(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년05월08일
(11) 등록번호 10-0896391
(24) 등록일자 2009년04월28일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2007-7025337(분할)
(22) 출원일자 2007년10월31일
심사청구일자 2007년10월31일
번역문제출일자 2007년10월31일
(65) 공개번호 10-2007-0118680
(43) 공개일자 2007년12월17일
(62) 원출원 특허 10-2006-7001743
원출원일자 2006년01월25일
심사청구일자 2006년01월26일
(86) 국제출원번호 PCT/JP2005/000698
국제출원일자 2005년01월20일
(87) 국제공개번호 WO 2005/071558
국제공개일자 2005년08월04일
(30) 우선권주장
JP-P-2004-00012594 2004년01월21일 일본(JP)
JP-P-2004-00117437 2004년04월13일 일본(JP)
(56) 선행기술조사문헌
KR1020010088530 A*
KR1020030049387 A*
KR1020030060342 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
가부시키가이샤 히타치세이사쿠쇼
일본국 도쿄토 치요다쿠 마루노우치 1초메 6반 6고
(72) 발명자
가또, 다까또시
일본 100-8220 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 마루노우찌센터 빌딩 12층 가부시키가이샤 히타치세이사쿠쇼지적재산권본부 내
미즈시마, 나가마사
일본 100-8220 도꾜도 지요다꾸 마루노우찌 1쪼메 6-1 마루노우찌센터 빌딩 12층 가부시키가이샤 히타치세이사쿠쇼지적재산권본부 내
(뒷면에 계속)
(74) 대리인
구영창, 양영준, 장수길

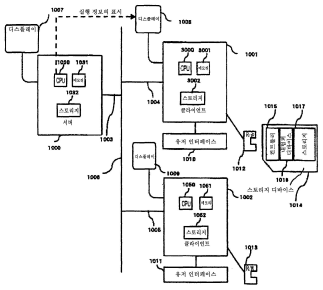
전체 청구항 수 : 총 15 항 심사관 : 이종익

(54) 외장 기기

(57) 요 약

이용자가 불특정 클라이언트로부터 서버에 대하여 암호 통신을 행하면서 액세스해서 업무 수행을 행하는 시큐어 리모트 액세스 시스템에서, 이용자의 인증 디바이스로서 내탬퍼 디바이스를 내장하는 스토리지 디바이스를 이용함으로써, 이용자의 편리성을 향상시키는 시큐어 리모트 액세스 시스템을 제공한다. 인정된 내탬퍼 디바이스를 탑재한 스토리지 디바이스를 이용자에게 배포하여 이용자가 스토리지 디바이스를 불특정 클라이언트에 접속해서, 스토리지 디바이스 내의 인증 정보와 애플리케이션을 이용하여 서버를 원격 조작하는 서버 클라이언트 시스템을 제공함으로써, 이용자의 사용 편리성을 향상시키는 것이 가능하고, 결과적으로 심리스하게 직장 내외에서의 업무 수행 기능을 이용할 수 있고, 또한 조작한 클라이언트 내에 남는 기밀 정보를 저감함으로써, 유저의 클라이언트 이용 시의 시큐러티 및 편리성을 향상시키는 리모트 액세스 시스템을 제공할 수 있다.

대 표 도 - 도1



(72) 발명자

쯔네히로, 다까시

일본 100-8220 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1 마루노우찌센터 빌딩 12층 가부시키가이샤 히타치세이사쿠쇼지적재산권본부 내

가야시마, 마꼬또

일본 100-8220 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1 마루노우찌센터 빌딩 12층 가부시키가이샤 히타치세이사쿠쇼지적재산권본부 내

나까가와, 가즈시

일본 100-8220 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1 마루노우찌센터 빌딩 12층 가부시키가이샤 히타치세이사쿠쇼지적재산권본부 내

특허청구의 범위

청구항 1

클라이언트 기기에 접속부를 통해서 접속되고, 스토리지를 포함하는 외장 기기로서,

인증 정보와,

상기 외장 기기의 송신 장치로부터 상기 클라이언트 기기에 송신되고, 상기 클라이언트 기기가 포함하는 메모리 상에 로드되고, 상기 클라이언트 기기가 포함하는 CPU에 의해 실행되어, 상기 클라이언트 기기에, 상기 외장 기기로부터 OS 프로그램을 수신시키는 부트 프로그램과,

상기 외장 기기의 송신 장치로부터 상기 클라이언트 기기에 송신되고, 상기 클라이언트 기기가 포함하는 메모리 상에 로드되고, 상기 클라이언트 기기가 포함하는 CPU에 의해 실행되어, 상기 클라이언트 기기에, 상기 외장 기기로부터 원격 조작 프로그램을 수신시키는 상기 OS 프로그램과,

상기 외장 기기의 송신 장치로부터 상기 클라이언트 기기에 송신되고, 상기 클라이언트 기기가 포함하는 메모리 상에 로드되고, 상기 클라이언트 기기가 포함하는 CPU에 의해 실행되어, 상기 클라이언트 기기에, 상기 외장 기기의 이용자로부터 취득하는 식별 정보를 이용해서 상기 인증 정보를 수신시키고, 상기 인증 정보를 이용해서 상기 클라이언트 기기에 네트워크를 통해서 접속되는 서버와 상기 클라이언트 기기 사이에 통신로를 구축시켜, 상기 서버를 원격 조작시키는 상기 원격 조작 프로그램

을 상기 스토리지에 가지며,

상기 인증 정보를 가지는 스토리지는, 내탬퍼성을 가지는 스토리지인 것을 특징으로 하는 외장 기기.

청구항 2

제1항에 있어서,

상기 부트 프로그램은, 상기 외장 기기로부터 OS 프로그램을 수신시키기 전에, 상기 클라이언트 기기의 인증을 행하게 하는 것을 특징으로 하는 외장 기기.

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

제1항에 있어서,

상기 부트 프로그램, 상기 OS 프로그램 및 상기 원격 조작 프로그램이 로드되는 상기 클라이언트 기기가 포함하는 메모리는, 휘발성 메모리인 것을 특징으로 하는 외장 기기.

청구항 7

제1항 또는 제2항에 있어서,

상기 스토리지가 가지는 인증 정보는, 상기 통신로의 구축에 관한 키 정보를 포함하는 것을 특징으로 하는 외장 기기.

청구항 8

제1항 또는 제2항에 있어서,

상기 외장 기기의 이용자로부터 취득하는 식별 정보를 이용해서 상기 클라이언트 기기가 수신하는 인증 정보는, 상기 스토리지가 가지는 인증 정보를 이용해서 상기 외장 기기가 작성하는 전자 서명인 것을 특징으로 하는 외장 기기.

청구항 9

제1항 또는 제2항에 있어서,

상기 스토리지는, 상기 외장 기기의 송신 장치로부터 상기 클라이언트 기기에 송신되고, 상기 클라이언트 기기가 포함하는 메모리 상에 로드되고, 상기 클라이언트 기기가 포함하는 CPU에 의해 실행되는, 상기 내탬퍼성을 가지는 스토리지를 포함하는, 상기 외장 기기의 스토리지에 관한 디바이스 드라이버를 더 갖고,

상기 OS 프로그램은, 상기 디바이스 드라이버를, 상기 외장 기기의 송신 장치로부터 상기 클라이언트 기기에, 상기 원격 조작 프로그램이 송신되기 전에 송신시키고, 상기 클라이언트 기기가 포함하는 메모리 상에 로드시키고, 상기 클라이언트 기기가 포함하는 CPU에 의해 실행시켜, 상기 클라이언트 기기로부터 상기 접속부를 통해 상기 외장 기기의 상기 내탬퍼성을 가지는 스토리지를 포함하는 스토리지에의 액세스를 가능하게 하는 것을 특징으로 하는 외장 기기.

청구항 10

제2항에 있어서,

상기 부트 프로그램의, 상기 외장 기기로부터의 OS 프로그램의 수신은, 상기 클라이언트 기기의 인증이 실패했을 경우에 행해지는 것을 특징으로 하는 외장 기기.

청구항 11

제2항에 있어서,

상기 부트 프로그램이 상기 클라이언트 기기에 행하게 하는 인증은, 상기 클라이언트 기기가 포함하는 디바이스의 고유 식별자를 검증하는 것인 것을 특징으로 하는 외장 기기.

청구항 12

제11항에 있어서,

상기 클라이언트 기기가 포함하는 디바이스는, CPU, 메모리, 상기 스토리지, 또는 네트워크 카드인 것을 특징으로 하는 외장 기기.

청구항 13

제12항에 있어서,

상기 클라이언트 기기가 포함하는 디바이스의 고유 식별자는, 제조 번호, 또는 MAC 어드레스인 것을 특징으로 하는 외장 기기.

청구항 14

제2항에 있어서,

상기 부트 프로그램은,

상기 클라이언트 기기의 인증이 성공한 후, 또한,

상기 클라이언트 기기가 포함하는 스토리지에 암호화 또는 패스워드 로크가 걸려 있는지 여부를 상기 외장 기기에 조사시키고,

상기 클라이언트 기기가 포함하는 스토리지에 암호화 또는 패스워드 로크가 걸려 있었을 경우, 상기 외장 기기의 이용자로부터 상기 암호화 또는 패스워드 로크의 해제 정보를 수신시켜, 그 해제 정보를 이용해서 상기 암호화 또는 패스워드 로크를 해제할 수 없는 경우에, 상기 외장 기기로부터 OS 프로그램을 수신시키는 것을 특징으로 하는 외장 기기.

청구항 15

제14항에 있어서,

상기 부트 프로그램이 상기 클라이언트 기기의 인증에 성공했을 경우, 또는 상기 부트 프로그램이 상기 클라이언트 기기가 포함하는 스토리지의 암호화 또는 패스워드 로크의 해제에 성공했을 경우, 상기 클라이언트 기기가 포함하는 스토리지가 가지는 OS 프로그램을 실행시키는 것을 특징으로 하는 외장 기기.

청구항 16

제1항 또는 제2항에 있어서,

상기 외장 기기의 스토리지는, 상기 외장 기기로부터 상기 클라이언트 기기에, 상기 OS 프로그램 대신에 송신되는 더미 데이터를 더 갖고,

상기 부트 프로그램은, 상기 클라이언트 기기가 상기 더미 데이터를 수신했을 경우, 상기 클라이언트 기기에 미리 정해진 OS 프로그램을 읽어들이는 곳의 기기로부터 OS 프로그램을 읽어내는 것을 특징으로 하는 외장 기기.

청구항 17

제16항에 있어서,

상기 외장 기기는, 상기 클라이언트 기기에 상기 OS 프로그램 및 상기 더미 데이터 중 어느 하나를 송신하는 것을 결정하는 선택부를 더 갖는 것을 특징으로 하는 외장 기기.

청구항 18

제1항 또는 제2항에 있어서,

상기 외장 기기의 이용자로부터 취득하는 식별 정보는, 암증 번호, 패스워드, 패스프레이즈, 원타임 패스워드, 또는 상기 이용자의 생체 인증 정보인 것을 특징으로 하는 외장 기기.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> <참조에 의한 인용>

<2> 본 출원은, 2004년 1월 21일에 출원된 일본특허출원 제2004-012594호, 2004년 4월 13일에 출원된 일본특허출원 제2004-117437호의 우선권을 주장하고, 그 내용을 참조함으로써 본 출원에 인용한다.

<3> 본 발명은, 서버를, 네트워크를 통하여 안전하게 원격 조작하는 것을 가능하게 하는 시큐어 리모트 액세스 시스템에 관한 것이다. 특히, 클라이언트를 적절하게 서버에 접속하기 위한, 내탬퍼 디바이스와, 클라이언트, 혹은 내탬퍼 디바이스 상에 기록하는 프로그램, 및 리모트 액세스 시스템을 동작시키기 위한 네트워크 접속 기술에 관한 것이다.

배 경 기 술

<4> 최근, 퍼스널 컴퓨터(PC)나 네트워크 기기의 저가격화가 진행되어, 종업원의 대부분에게 PC와 같은 업무에 이용하는 단말기를 배포해서 업무를 행하도록 하고 있는 기업이 다수를 차지하게 되었다. PC가 저가격화하여 이용이 증가하면, 기업 내의 기기 관리자의 메인터넌스 작업을 행할 필요가 있는 PC의 수도 비례하여 증가한다. 이 메인터넌스 작업이란, 예를 들면, 오퍼레이팅 시스템(OS)이나 업무 애플리케이션의 버전업이나 버그 픽스, 하드웨어적인 장해에의 대응, 바이러스 대책이나 바이러스 구제 등을 들 수 있다. 이러한 메인터넌스 작업을 행하는 관리 코스트는 매우 커서, 종업원 수가 증가하면 비례해서 막대하게 된다.

<5> 이 관리 코스트를 저감하기 위한 일 방법으로서, 서버 클라이언트 방식이라고 불리는 시스템 운용의 방식이 취해지고 있다. 이것은, 주된 프로그램이나 데이터를 서버측에 축적해서, 예를 들면 Thin Client(신 클라이언트)와 같은 클라이언트측에 축적하는 데이터를 저감시킨 것이다.

<6> 서버 클라이언트 방식에서는, 연산 처리나 데이터의 축적은 주로 서버측에서 행해지기 때문에, 신 클라이언트와 같은 클라이언트측에서 개개로 OS나 업무에 이용하는 애플리케이션의 버전업이나 버그 픽스, 바이러스 대책이나 바이러스 구제 등을 행할 필요성이나 빈도가 감소하기 때문에, 전체 관리 코스트를 저감할 수 있다.

<7> 또한, 최근, IC 칩이라고 불리는 프로세서를 카드 내에 내장한 IC 카드(별칭 스마트 카드)가, 전자 인증 기능을 갖는 키 디바이스로서 주목받고 있다. IC 카드란, 주로 내부의 IC 카드 모듈에 중앙 연산 처리 장치(CPU)를 내장하고 있는 카드를 가리킨다. IC 카드의 메모리에는 ROM, EEPROM 등이 사용된다. IC 카드는, 카드 자체가 연산 기능을 갖기 때문에, 호스트로부터의 기입 및 판독 지시가 있을 때, 정당한 유저로부터 액세스가 행해진 것인지의 여부를 자체적으로 판단하는 기능을 갖는다. 또한, CPU 자체의 위조가 곤란하기 때문에, 내탬퍼 디바이스인 IC 카드 모듈(IC 카드 칩)이 발하는 정보의 개찬이나, 부정하게 IC 카드 모듈 내부에 액세스하는 것이 어렵다. 이 때문에, 높은 시큐러티 레벨을 갖는 시스템을 구축 가능하다. 대부분의 IC 카드는, 유저가 등록한 개인 인증 번호(PIN 코드)와 카드 내부에 보유된 PIN 코드를 대조하는 등 하여, IC 카드 내의 정보를 적절하게 리더 라이터 혹은 호스트 출력할지 혹은 하지 않을지 등의 제어를 행하는 것이 가능하다. IC 카드는 내부에 EEPROM이나 RAM 등의 재기입 가능한 메모리를 갖고, 유저나 카드 발행자의 애플리케이션이나 정보를 저장할 수 있다. IC 카드는, 외부로부터 입력되는 정보에 대하여, 그 해당하는 카드에만 존재 가능한 정보(비밀 키 등)를 이용한 연산을 하는 등 하여, 카드 외부에 카드 소유자밖에 알 수 없는 정보 혹은 만들 수 없는 정보 등을 출력함으로써 카드 소유자를 인증시키거나, 부인 방지를 위한 정보를 출력하거나 하는 것이 가능하다.

<8> 또한, 플래시 메모리 카드는 불휘발성 메모리 모듈을 내장한 메모리 카드로서, 유저의 정보를 메모리 카드 내에 기억하는 것이 가능하다. 플래시 메모리 카드의 대부분은 「제3자로부터의 공격에 대한 하드웨어적인 내성」(내탬퍼성)을 갖고 있지 않다. 내탬퍼성을 갖지 않는 플래시 메모리 카드는, 도난, 분실 시에 카드가 분해되어서, 카드 내의 메모리 혹은 컨트롤러를 해석함으로써, 보유되어 있는 정보가 제3자에게 누설될 가능성이 적지 않다.

<9> 또한, 일본특허공개 2001-209773호 공보에 개시된 바와 같이, 플래시 메모리 인터페이스와 IC 카드 기능을 갖는 플래시 메모리 카드가 개시되어 있다. 이 플래시 메모리 인터페이스와 IC 카드 기능을 갖는 플래시 메모리 카드는, 그 기억 용량의 크기때문에, 퍼스널 컴퓨터나 워크스테이션에 구축된 유저의 보관 문서나 설정 파일 등을 카드 내에 보존하여 갖고 다니는 데 편의성이 좋다.

발명의 내용

해결 하고자하는 과제

<10> 상술한 서버 클라이언트 방식에서는, 서버와 클라이언트 간의 인증이나 데이터의 교환은 네트워크를 통하여 행해진다. 이 때문에, 네트워크 상의 하나의 클라이언트로부터 서버에의 액세스를 행할 때에, 서버측에서는 액세스하여 온 클라이언트가 정당한 클라이언트인지의 여부, 또한, 클라이언트를 이용하고 있는 이용자가 정당한 이용자인지의 여부 등의 검증 작업을 행할 필요가 있다. 또한, 클라이언트측에서도, 액세스하고 있는 서버가 정당한 서버인지의 여부를 검증하지 않고는 자신이 하고자 하는 업무를 행할 수 없다. 만일 상술한 바와 같은 검증을 행하지 않으면, 서버측에 축적된 데이터나 이용자가 가진 정보가 제3자에게 누설될 가능성이 있다. 따라서, 네트워크 상에서의 인증이나, 업무 수행 중의 송신 정보 등의 암호화 등의 시큐러티를 충분히 높일 필요가 있다.

<11> 본 발명의 목적은, IC 카드에 실장되는 IC 칩과 같은 인정된 내탬퍼 디바이스 내에 이용자의 인증 정보를 저장하고, 또한, 대용량의 파일을 안전하게 저장해서 갖고 다닐 수 있는 플래시 메모리 카드와 같은 스토리지 디바이스를 인증 디바이스로 하는 서버 클라이언트 시스템에 의해 유저의 편리성을 향상시키는 것에 있다.

<12> 또한, 그 서버 클라이언트 시스템에 사용 가능한 인증용 스토리지 디바이스를 제공하는 것도 본 발명의 목적이다.

<13> 본 발명의 상기 및 그 밖의 목적과 신규한 특징은 본 명세서의 설명 및 첨부 도면으로부터 명백하게 될 것이다.

과제 해결수단

<14> 본원에서 개시되는 발명 중 대표적인 것의 개요를 설명하면, 하기와 같다. 즉, 상술한 목적을 달성하기 위해, 본 발명에 따른 리모트 액세스 시스템은, 내탬퍼 디바이스와 스토리지와 컨트롤러의 기능을 실장한 스토리지 디바이스와, 상기 스토리지 디바이스를 접속하기 위한 리더 라이터와, 상기 리더 라이터와 접속하는

클라이언트와, 네트워크를 통하여 상기 클라이언트로부터 원격 조작되는 서버와 네트워크 상의 암호 통신을 행하기 위한 게이트웨이를 구비하고, 상기 스토리지 내에, 상기 서버를 원격 조작하는 애플리케이션과, 상기 네트워크 상의 통신을 암호화하는 암호화 애플리케이션을 기록하고 있고, 상기 게이트웨이와 상기 클라이언트의 암호 통신을 행하기 위한 인증 정보를 상기 내탬퍼 디바이스 내에 저장하고 있는 것을 특징으로 한다.

효 과

<15> 본 발명에 따르면, 인정된 내탬퍼 디바이스를 탑재한 스토리지 디바이스를 이용자에게 배포하여 이용자가 스토리지 디바이스를 불특정 클라이언트에 접속해서 스토리지 디바이스 내의 인증 정보와 애플리케이션을 이용하여 서버를 원격 조작하는 서버 클라이언트 시스템을 제공함으로써, 이용자의 사용 편리성을 향상시키는 것이 가능하고, 결과적으로 심리스하게 직장 내외에서의 업무 수행 기능을 이용할 수 있고, 또한, 조작한 클라이언트 내에 남는 기밀 정보를 저감함으로써 유저의 클라이언트 이용 시의 시큐러티 및 편리성을 향상시키는 리모트 액세스 시스템을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

<16> 본 발명의 실시예에 대하여, 첨부 도면을 참조하면서 이하 상세히 설명한다. 또한, 도면 중에서 동일한 참조 번호를 붙인 것은 동일한 기능을 갖는 구성 요소를 나타내고, 설명의 편의상, 그 상세한 설명은 생략한다.

<17> (제1 실시예)

<18> 도 1 내지 도 7을 이용하여, 본 발명에 따른 시큐어 리모트 액세스 시스템의 제1 실시예를 설명한다.

<19> 도 1은 본 발명의 제1 실시예를 나타내는 리모트 액세스 시스템을 도시하는 도면이다.

<20> 이용자가 사용하는 서버(1000)와 복수의 클라이언트(클라이언트(1001) 및 클라이언트(1002))는 네트워크 케이블(1003, 1004 및 1005)을 통하여 네트워크(1006)에 접속되어 있다. 네트워크 케이블(1003, 1004 및 1005)과 네트워크(1006)는, 도시하지 않은 네트워크 허브나 스위치에 의해 적절하게 접속되고, 네트워크 케이블(1003, 1004, 1005) 및 네트워크(1006) 상의 접속된 기기에의 패킷의 라우팅이 적절하게 행해져, 정상적으로 통신이 가능한 상태에 있다. 서버(1000)는, 도시하지 않은 디스플레이 인터페이스를 통해서 디스플레이(1007)와 접속되어 있다. 클라이언트(1001 및 1002)도 마찬가지로, 도시하지 않은 디스플레이 인터페이스를 통하여 각각 디스플레이(1008 및 1009)와 접속되어 있다. 클라이언트(1001 및 1002)에는 각각 유저 인터페이스(1010 및 1011)가 접속되어 있다. 유저 인터페이스(1010 및 1011)는, 키보드나 마우스, 트랙볼, 터치 패널, 터치 패드, 지문 리더, 생체 정보 판독 장치 등에 의해 구성되는, 클라이언트(1001 및 1002)의 이용자의 입력 정보를 각각 클라이언트(1001 및 1002)에 송신하는 기능을 갖는다.

<21> 리더 라이터(1012 및 1013)는 각각 클라이언트(1001 및 1002)에 접속되어 있고, 스토리지 디바이스(1014)를 삽입하는 기능을 갖는다. 스토리지 디바이스(1014) 내의 후술하는 단자(2000)는 리더 라이터(1012)의 도시하지 않은 단자와 접속되어, 클라이언트(1001)와 통신을 행할 수 있다. 스토리지 디바이스(1014)는 이용자가 휴대하여 갖고 다니는 것이 가능하고, 클라이언트(1001) 이외의, 예를 들면 클라이언트(1002)와 같은 기기에서도 이용이 가능한 설계로 되어 있다.

<22> 스토리지 디바이스(1014)는 내부에 컨트롤러(1015), 내탬퍼 디바이스(1016), 스토리지(1017)를 실장하고 있다. 컨트롤러(1015), 내탬퍼 디바이스(1016), 스토리지(1017)는 각각 별개의 집적 회로로서 실장되어 있도록 설명되어 있지만, 기능을 통합한 하나의 집적 회로로서 실장하여도 된다. 내탬퍼 디바이스(1016)는, 예를 들면 IC 카드 칩 등의, 시큐러티 평가 단체가 정한 기준에 따라 인정을 받거나, 받을 수 있는 수준의 내탬퍼성을 갖는 디바이스이다.

<23> 서버(1000) 내부에는 CPU(1030), 메모리(1031), 스토리지(1032)가 실장되어 있다. 클라이언트(1001)에는 CPU(3000), 메모리(3001), 스토리지(3002), 클라이언트(1002)에는 CPU(1050), 메모리(1051), 스토리지(1052)가 실장되어 있다.

<24> CPU(1030) 상에서 실행된 결과는, 통상적으로, 디스플레이(1007)에 의해 표시되지만, 서버 클라이언트형의 처리를 요구하는 접속이 클라이언트(1001)로부터 서버(1000)로 행해지고, 인증이 확립되어, 서버(1000)와 클라이언트(1001)의 원격 조작용의 암호 통신이 확립된 경우, 클라이언트(1001)를 통하여 서버(1000) 상에서 프로그램을 실행한 처리 결과는 디스플레이(1008)에 표시된다. 이 때, 디스플레이(1008) 상에 표시되는 정보는, 디스플레이(1007)에 표시되는 정보와 표시 방법을 동일하게 해 두고, 유저는, 클라이언트(1001)와 유저 인터페이스

(1010)를 이용하고 있는 것과 서버(1000)를 직접 조작하고 있는 것과 마찬가지로 감지하기 때문에, 이용자의 유저빌리티를 높일 수 있다.

<25> 도 2에, 스토리지 디바이스(1014)의 상세 내용을 나타낸 블록 구성도를 도시한다. 스토리지 디바이스(1014)는, 단자(2000), 컨트롤러(1015), 내탬퍼 디바이스(1016), 스토리지(1017)를 실장하고 있고, 각각이, 도시하는 바와 같이 접속되어 있다. 컨트롤러(1015)는 내부에 CPU(2001), 메모리(2002), 불휘발 메모리(2003), 인터페이스(I/F)(2004, 2005, 2006)를 갖는다. 스토리지(1017)는 플래시 메모리, 하드디스크, EEPROM, MRAM, MO, 광 디스크 등의 불휘발성의 기억 매체이다. 본 실시예에서는, 스토리지(1017)가 플래시 메모리라고 하는 전제에서 설명을 행하지만, 다른 종류의 기억 매체이어도 된다.

<26> 컨트롤러(1015) 내의 CPU(2001)는 불휘발 메모리(2003)로부터 메모리(2002)에 로드된 애플리케이션을 실행하고, 스토리지(1017)의 파일 관리나 내탬퍼 디바이스(1016)의 리세트나 제어 등의, 내탬퍼 디바이스(1016) 및 단자(2000) 및 스토리지(1017) 간의 통신의 관리를, I/F(2004~2006)를 통하여 행한다.

<27> 불휘발 메모리(2003)는 공개 키 연산 프로그램(2050), 공통 키 연산 프로그램(2051) 및 스토리지(1017) 내의 파일 관리 프로그램(2052)을 포함한다. 또한, 불휘발 메모리(2003)는 해시의 연산, 디지털 서명, 증명서의 검증, 키의 생성 등을 행하는 프로그램을 갖고 있어도 된다.

<28> 내탬퍼 디바이스(1016)는 내부에 CPU(2030), 메모리(2031) 및 스토리지(2032)를 포함한다. 코프로세서(2033)는 CPU(2030)의 연산 기능 중 암호 기능 등을 보완하는 코프로세서인데, CPU(2030)의 계산 속도가 고속인 경우, 실장하지 않아도 된다. CPU(2030)는 스토리지(2032)로부터 메모리(2031)에 로드된 애플리케이션을 실행하고, 후술하는 공통 키에 의한 암·복호, 비대칭 키에 의한 암·복호, 스토리지(2032) 내의 파일 관리, 해시의 연산, 디지털 서명, 증명서의 검증, 키의 생성 등을 행하는 기능을 갖는다. 내탬퍼 디바이스(1016)는, 전압 변동 등의 다양한 공격에 대하여 강한 내성이 있는, 시큐러티 평가 단체가 정한 기준에 따라 인정을 받거나, 받는 것이 가능한 수준의 내탬퍼성을 갖는 디바이스이다.

<29> 스토리지(2032)는 EEPROM, MRAM, 플래시 메모리 등의 불휘발성 스토리지이다. 스토리지(2032)는 내부에 비밀 키(2040), PIN 정보(2041), 로그 정보(2042), 증명서(2043), 공개 키(2044), PIN 검증 프로그램(2045), 키 증명서 저장 프로그램(2046), 공개 키 연산 프로그램(2047), 공통 키 연산 프로그램(2048), 키 생성 프로그램(2049) 등을 보존한다. 보존된 프로그램은 하나이어도 복수이어도 된다. 스토리지(2032) 내의 데이터나 프로그램은 메모리(2031)에 로드되고, CPU(2030)를 동작시키거나, 컨트롤러(1015)를 경유하여 내탬퍼 디바이스(1016) 외부로 송신된다.

<30> 비밀 키(2040)는 이용자의 인증이나 통신로를 암호화하는 등을 위한 키로서, 하나이어도 복수개이어도 된다. 비밀 키(2040)는 대응하는 키 알고리즘의 종류에 따라서 다른 포맷으로써 기술된다. 비밀 키(2040) 내의 하나의 비밀 키에 대응하는 공개 키의 모임이 공개 키(2044)이고, 대응하는 증명서의 모임이 증명서(2043)이다. 증명서(2043)는 비밀 키(2040)에 대응하는 공개 키(2044)의 증명서로서, 서버(1000)나 외부 인증국에서 발행된 것이다. 또한, 증명서(2043)는 공개 키(2044)의 증명서와 그 밖의 증명서를 발행한 증명 기간의 루트 인증국이나 중간 인증국의 증명서 등, 그 밖의 인증 정보를 포함한다. 증명서(2043)의 포맷은, 예를 들면 국제전기통신연합(ITU)이 정한 X.509의 사양을 만족하는 것이다. 증명서(2043) 내에 저장되는 정보는, 공개 키와 공개 키에 대한 서명 외에, 예를 들면 증명서의 버전 번호, 증명서의 시리얼 번호, 이용자의 공개 키의 정보, 증명서를 발행한 인증국의 정보, 증명서의 유효 기간, 성명이나 전자 메일 어드레스 등의 이용자의 정보 및 확장 영역 등의 항목으로 구성된다. 증명서(2010)는, 카드 내로부터 클라이언트(1001 및 1002), 서버(1000) 내에서, 인증 정보의 검증이나 데이터나 세션 키 등의 암호화에 이용된다.

<31> PIN 정보(2041)는, 내탬퍼 디바이스(1016) 외부로부터 내탬퍼 디바이스(1016) 내부의 정보를 출력시키거나, 연산을 행하게 하거나 하는 이용자의 권리를 검증하기 위한 정보이다. PIN 정보(2041)는 암증 번호(PIN 코드)이어도 되고, 패스프레이즈라고 불리는 자릿수가 긴 문자열이어도 되고, 지문, 홍채, 얼굴형, 성문, 정맥 등에 의한 생체 인증의 근거로 되는 생체 인증 정보이어도 된다.

<32> 로그 정보(2042)는 내탬퍼 디바이스(1016)의 이용 이력이 기록된 것으로, CPU(3000 혹은 2001 혹은 2030)가 동작할 때마다 추기되거나, 내탬퍼 디바이스(1016)의 외부로부터 적절한 권리를 가진 이용자가 추기하거나, 판독하거나 한다. 로그 정보(2042)는, 제3자로부터의 개찬을 방지하기 위해서, 해시값의 서명을 부가하여 기록한다.

<33> PIN 검증 프로그램(2045)은, PIN 정보(2041)가 내탬퍼 디바이스(1016) 외부로부터 검증용으로 입력된 PIN 정보

와 합치하는지를 검증하는 프로그램이다. 검증 결과가 정당하다면, 내탬퍼 디바이스(1016)는 이용자가 내부의 정보나 연산 자원을 이용 가능한 상태로 한다. PIN 검증 프로그램(2045)은 스토리지(2032) 내에 있고, 메모리(2031)에 로드되는 프로그램이나 스토리지(2032) 상에 보존되는 정보마다 이용 권한을 정하고, 개별적으로 인증을 행한다. 예를 들면, 내탬퍼 디바이스가 통전된 후의 이용 시에 한번 PIN 검증 프로그램에 의해 정당하다고 판단된 이용자에게는 이후의 액세스에서 PIN 검증을 구하지 않거나, 이용할 때마다 PIN 검증을 행하거나 할 수 있도록 설정할 수 있다.

<34> 키 증명서 저장 프로그램(2046)은, 스토리지(2032) 내에 보존되어 있는 비밀 키(2040)나 공개 키(2044)나 증명서(2043)를 내탬퍼 스토리지(1016) 외부에 출력하거나, 내탬퍼 스토리지(1016) 외부로부터 내부로 취득하여 스토리지(2032) 내에 저장하거나 하는 기능을 갖는다. 키 증명서 저장 프로그램(2046)을 이용하기 위해서는 PIN 검증 프로그램(2045)에 의한 검증이 종료될 필요가 있다. 단, 증명서(2043)나 공개 키(2044)를 출력하는 것뿐이라면, PIN 검증 프로그램(2045)에 의한 검증이 불필요한 것으로 하여도 된다. 키 증명서 저장 프로그램(2046)은, 외부에 키나 증명서를 입출력할 때에 외부의 CPU(3000 혹은 2001 혹은 2030)와 세션 키를 교환해서, 안전한 암호화 통신로를 설치하고, 키나 증명서를 주고 받는 기능을 갖고 있다.

<35> 공개 키 연산 프로그램(2047) 및 공통 키 연산 프로그램(2048)은 각각 상술한 공개 키 연산 프로그램(2050) 및 공통 키 연산 프로그램(2051)과 마찬가지의 기능을 갖는다. 키 생성 프로그램(2049)은, 비밀 키(2040) 및 공개 키(2044) 중 하나의 키의 페어나 대상 키의 비밀 키(공통 키)를 생성하는 기능을 갖는다. 작성된 공개 키나 공통 키는 스토리지(2032) 내에 보존되거나, 외부에 출력된다. 비대칭 키의 비밀 키는 비밀 키(2040) 내에 보존된다.

<36> 스토리지(1017)는, 내부에, 이용자를 식별하기 위한 증명서(2010), 이용자가 스토리지 디바이스(1014)를 이용하여 조작을 행한 로그 정보(2011), 디바이스 액세스용 라이브러리(2012), 디바이스 관리용 프로그램(2013), 디바이스 드라이버(2014), 인터페이스 핸들러(2015), 인스톨러(2016), 원격 조작 단말기용 애플리케이션(2017), 암호화 통신로 구축용 애플리케이션(2018), 업무 애플리케이션(2019), 일시 기억 영역(2020), 인증 정보의 카피(2021)를 기록하고 있다.

<37> 증명서(2010)는, 클라이언트(1001)나 서버(1000)가 이용자나 스토리지 디바이스(1014)를 식별하는 연산을 행하기 위해 이용한다. 증명서(2010)의 포맷은, 예를 들면 ITU가 정한 X.509의 사양을 만족하는 것 등이면 된다. 증명서(2010) 내에는, 예를 들면 증명서의 버전 번호, 증명서의 시리얼 번호, 이용자의 공개 키의 정보, 증명서를 발행한 인증국의 정보, 증명서의 유효 기간, 성명, 전자 메일 어드레스나 스토리지 디바이스 고유의 식별 번호 등의 이용자나 스토리지 디바이스의 정보, 확장 영역 등의 것이 기록되어 있다. 증명서(2010)는 스토리지 디바이스(1014) 내나 클라이언트(1001), 서버(1000) 내에서 인증 정보의 검증이나 데이터나 세션 키 등의 암호화에 이용된다.

<38> 로그 정보(2011)는, 이용자가 스토리지 디바이스(1014)를 이용하여 조작을 행한 때에, CPU(2001) 혹은 CPU(2030) 혹은 클라이언트(1001) 혹은 서버(1000)의 지시에 의해 갱신된다. 로그 정보(2011)는, 서버(1000) 상의 애플리케이션이나 클라이언트(1001) 상의 애플리케이션에서 이용되거나, 이용자가 자신의 이용 상황을 확인하기 위해 이용된다. 로그 정보(2011)는, 제3자로부터의 개찬을 방지하기 위해서, 해시값의 서명을 부가하여 기록한다.

<39> 디바이스 액세스용 라이브러리(2012)는, 클라이언트(1001)에서 동작하는 복수의 애플리케이션이 스토리지(1017)에 액세스할 때에 이용하는, 파일 관리, 해시의 연산, 디지털 서명, 증명서의 검증, 키의 생성 등의 기능을 이용하기 위한 함수군이다. 통상적으로, 후술하는 인스톨러(2016)에 의해서, 클라이언트(1001)에 인스톨되어 이용하지만, 직접, 디바이스 액세스용 라이브러리(2012)가 클라이언트(1001) 상의 애플리케이션에서 이용되어도 된다.

<40> 디바이스 관리용 툴(2013)은 스토리지 디바이스(1014)를 관리하기 위한 툴로서, 예를 들면, 이용자의 인증 번호를 변경하는 툴이나 폐색된 스토리지 디바이스를 초기화하는 툴이나 스토리지 디바이스 상의 프로그램이나 펌웨어, 키 정보, 증명서의 재기입 툴이나, 스토리지 디바이스(1014)를 디버그할 때에 필요하게 되는 디버그용 모니터링 툴이나, 스토리지 디바이스의 메뉴얼이나 헬프 파일이나, 원격지로부터 서버의 전원을 투입하는 Wake up on LAN과 같은 기능 등을 이용하여 클라이언트(1001)나 서버(1000)를 리모트로부터 전원 투입이나 전원 차단을 하는 전원 관리 툴을 포함한다. 디바이스 관리용 툴(2013)은, 후술하는 인스톨러(2015)에 의해 클라이언트(1001)에 인스톨되어도 되고, 이용자가 클라이언트(1001)에 직접 로드하여 이용하여도 된다.

<41> 디바이스 드라이버(2014)는 스토리지 디바이스(1014)의 동작에 필요한 정보를 OS에 제공하거나, 동작을 관리하는 프로그램으로서, 후술하는 인스톨러(2015)에 의해 클라이언트(1001)에 인스톨된다.

<42> 인터페이스 핸들러(2015)는 디바이스 드라이버(2014)를 관리하는 미들웨어로서, 클라이언트(1001)나 서버(1000) 상에서 동작하는 애플리케이션과 디바이스 드라이버(2014)를 접속시키는 역할을 한다.

<43> 인스톨러(2016)는 스토리지(1017) 상에 존재하는 애플리케이션이나 정보, 드라이버 등을 클라이언트(1001)나 서버(1000)에 인스톨할 때에 이용자가 이용한다. 인스톨러(2016)에 의해서 인스톨되는 애플리케이션이나 정보, 드라이버 등은 인스톨 종료 후에 스토리지(1017)로부터 삭제되어도 되지만, 이용자가 별도의 기기에 접속하여 스토리지 디바이스(1014)를 이용할 때를 위해 스토리지(1017) 상에 보존해 둔다.

<44> 원격 조작 단말기용 애플리케이션(2017)은 클라이언트(1001)에서 서버(1000)를 원격 조작하기 위해 이용한다. 원격 조작 단말기용 애플리케이션(2017)은, 터미널 서비스나 리모트 데스크탑 등의 클라이언트(1001)나 서버(1000)의 OS가 가진 표준 서비스나 애플리케이션이어도 된다. 원격 조작 단말기용 애플리케이션(2017)은 인스톨러(2016)에 의해서 클라이언트(1001)에 인스톨되어 이용되거나, 혹은 스토리지 디바이스(1014)로부터 클라이언트(1001)에 직접 로드되어 이용된다.

<45> 암호화 통신로 구축용 애플리케이션(2018)은 클라이언트(1001)와 서버(1000) 간의 통신을 암호화시키기 위해서 이용된다. 암호화 통신로 구축용 애플리케이션(2018)은 서버(1000)와 클라이언트(1001) 사이에서 비밀 키를 공유시키고, 그 비밀 키를 이용함으로써 서버(1000)와 클라이언트(1001) 사이에 암호화 통신로를 성립시킨다. 이 비밀 키의 공유에 내탬퍼 디바이스(1016) 내의 비밀 키 등의 비밀 정보를 이용하여도 되고, 비밀 키를 공유하는 프로세스 내에 내탬퍼 디바이스(1016) 내의 비밀 정보를 이용한 인증을 이용하여도 된다.

<46> 업무 애플리케이션(2019)은 이용자가 클라이언트(1001)를 이용할 때에 이용하는 애플리케이션이다. 업무 애플리케이션(2019)은, 예를 들면 서버 상의 웹 베이스의 애플리케이션을 이용하는 것이면, 웹 브라우저이고, 데이터베이스를 이용하는 것이면, 데이터베이스 조작용 클라이언트이다. 스토리지(1017) 상의 모든 정보가, 내탬퍼 디바이스(1016) 내에 있는 비밀 키(2040) 중 몇개의 비밀 키가 서버(1000) 혹은 클라이언트(1001) 상에 보유하는 비밀 키 중의 몇개에 의해 암호화되어 있어도 되고, 평문으로 기록되어 있어도 된다. 전자이면, 이용자에게 제공하는 시큐러티가 향상된다. 또한, 컨트롤러(1015)나 내탬퍼 디바이스(1016) 내에서 이용자 인증이 완료되어 있지 않으면 스토리지(1017)에 액세스할 수 없게 되어 있는 경우, 이용자에게 제공하는 시큐러티가 향상된다.

<47> 일시 기억 영역(2020)은, 업무 애플리케이션(2019) 등의 애플리케이션을 클라이언트(1001) 상에서 실행할 때에, 애플리케이션이 작성하는 일시 파일을 보존해 두는 영역이다. 업무 애플리케이션(2019)이나 서버(1000) 혹은 클라이언트(1001) 상의 업무 수행용 애플리케이션은, 비트맵의 캐시 등의 일시 기억 파일을 일시 기억 영역(2020) 내에 작성한다. 일시 기억 영역이 암호화되어 있지 않은 경우, 이용자가 이용을 정지할 때에는, 컨트롤러(1015) 혹은 클라이언트(1001) 상의 OS 혹은 애플리케이션의 지시에 의해 일시 기억 파일은 소거된다. 이에 의해, 이용자가 작성하는 일시 파일은 스토리지 디바이스 상에 기억되어서, 클라이언트(1001) 내의 정보가 제3자에 의해 위험에 처하여도 이용자가 이용한 정보는 안전하게 보호되어, 전원을 차단한 클라이언트(1001)로부터의 이용자의 기밀 정보나 프라이버시를 포함한 정보는 더욱 누설되기 어렵게 된다.

<48> 도 12에, 스토리지(1017) 상에 기록된 업무 애플리케이션(2019)이나 클라이언트(1001) 등에 인스톨된 애플리케이션에서 일시 기억 영역(2020)을 이용할 때의 처리 방법을 플로우차트로써 나타낸 도면을 도시한다. 도 12의 플로우차트에 도시되는 처리는, 애플리케이션이 실행되는 CPU(1030 혹은 3000)에서 행해진다. 예를 들면, 원격 조작 단말기용 애플리케이션(2017)이나 업무 애플리케이션(2019)은 CPU(3000) 상에서 실행되고, 서버(1000) 상의 애플리케이션은 CPU(1030) 상에서 실행되게 된다. 이 때, 이용자가 이용하는 애플리케이션이 기동되면(12000), 일시 기억 영역(2020)이 애플리케이션에 정의되어 있는지의 여부와 이용 가능한지의 여부가 조사된다(12001). 처리 12001에서, 미정의 혹은 이용 불가능의 경우, 일시 기억 영역(2020)의 영역 정의와 이용 가능화(12002)가 행해진다. 다음으로, 일시 기억 영역의 용량이 충분한가 등 이용 가능한지의 여부의 체크가 행해진다(12004). 용량 부족 등의 문제가 검출된 경우에는, 용량 부족 등 문제 해결 처리가 행해져서(12005) 이상 상태로부터 복귀 가능하면(12006) 처리가 계속되지만, 그렇지 않은 경우에는, 애플리케이션은 이상 종료된다(12007). 다음으로, 애플리케이션의 처리가 개시되고(12003), 일시 기억 영역(2020)에의 입출력이 행해진다(12008). 애플리케이션의 처리가 계속되게 되면, 처리 12004로 되돌아간다. 애플리케이션이 종료되는 경우, 일시 기억 영역(2020)에의 입출력(12010)이 행해진다. 처리 12010은 애플리케이션이 이용한 정보의 소거와 그 확인 작업이다. 처리 12010에 의해 이용자가 이용한 정보가 적절하게 보전되거나, 대부분의 경우에는 소거됨으

로써, 이용자가 갖는 프라이버시를 포함하는 정보나 은닉 정보가 보호된다. 이상이 없으면, 애플리케이션은 종료된다(12011).

<49> 애플리케이션에 따라, 일시 기억 영역(2020)의 정의 방법이 몇가지 존재한다. 하나의 방법은, 애플리케이션이 기동될 때에, 이용자마다 클라이언트(1001) 상에 설치된 이용자의 프로파일에 기재되어 있는 일시 기억 영역의 설정을 애플리케이션이 판독함으로써, 일시 기억 영역(2020)의 장소를 애플리케이션이 특정하는 방식이다. 이 때, 이용자의 프로파일은 OS 혹은 애플리케이션에 의해서 정의되는 이용자의 설정 정보로서, 스토리지(3002) 혹은 스토리지(1017)에 기록되어 있다. 또 하나의 방법은, 애플리케이션이 기동될 때에, 이용자에 대하여, OS 혹은 애플리케이션이 다이얼로그 등의 확인 수단을 디스플레이(1008) 상에 표시하는 등 하여, 이용자에게 입력을 촉구해서, 애플리케이션이 일시 기억 영역의 설정을 특정하는 것이다. 이 확인 수단은, 대부분은 애플리케이션의 최초의 기동 시에 행해지지만, 매기동 시에 행해져도 된다. 이상 중 어느 하나의 방법에 의해, 애플리케이션은 이용자의 이용 환경에 대응한 일시 기억 영역의 설정을 행한다. 한번 이용자가 정의한 정보는, 클라이언트 상의 스토리지(3002) 혹은 스토리지(1017) 상에 정보를 기록함으로써, 애플리케이션 기동 시에 애플리케이션이 재차 이용하면 된다.

<50> 인증 정보의 카피(2021)는, 내탬퍼 디바이스(1016) 내에 있는 공개 키(2044)나 증명서(2043)나 PIN 정보(2041) 등의 카피이다.

<51> 도 3에 인증 정보의 카피(2021)의 예를 도시한다. 증명서 1(5001)~증명서 N(5003)은 증명서(2043)의 일부이다. 미들웨어의 인증 정보(5004)는, 서버(1000)혹은 클라이언트(1001)의 미들웨어가 인증 정보의 카피가 개찬되어 있지 않은지를 검사하는 해시값과 서명이나 미들웨어의 버전 정보, 인증 정보의 카피가 작성된 시각 정보 등의 미들웨어의 인증 정보가 포함된다.

<52> 일반적으로, 내탬퍼 디바이스(1016), 컨트롤러(1015) 간의 통신 속도는 스토리지(1017), 컨트롤러(1015) 간의 통신 속도보다 느린 것이 많다. 이 때문에, 클라이언트(1001) 상의 OS 혹은 애플리케이션이 내탬퍼 디바이스(1016) 내의 인증 정보를 스토리지(1017)에 캐시 혹은 카피해 둠으로써, 이용자가 스토리지 디바이스를 이용할 때에 증명서(2043)의 판독에 요하는 시각을 단축시킬 수 있어, 이용 가능성을 향상시킬 수 있다. 인증 정보의 카피(2021)는 스토리지 디바이스(1014)가 이용될 때마다 검증되는 것이 바람직하고, 이 때, 인증 정보의 카피(2021) 내의 해시값이나 내탬퍼 디바이스(1016) 내의 비밀 키에 의한 서명이나, 클라이언트(1001) 상의 OS 혹은 애플리케이션에 의한 서명이 이용된다.

<53> 도 4에, 클라이언트(1001)의 상세 내용을 나타낸 블록 구성도를 도시한다. 클라이언트(1001)는 내부에 CPU(3000), 메모리(3001), 스토리지(3002), 인터페이스(I/F)(3020, 3021, 3022, 3023)를 갖는다. 스토리지(3002)는 플래시 메모리, 하드디스크, EEPROM, MRAM, MO, 광 디스크 등의 불휘발성의 기억 매체이다.

<54> CPU(3000)는 스토리지(3002)로부터 메모리(3001)에 로드된 애플리케이션을 실행하고, 디스플레이(1008), 네트워크(1006), 유저 인터페이스(1010), 리더 라이터(1012)와의 통신을 각각 I/F(3020, 3021, 3022, 3023)를 통하여 행한다.

<55> 스토리지(3002)에는, 증명서(3010), 로그 정보(3011), 디바이스 액세스용 라이브러리(3012), 디바이스 관리용 툴(3013), 디바이스 드라이버(3014), 인터페이스 핸들러(3015), 원격 조작 단말기용 애플리케이션(3016), 암호화 통신로 구축용 애플리케이션(3017), 업무 애플리케이션(3018)이 보존된다.

<56> 증명서(3010)는, 클라이언트(1001)나 서버(1000)가, 이용자나 스토리지 디바이스(1014)를 식별하는 연산을 행하기 위해 이용한다. 증명서(3010)의 포맷은, 예를 들면 ITU가 정한 X.509의 사양을 만족하는 것 등이면 된다.

<57> 증명서(3010) 내에는, 예를 들면 증명서의 버전 번호, 증명서의 시리얼 번호, 이용자의 공개 키의 정보, 증명서를 발행한 인증국의 정보, 증명서의 유효 기간, 성명, 전자 메일 어드레스나 스토리지 디바이스 고유의 식별 번호 등의 이용자나 스토리지 디바이스의 정보, 확장 영역 등의 것이 기록되어 있다. 증명서(3010)는, 스토리지 디바이스(1014) 내의 증명서(2043)나 스토리지(1017) 내의 증명서(2010)의 카피나 독자적으로 이용자가 등록한 이용자나 증명서를 증명하는 루트 인증국이나 중간 인증국이나 스토리지 디바이스(1014) 등의 내탬퍼 디바이스의 증명서로서, 클라이언트(1001), 서버(1000) 내에서, 인증 정보의 검증이나 데이터나 세션 키 등의 암호화에 이용된다.

<58> 로그 정보(3011)는, 이용자가 클라이언트(1001)의 조작을 행한 경우에, CPU(3000) 혹은 서버(1000)의 지시에 의해 갱신된다. 로그 정보(3011)는, 서버(1000) 상의 애플리케이션이나 클라이언트(1001) 상의 애플리케이션에서 이용되거나, 이용자가 자신의 이용 상황을 확인하기 위해 이용된다. 로그 정보(3011)는, 제3자로부터의 개찬을

방지하기 위해서, 해시값의 서명을 부가하여 기록한다.

<59> 도 5에, 이용자가 클라이언트(1001)에 스토리지 디바이스(1014)를 삽입하여 서버(1000)를 이용할 때의 이용자, 스토리지 디바이스(1014), 클라이언트(1001), 서버(1000) 사이에서 행해지는 통신의 상세 내용을 나타낸 도면을 도시한다. 이용자는, 클라이언트(1001)의 이용을 개시하기까지 이용자의 인증 정보나 클라이언트(1001)를 동작시키기 위한 애플리케이션이 보존된 스토리지 디바이스(1014)를, 클라이언트(1001)의 리더 라이터에 접속한다. 이용자가 클라이언트(1001)를 이용한 적이 없는 경우에는, 이용자는 스토리지 디바이스(1014) 내의 인스톨러(2016)를 이용하여 디바이스 드라이버(2014)나 디바이스 관리 툴(2013)이나 원격 단말기용 애플리케이션(2017)과 같은 서버(1000)를 조작하기 위해 필요한 정보 혹은 애플리케이션을 클라이언트(1001)에 인스톨한다. 이때, 클라이언트(1001)에 의해서 스토리지 디바이스(1014)로부터 직접 실행할 수 있는 애플리케이션의 인스톨을 행할 필요는 없다.

<60> 이용자는, 우선, 시퀀스 4000에 도시하는 바와 같이, 클라이언트(1001)에 동작 확인 요구를 행한다. 클라이언트(1001)는 서버(1000)에 서버 동작 확인을 행하고(4001), 이용자는 서버(1000)의 동작을 확인할 수 없었던 경우에는, 스토리지 디바이스(1014) 상의 혹은 인스톨러(2016)로써 클라이언트(1001) 상에 준비된 원격지로부터 서버의 전원을 투입하는 로컬 에리어 네트워크(LAN)를 이용하여 기기의 전원 투입을 행하도록 하는 Wake up on LAN과 같은 기능을 이용하여 서버(1000)의 전원 투입을 행한다. 이 경우, 서버(1000)의, 네트워크에 대한 I/F만은 항상 통전되어 있고, ID와 패스워드의 세트나 네트워크 보드의 MAC 어드레스 등, 임의의 인증 정보를 이용하여 서버(1000)의 기동이 행해진다(4002, 4003). 이 조작에 의해 서버(1000)는 기동된다(4004). 서버의 기동이 완료되었을 때, 이용자는 클라이언트(1001)에 로그인 요구를 입력한다(4005). 클라이언트(1001) 내에 원격 조작 애플리케이션(2017) 및 암호화 통신로 구축용 애플리케이션(2018)이 인스톨되어 있지 않은 경우, 이 시점에서 클라이언트(1001)에 로드된다(4006). 다음으로, 클라이언트(1001)로부터 서버(1000)에 로그인 요구가 행해진다(4007). 서버(1000)의 리모트 기기로부터의 로그인에 대한 시큐러티 폴리시의 설정에 의하지만, 로그인 시에, 이용자의 인증에서 공개 키 인프라 스트럭쳐(PKI)를 이용한 인증이 필요 혹은 가능한 경우, 서버(1000)로부터의 인증 정보의 요구(4008), 클라이언트(1001)로부터의 증명서의 요구(4009), 스토리지 디바이스(1014)로부터의 증명서의 송신(4010), 클라이언트(1001)로부터의 서명의 요구(4011)가 행해진다. 스토리지 디바이스(1014)에서 서명을 행하는 경우, 이용자의 인증이 필요하게 된다. 이용자의 인증은, 암증 번호, 패스워드, 패스프레이즈, 원타임 패스워드, 지문 정보 등의 생체 인증 정보 등에 의해 행해진다.

<61> 본 실시예에서는 암증 번호를 이용한 예를 설명한다. 스토리지 디바이스(1014)로부터의 암증 번호 요구(4012)가 행해진 후, 클라이언트(1001)로부터 이용자에게 암증 번호 요구 표시(4013)가 디스플레이(1008) 등을 이용하여 행해진다. 이용자가 암증 번호를 유저 인터페이스(1010)와 클라이언트(1001)를 통하여 스토리지 디바이스(1014)에 송신하면(4014, 4015), 스토리지 디바이스(1014) 내의 CPU(2001) 혹은 CPU(2030)에서, 서버(1000), 클라이언트(1001)로부터 송신된 정보에 대하여, 비밀 키(2040) 중 하나 혹은 몇개를 이용한 전자 서명이 작성된다(4016). 작성된 서명은 클라이언트에 송신된다(4017). 클라이언트(1001)는 증명서(2010, 2043) 등의 인증 정보와 작성된 서명의 송신을 행한다(4018). 다음으로, 서버(1000) 및 클라이언트(1001)는 비밀 키나 공개 키 등의 서로의 키 정보와 증명서를 이용하여 비밀 공유 키의 키 교환을 행한다(4019). 이 키 교환(4019)은 원격 조작 단말기용 애플리케이션(2017)이나 암호화 통신로 구축용 애플리케이션(2018)에 의해 행해진다. 시퀀스 4019에서 교환된 비밀 공유 키를 이용하여, 서버(1000) 및 클라이언트(1001)는 암호화 통신로를 구축해서, 양자 사이에서 통신되는 정보는 암호화된다. 암호화 통신로가 구축된 단계에서, 유저는, 서버(1000) 또는 클라이언트(1001), 스토리지 디바이스(1014) 상에 보존되어 있는 애플리케이션을 기동하여, 업무 수행을 한다(4020).

<62> 업무 수행 중에는, CPU(2001) 혹은 CPU(2030) 혹은 서버(1000) 혹은 클라이언트(1001)는 로그 정보(2011, 2042, 3011)에 정보를 추기하고, 이용자의 업무 수행을 적절하게 감시한다. 기재된 로그 정보는 개찬 방지 처리가 실시되어서, 스토리지 디바이스(1014)나 클라이언트(1001) 내에 보존되는데, 이용자의 이용 개시 시나 이용 종료 시 등 적절한 타이밍에서 서버(1000)에 송신된다.

<63> 이용자가 이용하는 서버(1000)의 관리를 행하는 관리자는 로그 정보(2011, 2042, 3011)의 정보와 서버(1000)에 송신되는 정보를 감사해서, 이용자가 관리자가 작성한 폴리시에 위반하는 이용을 행한 때에, 서버(1000) 혹은 클라이언트(1001) 혹은 스토리지 디바이스(1014)의 이용을 정지하는 오퍼레이션을 행한다. 폴리시 위반은, 예를 들면 로그의 개찬이나, 이상한 이용 시간, 이상한 통신량, 네트워크(1006)를 통한 이상한 액세스, 클라이언트(1001) 내에 존재하는 이상한 파일의 검출, 파일이나 애플리케이션의 업데이트의 불비 등이 해당한다. 서버(1000) 혹은 클라이언트(1001) 혹은 스토리지 디바이스(1014)의 이용을 정지하는 오퍼레이션이란, 서버(1000) 및 클라이언트(1001)에의 이용자의 로그인의 금지나 전원 차단, 스토리지 디바이스(1014)의 폐색 등이

해당한다. 스토리지 디바이스(1014)의 폐색이란, PIN 검증 프로그램(2045)이 이용하는 정보를 변경해서, 이용자가 스토리지 디바이스(1014)를 이용할 수 없도록 하는 것이다.

<64> 이용자의 업무 등, 서버(1000) 이용이 종료된 경우, 이용자는 클라이언트(1001)에 대하여 서버 차단 요구를 행한다(4021). 서버 차단 요구는 클라이언트(1001)로부터 서버(1000)에 송신된다(4022). 서버(1000) 및 클라이언트(1001)는 세션 차단(4023)을 행한다. 서버(1000)는 이용자의 이용 정보의 로그를 서버(1000) 상에 기억하고(4024), 서버(1000)의 서버 전원 차단을 행한다. 이용자가 서버 차단 요구(4021)를 행하지 않으면, 서버 전원 차단(4025)은 행해지지 않는다. 서버 전원 차단 후에는 또한, 도 5에 도시하는 시퀀스로 업무 수행이 행해진다.

<65> 도 6은 이용자가 서버(1000) 및 클라이언트(1001) 및 스토리지 디바이스(1014)를 이용하기 위해 관리자가 행하는 스토리지 디바이스(1014)의 초기화 조작을 설명한 도면이다. 도 6에서 설명되는 일련의 동작은 도 5에 도시한 이용자의 이용이 개시되기 전 혹은 이용자가 카드를 폐색 혹은 분실해서 이용 권한을 잃어버렸을 때에 행해진다.

<66> 클라이언트(6000)는, 클라이언트(1001)와 마찬가지로, 디스플레이나 유저 인터페이스나 리더 라이터를 접속한 클라이언트로서, 관리자가 스토리지 디바이스(1014)의 기입을 행하기 위해 이용한다.

<67> 우선, 관리자는 이용자의 성명, 유저 번호, 전자 메일 어드레스나 스토리지 디바이스 고유의 식별 번호 등을, 클라이언트(6000)를 통하여 서버(1000)에 등록함으로써, 서버(1000)에서 이용자의 인증 정보를 작성한다. 이용자의 인증 정보 및 증명서의 작성과 기입 요구를 행한다(6001). 여기서, 스토리지 디바이스(1014)에는, 이미 스토리지 디바이스 공급자로부터 키 증명서 저장 프로그램(2046) 등의 각종 프로그램이 기입되어 있다. 또한, 이용자의 공개 키 증명서는, 스토리지 디바이스(1014), 혹은 클라이언트(6000), 혹은 관리자 중 어느 하나가 별도 생성한 비밀 키에 대응하는 공개 키를, 6001에서 송부함으로써 얻어진다. 작성된 인증 정보와 공개 키 증명서는 클라이언트(6000)를 경유하여 스토리지 디바이스에 기입된다(6002). 다음으로, 관리자는 스토리지 디바이스(1014) 내의 인증 정보와 키의 이용권을 컨트롤하기 위한 정보를 변경한다(6003, 6004). 이 조작에 의해서, 스토리지 디바이스(1014)는 서명 요구나 키 재기입 요구, 키의 익스포트·임포트 요구에 대한 이용권을 변경한다. 이용권의 변경은, 정보에 대한 액세스 키의 변경이나, 암증 번호의 변경이다. 변경된 액세스 키나 암증 번호는 관리자가 보관하거나, 다른 내탬퍼 디바이스에 저장하거나, 이용자에게 통지한다.

<68> 다음으로, 관리자는 애플리케이션의 기입 요구를 행하고, 클라이언트(6000)는 애플리케이션의 기입을 행한다. 여기서 말하는 애플리케이션이란, 디바이스 액세스용 라이브러리(2012), 디바이스 관리용 툴(2013), 디바이스 드라이버(2014), 인터페이스 핸들러(2015), 인스톨러(2016), 원격 조작 단말기용 애플리케이션(2017), 암호화 통신로 구축용 애플리케이션(2018), 업무 애플리케이션(2019) 등이다.

<69> 다음으로, 관리자는 서버 접속 시험 요구(6007)를 행하고, 서버 접속 시험이 행해진다(6008). 서버 접속 시험(6008)은, 도 5에서 도시한 이용자가 행하는 서버에의 접속이나 업무 수행의 프로세스를 관리자가 행하고, 스토리지 디바이스(1014) 내에 기록된 정보나 애플리케이션의 유효성을 확인하는 것이다. 접속과 업무 수행 프로세스가 정확하게 행해진 경우, 스토리지 디바이스(1014)는 이용자에게 송부된다. 이 때, 스토리지 디바이스(1014)에는 이용자의 ID나 얼굴 사진이나 성명 등이 인쇄되거나, 시일 침이 부착되는 등이 이루어진다. 또한, 스토리지 디바이스(1014)를 관리하기 위한 정보에 대한 액세스 키나 암증 번호도, 스토리지 디바이스(1014)를 송부하는 것과는 별도의 봉서 등의 방법으로 이용자에게 송부된다.

<70> 도 11은 본 실시예의 클라이언트(1001) 상에서 동작하는 미들웨어에 대하여 설명한 도면이다. 클라이언트(1001) 상에서 동작하는 원격 조작 단말기용 애플리케이션(2017)이나 암호화 통신로 구축용 애플리케이션(2018), 업무 애플리케이션(2019)과 같은 애플리케이션(11000)은, 도시하는 바와 같이, 2개의 경로를 이용하여 리더 라이터(1012) 및 스토리지 디바이스(1014)에 액세스를 행한다. 카드 내의 파일 액세스나 파일 관리를 행하고자 하는 경우에는, 파일 액세스용 API(11001), 파일 액세스용 드라이버(11002), 리더 라이터(1012) 내의 리더 라이터 펌웨어(11003)를 경유하여, 스토리지 디바이스(1014) 내의 카드 OS 및 애플리케이션(11004)이 호출된다. 또한, 카드 내의 내탬퍼 디바이스(2032)에 명령을 발하는 등, 시큐러티 인증에 관계되는 명령을 실행하고자 하는 경우에는, 인터페이스 핸들러(3015), 디바이스 드라이버(3014), 리더 라이터(1012) 내의 리더 라이터 펌웨어(11003)를 경유하여, 스토리지 디바이스(1014) 내의 카드 OS 및 애플리케이션(11004)이 호출된다. 이 때, 파일 액세스용 드라이버(11002), 리더 라이터 펌웨어(11003), 디바이스 드라이버(3014)는 서로의 명령이 동시에 발생하는 일이 없도록 항상 스토리지 디바이스(1014)와 리더 라이터(1012)의 액세스 상태를 감시하고, 스토리지 디바이스(1014)에 대하여 적절한 액세스가 이루어지도록 자체적으로 명령의 스토크나 거부 등의 폭주 제

어를 행한다.

<71> 도 13은, 디바이스 드라이버(3014)와 파일 액세스용 드라이버(11002)가 행하는 폭주 제어를, 플로우차트를 이용하여 설명한 도면이다. 디바이스 드라이버(3014 및 11002)는 OS 기동 시 등에 초기화되어, 처리가 개시된다(13000). 파일 액세스용 드라이버(11002)에의 요구 혹은 대기 요구가 있는지의 여부에 대한 체크가 행해지고(13001), 요구가 있었던 경우, 리더 라이터를 통한 카드에의 파일 액세스가 행해진다(13002). 다음으로, 디바이스 드라이버(3014)에의 요구가 있는지의 여부의 체크가 행해진다(13003). 있는 경우에는, 리더 라이터를 통한 CPU(2030)에의 액세스가 행해진다(13004). 파일 액세스용 드라이버(11002)에의 요구가 이 시점에서 있는지의 여부에 대한 체크가 행해지고(13005), 요구가 있었던 경우, 파일 액세스용 드라이버(11002)에의 요구 대기 처리가 행해진다. 이 요구 대기 처리는 파일 액세스용 드라이버(11002)에서 행해지고, 요구 대기용으로 만들어진 메모리 영역에, 대기할 요구가 스토크된다. 스토크된 요구는, 다음에 처리 13002가 실행될 때에 처리된다. 단, 처리 13002에 의해 처리가 행해지기까지의 스토크해 있는 시간이 미리 정한 일정량을 초과한 경우에는, 처리 13005 내에서, 애플리케이션에 타임 아웃 등 이상을 통지하고, 처리를 파기한다. 디바이스 드라이버(3014)에의 요구가 종료되었다고 인식할 수 있는지의 여부에 대한 체크가 행해지고(13007), 처리가 완료되지 않은 경우에는, 처리 13004에서부터 재처리가 행해진다.

<72> 또한, OS로부터의 종료 요구가 체크되고(13008), 요구가 없는 경우에는, 재처리 13001에서부터 처리가 개시된다. 상술한 바와 같은 디바이스 드라이버(3014) 및 파일 액세스용 드라이버(11002)에 의한 폭주 제어에 의해, 리더 라이터를 통한 스토리지 디바이스(1014)의 액세스는 일반적인 스토리지 디바이스와 마찬가지로 유지된다. 폭주 제어란, 파일 액세스에 관한 명령과, 내탬퍼 디바이스에 대한 명령의 폭주를 제어함으로써, 파일 액세스용 드라이버(11002)는, 일반적인 매스 스토리지 디바이스 드라이버로도, 매스 스토리지 디바이스 드라이버에 접속하는 업퍼 필터 드라이버나 로어 필터 드라이버로도 행해도 된다. 또한, 리더 라이터 펌웨어에 명령을 퇴피시키는 메모리 영역 혹은 버퍼를 설치하고, 명령을 대기시켜, 폭주를 제어하여도 된다.

<73> 또한, 폭주 제어에 대하여 상세히 설명한다. 폭주 제어란, 후술하는 바와 같은 대기 처리 혹은 경합 해결 처리를 나타낸다. 여기서, 폭주를 제어하는 것은, 후술하는 대기시켜진 커맨드 리스트를 클라이언트 상의 메모리 영역에 작성하여 소프트웨어적으로 처리하여도 되고, 리더 라이터의 펌웨어에 의해 소프트웨어적으로 해결하여도 되며, 리더 라이터 상에 버퍼를 설치하여 하드웨어적으로 해결하여도 된다.

<74> 도 14는 디바이스 드라이버(3014)와 파일 액세스용 드라이버(11002)에서의 폭주 제어에 의해 발하여지는 커맨드의 양태를 나타내는 타임차트이다. CPU(2030)에의 액세스를 위한 커맨드 1, 커맨드 2가 순서대로 드라이버로부터 발하여지도록 애플리케이션으로부터 지시가 있었다고 하자. 도 14의 파일 액세스용 커맨드에 나타낸 바와 같이, 커맨드 1이 스토리지 디바이스(1014)에 발하여지고, 그 응답으로서 리스폰스 1이 있다. 다음으로, 커맨드 2가 스토리지 디바이스(1014)에 발하여지고, 그 응답으로서 리스폰스 2가 있다. 이 커맨드의 발행, 응답 사이에 파일 액세스용 커맨드 3이나 커맨드 4가 발하여졌다고 하자. 이 때, 파일 액세스용 드라이버는 커맨드 3이나 커맨드 4를 대기시켜진 커맨드 리스트에 저장한다. 도 13에서의 처리 13002에서 CPU(2030)에의 액세스를 위한 커맨드로부터의 입력이 없다고 판단되는 경우, 대기시켜진 파일 액세스용 커맨드 3이 발하여지고, 그 리스폰스 3의 응답이 있다. 다음으로, 대기시켜진 파일 액세스용 커맨드 4가 발하여지고, 그 리스폰스 4의 응답이 있다. 전체적으로, 스토리지 디바이스(1014)에 송수신되는 커맨드와 리스폰스는, 예를 들면, 도 14에서의 「모든 커맨드와 리스폰스」에 나타낸 바와 같이, 순서대로 커맨드 1, 리스폰스 1, 커맨드 2, 리스폰스 2, 커맨드 3, 리스폰스 3, 커맨드 4, 리스폰스 4와 같이 된다.

<75> 상술한 바와 같이, 본 실시예에서 설명한 클라이언트(1001)는, 내탬퍼 스토리지 기능을 탑재한 스토리지 디바이스(1014)를 삽입하여 서버(1000)를 원격 조작함으로써, 이용자에게 안전하고, 사용 편리성 좋게 이용할 수 있는 업무 시스템을 구성하는 것이 가능하게 된다.

<76> 또한, 이용자는, 이용하는 클라이언트(1001)로부터 클라이언트(1002)로 변경하였다고 하여도, 클라이언트(1001)를 이용하는 것과 마찬가지의 조작 감각으로써 업무 수행을 행할 수 있기 때문에, 이용자의 사용 편리성이 향상된다.

<77> 또한, 이용자가 이용을 정지할 때에는, 이용자가 이용하고 있었던 일시 기억 파일이 소거되기 때문에, 클라이언트(1001) 내의 정보가 제3자에 의해서 위험에 처하여도 이용자가 이용한 정보는 안전하게 보호되어, 전원을 차단한 클라이언트(1001)로부터의 이용자가 이용한 기밀 정보나 프라이버시를 포함한 정보는 더욱 누설되기 어렵게 됨으로써, 이용자의 편리성을 향상시킨다.

<78> 또한, 본 실시예에서는 클라이언트(1001) 및 서버(1000)를 별개의 구성으로 하여 설명하였지만, 반대로 클라이언트(1001)가 서버(1000)의 기능을 겸하거나, 서버(1000)를 클라이언트(1001) 대신에 사용하거나 하는 것이 가능하여도 된다. 또한, 서버(1000), 클라이언트(1001, 1002)는, PC나 Personal Digital Assistants(PDA), 워크스테이션인 것으로 설명하였지만, 고기능 복사기, 현금 자동 지불기(ATM), 휴대 전화기, 디지털 스틸 카메라, 비디오 카메라, 음악 재생(녹음) 장치, 판매 시점 상품 관리 시스템, 가두 단말기, Intelligent Transport Systems(ITS)용 송신기, 발권기, 결제 단말기, 개찰기, 자동 판매기, 입퇴실 관리 장치, 게임기, 공중 전화기, 주문 접수용 휴대 단말기, 전자 지갑, 유료 방송 수신기, 의료 카드 관리 장치 등으로 하여도 마찬가지이다.

<79> (제2 실시예)

<80> 도 7 내지 도 9를 이용하여, 본 발명에 따른 시큐어 리모트 액세스 시스템의 제2 실시예를 설명한다.

<81> 도 7은 본 발명의 제2 실시예의 리모트 액세스 시스템을 도시하는 도면이다.

<82> 이용자가 사용하는 서버(1000)와 클라이언트(1001), 스토리지 디바이스(1014)는 제1 실시예에서 설명한 것과 마찬가지이다. 게이트웨이(7000)는, 클라이언트(1001)와 서버(1000)의 통신의 암호화와 이용자, 이용 기기 인증을 행하는 중계 기기이다.

<83> 게이트웨이(7000)는, 일반적으로, 파이어월, 암호화 게이트웨이, 버추얼 프라이빗 네트워크(VPN) 게이트웨이 등으로 불린다. 본 실시예에서는, 게이트웨이(7000)는 파이어월과 암호 통신 기능이 인스톨된 서버기인 것으로 하여 설명을 행하지만, 예를 들면, 네트워크 라우터나 무선 LAN 액세스 포인트, 네트워크 허브, 브로드밴드 라우터 등이어도 된다. 네트워크(7001)는, 예를 들면 인터넷이나 지역 IP 네트워크와 같은 공중 회선으로서, 네트워크(1006)로부터 통신 내용의 도청이나 개찬의 위험성이 높은 네트워크이다. 클라이언트(1001)는, 네트워크(7001)를 통하여 서버(1000)를 원격 조작하기 때문에, 게이트웨이(7000)와 클라이언트(1001) 사이에서 암호 통신과 암호 통신을 행하기 위한 인증을 행한다.

<84> 게이트웨이(7000)는, CPU(7002), 메모리(7003), 스토리지(7004)를 갖고, 동작 시에 스토리지(7004) 내에 설정된 암호 통신 및 인증용 애플리케이션이 메모리(7003)에 로드되고, CPU(7002)에서 통신의 제어를 행한다. 게이트웨이(7000)는 인증용 서버(7005)에 직접 혹은 네트워크를 경유하여 접속하고 있다. 인증용 서버(7005)는 게이트웨이(7000)에 의해 암호 통신을 행할 때의 인증 정보를 축적해서, 게이트웨이(7000)의 문의에 대하여 응답하거나, 접속된 리더 라이터(7007)를 통하여 스토리지 디바이스(1014)의 초기화나 활성화, 개인화 등을 행한다. 인증용 서버(7005)는 내부 인증국을 갖고 있어도 되고, 외부 인증국의 증명서 리스트나 증명서 리보케이션 리스트를 관리하여 게이트웨이(7000)에 통지하는 역할만을 갖고 있어도 된다.

<85> 도 8에, 본 실시예의 리모트 액세스 시스템을 이용할 때의 스토리지 디바이스(1014)의 초기화와 이용자가 클라이언트(1001)에 스토리지 디바이스(1014)를 삽입하여 서버(1000)를 이용할 때의 관리자, 이용자, 스토리지 디바이스(1014), 클라이언트(1001), 게이트웨이(7000), 서버(1000) 사이에서 행해지는 통신의 상세 내용을 나타낸 도면을 도시한다.

<86> 관리자는 스토리지 디바이스(1014)를 인증 서버(7005)와 통신이 가능한 리더 라이터(7007)에 삽입한다. 관리자는, 이용자의 성명, 유저 번호, 전자 메일 어드레스나 스토리지 디바이스 고유의 식별 번호 등을, 클라이언트(1001)를 통하여 인증 서버(7005)에 등록함으로써, 인증 서버(7005)에서 이용자의 인증 정보를 작성한다. 이용자의 인증 정보 및 증명서의 작성과 기입 요구를 행한다(8001). 여기서, 스토리지 디바이스(1014)에는, 이미 스토리지 디바이스 공급자로부터 키 증명서 저장 프로그램(2046) 등의 각종 프로그램이 기입되어 있다. 또한, 이용자의 공개 키 증명서는, 스토리지 디바이스(1014) 혹은 인증 서버(7005) 혹은 관리자가 별도 생성한 비밀키에 대응하는 공개 키를 8001에서 송부함으로써 얻어진다. 작성된 인증 정보와 공개 키 증명서는 스토리지 디바이스(1014)에 기입된다. 다음으로, 관리자는 스토리지 디바이스(1014) 내의 인증 정보와 키의 이용권을 컨트롤하기 위한 정보를 변경한다(8003, 8004). 이 조작에 의해서, 스토리지 디바이스(1014)는 서명 요구나 키 재기입 요구, 키의 익스포트·임포트 요구에 대한 이용권을 변경한다. 이용권의 변경은, 정보에 대한 액세스 키의 변경이나, 암증 번호의 변경이다. 변경된 액세스 키나 암증 번호는 관리자가 보관하거나, 다른 내탬퍼 디바이스에 저장하거나, 이용자에게 통지한다.

<87> 다음으로, 관리자는 애플리케이션의 기입 요구를 행하고, 인증 서버(7005)는 애플리케이션의 기입을 행한다. 여기서 말하는 애플리케이션이란, 디바이스 액세스용 라이브러리(2012), 디바이스 관리용 툴(2013), 디바이스 드라이버(2014), 인터페이스 핸들러(2015), 인스톨러(2016), 원격 조작 단말기용 애플리케이션(2017), 암호화 통신로 구축용 애플리케이션(2018), 업무 애플리케이션(2019) 등이다.

<88> 다음으로, 관리자는 서버 접속 시험 요구(8007)를 행하고, 서버 접속 시험이 행해진다(8008). 서버 접속 시험(8007)은 스토리지 디바이스(1014) 내에 기록된 정보나 애플리케이션의 유효성을 확인하는 것이다. 접속과 업무 수행 프로세스가 정확하게 행해진 경우, 스토리지 디바이스(1014)는 이용자에게 송부된다(8009). 이 때, 스토리지 디바이스(1014)를 관리하기 위한 정보에 대한 액세스 키나 암증 번호도, 스토리지 디바이스(1014)를 송부하는 것과는 별도의 봉서 등의 방법으로 이용자에게 송부된다.

<89> 다음으로, 이용자는, 클라이언트(1001)의 이용을 개시하기까지 이용자의 인증 정보나 클라이언트(1001)를 동작시키기 위한 애플리케이션이 보존된 스토리지 디바이스(1014)를, 클라이언트(1001)의 리더 라이터에 접속한다. 이용자가 클라이언트(1001)를 이용한 적이 없는 경우에는, 이용자는 스토리지 디바이스(1014) 내의 인스톨러(2016)를 이용하여 디바이스 드라이버(2014)나 디바이스 관리 툴(2013)이나 원격 단말기용 애플리케이션(2017)과 같은 서버(1000)를 조작하기 위해 필요한 정보 혹은 애플리케이션을 클라이언트(1001)에 인스톨한다. 이 때, 클라이언트(1001)에 의해 스토리지 디바이스(1014)에서 직접 실행할 수 있는 애플리케이션의 인스톨을 행할 필요는 없다.

<90> 이용자는, 우선, 시퀀스 8010에 나타낸 바와 같이, 클라이언트(1001)에 게이트웨이 접속 요구를 행한다. 클라이언트(1001)는 게이트웨이(7000)에 서버 동작 확인을 행하고(8011), 게이트웨이(7000)의 리모트 기기로부터의 로그인에 대한 시큐러티 폴리시의 설정에 의하지만, 이용자의 인증을 PKI를 이용한 인증이 필요 혹은 가능한 경우, 게이트웨이(7000)로부터의 인증 정보의 요구(8012), 클라이언트(1001)로부터의 증명서의 요구(8013), 스토리지 디바이스(1014)로부터의 증명서의 송신(8014), 클라이언트(1001)로부터의 서명의 요구(8015)가 행해진다. 스토리지 디바이스(1014)에서 서명을 행하는 경우, 이용자의 인증이 필요하게 된다. 이용자의 인증은, 암증 번호, 패스워드, 패스프레이즈, 원타임 패스워드, 지문 정보 등의 생체 인증 정보 등에 의해 행해진다. 본 실시예에서는 암증 번호를 이용한 예를 설명한다. 스토리지 디바이스(1014)로부터의 암증 번호 요구(8016)가 행해진 후, 클라이언트(1001)로부터 이용자에게 암증 번호 요구 표시(8017)가 디스플레이(1008) 등을 이용하여 행해진다. 이용자가 암증 번호를 유저 인터페이스(1010)와 클라이언트(1001)를 통하여 스토리지 디바이스(1014)에 송신하면(8018, 8019), 스토리지 디바이스(1014) 내의 CPU(2001) 혹은 CPU(2030)에서, 서버(1000), 클라이언트(1001)로부터 송신된 정보에 대하여, 비밀 키(2040) 중의 하나 혹은 몇개를 이용한 전자 서명이 작성된다(8020). 작성된 서명은 클라이언트에게 송신된다(8021). 클라이언트(1001)는 증명서(2010, 2043) 등의 인증 정보와 작성된 서명의 송신을 행한다(8022). 다음으로, 서버(1000) 및 클라이언트(1001)는, 비밀 키나 공개 키 등의 서로의 키 정보와 증명서를 이용하여, 비밀 공유 키의 키 교환을 행한다(8023). 이 키 교환(8023)은 암호화 통신로 구축용 애플리케이션(2018)에 의해 행해진다. 시퀀스 8023에서 교환된 비밀 공유 키를 이용하여, 게이트웨이(7000) 및 클라이언트(1001)는 암호화 통신로를 구축하고, 양자 사이에서 통신되는 정보는 암호화된다.

<91> 다음으로, 이용자는, 시퀀스 8030에 나타낸 바와 같이, 클라이언트(1001)에게 동작 확인 요구를 행한다. 클라이언트(1001)는 서버(1000)에게 서버 동작 확인을 행하고(8031), 이용자는 서버(1000)의 동작을 확인할 수 없었던 경우에는, 스토리지 디바이스(1014) 혹은 인스톨러(2016)에 의해 클라이언트(1001) 상에 준비된 원격지로부터 서버의 전원을 투입하는 LAN을 이용하여 기기의 전원 투입을 행하도록 하는 Wake up on LAN과 같은 기능을 이용하여 서버(1000)의 전원 투입을 행한다. 이 경우, 서버(1000)의, 네트워크에 대한 I/F는 항상 통전되어 있고, ID와 패스워드의 세트나 네트워크 보드의 MAC 어드레스 등, 임의의 인증 정보를 이용하여 서버(1000)의 기동이 행해진다(8032, 8033). 이 조작에 의해, 서버(1000)는 기동된다(8034). 서버의 기동이 완료되었을 때, 이용자는 클라이언트(1001)에 로그인 요구를 입력한다(8035). 이 조작은 클라이언트(1001) 내의 원격 조작 애플리케이션(2017)에 의해 행해진다. 원격 조작 애플리케이션이 인스톨되어 있지 않은 경우, 이 시점에서 클라이언트(1001)에 로드된다. 서버(1000)의 리모트 기기로부터의 로그인에 대한 시큐러티 폴리시의 설정에 의하지만, 로그인 시에, 이용자의 인증을, PKI를 이용한 인증이 필요 혹은 가능한 경우, 서버(1000)로부터의 인증 정보의 요구 등이 행해지고, 8012~8023과 마찬가지의 서명의 작성과 송신이 서버(1000)에 대하여 행해진다. 이용자는, 게이트웨이(7000)에서 강고한 인증을 통과하고 있기 때문에, 서버(1000)가 게이트웨이(7000)로부터의 통신을 신뢰할 수 있다고 하면, 로그인 요구(8035)를 행할 때의 서버(1000)의 인증은 ID와 패스워드 인증 등의 간편한 것이어도 된다.

<92> 암호화 통신로 구축과 서버(1000)에의 로그인이 완료된 단계에서, 유저는, 서버(1000) 또는 클라이언트(1001), 스토리지 디바이스(1014) 상에 보존되어 있는 애플리케이션을 기동해서, 업무 수행을 한다(8036).

<93> 업무 수행 중에는, CPU(2001) 혹은 CPU(2030) 혹은 서버(1000) 혹은 클라이언트(1001)는 로그 정보(2011, 2042, 3011)에 정보를 추기하고, 이용자의 업무 수행을 적절하게 감시한다. 기재된 로그 정보는 개찬 방지 처리가 실시되어서, 스토리지 디바이스(1014)나 클라이언트(1001) 내에 보존되는데, 이용자의 이용 개시 시나 이

용 종료 시 등 적절한 타이밍에서 서버(1000)에 송신된다.

<94> 이용자가 이용하는 서버(1000)의 관리를 행하는 관리자는 로그 정보(2011, 2042, 3011)의 정보와 서버(1000)에 송신되는 정보를 감사해서, 이용자가 관리자가 작성한 폴리시에 위반하는 이용을 행한 때에, 서버(1000) 혹은 클라이언트(1001) 혹은 스토리지 디바이스(1014)의 이용을 정지하는 오퍼레이션을 행한다. 폴리시 위반은, 예를 들면 로그의 개찬이나, 이상한 이용 시간, 이상한 통신량, 네트워크(1006)를 통한 이상한 액세스, 클라이언트(1001) 내에 존재하는 이상한 파일의 검출, 파일이나 애플리케이션의 업데이트의 불비 등이 해당한다. 서버(1000) 혹은 클라이언트(1001) 혹은 스토리지 디바이스(1014)의 이용을 정지하는 오퍼레이션이란, 서버(1000) 및 클라이언트(1001)에의 이용자의 로그인의 금지나 전원 차단, 스토리지 디바이스(1014)의 폐색 등이 해당한다. 스토리지 디바이스(1014)의 폐색이란, PIN 검증 프로그램(2045)이 이용하는 정보를 변경해서 이용자가 스토리지 디바이스(1014)를 이용할 수 없도록 하는 것이다. 이용자의 업무 등, 서버(1000)의 이용이 종료된 경우, 이용자는 클라이언트(1001)에 대하여 서버 차단 요구를 행한다(8037). 서버 차단 요구는 클라이언트(1001)로부터 서버(1000)에 송신된다(8038). 서버(1000) 및 클라이언트(1001)는 세션 차단(8039)을 행한다. 서버(1000)는 이용자의 이용 정보의 로그를 서버(1000) 상에 기억하고(8040), 서버(1000)의 서버 전원 차단을 행한다. 이용자가 서버 차단 요구(8037)를 행하지 않으면, 서버 전원 차단(8041)은 행해지지 않는다. 서버 전원 차단 후에는 또한, 8010 이후의 시퀀스로 업무 수행이 행해진다.

<95> 도 9에, 본 실시예의 리모트 액세스 시스템의 네트워크 구성을 나타낸 블록도를 도시한다. 도면 중 참조 부호 9000으로 나타내어진 네트워크와 네트워크에 접속된 기기의 그룹은, 이용자가 중심적으로 이용하는 네트워크와 기기의 그룹이다. 네트워크와 기기의 그룹(9000)은, 예를 들면, 이용자가 항상 근무하는 사무실의 로컬 에리어 네트워크(LAN)와 LAN에 접속된 기기이다. 9000 내에는, 유저가 이용 가능한 서버(1000), 클라이언트(1002), 부문 서버(9001), PC(9002), 게이트웨이(9006, 7000), 인증 서버(7005)가 LAN(9003)을 중심으로 접속되어 있다. 또한, 참조 부호 9010으로 나타내어진 네트워크와 네트워크에 접속된 기기의 그룹은, 이용자가 출장 시 등에 이용하는 소속 외의 사업부 등의 WAN 상의 네트워크와 기기의 그룹이다. 9010 내에는, 유저가 이용 가능한 클라이언트(9008), 게이트웨이(9007)가 네트워크(9005)를 중심으로 하여 접속되어 있다. 또한, 네트워크(7001)와 같은 사외의 네트워크에 라우터(9004)를 통하여 클라이언트(1001)가 접속되어 있다.

<96> 여기서, 이용자는 스토리지 디바이스(1014)를 갖고 다님으로써, LAN 상의 클라이언트(1002), WAN 상의 클라이언트(9008), 인터넷을 통하여 LAN(9003)에 접속하고 있는 클라이언트(1001)를 이용해서, LAN(9003)과 접속된 서버(1000), 부문 서버(9001), PC(9002)를 이용할 수 있다. 이 때, LAN 상의 클라이언트(1002), WAN 상의 클라이언트(9008)로부터 LAN(9003)과 접속된 서버(1000), 부문 서버(9001), PC(9002)를 이용할 때에는, 게이트웨이(9007, 9006)에서는 통신의 암·복호를 행하지 않고, 게이트웨이(7000)를 이용하는 경우, 통신의 암·복호를 행하도록 하면, 이용자의 이용 수순의 간략화를 도모하면서, 통신 내용의 은닉이 가능하다. 여기서, 부문 서버(9001)란, LAN 상에 설치된 웹 서버나 메일 서버나 리모트 로그인하여 연산을 행하는 터미널 서버 등을 나타낸다. PC(9002)는, 이용자가 소속된 부문이 공유 등으로 이용하고 있는 공유 자원 관리용 PC나 출장자용 대출 PC 등을 나타낸다.

<97> 상술한 바와 같이, 본 실시예에서 설명한 클라이언트(1001)는, 내탬퍼 스토리지 기능을 탑재한 스토리지 디바이스(1014)를 삽입하여 서버(1000), 부문 서버(9001), PC(9002) 등을 원격 조작함으로써, 이용자에게 안전하고, 사용 편리성 좋게 이용할 수 있는 업무 시스템을 구성하는 것이 가능하게 된다.

<98> 또한, 이용자는, 이용하는 클라이언트(1001)로부터 클라이언트(1002, 9008)로 변경하였다고 하여도, 여러 가지 다른 업무 집행 장소에서, 클라이언트(1001)를 이용하는 것과 마찬가지의 조작 감각으로 업무 수행을 행할 수 있기 때문에, 이용자의 사용 편리성이 향상된다. 또한, 서버(1000), 클라이언트(1001, 1002, 9008)는, PC나 PDA, 워크스테이션인 것으로 설명하였지만, 고기능 복사기, ATM, 휴대 전화기, 디지털 스틸 카메라, 비디오 카메라, 음악 재생(녹음) 장치, 판매 시점 상품 관리 시스템, 가두 단말기, ITS용 송신기, 발권기, 결제 단말기, 개찰기, 자동 판매기, 입퇴실 관리 장치, 게임기, 공중 전화기, 주문 접수용 휴대 단말기, 전자 지갑, 유료 방송 수신기, 의료 카드 관리 장치 등으로 하여도 마찬가지다.

<99> (제3 실시예)

<100> 도 10을 이용하여, 본 발명에 따른 시큐어 리모트 액세스 시스템의 제3 실시예를 설명한다.

<101> 도 10은 본 발명의 제3 실시예를 나타내는 리모트 액세스 시스템을 도시하는 도면이다.

<102> 이용자가 사용하는 서버(10000)는 서버(1000)와 동등한 기능을 갖는 복수개의 서버(PC)의 집합체이다. 서버

(10000)는, 서버(10032, 10042, …, 10052) 상에 있는, 각각 CPU(10030, 10040, …, 10050), 메모리(10031, 10041, …, 10051)에 의해 동작한다. 도 10에서는, 이용자는 서버(10032)를 이용하여, CPU(10030) 상에서 실행된 정보를 디스플레이(1008)에 출력시켜 업무를 수행하고 있다. 서버(10000)는 절환기(10004)를 이용하여 서버(10032, 10042, …, 10052)와 접속하는 유저 인터페이스(10003) 및 디스플레이(10002)를 선별하고 있다. 또한, 서버(10000)는 제어 장치(10001)에 접속되어 있다. 제어 장치(10001)는 네트워크(1005)에 접속되어 있어, 서버(10000)와 마찬가지로 스토리지 디바이스(1014)를 갖는 적절한 이용자가 이용 가능하다. 여기서, 이용자가 서버(10032, 10042, …, 10052) 중 어느 하나를 이용하려고 하였을 때에, 제어 장치(10001)는 서버(10032, 10042, …, 10052)의 전원 관리, 전원의 온·오프 상태의 클라이언트에의 통지를 행한다. 특히, 클라이언트(1001)로부터의 서버(10032, 10042, …, 10052)에의 통신이 불통되었을 때에는, 이용자는 제어 장치(10001)에 로그인하여, 서버(10032, 10042, …, 10052)의 상태를 확인하거나, 전원을 온·오프하거나 한다. 제어 장치(10001) 내에는 하드디스크나 플래시 메모리 등의 서버 부팅용 스토리지가 실장되어 있어, 이 스토리지 상의 데이터를 이용하여 서버(10032~10052)가 부팅 업된다. 이에 의해, 이용자의 서버 관리의 공수가 감소된다.

<103> 상술한 바와 같이, 본 실시예에서 설명한 서버(10000) 및 제어 장치(10001)를, 내탬퍼 스토리지 기능을 탑재한 스토리지 디바이스(1014)를 삽입한 클라이언트(1001)에서 이용함으로써, 서버(10000)는, 하나의 개체의 내부에 복수의 유사한 기능을 갖는 서버를 갖는 특징으로부터, 관리자의 서버(10032, 10042, …, 10052)의 관리 공수를 삭감할 수 있다. 또한, 이용자가 제어 장치(10001)를 이용함으로써 서버의 전원 관리 등을 용이하게 행할 수 있기 때문에, 이용자의 사용 편리성이 향상된다.

<104> (제4 실시예)

<105> 도 1, 도 15, 도 16을 이용하여, 본 발명에 따른 시큐어 리모트 액세스 시스템의 제4 실시예를 설명한다. 본 실시예는, 시큐어 리모트 액세스 시스템을 이용하는 이용자가, 많은 사람들이 사용하는 공중의 클라이언트 기기를 통하여 업무를 수행하는 경우에 유효하다.

<106> 일반적으로, 공중의 클라이언트 기기에는, 임의의 개인 혹은 복수의 이용자가 사용하기 위한 애플리케이션이나 개인적인 설정 정보 등이 보존되어 있다. 본 실시예에서는 이들 애플리케이션이나 개인 설정 정보를 클라이언트 기기(1001) 내부의 스토리지(3002)에 인스톨이나 저장을 하지 않도록 하는 시큐어 리모트 액세스 시스템을 제시한다. 또한, 이용자의 조작량을 경감함으로써 편리성이 높은 시큐어 리모트 액세스 시스템을 제시한다.

<107> 도 15는 본 발명의 제4 실시예에서의 스토리지 디바이스(1014)의 상세 내용을 도시한 블록 구성도이다. 본 실시예에서는, 제1 실시예에서의 스토리지 디바이스(1014) 내부의 스토리지(1017) 내에, 새롭게 부트 프로그램(15001)과 OS 프로그램(15002)을 추가한다. 부트 프로그램(15001)은, 클라이언트(1001)가 기동될 때에, 그 BIOS(Basic Input/Output System)에 의해서 최초에 실행되는 프로그램으로서, 클라이언트(1001)용 OS를 기동시키는 역할을 갖는다. OS 프로그램(15002)은, 상기 부트 프로그램(15001)에 의해서 스토리지 디바이스(1014)로부터 클라이언트(1001) 내부의 메모리(3001) 상에 판독되어 기동되는 클라이언트(1001)용 OS의 프로그램이다.

<108> 이용자가 사용하는 서버(1000)와 클라이언트(1001, 1002)는 제1 실시예에서 설명한 것과 마찬가지이다.

<109> 도 16은, 이용자가 클라이언트(1001)에 도 15에 도시한 스토리지 디바이스(1014)를 삽입하여 서버(1000)를 이용할 때의 이용자, 스토리지 디바이스(1014), 클라이언트(1001), 서버(1000) 사이에서 행해지는 통신의 상세 내용을 도시한 도면이다. 이용자는 클라이언트(1001)를 기동하기까지 이용자의 인증 정보나 클라이언트(1001)를 동작시키기 위한 부트 프로그램, OS 프로그램, 애플리케이션 등이 보존된 스토리지 디바이스(1014)를 클라이언트(1001)의 리더 라이터(1012)에 접속해 놓을 필요가 있다. 또한, 클라이언트(1001)의 BIOS는, 리더 라이터(1012)를 통해서 부트 프로그램을 검출하는 것이, 스토리지(3002)를 통해서 검출하는 것에 우선하도록 미리 설정되어 있을 필요가 있다. 제1 실시예와의 차이는, 이용자가 클라이언트(1001)를 이용한 적이 없는 경우에서도, 이용자는 디바이스 드라이버(2014)나 디바이스 관리 툴(2013)이나 원격 단말기용 애플리케이션(2017)과 같은 서버(1000)를 조작하기 위해 필요한 정보 혹은 애플리케이션을 클라이언트(1001)의 스토리지(3002)에 인스톨할 필요가 없다는 것이다.

<110> 이용자는, 우선, 시퀀스 16001에 나타낸 바와 같이, 클라이언트(1001)의 전원을 투입한다. 이에 의하여, 클라이언트(1001)의 BIOS가 기동하고(16002), 스토리지 디바이스(1014)에 부트 프로그램(15001)을 요구한다(16003). 스토리지 디바이스(1014)는 이에 응하여 부트 프로그램(15001)을 송신한다(16004). 클라이언트(1001)의 BIOS는 부트 프로그램(15001)을 실행해서 부팅 처리를 개시한다(16005). 부팅 처리 중에는, 부트 프로그램(15001)에 의해서, 스토리지 디바이스(1014)에 OS 프로그램(15002)을 요구한다(16006). 스토리지 디바이

스(1014)는 이에 응하여 OS 프로그램(15002)을 송신한다(16007). OS 프로그램(15002)은 클라이언트(1001) 내부의 메모리(3001) 상에 판독되고, 기동된다(16008). 이것 이후, 스토리지 디바이스(1014)에 저장되어 있는 애플리케이션, 라이브러리, 드라이버, 관리 툴 등(2012~2019)은, 이 OS 상에 판독되고 동작하는 것이 가능하게 된다. OS 프로그램(15002)에는 OS 기동 직후 자동적으로 특정 애플리케이션을 실행하도록 기술되어 있다. 이에 따라, 클라이언트(1001)는 원격 조작 애플리케이션(2017) 및 암호화 통신로 구축용 애플리케이션(2018), 또한 그 실행에 필요한 라이브러리, 드라이버 등을 스토리지 디바이스(1014)에 요구한다(16009). 스토리지 디바이스(1014)는 이에 응하여 이들 애플리케이션을 송신한다(16010). 그리고, 클라이언트(1001)는 이들 애플리케이션을 기동한다(16011).

<111> 이들 애플리케이션 프로그램에는, 이용자가 접속하고자 하는 서버의 IP 어드레스가 미리 기술되어 있다. 클라이언트(1001)는 자동적으로 그 IP 어드레스의 서버(1000)에 동작 확인을 행한다(16012). 클라이언트(1001)는 서버(1000)의 동작을 확인할 수 없었던 경우에는, Wake on LAN과 같은 기능을 이용하여 서버(1000)의 전원 투입을 행한다. 이 경우, 서버(1000)의, 네트워크에 대한 I/F만은 항상 통전되어 있고, ID와 패스워드의 세트나 네트워크 보드의 MAC 어드레스 등, 임의의 인증 정보를 이용하여 서버(1000)의 기동이 요구된다(16013). 이에 따라, 서버(1000)는 기동된다(16014). 서버의 기동이 완료되었을 때, 클라이언트(1001)로부터 자동적으로 서버(1000)에 로그인 요구가 행해진다(16015). 서버(1000)의 리모트 기기로부터의 로그인에 대한 시큐러티 폴리시의 설정에 의하지만, 로그인 시에, 이용자의 인증에서 공개 키 인프라 스트럭처(PKI)를 이용한 인증이 필요 혹은 가능한 경우, 서버(1000)로부터 클라이언트(1001)에 인증 정보를 요구하고(16016), 클라이언트(1001)로부터 스토리지 디바이스(1014)에 증명서를 요구하여(16017), 스토리지 디바이스(1014)로부터 클라이언트(1001)에 증명서를 송신하고(16018), 클라이언트(1001)로부터 스토리지 디바이스(1014)에 서명을 요구한다(16019).

<112> 스토리지 디바이스(1014)에서 서명을 행하는 경우, 이용자의 인증이 필요하게 된다. 이용자의 인증은, 암증 번호, 패스워드, 패스프레이즈, 원타임 패스워드, 지문 정보 등의 생체 인증 정보 등에 의해 행해진다. 본 실시예에서는 암증 번호를 이용한 예를 설명한다. 스토리지 디바이스(1014)로부터의 암증 번호 요구(16020)가 행해진 후, 클라이언트(1001)로부터 이용자에게 암증 번호 요구 표시(16021)가 디스플레이(1008) 등을 이용하여 행해진다. 이용자가 암증 번호를 유저 인터페이스(1010)와 클라이언트(1001)를 통하여 스토리지 디바이스(1014)에 송신하면(16022, 16023), 스토리지 디바이스(1014) 내의 CPU(2001) 혹은 CPU(2030)에서, 서버(1000), 클라이언트(1001)로부터 송신된 정보에 대하여, 비밀 키(2040) 중 하나 혹은 몇개를 이용한 전자 서명이 작성된다(16024). 작성된 서명은 클라이언트에 송신된다(16025). 클라이언트(1001)는 증명서(2010, 2043) 등의 인증 정보와 작성된 서명의 송신을 행한다(16026).

<113> 다음으로, 서버(1000) 및 클라이언트(1001)는, 비밀 키나 공개 키 등의 서로의 키 정보와 증명서를 이용하여, 비밀 공유 키의 키 교환을 행한다(16027). 이 키 교환(16027)은 원격 조작 단말기용 애플리케이션(2017)이나 암호화 통신로 구축용 애플리케이션(2018)에 의해 행해진다. 시퀀스 16027에서 교환된 비밀 공유 키를 이용하여, 서버(1000) 및 클라이언트(1001)는 암호화 통신로를 구축하고, 양자 사이에서 통신되는 정보는 암호화된다. 암호화 통신로가 구축된 단계에서, 이용자는, 서버(1000), 클라이언트 내의 메모리(3001), 또는 스토리지 디바이스(1014) 상에 저장되어 있는 애플리케이션을 기동해서, 업무 수행을 한다(16028).

<114> 업무 종료 후, 클라이언트(1001)는 도 5의 시퀀스 4021~4025와 같이 서버(1000)와의 통신을 차단하고, 이용자는 클라이언트(1001)의 전원을 차단하여 스토리지 디바이스(1014)를 리더 라이터(1012)로부터 발취한다. 이에 의해서, 메모리(3001) 상의 정보도 휘발되기 때문에, 클라이언트(1001) 내부에는 이용자가 사용한 애플리케이션이나 개인 정보 등이 일체 남지 않는다. 이에 의해, 공중의 클라이언트를 사용한 시큐어 리모트 액세스 시스템에서, 이용자의 프라이버시가 보호된다.

<115> 또한, 클라이언트(1001) 상에서 동작하는 OS 프로그램은 이용자 자신이 스토리지 디바이스(1014) 내에 관리하고 있기 때문에, 클라이언트에 인스톨되어 있는 OS에 제3자가 은밀하게 설치한 컴퓨터 바이러스 등의 부정 프로그램에 의해 이용자의 암증 번호가 도청되는 등의 위험도 회피된다. 이에 의해, 공중의 클라이언트를 사용한 시큐어 리모트 액세스 시스템에서, 이용자의 시큐러티도 보호된다.

<116> 또한, 도 16과 같이, 이용자가 클라이언트(1001)의 이용을 개시하고 나서 업무 대상 서버(1000)에 접속하기까지의 동안의 과정은, 부트 프로그램(15001)과 OS 프로그램(15002)에 의해 자동화되어 있기 때문에, 이용자의 조작은 전원 투입(16001)과 암증 번호 송신(16022)만이다. 이에 의해, 이용자에게 있어서의 시큐어 리모트 액세스 시스템의 편리성이 향상된다.

<117> (제5 실시예)

<118> 제5 실시예는, 제4 실시예에서의 시큐어 리모트 액세스 시스템을 이용하는 이용자가, 안전하다고 신용할 수 있는 클라이언트를 통하여 업무를 수행하는 경우에 유효하다.

<119> 제4 실시예에서의 시큐어 리모트 액세스 시스템에서는, 클라이언트(1001)에서 동작하는 OS를 스토리지 디바이스(1014)로부터 판독하고 있다. 그러나, 이용자가, 공중 클라이언트 기기와 같이 안전성이 보증되지 않는 클라이언트 기기가 아니라, 자신이 소유하는 PC나 렌탈 오피스나 출장처의 관리된 오피스의 PC와 같이 안전하다고 신용할 수 있는 클라이언트를 사용하는 경우에는, OS를 스토리지 디바이스(1014)로부터 판독하지 않고서, 클라이언트 내에 인스톨되어 있는 OS를 이용하여도 된다.

<120> 이 때문에, 본 실시예의 리더 라이터(1012)는 기동 모드를 선택하는 기능을 갖는다. 구체적으로는, 도 17a와 같이, 기계적인 스위치를 탑재하고 있다. 이 스위치는, 제4 실시예에서의 부트 프로그램(15001)을 스토리지 디바이스(1014)로부터 클라이언트(1001)에 송신 가능하게 하거나, 불가능하게 하는 것을 절환할 수 있다. 이 스위치로 부트 프로그램(15001)을 송신 가능하게 하면, 시큐어 리모트 액세스 시스템은 도 16과 같이(즉, 제4 실시예와 같이) 동작한다.

<121> 한편, 부트 프로그램(15001)을 송신 불가능하게 하면, OS 프로그램(15002)이 아니라, 클라이언트 내에 인스톨되어 있는 OS가 기동하기 때문에, 시큐어 리모트 액세스 시스템은 도 5와 같이(즉, 제1 실시예와 같이) 동작한다. 도 17a는 그 처리를 도시한 도면이다. 이용자는 스위치(17000)로 부트 프로그램(15001)을 송신할지의 여부를 선택한다. 부트 프로그램을 송신하지 않는 것을 선택한 경우, 스토리지 디바이스(1014)로부터는, 클라이언트 기기에 더미 데이터(17001)가 송신된다. 더미 데이터(17001)가 클라이언트(1001)의 메모리(3001) 상에 로드되면, BIOS는 스토리지 디바이스(1014)를 통한 OS 기동에 실패하기 때문에, 그 대신에, 스토리지(3002) 내의 OS를 기동한다.

<122> 또한, 해당 스위치 등의 절환 수단을 이용하여, 기억 매체측(리더 라이터(1012)도 포함함)으로부터 OS 프로그램(15002)에의 송신 가부를 선택하여도 된다. 단, 이 경우, 부트 프로그램은 기억 매체측으로부터 클라이언트 기기로 보내어져 있다. 해당 절환 수단을 조작하여, OS 프로그램을 보내지 않는 설정으로 한 경우, 기억 매체측으로부터 클라이언트 기기로는 더미 데이터가 송신된다. 더미 데이터를 수신한 부트 프로그램은, 부트 프로그램에 미리 설정된 OS 프로그램의 판독처의 기기로부터 OS 프로그램을 판독하게 된다. 이 경우, OS 프로그램의 판독처의 기기로서는, 클라이언트(1001) 내의 스토리지(3002)이어도, 네트워크 상의 계산기 상의 스토리지이어도 된다.

<123> 또한, 도 17a, 도 17b에서, 기억 매체측으로부터의 부팅 프로그램의 송신이 거부된 경우이고, 또한, 클라이언트 기기측의 부팅 프로그램을 로드한 경우에도, 상술한 바와 마찬가지로, 해당 부팅 프로그램의 내용에 따라, 자신의 기기 혹은 다른 기기의 기억 장치로부터 OS 프로그램을 판독하는 것이 가능하다.

<124> 이러한 기동 모드를 선택하기 위한 기계적인 스위치는 스토리지 디바이스(1014)에 탑재하여도 된다. 일반적으로, PC용 디스크 디바이스에서, 부트 프로그램이 저장되어 있는 영역은 최초의 논리 섹터 어드레스로 나타내어지는 영역이다. 이 스위치로, 그 영역의 데이터의 판독을 허가할지의 여부를 절환함으로써, 부트 프로그램(15001)의 송신을 제어할 수 있다. 결과적으로, 이 스위치로 기동 모드를 선택할 수 있다. 도 17b는 그 처리를 도시한 도면이다. 스위치(17002)로, 부트 프로그램(15001)을 송신할지, 더미 데이터(17003)를 송신할지를 선택한다. 더미 데이터(17003)가 클라이언트(1001)의 메모리(3001) 상에 로드되면, BIOS는 스토리지 디바이스(1014)를 통한 OS 기동에 실패하기 때문에, 그 대신에, 스토리지(3002) 내의 OS를 기동한다.

<125> 기동 모드를 선택하는 또 하나의 방식으로서는, 부팅 프로그램(15001)이 클라이언트(1001)를 구성하는 여러 가지 디바이스를 조사함으로써, 그것이 안전한 단말기라고 신용할 수 있는지의 여부를 판별하는 방법이다. 도 17c는 그 처리를 도시한 도면이다. 메모리(3001) 상에 로드된 부트 프로그램(15001)이 클라이언트(1001)를 신용할 수 없는 것이라고 판단하였다면, OS 프로그램(15002)을 메모리(3001) 상에 로드해서 기동한다. 신용할 수 있는 것이라고 판단하였다면, 스토리지(3002) 내의 OS를 기동한다. 또한, 클라이언트(1001) 내의 디바이스를 조사할 때에, 스토리지 디바이스(1014) 내의 내탬퍼 디바이스(1016)를 이용하여 디바이스 인증 처리를 실행하면, 더욱 신뢰성의 확증이 얻어진다. 이 경우, 미리 내탬퍼 디바이스(1016) 내의 스토리지(2032) 내에 디바이스 인증 처리 프로그램이나 디바이스 인증 처리에 필요한 키나 증명서 등을 저장해 놓고, 부트 프로그램(15001)으로부터의 지시에 따라 스토리지 디바이스(1014) 내의 CPU(2030)가 디바이스 인증 처리를 실시하는 것이 바람직하다. 부트 프로그램(15001)이 클라이언트(1001)를 구성하는 여러 가지 디바이스를 조사하는 방법은, 예를 들면, 부트 프로그램(15001)이 클라이언트(1001) 내에 있거나 클라이언트(1001)에 접속되어 있는 CPU나 메모리, 스토리지 디바이스, 네트워크 카드 등에 할당된 제조 번호나 MAC 어드레스와 같이, 번호와 부품에 일대일

로 붙여진 번호나 증명서를 조사나 검증하는 것이다. 이 번호나 증명서는 각 CPU나 메모리, 스토리지 디바이스, 네트워크 카드의 제조자나 클라이언트나 부품의 제조자나 관리자 등이 번호 부여를 행한다.

<126> 도 17c에서 기동 모드를 선택하는 또 하나의 방법으로서는, 스토리지(3002) 내의 OS가 암호화나 패스워드 로크가 걸린 상태인지의 여부를 조사하고 나서, OS 프로그램(15002)을 메모리(3001) 상에 로드하여 기동하도록 하여도 된다. 이 경우, 상술한 디바이스 인증은 기억 매체측의 CPU(2030)가 행하고, 스토리지(3002) 내의 OS가 암호화나 패스워드 로크가 걸린 상태인지의 여부의 조사는 클라이언트 기기측의 CPU(3000)가 행하게 된다.

<127> 도 18은 도 17c를 이용하여 설명한 제5 실시예의 OS의 기동을 행할 때의 동작을 설명하기 위한 플로우차트이다.

<128> 부트 프로그램의 기동 후(18000), 상술한 방법에 의해, 클라이언트(1001)에 기억 매체로부터 로드된 부트 프로그램(15001)이, 디바이스 인증에 필요한 정보를 모아 CPU(2030)에 송신하고, 해당 CPU(2030)에서 디바이스 인증이 성공하였는지의 여부가 판정된다(18001).

<129> 판정 결과가 인증 성공("예")이었던 경우, 스토리지(3002)가 패스워드 로크 등의 로크 기능이나 암호화 기능에 의해서 패스워드 등의 정보의 입력 없음에는 내부에 저장되어 있는 OS 등의 데이터를 판독할 수 없게 되어 있는지의 여부가 판정된다(18002).

<130> 다음으로, 스토리지 디바이스(1014)로부터 인증 정보가 취득될 수 있을지가 판정된다(18003). 18003에서의 판정이 실패한 경우("아니오"), 이용자로부터 로크나 암호화를 해제하는 정보의 입력을 촉구하도록 화면 표시하고, 입력을 CPU(3000) 및 스토리지(3002)에 송신한다(18004). 18003의 판정에 성공("예")한 경우 혹은 18004의 동작을 종료한 경우, 스토리지(3002)는 수취한 정보를 이용하여, 예를 들면 패스워드의 비교 등, 내부에 저장되어 있는 정보에 수취한 정보가 적합한지의 여부의 검사를 행한다(18005). 수취한 정보가 검사에 합격하면("예"), 이용자는 스토리지(3002)의 정당한 이용권을 가진 것이 증명되므로, 스토리지(3002) 내부에 저장되어 있는 OS 프로그램(15002)이나 그 밖의 데이터가 이용 가능하게 된다. 따라서, 스토리지 디바이스(3002)를 이용하여 OS의 기동이 행해지고(18006), OS의 기동은 종료한다(18007). 18002의 판정이 실패("아니오")인 경우에는, 로크나 암호화가 되어 있지 않다는 것이기 때문에, 스토리지 디바이스(3002)를 이용하여 OS의 기동이 행해지고(18006), OS의 기동은 종료한다(18007). 18005의 판정에 실패한 ("아니오") 경우 혹은 18001의 판정에 실패한 경우("아니오"), OS 프로그램(15002)을 메모리(3001) 상에 로드하여 기동하고(18008), OS의 기동은 종료한다(18009).

<131> 또한, 도 17c에서, 인증의 판단 결과에 기초하여 OS의 판독 절환을 행하는 수단은, 스위치와 같은 기계적 수단이어도 되고, 컨트롤러와 버스의 조합과 같은 소프트웨어적 수단이어도 된다.

<132> 이상과 같이, 제5 실시예에서 설명한 스토리지 디바이스 및 리더 라이터 및 클라이언트를 이용함으로써, 클라이언트가 신뢰될 수 있는지의 여부 또는 클라이언트 내의 OS나 스토리지가 이용 가능한지의 여부 등을 판정하여, 적절하게 이용자가 이용할 부트 프로그램이나 OS 프로그램을 선택할 수 있어, 이용자의 클라이언트를 이용할 때의 안전성을 높일 수 있다. 또한, 자동적으로 기동할 OS를 선택하거나, 인증 정보를 입력시킴으로써, 이용자의 편리성을 높인 시큐어 리모트 액세스 시스템을 제공할 수 있다.

<133> 상기 설명은 실시예에 대하여 이루어졌지만, 본 발명은 이에 한정되지 않고, 본 발명의 정신과 이하의 특허청구범위의 범위 내에서 다양한 변경 및 수정을 할 수 있다는 것은 당업자에게 분명하다.

도면의 간단한 설명

<134> 도 1은 본 발명의 제1 실시예의 시큐어 리모트 액세스 시스템을 설명하기 위한 블록 구성도.

<135> 도 2는 본 발명의 제1 실시예의 스토리지 디바이스를 설명하기 위한 블록 구성도.

<136> 도 3은 본 발명의 제1 실시예의 인증 정보의 카피의 구성을 도시하는 도면.

<137> 도 4는 본 발명의 제1 실시예의 클라이언트의 상세 내용을 도시한 블록 구성도.

<138> 도 5는 본 발명의 제1 실시예의 이용자, 스토리지 디바이스, 클라이언트, 서버 사이에서 행해지는 통신의 상세 내용을 도시한 도면.

<139> 도 6은 본 발명의 제1 실시예의 관리자가 행하는 스토리지 디바이스의 초기화 조작을 설명한 도면.

<140> 도 7은 본 발명의 제2 실시예의 리모트 액세스 시스템을 도시하는 도면.

<141> 도 8은 본 발명의 제2 실시예의 이용자, 관리자, 스토리지 디바이스, 클라이언트, 게이트웨이, 서버 사이에서 행해지는 통신의 상세 내용을 도시한 도면.

<142> 도 9는 본 발명의 제2 실시예의 리모트 액세스 시스템의 네트워크 구성을 도시한 블록도.

<143> 도 10은 본 발명의 제3 실시예를 나타내는 리모트 액세스 시스템을 도시하는 도면.

<144> 도 11은 본 발명의 제1 실시예의 소프트웨어 구성을 도시하는 도면.

<145> 도 12는 본 발명의 제1 실시예의 애플리케이션으로부터 일시 기억 영역을 이용할 때의 처리 방법을 도시하는 플로우차트.

<146> 도 13은 본 발명의 제1 실시예의 드라이버에서의 폭주 제어를 행할 때의 처리 방법을 도시하는 플로우차트.

<147> 도 14는 본 발명의 제1 실시예의 드라이버에서의 폭주 제어를 도시하는 타임차트.

<148> 도 15는 본 발명의 제4 실시예의 스토리지 디바이스를 설명하기 위한 블록 구성도.

<149> 도 16은 본 발명의 제4 실시예의 이용자, 스토리지 디바이스, 클라이언트, 서버 사이에서 행해지는 통신의 상세 내용을 도시한 도면.

<150> 도 17a는 본 발명의 제5 실시예의 스토리지 디바이스, 리더 라이터, 클라이언트 사이에서 행해지는 처리를 도시한 도면.

<151> 도 17b는 본 발명의 제5 실시예의 스토리지 디바이스, 리더 라이터, 클라이언트 사이에서 행해지는 처리를 도시한 도면.

<152> 도 17c는 본 발명의 제5 실시예의 스토리지 디바이스, 리더 라이터, 클라이언트 사이에서 행해지는 처리를 도시한 도면.

<153> 도 18은 본 발명의 제5 실시예의 OS의 기동을 행할 때의 동작을 설명하기 위한 플로우차트.

<154> <도면의 주요 부분에 대한 부호의 설명>

<155> 1000: 서버

<156> 1001, 1002: 클라이언트

<157> 1003, 1004, 1005: 네트워크 케이블

<158> 1006: 네트워크

<159> 1007, 1008, 1009: 디스플레이

<160> 1010, 1011: 유저 인터페이스

<161> 1012, 1013: 리더 라이터

<162> 1014: 스토리지 디바이스

<163> 2000: 단자

<164> 1015: 컨트롤러

<165> 1016: 내탬퍼 디바이스

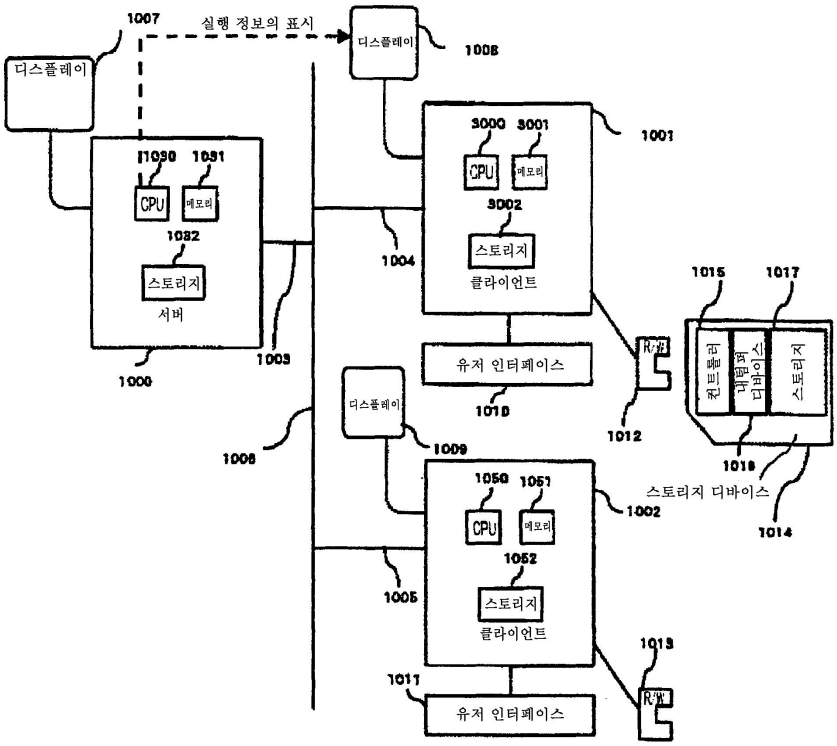
<166> 1017, 1032, 1052, 3002: 스토리지

<167> 1030, 1050, 3000, : CPU

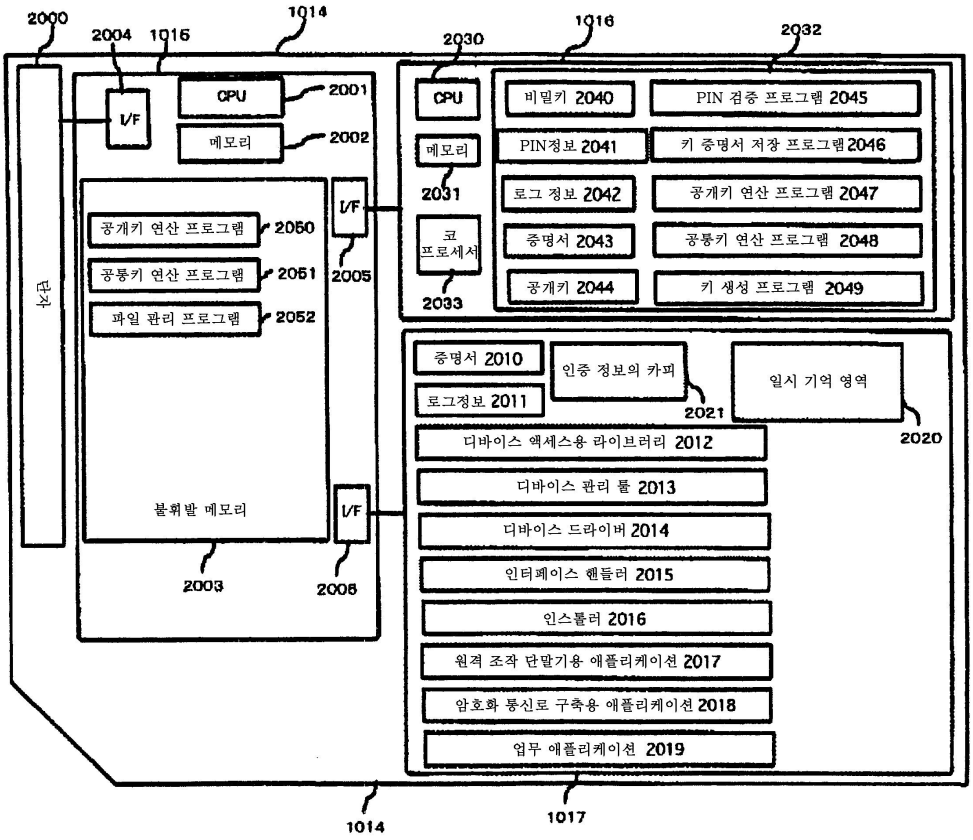
<168> 1031, 1051, 3001: 메모리

도면

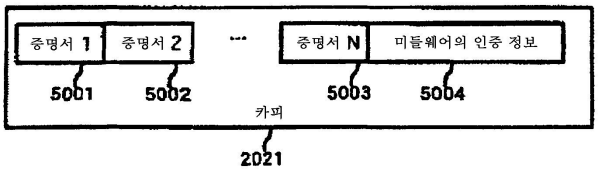
도면1


1007
실행 정보의 표시
디스플레이
디스플레이
1008
3000
3001
CPU
메모리
1001
3002
스토리지
클라이언트
1004
1015
1017
1050
1051
CPU
메모리
1032
스토리지
서버
1003
1000
유저 인터페이스
1010
1012
컨트롤러
네트워크 인터페이스
스토리지
1018
스토리지 디바이스
1014
디스플레이
1009
1008
1050
1051
CPU
메모리
1002
1052
스토리지
클라이언트
1005
1013
1011
유저 인터페이스

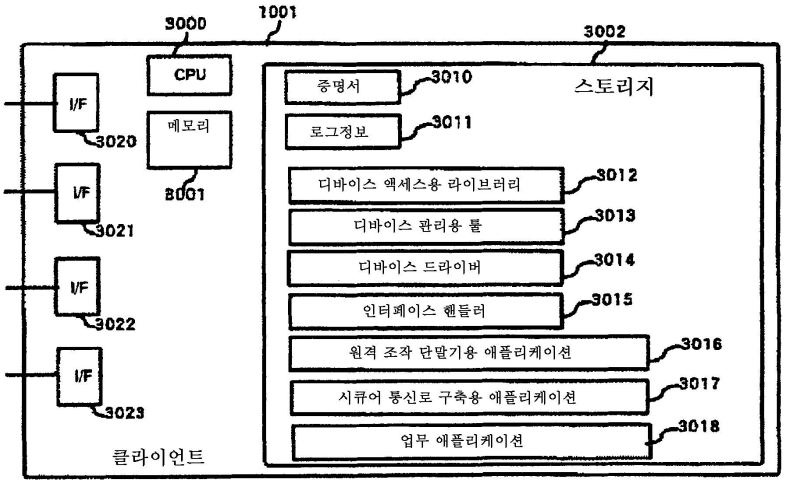
도면2


2000
2004
1015
1014
2030
1016
2032
CPU
2001
메모리
2002
I/F
공개키 연산 프로그램
2050
공통키 연산 프로그램
2051
파일 관리 프로그램
2052
I/F
2005
불휘발 메모리
2003
I/F
2006
본체
CPU
메모리
2031
코 프로세서
2033
비밀키 2040
PIN 검증 프로그램 2045
PIN정보 2041
키 증명서 저장 프로그램2046
로그 정보 2042
공개키 연산 프로그램 2047
증명서 2043
공통키 연산 프로그램 2048
공개키 2044
키 생성 프로그램 2049
증명서 2010
인증 정보의 카피
2021
일시 기억 영역
2020
로그정보 2011
디바이스 액세스용 라이브러리 2012
디바이스 관리 툴 2013
디바이스 드라이버 2014
인터페이스 핸들러 2015
인스톨러 2016
원격 조작 단말기용 애플리케이션 2017
암호화 통신로 구축용 애플리케이션 2018
업무 애플리케이션 2019
1014
1017

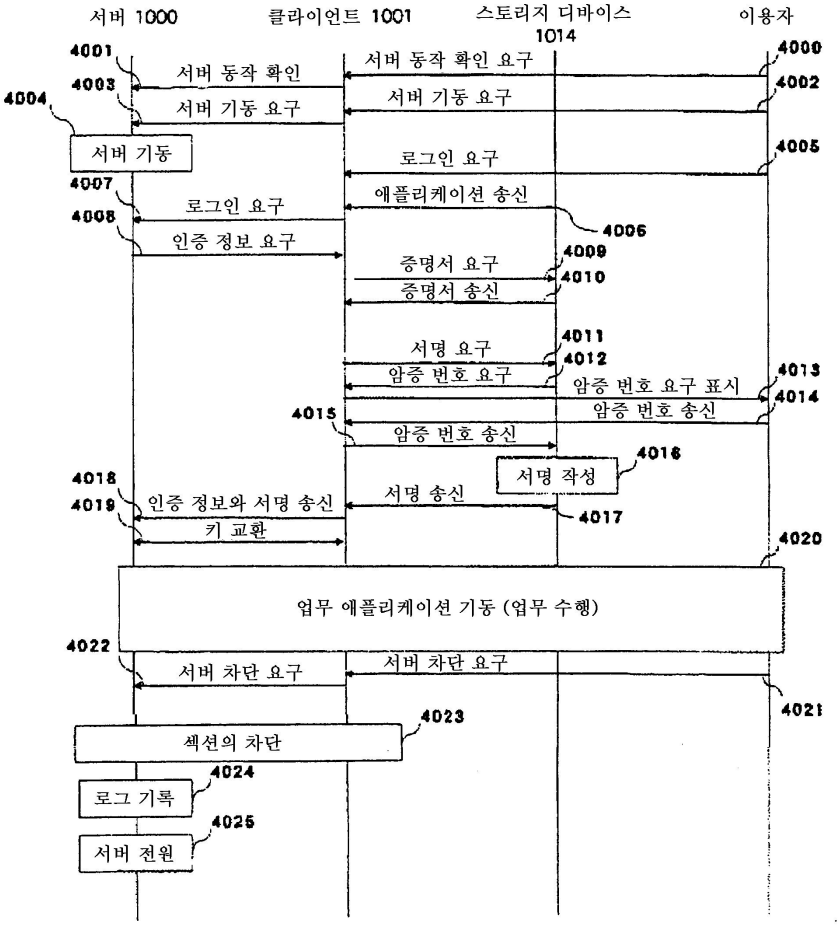
도면3


증명서 1
증명서 2
...
증명서 N
미들웨어의 인증 정보
5001
5002
5003
5004
카피
2021

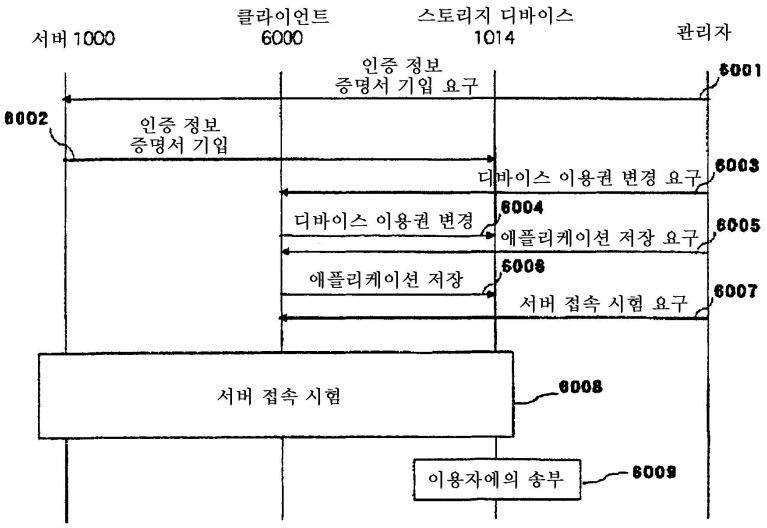
도면4


3000
1001
3002
CPU
메모리
8001
I/F
3020
I/F
3021
I/F
3022
I/F
3023
클라이언트
증명서
3010
스토리지
로그정보
3011
디바이스 액세스용 라이브러리
3012
디바이스 관리용 툴
3013
디바이스 드라이버
3014
인터페이스 핸들러
3015
원격 조작 단말기용 애플리케이션
3016
시큐어 통신로 구축용 애플리케이션
3017
업무 애플리케이션
3018

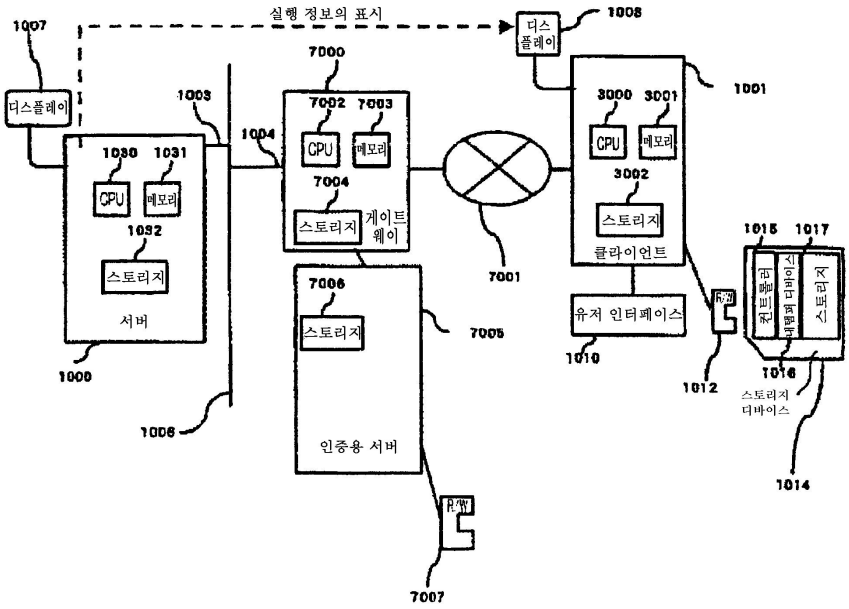
도면5


서버 1000
클라이언트 1001
스토리지 디바이스
1014
이용자
4001
서버 동작 확인
서버 동작 확인 요구
4000
4003
서버 기동 요구
서버 기동 요구
4002
4004
서버 기동
로그인 요구
4005
4007
로그인 요구
애플리케이션 송신
4006
4008
인증 정보 요구
증명서 요구
4009
증명서 송신
4010
서명 요구
4011
암증 번호 요구
4012
암증 번호 요구 표시
4013
암증 번호 송신
4014
4015
암증 번호 송신
서명 작성
4016
4018
인증 정보와 서명 송신
서명 송신
4019
키 교환
4017
4020
업무 애플리케이션 기동 (업무 수행)
4022
서버 차단 요구
서버 차단 요구
4021
섹션의 차단
4023
4024
로그 기록
4025
서버 전원

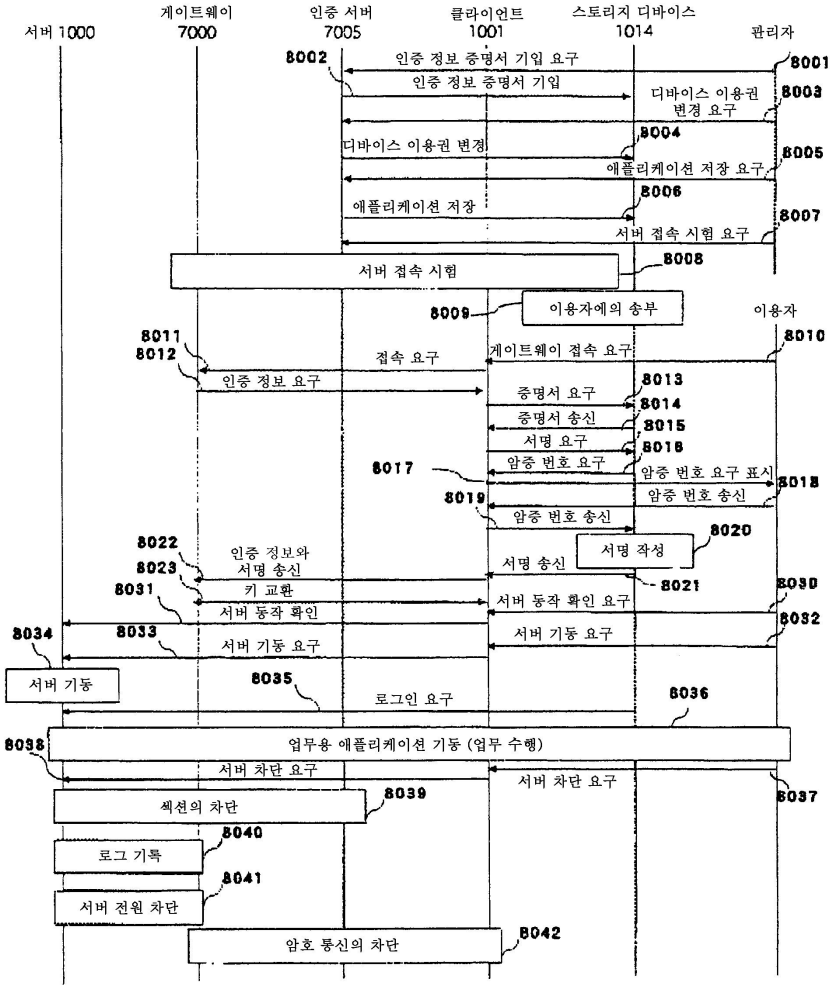
도면6


서버 1000
클라이언트 6000
스토리지 디바이스 1014
관리자
인증 정보 증명서 기입 요구
6001
6002
인증 정보 증명서 기입
디바이스 이용권 변경 요구
6003
디바이스 이용권 변경
6004
애플리케이션 저장 요구
6005
애플리케이션 저장
6006
서버 접속 시험 요구
6007
서버 접속 시험
6008
이용자에의 송부
6009

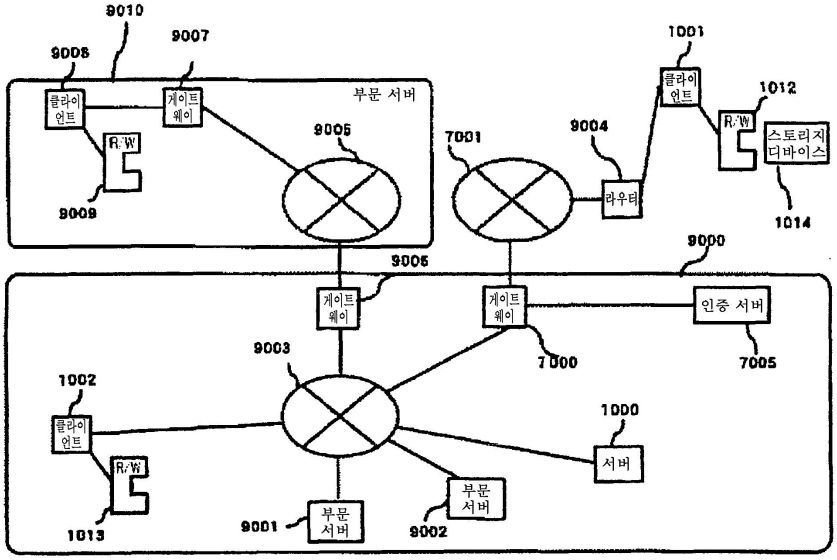
도면7


실행 정보의 표시
1007
디스플레이
1008
디스플레이
7000
1003
1004
7002
7003
CPU
메모리
7004
스토리지
게이트웨이
1001
3000
3001
CPU
메모리
3002
스토리지
클라이언트
1030
1031
CPU
메모리
1032
스토리지
서버
1000
7001
7006
스토리지
7005
인증용 서버
1006
유저 인터페이스
1010
1012
1015
1017
시큐리티 관리 프로그램
스토리지
1016
스토리지 디바이스
1014
7007

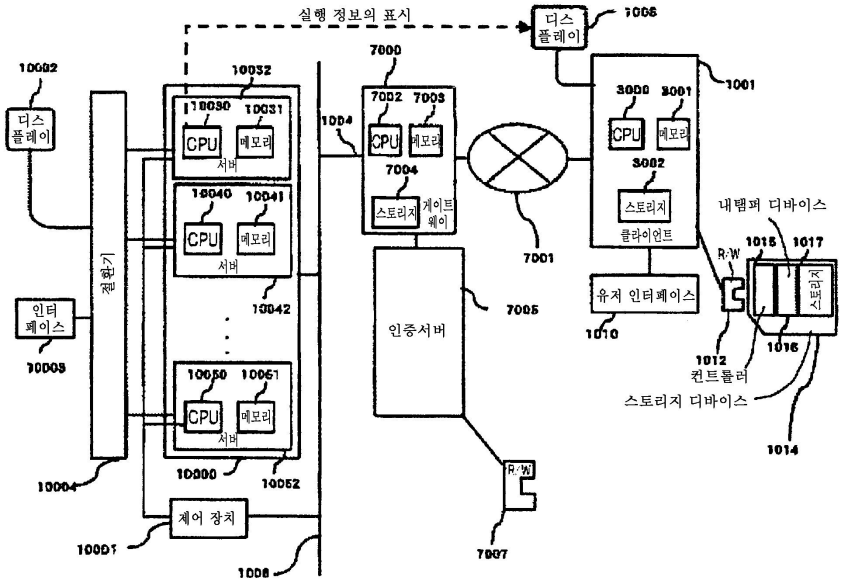
도면8


서버 1000
게이트웨이 7000
인증 서버 7005
클라이언트 1001
스토리지 디바이스 1014
관리자
이용자
8001 인증 정보 증명서 기입 요구
8002 인증 정보 증명서 기입
8003 디바이스 이용권 변경 요구
8004 디바이스 이용권 변경
8005 애플리케이션 저장 요구
8006 애플리케이션 저장
8007 서버 접속 시험 요구
8008 서버 접속 시험
8009 이용자에의 송부
8010
8011 접속 요구
8012 게이트웨이 접속 요구
인증 정보 요구
8013 증명서 요구
8014 증명서 송신
8015 서명 요구
8016 암증 번호 요구
8017 암증 번호 요구 표시
8018 암증 번호 송신
8019 암증 번호 송신
8020 서명 작성
8021 서명 송신
8022 인증 정보와 서명 송신
8023 키 교환
8030 서버 동작 확인 요구
8031 서버 동작 확인
8032 서버 기동 요구
8033 서버 기동 요구
8034 서버 기동
8035 로그인 요구
8036
8037 서버 차단 요구
8038 서버 차단 요구
업무용 애플리케이션 기동 (업무 수행)
8039 섹션의 차단
8040 로그 기록
8041 서버 전원 차단
8042 암호 통신의 차단

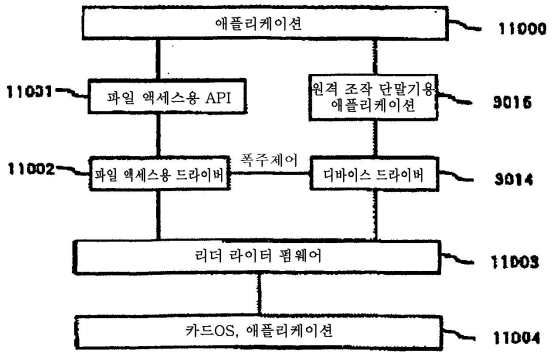
도면9


9010
9007
9008
부문 서버
클라이언트
게이트웨이
R/W
9009
9005
7001
9004
1001
클라이언트
1012
R/W
스토리지 디바이스
1014
라우터
9000
9006
게이트웨이
게이트웨이
인증 서버
7000
7005
9003
1002
클라이언트
R/W
1013
1000
서버
부문 서버
9001
부문 서버
9002

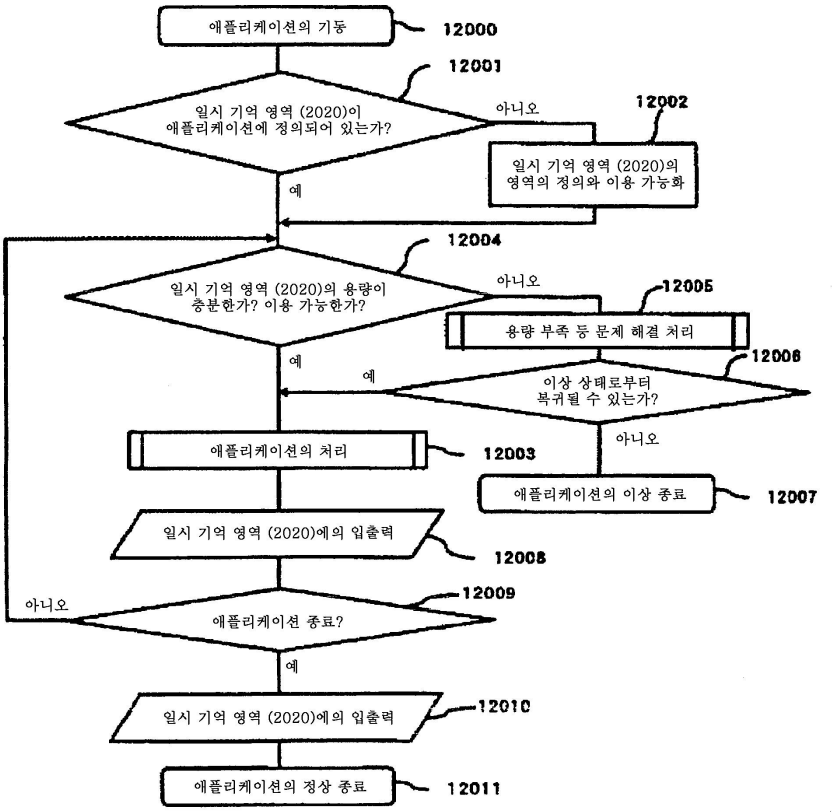
도면10


실행 정보의 표시
디스플레이
CPU
메모리
서버
게이트웨이
스토리지
클라이언트
인증서버
유저 인터페이스
내탬퍼 디바이스
R/W
컨트롤러
스토리지 디바이스
인터페이스
접속기
제어 장치

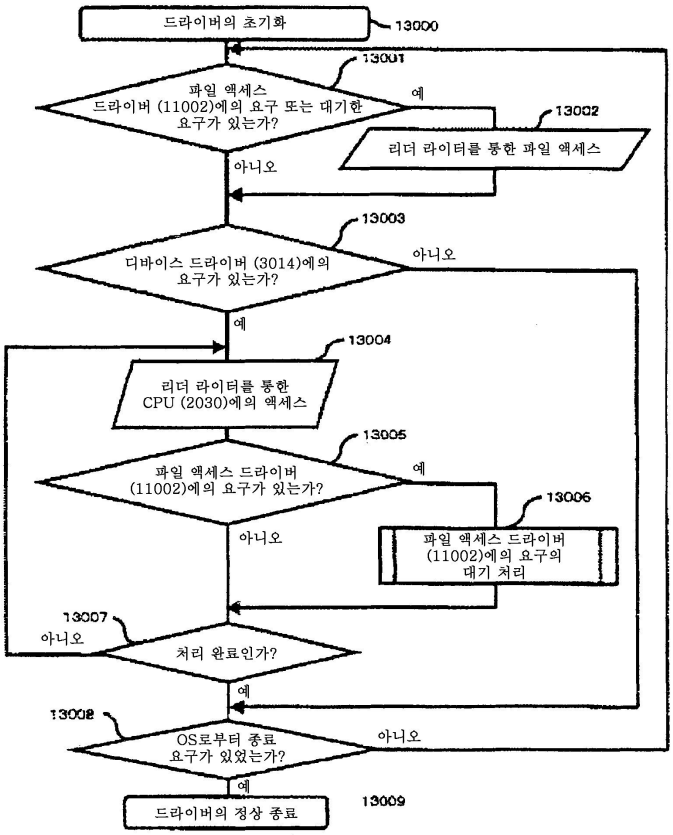
도면11


애플리케이션
11000
파일 액세스용 API
11001
원격 조작 단말기용 애플리케이션
9016
폭주제어
파일 액세스용 드라이버
11002
디바이스 드라이버
9014
리더 라이터 펌웨어
11003
카드OS, 애플리케이션
11004

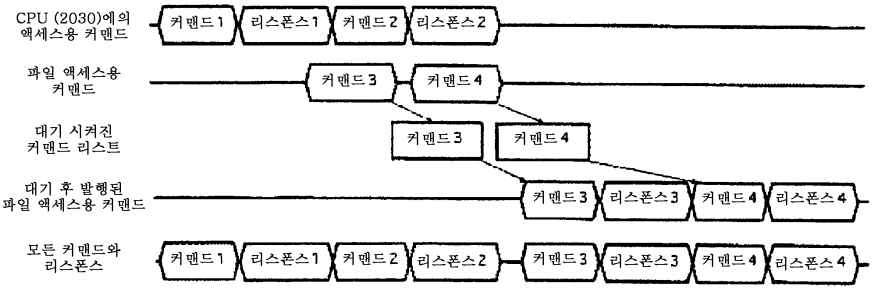
도면12


애플리케이션의 기동
12000
12001
일시 기억 영역 (2020)이 애플리케이션에 정의되어 있는가?
아니오
12002
일시 기억 영역 (2020)의 영역의 정의와 이용 가능화
예
12004
일시 기억 영역 (2020)의 용량이 충분한가? 이용 가능한가?
아니오
12005
용량 부족 등 문제 해결 처리
예
12006
이상 상태로부터 복귀될 수 있는가?
예
아니오
애플리케이션의 처리
12003
애플리케이션의 이상 종료
12007
일시 기억 영역 (2020)에의 입출력
12008
12009
애플리케이션 종료?
아니오
예
일시 기억 영역 (2020)에의 입출력
12010
애플리케이션의 정상 종료
12011

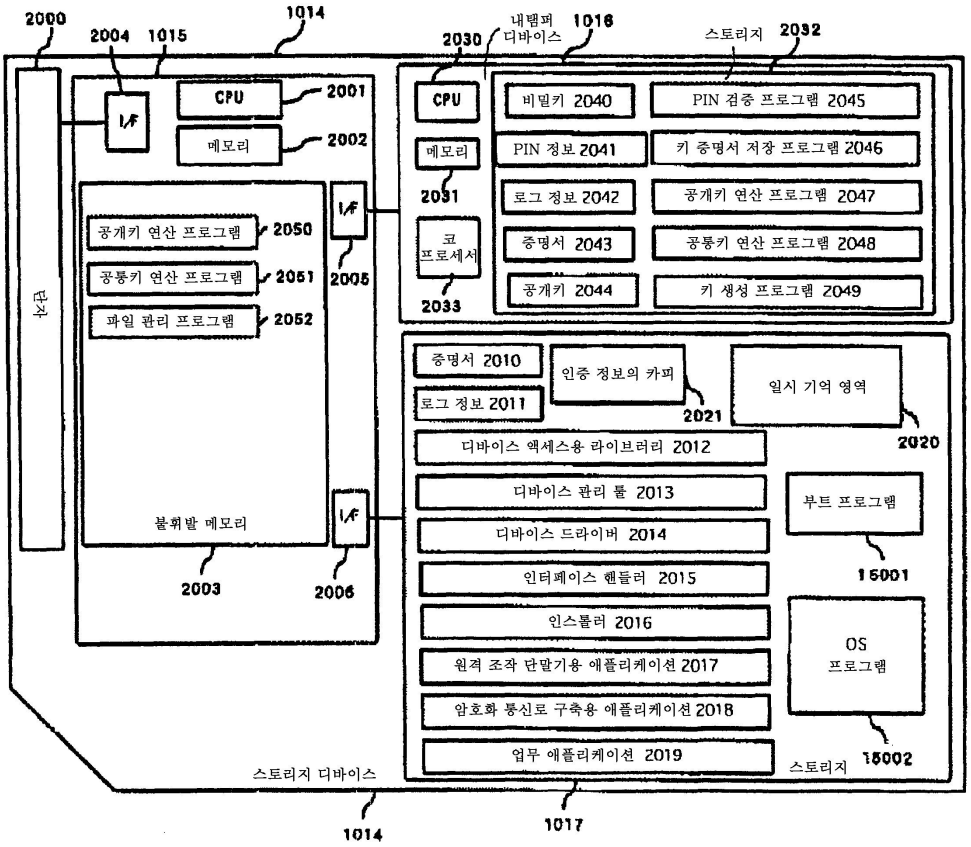
도면13


드라이버의 초기화
13000
13001
파일 액세스 드라이버 (11002)에의 요구 또는 대기한 요구가 있는가?
예
13002
리더 라이터를 통한 파일 액세스
아니오
13003
디바이스 드라이버 (3014)에의 요구가 있는가?
아니오
예
13004
리더 라이터를 통한 CPU (2030)에의 액세스
13005
파일 액세스 드라이버 (11002)에의 요구가 있는가?
예
13006
파일 액세스 드라이버 (11002)에의 요구의 대기 처리
아니오
13007
아니오
처리 완료인가?
예
13008
OS로부터 종료 요구가 있었는가?
아니오
예
드라이버의 정상 종료
13009

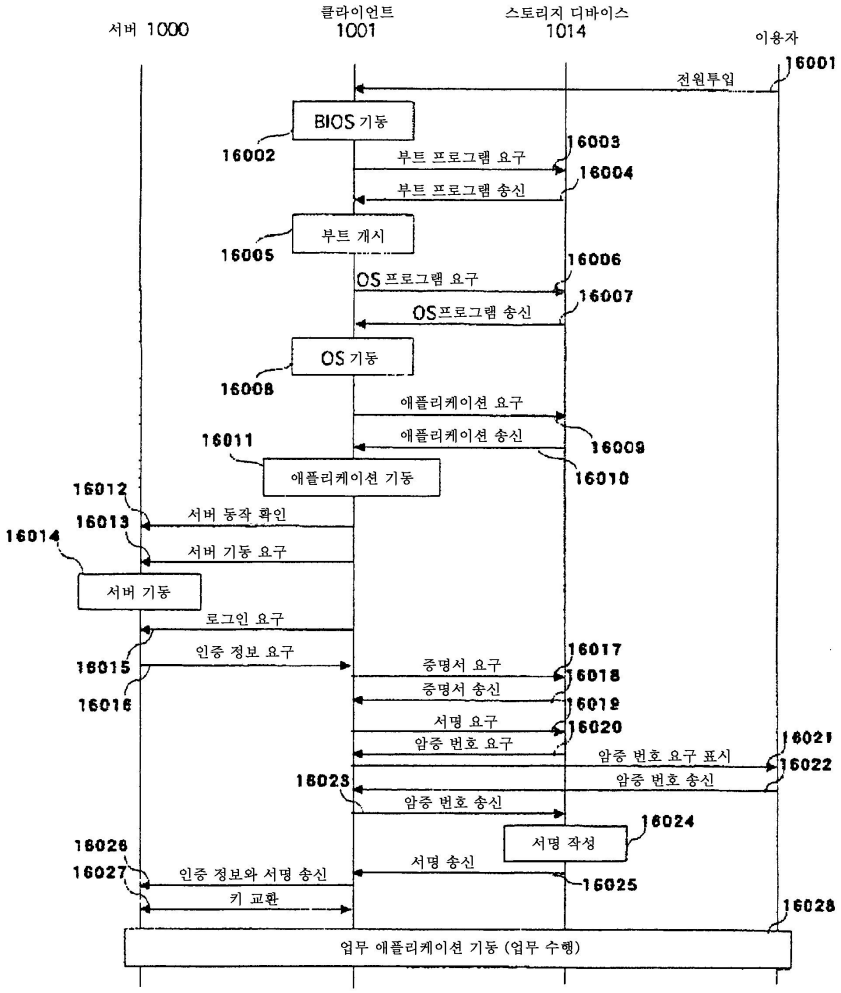
도면14


CPU (2030)에의 액세스용 커맨드
커맨드 1
리스폰스 1
커맨드 2
리스폰스 2
파일 액세스용 커맨드
커맨드 3
커맨드 4
대기 시켜진 커맨드 리스트
커맨드 3
커맨드 4
대기 후 발행된 파일 액세스용 커맨드
커맨드 3
리스폰스 3
커맨드 4
리스폰스 4
모든 커맨드와 리스폰스
커맨드 1
리스폰스 1
커맨드 2
리스폰스 2
커맨드 3
리스폰스 3
커맨드 4
리스폰스 4

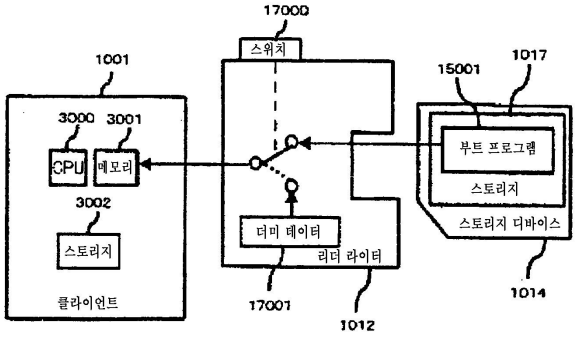
도면15


2000
2004
1015
1014
내펌퍼 디바이스
1016
2030
스토리지
2032
I/F
CPU
2001
메모리
2002
CPU
비밀키 2040
PIN 검증 프로그램 2045
메모리
PIN 정보 2041
키 증명서 저장 프로그램 2046
2031
로그 정보 2042
공개키 연산 프로그램 2047
I/F
공개키 연산 프로그램
2050
코 프로세서
증명서 2043
공통키 연산 프로그램 2048
공통키 연산 프로그램
2051
2005
공개키 2044
키 생성 프로그램 2049
2033
파일 관리 프로그램
2052
증명서 2010
인증 정보의 카피
2021
일시 기억 영역
2020
로그 정보 2011
디바이스 액세스용 라이브러리 2012
디바이스 관리 툴 2013
부트 프로그램
I/F
불휘발 메모리
디바이스 드라이버 2014
15001
인터페이스 핸들러 2015
2003
2006
인스톨러 2016
OS 프로그램
원격 조작 단말기용 애플리케이션 2017
암호화 통신로 구축용 애플리케이션 2018
15002
업무 애플리케이션 2019
스토리지
스토리지 디바이스
1014
1017

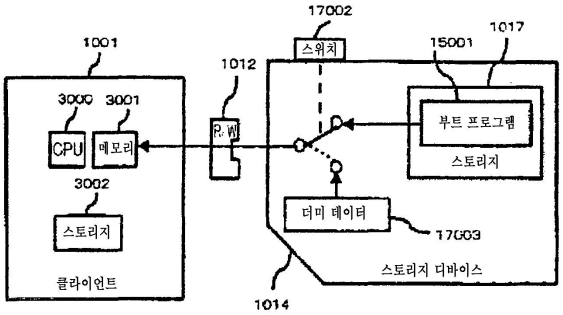
도면16


서버 1000
클라이언트 1001
스토리지 디바이스 1014
이용자
16001
전원투입
BIOS 기동
16002
16003
부트 프로그램 요구
16004
부트 프로그램 송신
부트 개시
16005
16006
OS 프로그램 요구
16007
OS프로그램 송신
OS 기동
16008
애플리케이션 요구
16009
애플리케이션 송신
16010
16011
애플리케이션 기동
16012
서버 동작 확인
16013
16014
서버 기동 요구
서버 기동
로그인 요구
인증 정보 요구
16015
16016
16017
증명서 요구
16018
증명서 송신
16019
서명 요구
16020
암증 번호 요구
16021
암증 번호 요구 표시
16022
암증 번호 송신
16023
암증 번호 송신
16024
서명 작성
16025
서명 송신
16026
16027
인증 정보와 서명 송신
키 교환
16028
업무 애플리케이션 기동 (업무 수행)

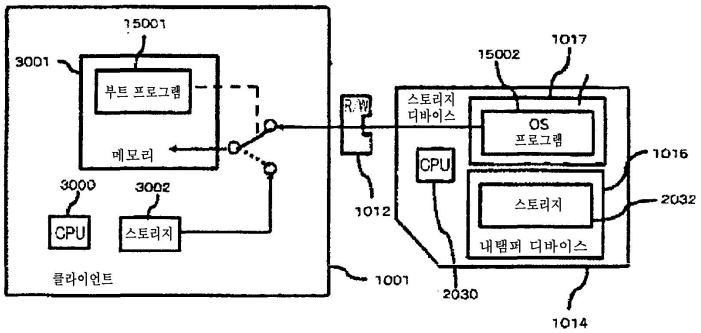
도면17a


17000
스위치
1001
3000
3001
CPU
메모리
3002
스토리지
클라이언트
더미 데이터
리더 라이터
17001
1012
15001
1017
부트 프로그램
스토리지
스토리지 디바이스
1014

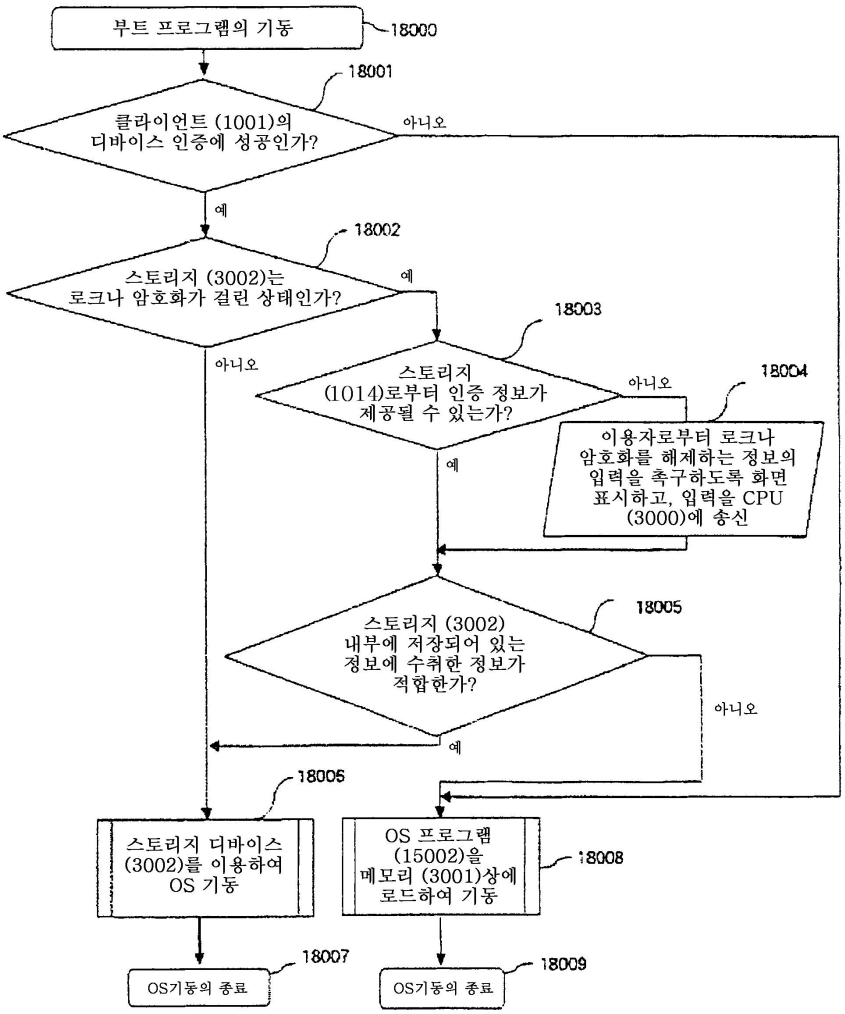
도면17b


17002
스위치
1001
1012
15001
1017
3000
3001
CPU
메모리
R/W
부트 프로그램
스토리지
3002
스토리지
더미 데이터
17003
클라이언트
스토리지 디바이스
1014

도면17c


15001
3001
부트 프로그램
메모리
3000
3002
CPU
스토리지
클라이언트
1001
R/W
1012
스토리지
디바이스
15002
1017
OS
프로그램
CPU
1016
스토리지
2032
내뱀퍼 디바이스
2030
1014

도면18


부트 프로그램의 기동
18000
18001
클라이언트 (1001)의 디바이스 인증에 성공인가?
아니오
예
18002
스토리지 (3002)는 로크나 암호화가 걸린 상태인가?
예
아니오
18003
스토리지 (1014)로부터 인증 정보가 제공될 수 있는가?
아니오
18004
이용자로부터 로크나 암호화를 해제하는 정보의 입력을 촉구하도록 화면 표시하고, 입력을 CPU (3000)에 송신
예
18005
스토리지 (3002) 내부에 저장되어 있는 정보에 수취한 정보가 적합한가?
아니오
예
18005
스토리지 디바이스 (3002)를 이용하여 OS 기동
OS 프로그램 (15002)을 메모리 (3001)상에 로드하여 기동
18008
18007
OS기동의 종료
18009
OS기동의 종료