중부대학교

IoT 환경 속 개인정보 보호 제도 개선 제안서

목 차

제1장. IoT 법안 필요성

1.1 국내 및 국외 사례

- 월패드 해킹 사건 (2022년)

  40만 개 이상의 아파트 월패드가 해킹당한 사건은 IoT 기기의 보안 취약점을 극명히 보여주는 사례이다. 해커는 인터넷 공유기를 경유해 아파트 관리 서버에 침투한 후, 월패드에 악성 프로그램을 설치하여 개인 정보 및 가정 내 영상 데이터를 탈취하였다. 이러한 사건은 보안 강화의 필요성과 중앙 관리형 IoT 시스템의 위험성을 시사한다.

  - 문제점 : 초기 설정 비밀번호가 변경되지 않거나, 보안 패치가 부족한 환경에서 이러한 해킹 시도가 가능하다.
  - 결과 : 다수의 가구가 사생활 침해를 경험하였으며, 개인정보 유출로 인한 2차 피해 우려가 제기된다.

- Mirai 봇넷을 이용한 DDoS 공격 (2016년)

  해커들은 감염된 IoT 기기를 봇넷으로 연결해 미국 동부 지역의 주요 웹사이트(예: CNN, Amazon, Netflix)를 대상으로 대규모 분산 서비스 거부(DDoS) 공격을 감행하였다. 이 공격으로 인해 수백 개의 웹사이트가 몇 시간 동안 다운되었으며, 서비스 제공자들에게 막대한 피해를 입혔다.

  - 문제점 : 보안 취약점을 가진 IoT 기기가 대규모 사이버 공격의 도구로 활용되었다.
  - 결과 : IoT 보안 강화 및 국제적 협력의 중요성이 대두되었다.

1.2 외국 법안

- 영국 PSTI 법

  2022년에 도입된 PSTI(Product Security and Telecommunications Infrastructure) 법은 IoT 기기의 보안을 강화하기 위한 종합적인 법률이다.

  - 주요 내용 :
    - 기본 비밀번호 금지: IoT 기기는 고유 비밀번호를 제공해야 하며, 초기 설정 단계에서 강력한 비밀번호로 변경이 필수이다.
    - 보안 업데이트 기간 공개: 제조사는 기기의 보안 업데이트 지원 기간을 명시해야 한다.
    - 취약점 보고 정책: 보안 취약점 발생 시 이를 보고하고 해결할 책임을 부과한다.
  - 효과: 규정을 위반한 제조업체는 민사적 또는 형사적 처벌을 받을 수 있으며, 영국 내 유통이 제한된다.

- 미국 IoT Cybersecurity Improvement Act (2020년)

  미국 연방 정부가 사용하는 IoT 기기의 보안 기준을 의무화한 법안으로, 최소한의 보안 표

준을 준수하도록 요구한다.

- 주요 내용 :
  - 연방 정부와 계약하는 기업은 IoT 기기 보안 요건을 충족해야 하며, 이를 위반하면 계약상 불이익을 받는다.
  - 보안 인증, 데이터 암호화, 취약점 패치 등 보안 기본 사항 준수를 요구한다.
- 한계: 연방 정부 기기에만 적용되며 민간 부문에는 강제되지 않는다. 그러나 민간 기업들도 이를 모범 사례로 삼아 자발적으로 도입하고 있다.

- 시사점:

  외국의 사례는 IoT 보안 강화를 위해 구체적인 법적 기준을 마련하고 강제성을 부여한 점에서 참고할 만하다. 국내에서도 이와 유사한 법안을 도입해 사전 예방적 보안 조치를 강화하고, 법적 제재를 통해 제조사 및 유통업체의 책임감을 높이는 것이 필요하다.

제2장. 적용 가능 법안 소개

2.1 국내 IoT 보안 인증제도의 현황

• 현재 KISA가 주관하는 IoT 보안 인증제도가 운영되고 있으나, 다음과 같은 문제점이 존재한다.

  • 참여율 저조: 인증은 자발적으로 진행되며, 강제성이 없어 많은 기업이 참여하지 않는다.

  • 보안 항목 부족: 기존 인증제도는 주로 전기 안전 및 품질 기준에 초점이 맞춰져 있으며, 사이버 보안 항목은 부재하다.

- 개선 방향:
  - 기존 KC 인증에 보안 관련 항목 추가(예: 암호화, 인증 절차, 취약점 관리).
  - 인증 미준수 기업에 대한 제재 도입 및 소비자 보호를 위한 보안 인증 의무화.

2.2 새로운 법적 제도 제안

- 법률 프레임워크:

  1. IoT 보안 최소 기준 의무화:
     - 초기 설정 단계에서 비밀번호 변경 강제.
     - 데이터 전송 암호화(TLS 1.3 이상) 및 저장 데이터 암호화(AES-256 적용).
     - 정기적인 소프트웨어 업데이트 제공 및 무결성 검증.

  2. 기업 책임 강화:
     - 보안 취약점 발견 시 보고 의무화 및 신속한 패치 제공(48시간 내).
     - 보안 기준 미준수 시 행정적 또는 법적 제재 부과.

  3. 소비자 보호 조치:
     - 보안 사고 발생 시 제조사 또는 유통사가 소비자 피해를 보상할 의무를 명시.
     - 보안 결함으로 인한 중대한 사고 발생 시 제품 리콜 의무화.

- 효율성 제고 방안:

  • 영국 PSTI 법처럼 단독 법안을 마련하기보다는, 기존 인증 제도에 보안 요건을 추가해 기업의 부담을 줄이면서 실효성을 확보하는 것이 효과적이다.

  • 국제 표준(예: ISO/IEC 27001, ETSI EN 303 645)을 참고하여 국내 인증 기준과의 호환성을 강화해야 한다.

제3장. 보안성 검토를 위한 체크리스트

구분	항목	세부 내용	결과
초기 설정 보안	안전한 인증 정보 강제	초기 설치 시 강력한 비밀번호 설정을 강제하는가?	
		비밀번호 미설정 시 기기 작동을 제한하도록 설계되었는가?	
	비밀번호 설정 인터페이스	직관적이고 사용자 친화적인 비밀버호 설정 인터페이스 (NFCM QR코드, 버튼 등)를 제공하는가?	
		비밀번호 설정 시 강도 검증 및 약한 비밀번호 경고 기능을 포함하는가?	
보안 업데이트 및 유지관리	자동화된 업데이트 기능	보안 취약점 대응을 위한 자동 업데이트 기능 제공여부	
		업데이트 과정에서 파일의 무결성 및 출처인증이 보장되는가?	
	업데이트 후 보안 강화	기존 설정보다 강화된 보안 옵션을 제공하는가?	
데이터 전송 및 기기 인증	데이터 전송 보호	네트워크 분리 상태에서도 안전한 업데이트가 가능한가?	
		TLS, DTLS 등의 암호화 프로토콜을 사용하여 데이터 전송을 보호하는가?	
	기기 인증	IoT 기기가 상호 인증 기능을 지원하며 국가/국제 표준 (ISO/IEC 등)을 준수하는가?	
		기기 ID 또는 디지털 인증서를 통해 각 기기를 고유하게 식별하고 인증할 수 있는가?	
네트워크 및 장치 보안	DDoS 방어 기능	IoT 기기와 네트워크가 대량의 트래픽으로 인한 서비스 거부 공격 (DDoS)을 탐지하고 방어할 수 있는가?	
		DDoS 공격 방지를 위해 네트워크 트래픽 제한 및 필터링 설정이 가능한가?	
		DDoS 완화 솔루션(예 : 클라우드 기반 DDoS 방어 서비스)을 활용하여 대규모 공격에 대비하고 있는가?	
	봇넷 활동 탐지 및 차단	Botnet 활동(비인가 명령 실행, 이상 트래픽 전송 등)을 탐지하고 차단할 수 있는가?	
		봇넷 활동 탐지를 위해 IDS/IPS(침입 탐지/ 방지 시스템) 또는 AI기반 분석 기술을 활용하고 있는가?	
		홈게이트웨이와 단지 서버가 IoT 기기의 원격 제어 명령을 감시하며 비인가 접근 시 즉각 차단할 수 있는가?	
	보안 업데이트	봇넷 및 DDoS 공격에 의해 발생할 수 있는 취약점을 막기 위해 정기적인 보안	

		업데이트 기능이 제공되는가?	
물리적 보안 및 유지관리	홈게이트웨이 보안	홈게이트웨이가 데이터 통신의 안전성을 보장하는 보안 프로토콜을 준수하며, 안전한 파라미터가 설정되어 있는가?	
		비인가 접근 시 자동으로 네트워크 차단 및 사용자에게 알림 제공이 가능한가?	
	단지 서버 보호	단지 서버가 비인가 데이터 접근 및 보안 위협 탐지/차단 기능을 포함하는가?	
		보안 위협 발생 시 실시간 모니터링과 로그 저장 기능을 제공하는가?	
법적 인증 및 보안 기준 준수	보안 인증 기준	IoT 기기가 국가가 정한 보안 인증 기준(예: IoT 보안 인증제)을 충족하는가?	
		홈네트워크 IoT 기기가 보안 로그 관리 및 데이터 전송 보호 기능을 포함하는가?	

제4장. 사후관리

사후관리와 표 도입 이유

1. IoT 제품 리콜의 문제점

- 보안 결함이 발생했을 경우, 다음과 같은 문제가 발생할 가능성이 있음
  - 피해 유형의 모호성: 개인정보 유출, 다른 기기로의 공격 전파 등 간접적 피해가 주로 발생하며, 이는 기존 리콜 사유에 포함되지 않음.
  - 책임 소재의 불분명: 보안 결함으로 인해 간접적으로 영향을 받은 다른 기기에 대한 법적 책임 규정이 부족.
  - 예시:
    - 해킹으로 인한 IoT 기기 오작동 및 데이터 유출.
    - 네트워크 취약점이 연결된 다른 기기로 확산되어 피해를 확대.

2. 사후 관리 제도 개선 방향

- 리콜 기준 확대:
  - 보안 결함이 타 디바이스 및 네트워크 안정성에 위협을 가할 경우를 리콜 사유에 포함해야 함.
  - 데이터 유출, 시스템 다운타임, 간접적 피해 등도 리콜 사유로 명확히 명시.
- 소프트웨어 업데이트 의무화:
  - 리콜 대신 보안 패치 및 펌웨어 업데이트를 통한 문제해결을 우선 적으로 고려.
  - 자동 업데이트 과정에서 무결성 보장(변조 방지)을 법적으로 요구하여 신뢰성을 강화.

사후관리	중대한 보안성 결함 시 리콜	타 디바이스 또는 네트워크 안전성을 위협하는 보안 결함 시 리콜해야 한다.
	보안 취약점으로 인한 피해 대응	데이터 유출, 시스템 다운타임, 간접적 피해를 초래하는 보안 결함 시 리콜해야 한다.
	업데이트로 해결 가능한 경미한 결함	경미한 보안 결함은 소프트웨어 또는 펌웨어 업데이트로 해결해야 한다.
	리콜 절차의 투명성	리콜 과정에서 사용자의 신체적, 재산적 피해를 최소화하기 위한 절차를 마련해야 한다.

참고자료

KISA 한국인터넷진흥원 - IoT 공통보안가이드

<논문>
사물인터넷(IoT) 환경에서 개인정보보호 강화를 위한 제도 개선 방안
사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안
사물인터넷환경에서의 스마트홈 서비스 침해 위협 분석 및 보안 대책 연구