홈네트워크 보안가이드

2024년 6월 27일

과학기술정보통신부
Ministry of Science and ICT

한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

가이드 제·개정 연혁

• 이 가이드는 「지능형 홈네트워크 설비 설치 및 기술기준」 제14조의2(홈네트워크 보안)제1항 및 제2항에 해당되는 부분에 대한 설명으로 제·개정 연혁은 다음과 같다.

가이드	주요내용	제·개정 (년.월)	버전
홈네트워크 보안가이드	• 홈네트워크 보안에 관한 사항 제정	제정 (2022.12.16.)	V1.0
‘’	• 홈네트워크 기술 예시 보완 등 일부 수정	개정 (2023.7.31.)	V1.1
‘’	• 홈네트워크 설비 구성요소 예시 부록 추가	개정 (2024.6.27.)	V1.2

목 차

홈네트워크 보안

1. 일반사항

1.1 적용범위

(1) 본 가이드는 「지능형 홈네트워크 설비 설치 및 기술기준」(국토교통부고시, 산업통상자원부고시, 과학기술정보통신부고시) 제14조의2(홈네트워크 보안) 제1항과 제2항에 대하여 세부사항을 설명하는 것으로 그 적용범위를 한정한다.

1.2 참고기준

1.2.1 관련 법규

(1) 본 가이드와 관련된 법령 및 고시는 다음과 같다.

- 「주택법」 제2조제13호
- 「주택건설기준 등에 관한 규정」 제32조의2
- 「지능형 홈네트워크 설비 설치 및 기술기준」 제14조의2(홈네트워크 보안) 제1항과 제2항

1.2.2 참고 문헌

(1) 본 가이드는 아래의 기준 및 해설서를 참고하여 작성하였다.

- ITU-T Rec. X.1111 (02/2007) Framework of security technologies for home network
- ISO/IEC 27002(Second edition 2013.10) Information technology - Security techniques - Code of practice for information security controls
- 정보통신망연결기기등 정보보호인증기준 상세 해설서('22.8)
- 정보보호 및 개인정보보호 관리체계 (ISMS-P) 인증기준 안내서('22.4)
- 정보보호시스템 및 네트워크 장비 국가용 보안요구사항('21.4)

1.3 용어정의

(1) 홈네트워크 설비 : 주택의 성능과 주거의 질 향상을 위하여 세대 또는 주택단지 내 지능형 정보통신 및 가전기기 등의 상호 연계를 통하여 통합된 주거서비스를 제공하는 설비로 홈네트워크망, 홈네트워크장비, 홈네트워크사용기기로 구분

(2) 홈네트워크망 : 홈네트워크장비 및 홈네트워크사용기기를 연결하는 것을 말하며 단지망과 세대망으로 구분

(3) 단지망 : 집중구내통신실에서 세대까지를 연결하는 망

(4) 세대망 : 전유부분(각 세대내)을 연결하는 망

(5) 홈네트워크장비 : 홈네트워크망을 통해 접속하는 장치를 말하며 홈게이트웨이, 세대단말기, 단지네트워크장비, 단지서버 등으로 구분

(6) 홈게이트웨이 : 전유부분에 설치되어 세대내에서 사용되는 홈네트워크사용기기들을 유무선 네트워크로 연결하고 세대망과 단지망을 상호 접속하는 장치(단, 세대단말기가 홈게이트웨이 기능을 포함하는 경우는 세대단말기로 대체 가능)

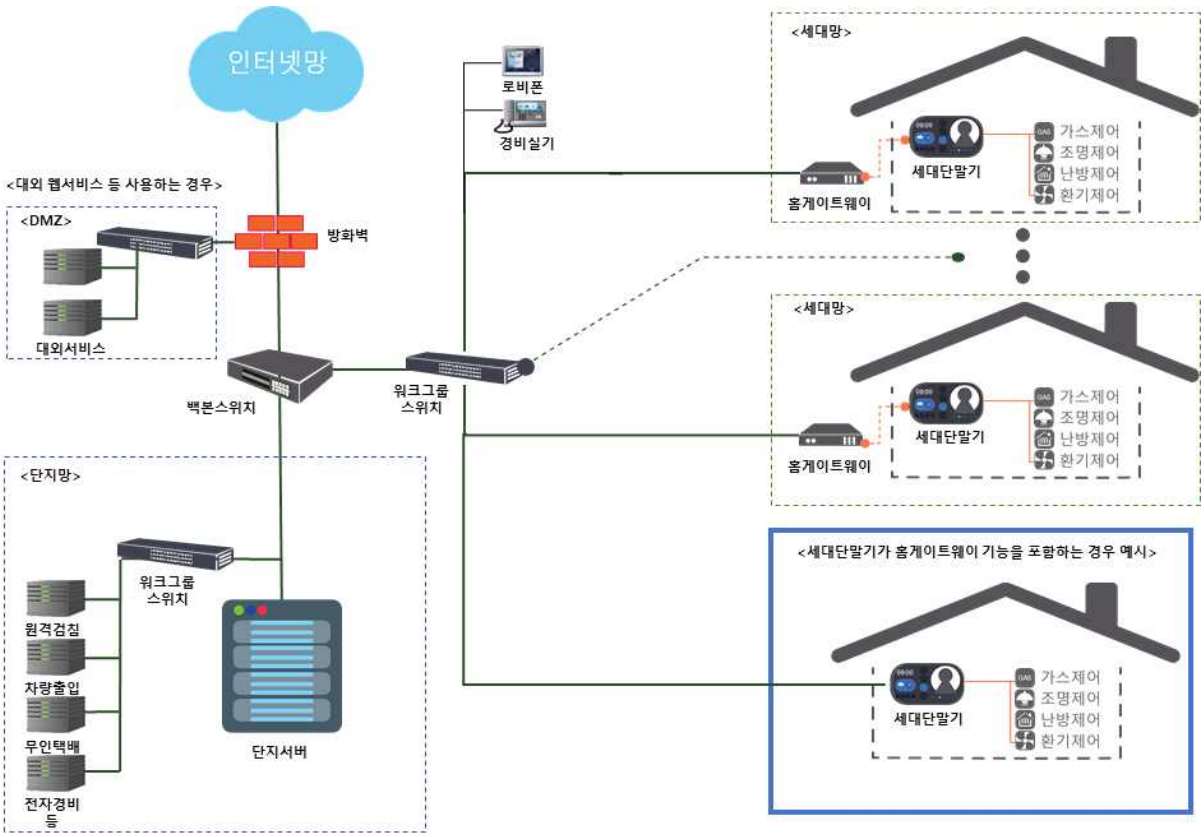
(7) 세대단말기(월패드) : 세대 및 공용부의 다양한 설비의 기능 및 성능을 제어하고 확인할 수 있는 기기로 사용자인터페이스를 제공하는 장치

(8) 단지네트워크장비 : 세대내 홈게이트웨이와 단지서버간의 통신 및 보안을 수행하는 장비로서, 백본(Backbone), 방화벽(Firewall), 워크그룹스위치 등 단지망을 구성하는 장비

(9) 단지서버 : 홈네트워크 설비를 총괄적으로 관리하며, 이로부터 발생하는 각종 데이터의 저장·관리·서비스를 제공하는 장비

(10) 홈네트워크사용기기 : 홈네트워크 망에 접속하여 사용하는 원격제어기기, 원격검침시스템, 감지기, 전자출입시스템, 차량출입시스템, 무인택배시스템, 영상정보처리기기, 전자경비시스템 등의 장비

<그림 1> 홈네트워크 설비 구성요소 예시



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있으며, 추가 예시는 [부록] 참고

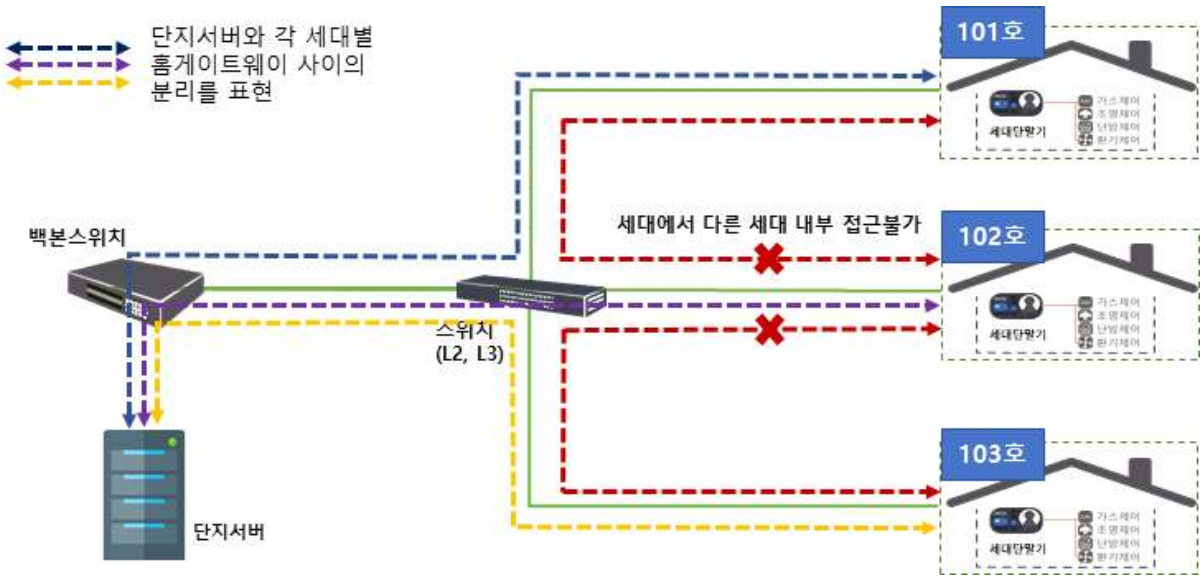
2. 홈네트워크 구성

지능형 홈네트워크 설비의 설치 및 기술기준
제14조의2(홈네트워크 보안) ① 단지서버와 세대별 홈게이트웨이 사이의 망은 전송되는 데이터의 노출, 탈취 등을 방지하기 위하여 물리적 방법으로 분리하거나, 소프트웨어를 이용한 가상사설통신망, 가상근거리통신망, 암호화기술 등을 활용하여 논리적 방법으로 분리하여 구성하여야 한다.

세대별 홈네트워크 분리 요건에 따라, 각 세대와 단지서버 사이의 망은 전송되는 데이터의 노출, 탈취 등을 방지하기 위해 분리하여 구성하여야 하며, 각 세대망은 단지서버 외에 다른 세대의 내부로 접근 할 수 없어야 한다. 이를 구현하기 위하여 물리적 방법 또는 논리적 방법을 활용할 수 있다.

※ 논리적 망분리를 구현할 수 있는 신기술들을 반영해 나갈 계획임

<그림 2> 세대별 홈네트워크 구성 요건 개념도



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

2.1 물리적 분리 방법

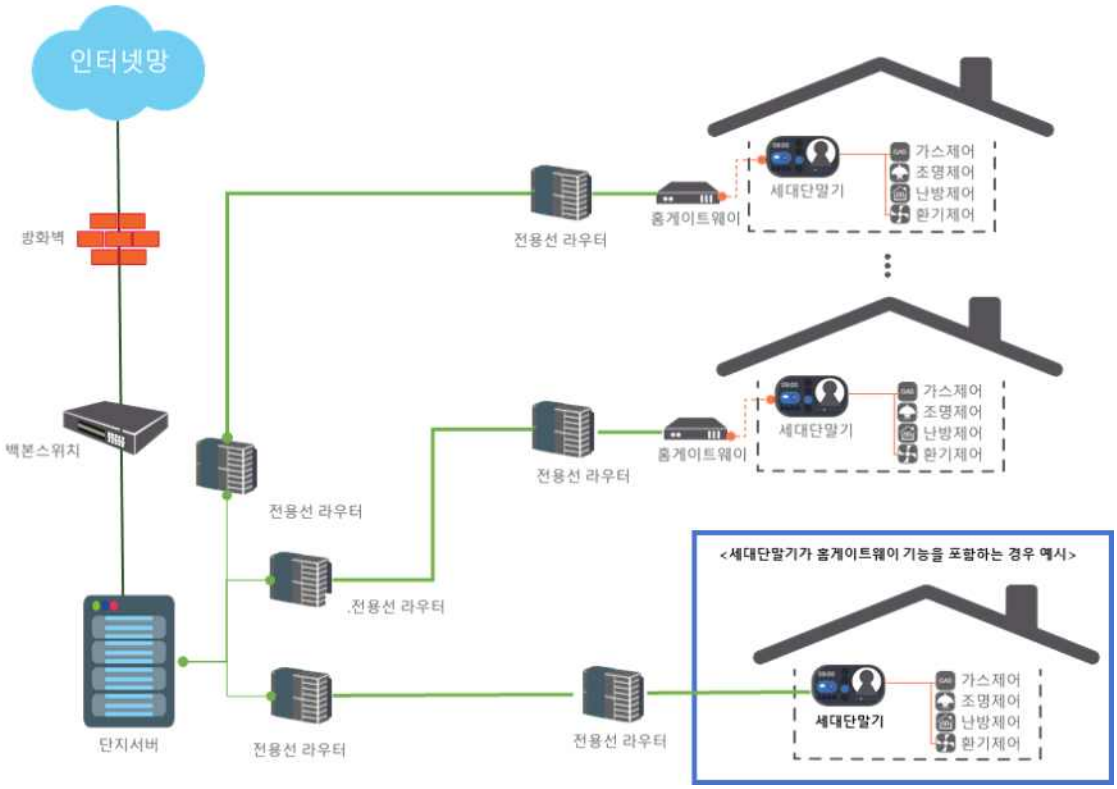
물리적 분리는 단지서버와 각 세대망 사이의 네트워크 구성을 물리적인 단일 네트워크로 연결하여 구성하는 방법을 의미한다. 단지서버와 각 세대망을 연결하는 네트워크를 세대마다 독립적으로 구축하여 단지서버에 연결되어야 하는 세대수만큼 개별 구축한다.

2.1.1. 물리적 기술예시① - 전용선 라우터를 이용한 분리

(1) 단지서버로부터 각 세대망까지 성형배선[1] 등의 방식으로 케이블을 연결하여 물리적으로 회선을 분리하여 구축하는 방법 등을 사용한다.

(2) 단지서버에서 각 세대로 통신을 위해 인입되는 물리적인 네트워크 케이블을 세대별로 각각 설치하여야 한다. 전용선 라우터 등을 활용하여 세대망을 단일회선으로 구성하여 연결한다.

<그림 3> 전용선 라우터를 이용한 물리적 분리 예시



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

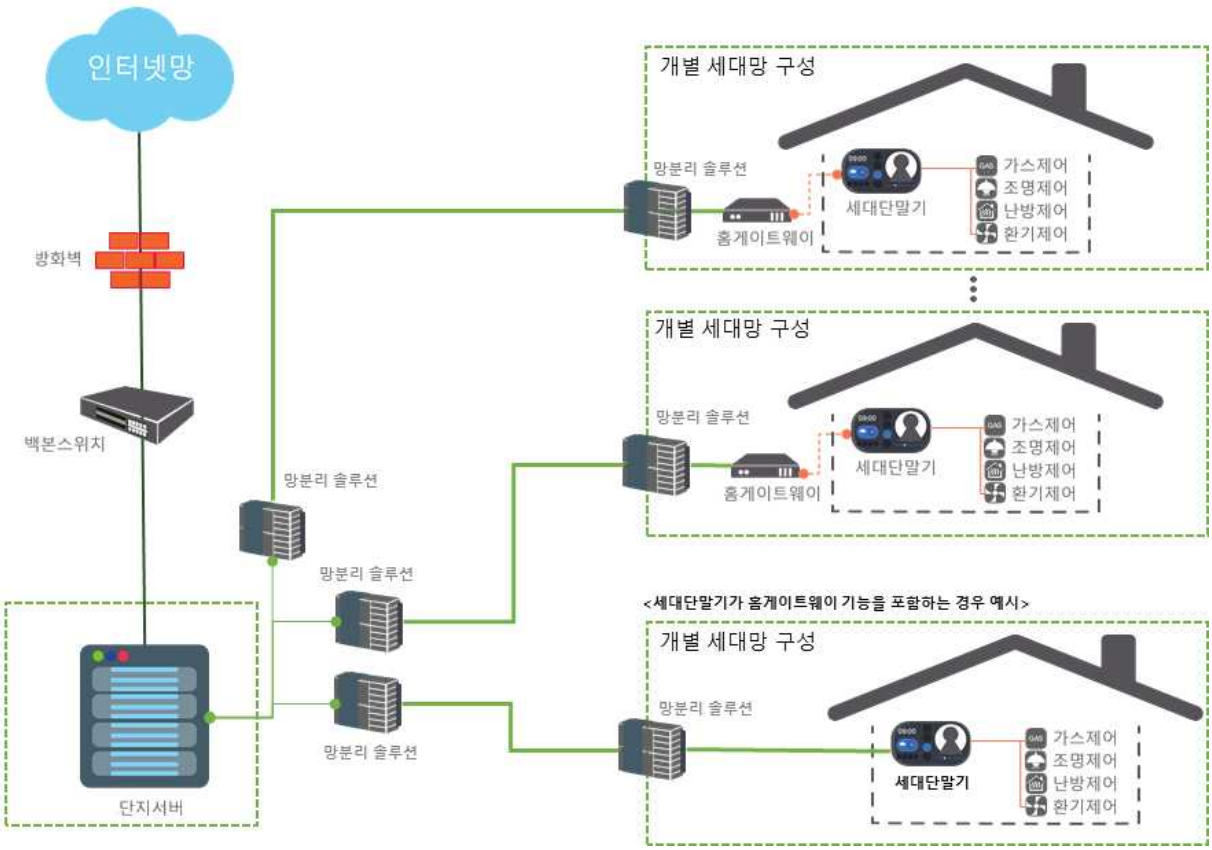
1) 성형배선 : 세대단자함에서 각각의 직렬단자까지 직접 배선되는 방식(「방송 공동수신설비의 설치 기준에 관한 고시」 제2조 제14호)

2.1.2. 물리적 기술예시② - 망분리 솔루션 이용한 분리

(1) 망분리 솔루션[2]을 이용하여 단지서버망과 개별 세대망을 각각 구성하고 개별 세대망과 서버망을 연계시켜 통신이 가능하게 하도록 구성한다.

(2) 세대에서는 단지서버로만 통신가능하며, 세대에서 다른 세대의 내부로의 접속은 불가능하게 구성한다.

<그림 4> 망분리 솔루션 이용한 분리 예시



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

2) 망분리 솔루션은 국가정보원의 "정보보호시스템 및 네트워크 장비 국가용 보안요구사항"의 "구간 보안 제품군" 중 "망간 자료전송제품 보안요구사항"을 참조

2.2 논리적 분리 방법

논리적 분리 방법은 네트워크 회선을 타세대와 공동으로 이용하더라도 물리적으로 분리된 것과 유사하게 운영하는 방법을 의미한다. 이를 구현하기 위해서는 가상사설통신망(VPN), 가상근거리 통신망(VLAN) 등의 기술을 이용할 수 있다.

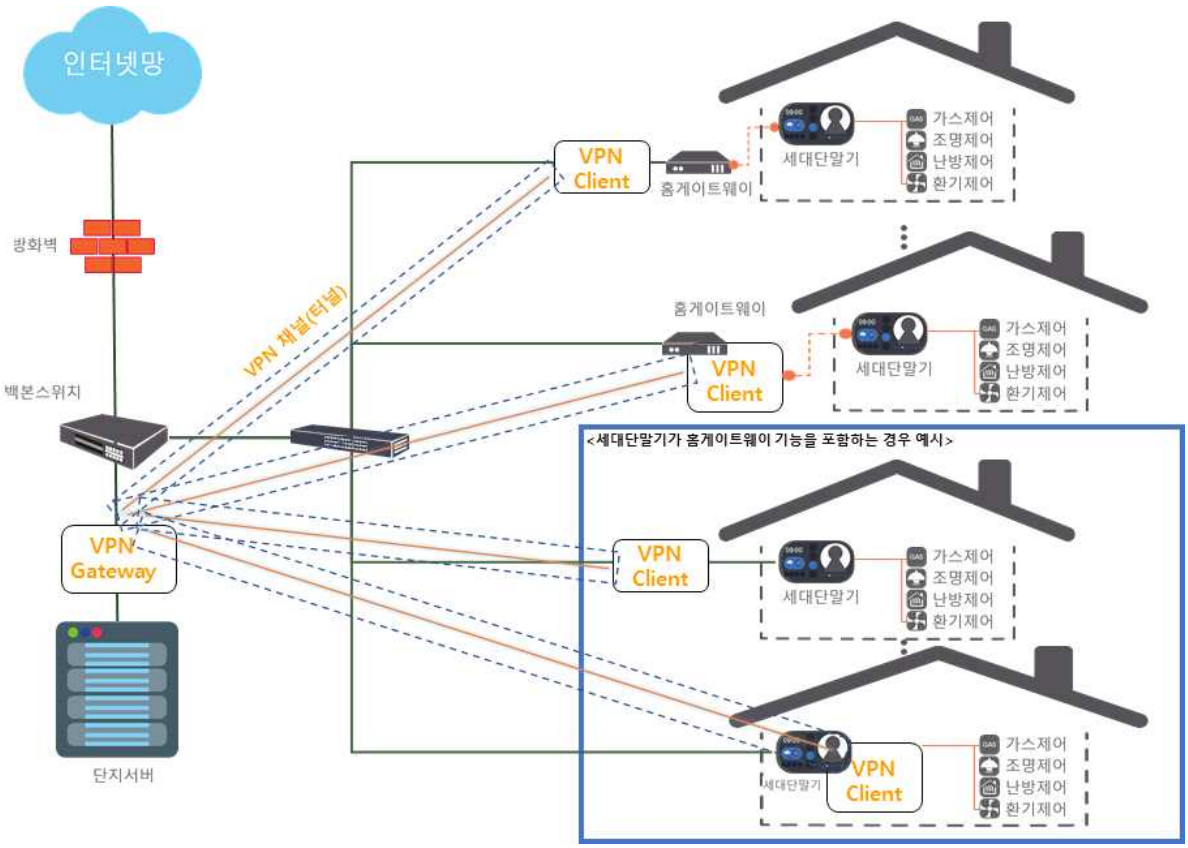
2.2.1. 논리적 기술예시① - VPN을 이용한 기술

(1) 가상사설통신망(Virtual private network, 'VPN')은 VPN 게이트웨이와 VPN 클라이언트간 가상경로를 설정하는 채널(터널)을 만들고 이를 통해 송수신되는 데이터를 보호하는 기술이다. 이를 통해 각 세대망은 단지서버 외에 다른 세대의 내부로 접근 할 수 없도록 한다.

※ VPN의 구성은 L2 VPN(Layer 2 VPN), L3 가상 네트워크(IPSec VPN, IP Tunnel, Virtual Routing 등), SSL VPN 등의 방식으로 구현할 수 있다.

(2) 단지서버와 각 세대망 간에는 홈네트워크 서비스 및 운영을 위해 필요한 통신만 허용하고 세대에서 다른 세대의 내부로 접속이 불가능하도록 접근제어(IP 주소, Port 등)를 설정하여 관리한다.

<그림 5> VPN을 이용한 기술 예시



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

고려사항

- 가상사설통신망(VPN)을 이용한 방법 중 구간 내 암호화 기능을 포함하고 있지 않는 경우에는 네트워크 스니핑으로 인한 피해를 예방하기 위해 통신 암호화 등의 추가 보안을 적용한다.
- VPN 게이트웨이는 단지서버와 홈게이트웨이 사이 안전한 통신채널을 형성
- VPN 클라이언트는 VPN 게이트웨이에 안전하게 접속하게 해줌
- VPN 게이트웨이, VPN 클라이언트, VPN 관리서버, VPN 관리도구 등의 다양한 요소로 구성 될 수 있음
- 전송데이터 암호방식은 안전도 112비트 이상으로 설정한다.
- 전송데이터 위·변조를 방지하도록 무결성 방식은 안전도 112비트 이상으로 설정한다.

<국내・외 권고 암호 알고리즘 예시(112 비트 이상)>

구분		암호 알고리즘
대칭키 암호 알고리즘		・SEED, HIGHT ・ARIA-128/192/256 ・LEA-128/192/256 ・AES-128/192/256 ・3TDEA
해시 함수	단순해시/전자서명용	・SHA-224/256/384/512 ・SHA-512/224, SHA-512/256
	메시지인증/키유도/ 난수생성용	・SHA3-224/256/384/512 ・LSH-224/256/384/512 ・LSH-512/224, SHA-512/256
공개키 암호 알고리즘	키 공유용	・[이산대수 문제] DH, MQV ・[타원곡선] ECMQV, ECDH
	암·복호화용	・[인수분해 문제] RSAES, RSA
	전자서명용	・[인수분해 문제] RSA-PSS, RSA ・[이산대수 문제] KCDSA, DSA ・[타원곡선] ECDSA, EC-KCDSA, ECDSA

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

2.2.2. 논리적 기술예시② - VLAN을 이용한 기술

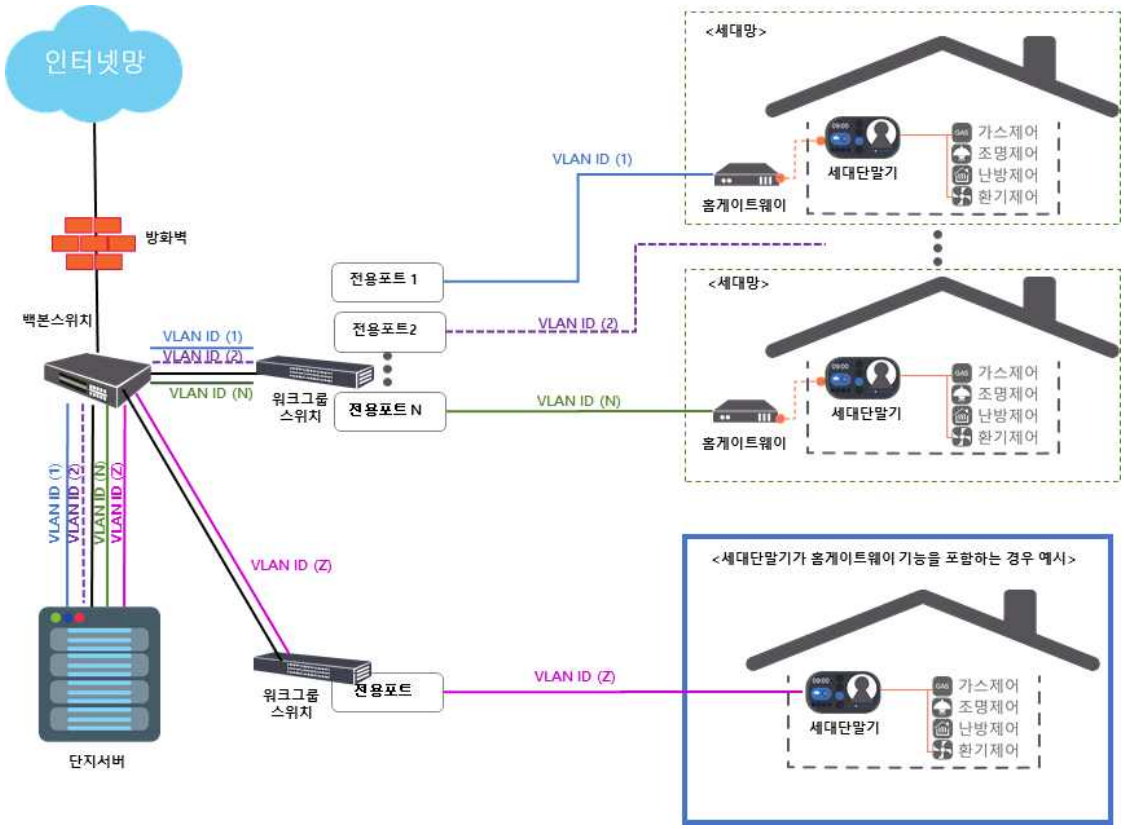
(1) 가상근거리통신망(VLAN)은 네트워크 스위치를 이용하여 각 세대별로 개별 네트워크를 별도로 할당함으로써 개별 세대 네트워크망을 논리적으로 분리하는 기술로 각 세대망은 단지서버 외에 다른 세대의 내부로 접근 할 수 없도록 한다.

※ VLAN은 일반적인 VLAN(IEEE 802.1Q)과 VxLAN(Virtual Extensible LAN) 등의 방식으로 구현할 수 있다.

(2) 네트워크 스위치(L2, L3 등) 를 이용하여 세대별 가상근거리통신망(VLAN)을 구성한다. 구성 방식에는 포트 기반 구성, IP 주소 기반 구성, MAC 기반 구성 등이 있다.

(3) 단지서버와 각 세대망 간에는 홈네트워크 서비스 및 운영을 위해 필요한 통신만 허용하고 세대에서 다른 세대의 내부로 접속이 불가능하도록 접근제어(IP 주소, Port 등)를 설정하여 관리한다.

<그림 6> VLAN을 이용한 기술 예시



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

고려사항
• 네트워크 스위치 장비 교체 등의 이슈 발생 시 VLAN 구성을 유지하고 지속적으로 관리될 수 있도록 한다. • 가상근거리통신망(VLAN)을 이용한 방법은 구간 내 암호화 기능을 포함하고 있지 않으므로 네트워크 스니핑으로 인한 피해를 예방하기 위해 통신 암호화 등의 추가 보안을 권고한다.

3. 홈네트워크장비 보안요구사항

지능형 홈네트워크 설비 설치 및 기술기준

제14조의2(홈네트워크 보안) ② 홈네트워크장비는 보안성 확보를 위하여 별표 1에 따른 보안요구사항을 충족하여야 한다. 다만,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따라 정보보호 인증을 받은 세대단말기는 별표1 보안요구사항을 충족한 것으로 인정한다.

[별표 1] 홈네트워크장비에 대한 보안요구사항

구분	보안요구사항
1. 데이터 기밀성	이용자 식별정보, 인증정보, 개인정보 등에 대해 암호 알고리즘, 암호키 생성·관리 등 암호화 기술과 민감한 데이터의 접근제어 관리기술 적용으로 기밀성을 구현 ※ 데이터의 처리(생성, 읽기, 쓰기, 변경, 삭제, 저장 등)가 아닌 단순 전송 등을 담당하는 워크그룹 스위치 등은 적용 제외
2. 데이터 무결성	이용자 식별정보, 인증정보, 개인정보 등에 대해 해쉬함수, 전자서명 등 기술 적용으로 위·변조 여부 확인 및 방지 조치 ※ 데이터의 처리(생성, 읽기, 쓰기, 변경, 삭제, 저장 등)가 아닌 단순 전송 등을 담당하는 워크그룹 스위치 등은 적용 제외
3. 인증	사용자 확인을 위하여 전자서명, 아이디/비밀번호, 일회용비밀번호(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

3.1 일반사항

홈네트워크장비는 홈네트워크망을 통해 접속하는 장치를 말하며 홈게이트웨이, 세대단말기, 단지네트워크장비, 단지서버 등으로 구분한다. 장비별 적용되는 보안요구사항은 아래와 같다.

[표 1] 「지능형 홈네트워크 설비 설치 및 기술기준」 홈네트워크장비 보안요구사항 적용표

홈네트워크장비		1. 데이터 기밀성	2. 데이터 무결성	3. 인증	4. 접근통제	5. 전송데이터 보안
단지 네트워크 장비	백본	○	○	○	○	○
	방화벽	○	○	○	○	○
	워크그룹 스위치	X	X	○	○	○
홈게이트웨이		○	○	○	○	○
세대단말기		○	○	○	○	○
단지서버		○	○	○	○	○

3.2 단지네트워크장비 보안

단지네트워크장비는 세대내 홈게이트웨이와 단지서버간의 통신 및 보안을 수행하는 장비로서, 백본(Backbone)[3], 방화벽(Firewall)[4], 워크그룹 스위치 등 단지망 구성 장비를 말한다.

3.2.1. 백본

단지네트워크장비 중 백본은 홈네트워크에서 인터넷망, 단지서버, 세대내 홈게이트웨이 사이를 네트워크로 연결시켜 주는 고속 통신망 역할을 하는 장비를 말한다.

(1) 데이터 기밀성

기준설명
백본에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.

[권장사항]

① 백본에 접속할 경우, 관리자 모드 진입에 사용하는 비밀번호 저장 시 SHA2 이상의 안전한 알고리즘[5]으로 암호화하여 저장한다.

(2) 데이터 무결성

기준설명
백본에 저장된 데이터의 위・변조를 방지하고 위・변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.

[권장사항]

① 백본 설정 파일의 위·변조 여부를 확인할 수 있도록 설정값을 백업하여 확인하거나, 설정 파일의 무결성 검증방안을 마련하여 적용한다.

---

3) 백본(Backbone) : 소규모의 근거리 통신망(LAN) 또는 지선 근거리 통신망(branch LAN) 상호 간의 통신량을 전송하는 주요 전송로, [출처 : TTA, 정보통신용어사전]

4) 방화벽(Firewall) : 외부의 침입으로부터 자사의 네트워크를 보호하기 위하여 게이트웨이에 설치되는 접속 장치나 기능, [출처 : TTA, 정보통신용어사전]

5) 안전한 알고리즘 : 암호강도 112비트 이상의 해쉬함수(SHA-256, SHA-512 등) 사용을 권장한다. [출처 : KISA, 암호 알고리즘 및 키 길이 이용 안내서, 2018]

② 백본은 제조사가 제공하는 최신 보안패치를 적용한다.

(3) 인증

기준설명
사용자 인증을 위해 백본에 안전한 인증수단을 적용하는 것을 말한다.

[권장사항]

① 백본 접속을 위한 기본 계정(Default) 비활성화하거나 쉽게 유추할 수 없도록 변경하여 사용하고 불필요한 계정은 즉시 삭제한다. 백본에서 기본 계정 삭제, 비활성화/변경 기능을 제공하지 않는 경우는 이를 적용하지 아니할 수 있다.

② 인가된 사용자(예: 관리자 등)만이 백본에 로그인(예: 콘솔 로그인, 터미널 로그인, 기타서비스 로그인 등)할 수 있도록 인증 기능을 적용한다. 사용자 확인을 위한 인증수단으로는 아이디/비밀번호, 일회용비밀번호(OTP), 생체인증, 전자서명 등을 적용할 수 있다.

③ 제조업체가 설정한 기본 비밀번호(Default Password)는 변경하여 사용한다. 비밀번호는 아래의 내용을 참고하여 설정한다.

가. 비밀번호는 영문자, 숫자, 특수문자 중 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

나. 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 일련번호 등)를 포함하는 비밀번호 사용은 제한한다.

다. 비밀번호 변경 주기(예: 6개월 등)를 설정한다.

④ 백본 접속에 대한 인증시도가 일정횟수 이상(예: 5회 등) 실패할 경우, 접근을 제한(예: 계정 잠금 5분 등)하도록 설정한다.

⑤ 접속(예: 콘솔연결, 터미널 연결 등) 후 일정시간 이상 작업을 하지 않는 경우 자동으로 접속이 차단되도록 설정(예: 10분 이내)을 한다.

(4) 접근통제

기준설명
백본으로의 비인가 접근을 통제하고 서비스 목적에 따른 접근권한을 최소한으로 부여하고, 불필요한 서비스를 비활성화하여 사용목적 이외의 접근을 통제하는 것을 말한다.

[권장사항]

① 원격 네트워크를 이용하여 백본으로 접속하는 경우, 지정된 단말(IP 또는 MAC주소 등 등록)에서만 접속할 수 있도록 한다.

② 백본 설정 파일의 접근권한을 최소화한다.

③ 불필요한 서비스(echo, discard, chargen, finger, tftp 등)를 비활성화한다.

④ 관리자 웹페이지가 존재하는 경우 비활성화한다.

⑤ 불필요한 I/O 포트 및 네트워크 인터페이스는 비활성화한다.

(5) 전송데이터 보안

기준설명
백본을 통해 전송되는 데이터의 보호를 위해, 트래픽 흐름 제어를 위한 기능을 적용하는 것을 말한다.

[권장사항]

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. 허용규칙에 적용되지 않은 경우, 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.

② 네트워크를 통해 원격에서 백본에 접속하는 경우 암호통신 프로토콜을 적용한다.

가. 백본 설정을 위한 원격터미널 접속 시 SSH V2 이상을 적용하여 연결한다.

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

③ 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

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

3.2.2. 방화벽

단지네트워크장비 중 방화벽은 홈네트워크를 보호하기 위해 네트워크 트래픽 통제 등이 가능한 보안 장비를 말한다.

(1) 데이터 기밀성

기준설명
방화벽에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.

[권장사항]

① 방화벽에 접속할 경우, 관리자 모드 진입에 사용하는 비밀번호 저장 시 SHA2 이상의 안전한 알고리즘으로 암호화하여 저장한다.

(2) 데이터 무결성

기준설명
방화벽에 저장된 데이터와 업데이트 파일의 위・변조를 방지하고, 위・변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.

[권장사항]

① 방화벽 S/W를 업데이트 할 경우, 파일 설치 전 무결성 검증을 시행한다.

② 제조사가 제공하는 최신 보안패치를 적용한다.

(3) 인증

기준설명
인가된 관리자만이 방화벽의 정보흐름통제 규칙을 설정 및 관리 할 수 있는 기능을 수행할 수 있도록 안전한 인증수단을 적용하는 것을 말한다.

[권장사항]

① 방화벽 출고 시 설정되어 나오는 기본 계정을 비활성화하거나 쉽게 유추할 수 없도록 변경하여 사용하고 불필요한 계정은 즉시 삭제한다. 방화벽에서 기본 계정의 삭제, 비활성화 또는 변경 기능을 제공하지 않는 경우는 이를 적용하지 아니할 수 있다.

② 허가된 사용자만이 방화벽에 접속할 수 있도록 인증 기능을 적용한다. 사용자 확인을 위한 인증수단으로는 아이디/비밀번호, 일회용비밀번호(OTP), 생체인증, 전자서명 등을 적용할 수 있다.

③ 제조사가 설정한 기본 비밀번호(Default Password)는 변경하여 사용한다. 비밀번호는 아래의 내용을 참고하여 설정한다.

가. 비밀번호는 영문자, 숫자, 특수문자 중 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

나. 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 일련번호 등)를 포함하는 비밀번호 사용 제한한다.

다. 비밀번호 변경 주기(예: 6개월 등)를 설정한다.

④ 인증시도가 일정횟수 이상(예: 5회 등) 실패할 경우 접근을 제한(예: 계정 잠금 5분 등)하도록 설정한다.

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

⑥ 관리자 웹페이지의 동시 접속을 제한한다.

(4) 접근통제

기준설명
서비스 목적에 따른 접근권한을 최소한으로 부여하여 방화벽으로 비인가자가 접근하는 것을 통제하고 방화벽 접근내역을 추적할 수 있도록 로그를 남기는 것을 말한다.

[권장사항]

① 네트워크를 통해 원격에서 방화벽으로 접속이 필요한 경우, 지정된 단말(IP 또는 MAC주소 등 등록)에서만 접속할 수 있도록 한다.

② 방화벽 설정 파일의 접근권한을 최소화한다.

③ 공용계정은 사용하지 않도록 한다.

④ 방화벽 정책(Rule) 적용에 따른 성공/실패 로그, 관리자 계정 수행 행위 로그, 시스템 중요 이벤트 발생 시 로그 등을 생성·저장할 수 있도록 설정한다.

(5) 전송데이터 보안

기준설명
용도에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역간 트래픽 흐름을 통제하여야 하며 관리자가 설정한 정책에 따라 정보흐름을 통제하는 것을 말한다.

[권장사항]

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 공개서버가(대외 웹서비스 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.

다. 세대망을 연결하는 워크그룹 스위치 영역, 단지서버 및 관리서버를 연결하는 내부망, 세대 공용 홈네트워크사용기기(원격검침, 무인택배, 차량출입통제 등)를 연결하는 세대

공용망 등 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.

3.2.3. 워크그룹 스위치

워크그룹 스위치는 동단자함(IDF) 등에 설치되어 각 세대와 주배선반(MDF)의 백본(Back-bone) 스위치 사이의 트래픽을 전달하는 기능을 제공하는 장비를 말한다.

(1) 인증

기준설명
워크그룹 스위치에 접근 시 안전한 인증수단을 적용하여 사용자를 인증하는 것을 말한다.

[권장사항]

① 워크그룹 스위치 관리를 위해 기본 계정을 비활성화하거나 쉽게 유추할 수 없도록 변경

하여 사용하고 불필요한 계정은 즉시 삭제한다. 워크그룹 스위치에서 기본 계정의 삭제, 비활성화 또는 변경 기능을 제공하지 않는 경우는 이를 적용하지 아니할 수 있다.

② 허가된 사용자만이 워크그룹 스위치에 로그인(예: 콘솔 로그인, 터미널 로그인, 기타서비스 로그인 등)할 수 있도록 인증 기능을 적용한다.

③ 제조업체가 설정한 기본 비밀번호(Default Password)는 변경하여 사용한다. 비밀번호는 아래의 내용을 참고하여 설정한다.

가. 비밀번호는 영문자, 숫자, 특수문자 중 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

나. 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 일련번호 등)를 포함하는 비밀번호 사용 제한한다.

다. 비밀번호 변경 주기(예: 6개월 등)를 설정한다.

④ 워크그룹 스위치 접속에 대한 인증시도가 일정횟수 이상(예: 5회 등) 실패할 경우, 접근을 제한(예: 계정 잠금 5분 등)하도록 설정한다.

⑤ 접속(예: 콘솔연결, 터미널 연결 등) 후 일정시간 이상 작업을 하지 않는 경우 자동으로 접속이 차단되도록 설정(예: 10분 이내)을 한다.

(2) 접근통제

기준설명

서비스 목적에 따른 접근권한을 최소한으로 부여하여 워크그룹 스위치에 비인가 접근을 통제하는 것을 말한다.

[권장사항]

① 네트워크를 통해 원격에서 워크그룹 스위치에 접속하는 경우 지정된 단말(IP 또는 MAC주소 등 등록)에서만 접속할 수 있도록 한다. 스위치에서 접속 가능한 IP주소 제한 기능이 지원하지 않는 경우 이를 적용하지 아니할 수 있다.

② 워크그룹 스위치 설정 파일의 접근권한을 최소화한다.

③ 관리자 웹페이지가 존재하는 경우 비활성화한다.

④ 불필요한 I/O 포트 및 네트워크 인터페이스는 비활성화한다.

(3) 전송데이터 보안

기준설명
워크그룹 스위치에 트래픽 흐름을 통제하는 기능을 적용하는 것을 말한다.

[권장사항]

① 워크그룹 스위치에서 트래픽 흐름제어 설정을 지원하는 경우 다음을 참고하여 설정한다.

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

② 원격 네트워크를 통해 워크그룹 스위치에 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

3.3 홈게이트웨이 보안

홈게이트웨이는 전유부분에 설치되어 세대내에서 사용되는 홈네트워크사용기기들을 유무선 네트워크로 연결하고 세대망과 단지망을 상호 접속하는 장치를 말한다. 홈게이트웨이와 세대단말기 기능을 통합한 세대단말기의 경우 **3.4 세대단말기 보안**을 적용한다.

(1) 데이터 기밀성

기준설명
홈게이트웨이에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.

[권장사항]

① 홈게이트웨이 관리자 모드 진입 시에 사용하는 비밀번호 저장 시 SHA2 이상의 안전한

알고리즘으로 암호화하여 저장한다.

(2) 데이터 무결성

기준설명
홈게이트웨이에 저장된 데이터의 위·변조를 방지하고 위·변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.

[권장사항]

① 홈게이트웨이 S/W를 업데이트 할 경우, 파일 설치 전 무결성 검증을 시행한다.

② 제조사가 제공하는 최신 보안패치를 적용한다.

(3) 인증

기준설명
홈게이트웨이에서 안전한 인증수단으로 사용자에 대한 인증을 수행하는 것을 말한다.

[권장사항]

① 홈게이트웨이의 출고 시 설정되어 나오는 기본 계정을 비활성화하거나 쉽게 유추할 수 없도록 변경하여 사용하고 불필요한 계정은 즉시 삭제한다. 홈게이트웨이에서 기본 계정의 삭제, 비활성화 또는 변경 기능을 제공하지 않는 경우는 이를 적용하지 아니할 수 있다.

② 허가된 사용자만이 홈게이트웨이에 접속할 수 있도록 인증 기능을 적용한다. 사용자 확인을 위한 인증수단으로는 아이디/비밀번호, 일회용비밀번호(OTP), 생체인증, 전자서명 등을 적용할 수 있다.

③ 제조사가 설정한 기본 비밀번호(Default Password)는 변경하여 사용한다. 비밀번호는 아래의 내용을 참고하여 설정한다.

가. 비밀번호는 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다.

나. 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 일련번호 등)를 포함하는 비밀번호 사용 제한한다.

다. 비밀번호 변경 주기(예: 6개월 등)를 설정한다.

④ 인증시도가 일정횟수 이상(예: 5회 등) 실패할 경우 접근을 제한(예: 계정 잠금 5분 등)하도록 설정한다.

⑤ 접속(예: 콘솔연결, 터미널 연결 등) 후 일정시간 이상 작업을 하지 않는 경우 자동으로 접속이 차단되도록 설정(10분 이내)을 한다.

(4) 접근통제

기준설명
서비스 목적에 따른 접근권한을 최소한으로 부여하여 홈게이트웨이에 비인가자가 접근하는 것을 통제하고 홈게이트웨이 접근내역을 추적할 수 있도록 로그를 남기는 것을 말한다.

[권장사항]

① 세대망 이외(단지망, 인터넷망 등)에서 홈게이트웨이로 원격 접속은 제한한다.

② 홈게이트웨이에 접속허용 가능한 IP주소를 개별 주소 단위로 등록하고, 등록되지 않은 IP 주소는 접속을 차단한다.

③ 단지 내 네트워크를 통해 원격에서 홈게이트웨이에 접속하는 경우 지정된 단말(IP 또는 MAC주소 등 등록)에서만 접속할 수 있도록 한다.

④ 홈게이트웨이 설정 파일의 접근권한을 최소화한다.

⑤ 공용계정은 사용하지 않도록 한다.

⑥ 불필요한 서비스(echo, discard, chargen, finger, tftp 등) 비활성화한다.

⑦ 불필요한 I/O 포트 및 네트워크 인터페이스는 비활성화한다.

⑧ 관리자 웹페이지가 존재하는 경우 비활성화한다.

(5) 전송데이터 보안

기준설명
용도에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역간 트래픽 흐름을 통제하는 것을 말한다.

[권장사항]

① 홈게이트웨이에서 트래픽 흐름제어 설정 기능을 지원하는 경우 다음을 참고하여 설정한다.

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

나. 허용규칙에 적용되지 않은 경우 모든 트래픽 전달을 차단하는 기본 거부규칙을 설정한다.

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

② 세대망에서 홈게이트웨이로 원격 접속 시 암호통신 프로토콜을 적용한다.

가. 홈게이트웨이설정을 위한 원격터미널 접속 시 SSH V2 이상을 적용하여 연결한다.

나. 관리자 웹페이지는 이용하는 경우에만 활성화하고 HTTPS 통신을 사용한다.

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

③ SNMP 서비스를 사용하지 않는 경우 비활성화한다. 필요시 SNMP 서비스를 사용하는 경우에는 SNMP v3을 사용한다.

3.4 세대단말기 보안

세대단말기(월패드)는 세대 및 공용부의 다양한 설비의 기능 및 성능을 제어하고 확인할 수 있는 기기로 사용자인터페이스를 제공하는 장치를 말한다. 홈게이트웨이와 세대단말기 기능을 통합한 세대단말기의 경우 세대단말기 보안을 적용된다. **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따른 정보보호 인증을 받은 세대단말기는 아래 보안요구사항을 준수한 것으로 인정하므로 인증을 받은 세대단말기는 아래 보안요구사항을 충족한 것으로 인정한다.** 세대단말기 보안요구사항은 아래와 같다.

(1) 데이터 기밀성

기준설명

세대단말기에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.

[권장사항]

① 중요정보를 전송하거나 저장 시 안전한 암호 알고리즘을 사용하여 암호화한다.

<국내・외 권고 암호 알고리즘 예시(112 비트 이상)>

구분		암호 알고리즘
대칭키 암호 알고리즘		・SEED, HIGHT ・ARIA-128/192/256 ・LEA-128/192/256 ・AES-128/192/256 ・3TDEA
해시 함수	단순해시/전자서명용	・SHA-224/256/384/512 ・SHA-512/224, SHA-512/256
	메시지인증/키유도/ 난수생성용	・SHA3-224/256/384/512 ・LSH-224/256/384/512 ・LSH-512/224, SHA-512/256
공개키 암호 알고리즘	키 공유용	・[이산대수 문제] DH, MQV ・[타원곡선] ECMQV, ECDH
	암·복호화용	・[인수분해 문제] RSAES, RSA
	전자서명용	・[인수분해 문제] RSA-PSS, RSA ・[이산대수 문제] KCDSA, DSA ・[타원곡선] ECDSA, EC-KCDSA, ECDSA

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

② 개인정보 수집 및 처리 시 개인정보 관련 법적 요구사항을 준수한다.

③ 사용자 필요, 폐기, 교체하는 경우 저장되어 중요정보를 완전하게 삭제하는 기능을 포함한다.

④ 기기별로 고유한 암호키를 생성한다.

(2) 데이터 무결성

기준설명

세대단말기에 저장되는 데이터의 위・변조를 방지하고 위・변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.

[권장사항]

① 세대단말기는 제조사가 제공하는 최신 보안패치를 적용한다.

② 기기 모델명 및 제품정보(소프트웨어·펌웨어)의 식별정보를 확인하기 위한 수단을 제공한다.

③ 안전한 소프트웨어 업데이트 수행을 위해, 사전에 업데이트 파일의 무결성을 검증한다.

④ 업데이트 발생 시 사용자에게 적절한 알림 수단을 통해 정보를 제공한다.

(3) 인증

기준설명

세대단말기에 접속하기 위해 사용되는 인증정보는 정당한 사용자인지 검증할 수 있도록 안전한 인증방식을 지원하는 것을 말한다.

[권장사항]

① 초기 인증정보는 변경하거나 생성되어야 하고, 인증정보의 안전성을 검증한다. 기본 인증정보가 존재하지 않는 경우 초기 인증정보(비밀번호 등)를 생성하도록 하며, 생성된 인증정보를 이용하여 로그인 이후 접속이 가능하도록 한다.

가. 비밀번호는 영문자, 숫자, 특수문자 중 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정한다. 아이디 없이 비밀번호만 입력하고 입력 문자가 숫자로 제한되는 경우 비밀번호는 충분한 길이(예: 관리자 기능은 8자리 이상)의 숫자가 입력될 수 있도록 한다.

나. 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 제품 일련번호 등)를 포함하는 비밀번호 사용 제한한다.

다. 비밀번호 변경 주기(예: 6개월 등)를 설정한다.

라. 관리자 비밀번호는 다른 기기와 동일한 비밀번호를 사용하지 않는다.

② 관리기능 또는 중요정보에 접근 시 사용자 인증을 수행하고, 서비스 이용에 필요한 최소한의 권한만을 부여한다.

③ 다른 기기와 연결 또는 중요정보 전송 시 기기의 식별정보가 신뢰성이 있음을 확인하는 인증을 선행한다.(시리얼통신으로 세대단말기와 직접 연결되어있는 경우는 제외)

④ 사용자가 연속적으로 인증 실패 시 추가적인 인증을 시도하지 못하도록 제한한다.

⑤ 인증정보가 출력장치에 노출되지 않아야 하고, 인증실패 사유에 대한 피드백 정보가 제공되지 않아야 한다.

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.

(4) 접근통제

기준설명
서비스 목적에 따라 접근권한을 최소한으로 부여하여 세대단말기로 비인가 접근을 통제하고 접근권한을 관리하는 것을 말한다.

※ 긴급상황 등에 대비하여 경비실이나 세대간 통화가 필요한 경우에 한하여, 적절한 보안조치(접근제어, 접근기록관리 등)를 강구하여 활용하여야 한다.

[권장사항]

① 세대단말기 운용에 불필요한 네트워크 포트 및 서비스는 제공되지 않도록 제거하거나 비활성화한다.

② 지원되는 네트워크 인터페이스[6]가 세대단말기 운용이 필요한 것인지를 확인하고, 불필요한 네트워크 인터페이스는 비활성화한다.

③ 접근통제, 인증, 안전한 보안채널이 적용된 신뢰된 환경에서만 원격 접속이 가능하도록 통제한다.

④ 불필요한 외부 인터페이스[7]는 비활성화하고, 필요 시 접근통제 기능을 구현한다.

⑤ 개발자가 펌웨어를 디버깅하기 위해 사용되는 내부 인터페이스[8]를 비활성화한다.

(5) 전송데이터 보안

기준설명
세대단말기와 단지서버와의 데이터 전송 시 유출 또는 탈취되지 않도록 하는 것을 말한다.

[권장사항]

① 세대단말기에 허가되지 않은 다른 네트워크 트래픽이 유입되지 않도록 차단한다.

② 전송되는 정보가 유출 또는 탈취되지 않도록 안전한 암호화 프로토콜을 이용하여 전송한다.

---

6) 네트워크인터페이스 예시 : BLE, WiFi, NFC, Zigbee, LTE-M, Ethernet 등

7) 외부인터페이스 예시 : USB, SD Card Slot, RS232 등

8) 내부인터페이스 예시 : UART, JTAG 등

<table>
<tr><th>통신 프로토콜</th><th>데이터 보호 방안</th></tr>
<tr><td>ZigBee</td><td>· ZigBee에서 CCM 운영모드는 AES-CBC-MAC-128(메시지 인증) 또는 AES-CCM-128(암호화 및 메시지 인증)를 지원한다.</td></tr>
<tr><td>Bluetooth</td><td>· BLE 4.0/4.1을 포함하여 낮은 버전의 기기는 보안모드 1의 보안레벨 3(암호화된 인증 페어링)을 적용하고, BLE 4.2 기기 및 서비스는 보안모드 1의 보안레벨 4 (암호화된 저전력 보안연결 인증)를 적용
<table>
<tr><th>보안레벨</th><th>저전력 보안모드 1</th><th>저전력 보안모드 2</th></tr>
<tr><td>1</td><td>보안 없음(인증·암호화 없음)</td><td>데이터 서명을 통한 인증되지 않은 페어링</td></tr>
<tr><td>2</td><td>암호화되지 않은 페어링</td><td>데이터 서명을 통한 인증된 페어링</td></tr>
<tr><td>3</td><td>암호화된 인증 페어링</td><td>-</td></tr>
<tr><td>4</td><td>128비트 암호화키로 암호화된 저전력 보안연결 인증</td><td>-</td></tr>
</table></td></tr>
<tr><td>6LoWPAN</td><td>· IPv6를 사용하는 통신으로 기밀성을 위해서 MTU에 대한 암호화 기법으로 AES-128 비트를 사용하고, IPSec을 이용하여 기밀성 및 무결성을 보장한다.</td></tr>
<tr><td>Z-Wave</td><td>· Z-Wave 인증을 받고 S2(시큐리티 2) 프레임워크를 적용한다.</td></tr>
<tr><td>LoRa</td><td>· FRM Payload에 대한 기밀성을 위해서 AES-128 비트를 사용하며, 무결성을 보장하기 위해서 RFC 4493에서 제시된 AES-CMAC를 사용한다.</td></tr>
<tr><td>CoAP</td><td>· 유니캐스트에 대한 보안만 제공하고 있으며, DTLS에 기반하고 있어 대칭키 암호(AES), 공개키 암호(ECC), 해시함수(SHA 등)을 사용한다.</td></tr>
<tr><td>MQTT</td><td>· MQTT 보안을 위해서는 SSL(TLS/DTLS)를 사용해야 하며, MQTT 표준에서는 ISO29192 표준에 정의된 경량암호 알고리즘을 사용할 것을 권장한다.</td></tr>
<tr><td>DDS</td><td>· 기밀성 및 사용자 위장을 방지하기 위해서 PKI-RSA/DSA-DH, AES-CTR-HMAC-RSA /DSA-DH 알고리즘 사용을 권장한다.</td></tr>
<tr><td>WiFi</td><td>· WPA2 방식을 적용하고, 비밀키는 특수문자를 포함한 임의의 문자를 사용하여 최대한의 자릿수를 사용한다.</td></tr>
<tr><td>TLS/DTLS</td><td>· SSL을 기반으로 구현된 보안프로토콜로 대칭키 암호(AES, Blowfish 등), 해시 알고리즘(SHA, HMAC 등) 및 공개키 암호 알고리즘(RSA, ECC)을 제공한다. TLS 1.2의 경우 TCP 통신에서의 보안프로토콜로 주로 이용되며, DTLS는 UDP 통신상에서 보안프로토콜로 사용된다.</td></tr>
</table>

※출처 : 정보통신망연결기기등 정보보호인증기준 상세해설서(KISA, 2022)

3.5 단지서버 보안

단지서버는 홈네트워크 설비를 총괄적으로 관리하며, 이로부터 발생하는 각종 데이터의 저장 · 관리하며 입주자 등에게 서비스를 제공하는 장비를 말한다. 단지서버는 운영체제 및 홈네트워크 설비를 관리하기 위하거나 입주자 등에게 서비스하기 위한 응용프로그램을 설치하여 이용하게 된다.

(1) 데이터 기밀성

기준설명
단지서버에 저장된 데이터를 비인가자가 읽을 수 없도록 안전한 알고리즘을 사용하여 암호화하는 것을 말한다.

[권장사항]

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

기준설명
단지서버에 저장된 데이터의 위・변조를 방지하고 위・변조 발생 시 이를 알 수 있도록 관리하는 것을 말한다.

[권장사항]

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

② 응용프로그램이 TLS 프로토콜 이용 시 SHA2 이상의 안전한 무결성 알고리즘(SHA-256, SHA-512 등)이 포함된 사용옵션 설정한다.

(3) 인증

기준설명
단지서버에서 안전한 인증수단을 적용하여 사용자를 인증하는 것을 말한다.

[권장사항]

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. 기본 계정(Default) 삭제/비활성화하거나 하거나, 쉽게 유추할 수 없도록 변경하여 사용한다. 다만, 운영체제 및 관련 소프트웨어에서 기본 계정의 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 영문자, 숫자, 특수문자 중 2조합 10자리 이상 또는 3조합 8자리 이상으로 설정하고, 비밀번호 내에 유추하기 쉬운 정보(ID 포함, 4자 이상 동일/연속 문·숫자, 제품명, 제품 일련번호 등)가 포함되지 않도록 한다.

다. 비밀번호 변경 주기(예: 6개월 등) 설정 및 이전 비밀번호 재사용 제한 횟수 설정한다.

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

기준설명
서비스 목적에 따른 접근권한을 최소한으로 부여하여 단지서버에 비인가 접근을 통제하고 로그를 남기는 것을 말한다.

[권장사항]

① 유닉스/리눅스 OS 접근통제

가. root 계정으로의 원격 접속, 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) 한다.

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. DBA 및 시스템 테이블 접근권한 최소화한다.

마. 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 VPN 등 안전한 접속 수단을 적용한다.

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 비활성화한다.

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) 최소화한다.

⑤ 단지서버 관리 등을 목적으로 홈네트워크망 외부에서 단지서버로 접속하는 것은 원칙적으로 차단한다. 다만, 불가피한 사유로 외부 접속이 필요한 경우에는 VPN 등 안전한 접속수단을 적용하고 아이디/비밀번호 외에 일회용비밀번호(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, Remote Registry 등

⑦ 인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위해 단지서버에서의 불필요한 인터넷 접속 및 서비스(P2P, 웹하드, 메신저 등)를 제한한다.

⑧ 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.

(5) 전송데이터 보안

기준설명
단지서버에서 데이터 전송 시 유출 또는 탈취되지 않도록 구현하는 것을 말한다.

[권장사항]

① 관리를 위해 네트워크에서 단지서버로 접속하는 경우 암호통신 프로토콜을 적용한다.

가. 서버설정을 위한 원격터미널 접속 시 SSH V2 이상을 적용하여 연결한다.

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

다. 원격 접속 시 SSL을 지원하는 경우 활성화한다.

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

③ 단지서버의 응용프로그램에서 대외 웹서비스를 제공하기 위해 인터넷 등 외부 네트워크에 공개되는 웹서버를 운영하는 경우 내부 네트워크와 분리된 DMZ에 설치한다.

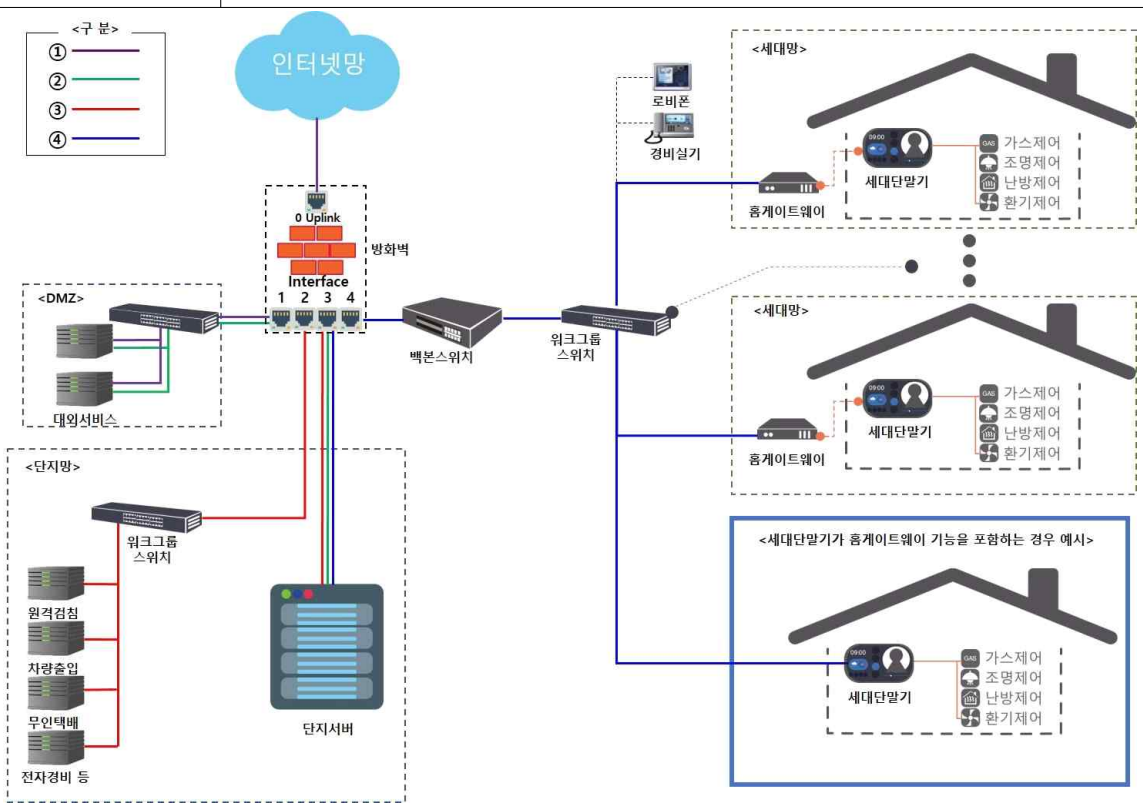
<참고> 단지서버에서 개인정보를 처리하는 경우

단지서버에서 입주민의 이름, 이메일, 휴대폰번호 등 개인정보를 수집, 저장 등 처리하는 경우에는 「개인정보 보호법」 제29조(안전조치 의무)에 따른 안전성 확보에 필요한 기술적·관리적 및 물리적 조치의 의무가 있다. 이에 따른 세부 조치사항은 개인정보보호법 고시(「개인정보의 안전성 확보조치 기준」, 「개인정보의 기술적·관리적 보호조치 기준」)를 참고하여 조치할 필요가 있다.

부록

홈네트워크 필수설비인 방화벽을 활용하여 홈네트워크망을 구성할 수 있는 방법을 소개한다. 아래 참고사항은 홈네트워크 설비 구축 · 운영 시 방화벽 기능을 활용하여 보안성을 강화할 수 있는 예시로 홈네트워크 설비를 구축 · 운영하는 환경에 따라 다양하게 구성 · 운영할 수 있다.

참고사항



※ 이해를 돕기 위한 개념도로 실제 홈네트워크 환경과 상이 할 수 있음

구분	출발지 (목적지)	목적지 (출발지)	방화벽 정책
①	인터넷망 (Uplink 0)	DMZ (Interface 1)	인터넷망과 DMZ 사이의 통신은 최소한(허용된 IP, Port 등)만 허용
②	DMZ (Interface 1)	단지서버 (Interface 3)	단지서버와 DMZ 사이의 통신은 최소한(허용된 IP, Port 등)만 허용
③	원격검침시스템 등 (Interface 2)	단지서버 (Interface 3)	단지서버와 원격검침시스템 등 일부 시스템 사이의 통신은 최소한(허용된 IP, Port 등)만 허용
④	단지서버 (Interface 3)	세대망 (Interface 4)	단지서버와 각 세대별 홈게이트웨이 사이의 통신은 최소한(허용된 IP, Port 등)만 허용

※ 방화벽 활용을 위한 예시로 운영 환경에 적합한 홈네트워크망 구성 및 정책 수립 필요

참고사항

☐ **공인시험기관**(보안기능 시험제도)

o 보안기능 시험제도 : 보안적합성 검증절차 간소화를 위해 정보보호시스템·네트워크 장비 등 IT 제품에 대해 공인시험기관이 '국가용 보안요구사항' 만족 여부를 시험하여 안전성을 확인해 주는 제도

< 공인시험기관 현황 >

시험기관	홈페이지	연락처
한국정보통신기술협회(TTA)	www.tta.or.kr	(디지털정보보호단) 010-5111-1404 (방송통신인프라단) 010-5110-1564
한국기계전기전자시험연구원(KTC)	www.ktc.re.kr	031-428-3765
한국정보보안기술원(KOIST)	www.koist.kr	02-586-1230
한국아이티평가원(KSEL)	www.ksel.co.kr	02-400-8221
한국시스템보증(KoSyAs)	www.kosyas.com	02-2088-5099
한국전자통신연구원(ETRI) ICT시험연구센터	www.etri.re.kr	042-860-5336

※ 「보안기능 시험」 외에 VLAN 등 특정 기능항목에 대한 검증이 필요한 경우, 시험기관에 시험의뢰를 문의하시기 바랍니다.(다만, 시험기관마다 상황이 다를 수 있으므로 개별적인 협의 필요)

☐ **보안점검단** 「초고속정보통신건물인증 업무처리지침('23.6월 개정)」

주요 개정사항
홈네트워크건물인증을 받고자하는 신청인은 「지능형 홈네트워크 설비 설치 및 기술기준」 제14조의2(홈네트워크 보안)에 해당하는 사항에 대하여 한국정보통신진흥협회 보안점검단이 발급한 보안점검성적서, 보안점검결과서를 제출하여야 한다. 다만, AAA등급(홈IoT)을 신청하는 경우에는 홈IoT 기기를 제어하는 앱과 심사항목(2) 중 설치된 무선기기를 포함한다. (「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의6에 따라 정보보호인증을 받은 기기 및 앱의 경우 보안요구사항을 충족한 것으로 인정한다.)

※ 홈네트워크건물인증을 받고자 하는 경우 고시 제14조의2(홈네트워크 보안)에 해당하는 사항에 대하여 한국정보통신진흥협회(KAIT) 보안점검단을 통하여 보안점검결과서를 발급받으실 수 있습니다.

☐ **안전성 검증필 제품현황**

※ 안전성 검증필 제품목록(VPN, L3 스위치 등)은 **"국가사이버안보센터(www.ncsc.go.kr) → 보안적합성검증 → 안전성 검증필 제품목록"** 에서 확인할 수 있습니다.

홈네트워크 보안 가이드

2024년 6월 발행

한국인터넷진흥원