

개인정보보호 정책 및 기술 아이디어 공모 서식

구 분	주요내용
공모 주제	IoT 환경에서의 개인정보 보호
제안 배경	<p>현재 우리나라에는 사물인터넷(IoT) 보안과 관련된 명확한 법률이 제정되어 있지 않으며, 한국인터넷진흥원(KISA)과 미래창조과학부에서 제공하는 가이드라인만 존재한다. IoT 보안 인증제도가 운영 중이지만, 2024년 10월 기준으로 대기업과 해외 기업의 인증 신청이 없고 중소기업의 참여율 또한 저조하다. 이러한 문제는 현행 인증제도가 자율적 운영에 기반하고 있어 강제력이 부족하기 때문이다. 따라서 IoT 보안 인증제도의 실효성을 높이기 위해 법적 기반 마련과 강제적 참여 유도가 필요하다.</p>
주요 내용	<p>IoT 기술이 빠르게 발전하면서 보안 위협도 증가하고 있다. 2016년 미국의 인터넷 호스팅 업체 Dyn에 대한 DDoS 공격과 2022년 국내 아파트 월패드 해킹 사건은 보안이 취약한 IoT 기기들이 악용되어 심각한 피해를 일으킨 대표적인 사례다. 이러한 사건들은 사생활 침해와 서비스 마비를 초래하며 IoT 보안 강화의 필요성을 보여준다.</p> <p>국내에서는 사물인터넷 보안 관련 법률이 부족한 상황이다. KISA와 일부 기관에서 가이드라인을 제공하고 있지만 강제력이 없어 보안 인증 참여율이 저조하다.</p> <p>이 문제를 해결하기 위해 '지능형 홈네트워크 설비 설치 기준'에 IoT 보안 항목을 추가하는 것이 필요하다. 새로운 제도를 만드는 대신 기존 인증제도를 활용하면 효율적으로 보안을 강화할 수 있다. 기술 기준과 사후 관리를 통해 보안을 체계적으로 유지하면 보안 위협을 사전에 예방하고 신속하게 대응할 수 있다.</p> <p>또한, 보안 체크리스트를 도입해 IoT 기기와 인프라를 점검해야 한다. DDoS 공격 방지, 안전한 인증 정보 관리, 기기 인증 등을 철저히 확인하면 보안성을 강화하고, 보안 위협에 더욱 효과적으로 대응할 수 있다.</p>
기대 효과	IoT 환경에서 발생할 수 있는 보안 위협을 예방하고, DDoS 공격이나 개인정보 유출과 같은 사고를 줄일 수 있다. 특히 '지능형 홈네트워크 설비 설치 기준'과 같은 법적 기준을 강화해 사

	<p>용자들이 더 안전하게 스마트 기술을 사용할 수 있도록 한다. 또한 보안 체크리스트를 도입해 보안 위험을 사전에 점검하고, 문제가 발생했을 때 신속하고 투명하게 대응하여, 이를 통해 사 용자 신뢰를 높이고, IoT 기술의 지속적인 발전에 긍정적인 영 향을 줄 수 있다.</p>
참고 문헌	<p>KISA 한국인터넷진흥원 - IoT 공통보안가이드</p> <p><논문> 사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안 사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대 응 방안 사물인터넷환경에서의 스마트홈 서비스 침해 위협 분석 및 보 안 대책 연구</p>