(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년03월31일
(11) 등록번호 10-0817651
(24) 등록일자 2008년03월21일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2006-0014967
(22) 출원일자 2006년02월16일
심사청구일자 2006년02월16일
(65) 공개번호 10-2006-0128618
(43) 공개일자 2006년12월14일
(30) 우선권주장
JP-P-2005-00169403 2005년06월09일 일본(JP)
(56) 선행기술조사문헌
KR1020010043329 A*
(뒷면에 계속)

(73) 특허권자
가부시키가이샤 히타치세이사쿠쇼
일본국 도쿄토 치요다쿠 마루노우치 1초메 6반 6고
(72) 발명자
가또 다까또시
일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내
쯔네히로 다까시
일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내
하따노 또미히사
일본 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 가부시키가이샤히타치세이사쿠쇼 지적재산권본부 내
(74) 대리인
구영창, 장수길

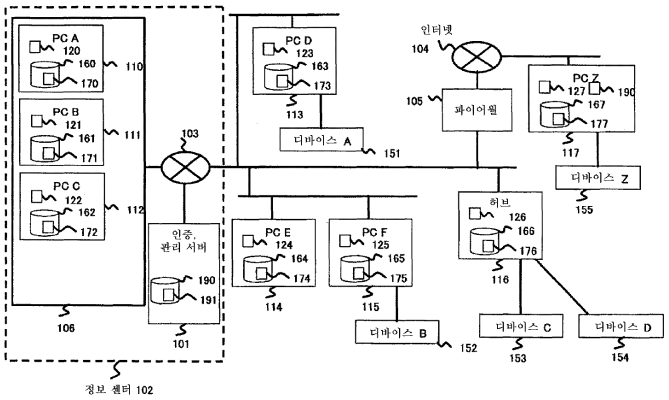
전체 청구항 수 : 총 17 항 심사관 : 안철용

(54) 디바이스 관리 시스템

(57) 요 약

서버 클라이언트 방식의 시스템에서, 이용자의 편리성을 저해하지 않고, 안전하게 디바이스를 공유하는 기능을 구비하는 디바이스 관리 시스템을 제공한다. 디바이스는, 이용자가 이용하는 단말기 혹은 네트워크에 접속된 허브에 접속한다. 단말기 등에 인스톨된 디바이스 드라이버 기능과 통신 기능을 구비하는 디바이스 관리 매니저와, 서버에 인스톨된 디바이스 드라이버 기능과 통신 기능을 갖는 가상 디바이스 매니저와, 디바이스의 액세스 권한을 관리하는 인증 서버에 의해 디바이스에의 액세스를 관리하면서 디바이스를 가상적으로 서버에 직접 접속된 것과 마찬가지로 이용 가능하게 한다.

대표도



(56) 선행기술조사문헌
JP2003233589 A
JP2003330801 A
US20020083342 A1
US6327613 B1
WO9945454 A1
*는 심사관에 의하여 인용된 문헌

특허청구의 범위

청구항 1

어플리케이션 프로그램을 실행하는 서버와, 상기 서버에 상기 어플리케이션 프로그램의 실행의 지시를 부여하고, 상기 서버로부터 실행 결과를 수취하는 클라이언트와, 상기 클라이언트를 인증하는 인증 서버가 네트워크로 접속된 시스템에서, 상기 클라이언트에 접속된 디바이스를, 상기 서버로부터 제어하는 디바이스 관리 시스템으로서,

상기 클라이언트는, 그 클라이언트에 접속하고 있는 디바이스의 디바이스 드라이버와 데이터를 송수신함과 함께 상기 서버와의 사이에서 그 데이터를 송수신하는 디바이스 관리 수단을 포함하고,

상기 인증 서버는, 상기 디바이스 관리 시스템 내의 각 디바이스의 이용 권한을 관리하는 디바이스 정보 유지 수단을 포함하고,

상기 서버는, 그 서버 내에서 동작하는 어플리케이션과, 상기 디바이스 관리 수단과의 사이에서 상기 네트워크를 통하여 행해지는 데이터의 송수신을, 상기 디바이스 정보 유지 수단에 유지되고 있는 상기 이용 권한에 따라서, 제어하는 가상 디바이스 관리 수단을 포함하고,

상기 가상 디바이스 관리 수단은, 상기 디바이스 관리 수단을 통하여, 상기 디바이스에 데이터를 송수신하고,

상기 클라이언트 상에서 실행되는 제2 어플리케이션은, 상기 디바이스 관리 수단을 통하여 상기 디바이스에 데이터를 송수신하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 2

어플리케이션 프로그램을 실행하는 서버와, 상기 서버에 상기 어플리케이션 프로그램의 실행의 지시를 부여하고, 상기 서버로부터 실행 결과를 수취하는 클라이언트와, 상기 클라이언트를 인증하는 인증 서버가 네트워크로 접속된 시스템에서, 상기 클라이언트에 접속된 디바이스를, 상기 서버로부터 제어하는 디바이스 관리 시스템으로서,

상기 클라이언트는, 그 클라이언트에 접속하고 있는 디바이스의 디바이스 드라이버와 데이터를 송수신함과 함께 상기 서버와의 사이에서 그 데이터를 송수신하는 디바이스 관리 수단을 포함하고,

상기 인증 서버는, 상기 디바이스 관리 시스템 내의 각 디바이스의 이용 권한을 관리하는 디바이스 정보 유지 수단을 포함하고,

상기 서버는, 그 서버 내에서 동작하는 어플리케이션과, 상기 디바이스 관리 수단과의 사이에서 상기 네트워크를 통하여 행해지는 데이터의 송수신을, 상기 디바이스 정보 유지 수단에 유지되고 있는 상기 이용 권한에 따라서, 제어하는 가상 디바이스 관리 수단을 포함하고,

상기 디바이스 관리 수단은, 상기 디바이스가 접속되었을 때, 그 디바이스를 특정하는 정보인 디바이스 정보를 상기 인증 서버에 송신하고,

상기 인증 서버는, 미리 설정된 상기 각 디바이스의 이용 권한을 유지하는 폴리시 유지 수단을 더 포함하고,

상기 디바이스 정보를 수취하면, 상기 폴리시 유지 수단에 유지되고 있는 정보에 따라서, 상기 디바이스 정보 유지 수단에 상기 수취한 디바이스 정보로 특정되는 디바이스의 이용 권한을 등록하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 3

제1항에 있어서,

상기 클라이언트는, 상기 서버에 액세스 요구를 송신하고,

상기 서버가 상기 액세스 요구를 수취하면, 상기 서버가 포함하는 가상 디바이스 관리 수단은, 상기 디바이스 정보 유지 수단을 참조하여, 상기 액세스 요구의 송신원의 클라이언트의 이용자가 이용 권한을 갖는 디바이스가 접속되어 있는 클라이언트 장치가 포함하는 디바이스 관리 수단과의 사이에 통신로를 형성함으로써, 상기 제어

를 행하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 4

제3항에 있어서,

상기 가상 디바이스 관리 수단은, 상기 서버가 상기 액세스 요구를 수취하면, 상기 디바이스 정보 유지 수단을 참조하기 전에, 상기 인증 서버에, 상기 디바이스 정보 유지 수단의 정보를 갱신하는 갱신 지시를 송신하고,

상기 인증 서버는, 상기 갱신 지시를 수취하면, 상기 네트워크에 접속되어 있는 클라이언트에 대하여, 상기 디바이스 정보와 함께 해당 디바이스의 현재의 사용 상황을 나타내는 정보인 디바이스 상태 정보의 취득을 지시하고, 지시에 대하여 회신된 상기 디바이스 정보 및 상기 디바이스 상태 정보에 따라서, 상기 디바이스 정보 유지 수단의 정보를 갱신하고,

상기 클라이언트가 상기 디바이스 정보 및 상기 디바이스 상태 정보의 취득의 지시를 수취하면, 상기 클라이언트가 포함하는 상기 디바이스 관리 수단은, 상기 클라이언트에 접속되어 있는 디바이스의 상기 디바이스 정보 및 상기 디바이스 상태 정보를 취득하여 상기 인증 서버에 회신하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 5

제4항에 있어서,

상기 디바이스 정보 유지 수단은, 각 디바이스에 대해 배타 제어의 필요 유무 및 각 디바이스의 현재의 사용 상황을 더 유지하고,

상기 가상 디바이스 관리 수단은, 상기 서버가 상기 액세스 요구를 받았을 때, 해당 이용 요구의 요구원이 이용 권한을 갖는 디바이스가 상기 배타 제어가 필요한 것으로서, 상기 사용 상황이 다른 이용자에게 점유되어 있음을 나타내는 것인 경우, 상기 사용 상황이 해당 점유가 끝났음을 나타내는 것으로 갱신되고 나서, 해당 디바이스가 접속되어 있는 클라이언트의 상기 디바이스 관리 수단과의 사이에 통신로를 형성하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 6

제3항에 있어서,

상기 클라이언트는, 유저 인터페이스를 포함하고,

상기 유저 인터페이스를 통하여 유저로부터 유저를 특정하는 정보 및 비밀 번호를 상기 액세스 요구로서 입력을 접수하고, 상기 서버에 송신하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 7

제3항에 있어서,

상기 클라이언트는, 상기 디바이스 정보와 함께, 해당 디바이스를 이용하는 요구인 디바이스 이용 요구를 상기 서버에 송신하고,

상기 가상 디바이스 관리 수단은, 해당 가상 디바이스 관리 수단을 포함하는 상기 서버가 상기 액세스 요구를 수신하면, 해당 액세스 요구로 특정되는 디바이스의 동작을 확인하는 동작 확인 지시를 상기 통신로를 통하여 해당 디바이스가 접속되어 있는 클라이언트가 포함하는 디바이스 관리 수단에 송신하는 동작 확인 지시 수단과,

상기 통신로를 이용한 통신이 정상적으로 행해지고 있는지의 여부를 감시하는 통신 상태 감시 수단과,

상기 동작 확인 지시에 대한 회신이, 동작 상태가 부정함을 나타내는 것인 경우, 또는, 상기 통신 상태 확인 수단에서, 상기 통신이 정상적으로 행해지고 있지 않음이 상기 감시에 의해 검출된 경우, 상기 인증 서버에 그 취지를 통지하는 부정 통지 수단을 더 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 8

제7항에 있어서,

상기 디바이스 관리 수단은,

상기 통신로 형성 후, 상기 통신로를 통한 통신의 상태 및 그 디바이스 관리 수단을 포함하는 클라이언트에 접속되어 있는 디바이스의 동작 상태를 감시하는 감시 수단과,

상기 감시에 의해, 부정한 상태임이 검출된 경우, 상기 인증 서버에 그 취지를 통지하는 제2 부정 통지 수단을 더 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 9

제7항에 있어서,

상기 인증 서버는, 상기 통지 수단 또는 상기 제2 부정 통지 수단으로부터 부정한 상태인 취지의 통지를 받은 경우, 그 부정한 상태에 있는 디바이스 및 부정한 상태에 있는 통신로가 통신 대상으로 하고 있는 디바이스를, 상기 디바이스 정보 유지 수단으로부터 삭제하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 10

제1항에 있어서,

상기 디바이스 관리 수단, 상기 가상 디바이스 관리 수단, 및, 상기 인증 서버는, 각각, 송수신한 데이터 및 이벤트를 로그로서 기록하는 로그 유지 수단을 포함하고,

상기 인증 서버는, 자신의 로그 유지 수단에 기록된 로그와, 상기 디바이스 관리 수단의 로그 유지 수단에 기록된 로그와, 상기 가상 디바이스 관리 수단의 로그 유지 수단에 기록된 로그를, 수집하여 표시하는 표시 수단을 더 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 11

제10항에 있어서,

상기 인증 서버는, 상기 통지 수단 또는 상기 제2 부정 통지 수단으로부터 부정한 상태인 취지의 통지를 받은 경우, 해당 통지를, 상기 인증 서버의 로그 유지 수단에 유지하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 12

제2항에 있어서,

상기 가상 디바이스 관리 수단은, 현 시점에서 해당 디바이스 관리 시스템에서 이용 가능한 디바이스의 상기 디바이스 정보를 표시하는 제2 표시 수단을 더 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 13

제1항에 있어서,

상기 네트워크에 접속하는 인터페이스를 포함하는 제2 디바이스를 더 포함하고,

상기 디바이스는,

상기 서버와의 사이에서 데이터의 송수신을 행하는 제2 디바이스 관리 수단과,

해당 디바이스가 상기 네트워크에 접속되었을 때, 해당 디바이스의 상기 디바이스 정보를 상기 인증 서버에 송신하는 디바이스 접속 수단을 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 14

제13항에 있어서,

상기 제2 디바이스는, 해당 디바이스의 이용자를 인증하는 정보를 취득하고, 상기 인증 서버에 송신하는 인증 수단을 더 포함하는 것을 특징으로 하는 디바이스 관리 시스템.

청구항 15

삭제

청구항 16

어플리케이션 프로그램을 실행하는 서버와, 상기 서버에 상기 어플리케이션 프로그램의 실행의 지시를 부여하고, 상기 서버로부터 실행 결과를 수취하는 클라이언트와, 상기 클라이언트를 인증하는 인증 서버가 네트워크로 접속된 시스템에서, 상기 클라이언트에 접속된 디바이스를, 상기 서버로부터 제어하는 디바이스 관리 시스템에서의 상기 클라이언트로서,

상기 클라이언트에 접속되어 있는 디바이스의 디바이스 드라이버와 데이터를 송수신함과 함께 상기 서버와의 사이에서 그 데이터를 송수신하는 디바이스 관리 수단을 포함하고,

상기 디바이스 관리 수단은,

상기 클라이언트에 디바이스가 접속되었을 때, 또는, 상기 인증 서버로부터 지시를 받았을 때, 해당 접속된 디바이스를 특정하는 디바이스 정보를 상기 인증 서버에 송신하는 것을 특징으로 하는 클라이언트.

청구항 17

제16항에 있어서,

상기 디바이스 관리 수단은,

상기 인증 서버로부터 지시를 받았을 때, 상기 디바이스 정보와 함께, 해당 디바이스의 사용 상황을 나타내는 디바이스 상태 정보도 회신하는 것을 특징으로 하는 클라이언트.

청구항 18

어플리케이션 프로그램을 실행하는 서버와, 상기 서버에 상기 어플리케이션 프로그램의 실행의 지시를 부여하고, 상기 서버로부터 실행 결과를 수취하는 클라이언트와, 상기 클라이언트를 인증하는 인증 서버가 네트워크로 접속된 시스템에서, 상기 클라이언트에 접속된 디바이스를, 상기 서버로부터 제어하는 디바이스 관리 시스템에서의 상기 서버로서,

상기 인증 서버에 유지되고 있는 상기 디바이스 관리 시스템 내의 각 디바이스의 이용 권한에 기초하여, 상기 클라이언트와의 사이에 통신로를 형성하는 통신로 형성 수단과,

해당 서버 내에서 동작하는 어플리케이션 프로그램과 상기 클라이언트에 접속된 디바이스를 동작시키기 위한 데이터의 송수신을 행하는 디바이스 드라이버 수단과,

상기 통신로 형성 수단에서 형성한 통신로를 통하여, 상기 디바이스 드라이버 수단이 송수신하는 데이터를, 상기 클라이언트와 송수신하는 통신 수단

을 포함하고,

상기 서버는, 상기 클라이언트로부터의 액세스 요구를 수취하면, 상기 인증 서버에, 상기 디바이스의 이용 권한을 갱신하는 갱신 지시를 송신하고, 상기 디바이스 드라이버 수단은, 상기 인증 서버에 상기 클라이언트로부터 송신된 상기 디바이스의 이용 권한에 기초하여, 상기 클라이언트와 데이터를 송수신하는 것을 특징으로 하는 서버.

명 세 서

발명의 상세한 설명

발명의 목적

종래기술의 문헌 정보

<16> [특허 문헌1] 특개2005-12775호 공보

발명이 속하는 기술 및 그 분야의 종래기술

<17> 본 발명은, 네트워크를 통하여 서버에 접속하는 디바이스에의 액세스를 관리하는 기술에 관한 것이다. 특히, 디바이스가 서버에 직접 접속하고 있는 경우와 마찬가지로 해당 디바이스를 가상적으로 이용 가능한

시스템에서, 안전하면서 간편하게 원격 조작 가능하게 하는 기술에 관한 것이다.

<18> 인터넷이나 기업 내의 인트라넷 등의 네트워크를 통한 통신을 행할 때에 이용 가능하게 되는 1인당 데이터 전송 대역이 광대역화되고 있다. 기업 내부의 기기로부터 외부의 서버에의 액세스는 물론, 가정이나 호텔, 핫 스폿(등록 상표) 등으로부터 기업 내부의 기기에 수 Mbps ~ 수십 Mbps의 대역에서 액세스가 가능하도록 되어 있다. 인터넷을 가정이나 거리에서 이용하는 경우, 항시 접속 가능하고 가격도 저렴하게 되어 있다.

<19> 또한, 퍼스널 컴퓨터(PC)나 PDA, 휴대 전화 등의 정보 기기의 저가격화가 진행되어, 대부분의 종업원에게 정보 단말기를 배포하여, 업무를 행하도록 하고 있는 기업이 늘어나고 있다. 많은 기업이, 신속한 업무 수행을 위해, 출장처나 자택, 이동중 등의 사무실 밖의 장소에서 정보 기기를 이용하여, 기업 내의 PC나 서버 등의 기기에 액세스하는 것을 허가하도록 되어 있다.

<20> 이러한 액세스는 리모트 액세스 기능이라고 불리며, 암호 통신을 행하는 버추얼 프라이비트 네트워크(VPN) 기능을 갖는 서버가 사내에 설치되고, 이 서버에 의해, 사무실 밖의 정보 기기와의 통신에서, 도중 경로 상의 통신을 암호화하는 등의 관리가 행해지고 있다. 사무실 밖으로부터의 리모트 액세스가 일반적으로 됨에 따라, 사무실의 밖으로부터 메일 서버나 WEB 서버에 액세스하여, 부분적인 업무를 수행할 뿐 아니라, 사무실 내에 재적하고 있을 때에 행하고 있는 것과 같은 업무의 대부분을 원격지에서 행하는 업무 형태로 계속 시프트하고 있다.

<21> 이러한 업무 형태를 위해 도입되는 한 방법으로서, 서버 클라이언트 방식이라는 시스템 운용의 방식을 들 수 있다. 서버 클라이언트 방식의 시스템은, 네트워크 컴퓨팅 시스템이나 서버 베이스드 컴퓨팅 등으로 불리며, 주된 프로그램이나 데이터를 서버측에 축적하고, PC나 신 클라이언트와 같은 클라이언트측으로부터 조작하는 것이다. 서버 클라이언트 방식에서는, 연산 처리나 데이터의 축적은 주로 서버측에서 행해지기 때문에, 신 클라이언트와 같은 클라이언트측에서 개별적으로 OS나 업무에 이용하는 어플리케이션의 버전업이나 백픽스, 바이러스 대책이나 바이러스 구제 등을 행할 필요성이나 빈도가 감소하여, 전체적인 관리 비용을 저감할 수 있고, 안전성이 증가한다(예를 들면, 특개2005-12775호 공보 참조).

발명이 이루고자 하는 기술적 과제

<22> 전술한 서버 클라이언트 방식에서는, 서버와 클라이언트는, 물리적으로 떨어진 장소에 설치되어 있어도 된다.

<23> 이러한 서버 클라이언트 방식에서, 이용자가 CD-ROM 드라이브나 프린터 등의 정보 기기에 접속되는 주변 기기(이후, 본 명세서에서는 디바이스라고 함)를 서버 상에서 이용하는 방법으로서, 서버에 직접 해당 디바이스를 접속하여 이용하는 방법이 있다. 이 경우, 클라이언트측에는 해당 디바이스의 드라이버를 인스톨하지 않더라도, 클라이언트는, 서버측의 드라이버에 의해 해당 디바이스를 사용할 수 있다. 또한, 복수의 클라이언트에 의해 해당 디바이스를 공유할 수도 있다. 그러나, 이 경우, 클라이언트측의 조작 환경에 서버에 직접 접속된 디바이스(예를 들면, CD-ROM)의 드라이버가 없기 때문에, CD-ROM의 추출 등의 조작은 행할 수 없다.

<24> 또한, 인트라넷 등의 네트워크 상에 해당 디바이스를 공유의 디바이스로서 배치하고, 클라이언트측에 해당 디바이스의 드라이버를 인스톨하여, 그 드라이버에 의해 해당 디바이스를 사용하는 방법이 있다. 이 경우, CD-ROM 드라이브 상에 CD-ROM을 삽입한 후에, 액세스 제한 등의 조치를 취하지 않으면, 해당 디바이스의 드라이버를 유지하고 있는 제삼자에게 부정하게 액세스될 가능성이 있고, 시큐러티의 면에서의 문제가 있다. 특히, 서버가 네트워크 상에 존재하는 경우에는, 복수의 클라이언트가 사용 가능한 공유 디바이스를 서버에 가상적으로 접속하는 것은, 시큐러티 상의 리스크를 수반하므로, 인증이나 암호화 등의 시큐러티를 충분히 높일 필요가 있다.

<25> 또한, CD-ROM 드라이브와 같이 일반적인 디바이스이면, 각 클라이언트가 드라이버를 갖고, 서버 및 클라이언트의 OS가 디바이스 공유를 행하는 기능을 제공하고 있을 가능성이 높기 때문에, 본 방법으로 디바이스의 공유를 행하는 것은 가능하다. 그러나, 특별한 기능을 갖는 드라이버를 필요로 하는 특수한 디바이스인 경우, 해당 디바이스를 공유하기 위한 전용의 기능이 필요하고, 일반적으로 이러한 기능을 OS에서는 제공하지 않는 경우가 많기 때문에, 클라이언트측에 디바이스의 드라이버를 구비한 구성에 의한 디바이스의 공유의 실현은 어렵다.

발명의 구성 및 작용

<26> 본 발명은, 상기 사정을 감안하여 이루어진 것으로, 서버 클라이언트 방식에서 디바이스를 공유하는 경우, 이용자의 편리성을 저해하지 않고, 시스템 내의 시큐러티를 향상시킨다.

<27> 이 때문에, 본 발명은, 네트워크에 접속된 디바이스를 가상적으로 서버 상에서 동작시키는 경우의 디바이스의 액세스 권한을 관리한다.

<28> 구체적으로는, 어플리케이션 프로그램을 실행하는 서버와, 상기 서버에 상기 어플리케이션 프로그램의 실행의 지시를 부여하고, 해당 서버로부터 실행 결과를 수취하는 클라이언트와, 상기 클라이언트를 인증하는 인증 서버가 네트워크로 접속된 시스템에서, 상기 클라이언트에 접속된 디바이스를, 상기 서버로부터 제어하는 디바이스 관리 시스템으로서,

<29> 상기 클라이언트는, 해당 클라이언트에 접속하고 있는 디바이스의 디바이스 드라이버와 데이터를 송수신함과 함께 상기 서버와의 사이에서 해당 데이터를 송수신하는 디바이스 관리 수단을 구비하고,

<30> 상기 인증 서버는, 해당 디바이스 관리 시스템 내의 각 디바이스의 이용 권한을 관리하는 디바이스 정보 유지 수단을 구비하고,

<31> 상기 서버는, 해당 서버 내에서 동작하는 어플리케이션과, 상기 디바이스 관리 수단과의 사이에서 상기 네트워크를 통하여 행해지는 데이터의 송수신을, 상기 디바이스 정보 유지 수단에 유지되고 있는 상기 이용 권한에 따라서, 제어하는 가상 디바이스 관리 수단을 구비하는 것

<32> 을 특징으로 하는 디바이스 관리 시스템을 제공한다.

<33> 본 발명의 실시예에 대해, 첨부 도면을 참조하면서 이하 상세하게 설명한다.

<34> <<제1 실시예>>

<35> 이하 도면을 이용하여, 본 발명에 따른 디바이스 관리 시스템의 제1 실시예를 설명한다.

<36> 도 1은, 본 실시예의 디바이스 관리 시스템의 상세한 블록도이다. 본 실시예의 디바이스 관리 시스템은, 인증 관리 서버(101), 네트워크(103), 블레이드 서버(106)를 구비하는 정보 센터(102)와, 해당 정보 센터의 네트워크(103)에 접속하는 PC 등의 클라이언트 장치를 구비한다.

<37> 정보 센터(102)는, 정보 기기를 관리하는 센터에서 통상 입퇴실이 제한되고, 설치하는 기기가 관리 감시되고 있는 에리어이다. 정보 센터(102)의 설치 장소는, 한정되지 않는다. 예를 들면, 이용자가 클라이언트 장치 등의 단말기를 이용하는 장소에 설치되어도 되고, 떨어진 장소에 설치되어 있어도 된다. 이용자가 단말기를 사무실 등에서 이용하는 경우, 정보 센터(102)는 이용자를 관리하는 기업 단체의 건물 내에 설치되어도 된다. 이용자가 일반 소비자이고 자택이나 호텔, 길거리 등으로부터 서비스 제공 기업의 서버를 이용하는 경우, 정보 센터(102)는 인터넷 서비스 프로바이더나 서버 렌탈 기업, 어플리케이션 서비스 프로바이더 등이 관리하는 건물 내에 설치되어 있어도 된다. 또한, 이용자 자택이나 사무실의 일각에 서버를 집중시킨 에리어이어도 된다.

<38> 인증 관리 서버(101)는, 디바이스나 이용자의 인증과 관리를 행하는 서버로서, 정보 센터(102)의 관리자가 관리한다. 인증 관리 서버(101)가 이들을 실현하기 위해 유지하는 각종의 데이터에 대해서는, 후술한다. 인증 관리 서버(101)는, 통신 인터페이스, CPU 및 메모리를 구비하는 정보 처리 장치로 실현되고, CPU가 메모리에 저장된 프로그램을 실행함으로써, 각 기능을 실현한다. 또한, 각 기능을 실현하는 프로그램은, 기억 매체, 또는, 반송파, 디지털 신호, 통신선을 포함하는 통신 매체를 통하여, 다른 장치로부터 취득해도 된다.

<39> 블레이드 서버(106)는, 내부에 복수의 서버 혹은 PC를 갖는 기기로서, 도시하지 않은 전원, 내부 기기와 네트워크(103)를 결선하는 인터페이스 기능, 관리 장치 등을 구비한다. 본 실시예에서는, PC-A(110), PC-B(111), PC-C(112)를 내부에 구비하는 경우를 예로 들어 설명한다. 물론, 블레이드 서버(106)의 구성은, 이것에 한정되지 않고, 이들 이외의 PC나 서버를 착탈하는 것이 가능하다.

<40> 네트워크(103)는, 인증 관리 서버(101), PC-A(110), PC-B(111), PC-C(112) 등을 서로 접속한다. 본 실시예에서는, TCP/IP 프로토콜을 이용하여 통신을 행하는 네트워크로서 이하에 설명한다. 물론, 그 이외의 프로토콜에 따른 통신을 행하는 것이어도 된다.

<41> 또한, 본 실시예의, PC-A(110), PC-B(111), PC-C(112)는, 블레이드 서버(106) 내부에 구성되어 있지만, 블레이드 서버(106) 내부나 또한 정보 센터(102) 내에 설치되어 있지 않더라도 네트워크(103) 상에 존재하면 된다. PC-A(110), PC-B(111), PC-C(112)는, PC로 기술하고 있지만, 서버이든 워크스테이션이든 내장이든, 기억 매체에 저장하고 있는 OS나 어플리케이션을 메모리와 CPU 상에서 실행하는 정보 기기이면 특별히 한정되지 않는다.

<42> 도 15는, PC-A(110)의 하드웨어 구성도이다. PC-A(110)는, 하드 디스크 드라이브나 플래시 메모리 등의 스토리지(160)와 메모리(110a)와 CPU(110b)와 통신을 위한 인터페이스인 통신 인터페이스(110c)를 구비한다. PC-A(110)에서는, 메모리에 읽어 들여진 프로그램이 CPU에 의해 실행됨으로써, 각 처리부가 실현된다. 또한, 각 프로그램은, 기억 매체, 또는 통신 매체를 통하여, 다른 장치로부터 취득하는 것도 가능하다. 또한, 통신 매체

란, 반송파, 디지털 신호, 통신선을 포함한다.

<43> PC-A(110)는, 이용자의 지시에 따라서, 연산을 행한다. 연산 결과는 PC-A(110) 또는 블레이드 서버(106)에 접속된 도시하지 않은 디스플레이에 표시된다. 스토리지(160)에는, 가상 디바이스 매니저(120)가 관리자에 의해 인스톨되어 있다. PC-A(110)가 기동되면 스토리지(160)로부터 OS가 메모리(110b)에 읽어 들여지고, CPU(110a)에 의해 실행되어 이용 가능 상태로 된 후, 가상 디바이스 매니저(120)가 메모리(110b)에 읽어 들여지고, CPU(110a)에 의해 실행되어 가상 디바이스가 이용 가능하게 된다.

<44> 여기서 말하는 가상 디바이스란, PC-A(110)에 네트워크(103) 등을 통하여 접속되어 있는 디바이스를, 마치 PC-A(110)에 직접 접속되어 있는 디바이스인 것처럼 이용 가능하게 하는 구조이다. 본 구조에 의해, 떨어진 장소에 접속되어 있는 디바이스가, PC-A(110)에 물리적으로 접속되어 있는 디바이스와 마찬가지로 이용 가능하게 된다.

<45> 가상 디바이스 매니저(120)는, PC-A(110)에 네트워크(103)를 통하여 접속되어 있는 디바이스 A(151)와의 사이에서의 데이터의 송수신을 행하기 위한 제어를 행하는 소프트웨어이다. 디바이스 A(151)를, 가상적으로, 서버에 직접 접속하고 있는 경우와 마찬가지로 사용 가능하게 하는 기능을 실현하는 것이다. 상세 내용에 대해서는, 후술하는 디바이스 관리 매니저(123)의 동작과 함께 후술한다.

<46> 또한, 스토리지(160)에는, 가상 디바이스 매니저(120)가 송수신한 데이터 및 가상 디바이스 매니저(120)에서 발생한 이벤트가 로그(170)로서 축적된다. 로그(170)의 상세 내용에 대해서는 후술한다.

<47> PC-B(111) 및 PC-C(112)도 PC-A(110)와 마찬가지의 구성을 구비하고, 각각 내부에 스토리지(161, 162)를 구비함과 함께, 가상 디바이스 매니저(121, 122)가 인스톨되고, 기동 후에 동작한다. 이후, 특히 PC-A(110), PC-B(111), PC-C(112)를 구별할 필요가 없는 경우, PC-A(110)를 대표로서 설명한다.

<48> 또한, 스토리지(160 ~ 162)는, 블레이드 서버(106) 내에 존재하지 않고, 네트워크(103) 상에 존재하고 있어도 된다.

<49> 다음으로, 클라이언트 장치로서 네트워크(103)에 접속되어 있는 기기에 대해 설명한다.

<50> 본 실시예에서는, 클라이언트 장치로서, PC-D(113)와, PC-E(114)와, PC-F(115)와, 허브(116)와, 파이어월(105) 및 인터넷(104)을 통하여 접속하는 PC-Z(117)를 구비하는 경우를 예로 들어 설명한다. 또한, PC-D(113)에는 디바이스 A(151)가, PC-F(115)에는 디바이스 B(152)가, 허브(116)에는 디바이스 C(153) 및 디바이스 D(154)가, PC-Z(117)에는 디바이스 Z(155)가 접속되는 경우를 예로 들어 설명한다. 각 클라이언트 장치 및 디바이스의 접속 구성은 이것에 한정되지 않는다.

<51> PC-D(113)는, 이용자의 지시에 따라서 연산을 행하고, 필요에 따라 디바이스를 이용하여, 연산 결과를 이용자에게 제시하는 정보 처리 장치이다. 하드웨어 구성, 각 처리부의 실현 방법은, 상기 PC-A(110)와 기본적으로 마찬가지이다. PC-D(113)는, 네트워크(103)에 도시하지 않은 네트워크 인터페이스를 통하여 접속하고 있다. PC-D(113)는, 하드 디스크 드라이브 혹은 플래시 메모리 등 스토리지(163) 및 도시하지 않은 메모리 및 CPU를 구비하고, 이용자의 지시에 의해서 연산을 행한다. 연산 결과는, PC-D(113)에 접속되어 있는 도시하지 않은 디스플레이에 표시된다. 이용자로부터의 지시는 도시하지 않은 키보드나 마우스 등의 유저 인터페이스를 통하여 PC-D(113)에 송신된다.

<52> 또한, PC-D(113)는, 스토리지(163)에 디바이스 관리 매니저(123)가 인스톨되어 있다. PC-D(113)가 기동되면 스토리지(163)로부터 OS가 메모리에 읽어 들여지고, CPU가 실행함으로써 이용 가능 상태로 된 후, 디바이스 관리 매니저(123)가 메모리에 읽어 들여지고, CPU가 실행함으로써, 접속된 디바이스 A(151)가 PC-A(110)에서 가상 디바이스로서 이용 가능하게 된다. 또한, 스토리지(163)에는, 디바이스 관리 매니저(123)가 송수신한 데이터 등이 로그(173)로서 축적된다. 로그(173)의 상세 내용에 대해서는 후술한다.

<53> 디바이스 관리 매니저(123)는, PC-D(113)가, 디바이스 A(151)를, 블레이드 서버(106)의 PC-A(110)의 가상 디바이스로서 이용하기 위한 소프트웨어이다. 상세 내용에 대해서는, 가상 디바이스 매니저(120)의 동작과 함께 후술한다.

<54> PC-E(114), PC-F(115), PC-Z(117)는 기본적으로 PC-D(113)와 마찬가지의 구성을 구비하고, 각각, 스토리지(164, 165, 167)를 구비한다. 또한, 디바이스 관리 매니저(124, 125, 127)가 실현된다. 또한, 각 스토리지에는, 로그(174, 175, 177)가 각각 저장된다.

<55> 또한, 허브(116)는, PC-D(113)로부터 표시 화면 등의 일반적인 PC의 기능의 일부가 삭제된 것이다. 즉, 도시하지 않은 네트워크 인터페이스를 통하여 네트워크(103)에 접속하고, 하드 디스크 드라이브 혹은 플래시 메모리 등 스토리지(166) 및 도시하지 않은 메모리 및 CPU를 구비하고, 연산을 행한다. 하드웨어 구성, 각 처리부의 실현 방법은, PC-A(110)와 기본적으로 마찬가지이다. 디바이스 관리 매니저(126)를 실현함과 함께, 스토리지(166)에는 로그(176)를 유지한다. 이후, 특히 PC-D(113), PC-E(114), PC-F(115), PC-Z(117), 허브(116)를 구별할 필요가 없는 경우, PC-D(113)를 대표로서 설명한다.

<56> 디바이스 A(151)는, 정보 기기에 접속되는, 예를 들면, CD-ROM이나 프린터 등의 주변 기기이다. 디바이스 A(151)는, PC-D(113)와 디바이스 접속용의 인터페이스를 통하여 접속되어 있다. 디바이스 접속용의 인터페이스는, 예를 들면 유니버설 시리얼 버스(USB), 와이어리스 USB, 근거리 무선 통신 인터페이스, 적외선 통신 인터페이스, 시리얼 포트 인터페이스, 패러랠 포트 인터페이스, IEEE 1394 인터페이스, PS/2 인터페이스(등록상표), 오디오 인터페이스 등의 디바이스를 PC에 접속하기 위한 인터페이스를 생각할 수 있다. 본 실시예에서는, 인터페이스가 USB인 경우를 예로 들어 설명하지만, 인터페이스는 이것에 한정되지 않는다.

<57> 또한, 디바이스 A(151)는, 접속되어 있는 PC-D(113)에 인스톨되어 있는 디바이스 관리 매니저(123)에 의해, 가상 디바이스로서 본 시스템에서 이용된다. 이후, 디바이스 관리 매니저(123)를, 디바이스 A(151)를 관리하는 디바이스 관리 매니저라고 한다.

<58> 그 밖에, 각 PC 및 허브에 접속되어 있는 디바이스 B(152), C(153), D(154)도 디바이스 A(151)와 마찬가지의 주변 기기로서, 본 실시예에서는, 일례로서 USB 인터페이스를 통하여 PC 또는 허브에 접속되어 있다. 이후, 특별히 디바이스 A(151), 디바이스 B(152), 디바이스 C(153), 디바이스 D(154)를 구별할 필요가 없는 경우, 디바이스 A(151)를 대표로서 설명한다.

<59> 다음에 인증 관리 서버(101)가 유지하는, 폴리시 테이블(1400), 디바이스 관리 테이블(200) 및 이용자 정보 데이터베이스(300)에 대해 설명한다. 인증 관리 서버(101)는, 가상 디바이스 매니저(120)와 디바이스 관리 매니저(123)와 함께, 각 디바이스에의 액세스를 제어한다.

<60> 폴리시 테이블(1400)은, 본 시스템 내에서 관리자가 관리하는 디바이스에 관한 액세스 폴리시가 등록된다. 예를 들면, 디바이스마다의 이용 권한, 디바이스가 접속되는 클라이언트 장치에 따른 이용 권한 등이 등록된다. 본 테이블은, 미리 관리자 등에 의해 설정된다. 폴리시 테이블(1400)은, 시스템의 관리자가 자유롭게 변경하는 것이 가능하다. 또한, 폴리시 테이블(1400)을 설정하지 않는 것에 의해, 자동적으로는 디바이스 정보 테이블(200) 상의 룰을 변경할 수 없고, 수동에 의해서만 변경할 수 있도록 시스템을 구성하는 것도 가능하다. 관리자는 자신이 관리하는 시스템에 정할 폴리시에 따라 폴리시 테이블(1400)을 구성한다.

<61> 도 2에 폴리시 테이블(1400)의 일례를 도시한다. 도 2에 도시한 바와 같이, 폴리시 테이블(1400)은, 폴리시마다, 폴리시 번호(1401), 디바이스명(1402), 접속 어플리케이션의 어드레스(1403), 접속 어플리케이션의 네트워크 인터페이스 ID(1404), 벤더 ID(1405), 제품 ID(1406), 시리얼 번호(1407), 디바이스 종별(1408), 배타 제어(1409), 이용 가부(1410), 이용 가능 ID(1411)가 기록된다. 물론, 그 밖의 항목이 기록되어 있어도 된다.

<62> 폴리시 번호(1401)는, 폴리시 테이블(1401)에 관리자에 의해서 폴리시가 등록될 때, 각 폴리시에 자동적으로 부여되는 식별 번호이다. 본 시스템 상에서 이용 가능한 기기나 디바이스가 증감하였을 때, 폴리시 테이블(1400)에 등록되어 있는 폴리시에 따라서 후술하는 디바이스 정보 테이블(200)의 레코드가 생성된다. 복수의 폴리시에 적합한 기기나 디바이스가 시스템 상에 증감하였을 때, 폴리시는, 미리 정해진 우선 순서로 적용된다.

<63> 디바이스명(1402), 접속 어플리케이션의 어드레스(1403), 접속 어플리케이션의 네트워크 인터페이스 ID(1404), 벤더 ID(1405), 제품 ID(1406), 시리얼 번호(1407), 디바이스 종별(1408)은, 후술하는 디바이스 정보 테이블(200)에 기재되는 내용과 마찬가지로, 기기 혹은 디바이스의 정보를 나타내고 있다. 관리자는 각각의 폴리시마다 해당하는 디바이스명, 접속 어플리케이션의 어드레스, 접속 어플리케이션의 네트워크 인터페이스 ID, 벤더 ID, 제품 ID, 시리얼 번호, 디바이스 종별의 조건을 설정한다. 이들의 상세 내용은, 디바이스 정보 테이블(200)의 설명에서 설명한다.

<64> 배타 제어(1409)는, 디바이스를 이용자가 이용할 때, 다른 이용자로부터의 이용을 금지하는지의 여부를 정의하는 값이다. "필수" "가능" "불필요" "불문(*)"의 설정이 가능하다. "불문(*)"의 경우, 기본적으로는 불필요와 마찬가지로 취급하지만, 디바이스의 종별, 클래스마다 자동 설정되도록 구성해도 된다. 여기서, 클래스란, 예를 들면, 키보드, 스토리지 등, 동일한 디바이스 드라이버(클래스 드라이버)에서 동작하는 디바이스 종별을 말한다.

<65> 이용 가부(1410)는, 디바이스의 이용 허가를 행할 때의 인증 관리 서버(101)의 거동을 나타내는 것으로, "가능" "금지" "경고"의 설정이 가능하다. "가능"이 설정되어 있는 폴리시는, 해당하는 기기나 디바이스를, 후술하는 이용 가능 ID(1411)에 기재되어 있는 이용자에게 자동적으로 이용 가능하다고 하는 폴리시이다. "금지"가 설정되어 있는 폴리시는, 해당하는 기기나 디바이스를, 후술하는 이용 가능 ID(1411)에 기재되어 있는 이용자에게 자동적으로 이용 불가능하다고 하는 폴리시이다. "경고"가 설정되어 있는 폴리시는, 해당하는 기기나 디바이스를, 후술하는 이용 가능 ID(1411)에 기재되어 있는 이용자에게 경고 표시 후에 자동적으로 이용 가능하다고 하는 폴리시이다. 경고 표시는 폴리시마다 설정 가능하다.

<66> 또한, 도면 중의 * 표시는 불문(정의 없음)의 의미로서, 관리 인증 서버(101)는 기술 내용과 실제의 정보와의 매칭을 행한다.

<67> 예를 들면, 도 2에서는, 폴리시 번호(1401)가 1인 폴리시는, 디바이스명(1402), 접속 어플리케이션의 어드레스(1403), 접속 어플리케이션의 네트워크 인터페이스 ID(1404), 시리얼 번호(1407), 디바이스 종별(1408)은 불조회 폴리시이다. 즉, 벤더 ID(1405)가 "1001"이고, 제품 ID(1406)가 "1001"인 디바이스에 대한 폴리시의 조회가 있었던 경우, 그 디바이스명, 접속 어플리케이션의 어드레스, 접속 어플리케이션의 네트워크 인터페이스 ID, 시리얼 번호, 디바이스 종별에 상관없이, 배타 제어(1409)는 "불필요", 이용 가부(1410) "가능", 이용 가능 ID(1411)는 20000001, 20000010 등이 디바이스 정보 테이블(200)에 기록된다.

<68> 또한, 폴리시 번호(1401)가 2인 폴리시는, 벤더 ID가 "1105"이고 디바이스 종별이 "B Ltd."로부터 시작되는 디바이스에 대해서만, 자동적으로 배타 제어 "필수"이고 이용 가능 ID는 20000011로 설정되는 폴리시이다.

<69> 그리고, 폴리시 번호(1401)가 3인 폴리시는, 접속 어플리케이션의 어드레스(1403)가 192.168.1.1이고 접속 어플리케이션의 네트워크 인터페이스 ID(1404)가 "00:00:00:00:00:01"인 클라이언트 장치에 접속되어 있는 디바이스에 대하여, 자동적으로 배타 제어(1409)는 "불문"이고 이용 가부(1410)에 대해서는 "경고" 표시를 하여 모든 유저에게 이용 가능하다고 설정되는 폴리시이다.

<70> 또한, 폴리시 번호(1401)가 n인 폴리시는, 모든 디바이스에 대하여 이용이 금지되는 설정의 폴리시이다. 즉, 폴리시 테이블(1400)에 미등록의 디바이스에 대한 등록의 의뢰가 있었던 경우, 인증 관리 서버(101)는, 폴리시 번호(1401)가 n의 란을 참조하여, 디바이스 정보 테이블(200)에 배타 제어(1409)는 "불필요", 이용 가부(1410)는 "금지"라고 설정한다.

<71> 다음에 디바이스 정보 테이블(200)에 대해 설명한다. 디바이스 정보 테이블(200)은, 본 시스템에 접속되어 있는 각 디바이스의 액세스를 관리하기 위해 필요한 정보를 관리하는 것이다. 등록되는 각 레코드는, 디바이스 관리 매니저(123)로부터, 자신이 관리하고 있는 디바이스를 본 시스템 내에서 공유 가능하게 하는 요구(이후, 디바이스 접속 요구라고 함)와 함께 송신되는 디바이스를 특정하는 각종의 정보(이후, 디바이스 정보라고 함)에, 폴리시 테이블(1400)에 등록되어 있는 폴리시를 더한 것에 따라서 생성된다. 가상 디바이스 매니저(120)는, 디바이스 정보 테이블(200)을 이용하여, 각 디바이스의 이용의 가부를 제어한다.

<72> 디바이스 관리 매니저(123)로부터는, 디바이스가 접속되었을 때, 또는, 제거되었을 때, 디바이스 정보로서, 송신원의 클라이언트 장치를 네트워크(103) 상에서 특정하는 정보(본 실시예에서는, IP 어드레스와 MAC 어드레스)와, 해당 디바이스를 특정하는 정보(본 실시예에서는, 벤더 ID와 제품 ID와 시리얼 번호)와, 접속되었는지, 또는, 제거되었는지를 나타내는 정보가 적어도 송신된다. 인증 관리 서버(101)는, 폴리시 테이블(1400)에 따라서, 레코드를 생성하고, 디바이스 정보 테이블(200)에 등록한다.

<73> 또한, 클라이언트 장치 자체가 네트워크(103)로부터 분리되는 경우, 해당 클라이언트 장치를 특정하는 정보와, 분리된 것을 나타내는 정보가 인증 관리 서버(101)에 송신된다.

<74> 인증 관리 서버(101)는, 예를 들면, 디바이스가 증감하였을 때, 클라이언트 장치가 분리되었을 때, 시스템을 이용하는 이용자가 증감하였을 때, 네트워크의 구성이 변경되었을 때 등의, 인증 관리 서버(101)가 관리하는 시스템의 구성에 변경이 있었을 때, 폴리시 테이블(1400)의 레코드에 변경이 있었을 때, 관리자로부터 디바이스 정보 테이블(200)의 갱신의 지시를 접수하였을 때, 디바이스 정보 테이블(200)을 갱신한다. 또한, 후술하는 바와 같이, 스테이터스에 대해서는, 소정 기간마다 갱신된다.

<75> 도 3은, 디바이스 정보 테이블(200)의 일례를 도시하는 도면이다. 도 3에 도시한 바와 같이, 디바이스 정보 테이블(200)은, 디바이스 ID(201), 디바이스명(202), 접속 어플리케이션의 어드레스(203), 접속 어플리케이션의 네트워크 인터페이스 ID(204), 벤더 ID(205), 제품 ID(2060, 시리얼 번호(207), 디바이스 종별(208), 배타 제

어(209), 스테이터스(210), 이용 가능 ID(211), 이용 유저 ID(212)를 구비한다.

<76> 디바이스 ID(201)는, 관리하는 각 디바이스를 일의적으로 식별하기 위한 것으로, 새로 등록의 요구가 있을 때마다 자동적으로 작성된다. 또한, 인증 관리 서버(101)나 디바이스 관리 매니저(123)의 기동이나 종료, 디바이스의 삽입 인출 때마다 변경될 가능성이 있는 일시적인 ID이다.

<77> 디바이스명(202)은, 디바이스를 부르기 쉽게 하기 위한 명칭으로서, 미리 관리자 또는 이용자가 설정한다. 관리자가 설정하는 경우에는, 폴리시 테이블(1400)에 디바이스명을 등록해 놓고, 디바이스 정보 테이블(200)의 레코드를 생성할 때에 폴리시 테이블(1400)로부터 추출하여 등록된다. 한편, 이용자가 설정하는 경우에는, 디바이스 정보에 포함시켜 인증 관리 서버(101)에 통지된다.

<78> 접속 어플리케이션의 어드레스(203)는, 디바이스가 접속되어 있는 클라이언트 장치(디바이스 A(151)의 예에서는 PC-D(113))의 IP 어드레스가 기록된다. 이들은, 디바이스 정보로서 통지된다. 이 어드레스는 상기 클라이언트 장치가 서브 넷 사이를 이동 등을 한 경우, 이용중이라 하더라도 적절하게 변경될 가능성이 있다.

<79> 네트워크 인터페이스 ID(204)는, 디바이스가 접속되어 있는 클라이언트 장치(디바이스 A(151)의 예에서는 PC-D(113))의 네트워크 인터페이스의 ID를 나타내는 번호가 기록된다. 본 실시예와 같이 네트워크가 TCP/IP 프로토콜을 이용하고 있는 경우, 네트워크 인터페이스 ID로서 MAC 어드레스가 사용된다. 네트워크 인터페이스 ID(204)는, 접속 어플리케이션의 어드레스와 상이하고, 기기에 고유한 것으로서, 기기가 변경되지 않으면 변경되지 않는다.

<80> 벤더 ID(205), 제품 ID(206), 시리얼 번호(207)는, 디바이스 자체에 미리 부여되어 있는 디바이스의 식별 번호로서, 클라이언트 장치(디바이스 A(151)의 예에서는 PC-D(113))에 디바이스가 접속되었을 때, 디바이스 정보로서 취득된다. 이들의 정보는, 디바이스 정보로서 클라이언트 장치로부터 인증 관리 서버(101)에 송신된다. 각 디바이스는, 벤더 ID, 제품 ID, 시리얼 번호의 조에 의해 식별된다. 벤더 ID 및 제품 ID는, 벤더 및 제품마다 일의적으로 붙여지는 ID이다. 또한, 시리얼 번호는, 제품 하나하나에 개별적으로 붙여지는 번호이다.

<81> 디바이스 종별(208)은, 이용자의 이해를 위해 벤더나 관리자가 붙이는 명칭이다. 벤더가 붙이는 경우에는, 디스크립터와 같은 디바이스 정보로부터 추출되고, 디바이스 정보에 포함시켜 통지된다. 한편, 관리자가 붙이는 경우에는, 폴리시 데이터베이스(1400)에 미리 등록된다.

<82> 배타 제어(209)는, 디바이스를 이용자가 이용할 때, 다른 이용자로부터의 이용을 금지하는지의 여부를 나타내는 정의 정보이다. 배타 제어(209)가 "필수"로 되어 있는 경우, 디바이스의 이용에 관해서 배타 제어가 이루어지고, 디바이스의 이용 개시로부터 이용자가 이용을 종료할 때까지, 해당 디바이스는 다른 이용자의 액세스로부터 보호된다. 배타 제어(209)가 "가능"으로 되어 있는 경우, 디바이스 로 정보를 송수신하고 있는 기간만 디바이스는 다른 이용자의 이용으로부터 보호된다. 배타 제어(209)가 "불필요"로 되어 있는 경우에는, 배타 제어는 행해지지 않는다. 본 정보는, 폴리시 테이블(1400)로부터 추출되고, 등록된다.

<83> 스테이터스(210)는, 디바이스의 이용 상황을 나타내는 정보이다. 본 정보는, 인증 관리 서버(101)가 소정 시간마다 각 접속 클라이언트 장치에 폴링을 행하여, 취득한다. 스테이터스(210)가 "점유중"으로 되어 있는 경우, 이용자가 배타 처리를 하면서 해당 디바이스를 이용하고 있는 상태를 나타낸다. 스테이터스(210)가 "이용중"으로 되어 있는 경우, 이용자가 배타 처리는 행하지 않고 해당 디바이스를 이용하고 있는 상태를 나타낸다. 스테이터스(210)가 "통신중"으로 되어 있는 경우, 이용자가, 통신중에만 배타 제어를 이용하고, 통신이 종료되는 대로 신속하게 점유 상태를 해소하는 상황을 나타낸다. 스테이터스(210)가 "불명"으로 되어 있는 경우, 예를 들면, 인증 관리 서버(101)에의 통지 없음으로 디바이스 관리 매니저(123)가 통신할 수 없게 된 상태를 나타낸다. 스테이터스(210)가 "불명" 상태로 된 경우, 일정 시간이 지나면 인증 관리 서버(101)는, 해당하는 디바이스 관리 매니저(123)의 정지와 해당 디바이스 관리 매니저(123)가 인스톨되어 있는 PC-D(113)에 접속되어 있던 디바이스 A(151)를 정지하도록 제어한다. 스테이터스(210)가 "절단"으로 되어 있는 경우, 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)와 통신은 되고 있지만, 디바이스 관리 매니저(123)와 해당 디바이스 A(151)와의 사이의 통신을 할 수 없는 상태를 나타낸다. 또한, 스테이터스(210)가 "미사용"으로 되어 있는 경우에는, 어떤 클라이언트 장치도 사용하지 않는 상태를 나타낸다.

<84> 이용 가능 ID(211)는, 해당 디바이스에의 접속이 허가되는 이용자 혹은 그룹의 ID가 기록된다. 본 정보는, 폴리시 테이블(1400)로부터 추출된다. 복수의 이용자 혹은 그룹에 해당 디바이스에의 접속이 허가되어 있는 경우에는, 모든 허가되어 있는 이용자 혹은 그룹의 ID가 등록된다. 이용 가능 ID(211)는, 미정의, 즉, 어느 쪽의 ID도 등록되어 있지 않은 상태이어도 된다. 미정의의 경우, 어느 쪽의 이용자 혹은 그룹도, 접속이 허가된다.

<85> 이용 유저 ID(212)는, 현재, 해당 디바이스를 이용하고 있는 이용자의 ID가 기록된다. 본 정보는, 인증 관리 서버(101)가 소정 시간마다 각 접속 기기에 폴링을 행하여, 취득한다.

<86> 다음으로, 인증 관리 서버(101)가 유지하는 이용자 정보 데이터베이스(300)에 대해 설명한다. 본 데이터베이스(300)는, 이용자가 네트워크(103)에 접속되어 있는 정보 센터(102) 밖의 기기로부터, 정보 센터(102) 내의 기기에의 접속을 요구한 경우, 접속을 요구하는 이용자가 허가 가능한 이용자 권한을 유지하고 있는지의 여부를 판정(인증)하기 위해 이용된다. 본 데이터베이스는, 미리 관리자에 의해 등록된다.

<87> 도 4는, 인증 관리 서버(101)가 유지하는 이용자 정보 데이터베이스(300)의 일례이다. 도 4에 도시한 바와 같이, 이용자 정보 데이터베이스(300)에는, 이용자 ID(301), 이용자명(302), 소속 그룹(303), 증명서(304), 유효 기간(305), 증명서 인증 가능(306), 암호 해시 방식(307), 패스워드(308), 패스워드 인증 가부(309)의 각 항목이, 유저마다 등록된다.

<88> 이용자 ID(301)는 이용자를 식별하기 위한 ID로서, 이용자마다 미리 부여된다. 이용자의 이용 권리가 변경되지 않으면 통상 변경은 되지 않는다. 이용자명(302)은, 이용자의 명칭을 나타내는 문자열이다. 이용자명(302)은, 이용 정보를 표시할 때에 이용된다. 소속 그룹(303)은, 이용자가 소속하는 그룹을 나타내는 정보이다. 본 실시예에서는, 각종의 이용 권한은 그룹 단위로 할당되도록 구성되어 있다. 소속 그룹(303)은, 각 이용자가 부여되어 있는 권한에 해당하는 그룹이 나타난다. 한 사람의 이용자가 복수의 그룹에 소속, 즉, 소속 그룹(303)에 복수의 그룹이 등록되어 있어도 된다. 또한, 소속 그룹은 미정의이어도 된다. 미정의의 경우, 해당 이용자에게는, 모든 이용 권한이 부여되어 있지 않은 것으로 된다.

<89> 증명서(304)는, 이용자의 인증에 이용하는 공개 키 증명서를 특정하는 정보이다. 증명서(304)로서 기록되어 있는 공개 키 증명서는, 그 유효성이 인증 관리 서버에서 검증 가능하게 되어 있는 것일 필요가 있다. 예를 들면, 인증 관리 서버(101) 내에 인증국을 가지고, 그 인증국이 발행을 행하도록 구성해도 된다.

<90> 유효 기간(305)은, 이용자가, 블레이드 서버(106) 내의 PC나 디바이스를 이용하는 권리를 갖는 기간이다. 유효 기간(305)이 미정의인 경우, 이용자는 PC를 이용할 권리가 없다. 유효 기간은 연, 월, 일 등을 이용한 기간의 설정 이외에 매주 월요일, 매일 8시 45분부터 17시 15분과 같은 기간의 설정도 가능하다. 유효 기간(305)은, 증명서(304)에 나타나는 공개 키 증명서의 유효 기한과는 독립적으로 설정할 수 있다.

<91> 증명서 인증 가능(306)은, 증명서 인증을 인정할지의 여부를 나타내는 정보이다. 암호 해시 방식(307)은, 인정하는 공개 키 인프라스트럭처를 이용하여 인증하는 경우의 암호 해시의 방식의 기재이다. 암호 해시 방식(307)이 미정의인 경우에는, 인증 관리 서버로부터 암호 해시 방식에 대한 제한은 없다. 이 경우라 하더라도, 클라이언트(이용자가 사용하는 PC 등) 등에 실장되어 있지 않은 방식으로는 인증은 행할 수 없다. 패스워드(308)는, 패스워드를 이용하여 인증이 행해지는 경우의 패스워드이다. 패스워드(308)로서, 해시값이나 암호화 등이 실시된 정보가 기록된다. 패스워드 인증 가부(309)는, 패스워드를 이용하여 인증하는 것이 가능한지 불가능한지를 나타내는 정보이다.

<92> 블레이드 서버(106)가 인증 관리 서버(101)에 인증 정보를 확인하여 인증을 얻는 것은, 이용자 정보 데이터베이스(300)에 기초한 패스워드나 공개 키 인프라스트럭처를 이용한 인증을 거쳐, 이용자가 블레이드 서버(106) 내의 PC를 이용 가능한 권한을 취득한 경우이다.

<93> 본 실시예에서는, 인증은, 1)액세스해 온 이용자가, 블레이드 서버(106)에의 액세스하는 권한을 갖는 사람인지의 여부, 그리고, 2)블레이드 서버(106) 내의 PC-A(110)가 할당된 후, 해당 PC-A(110)의 자원(프로그램이나 가상 디바이스)을 이용하는 권한을 갖는 사람인지의 여부의, 2 단계로 행해진다. 어떠한 경우에도, 이용자는 이용자 인증용 정보를 적어도 포함하는 인증 요구를 블레이드 서버(106) 또는 PC-A(110)에 송신하고, 인증 요구를 수취한 블레이드 서버(106) 또는 PC-A(110)는, 인증 관리 서버(101)에 액세스하여, 이용자 정보 데이터베이스(300)에 등록되어 있는 레코드와 대조하여, 인증을 행한다. 여기서, 이용자 인증용 정보란, 이용자 ID 및 패스워드, 혹은, 이용자마다 등록된 공개 키 정보에 대응하는 서명을 말한다.

<94> 다음으로, 정보 센터(102) 내의 각 PC의 이용 상황의 관리에 이용되는 PC 이용 관리 테이블(400)에 대해 설명한다. 도 5는, 블레이드 서버(106)가 유지하는, PC 이용 관리 테이블(400)의 일례이다.

<95> PC 이용 관리 테이블(400)에는, 정보 센터(102) 내의 각 PC마다, PC명(401), 네트워크명(402), IP 어드레스(403), MAC 어드레스(404), 이용원 단말기(405), 이용원 네트워크명(406), 이용원 IP 어드레스(407), 이용원 MAC 어드레스(408), 이용자 ID(409), 스테이터스(410), 접속 개시 시각(411), 접속 종료 시각(412), 동작 확인

시각(413)이 등록된다.

<96> PC명(401)은, 정보 센터(102) 내의 PC를 식별하는 PC의 명칭이다. 이것은, 관리자가 중복이 없도록 미리 정하여 등록한다. 네트워크명(402)은, 네트워크 상에서 PC를 식별할 때에 이용되는 명칭이다. 이것은, 관리자가 중복이 없도록 미리 정하여 등록한다. 각 PC에 대해, 네트워크명(402)과 PC명(401)은 동일한 명칭이 부여되어도 되고 서로 다른 명칭이 부여되어도 된다.

<97> IP 어드레스(403)는, 각각의 PC에 부여된 IP 어드레스이다. MAC 어드레스(404)는, 각각의 PC 상의 네트워크 인터페이스에 일의적으로 정해져 있는 어드레스이다.

<98> 이용원 단말기(405)는, 현 시점에서 이 정보 센터(102) 내의 PC를 원격 조작하고 있는 클라이언트 장치의 명칭이다. 이 명칭도, 관리자가 중복이 없도록 미리 정하여 등록한다. 관리자는 명칭을 자유롭게 설정, 변경할 수 있다. 해당 정보 센터(102) 내의 PC가 클라이언트 장치에 의해서 이용되고 있지 않은 경우, 이용원 단말기(405)는 미정의로 된다. 이용원 네트워크명(406)은, 네트워크(103) 상에서 이용원을 식별할 때에 이용되는 명칭이다. 관리자가 중복이 없도록 미리 정하여 등록한다. 또한, 이용원 단말기(405) 및 이용원 네트워크명은 동일한 명칭이어도 된다.

<99> 이용원 IP 어드레스(407)는, 클라이언트 장치의 IP 어드레스이다. 이용원 MAC 어드레스(408)는, 클라이언트 장치의 네트워크 인터페이스에 일의적으로 정해진 어드레스이다.

<100> 이용자 ID(409)는, 클라이언트 장치를 이용하고 있는 이용자의 이용자 ID이다. 클라이언트 장치가 사용되고 있지 않은 경우, 이용자 ID(409)는 미정의로 된다.

<101> 스테이터스(410)는, 해당 PC가 가동중인지의 여부를 나타내는 정보이다. 스테이터스(410)에 기록되는 정보에는, "가동중", "확인중", "대기중"의 3종류가 있다. 스테이터스(410)가 "가동중"인 PC는, 이용자 ID(409)에 등록되어 있는 ID를 갖는 이용자가 이용원 단말기(405)에 특정되어 있는 클라이언트 장치를 통하여 이용중임을 나타낸다. 스테이터스(410)가 "확인중"인 경우, 인증 관리 서버(101)에서 클라이언트 장치가 PC를 이용하고 있는지의 여부를 확인중인 상태, 또는, 확인이 완료되지 않은 상태임을 나타낸다. 스테이터스(408)가 "대기중"인 PC는, 클라이언트 장치가 PC의 이용을 대기하고 있는 상태, 즉, 클라이언트 장치가 PC를 이용하고 있지 않은 상태임을 나타내고 있다.

<102> 접속 개시 시각(411)은, 이용자 ID(409)로 특정되는 이용자가 이용원 단말기(405)로 특정되는 클라이언트 장치를 통하여 PC의 조작을 개시한 시각을 나타낸다. 접속 종료 시각(412)은, 이용자 ID(409)로 특정되는 이용자가 이용원 단말기(405)로 특정되는 클라이언트 장치를 통하여 행하는 PC의 조작을 종료한 시각을 나타낸다. 동작 확인 시각(413)은, 가상 디바이스 매니저(120)로부터 인증 관리 서버(101)에 대하여 채널의 생성, 소멸 등이 발생하였을 때에 행해진 통신의 최종 시각을 나타낸다.

<103> 블레이드 서버(106)는, 구성하는 각 PC의 이용 상황에 변경이 있을 때에, 본 데이터베이스를 갱신한다.

<104> 다음으로, 본 실시예의 디바이스 관리 시스템에서, 디바이스를 공유 가능한 상태로 설정하고, 설정 후에 디바이스를 공유하는 처리(이후, 디바이스 공유 처리라고 함)에 대해 설명한다. 여기서는, 이용자가 클라이언트 장치인 PC-D(113)를 이용하여 정보 센터(102) 내의 블레이드 서버(106)를 구성하는 기기 중 PC-A(110)을 원격 조작하고, PC-D(113)에 접속되어 있는 디바이스 A(151)를 공유 가능하게 하는 경우를 예로 들어 설명한다. 물론, 다른 이용자 단말기, 다른 블레이드 서버(106)를 구성하는 기기, 다른 디바이스이어도, 디바이스 공유 처리의 순서는 마찬가지이다.

<105> 도 6은, 상기 예에서의 디바이스 공유 처리의 처리 플로우이다.

<106> 이용자는 PC-D(113)에 기동 지시를 행한다(501). 이용자로부터의 기동 지시를 접수한 PC-D(113)는, 스토리지(163)로부터 OS나 어플리케이션을 로드하여 기동한다(502). 여기서, OS나 어플리케이션은, 네트워크 상에 존재하는 스토리지로부터 로드해도 된다. 이때, 디바이스 관리 매니저(123)도 기동된다.

<107> 스텝 502에서 기동된 디바이스 관리 매니저(123)는, PC-D(113)에 접속되어 있는 디바이스 A(151)의 정보를 취득한다(503). 접속되어 있는 디바이스의 정보의 취득은, 기동 시에, 호스트(본 실시예에서는, PC-D(113))측으로부터의 요구에 따라 디바이스측으로부터 호스트에 디바이스 전체의 정보에 관한 데이터인 디스크립터의 정보가 송신됨으로써 행해진다(504). 디스크립터에는, 예를 들면, 디바이스의 종별을 나타내는 코드, 디바이스의 클래스의 코드, 해당 디바이스의 제조 벤더의 ID, 제품 ID, 시리얼 번호 등이 포함된다. PC-D(113)에서는 스텝 503에서 취득한 디바이스의 정보에 데이터에 기초하여 디바이스 A(151)를 구동하는 디바이스 드라이버가 읽어 들여

져, 동작한다. 디바이스 관리 매니저(123)는, 관리하는 디바이스(여기서는, 디바이스 A(151))의 드라이버 혹은 필터 드라이버의 기능을 실현함으로써, 본 디바이스를 본 시스템 내에서 공유 가능한 상태로 하고, 해당 디바이스에 송수신되는 정보를 제어한다.

<108> 디바이스 관리 매니저(123)는, PC-D(113)에 접속되어 있는 디바이스 A(151)의 동작을 확인한 후, 디바이스 접속 요구와 함께 스텝 503에서 취득한 디바이스 A(151)의 디바이스의 정보로부터 추출한 디바이스 정보를 인증 관리 서버(101)에 송신한다(504). 인증 관리 서버(101)에서는, 디바이스 접속 요구 및 디바이스 정보를 수신하면, 폴리시 테이블(1400) 내의 데이터와 대조하여, 디바이스 접속 요구가 있었던 디바이스에 관한 폴리시를 디바이스 정보 관리 테이블(200)에 등록한다.

<109> 한편, PC-D(113)의 기동이 완료되면, PC-D(113)는, 기동이 완료된 취지를 디스플레이에 표시한다(506). 이용자는, 기동이 완료된 것을 확인하면, 정보 센터(102) 내의 블레이드 서버(106)를 구성하는 PC의 이용을 개시하도록 지시를 행한다. 본 실시예에서는, 이용 개시의 지시는, 이용자 ID 및 패스워드의 입력이다.

<110> PC-D(113)는, 이용자로부터 이용 개시의 지시를 접수하면(507), 블레이드 서버(106)를 이용하는 요구(이후, 서버 이용 개시 요구라 함)로 하여, 접수한 이용자 인증용 정보를 블레이드 서버(106)에 송신한다(508).

<111> 블레이드 서버(106)는, 서버 이용 개시 요구를 수취하면, 이용자가 블레이드 서버(106)의 적절한 이용 권한을 갖는지의 여부의 인증을 행한다(509). 구체적으로는, 블레이드 서버(106)는, 이용 개시 요구에 포함되는 이용자 ID 및 패스워드를 인증 관리 서버(101)에 송신하고, 인증을 의뢰한다(510). 인증 관리 서버(101)에서는, 수취한 이용자 인증용 정보를 이용자 정보 데이터베이스와 대조하여, 인증을 행하고, 결과를 블레이드 서버(106)에 회신한다. 여기서는, 이용자가 블레이드 서버(106) 자체에 액세스 권한을 갖는 사람인지의 여부를 인증한다.

<112> 블레이드 서버(106)가, 인증 관리 서버(101)로부터 인증 성공의 회신을 받은 경우, 블레이드 서버(106)는, 액세스해 온 이용자가 블레이드 서버(106)의 이용을 허가받은 것으로 판단하여, 블레이드 서버(106)를 구성하는 PC 중에서, 해당 이용자가 이용할 PC를 결정한다. PC는, 이용 순서에 따라서 적절하게 할당되거나, 미리 이용자에게 일대일 등으로 할당되거나, 이용자에게 할당된 어떠한 권한에 따라서 할당되거나 하는 어느 쪽의 형태이어도 된다. 어느 쪽의 형태를 취할지는 관리자가 결정한다. 여기서는, 블레이드 서버(106)가, 액세스해 온 이용자에게 PC-A(110)를 할당한 것으로 하여, 설명한다. 다른 PC를 할당한 경우에도, 처리는 마찬가지이다.

<113> 블레이드 서버(106)는, PC-D(113)에 할당하는 PC를 PC-A(110)로 결정하면, PC-A(110)의 기동 상황의 확인을 행한다(511). PC-A(110)가 기동되어 있지 않은 경우, PC-A(110)를 기동하는 요구를 PC-A(110)에 행한다(512). 송신한 요구에 따라서 PC-A(110)가 기동하면(513), PC-A(110)는, 기동 완료를 나타내는 정보를 블레이드 서버(106)에 통지한다(514). 또한, PC-A(110)가 이미 기동되어 있는 경우, 예를 들면, PC-A(110)가 서버 기능을 갖고, 복수인이 동시에 이용할 수 있는 환경으로서, 항상 통전되어 있는 경우 등, 스텝 511로부터의 PC의 기동 조작은 불필요하다.

<114> 또한, PC의 가동 상황은, PC 이용 관리 테이블(400)에 액세스하고, 해당하는 PC명(401)의 스테이터스(410)를 확인함으로써 행한다. 기동 후, 할당한 클라이언트 장치를, 해당하는 PC명(401)의 이용원 단말기(405)로서 추기한다.

<115> 한편, PC-A(110)가 기동하면, PC-A(110) 내에 인스톨되어 있는 가상 디바이스 매니저(120)는, 이용 가능한 디바이스를 확인한다(515). 구체적으로는, 가상 디바이스 매니저(120)는, 인증 관리 서버(101)에, 가상 디바이스 매니저(120)가 가동하는 PC(여기서는, PC-A(110))가 이용 가능한 디바이스의 조사의 요구(이후, 이용 가능 디바이스 조사 요구라고 함)를 송신한다(516).

<116> 이용 가능 디바이스 조사 요구를 수취한 인증 관리 서버(101)는, 디바이스의 조사와 확인을 행한다(517). 구체적으로는, 이용 가능 디바이스 조사 요구를 수취한 인증 관리 서버(101)는, 먼저, 신규 디바이스가 새로 등록되어 있는지의 여부를 확인하여, 이미 유지하고 있는 디바이스 정보 테이블(200)의 갱신을 행한다(518). 인증 관리 서버(101)는, 이용 가능 디바이스 조사 요구를 받아, 현 시점에서 디바이스 정보 테이블(200)에 등록되어 있는 각 디바이스에 대해, 해당 디바이스가 접속되어 있는 각각의 PC 또는 허브 등의 클라이언트 장치의 디바이스 관리 매니저를 향해, 등록되어 있는 각 디바이스가 여전히 이용 가능한지의 여부의 조회를 행한다(519).

<117> 인증 관리 서버(101)로부터 조회를 받은 각 클라이언트 장치의 디바이스 관리 매니저는, 현 시점에서의 조회를 받은 디바이스의 이용의 가부를 인증 관리 서버(101)에 회신한다(520). 또한, 각 디바이스 관리 매니저는, 이용의 가부를 나타내는 정보로서, 해당 디바이스가 이미 절단되어 있던 경우에는, 절단되어 있는 것을, 접속되어

있는 경우에는, 각 디바이스의 "점유중", "이용중", "통신중" 등의 현재의 스테이터스를 회신한다. 인증 관리 서버(101)는 각 디바이스 관리 매니저로부터 수취한 정보를 이용하여, 디바이스 정보 테이블(200)을 갱신한다. 절단되어 있다는 정보를 받은 경우에는, 해당 디바이스에 관한 레코드를 삭제한다.

<118> 그리고, 인증 관리 서버(101)는, 디바이스 정보 테이블(200)에 등록되어 있는 디바이스를 현 시점에서의 이용 가능 디바이스로 하여, 조회원의 가상 디바이스 매니저(120)에 송신한다(521).

<119> 다음으로, 가상 디바이스 매니저(200)는, 디바이스 정보 테이블(200)의 정보에 기초하여, 디바이스를 공유하는 처리를 행한다. 현 시점에서는, 가상 디바이스 매니저(120)는, 이용자의 인증을 행하고 있지 않는 상태이므로, 이용 가능 디바이스의 체크를 행할 때에 디바이스 정보 테이블에서 이용 가능 ID의 제한이 있는 디바이스에 대해서는 공유 처리를 행할 수 없다. 따라서, 가상 디바이스 매니저(200)는, 디바이스 정보 테이블(200)에 등록되어 있는 디바이스로서, 이용 가능 I D(211)가 미정의의 디바이스를 추출하고, 이들의 이용 가능한 디바이스와의 사이에서, 채널을 생성하는 등의 통신 준비를 행한다(522, 523).

<120> 또한, 인증 관리 서버(101)는, 가상 디바이스 매니저(120)로부터 이용 가능 디바이스 조사 요구를 받은 경우(516), 각 디바이스 관리 매니저(123)에 조회를 행하지 않고, 그 시점에서 디바이스 정보 테이블(200)에 등록되어 있는 디바이스로서, 이용 가능 ID(211)가 미정의의 디바이스를 추출하고, 조회원의 가상 디바이스 매니저(120)에 회신하도록 구성해도 된다(521). 이 경우, 스텝 517 ~ 스텝 520의 처리는 행해지지 않는다.

<121> 또한, 채널의 생성은, 가상 디바이스 매니저(120)가, 스텝 521에서 이용 가능 디바이스로서 수취한 각 디바이스가 접속되어 있는 클라이언트 장치가 구비하는 디바이스 관리 매니저와의 사이에서, 서로의 IP 어드레스와 인증 관리 서버(101)로부터 주어진 정보를 바탕으로 상호 인증, 키 교환을 행하고, 암호 통신로를 형성함으로써 행해진다(523).

<122> 상호 인증의 방법의 일례로서, 인증 관리 서버(101)가, 디바이스 관리 매니저(123)에 대해서는 디바이스 정보 송수신 시에, 또한 가상 디바이스 매니저(120)에 대해서는 이용 디바이스 회신 시에, 각각 프리쉐어드 키(사전 공유 키)를 안전하게 송부해 놓고, 그 사전 공유 키를 바탕으로 인증을 행하는 방식을 들 수 있다. 상호 인증의 방식은 특별히 본 방법에 한정되지 않고, 채널의 생성을 행하고 있는 상대가, 특정한 디바이스 관리 매니저와 가상 디바이스 매니저임을 확인할 수 있으면 된다.

<123> 상호 인증이 종료된 후, 가상 디바이스 매니저(120)와 디바이스 관리 매니저와의 사이에서 ID 정보 및 데이터를 교환하기 위한 암호용의 키가 교환된다. 이후, 여기서 교환된 암호용의 키를 이용하여 디바이스 관리 매니저와 가상 디바이스 매니저(120)가 통신을 행한다. 이 때문에, 제삼자에게는 ID 정보 및 데이터를 주고 받는 통신은 도청 불가능하게 된다. 이 암호용의 키는, 고정값이어도 되지만, 한 번의 이용마다 혹은 일정한 기간에 파기되어, 새로운 암호용의 키가 생성되도록 해도 된다.

<124> 본 실시예에서는, 이와 같이 가상 디바이스 매니저(120)와 디바이스 관리 매니저(123)와의 사이에서 채널이 생성된 경우, 해당 디바이스 관리 매니저(123)가 관리하는 디바이스가 공유 가능한 상태로 되었다고 한다. 이와 같은 제삼자에게 도청 불가능한 통신로(채널)에 의해, PC-A(110)는, PC-A(110)에 디바이스 A(151)가 직접 접속된 경우와 마찬가지로, 디바이스 A(151)를 제어할 수 있다.

<125> 즉, 본 실시예에서, "디바이스의 공유"란, PC-A(110)에 디바이스 A(151)가 직접 접속되었을 때와 마찬가지로 PC-A(110)가 처리를 행할 수 있도록 PC-A(110)가 동작하는 것이다. 예를 들면, PC-D(113)에 접속되어 있는 디바이스 A(151)에 대하여 "디바이스의 공유"가 실현된 경우, 디바이스 A(151)로부터 디바이스 관리 매니저(123), 가상 디바이스 매니저(120)를 통하여 PC-A(110)가 디바이스 A(151) 내에 설정되어 있는 통신 방식이나 디스크립터를 읽어내거나, 리세트하거나 할 수 있다.

<126> 또한, PC-A(110)에서, 디바이스 A(151)를 과거에 이용한 적이 없는 경우, 필요한 디바이스 드라이버를 인스톨한다. 일반적으로는, 디바이스의 공유가 행해졌을 때, PC-A(110) 상에서 동작하고 있는 오퍼레이팅 시스템이 새로 추가된 디바이스를 자동적으로 인식하고, 해당 디바이스의 동작에 필요한 디바이스 드라이버의 인스톨 작업을 행한다. 이러한 인스톨 작업은, PC-A(110)에서 처음으로 사용하는 디바이스가 PC-A(110)와 다른 기기와의 사이에서 공유되었을 때에 발생하고, 과거에 사용한 디바이스이면, 이미 필요한 드라이버가 PC-A(110)에 인스톨되어 있기 때문에, 발생하지 않는다.

<127> 또한, PC-A(110) 상에서 동작하고 있는 오퍼레이팅 시스템이 상기한 바와 같은 자동적으로 디바이스를 인식하고, 필요한 디바이스 드라이버의 인스톨을 행하는 기능을 갖지 않는 경우에는, 관리자 또는 이용자가 수동으로 디바이스 드라이버의 인스톨을 행하고, 디바이스가 이용 가능해지도록 PC-A(110)의 설정을 변경한다.

<128> 또한, 복수의 이용자가 디바이스 A(151)를 공유하고 있는 경우, 각 이용자가 각각 독립적으로 리세트를 지시하거나, 통신하거나 하는 경우가 있다. 이러한 경우에는, 디바이스 관리 매니저(123)는, 리세트를 접수하지 않는 순서로 변경하거나, 이미 디바이스 A(151)로부터 취득하여, 디바이스 관리 매니저(123) 내에 보존하고 있던 정보를 대신하여 송신하거나 하도록 구성한다. 구체적으로는, 가상 디바이스 매니저(120)로부터의 특정한 통신에 대하여, 미리 정해진 응답을 행한다.

<129> 또한, 여기서 생성된 채널의 정보는, 인증 관리 서버(101)에 송신되고 (591), 인증 관리 서버(101)에서는, 수취한 정보를 이용하여 디바이스 정보 테이블(200)을 갱신한다(592).

<130> 이상의 처리에 의해 PC-A(110)가 PC-D(113)의 이용자에 의해 이용 가능하게 된다.

<131> 다음으로, 이용자가 PC-D(113)를 통하여 PC-A(110)의 이용을 요구한다. 즉, PC-D(113)는 이용자로부터 PC-A(110)를 이용하는 지시를 접수하면, PC-D(113)는 PC를 이용하는 요구(이후, PC 이용 요구라고 함)를 생성하고, 그것을 PC-A(110)에 송신한다(524). 이 PC 이용 요구에는, 이용자를 특정하는 정보, 예를 들면, 이용자 ID, 패스워드 등이 포함된다.

<132> PC-A(110)는, PC 이용자 요구를 수취하고, 로그인 처리를 행한다(525). 로그인 처리는, 우선 PC-A(110)는, 이용자 요구에 포함되는 이용자를 특정하는 정보를 인증 관리 서버(101)에 송신한다. 인증 관리 서버(101)는, 수취한 이용자를 특정하는 정보와 이용자 정보 데이터베이스(300)에 저장되어 있는 정보를 대비하여, 이용자의 인증을 행하고, 결과를 PC-A(110)에 회신한다. 또한, 미리, 이용자 정보 데이터베이스(300) 내의 항목 중, 로그인 시의 이용자 인증에 필요한 항목만 PC-A(110)도 유지하고, 로그인 시의 인증을 PC-A(110)에서 행하도록 구성해도 된다.

<133> 다음으로, 가상 디바이스 매니저(120)는, 이용 가능 디바이스의 체크를 행한다. 여기서는, 가상 디바이스 매니저(120)는, 로그인한 이용자에 대한 이용 가능 디바이스를 추출한다. 이용 가능 디바이스를 추출하는 순서는, 상기 516에서 설명한 것과 기본적으로 마찬가지이다. 로그인한 이용자의 ID도 조회 시에 인증 관리 서버(101)에 송신하고, 해당 이용자의 ID가 이용 가능 ID로서 등록되어 있는 것만의 회신을 받아도 된다.

<134> 인증 관리 서버(101)는, 전술한 처리와 마찬가지로, 디바이스 정보 테이블(200)에 등록되어 있는 모든 디바이스에 대해, 해당 디바이스가 접속되어 있는 클라이언트 장치의 디바이스 관리 매니저에게 최신의 정보를 조회하고, 회신을 받아, 디바이스 정보 테이블(200)을 갱신한 후, 조회원의 가상 디바이스 매니저(120)에게 회신한다(529 ~ 532). 또한, 전술한 바와 마찬가지로, 인증 관리 서버(101)는, 이용 가능 디바이스 조사 요구에 따라서, 디바이스 정보 테이블(200)을 참조하여, 현 시점에서 해당 이용자에게 이용 가능한 것으로서 등록되어 있는 디바이스를, 조회원의 가상 디바이스 매니저(120)에 회신하도록 구성해도 된다(532).

<135> 첫회의 이용 가능 디바이스의 체크(516 ~ 521)에서는, 이용자가 특정되어 있지 않았기 때문에, 이용 가능 ID가 한정되어 있는 디바이스에 대해서는, 공유 처리, 즉, 통신로를 설정할 수 없었다. 그러나, 이용자의 로그인(525) 이후에는, 이용 가능 ID 중에 이용자의 ID 혹은 이용자가 소속하는 그룹의 ID가 들어 있는 디바이스는 이용이 가능하게 된다. 따라서, 이 시점에서 새로 이용이 가능해진 디바이스와의 사이에서, 전술한 바와 마찬가지로, 통신로(채널)를 개설한다(533 ~ 534).

<136> 또한, 이용 가능 디바이스와의 통신 준비(533)의 단계에서, 이용 가능 디바이스의 일람을 PC-A(110)의 화면, PC-D(113), 또는, 정보 센터(102) 내의 관리자가 확인 가능한 화면에 표시하도록 구성해도 된다. 이 경우, 이들의 화면에는, 현재 공유되어 있는 디바이스와, 접속 가능한 디바이스 등의 리스트가 표시되게 된다. 가상 디바이스 매니저(120)가 유지하고 있는 전회 종료 시각에 디바이스 공유 리스트에 있고, 현재 이용 가능한 디바이스는 이용자의 지시 없음에 채널의 생성을 행하는 것, 즉, 디바이스의 공유를 행할 수 있다. 디바이스의 공유를 행하는 것이 가능한 디바이스에 대한 공유 설정을, 이용자의 지시 없음에 행할지의 여부는, 관리자 또는 이용자에 의해 설정할 수 있도록 구성하는 것이 가능하다.

<137> 생성된 채널의 정보는, 인증 관리 서버(101)에 송신된다(593). 인증 관리 서버(101)에서는, 수취한 채널의 정보에 따라서 디바이스 정보 테이블(200)을 갱신한다(594). 그 후, PC-A(110)의 이용이 개시된다(535).

<138> 여기서, 이용 가능 디바이스의 체크, 이용 가능 디바이스 조사 요구, 디바이스의 조사와 확인, 디바이스 이용 가불가 조회, 디바이스 정보 취득, 디바이스 정보 송신 이용 가능 디바이스 회신(526 ~ 534), 채널 생성 정보의 송신(593), 및 테이블의 갱신(594)은, PC의 이용(535) 중 적절하게 반복하여 실행되고, 인증 관리 서버(101)가

갖는 디바이스 정보 테이블은 항상 최신의 상태로 계속 갱신된다.

<139> 여기서, 이용자가 로그인한 후의 가상 디바이스 매니저(120)에 의한 이용 가능 디바이스의 체크는, 정기적으로 행하는 것이 바람직하다. 가상 디바이스 매니저(120)는, 정기적으로 디바이스 정보 테이블(200)을 확인하고, 스테이터스의 변경에 의한 공유의 가부의 변화를 확인한다.

<140> 한편, 디바이스 정보 테이블(200)은, 디바이스 관리 매니저(120)에 의해, 디바이스의 접속 상황의 변화, 스테이터스의 변화 등, 디바이스에 관한 상태의 변화가 발생할 때마다, 변화 후의 상태를 나타내는 정보와 함께 갱신하도록 인증 관리 서버(101)에 통지가 이루어진다.

<141> 이상의 처리를 거쳐, 디바이스 관리 매니저(123)와 가상 디바이스 매니저(120)가 동작하여, 통신함으로써 디바이스 A(151)는, PC-A(110)의 디바이스로서 동작할 수 있다. 즉, 디바이스 A(151)에 대해, 디바이스의 공유가 실현된다.

<142> 다음으로, 본 실시예의 디바이스 관리 시스템에서의 디바이스 공유 종료 시의 처리에 대해 설명한다. 도 7은, 본 실시예의 디바이스 공유 처리 종료 시의 처리 플로우이다.

<143> 도 7에 도시한 바와 같이, 이용자는 PC-D(113)를 이용하여 PC-A(110)를 원격 조작하고, 디바이스 A(151)의 이용을 종료하여, 다른 이용자에게 디바이스 A(151)를 해방한다.

<144> 이용자는, PC-D(113)에 대하여 디바이스 이용 종료 지시를 행한다(601). PC-D(113)는, 이용자로부터 디바이스 이용 종료의 지시를 수취하면, 가상 디바이스 매니저(120)에 디바이스 이용 종료의 요구(이후, 디바이스 이용 종료 요구라고 함)를 송신한다(602). 가상 디바이스 매니저(120)는, 디바이스 이용 종료 요구를 수취하면, 이용 종료 디바이스의 체크를 행한다(603). 구체적으로는, 가상 디바이스 매니저(120)는, PC-A(110)에서, 디바이스의 이용을 종료해도 되는지의 여부를 판단한다.

<145> 예를 들면, PC-A(110) 상의 어플리케이션이나 다른 클라이언트 장치가 디바이스 이용 종료 요구의 대상 디바이스를 이용중인 경우, 이용은 종료할 수 없다. 이 경우에는, 이들의 어플리케이션이나 다른 클라이언트 장치가 디바이스 이용 종료 요구의 대상 디바이스의 이용을 종료할 때까지 종료 처리를 대기한다. 이 경우, PC-D(113)에 지시된 디바이스의 종료는 할 수 없다는 취지를 통지한다. PC-D(113)는 수취한 통지를 이용자에게 표시 등에 의해 통지한다.

<146> 또한, 이 통지는 반드시 행할 필요는 없으며, 예를 들면, 소정 시간 이상 대기 후라 하더라도 이용 종료를 행할 수 없는 경우만 통지하도록 구성해도 된다. 물론, 이용 종료 디바이스의 체크(603)에서, 이용 종료가 가능한 경우에는, 디바이스를 특정하는 정보와 함께, 해당 디바이스의 이용을 종료한 취지의 통지인 이용 종료 디바이스 송신을, 인증 관리 서버(101)에 행한다(604).

<147> 다음으로, 인증 관리 서버(101)는, 이용 종료 디바이스 송신을 받아, 디바이스의 조사와 확인을 행한다(605). 구체적으로는, 디바이스 이용 종료 요구원의 디바이스 관리 매니저(123)에, 지시된 디바이스의 이용이 종료하였음을 나타내는 정보인 디바이스 해방 정보 송신을 행한다(606).

<148> 디바이스 관리 매니저(123)는, 디바이스의 조사와 확인을 행한다(607). 여기서는, 디바이스로부터의 응답의 유무를 조사하는 등의 조사가 행해진다. 응답이 없으면, 디바이스 정보 테이블(200)의 해당하는 디바이스의 스테이터스를 "불명"으로 한다.

<149> 한편, 디바이스로부터 통상의 응답이 얻어진 경우에는, 디바이스 관리 매니저(123)는, 가상 디바이스 매니저(120)와의 사이에 확립되어 있던 채널을 파기하고 (608), 채널의 파기에 성공한 경우, 인증 관리 서버(101)에 채널의 파기를 끝냈음을 나타내는 정보인 채널 파기 정보를 송신한다(609).

<150> 인증 관리 서버(101)는, 채널 파기 정보를 받아, 디바이스 정보 테이블(200)의 갱신(610)을 행한다. 즉, 이 시점에서, 인증 관리 서버(101)는, 채널이 파기된 디바이스에 대해, 디바이스 정보 테이블(200)의 스테이터스(210)를, 예를 들면, " 점유중", "이용중", "통신중" 등으로부터, "미사용"으로 변경한다.

<151> 인증 관리 서버(101), 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)는, 도 6 및 도 7을 이용하여 설명한 일련의 동작에서 송신 혹은 수신한 데이터를, 각각 로그(191, 173, 170)로 하여 스토리지(190, 163, 160)에 기록한다.

<152> 다음으로, 도 6의 처리를 끝내고, 디바이스 A(151)가 공유 가능하게 되어 PC-A(110)의 디바이스로서 동작시킬 수 있도록 된 후의, 디바이스 관리 매니저(123)와 가상 디바이스 매니저(120)와의 사이의 데이터의 송수신 제어

의 상세 내용에 대해 설명한다.

<153> 도 8은, 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)와, PC-A(110) 및 PC-D(113)의 디바이스 드라이버 및 어플리케이션과의 관계(소프트웨어 스택)를 설명하기 위한 도면이다.

<154> PC-D(113)에 접속되어 있는 디바이스 A(151)를 PC-D(113) 상에서 동작하고 있는 어플리케이션(1211)으로부터 조작하여, 커맨드를 송수신하는 경우, 통상적으로, 디바이스 드라이버 인터페이스(1212)를 통하여, 복수의 드라이버(1213 ~ 1215)를 경유할 필요가 있다. 여기서, 드라이버(1213), 드라이버(1214)는, 디바이스 A(151)가 접속하고 있는 접속 인터페이스의 드라이버 등으로서, 드라이버(1213)는 가장 상위의 드라이버로서 드라이버(1214), 드라이버(1215)의 순으로 하위의 디바이스 단위의 드라이버로 된다.

<155> 디바이스 관리 매니저(123)는, 필터 드라이버(1210)를 구비한다. 필터 드라이버(1210)는, 드라이버(1213 ~ 1215)의 상위 필터 드라이버(어퍼 필터 드라이버) 혹은 하위 필터 드라이버(로워 필터 드라이버)로서 동작하고, 도시하는 화살표의 경로로 드라이버(1213 ~ 1215)를 이용하여 디바이스 A(151)와의 데이터의 송수신을 행한다. 즉, 필터 드라이버(1210)는, 디바이스 A(151)와, 드라이버(1215) 및 드라이버(1214)를 통하여 데이터의 송수신을 행한다.

<156> 또한, 필터 드라이버(1210)는 필터 드라이버로서 기재하고 있지만, 드라이버(1213 ~ 1215)의 기능의 일부 혹은 전부를 갖고 있어도 되고, 그 경우에는 일종의 디바이스 드라이버로서 행동한다.

<157> 디바이스 관리 매니저(123)와 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)가 구비하는 통신 모듈(1209)과 가상 디바이스 매니저(120)가 구비하는 통신 모듈(1206)과의 사이에서, 네트워크(103)를 통하여 데이터의 송수신을 행함으로써, 통신을 행한다.

<158> 가상 디바이스 매니저(120)는 디바이스 드라이버(1205)를 구비하고, 디바이스 드라이버(1205)는, PC-A(110) 내에서 동작하는 어플리케이션(1200) 등과 디바이스 A(151)와의 사이에서 데이터 송수신을 행할 때의 정보의 교환을 행한다.

<159> 어플리케이션(1200)과 디바이스 드라이버(1205)와의 사이의 데이터의 송수신은, 도시하는 화살표와 같이 어플리케이션(1200)으로부터 직접 행해지는, 디바이스 드라이버 인터페이스(1201)를 통하여 행해지거나, 또는, 드라이버(1202 ~ 1204)를 통하여 행해진다.

<160> GUI(1207 및 1208)는, 각각 가상 디바이스 매니저(120) 및 디바이스 관리 매니저(123)의 그래피컬 유저 인터페이스로서, 유저에의 정보 제공이나 유저로부터의 정보의 입력을 수취하는 역할을 다한다.

<161> 이상과 같이, 가상 디바이스 매니저(120)는, PC-A(110) 내의 어플리케이션으로부터, 본 실시예의 디바이스 관리 시스템 내에 존재하는 디바이스에 대한 데이터의 송수신을 행하는 입구로 된다. 가상 디바이스 매니저(120)는, 내부에 디바이스 드라이버(1205)와 통신 모듈(1206)을 구비하고, 네트워크(103)를 통하여 디바이스 관리 매니저(123) 및 인증 관리 서버(101)와 통신을 행하는 기능을 구비한다.

<162> 또한, 디바이스 관리 매니저(123)는, PC-D(113)에 접속된 디바이스 A(151)로부터 본 실시예의 디바이스 관리 시스템 내에 존재하는 PC 등과 송수신을 행하기 위한 입구로 되는, 디바이스 관리 매니저(123)는, 내부에 필터 드라이버(1210)와 통신 모듈(1209)을 구비하고, 네트워크(103)를 통하여 가상 디바이스 매니저(120) 및 인증 관리 서버(110)와 통신을 행하는 기능을 구비한다.

<163> 다음으로, 도 6에 도시한 채널의 생성(523 및 534)이 종료되고, 가상 디바이스 매니저(120)가 디바이스 A(151)를 컨트롤 가능하게 된 후에, 디바이스 A(151)를 이용하는 명령이 가상 디바이스 매니저(120)에 주어진 경우의 동작을 설명한다. 도 9는, 본 실시예의 디바이스 관리 시스템에서의 디바이스 이용 시의, 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)의 동작을 설명하는 플로우이다. 여기서는, 가상 디바이스 매니저(120) 측으로부터 트리거가 걸린 경우의 처리에 대해 설명한다.

<164> 도 6에 도시한 채널의 생성(523 및 534)이 종료되고, 가상 디바이스 매니저(120)가 디바이스 A(151)를 컨트롤 가능하게 된 후에, 디바이스 A(151)를 이용하는 명령이 가상 디바이스 매니저(120)에 주어지면(개시 700), 가상 디바이스 매니저(120)는, 디바이스 A(151)가 동작하는지의 여부를 확인한다(701). 구체적으로는, 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)에 소정의 커맨드를 송신하여, 디바이스 A(151)의 스테이터스의 취득의 가부, 통신 가능한 상태인지의 여부를 조회한다. 또는, 통신 경로가 확보되어 있는 상태인지를 확인한다. 그리고, 디바이스 관리 매니저(123)로부터의 회신 내용에 의해 판단한다.

<165> 동작하지 않은 경우, 디바이스 A(151)가 부정한 상태에 있음을 인증 관리 서버(101)에 통지하고, 인증 서버(101) 및 가상 디바이스 매니저(120) 각각이 로그(191, 170)에 기재한다(702). 가상 디바이스 매니저(120)는, 로그(170)에의 기재를 끝내면, 주어진 명령에 대한 처리를 부정 종료한다(716). 이때, 가상 디바이스 매니저(120)는, 부정 종료를 나타내는 에러 메시지를 이용자에게 통지해도 된다. 또한, 부정한 상태에 있다는 통지를 받았을 때, 자동적으로 디바이스 A(151)와의 통신의 종료 처리를 행하도록 구성해도 된다. 또한, 동작 확인의 시행은 복수회 행하고, 복수회 행하였다고 하더라도 부정한 상태라는 통지가 계속되는 경우, 702로 진행하도록 구성해도 된다.

<166> 한편, 스텝 701에서 디바이스 A(151)의 동작이 확인된 경우, 가상 디바이스 매니저(120)는 인증 관리 서버(101) 및 디바이스 관리 매니저(123)에 필요에 따라 생존 확인을 위한 통지를 행한다(703). 본 처리에 의해 인증 관리 서버(101) 및 디바이스 관리 매니저(123)는 디바이스 A(151)와의 채널이 확립되어 있는 것의 확인이 가능하게 된다.

<167> 다음으로, 가상 디바이스 매니저(120)는, 디바이스 A(151)를 이용하는 트리거로 되는 지시(예를 들면 PC-A(110)로부터)를 받았는지의 여부를 판별한다(704). 트리거로 되는 지시가 없다고 판별된 경우, 스텝 701로 되돌아간다.

<168> 한편, 트리거로 되는 지시가 있다고 판별된 경우, 가상 디바이스 매니저(120)에서, 디바이스 인터페이스 프로토콜에 의거한 트랜잭션을 생성한다(705). 그리고, 생성된 트랜잭션은 네트워크 프로토콜에 규정된 프로토콜로 변환되어 디바이스 관리 매니저(123)에 송신된다(706).

<169> 다음으로, 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)에 트랜잭션(데이터)이 정확하게 도달되었는지, 정확하게 도달되지 않은 경우 그 횟수가 미리 지정한 횟수를 넘지 않았는지를 판단한다.

<170> 구체적으로는, 먼저, 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)에 데이터가 정확하게 도달하지 않은 횟수가 지정 횟수에 도달하였는지의 여부를 판별한다(707).

<171> 지정 횟수에 도달한 경우, 가상 디바이스 매니저(120)는, 통신이 부정한 상태에 있다고 판단하여, 이것을 인증 관리 서버(101)에 통지함과 함께, 로그(170)에 기록한다. 통신이 부정한 상태에 있다는 정보는, 인증 관리 서버(101)의 로그(191)에서도 기록하도록 구성해도 된다. 가상 디바이스 매니저(120)는, 로그(170)에의 기재가 종료된 후, 부정 종료된다(709). 가상 디바이스 매니저(120)는, 에러를 이용자에게 통지해도 되고, 자동적으로 디바이스 A(151)와의 통신의 종료 처리에 들어가도 된다.

<172> 한편, 스텝 707에서 횟수가 지정 횟수에 도달하지 않은 경우, 가상 디바이스 매니저(120)는, 디바이스 관리 매니저(123)에 정확하게 데이터가 도달하였는지의 여부의 체크를 행한다(710). 구체적으로는, 송신한 데이터에 대한 레스펀스에 의해, 부정이라고 판단된 경우, 혹은, 소정의 시각까지 레스펀스가 없는 경우, 정확하게 도달하지 않았다고 판단한다. 그리고, 정확하게 도달하지 않았다고 판단된 경우, 정확하게 도달하지 않은 횟수를 1 인크리먼트하고, 스텝 707로 되돌아간다.

<173> 스텝 710에서 정확하게 데이터가 도달한 경우, 가상 디바이스 매니저(120)는, 송신하고 있지 않은 트랜잭션이 있는지의 여부를 확인한다(711). 그리고, 미송신의 트랜잭션이 있는 경우, 스텝 706으로 되돌아가, 처리를 반복한다.

<174> 미송신의 트랜잭션이 없는 경우, 가상 디바이스 매니저(120)는, 수신할 트랜잭션이 있는지의 여부의 체크를 행한다(712). 이것은, 양자 사이의 통신로를 설정하였을 때에 미리 정해진 데이터량분의 데이터의 송신이 끝났는지의 여부에 의해 판단한다.

<175> 수신할 트랜잭션이 있는 경우, 가상 디바이스 매니저(120)는, 수신한 데이터를 디바이스 인터페이스 프로토콜로 변환한다(713). 다음에 추출한 데이터를 디바이스 드라이버에 송신하고(714), 스텝 712로 되돌아간다.

<176> 한편, 스텝 712에서 수신할 트랜잭션이 없는 경우, 가상 디바이스 매니저(120)는, 처리를 종료한다(715).

<177> 또한, 상기 처리에서, 처리가 부정 종료된 경우(스텝 716, 709), 인증 관리 서버(101), 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)는, 처리가 부정 종료된 시점에서, 적절하게 이용할 수 있는 디바이스를 재확인하고, 인증 관리 서버(101) 내의 디바이스 정보 관리 테이블(200)을 갱신한다. 즉, 가상 디바이스 드라이버(120)는, 디바이스를 재확인할 수 있으면, 다시 정상적인 통신을 행하여, 채널의 생성이 가능하면 생성하고, 디바이스 정보 테이블(200)의 스테이터스를 "점유중", "통신중", "이용중"으로 한다.

<178> 다음으로, 도 6에 도시한 채널의 생성(523 및 534)이 종료되고, 디바이스 관리 매니저(123)가 디바이스 A(151)를 컨트롤 가능하게 된 후에, 디바이스 A(151)가 디바이스 관리 매니저(123)에 대하여, 정보를 송신하는 경우의 동작을 설명한다. 도 10은, 본 실시예의 디바이스 관리 시스템에서의 디바이스 이용 시의 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)의 동작을 설명하는 플로우이다. 여기서는, 디바이스 A(151)측으로부터 트리거가 걸린 경우의 처리에 대해 설명한다.

<179> 도 6에 도시한 채널의 생성(523 및 534)이 종료되고, 디바이스 관리 매니저(123)가 디바이스 A(151)를 컨트롤 가능하게 된 후에, 디바이스 A(151)가 디바이스 관리 매니저(123)에 정보를 송신하면(개시 800), 디바이스 관리 매니저(123)는, 디바이스 A(151)가 동작하는지의 여부를 확인한다(801). 동작 확인은, 도 9의 처리와 마찬가지이다.

<180> 동작하지 않은 경우, 디바이스 A(151)가 부정한 상태에 있음을 인증 관리 서버(101)에 통지하고, 인증 서버(101) 및 디바이스 관리 매니저(123) 각각이 로그(191, 173)에 기재한다(802). 디바이스 관리 매니저(123)는, 로그(173)에의 기재를 끝내면, 부정 종료한다(816). 이때, 디바이스 관리 매니저(123)는, 부정 종료를 나타내는 에러 메시지를 이용자에게 통지해도 된다. 또한, 부정한 상태에 있는 것의 통지를 받았을 때, 자동적으로 디바이스 A(151)와의 통신의 종료 처리를 행하도록 구성해도 된다. 또한, 동작 확인의 시행은 복수회 행하고, 복수회 행하였다고 하더라도 부정한 상태라는 통지가 계속되는 경우, 802로 진행하도록 구성해도 된다.

<181> 한편, 스텝 801에서 디바이스 A(151)의 동작이 확인된 경우, 디바이스 관리 매니저(123)는, 인증 관리 서버(101) 및 가상 디바이스 매니저(120)에 필요에 따라 생존 확인을 위한 통지를 행한다(803). 본 처리에 의해 인증 관리 서버(101) 및 가상 디바이스 매니저(120)는 디바이스 A(151)와의 채널이 확립되어 있는 것의 확인이 가능하게 된다.

<182> 다음으로, 디바이스 관리 매니저(123)는, 디바이스 A(151)를 이용하는 트리거로 되는 지시를(예를 들면 PC-A(110)로부터) 받았는지의 여부를 판별한다(804). 트리거로 되는 지시가 없다고 판별된 경우, 스텝 801로 되돌아간다.

<183> 한편, 트리거로 되는 지시가 있었다고 판별된 경우, 디바이스 관리 매니저(123)에서, 디바이스 인터페이스 프로토콜에 의거한 트랜잭션을 생성한다(805). 그리고, 생성된 트랜잭션은 네트워크 프로토콜로 정의된 패킷으로 변환되어 가상 디바이스 매니저(120)에 송신된다(806).

<184> 다음으로, 디바이스 관리 매니저(123)는, 가상 디바이스 매니저(120)에 정확하게 트랜잭션(데이터)이 도달하고 있거나, 정확하게 도달하지 않은 경우, 그 횟수가 미리 지정한 횟수를 넘지 않았는지를 판단한다.

<185> 구체적으로는, 먼저, 디바이스 관리 매니저(123)는, 가상 디바이스 매니저(120)에 데이터가 정확하게 도달하지 않은 횟수가 지정 횟수에 도달하였는지의 여부를 판별한다(807).

<186> 지정 횟수에 도달한 경우, 디바이스 관리 매니저(123)는, 통신이 부정한 상태에 있다고 판단하여, 이것을 인증 관리 서버에 통지함과 함께, 로그(173)에 기록한다. 통신이 부정한 상태에 있다는 정보는, 인증 관리 서버(101)의 로그(191)에라도 기록하도록 구성해도 된다. 디바이스 관리 매니저(123)는, 로그(173)에의 기재가 종료된 후, 부정 종료된다(809). 디바이스 관리 매니저(123)는, 에러를 이용자에게 통지해도 되고, 자동적으로 디바이스 A(151)와의 통신의 종료 처리에 들어가도 된다.

<187> 한편, 스텝 807에서 횟수가 지정 횟수에 도달하지 않는 경우, 디바이스 관리 매니저(123)는, 가상 디바이스 매니저(120)에 정확하게 데이터가 도달해 있는지의 여부의 체크를 행한다(810). 여기서, 정확하게 도달하지 않았다고 판단된 경우, 정확하게 도달하지 않은 횟수를 1 인크리먼트하고, 스텝 807로 되돌아간다.

<188> 스텝 810에서 정확하게 데이터가 도달한 경우, 디바이스 관리 매니저(123)는, 송신하지 않은 트랜잭션이 남아 있는지의 여부의 체크를 행한다(811). 그리고, 미송신의 트랜잭션이 남아 있는 경우, 스텝 806으로 되돌아가, 처리를 반복한다.

<189> 미송신의 트랜잭션이 남아 있지 않은 경우, 디바이스 관리 매니저(123)는, 수신할 트랜잭션이 있는지의 여부의 체크를 행한다(812).

<190> 수신할 트랜잭션이 있는 경우, 디바이스 관리 매니저(123)는, 수신한 데이터를 디바이스 인터페이스 프로토콜로 변환한다(813). 그리고, 추출한 데이터를 디바이스 드라이버에 송신하고(814), 스텝 812로 되돌아간다.

<191> 한편, 스텝 812에서 수신할 트랜잭션이 없는 경우, 디바이스 관리 매니저(123)는, 처리를 종료한다(815).

<192> 또한, 상기 처리에서, 처리가 부정 종료된 경우(스텝 816, 809), 인증 관리 서버(101), 디바이스 관리 매니저(123) 및 가상 디바이스 매니저(120)는, 처리가 부정 종료된 시점에서, 적절하게 이용할 수 있는 디바이스를 재확인하고, 인증 관리 서버(101) 내의 디바이스 정보 관리 테이블(200)을 갱신한다. 즉, 디바이스 관리 매니저(120)는, 디바이스를 재확인할 수 있으면, 다시 정상적인 통신을 행하고, 채널의 생성이 가능하면 채널을 생성하고, 디바이스 정보 관리 테이블(200)의 스테이터스를 "점유중", "통신중", "이용중"으로 한다.

<193> 이상의 동작에 의해 인증 관리 서버(101) 및 가상 디바이스 매니저(120) 및 디바이스 관리 매니저(123)에 의해 축적된 로그(191, 170, 173)는, 네트워크 관리자에 의해, 인증 관리 서버(101) 혹은 그 밖의 관리 기기에 인스톨된 관리 어플리케이션에 의해서 표시된다.

<194> 도 11에 관리 어플리케이션에 의해 표시되는 로그 관리 화면의 일례를 도시한다. 도 11에 도시한 관리 로그는, 인증 관리 서버(101), 가상 디바이스 매니저(120) 및 디바이스 관리 매니저(123) 내에 보존된 로그(191, 170, 173)를, 인증 관리 서버(101)가 수집하고, 자신의 스토리지(190) 혹은 메모리에 축적한 것을 표시한 것이다.

<195> 이 표시를 위한 어플리케이션(관리 어플리케이션)은, 인증 관리 서버(101) 이외에 있어도 된다. 그 경우, 인증 관리 서버(101)로부터의 허락을 받아 표시가 행해진다. 정보 센터(102) 및 블레이드 서버(106)가 복수 존재하는 구성에서는, 관리 어플리케이션은, 인증 관리 서버(101) 이외의 인증 관리 서버와 그 관리하는 어플리케이션으로부터 로그를 수집하고, 모은 로그를 합한 것을 표시해도 된다.

<196> 디바이스 관리 화면(1000)은, 관리 어플리케이션이 표시하는 디바이스의 관리를 행하기 위한 화면이다. 디바이스 관리 화면(1000)에는, 축적된 각 로그(191, 170, 173)의, 번호(1001), 시각(1002), 디바이스 ID(1003), 디바이스명(1004), 어드레스(소스)(1005), 네트워크 인터페이스 ID(소스)(1006), 어플리케이션 ID(1007), 어드레스(호스트)(1008), 네트워크 인터페이스 ID(호스트)(1009), 어플리케이션 ID(1010), 벤더 ID(1011), 제품 ID(1012), 시리얼 번호(1013), 디바이스명(1014), 이용 유저 ID(1015), 정보(1016), 비고(1017)의 각 항목이 표시된다.

<197> 번호(1001)는, 로그를 관리하기 위한 번호로서, 로그가 축적될 때마다 자동적으로 부여된다. 시각(1002)은, 로그가 기록된 일시이다. 정보(1016)는, 로그(170, 173, 191)에 로그로서 기록된 이벤트의 내용이 상세하게 표시된다.

<198> 어드레스(소스)(1005), 어드레스(호스트)(1008)는, 소스 및 호스트(디스티네이션)의 어드레스를 나타낸다. 네트워크 인터페이스 ID(소스)(1006) 및 네트워크 인터페이스 ID(호스트)(1009)는, 소스 및 호스트(디스티네이션)의 네트워크 인터페이스 ID를 나타낸다. 비고(1017)에는, 정보(1016)에서 표시할 수 없는 정보, 예를 들면, 관리자에게 주의를 재촉하는 정보, 정보(1016)를 보충하는 정보가 표시된다.

<199> 그 밖의 항목은 도 2 ~ 도 4를 이용하여 설명한 디바이스 정보 테이블(200), 이용자 정보 데이터베이스(300), PC 이용 관리 테이블(400)의 동명의 항목과 동일한 것이다.

<200> 또한, 인증 관리 서버(101)는, 디바이스 관리 화면(1000)에 표시되는 각 정보를 검색하는 기능을 가진 관리 어플리케이션을 탑재하고 있다. 디바이스 관리 화면(1000)에 나타내는 정보를 관리 어플리케이션이 표시함으로써, 어떤 기기나 디바이스가 어떠한 상태인지를 순간적으로 파악할 수 있어, 시스템 전체의 편리성이 향상된다. 예를 들면, 부정한 인증이 발생한 경우의 정보만을 검색하여 표시하고, 감시함으로써, 부정 액세스를 발견하여, 그 대책을 강구할 수 있다. 또한, 적절하게 디바이스를 이용할 수 없는 경우의 정보만을 검색하여 표시하고, 감시함으로써, 시스템 내에서 발생하고 있는 트러블을 조기 발견하여, 대응할 수 있다. 또한, 관리 어플리케이션에 의해 로그 전체를 일람하는 것과 비교하여 표시를 보기 편하게 함으로써, 관리자의 오퍼레이션 미스를 줄일 수 있다. 이들에 의해, 시스템 전체의 시큐러티가 향상된다는 효과가 얻어진다.

<201> 다음으로, 가상 디바이스 매니저(120)가 생성하고 표시시키는 디바이스 관리 화면의 상세 내용에 대해 설명한다. 도 12는, 가상 디바이스 매니저(120)의 디바이스 관리 화면의 일례이다.

<202> 도 12에 도시한 바와 같이, 디바이스 관리 화면(900)은, 인증 관리 서버 표시부(901)와, 접속 PC 허브 표시부(902, 905, 908, 911)와, 디바이스 표시부(903, 906, 909, 912)와, 접속 절단 지시부(904, 907, 910, 913)를 구비한다.

<203> 가상 디바이스 매니저(120)는, 기동되면 미리 지정되어 있는 인증 관리 서버(101)에, 이용 가능한 디바이스 정보를 취득하도록 요구를 보낸다.

<204> 인증 관리 서버(101)에서, 이용자의 인증에 성공한 후, 디바이스 관리 매니저(123)로부터 디바이스 관리 정보가

가상 디바이스 매니저(120)에 송부된다. 수취한 디바이스 관리 정보에 따라서, 가상 디바이스 매니저(120)는, 이용 가능한 디바이스의 정보 등을 관리한다.

<205> 도 12에서 인증 관리 서버 표시부(901)에는, 가상 디바이스 매니저(120)가 통신하고 있는 인증 관리 서버(101)가 표시된다. 도 12에 도시하는 예에서는 가상 디바이스 매니저(120)가 인증 관리 서버(101)와 통신에 성공하고 있는 모습이 표시되어 있다. 여기서, 192.168.0.1로 표시되어 있는 것은, 인증 관리 서버(101)의 어드레스이다.

<206> 스테이터스(920)에는, 인증 관리 서버(101)의 스테이터스가 표시된다. 여기서는, 스테이터스로서 이용 가능 유저 ID는 무엇인지, 이용자명은 무엇인지 등이 표시되어 있다. 도 12의 예에서는 유저 A가 인증되어 있는 모습이 표시되어 있다.

<207> 접속 PC 허브 표시부(902, 905, 908, 911)는, 접속되어 있는 PC, 허브의 정보가 표시된다. 또한, 이용자가 현재 사용중인 디바이스가 색 분리되어 표시되어 있다.

<208> 디바이스 표시부(903, 906, 909, 912)에는, 디바이스의 명칭이나 스테이터스, 이용자 ID 등의 정보가 표시되고, 이용자가 어떤 디바이스를 사용하는 것이 가능한지 등의 정보가 이해하기 쉽게 표시된다.

<209> 접속 절단 지시부(904, 907, 910, 913)에는, 디바이스의 이용이나 전유화, 이용 정지, 예약 등, 이용자가 지시를 부여할 수 있는 선택지를 표시시킨다. 가상 디바이스 매니저(120)는, 예약 버튼의 누름을 접수함으로써, 현재 다른 사람이 이용중인 디바이스의 이용 예약을 행한다. 그리고, 디바이스가 이용 가능하게 된 경우, 인증 관리 서버(101) 혹은 디바이스 관리 매니저(123)에게 이용 가능하게 된 취지의 통지를 행한다. 통지를 받은 디바이스 관리 매니저(123)는, 이용자에게 이용 가능하게 된 취지의 통지를 행한다. 도 12의 예에서는, 이용자가 이용할 수 있는 디바이스는 해칭으로 나타내고, 또한 이용자가 행하는 것이 가능한 조작은 굵은 글자의 버튼으로 나타내며, 조작하기 쉽게 되도록 배려되어 있다.

<210> 이상, PC-D(113)를 이용하여 블레이드 서버(106) 내의 PC-A(110)를 이용하는 서버 클라이언트 방식에 대해 설명하였다.

<211> 이미 설명한 예와 마찬가지로 네트워크(103) 및 인터넷(104)에 접속된 클라이언트 장치로부터, 블레이드 서버(106) 내의 어느 하나의 PC를 이용하고, 또한, 디바이스 A(151) ~ 디바이스 Z(155)를 사용하는 것이 가능하다.

<212> 여기서, 허브(116)는, PC로서의 기능은 갖지 않지만, 내부에 관리 매니저(126) 및 스토리지(176)를 갖는 내장 기기이다. PC-E(114)와 같이 디바이스를 접속하지 않은 PC를 이용하는 경우에도, PC-D(113)의 예와 마찬가지로 다른 PC 등에 접속되어 있는 디바이스를 사용하는 것이 가능하다. 또한, 허브(116)와 같이 복수대의 디바이스를 접속하고 있어도 마찬가지이다.

<213> 또한, 인터넷(104) 및 파이어월(105)을 통한 PC-Z(117)를 이용하여 네트워크(103) 상의 PC나 디바이스를 이용하는 경우에도, 기본적으로 마찬가지이다. 단, 이 경우, PC-Z(117)는, 인터넷(104) 상의 통신을 암호화하는 암호화 어플리케이션(190)을 내부에 갖고, 암호화하여 통신을 행하는 것이 바람직하다.

<214> 상기한 바와 같이, 본 실시예에 제시한 디바이스 관리 시스템은, 관리된 디바이스에 관해서 가상 디바이스 매니저(120)와 디바이스 관리 매니저(123)와 인증 관리 서버(101)에 의해 클라이언트 장치를 통하여 네트워크(103)에 접속된 디바이스를 관리함으로써, 시스템 내에서의 디바이스의 공유를, 안전하고 이용자에게 사용하기 편하게 실현할 수 있다.

<215> 또한, 본 실시예에 따르면, 다른 클라이언트 장치에 접속되어 있는 디바이스라 하더라도, 마치 서버에 직접 접속된 디바이스인 것처럼 사용하는 것이 가능하게 된다. 즉, 디바이스가, 다른 클라이언트 장치에 접속되어 있는 경우라 하더라도, 그 디바이스를 사용하기 때문에, 각 클라이언트 장치에는 특별한 구성이 필요하지 않다. 따라서, 디바이스를, 가상적으로 서버에 접속하는 경우에도, 직접 서버에 접속하는 경우에도, 동일한 구성을 취하는 것이 가능해지고, 시스템 전체의 제조 비용을 저감할 수 있다.

<216> 또한, 본 실시예에 따르면, 인증 관리 서버(101)에 의해, 디바이스의 허가, 불허가를 관리하고, 허가되지 않은 디바이스는 가상 디바이스로서 이용할 수 없는 설정으로 할 수 있다. 이 때문에, 네트워크(103) 상에 접속되는 디바이스의 적절한 관리를 행할 수 있고, 서버 클라이언트 시스템에서, 원격지에 있는 서버와의 사이에서, 디바이스를 공유하는 경우의 안전성을 높일 수 있다.

<217> 또한, 디바이스를 공유 가능한 상태로 하는 순서에서 인증을 행하고, 디바이스를 이용자가 이용할 수 있는지의 여부를 룰 부여함으로써, 이용자가 가까이에서 조작하는 PC, 신 클라이언트 등의 단말기와 원격지에 있는 서버와의 사이에서 디바이스를 공유하는 안전하면서 간편한 수단을 제공할 수 있기 때문에, 시스템 이용 시의 시큐러티가 향상됨과 함께, 이용자의 편리성도 향상된다.

<218> 본 실시예에서는, 전술된 바와 같이, 주된 프로그램이나 데이터를 서버측에 축적하고, 클라이언트측은 주로 서버에 조작 지시를 부여하기만 하는 구성을 갖는 서버 클라이언트 시스템이다. 따라서, 조작측의 클라이언트 장치 내에 남는 기밀 정보를 저감하는 등의 특징을 계속 남기면서, 클라이언트 이용 시의 시큐러티 및 편리성을 향상시킨 정보 처리 시스템을 제공할 수 있다.

<219> 또한, 상기한 실시예에서는, 서버나 클라이언트에 대응하는 정보 기기를 모두 PC로서 설명하였지만, 한쪽 및 양쪽이 서버, Personal Digital Assistants(PDA), 워크스테이션, 고기능 복사기, 현금 자동 인출기(ATM), 휴대 전화, 디지털 스틸 카메라, 음악 재생(녹음) 장치, 판매 시점 상품 관리 시스템, 길모퉁이 단말기, Intelligent Transport systems(ITS)용 송신기, 매표기, 결제 단말기, 자동 판매기, 입퇴실 관리 장치, 게임기, 공중 전화, 주문 받기용 휴대 단말기 등이어도 된다. 이들의 경우도 마찬가지의 효과가 얻어진다.

<220> <<제2 실시예>>

<221> 다음으로, 본 발명을 적용한 제2 실시예에 대해 설명한다. 본 실시예는, 기본적으로 전술한 제1 실시예와 동일하다. 단, 제1 실시예에서는, 디바이스는, PC 또는 허브 등을 통하여 네트워크(103)에 접속되어 있지만, 본 실시예에서는, 디바이스가 직접 네트워크(103)에 접속된다. 이 때문에, 본 실시예의 디바이스는, 디바이스 관리 매니저 등을 내부에 구비한다.

<222> 도 13은, 본 실시예의 디바이스 관리 시스템의 상세한 블록도이다. 도 13에서, 도 1에 도시하는 제1 실시예의 동명의 기기는, 기본적으로 마찬가지의 구성을 갖는 것이다. 본 실시예에서는, 또한, 디바이스 X(1101)가 네트워크(103)에 접속되어 있다.

<223> 디바이스 X(1101)는, CD-ROM 등의 스토리지 디바이스, 또는, 키보드, 디스플레이 등의 휴먼 인터페이스 디바이스 등의 주변 기기이다. 도 13에 도시한 바와 같이, 본 실시예의 디바이스 X(1101)는, 제1 실시예의 허브(116)의 기능을 내부에 포함하고 있다. 즉, 디바이스 X(1101)는, 도시하지 않은 네트워크 인터페이스를 통하여 네트워크(103)에 접속하고, 하드 디스크 드라이브 혹은 플래시 메모리 등 스토리지(1166) 및 도시하지 않은 메모리 및 CPU를 구비하고, 연산을 행하는 허브(1116)를 구비한다. 디바이스 X(1101)는, 허브(1116)에서, 디바이스 관리 매니저(1126)를 실현한다. 또한, 스토리지(1166)에는 로그(1176)를 유지한다.

<224> 따라서, 본 실시예의 디바이스 X(1101)는, 제1 실시예의 각 디바이스와 마찬가지로, 블레이드 서버(106) 내의 PC 등의 가상 디바이스로서 이용자는 이용할 수 있다. 또한, 제1 실시예의 허브(116)와 마찬가지로, 디바이스 관리 매니저(1126)에 의해, 본 디바이스 관리 시스템 내에서, 적절한 관리를 받을 수 있다.

<225> 즉, 본 실시예에 도시한 디바이스 관리 시스템은, 제1 실시예에 기술한 디바이스 관리 시스템의 특징 이외에, 또한 디바이스 X(1101)와 같이 허브(116)의 기능을 갖는 디바이스를 네트워크(103)에 직접 접속할 수 있는 편리성을 갖는다.

<226> 이 편리성에 의해, 본 실시예에 기술한 디바이스 관리 시스템은, 제1 실시예에 제시한 디바이스 관리 시스템의 효과 이외에, 이용자가 디바이스를 접속하는 허브나 PC를 한정하지 않더라도, 네트워크(103) 상에 디바이스 X(1101)를 삽입함으로써, 즉, 네트워크(103)가 갖는 인터페이스에 디바이스 X(1101)를 직접 접속함으로써, 네트워크 상의 PC로부터 디바이스 X를 이용하는 것이 가능하게 된다. 또한, 디바이스를 접속하는 허브나 PC가 불필요하게 된다. 따라서, 높은 안전성을 유지하면서, 이용자의 편리성이 더욱 높아진다. 그리고, 시스템 구성의 비용이 저감한다.

<227> <<제3 실시예>>

<228> 다음으로, 본 발명을 적용한 제3 실시예에 대해 설명한다. 본 실시예는, 기본적으로 전술한 제2 실시예와 동일하다.

<229> 도 14는, 본 실시예의 디바이스 관리 시스템의 상세한 블록도이다. 도 14에 도시한 바와 같이, 본 실시예의 디바이스 관리 시스템은, 제2 실시예의 디바이스 관리 시스템과 마찬가지로, CD-ROM 등의 스토리지 디바이스, 또는, 키보드, 디스플레이 등의 휴먼 인터페이스 디바이스 등의 주변 기기로서, 도시하지 않은 네트워크 인터페이스를 통하여 네트워크(103)에 접속하고, 하드 디스크 드라이브 혹은 플래시 메모리 등 스토리지(1166) 및 도시

하지 않은 메모리 및 CPU를 구비하고, 연산을 행하는 허브(1116)를 구비하는 디바이스 Y(1201)를 구비한다.

<230> 본 실시예의 디바이스 Y(1201)는, 또한, 허브(1116) 내부에, 인체 통신용 인증 장치(1206)를 구비하고, 디바이스 Y(1201) 내의 허브(1116)의 외부에 인체 통신용 송수신기(1203)를 구비한다.

<231> 이용자는, 도시하지 않은 인체 통신용 송수신기를 착용하고, 디바이스 Y(1201)의 인체 통신용 송수신기(1203)에 접촉한다. 인증 정보는, 인증 관리 서버(101), 인체 통신용 인증 장치(1206), 인체 통신용 송수신기(1203), 이용자가 착용한 도시하지 않은 인체 통신용 송수신기의 순으로 이들의 기기의 사이에서 송수신되고, 이용자의 인증이 행해진다.

<232> 본 실시예에서는, 인증이 성공한 경우에만, 디바이스 Y(1201)가 네트워크(103) 상의 PC의 디바이스로서 이용 가능하게 된다.

<233> 상기한 바와 같이, 본 실시예에 도시한 디바이스 관리 시스템은, 제2 실시예에 제시한 디바이스 관리 시스템의 특징을 가지면서, 또한 디바이스 Y(1201)와 같이 인체 통신용 인증 장치 및 인체 통신용 송수신기를 갖는 디바이스를 네트워크(103)에 직접 접속할 수 있는 편리성을 갖는다.

<234> 이 편리성에 의해, 본 실시예에 도시한 디바이스 관리 시스템은, 제2 실시예에 제시한 디바이스 관리 시스템의 특징을 가지면서, 이용자가 인증하는 디바이스에 접촉하는 것만으로 디바이스를 네트워크(103) 상의 PC의 디바이스로서 이용하는 것이 가능해지고, 또한 안전성 및 이용자의 편리성이 높아진다.

발명의 효과

<235> 본 발명에 따르면, 서버 클라이언트 방식에서 디바이스를 공유하는 경우, 이용자의 편리성을 저해하지 않고, 시스템 내의 시큐러티를 향상시킬 수 있다.

도면의 간단한 설명

<1> 도 1은 제1 실시예의 디바이스 관리 시스템의 블록도.

<2> 도 2는 제1 실시예의 폴리시 테이블의 일례를 도시하는 도면.

<3> 도 3은 제1 실시예의 디바이스 정보 테이블의 일례를 도시하는 도면.

<4> 도 4는 제1 실시예의 인증 관리 서버가 유지하는 이용자 정보 데이터베이스의 일례를 도시하는 도면.

<5> 도 5는 제1 실시예의 블레이드 서버가 유지하는, PC 이용 관리 테이블의 일례.

<6> 도 6은 제1 실시예의 디바이스 공유 처리의 처리 플로우.

<7> 도 7은 제1 실시예의 디바이스 공유 처리 종료 시의 처리 플로우.

<8> 도 8은 제1 실시예의 디바이스 관리 매니저, 가상 디바이스 매니저의 동작을 설명하기 위한 도면.

<9> 도 9는 제1 실시예의 디바이스 이용 시의 동작을 설명하는 플로우.

<10> 도 10은 제1 실시예의 디바이스 이용 시의 동작을 설명하는 플로우.

<11> 도 11은 관리 어플리케이션에 의해 표시되는 로그 관리 화면의 일례를 도시하는 도면.

<12> 도 12는 제1 실시예의 가상 디바이스 매니저의 디바이스 관리 화면의 일례를 도시하는 도면.

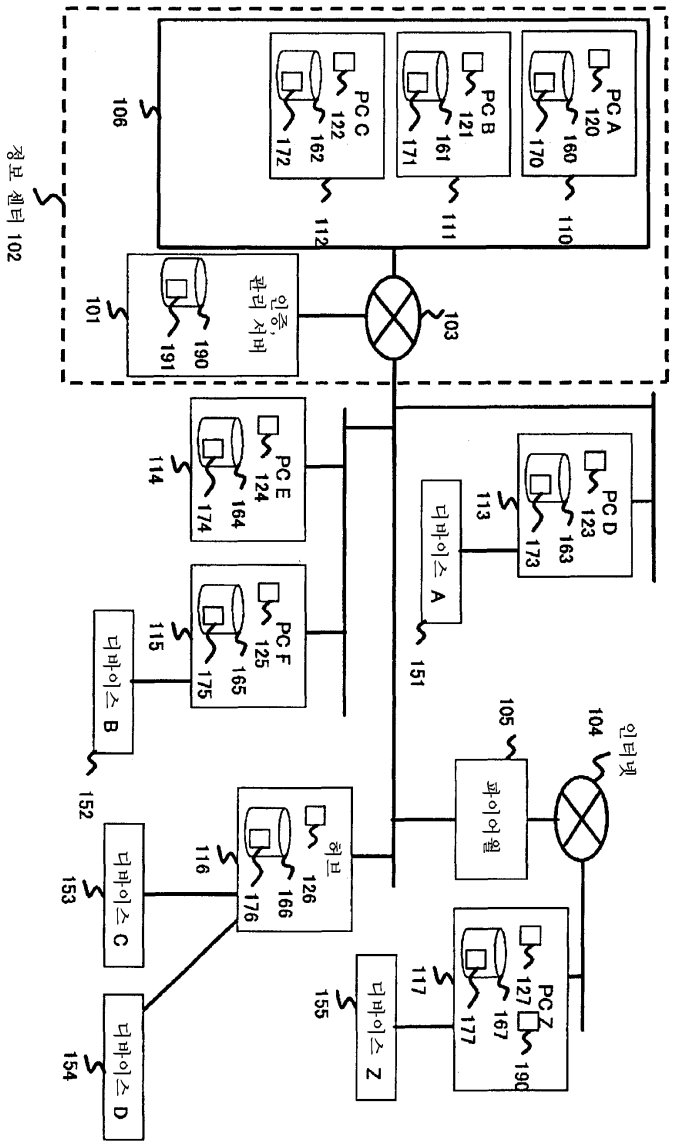
<13> 도 13은 제2 실시예의 디바이스 관리 시스템의 블록도.

<14> 도 14는 제3 실시예의 디바이스 관리 시스템의 블록도.

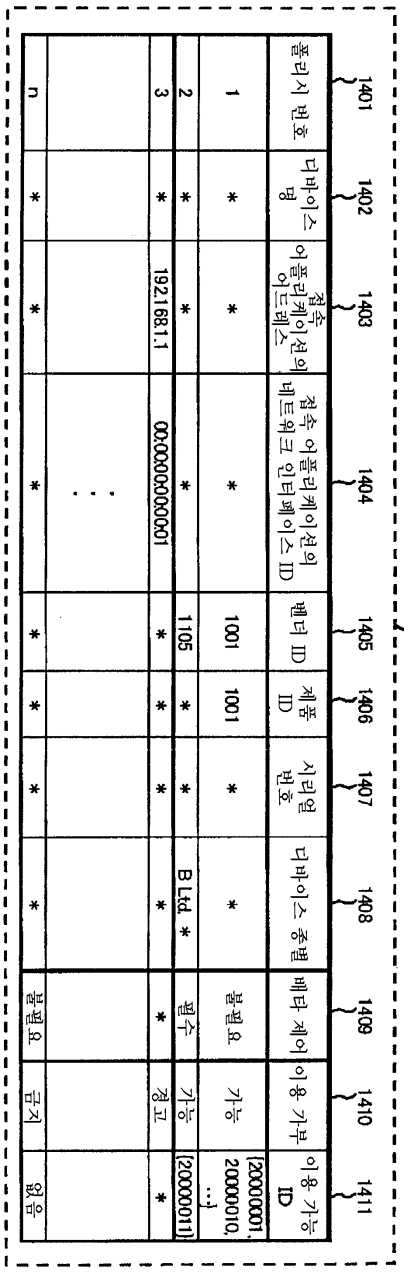
<15> 도 15는 제1 실시예의 PC-A의 하드웨어 구성도.

도면

도면1

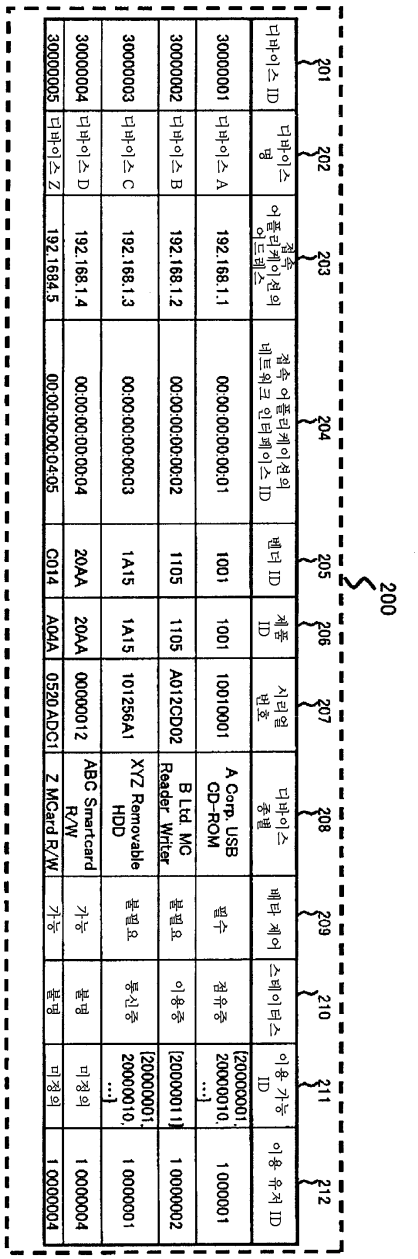

정보 센터 102
106
PC A 120 160 170
PC B 121 161 171
PC C 122 162 172
110
111
112
인증, 관리 처버 101 190 191
103
PC D 123 163 173
113
디바이스 A
151
PC E 124 164 174
114
PC F 125 165 175
115
디바이스 B
152
105
파이어월
104
인터넷
116
허브 126 166 176
디바이스 C
153
디바이스 D
154
117
PC Z 127 167 177 190
디바이스 Z
155

도면2

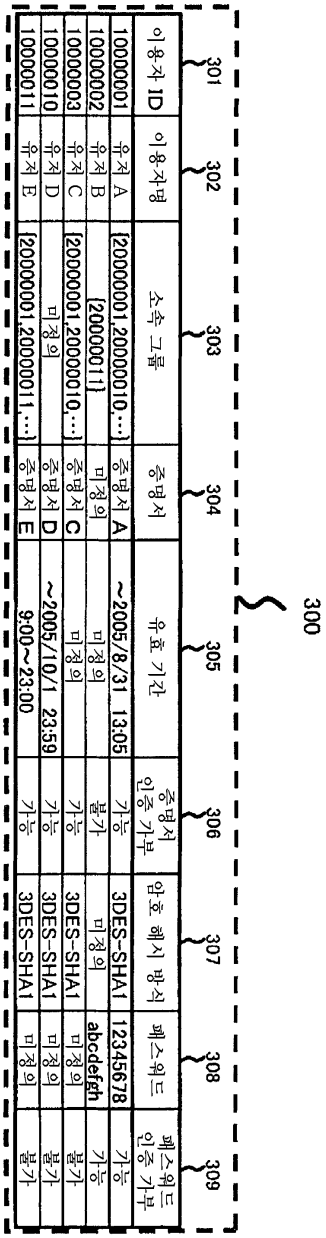


폴리시 번호	디바이스 명	접속 어플리케이션의 아드레스	접속 어플리케이션의 네트워크 인터페이스 ID	벤더 ID	제품 ID	시리얼 번호	디바이스 종별	베타 제어	이용 가부	이용 가능 ID
1	*	*	*	1001	1001	*	*	불필요	가능	[20000001, 20000010, ...]
2	*	*	*	1105	*	*	B Ltd. *	필수	가능	[20000011]
3	*	192.168.1.1	00:00:00:00:00:01	*	*	*	*	*	경고	*
			. . .							
n	*	*	*	*	*	*	*	불필요	금지	없음

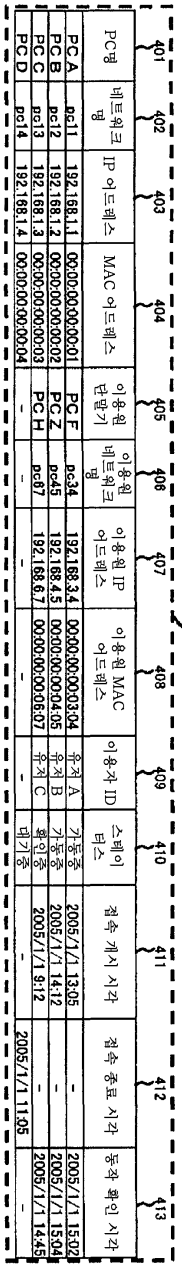
도면3


200
201
202
203
204
205
206
207
208
209
210
211
212
디바이스 ID
디바이스 명
접속 어플리케이션의 어드레스
접속 어플리케이션의 네트워크 인터페이스 ID
벤더 ID
제품 ID
시리얼 번호
디바이스 출력
페어 제어
스테이터스
이용 가능 ID
이용 유저 ID
30000001 디바이스 A 192.168.1.1 00:00:00:00:00:01 1001 1001 10010001 A Corp. USB CD-ROM 필수 접유중 [20000001, 20000010, ...] 1 0000001
30000002 디바이스 B 192.168.1.2 00:00:00:00:00:02 1105 1105 A012CD02 B Ltd. MC Reader Writer 불필요 이용중 [20000011] 1 0000002
30000003 디바이스 C 192.168.1.3 00:00:00:00:00:03 1A15 1A15 101256A1 XYZ Removable HDD 불필요 통신중 [20000001, 20000010, ...] 1 0000001
30000004 디바이스 D 192.168.1.4 00:00:00:00:00:04 20AA 20AA 00000012 ABC Smartcard R/W 가능 불명 미정의 1 0000004
30000005 디바이스 Z 192.1684.5 00:00:00:00:04:05 C014 A04A 0520ADC1 Z MCard R/W 가능 불명 미정의 1 0000004

도면4


300
301
302
303
304
305
306
307
308
309
이용자 ID
이용자명
소속 그룹
증명서
유효 기간
증명서 인증 가부
암호 해시 방식
패스워드
패스워드 인증 가부
10000001 유저 A [20000001,20000010,…] 증명서 A ~2005/8/31 13:05 가능 3DES-SHA1 12345678 가능
10000002 유저 B [20000011] 미정의 미정의 불가 미정의 abcdefgh 가능
10000003 유저 C [20000001,20000010,…] 증명서 C 미정의 가능 3DES-SHA1 미정의 불가
10000010 유저 D 미정의 증명서 D ~2005/10/1 23:59 가능 3DES-SHA1 미정의 불가
10000011 유저 E [20000001,20000011,…] 증명서 E 9:00~23:00 가능 3DES-SHA1 미정의 불가

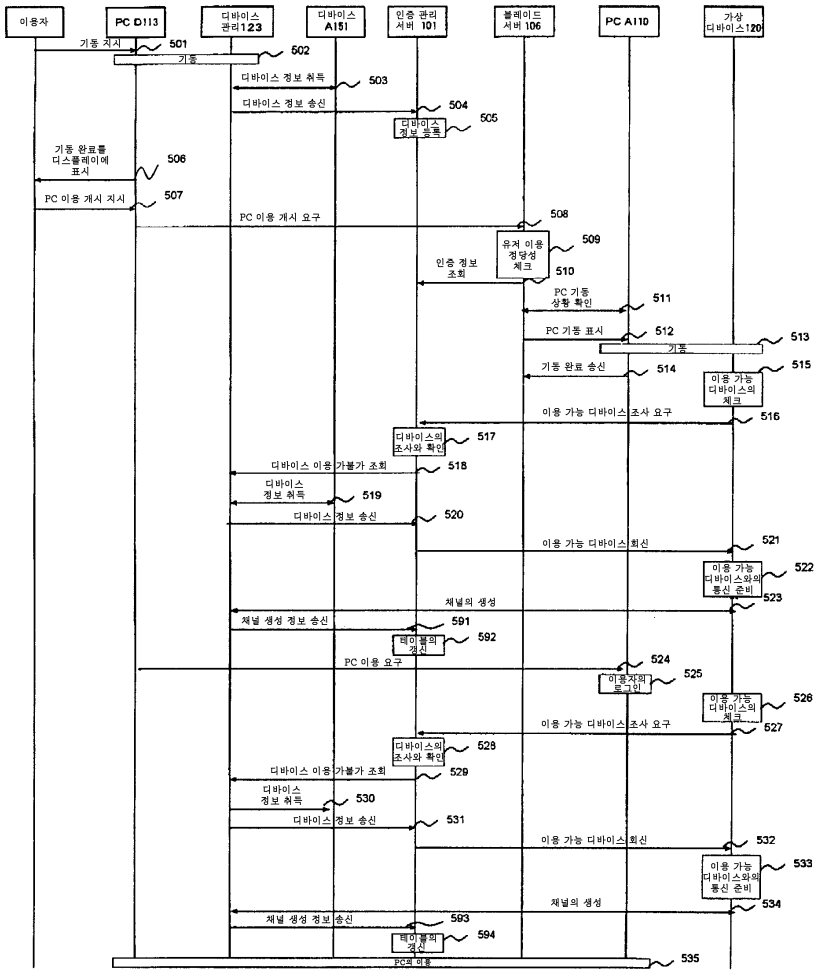
도면5



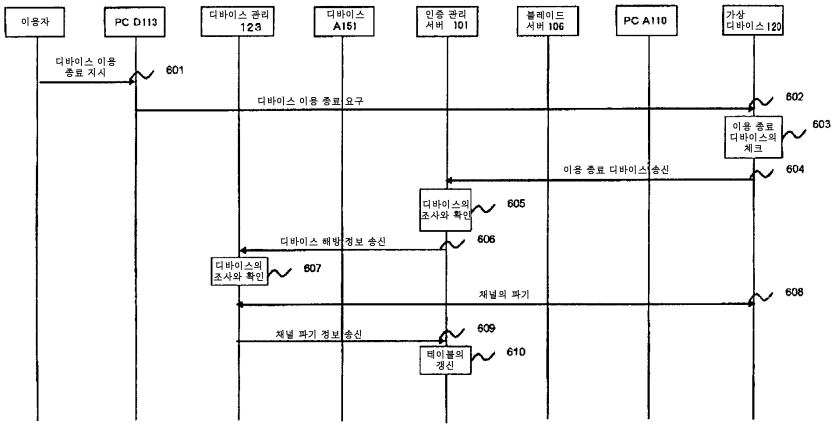
400

401 PC명	402 네트워크 명	403 IP 어드레스	404 MAC 어드레스	405 이용원 단말기	406 이용원 네트워크 명	407 이용원 IP 어드레스	408 이용원 MAC 어드레스	409 이용자 ID	410 스테이 터스	411 접속 개시 시각	412 접속 종료 시각	413 동작 확인 시각
PC A	pc11	192.168.1.1	00:00:00:00:00:01	PC F	pc34	192.168.3.4	00:00:00:00:03:04	유저 A	가동중	2005/1/1 13:05	-	2005/1/1 15:02
PC B	pc12	192.168.1.2	00:00:00:00:00:02	PC Z	pc45	192.168.4.5	00:00:00:00:04:05	유저 B	가동중	2005/1/1 14:12	-	2005/1/1 15:04
PC C	pc13	192.168.1.3	00:00:00:00:00:03	PC H	pc87	192.168.6.7	00:00:00:00:06:07	유저 C	확인중	2005/1/1 9:12	-	2005/1/1 14:45
PC D	pc14	192.168.1.4	00:00:00:00:00:04	-	-	-	-	-	대기중	-	2005/1/1 11:05	-

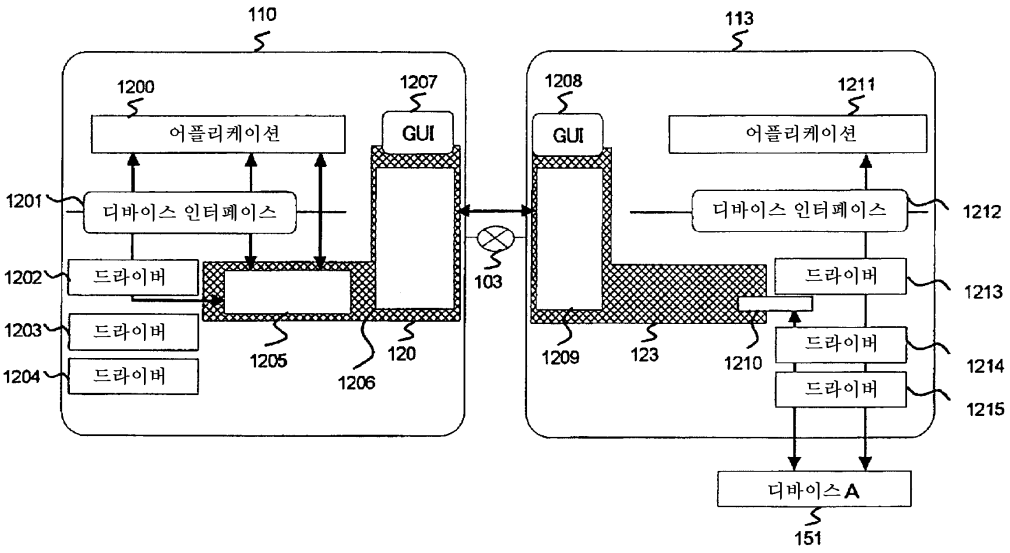
도면6


이용자
PC D113
디바이스 관리123
디바이스 A151
인증 관리 서버 101
블레이드 서버 106
PC A110
가상 디바이스120
기동 지시
501
기동
502
디바이스 정보 취득
503
디바이스 정보 송신
504
디바이스 정보 등록
505
기동 완료를 디스플레이에 표시
506
PC 이용 개시 지시
507
PC 이용 개시 요구
508
유저 이용 정당성 체크
509
인증 정보 조회
510
PC 기동 상황 확인
511
PC 기동 표시
512
기동
513
기동 완료 송신
514
이용 가능 디바이스의 체크
515
이용 가능 디바이스 조사 요구
516
디바이스의 조사와 확인
517
디바이스 이용 가불가 조회
518
디바이스 정보 취득
519
디바이스 정보 송신
520
이용 가능 디바이스 회신
521
이용 가능 디바이스와 통신 준비
522
채널의 생성
523
채널 생성 정보 송신
591
테이블의 갱신
592
PC 이용 요구
524
이용자의 로그인
525
이용 가능 디바이스의 체크
526
이용 가능 디바이스 조사 요구
527
디바이스의 조사와 확인
528
디바이스 이용 가불가 조회
529
디바이스 정보 취득
530
디바이스 정보 송신
531
이용 가능 디바이스 회신
532
이용 가능 디바이스와 통신 준비
533
채널의 생성
534
채널 생성 정보 송신
593
테이블의 갱신
594
PC의 이용
535

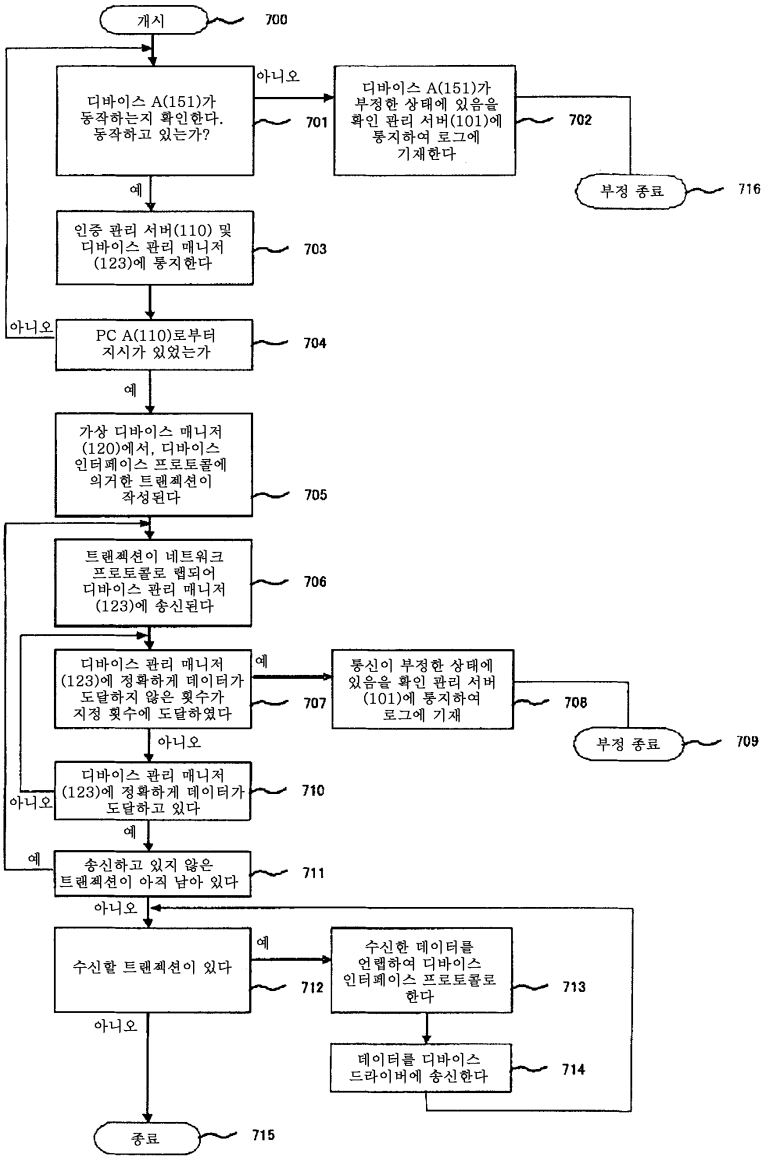
도면7


이용자
PC D113
디바이스 관리 123
디바이스 A151
인증 관리 서버 101
블레이드 서버 106
PC A110
가상 디바이스120
디바이스 이용 종료 지시
601
디바이스 이용 종료 요구
602
이용 종료 디바이스의 체크
603
이용 종료 디바이스 송신
604
디바이스의 조사와 확인
605
디바이스 해방 정보 송신
606
디바이스의 조사와 확인
607
채널의 파기
608
채널 파기 정보 송신
609
테이블의 갱신
610

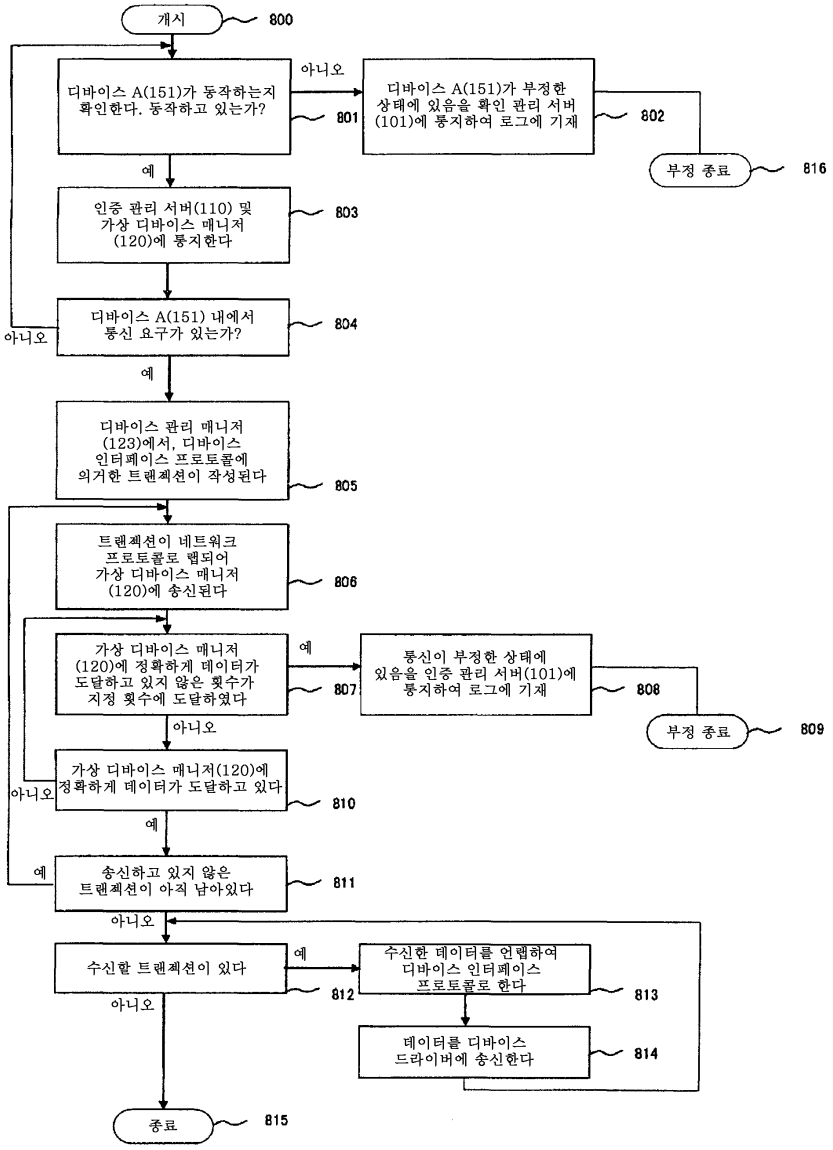
도면8


110
113
1200
1207
1208
1211
어플리케이션
GUI
GUI
어플리케이션
1201
디바이스 인터페이스
디바이스 인터페이스
1212
1202
드라이버
드라이버
1213
1203
드라이버
드라이버
1214
1204
드라이버
드라이버
1215
103
1205
120
1206
1209
123
1210
디바이스A
151

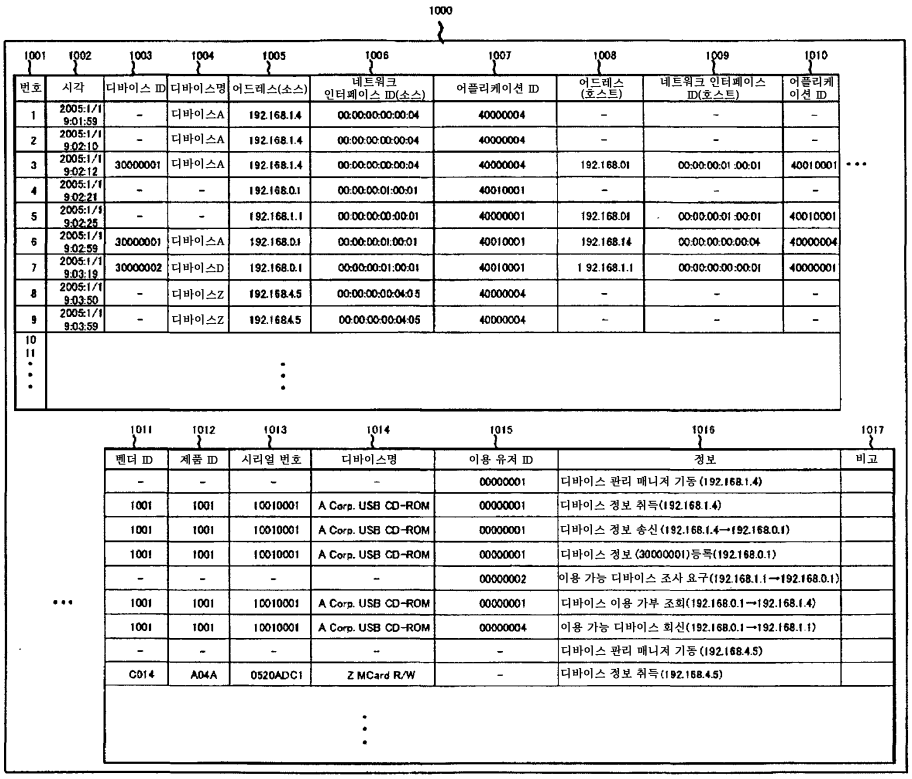
도면9


개시
700
디바이스 A(151)가 동작하는지 확인한다. 동작하고 있는가?
701
아니오
디바이스 A(151)가 부정한 상태에 있음을 확인 관리 서버(101)에 통지하여 로그에 기재한다
702
부정 종료
716
예
인증 관리 서버(110) 및 디바이스 관리 매니저(123)에 통지한다
703
아니오
PC A(110)로부터 지시가 있었는가
704
예
가상 디바이스 매니저(120)에서, 디바이스 인터페이스 프로토콜에 의거한 트랜잭션이 작성된다
705
트랜잭션이 네트워크 프로토콜로 랩되어 디바이스 관리 매니저(123)에 송신된다
706
디바이스 관리 매니저(123)에 정확하게 데이터가 도달하지 않은 횟수가 지정 횟수에 도달하였다
707
예
통신이 부정한 상태에 있음을 확인 관리 서버(101)에 통지하여 로그에 기재
708
부정 종료
709
아니오
디바이스 관리 매니저(123)에 정확하게 데이터가 도달하고 있다
710
아니오
예
송신하고 있지 않은 트랜잭션이 아직 남아 있다
711
예
아니오
수신할 트랜잭션이 있다
712
예
수신한 데이터를 언랩하여 디바이스 인터페이스 프로토콜로 한다
713
데이터를 디바이스 드라이버에 송신한다
714
아니오
종료
715

도면10


개시
800
디바이스 A(151)가 동작하는지 확인한다. 동작하고 있는가?
801
아니오
디바이스 A(151)가 부정한 상태에 있음을 확인 관리 서버(101)에 통지하여 로그에 기재
802
부정 종료
816
예
인증 관리 서버(110) 및 가상 디바이스 매니저(120)에 통지한다
803
디바이스 A(151) 내에서 통신 요구가 있는가?
804
아니오
예
디바이스 관리 매니저(123)에서, 디바이스 인터페이스 프로토콜에 의거한 트랜잭션이 작성된다
805
트랜잭션이 네트워크 프로토콜로 랩되어 가상 디바이스 매니저(120)에 송신된다
806
가상 디바이스 매니저(120)에 정확하게 데이터가 도달하고 있지 않은 횟수가 지정 횟수에 도달하였다
807
예
통신이 부정한 상태에 있음을 인증 관리 서버(101)에 통지하여 로그에 기재
808
부정 종료
809
아니오
가상 디바이스 매니저(120)에 정확하게 데이터가 도달하고 있다
810
아니오
예
송신하고 있지 않은 트랜잭션이 아직 남아있다
811
예
아니오
수신할 트랜잭션이 있다
812
예
수신한 데이터를 언랩하여 디바이스 인터페이스 프로토콜로 한다
813
데이터를 디바이스 드라이버에 송신한다
814
아니오
종료
815

도면11

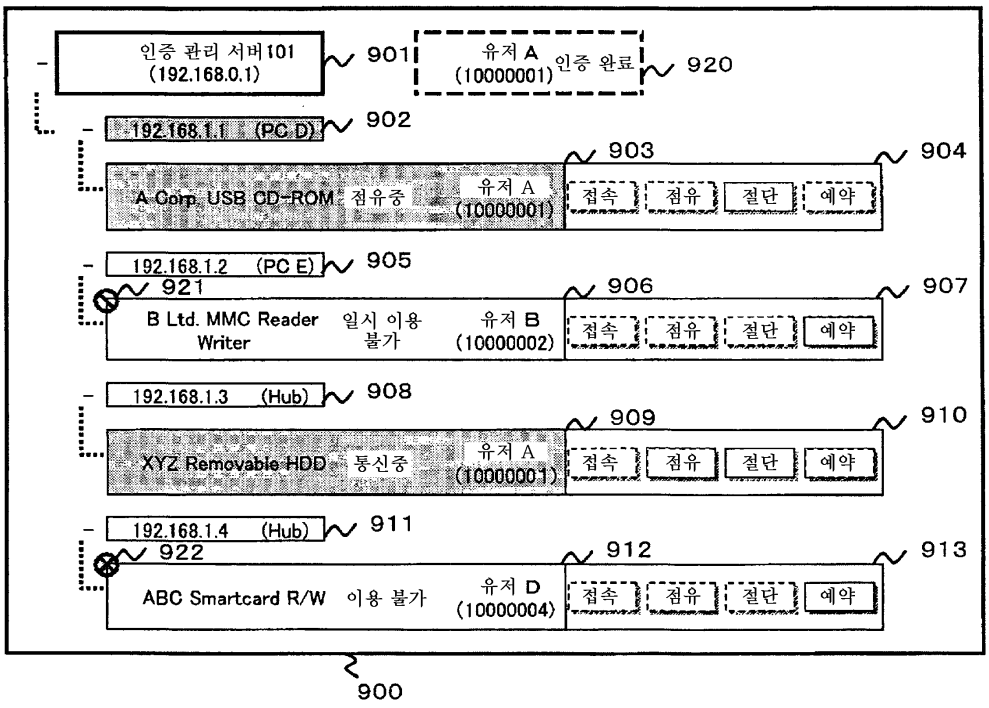


1000

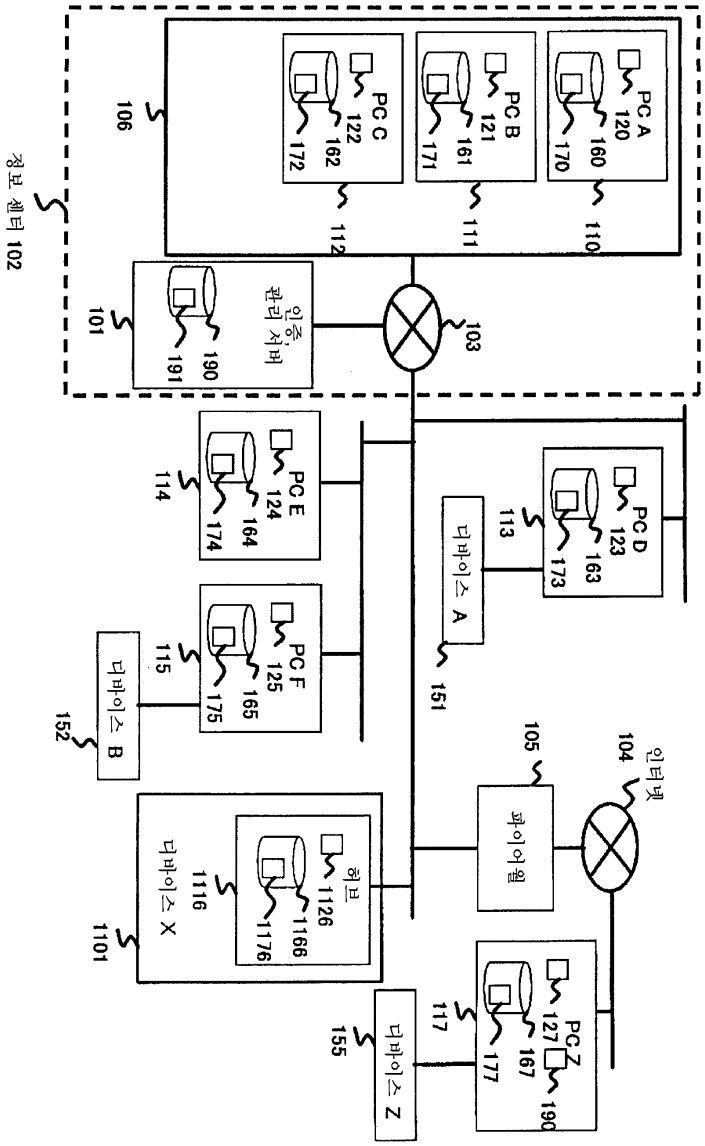
1001 번호	1002 시각	1003 디바이스 ID	1004 디바이스명	1005 어드레스(소스)	1006 네트워크 인터페이스 ID(소스)	1007 어플리케이션 ID	1008 어드레스 (호스트)	1009 네트워크 인터페이스 ID(호스트)	1010 어플리케이션 ID
1	2005:1/1 9:01:59	-	디바이스A	192.168.1.4	00:00:00:00:00:04	40000004	-	-	-
2	2005:1/1 9:02:10	-	디바이스A	192.168.1.4	00:00:00:00:00:04	40000004	-	-	-
3	2005:1/1 9:02:12	30000001	디바이스A	192.168.1.4	00:00:00:00:00:04	40000004	192.168.0.1	00:00:00:01 :00:01	40010001
4	2005:1/1 9:02:21	-	-	192.168.0.1	00:00:00:01:00:01	40010001	-	-	-
5	2005:1/1 9:02:25	-	-	192.168.1.1	00:00:00:00:00:01	40000001	192.168.0.1	00:00:00:01 :00:01	40010001
6	2005:1/1 9:02:59	30000001	디바이스A	192.168.0.1	00:00:00:01:00:01	40010001	192.168.1.4	00:00:00:00:00:04	40000004
7	2005:1/1 9:03:19	30000002	디바이스D	192.168.0.1	00:00:00:01:00:01	40010001	1 92.168.1.1	00:00:00:00:00:01	40000001
8	2005:1/1 9:03:50	-	디바이스Z	192.168.4.5	00:00:00:00:04:05	40000004	-	-	-
9	2005:1/1 9:03:59	-	디바이스Z	192.168.4.5	00:00:00:00:04:05	40000004	-	-	-
10 11									

1011 벤더 ID	1012 제품 ID	1013 시리얼 번호	1014 디바이스명	1015 이용 유저 ID	1016 정보	1017 비고
-	-	-	-	00000001	디바이스 관리 매니저 기동(192.168.1.4)	
1001	1001	10010001	A Corp. USB CD-ROM	00000001	디바이스 정보 취득(192.168.1.4)	
1001	1001	10010001	A Corp. USB CD-ROM	00000001	디바이스 정보 송신(192.168.1.4→192.168.0.1)	
1001	1001	10010001	A Corp. USB CD-ROM	00000001	디바이스 정보(30000001)등록(192.168.0.1)	
-	-	-	-	00000002	이용 가능 디바이스 조사 요구(192.168.1.1→192.168.0.1)	
1001	1001	10010001	A Corp. USB CD-ROM	00000001	디바이스 이용 가부 조회(192.168.0.1→192.168.1.4)	
1001	1001	10010001	A Corp. USB CD-ROM	00000004	이용 가능 디바이스 회신(192.168.0.1→192.168.1.1)	
-	-	-	-	-	디바이스 관리 매니저 기동(192.168.4.5)	
C014	A04A	0520ADC1	Z MCard R/W	-	디바이스 정보 취득(192.168.4.5)	

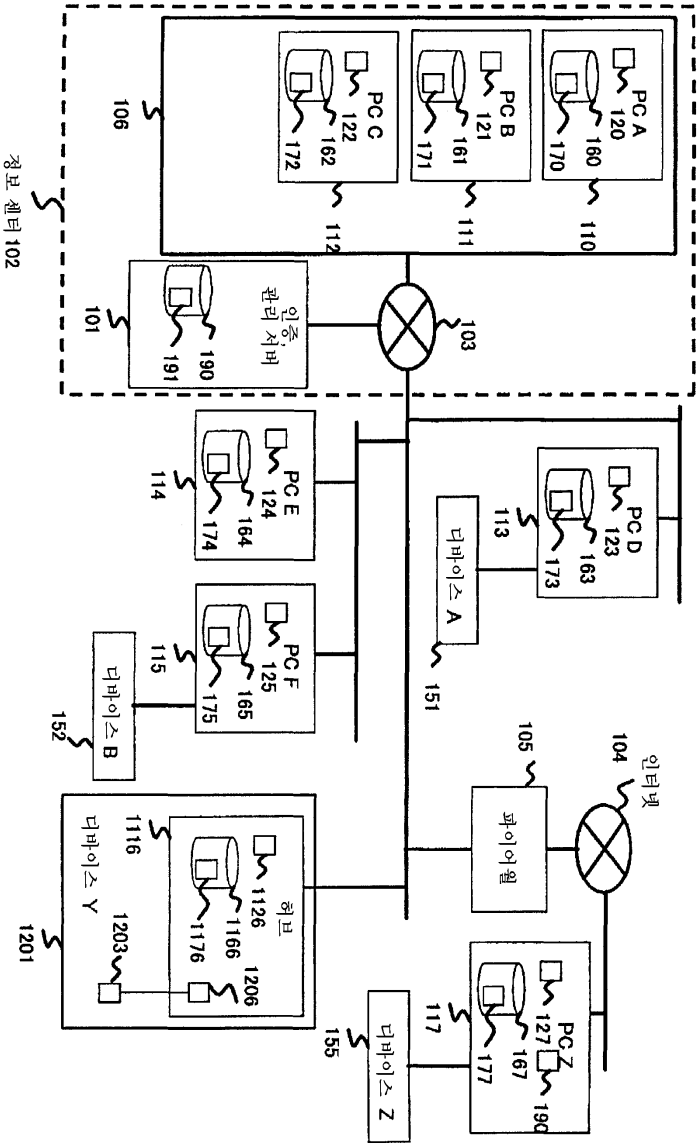
도면12



도면13


정보 센터 102
106
PC A 120 160 170
PC B 121 161 171
PC C 122 162 172
110
111
112
103
101
인증 관리 서버 190 191
PC D 123 163 173
113
디바이스 A 151
PC E 124 164 174
114
PC F 125 165 175
115
디바이스 B 152
인터넷 104
105
파이어월
허브 1126 1166 1176
디바이스 X 1116
1101
PC Z 127 167 190
117
디바이스 Z 155

도면14


정보 센터 102
106
PC A 120 160 170
PC B 121 161 171
PC C 122 162 172
110
111
112
인증 관리 서버 101 190 191
103
PC D 123 163 173
디바이스 A 113
151
PC E 124 164 174
114
PC F 125 165 175
115
디바이스 B 152
105
파이어월
104
인터넷
디바이스 Y 1201
1116
허브 1126 1166 1176 1206
1203
디바이스 Z 155
117
PC Z 127 167 177 190

도면15