

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일

2017년 11월 30일 (30.11.2017) WIPO | PCT



(10) 국제공개번호

WO 2017/204566 A1

(51) 국제특허분류:

H04L 29/06 (2006.01)

(21) 국제출원번호:

PCT/KR2017/005428

(22) 국제출원일:

2017년 5월 24일 (24.05.2017)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(30) 우선권정보:

10-2016-0063629 2016년 5월 24일 (24.05.2016) KR

(71) 출원인: 주식회사 케이티 (KT CORPORATION) [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).

(72) 발명자: 김태균 (KIM, Tae-Gyun); 13618 경기도 성남시 분당구 미금로 215, 806동 1502호, Gyeonggi-do (KR). 이형우 (LEE, Hyung-Woo); 03155 서울시 종로구 종로 3길 33, Seoul (KR). 서경덕 (SEO, Kyung-Deok); 55087

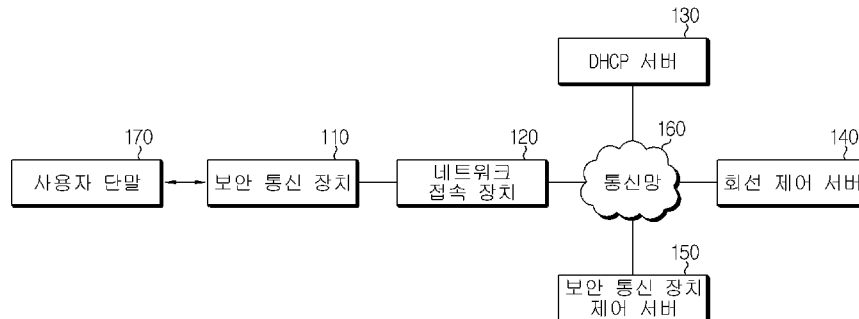
전라북도 전주시 완산구 삼천천변1길 32, 101동 1802호, Jeollabuk-do (KR). 조대성 (CHO, Dae-Sung); 06113 서울시 강남구 강남대로126길 76, 302호, Seoul (KR). 강봉권 (KANG, Bong-Kwon); 16043 경기도 의왕시 오리나무 1길 41, 4층, Gyeonggi-do (KR). 신명순 (SHIN, Myung-Soon); 14070 경기도 안양시 동안구 귀인로 237, 204동 801호, Gyeonggi-do (KR).

(74) 대리인: 특허법인 필앤온지 (PHIL & ONZI INT'L PATENT & LAW FIRM); 06643 서울시 서초구 서초중앙로 36, 3층, 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,

(54) Title: LINE CONTROL DEVICE AND METHOD

(54) 발명의 명칭: 회선 제어 장치 및 방법



- 110 ... Security communication device
- 120 ... Network access device
- 130 ... DHCP server
- 140 ... Line control server
- 150 ... Security communication device control server
- 160 ... Communication network
- 170 ... User terminal

(57) Abstract: According to one aspect of the present invention, a line control device for managing a security communication device controlling an Internet network access of a user terminal between the user terminal and a network access device comprises: a line information collection unit for collecting line information from the network access device; a state checking unit for identifying a device connected to the network access device in the collected line information, and checking the state of the identified device in a security communication device control server; and a line blocking unit for selectively blocking a line of the network access device according to the state checking result of the identified device.

PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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 제21조(3))

(57) 요약서: 본 발명의 일 측면에 따른, 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 관리하기 위한 회선 제어 장치는, 상기 네트워크 접속 장치로부터 회선 정보를 수집하는 회선 정보 수집부; 상기 수집된 회선 정보에서 네트워크 접속 장치에 연결된 장치를 식별하고, 식별된 장치의 상태를 보안 통신 장치 제어 서버에서 확인하는 상태 확인부; 및 상기 식별된 장치의 상태 확인 결과에 따라 상기 네트워크 접속 장치의 회선을 선택적으로 차단하는 회선 차단부를 포함한다.

명세서

발명의 명칭: 회선 제어 장치 및 방법

기술분야

- [1] 본 출원은 2016년 05월 24일에 출원된 한국 특허출원 제10-2016-0063629호를 기초로 한 우선권 주장을 수반하며, 해당 특허출원의 명세서 및 도면에 개시된 모든 내용은 본 출원에 원용된다.
- [2] 본 발명은 회선 제어 장치 및 방법에 관한 것으로, 보다 구체적으로 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 관리하기 위한 회선 제어 장치 및 방법에 관한 것이다.

배경기술

- [3] 인터넷 통신이 가능한 사용자 단말, 예를 들어 컴퓨터로 인터넷을 접속하기 위해서는 사용자 단말을 L2 스위치 등과 같은 인터넷망에 연결된 네트워크 접속 장치에 연결해야 한다. 이러한 네트워크 접속 장치는 통신 회사의 네트워크 장비로서 고객이 인터넷 가입을 하면 네트워크 접속 장치의 회선을 개방하여 인터넷 연결이 가능하도록 한다.
- [4] 인터넷 가입 고객이 기업인 경우, 일반적으로 하나의 네트워크 접속 장치를 통해 다수의 사용자들이 인터넷을 이용하게 되고, 따라서 기업은 보안을 위해 인터넷 사용 범위를 통제하려는 시도를 한다. 일반적으로 인터넷 사용 범위를 통제하는 방식으로 소프트웨어 또는 별도의 하드웨어 장비를 이용한다. 그런데 소프트웨어 방식의 경우 사용자에 의해 강제로 소프트웨어가 종료될 수 있고, 또는 소프트웨어가 저장된 저장 매체를 포맷하여 소프트웨어를 제거하여 불법적인 인터넷 사용을 할 가능성이 있다.
- [5] 따라서 이러한 소프트웨어 방식의 한계를 극복하기 위해 별도의 하드웨어 장비, 즉 보안 통신 장치를 이용하여 인터넷 사용 범위를 통제하는 시도가 있다. 즉, 네트워크 접속 장치에 별도의 보안 통신 장치를 연결하고, 사용자 단말은 그 보안 통신 장치에 연결해야만 인터넷 접속이 되고, 보안 통신 장치는 사용자 단말의 인터넷 사용 범위를 제한한다. 그런데 이러한 보안 통신 장치를 이용하더라도 사용자가 보안 통신 장치를 제거하여 네트워크 접속 장치에 직접 사용자 단말을 연결하는 시도를 막을 수 없고, 또는 사용자 단말을 소프트웨어적으로 보안 통신 장치인 것처럼 변조한 후 보안 통신 장치 없이 네트워크 접속 장치에 직접 연결하여 인터넷에 접속하는 경우 차단을 할 수 없다.

발명의 상세한 설명

기술적 과제

- [6] 본 발명은 상기와 같은 문제점을 해결하기 위해 제안된 것으로, 보안 통신

장치를 통해 인터넷 접속을 통제하는데 있어서 상기 보안 통신 장치를 제거하거나 사용자 단말을 상기 보안 통신 장치인 것처럼 변조하여 직접 사용자 단말로 인터넷 접속을 하는 것을 차단하기 위한 회선 제어 장치 및 방법을 제공하는데 그 목적이 있다.

과제 해결 수단

- [7] 상기 목적을 달성하기 위한 본 발명의 일 측면에 따른, 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 관리하기 위한 회선 제어 장치는, 상기 네트워크 접속 장치로부터 회선 정보를 수집하는 회선 정보 수집부; 상기 수집된 회선 정보에서 네트워크 접속 장치에 연결된 장치를 식별하고, 식별된 장치의 상태를 보안 통신 장치 제어 서버에서 확인하는 상태 확인부; 및 상기 식별된 장치의 상태 확인 결과에 따라 상기 네트워크 접속 장치의 회선을 선택적으로 차단하는 회선 차단부를 포함한다.
- [8] 상기 회선 차단부는, 상기 보안 통신 장치 제어 서버에서 확인된 상기 식별된 장치의 상태가 정상 상태인 경우, 상기 네트워크 접속 장치의 회선을 유지하고 비정상 상태인 경우 회선을 차단할 수 있다.
- [9] 상기 보안 통신 장치는, 상기 사용자 단말과 연결될 경우 상기 보안 통신 장치 제어 서버로 주기적으로 상태 정보를 전송하고, 상기 사용자 단말과의 연결이 해제되는 경우 연결 해제 메시지를 상기 보안 통신 장치 제어 서버로 전송하고 상태 정보의 주기적 전송을 중단할 수 있다.
- [10] 상기 상태 확인부는, 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로 상기 연결 해제 메시지가 수신되지 않고 상태 정보의 전송 주기 동안 상태 정보가 수신되지 않은 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신할 수 있다.
- [11] 상기 상태 확인부는, 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로의 상태 정보의 주기적 전송 기록이 없는 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신할 수 있다.
- [12] 상기 회선 차단부는, 주기적으로 상기 보안 통신 장치 제어 서버에서 상기 식별된 장치의 상태를 확인할 수 있다.
- [13] 상기 회선 정보는, 상기 네트워크 접속 장치의 포트 번호 및 해당 포트 번호에 연결된 장치의 식별정보를 포함하고, 상기 상태 확인부는, 상기 회선 정보에 포함된 상기 장치의 식별정보를 이용하여 상기 식별된 장치의 상태를 확인하며, 상기 회선 차단부는, 상기 네트워크 접속 장치로 상기 포트 번호의 차단 명령을 전송할 수 있다.
- [14] 상기 목적을 달성하기 위한 본 발명의 다른 측면에 따른, 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 회선 제어 서버에서 관리하는 방법은, 상기 네트워크

접속 장치로부터 회선 정보를 수집하는 단계; 상기 수집된 회선 정보에서 네트워크 접속 장치에 연결된 장치를 식별하고, 식별된 장치의 상태를 보안 통신 장치 제어 서버에서 확인하는 단계; 및 상기 식별된 장치의 상태 확인 결과에 따라 상기 네트워크 접속 장치의 회선을 선택적으로 차단하는 단계를 포함한다.

[15] 상기 차단하는 단계는, 상기 보안 통신 장치 제어 서버에서 확인된 상기 식별된 장치의 상태가 정상 상태인 경우, 상기 네트워크 접속 장치의 회선을 유지하고 비정상 상태인 경우 회선을 차단할 수 있다.

[16] 상기 보안 통신 장치는, 상기 사용자 단말과 연결될 경우 상기 보안 통신 장치 제어 서버로 주기적으로 상태 정보를 전송하고, 상기 사용자 단말과의 연결이 해제되는 경우 연결 해제 메시지를 상기 보안 통신 장치 제어 서버로 전송하고 상태 정보의 주기적 전송을 중단할 수 있다.

[17] 상기 확인하는 단계는, 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로 상기 연결 해제 메시지가 수신되지 않고 상태 정보의 전송 주기 동안 상태 정보가 수신되지 않은 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신할 수 있다.

[18] 상기 확인하는 단계는, 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로의 상태 정보의 주기적 전송 기록이 없는 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신할 수 있다.

발명의 효과

[19] 본 발명은, 보안 통신 장치를 제거하거나 사용자 단말을 상기 보안 통신 장치인 것처럼 변조하여 직접 사용자 단말로 인터넷 접속을 하는 것을 차단하여 기업, 군부대 등의 보안이 중요한 그룹의 보안을 강화할 수 있다.

도면의 간단한 설명

[20] 도 1은 본 발명의 일 실시예에 따른 인터넷 접속을 통제하는 시스템을 나타낸 도면이다.

[21] 도 2는 본 발명의 일 실시예에 따른 회선 제어 서버의 구성을 나타낸 도면이다.

[22] 도 3은 본 발명의 일 실시예에 따른 회선 제어 방법을 설명하는 흐름도이다.

[23] 도 4는 본 발명의 다른 실시예에 따른 회선 제어 방법을 설명하는 흐름도이다.

발명의 실시를 위한 형태

[24] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일 실시예를 상세히 설명하기로 한다.

[25] 도 1은 본 발명의 일 실시예에 따른 인터넷 접속을 통제하는 시스템을 나타낸

도면이다.

- [26] 도 1을 참조하면, 본 실시예에 따른 시스템은, 보안 통신 장치(110), 네트워크 접속 장치(120), DHCP 서버(130), 회선 제어 서버(140), 보안 통신 장치 제어 서버(150), 통신망(160) 및 사용자 단말(170)을 포함한다.
- [27] 사용자 단말(170)은, 인터넷 통신이 가능한 단말로서, 예를 들어, 노트북, 데스크톱 컴퓨터, 태블릿 PC 등을 포함한다. 바람직하게, 본 실시예에서 사용자 단말(170)은 일반적인 이동통신망을 통해서는 통신을 할 수 없고, 무선랜, 또는 유선 인터페이스를 통한 인터넷 통신이 가능한 단말인 것이 바람직하다. 그러나 여기에 제한된 것은 아니며, 보안 통신 장치(110)가 설치되는 지역이 이동통신망의 서비스 지역이 아닌 경우, 사용자 단말(170)은 보안 통신 장치(110)와 연결될 수 있는 스마트폰 등도 포함할 수 있다.
- [28] 보안 통신 장치(110)는 LAN 케이블을 통해 네트워크 접속 장치(120)와 연결되고 사용자 단말(170)과는 무선 또는 유선으로 연결되어 사용자 단말(170)의 네트워크 접속 장치(120)로의 접속을 통제한다. 보안 통신 장치(110)는 프로세서(CPU), 운영체제(OS) 및 메모리를 구비한 하드웨어 보안 장치로서, 사용자 단말(170)에 연결되면 전력을 공급받아 부팅하고, 사용자 단말(170)과 독립적인 시스템으로 동작한다. 또한 보안 통신 장치(110)는 사용자 단말(170)에 연결되면 사용자 단말(170)의 일부 기능을 비활성화(disable)시킬 수 있다. 예를 들어, 사용자 단말(170)의 통신 기능을 비활성화시킬 수 있다.
- [29] 보안 통신 장치(110)는 사용자 단말(170)이 연결되어 전력을 공급받아 부팅되면, 상태 정보를 주기적으로 보안 통신 장치 제어 서버(150)로 전송한다. 그리고 보안 통신 장치(110)는 사용자 단말(170)과 정상적으로 연결이 해제되면, 연결 해제 메시지를 보안 통신 장치 제어 서버(140)로 전송하고, 보안 통신 장치(110)는 더 이상 전력 공급이 중단되므로 상태 정보를 전송하지 않는다. 상태 정보에는, 전송 시간, 고유 식별코드, 보안 통신 장치(110)의 MAC 주소 등을 포함한다.
- [30] 보안 통신 장치(110)는 통신 인터페이스를 통해 사용자 단말(170)과 연결될 수 있다. 통신 인터페이스는 다양한 유무선 인터페이스 중에서 선택될 수 있다. 예를 들면, 통신 인터페이스는 USB 인터페이스일 수 있으나, 사용자 단말(170)과 연결될 수 있는 다른 통신 인터페이스도 가능하다. 또한, 보안 통신 장치(110)는 네트워크 접속 장치(120)와 연결이 가능한 통신 인터페이스를 더 포함하고, 예를 들어 유선 케이블로 통신망에 접속할 수 있는 유선 통신 인터페이스를 포함할 수 있다.
- [31] 보안 통신 장치(110)는 접속 허용 인터넷 주소의 리스트인 화이트 리스트를 메모리에 저장하고, 사용자 단말(170)이 상기 화이트 리스트에 있는 인터넷 주소로만 접속할 수 있도록 통제한다. 보안 통신 장치(110)는 보안 통신 장치 제어 서버(150)로부터 화이트 리스트를 수신하여 업데이트할 수 있다. 또한 보안 통신 장치(110)는 생체 정보를 인식하는 센서를 포함하여 사용자의 생체 정보를

인식하고, 미리 저장된 생체 정보와 비교하여 일치할 경우에 사용을 가능하게 할 수 있다.

- [32] 네트워크 접속 장치(120)는 보안 통신 장치(110)와 통신망(160)을 연결하는 장비로서, L2 스위치, L3 스위치 등을 포함한다. L2 스위치는, OSI(Open System Interconnection) 7 레이어 모델 중 데이터 링크 레이어의 역할을 수행하며, 구체적으로, 물리적인 네트워크 사이의 데이터 전송을 담당하고, 물리적 어드레싱, 오류 검출, 프레임의 전달 및 데이터의 흐름 제어를 관리한다. L2 스위치의 하나의 포트에는 하나의 인터넷 회선이 연결될 수 있다. L2 스위치는 각 포트에 연결된 장치들의 MAC 주소를 획득하고, 이를 MAC 테이블에 저장한다. 따라서 본 실시예에서는 MAC 테이블에 보안 통신 장치(110)의 MAC 주소 및 포트 번호가 매칭되어 저장된다. L2 스위치는 통신망(160)을 통해 프레임이 수신되면, MAC 테이블을 참조하여, 어떤 포트에 해당 프레임을 보낼 것인지를 결정한다. L3 스위치는 OSI 7 레이어 모델 중 네트워크 레이어의 역할을 수행하며, 보안 통신 장치(110) 및 사용자 단말(170)의 IP 주소를 MAC 주소에 대응시키기 위해 ARP(Address Resolution Protocol) 프로토콜을 사용하고 이러한 내용을 ARP 테이블에 저장한다. 즉, ARP 테이블을 조회해보면 장치들의 IP 주소와 그에 대응하는 MAC 주소를 확인할 수 있다.
- [33] DHCP(Dynamic Host Configuration Protocol) 서버(130)는 IP 주소들의 풀(Pool)을 관리하고 IP 주소 할당 요청을 수신하면 상기 풀에서 IP 주소를 검색하여 할당한다. 본 실시예에서 사용자 단말(170)이 보안 통신 장치(110)에 연결되어 IP 주소 할당 요청이 수신되면 상기 보안 통신 장치(110) 및 상기 사용자 단말(170)로 IP 주소를 할당한다. IP 주소 할당 요청에는 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소가 포함될 수 있다. DHCP 서버(130)는 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소를 회선 제어 서버(140)로 전송하여 인증을 요청하고 인증 성공 응답이 수신될 때 IP 주소를 할당할 수 있다. 또는 DHCP 서버(130)는 보안 통신 장치(110)의 MAC 주소만을 회선 제어 서버(140)로 전송하여 인증을 요청할 수도 있다.
- [34] 보안 통신 장치 제어 서버(150)는 상기 보안 통신 장치(110)를 제어한다. 보안 통신 장치 제어 서버(150)는, 보안 통신 장치별로 접속 허용 인터넷 주소의 리스트인 화이트 리스트를 저장 관리하고, 보안 통신 장치(110)의 접속시 화이트 리스트를 보안 통신 장치(110)로 전송하고 업데이트할 수 있다. 실시 형태에 따라, 보안 통신 장치별로 복수의 사용자 단말의 식별정보(예, MAC 주소)를 저장하고, 각 사용자 단말마다 화이트 리스트를 다르게 할 수 있다.
- [35] 보안 통신 장치 제어 서버(150)는 전력이 공급된 보안 통신 장치(110)로부터 주기적으로 상태 정보를 수신하여 저장한다. 저장되는 상태 정보에는 수신 시간, 보안 통신 장치(110)의 고유 식별코드, MAC 주소 등을 포함한다. 보안 통신 장치 제어 서버(150)는, 회선 제어 서버(140)로부터 특정 보안 통신 장치(110)에 대한 상태 정보 요청을 수신하면, 해당하는 특정 보안 통신 장치(110)의 상태 정보를

검색하고, 검색 결과에 따라 플래그를 포함하는 상태 정보 응답을 회신한다. 여기서 플래그는 정상 플래그 또는 비정상 플래그를 포함한다. 정상 플래그는, 보안 통신 장치(110)가 정상적으로 네트워크 접속 장치(120)에 연결되어 있음을 나타내고, 비정상 플래그는 보안 통신 장치(110)가 네트워크 접속 장치(120)에 정상적으로 연결되어 있지 않음을 나타낸다. 비정상 플래그의 경우는, 예를 들어 전력이 공급된 보안 통신 장치(110)가 네트워크 접속 장치(120)에 정상적으로 연결되어 있다가 강제로 네트워크 접속 장치(120)로부터 제거되는 경우이다. 보안 통신 장치 제어 서버(150)는, 보안 통신 장치(110)의 상태 정보 수신 주기가 도래했음에도 더 이상 상태 정보가 수신되지 않고 연결 해제 메시지도 수신되지 않은 경우, 비정상 플래그를 설정한다. 또는, 보안 통신 장치 제어 서버(150)는, 상태 정보가 수신되지 않은 보안 통신 장치(110)에 대한 상태 정보 요청이 수신되는 경우에도 비정상 플래그를 포함하는 상태 정보 응답을 회신한다.

- [36] 보안 통신 장치 제어 서버(150)는, 회선 제어 서버(140)로부터 특정 보안 통신 장치(110)에 대한 상태 정보 요청을 수신하면, 해당하는 특정 보안 통신 장치(110)의 상태 정보를 검색하고 정상 플래그 또는 비정상 플래그를 포함하는 상태 정보 응답을 회선 제어 서버(140)로 전송한다. 상태 정보 요청에는 보안 통신 장치(110)의 MAC 주소 또는 IP 주소가 포함될 수 있다.
- [37] 회선 제어 서버(140)는, 보안 통신 장치(110)를 이용한 인터넷 접속 통제 서비스에 가입한 가입자의 정보를 저장한다. 가입자의 정보는, 예를 들어, 기업명, 네트워크 접속 장치(120)의 정보(IP 주소, MAC 주소, 포트 번호 등), 보안 통신 장치(110)의 식별정보(예, MAC 주소), 기업 내 인터넷 사용이 허가된 사용자 단말들의 식별정보(예, MAC 주소)를 포함할 수 있다.
- [38] 회선 제어 서버(140)는, DHCP 서버(130)로부터 IP 주소 할당을 위한 인증 요청이 수신되면, 상기 가입자 정보를 기초로 인증 응답을 회신한다. 인증 요청에는, 보안 통신 장치(110)의 식별정보가 포함될 수 있고, 회선 제어 서버(140)는 인증 요청에 포함된 보안 통신 장치(110)의 식별정보가 가입자 정보와 일치하는 경우에 인증 성공 응답을 회신한다. 또한 인증 요청에는, 사용자 단말(170)의 식별정보가 더 포함될 수 있고, 회선 제어 서버(140)는 보안 통신 장치(110)의 식별정보 및 사용자 단말(170)의 식별정보가 모두 가입자 정보와 일치하는 경우에 인증 성공 응답을 회신할 수 있다.
- [39] 회선 제어 서버(140)는, 주기적으로 네트워크 접속 장치(120)의 회선 정보를 수집한다. 여기서 회선 정보는, 네트워크 접속 장치(120)의 IP 주소, 포트 번호, 그리고 각 포트 번호별 접속되어 있는 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함한다.
- [40] 회선 제어 서버(140)는, 상기 수집된 회선 정보에서 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)를 식별하고, 식별된 보안 통신 장치(110)에 대한 상태 정보를 보안 통신 장치 제어 서버(150)로 요청하여 상태 정보 응답을 수신한다. 회선 제어 서버(140)는, 상기 상태 정보 응답에 기초하여 상기

네트워크 접속 장치(120)의 회선을 선택적으로 차단한다.

[41] 구체적으로, 회선 제어 서버(140)는, 상기 식별된 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함하는 상태 정보 요청을 보안 통신 장치 제어 서버(150)로 전송한다. 그리고 회선 제어 서버(140)는 보안 통신 장치 제어 서버(150)로부터 상태 정보 응답을 수신하고, 상태 정보 응답에 포함된 플래그에 따라 상기 네트워크 접속 장치(120)의 회선을 선택적으로 차단한다. 정상 플래그가 있는 경우, 회선 제어 서버(140)는 네트워크 접속 장치(120)의 회선을 유지하고, 비정상 플래그가 있는 경우, 네트워크 접속 장치(120)로 특정 포트에 대한 차단 명령을 전송한다.

[42] 또한, 회선 제어 서버(140)는, 복수의 네트워크 접속 장치(120)로부터 수집된 회선 정보에서 동일한 보안 통신 장치(110)의 MAC 주소가 발견되는 경우 부정 사용이라 판단하여 해당하는 복수의 네트워크 접속 장치(120)로 해당 MAC 주소가 발견된 포트에 대한 차단 명령을 전송할 수 있다. 예를 들어, 제 1 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)에 제 1 사용자 단말을 연결한 후에, 다른 제 2 네트워크 접속 장치(120)에 MAC 주소를 변조한 제 2 사용자 단말을 연결하여 인터넷을 이용할 수 있는데, 이러한 경우에 제 1, 2 네트워크 접속 장치(120)의 해당하는 포트는 접속이 차단된다.

[43] 도 2는 본 발명의 일 실시예에 따른 회선 제어 서버의 구성을 나타낸 도면이다.

[44] 도 2에 도시된 회선 제어 서버(140)는, 메모리, 메모리 제어기, 하나 이상의 프로세서(CPU), 주변 인터페이스, 입출력(I/O) 서브시스템, 디스플레이 장치, 입력 장치 및 통신 회로를 포함할 수 있다. 이러한 구성요소는 하나 이상의 통신 버스 또는 신호선을 통하여 통신한다. 이러한 여러 구성요소는 하나 이상의 신호 처리 및/또는 애플리케이션 전용 집적 회로(application specific integrated circuit)를 포함하여, 하드웨어, 소프트웨어 또는 하드웨어와 소프트웨어 둘의 조합으로 구현될 수 있다.

[45] 메모리는 고속 랜덤 액세스 메모리를 포함할 수 있고, 또한 하나 이상의 자기 디스크 저장 장치, 플래시 메모리 장치와 같은 불휘발성 메모리, 또는 다른 불휘발성 반도체 메모리장치를 포함할 수 있다. 프로세서 및 주변 인터페이스와 같은 서버의 다른 구성요소에 의한 메모리로의 액세스는 메모리 제어기에 의하여 제어될 수 있다. 메모리에는, 보안 통신 장치(110)를 이용한 인터넷 접속 통제 서비스에 가입한 가입자의 정보가 저장된다. 가입자 정보는, 입력 장치에 의해 입력될 수 있다. 가입자의 정보는, 예를 들어, 기업명, 네트워크 접속 장치(120)의 정보(IP 주소, MAC 주소, 포트 번호 등), 보안 통신 장치(110)의 식별정보(예, MAC 주소), 기업 내 인터넷 사용이 허가된 사용자 단말들의 식별정보(예, MAC 주소)를 포함할 수 있다.

[46] 주변 인터페이스는 서버의 입출력 주변 장치를 프로세서 및 메모리와 연결한다. 하나 이상의 프로세서는 다양한 소프트웨어 프로그램 및/또는 메모리에 저장되어 있는 명령어 세트를 실행하여 시스템을 위한 여러 기능을

수행하고 데이터를 처리한다. 일부 실시예에서, 소프트웨어 구성요소는 운영 체제, 그래픽 모듈(명령어 세트), 본 발명을 위한 동작을 수행하기 위한 프로그램이 탑재(설치)된다. 운영 체제는, 예를 들어, 다윈(Darwin), RTXC, LINUX, UNIX, OS X, WINDOWS 또는 VxWorks, 안드로이드, iOS 등과 같은 내장 운영체제일 수 있고, 일반적인 시스템 태스크(task)(예를 들어, 메모리 관리, 저장 장치 제어, 전력 관리 등)를 제어 및 관리하는 다양한 소프트웨어 구성요소 및/또는 장치를 포함하고, 다양한 하드웨어와 소프트웨어 구성요소 사이의 통신을 촉진시킨다. 그래픽 모듈은 디스플레이 장치 상에 그래픽을 제공하고 표시하기 위한 주지의 여러 소프트웨어 구성요소를 포함한다.

"그래픽(graphics)"이란 용어는 텍스트, 웹 페이지, 아이콘(예컨대, 소프트 키를 포함하는 사용자 인터페이스 대상), 디지털 이미지, 비디오, 애니메이션 등을 제한 없이 포함하여, 표시될 수 있는 모든 대상을 포함한다. 일부 실시예에서, 주변 인터페이스, 프로세서 및 메모리 제어기는 칩과 같은 단일 칩 상에서 구현될 수 있다. 일부 다른 실시예에서, 이들은 별개의 칩으로 구현될 수 있다.

- [47] I/O 서브시스템은 디스플레이 장치, 입력 장치와 같은 장치의 입출력 주변장치와 주변 인터페이스 사이에 인터페이스를 제공한다. 디스플레이 장치는 LCD(liquid crystal display) 기술 또는 LPD(light emitting polymer display) 기술을 사용할 수 있고, 이러한 디스플레이 장치는 용량형, 저항형, 적외선형 등의 터치 디스플레이일 수 있다. 터치 디스플레이는 시스템과 사용자 사이에 출력 인터페이스 및 입력 인터페이스를 제공한다. 터치 디스플레이는 사용자에게 시각적인 출력을 표시한다. 시각적 출력은 텍스트, 그래픽, 비디오와 이들의 조합을 포함할 수 있다. 시각적 출력의 일부 또는 전부는 사용자 인터페이스 대상에 대응할 수 있다. 터치 디스플레이는 사용자 입력을 수용하는 터치 감지면을 형성한다. 프로세서는 시스템에 연관된 동작을 수행하고 명령어들을 수행하도록 구성된 프로세서로서, 예를 들어, 메모리로부터 검색된 명령어들을 이용하여, 시스템의 컴포넌트 간의 입력 및 출력 데이터의 수신과 조작을 제어할 수 있다.

- [48] 통신 회로는 이더넷 통신 회로 및 RF 회로를 포함할 수 있다. 이더넷 통신 회로는 유선 통신을 수행하고, RF 회로는 전자파를 송수신한다. RF 회로는 전기 신호를 전자파로 또는 그 반대로 변환하며 이 전자파를 통하여 통신 네트워크, 다른 이동형 게이트웨이 및 통신 장치와 통신한다.

- [49] 도 2를 참조하면, 회선 제어 서버(140)는, 인증부(210), 회선 정보 수집부(220), 상태 확인부(230) 및 회선 차단부(240)를 포함할 수 있다. 이러한 구성요소는 프로그램으로 제작되어 메모리에 저장되어 프로세서에 의해 동작될 수 있고, 또는 소프트웨어 및 하드웨어의 조합으로 제작될 수도 있다.

- [50] 인증부(210)는, 네트워크 접속 장치(120)에 연결된 장치에 대한 IP 주소 할당 여부를 결정한다. 구체적으로, 인증부(210)는, DHCP 서버(130)로부터 IP 주소 할당을 위한 인증 요청이 수신되면, 메모리에 저장된 가입자 정보를 기초로 인증

응답을 회신한다. 인증 요청에는, 보안 통신 장치(110)의 식별정보가 포함될 수 있고, 인증부(210)는 인증 요청에 포함된 보안 통신 장치(110)의 식별정보가 가입자 정보와 일치하는 경우에 인증 성공 응답을 회신한다. 또한 인증 요청에는, 사용자 단말(170)의 식별정보가 더 포함될 수 있고, 인증부(210)는 보안 통신 장치(110)의 식별정보 및 사용자 단말(170)의 식별정보가 모두 가입자 정보와 일치하는 경우에 인증 성공 응답을 회신할 수 있다.

- [51] 회선 정보 수집부(220)는, 주기적으로 네트워크 접속 장치(120)의 회선 정보를 수집한다. 여기서 회선 정보는, 네트워크 접속 장치(120)의 IP 주소, 포트 번호, 그리고 각 포트 번호별 접속되어 있는 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함한다.
- [52] 상태 확인부(230)는, 상기 수집된 회선 정보에서 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)를 식별하고, 식별된 보안 통신 장치(110)에 대한 상태 정보를 보안 통신 장치 제어 서버(150)에서 확인한다. 상태 확인부(230)는, 상기 식별된 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함하는 상태 정보 요청을 보안 통신 장치 제어 서버(150)로 전송하고, 이에 대한 상태 정보 응답을 수신한다.
- [53] 회선 차단부(240)는, 상기 상태 정보 응답에 포함된 플래그에 따라 상기 네트워크 접속 장치(120)의 회선을 선택적으로 차단한다. 정상 플래그가 있는 경우, 회선 차단부(240)는 네트워크 접속 장치(120)의 회선을 유지하고, 비정상 플래그가 있는 경우, 네트워크 접속 장치(120)로 특정 포트에 대한 차단 명령을 전송한다.
- [54] 또한, 회선 차단부(240)는, 복수의 네트워크 접속 장치(120)로부터 수집된 회선 정보에서 동일한 보안 통신 장치(110)의 MAC 주소가 발견되는 경우 부정 사용이라 판단하여 해당하는 복수의 네트워크 접속 장치(120)로 해당 MAC 주소가 발견된 포트에 대한 차단 명령을 전송할 수 있다. 예를 들어, 제 1 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)에 제 1 사용자 단말을 연결한 후에, 다른 제 2 네트워크 접속 장치(120)에 MAC 주소를 변조한 제 2 사용자 단말을 연결하여 인터넷을 이용할 수 있는데, 이러한 경우에 제 1, 2 네트워크 접속 장치(120)의 해당하는 포트는 접속이 차단된다.
- [55] 도 3은 본 발명의 일 실시예에 따른 회선 제어 방법을 설명하는 흐름도이다.
- [56] 도 3을 참조하면, 사용자는 네트워크 접속 장치(120)와 유선 케이블로 연결되어 있는 보안 통신 장치(110)를 사용자 단말(170)에 연결한다(S301). 예를 들어, 보안 통신 장치(110)는 USB 통신을 지원하여 사용자 단말(170)의 USB 포트에 연결될 수 있다.
- [57] 사용자 단말(170)은 보안 통신 장치(110)로 전력을 공급하고, 보안 통신 장치(110)는 부팅되어 IP 주소 할당 요청을 DHCP 서버(130)로 전송한다(S303). IP 주소 할당 요청에는 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소가 포함된다.

- [58] DHCP 서버(130)는, IP 주소를 할당하기에 앞서, 상기 IP 주소 할당 요청에 포함된 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소를 포함하는 인증 요청을 회선 제어 서버(140)로 전송한다(S305). 회선 제어 서버(140)는, 서비스에 가입된 가입자의 정보로서, 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소를 저장하고 있으므로, 상기 인증 요청에 포함된 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소와 상기 가입자의 정보를 비교하여 인증을 수행한다.
- [59] 회선 제어 서버(140)는 인증에 성공하는 경우 인증 성공 응답을 DHCP 서버(130)로 회신하고, 인증에 실패하는 경우 인증 실패 응답을 DHCP 서버(130)로 회신한다(S307). 본 실시예에서는 인증에 성공한 것으로 설명한다. 실시 형태에 따라, 단계 S305에서 인증 요청에 사용자 단말(170)의 MAC 주소가 포함되어 있지 않을 수 있다. 이 경우, 회선 제어 서버(140)는, 보안 통신 장치(110)의 MAC 주소만을 상기 가입자의 정보와 비교하여 인증을 수행할 수 있다. 이 실시 형태는, 인터넷을 이용할 수 있는 사용자 단말(170)을 지정하지 않은 실시예이다.
- [60] 단계 S305 및 단계 S307을 통해, 지정되지 않은 사용자 단말(170)을 이용하거나, 또는 지정되지 않은 보안 통신 장치(110)를 이용하여 인터넷을 이용하는 것을 방지할 수 있다.
- [61] 인증 성공 응답을 수신한 DHCP 서버(130)는, 보안 통신 장치(110) 및 사용자 단말(170)로 IP 주소를 할당한다(S309, S311). IP 주소를 할당받은 보안 통신 장치(110)는 주기적으로 상태 정보를 보안 통신 장치 제어 서버(140)로 전송한다(S313). 상태 정보는, 전송하는 시간, 고유 식별코드, 보안 통신 장치(110)의 MAC 주소 등을 포함한다.
- [62] 한편, 회선 제어 서버(140)는 주기적으로 네트워크 접속 장치(120)로부터 회선 정보를 수집한다(S315). 여기서 회선 정보는, 네트워크 접속 장치(120)의 IP 주소, 포트 번호, 그리고 각 포트 번호별 접속되어 있는 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함한다.
- [63] 회선 제어 서버(140)는, 상기 수집된 회선 정보에서 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)를 식별하고, 식별된 보안 통신 장치(110)에 대한 상태 정보 요청을 보안 통신 장치 제어 서버(150)로 전송한다(S317). 이때 상태 정보 요청에는 상기 식별된 보안 통신 장치(110)의 식별정보(예, MAC 주소, IP 주소)를 포함한다.
- [64] 보안 통신 장치 제어 서버(150)는, 상기 식별된 보안 통신 장치(110)의 식별정보를 이용하여 대응하는 상태 정보를 검색하고 그 검색된 상태 정보를 포함하는 상태 정보 응답을 회선 제어 서버(140)로 전송한다(S319). 상태 정보 응답에는 상기 식별된 보안 통신 장치(110)가 정상적으로 접속되어 있음을 나타내는 정상 플래그가 포함될 수 있다. 따라서 회선 제어 서버(140)는 네트워크 접속 장치(120)의 회선을 차단하지 않고 유지한다.
- [65] 보안 통신 장치(110)가 정상적으로 종료되지 않고 강제로 네트워크 접속

장치(120)와의 연결이 해제될 수 있다. 예컨대, 사용자가 악의적인 목적으로 보안 통신 장치(110)를 제거할 수 있다(S323). 이와 같이 보안 통신 장치(110)가 제거되면, 정상적인 연결 해제 메시지가 보안 통신 장치 제어 서버(150)로 전송되지 않는다.

[66] 따라서, 보안 통신 장치 제어 서버(150)에는 상태 정보 수신 주기가 도래함에도 더 이상 상태 정보가 수신되지 않고 연결 해제 메시지도 수신되지 않았으므로 비정상적으로 연결이 해제된 것으로 판단하여 이에 대한 비정상 플래그를 포함하는 상태 정보 응답을 회선 제어 서버(140)로 전송한다(S325). 그리고 회선 제어 서버(140)는 네트워크 접속 장치(120)로 보안 통신 장치(110)가 연결되어 있던 회선, 즉 포트를 차단하는 명령을 전송한다(S327). 따라서 보안 통신 장치(110)가 강제로 제거된 회선으로는 더 이상의 접속이 불가능해져, 보안 통신 장치(110) 없이 사용자 단말(170)을 직접 네트워크 접속 장치(120)에 연결하여 인터넷을 이용할 수 없다.

[67] 도 4는 본 발명의 다른 실시예에 따른 회선 제어 방법을 설명하는 흐름도이다.

[68] 도 4를 참조하면, 사용자는 보안 통신 장치(110)와 동일한 MAC 주소를 갖도록 사용자 단말(170)의 MAC 주소를 변조할 수 있다(S401). 그리고 사용자는 사용자 단말(170)을 직접 네트워크 접속 장치(120)에 연결한다(S403). 사용자 단말(170)은, IP 주소 할당 요청을 DHCP 서버(130)로 전송한다(S405). IP 주소 할당 요청에는 사용자 단말(170)의 MAC 주소가 포함된다.

[69] DHCP 서버(130)는, IP 주소를 할당하기에 앞서, 상기 IP 주소 할당 요청에 포함된 사용자 단말(170)의 MAC 주소를 포함하는 인증 요청을 회선 제어 서버(140)로 전송한다(S407). 회선 제어 서버(140)는, 서비스에 가입된 가입자의 정보로서, 사용자 단말(170) 및 보안 통신 장치(110)의 MAC 주소를 저장하고 있고, 상기 인증 요청에 포함된 사용자 단말(170)의 MAC 주소는 보안 통신 장치(110)의 MAC 주소와 동일하므로, 회선 제어 서버(140)는 인증 성공 응답을 DHCP 서버(130)로 전송한다(S409).

[70] 인증 성공 응답을 수신한 DHCP 서버(130)는, 사용자 단말(170)로 IP 주소를 할당한다(S411). 사용자 단말(170)이 직접 네트워크 접속 장치(120)에 연결하였으므로, 보안 통신 장치(110)는 상태 정보를 보안 통신 장치 제어 서버(140)로 전송하지 않는다.

[71] 한편, 회선 제어 서버(140)는 주기적으로 네트워크 접속 장치(120)로부터 회선 정보를 수집한다(S413). 여기서 회선 정보는, 네트워크 접속 장치(120)의 IP 주소, 포트 번호, 그리고 각 포트 번호별 접속되어 있는 장치의 식별정보(예, MAC 주소, IP 주소)를 포함한다. 본 실시예에서는 특정 포트에 접속되어 있는 장치의 식별정보로서 사용자 단말(170)의 식별정보가 포함된다.

[72] 회선 제어 서버(140)는, 상기 수집된 회선 정보에서 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)를 식별한다. 본 실시예에서는 보안 통신 장치(110) 없이 사용자 단말(170)이 직접 네트워크 접속 장치(120)에 연결되어 있고, 사용자

단말(170)의 MAC 주소는 보안 통신 장치(110)의 MAC 주소와 동일하므로, 사용자 단말(170)을 보안 통신 장치(110)인 것으로 식별한다. 회선 제어 서버(140)는 보안 통신 장치(110), 즉 사용자 단말(170)에 대한 상태 정보 요청을 보안 통신 장치 제어 서버(150)로 전송한다(S415). 이때 상태 정보 요청에는 사용자 단말(170)의 식별정보(예, MAC 주소, IP 주소)를 포함한다.

- [73] 보안 통신 장치(110)는 상태 정보를 보안 통신 장치 제어 서버(140)로 전송하지 않았으므로, 보안 통신 장치 제어 서버(150)에는, 사용자 단말(170)의 식별정보(예, MAC 주소, IP 주소)에 대응하는 상태 정보가 없다. 따라서 보안 통신 장치 제어 서버(150)는 비정상 플래그를 포함하는 상태 정보 응답을 회선 제어 서버(140)로 전송한다(S417). 비정상 플래그를 수신하였으므로, 회선 제어 서버(140)는 네트워크 접속 장치(120)로 사용자 단말(170)이 연결되어 있는 회선, 즉 포트를 차단하는 명령을 전송한다(S419). 따라서 MAC 주소를 변조하여 접속한 사용자 단말(170)은 더 이상 인터넷을 이용할 수 없다.
- [74] 도 3 및 도 4를 참조하여 설명한 실시예는, 하나의 네트워크 접속 장치(120)에서의 부정 사용의 예를 설명한다. 다른 실시예로서, 제 1 네트워크 접속 장치(120)에 연결된 보안 통신 장치(110)에 제 1 사용자 단말을 연결한 후에, 다른 제 2 네트워크 접속 장치(120)에 MAC 주소를 변조한 제 2 사용자 단말을 연결하여 인터넷을 이용할 수 있다. 이 경우, 회선 제어 서버(140)는 도 4의 실시예에서와 같이 상태 정보 확인을 하지 않고, 회선 정보 수집을 할 때 서로 다른 복수의 네트워크 접속 장치(120)에서 동일한 MAC 주소가 발견되면 해당 복수의 네트워크 접속 장치(120)로 해당 MAC 주소가 발견된 포트에 대한 차단 명령을 전송할 수 있다.
- [75] 본 명세서는 많은 특징을 포함하는 반면, 그러한 특징은 본 발명의 범위 또는 특허청구범위를 제한하는 것으로 해석되어서는 안 된다. 또한, 본 명세서에서 개별적인 실시예에서 설명된 특징들은 단일 실시예에서 결합되어 구현될 수 있다. 반대로, 본 명세서에서 단일 실시예에서 설명된 다양한 특징들은 개별적으로 다양한 실시예에서 구현되거나, 적절히 결합되어 구현될 수 있다.
- [76] 도면에서 동작들이 특정한 순서로 설명되었으나, 그러한 동작들이 도시된 바와 같은 특정한 순서로 수행되는 것으로, 또는 일련의 연속된 순서, 또는 원하는 결과를 얻기 위해 모든 설명된 동작이 수행되는 것으로 이해되어서는 안 된다. 특정 환경에서 멀티태스킹 및 병렬 프로세싱이 유리할 수 있다. 아울러, 상술한 실시예에서 다양한 시스템 구성요소의 구분은 모든 실시예에서 그러한 구분을 요구하지 않는 것으로 이해되어야 한다. 상술한 프로그램 구성요소 및 시스템은 일반적으로 단일 소프트웨어 제품 또는 멀티플 소프트웨어 제품에 패키지로 구현될 수 있다.
- [77] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 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.

청구범위

- [청구항 1] 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 관리하기 위한 회선 제어 장치에 있어서,
상기 네트워크 접속 장치로부터 회선 정보를 수집하는 회선 정보 수집부;
상기 수집된 회선 정보에서 네트워크 접속 장치에 연결된 장치를 식별하고, 식별된 장치의 상태를 보안 통신 장치 제어 서버에서 확인하는 상태 확인부; 및
상기 식별된 장치의 상태 확인 결과에 따라 상기 네트워크 접속 장치의 회선을 선택적으로 차단하는 회선 차단부를 포함하는 회선 제어 장치.
- [청구항 2] 제 1 항에 있어서,
상기 회선 차단부는,
상기 보안 통신 장치 제어 서버에서 확인된 상기 식별된 장치의 상태가 정상 상태인 경우, 상기 네트워크 접속 장치의 회선을 유지하고 비정상 상태인 경우 회선을 차단하는 회선 제어 장치.
- [청구항 3] 제 2 항에 있어서,
상기 보안 통신 장치는,
상기 사용자 단말과 연결될 경우 상기 보안 통신 장치 제어 서버로 주기적으로 상태 정보를 전송하고, 상기 사용자 단말과의 연결이 해제되는 경우 연결 해제 메시지를 상기 보안 통신 장치 제어 서버로 전송하고 상태 정보의 주기적 전송을 중단하는 회선 제어 장치.
- [청구항 4] 제 3 항에 있어서,
상기 상태 확인부는,
상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로 상기 연결 해제 메시지가 수신되지 않고 상태 정보의 전송 주기 동안 상태 정보가 수신되지 않은 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신하는 회선 제어 장치.
- [청구항 5] 제 3 항에 있어서,
상기 상태 확인부는,
상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로의 상태 정보의 주기적 전송 기록이 없는 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신하는 회선 제어 장치.
- [청구항 6] 제 1 항 내지 제 5 항 중 어느 한 항에 있어서,
상기 회선 차단부는,
주기적으로 상기 보안 통신 장치 제어 서버에서 상기 식별된 장치의 상태를 확인하는 회선 제어 장치.
- [청구항 7] 제 1 항 내지 제 5 항 중 어느 한 항에 있어서,

상기 회선 정보는, 상기 네트워크 접속 장치의 포트 번호 및 해당 포트 번호에 연결된 장치의 식별정보를 포함하고,
 상기 상태 확인부는, 상기 회선 정보에 포함된 상기 장치의 식별정보를 이용하여 상기 식별된 장치의 상태를 확인하며,
 상기 회선 차단부는, 상기 네트워크 접속 장치로 상기 포트 번호의 차단 명령을 전송하는 회선 제어 장치.

[청구항 8] 사용자 단말과 네트워크 접속 장치 사이에서 상기 사용자 단말의 인터넷 네트워크 접속을 통제하는 보안 통신 장치를 회선 제어 서버에서 관리하는 방법에 있어서,
 상기 네트워크 접속 장치로부터 회선 정보를 수집하는 단계;
 상기 수집된 회선 정보에서 네트워크 접속 장치에 연결된 장치를 식별하고, 식별된 장치의 상태를 보안 통신 장치 제어 서버에서 확인하는 단계; 및
 상기 식별된 장치의 상태 확인 결과에 따라 상기 네트워크 접속 장치의 회선을 선택적으로 차단하는 단계를 포함하는 방법.

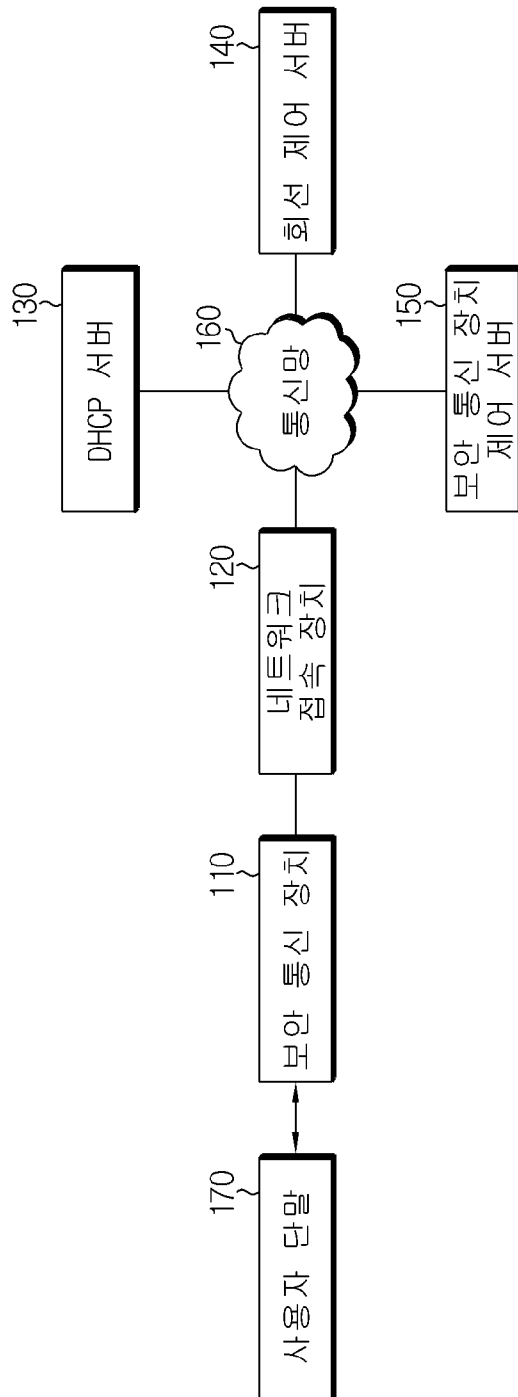
[청구항 9] 제 8 항에 있어서,
 상기 차단하는 단계는,
 상기 보안 통신 장치 제어 서버에서 확인된 상기 식별된 장치의 상태가 정상 상태인 경우, 상기 네트워크 접속 장치의 회선을 유지하고 비정상 상태인 경우 회선을 차단하는 방법.

[청구항 10] 제 9 항에 있어서,
 상기 보안 통신 장치는,
 상기 사용자 단말과 연결될 경우 상기 보안 통신 장치 제어 서버로 주기적으로 상태 정보를 전송하고, 상기 사용자 단말과의 연결이 해제되는 경우 연결 해제 메시지를 상기 보안 통신 장치 제어 서버로 전송하고 상태 정보의 주기적 전송을 중단하는 방법.

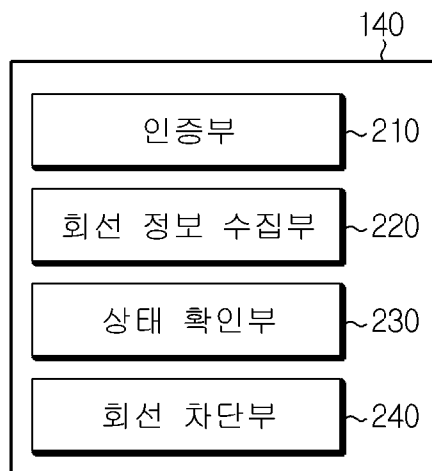
[청구항 11] 제 10 항에 있어서,
 상기 확인하는 단계는,
 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로 상기 연결 해제 메시지가 수신되지 않고 상태 정보의 전송 주기 동안 상태 정보가 수신되지 않은 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신하는 방법.

[청구항 12] 제 10 항에 있어서,
 상기 확인하는 단계는,
 상기 식별된 장치로부터 상기 보안 통신 장치 제어 서버로의 상태 정보의 주기적 전송 기록이 없는 경우, 상기 보안 통신 장치 제어 서버로부터 비정상 플래그를 포함하는 상태 정보 응답을 수신하는 방법.

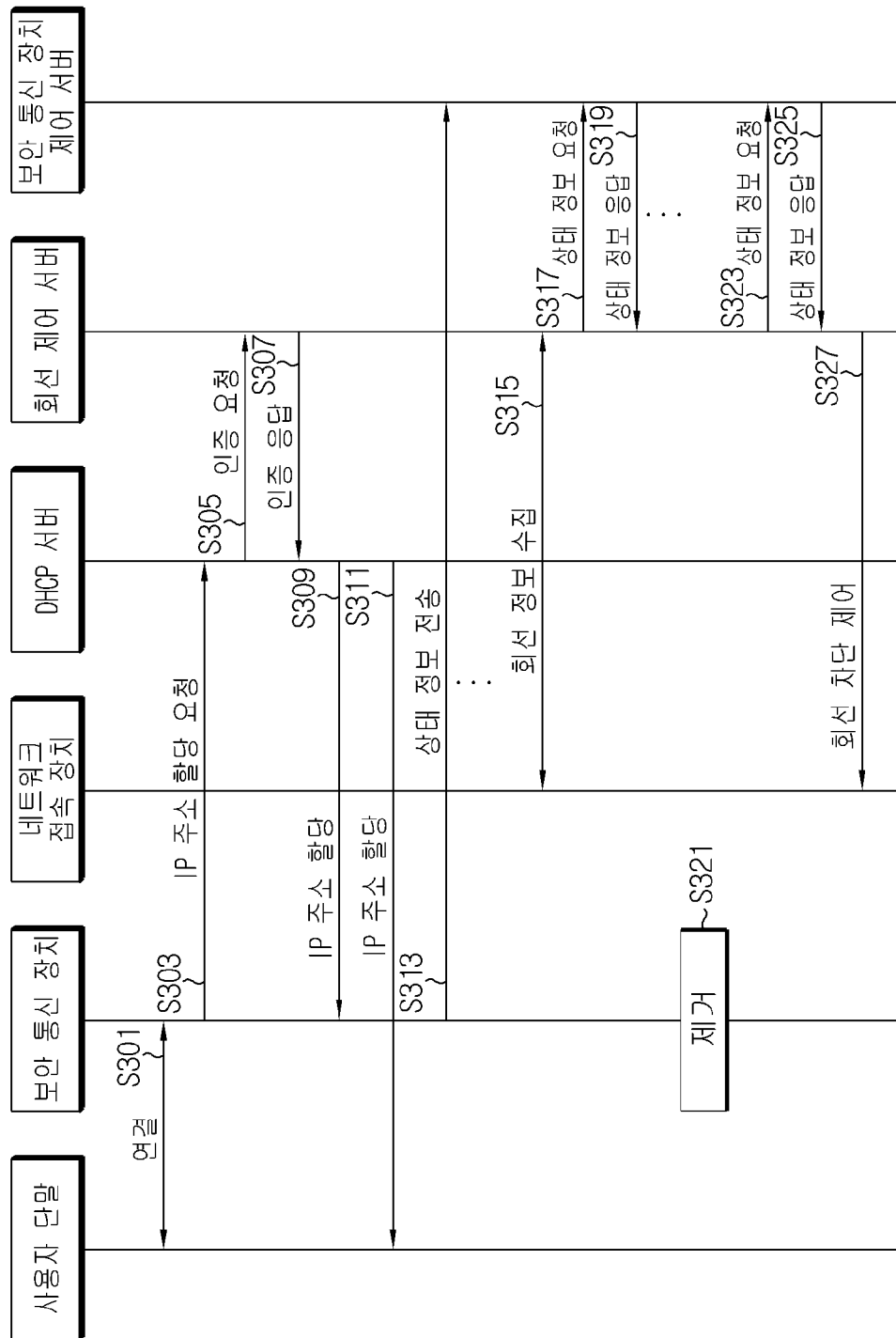
[도1]



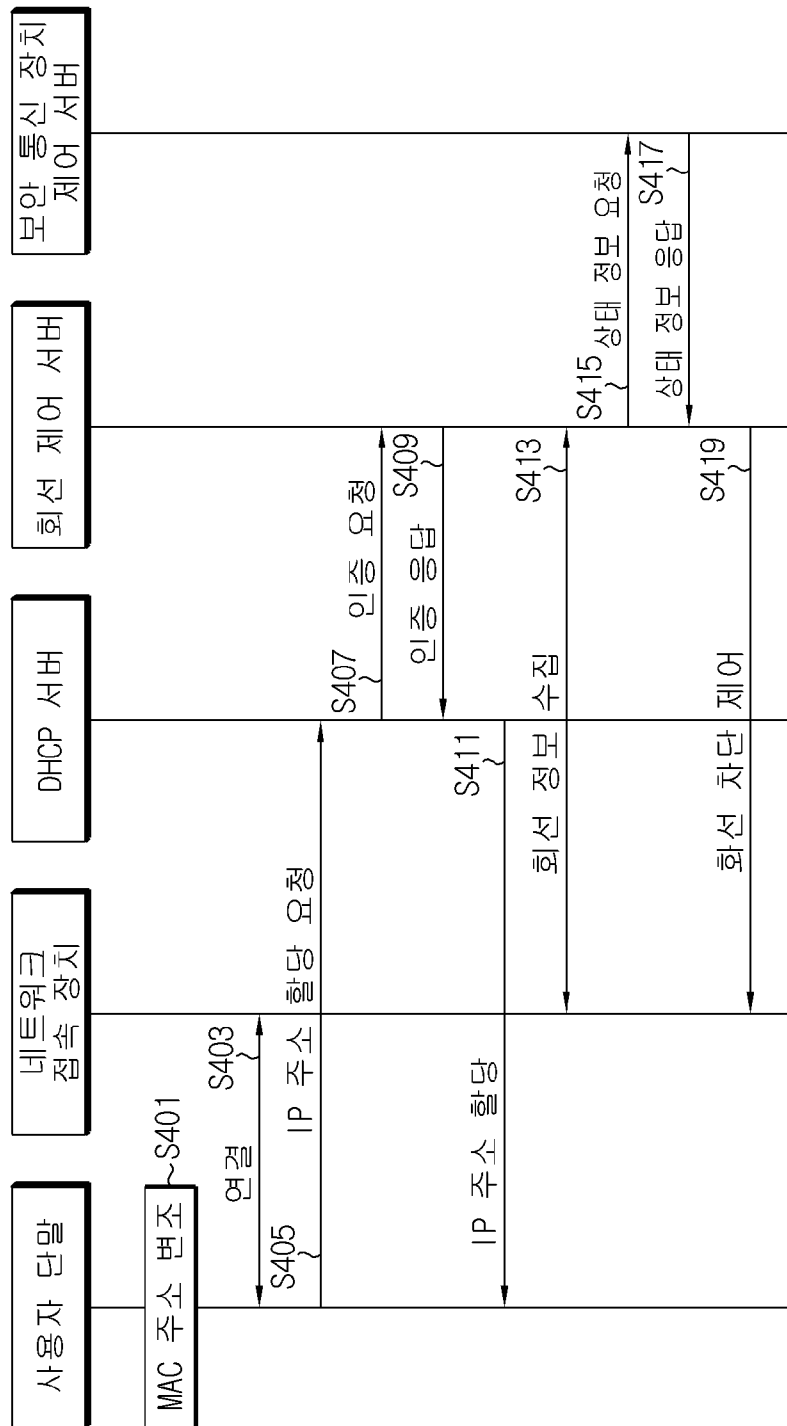
[도2]



[도3]



[도4]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/005428**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 21/20; H04L 12/26; H04L 12/66; H04L 9/32; H04W 12/08; H04L 9/00; H04L 12/28; G06F 13/00; G06F 21/00

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: terminal, connection control, block, periodic, connection release message

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2006-251851 A (QUALITY K.K.) 21 September 2006 See paragraphs [0062]-[0076], [0096]-[0097] and figures 1-4.	1-2,7-9
Y		6
A		3-5,10-12
Y	KR 10-2011-0008855 A (SAINT SECURITY CO., LTD.) 27 January 2011 See paragraphs [0024]-[0028] and figures 1-2.	6
A	KR 10-1486307 B1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 29 January 2015 See paragraphs [0029]-[0069] and figures 1-4.	1-12
A	KR 10-2010-0007109 A (SAMSUNG NETWORKS INC.) 22 January 2010 See paragraphs [0047]-[0081] and figures 4-6.	1-12
A	US 7861081 B2 (YEAP, Tet Hin et al.) 28 December 2010 See column 4, line 17-column 7, line 51 and figures 1-5.	1-12



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

21 AUGUST 2017 (21.08.2017)

Date of mailing of the international search report

22 AUGUST 2017 (22.08.2017)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-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/KR2017/005428

Patent document cited in search report	Publication date	Patent family member	Publication date
JP 2006-251851 A	21/09/2006	JP 3728536 B1	21/12/2005
KR 10-2011-0008855 A	27/01/2011	KR 10-1081992 B1	09/11/2011
KR 10-1486307 B1	29/01/2015	US 2015-0143454 A1	21/05/2015
KR 10-2010-0007109 A	22/01/2010	NONE	
US 7861081 B2	28/12/2010	CA 2552987 A1	06/10/2005
		CA 2552987 C	28/05/2013
		US 2005-0216747	29/09/2005
		A1 WO 2005-093542 A1	06/10/2005

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; G06F 21/20; H04L 12/26; H04L 12/66; H04L 9/32; H04W 12/08; H04L 9/00; H04L 12/28; G06F 13/00; G06F 21/00

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: 단말, 접속 통제, 차단, 주기적, 연결 해제 메시지

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	JP 2006-251851 A (QUALITY K.K.) 2006.09.21 단락 [0062]-[0076], [0096]-[0097] 및 도면 1-4 참조.	1-2, 7-9
Y		6
A		3-5, 10-12
Y	KR 10-2011-0008855 A ((주) 세인트 시큐리티) 2011.01.27 단락 [0024]-[0028] 및 도면 1-2 참조.	6
A	KR 10-1486307 B1 (한국전자통신연구원) 2015.01.29 단락 [0029]-[0069] 및 도면 1-4 참조.	1-12
A	KR 10-2010-0007109 A (삼성네트웍스 주식회사) 2010.01.22 단락 [0047]-[0081] 및 도면 4-6 참조.	1-12
A	US 7861081 B2 (TET HIN YEAP 등) 2010.12.28 컬럼 4, 라인 17 - 컬럼 7, 라인 51 및 도면 1-5 참조.	1-12

☐ 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 08월 21일 (21.08.2017)

국제조사보고서 발송일

2017년 08월 22일 (22.08.2017)

ISA/KR의 명칭 및 우편주소



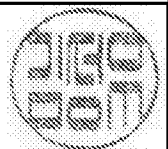
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

김성우

전화번호 +82-42-481-3348



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
JP 2006-251851 A	2006/09/21	JP 3728536 B1	2005/12/21
KR 10-2011-0008855 A	2011/01/27	KR 10-1081992 B1	2011/11/09
KR 10-1486307 B1	2015/01/29	US 2015-0143454 A1	2015/05/21
KR 10-2010-0007109 A	2010/01/22	없음	
US 7861081 B2	2010/12/28	CA 2552987 A1	2005/10/06
		CA 2552987 C	2013/05/28
		US 2005-0216747 A1	2005/09/29
		WO 2005-093542 A1	2005/10/06