를 연결하는 공통언어. IP 기반 스마트홈 표준으로, 서로 다른 브랜드와 생태계의 기기가 보다 일관된 방식으로 연결·동작하도록 설계. Matter의 핵심 가치는 상호운용성, 신뢰성, 보안, 단순성이며, 여러 브랜드의 기기가 네이티브하게 함께 작동하는 것을 목표로 함
  - 단순 통신 프로토콜을 넘어 기기 발견→기기 유형·기능 인식→상태 조회→제어 명령 전달을 공통 구조로 표준화하고 있으며, Matter 1.6에서는 기기가 자신의 기능, 운전 상태, 안전 관련 정보를 생태계에 보다 명확히 전달하도록 개선되었으며, 컨텍스트와 사용자 선호에 따른 제어도 강화됨
- Home LLM·SLM은 Matter 위에서 의미를 해석함. 사용자의 명령, 가정 내 상황, 가전·기기의 작동 순서 등을 판단하여 행동계획으로 변환하고, Matter는 해당 가전·기기들의 기능과 상황을 확인한 뒤, 표준화된 방식으로 제어 명령을 전달하는 역할을 수행
  - 자연어·맥락→Home LLM/SLM이 이해·추론→적절한 기기·기능 선택→Matter가 표준화된 제어 수행의 구조를 가짐
  - Home LLM은 상위 수준에서 사용자의 복합 의도 이해, 여러 방과 기기를 아우르는 계획 수립, 외부 날씨·일정·에너지 서비스 연결, 다수 기기에 대한 복합 명령 생성 등을 담당
  - Home SLM은 Matter 기기와 더 가까운 로컬 계층에서 현재 센서 상태 확인, 반복 명령 처리, 로컬 자동화, 개인화된 설정 적용, 민감정보를 외부로 보내지 않고 처리하는 역할을 담당

그림 3. Home LLM·SLM과 Matter 결합 구조



출처 : 한국AI스마트홈산업협회

- Matter는 기기와 플랫폼이 서로 이해할 수 있게 만드는 공통 연결 언어이고, Home LLM·SLM은 그 위에서 사용자 의도와 상황을 해석해 무엇을 할지 결정하는 판단·지능 계층임. 여기에서 Matter의 전략적 가치는 AI 홈 에이전트가 특정 제조사의 폐쇄형 생태계를 넘어 더 많은 이기종 기기를 제어할 수 있도록 행동 공간을 확장하는데 있음

- Home LLM·SLM과 Matter의 결합 구조의 장점은 AI와 기기 제어 계층을 분리하고, 제조사의 종속성을 낮출 수 있으며, AI 홈 에이전트의 확장성을 높일 수 있음
  - (AI와 기기 제어 계층 분리) AI 모델이 바뀌어도 Matter를 지원하는 기기와 계속 연결될 수 있음
  - (제조사의 종속성을 낮춤) 한 회사의 AI 플랫폼이 다른 제조사의 Matter 기기를 제어할 수 있음
  - (AI 홈 에이전트의 확장성 향상) 새로운 Matter 기기가 추가되면 AI 에이전트의 행동 범위도 자연스럽게 확장
- 종합하면, Matter와 Home LLM·SLM의 결합은 향후 지능형 홈이 AI가 판단하고 표준화된 기기 생태계가 행동하는 구조로 발전할 가능성을 보여줌. Matter가 제조사별로 파편화된 기기 연결과 제어를 공통화하면, Home LLM은 복잡한 사용자 의도와 상황을 이해해 계획을 수립하고 Home SLM은 가정 내부에서 이를 빠르고 안전하게 실행. 이에 따라, 지능형 홈의 경쟁력도 개별 가전의 기능에서 벗어나 AI 모델–홈 플랫폼–Matter–기기를 얼마나 매끄럽게 통합하는가로 이동할 것으로 예상됨

07 개인정보와 보안: Home SLM의 전략적 가치

- 개인정보 보호·보안과 관련하여 Home SLM의 가장 중요한 가치는 단순히 작고 가벼운 모델이라는 데 있지 않음. 가정은 음성·영상·출입·생활패턴·건강·에너지 사용처럼 민감도가 높은 데이터가 상시 생성되는 공간이기 때문에, 이러한 데이터를 가능한 한 집 안에서 처리하는 Privacy Layer, 즉, 개인정보 보호 계층으로서 Home SLM의 전략적 중요성이 커지고 있음
- 가정 내 데이터는 다른 AI 서비스보다 민감도가 매우 높음. 지능형 홈은 사용자의 일상과 물리적 공간을 지속적으로 관찰함. 따라서, 지능형 홈 기기는 네트워크 보안뿐 아니라 정보 프라이버시와 물리적 안전까지 영향을 줄 수 있으며, 음성비서, 카메라, 온도조절기 등 다양한 기기가 민감한 데이터를 수집할 수 있음
  - 가정 내 모든 원천 데이터를 클라우드 LLM으로 지속 전송하는 구조는 개인정보 측면에서 부담이 매우 큼. 기존 LLM 기반 지능형 홈이 개인화 서비스를 위해 사용자 명령, 사용자 프로필, 홈 구성 정보를 원격 서버로 전송하는 구조 자체가 개인정보에 있어 위험 요소임
- 이러한 문제 때문에, 모든 데이터를 클라우드 LLM으로 보내는 구조보다, 가정 내부에서 먼저 처리한 뒤, 필요한 정보만 선택적으로 상위 LLM에 전달하는 구조가 중요해질 것으로 예상됨
  - 카메라·마이크·웨어러블·스마트락·환경센서가 생성하는 대규모 데이터를 모두 클라우드로 보내면 지연, 네트워크 비용, 인터넷 의존성, 전송 과정에서의 프라이버시 위험이 증가함. 반면, Edge AI는 로컬에서 데이터 처리와 추론을 수행해 외부로 나가는 민감 데이터의 양을 크게 줄일 수 있음

- Home SLM은 원시 데이터의 로컬 처리, 민감 정보 제거·비식별화를 통해 데이터 최소화 역할을 담당하는 Privacy Layer로 단순히 로컬에서 답변을 생성하는 것보다 더 적극적인 개인정보 보호가 가능
  - (원시데이터 로컬 처리) Raw Data→Feature·Intent·Summary로 변환한 뒤 외부 전송하는 구조로 데이터 최소화 원칙에 부합
  - (민감정보 제거·비식별화) 이름, 의료기관, 구체적인 개인정보와 같은 민감정보를 로컬에서 제거하고 상위 모델의 추론에 필요한 최소한의 의미 정보만 전달
  - 원시데이터 로컬 처리와 민감정보 제거·비식별화는 현재까지 모든 Home SLM에 표준화된 기능은 아니며, 프라이버시 보존형 Home AI에서 적용 가능한 방향이라는 점에서 의미가 있음
- Home SLM은 영상·음성·센서의 원본 데이터를 Home SLM에서 처리하고, 의도·이벤트·특징을 추출하여 민감정보를 제거하거나 요약한 뒤, 필요한 경우에만 Home LLM에 전달하는 구조를 가지게 될 것으로 예상됨
- 또한, Home SLM에서의 민감정보 처리는 개인정보 보호 외에도 운영 안정성과 보안 측면에서도 가치가 있는 것으로 분석됨. Home SLM을 이용해 민감정보를 로컬에서 처리하면 외부 서버로 이동하는 데이터와 공격 노출면을 줄일 수 있음. 또한 인터넷 연결이 끊기더라도, 기본 기기 제어, 홈 자동화, 보안 이벤트 분석, 사용자 개인화 기능 등을 계속 활용할 수 있어 지능형 홈의 복원력을 높이는 효과도 기대할 수 있음
- 향후, 지능형 홈의 개인정보보호는 단순히 개인정보 처리방침이나 암호화에 의존하기 보다는 AI 아키텍처 자체에서 민감 정보의 이동을 최소화하는 방향으로 발전할 것으로 예상됨. 즉, Home SLM이 단순히 Home LLM의 성능을 보완하는 모델이 아니라, 가정과 Home LLM 사이의 개인정보 경계(Privacy Boundary) 역할을 담당하게 될 것으로 예상됨

08 시사점

- 지능형 홈의 경쟁축이 연결성에서 지능화 수준으로 이동할 것으로 예상됨. 기존 스마트홈 경쟁이 얼마나 많은 기기를 연결하고 자동화할 수 있는가에 초점을 맞췄다면, Home LLM·SLM 확산 이후에는 사용자의 의도·생활패턴·공간 상황을 얼마나 정확히 이해하고 적절한 행동으로 연결하는가가 핵심 경쟁요소가 될 것으로 분석됨. 이에 따라, 지능형 홈은 단순 기기 제어 플랫폼이 아니라 추론·계획·개인화 능력을 갖춘 지능형 생활 플랫폼으로 발전할 것으로 예상됨

- Home LLM과 Home SLM은 경쟁관계가 아니라 역할 분담형 구조로 발전할 것으로 예상됨. Home LLM은 복합 의도 이해, 고난도 추론, 계획 수립, 외부 서비스 연계 등 상위 지능 계층을 담당하고, Home SLM은 실시간 기기제어, 반복 명령 처리, 개인화, 민감정보 처리 등 로컬 실행 계층을 담당하는 방향으로 역할이 분화될 가능성이 높은 것으로 분석됨. 따라서, 향후 지능형 홈의 핵심은 하나의 거대한 모델이 모든 기능을 처리하는 것이 아니라 Home LLM+Home SLM의 협업 구조가 될 것으로 분석됨
- Cloud–Edge–Device 기반의 계층형 AI 아키텍처가 표준 구조로 부상할 것으로 예상됨. 복잡한 추론과 외부 지식 활용은 Cloud의 Home LLM이 담당하고, 가정 내부의 즉각적인 판단과 개인화는 Edge/Home Hub의 SLM이 담당하며, 개별 Device AI가 센싱과 실행을 담당하는 구조가 유력한 것으로 분석됨. 이는 AI 연산을 기능별·민감도별로 분산해 성능·응답속도·비용·보안성을 동시에 확보하는 구조이며, 향후, 지능형 홈 플랫폼의 경쟁력은 개별 모델의 성능 자체보다 Cloud–Edge–Device 간 AI 오케스트레이션 능력에서 결정될 가능성이 높은 것으로 분석됨
- Home SLM은 경량 모델을 넘어 Privacy Layer로 전략적 가치가 확대될 것으로 예상됨. 가정에서는 음성·영상·출입·건강·생활패턴 등 고위험·고민감 데이터가 지속적으로 생성되기 때문에 모든 원시 데이터를 클라우드 LLM으로 전송하는 구조에는 한계가 있음. Home SLM은 데이터를 로컬에서 분석하고 필요한 의미·의도·요약 정보만 상위 LLM에 전달함으로써 데이터 최소전송, 개인정보 보호, 네트워크 장애 대응, 비용 절감을 동시에 구현할 수 있음. 이에 따라, Home SLM은 향후 Local Executor+Personalization Engine+Privacy Layer의 역할을 통합하는 핵심 계층으로 자리잡을 것으로 예상됨
- Matter와 결합되면서 AI가 판단하고 표준화된 기기가 행동하는 구조가 형성될 것으로 예상됨. Matter가 서로 다른 제조사의 기기를 연결·식별·제어하는 공통 언어라면, Home LLM·SLM은 그 위에서 사용자 의도와 상황을 해석하고 어떤 행동을 수행할지 판단하는 지능 계층으로 역할이 분화됨. 이에 따라, 향후 지능형 홈은 Home LLM(추론·계획)→Home SLM(로컬 실행·개인화)→Matter(기기 상호운용)→Device(실제 동작)의 구조로 발전할 것으로 예상됨. 이는 특정 제조사에 종속된 폐쇄형 지능형 홈에서 개방형 지능형 홈 플랫폼으로 전환되는 기반이 될 수 있을 것으로 예상됨

Ⅳ. 지능형 홈 인공지능 동향

가정용 휴머노이드 개발 동향

01 가정용 휴머노이드 로봇의 부상

- 가정용 로봇은 그동안 로봇청소기, 잔디깎이 로봇, 반려·커뮤니케이션 로봇처럼 특정 작업에 최적화된 단일 기능형 기기가 중심이었으나, 최근에는 인간 중심으로 설계된 주거공간에서 여러 가사 업무를 수행하는 범용 휴머노이드 로봇의 개발이 추진되고 있음
- 최근 등장하는 가정용 휴머노이드는 물건 운반, 정리·수납, 세탁물 처리, 식사 준비 보조, 청소 보조, 가전 조작, 사용자 요청 대응 등 여러 종류의 작업을 수행하는 것을 목표로 하고 있음
- 즉, 가정 생활을 변화시키기 위해 설계된 소비자용 휴머노이드 개념으로 일상적인 집안일과 개인화된 지원을 하나의 로봇에서 수행하는 방향이 제시되고 있음. 즉, 특정 업무 하나를 반복 수행하는 전용로봇에서 동일한 로봇이 다양한 가사 업무를 학습하고 수행하는 범용 휴머노이드 로봇으로 패러다임이 변화하고 있음
- 가정용 휴머노이드 로봇이 부상하는 이유로는 인간의 신체와 행동을 기준으로 설계된 가정 내에서는 가정용 휴머노이드 로봇이 인간의 형태와 동작방식을 닮는 것이 기존 주거환경에 적응하기 유리하기 때문임
  - 문손잡이, 계단, 싱크대, 냉장고, 세탁기, 서랍, 수납장 등 대부분의 주거 설비가 인간의 신장·팔 길이·손 구조와 행동방식에 맞춰져 있음. 따라서, 실제 가정의 계단, 좁은 코너, 변화하는 공간배치에 맞게 이동해야 하며, 인체에 맞춰 설계된 거주환경에서 섬세한 가사 작업을 수행하기 위한 것이 요구됨
  - 다만, 가정용 휴머노이드 로봇이 반드시 이족보행이어야 하는 것은 아니며, 안전성과 안정성을 고려해 휠 기반 이동 구조가 선택되기도 함. 실제 가정에서는 인간형 상체와 손의 조작성은 유지하면서 이동 방식은 목적에 맞게 최적화하는 형태도 나타나고 있음
- 초기 휴머노이드는 제조·물류와 같이 작업환경이 상대적으로 구조화돼 있고 경제적 효과를 측정하기 쉬운 산업현장을 중심으로 개발돼 왔으나, 최근 기업들은 산업현장에서 축적한 이동·조작·AI 기술을 가정으로 확대하고 있음

- 휴머노이드 로봇은 공장·물류 공간→상업 공간→가정으로 적용 범위를 확장하고 있으며, 가정이 차세대 범용 휴머노이드의 중요한 목표 시장으로 부상하고 있음

- 가정은 산업 현장보다 훨씬 어려운 환경이라는 점에서 대체로 공통된 인식이 형성되어 있음. 공장은 작업대와 부품 위치, 이동경로, 작업순서가 상대적으로 표준화돼 있지만, 가정은 주택마다 공간구조가 다르고, 가구→물건의 위치가 계속 바뀌며, 아이·반려동물·사람이 함께 움직이고, 작업 지시가 모호하며, 예상하지 못한 상황이 빈번하게 발생
  - 따라서, 가정용 휴머노이드의 부상은 단순히 산업용 로봇을 가정으로 가져오는 것이 아니라, 정형화된 작업을 반복하는 로봇에서 비정형 공간을 이해하고 새로운 작업에 적응하는 범용 Physical AI로의 전환을 의미
- 가정용 휴머노이드 로봇은 기존 가정용 로봇처럼 독립적으로 작동하기 보다는 AI 홈 플랫폼·스마트 가전과 연결되고, AI 홈 생태계의 일부로 편입·진화하는 것을 의미
  - 단순히 물건을 움직이고, 기기를 작동시키는 것이 아니라, AI 홈 생태계와 연결되어, 가전·기기를 제어하고, 사용자 일정과 주변 환경을 고려해 작업의 우선 순위를 조정
  - AI 홈 센서가 현재 집 상태를 파악하고, Home AI Agent가 필요한 작업을 판단하며, 스마트 가전이 자동화 가능한 작업을 수행할 때, 가정용 휴머노이드 로봇은 물건 이동·수납 정리 등 물리적 작업을 수행하는 등 역할을 분담하는 구조를 형성
  - 기존 스마트홈이 주로 전기적·디지털 제어를 수행했다면, 가정용 휴머노이드가 결합되면서, 실제 물체를 작동하고 움직이는 Physical Automation까지 확장된다는 의미
- 한편, 가정용 휴머노이드는 동일한 하드웨어에 소프트웨어와 AI 모델을 업데이트하여, 새로운 가사작업을 계속해서 추가하는 구조가 가능해짐. 따라서 가정용 휴머노이드 로봇은 AI가 학습할 수 있는 업무 범위, 행동 데이터, 소프트웨어 업데이트 능력이 중요해질 것으로 분석됨
  - 가정용 휴머노이드의 부상은 단순히 새로운 로봇 제품군의 등장이 아니라, 가정용 기기가 기능이 고정된 가전에서 계속해서 학습하는 범용 피지컬 AI 플랫폼으로 변화하는 것을 의미하는 것으로 분석됨

02 가정용 휴머노이드 로봇의 개념 및 기술 요건

- 가정용 휴머노이드 로봇은 인간의 생활 공간에서 사람과 함께, 이동·상호작용하며, 다양한 가사·생활 업무를 자율적으로 수행하도록 설계된 범용 서비스 로봇임. 따라서, 비정형 공간, 다양한 물체, 가족 구성원·반려동물과의 공존, 자연어 지시, 안전한 물리적 접촉까지 동시에 대응해야 한다는 점에서 일반 휴머노이드 로봇이나 기존 가정용 로봇에 비해 요구되는 기술 수준이 훨씬 더 복잡하고 복합적임

- (ISO) ISO 13482는 개인지원 로봇을 사용자의 삶의 질 향상을 직접 지원하는 로봇으로 정의하고, 이동형 서비스 로봇·신체지원 로봇·탑승형 로봇 등에 대해 인간과의 물리적 접촉을 고려한 안전설계와 위험저감을 요구함
  - 현재의 가정용 휴머노이드가 이 표준의 모든 범주와 일치하는 것은 아니지만, 사람과 동일 공간에서 움직이고 접촉하는 서비스 로봇의 안전 요구를 이해하는 핵심 기준으로 활용할 수 있음
- 가정용 휴머노이드는 인간형 외관보다 인간 환경에서 범용 작업을 수행하는 것이 본질임. 가정용 휴머노이드의 핵심은 반드시 사람과 똑같이 생겼다는 데 있지 않으며, 보다 중요한 것은 인간을 기준으로 설계된 주거공간과 도구를 별도 개조 없이 사용할 수 있는 신체구조와 지능을 갖추는 것임
  - 문·서랍·냉장고·세탁기·싱크대·식기·의류 등 가정의 대부분의 설비와 물체는 인간의 키, 팔 길이, 손가락 구조, 동작범위를 전제로 설계돼 있기 때문에, 가정용 휴머노이드는 적어도 이동→인지→판단→조작→상호작용→학습의 기능을 갖춰야 함
- 따라서, 가정용 휴머노이드가 갖춰야 할 7개 핵심 기술 요건은 ▲ 복잡한 주거환경을 이해하는 고도화된 인지·센싱, ▲ 인간 수준에 가까운 정밀 조작·손 기술, ▲ 안전한 이동성과 인간-로봇 공존, ▲ 범용 이동·전신 제어와 공간 적응성, ▲ 자연어 이해·Physical AI·자율 계획 능력, ▲ 장시간·저소음·자가충전 등 가전 수준의 사용성, ▲ 지능형홈·가전과의 연계 능력 등으로 분석됨

그림 4. 가정용 휴머노이드 로봇의 기술 요건



출처 : 한국AI스마트홈산업협회

- (복잡한 주거환경을 이해하는 고도화된 인지·센싱) 물건의 위치가 계속 변하고 사람·아이·반려동물이 예측하기 어렵게 움직이는 비정형 환경이기 때문에, 단순히 물체를 인식하는 것을 넘어 사람·물체·공간 인식, 깊이·거리 측정, 장애물·계단 탐지, 재실상태 파악, 물체의 상태·재질 파악, 손과 물체 간 접촉 감지 등이 요구됨. 즉, 가정용 휴머노이드의 센싱은 단순한 보는 능력에서 시각·촉각·힘·공간정보를 융합해 실제 물리적 상황을 이해하는 멀티모달 Physical Perception으로 발전해야 함
- (인간 수준에 가까운 정밀 조작·손 기술) 가정용 휴머노이드의 상용화에서 가장 어려운 부분 중 하나는 손과 팔을 이용한 조작 능력으로, 가정에서는 동일한 로봇이 컵, 유리잔, 옷, 수건, 비닐, 식재료, 문손잡이, 전자제품 등 크기·재질·형태가 전혀 다른 물체를 다뤄야 하기 때문임. 따라서, 고자유도, 힘제어, 촉각센싱, 순응성 등이 동시에 요구됨
- (안전한 이동성과 인간-로봇 공존) 가정에서는 로봇과 사람을 안전펜스 등으로 분리할 수 없기 때문에, 가정용 휴머노이드에서 안전은 부가기능이 아니라 제품 설계의 핵심 전제조건임. ISO 13482는 개인지원 로봇에 대해 본질적 안전설계, 보호조치, 물리적 인간-로봇 접촉에서 발생하는 위험(충돌, 움직임, 에너지 저장장치, 잘못된 자율판단 등)의 저감을 요구하고 있음. 따라서, 가정용 휴머노이드에서는 최고속도·최대힘보다 충돌 시 얼마나 안전하게 양보하고 멈출 수 있는가가 더 중요한 설계지표임
- (범용 이동·전신 제어와 공간 적응성) 가정에서는 단순 직선 주행뿐 아니라, 좁은 통로 이동, 방향 전환, 의자·가구 회피, 바닥의 물건 집기, 높은 선반 접근, 문 열기, 계단 이동과 같은 자유도 높은 이동성이 요구됨. 따라서, 이족보행 자체가 가정용 휴머노이드의 필수조건이라고 보기는 어렵고, 실제 적용환경에 맞는 안정적 이동성이 중요한 요소가 됨
- (자연어 이해·Physical AI·자율 계획 능력) 가정 사용자는 로봇 프로그래밍 전문가가 아니기 때문에, 모호한 자연어 명령을 이해하고, 현재 상태 파악→필요한 작업 분해→행동 순서 계획→물체 조작→결과 확인까지 수행해야 함. 가정용 휴머노이드에서 핵심 AI는 단순 LLM이 아니라, 비전·언어·행동·월드모델·계획이 결합된 피지컬 AI가 되어야 가정 내에서의 원활한 업무와 작업 수행이 가능해짐
- (장시간·저소음·자가충전 등 가전 수준의 사용성) 산업용 로봇은 별도의 작업공간과 유지관리 인력이 있지만 가정용 제품은 사용자가 관리하지 않아도 일반 가전처럼 작동해야 하는 제약조건이 있음. 따라서, 낮은 작동소음, 장시간 구동, 자동 충전, 높은 신뢰성, 세척·교체가 쉬운 외장, 최소한의 유지보수, 지속적인 소프트웨어 업데이트 등이 필수적으로 요구됨. 가정용 휴머노이드는 로봇 성능뿐 아니라 냉장고나 세탁기처럼 일상적으로 사용할 수 있는 Consumer-grade Reliability가 중요

- (지능형홈·가전과의 연계 능력) 가정용 휴머노이드는 모든 일을 물리적으로 직접 할 필요가 없으며, 지능형 홈 플랫폼을 통해 직접 제어하는 것이 효율적임. Home AI Agent가 판단·계획하고, Smart Home Platform이 기기·환경 데이터를 통합하면, 가정용 휴머노이드 로봇은 실제 물리적 작업만 수행하면 됨. 따라서, 지능형홈 연계성은 가정용 휴머노이드의 옵션이 아니라 작업 범위와 효율을 확대하는 핵심 기술요건이 될 것으로 분석됨

03 주요 가정용 휴머노이드 로봇 동향

- 1X Tech, Figure AI, NEURA, X Square, LG전자 등 국내외 기업들은 실제 가사 수행 능력, 가정 내 비정형 환경에서의 안정성, VLA·피지컬 AI 기반 자율성, 실환경 데이터 확보, 지능형홈·가전 생태계와의 연계에 중점을 두고 경쟁력 확보에 주력
- (1X Tech) NEO는 현재 주요 휴머노이드 가운데 가정용 시장을 가장 명확하게 전면에 내세운 제품으로 분석되며, 2025년 10월 NEO를 consumer-ready humanoid robot designed to transform life at home으로 발표
  - 특정 한 가지 가사일만 수행하는 것이 아니라, 사용자가 지정한 여러 일을 수행하는 것이 목표이며, 로봇이 모르는 작업은 원격 가이드를 통해 수행하면서 새로운 데이터를 확보하는 방식과 실제 가정에서 데이터를 지속적으로 축적하고 이를 AI 모델 개선에 사용하는 전략을 채택
  - 로봇 판매→실제 가정 투입→사용자 작업 데이터 확보→AI 학습→작업 범위 확대라는 데이터 플라이휠을 먼저 구축하는데 주력. 또한, 1X는 초기 NEO를 2만 달러 구매 또는 향후 월 499달러 구독 방식으로 제시하고 있는데, 이는 단순 하드웨어 판매보다는 장기적으로 Robot-as-a-Service(RaaS)+AI 업데이트 구조를 지향하고 있는 것으로 분석됨
- (Figure AI) Figure 03은 2025년 10월 공개됐으며, 처음부터 Helix, Home, Mass Manufacturing을 고려해 재설계되었으며, 산업현장에서 축적한 휴머노이드 경험을 기반으로 이제 더 복잡한 환경인 가정으로 이동함을 강조
  - Figure 03은 카메라·센서(환경 인식)→Helix(자연어·상황 이해, 작업 계획·행동 결정)→Figure 03(양손·전신으로 실제 작업 수행)로 이어지는 과정에서 VLA(Vision-Language-Action) 기반 Physical AI인 Helix가 핵심
  - 기존 세대보다 카메라 프레임률을 2배 높이고 지연시간을 1/4 수준으로 낮췄으며, 카메라 시야도 60% 확대. 손바닥 카메라와 촉각센서도 추가해 가정의 좁고 복잡한 공간에서 정밀조작 성능을 높였으며, 이전 모델 대비 질량 8% 감소, 외장 변경(금속→섬유 소재), 충돌·끼임 위험 부위에 다중밀도 폼 적용, 배터리 안전보호 강화, 자동 무선충전, 음성 상호작용 개선 등 가정용 안전 설계를 강화한 것이 특징

- 한편, 최대 10Gbps mmWave 방식으로 대규모 로봇 데이터를 전송하도록 설계돼 Fleet Data→AI 학습→성능 개선 구조를 지향하는 방향으로 설계

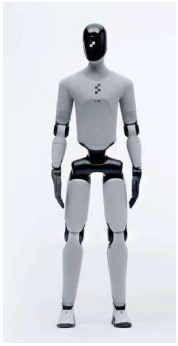
- (NEURA Robotics) 4NE-1은 가정·일상·직장에서 사용할 수 있는 범용 휴머노이드라는 점을 강조하면서, 가정에서는 청소·다림질·세탁 등 반복적인 일을 대신하는 것을 목표로 함
  - 시각, 청각, 촉각, 3D Vision, Force·Torque Sensor, 비접촉 사람 감지 등을 통합하고 있으며, 특히, 사람과 같은 공간에서 안전하게 작동할 수 있는 Touchless Human Detection을 가정 적용의 핵심 기술로 제시
- (XSQUARE) Quanta X2를 차세대 범용 휠형 휴머노이드로 개발하고 있으며, 자사의 embodied foundation model WALL 계열과 결합해 제조·물류뿐 아니라 Home-based Services를 공식 적용영역으로 제시
  - 62 DoF, 20 DoF Dexterous Hand, RGB-D·LiDAR·TOF 등 다중센서, 양팔 최대 12kg Payload, 범용 Embodied Foundation Model 등을 결합
  - WRC 2026에서 두 대의 휠형 휴머노이드가 가정 환경에서의 음성 명령에 따라, 생활용품 정리, 물건 가져오기·전달, 청소, 식물 물주기, 반려동물 관련 업무 등을 수행한 바 있음
- (LG전자) CLOiD는 2026년 CES에서 공개된 가정 특화 AI 로봇으로, 로봇 자체를 독립적인 범용 플랫폼으로 보기보다 AI가전·ThinQ·AI홈 플랫폼과 결합된 가사 실행 에이전트로 접근하고 있다는 점이 특징
  - 냉장고에서 우유 꺼내기, 오븐에 빵 넣기, 일정에 필요한 물건 준비하기, 세탁기 작동, 세탁된 수건 접기·정리, 로봇청소기의 장애물 치우기 등 상당히 구체적인 가사 시나리오를 수행
  - 양팔은 각각 7자유도로 움직이며, 인간용으로 설계된 가전·가구를 조작할 수 있지만, 어린이·반려동물이 함께 생활하는 가정을 고려해 이족보행보다 안정적인 휠 기반 자율주행 방식을 채택
  - 수만 시간 규모의 가사업무 데이터를 기반으로 VLM(공간·물체·상황 이해)·VLA(이해한 내용을 실제 로봇 행동으로 전환)를 활용하고 있으며, 머리 부분은 이동형 AI홈 허브 역할을 하며 사용자와 소통하고 주변 환경과 라이프스타일을 학습하면서 ThinQ 생태계의 가전까지 직접 제어를 담당. 즉, CLOiD Physical AI+ThinQ AI Home+LG AI Appliances가 핵심 구조
- Mentee Robotics의 MenteeBot, UBTECH의 Walker X, Fourier GR-3 등도 가정용 휴머노이드 시장을 목표로 확장을 지속하고 있음

그림 5. 주요 가정용 휴머노이드 로봇 현황

NEO



Figure 03



4NE-1



Quanta X2



CLOiD



04 Physical AI·VLA가 핵심 경쟁축

- 가정용 휴머노이드의 경쟁축은 단순한 이족보행, 관절 수, 최대 하중 같은 하드웨어 성능에서 환경을 보고(Vision), 인간의 지시를 이해하고(Language), 실제 행동으로 옮기는(Action) Physical AI 능력으로 빠르게 이동
- 특히, VLA(Vision-Language-Action)는 로봇이 자연어 명령과 시각정보를 결합해 물리적 행동을 생성하도록 하는 핵심 기술로, 범용 휴머노이드의 지능을 결정하는 중심 계층으로 부상
  - Google DeepMind는 Gemini Robotics를 VLA 모델로 정의하며, 시각·언어 입력을 로봇의 실제 행동으로 직접 변환하는 구조를 제시
- (경쟁의 중심이 움직임에서 인지·추론·행동 통합으로 이동) 범용 가정용 휴머노이드에는 단순 인식모델이나 LLM만이 아니라, 시각·언어·공간 추론·행동계획·모터 제어를 하나로 연결하는 Physical AI가 필요
  - 기존 로봇은 주로 사전에 정의된 환경에서 정해진 동작을 반복했으나, 가정은 물건 위치가 수시로 바뀌고, 같은 명령도 상황에 따라 다른 행동이 필요하기 때문에 단순 모션 제어만으로는 대응하기 어려움. 따라서 공간 인식→정리 대상 식별→우선순위 판단→이동경로 계획→물체 파지→적절한 장소로 이동·배치까지 수행해야 함
- (VLA는 언어를 행동으로 바꾸는 핵심 모델) VLM은 이미지·영상과 언어를 이해하는데 그쳤으나, VLA는 이보다 더 나아가 이미지·영상+언어를 이해하고, 로봇의 실제 행동 출력을 생성함으로써, Vision·Language·Action을 하나의 모델안에서 연결
  - 이를 토대로 예측하면, 가정용 휴머노이드의 AI가 무엇을 해야 하는지 판단하는 단계에서 어떻게 움직여야 하는지 결정하는 단계로 발전할 것으로 예상됨

- 가정용 휴머노이드 기업들은 VLA 역량과 경쟁력을 높이는데 주력하고 있으며, Google DeepMind와 같은 AI 모델 기업도 VLA 경쟁에 참여
  - (Figure AI) “좋은 로봇 하드웨어에 AI를 추가하는 것”에서 “AI 모델의 성능을 극대화하기 위해 하드웨어와 센서를 함께 설계하는 것”으로 방향을 설정
  - (1X Tech) Redwood를 휴머노이드 형태에 특화된 vision-language transformer로 설명하며, 물체 가져오기, 문 열기, 집 안 이동 등 end-to-end mobile manipulation을 수행하도록 개발
  - (LG전자) VLA를 로봇 단독으로 활용하지 않고 ThinQ·ThinQ ON과 연결한다는 점에서 차별화를 시도
  - (Google DeepMind) Gemini Robotics를 통해 VLA를 범용 로봇 intelligence layer로 발전시키고 있음. 2025년 공개한 Gemini Robotics On-Device는 로봇 자체에서 로컬로 실행되도록 최적화된 VLA로, 일반적인 조작 능력과 빠른 작업 적응을 지원
- 가정용 휴머노이드의 피지컬 AI 경쟁은 Generality, Embodied Reasoning, Dexterity, Adaptability, Learning이 결정할 것으로 예상되며, 새로운 환경에 적응하고, 예상치 못한 변화에 따라 행동을 수정하는 능력에 대한 중요도가 높아질 것으로 예상됨

표 8. 가정용 휴머노이드 로봇에서 피지컬 AI의 경쟁 요소

구분	주요 내용	가정에서의 중요성
Generality	새로운 물체·공간·작업에 대한 일반화	모든 가정의 환경이 다름
Embodied Reasoning	공간·물리 법칙을 고려한 추론	물체 위치·힘·충돌 고려 필요
Dexterity	손·팔·전신을 이용한 정밀조작	의류·식기·도구 등 다양한 물체 처리
Adaptability	환경 변화에 따른 실시간 재계획	사람·물체 위치가 계속 변함
Learning	시연·경험으로 새로운 작업 습득	모든 가사업무를 사전에 프로그래밍 불가

출처 : 한국AI스마트홈산업협회

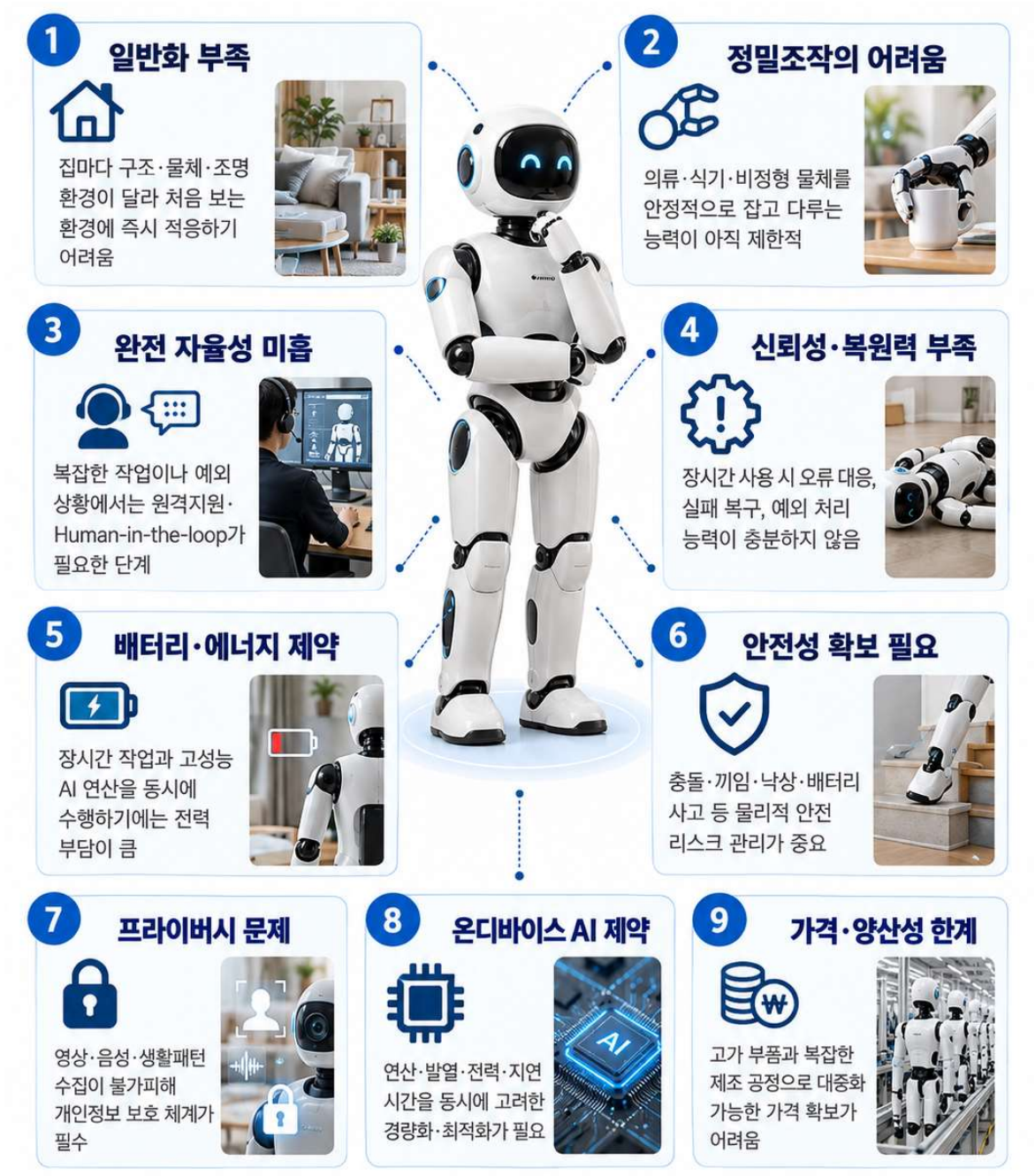
- 한편, 향후에는 가정용 휴머노이드에 있어서 VLA가 모든 것을 처리하는 것이 아닌 상위 추론 모델과 VLA의 실행 모델이 결합되는 구조로 발전할 것으로 예상됨. Embodied Reasoning Model은 목표 이해, 공간추론, 작업계획, 외부 정보 검색, 작업 성공 여부 판단 등을 담당하고, VLA는 시각·언어 입력 처리, 세부 행동 결정, 모터 명령 생성 등을 담당하는 구조임
  - 즉, AI홈 에이전트 또는 상위 Physical AI가 작업을 계획하고, VLA가 움직이는 방향을 결정하는 구조로 분화될 것으로 예상됨

05 가정용 휴머노이드 로봇의 한계

- 가정용 휴머노이드 로봇은 빠르게 발전하고 있지만, 아직 사람처럼 다양한 가사를 안정적으로 수행하는 완전 자율형 로봇 단계에 도달했다고 보기는 어려움. 이는 기술 자체의 부족이라기보다 가정이라는 비정형 환경에서 장시간 안정적으로 작동해야 한다는 요구조건이 가장 큰 영향을 미치는 것으로 분석됨
- 현재 가정용 휴머노이드 로봇의 한계점은 일반화 성능 부족, 로봇에게 어려운 가사 업무, 완전 자율화의 부족, 장시간 작업의 신뢰성·복원력 부족, 배터리와 에너지 효율성 한계, 안전성 확보, 개인정보·프라이버시 문제, Physical AI의 계산량과 온디바이스 컴퓨팅 한계 등인 것으로 분석됨
  - (일반화 성능 부족) 가정은 공장보다 훨씬 복잡하며, 같은 작업이라도 집마다 가구 배치, 물체 위치, 조명, 바닥 상태, 사용자 행동이 다르기 때문에, 어떠한 환경에서도 처음 보는 상황에 대한 대응력이 매우 중요하며, 현재 가정용 휴머노이드는 이러한 상황에 대해 발전하는 과정에 있다고 보는 것이 적절한 분석임
  - (로봇에게 어려운 가사 업무) 가정용 로봇은 단순 이동보다 매니퓰레이션(물체를 잡고 다루는 능력) 능력이 훨씬 더 어려운 작업으로 지적됨. 세탁이라는 작업도 옷 종류와 재질 구분, 구겨진 옷 집기, 세탁기 문 열기, 세탁물 투입, 세제 처리, 완료 후 꺼내기, 서로 다른 형태의 옷 접기 등 각 과정에서 서로 다른 물리적 추론과 조작이 필요하기 때문임. 즉, 인간에게 무의식적으로 쉬운 물체 조작도 로봇에게는 시각·촉각·힘제어·전신협응이 결합된 고난도 문제임
  - (완전 자율화의 부족) 현재 가정용 휴머노이드 상당수는 완전 자율화보다는 자율 AI+원격조작·인간지원의 혼합 단계에 있는 것으로 분석됨. 즉, 사람이 원격조작하는 단계에서 대부분 자율 수행·어려운 상황만 인간 개입 단계로 진행하는 과정이며, 거의 모든 작업을 자율수행 하는 단계에는 이르지 못한 상황임. 따라서, 현재 휴머노이드 로봇들의 마케팅 영상이나 기업들의 주장에서 하나의 작업을 수행하는 것이 아닌, 사용자 개입 없이 매일 수십 개의 작업을 장시간 안정적으로 수행하는 것은 구분해서 살펴볼 필요가 있음
  - (장시간 작업의 신뢰성·복원력 부족) 가정용 휴머노이드 로봇은 하나의 작업을 몇 분간 성공하는 것보다는 매일 수시간씩 안정적으로 작동해야 한다는 점이 매우 중요한 요소임. 가정 내 다양한 실패가 예상되는 상황에서도 하드웨어 신뢰성, 안전성, 충전, 데이터 오프로딩까지 지속적이면서 자율적인 운영 및 관리 능력을 갖춰야 할 것으로 분석됨
  - (배터리와 에너지 효율성 한계) 휴머노이드는 많은 관절·모터·센서·컴퓨팅 장치를 동시에 구동하기 때문에 에너지 소비가 많을 수 밖에 없음. 따라서, 충전시간을 지속적으로 관리하기 보다는 로봇이 스스로 충전하고, 다시 작업을 시작하는 방식이 중요해 질 것으로 예상됨. 따라서 단순 배터리 용량보다 에너지 효율, 자동충전, 작업 중 전력관리, AI 연산 효율 능력이

중요해질 것으로 예상됨

그림 6. 가정용 휴머노이드 로봇의 한계



출처 : 한국AI스마트홈산업협회

- (안전성 확보) 가정용 휴머노이드 로봇은 가정 내에서 인간과 같이 활동하기 때문에, 산업용 로봇보다 훨씬 더 높은 수준의 안전성이 요구됨. 현재 가정용 휴머노이드의 안전성을 위한 적합한 표준이나 인증이 없는 만큼, 안전 표준화가 시급히 필요한 상황임

- (개인정보·프라이버시 문제) 가정용 휴머노이드는 일반 지능형홈 가전보다 훨씬 더 프라이버시 문제에 민감한 문제를 내포하고 있는 것으로 분석됨. 카메라 영상, 음성, 가족 구성원, 출입정보, 집안 구조, 물건 위치, 생활습관, 행동패턴 등을 지속적으로 관찰하고 학습해야 하며, AI 성능 향상을 위해서는 이러한 데이터를 클라우드로 업로드해야 하기 때문에, 프라이버시 문제는 더욱 더 중요할 수 밖에 없음. 따라서, 향후 가정용 휴머노이드 로봇의 상용화 단계에서는 Local Processing + 최소 전송 + 사용자 동의 + 민감영역 비수집 등의 Privacy-by-Design 구조가 필수적으로 요구됨
- (Physical AI의 계산량과 온디바이스 컴퓨팅 한계) 가정용 휴머노이드 로봇은 카메라 영상을 기반으로 실시간 분석하면서, 인지→추론→행동계획→모터제어를 수 밀리초 단위로 수행해야 하기 때문에, 클라우드에 의존하면 지연이 발생하고, 인터넷 장애에 취약하게 됨. 따라서 모델 경량화와 실시간 추론 최적화가 필수적으로 요구됨

06 데이터 확보가 새로운 핵심 경쟁력으로 부상

- 가정용 휴머노이드 로봇의 경쟁력은 하드웨어 성능이나 VLA 모델 자체만으로 결정되기 어려움. 실제 가정은 구조·가구·물체·사용자 행동이 집마다 모두 다르기 때문에, 로봇이 새로운 환경과 작업에 일반화하려면 대규모이면서도 다양하고 품질 높은 실제 행동 데이터가 필요함. 이에 따라 휴머노이드 산업의 핵심 경쟁자산이 모터·관절·센서에서 'Embodied Data'로 확대되고 있음
- 가정용 휴머노이드 로봇은 일반적인 LLM과 달리 상황→물체→행동→결과가 연결된 물리적인 행동 데이터가 필요하며, 또한 한 가정(공간)에서만 수집된 데이터 만으로는 일반화할 수 없음
- 따라서, 다양한 로봇·환경·기술을 포함한 대규모 데이터셋 구축이 필수적이며, 데이터의 다양성(주택 구조, 가구·생활용품, 사용자 행동, 실패·예외 상황 등)을 폭넓게 확보하는 것이 중요
- 다양한 데이터를 확보하기 위해 Figure AI는 로봇이 직접 모든 데이터를 만들도록 기다리지 않고, 사람이 실제 집에서 수행하는 행동 데이터를 대규모로 수집해 로봇 학습에 전이하고 있으며, 1X Tech는 웹 규모 미디어+1인칭 인간 영상+시뮬레이션+원격조작 로봇 데이터+실제 NEO 운용 데이터를 결합하는 전략을 제시하면서 범용 데이터 규모 경쟁보다는 가정·가사업무라는 특정 도메인의 전문 데이터 확보에 초점을 두고 있음
- 즉, 가정용 휴머노이드 로봇의 피지컬 AI를 학습하기 위해서는 데이터 규모, 다양성, 품질, 실패 데이터, 멀티모달성, 행동 라벨, 연속성 등과 같이 양보다는 행동 데이터의 질·다양성·구조화가 중요한 것으로 분석됨

- 다만, 현재까지 배치된 가정용 휴머노이드 로봇이 적기 때문에, 인간의 데이터는 로봇 데이터의 부족을 보완하는 하나의 수단이 될 수 있음. 즉, 로봇이 직접 행동한 데이터만 사용하는 것이 아니라, 인간 행동+로봇 행동+시뮬레이션 데이터를 모두 활용하는 것이 바람직한 것으로 분석됨
- 또한, 실제 가정 데이터만으로 학습하면, 비용과 시간이 많이 소요되기 때문에, 시뮬레이션과 합성 데이터를 통해 데이터 부족을 보완하기 위해, 고품질 시뮬레이션 환경과 합성 데이터를 생성하여 활용하는 것이 데이터 확보 경쟁에서 유리한 위치를 차지하는데 큰 도움이 될 것으로 예상됨
- 종합하면, Real Data+Human Data+Teleoperation+Simulation+Synthetic Data를 통합하여 효율적으로 활용하는 것이 데이터 경쟁력을 확보하는 최선의 방법이 될 것으로 예상되며, 이를 토대로 데이터 수집(로봇·사람)→학습(VLA·월드 모델)→작업·환경 성능 향상→더 많은 가정 배치→더 다양한 실제 데이터 확보→모델 고도화의 Physical AI 데이터 Flywheel을 구축하는 것이 매우 중요한 요소가 될 것으로 분석됨

07 가정용 휴머노이드 로봇의 비즈니스 전략 분석

- 가정용 휴머노이드 시장에서 핵심 비즈니스 전략은 크게 ▲ 고가 일시판매+구독형 모델의 병행, ▲ 로봇 판매+지속적 기능 추가, ▲ 로봇 단독보다 스마트홈·가전 생태계와 결합, ▲ 산업용→상업용→가정용 단계적 확장 등 4가지 유형으로 살펴볼 수 있음
- (고가 일시판매+구독형 모델의 병행) 가정용 휴머노이드는 초기 가격이 높기 때문에 일시판매만으로 대중화를 추진하기 어려움. 이에 따라 초기 고가 판매와 월 구독형 모델을 병행하는 전략임
  - 하드웨어+소프트웨어+서비스+원격지원을 묶는 Robot-as-a-Service(RaaS) 또는 구독형 서비스로, 로봇은 구매 이후에도 AI 기능이 지속적으로 업데이트되기 때문에, 일회성 판매보다 반복 수익을 확보할 수 있는 모델로 유리
- (로봇 판매+지속적 기능 추가) 가정용 휴머노이드는 출시 시점부터 모든 작업을 완벽하게 수행하기 어렵기 때문에, 초기에는 제한된 기능으로 판매한 뒤, 소프트웨어 업데이트를 통해 작업 범위를 넓히는 방식이 현실적인 것으로 분석됨. 제품 출시→사용자 사용→데이터 확보 → AI 업데이트→기능 증가 과정에서 로봇 판매가 끝이 아니라, AI 서비스를 제공하기 위한 장기적 고객관계의 형성이 중요
- (로봇 단독보다 스마트홈·가전 생태계와 결합) 독립적인 범용 로봇 사업이 아니라, AI, 지능형 홈 플랫폼, 지능형 홈 가전이 연결되는 생태계 구축형 비즈니스로, AI-powered Appliances +AI Orchestration+Autonomous Home Robots+Service의 결합이 핵심 구조. 가전 기업들이 가정용 휴머노이드를 통해 플랫폼 사업자로 확장할 수 있는 효율적인 비즈니스

전략으로 분석됨

- (산업용→상업용→가정용 단계적 확장) 일부 기업은 가정시장에 바로 진입하기보다 산업 현장에서 먼저 기술·신뢰성·경제성을 검증한 뒤 가정으로 확장하는 단계적 전략을 추진. 이러한 전략은 산업 현장에서의 실제 경험의 축적과 이를 기반으로 인지 안전 기술을 확보할 수 있다는 점에서 유리할 수 있으나, 산업 현장과 가정 내의 환경이 매우 다르다는 점, 가정 시장에 직접 진출한 경쟁사 대비 시간이 더 소요된다는 점에서 불리
- 여러 비즈니스 전략들이 있지만, 향후 가정용 휴머노이드의 소프트웨어화가 가속화되고 표준화되면, 장기적으로는 스마트폰과 유사하게 앱스토어형 생태계로 진화할 것으로 예상됨. 현재까지 주요 기업들이 로봇 앱스토어를 상용화했다고 보기는 어렵지만, 현재 기업들이 추구하는 하드웨어 설치 후, 소프트웨어·서비스 지속 추가 방향과 일맥상통한다는 점에서 주된 비즈니스 모델로 자리잡을 것으로 예상됨

그림 7. 가정용 휴머노이드 비즈니스 전략



출처 : 한국AI스마트홈산업협회

08 지능형홈과 휴머노이드 로봇의 융합

- 지능형 홈과 휴머노이드 로봇의 융합은 지능형홈의 자동화 범위를 디지털·전기적 제어에서 물리적 행동까지 확장시키는 발전이며, 휴머노이드가 결합된 AI Home은 사용자의 의도와 상황을 이해하고, 필요한 물리적 작업까지 실제 공간에서 수행하는 구조로 진화하게 될 것으로 예상됨
- 가정용 휴머노이드 로봇은 물리적으로 물체를 잡고 옮겨야 하는 작업과 같은 지능형 홈의 한계를 물리적 실행 계층을 담당하면서 보완할 수 있다는 점에서 피지컬 AI의 실행자로서 역할을 수행
- 따라서, 지능형홈과 휴머노이드 로봇의 융합은 현재 기기 연결성과 패턴화된 실행 중심에서 Context-aware AI·Intelligent Devices·Physical Robot이 결합된 진정한 의미에서의 Intelligent Home으로 진화한다고 볼 수 있음
- 즉, 고정된 설비와 가전을 이해하고 제어하는 제한적 지능형 홈에서 고정되지 않은 설비와 가전을 넘어 공간까지 다루는 이동형 피지컬 AI 홈을 구현하는 것이며, 여기에 Matter가 결합되면, 이기종 지능형홈까지 확장되는 효과가 발생할 것으로 예상됨
- 특정 제조사 제품만 제어하는 폐쇄형 휴머노이드 로봇이 아니라 다양한 브랜드의 가전·센서·설비와 협업하는 범용 홈 로봇으로 발전하게 될 것으로 예상됨
- 최종적으로는 가정용 휴머노이드 로봇이 결합된 지능형 홈은 현재의 디지털 자동화에서 가정 내 기기·설비·공간을 모두 아우르는 피지컬 자동화로 확대되며, 가정 내 기기·설비·공간 자체도 휴머노이드 친화적으로 변화될 것으로 예상됨
  - 가구 및 인테리어 구조, 표준화된 수납 구조, 충전 공간, 문턱 최소화, 최적화된 로봇 이동 경로, 로봇 도크 등이 주택 설계에 기본 인프라로 반영되는 Robot-ready Home으로 진화할 것으로 예상됨

09 안전·프라이버시·신뢰성·가격 문제

- 가정용 휴머노이드 로봇의 상용화가 가속되고, 저변이 확산되기 위해서는 단순 가사 업무의 수행뿐만 아니라, 안전성·프라이버시·신뢰성·가격 문제의 해결이 뒷받침되어야 할 것으로 분석됨
- 사람과 같은 공간에서 동작하는 로봇이기 때문에, 안전성 확보가 가장 핵심적인 요인임. 가정용 휴머노이드로 인한 충돌·끼임·낙상·물체 낙하·배터리 이상과 같은 위험을 로봇 설계 단계에서 최대한 줄여야 함

- 따라서, 안전성은 단순 인증요건이 아니라 제품 설계의 전제조건이며, 향후 최대 속도·출력보다 충돌 시 얼마나 안전하게 정지·양보하고, 고장 발생 시 위험상태로 전이되지 않는가에 의해 경쟁력이 좌우될 것으로 예상됨

- 가정 내부를 항상 보고 듣는 로봇이기 때문에, 프라이버시·사이버보안 문제가 소비자 감수성을 자극할 것으로 예상됨. 즉, 가정용 휴머노이드는 작동을 위해 카메라·마이크·공간지도·사용자 프로필·행동데이터를 지속적으로 수집
  - 이는 기존 스마트스피커나 CCTV보다 더 넓은 범위의 가정정보를 처리한다는 의미이며, 가정용 휴머노이드 로봇이 다른 시스템에 대한 공격의 피벗 포인트가 되거나, 가정용 휴머노이드 자체가 공격 대상이 될 수 있음
  - 따라서, 가정용 휴머노이드 로봇은 로컬 처리→최소전송→암호화→권한분리→사용자 동의→데이터 삭제권이 기본 구조가 되어야 함
- 한 번의 성공보다는 매일 실패하지 않는 신뢰성이 중요. 가정용 휴머노이드의 성공 요소는 매일 수시간씩 반복적으로 오류없이 동작하는 것으로 가정 내 예외 상황 속에서도 작동과 작업 수행의 신뢰성을 확보해야 함. 따라서, 단순 고장률뿐 아니라, 인식오류·행동실패·네트워크 장애 발생 시 스스로 복구하고 안전상태로 전환하는 Operational Resilience까지 포함
- 마지막으로, 소비자가 지불 가능한 수준까지 원가를 낮추는 것이 최대 사업화 과제로 분석됨. 가정용 휴머노이드는 고자유도 액추에이터, 정밀센서, 배터리, 고성능 AI 컴퓨팅, 손·관절 시스템 등 고가 부품을 다수 사용하며, 외관 역시 인간 친화적인 디자인을 채용하기 때문에, 구매 가격이 자동차나 프리미엄 서비스에 가까운 비용 구조를 가짐
  - 이를 해결하기 위한 방안으로 대량 생산·공급(단가 하락)을 생각해 볼 수 있지만, 현재까지 가정 내 공간·인프라가 휴머노이드 친화적으로 설계·배치·구현되어 있지 않기 때문에, 단기간에 대량 도입과 활용에는 한계가 있을 것으로 분석됨
  - 따라서, 단순 판매 가격보다는 구매가+구독료+유지보수+수리+배터리+AI 서비스를 포함한 총소유비용(TCO)을 소비자가 받아들일 수 있는 수준으로 낮추는 것이 경쟁력이 될 것으로 예상됨

10 시사점

- 가정용 휴머노이드 로봇은 단일 기능형 기기에서 범용 피지컬 AI로 진화하고 있음. 기존 가정용 로봇이 청소·잔디관리 등 특정 작업을 수행하는 전용기기였다면, 최근 가정용 휴머노이드는 물건 운반·정리·세탁·조리보조·가전조작 등 다양한 업무를 하나의 로봇에서 수행하는 방향으로 발전

- 동일한 하드웨어에 AI 모델과 소프트웨어를 지속 업데이트해 새로운 작업을 추가할 수 있다는 점에서, 가정용 휴머노이드는 기능이 고정된 가전이 아니라 계속 학습하고 기능이 확장되는 범용 Physical AI 플랫폼으로 변화할 것으로 예상됨

- 경쟁의 핵심이 하드웨어에서 VLA+Embodied Data+일반화 능력으로 이동하고 있음. 향후 경쟁력은 이족보행·관절 수·최대 하중보다 환경을 보고(Vision), 인간의 지시를 이해하고(Language), 실제 행동으로 연결(Action)하는 VLA와 Physical AI 성능에서 결정될 가능성이 높은 것으로 분석됨
  - 가정은 집마다 공간구조·물체·생활방식이 달라 사전 프로그래밍만으로 대응하기 어렵기 때문에, 새로운 환경에 적응하는 Generality·Embodied Reasoning·Dexterity·Adaptability·Learning이 중요해질 것으로 예상됨
  - 동시에, Physical AI 성능의 핵심 입력자산으로 Embodied Data가 부상하고 있음. 실제 가정 데이터뿐 아니라 인간 행동, 원격조작, 시뮬레이션, 합성데이터를 결합하고, 이를 다시 모델 개선과 로봇 배치로 연결하는 Physical AI Data Flywheel 구축이 중요해지고 있음

- 휴머노이드 단독 경쟁보다 AI Home+가전+로봇+서비스 생태계 경쟁으로 확대되고 있음. 가정용 휴머노이드는 독립적으로 모든 가사를 수행하기보다, AI 홈 에이전트·스마트홈 플랫폼·스마트가전과 역할을 분담하는 구조가 더 효율적임
  - 비즈니스 모델도 하드웨어 일회성 판매보다 판매+구독, 기능 업데이트, RaaS, AI 서비스, 스마트홈 생태계 연계로 확대될 가능성이 높으며, 장기적으로 소프트웨어와 기능 모듈이 표준화되면 스마트폰과 유사한 앱스토어형 로봇 생태계로 진화할 가능성도 고려되어야 하며, 반복 수익과 플랫폼 락인 효과가 중요해질 것으로 분석됨

- 시장 확산은 기술 가능성보다 안전·신뢰성·프라이버시·경제성이 핵심 요인으로 작용할 전망임. 가정용 휴머노이드의 가장 큰 과제는 작업 수행보다는 감당 가능한 비용으로 어느 가정에서든 안전하게 장시간·안정적으로 작동하느냐임
  - 따라서, 단기적으로는 완전 자율형 범용 로봇의 대중화보다는 제한된 기능과 Human-in-the-loop를 결합한 단계적 시장 확산이 현실적일 것으로 분석됨

V. 지능형 홈 보안 동향



AI 홈 에이전트 확산과 음성·영상·데이터 보안

01 AI 홈 에이전트 확산과 보안환경 변화

- AI 홈 에이전트의 확산은 스마트홈 보안환경을 단순한 연결된 기기의 해킹 방지 문제에서, 상시 수집되는 음성·영상·행동 데이터 보호와 AI 판단·자동화의 안전성까지 포함하는 복합 보안 문제로 변화시키고 있음
- AI 홈 에이전트가 일정·생활패턴·주거환경·가전 사용정보를 종합해 사용자의 의도와 상황을 이해하고, 여러 기기와 서비스를 직접 조정하기 시작하면서 보안의 보호대상도 개별 IoT 기기에서 사용자 계정·데이터·AI 모델·자동화 권한·물리적 공간 전체로 확대됨
- (기기 보안에서 AI 에이전트 권한 보안으로 확대) 기존 스마트홈은 도어록·카메라·스피커·조명 등 각각의 기기를 안전하게 연결하고 인증하는 것이 주요 보안과제였으나, AI 홈 에이전트가 여러 기기를 한 번에 조정하는 구조에서는 에이전트 계정 하나가 다수의 기기·서비스에 대한 통합 제어권을 갖게 되는 문제가 발생
  - 스마트홈 환경에서 음성비서와 개인 IoT 기기가 공격자의 pivot point로 악용돼 다른 정보시스템에 접근할 수 있기 때문에, 계정 탈취나 권한 오남용이 디지털 피해를 넘어 실제 주거공간의 물리적 제어로 연결될 가능성이 커지고 있으며, 인증·접근통제·네트워크 분리·지속 모니터링과 같은 핵심 대응수단의 마련이 필요
- (Always-on sensing 확대로 데이터 수집 범위와 지속성이 증가) AI 홈 에이전트가 사용자의 상황을 선제적으로 이해하려면 집 안의 변화와 생활패턴을 지속적으로 인식해야하며, 따라서 카메라·마이크·재실센서·환경센서 등이 상시 또는 준상시 상태로 데이터를 생성하는 비중이 높아질 수 밖에 없음
  - AI 홈 에이전트는 개인화를 위해 더 많은 데이터를 더 지속적으로 요구하기 때문에, 보안의 핵심이 데이터의 유출 가능성보다 필요 이상의 데이터 수집 여부, 언제·어떤 과정에서 어떠한 데이터가 수집되고 있는지 사용자가 인식할 수 있는가까지 확대

- (음성·영상이 명령 데이터에서 맥락 데이터로 변화) 기존 지능형홈은 단순 명령을 처리하는 것이 중심이었지만, AI 홈 에이전트에서는 음성과 영상이 사용자의 의도·행동·상태·생활맥락을 추론하는 데이터로 활용됨
  - 따라서, 재실 여부, 행동패턴, 공간 상태, 물체 위치, 위험상황 등과 같은 로컬 이벤트 감지 자체가 프라이버시 보호의 대상이 되고 있으며, Raw Data→Event·Intent·Context로 변환되는 과정 전체를 보호해야 할 필요성이 높아짐
- (Cloud 의존 확대와 동시에 Local AI 요구도 증가) AI 홈 에이전트의 복잡한 추론과 서비스 연계를 위해 클라우드 AI의 활용은 확대되지만, 음성·영상과 같은 민감 데이터까지 모두 클라우드로 전송하는 것은 프라이버시와 지연 측면에서 많은 부담이 발생함
  - 따라서, 민감·실시간 데이터는 로컬 처리하고, 복잡한 추론만 필요 시 클라우드 활용하는 Local-first Hybrid 보안 구조로 전환될 가능성이 높은 것으로 분석됨
- (잘못된 AI의 판단 자체가 새로운 보안·안전 리스크로 부상) 기존 IoT 보안은 외부 공격자에 의한 침해가 핵심이었지만, AI 홈 에이전트에서는 AI의 잘못된 추론·오인식·자동화 실행 자체도 위험요인이 될 것으로 예상됨
  - Matter 1.6이 단순 명령 전달에서 벗어나 기기의 현재 상태·사용자 선호·안전정보를 함께 반영하는 context-driven control을 강화한 것도 이러한 문제와 연결되는 것으로 분석됨. 따라서, 향후 AI 홈 보안은 Cybersecurity뿐만 아니라 AI Safety, Automation Safety까지 포함해야 할 필요성이 커지고 있음
- (보안의 범위가 제품에서 생태계 전체로 확대) AI 홈 에이전트는 단일 제조사의 기기만 제어하는 것이 아니라 Matter, Homey 등 상호운용 플랫폼을 통해 서로 다른 브랜드의 제품·서비스를 연결하기 때문에, 이기종 지능형 홈에서 관리자와 컨트롤러의 신뢰성을 높이기 위한 보안 기능이 강화되고 있음
  - CSA도 Matter를 설계할 때부터 보안과 프라이버시를 핵심 원칙으로 상정하고 있으며, 연결되는 IoT 기기가 많아질수록 공격면이 증가하기 때문에 보안대상은 AI Agent, Account, Hub, Camera, Voice Device, Lock, Cloud, Third-party Service 전체로 확대됨

02 AI 홈 에이전트가 처리하는 음성·영상 데이터에 따른 보안 위험

- AI 홈 에이전트는 기존 스마트홈보다 훨씬 다양한 음성·영상 데이터를 처리하기 때문에, 음성·영상이 단순 명령 입력이나 녹화 데이터에 머무르지 않고, 사용자의 신원·행동·상태·생활맥락을 추론하는 Context Data로 활용된다는 점에서 심각한 보안 문제가 발생할 수 있음

- (음성 데이터) AI 홈 에이전트 시대의 음성 데이터는 단순 명령어가 아니라 사용자의 신원·선호·일정·건강·생활패턴을 추론할 수 있는 고민감 맥락 데이터로 확대되고 있으며, 비인가 명령·음성 스푸핑·사적 대화 노출 위험도 함께 증가하는 위험성을 내포함
- (주변 소리 데이터) AI 홈 에이전트는 오디오 원본을 듣는 것뿐 아니라 Raw Audio→Event Detection→Context Inference로 처리 범위를 확장하기 때문에, 이러한 상시 이벤트 감지가 사용자 재실, 취침, 건강 이상, 반려동물 등을 간접적으로 추론할 수 있으며, 이에 따라 보안도 녹음 파일 자체 보호뿐 아니라, 파생된 이벤트·추론 데이터 보호로 확대되어야 함
- (영상 데이터) 카메라 장치는 단순 영상 촬영장치에서 AI 홈의 공간·재실 센서로 변화하고 있으며, 단순 녹화·감시 목적에서 공간·인물·행동 상태를 인식하는 AI 입력데이터로 전환되고 있음. 카메라가 AI 홈 에이전트의 핵심 Context Sensor로 부상하면서, 사생활 노출, 해킹·무단 열람, 클라우드 저장 위험에 노출되고 있음
- (얼굴·생체 데이터) AI 카메라가 고도화되면서 영상에서 얼굴 특징·신체 특성·개인별 프로필까지 추출할 수 있으며, 이는 방문자의 동의 없이 얼굴정보 수집, 오인식으로 잘못된 사용자 판단, 얼굴 프로필 유출, 홈 구성원 간 과도한 접근 권한, 생체 정보 장기 저장과 같은 위험에 노출될 수 있음
- (재실·동작 데이터) 영상보다 덜 민감해 보이지만, 생활패턴을 추론할 수 있다는 점에서 기상·취침 시간, 외출·귀가 패턴, 특정 방 사용시간, 가족 구성원의 생활습관 등이 침해 위험에 노출될 수 있음
- (출입·보안 영상) AI홈 에이전트가 도어벨·카메라·도어록과 연결되면, 방문자 인식→판단→도어록·조명·알람 제어까지 연결되면서 디지털 데이터가 물리적 보안으로 직결됨. 이러한 경우, 계정이나 에이전트 권한이 탈취되면, 단순 개인정보 유출에서 그치는 것이 아니라, 실제 물리적 공간의 통제권 침해로 발전할 수 있음

표 9. 지능형 홈 데이터 종류별 보안 위험 및 대응방안

데이터	주요 발생 기기	AI 활용	핵심 위험	대응방향
음성·대화	스피커·TV·홈허브	자연어·의도·개인화	사적 대화, 스푸핑	Wake-word·로컬 처리·강한 인증
환경음(주변소리)	카메라·스피커	경보기·기침·이상음 탐지	상시청취·민감상황 추론	Local Event Detection
실시간 영상	카메라·도어벨	사람·행동·물체 인식	무단 열람·클라우드 유출	로컬 분석·암호화
얼굴·생체	카메라·디스플레이	사용자 인식·개인화	생체정보 유출·동의 문제	On-device Recognition
재실·행동	센서·카메라	자동화·Context 이해	생활패턴 프로파일링	최소저장·목적 제한
출입 영상	도어벨·도어록	방문자·보안 판단	계정탈취→물리적 접근	MFA·권한분리·로컬 검증

출처 : 한국AI스마트홈산업협회

03 주요 보안·프라이버시 위험

- AI 홈 에이전트에서는 보안·프라이버시 위험을 기존 지능형 홈보다 훨씬 광범위하게 인식해야 함. 센서가 계속 데이터를 수집하고, 일부 데이터가 클라우드로 전송되며, 하나의 계정·에이전트가 여러 기기를 제어하고, AI 판단이 실제 자동화로 이어지며, 이러한 시스템이 수년간 가정에 남아 사용되기 때문임
- (Always-on sensing) 상시 감지가 만드는 지속적 관찰에 의한 위험 발생. AI 홈 에이전트가 사용자의 상황을 선제적으로 이해하려면 마이크·카메라·모션·재실·환경센서가 상시 또는 준상시로 작동함. 문제는 단일 데이터보다 장시간 축적된 데이터가 사용자의 생활패턴과 민감한 상황을 추론한다는 점이며, 이에 따라 데이터 수집 지속시간과 파생정보 자체가 핵심 프라이버시 위험으로 부상
- (Cloud transmission) 편의성과 AI 성능 향상의 대가로 데이터 노출면이 확대된다는 문제 발생. 복잡한 음성·영상 분석과 생성형 AI 기능을 제공하기 위해 클라우드 처리가 사용될 수 있지만, 기기→가정 네트워크→클라우드→AI 서비스→ 3자 연동 서비스 등의 과정에서 위험 지점이 늘어남. 따라서, 전송 중 탈취, 클라우드 계정 침해, 서버 측 오설정, 과도한 보관, 제3자 서비스로의 추가 전달 등의 위험이 발생할 수 있음
- (Account takeover→Physical control) 계정 탈취가 실제 주거공간 제어로 연결될 수 있는 문제 발생. AI 홈 에이전트는 조명·냉난방·카메라·도어록·가전·보안시스템 등 여러 기기를 통합 제어하기 때문에, 공격자가 계정이나 에이전트 권한을 탈취하면, 단순 개인정보 접근이 아니라, 공격자가 다수 지능형 홈 기기를 제어하고, 물리적 공간 변화까지 일으킬 수 있는 위험이 발생할 수 있음
- (AI 오인식·잘못된 자동화) 외부 위협에 의한 해킹이 없어도 발생할 수 있는 새로운 위협으로 부상. 외부 공격이 없어도 AI가 상황을 잘못 해석해 음성을 다른 명령으로 오인, 사용자가 없는 것으로 잘못 판단, 다른 가족의 행동을 사용자 의도로 오해, 과거 패턴을 근거로 잘못된 자동화 실행, 서로 다른 홈 플랫폼의 자동화 규칙 충돌 등의 부적절한 행동을 수행할 수 있다는 문제점이 발생할 수 있음
- (장시간 사용에 따른 보안 노후화) 가전의 수명과 소프트웨어 지원기간의 불일치로 인해 제품은 계속 작동하지만, 보안 지원이 완료되는 문제점이 발생할 수 있음. 냉장고·TV·도어록·카메라·홈허브는 수년 이상 설치된 상태로 운영될 수 있지만 소프트웨어·라이브러리·클라우드 플랫폼의 취약점은 계속 새롭게 발견될 수 있음. 따라서 제품 수명주기 관점에서 보안의 관리와 지속적 업데이트가 중요

표 10. 주요 보안·프라이버시 위험과 대응방안

위험	핵심 원인	주요 피해	대응방안
Always-on sensing	상시 음성·영상·센서 수집	생활패턴·민감정보 추론	최소수집, 센서 상태 표시, 로컬 처리
Cloud transmission	원본 데이터 외부 전송	유출·과도한 저장·제3자 노출	Local-first, 최소전송, 암호화
Account takeover → Physical control	통합 계정·에이전트 권한	도어록·카메라·가전 등 물리적 제어	MFA, 권한분리, 고위험 명령 재인증
AI 오인식·잘못된 자동화	상황오판·명령오인·자동화 충돌	잘못된 기기 동작·안전사고	상태 검증, 정책 기반 실행, Human override
장기 보안 노후화	긴 제품수명·지원 종료	패치되지 않은 취약점 누적	장기 업데이트, CVD, 지원기간 명시

출처 : 한국AI스마트홈산업협회

04 EU: 홈 에이전트를 중요 디지털 제품으로 분류하고, 보안·투명성 규율을 강화

- EU의 최근 제도는 AI 홈 에이전트를 단순한 편의 기능이나 스마트스피커의 부가기능으로 보지 않고, 다른 서비스와 연결되고 주거공간의 기기를 제어하며 음성·영상 등 민감 데이터를 처리하는 사이버보안상 중요한 제품군으로 관리하는 방향으로 전환되고 있음
- (CRA) AI 홈 에이전트를 일반 IoT보다 높은 사이버보안 관리대상으로 분류. Cyber Resilience Act(Regulation (EU) 2024/2847)는 Smart home general purpose virtual assistants를 Class I 중요 디지털 제품으로 분류. 스마트스피커 내장형 가상비서뿐 아니라 조건을 충족하는 독립형 가상비서도 포함
  - 기존 스마트스피커(음성명령·콘텐츠 제공기기)에서 AI Home Agent(음성·영상 데이터 처리, 외부 서비스 접근, 다수의 홈 IoT 제어, 실제 주거환경에 영향을 주는 중앙 제어형 디지털 제품)로 관점 변화
- (ETSI) EN 304 631, Cybersecurity requirements for smart home general purpose virtual assistants를 개발 중. 이 표준은 CRA Annex I의 필수 사이버보안 요구사항에 대한 적합성을 입증할 수 있도록 스마트홈 범용 가상비서의 기술 요구사항과 평가기준을 구체화하는 것이 목적
  - 현재 EN 304 631 V1.0.0은 아직 최종 발행 표준이 아니라 Draft 단계이며, ETSI Work Programme상 2026년 9월 EC 평가 단계에 들어갔으며 최종화 절차가 진행 중

- EN 304 631 초안은 Always-on 환경에서 가장 민감한 문제인 지금 카메라나 마이크 데이터가 어떻게 처리되고 있는가를 사용자가 인지할 수 있도록 요구하고 있음. 특히, 지속적으로 음성·영상을 캡처하여 이벤트를 감지하는 시스템에서, 데이터가 단순 로컬 이벤트 감지 단계를 넘어 추가 처리될 경우 시각적 또는 청각적 표시를 통해 실시간으로 사용자에게 알려야 하는 구조를 규정
  - [CONF-MON-HW] 하드웨어 구성요소의 음성·영상 처리상태 표시
  - [CONF-MON-UI] UI가 있는 소프트웨어 구성요소에서의 상태 표시
  - [CONF-MON-API] UI가 없는 구성요소의 경우 API를 통해 상태 전달
  - 지속적으로 캡처한 데이터가 event-detection loop를 넘어 처리되는 경우, 실시간 표시를 요구하며, 이는 단순히 카메라 전원이 켜져 있다는 표시보다 한 단계 발전된 개념임
- EN 304 631 초안에는 [CONF-CAPT-MUTE] Mechanism to disable capture가 포함되어 있으며, 음성 또는 영상을 캡처하는 센싱 기능을 가진 홈 가상비서는 사용자가 데이터 수집 자체를 억제할 수 있는 메커니즘(카메라 커버, 마이크 연결을 차단하는 스위치 등)을 제공해야 함
  - 특히, [CONF-CAPT-MUTE-DISABLE]는 하드웨어 구성요소의 수집을 비활성화한 경우 이를 다시 허용하려면 해당 하드웨어의 물리적 사용자 인터페이스를 사용하도록 하는 구조를 요구. (예; 앱에서 마이크 수집을 차단했다면, 다시 켜기 위해서는 실제 기기의 버튼을 눌러야 하는 방식). 이는 원격 해킹이나 계정 탈취만으로 센서가 다시 켜지는 위험을 낮추려는 설계로 해석됨
- EN 304 631은 별도 Data minimisation 항목을 두고 있음. [DMIN-DJST]에서는 스마트홈 가상비서가 기밀성 데이터(confidential data)를 본래의 의도된 목적에 필요한 범위에서만 처리하도록 요구하고 있음
  - 이는 AI 성능 향상을 이유로 수집 가능한 데이터를 모두 클라우드로 전송하는 구조에서 목적 정의→필요한 데이터만 수집→필요한 범위만 처리하는 Privacy·Security-by-Design 구조로의 전환을 의미하는 것으로 분석됨
- EN 304 631의 [DMIN-USERINFO]는 음성 또는 영상 입력 데이터를 처리하는 경우 사용자가 이해하기 쉬운 언어로 데이터 캡처 및 전송 시간, 파생 데이터 전송 시간, 원본 데이터 저장 시간, 파생 데이터 저장 시간, 저장 데이터 보존 기간 등의 내용을 알려야 함을 요구하는데, 특히, derived data(파생 데이터)까지 포함했다는 점에서 중요
  - 원본 영상·음성을 AI가 분석해 생성한 정보도 사용자가 이해할 수 있도록 처리방식을 설명해야 한다는 방향으로, AI 홈 데이터 보호의 범위가 음성·영상 원본 데이터에 국한되지 않고, AI가 생성한 이벤트·행동·상태 등 파생정보까지 확대되고 있음을 의미
- EN 304 631 초안의 [DMIN-LOCAL]은 음성·영상 데이터를 지속 모니터링하여 특정 이벤트를 감지한 뒤 추가 처리를 시작하는 경우, 이벤트가 감지되기 전의 원본 데이터를 공용 통신망(public communication interface)을 통해 전송해서는 안 된다는 의미

- 마이크 음성 지속 수집→클라우드 전송→Wake word 탐지→AI 처리에서 마이크 음성 지속 수집→기기 내부에서 Wake word 탐지→이벤트 발생→ 필요한 데이터만 추가 처리·클라우드 전송하는 구조로 변환하는 것이며, 이는 단순 보안기능만 규정하는 것이 아니라 AI 홈 아키텍처를 Local-first 방향으로 유도할 수 있는 요구사항으로 분석됨

● 한편, CRA·EN 304 631이 제품의 사이버보안과 음성·영상 데이터 처리에 초점을 맞춘다면, AI Act 제50조는 AI와의 상호작용 자체의 투명성을 강화하고 있음

- AI 시스템 제공자는 사람이 AI와 직접 상호작용하는 경우 그 상대가 AI 시스템임을 명확하게 알 수 있도록 시스템을 설계해야 하며, AI 홈 에이전트가 사용자와 자연스럽게 대화하더라도, 사용자가 AI 시스템과 상호작용하고 있다는 사실을 인지할 수 있어야 하는 방향임
- 특히, 사용자가 AI와 직접 상호작용할 때 AI임을 알리는 것 외에도 감정인식·생체분류 시스템에 노출되는 사람에게 이를 알릴 의무, AI 생성·조작 콘텐츠의 기계판독 가능 표시 및 일부 딥페이크 표시 등을 규정하고 있으며, AI 홈이 향후 얼굴·음성 등을 이용해 감정인식 또는 생체분류까지 수행한다면 Article 50과의 연관성이 더 커질 수 있음

표 11. EU 규제 방향

CRA(Cyber Resilience Act)	ETSI EN 304 631	AI Act
▪ AI 홈 에이전트를 중요 디지털 제품으로 분류 ▪ 제품 전체의 사이버보안 확보	▪ 홈 에이전트에 특화된 구체적 보안설계 ▪ 센서 상태 표시 ▪ 센서 차단 ▪ 데이터 최소화 ▪ 처리방식 설명 ▪ Local Event Detection	▪ 사용자가 AI와 상호작용하고 있음을 인지 ▪ 감정인식·생체분류 등의 사용 투명성 ▪ 생성·조작 콘텐츠 표시

출처 : 한국AI스마트홈산업협회

05 카메라 AI와 프라이버시 존(zone)

● AI 홈 환경에서 카메라는 단순 영상 녹화 장치를 넘어 사람·행동·물체·재실 여부를 인식하고 자동화를 유발하는 AI 센서로 변화. 이에 따라, 카메라의 프라이버시 보호도 단순 녹화 ON/OFF에서 벗어나, 카메라 시야 중 민감 영역을 사전에 제외하거나 AI 분석 대상에서 배제하는 프라이버시 존 중심으로 발전

● (CCTV에서 Context Sensor로 진화) 기존 홈카메라의 주요 기능은 녹화·실시간 보기·모션 감지였지만, 최근 Camera AI는 사람 감지, 얼굴 인식, 반려동물·차량·물체 구분, 행동·움직임 분석, 재실 여부 판단, 방문자·택배 탐지 등으로 확대

- 따라서, 카메라가 생성하는 정보도 원본 영상, 물체·사람 탐지, 이벤트, 신원·맥락, 홈자동화 등으로 확대되고 있으며, 행위자·행위 장소·행위 내용을 해석하는 AI 홈의 핵심 Context Sensor로 변화

- Camera AI 확산으로 프라이버시 위험도 확대되고 있음. 단순 영상 유출보다 얼굴 인식 정보와 사람·사물·활동 탐지 등 추론·파생정보까지 유출될 수 있으며, 제조사의 투명성과 사용자 제어 옵션이 부족할 경우 프라이버시 위험 대응이 어려워짐
- 사용자가 카메라 화면에서 특정 영역을 지정하여 표시·녹화 또는 분석 대상에서 사전에 차단(제외)하는 프라이버시 존(Privacy Zone) 기능의 중요성이 높아지고 있음. 프라이버시 존이 지정되면, 실시간 화면과 녹화영상에서 해당 존은 검은 영역으로 처리되고 영상으로 기록되지 않음
- Privacy Zone의 핵심은 녹화 후 가리기(블러 처리)보다 사전에 처리 자체를 최소화하는 것임. 원본 영상의 저장·전송·AI 분석 이전 단계에서 배제되는 구조가 더 바람직하다는 의미로, ETSI는 Privacy by Design을 정보시스템의 설계·아키텍처 단계에서부터 개인정보 처리를 줄이고 불필요한 처리를 방지하는 접근으로 정의
- 현재 프라이버시 존은 대부분 사용자가 직접 화면의 특정 영역을 지정하는 Static Zone 방식이지만, 향후, AI 홈에서는 특정 사람 자동 마스킹, TV·PC 화면 자동 마스킹, 거울·창문 자동 제외, 욕실·침실 영역 인식, 어린이 얼굴 자동 보호, 방문자만 익명화 등과 같이 AI 기반 Dynamic Privacy Zone으로 발전할 것으로 예상됨
- 한편, 프라이버시 존은 유용한 기능이지만, 완전한 보호수단은 아니기 때문에, 영상 영역 제어, 음성 제어, AI 분석범위 제어, 저장·전송 최소화가 함께 사용되어야 더욱 효과적일 것으로 분석됨

06 카메라·도어록·음성기기도 별도 보안체계로 분화

- AI 홈이 고도화되면서 스마트홈 보안은 모든 기기에 동일한 보안기준을 적용하는 방식에서 벗어나, 기기가 처리하는 데이터와 실제 기능의 위험도에 따라 별도의 보안요건을 적용하는 방향으로 변화되고 있음
- 카메라는 영상·얼굴·행동정보를, 도어록은 실제 주거공간의 출입권한을, 음성기기·AI 홈 에이전트는 상시 음성과 다수 기기의 제어권한을 다루므로, 위험의 성격 자체가 서로 다르다는 특성이 반영되어야 하기 때문임
  - 기존에는 ETSI EN 303 645가 소비자 IoT 전반에 대한 공통 보안 기준을 제시했다면, CRA 대응 과정에서는 스마트홈 범용 가상비서용 EN 304 631과 스마트 도어록·보안카메라 등 보안기능 제품용 EN 304 632가 별도로 개발되고 있음(버티컬 보안 표준으로 세분화)

- (보안 카메라) Camera AI가 발전하면서 보호 대상이 영상 원본에서 사람·차량·동물 탐지, 얼굴정보, 행동·재실정보, 생활패턴 등으로 확대되고 있으며, 이에 따라, 영상·음성 전송 암호화, 저장 데이터 보호, 카메라 접근권한 관리, 영상 스트림 인증, 프라이버시 존·마스킹, AI 분석에 대한 범위 통제 등이 핵심으로 부각
  - ONVIF Profile T도 HTTPS 기반 영상 스트리밍, 모션·탬퍼링 이벤트, 메타데이터 스트리밍을 다루고 있으며, ETSI EN 304 632 초안은 보호해야 할 데이터 자산에 video input data와 audio input data를 명시하고 있음
  - 따라서, 단순 계정 보안을 넘어 영상 스트림의 기밀성, 저장·전송 보호, AI 분석 영역 및 사용자 프라이버시 통제를 중심으로 특화된 보안체계가 요구됨
- (스마트도어록) 스마트도어록은 카메라와 달리 인증 우회→잠금 해제 명령→실제 출입으로 이어지는 위험성이 더 크기 때문에, 높은 수준의 인증·권한관리·무결성·가용성이 더 중요한 요소로 부각됨
  - 특히, 네트워크 또는 클라우드 장애 상황, 저전력 상황 등에서도 핵심 잠금·해제 기능을 유지할 수 있는 로컬 동작과 비상 대응체계, 핵심 기능 우선 작동, 비가용 상태 사용자 알림 등이 주요 보안요건이 되고 있음
- (음성기기·AI 홈에이전트) 음성기기와 AI 홈 에이전트는 상시 대기, 자연어 명령 처리, 사용자 계정 연결, 다중 스마트 기기 동시 제어 등의 특성을 갖기 때문에, 음성 정보 프라이버시, 사용자 인증, AI 명령 검증, 홈 제어권 보호 등의 보안이 중요한 요소임
  - ETSI가 일반 보안카메라·도어록과 동일 표준으로 묶지 않고, EN 304 631 Smart home general purpose virtual assistants라는 별도 표준으로 개발하는 이유도 이러한 특성 때문이며, 음성·영상 처리상태의 실시간 표시, 음성·영상 캡처 중단 기능, 물리적 인터페이스를 통한 센서 재활성화, 데이터 최소화 등의 Always-on Assistant에 특화된 사항을 요구함

※ 현재(2026년 10월 기준) EN 304 631·304 632는 아직 최종 확정 발행본이라기보다 CRA 조화표준 제정을 위한 Draft/승인 절차 중

- 향후 AI 홈 보안은 하나의 보안 계층에서 다층 구조로 변화할 것으로 예상됨. 즉, 공통된 보안 기반 위에 제품 위험별 버티컬 보안 계층이 추가되는 구조로 발전할 것으로 예상됨. 이는 AI 홈 보안이 향후 단순 Device Security를 넘어 위험 기반 에이전트 인증·권한으로 발전하는 것을 의미하기 때문에, AI 홈 사업자들은 기기 위험도에 따라 AI 에이전트의 실행 권한도 차등화하는 방안을 마련해야 할 것으로 분석됨

표 12. ETSI 보안 표준 구조

제품군	ETSI 표준	주요 대상
소비자 IoT 공통	EN 303 645	스마트홈+소비자 IoT 전반
AI 홈 에이전트+음성 비서	EN 304 631	Smart Home General Purpose Virtual Assistant (기밀성+인증·권한관리)
스마트홈 보안기기	EN 304 632	도어록(무결성+가용성) 보안카메라(기밀성) 베이비모니터·알람 등

출처 : 한국AI스마트홈산업협회

표 13. 향후 AI 홈 보안 구조 변화

Common IoT Baseline	Home Agent Security	Camera Security	Access Security
▪ 보안 업데이트 ▪ 취약점 관리 ▪ 암호화 ▪ 인증 ▪ 제품수명주기 보안	▪ 계정·권한 ▪ AI 명령 ▪ 음성 데이터 ▪ 센서 제어	▪ 영상 암호화 ▪ 프라이버시 존 ▪ AI 분석 통제 ▪ 영상 접근권한	▪ 도어락 인증 ▪ 잠금·해제 권한 ▪ 로컬 핵심 기능 수행 ▪ 물리적 변조 탐지

출처 : 한국AI스마트홈산업협회

07 AI 홈 보안 구조: Cloud First→Local→Hybrid

- AI 홈 에이전트의 보안은 프라이버시 보호, 지연시간 단축, 네트워크 장애 대응, 클라우드 공격면 축소를 위해 기존 Cloud-first 방식에서, 민감·실시간 데이터는 집 안에서 먼저 처리하고 복잡한 추론이나 외부 서비스 연계만 클라우드를 활용하는 Local-first Hybrid 구조로 이동하고 있음
- (Cloud-first 구조의 한계) 기존 지능형 홈·음성비서는 상당수 기능을 클라우드 중심으로 구현했는데, 이러한 구조는 고성능 서버와 대규모 AI 모델을 활용할 수 있다는 장점이 있지만, AI 홈 에이전트가 음성·영상·재실·생활패턴을 상시 처리하기 시작하면서 한계에 직면
  - 집 안의 음성·영상이 외부 네트워크를 거치면서 데이터 노출면 확대, 네트워크나 클라우드 장애 시 기능 저하, 실시간성이 필요한 재실·카메라 이벤트·기기 제어에서 지연 발생 등의 문제 발생

- Local-first의 핵심은 AI를 무조건 기기 내부에 모두 넣는 것이 아니라, 민감하고 반복적으로 발생하는 1차 판단을 로컬에서 처리하는 것임. 원본 음성·영상을 외부로 지속 전송하는 대신 기기·홈허브에서 이벤트를 먼저 탐지하고, 필요한 이벤트·메타데이터만 상위 AI 에이전트나 클라우드로 전달하는 구조로 발전
- 한편, 카메라 AI에서도 로컬 처리가 확대되고 있음. 구글 Nest Hub Max의 Camera Sensing은 카메라 영상을 Google 서버로 전송하지 않고 기기 자체에서 실시간 분석하며, Face Match·Quick Gestures 등에 활용하며, 사용자는 해당 기능을 끌 수도 있음
  - 최신 Nest 카메라·도어벨 일부 모델은 얼굴을 비교하기 위한 생체 특징값(faceprint)을 카메라 내부에서 생성·매칭하고 외부 서비스로 보내지 않으며, 최신 모델의 familiar face 정보도 기기 내부 메모리에 저장되는 방향으로 바뀜
  - 이는 단순 성능 최적화라기보다, 원본 데이터→로컬 AI→얼굴·사람·이벤트 판단→최소 결과만 공유하는 Privacy-enhancing Architecture로 볼 수 있음
- Local-first는 ETSI EN 304 631이 Local Event Detection을 명시하면서, 규제·표준에도 반영되고 있음. 스마트홈 범용 가상비서가 음성·영상 데이터를 지속적으로 모니터링해 이벤트를 감지하는 경우, 이벤트가 탐지되기 전에는 해당 원본 데이터를 공용 통신 인터페이스를 통해 전송하지 않도록 요구하는 [DMIN-LOCAL] Local event detection 조항을 포함
- 다만, 모든 AI 홈 기능을 로컬에서 처리하는 것은 능사가 아님. 로컬 기기는 연산능력, 메모리, 전력, 발열, 모델 크기에 제약이 있기 때문임. 따라서, 대형 LLM·멀티모달 모델, 장기 개인화, 복잡한 계획·추론, 외부 웹·서비스 검색, 여러 기기·계정 간 데이터 통합에 강점을 가지고 있는 클라우드와 역할을 분담하는 것이 가장 현실적 방안임
- 또한, Local-first도 새로운 보안 위험이 존재함. AI 모델과 생체정보가 홈허브·카메라 내부에 저장되면 공격자가 기기를 탈취하거나 펌웨어를 해킹했을 때 새로운 위험이 발생할 수 있기 때문에, 로컬에서도 Secure Boot, Hardware Root of Trust, 암호화된 로컬 저장, 모델 무결성 검증, 안전한 OTA 업데이트, 기기 인증, 로컬 접근권한 통제 등의 보안 요소가 필요
- 종합해보면, AI 홈 에이전트의 보안은 클라우드와 로컬의 2분법적 구분보다 Device AI가 센싱·1차 이벤트 감지를, Home Edge·AI Hub가 맥락 판단·기기 제어를, Cloud AI가 대규모 LLM 기반의 복잡한 추론과 외부 서비스 연계를 담당하는 3계층 Hybrid 구조가 확산될 것으로 예상되며, 이는 프라이버시·저지연·장애 대응·공격면 축소를 동시에 확보하기 위한 AI 홈 보안의 핵심 아키텍처가 될 것으로 분석됨

08 시사점

- AI 홈 에이전트 보안의 중심이 개별 기기에서 AI 에이전트·데이터·물리공간 전체로 확대되고 있음. 즉, AI 홈 에이전트는 여러 기기와 서비스를 동시에 연결·제어하기 때문에 보안의 보호대상이 AI Agent, 사용자 계정, 음성·영상 데이터, 자동화 권한, 클라우드, 제3자 서비스, 실제 주거공간까지 확대됨
  - AI 홈 에이전트의 확산으로 스마트홈 보안의 관리단위가 개별 IoT 기기에서 에이전트·계정·데이터·자동화 권한·물리공간을 포괄하는 통합 보안체계로 확대되고 있음. 특히, 에이전트의 중앙 제어권이 커질수록 단일 계정 침해가 실제 주거환경의 물리적 통제로 연결될 수 있어, 강력한 인증·권한분리·고위험 명령 재인증이 핵심 보안요건으로 부상
- 음성·영상 보안은 원본 보호에서 이벤트·맥락·파생정보 보호로 고도화되고 있음. AI 홈 에이전트에서는 Always-on sensing이 늘어나면서, 단편적 데이터보다 장기간 축적된 데이터가 더 민감한 생활 정보를 포함하고 있으며, 사용자의 신원·행동·재실·건강·생활패턴을 추론하는 Context Data로 활용됨. 이에 따라, 보호대상도 Raw Audio·Video에서 얼굴·생체정보, 이벤트, 재실정보, 행동패턴, 생활맥락 등 AI가 생성한 파생정보까지 확대되고 있음
  - 향후 프라이버시 보호는 데이터 유출 방지뿐만 아니라, 수집되는 정보, 수집되는 기간, 추론·변환되는 정보, 정보의 활용 범위까지 통제하는 방향으로 고도화될 필요가 있음
- AI 홈 에이전트 환경에서의 보안체계는 공통 IoT 기준에서 기기별 위험 기반 버티컬 보안으로 분화되고 있음. 각 보안 기기별로 처리 데이터와 물리적 위험과 그에 따른 영향이 다르기 때문에, 동일한 보안 기준만으로는 충분하지 않으며, 보안 기기에 대한 위험 특성별로 기밀성, 무결성, 가용성, 인증·권한 관리가 다르게 적용되어야 함
  - 향후 AI 홈 사업자는 기기 위험도에 따라 에이전트의 실행권한과 인증수준까지 차등화하는 Risk-based Authorization 체계를 마련할 필요가 있음
- AI 홈 에이전트 환경의 보안 아키텍처는 Cloud-first에서 Device-Edge·AI Hub-Cloud 3계층 Hybrid 구조로 전환될 것으로 예상됨. 민감·반복적인 1차 판단은 로컬에서 처리하고, 필요한 이벤트·메타데이터만 상위 에이전트나 클라우드로 전달하는 Local-first Hybrid 구조가 확산될 것으로 예상됨
  - 민감 데이터의 외부 전송을 최소화하면서도 저지연·장애 대응·고성능 AI 기능을 동시에 확보하기 위한 구조로, 향후 AI 홈 경쟁력의 핵심 보안 아키텍처가 될 것으로 분석됨

Ⅵ. 지능형 홈 에너지 동향

AI 기반 HEMS의 부상: 주택 전체 에너지 오케스트레이션

01 지능형 홈 에너지 관리 패러다임의 변화

- 지능형 홈의 에너지 관리는 과거 가전 자체의 효율을 높이는 방식에서 센서·AI·연결기술을 활용한 개별 기기 최적화를 거쳐 최근에는 주택 전체의 생산·저장·소비를 통합적으로 조정하는 AI 기반 에너지 오케스트레이션으로 발전

표 14. 지능형 홈 에너지 관리 패러다임 변화

단계	핵심 기술	관리 단위	핵심 목표
고효율 하드웨어	인버터·모터·단열	개별 제품	소비전력 최소화
Sensor 기반 효율화	재실·환경센서	개별 기기	실제 사용환경 기반 절전
AI 가전 절전	AI·패턴학습	개별 AI 가전	예측·개인화 절전
Connected Energy Management	IoT·플랫폼	연결기기	통합 모니터링·자동화
HEMS	Smart Meter·DER 통합	주택 전체	생산·저장·소비 통합관리
AI Energy Orchestration	AI·예측·최적화	Home + Grid	비용·탄소·쾌적성 동시 최적화

출처 : 한국AI스마트홈산업협회

- (고효율 하드웨어) 기기 자체의 효율이 경쟁의 중심으로, 냉장고·에어컨·세탁기·TV 등 개별 가전의 에너지 효율 개선이 가정 에너지 절감의 출발점. 대표적으로 고효율 모터, 인버터 압축기, 단열 성능 향상, 전력변환 효율 개선, 대기전력 절감 등 하드웨어 성능 자체를 개선하는 방식으로 에너지 관리의 단위는 개별 기기·설비 중심임

- (Sensor 기반 효율화) 센서와 제어기술이 결합되면서 가전이 사용자의 상태와 환경을 감지해 불필요한 에너지 소비를 줄이는 방식으로 발전. 가전이 환경·재실·사용상태를 감지하고 운전조건을 자동 조절하면서, 에너지 절감의 기준이 '제품 자체의 정격 효율'에서 '실제 사용상황을 반영한 운전 효율'로 확대됨
- (AI 가전 절전) AI 기술이 적용되면서 가전은 단순 센서 반응을 넘어 사용패턴·환경·요금조건·사용자 선호를 종합해 에너지 사용을 자동 최적화하기 시작. 센서 기반 현재 상태 판단에서 AI 기반 미래 상황과 사용자 패턴까지 예측하는 방향으로 발전
- (Connected Energy Management) AI 절전 기능이 여러 가전에 확산되면서 개별 가전·기기의 효율보다 여러 기기의 에너지 정보를 한 플랫폼에서 연결·관리하는 단계로 발전. 에너지 사용량을 플랫폼에서 확인하고 자동화하는 구조로 에너지 관리의 단위가 개별 가전·기기에서 연결된 가전·기기로 확대되고, 실시간 사용량 모니터링과 기기간 자동화가 가능해짐
- (HEMS) 기기 관리에서 주택 전체 에너지 흐름 관리로 확대되는 단계. HEMS는 그리드·스마트미터·가전 및 기기·HVAC/히트펌프·태양광·배터리·전기차 등을 연결해 주택 전체의 에너지 생산·저장·소비를 통합으로 관리
- (AI Energy Orchestration) 단순한 HEMS를 넘어 AI가 주택 전체 에너지 흐름을 예측하고 자동 조정하는 Energy Orchestration 단계로, 예상 전력수요, 전기요금, 태양광 예상 발전량, 배터리 잔량, EV 충전 필요시간, 사용자 일정, 쾌적성, 전력망 상태, 탄소집약도 등을 동시에 고려. 최소 전력 사용뿐만 아니라, 비용·탄소·쾌적성·에너지 자립성·전력망 상태를 동시에 최적화하는 방향으로 발전

02 AI 가전의 에너지 지능화

- 최근 AI 홈 에이전트의 확산으로 가정 에너지 관리 방식도 단순히 부품 효율을 높여 소비전력을 줄이는 방식에서 벗어나, 사용자의 생활패턴·재실상태·환경·요금조건 등을 인지하고 스스로 운전조건을 바꾸는 상황인지형 절전(Context-aware Energy Saving)으로 발전
  - 기존 고효율 가전의 핵심은 인버터 모터·압축기, 단열재, 고효율 전력변환 등 하드웨어 자체 효율 향상에 있었음. 반면 AI 가전은 동일한 하드웨어를 사용하더라도 언제, 어떻게 작동할지를 AI가 조절해 실제 사용단계의 에너지 소비를 줄이는 방식으로 진화
  - (LG전자) 냉장고의 AI Saving Mode는 약 3주간의 사용패턴을 분석해 문이 상대적으로 적게 열리는 시간대를 파악하고, 해당 시간대에 냉각을 최적화해 에너지 사용을 절감. 이는 단순히 압축기 효율을 높이는 것이 아니라 사용패턴을 학습한 뒤 운전강도를 조절하는 형태임

- (Google) Nest Thermostat도 사용자의 온도 설정 습관을 학습해 자동 일정을 생성하고, 사용자가 외출하면 재실센서와 휴대전화 위치정보를 바탕으로 절전 온도로 전환함. 즉, 에너지 효율이 정격성능 중심에서 실제 생활상황 기반으로 이동
- 에너지 효율의 개념도 제품이 얼마나 적은 전력을 사용하는가에서 사용자가 실제로 어떻게 사용하는지를 고려해 얼마나 효율적으로 운전하는가로 변화하고 있음

- 가정 에너지 관리에서 AI의 역할도 감지에서 예측과 개인화로 고도화되고 있으며, AI 가전은 과거 사용 이력과 환경정보를 학습해 향후 사용패턴을 예측하고 개인별 최적 운전을 수행하는 방향으로 진화. 최근의 기술 흐름은 센서 기반 감지와 조절에서 인공지능 기반 최적화로 발전
  - (삼성전자) SmartThings의 AI 절약모드는 냉장고에서 설정온도와 냉각방식을 자동 조정하고, 에어컨에서는 사용패턴을 분석해 설정온도를 조정하는 기능을 제공. 세탁기·건조기에서도 AI 절약모드를 적용해 제품별 운전방식을 최적화
  - (Google) Nest는 외출 여부, 외부온도, 사용자가 선호하는 실내온도 등을 기반으로 냉난방을 조정하며, 계절별 절전과 러시아워 절전 프로그램까지 연계
- AI 절전 기능이 냉난방 중심에서 주요 가전 전반으로 확대되는 추세로, 예를 들면, TV는 주변환경과 영상에 따라 화면 밝기를 조절하고, 냉장고는 냉각방식을 조절하며, 세탁기·건조기는 세탁·건조 단계의 에너지 사용을 최적화하고, 에어컨은 사용패턴을 분석해 설정온도를 자동 조정하는 방식
  - (삼성전자) 내부 시험기준으로 AI Energy Mode 적용 시 에어컨에서 단계에 따라 최대 10~30% 수준의 절전효과를 제시하고 있으며, 식기세척기 등으로도 AI Energy Mode 적용대상을 확대
  - (LG전자) 냉장고에서 사용패턴을 분석한 AI Saving Mode를 제공하고 있고, AI Home 전반에서는 가전사용과 생활맥락을 종합해 기기·서비스를 조정하는 방향으로 확대
- AI 절전 기준은 에너지 절감률에서 사용자 불편 최소화까지 확대되면서 에너지 절감, 쾌적성, 제품 성능, 사용자 선호 사이의 균형을 찾는 방향으로 발전. AI 절전의 목표는 최대 절감률 자체보다 제품 성능과 사용자 쾌적성을 유지하면서 불필요한 에너지 소비를 줄이는 방향으로 변화하고 있으며, 이에 따라 절감률뿐 아니라 개인별 선호·생활패턴·환경조건을 얼마나 정밀하게 반영하여 절전과 편의의 균형을 구현하는 것이 가전 에너지 관리의 경쟁력이 될 전망

03 HEMS와 주택 전체 에너지 오케스트레이션

- HEMS(Home Energy Management System)는 과거 스마트미터 데이터를 기반으로 가정의 전력 사용량을 보여주고 사용자가 직접 절전하도록 유도하는 시스템에서, 최근에는 가전·태양광·가정용 배터리·EV 충전까지 하나의 플랫폼에서 연결하고 AI가 자동으로 운전시간과 에너지 흐름을 최적화하는 주택 전체 에너지 오케스트레이션 시스템으로 진화
- 전통적 HEMS에서는 Smart Meter → 사용량 측정·시각화 → 사용자 판단 → 사용자 절전이라는 흐름이었으나, 최근 AI기반 HEMS에서는 Smart Meter+Appliance+ Solar+Battery+ EV→예측·판단→자동 최적화하는 과정으로 진화
- 전통적 HEMS는 스마트미터 데이터를 활용해 주택의 전력사용량과 비용을 가시화하고 이를 기반으로 사용자의 자발적인 절전행동을 유도하는 Energy Monitoring & Feedback 중심 시스템으로 발전
  - 전통적 HEMS는 정보를 보여주는 것만으로는 지속적인 최적화가 어렵고, 가전·기기의 작동을 사용자가 지속적으로 확인하고, 직접 행동해야 한다는 한계가 있으며, 태양광과 ESS까지 설치되면 현재 발전량, 충전 시작 시간, 충전 우선 순위, 저렴한 전력망, 배터리 잔량 등 여러 조건을 고려한 판단은 더욱 복잡해짐
- 최근 HEMS는 기기 연결에서 가정 내 에너지 자원을 통합하는 방향으로 확대되고 있음. 스마트미터, HVAC·히트펌프, 지능형 가전, 태양광, 배터리, 전기차·충전을 통합 연결하여 관리하는 방향으로 발전
  - Matter 1.4에서 Solar Power, Batteries, Heat Pumps, Water Heaters 등 새로운 에너지 관리 기기 유형을 추가했으며, 가정 내 에너지 소비·생산·저장을 스마트홈에서 보다 효율적으로 관리할 수 있도록 기능을 확대
  - 또한, Matter 1.5에서는 한 단계 더 나아가 전력망의 가격·요금·탄소집약도 정보까지 에너지 관리에 활용할 수 있도록 기능을 확장
  - 이에 따라, HEMS의 관리 단위도 가전·기기의 개별 에너지 소비에서 가정 전체의 에너지 흐름 관리로 변화하고 있음
- 또한, 태양광과 배터리의 결합으로 HEMS가 에너지 소비 관리에서 생산·저장 관리까지 확대되고 있음. 가정이 전기를 공급받아 소비하는 소비자에서 전력을 직접 생산하는 프로슈머가 되기 때문임
  - 따라서, HEMS는 전력망→가정이라는 단방향 에너지 흐름만 관리하는 것이 아니라, 태양광→가정, 태양광→배터리, 배터리→가정, 전력망→배터리, 가정→전력망 등 여러 방향의 에너지 관리를 동시에 수행하는 방향으로 발전

- 즉, HEMS가 단순 에너지 모니터링 시스템에서 실제 에너지 흐름을 결정하는 에너지 컨트롤 시스템으로 변화하고 있음

- 한편, 전기차·충전시스템이 연결되면서 HEMS는 주택 최대 부하 관리까지 담당하게 됨. 전기차 배터리 잔량, 출발 시간, 필요한 충전량, 시간대별 전력 가격, 태양광 발전량, 주택 전체 전력 부하 등을 함께 고려해 충전 시점을 자동 조정하는 방향으로 발전함
- 이에 따라, HEMS는 전체 에너지 수요 예측, 태양광 발전량 확인, 배터리 잔량 확인, EV 충전 필요량 확인, 가전 운전시간 조정, 전기요금·피크 반영, 각 자원에 운전명령 배분을 수행하는 Energy Orchestration으로 변화하고 있음. 여기에 AI가 결합되면서, HEMS는 반응형에서 예측형으로 진화하고 있음

표 15. 전통적 HEMS와 최근 HEMS 비교

구분	전통적 HEMS	최근 AI 기반 HEMS
주요 자원	스마트 미터 중심	스마트미터+가전·기기+태양광+ESS+EV
핵심 기능	사용량 측정·시각화	생산·저장·소비 통합제어
판단 주체	사용자	AI·알고리즘
제어	사용자 직접	자동제어
관리 방식	사후 확인	(발전·수요·가격분석·최적화·충전계획·스케줄링) 실시간+예측
관리 목표	절전	비용·피크·탄소·쾌적성 최적화
관리 단위	개별 소비	가정 전체 에너지 흐름
시스템 역할	Energy Monitor	Energy Orchestrator

출처 : 한국AI스마트홈산업협회

04 AI 기반 HEMS의 핵심 기능 고도화

- AI 기반 HEMS의 핵심 기능은 수요 예측, 가격 최적화, 탄소 최적화, 생활패턴 최적화로, 단순히 현재 전력사용량을 보고 제어하는 수준을 넘어, 앞으로의 수요·가격·탄소집약도·사용자 행동을 예측하고 이를 바탕으로 가전·ESS·태양광·EV의 운전시점을 자동으로 조정. 즉, HEMS가 반응형 조정에서 예측·자동화 기반의 최적화로 발전하고 있음
- (수요 예측) AI HEMS는 과거 사용패턴·날씨·시간대·태양광 발전량 등을 기반으로 향후 주택의 전력수요와 에너지 생산량을 예측하고, 예상되는 피크 이전에 ESS 충전이나 가전 운전시간을 조정하는 예측형 에너지 관리로 발전하고 있음. 이에 따라, HEMS의 역할도 사후적인 사용량 관리에서 사전적인 부하계획 및 Peak Shaving으로 확대되고 있음

- (가격 최적화) AI 기반 HEMS는 단순 소비전력 절감에서 벗어나 시간대별 전기요금과 전력 구매·판매가격을 분석해 ESS 충·방전, EV 충전, 가전 운전시간을 자동 이동하는 가격 최적화 기능으로 고도화되고 있음. 이에 따라, 향후 에너지 관리의 핵심은 얼마나 적게 사용하는가뿐만 아니라 언제 구매·저장·소비·판매하는가를 최적화하는 방향으로 이동할 것으로 예상됨
- (탄소 최적화) AI HEMS는 전기요금뿐 아니라 전력망의 실시간·예측 탄소집약도를 활용해 탄소배출이 낮은 시간대로 가전·EV 등의 사용시간을 이동시키는 탄소 최적화 기능으로 확대되고 있음. Matter 1.5가 가격·요금과 함께 Grid Carbon Intensity를 표준 데이터로 지원하기 시작한 것은 홈 에너지 관리의 목표가 비용 최소화에서 비용·탄소의 동시 최적화로 확대되고 있음을 보여줌
- (생활 패턴 최적화) AI HEMS가 사용자의 기상·외출·귀가·가전 사용·EV 출발시간과 쾌적성 선호를 학습해 에너지 사용을 조정하는 기능으로, 절감효과와 사용 편의 사이의 균형을 확보하는 것이 핵심임. 향후, AI HEMS는 사용자가 매번 절전행동을 선택하는 방식보다 기존 생활패턴을 최대한 유지하면서 백그라운드에서 자동으로 부하를 조정하는 방향으로 진화할 것으로 예상됨
- 이러한 네 가지 기능은 독립적으로 작동하는 것이 아니라, 사용자 일정을 기반으로 비용, 탄소배출, 주택 피크를 최소화하기 위한 충전(시간·속도)을 결정하는 방식으로 작동

표 16. AI HEMS의 핵심 기능

기능	주요 입력 데이터	최적화 대상	기대 효과
수요 예측	과거 사용량, 날씨, 태양광, 시간대	향후 전력수요·발전량	Peak Shaving·사전 충전
가격 최적화	TOU·실시간 요금, 구매·판매가격	충전·방전·기기 운전시간	전기요금 절감
탄소 최적화	Grid Carbon Intensity, 재생에너지 정보	전력 사용시간	탄소배출 저감
생활패턴 최적화	재실·일정·사용패턴·선호	가전·HVAC·EV 운전	편의·쾌적성 유지

출처 : 한국AI스마트홈산업협회

05 태양광·ESS·EV까지 연결하는 Home Energy Ecosystem

- AI 기반 HEMS의 발전은 에너지 관리대상을 가전 중심에서 태양광·ESS·EV까지 포함하는 주택 전체 분산에너지 자원으로 확대. 가정이 단순한 전력 소비처가 아니라 전력을 생산하고, 저장하고, 필요 시 이동·재분배하는 에너지 허브로 전환되는 것이 핵심 변화임

- (에너지 소비자에서 프로슈머로 전환) 태양광·ESS의 확산으로 가정은 단순 전력 소비자에서 직접 전력을 생산·저장하고 필요 시 계통과 교환하는 프로슈머로 전환되고 있으며, 이에 따라 HEMS의 역할도 소비량 관리에서 분산에너지 자원의 통합 운용으로 확대되고 있음
  - 태양광, 배터리, EV 등은 대표적인 분산에너지자원으로, 분산에너지원의 확산으로 전력은 대규모 발전소에서 일방향으로 공급되는 구조에서 지역에서 생산·소비·저장되는 양방향 구조로 변화. 또한, 가정은 잉여 태양광 전력을 계통으로 보내거나 저장해 나중에 사용할 수 있음
- (태양광으로 전력 소비 관리에서 발전량 관리까지 추가) 태양광이 HEMS에 연결되면 전력 소비뿐만 아니라, 생산까지 관리하게 되며, 현재 태양광 발전량, 일사량·날씨, 가정 전력수요, ESS 충전여력, EV 충전 필요량 등을 종합해 자가소비를 최대화하게 되며, 잉여 전력이 발생하면, 가전 사용, ESS 충전, EV 충전, 계통 송전에 대한 배분을 결정
- (ESS는 시간적으로 에너지를 이동시키는 핵심 자원) 태양광은 발전량이 시간·날씨에 따라 크게 달라지므로 ESS가 결합될 때 활용가치가 높아짐. 태양광 잉여전력 저장, 저녁 피크시간 방전, 저가시간대 충전, 정전 시 비상전력 공급, 전력망 피크 완화 등이 ESS의 핵심 역할이며, ESS는 단순 백업 배터리가 아니라 AI HEMS가 주택 전체 에너지 흐름을 조정하기 위한 시간적 완충자원이 됨
- (EV는 대규모 부하에서 이동형 에너지 자원으로 확대) EV는 가정 내 대규모 신규 전력부하인 동시에 향후 V2H·V2G를 통해 이동형 에너지 저장자원으로 활용될 수 있어, HEMS의 핵심 관리대상으로 부상하고 있음. 이에 따라, AI HEMS는 단순 EV 충전을 넘어 출발시간·요금·태양광·ESS 상태를 종합해 충·방전 시점을 조정하는 방향으로 발전할 것으로 예상됨
- 핵심은 태양광·ESS·EV가 각각 존재하는 것만으로 Home Energy Ecosystem이 완성되는 것은 아니며, AI HEMS가 각 자원의 상태를 실시간으로 파악하고 어떤 자원을 언제, 어떤 순서로 활용할지 결정함으로써, Home Energy Ecosystem이 완성됨

표 17. Home Energy Ecosystem에서 주요 자원의 역할

자원	기존 역할	Home Energy Ecosystem에서의 역할
지능형 가전	전력 소비	유연한 부하·운전시간 조정
태양광	전력 생산	발전예측·자가소비 최적화
ESS	저장·비상전원(방전)	가격·피크·자가소비 최적화
EV	이동·충전	유연한 부하→이동형 ESS
전력망	전력 공급	구매·판매·DR·VPP 연계
AI HEMS	모니터링	생산·저장·소비 통합 오케스트레이션

출처 : 한국AI스마트홈산업협회

06 Matter 기반 개방형 홈 에너지 생태계

- 기존 HEMS는 대체로 특정 제조사 또는 플랫폼의 가전·배터리·EV 충전기 등을 중심으로 구성되어, 이기종 기기 간 데이터 모델과 제어방식이 달라 통합 에너지 관리에 한계가 존재. 최근 Matter는 단순 스마트홈 연결 표준에서 벗어나 전력 사용량·발전량·가격·탄소집약도·충전계획까지 표준화하는 방향으로 확장되면서, 개방형 Home Energy Ecosystem의 공통 인프라로 발전하고 있음
- 기존 HEMS는 제조사별 독자 플랫폼과 API를 중심으로 구축돼 자사 기기의 에너지 관리에는 유리하지만, 태양광·ESS·EV·가전 등 서로 다른 제조사의 에너지 자원을 하나의 시스템에서 통합 관리하기 어렵다는 한계를 가지고 있음. 이에 따라, 주택 전체 에너지 오케스트레이션을 위해서는 기기 간 공통 에너지 데이터 모델과 제어 인터페이스의 필요성이 확대되고 있음
- (Matter 1.3) 기기가 순간 전력, 전압, 전류, 누적 전력사용량, 발전량 등을 표준 방식으로 보고할 수 있는 Energy Reporting 기능을 도입했으며, EV 충전설비를 에너지 관리 기기로 지원하기 시작
  - 이에 따라, HEMS 측면에서는 제조사가 다른 기기도 Matter를 지원하면 동일한 방식으로 에너지 데이터를 읽고 활용할 수 있는 기반이 만들어짐
- (Matter 1.4) 태양광, 배터리·배터리에너지저장시스템, 히트펌프, 온수기를 새로운 에너지 관리 기기로 추가하면서, 에너지 관리 범위가 크게 확대되면서 에너지 기기 코디네이터로 확장됨

- 특히, 배터리는 주택이나 전력망으로 에너지를 다시 공급할 수 있도록 지원하며, HEMS를 통해 부하균형과 가상발전소에도 활용될 수 있으며, 또한, Device Energy Management 기능을 통해 에너지 소비기기가 전력사용 예측과 전력관리 요구에 따라 운전 시작시간을 조정할 수 있음. 또한, 전기차전원공급장치도 사용자의 충전 선호도를 표현할 수 있는 기능이 강화됨

- (Matter 1.5) 에너지 가격·요금·탄소정보까지 표준화하는 등 에너지 관리가 한 단계 더 고도화됨. Electrical Energy Tariff 관련 기능을 추가해 유틸리티·전력망 운영자·에너지 서비스가 실시간 가격, 예측 가격, 요금정보, 전력망 탄소집약도를 Matter 표준 형식으로 기기에 전달할 수 있도록 지원
  - 기기들은 이러한 데이터를 이용하여 실제 에너지 비용 산출, 탄소영향 계산, 사용시간 자동 변경, 사용자 선호에 따른 비용·탄소 최적화 등을 수행할 수 있음. 이는 Matter가 단순히 에너지 사용량을 알려주는 수준을 넘어 사용 시간에 따른 비용과 탄소 절감까지 판단하는 데이터 기반까지 표준화하고 있다는 것을 의미
- (Matter 1.6) 새로운 에너지 기기 종류를 대폭 늘리기보다, 여러 플랫폼과 기기가 동시에 존재하는 환경에서 상태·사용자 선호·운영제약을 서로 공유하고 더 지능적으로 제어하는 방향으로 강화됨. 즉, 다중 플랫폼 환경에서 맥락 기반 제어가 강화되는 방향임
  - Thermostat Suggestions 기능은 플랫폼이 직접 명령을 강제로 실행하는 대신, 시간 제한이 있는 제안(suggestion)을 보내고 기기가 사용자 선호, 현재 환경, 기존 설정, 수요 반응 참여 상태 등을 고려해 실행 여부를 판단하도록 함
  - 즉, 여러 플랫폼이 절전, 쾌적성, 분산전원, 공기질 등 서로 다른 목표로 명령을 보낼 경우, 단순 명령 우선순위가 아니라 기기의 현재 맥락과 사용자 정책을 반영해 조정함
- Matter가 AI 기반 HEMS의 역할을 하는 것은 아니지만, HEMS의 공통 언어 역할을 수행하게 될 것으로 예상됨
  - Matter는 기기 검색, 상태 공유, 에너지 측정정보, 에너지 계획, 제어 요청 등을 표준화하는 연결+데이터 모델 계층으로 AI HEMS는 Matter 상위에서 수요 예측, 가격 최적화, 탄소 최적화, ESS 충·방전 계획, EV 충전계획, 부하 이동을 수행하는 Optimization·Orchestration 계층으로 작동
  - Matter 기반 HEMS에서는 각 기기가 에너지 관련 상태와 요구조건을 공통 형식으로 표현할 수 있으며, HEMS는 각 기기의 정보를 공통 방식으로 이해하게 됨. 즉, Matter의 역할은 에너지 최적화를 직접 수행하는 AI의 역할이 아니라, 서로 다른 에너지 기기가 HEMS와 통신할 수 있게 만드는 공통 데이터·제어 역할을 담당함
- Matter가 확대되면 제조사별 종속형 HEMS가 개방형 Home Energy Ecosystem으로 변화하게 될 것으로 예상됨

- Matter 1.4에서는 배터리를 any controller potentially serving as the management system이라고 설명해, 특정 제조사 플랫폼만이 아니라 다양한 컨트롤러가 HEMS 역할을 수행할 수 있는 방향을 제시하고 있으며, Matter 자체도 Enhanced Multi-Admin 등을 통해 여러 생태계가 동일 기기를 공유·제어할 수 있는 구조를 강화하고 있음
- 최종적으로 Matter가 확대되면 이상적으로는 A사 가전+B사 태양광+C사 ESS+D사 EV 충전을 하나의 HEMS가 공통 인터페이스로 관리하는 구조가 가능해짐

● 마지막으로 Matter와 전력망 표준과의 연계도 중요한 요소임. Home Energy Ecosystem이 주택 내부에 머무르지 않으려면 전력회사·DR 시스템과도 연결돼야하기 때문임

- CSA와 OpenADR Alliance는 2026년 공식 협력관계를 구축해 Matter 스마트홈 기기와 OpenADR 기반 전력망 수요반응 시스템을 연결하는 작업을 추진하고 있으며, CSA는 Matter가 OpenADR 3.0 등과 결합해 주택 내부와 전력망 양쪽의 에너지 밸런싱을 지원할 수 있다고 설명하고 있음
- 따라서, 향후 구조는 유틸리티·전력망(OpenADR 등)→AI HEMS(Matter)→태양광+ESS+EV+Appliance와 같은 형태가 될 가능성이 높은 것으로 분석됨

표 18. Matter 에너지 관리 기능의 진화

버전	주요 에너지 기능	의미
Matter 1.3	전력·에너지 측정, 전기차전원공급장치	에너지 데이터 표준화 시작
Matter 1.4	태양광, 배터리, 히트펌프, 온수기, 기기 에너지 관리	주택 에너지 자원 통합
Matter 1.5	가격·요금·전력망 탄소 집약도	비용·탄소 최적화 기반
Matter 1.6	맥락·선호 기반 제어, 다중 생태계 개선	지능형 오케스트레이션 기반 강화

출처 : 한국AI스마트홈산업협회

07 시사점

● (에너지 효율 경쟁의 단위가 개별 가전에서 주택 전체로 확대) 지능형 홈의 에너지 경쟁은 개별 가전의 고효율 성능 중심에서 주택 전체의 에너지 흐름을 통합 최적화하는 방향으로 전환되고 있음. 이에 따라, 향후 가전·스마트홈 기업의 경쟁력은 제품별 절감률보다 가전·설비·분산에너지 자원을 하나의 플랫폼에서 얼마나 효과적으로 조정할 수 있는가에 의해 좌우될 것으로 예상됨

- (HEMS가 에너지 모니터에서 AI 에너지 오케스트레이터로 진화) AI 기반 HEMS는 단순 사용량 모니터링 시스템에서 전력수요·발전량·요금·탄소·사용자 행동을 예측하고, 가전·ESS·EV의 운전순서와 시간을 자동 결정하는 'Energy Orchestrator'로 진화하고 있음. 향후, HEMS의 핵심 경쟁력은 하나의 목표만 최적화하는 것이 아니라 비용·탄소·피크·쾌적성·자가소비를 동시에 조정하는 다목적 최적화 역량에 있을 것으로 분석됨
- (태양광·ESS·EV 결합으로 가정이 소비자에서 에너지 허브로 전환) 태양광·ESS·EV의 결합은 가정을 단순 전력 소비자에서 생산·저장·이동이 가능한 분산에너지 자원으로 전환시키고 있음. 이에 따라, AI HEMS는 소비량 관리 시스템을 넘어 가정 내 분산에너지 자원의 운영을 총괄하는 Home Energy Hub로 발전하며, 장기적으로는 분산전원·가상발전소 등 전력망 서비스까지 연결되는 Grid-interactive Home의 핵심 기반이 될 것으로 전망됨
- (Matter가 제조사 종속형 HEMS를 개방형 Home Energy Ecosystem으로 전환) Matter의 에너지 관리 기능 확대는 HEMS를 제조사별 폐쇄형 플랫폼에서 이기종 가전·태양광·ESS·EV가 연결되는 개방형 Home Energy Ecosystem으로 전환시키는 기반이 될 것으로 예상됨. 이에 따라, 향후 경쟁축은 자사 기기를 많이 보유한 Device Lock-in보다 다양한 에너지 자원을 공통 인터페이스로 연결하고 상위 AI가 이를 얼마나 효과적으로 최적화하는가에 초점이 맞춰질 가능성이 높은 것으로 분석됨