지능형 홈네트워크 세대간 망분리 방안

글 김유환 / 전기팀 차장 **전화** 02-3433-7427 **E-mail** hwani04@ssyenc.com

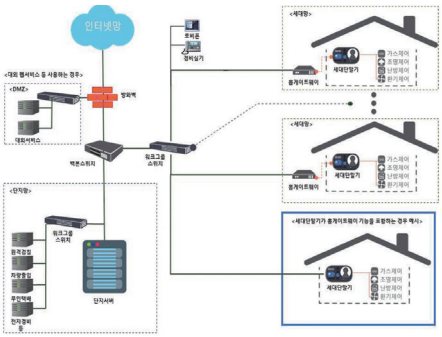
01 지능형 홈네트워크

지능형 홈네트워크는 세대 내 조명, 난방, 가스 제어는 물론 방문자 확인 및 세대 방범이 가능한 첨단 홈네트워크 시스템을 의미한다.

홈네트워크는 세대 월패드를 통하여 경비실 및 관리실 통화, 세대간 화상통화 등이 가능하며 공동현관 및 현관 방문자 확인 및 문 열림 기능을 수행한다. 또한 조명, 난방, 가스, 환기, 에어컨 제어가 가능하며 일괄소등을 통하여 전체 조명을 켜고 끌 수 있다.

그뿐만 아니라 원격검침 및 에너지 모니터링을 통한 에너지 사용량을 확인 할 수 있고, 택배도착알림, 방문자 차량조회, 어린이놀이터의 CCTV 확인, 전기차 충전상태, 날씨 및 미세먼지 정보 제공 등 다양한 기능을 가지고 있다.

[그림 1] 홈네트워크 구성도 예시



이런 다양한 기능을 구현하기 위해서 홈네트워크는 인터넷 망을 통하여 홈네트워크 서버 및 주변 기기들로 구성되어 있다.

특히 방재실에 있는 서버와 세대 간에는 워크그룹 스위치를 통하여 연결되는데 보통 1개의 워크그룹 스위치에는 24세대가 연결되어 있다.

그리고 방화벽 등 보안시스템을 적용하여 인터넷 망의 외부로 부터의 침입 등을 보호하고 있다.

그러나 최근 세대내부에서 다른 세대 월패드 및 워크그룹스위치 등을 해킹하여 다른 세대의 실내용 카메라를 활용하여 집안 내부를 촬영하여 사진과 영상을 유포 하는 등 사생활 피해 사례가 발생하고, 해킹을 통하여 현관문 등 제어가 가능하여 문제가 되고 있다.

[그림 2] 증가하는 홈네트워크 범죄 유형

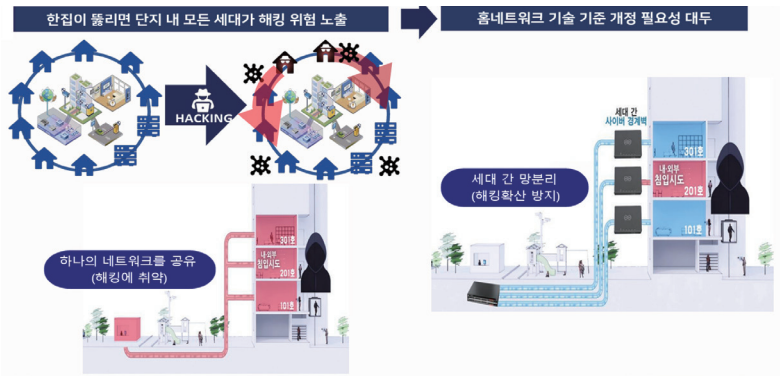
[그림 3] 홈네트워크 피해 언론보도

근본적인 원인은 인터넷망과 단지는 방화벽을 통하여 보안이 이루어 지고 있지만, 세대와 세대간에는 보안이 취약하기 때문이다.

한 집이 뚫리면 모든 세대가 뚫리는 이런 현상은 단지 내 인터넷이 세대 간 구분없이 하나의 단일망으로 연결되 발생하는 치명적인 약점이다.

따라서 홈네트워크 기술기준 개정의 필요성이 대두되었고 네트워크 보안효과를 위하여 세대 간 망분리하는 방안을 2021년 12월 31일 고시하여, 2022년 7월 1일부터 홈네트워크를 설치하기 위해서는 망분리가 되어있는 홈네트워크 시스템을 구축하여야 한다.

[그림 4] 홈네트워크 기술 기준 개정 필요성



02 지능형 홈네트워크 관련 법규

2.1 주택건설기준 등에 관한 규정

제3조의2 (지능형 홈네트워크 설비)

주택에 지능형 홈네트워크 설비(주택의 성능과 주거의 질 향상을 위하여 세대 또는 주택단지 내 지능형 정보통신 및 가전기기 등의 상호 연계를 통하여 통합된 주거서비스를 제공하는 설비를 말한다)를 설치하는 경우에는 국토교통부장관, 산업통상자원부장관 및 과학기술정보통신부장관이 협의하여 공동으로 고시하는 지능형 홈네트워크 설비 설치 및 기술기준에 부합하여야 한다.

2.2 지능형 홈네트워크 설비 설치 및 기술기준 제14조의 2(홈네트워크 보안)제1항과 제2항 개정

제14조의2 (홈네트워크 보안)

① 단지서버와 세대별 홈게이트웨이 사이의 망은 전송되는 데이터의 노출, 탈취 등을 방지하기 위하여 물리적 방법으로 분리 하거나, 소프트웨어를 이용한 가상사설 통신망, 가상근거리통신망, 암호화기술 등을 활용하여 논리적 방법으로 분리하여 구성하여야 한다.

② 홈네트워크 장비는 보안성 확보를 위하여 별표1에 따른 보안 요구사항을 충족하여 야 한다. 다만, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제48조 6에 따라 정보보호인증을 받은 세대단말기는 별표 1 보안요구 사항을 충족한 것으로 인정한다.

③ 홈네트워크사용기기 및 세대단말기는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제48조의6에 따라 정보보호 인증을 받은 기기로 설치할 수 있다.

[별표 1] 홈네트워크장비에 대한 보안요구사항

구분	보안요구사항
1. 데이터 기밀성	이용자 식별정보, 인증정보, 개인 정보 등에 대해 암호 알고리즘, 암호키 생성·관리 등 암호화 기술과 민감한 데이터의 접근제어 관리기술 적용으로 기밀성을 구현
2. 데이터 무결성	이용자 식별정보, 인증정보, 개인정보 등에 대해 해쉬함수, 전자서명 등 기술 적용으로 위·변조 여부 확인 및 방지 조치
3. 인증	사용자 확인을 위하여 전자서명, 아이디/비밀번호, 일회용비밀번호 (OTP)등을 통해 신원 확인 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

법규 개정의 사유는 홈네트워크 설치, 이용 증가 및 IoT기술 발전에 따라 홈네트워크를 통하여 발생 할 수 있는 보안사고의 예방과 망의 안정적인 운영을 위한 조치이며, 정부는 해킹위협이 증가하고 있는 월패드 등 지능형 홈네트워크의 보안성 강화를 위해 한국 정보통신 진흥협회를 통한 정책연구 결과를 토대로 보안전문가, 건설사, 정보통신공사업자 등 관련 업계의 의견 수렴을 통해 2021년 12월 31일 개정안을 고시(국토교통부, 산업통상자원부, 과학 기술정보통신부) 하였고, 2022년 7월 1일부터 시행하여 고시 시행 이후 주택 건설 사업을 승인받아 시행하는 건설사 등은 홈네트워크 설비를 설치할 때, 개정된 고시 내용을 준수해야 한다.

개정된 주요 내용은 단지서버와 세대별 홈게이트웨이 사이의 망은 물리적 또는 논리적 방법으로 분리하여 구성하여야 한다.

또한 홈네트워크 장비는 보안성 확보를 위하여 데이터 기밀성 등 보안 요구사항을 충족하여야 한다.

2.3 지능형 홈네트워크 설비 설치 및 기술기준에서 정의하는 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, 홈네트워크 사용 기기로 구분

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

(3) 단지망 : 집중구내통신실에서 세대까지를 연결 하는 망

(4) 세대망 : 전유부분(각 세대내)을 연결하는 망

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

(6) 홈게이트웨이 : 전유부분에 설치되어 세대내에서 사용되는 홈네트워크사용기기들을 유무선 네트 워크로 연결하고 세대망과 단지망을 상호 접속 하는 장치(단, 세대단말기가 홈게이트 웨이 기능을 포함하는 경우는 세대단말기로 대체 가능)

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

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

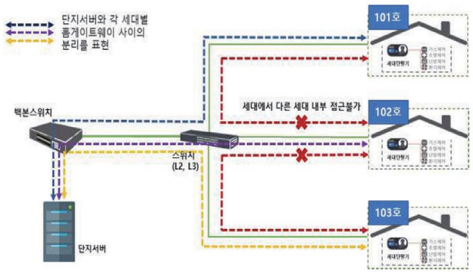
(9) 단지서버 : 홈네트워크 설비를 총괄적으로 관리하며, 이로부터 발생하는 각종 데이터의 저장, 관리, 서비스를 제공하는 장비

(10) 홈네트워크사용기기 : 홈네트워크 망에 접속하여 사용하는 원격제어기기, 원격검침시스템, 감지기, 전자출입시스템, 차량출입시스템, 무인 택배시스템, 영상정보처리기기, 전자경비 시스템 등의 장비

03 세대 간 망분리 방법

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.

[그림 5] 망분리를 위한 세대별 홈넷 구성 요건



3.1 물리적 망분리

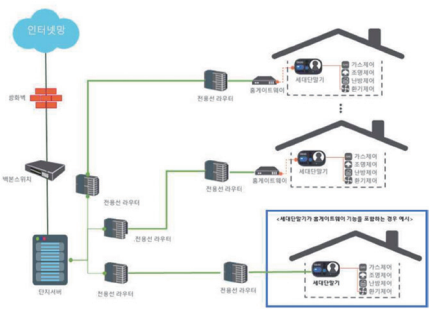
물리적 분리는 단지서버와 각 세대망 사이의 네트워크 구성을 물리적인 단일 네트워크로 연결하여 구성하는 방법을 의미한다. 단지서버와 각 세대망을 연결하는 네트워크를 세대마다 독립적으로 구축하여 단지서버에 연결되어야 하는 세대수 만큼 개별 구축한다.

3.1.1 전용선 라우터를 이용한 분리

(1) 단지서버로부터 각 세대망까지 성형배선❶ 등 의 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.

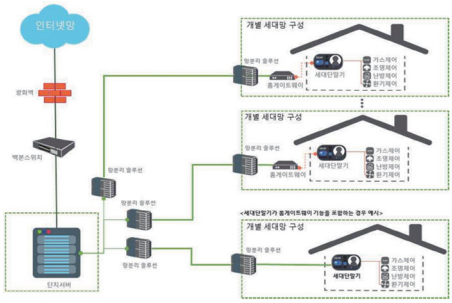
[그림 6] 전용선 라우터를 이용한 물리적 분리



❶ 성형배선: 세대단자함에서 각각의 직렬단자까지 직접 배선되는 방식(「방송 공동수신설비의 설치 기준에 관한 고시」제2조 14호)

3.1.2 망분리 솔루션을 이용한 분리

[그림 7] 망분리 솔루션을 이용한 분리



(1) 망분리 솔루션❷을 이용하여 단지 서버망과 개별 세대망을 각각 구성하고 개별 세대망과 서버망을 연계시켜 통신이 가능하게 하도록 구성한다.

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

3.2 논리적 망분리

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

3.2.1 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(Layer2 VPN), L3 가상네트워크(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.

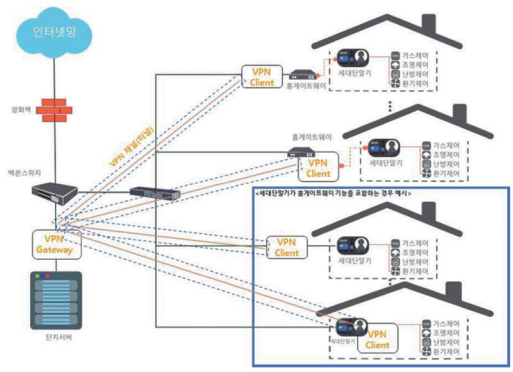
(3) 고려사항

① 가상시설통신망(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.

② VPN 게이트웨이는 단지서버와 홈게이트웨이 사이 안전한 통신채널을 형성

③ VPN 클라이언트는 VPN 게이트웨이에 안전 하게 접속하게 해줌

[그림 8] VPN을 이용한 기술 예시



❷ 망분리 솔루션은 국가정보원의 "정보보호 시스템 및 네트워크 장비 국가용 보안요구사항"의 "구간보안 제품군"중 "망간 자료전송제품 보안요구사항"을 참조

④ VPN 게이트웨이, VPN 클아이언트, VPN 관리서버, VPN 관리도구 등의 다양한 요소로 구성 될 수 있음

⑤ 전송데이터 암호방식은 안전도 112비트 이상으로 설정한다.

⑥ 전송데이터 위·변조를 방지하도록 무결성 방식은 안전도 112비트 이상으로 설정한다.

3.2.2 VLAN을 이용한 기술

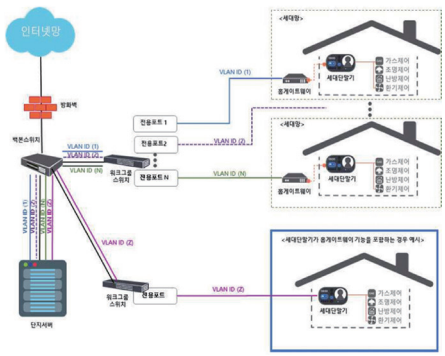
(1) 가상근거리통신망(VLAN)은 네트워크 스위치를 이용하여 각 세대별로 개별 네트워크를 별도로 할당함으로써 세대 네트워크망을 논리적으로 분리하는 기술로 각 세대망은 단지서버 외에 다른 세대의 내부로 접근 할 수 없도록 한다.

※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. 구성방식에는 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(IP주소, Port 등)를 설정하여 관리한다.

[그림 9] VLAN을 이용한 기술



(4) 고려사항

① 네트워크 스위치 장비 교체 등의 이슈 발생 시 VLAN 구성을 유지하고 지속적으로 관리될 수 있도록 한다.

② 가상근거리통신망(VLAN)을 이용한 방법은 구간 내 암호화 기능을 포함하고 있지 않으므로 네트워크 스니핑으로 인한 피해를 예방 하기 위해 통신 암호화 등의 추가 보안을 권장 한다.

04 세대 간 망분리 비교

구 분	기술구분		세부기술
물리적 방법	전용선		케이블 분리 구축
	망분리 솔루션		세대망과 서버망 연계
논리적 방법	VPN	하드웨어	IP Tunnel & VRF IPSec VPN
		소프트웨어	SSL VPN
	VLAN		네트워크 스위치할당

물리적 망분리를 적용하려면 기존에 단지서버에서 워크그룹스위치로 광케이블을 공용으로 이용했으나 각 세대마다 각각 설치하여야 하기 때문에 논리적 방법에 대비하여 비용 상승이 발생한다.

또한 논리적 망분리는 물리적 망분리보다는 금액이 저렴하지만 세대정보 노출 취약 구간(공용부 워크그룹 스위치 및 다른 시스템 서버 등을 통한 해킹)이 존재하기 때문에 암호화 기능 추가 적용도 검토가 필요하다.

※ 참고문헌

01. 홈네트워크 보안 가이드