

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017년 8월 3일 (03.08.2017)



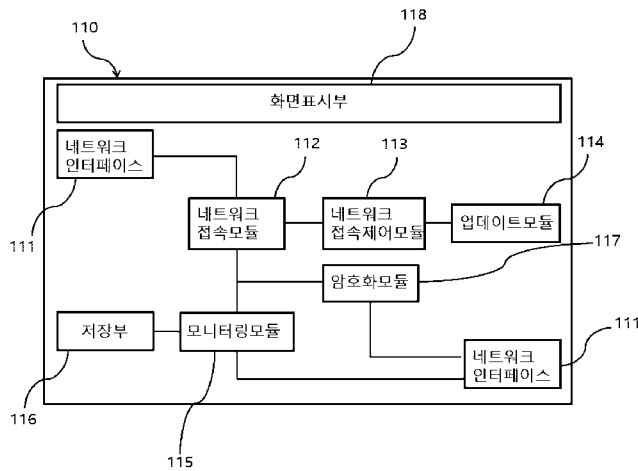
(10) 국제공개번호
WO 2017/131346 A1

- (51) 국제특허분류:
H04L 29/06 (2006.01)
- (21) 국제출원번호: PCT/KR2016/015191
- (22) 국제출원일: 2016년 12월 23일 (23.12.2016)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2016-0009386 2016년 1월 26일 (26.01.2016) KR
- (71) 출원인: 한국기초과학지원연구원 (KOREA BASIC SCIENCE INSTITUTE) [KR/KR]; 34133 대전시 유성구 과학로 169-148 (어은동), Daejeon (KR).
- (72) 발명자: 송중호 (SONG, Jung Ho); 34022 대전시 유성구 배울 2로 6, 108 동 204 호, Daejeon (KR). 윤진 (YOON, Jin); 35407 대전시 서구 복수동로 21-20, 201 동 1702 호, Daejeon (KR). 이도섭 (LEE, Do Sub); 35245 대전시 서구 둔산로 201, 103 동 705 호, Daejeon (KR). 이민주 (LEE, Min Ju); 34403 대전시 대덕구 계족산로 136, 503 동 301 호, Daejeon (KR). 김학민 (KIM, Hak Min); 30101 세종시 만남로 187, 1603 동 1901, Sejong (KR). 백성연 (BAEK, Seong Yeon); 34178 대전시 유성구 계룡로 66 번길 35, 405 호, Daejeon (KR).
- (74) 대리인: 장한특허법인 (CHANG & HAN PATENT & LAW FIRM); 06631 서울시 서초구 서초대로 356 (서초동, 서초지웰타워 14 층), Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH,

[다음 쪽 계속]

(54) Title: NETWORK ACCESS CONTROL SYSTEM AND CONTROL METHOD THEREFOR

(54) 발명의 명칭: 네트워크 접속 제어 시스템 및 제어 방법



- 111 ... Network interface
112 ... Network access module
113 ... Network access control module
114 ... Update module
115 ... Monitoring module
116 ... Storage unit
117 ... Encryption module
118 ... Screen display unit

(57) Abstract: The present invention relates to a network access control system and a control method for controlling the network access of a user by using a portable access controller, the system comprising: a portable access controller connected to a portable computing device for enabling network access, so as to manage the network access of the portable computing device on the basis of a network security policy; and a network management unit connected, through the network, to the portable access controller so as to provide the network security policy to the portable access controller, and performing a device authentication for the portable computing device.

(57) 요약서: 본 발명은 휴대용 접속제어기를 이용하여 사용자의 네트워크 접속을 제어하는 네트워크 접속 제어 시스템 및 제어 방법에 관한 것으로, 네트워크 접속이 가능한 휴대용 컴퓨팅 기기에 연결되어 네트워크 보안정책을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속을 관리하는 휴대용 접속제어기 및 상기 휴대용 접속제어기에 상기 네트워크를 통해 연결되어 상기 휴대용 접속제어기에 상기 네트워크 보안정책을 제공하며, 상기 휴대용 컴퓨팅 기기의 기기 인증을 수행하는 네트워크관리부를 포함한다.



TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

- 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 네트워크 접속 제어 시스템 및 제어 방법

기술분야

- [1] 본 발명은 휴대용 접속제어기를 이용하여 사용자의 네트워크 접속을 제어하는 네트워크 접속 제어 시스템 및 제어 방법에 관한 것이다.

배경기술

- [2] 기술의 발달로 인해 인터넷 등과 같은 네트워크를 사용할 수 있는 기기가 기하급수적으로 늘어나고 있으며 이러한 기기가 소형화되고 있다. 이러한 이유로 사용자들은 소형화된 장치를 직접 들고 다니면서 필요에 의해 네트워크에 접속하여 필요한 업무를 수행한다. 이러한 변화로 인하여 네트워크 접속을 위해 관리하고 유지하기 위해 사용된 기술 역시 변화 또는 변모하고 있다.
- [3] 일반적으로 모든 사용자가 접속 할 수 있는 네트워크망을 제외하고, 조직 및 기관에서 관리하는 네트워크에 접속 및 사용을 하고자 하는 경우에 사용자의 휴대용 컴퓨팅 기기에 별도의 관리 또는 보안 프로그램을 설치해야 한다.
- [4] 그러나, 네트워크의 접속을 관리하고 보호하기 위해서 설치되는 프로그램이 휴대용 컴퓨팅 기기에 설치되는 경우, 해당 기기의 운영체제 및 프로그램적인 요인으로 인하여 정상적으로 동작하지 않거나 설치되지 못하는 상황이 발생하기도 하며, 바이러스가 사용자의 휴대용 컴퓨팅 기기에 설치되어, 해당 프로그램을 통해서 네트워크 연결이 허용되는 경우, 감염된 휴대용 컴퓨팅 기기와 연결된 동일 네트워크에 연결되어 있는 모든 컴퓨팅 기기가 감염되거나, 주요 데이터가 유출될 수 있다.
- [5] 상기와 같은 상황을 해결하기 위해 조직 및 기관에서는 고비용의 보안 시스템을 설치하여 운영해야 하며, 신규 서비스 및 시스템을 보호하는 장비를 추가적으로 구축해야 하는 문제가 있고, 다양한 보안 시스템 및 장비를 운영함으로써 인하여 네트워크 구조가 복잡해지는 문제가 있다.
- [6] 더구나, 휴대용 컴퓨팅 기기에서 네트워크를 접속하고자 하는 경우, 네트워크 관리자가 각각의 휴대용 컴퓨팅 기기가 네트워크 접속을 식별할 수 있는 정보(예를 들어 IP주소)를 설정해야 하고, 각각의 휴대용 컴퓨팅 기기별로 별도의 보안정책을 입력해야 한다.
- [7] 그리고 컴퓨팅 기술이 발전하여 사용자가 업무에 사용하는 네트워킹이 가능한 휴대용 컴퓨팅 기기 기기가 늘어남에 따라 네트워크 보안정책 및 네트워크 접속 관리가 어려운 문제점이 있다.
- [8] (선행기술문헌)
- [9] (특허문헌)
- [10] 한국공개특허공보 제2013-0040662호

발명의 상세한 설명

기술적 과제

- [11] 본 발명의 목적은 사용자가 소지한 휴대용 컴퓨팅 기기의 네트워크 보안정책 및 네트워크 접속 관리를 간편하고 세밀하게 할 수 있는 네트워크 접속 제어 시스템 및 제어 방법을 제공하는 것이다.
- [12] 본 발명의 또 다른 목적은 사용자의 권한 및 업무 기능에 따라 네트워크 보안정책 및 네트워크 접속을 제어할 수 있다.

과제 해결 수단

- [13] 본 발명의 상기 목적은, 네트워크 접속이 가능한 휴대용 컴퓨팅 기기에 연결되어 네트워크 보안정책을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속을 관리하는 휴대용 접속제어기 및 상기 휴대용 접속제어기에 상기 네트워크를 통해 연결되어 상기 휴대용 접속제어기에 상기 네트워크 보안정책을 제공하며, 상기 휴대용 컴퓨팅 기기의 기기인증을 수행하는 네트워크관리부를 포함하는 네트워크 접속 제어 시스템 및 제어 방법이 제공됨에 달성된다.

발명의 효과

- [14] 이상에서 설명한 바와 같이, 본 발명에 따른 네트워크 접속 제어 시스템 및 제어 방법은 관리자가 사용자가 소지한 휴대용 컴퓨팅 기기의 네트워크 보안정책 및 네트워크 접속 관리를 간편하고, 세밀하게 할 수 있다.
- [15] 또한, 본 발명에 따른 네트워크 접속 제어 시스템 및 제어 방법은 사용자의 권한 및 업무 기능에 따라 네트워크 보안정책 및 네트워크 접속을 제어할 수 있다.

도면의 간단한 설명

- [16] 도 1은 본 발명의 실시예에 따른 네트워크 접속 제어 시스템을 나타낸 개략도.
- [17] 도 2는 도 1의 휴대용 접속제어기의 구성을 나타낸 블록도.
- [18] 도 3은 본 발명의 실시예에 따른 네트워크 접속 제어 과정을 나타낸 순서도.

발명의 실시를 위한 최선의 형태

- [19] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 그러나 특정한 구조적 내지 기능적 설명들은 단지 본 발명의 실시예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 실시예들은 다양한 형태로 실시될 수 있고, 본문에 설명된 실시예들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 위치에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.
- [20] 부가적으로, 각 도면에 걸쳐 표시된 동일 참조 부호는 동일 구성 요소를 지칭하며, 본 발명의 설명된 실시예의 논의를 불필요하게 불명료하도록 하는 것을 피하기 위해 공지된 특징 및 기술의 상세한 설명은 생략될 수 있다. 본 명세서에서 제1, 제2 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로서, 구성요소가 상기 용어들에 의해 제한되는

것은 아니다.

- [21] 본 발명을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.
- [22] 도 1은 본 발명의 실시예에 따른 네트워크 접속 제어 시스템을 나타낸 개략도이고, 도 2는 도 1의 휴대용 접속제어기의 구성을 나타낸 블록도이다.
- [23] 도 1 및 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 네트워크 접속 제어 시스템은 휴대용 접속제어기(110) 및 네트워크관리부(120)를 포함한다.
- [24] 본 발명의 실시예에 따른 네트워크 접속 제어 시스템은 사용자가 네트워크 접속이 가능한 휴대용 컴퓨팅 기기(101)를 사용하여 네트워크(102)에 접속하고자 하는 경우, 휴대용 컴퓨팅 기기(101)와 네트워크(102)의 접속을 제어 및 관리할 수 있는 제어 시스템 및 제어 방법을 제공하는데 기술적 주안점을 두고 있다.
- [25] 여기서, 상기 휴대용 컴퓨팅 기기(101)는 사용자가 소유하여 네트워크 접속이 가능한 장치로 스마트폰, 노트북, 스마트 패드 등일 수 있으며, 사용자가 휴대 가능하고 네트워크(102)와의 접속이 가능한 장치라면 어떠한 장치도 무방하다.
- [26] 상기 휴대용 접속제어기(110)는 네트워크(102)접속이 가능한 휴대용 컴퓨팅 기기(101)에 연결되어 네트워크 보안정책을 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속을 관리할 수 있다.
- [27] 여기서, 상기 휴대용 접속제어기(110)는 사용자가 휴대 가능하도록 구성될 수 있다. 이때, 상기 휴대용 컴퓨팅 기기(101)는 다수가 구비될 수 있는데, 상기 휴대용 접속제어기(110)는 다수의 휴대용 컴퓨팅 기기(101) 중 적어도 어느 하나와 연결되어 네트워크(102) 접속을 관리할 수 있다. 또한, 상기 휴대용 접속제어기(110)는 동시에 다수의 휴대용 컴퓨팅 기기(101)와 연결될 수 있으며, 다수의 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속을 동시에 관리할 수 있다.
- [28] 한편, 상기 휴대용 접속제어기(110)는 네트워크인터페이스(111), 네트워크접속모듈(112) 및 네트워크접속제어모듈(113)을 포함할 수 있다.
- [29] 상기 네트워크인터페이스(111)는 휴대용 컴퓨팅 기기(101)와 네트워크(102)에 각각 연결되어 휴대용 접속제어기(110)를 휴대용 컴퓨팅 기기(101)와 네트워크(102) 사이에 연결할 수 있다. 여기서, 상기 네트워크인터페이스(111)는 무선 또는 유선 방식으로 휴대용 컴퓨팅 기기(101)와 네트워크(102)에 휴대용 접속제어기(110)를 연결할 수 있다.
- [30] 상기 네트워크접속모듈(112)은 네트워크인터페이스(111)와 연결되어 네트워크(102) 접속을 요청할 수 있다. 여기서, 상기 네트워크접속모듈(112)은 네트워크인터페이스(111)에 휴대용 컴퓨팅 기기(101)와 네트워크(102)가 연결되는 경우, 네트워크(102)와의 접속을 요청할 수 있다. 이때, 상기 네트워크접속모듈(112)은 네트워크인터페이스(111)에 연결되는 휴대용 컴퓨팅 기기(101)가 신규 휴대용 컴퓨팅 기기(101) 인지 확인하는 기기인증을 요청할 수

있다.

- [31] 상기 네트워크접속제어모듈(113)은 네트워크접속모듈(112)에 연결되어 네트워크 보안정책을 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [32] 여기서, 상기 네트워크 보안정책은 인증정보, IP 주소, 포트번호, 접속 허용 횟수, 접속 허용 시간, 전송데이터양 중 어느 하나일 수 있다.
- [33] 한편, 상기 네트워크접속제어모듈(113)은 미리 저장된 인증정보를 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [34] 구체적으로 상기 네트워크접속제어모듈(113)은, 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 연결된 휴대용 컴퓨팅 기기(101)의 인증정보가 네트워크접속제어모듈(113)에 저장되어 있는지 확인하고, 인증정보가 네트워크접속제어모듈(113)에 저장되어 있는 경우 네트워크(102) 접속을 허용하고, 인증정보가 저장되어있지 않는 경우 네트워크(102) 접속 허용을 불가할 수 있다.
- [35] 또한, 상기 네트워크접속제어모듈(113)은 미리 저장된 IP 주소를 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [36] 구체적으로 상기 네트워크접속제어모듈(113)은 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 연결된 휴대용 컴퓨팅 기기(101)의 IP 주소가 네트워크접속제어모듈(113)에 저장되어 있는지 확인하고, IP 주소가 네트워크접속제어모듈(113)에 저장되어 있는 경우 네트워크(102) 접속을 허용하고, IP 주소가 저장되어있지 않는 경우 네트워크(102) 접속 허용을 불가할 수 있다.
- [37] 아울러, 상기 네트워크접속제어모듈(113)은 미리 저장된 포트정보를 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [38] 구체적으로 상기 네트워크접속제어모듈(113)은, 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 연결된 휴대용 컴퓨팅 기기(101)의 포트정보가 네트워크접속제어모듈(113)에 저장되어 있는지 확인하고, 포트정보가 저장되어 있는 경우 네트워크(102) 접속을 허용하고, 포트정보가 저장되어있지 않는 경우 네트워크(102) 접속 허용을 불가할 수 있다.
- [39] 그리고 상기 네트워크접속제어모듈(113)은, 미리 설정된 네트워크 접속 허용 횟수를 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다. 이때, 상기 네트워크접속제어모듈(113)에는 휴대용 컴퓨팅 기기(101)별로 네트워크 접속 허용 횟수가 미리 설정될 수 있고, 휴대용 접속제어기(110)별로 네트워크 접속 허용 횟수가 미리 설정될 수 있다.
- [40] 구체적으로 상기 네트워크접속제어모듈(113)은, 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 네트워크접속제어모듈(113)에 미리 설정된 휴대용 컴퓨팅 기기(101)별 네트워크 접속 허용 횟수와 휴대용 접속제어기(110)별 네트워크 접속 허용 횟수를 확인하고, 연결된 휴대용 컴퓨팅

기기(101)의 네트워크 접속 허용 횟수가 남아있는 경우 해당하는 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속을 허용하고, 네트워크 접속 허용 횟수가 남아있지 않는 경우 해당하는 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용을 불가할 수 있다. 또한, 상기 네트워크접속제어모듈(113)은 휴대용 접속제어기(110)별 네트워크 접속 허용 횟수가 남아있는 경우 연결된 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속을 허용하고, 네트워크 접속 허용 횟수가 남아있지 않는 경우 연결된 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용을 불가할 수 있다.

- [41] 아울러, 상기 네트워크접속제어모듈(113)은 미리 설정된 접속 허용 시간을 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [42] 구체적으로 상기 네트워크접속제어모듈(113)은, 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 접속을 요청한 시간이 미리 설정된 접속 허용 시간 내인지 확인하고, 접속 요청 시간이 미리 설정된 접속 허용 시간 내이면 네트워크(102) 접속을 허용하고, 접속 요청 시간이 미리 설정된 접속 허용 시간이면 네트워크(102) 접속 허용을 불가할 수 있다.
- [43] 한편, 상기 네트워크접속제어모듈(113)은 미리 설정된 전송데이터양을 토대로 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 허용 여부를 결정할 수 있다.
- [44] 구체적으로 상기 네트워크접속제어모듈(113)은, 네트워크접속모듈(112)의 네트워크(102) 접속 요청에 따라 미리 설정된 전송데이터양이 남았는지 확인하고, 미리 설정된 전송데이터양이 남았으며 네트워크(102) 접속을 허용하고, 미리 설정된 전송데이터양이 남지 않았으면 네트워크(102) 접속 허용을 불가할 수 있다.
- [45] 상기 업데이트모듈(114)은 네트워크접속제어모듈(113)에 연결되어 네트워크관리부(120)에서 제공되는 네트워크 보안정책을 업데이트할 수 있다.
- [46] 여기서, 상기 업데이트모듈(114)은 네트워크관리부(120)와 네트워크(102)를 통해 연결될 수 있다. 즉, 상기 업데이트모듈(114)은 관리자가 네트워크관리부(120)에 네트워크 보안정책을 설정하는 경우, 네트워크관리부(120)에서 제공되는 네트워크 보안정책을 네트워크제어모듈(113)에 수시로 업데이트할 수 있다.
- [47] 한편, 상기 휴대용 접속제어기(110)는 송수신되는 데이터를 모니터링하는 모니터링모듈(115) 및 모니터링모듈(115)에서 모니터링된 모니터링데이터가 저장되는 저장부(116)를 더 포함할 수 있다.
- [48] 여기서, 상기 모니터링모듈(115)은 네트워크접속모듈(112)에 연결되어 송수신되는 데이터를 모니터링할 수 있다. 또한, 상기 저장부(116)는 모니터링모듈(115)에서 모니터링된 모니터링데이터가 저장될 수 있다. 즉, 상기 모니터링모듈(115)은 어떠한 데이터가 송수신되는지 모니터링하여 저장부(116)에 저장할 수 있으므로, 보안이 필요한 데이터의 유출을 방지할 수

있다.

- [49] 한편, 상기 휴대용 접속제어기(110)는 네트워크접속모듈(112)에 연결되어 상기 네트워크 보안정책을 토대로 송수신되는 데이터를 암호화하는 암호화모듈(117)을 더 포함할 수 있다.
- [50] 여기서, 상기 암호화모듈(117)은 네트워크접속제어모듈(113)에 미리 설정된 IP 주소 또는 포트정보를 토대로 송수신되는 데이터를 암호화할 수 있다.
- [51] 구체적으로, 상기 네트워크접속모듈(112)에서 송수신되는 데이터에 대한 암호화가 요청되면, 네트워크접속제어모듈(113)은 암호화를 요청하는 IP 주소와 포트정보가 네트워크접속제어모듈(113)에 미리 설정된 IP 주소 또는 포트정보에 해당하는지 확인하고, 이에 해당하는 경우 암호화모듈(117)은 데이터를 암호화하여 송신 및 수신할 수 있다.
- [52] 이때, 상기 암호화모듈(117)에서 암호화가 수행되는 IP 주소와 포트정보는 업데이트모듈(114)을 통해 네트워크접속제어모듈(113)에 업데이트되어 변경될 수 있다.
- [53] 따라서, 상기 암호화모듈(117)을 통해 별도의 보안 프로그램을 설치하지 않고도 네트워크(102)를 통해 송수신되는 데이터를 안전하게 보호할 수 있으며, 업데이트모듈(114)을 통해 관리자는 필요에 따라 주요 데이터를 암호화하여 송수신할 수 있도록 제어할 수 있다.
- [54] 한편, 상기 휴대용 접속제어기(110)는 휴대용 컴퓨팅 기기(101)의 상태 및 네트워크(102) 접속 상태를 표시하는 화면표시부(118)를 더 포함할 수 있다.
- [55]
- [56] 여기서, 상기 화면표시부(118)는 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속 여부를 표시할 수 있다.
- [57] 상기 네트워크관리부(120)는 휴대용 접속제어기(110)에 네트워크(102)를 통해 연결되어 네트워크 보안정책을 제공하며, 휴대용 컴퓨팅 기기(101)의 기기인증을 수행할 수 있다.
- [58] 여기서, 상기 네트워크관리부(120)는 네트워크(102)를 통해 네트워크 보안정책을 휴대용 접속제어기(110)의 업데이트모듈(114)로 제공할 수 있다.
- [59] 또한, 상기 네트워크관리부(120)는 휴대용 접속제어기(110)에 연결되는 휴대용 컴퓨팅 기기(101)가 기기인증을 받지 않은 신규 휴대용 컴퓨팅 기기(101)인 경우, 기기인증을 수행할 수 있다.
- [60] 따라서, 상술한 휴대용 접속제어기(110)를 통해 휴대용 컴퓨팅 기기(101)의 네트워크(102) 접속을 관리함으로써, 관리자가 각각 휴대용 컴퓨팅 기기(101)를 모두 관리할 필요 없이 각각의 사용자가 휴대한 휴대용 접속제어기(110)만을 관리하여 복수의 휴대용 컴퓨팅 기기(101)를 관리할 수 있으므로, 네트워크 보안정책 및 네트워크 접속 관리를 간편하고, 세밀하게 할 수 있다.
- [61] 또한, 사용자가 휴대한 휴대용 접속제어기(110)를 관리함으로써, 사용자의 권한 및 업무 기능에 따라 네트워크 보안정책 및 네트워크 접속을 제어할 수

있다.

[62]

[63] 이하, 상술한 네트워크 접속 제어 시스템을 이용한 제어과정을 설명한다.

[64]

도 3은 본 발명의 실시예에 따른 네트워크 접속 제어 과정을 나타낸 순서도이다.

[65]

도 3에 도시된 바와 같이, 본 발명의 실시예에 따른 네트워크 접속 제어 과정은, 먼저, 휴대용 컴퓨팅 기기(101)가 휴대용 접속제어기(110)에 연결되면, 네트워크 접속을 요청할 수 있다(S1100).

[66]

다음으로, 휴대용 접속제어기(110)에서 미리 저장된 인증정보를 토대로 기기인증 여부를 확인하여 신규 휴대용 컴퓨팅 기기(101)인지 확인할 수 있다(S1200).

[67]

여기서, 네트워크 접속을 요청한 휴대용 컴퓨팅 기기(101)의 MAC 정보, IP 주소, 사용자정보 등의 기기정보와 휴대용 접속제어기(110)에 미리 저장된 인증정보를 비교하여 이미 기기인증이 수행된 휴대용 컴퓨팅 기기(101)인지를 판단할 수 있다.

[68]

다음으로, 휴대용 컴퓨팅 기기(101)의 기기정보를 확인한 결과에 따라 신규 휴대용 컴퓨팅 기기(101)이면, 네트워크관리부(120)에서 기기인증을 수행할 수 있다(S1300).

[69]

여기서, 네트워크 접속을 요청한 휴대용 컴퓨팅 기기(101)가 신규 휴대용 컴퓨팅 기기(101)인 경우, 휴대용 컴퓨팅 기기(101)에 기기인증을 위한 정보를 요청하여 수신하고, 이를 네트워크관리부(120)로 전송할 수 있다.

[70]

이후, 네트워크관리부(120)는 기기인증을 위한 정보가 수신되면, 수신되는 정보를 토대로 휴대용 컴퓨팅 기기(101)를 네트워크(102)의 접속을 허용할지를 판단할 수 있다.

[71]

다음으로, 네트워크(102)의 접속을 허용하는 경우, 해당 휴대용 컴퓨팅 기기(101)의 등록을 원하는 사용자에게 비밀번호와 같은 별도의 추가인증정보의 입력을 요청하여 추가인증정보를 수신하고, 수신된 추가인증정보와 기기인증을 위한 정보를 토대로 기기인증을 수행할 수 있다.

[72]

이때, 휴대용 컴퓨팅 기기(101)의 기기인증이 수행되지 않는 경우, 휴대용 접속제어기(110)로 기기인증 불가 메시지를 송신하여 화면표시부(118)에 기기인증 불가 메시지를 표시할 수 있다.

[73]

다음으로, 휴대용 접속제어기(110)에서 휴대용 컴퓨팅 기기(101)의 기기인증이 확인되면, 휴대용 접속제어기(110)는 네트워크관리부(120)에서 제공되는 네트워크 보안을 토대로 휴대용 컴퓨팅 기기(101)의 네트워크 접속 허용 여부를 결정할 수 있다(S1400).

[74]

여기서, 상기 네트워크 보안정책은 IP 주소, 포트번호, 접속 허용 횟수, 접속 허용 시간, 전송데이터량 중 어느 하나일 수 있다.

[75]

구체적으로, 네트워크 접속을 요청하는 휴대용 컴퓨팅 기기(101)의 IP 주소 및

포트번호가 네트워크관리부(120)에서 제공되는 IP 주소 및 포트번호와 동일한 경우 네트워크(102) 접속을 허용하고, 동일하지 않는 경우 네트워크(102) 접속 허용을 불가할 수 있다.

[76] 또한, 네트워크 접속을 요청하는 휴대용 컴퓨팅 기기(101)에 대응하여 네트워크관리부(120)에서 제공되는 접속 허용 횟수가 미리 설정된 접속 허용 횟수를 초과하지 않는 경우 네트워크(102) 접속을 허용하고, 미리 설정된 접속 허용 횟수를 초과하는 경우 네트워크(102) 접속 허용을 불가할 수 있다.

[77] 아울러, 네트워크 접속을 요청하는 휴대용 컴퓨팅 기기(101)에 대응하여 네트워크관리부(120)에서 제공되는 접속 허용 시간이 미리 설정된 접속 허용 시간 내인 경우 네트워크(102) 접속을 허용하고, 미리 설정된 접속 허용 시간이 아닌 경우 네트워크(102) 접속 허용을 불가할 수 있다.

[78] 그리고 네트워크 접속을 요청하는 휴대용 컴퓨팅 기기(101)에 대응하여 네트워크관리부(120)에서 제공되는 전송데이터양이 미리 설정된 전송데이터양을 초과하지 않는 경우 네트워크(102) 접속을 허용하고, 미리 설정된 전송데이터양을 초과한 경우 네트워크(102) 접속 허용을 불가할 수 있다.

[79] 본 명세서에서 '연결된다' 또는 '연결하는' 등과 이런 표현의 다양한 변형들의 지칭은 다른 구성요소와 직접적으로 연결되거나 다른 구성요소를 통해 간접적으로 연결되는 것을 포함하는 의미로 사용된다. 또한, 본 명세서에서 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 아울러 본 명세서에서 사용되는 '포함한다' 또는 '포함하는'으로 언급된 구성요소, 단계, 동작 및 소자는 하나 이상의 다른 구성요소, 단계, 동작, 소자 및 장치의 존재 또는 추가를 배제하지 않는다.

[80] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 명세서를 통해 개시된 모든 실시예들과 조건부 예시들은, 본 발명의 기술 분야에서 통상의 지식을 가진 당업자가 독자가 본 발명의 원리와 개념을 이해하도록 돕기 위한 의도로 기술된 것으로, 당업자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

[81] (부호의 설명)

[82] 101 : 휴대용 컴퓨팅 기기 102 : 네트워크

[83] 110 : 휴대용 접속제어기 111 : 네트워크인터페이스

[84] 112 : 네트워크접속모듈 113 : 네트워크접속제어모듈

[85] 114 : 업데이트모듈 115 : 모니터링모듈

[86] 116 : 저장부 117 : 암호화모듈

[87] 118 : 화면보시부 120 : 네트워크관리부

[88]

"Not Furnished Upon Filing"

청구범위

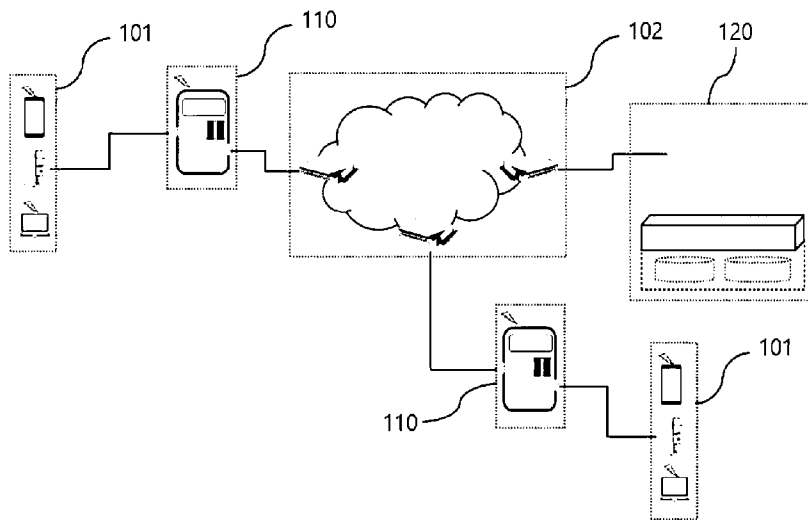
- [청구항 1] 네트워크 접속이 가능한 휴대용 컴퓨팅 기기에 연결되어 네트워크 보안정책을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속을 관리하는 휴대용 접속제어기; 및
상기 휴대용 접속제어기에 상기 네트워크를 통해 연결되어 상기 휴대용 접속제어기에 상기 네트워크 보안정책을 제공하며, 상기 휴대용 컴퓨팅 기기의 기기인증을 수행하는 네트워크관리부;
를 포함하는 네트워크 접속 제어 시스템.
- [청구항 2] 제1항에 있어서,
상기 휴대용 접속제어기는
다수의 휴대용 컴퓨팅 기기 중 적어도 어느 하나와 연결되는 네트워크 접속 제어 시스템.
- [청구항 3] 제1항에 있어서,
상기 휴대용 접속제어기는
상기 휴대용 컴퓨팅 기기와 상기 네트워크에 각각 연결되는
네트워크인터페이스;
상기 네트워크인터페이스와 연결되어 네트워크 접속을 요청하는
네트워크접속모듈;
상기 네트워크접속모듈에 연결되어 상기 네트워크 보안정책을 토대로
상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는
네트워크접속제어모듈; 및
상기 네트워크접속제어모듈에 연결되어 상기 네트워크관리부에서
제공되는 상기 네트워크 보안정책을 업데이트하는 업데이트모듈;
을 포함하는 네트워크 접속 제어 시스템.
- [청구항 4] 제3항에 있어서,
상기 휴대용 접속제어기는
상기 네트워크접속모듈에 연결되어 송수신되는 상기 데이터를
모니터링하는 모니터링모듈; 및
상기 모니터링모듈에서 모니터링한 모니터링데이터를 저장하는
저장부를 더 포함하는 네트워크 접속 제어 시스템.
- [청구항 5] 제3항에 있어서,
상기 휴대용 접속제어기는
상기 네트워크접속모듈에 연결되어 상기 네트워크 보안정책을 토대로
송수신되는 상기 데이터를 암호화하는 암호화모듈을 더 포함하는
네트워크 접속 제어 시스템.
- [청구항 6] 제3항에 있어서,
상기 휴대용 접속제어기는

- 상기 휴대용 컴퓨팅 기기의 상태 및 네트워크 접속 상태를 표시하는 화면 표시부를 더 포함하는 네트워크 접속 제어 시스템.
- [청구항 7] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 저장된 인증정보를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 8] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 저장된 IP 주소를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 9] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 저장된 포트정보를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 10] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 설정된 네트워크 접속 허용 횟수를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 11] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 설정된 네트워크 접속 허용 시간을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 12] 제3항에 있어서,
상기 네트워크접속제어모듈은
미리 설정된 전송데이터양을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 시스템.
- [청구항 13] 휴대용 컴퓨팅 기기가 휴대용 접속제어기에 연결되면, 네트워크 접속을 요청하는 접속 요청 단계;
상기 휴대용 접속제어기에서 미리 저장된 인증정보를 토대로 기기인증 여부를 확인하여 신규 휴대용 컴퓨팅 기기인지 확인하는 기기정보 확인 단계;
상기 휴대용 컴퓨팅 기기의 기기정보를 확인한 결과에 따라 신규 휴대용 컴퓨팅 기기이면, 네트워크관리부에서 기기인증을 수행하는 기기인증 단계;
상기 휴대용 접속제어기에서 상기 휴대용 컴퓨팅 기기의 기기인증이 확인되면, 상기 네트워크관리부에서 제공되는 네트워크 보안정책을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 결정 단계;

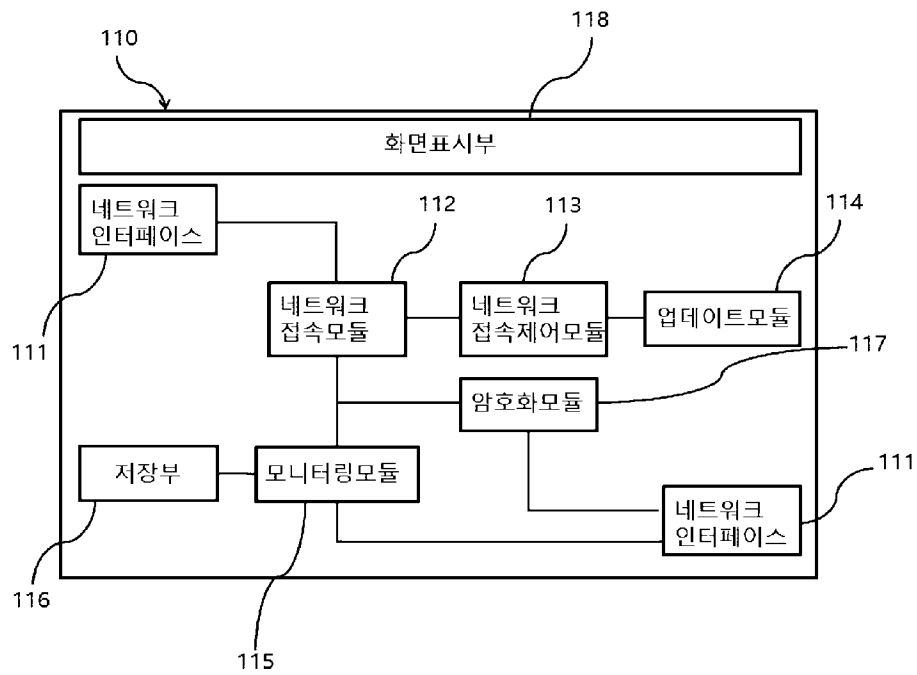
를 포함하는 네트워크 접속 제어 방법.

- [청구항 14] 제13항에 있어서,
상기 네트워크 접속 결정 단계는,
상기 네트워크관리부에서 제공되는 IP 주소를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 방법.
- [청구항 15] 제13항에 있어서,
상기 네트워크 접속 결정 단계는,
상기 네트워크관리부에서 제공되는 포트정보를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 방법.
- [청구항 16] 제13항에 있어서,
상기 네트워크 접속 결정 단계는,
상기 네트워크관리부에서 제공되는 네트워크 접속 허용 횟수를 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 방법.
- [청구항 17] 제13항에 있어서,
상기 네트워크 접속 결정 단계는,
상기 네트워크관리부에서 제공되는 네트워크 접속 허용 시간을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 방법.
- [청구항 18] 제13항에 있어서,
상기 네트워크 접속 결정 단계는,
상기 네트워크관리부에서 제공되는 전송데이터양을 토대로 상기 휴대용 컴퓨팅 기기의 네트워크 접속 허용 여부를 결정하는 네트워크 접속 제어 방법.

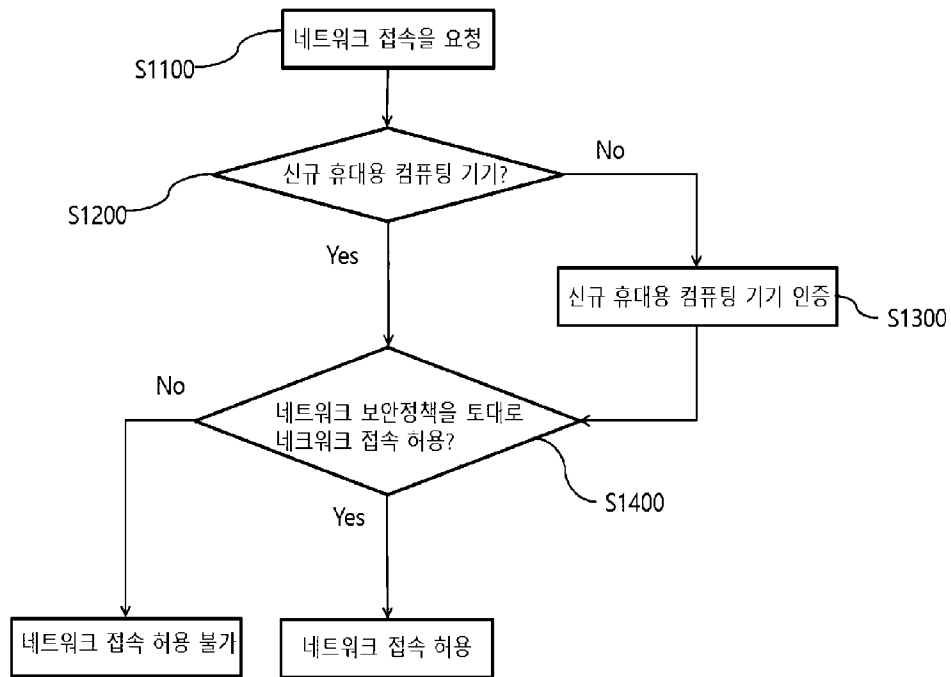
[도1]



[도2]



[도3]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/015191

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/06; G06F 21/44; G06F 21/20; G06F 21/51; G06F 21/35; G06F 17/60; H04W 40/24; H04W 12/08; H04L 12/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: portable, controller, network connection, authorization, authentication, security policy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2009-521820 A (PANASONIC CORPORATION) 04 June 2009 See paragraphs [0018], [0028]-[0029], [0031], [0034], [0057], [0067], [0073], [0088], [0091], [0095]-[0096], claims 1-2 and figures 1, 3.	1-5,7,13
Y		6,8-12,14-18
Y	JP 2015-166966 A (N WORK K.K.) 24 September 2015 See paragraphs [0032], [0056], [0058]-[0059] and figure 1.	6,10-11,16-17
Y	JP 4832516 B2 (FUJITSU LIMITED) 07 December 2011 See claims 11, 15-16 and figure 1.	8-9,14-15
Y	JP 2004-272792 A (TOSHIBA CORP.) 30 September 2004 See paragraph [0035] and figures 1, 5.	12,18
A	JP 2015-038667 A (BASIC K.K.) 26 February 2015 See claims 1-8 and figure 1.	1-18



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

25 APRIL 2017 (25.04.2017)

Date of mailing of the international search report

02 MAY 2017 (02.05.2017)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Sconsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2016/015191

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 2009-521820 A	04/06/2009	CN 101346968 A	14/01/2009
		CN 101346968 B	12/10/2011
		CN 102244868 A	16/11/2011
		EP 1966970 A1	10/09/2008
		EP 2144416 A1	13/01/2010
		JP 4857342 B2	18/01/2012
		US 2009-0313680 A1	17/12/2009
		US 8539554 B2	17/09/2013
		WO 2007-077958 A1	12/07/2007
JP 2015-166966 A	24/09/2015	NONE	
JP 4832516 B2	07/12/2011	JP 2009-138663 A1	01/10/2009
		WO 2007-138663 A1	06/12/2007
JP 2004-272792 A	30/09/2004	CN 1531247 A	22/09/2004
		EP 1473613 A1	03/11/2004
		US 2004-0243804 A1	02/12/2004
JP 2015-038667 A	26/02/2015	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; G06F 21/44; G06F 21/20; G06F 21/51; G06F 21/35; G06F 17/60; H04W 40/24; H04W 12/08; H04L 12/28

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 휴대, 제어기, 네트워크 접속, 허가, 인증, 보안 정책

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	JP 2009-521820 A (PANASONIC CORPORATION) 2009.06.04 단락 [0018], [0028]-[0029], [0031], [0034], [0057], [0067], [0073], [0088], [0091], [0095]-[0096], 청구항 1-2 및 도면 1, 3 참조.	1-5, 7, 13
Y		6, 8-12, 14-18
Y	JP 2015-166966 A (N WORK K.K.) 2015.09.24 단락 [0032], [0056], [0058]-[0059] 및 도면 1 참조.	6, 10-11, 16-17
Y	JP 4832516 B2 (FUJITSU LIMITED) 2011.12.07 청구항 11, 15-16 및 도면 1 참조.	8-9, 14-15
Y	JP 2004-272792 A (TOSHIBA CORP.) 2004.09.30 단락 [0035] 및 도면 1, 5 참조.	12, 18
A	JP 2015-038667 A (BASIC K.K.) 2015.02.26 청구항 1-8 및 도면 1 참조.	1-18

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2017년 04월 25일 (25.04.2017)

국제조사보고서 발송일

2017년 05월 02일 (02.05.2017)

ISA/KR의 명칭 및 우편주소



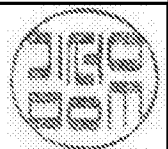
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

김성우

전화번호 +82-42-481-3348



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 2009-521820 A	2009/06/04	CN 101346968 A CN 101346968 B CN 102244868 A EP 1966970 A1 EP 2144416 A1 JP 4857342 B2 US 2009-0313680 A1 US 8539554 B2 WO 2007-077958 A1	2009/01/14 2011/10/12 2011/11/16 2008/09/10 2010/01/13 2012/01/18 2009/12/17 2013/09/17 2007/07/12
JP 2015-166966 A	2015/09/24	없음	
JP 4832516 B2	2011/12/07	JP 2009-138663 A1 WO 2007-138663 A1	2009/10/01 2007/12/06
JP 2004-272792 A	2004/09/30	CN 1531247 A EP 1473613 A1 US 2004-0243804 A1	2004/09/22 2004/11/03 2004/12/02
JP 2015-038667 A	2015/02/26	없음	