홈네트워크건물인증
보안점검 가이드

2024. 3. 1.

KAIT 한국정보통신진흥협회
Korea Association for ICT Promotion
정보통신인증센터

지침, 가이드 등의 제·개정 이력

번호	일자	내용	비고
-	2023.6.7.	o 초고속정보통신건물인증 업무처리 지침 개정 - 홈네트워크건물인증 AAA등급 기준 변경 - 홈네트워크 보안점검 전체등급 확대(2022.7.1. 주택승인신청부터) - (점검기관) 한국정보통신진흥협회 정보통신인증센터	-
1	2024.3.1. [제정]	홈네트워크건물인증 보안점검 가이드(KAIT) 제정	ver 1.0

홈네트워크건물인증 보안점검 운영방안

❑ 목 적

홈네트워크건물인증 보안점검은 홈네트워크 설비에 대한 보안 취약점을 사전에 점검하여 입주민에게 안전한 서비스를 사용할 수 있도록 지원하고자 함

❑ 신청 및 대상

홈네트워크건물인증 보안점검을 받고자 하는 건축물의 건축주(또는 건설사 등)는 「초고속정보통신건물인증 업무처리지침」 [별표 2] 홈네트워크건물인증 심사기준 주11)에 따라 등급별 보안점검 대상에 대하여 보안점검을 신청하여야 한다.

- 홈네트워크건물인증 등급별 보안점검 대상

AAA등급	▪ 스마트기기용 앱, 세대단말기, 무선방식이 적용된 홈네트워크 기기 ▪ 단지네트워크장비, 홈네트워크 단지서버
AA등급, A등급	▪ 세대단말기 ▪ 단지네트워크장비, 홈네트워크 단지서버

※ AA등급, A등급의 보안점검은 2022년 7월 1일 이후 사업계획승인을 신청한 건축물부터 적용
※ 단지네트워크장비, 단지서버 등은 지능형 홈네트워크 설비 설치 및 기술기준 제14조의2(홈네트워크 보안)를 적용
※ 홈게이트웨이가 설치된 경우 '홈네트워크 보안가이드(한국인터넷진흥원)'를 적용하여 보안점검을 진행

❑ 보안점검기관

- 한국정보통신진흥협회(KAIT) 정보통신인증센터

❑ 참고기준

- 「지능형 홈네트워크 설비 설치 및 기술기준」
- 홈네트워크 보안가이드 (KISA, 2023.7.)
- 정보통신망연결기기등 정보보호인증기준 상세 해설서(KISA, 2022.8.)
- 초고속정보통신건물인증 업무처리 지침(2023.6.7.)

Ⅰ 보안점검 절차

1 사전점검

1) 대상: 홈네트워크 기기를 제어하는 스마트기기용 앱, 세대단말기, 무선 방식을 적용한 홈네트워크 기기

2) 사전점검 신청 제출서류

- 신청인 : 건설사 또는 제조사 등

< 사전점검 신청 시 제출서류>
① [별지 제1호]의 홈네트워크건물인증 보안 사전점검 신청서
② [별지 제2호]의 홈네트워크건물 보안 사전점검 제품 내역서

2 현장점검

1) 대상: 단지네트워크장비, 홈네트워크 단지서버

2) 현장점검 신청 제출서류

- 신청인 : 건축주 또는 건설사

< 현장점검 신청 시 제출서류>
① [별지 3호]의 홈네트워크건물인증 보안 현장점검 신청서
② [별지 4호]의 홈네트워크건물 보안 현장점검 구성 내역서

3 보안점검 단계

1) 사전점검

보안점검 신청	자체평가서 제출	평가서 서면검토 및 개선요청	개선조치결과 제출	결과 통보
신청인 → KAIT	신청인 → KAIT	KAIT → 신청인	신청인 → KAIT	KAIT→ 심사센터 (신청인)

2) 현장점검

보안점검 신청	자체평가서 제출	평가서 검토/현장 방문점검/개선요청	개선조치결과 제출	결과 통보
신청인 → KAIT	신청인 → KAIT	KAIT→신청인	신청인 → KAIT	KAIT→ 심사센터

4 보안점검성적서 유효기간 및 재점검 절차

1) 보안점검성적서의 유효기간은 발급일로부터 1년이며, 유효기간내에 제품의 변경이 있는 경우 제조사는 보안가이드 내용을 준수하여 보안 활동을 지속적으로 수행하여야 한다.

2) 보안점검성적서의 유효기간 만료일 이전에 「Ⅲ 재점검 대상 기준」의 「2. 재점검 대상 기준」에 해당하는 변경사항이 발생한 경우 신청인은 해당 제품에 대하여 사전점검을 다시 신청하여야 한다.

3) 보안점검성적서의 유효기간 만료일 이전에 사전점검을 신청한 경우에는 만료 예정인 보안점검성적서의 유효기간을 3개월간 유예할 수 있다.

4) 「Ⅲ 재점검 대상 기준」의 「2. 재점검 대상 기준」에 해당하지 않는 경우 보안점검성적서의 유효기간을 1년씩 연장 신청할 수 있다.

5 홈네트워크건물인증 보안점검(사전점검, 현장점검) 수수료

1) 사전점검

구분	세대단말기	스마트기기용 앱	홈네트워크 기기(무선)
점검 수수료	12,000,000원 (소요기간 10일 이상)	9,600,000원 (소요기간 8일 이상)	8,400,000원 (소요기간 7일 이상)

※ 점검 수수료는 제품의 제조사(신청인)에서 납부하여야 함

※ 유효기간 만료일 이전에 재점검 대상 기준에 따라 사전점검을 재신청하는 경우에는 수수료의 50%를 적용함

※ 유효기간 연장 신청은 수수료의 30%(1회 무료), 파생모델은 수수료의 5%를 적용함

※ 점검 수수료는 변경될 수 있으며, IT컨설턴트(정보보호컨설턴트 포함직무) 직무의 노임단가를 적용함

2) 현장점검

구분	단지네트워크장비 및 단지서버 등	비고
점검 수수료	3,000원 / 세대당	-

※ 점검 수수료는 신청인(건축주 또는 건설사)이 납부하여야 함

■ 사전점검

1. 스마트기기용 앱

2. 세대단말기

3. 홈네트워크 기기 중 무선방식 제품

① 스마트기기용 앱

1 점검 대상

요구사항
스마트기기용 앱은 IoT 플랫폼(서버 등)과 홈네트워크 플랫폼(서버 등)간에 연동을 위해 전송되는 데이터 등을 대상으로 점검한다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따라 정보보호인증을 받은 경우에는 요구사항을 충족한 것으로 본다.

2 점검 항목

구 분			
1	사용자 관리	1-1	안전한 로그인 방식 적용
		1-2	안전한 사용자 인증 및 추가 사용자 관리
		1-3	사용자 인증 실패에 대한 안전한 관리
2	정보 관리	2-1	앱(IoT 서버)과 홈네트워크 플랫폼(서버)간 세션관리 정책 마련
		2-2	앱에서 홈네트워크 플랫폼(서버)간 중요정보는 안전하게 저장 및 전송
		2-3	앱 이용을 위한 개인정보의 수집, 이용, 처리 폐기 등은 법적 요구사항을 준수
3	소프트웨어 보안	3-1	소스코드는 시큐어 코딩, 난독화 적용
		3-2	소프트웨어 취약점 관리
4	소프트웨어 관리	4-1	앱의 정보, 업데이트 등의 관리

3 점검 기준

1. 사용자 관리

1-1. 안전한 로그인 방식 적용

요구사항

① 계정 로그인 방식의 경우 비밀번호는 영문, 숫자, 특수문자 2조합 8자리 또는 3조합 6자리 이상 적용

지문, 홍채 인식 등을 추가 인증 방식(간편 로그인 등)으로 적용할 경우 사용자 인증 정보(바이오 정보 등)는 안전하게 관리되어야 함

② 비밀번호는 로그인, 정보관리 등에서 입력 및 표기 시 평문으로 적용되지 않아야 함

비밀번호의 입력, 변경 등을 진행할 경우 노출되지 않도록 마스킹 처리 등 적용

1.2. 안전한 사용자 인증 및 추가 사용자 관리

요구사항

① 홈네트워크 이용을 위한 주사용자는 추가 인증 방식을 적용하여 안전하게 관리되어야 함

홈네트워크 기기 제어 등을 위한 주사용자 인증 방식은 세대단말기 인증, 단지 서버 등록 등 별도 방식을 적용

② 추가 사용자의 인증 및 권한은 안전하게 관리되어야 함

홈네트워크 기능 이용을 위해 추가 사용자 등록이 필요한 경우 주사용자에게 추가 사용자 인증, 권한 설정 등을 할 수 있도록 적용

1-3. 사용자 인증 실패에 대한 안전한 관리

요구사항

① 사용자 인증 실패 시 사유를 구체적으로 제시하지 않아야 함

로그인 실패 사유를 실패 항목으로 표시되지 않도록 적용

② 5회 이상 인증 실패 시 재시도 제한(5분 이상), 사용자 재검증 등의 절차 적용

일정 횟수(5회)이상 사용자 인증 실패 시 로그인 제한, 사용자 재검증 등 안전한 관리 정책 적용

2. 정보 관리

2-1. 앱(IoT 서버)과 홈네트워크 플랫폼(서버)간 세션관리 정책 마련

요구사항

① 안전한 세션정보(세션ID, 쿠키, 토큰 등) 관리정책 마련

세션정보 전송은 안전한 방식을 적용하여야 하고, 세션정보의 만료 및 재발급 기준, 재사용 방지 등은 안전한 관리 정책을 마련하여 적용

2-2. 앱에서 홈네트워크 플랫폼(서버)간 중요정보는 안전하게 저장 및 전송

요구사항

① 사용자 인증을 위한 중요정보는 암호화하여 저장

사용자 인증을 위한 중요정보는 앱, 서버 등에서 암호화하여 안전하게 저장

② 앱에서 전송되는 중요정보는 안전한 암호통신 프로토콜, 암호키, 암호 알고리즘 적용

앱과 홈네트워크 플랫폼(서버)간에 사용자 인증 등을 위한 중요정보는 암호통신 프로토콜을 적용하고, 암호 알고리즘 및 암호키 등은 관리기준을 마련하여야 함 ※ 암호 키 관리 안내서(KISA) 등 참조

2-3. 앱 이용을 위한 개인정보의 수집, 이용, 처리, 폐기 등은 법적 요구사항을 준수

요구사항

① 필수정보 외 불필요한 개인정보는 수집하지 않아야 함

가입 및 이용을 위해 수집하는 개인정보는 최소화하고 수집한 개인정보에 대해서는 관련 법류를 준수하여야 함 ※ 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 참고

3. 소프트웨어 보안

3-1. 소스코드는 시큐어 코딩, 난독화 적용

요구사항

① 소프트웨어 개발 보안가이드(행정안전부) 등의 준수

소프트웨어 개발 보안가이드(행정안전부), 8대 보안 취약점(국가정보원) 등 주요 보안 취약점에 대한 점검 및 조치를 통해 안전한 소프트웨어 사용

② 소스코드는 분석 방지를 위한 난독화 적용

소프트웨어 개발 및 변경 시 소스코드 분석이 어렵도록 난독화 방안을 마련하고 적용하여야 함

③ 불필요한 주석, 코드 등은 제거

소프트웨어 개발 및 변경 시 불필요한 주석, 코드는 제거하여야 함

④ 루팅 탐지 등 적용

루팅 또는 탈옥 운영체제 탐지 등 적용

3-2. 소프트웨어 취약점 관리

요구사항

① 공개영역에서 알려진 보안취약점의 점검 및 처리

공개된 보안취약점에 대한 관리, 조치, 대책 등의 방안을 마련하여 안전하게 관리되어야 함

② 안전한 공개·상용 소프트웨어의 사용

유효기간, 업데이트 등이 만료된 공개·상용 소프트웨어는 사용되지 않도록 관리 및 대책을 마련하여야 함

4. 소프트웨어 관리

4-1. 앱의 정보, 업데이트 등의 관리

요구사항

① 앱의 식별정보 확인 및 업데이트 발생 시 알림 정보 제공

앱의 모델명, 버전 정보 등을 확인할 수 있어야 하고, 업데이트 발생 시 알림(조회 포함) 등이 가능하여야 함

② 업데이트 파일 무결성 및 업데이트 서버 검증

안전한 업데이트를 위해 무결성 및 업데이트 서버 검증 등을 적용하여야 함

② 세대단말기

1 점검 대상

요구사항
세대단말기(월패드 등)에 홈게이트웨이를 포함할 수 있으며, 홈게이트웨이를 별도로 설치하는 경우 설치된 홈게이트웨이는 「홈네트워크 보안가이드(KISA, `23.7.31.) 3.3 홈게이트웨이 보안」을 적용하여 점검한다. 세대단말기의 사용자 인터페이스를 이동형 무선기기로 적용할 경우 홈네트워크 단지망과 연결되고 이동형 무선기기를 제어하는 설비를 포함하여 보안점검 대상으로 본다. (예: 운영체제 또는 제어기능이 포함된 거치대/크래들 등) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따라 정보보호인증을 받은 경우에는 요구사항을 충족한 것으로 본다.

2 점검 항목

구 분		
1	데이터 기밀성	세대단말기에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.
2	데이터 무결성	세대단말기에 저장되는 데이터의 위·변조를 방지하고 위·변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.
3	인증	세대단말기에 접속하기 위해 사용되는 인증정보는 정당한 사용자인지 검증할 수 있도록 안전한 인증방식을 지원하는 것을 말한다.
4	접근통제	서비스 목적에 따라 접근권한을 최소한으로 부여하여 세대단말기로 비인가 접근을 통제하고 접근 권한을 관리하는 것을 말한다.
5	전송데이터 보안	세대단말기와 단지서버간의 데이터 전송시 유출 또는 탈취되지 않도록 하는 것을 말한다.

3 점검 기준

1) 데이터 기밀성

요구사항

① 불필요한 중요정보 수집은 최소화하고 수집이 필요한 중요정보는 암호 알고리즘을 이용하여 안전하게 저장하여야 하며, 사용자 및 관리자가 필요 시 완전하게 삭제할 수 있는 기능이 있어야 한다.

※ 중요정보 : 인증정보(비밀번호 등), 개인정보(이름, 생년월일, 주소 등), 데이터 암호화 키(DEK)

② 기기에서 전송 또는 저장되는 중요정보를 국내·외에서 검증된 보안 강도 112비트 이상의 암호 알고리즘을 적용하여야 하고, 기기마다 암호키를 다르게 생성·사용하도록 하여야 한다.

※ 암호 알고리즘 및 키 길이 이용 안내서(KISA, 2018) 참고

③ 개인정보 수집 및 처리 시 개인정보 관련 법적 요구사항을 준수한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ②, ③번 항목은 적용을 권장한다.

2) 데이터 무결성

요구사항

① 세대단말기는 운영체제 버전별로 제조사가 제공하는 최신 보안 패치를 적용하여야 하고, 제품 모델명 및 정보(소프트웨어 등)를 식별할 수 있도록 하여야 한다.

② 업데이트 발생 시 이용자에게 알림 수단을 통해 정보를 제공하여야 하고, 업데이트 파일은 무결성 검사를 통해 안전성을 검증해야 한다.

③ 중요정보는 소스코드에 하드 코딩되지 않도록 하며, 평문 형태로 노출되지 않도록 하여야 한다.

④ 소스코드 난독화, 바이너리 난독화, 컴파일 옵션 활용 등의 소스코드 난독화를 적용하여야 한다.

⑤ 소프트웨어 설계, 개발 단계에서 소스코드 개발 언어별로 시큐어 코딩 규칙을 적용해야 한다.

⑥ 디버깅 코드, 시험용 코드, 주석, 백도어 등 운영에 불필요한 기능 및 코드는 제거하여야 한다.

※ 유지보수를 위한 디버깅 코드는 제외

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ⑤, ⑥번 항목은 적용을 권장한다.

3) 인증

요구사항

① 관리자용(사용자 제외) 인증정보를 비밀번호로 적용하는 경우 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

※ 관리자용 비밀번호는 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 제품 일련번호 등)를 포함하는 비밀번호 사용 제한

※ 계정없이 비밀번호만 입력하고, 입력 문자가 숫자로만 제한되는 경우 8자리 이상을 적용할 수 있음

※ 관리자용 비밀번호는 다른 기기와 동일한 비밀번호를 사용하지 않음

② 사용자용 인증정보(비밀번호 등)는 관리기능(기기 및 서비스 설정 등)과 서비스 이용을 위한 기능으로 구분하여 적용할 수 있다.

※ 사용자용 관리기능 설정 접근 비밀번호는 2조합 8자리 이상 또는 3조합 6자리 이상으로 설정하고, 입력 문자가 숫자로만 제한되는 경우 8자리 이상을 적용할 수 있음

※ 사용자용 서비스 기능(방범·비상 해제, 공동현관 출입 비밀번호 등) 이용을 위한 비밀번호는 4자리 이상으로 적용할 수 있음

※ 사용자용 관리기능 인증정보(비밀번호 등)는 변경 주기(예: 6개월)를 사용자가 설정할 수 있어야 하고, 변경 주기 알림 기능을 적용할 수 있어야 함(알림 발생 시 해제 기능 적용 가능)

③ 비밀번호가 평문으로 표시되지 않도록 하여야 하고, 일정 횟수(예: 5회) 이상 인증을 실패한 경우 일정 시간(예: 5분) 이상 재시도 되지 않도록 하여야 한다.

※ 비밀번호를 평문으로 표시되도록 사용자가 선택하는 기능은 포함할 수 있음

④ 관리기능 또는 중요정보에 접근 시 사용자 인증을 수행하고, 서비스 이용에 필요한 최소한의 권한만 부여한다.

※ 사용자 권한 제한 : 네트워크 및 보안 설정, 소스 코드 접근, 제품 중요 정보 등

⑤ 다른 기기와 연결 또는 중요정보 전송 시 기기의 식별정보가 신뢰성이 있음을 확인하는 인증을 선행한다.

※ 시리얼통신으로 세대단말기와 직접 연결되어 있는 경우에는 제외 가능

⑥ 세션을 활용한 통신을 하는 경우, 세션 연결 이후 일정한 시간 동안 사용하지 않으면 해당 세션을 잠그거나 종료시켜야 하고, 재접속 시 세션 정보가 재사용되는 것을 방지한다.

⑦ 불필요한 계정은 제거하거나 비활성화한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ①, ②번 항목은 다음 기준을 적용할 수 있다.

- 관리자용(사용자 제외) 비밀번호는 2조합 6자리 이상으로 설정한다.
  ※ 관리자용 비밀번호 입력이 숫자로만 제한되는 경우는 8자리 이상을 적용
  ※ 사용자용 초기 인증정보(비밀번호 등)는 변경·생성하여야 함
  ※ 홈네트워크 서비스를 사용하기 위한 인증정보(비밀번호 등)는 4자리 이상으로 적용할 수 있음 (일반 설정, 방범·비상 해제, 공동현관 출입 비밀번호 등)

4) 접근통제

요구사항

① 불필요한 네트워크 포트 및 서비스는 제거하거나 비활성화시켜야 한다.

※ 외부 접속 서비스(Telnet, FTP, SNMP 등)를 사용하는 경우 비인가자 접근을 방지할 수 있도록 IP주소 제한, 비밀번호 설정 등을 적용하여야 한다.

② 불필요한 USB, SD카드, 이더넷(LAN) 포트 등은 제거하거나 최소화하고 사용하지 않는 포트는 비활성화할 수 있도록 하여야 한다.

※ 미사용 포트는 비활성화 기본 설정, 홈네트워크 관리자만 활성화 권한 설정

③ 세대단말기는 원격접속이 허용되지 않도록 하여야 한다.

※ 원격접속이 필요한 경우 접근통제, 인증, 안전한 보안채널이 적용된 신뢰된 환경에서만 원격접속이 가능하도록 통제

④ 개발자가 펌웨어를 디버깅하기 위해 사용되는 내부 인터페이스를 비활성화하거나 안전한 접속수단을 제공하여야 한다.

⑤ 디버그 로그는 비활성화하여야 하지만 제품의 디버깅을 위해 로그를 수집하는 경우 안전한 활성화 방법을 제공하고 지정된 IP로만 수집이 가능하도록 하여야 한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ③, ④, ⑤번 항목은 적용을 권장한다.

5) 전송데이터 보안

요구사항

① 지정된 IP 또는 MAC 주소의 네트워크 트래픽만 허용하여야 한다.

※ 지정 설비는 경비실, 관리실, 공동 현관, 단지서버 등 단지내에 설치된 설비로 제한

※ 외부 인터넷망과 직접 연결되지 않도록 하여야 하며, 외부 인터넷망 연결이 필요한 경우 안전한 암호화 프로토콜을 이용하여 전송되어야 함

② 단지서버~백본~워크그룹스위치~세대단말기간 전송데이터는 암호화 프로토콜을 이용하여 전송한다.

※ 전송 암호화 프로토콜은 TLS1.2 이상 적용을 권장함(취약한 알고리즘은 제외)

③ 세대단말기에 Wifi 연결 기능을 적용하는 경우 안전한 보안규격(WPA3 이상)을 적용하여야 한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ③번 항목은 적용을 권장한다.

③ 홈네트워크 기기 중 무선방식 제품

1 점검 대상

요구사항
댁내 설치되는 홈네트워크 기기 중 무선방식이 적용된 제품을 대상으로 하며, 세대 단말기와 무선방식 제품간에 시리얼 통신방식으로 제어신호를 전송하거나 단방향으로만 신호를 보내는 제품은 점검 대상에서 제외할 수 있다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따라 정보보호인증을 받은 경우에는 요구사항을 충족한 것으로 본다.

2 점검 항목

구 분			
1	사용자 관리	1-1	안전한 연결 및 권한 관리
		1-2	안전한 인증방식 사용
2	정보 관리	2-1	세대단말기와 전송되는 정보의 안전한 관리
		2-2	중요정보의 저장 및 관리
		2-3	모델명 및 제품정보
3	소프트웨어 관리	3-1	공개된 보안취약점 조치
		3-2	안전한 업데이트 관리
4	하드웨어 관리	4-1	인터페이스 관리

3 점검 기준

1. 사용자 관리

1-1. 안전한 연결 및 권한 관리

요구사항

① 하나의 세대단말기만 연결될 수 있도록 최초 연결 시 고유번호 등을 이용한 안전한 연결 방식 적용

다른 세대의 세대단말기에서 연결할 수 없도록 하여야 하며, 최초 연결 시 해당 기기만 연결되는 방식을 적용

1-2. 안전한 인증방식 사용

요구사항

① 앱, 세대단말기 외에 해당 기기로 설정 변경 등을 위해 접근이 가능한 경우 비밀번호 등의 안전한 인증방식 적용

비밀번호 방식의 경우 입력 시 평문으로 적용되지 않도록 하여야 하며, 세대 내부에 설치되는 기기는 물리적 방식으로 적용할 수 있음

② 기기 접근을 위한 인증 실패 시(5회 이상) 일정 시간 접근 제한 또는 잠금 등을 적용

5회 이상 기기 인증 실패 시 비상 알림, 기기 잠금 등을 통해 추가 접근을 방지하여야 함

2. 정보 관리

2-1. 세대단말기와 전송되는 정보의 안전한 관리

요구사항

① 세대단말기와 기기간 전송되는 정보는 변조되지 않도록 안전하게 전송되어야 함

암호통신 또는 암호 알고리즘 등을 적용하여 안전하게 정보를 전송하여야 함 ※ 접점방식, 시리얼 통신(RS485 등) 방식 등의 경우에는 제외할 수 있음

2-2. 중요정보의 저장 및 관리

요구사항

① 비밀번호, 사용자 인증 정보 등 중요정보를 기기에 저장할 경우 암호화하거나 이에 준하는 방식을 적용

중요정보는 소스코드에 하드코딩이 되지 않도록 하여야 하며, 정보를 쉽게 유추할 수 없도록 암호화 등의 방식을 적용하여야 함

2-3. 모델명 및 제품정보

요구사항

① 해당 기기의 모델명 및 소프트웨어 정보 등을 확인할 수 있어야 함

제품정보 등을 물리적으로 표시되어야 하며, 표시가 어려운 소형 기기의 경우에는 약어, 기호 등으로 표시하거나 제외할 수 있음

3. 소프트웨어 관리

3-1. 공개된 보안취약점 관리

요구사항

① 한국인터넷진흥원(KISA) 등에서 공개된 보안취약점은 조치가 되어야 함

국내 주요 보안취약점 공개 사이트에서 기기와 관련된 보안취약점은 조치가 되어야 함

3-2. 안전한 업데이트 관리

요구사항

① 펌웨어, 소프트웨어 등의 업데이트가 가능한 기기의 경우 업데이트 파일은 무결성 검증 및 검증된 업데이트 서버를 통해 진행되도록 하여야 함

기기는 검증된 업데이트 파일이 설치되도록 하여야 함

4. 하드웨어 관리

4-1. 인터페이스 관리

요구사항

① 외부 연결용 인터페이스는 제거 또는 비활성화하여야 하며, 유지보수용으로 필요한 경우 관리자만 접근할 수 있도록 하여야 함

기기 외관 및 내부의 외부 연결용 인터페이스는 비인가자의 접근을 방지할 수 있어야 함

■ 현장점검

4. 단지네트워크장비(백본, 방화벽, 워크그룹스위치)

5. 홈네트워크 단지서버

④ 단지네트워크장비 (백본, 방화벽, 워크그룹스위치)

1 점검 대상

기본 요구사항
백본, 방화벽은 「보안기능 확인서」(정보보호제품 평가·인증 가능)*를 제출하여야 하며, 단지네트워크장비와 홈네트워크 단지서버가 설치된 장소 및 설치함(랙)은 외부인이 신체적인 접근을 할 수 없도록 잠금장치 등을 설치하여야 한다. *** `보안기능 확인서`는 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택은 적용을 권장한다.** **홈네트워크 단지서버가 설치되는 방재실 또는 집중구내통신실에는 CCTV 카메라를 설치하여 관리하여야 한다.**

2 점검 항목

구 분		
1	홈네트워크 단지망 보안	「지능형 홈네트워크 설비 설치 및 기술기준」 제14조의2(홈네트워크 보안) 제1항의 내용을 적용하여야 한다.
2	데이터 기밀성	중요정보(이용자 식별정보, 인증정보, 개인정보 등)에 대해 암호알고리즘, 암호키 생성·관리 등 암호화 기술과 민감한 데이터의 접근제어 관리기술 적용으로 기밀성 구현 (워크그룹스위치 제외)
3	데이터 무결성	중요정보(이용자 식별정보, 인증정보, 개인정보 등)에 대해 해쉬함수, 전자서명 등 기술 적용으로 위·변조 여부 확인 및 방지조치 (워크그룹스위치 제외)
4	인증	단지네트워크장비는 사용자 확인을 위하여 전자서명, 아이디/비밀번호, 일회용 비밀번호(OTP) 등을 통해 신원확인 및 인증기능을 구현
5	접근통제	자산·사용자 식별, IP관리, 단말인증 등 기술을 적용하여 사용자 유형 분류, 접근권한 부여·제한 기능 구현을 통해 인가된 사용자 이외에 비인가된 접근을 통제
6	전송데이터 보안	승인된 홈네트워크장비 간에 전송되는 데이터가 유출 또는 탈취되거나 흐름의 전환 등이 발생하지 않도록 전송데이터 보안 기능을 구현

3 점검 기준

1) 홈네트워크 단지망 보안

※ 2022년 7월 1일 이전에 주택사업계획 승인을 받은 공동주택은 적용을 권장한다.

요구사항

① 단지서버(백본)와 세대별로 설치된 세대단말기간에 전송되는 데이터는 노출, 탈취 등의 방지를 위해 다른 세대로 접근할 수 없도록 물리적 또는 논리적 방법 중에서 1개 이상 방식을 적용하여 방지하여야 한다.

※ 물리적 방식 종류 : 백본과 세대단말기간 1:1 성형배선, 홈네트워크 단지망을 PON(Passive Optical Network)방식으로 연결 등

※ 논리적 방식 종류 : 단지서버(백본)와 세대단말기간에 가상사설통신망(L2 VPN [Layer 2 VPN], L3 가상 네트워크[IPSec VPN, IP Tunnel, Virtual Routing 등], SSL VPN 등), 가상근거리통신망(VLAN[IEEE 802.1Q], VxLAN[Virual Extensible LAN] 등), 보안적합성 검증을 받은 시스템 등

방식별 요구사항

물리적 방식	**1:1 성형배선 방식**	o 백본(L3스위치) 장비에서 세대단말기(또는 홈게이트웨이)까지 배선(UTP, 광케이블 등)을 1:1 성형배선으로 설치한 경우 - 동별 워크그룹스위치(L2스위치)를 설치할 수 없음 - 백본(L3스위치) 장비는 VLAN 설정 등을 통해 세대간 네트워크 접근을 방지하여야 함 o 전용선 라우터를 이용한 경우 - 물리적인 네트워크 케이블을 세대별로 각각 설치하고 전용선 라우터 등을 활용하여 세대망을 단일회선으로 구성하여야 함
	수동 광통신망 방식 (Passive Optical Network, PON방식)	o 백본(OLT) 장비에서 세대까지 광케이블을 설치하고 동별 스플리터를 설치하여 광가입자망을 구성한 경우 - 백본(OLT) 장비는 세대간 네트워크 접근통제를 위한 보안기능을 적용하여야 함 - 세대별로 설치되는 ONT(Optical Network Terminal)는 무결성 보장 등의 보안 기능 적용
	망분리 솔루션	o 단지서버망과 개별 세대망을 망분리 솔루션을 이용하여 각각 구성하고, 세대에서 다른 세대의 내부로의 접속은 불가능하게 구성 - 국가정보원의 `망간 자료전송제품 보안요구사항`을 참조

방식별 요구사항		
논리적 방식	**VPN 이용 기술**	o 단지서버와 세대단말기 사이에 VPN Gateway와 VPN 클라이언트(내·외장)를 설치하여 가상 터널을 만들고 송수신되는 데이터를 암호화하여 전송 - 기술의 종류에는 L2 VPN [Layer 2 VPN], L3 가상 네트워크[IPSec VPN, IP Tunnel, Virtual Routing 등], SSL VPN 등이 있음 - 워크그룹스위치가 설치된 경우 사용하지 않는 포트는 접근통제 하여야 함 o VPN 기술을 적용한 경우 다른 세대로의 네트워크 접근 가능 여부와 네트워크 트래픽 분석을 통한 전송 데이터 암호화 적용 여부 등을 점검함 - 전송 데이터 암호방식, 무결성 방식은 안전도 112비트 이상 설정 (암호 알고리즘 및 키 길이 이용 안내서, KISA 2018 참조)
	VLAN 이용 기술	o 백본장비(L3), 워크그룹스위치(L2)에 세대별로 구분되도록 가상 근거리통신망(VLAN)을 구성하고, 구성방식에는 포트, IP주소, MAC 기반 구성 등이 있음 - 종류에는 VLAN[IEEE 802.1Q], VxLAN[Virual Extensible LAN] 등이 있음 - 워크그룹스위치의 사용하지 않는 포트는 접근통제하여야 함 o VLAN 기술을 적용한 경우 전송 데이터는 암호화 프로토콜(TLS 1.2 이상)을 적용하여야 하며, 다른 세대로의 네트워크 접근 가능 여부와 네트워크 트래픽 분석을 통한 전송 데이터 암호화 적용 여부 등을 점검함
	암호화 기술 등	o 단지서버와 세대별 사이의 망을 전송 데이터 노출, 탈취 등을 방지할 수 있고 분리 구성할 수 있는 국내·외 표준으로 검증된 기술

2) 데이터 기밀성 [방화벽, 백본]

요구사항

① 관리자 접속을 위해 사용하는 비밀번호 등의 중요정보는 암호화하여 저장한다.

※ SHA2 이상의 알고리즘 등

3) 데이터 무결성 [방화벽, 백본]

요구사항

① 제품 제조사가 제공하는 최신 보안패치를 적용하여야 하고, 제품 모델명 및 정보(소프트웨어 등)를 식별할 수 있도록 하여야 한다.

② 백본은 설정파일의 위·변조 여부를 확인할 수 있도록 설정값을 백업하여 확인하거나 설정 파일의 무결성 검증방안을 마련하여 적용하여야 한다.

③ 방화벽은 소프트웨어를 업데이트는 하는 경우 파일 설치 전 무결성 검증을 시행하여야 한다.

4) 인증 [방화벽, 백본, 워크그룹스위치]

요구사항

① 제조사에서 설정한 관리자용 기본 비밀번호는 변경하여야 하고, 비밀번호는 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

※ 관리자용 비밀번호는 변경 주기(예: 6개월 등)를 설정할 수 있어야 하고, 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 일련번호 등)를 포함하는 비밀번호 사용은 제한한다.

② 접속인증 시도가 일정 횟수 이상(예: 5회 등) 실패하는 경우 접근을 제한하도록 설정하고(예: 잠금 5분 등), 관리자 설정 등에 접속 후 일정시간(예: 10분) 이상 작업을 하지 않는 경우 자동으로 접속이 차단되도록 설정한다.

※ 불필요한 계정은 제거하거나 비활성화하여야 하고, 기본 계정은 비활성화하거나 유추가 어려운 계정으로 변경하여야 한다.

5) 접근통제 [방화벽, 백본, 워크그룹스위치]

요구사항

① 공동주택 단지 외부에서 관리 및 설정을 위한 원격접속은 할 수 없도록 하여야 한다. 원격접속이 필요한 경우 지정된 단말(IP, MAC 주소 등)에서만 접속할 수 있도록 하여야 한다.

※ IP주소 제한 기능을 지원하지 않는 워크그룹스위치는 제외 가능

② 설정 파일의 접근권한을 최소화하고, 관리자 웹페이지가 있는 경우 비활성화하거나 일정시간 작업이 없는 경우 접속을 차단하도록 설정하여야 한다.

③ 방화벽은 정책(Rule) 적용에 따른 중요 이벤트 발생 시 로그 등을 저장할 수 있도록 하여야 한다.

④ 워크그룹스위치의 불필요한 I/O 포트 및 네트워크 인터페이스는 비활성화한다.

⑤ 백본의 경우 불필요한 서비스(echo, discard, chargen, finger, tftp 등)를 비활성화한다.

6) 전송데이터 보안 [방화벽, 백본, 워크그룹스위치]

요구사항

o 백본

① 백본에서 트래픽 흐름 제어 설정 시 다음을 참고하여 설정한다.

가. 네트워크 ACL(Access Control List)을 활용하여 IP주소, Port번호 등으로 접근을 제한하여 서브넷(subnet) 등 네트워크 영역 간 인가받지 않은 트래픽 흐름을 통제한다.

나. 허용규칙 이외에 모든 트래픽 전달을 차단하는 거부규칙을 설정한다.

다. 단지서버와 다른 홈네트워크장비(예: 단지네트워크장비 등) 사이에 방화벽이 존재하지 않는 경우에는 백본의 ACL을 통해 단지서버로의 비인가된 접근을 차단할 수 있도록 설정한다.

※ 또는, 단지서버에 소프트웨어 방화벽 등을 설치하여 비인가 접근 차단 설정을 적용할 수 있음

라. `홈네트워크 단지망 보안` 적용 방식에 따라 백본의 ACL, 트래픽 제어, 비인가 접근 차단 기능 등의 설정이 불필요한 경우 제외할 수 있다.

마. 다만, 백본은 VLAN 사이의 라우팅만 구성하고 불필요한 설정은 하지 않아야 하며, VLAN간 트래픽 흐름제어가 필요한 경우 방화벽을 활용해 비인가된 접근을 차단할 수 있다.

② 네트워크를 통해 원격에서 백본에 접속하는 경우 암호통신 프로토콜을 적용한다.

가. 백본 설정을 위한 원격터미널 접속 시 안전한 접속방법을 이용하여 연결한다. (SSH V2 등)

나. 기타 암호화되지 않는 서비스(HTTP, TELNET, FTP, TFTP 등) 는 비활성화한다.

③ 불필요한 I/O 포트 및 네트워크 인터페이스는 비활성화한다.

④ 외부로부터의 네트워크 경로 위변조를 방지하는 기능을 제공하는 경우 이를 활성화한다.

가. ARP 스푸핑 방지 기능 활성화

나. IP 스푸핑 방지 기능 활성화

다. 기타 네트워크 공격(SYN Flooding, UDP Flooding, ICMP Router Redirection, LAND Attack, smurf, Direct Broadcast Attack 등)에 대응하는 기능 활성화

⑤ SNMP 서비스를 사용하지 않는 경우 비활성화한다. (필요시 SNMP 서비스를 사용하는 경우에는 SNMP v3을 사용한다.)

o 방화벽

① 방화벽을 통해 전송되는 데이터를 보호하기 위해 다음과 같이 네트워크 영역을 구성한다.

가. 네트워크 설정 정책에 따라, 대역대별 IP주소 부여 기준을 마련하고, 단지서버 등 내부 서버는 사설 IP로 할당한다.

나. 인터넷망을 통해 접속하는 대외 웹서비스(또는 홈페이지 등) 존재하는 경우, 내부 네트워크와 분리된 DMZ(Demilitarized Zone)를 별도로 구성한다. 인터넷과 DMZ 사이의 통신 및 DMZ와 내부 네트워크 사이의 통신은 서비스를 위해 필요한 최소한의 IP주소 및 포트(Port)만 허용하고, 그 외의 모든 접근은 차단되도록 설정한다. 다만, 대외 웹서비스(또는 홈페이지 등)를 외부 클라우드 서버로 운영하는 경우 DMZ를 제외할 수 있다.

다. 세대망을 연결하는 워크그룹스위치 영역, 단지서버 및 관리서버를 연결하는 내부망, 세대 공용 홈네트워크사용기기(원격검침, 무인택배, 차량출입통제 등)를 연결하는 세대 공용망 등은 용도에 따라 네트워크 영역을 분리하여 설정한다

② 방화벽의 정책(Rule)은 최소 권한의 원칙에 따라 다음과 같이 설정한다.

가. 허용된 IP, 포트(Port)가 아닌 경우 기본적으로 모든 접근이 차단되도록 정책을 설정한다.

나. 인터넷에서 홈네트워크망(단지망 및 세대망)으로의 접근은 원칙적으로 모두 차단한다.

다. 네트워크 설정 정책에 따라, 최소한의 출발지 및 목적지의 IP주소·포트(Port) 단위로 세분화하여 설정한다.

라. 중요 포트(예 : DB 포트, SSH 포트 등)의 접속은 인가된 출발지(공인 IP, 네트워크 대역, 세대망 대역은 출발지 설정 불가)에서만 제한적으로 허용하도록 설정한다.

마. 단지서버에 대해 불필요한 아웃바운드 정책이 존재하지 않도록 설정한다.

바. 세대단말기 등 홈네트워크망에서 단지서버로의 접근은 홈네트워크망 IP 주소로부터 단지서버의 IP주소 및 포트(Port)로만 접근할 수 있도록 설정한다.

사. 공개 웹서버 운영 등에 따라 인터넷을 통한 접근이 필요한 경우 해당 공개서버 운영에 필요한 IP주소와 포트(Port)번호(예: 443 등)만 접근을 허용하도록 설정한다

③ 네트워크를 통해 원격에서 방화벽에 접속하는 경우 암호통신 프로토콜(HTTPS, SSH, SFTP 등)을 적용한다.

④ SNMP 서비스를 사용하지 않는 경우 비활성화한다. (필요시 SNMP 서비스를 사용하는 경우에는 SNMP v3을 사용한다.)

o 워크그룹스위치

① 트래픽 흐름제어 설정을 지원하는 경우 다음을 참고하여 설정한다.

가. 워크그룹스위치의 관리/설정 영역(SSH, 관리웹페이지)에 접근하는 경우 IP주소, 포트번호 등의 접근을 제한하여 트래픽 흐름을 통제할 수 있다.

② 원격 네트워크를 통해 워크그룹스위치에 접속하는 경우, 암호통신 프로토콜을 적용한다.

가. 기타 암호화되지 않는 서비스(HTTP, TELNET, FTP, TFTP 등)는 비활성화한다.

③ 네트워크 경로 위변조를 방지하는 기능을 제공하는 경우 이를 활성화한다.

가. ARP 스푸핑 방지 기능 활성화

나. IP 스푸핑 방지 기능 활성화

다. 기타 네트워크 공격(SYN Flooding, UDP Flooding, ICMP Router Redirection, LAND Attack, smurf, Direct Broadcast Attack 등)에 대응하는 기능 활성화

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 워크그룹스위치는 점검에서 제외할 수 있다. 다만 워크그룹스위치는 원격접속을 제한하거나 안전한 계정 관리 등을 통해 비인가자의 접근을 차단하여야 한다.

⑤ 홈네트워크 단지서버

1 점검 대상

기본 요구사항
홈네트워크 단지서버에는 악성코드 은닉 탐지 도구를 설치하여야 하고, 탐지 실행 주기 설정, 탐지 내용 확인, 업데이트 확인 등에 대한 관리 매뉴얼을 관리사무소에 제공하여야 한다. 관리용 PC가 설치된 경우 외부 인터넷을 별도로 연결하지 말아야 하며 악성코드 은닉 탐지 도구의 설치를 권장한다.

2 점검 항목

구 분		
1	데이터 기밀성	중요정보(이용자 식별정보, 인증정보, 개인정보 등)에 대해 암호 알고리즘, 암호키 생성·관리 등 암호화 기술과 민감한 데이터의 접근제어 관리기술 적용으로 기밀성 구현
2	데이터 무결성	중요정보(이용자 식별정보, 인증정보, 개인정보 등)에 대해 해쉬함수, 전자서명 등 기술 적용으로 위·변조 여부 확인 및 방지 조치
3	인증	사용자 확인을 위하여 전자서명, 아이디/비밀번호, 일회용 비밀번호(OTP) 등을 통해 신원확인 및 인증 기능을 구현
4	접근통제	자산·사용자 식별, IP관리, 단말인증 등 기술을 적용하여 사용자 유형 분류, 접근권한 부여·제한 기능 구현을 통해 인가된 사용자 이외에 비인가된 접근을 통제
5	전송데이터 보안	승인된 홈네트워크장비 간에 전송되는 데이터가 유출 또는 탈취되거나 흐름의 전환 등이 발생하지 않도록 전송데이터 보안 기능을 구현

3 점검 기준

1) 데이터 기밀성

요구사항

① 운영체제(OS), 관련소프트웨어(WEB, WAS, DBMS), 응용프로그램 등 단지서버에서 사용되는 비밀번호는 비밀번호 저장 시 SHA2 이상의 안전한 알고리즘으로 암호화하여 저장한다.

② 응용프로그램에서 입주민의 이름, 이메일, 휴대폰번호 등 개인정보를 수집, 저장 등 처리하는 경우에는 암호화하여 저장한다.

2) 데이터 무결성

요구사항

① 단지서버를 구성하는 운영체제(OS), 관련 소프트웨어(WEB, WAS, DBMS 등)는 최신 보안패치가 적용된 버전으로 운영한다.

※ 준공예정일(사용승인예정일) 기준으로 소프트웨어 배포 버전별 기술지원 종료 기간(EOS)이 지난 버전은 사용할 수 없음

② 응용프로그램이 TLS 프로토콜 이용 시 SHA2 이상의 안전한 무결성 알고리즘이 포함된 사용 옵션을 설정한다.

3) 인증

요구사항

① 정당한 사용자만이 단지서버를 구성하는 운영체제(OS) 및 관련 소프트웨어(WEB, WAS, DBMS 등)에 접속할 수 있도록 인증 기능을 적용한다. 이때 사용자 확인을 위한 인증수단으로는 아이디/비밀번호, 일회용비밀번호(OTP), 생체인증, 전자서명 등을 적용할 수 있다.

② 단지서버를 구성하는 운영체제(OS), 관련 소프트웨어(WEB, WAS, DBMS 등) 및 응용프로그램의 계정은 다음과 같이 설정한다.

가. 기본계정(Default) 삭제/비활성화하거나 하거나, 쉽게 유추할 수 없도록 변경하여 사용한다. 다만, 운영체제 및 관련 소프트웨어에서 기본계정의 삭제, 비활성화 또는 변경기능을 제공하지 않는 경우에는 적용하지 아니할 수 있다.

나. 관리자 계정 생성 기능을 지원하는 경우 ID를 유추하기 어렵게 설정한다.

다. 불필요한 또는 사용하지 않은 계정은 삭제/비활성화 한다.

③ 단지서버를 구성하는 운영체제(OS), 관련 소프트웨어(WEB, WAS, DBMS 등) 및 응용프로그램의 비밀번호는 다음과 같이 설정한다.

가. 기본 비밀번호(Default Password)는 변경하여 사용한다.

나. 비밀번호는 쉽게 유추할 수 없도록 문자, 숫자 등을 조합하여 최소 8자리 이상으로 설정하고, 비밀번호 내에 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 제품 일련번호 등)이 포함되지 않도록 한다.

다. 비밀번호 변경 주기(예: 6개월 등) 설정 및 이전 비밀번호 재사용 제한 횟수를 설정할 수 있어야 한다.(변경 주기는 관리사무소와 협의 후 설정할 수 있음)

라. 단지서버와 관련 소프트웨어(WEB, WAS, DBMS 등)는 동일한 관리자 비밀번호를 사용하지 않는다.

④ 단지서버에 대한 인증시도가 일정횟수 이상(예: 5회 등) 실패할 경우 접근을 제한하도록 설정한다.

⑤ 단지서버에 접속 후 일정시간(예 : 10분 이내) 이상 작업을 하지 않는 경우 자동으로 접속이 차단되도록 설정을 한다.

4) 접근통제

요구사항

① 유닉스/리눅스 OS 접근통제

가. root 계정으로의 원격접속, su 명령어 사용 권한 등을 제한한다.

나. 서버 OS가 제공하는 서비스 구동에 필요한 계정은 용도별로 개별 생성하고 서비스 실행에 필요한 최소 권한으로 변경한다.

다. 불필요한 서비스(telnet, ftp, DHCP, NIS, SNMP, samba, nfs-utils, postfix, dovecot, rpcbind, rsync 등)는 중지/비활성화/제거한다.

라. 서버 인바운드 및 아웃바운드 패킷을 제한하기 위한 호스트 방화벽 설정(TCP Wrapper, iptables, firewalld 등)을 할 수 있다.

② 윈도우 OS 접근통제

가. 단지서버와 대외 서비스용 웹서버는 물리적 분리

나. Administrator 계정명 변경 또는 비활성화하고 Administrators 그룹 구성원에 불필요한 계정을 삭제한다.

다. 기본 공유를 제거한다.

라. 원격 관리를 하지 않은 경우 Remote Registry 시작 유형을 사용 안함으로 설정한다.

마. 원격데스크톱 연결 허용 시 RDP 세션타임 아웃 및 암호통신을 설정한다.

바. 시스템 종료 권한을 제한한다.

사. 화면 보호기를 설정한다.

아. 자동 로그인 기능은 사용하지 않도록 한다.

자. 윈도우 시스템 디렉토리 접근권한은 최소화한다.

차. 윈도우 방화벽 활성화 및 인바운드/아웃바운드 규칙 설정(RDP 접속허용 IP 설정, DB 접속포트 제한 등)

③ DBMS 접근통제

가. 서비스 계정과 사용자 계정을 분리한다.

나. root 계정으로 서비스 계정을 사용하지 않도록 한다.

다. 접속지 제한 기능을 제공하는 경우 DB 접속 계정 별 IP주소 제한한다.

라. 원격접속 시 SSL을 지원하는 경우 활성화한다.

마. DBA 및 시스템 테이블 접근권한 최소화한다.

바. 샘플 DB 및 불필요한 DB 삭제한다.

④ 홈네트워크 서비스 프로그램 접근통제

가. 인터넷망에서 단지서버 관리자페이지 접속을 원칙적으로 하지 않도록 한다. 유지보수 등의 불가피한 사유로 외부접속이 필요한 경우 안전한 접속 수단을 적용하여야 한다.(전용선, SSH, VPN 등)

나. 단지서버 관리자페이지 접속 시 IP주소를 제한한다.

다. 장기 미사용 계정(3개월) 자동 잠금 및 잠금 조치 후 6개월 경과 시 권한을 회수한다.

라. 장애대응 등 유지보수용 계정에 대해 작업종료 시 즉시 비활성화 한다.

마. 서비스 용도에 따라 메뉴에 대한 접근권한 차등 부여 및 불필요한 정보 노출(일치검색 또는 다중 검색조건 조회기능, 목록 조회 시 마스킹, 화면복사 제한 등) 최소화 한다.

⑤ 단지서버 관리 등을 목적으로 홈네트워크망 외부에서 단지서버로 접속하는 것은 원칙적으로 차단한다. 다만, 불가피한 사유로 외부 접속이 필요한 경우에는 안전한 접속수단을 적용하고 아이디/비밀번호 외에 일회용 비밀번호(OTP), 생체인증 등 안전한 인증수단을 적용을 고려한다.

⑥ 단지서버는 필요한 서비스만 사용하고 미사용 서비스는 비활성화한다. 단지서버 운영체제별 비활성화 대상 주요 서비스는 다음과 같으며, 단지서버 특성상 필요한 서비스로 판단된다면 비활성화하지 아니할 수 있다.

가. 리눅스 서버 : finger, anonymous FTP, r 계열 서비스, NFS, RPC, tftp, talk 등

나. 윈도우 서버 : anonymous FTP, Alerter, DHCP Client, Print Spooler, emote Registry 등

⑦ 단지서버의 응용프로그램에서 대외 웹서비스(또는 홈페이지 등)를 제공하기 위해 인터넷 등 외부 네트워크에 공개되는 웹서버를 운영하는 경우 내부 네트워크와 분리된 DMZ에 설치한다. 다만, 대외 웹서비스(또는 홈페이지 등)를 외부 클라우드 서버로 운영하는 경우 DMZ를 제외할 수 있다.

⑧ 인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위해 단지서버에서 의 불필요한 인터넷 접속 및 서비스(P2P, 웹하드, 메신저 등)를 제한한다.

⑨ 네트워크를 통해 원격에서 단지서버를 구성하는 운영체제(OS) 및 관련 소프트웨어(WEB, WAS, DBMS 등)에 접속하는 경우 지정된 단말에서만 접속할 수 있도록 접속 가능한 IP주소 또는 MAC주소 등을 제한한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ⑤, ⑦번 항목은 적용을 권장한다.

5) 전송데이터 보안

요구사항

① 관리를 위해 네트워크에서 단지서버로 접속하는 경우 암호통신 프로토콜을 적용한다.

가. 서버설정을 위한 원격터미널 접속 시 안전한 접속방법을 이용하여 연결한다. (SSH V2 등)

나. 기타 암호화되지 않는 서비스(HTTP, TELNET, FTP, TFTP 등) 는 비활성화한다.

② 홈네트워크 서비스 프로그램이 세대단말기, 홈네트워크 사용기기와 통신하는 경우 동작 환경의 특성을 고려하여 적절한 전송구간 암호 방식을 선택하여 구현 및 적용한다.

< 권장사항 >

■ 2022년 7월 1일 이전에 주택사업계획 승인(신청 포함)을 받은 공동주택의 경우 ②번 항목은 적용을 권장한다.

Ⅲ 재점검 대상 선정 기준

① 파생모델 대상 기준

요구사항

● 보안점검을 받은 제품의 파생모델 선정 기준

(1) 방송통신기자재등의 적합성평가를 받은 제품은 관련 고시*에 따른 파생모델 기준을 적용한다, 다만 「2. 재점검 대상 기준」에 해당하는 하드웨어 및 소프트웨어의 변경이 있는 경우에는 제외한다.

(2) 보안점검을 받은 모델과 비교하여 「2. 재점검 대상 기준」에 해당하지 않는 하드웨어의 변경사항(액정 커버 및 사양, 색상, 로고 등)이 발생한 제품은 파생모델로 적용할 수 있다. 다만, 하드웨어 변경에 따른 일부 소프트웨어 변경사항이 「2. 재점검 대상 기준」에 해당하지 않는 경우에는 변경 내용에 대한 증적 및 설명 자료를 제출하여야 한다.

(3) 파생모델 대상 제품은 보안점검을 받은 제품과 비교하여 변경사항에 대한 증적 및 설명자료와 「2. 재점검 대상 기준」에 해당하는 사항이 없음에 대한 확약서를 제출하여야 한다.

● 파생모델 적용 변경사항 예시

- 액정 커버 변경: 미러형, 글라스형 등
- 외관 변경: 색상, 실크, 로고 등
- 통합형 세대단말기 버튼 변경: 조명, 문열림 등 일체형 버튼의 위치 및 수량
- 액정사양 변경: 액정의 크기, 사양(해상도), 인터페이스 등
- 기본 모델과 대비하여 「2. 재점검 대상 기준」에 해당하지 않는 하드웨어의 변경

* 방송통신기자재등의 적합성평가에 관한 고시 제2조제1항제4호
4. "파생모델"이란 기본모델과 전기적인 회로・구조・기능이 유사한 제품군으로 기본모델과 동일한 적합성평가번호를 사용하는 기자재를 말한다.

② 재점검 대상 기준

요구사항

● 보안점검을 받은 스마트기기용 앱, 세대단말기, 무선방식의 홈네트워크 기기는 다음과 같은 변경사항이 있는 경우에는 재점검을 진행한다.

(1) 하위 버전과 호환이 되지 않는 변경이 있는 경우

(2) 하드웨어 또는 소프트웨어가 대규모로 변경된 경우

(3) 통신방식, 암호화 알고리즘, 인증방식, 개인정보 관리정책, 데이터 통신에 영향을 주는 변경사항이 (1), (2)에 해당하는 경우

● 보안점검을 받은 스마트기기용 앱, 세대단말기, 무선방식의 홈네트워크 기기가 재점검 대상 기준에 포함되지 않는 변경이 발생한 경우에는 유효기간을 연장 신청을 할 수 있으며, 다음과 같은 서류를 제출하여야 한다.

(1) 변경사항에 대한 증빙자료 (변경사항 전체 내용으로 작성)

(2) 소스코드의 시큐어 코딩 점검 결과서

(3) 재점검 대상 기준에 해당하는 변경사항이 없음에 대한 확약서

※ 2022년 7월 이전에 보안점검성적서를 받은 제품은 보안점검성적서를 받은 날로부터 3년 이내인 경우 재점검을 신청할 수 있으며, 3년이 초과된 제품은 신규로 신청하여야 함

Ⅳ 별지 서식

[별지 제1호] 홈네트워크건물인증 보안 사전점검 신청서

[별지 제2호] 홈네트워크건물 보안 사전점검 제품 내역서

[별지 제3호] 홈네트워크건물인증 보안 현장점검 신청서

[별지 제4호] 홈네트워크건물 보안 현장점검 구성 내역서

[별지 제1호 서식]

홈네트워크건물인증 보안 사전점검 신청서

신청인	회사명			
	사업자등록번호			
	소재지(본사)			
신청대상	구분	□ 앱	□ 세대단말기	□ 홈네트워크 무선기기
	제품명			
	제조사			

담당자	성명		이메일		연락처	

홈네트워크건물인증 신청 현황	구 분		□ 공동주택 □ 오피스텔
	건축주		
	건설사		
	홈네트워크건물 등급		□ AAA등급 □ AA등급 □ A등급
	건축물 현황	명칭	
		주소	
		규모	동 세대 ㎡

홈네트워건물인증을 위한 보안 사전점검을 상기와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

한국정보통신진흥협회장 귀하

신청인 제출서류	홈네트워크건물인증 보안 사전점검 제품 내역서
기타사항	보안 사전점검 신청에 대해 개인정보(회사명, 성명, 연락처, 이메일, 주소) 수집·이용 동의여부 □

[별지 제2호 서식]

홈네트워크건물 보안 사전점검 제품 내역서

[해당사항 체크]

세대단말기	제품명	
	제조사	
	운영체제(OS)	☐ Android ☐ Linux ☐ Window ☐ 기타( )
	버전 정보	☐ 운영체제( ) ☐ 소프트웨어( ) ☐ 하드웨어( )
	개발 언어	☐ C ☐ C++ ☐ JAVA ☐ 기타( )
	정보보호인증	(IoT보안인증 번호)
	기타사항	(파생모델 등)
		(담당자 연락처 및 이메일)
스마트기기용 앱	제품명	
	제조사	☐ 개발( ) ☐ 운영( )
	운영체제	☐ Android ☐ iOS ☐ 기타( )
	버전 정보	☐ Android( ) ☐ iOS( ) ☐ 기타( )
	정보보호인증	(IoT보안인증 번호)
	기타사항	(담당자 연락처 및 이메일)
		(기타사항)
홈네트워크 무선기기	제품명	
	제조사	
	개발 언어	☐ C ☐ C++ ☐ JAVA ☐ 기타( )
	버전 정보	☐ 제품( ) ☐ 소프트웨어( ) ☐ 하드웨어( )
	외부 포트	☐ USB ☐ JTAG ☐ UART ☐ 없음 ☐ 기타( )
	무선통신	☐ ZigBee ☐ Bluetooth ☐ Wifi ☐ RF ☐ 기타( )
	업데이트	☐ 업데이트 기능 미제공 ☐ 업데이트 기능 제공
	관리 App	☐ 제공 ☐ 미제공
	정보보호인증	(IoT보안인증 번호)
	기타사항	(파생모델 등)
		(담당자 연락처 및 이메일)

[별지 제3호 서식]

■ 홈네트워크건물인증 보안 현장점검 신청서

※ □에는 해당되는 곳에 √표를 합니다.

신청인	건축주(건설사)			
	사업자번호			
	주 소			
	전화번호		이메일	
건축물	구 분	□ 공동주택 □ 오피스텔		
	이 름			
	주 소			
	건축허가번호			
	준공예정일			
	규 모	동 세대 ㎡		
신청내용	홈네트워크건물	□ AAA(홈IoT) □ AA □ A		
	보안점검	□ 세대단말기	□ 스마트기기용 앱	□ 홈네트워크 기기 (무선방식)
		□ 현장점검(단지네트워크장비, 단지서버 등)		

위와 같이 홈네트워크건물인증 보안점검을 신청합니다.

년 월 일

신청인 (서명 또는 인)

한국정보통신진흥협회장 귀하

신청인 제출서류	홈네트워크건물 보안 현장점검 구성 내역서(별지 제4호)	수수료 [별표 1]
기타 사항		

[별지 제4호 서식]

홈네트워크건물 보안 현장점검 구성 내역서

[해당사항 체크]

정보보안장비 (방화벽 등)	제품명	
	제조사	
	종류	□ 방화벽 □ IPS □ UTM □ 기타( )
	정보보호제품 평가·인증 등	□ 보안기능확인서 □ 보안적합성 평가 □ CC 평가·인증 □ 기타( )
	기타사항	(담당자 연락처 및 이메일)
네트워크장비 (백본)	제품명	
	제조사	
	정보보호제품 평가·인증 등	□ 보안기능확인서 □ 보안적합성 평가 □ CC 평가·인증 □ 기타( )
	기타	(담당자 연락처 및 이메일)
네트워크장비 (워크그룹스위치)	제품명	
	제조사	
	기타사항	(담당자 연락처 및 이메일)
서버	제조사	
	단지서버	□ Linux □ Windows □ UNIX □ 기타( )
	데이터베이스	□ MS-SQL □ DB2 □ Oracle □ 기타( )
	WAS	□ JEUS □ Tomcat □ Jboss □ 기타( )
	WEB	□ WebtoB □ Apache □ Iis □ 기타( )
	기타사항	(담당자 연락처 및 이메일)