



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0010553
(43) 공개일자 2009년01월30일

(51) Int. Cl.⁹

H04L 12/22 (2006.01) G06F 15/00 (2006.01)

(21) 출원번호 10-2007-0073751

(22) 출원일자 2007년07월23일

심사청구일자 2007년07월23일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

조충호

충남 천안시 신부동 대림한들아파트 205동 1105호

김세진

전북 정읍시 연지동 339-3 은호빌라 401호

(뒷면에 계속)

(74) 대리인

현중철

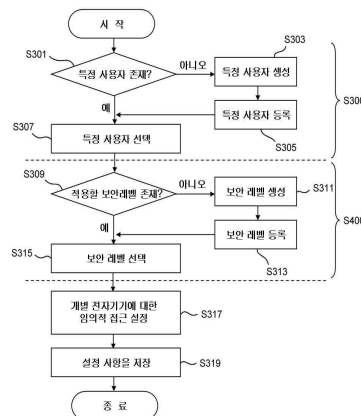
전체 청구항 수 : 총 11 항

(54) 홈네트워크 시스템의 보안정책 설정 방법

(57) 요약

본 발명은 홈네트워크 시스템의 보안정책 설정 방법에 관한 것이다. 본 발명은, 다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템에서, 보안정책을 설정하는 방법에 있어서, 특정 사용자가 선택되는 단계; 상기 특정 사용자에 대해, 상기 다수의 전자 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨들 중 특정 보안 레벨을 설정하는 강제적 접근 설정 단계; 및 상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를 포함하는 홈네트워크 시스템의 보안정책 설정 방법을 제공한다.

대표도 - 도3



(72) 발명자

임치현

서울 중구 광희동2가 218-4

정용화

대전 유성구 지족동 877 열매마을아파트 505동 40
2호

이성주

서울 마포구 성산2동 한맥아이홈 47-14 302호

양성현

서울 노원구 중계본동 진로대림아파트 101동 605호

특허청구의 범위

청구항 1

다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템에서, 보안정책을 설정하는 방법에 있어서,

특정 사용자가 선택되는 단계;

상기 특정 사용자에 대해, 상기 다수의 전자 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨들 중 특정 보안 레벨을 설정하는 강제적 접근 설정 단계; 및

상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 2

제 1 항에 있어서, 상기 사용자 선택 단계는,

상기 특정 사용자에 관한 정보가 존재하는 경우, 상기 특정 사용자가 선택되는 단계; 및

상기 특정 사용자에 관한 정보가 존재하지 않는 경우, 상기 특정 사용자에 관한 정보가 생성되고 상기 특정 사용자가 선택되는 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 3

제 1 항에 있어서, 상기 강제적 접근 설정 단계는,

상기 특정 보안 레벨이 존재하는 경우, 상기 특정 사용자에 대해 상기 특정 보안 레벨이 설정되는 단계; 및

상기 특정 보안 레벨이 존재하지 않는 경우, 상기 특정 보안 레벨이 생성된 후 상기 특정 사용자에 대해 상기 생성된 특정 보안 레벨이 설정되는 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 4

제 1 항에 있어서,

상기 강제적 접근 설정 단계 및 상기 임의적 접근 설정 단계에서 설정된 사항을 저장하는 단계를

더 포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 5

다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템과 통신 가능하고, 상기 홈네트워크 시스템의 보안정책을 설정하고 관리하는 보안정책 관리자 단말기에서, 상기 보안정책을 설정하는 방법에 있어서,

사용자별 보안정책에 관한 정보를 요청하는 메시지를 상기 홈게이트웨이로 전송하는 단계;

상기 홈게이트웨이로부터 상기 사용자별 보안정책에 관한 정보를 수신하는 단계; 및

상기 수신된 사용자별 보안정책에 관한 정보를 이용하여 특정 사용자에 대한 보안정책을 설정하는 단계를 포함하고,

상기 보안정책 설정 단계는,

상기 특정 사용자가 선택되는 단계;

상기 특정 사용자에 대해, 상기 다수의 전자 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수

의 보안 레벨들 중 특정 보안 레벨이 설정되는 강제적 접근 설정 단계; 및

상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 6

제 5 항에 있어서, 상기 사용자 선택 단계는,

상기 사용자별 보안정책에 관한 정보에 상기 특정 사용자에 관한 정보가 포함되어 있는 경우, 상기 특정 사용자가 선택되는 단계; 및

상기 사용자별 보안정책에 관한 정보에 상기 특정 사용자에 관한 정보가 포함되어 있지 않은 경우, 상기 특정 사용자에 관한 정보가 생성되고 상기 특정 사용자가 선택되는 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 7

제 5 항에 있어서, 상기 강제적 접근 설정 단계는,

상기 특정 보안 레벨이 존재하는 경우, 상기 특정 사용자에 대해 상기 특정 보안 레벨이 설정되는 단계; 및

상기 특정 보안 레벨이 존재하지 않는 경우, 상기 특정 보안 레벨이 생성된 후 상기 특정 사용자에 대해 상기 생성된 특정 보안 레벨이 설정되는 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 8

제 5 항에 있어서,

상기 보안정책 설정 단계에서 설정된 사항을 상기 사용자별 보안정책에 반영한 후 상기 사용자별 보안정책을 상기 홈네트워크로 전송하는 단계를

더 포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 9

다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈네트워크를 포함하는 홈네트워크 시스템에서, 보안정책을 설정하는 방법에 있어서,

상기 다수의 전자 기기들 각각에 대해 사용자의 접근 허용 여부를 설정하는, 다수의 보안 레벨들이 생성되는 단계;

특정 사용자에 대해, 상기 다수의 보안 레벨들 중 특정 보안 레벨이 설정되는 강제적 접근 설정 단계; 및

상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를

포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 10

제 9 항에 있어서,

상기 강제적 접근 설정 단계 및 임의적 접근 설정 단계에서 설정된 사항을 저장하는 단계를

더 포함하는 홈네트워크 시스템의 보안정책 설정 방법.

청구항 11

제 1 항 내지 제 10 항 중 어느 한 항의 방법을 컴퓨터로 실행시킬 수 있는 컴퓨터 프로그램을 기록한 컴퓨터로

읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 홈네트워크 시스템의 보안정책 설정 방법에 관한 것이다. 보다 상세하게는 홈네트워크 환경에서 다수의 전자 기기들을 제어하는 접근 권한에 대한 보안정책을 설정하는 방법에 있어서, 임의적 접근 제어 방식(Discretionary Access Control; DAC)과 강제적 접근 제어 방식(Mandatory Access Control; MAC)을 혼합하여 적용할 수 있는 홈네트워크 시스템의 보안정책 설정 방법에 관한 것이다.

배경 기술

- <2> 홈네트워크란, 가정내 정보 가전 제품과 같은 전자 기기들을 네트워크로 연결해 시간과 장소에 구애받지 않고 자유롭게 사용할 수 있도록 하는 네트워크 기술을 말한다.
- <3> 홈네트워크 구축 대상은 아날로그 형이 아닌 디지털 기기로서, 인터넷에 연결되어 작동 가능한 냉장고, 세탁기, 디지털TV, 디지털 캠코더, 카메라, 컴퓨터, 에어컨 등이 모두 가능하다.
- <4> 홈네트워크에 적용되는 통신 방식으로는, 유선 통신 및 무선 통신 모두 활용될 수 있다. 최근 집중적으로 연구되고 있는 무선 통신 기술로는, RF(Radio Frequency)를 이용하는 홈(Home) RF, 블루투스(Bluetooth), 무선 LAN, 적외선을 이용하는 IrDA 등이 있다.
- <5> 홈네트워크는 인터넷 프로토콜(Internet Protocol; IP) 기반이 사설망(Private Network)으로 이루어지며, 이를 통해 가정 내에서 사용되는 모든 형태의 가전기기들을 하나의 네트워크로 연결하여 통제한다.
- <6> 홈네트워크에서 홈게이트웨이(또는 홈서버)와 다양한 전자 기기들의 통신을 가능하게 하기 위한 미들웨어로, HAVI(Home AV Interoperability), UPnP(Universal Plug and Play), JINI, HWW(Home Wide Web) 등이 있다. 홈네트워크용 미들웨어는, 홈게이트웨이에 탑재되어 유무선 홈네트워킹 환경에서 다양한 기기를 제어하고 상호 정보교환을 보장하는 일종의 소프트웨어로서, 사용자가 H/W 및 O/S에 무관하게 일관성 있는 프로그램을 만들 수 있도록 API를 제공한다.
- <7> 이와 같은 홈네트워크 환경에서는 강력한 보안정책에 기반하여 전자기기를 사용하는 사용자의 접근이 허용되거나 제한된다. 그러나 일반적으로 사용하는 사용자의 접근권한을 설정하는 보안정책 적용 방식은, 각 사용자별로 접근할 수 있는 전자기기들 및 접근이 제한되는 전자기기들을 별도로 구분하여 설정하고 있기 때문에, 사용자의 수가 많아짐에 따라 적용되는 보안정책이 복잡해지고 관리가 어려운 문제점이 발생한다.
- <8> 또한 홈네트워크 환경을 이용하는 사용자의 접근권한을 설정하는 보안정책 설정 방법 중에서 각각의 전자기기들에 대한 접근 권한을 차별화하여 설정한 레벨 적용 방식이 있다.
- <9> 이러한 각 개별 사용자의 접근 권한을 해당되는 레벨로 설정하는 보안정책 방식은, 사용자가 많은 홈네트워크 환경에서 편리하게 보안정책을 적용할 수 있는 장점이 있으나, 특정 사용자에게 다른 접근 권한을 적용하기 위해서는 기존에 설정된 레벨 이외에 다른 레벨을 생성 및 설정하여 접근 권한을 적용해야 하는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

- <10> 본 발명은 상기와 같은 문제점을 해결하고 최근의 추세와 요청에 따라 제안된 것으로서, 임의적 접근 제어 방식과, 강제적 접근 제어 방식을 혼합하여 적용할 수 있는 홈네트워크 시스템의 보안정책 설정 방법을 제공하는데 그 목적이 있다.
- <11> 본 발명의 다른 목적은, 홈네트워크 환경에서 홈게이트웨이의 내부에 설정된 보안정책이 웹포탈에 접속한 사용자에게 의해 생성, 수정, 삭제 및 관리가 가능하도록 하는 홈네트워크 시스템의 보안정책 설정 방법을 제공하는 것이다.
- <12> 본 발명의 또 다른 목적은, 보안정책을 수립 및 관리하는 관리자가 홈네트워크의 외부에 존재하는 경우에도 홈

네트워크 내부의 전자기기를 제어하는 접근권한을 설정할 수 있도록 하는 홈네트워크 시스템의 보안정책 설정 방법을 제공하는 것이다.

과제 해결수단

- <13> 상기의 목적을 달성하기 위한 본 발명의 일 양상으로서, 본 발명에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템에서, 보안정책을 설정하는 방법에 있어서, 특정 사용자가 선택되는 단계; 상기 특정 사용자에 대해, 상기 다수의 전자 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨들 중 특정 보안 레벨을 설정하는 강제적 접근 설정 단계; 및 상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를 포함하여 이루어진다.
- <14> 상기 사용자 선택 단계는, 상기 특정 사용자에 관한 정보가 존재하는 경우, 상기 특정 사용자가 선택되는 단계; 및 상기 특정 사용자에 관한 정보가 존재하지 않는 경우, 상기 특정 사용자에 관한 정보가 생성되고 상기 특정 사용자가 선택되는 단계를 포함할 수 있다.
- <15> 상기 강제적 접근 설정 단계는, 상기 특정 보안 레벨이 존재하는 경우, 상기 특정 사용자에 대해 상기 특정 보안 레벨이 설정되는 단계; 및 상기 특정 보안 레벨이 존재하지 않는 경우, 상기 특정 보안 레벨이 생성된 후 상기 특정 사용자에 대해 상기 생성된 특정 보안 레벨이 설정되는 단계를 포함할 수 있다.
- <16> 본 발명의 일 양상에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 상기 강제적 접근 설정 단계 및 상기 임의적 접근 설정 단계에서 설정된 사항을 저장하는 단계를 더 포함할 수 있다.
- <17> 상기의 목적을 달성하기 위한 본 발명의 다른 양상으로서, 본 발명에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템과 통신 가능하고, 상기 홈네트워크 시스템의 보안정책을 설정하고 관리하는 보안정책 관리자 단말기에서, 상기 보안정책을 설정하는 방법에 있어서, 사용자별 보안정책에 관한 정보를 요청하는 메시지를 상기 홈게이트웨이로 전송하는 단계; 상기 홈게이트웨이로부터 상기 사용자별 보안정책에 관한 정보를 수신하는 단계; 및 상기 수신된 사용자별 보안정책에 관한 정보를 이용하여 특정 사용자에 대한 보안정책을 설정하는 단계를 포함하고, 상기 보안정책 설정 단계는, 상기 특정 사용자가 선택되는 단계; 상기 특정 사용자에 대해, 상기 다수의 전자 기기들에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨들 중 특정 보안 레벨이 설정되는 강제적 접근 설정 단계; 및 상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를 포함하여 이루어진다.
- <18> 본 발명의 일 양상에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 상기 보안정책 설정 단계에서 설정된 사항을 상기 사용자별 보안정책에 반영한 후 상기 사용자별 보안정책을 상기 홈게이트웨이로 전송하는 단계를 더 포함할 수 있다.
- <19> 상기의 목적을 달성하기 위한 본 발명의 또 다른 양상으로서, 본 발명에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 다수의 전자 기기들과, 상기 전자 기기들의 동작 및 상기 전자 기기들에 대한 사용자의 접근을 제어하는 홈게이트웨이를 포함하는 홈네트워크 시스템에서, 보안정책을 설정하는 방법에 있어서, 상기 다수의 전자 기기들 각각에 대해 사용자의 접근 허용 여부를 설정하는, 다수의 보안 레벨들이 생성되는 단계; 특정 사용자에 대해, 상기 다수의 보안 레벨들 중 특정 보안 레벨이 설정되는 강제적 접근 설정 단계; 및 상기 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 임의적 접근 설정 단계를 포함하여 이루어진다.
- <20> 본 발명에 의해 제공되는 홈네트워크 시스템의 보안정책 설정 방법들은, 컴퓨터로 실행시킬 수 있는 컴퓨터 프로그램으로 작성될 수 있고, 상기 컴퓨터 프로그램은 컴퓨터로 읽을 수 있는 기록매체에 기록되는 것이 가능하다.

효과

- <21> 상기에서 설명한 본 발명에 따른 홈네트워크 시스템의 보안정책 설정 방법에 의하면 다음과 같은 효과가 있다.
- <22> 첫째, 본 발명에 의하면, 임의적 접근 제어 방식과 강제적 접근 제어 방식이 혼용된 보안정책 설정 방법을 이용

함으로써, 보안정책이 효율적으로 관리될 수 있는 효과가 있다.

<23> 둘째, 본 발명에 의하면, 특정 사용자에게 특화된 보안정책이 효율적으로 수립 및 관리될 수 있는 효과가 있다.

<24> 셋째, 본 발명에 의하면, 웹포털에 접속한 보안정책 관리자에 의해 보안정책을 수립할 수 있으므로, 보안정책 관리자가 외부에 존재하는 경우에도 홈네트워크 내부의 전자기기들을 제어하는 접근권한을 설정할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<25> 본 발명의 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련된 다음의 상세한 설명을 통하여 보다 분명해질 것이다. 이하 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예들을 상세히 설명한다. 명세서 전체에 걸쳐서 동일한 참조번호들은 동일한 구성요소들을 나타낸다. 또한, 본 발명과 관련된 공지 기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우, 그 상세한 설명을 생략한다.

<26> 도 1은 본 발명의 일 실시예에 따른 홈네트워크 시스템의 블록 구성도이다. 도 1을 참조하여 본 발명의 일 실시예에 따른 홈네트워크 시스템을 상세히 설명하기로 한다.

<27> 본 발명의 일 실시예에 따른 홈네트워크 시스템은, 외부 제어 기기(110), 내부 제어 기기(140), 다수의 전자 기기들(170), 보안정책 관리자 단말기(200) 및 홈게이트웨이(300)를 포함할 수 있다.

<28> 상기 외부 제어 기기(110)는, 가정의 외부에서 상기 다수의 전자 기기들(170)을 제어할 수 있는 장치들이다. 상기 외부 제어 기기(110)의 예를 들면, 휴대폰(111) 또는 PC(Personal Computer, 112)가 있다. 상기 외부 제어 기기(110)는, 전화망(120)이나 인터넷(130)을 통해 상기 홈게이트웨이(300)와 통신할 수 있다. 상기 외부 제어 기기(110)는, 상기 다수의 전자 기기들(170)을 제어하기 위한 제어 신호를 상기 홈게이트웨이(300)로 전송한다.

<29> 상기 내부 제어 기기(140)는, 가정의 내부에서 상기 다수의 전자 기기들(170)을 제어할 수 있는 장치들이다. 상기 내부 제어 기기(140)의 예를 들면, 리모콘(141) 또는 월패드(Wall Pad, 142) 또는 PC(143)가 있다. 상기 내부 제어 기기(140)는, 상기 다수의 전자 기기들(170)을 제어하기 위한 제어 신호를 상기 홈게이트웨이(300)로 전송한다.

<30> 상기 보안정책 관리자 단말기(200)는, 보안정책 관리자가 로그인하여 상기 홈네트워크의 보안정책을 생성, 수정, 삭제 및 관리할 수 있도록 한다. 상기 보안정책 관리자 단말기(200)의 세부 구성 및 동작은 후술하기로 한다.

<31> 상기 홈게이트웨이(300)는, 가정 내의 전자 기기들 및 통신 장치들 사이에 정보를 공유 및 제어하고, 외부망과 내부망을 분리하며, 내부와 외부망 사이의 서비스를 가능케 하는 네트워크 및 서비스 제공 장치이다. 즉 상기 홈게이트웨이(300)는, 내·외부망 인터페이스, 네트워킹 기능, 보안 기능, 맥내장치들 간의 연동 및 서비스 제공 등을 제공할 수 있다.

<32> 상기 홈게이트웨이(300)는, 제한된 공개 IP(Internet Protocol) 주소를 구비하여 사설 IP 주소를 갖는 홈네트워크에 포함된 상기 다수의 전자 기기들(170)이 외부에서 입력되는 제어명령 신호를 수신하여 대응되는 동작을 수행할 수 있도록, 상기 입력되는 제어명령 신호를 상기 다수의 전자 기기들(170)에 전송한다.

<33> 예를 들어, 휴대폰(111) 또는 PC(112)를 통해 제어명령 신호를 수신한 홈게이트웨이(300)는, 상기 수신된 제어명령 신호로부터 상기 제어명령을 전송한 사용자 및 상기 제어명령의 종류를 검출하여, 보안정책 관리자에 의해 기 설정된 보안정책과 비교한다. 상기 홈게이트웨이(300)는, 상기 설정된 보안정책과 매칭되는 사용자 및 제어명령에 대해서는, 해당 전자 기기로의 접근을 수락하며, 해당 전자 기기로의 접근이 제한된 사용자 또는 명령에 대해서는 접근을 제한할 수 있다.

<34> 한편, 본 발명에서 보안정책 관리자에 의해 설정되는 상기 보안정책은, 임의적 접근 제어(Discretionary Access Control; DAC) 방식과 강제적 접근 제어 방식(Mandatory Access Control; MAC)이 혼합되어 적용될 수 있다. 상기 임의적 접근 제어 방식은, 사용자에게 따라 상기 다수의 전자 기기들(170)에 대한 접근 허용 여부를 상기 다수의 전자 기기들(170) 각각에 대해 개별적으로 설정하는 것이다. 상기 강제적 접근 제어 방식은, 상기 다수의 전자 기기들(170) 각각에 서로 다른 보안 레벨들을 설정하여, 특정 사용자에게 상기 서로 다른 보안 레벨들 중 특정 보안 레벨을 설정하는 것이다. 상기 임의적 접근 제어 방식과 상기 강제적 접근 제어 방식에 의한 보안정책 설정의 구체적인 예는 후술하기로 한다.

<35> 상기 홈게이트웨이(300)는, 상기 다수의 전자 기기들(170)과 연결되어 있다. 상기 다수의 전자 기기들(170)은,

일반 가정에서 구비하고 있는 보일러(171), 거실등(172), 도어락(173), 가스밸브(174) 및 방법장치(175) 등을 포함할 수 있다. 상기 다수의 전자 기기들(170)은, 도 1에는 도시되지 않았으나, 세탁기, 전기오븐, 기타 일반 가정에 구비될 수 있는 모든 전자 기기들을 포함할 수 있다.

- <36> 도 2는 본 발명의 일 실시예에 따른 보안정책 관리자 단말기와 홈게이트웨이의 블록 구성도이다. 도 2를 참조하여 본 발명의 일 실시예에 따른 보안정책 관리자 단말기(200)와 홈게이트웨이(300)를 상세히 설명하기로 한다.
- <37> 상기 보안정책 관리자 단말기(200)와 상기 홈게이트웨이(300)는, 특정 통신 프로토콜에 의해 통신할 수 있다. 예를 들어, 상기 보안정책 관리자 단말기(200)와 상기 홈게이트웨이(300)는, HSPP(Home Security Policy Protocol, 230)에 의해 데이터를 교환할 수 있다. 상기 HSPP(230)는, 본 명세서에서 설명되는 홈네트워크 시스템에서 적용되는, 상기 보안정책 관리자 단말기(200)와 상기 홈게이트웨이(300) 사이의 통신을 위한 통신 프로토콜이다. 상기 HSPP(230)는, 패킷(packet) 통신 방식으로, 소켓(socket) 통신 방식에 의할 수 있다.
- <38> 상기 홈게이트웨이(300)는, 보안정책 에이전트(305), 보안정책 저장부(310), 로그 저장부(315), 전자기기 제어 에이전트(320), 액티브 보안정책 저장부(325), 인증 에이전트(330), GUI(335) 및 보안정책 모듈(345)을 포함할 수 있다.
- <39> 상기 보안정책 에이전트(305)는, 보안정책 관리자에 의해 설정된 보안정책을 생성, 수정, 삭제 및 관리하기 위해 상기 보안정책 관리자 단말기(200)로부터 전송되는 보안정책 요청신호에 대응하여, 상기 보안정책 저장부(310)에 저장된 보안정책을 상기 HSPP(230)를 통해 상기 보안정책 관리자 단말기(200)로 전송할 수 있다.
- <40> 상기 보안정책 저장부(310)는, 상기 홈게이트웨이(300) 내부에 파일로 존재하는 보안정책을 저장한다. 상기 보안정책 저장부(310)는, 상기 홈게이트웨이(300)에서 보안정책을 적용할 경우에 직접 접근할 수 없게 하고, 보안정책의 보존을 위해 복제된 또는 메모리에 로드된 상기 액티브 보안정책 저장부(325)와 별도로 구성되어 안전한 보안정책 관리에 이용하는 것이 바람직하다.
- <41> 상기 전자기기 제어 에이전트(320)는, 상기 보안정책 모듈(345)로부터 수신한 전자기기 제어명령을 상기 홈게이트웨이(300)와 분리된 전자기기 제어 인터페이스 및 디스플레이어(400)로 전송하고, 대응되는 응답 신호를 수신한다.
- <42> 상기 액티브 보안정책 저장부(325)는, 상기 보안정책 저장부(310)에 저장된 상기 보안정책이 복제된 또는 메모리 로드된 보안정책이다. 사용자가 상기 GUI(335)를 통해 상기 다수의 전자 기기들(170)을 제어할 때, 상기 보안정책 모듈(345)은 상기 액티브 보안정책 저장부(325)에 저장된 보안정책을 이용하게 된다.
- <43> 상기 인증 에이전트(330)는, 외부에 위치하는 사용자가 GUI(335)를 통해 상기 다수의 전자 기기들(170)을 제어하기 위해서 사용자 인증을 받도록 하는 것으로서, 보안정책 모듈(345)을 통해 사용자를 인증한다.
- <44> 상기 GUI(335)는 웹포털(Web-Portal) 또는 홈포털(Home-Portal)을 의미하며, 사용자가 상기 다수의 전자 기기들(170)을 편리하게 제어할 수 있도록 그래픽 기반으로 제공된다.
- <45> 상기 보안정책 모듈(345)은, 상기 GUI(335)를 통해 상기 다수의 전자 기기들(170)을 제어하고자 하는 사용자에게 상기 액티브 보안정책 저장부(325)에 저장된 보안정책을 참고하여, 해당 사용자에게 상기 전자 기기(170)에 대한 권한을 부여하며, 상기 전자 기기(170)를 제어하기 위한 제어명령 신호를 상기 전자기기 제어 에이전트(320)로 전송한다.
- <46> 상기 보안정책 관리자 단말기(200)는, GUI(Graphic User Interface, 205), 인증 클라이언트(210), 보안정책 생성 모듈(215), 기존 보안정책 저장부(220) 및 임시 보안정책 저장부(225)를 포함할 수 있다.
- <47> 상기 보안정책 관리자 단말기(200)에 구비된 상기 GUI(205)는, 홈네트워크 상에서 사용자들의 보안정책을 관리하는데 있어서, 보안정책 관리자가 편리하도록 그래픽 기반으로 제공되는 인터페이스를 말한다.
- <48> 상기 인증 클라이언트(210)는, 상기 보안정책 관리자 단말기(200)를 통해 보안정책을 관리하려는 관리자가 상기 홈게이트웨이(300)에서 인증을 받도록 하는 것으로서, 관리자가 입력한 아이디 및 패스워드를 상기 홈게이트웨이(300)의 상기 인증 에이전트(330)로 전송한다. 상기 인증 에이전트(330)는, 관리자가 입력한 아이디 및 패스워드를 인증하며, 이에 대한 응답 신호를 상기 인증 클라이언트(210)로 전송한다.
- <49> 상기 보안정책 생성 모듈(215)은, 상기 홈게이트웨이(300)로부터 전송되어 상기 기존 보안정책 저장부(220)에 저장된 보안정책을 생성, 수정, 삭제 및 관리한다. 상기 보안정책 생성 모듈(215)에서 생성, 수정, 삭제된 보안정책이, 상기 홈게이트웨이(300)로 전송되는 것이다.

- <50> 상기 기존 보안정책 저장부(220)는, 보안정책 관리자가 상기 보안정책 관리자 단말기(200)를 통해서 상기 홈게이트웨이(300)로 보안정책 정보를 요청한 경우, 상기 요청에 대응하여 상기 홈게이트웨이(300)로부터 전송된 보안정책을 보안정책 관리자가 상기 GUI(205)를 통해 볼 수 있도록 파싱(parsing)하여 저장한다. 또한 보안정책 관리자가 상기 GUI(205)를 이용하여 보안정책을 생성, 수정, 삭제 및 관리하는 경우, 상기 기존 보안정책 저장부(220)에 저장된 보안정책이 상기 보안정책 생성 모듈(215)로 로드된다.
- <51> 상기 임시 보안정책 저장부(225)는, 상기 보안정책 생성 모듈(215)에서 생성, 수정, 삭제 및 관리된 보안정책을 저장한다. 상기 임시 보안정책 저장부(225)에 저장된 보안정책은, 상기 HSPP(230)을 통해 상기 홈게이트웨이(300)로 전송된다.
- <52> 한편, 외부에 위치하는 보안정책 관리자가 로그인할 경우, 도 2에 도시된 보안정책 관리자 설치 프로그램(340)을 다운로드받아 새로운 보안정책 관리자 단말기에 설치할 수 있다. 보안정책 관리자는 상기 설치된 보안정책 관리 프로그램을 이용하여 보안정책을 관리할 수 있다.
- <53> 한편, 도 1에 도시된 홈네트워크 시스템은, 도 2에 도시된 전자기기 제어 인터페이스 및 디스플레이어(400)를 포함할 수 있다.
- <54> 상기 전자기기 제어 인터페이스 및 디스플레이어(400)는, 전자기기 제어 에이전트(405), 미들웨어(410)를 포함할 수 있다.
- <55> 상기 전자기기 제어 에이전트(405)는, 상기 홈게이트웨이(300)로부터 전송된 전자기기 제어명령을 받아서 상기 미들웨어(410)로 전송한다.
- <56> 상기 미들웨어(410)는, 상기 전자기기 제어 에이전트(405)로부터 전송된 상기 전자기기 제어명령을 해당 전자기기에 알맞은 형태로 전송할 수 있다.
- <57> 도 3은, 본 발명의 일 실시예에 따른 홈네트워크 시스템의 보안정책 설정 방법의 흐름도이다. 도 3을 참조하여, 본 발명의 일 실시예에 따른 홈네트워크 시스템의 보안정책 설정 방법을 상세히 설명하기로 한다. 본 발명의 일 실시예에 따른 홈네트워크 시스템의 보안정책 설정 방법은, 도 1 및 도 2를 참조하여 설명한 홈네트워크 시스템에서 실행될 수 있다.
- <58> 먼저 보안정책이 적용될 사용자가 선택되는 과정이 수행된다[S300].
- <59> 여기서 상기 특정 사용자에게 관한 정보가 상기 홈게이트웨이(300)의 저장 영역에 존재하는지를 판단할 수 있다[S301]. 상기 특정 사용자에게 관한 정보는, 상기 보안정책 저장부(310)에 저장된 보안정책에 포함되어 있을 수 있다. 상기 보안정책 저장부(310)에 저장된 보안정책은, 파일(file) 또는 데이터베이스(database)의 형태로 존재할 수 있다. 예를 들어, 상기 보안정책은, 가족 구성원들의, 보안정책과 관련된 사용자 정보를 포함할 수 있다. 상기 사용자 정보는, 상기 보안정책 파일 또는 데이터베이스와는 별개의 파일 또는 데이터베이스로 존재할 수도 있다.
- <60> 상기 S301 단계의 판단 결과, 상기 특정 사용자에게 관한 정보가 존재하면, 상기 특정 사용자가 선택된다[S307].
- <61> 상기 S301 단계의 판단 결과, 상기 특정 사용자에게 관한 정보가 존재하지 않으면, 상기 특정 사용자에게 관한 정보가 생성되고[S303], 상기 생성된 특정 사용자에게 관한 정보가 상기 보안정책에 등록된 후[S305], 상기 특정 사용자가 선택된다[S307].
- <62> 그리고 상기 선택된 특정 사용자에게 대해, 강제적 접근 설정 과정이 수행된다[S400]. 상기 강제적 접근 설정 과정이란, 전술한 바와 같이, 상기 특정 사용자에게 대해, 상기 다수의 전자 기기들(170)에 대한 접근 허용 여부가 서로 다르게 설정되어 있는 다수의 보안 레벨들 중 특정 보안 레벨을 설정하는 것을 의미한다. 상기 다수의 보안 레벨들에 관한 정보는, 상기 보안정책 파일 또는 데이터베이스 자체에 포함될 수도 있고, 상기 보안정책 파일 또는 데이터베이스와는 별개의 파일 또는 데이터베이스로 존재할 수도 있다.
- <63> 보안정책 관리자는, 보안성에 따라 상기 다수의 전자 기기들(170)을 다수의 그룹들로 분류할 수 있다. 보안정책 관리자는, 상기 분류된 다수의 그룹들에 대해 상기 각 보안 레벨을 매칭시킬 수 있다.
- <64> 여기서, 보안정책 관리자가 상기 선택된 특정 사용자에게 대해 적용하고자 하는 특정 보안 레벨이, 상기 홈게이트웨이(300)의 저장 영역에 존재하는지를 판단할 수 있다[S309].
- <65> 상기 S309 단계의 판단 결과, 상기 특정 보안 레벨이 존재하면, 상기 특정 보안 레벨이 선택됨으로써 상기 선택

된 특정 사용자에게 대해 상기 특정 보안 레벨이 설정된다[S315]. 한편 상기 S309 단계의 판단 결과, 상기 특정 보안 레벨이 존재하지 않으면, 상기 특정 보안 레벨이 생성되고[S311], 상기 생성된 특정 보안 레벨이 등록된 후[S313], 상기 특정 보안 레벨이 선택된다[S315].

<66> 표 1은 강제적 접근 설정을 위한 보안 레벨의 예를 나타낸다.

표 1

<67>

보안 레벨	전자 기기
1	세탁기, 전기오븐
2	방범장치, 가스밸브, 보일러, 도어락
3	TV
4	거실등

<68> 표 1에서, 각 보안 레벨에 대해 적어도 하나의 전자 기기들이 매칭되어 있다. 예를 들어, 보안 레벨 2는, "방범 장치", "가스밸브", "보일러" 및 "도어락"에 대해 사용자의 접근을 허용하는 보안 레벨이다. 또한 예를 들어, 보안 레벨 3은, "TV"에 대해 사용자의 접근을 허용하는 보안 레벨이다.

<69> 또한 상기 각 보안 레벨은, 하위 레벨들에 대해 매칭된 전자 기기들에 대한 사용자의 접근을 허용하도록 설정될 수 있다. 예를 들어, 표 1에서 보안 레벨 2는, "방범 장치", "가스밸브", "보일러" 및 "도어락" 뿐만 아니라, 보안 레벨 3에 매칭된 "TV"와 보안 레벨 4에 매칭된 "거실등"에 대한 사용자의 접근까지 허용하도록 설정될 수 있다.

<70> 표 2는 표 1의 보안 레벨이 4명의 사용자에게 적용(강제적 접근 설정)된 보안정책의 예를 나타낸다.

표 2

<71>

전자기기	사용자 A	사용자 B	사용자 C	사용자 D
	(보안 레벨 1)	(보안 레벨 2)	(보안 레벨 3)	(보안 레벨 4)
세탁기	○	×	×	×
전기오븐	○	×	×	×
방범장치	○	○	×	×
가스밸브	○	○	×	×
보일러	○	○	×	×
도어락	○	○	×	×
TV	○	○	○	×
거실등	○	○	○	○

<72> 즉 사용자 A, 사용자 B, 사용자 C 및 사용자 D는 각각, 보안레벨 1, 보안레벨 2, 보안레벨 3 및 보안레벨 4가 설정되어 있다. 표 2에서 "○"는 접근 허용(許容)을 나타내고, "×"는 접근 불허(不許)를 나타낸다. 예를 들어, 상기 S400 단계가 사용자 C에 대해 표 2와 같이 완료되면, 사용자 C는 전자기기들 중 "TV"와 "거실등"에 대해서만 접근 가능하다.

<73> 표 3은 표 1의 보안 레벨이 4명의 사용자에게 적용(강제적 접근 설정)된 보안정책의 다른 예를 나타낸다.

표 3

<74>

전자기기	사용자 A	사용자 B	사용자 C	사용자 D
	(보안 레벨 1)	(보안 레벨 2)	(보안 레벨 3)	(보안 레벨 3)
세탁기	○	×	×	×
전기오븐	○	×	×	×
방범장치	○	○	×	×
가스밸브	○	○	×	×
보일러	○	○	×	×
도어락	○	○	×	×

TV	○	○	○	○
거실등	○	○	○	○

- <75> 표 3에서는, 사용자 A에 대해서는 보안 레벨 1이 설정되어 있고, 사용자 B에 대해서는 보안 레벨 2가 설정되어 있으며, 사용자 C와 사용자 D에 대해 보안레벨 3이 동일하게 설정되어 있다.
- <76> 상기 S400 단계에서 적용되는 보안 레벨의 개수가 너무 많으면, 보안정책 관리자의 관리가 힘들어지고, 신규 사용자에게 특정 보안 레벨을 설정할 때 설정하고자 하는 보안 레벨에 대응되는 전자 기기들을 일일이 확인하여야 하는 불편함이 발생한다. 또한 신규 사용자 또는 기존의 사용자에게 보안정책을 설정할 때, 신규 사용자 또는 기존의 사용자에게 대해 정확하게 일치하는 보안 레벨이 없을 수 있다. 이하 설명하는 임의적 접근 설정 과정은, 이와 같은 문제점을 해결할 수 있다.
- <77> 따라서 상기 선택된 특정 사용자에게 대해, 임의적 접근 설정 과정이 수행된다[S317]. 상기 S317 단계는, 상기 S400 단계에서 설정된 특정 보안 레벨이 접근을 허용하거나 제한하는 전자 기기들의 전부 또는 일부에 대해, 상기 특정 사용자의 접근 허용 여부가 재설정되는 단계이다.
- <78> 표 4는, 표 2의 사용자들에 대해 임의적 접근 설정된 보안정책의 예를 나타낸다.

표 4

<79>

전자기기	사용자 A	사용자 B	사용자 C	사용자 D
	(보안 레벨 1)	(보안 레벨 2)	(보안 레벨 3)	(보안 레벨 4)
세탁기	○	×	○	×
전기오븐	○	×	×	×
방범장치	○	○	×	×
가스밸브	○	○	×	×
보일러	○	○	×	×
도어락	○	○	×	○
TV	○	○	×	○
거실등	○	○	○	○

- <80> 예를 들어, 보안정책 관리자는, 사용자 C와 사용자 D의 요청에 의해 또는 자신의 판단에 의해, 사용자 C와 사용자 D의 접근 허용 전자 기기들을 수정해야 할 경우가 발생할 수 있다. 따라서 보안정책 관리자는, 상기 S317 단계에 의해, 상기 S400 단계에서 강제적으로 적용된 보안 레벨을 수정할 수 있다.
- <81> 예를 들어, 표 4에서는, 사용자 C에 대해서, S400 단계에서 접근이 허용되는 것으로 설정되었던 "TV"에 대해서는 접근이 불허되고, 접근이 불허되었던 "세탁기"에 대해서는 접근이 허용되는 것으로 설정되었다. 또한 예를 들어, 사용자 D에 대해서는, S400 단계에서 접근이 불허되었던 "도어락"과 "TV"에 대해서 접근이 허용되는 것으로 설정되었다.
- <82> 표 5는, 표 3의 사용자들에 대해 임의적 접근 설정된 보안정책의 예를 나타낸다.

표 5

<83>

전자기기	사용자 A	사용자 B	사용자 C	사용자 D
	(보안 레벨 1)	(보안 레벨 2)	(보안 레벨 3)	(보안 레벨 3)
세탁기	○	×	×	×
전기오븐	○	×	×	×
방범장치	○	○	×	○
가스밸브	○	○	×	×
보일러	○	○	×	×
도어락	○	○	×	×
TV	○	○	×	○
거실등	○	○	○	○

- <84> 표 5에서는, 사용자 C에 대해 표 3에서[S400 단계] 접근이 허용되었던 "TV"에 대해 접근이 불허되고, 사용자 D에 대해 표 3에서[S400 단계] 접근이 불허되었던 "방범장치"에 대해 접근이 허용되었다. 이와 같이 상기 S400 단계에서 동일한 보안 레벨로 설정되었던 사용자 C와 사용자 D에 대해, 상기 S317 단계에서 임의적 접근 설정 과정이 수행됨으로써 서로 다른 보안정책이 설정될 수 있다.
- <85> 그리고, 상기 특정 사용자에 대해, 상기 강제적 접근 설정 단계[S400] 및 상기 임의적 접근 설정 단계[S317]에서 설정된 사항을 저장한다[S319]. 상기 S319 단계는, 상기 보안정책이 새롭게 생성되거나, 기존에 저장되어 있던 보안정책이 갱신됨으로써 수행될 수 있다.
- <86> 도 4는, 보안정책 관리자 단말기와 홈게이트웨이 간에 송수신되는 데이터와 동작을 설명하기 위한 흐름도이다. 도 3을 참조하여 설명한 홈네트워크 시스템의 보안정책 설정 방법이 홈네트워크에서 수행되기 위해, 상기 보안정책 관리자 단말기(200)와 상기 홈게이트웨이(300) 간에 각종 데이터가 송수신되고, 이에 따라 상기 보안정책 관리자 단말기(200)와 상기 홈게이트웨이(300)는 각각 소정의 동작을 수행하여야 한다.
- <87> 먼저 보안정책 관리자 단말기(200)는, 보안정책 관리자의 인증(로그인)이 완료된 후, 사용자별 보안정책에 관한 정보를 요청하는 메시지를 상기 홈게이트웨이(300)로 전송한다[S401].
- <88> 상기 홈게이트웨이(300)는, 상기 메시지를 수신함에 따라, 상기 사용자별 보안정책에 관한 정보를 상기 보안정책 관리자 단말기(200)로 전송한다[S403].
- <89> 상기 보안정책 관리자 단말기(200)는, 상기 홈게이트웨이(300)로부터 전송된 사용자별 보안정책에 관한 정보를 이용하여, 특정 사용자에 대한 보안정책을 설정한다[S405]. 상기 S405 단계는, 상기 특정 사용자에 대한 보안정책을 생성, 수정, 삭제 및 관리하는 단계이다. 상기 S405 단계는, 도 3을 참조하여 설명한 본 발명의 일 실시예에 따른 홈네트워크 시스템의 보안정책 설정 방법에 의한, 사용자 선택 단계[S300], 강제적 접근 설정 단계[S400], 및 임의적 접근 설정 단계[S317]를 포함할 수 있다.
- <90> 상기 보안정책 관리자 단말기(200)는, 상기 S405 단계에서 새롭게 생성되거나 갱신된 사용자별 보안정책을 상기 홈게이트웨이(300)로 전송한다[S407].
- <91> 상기 홈게이트웨이(300)는, 상기 보안정책 관리자 단말기(200)로부터 전송된 사용자별 보안정책을 적용한다[S409].
- <92> 상기에서 설명한 본 발명에 의한 홈네트워크 시스템의 보안정책 설정 방법은, 컴퓨터에서 실행시키기 위한 프로그램으로 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공될 수 있다.
- <93> 본 발명에 의한 홈네트워크 시스템의 보안정책 설정 방법은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.
- <94> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는, ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.
- <95> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

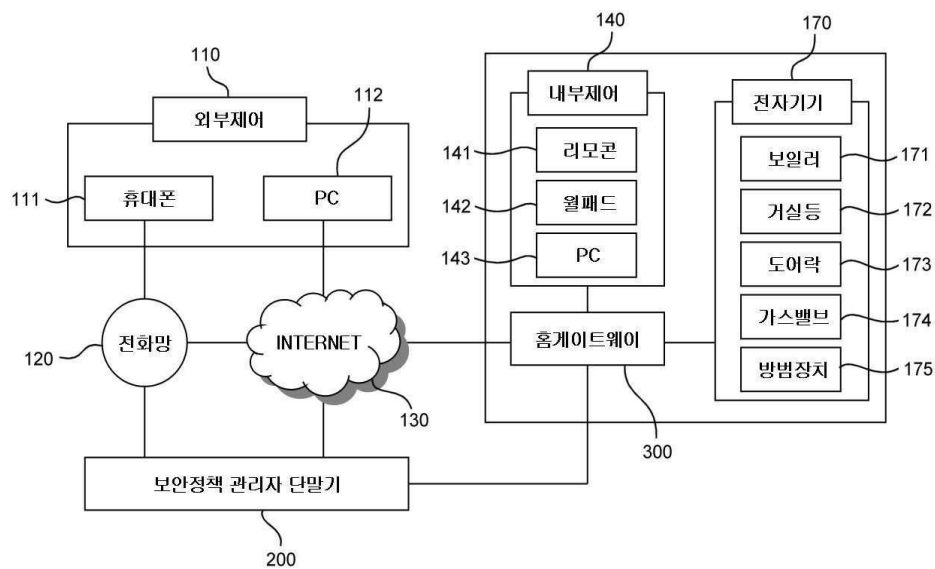
도면의 간단한 설명

- <96> 도 1은 본 발명의 일 실시예에 따른 홈네트워크 시스템의 블록 구성도이다.
- <97> 도 2는 본 발명의 일 실시예에 따른 보안정책 관리자 단말기와 홈게이트웨이의 블록 구성도이다.
- <98> 도 3은, 본 발명의 일 실시예에 따른 홈네트워크 시스템의 보안정책 설정 방법의 흐름도이다.
- <99> 도 4는, 보안정책 관리자 단말기와 홈게이트웨이 간에 송수신되는 데이터와 동작을 설명하기 위한 흐름도이다.

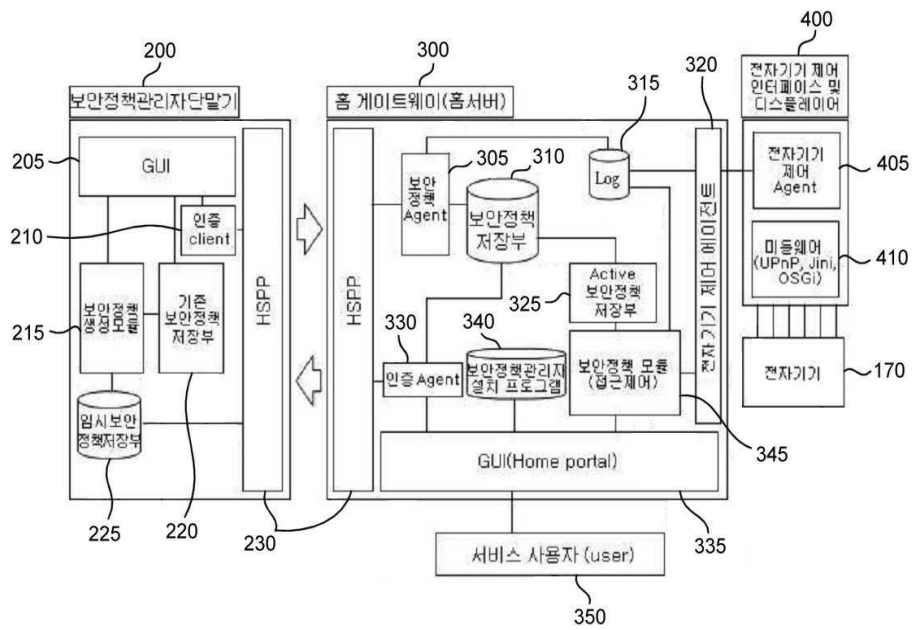
<100>	<<도면의 주요 부분에 대한 부호의 설명>	
<101>	110: 외부 제어 기기	120: 전화망
<102>	130: 인터넷	140: 내부 제어 기기
<103>	170: 다수의 전자 기기들	200: 보안정책 관리자 단말기
<104>	205: GUI(단말기 측)	210: 인증 클라이언트
<105>	215: 보안정책 생성 모듈	220: 기존 보안정책 저장부
<106>	225: 임시 보안정책 저장부	300: 홈게이트웨이
<107>	305: 보안정책 에이전트	310: 보안정책 저장부
<108>	315: 로그 저장부	320: 전자기기 제어 에이전트
<109>	325: 액티브 보안정책 저장부	330: 인증 에이전트
<110>	335: GUI(홈게이트웨이 측)	345: 보안정책 모듈

도면

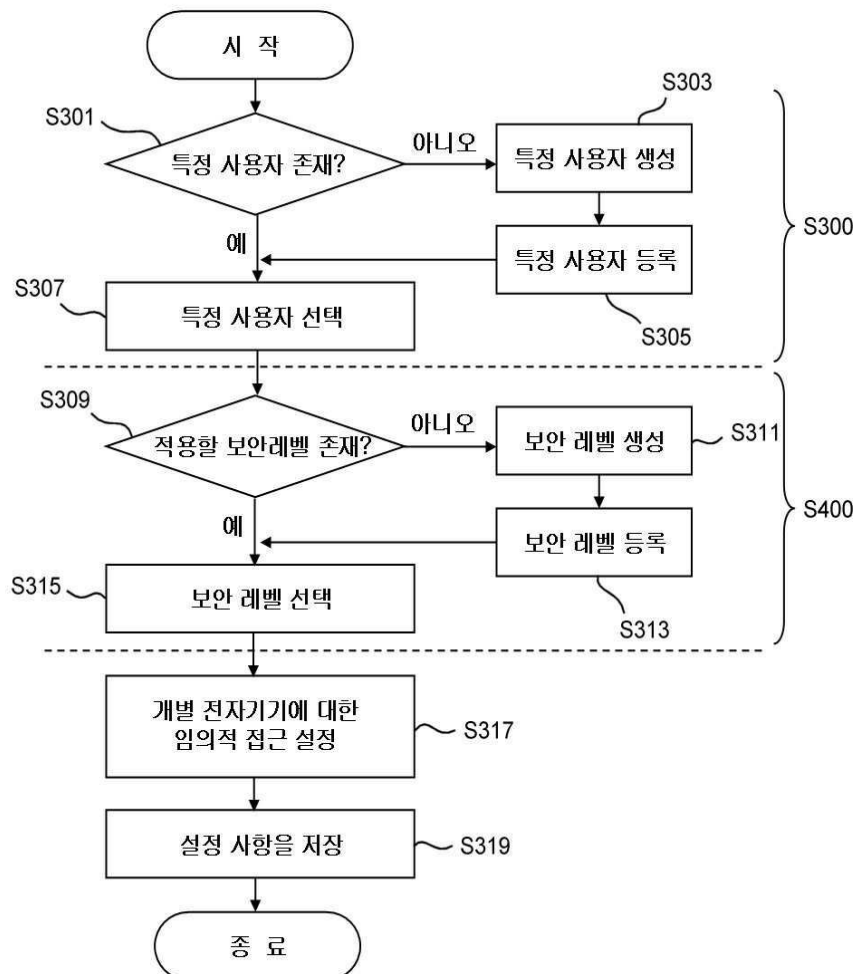
도면1



도면2



도면3



도면4

