IoT 무선기기 사이버보안 인증 대응을 위한 우선순위 기반 설계 프레임워크 연구 : EN 18031-1과 IEC 62443-4-1 기반

(A Study on a Priority-Based Security Design Framework for Cybersecurity Certification Compliance of IoT Wireless Devices: Based on EN 18031-1 and IEC 62443-4-1)

윤호상*, 허봉재**, 홍아름***

(Ho Sang Yoon, Bong Jai Huh, Ah Reum Hong)

요 약

본 연구는 유럽연합(EU)의 사이버보안 인증 표준 EN 18031-1을 기반으로 IoT 무선기기 개발 과정에 적용 가능한 우선순위 기반 보안 설계 프레임워크를 제안한다. 기존 연구가 보안 요구사항의 단순 나열 또는 정책적 분석에 주로 머문 것과 달리, 본 연구는 사이버보안 시험·평가 전문가를 대상으로 AHP 기법을 적용하여 인증 평가 항목의 상대적 중요도를 정량적으로 도출하였다. 분석 결과, 접근제어(0.284), 보안 통신(0.227), 인증 메커니즘(0.202)이 핵심 설계 요소로 확인되었으며, 상위 3개 항목이 전체 중요도의 71.3%를 차지하였다. 도출된 중요도를 기반으로 IEC 62443-4-1의 SDL 프로세스에 적용하여 Core - Enhanced - Basic의 3단계 보안 설계 프레임워크를 제안하였다. 제안된 프레임워크는 접근제어·인증·보안 통신을 필수 구현 항목(Core)으로, 업데이트·복원력·키 관리를 우선 보완 항목(Enhanced)으로, 로깅·확인 등 나머지 항목을 기본 준수 항목(Basic)으로 분류하여 SDL 8단계 개발 프로세스와 연계한 체계적 보안 설계 기준을 제시한다. 이를 통해 자원 제약 환경에서도 인증 대응 효율성을 향상시키고, 개발 초기 단계에서 보안 요구사항을 우선순위에 따라 체계적으로 반영할 수 있도록 지원한다.

■ 중심어 : 사물인터넷; 사이버보안 인증; EN 18031-1 ; AHP ; IEC 62443-4-1

Abstract

This study proposes a priority-based security design framework for IoT wireless devices based on the European Union (EU) cybersecurity certification standard EN 18031-1. Unlike previous studies that have primarily focused on enumerating security requirements or conducting policy-oriented analyses, this research quantitatively derives the relative importance of certification evaluation criteria by applying the Analytic Hierarchy Process (AHP) based on assessments from cybersecurity testing and evaluation experts. The analysis results indicate that access control (0.284), secure communication (0.227), and authentication mechanisms (0.202) are the most critical design elements, with the top three factors accounting for 71.3% of the overall importance. Based on these derived priorities, the study applies the results to the Secure Development Lifecycle (SDL) process defined in IEC 62443-4-1 and proposes a three-tier security design framework consisting of Core, Enhanced, and Basic levels. In the proposed framework, access control, authentication, and secure communication are classified as mandatory implementation items (Core), while update management, resilience, and key management are categorized as priority enhancement items (Enhanced). The remaining requirements, including logging and verification functions, are classified as basic compliance items (Basic). Furthermore, the framework presents systematic security design guidelines by linking these categories to the eight-stage SDL development process. The proposed framework improves certification compliance efficiency in resource-constrained environments and supports the systematic integration of prioritized security requirements during the early stages of IoT device development.

■ keywords : Internet of Things ; Cybersecurity Certification ; EN 18031-1 ; Analytic Hierarchy Process ; IEC 62443-4-1

Ⅰ. 서 론

사물인터넷(IoT) 기술의 확산은 가정, 산업, 의료, 교통 등 다양한 분야에서 디지털 전환을 촉진

* 정회원, 주식회사 에이치시티 연구소장, 경희대학교 AI 기술경영 전공
** 정회원, 주식회사 에이치시티 대표이사
*** 정회원, 경희대학교 AI 기술경영학과, 교수
접수일자 : 2026년 04월 28일
수정일자 : 2026년 05월 08일
게재확정일 : 2026년 05월 14일
교신저자 : 홍아름 e-mail : arhong@khu.ac.kr

하며, 무선기기를 기반으로 한 제품과 서비스의 시장 확대를 가속화하고 있다. 그러나 이러한 성장과 함께 개인정보 유출, 원격 제어 탈취, 서비스 장애 등 사회·경제적 문제로 이어질 수 있는 사이버보안 위협 또한 현실화되고 있으며, 이에 따라 IoT 무선기기의 보안성 확보는 선택이 아닌 필수 요소로 인식되고 있다.

특히 최근 국내 통신사에서 발생한 대규모 개인정보 침해 사고는 무선기기와 네트워크 전반에 대한 보안 관리의 중요성을 다시 한번 부각하는 계기가 되었다. 이러한 흐름에 대응하여 유럽연합(EU)은 무선기기 지침(Radio Equipment Directive, RED)을 개정하고, EN 18031-1을 포함한[1] EN 18031-X 시리즈 사이버보안 인증 표준을 통해 IoT 무선기기에 대한 보안 요구사항을 의무화하였다. 해당 규격은 2025년 8월부터 EU 시장에 유통되는 특정 범주의 무선기기에 적용되고 있다. 그러나 실제 IoT 제품 개발 환경에서는 제한된 인력과 자원으로 인해 다양한 보안 요구사항을 동시에 반영하는 데 어려움이 존재한다. 특히 EN 18031-1과 같이 다수의 세부 평가 항목으로 구성된 인증 규격의 경우, 모든 요구사항을 동일한 수준으로 적용하는 접근 방식은 개발 효율성을 저하시킬 수 있다.

한편, 기존 연구들은 주로 인증 요구사항의 개별 항목 분석이나 정책적 논의에 초점을 맞추고 있어, 개발 단계에서 자원 제약을 고려한 우선순위 기반 적용 방안은 충분히 제시되지 못하였다. 또한 EN 18031-1과 같은 복합적인 인증 기준을 실제 개발 프로세스에 체계적으로 통합하기 위한 방법론 역시 부족한 실정이다.

이에 본 연구는 EN 18031-1의 사이버보안 요구사항을 대상으로, 사이버보안 시험·평가 전문가의 관점에서 평가 항목의 상대적 중요도를 분석하고 우선순위를 도출하는 것을 목적으로 한다. 이를 위해 AHP(Analytic Hier archy Process) 기법을 활용하여 정량적 중요도 분석을 수행하고, 도출된 결과를 국제 보안 설계 표준인 IEC 62443-4-1의 SecureDevelopment Lifecycle(SDL) 프로세스에 적용한다. 나아가 본 연구는 단순한 중요도 분석에 그치지 않고, 우선순위 기반 보안 설계 프레임워크로 체계화함으로써 실제 개발 단계에서 활용 가능한할 수 있는 실무 중심의 적용 방안을 제시한다. 특히 본 연구의 주요 기여는 EN 18031-1 기반 사이버보안 인증 요구사항을 정량적으로 구조화하고 이를 SDL 프로세스에 반영하여 설계 의사결정에 활용 가능한 형태로 제시했다는 점에 있다. 이를 통해 기존 연구에서 부족했던 개발 단계에서의 실질적 적용 가능성을 보완하고, 제한된 자원 환경에서도 효율적인 인증 대응 전략 수립을 지원할 수 있는 실무적 기준을 제공한다.

II. 관련 연구

1. IoT 사이버보안 위협 및 정책 동향

사물인터넷(Internet of Things, IoT)은 고유 식별이 가능한 다양한 물리적 사물이 네트워크를 통해 상호 연결되어 데이터를 수집·전송·처리함으로써 다양한 서비스를 제공하는 융복합 기술로 설명된다[2]. IoT 기술은 스마트홈, 스마트 의료, 산업 자동화 등 다양한 분야로 확산하며 초연결사회(Hyper-Connected Society)의 핵심 기반으로 자리 잡고 있으나, 연결성 확대와 함께 보안 취약성 또한 구조적으로 증가하고 있다. 특히 소비자용 IoT 무선기기에서는 인증 메커니즘의 부재, 취약한 비밀번호 사용, 안전하지 않은 펌웨어 업데이트 절차 등으로 인해 개인정보 유출, 원격 제어 탈취, 서비스 장애와 같은 사이버보안 위협이 지속적으로 보고되고 있다[3]. 이러한 IoT 무선기기의 사이버보안 위협은 기술적 구조에 따라 기기(Device) 계층, 네트워크 계층, 플랫폼 및 서비스 계층으로 구분할 수 있다. 기기 계층에서는 하드 코딩된 인증 정보, 암호화되지 않은 저장 데이터 등이 주요 위협 요소로 지적되며, 네트워크

계층에서는 평문 통신, 중간자 공격 등의 위협이 존재한다.

정책적인 측면에서도 주요국은 이러한 위협에 대응하기 위해 제도적 보안 체계를 강화하고 있다. 미국은 CISA 전략계획을 중심으로 사이버 사고 대응 역량 고도화를 추진하고 있으며[4], EU는 CRA(Cyber Resilience Act)를 공표하여 제품 설계 단계에서부터 보안을 내재화하는 Security by Design 원칙을 의무화하고 있다. 국내의 경우 2022년 법제화를 통해 IoT 제품 정보보호 인증 제도를 운용 중이나, EU와의 상호인정(MRA)은 아직 미체결 상태이다. 표 1은 국내 인증 제도와 EU 규격의 주요 특성을 비교한 것이다.

표1. 국내 인증 제도 및 EU 규격 주요 특성

구분	국내 (KISA IoT 보안 인증)	EU (EN 18031-1 / RED)
인증 유형	자율(임의) 인증	의무 인증 (2025년 8월)
법적 근거	정보통신망법	Radio Equipment Directive (RED)
주요 요구사항	7개 영역, 50개 세부 항목	7개 평가 영역, 19개 세부 기준
국제 정합성	ITU-T 국제표준 채택	EN 18031-X, CRA 연계
상호인정 (MRA)	일부 국가와 추진 중	EU 내 공통 적용

2. EN 18031-1 요구사항

EN 18031-1은 RED의 사이버보안 요구사항을 충족하기 위해 IoT 무선기기의 보안성을 평가하는 표준으로, 적용 대상 장비의 범위, 보호해야 할 자산 유형, 적합성 평가 절차 및 구체적인 보안 요구사항을 규정하고 있다[1]. 본 표준의 요구사항은 ① 접근제어 메커니즘, ② 인증 메커니즘, ③ 보안 업데이트 및 저장 메커니즘, ④ 보안 통신 메커니즘, ⑤ 복원력·네트워크 모니터링·트래픽 제어 메커니즘, ⑥ 기밀 암호 키, ⑦ 일반 장비 기능 등 7개 평가 영역으로 구성된다[1].

IEC 62443-4-1(SDL)은 산업 제어시스템 및 관련 제품을 대상으로 하는 SDL 표준으로, 보안 관리, 보안 계획, 요구사항 정의, 설계, 구현, 검증, 확인, 유지관리 등 제품 생명주기 전 단계에서 수행해야 할 보안 활동을 규정하고 있다[5].

3. AHP 기법 관련 선행 연구

신영진(2019)은 IoT 시대에 적합한 개인정보보호정책의 우선순위를 분석하여, 정책적 측면 > 기술적 측면 > 운영 측면 순의 우선순위를 제시하였다[6]. 강다연·황종호(2019)는 KISA IoT 보안 시험 인증 기준을 토대로 인증, 암호, 데이터 보호 등 5가지 항목의 우선순위를 분석하였으며, 개인정보보호가 가장 높은 우선순위로 도출되었다[7]. 윤석진·김정덕(2019)은 Home IoT 가전의 보안 위협 모델링을 통한 보안 요구사항 분석에서 설계 기반의 보안 검증 절차가 필요함을 제시하였으며[8], 이동혁·박남제(2016)는 개발단계에서의 보안 설계와 정책적 보안 관리의 병행이 중요하다고 제안하였다[9]. 기존 연구들은 국내 인증 기준(KISA)을 중심으로 분석하거나, 정책·관리적 측면에 초점을 맞추었다. 본 연구는 EU 의무 인증 표준인 EN 18031-1을 대상으로 실제 시험·평가자 관점에서 중요도를 분석하고, 그 결과를 IEC 62443-4-1(SDL)과 연계한다는 점에서 차별성을 갖는다.

III. 본 론

1. 연구 설계 및 AHP 모형

본 연구는 EN 18031-1에 제시된 보안 요구사항을 체계적으로 분석하고, 각 요구사항의 상대적 중요도를 정량적으로 도출한 뒤, 그 결과를 IEC 62443-4-1(SDL)과 연계하여 우선순위 기반 보안 설계 프로세스를 제안하는 것을 목표로 한

다. AHP는 복수의 평가 기준을 계층적으로 구조화하고, 의사결정자의 쌍대비교 판단을 통해 각 기준의 상대적 중요도를 산출하는 다기준 의사결정 기법이다[10]. 본 연구에서는 EN 18031-1의 보안 요구사항을 7개 상위 평가 영역(계층 1)과 19개 세부 기준(계층 2)으로 계층화하였다. AHP 분석 모형은 EN 18031-1의 7개 평가 영역을 계층 1 요인으로, 각 영역에 속하는 세부 기준 19개를 계층 2 평가 요인으로 구성하였다. 그림 1은 분석 모형이다.

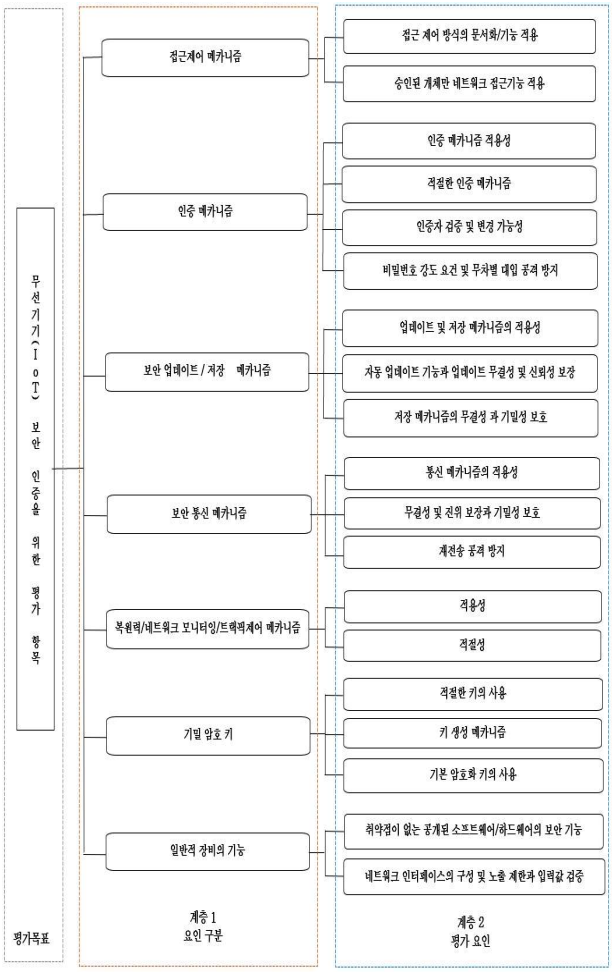


그림1. 분석 모형

2. 세부 기준 정의

표 2는 EN 18031-1의 7개 평가 영역에 포함된 19개 세부 기준을 정의한 것이다. 각 세부 기준은 British Standards Institution(2024)의 BS EN 18031-1 표준 문서를 기반으로 작성되었다[1].

표2. 세부 기준 정의

평가 영역	세부 기준	내용
접근제어 메커니즘	승인된 개체의 네트워크 접근	인증된 사용자·장치만 접근허용
	접근 제한/해제 기능	접근권한 제어 정책 적용
	사용자 정의 접근제어	역할 기반 접근제어 지원
인증 메커니즘	네트워크 접근 인증 방식	MFA, PKI 등 강인한 인증 체계
	사용자 정의 인증	사용자별 인증 설정 지원
	인증 정보 안전 저장	인증 자격 증명의 암호화 보관
보안 업데이트 및 저장	업데이트 메커니즘 적용성	무결성 검증된 업데이트 제공
	업데이트 검증 기능	서명 기반 업데이트 배포
보안 통신 메커니즘	통신 메커니즘 적용성	TLS 1.3 이상 암호화 통신
	통신 무결성 검증	데이터 위변조 방지
복원력· 모니터링	복원력 적용성	장애 후 신속 복구 기능
	네트워크 모니터링	이상 트래픽 탐지 기능
기밀 암호 키	적절한 키 사용	안전한 키 생성·분배·폐기
	키 생성 메커니즘	암호학적으로 안전한 키 생성
일반 장비 기능	취약점 없는 SW/HW	오픈소스 보안 취약점 사전 검증
	보안 기능 최소화	불필요한 기능 비활성화

3. AHP 설문 설계 및 자료 수집

AHP 설문에서는 Saaty(1980)가 제안한 9점 척도를 활용하여 각 계층 내 평가 항목 간 상대적 중요도를 쌍대비교 방식으로 측정하였다[11]. 설문 응답을 바탕으로 쌍대비교 행렬을 구성한 후, 각 행렬에 대해 고유벡터를 산출하여 항목별 상대적 가중치를 도출하였다.

유효성 검증은 일관성 비율(Consistency Ra tio, CR)과 일관성 지수(Consistency Index, C I)로 확인한다. CI와 CR은 식(1), (2)와 같이 정의된다.

$$CI = (\lambda max - n) / (n - 1) \quad \cdots\cdots\cdots (1)$$

$$CR = CI / RI \quad \cdots\cdots\cdots (2)$$

Saaty(1990)에 따르면 CR ≤ 0.1일 경우 합리적인 일관성을 갖는 것으로 판단한다[12].

본 연구의 전문가 설문 대상은 한국인정기구(KOLAS)에 등록된 시험기관의 IoT 무선기기 사이버보안 시험·인증 담당 시험 관리자 및 평가자 13명을 선정하여 진행하였다. 설문 시점이 EU 사이버보안 인증 의무화(2025년 8월) 초기로 타 기관의 참여가 제한되어 단일 기관에 소속된 전문가 집단을 대상으로 하였으며, 해당 기관은 비교 숙련도 평가를 통해 타 기관과 동등한 시험·평가 수준을 갖춘 전문가 집단으로 판단되어 조사 대상으로 선정하였다.

Ⅳ. 실험 결과 및 고찰

1. 일관성 검증 결과

본 연구에서 수행한 AHP 분석의 신뢰성을 확보하기 위해 설문 응답에 대한 일관성 검증을 수행하였다. 표 3과 같이 모든 분석 대상 응답이 허용 수준인 CR ≤ 0.1을 충족하는 것으로 확인되었다. 이는 설문 응답자가 평가 항목 간 중요도를 비교하는 과정에서 논리적 일관성을 유지하였음을 의미한다.

표3. AHP 일관성 검증 결과

항목		λ max	CI	CR
계층 1 요인 (평가 영역)		7.584	0.097	0.074
계층 2 요인 (세부 기준)	접근제어 메커니즘	2.000	0.000	-
	인증 메커니즘	4.189	0.063	0.070
	보안 업데이트/ 저장 메커니즘	3.026	0.013	0.023
	보안 통신 메커니즘	3.024	0.012	0.020
	복원력/ 네트워크 모니터링/ 트래픽 제어 메커니즘	2.000	0.000	-
	기밀 암호키	3.038	0.019	0.032
	일반적 장비의 기능	2.000	0.000	-

2. 계층 1 가중치 분석 결과

EN 18031-1의 보안 요구 항목인 계층 1(평가 영역)에 대한 가중치 분석 결과, 가장 높은 중요도를 보인 항목은 접근제어 메커니즘으로 가중치 0.284를 기록하였다. 이는 전체 평가 항목 중 1순위로, 인증된 주체만이 시스템 자원에 접근할 수 있도록 제한하는 구조적 설계의 중요성이 가장 높게 인식되고 있음을 의미한다. 두 번째로 높은 중요도를 보인 항목은 보안 통신 메커니즘(0.227)이며, 세 번째는 인증 메커니즘(0.202)으로 분석되었다. 이 세 항목이 전체 가중치의 0.713(전체의 약 71%)을 차지하여, IoT 무선기기 제품 개발 과정에서 집중적인 설계 검토가 필요한 핵심 영역임을 확인하였다. 표 4는 계층 1 평가 영역 가중치 분석 결과이다.

표4. 계층 1 평가 영역 가중치 분석 결과

계층 1 우선순위 중요도	가중치	순위
접근제어 메커니즘	0.284	1
인증 메커니즘	0.202	3
보안 업데이트/저장 메커니즘	0.073	4
보안 통신 메커니즘	0.227	2
복원력/네트워크 모니터링/ 트래픽 제어 메커니즘	0.067	5
기밀 암호키	0.062	6
일반적 장비의 기능	0.036	7

3. 계층 2 가중치 분석 결과

평가 영역에 대한 세부 기준인 계층 2에 대한 가중치 분석 결과, 접근제어 메커니즘 영역에서는 승인된 개체만 네트워크 접근 허용 항목이 0.672로 가장 높게 도출되었다. 인증 메커니즘 영역에서는 네트워크 접근 시 인증 방식적

용이 0.467로 가장 높은 중요도를 보였다. 보안 통신 메커니즘 영역에서는 통신 메커니즘 적용성이 0.549로 가장 높은 비중을 차지하였다. 표 5는 계층 2 가중치 분석 결과이다.

표5. 계층 2 세부 기준 가중치 분석 결과

계층 1	계층 2		
항목	항목	가중치	순위
접근제어 메커니즘	접근 제어방식의 문서화 / 기능 적용	0.207	2
	승인된 개체만 네트워크 접근기능 적용	0.672	1
인증 메커니즘	네트워크 접근 과정의 인증 방식 적용	0.467	1
	사용자 인터페이스 접근 과정의 인증 방식 적용	0.232	2
	인증자 검증 및 변경 가능성	0.141	3
	비밀번호 강도 요건 및 무차별 대입 공격 방지	0.103	4
보안 업데이트 / 저장 메커니즘	업데이트 및 저장 메커니즘의 적용성	0.488	1
	자동 업데이트 기능과 업데이트 무결성 및 신뢰성 보장	0.268	2
	저장 메커니즘의 무결성과 기밀성 보호	0.226	3
보안통신 메커니즘	통신 메커니즘의 적용성	0.549	1
	무결성 및 진위 보장과 기밀성 보호	0.217	2
	재전송 공격 방지	0.196	3
복원력/ 네트워크 모니터링/ 트래픽 제어 메커니즘	적용성	0.520	1
	적절성	0.357	2
기밀 암호 키	적절한 키의 사용	0.458	1
	키 생성 메커니즘	0.263	2
	기본 암호화 키의 사용	0.248	3
일반적 장비의 기능	취약점이 없는 공개된 소프트웨어/ 하드웨어의 보안 기능	0.644	1
	네트워크 인터페이스의 구성 및 노출 제한과 입력값 검증	0.318	2

4. 종합 가중치 및 우선순위 도출

각 계층별 가중치를 종합한 결과, 접근제어 메커니즘의 승인된 개체만 네트워크 접근 허용이 종합 가중치 0.191로 최우선 순위로 도출되었다. 이는 IoT 무선기기가 전파 기반 통신 환경에서 운용되는 특성상 네트워크 경계가 물리적으로 명확하지 않아 외부 공격에 취약하다는 점을 반영한 결과이다. 다음으로 보안 통신의 통신 메커니즘 적용성이 0.125, 인증 메커니즘의 네트워크 접근 인증 방식 적용이 0.094 순으로 높은 종합 가중치를 보였다. 표 6은 종합 가중치 분석 결과이다.

표6. 종합 가중치 분석 결과

계층 1			계층 2			종합 평가	
항목	가중치 (A)	순위	항목	가중치 (B)	순위	종합가중치 (AxB)	순위
접근 제어 메커니즘	0.284	1	접근 제어방식의 문서화 / 기능 적용	0.207	2	0.059	4
			승인된 개체만 네트워크 접근기능 적용	0.672	1	0.191	1
인증 메커니즘	0.202	3	네트워크 접근 과정의 인증 방식 적용	0.467	1	0.094	3

			사용자 인터페이스 접근 과정의 인증 방식 적용	0.232	2	0.047	6
			인증자 검증 및 변경 가능성	0.141	3	0.028	10
			비밀번호 강도 요건 및 무차별 대입 공격 방지	0.103	4	0.021	14
보안 업데이트/저장 메커니즘	0.073	4	업데이트 및 저장 메커니즘의 적용성	0.488	1	0.036	8
			자동 업데이트 기능과 업데이트 무결성 및 신뢰성 보장	0.268	2	0.020	15
			저장 메커니즘의 무결성 과 기밀성 보호	0.226	3	0.016	16
보안 통신 메커니즘	0.227	2	통신 메커니즘의 적용성	0.549	1	0.125	2
			무결성 및 진위 보장과 기밀성 보호	0.217	2	0.049	5
			재전송 공격 방지	0.196	3	0.044	7
복원력/네트워크 모니터링/트래픽 제어 메커니즘	0.067	5	적용성	0.520	1	0.035	9
			적절성	0.357	2	0.024	12
기밀 암호키	0.062	6	적절한 키의 사용	0.458	1	0.028	11
			키 생성 메커니즘	0.263	2	0.016	17
			기본 암호화 키의 사용	0.248	3	0.015	18
일반적 장비의 기능	0.036	7	취약점이 없는 공개된 소프트웨어/하드웨어의 보안 기능	0.644	1	0.023	13
			네트워크 인터페이스의 구성 및 노출 제한과 입력값 검증	0.318	2	0.011	19

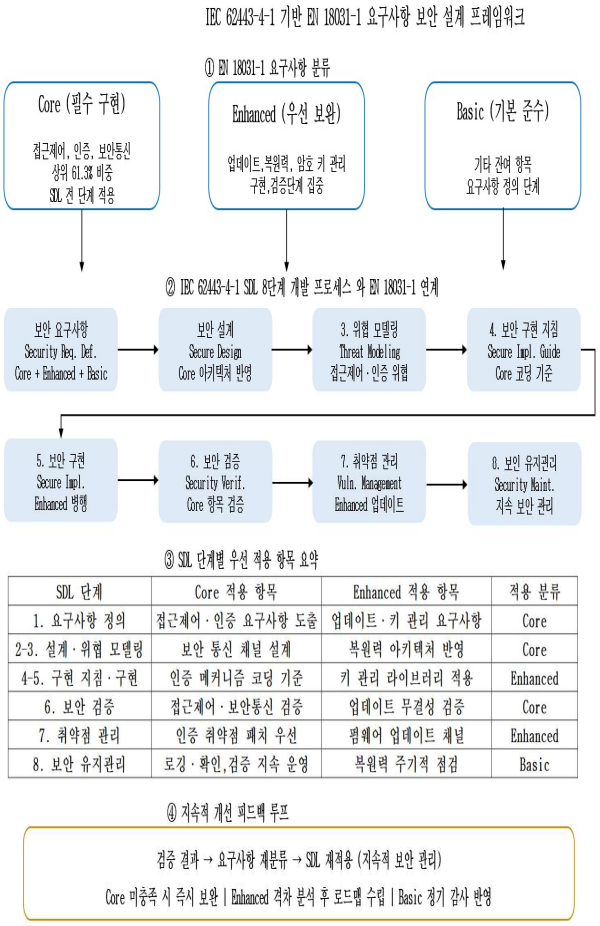
5. 우선순위 기반 보안 설계 방법

분석 결과를 바탕으로 EN 18031-1 요구사항을 세 단계로 분류하여 IEC 62443-4-1(SDL) 기반 보안 설계 프로세스에 적용할 것을 제안한다. 접근제어·인증·보안 통신(합산 가중치 0.713, 전체의 약 71%)은 필수 구현 항목(Core)으로 분류한다. 합산 가중치 0.713(전체의 약 71%)이 이 세 영역에 집중되어 있다는 것은 AHP 분석을 통해 도출된 정량적 근거로, 전문가들이 IoT 무선기기 보안에서 이 세 영역을 압도적으로 중요하게 인식하고 있음을 반영한다. 업데이트·복원력·키 관리는 우선 보완 항목(Enhanced), 나머지는 기본 준수 항목(Basic)으로 분류한다. 표 7은 SDL 단계별 우선 적용 항목을 요약 정리한 것이다.

표7. SDL 단계별 우선 적용 항목 요약

SDL 단계	Core 적용 항목	Enhanced 적용 항목	적용 분류
1. 요구사항 정의	접근제어·인증 요구사항 도출	업데이트·키 관리 요구사항	Core
2-3. 설계·위협 모델링	보안 통신 채널 설계	복원력 아키텍처 반영	Core
4-5. 구현 적용·구현	인증 메커니즘 코딩 기준	키 관리 라이브러리 적용	Enhanced
6. 보안 검증	접근제어·보안 통신 검증	업데이트 무결성 검증	Core
7. 취약점 관리	인증 취약점 패치 우선	펌웨어 업데이트 채널	Enhanced
8. 보안 유지관리	로깅·확인, 검증 지속 운영	복원력 주기적 점검	Basic

이와 같이 도출된 세 단계의 분류체계는 단순한 중요도 순서의 나열에 그치지 않고, 실제 개발 프로세스에서 단계별로 적용할 수 있는 설계 기준으로 구체화할 필요가 있다. 이를 위해 표 7과 같이 IEC 62443-4-1(SDL)의 8단계 개발 프로세스와 EN 18031-1 요구사항을 연계하여, 각 개발단계에서 우선하여 반영해야 할 항목을 체계적으로 구체화하였다. Core 항목은 SDL 초기 단계인 요구사항 정의 및 설계 단계부터 반드시 반영되어야 하며, Enhanced 항목은 구현 및 취약점 관리 단계에서 집중하여 적용하고, Basic 항목은 유지관리 단계에서 지속적으로 준수한다.



SDL 단계	Core 적용 항목	Enhanced 적용 항목	적용 분류
1. 요구사항 정의	접근제어 · 인증 요구사항 도출	업데이트 · 키 관리 요구사항	Core
2-3. 설계 · 위협 모델링	보안 통신 채널 설계	복원력 아키텍처 반영	Core
4-5. 구현 지침 · 구현	인증 메커니즘 코딩 기준	키 관리 라이브러리 적용	Enhanced
6. 보안 검증	접근제어 · 보안통신 검증	업데이트 무결성 검증	Core
7. 취약점 관리	인증 취약점 패치 우선	펌웨어 업데이트 채널	Enhanced
8. 보안 유지관리	로깅 · 확인,검증 지속 운영	복원력 주기적 점검	Basic

그림2. SDL 기반 요구사항 보안 설계 프레임워크

그림 2는 IEC 62443-4-1 기반 EN 18031-1 요구사항 보안 설계 프레임워크를 도식화한 것으로, ① EN 18031-1 요구사항 3단계 분류, ② SDL 8단계 프로세스 연계, ③ 단계별 우선 적용 항목, ④ 지속적 개선 피드백 루프의 4개 레이어로 구성된다. Core(접근제어·인증·보안 통신)는 전체 가중치의 0.713(전체의 약 71%)을 차지하는 항목으로, SDL 전 단계에 걸쳐 우선 적용된다. Enhanced(업데이트·복원력·키 관리)는 구현 및 검증 단계에 집중 배치되며, Basic (로깅·확인, 검증 등 잔여 항목)은 유지관리 단계에서 기본 준수한다. 피드백 루프는 검증 결과를 요구사항 재분류에 반영하는 지속적 개선 사이클을 의미한다.

6. 고 찰

분석 결과를 종합하면, IoT 무선기기 보안 인증 체계의 합리적인 설계를 위해서는 ① 접근제어 및 통신 보호기능을 우선으로 반영하고, ② 인증 절차의 기술적 고도화를 추진하며, ③ 보안 업데이트 및 유지관리 체계를 체계화하고, ④ 암호 키 관리 프로세스를 설계 단계에서부터 내재화할 필요가 있다.

본 연구 결과는 기존 선행 연구와도 정합성을 보인다. 승인된 개체만 접근을 허용하고 데이터 보호를 강화해야 한다는 결과는 강다연·황종호(2019)의 연구와 일치하며[7], 개발단계에서 보안성 검토와 설계 기반 검증 절차가 필요하다는 점에서 윤석진·김정덕(2019)의 연구와도 일치한다[8]. 다만, 본 연구의 결과는 제한된 표본을 기반으로 도출된 것으로, 실제 제품 개발 환경에 적용 시 개발 조직의 특성에 맞게 조정될 필요가 있다.

스마트미디어 환경에서 IoT 기기는 스마트TV, 커넥티드 카메라, 웨어러블 기기 등 다양한 미디어 플랫폼과 연동되는 구조를 갖는다. 이러한 맥락에서 접근제어 및 인증 메커니즘의 우선 설계는 단순한 기기 보안을 넘어 미디어 서비스 생태계 전반의 신뢰성과 직결되는 핵심 과제임을 확인할 수 있다.

V. 결 론

본 연구는 EU의 사이버보안 규격 EN 18031-1의 요구사항을 체계적으로 분석하고, AHP 기법을 통해 사이버보안 시험·평가 전문가 관점에서

평가 항목의 중요도 우선순위를 도출하였다. 분석 결과, 접근제어 메커니즘(0.284), 보안 통신 메커니즘(0.227), 인증 메커니즘(0.202)이 상위 3개 항목으로 선정되었으며, 이들의 합산 가중치는 0.713(전체의 약 71%)으로 나타났다. 종합 가중치에서는 승인된 개체만 네트워크 접근 허용이 0.191로 최우선 순위를 기록하였다.

도출된 중요도 우선순위를 IEC 62443-4-1 (SDL)의 8단계 개발 프로세스와 연계하여, Core/Enhanced/Basic 3단계 분류 기반의 우선순위 보안 설계 방법을 제안하였다. 이러한 방안은 자원 제약 환경에서도 인증 대응 효율성을 향상시키고, 개발 초기 단계에서 보안 요구사항을 우선순위에 따라 체계적으로 반영할 수 있도록 지원한다. 또한, 2025년 8월부터 시행 중인 EU 사이버보안 인증 의무화에 대응하는 실무적 기준을 제공하며, 2027년 CRA 시행에 대비한 사전 보안 설계 근거로도 활용될 수 있다. 한편, 실무적으로는 초기 인증 관련 정보가 제한적인 상황에서 개발자와 기업이 인증 준비 과정에서 참고할 수 있는 기준을 제공하며, 중소 IoT 기업의 인증 준비 부담을 완화하는 데 기여할 것으로 기대된다. 향후 연구에서는 제안된 보안 설계 모델을 실제 제품 개발 사례에 적용하여, 개발 일정 단축 및 인증 준비 효율성 향상 여부를 검증하는 실증 연구를 수행할 필요가 있다.

REFERENCES

[1] British Standards Institution, *BS EN 18031-1:2024 - Common security requirements for radio equipment: Internet connected radio equipment,* BSI Standards Limited, 2024.

[2] 김호원, 민경식, 박진상, “지능형 IoT 사회의 보안 이슈 분석: 디바이스 보안을 중심으로”, *KISA Insight,* 2022 제5권, 171-207쪽, 2022년 12월

[3] 백기승, “홈 가전 IoT 보안가이드”, *KISA 디지털 제품 보안 가이드라인*, 12-13쪽, 2017년 8월

[4] 김도원, 하병욱, 김성훈, “미국·EU·영국 등의 사이버보안 전략 분석 및 시사점”, *KISA Insight,* 2023 제1권, 2-13쪽, 2023년 2월

[5] International Electrotechnical Commission, *IEC 62443-4-1:Security for industrial automation and control systems-Part 4-1: Secure product development lifecycle requirements,* IEC, 2018.

[6] 신영진, “사물인터넷시대에 적합한 개인정보보호정책의 우선순위분석”, *한국지역정보화학회지*, 제22권 제2호, 25-57쪽, 2019년 6월

[7] 강다연, 황종호, “IoT 보안 인증서비스 인증기준 중요도 우선순위에 관한 연구”, *한국콘텐츠학회 논문지,* 제19권, 제7호, 13 - 21쪽, 2019년 7월

[8] 윤석진. *“Home IoT 가전기기의 보안성 향상을 위한 Security Development Lifecycle 적용 연구”, 중앙대학교 대학원 석사학위논문,* 2019년 8월

[9] 이동혁, 박남제, “IoT 제품 보안 인증 및 보안성 유지관리방안”,*한국통신학회지*, 제33권, 제12호, 28-34쪽, 2016년 12월

[10] 노경민, *“AHP 기법 및 로지스틱 회귀분석을 통한 승강기 안전품질 진단 예측 모형 개발”, 경상국립대학교 대학원 박사학위논문*, 2025년 2월

[11] T. L. Saaty, *The analytic hierarchy process*, New York, NY, USA: McGraw-Hill, 1980.

[12] T. L. Saaty, “How to make a decision: The analytic hierarchy process,” *European Journal of Operational Research*, vol. 48, no. 1, pp. 9-26, Sep. 1990.

저 자 소 개

윤호상(정회원)

국민대학교 전자공학과 졸업(공학사).
경희대학교 AI 기술경영학과 석사 졸업.
주식회사 에이치시티 연구소장

<주관심분야 : 빅데이터, 인공지능(AI), 기술경영, 사이버보안, EMC>

허봉재(정회원)

조선대학교 전자공학과 학사 졸업.
연세대학교 경영학과 석사 졸업.
주식회사 에이치시티 대표이사

<주관심분야 : 빅데이터, 인공지능(AI), 기술경영 >

홍아름(정회원)

서울대학교 경영학 석사 졸업.
서울대학교 경영학 박사 졸업.
경희대학교 AI 기술경영학과, 교수

<주관심분야 : 빅데이터 분석, AI 데이터 품질, 생성형 모델, 기술정책>