(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06Q 99/00 (2006.01)
G06F 19/00 (2006.01)

(11) 공개번호 10-2006-0041839
(43) 공개일자 2006년05월12일

(21) 출원번호 10-2005-0011369
(22) 출원일자 2005년02월07일

(30) 우선권주장 JP-P-2004-00033722 2004년02월10일 일본(JP)

(71) 출원인 소니 가부시키가이샤
일본국 도쿄도 시나가와구 기타시나가와 6쵸메 7반 35고

(72) 발명자 오모리,무쭈히로
일본, 도쿄, 시나가와-쿠, 키타시나가와 6-쵸메, 7-35

(74) 대리인 문경진
김학수

심사청구 : 없음

(54) 정보 처리 시스템과, 정보 처리 장치 및 방법과,프로그램과, 기록 매체

요약

유저에 대해서 최적한 정보를 확실하게 제공한다.

PK(개인용 키)는 유저에 관련된 정보인 PMD(Personal Meta Data)를 기억하고 있고, 그 PMD 중 서비스 시스템에 대해서 제공하는 것이 허가된 것만을 유저의 인체와 안테나(121) 사이의 거리에 의해 제어되는 통신인 준정전계 통신에 의해서, 서비스 시스템에 송신한다. 서비스 시스템은 준정전계 통신에 의해서 PK로부터 송신되어 오는 PMD를 수신한다. 또, 수신된 PMD를 기초로 해서, 서비스 시스템은 컨텐츠 데이터베이스로부터 유저에게 제공하는 컨텐츠를 취득하고, 이 컨텐츠를 유저에게 제공한다. 본 발명은 예를 들면 공공의 장소에 설치되는 정보 제시 시스템에 적용할 수가 있다.

대표도

도 27

명세서

도면의 간단한 설명

도 1은 거리와 전계 강도의 관계를 나타내는 그래프를 도시한 도면.

도 2는 주파수와 강도 경계 거리의 관계를 나타내는 그래프를 도시한 도면.

도 3은 준정전계가 형성되는 범위를 도시하는 개략도.

도 4는 거리와 전계 강도의 관계를 나타내는 그래프를 도시한 도면.

도 5는 거리와 전계 강도의 관계를 도시하는 도면,

도 6은 수신 상태와 거리의 또 다른 관계를 나타내는 그래프를 도시한 도면.

도 7은 PK 시스템의 구성예를 도시하는 개략도.

도 8은 PK의 하드웨어 구성예를 도시하는 블록도.

도 9는 pBase의 하드웨어 구성예를 도시하는 블록도.

도 10은 PK의 기억부의 기억 내용(contents)을 도시하는 개략도.

도 11은 PK에 새로운 서비스 시스템에 대응하는 서비스 ID를 등록할 때에 행해지는 처리를 도시하는 화살표도.

도 12는 암호에 의한 인증을 이용한 위장 방지 처리를 설명하는 화살표도,

도 13은 공개키 암호 방식에 의한 인증을 이용한 위장 방지 처리를 설명하는 화살표도.

도 14는 서비스 ID 등록 처리를 설명하는 흐름도.

도 15는 서비스 ID 매칭 처리를 설명하는 흐름도.

도 16은 PK, pBase 및 서비스 시스템 간의 PMD의 수수(주고받음)를 설명하는 개략도.

도 17은 pBase와 서비스 시스템 사이에서 행해지는 처리를 설명하는 화살표도.

도 18은 pBase와 서비스 시스템(24) 사이에서 행해지는 처리를 설명하는 화살표도.

도 19는 PMD의 내용의 예를 도시하는 도면.

도 20은 PMD의 내용의 예를 도시하는 도면.

도 21은 PMD의 내용의 예를 도시하는 도면.

도 22는 PMD 갱신 처리를 설명하는 흐름도.

도 23은 정보 기기를 퍼스널라이즈하는 PK 시스템의 구성예를 도시하는 개략도.

도 24는 퍼스널라이즈 처리를 설명하는 흐름도.

도 25는 PK와 pBase 사이에서 행해지는 PMD의 동기 처리를 설명하는 화살표도.

도 26은 PMD 동기 처리를 설명하는 흐름도.

도 27은 본 발명의 일실시예로 실행되는 서비스 제공 시스템의 구성예를 도시한 개략도.

도 28은 서비스 제공 시스템을 구성하는 PK와 서비스 시스템의 처리를 설명하는 화살표도.

도 29는 서비스 제공 시스템을 구성하는 PK의 처리를 설명하는 흐름도.

도 30은 서비스 제공 시스템을 구성하는 서비스 시스템의 처리를 설명하는 흐름도.

<도면 주요 부분에 대한 부호의 설명>

21: 네트워크 22: PK

23: pBase 24: 서비스 시스템

121: 안테나 122: 출력장치

131: 유저 정보 취득 모듈 132: 최적화 엔진

133: 컨텐츠 DB 134: 유저 DB.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 정보 처리 시스템, 정보 처리 장치 및 정보 처리 방법, 프로그램과 기록 매체에 관한 것으로서, 특히 예를 들면 공공의 환경 등에 있어서 유저에 대해서 최적한 정보를 확실하게 제공할 수 있도록 하는 정보 처리 시스템, 정보 처리 장치 및 정보 처리 방법, 프로그램과 기록 매체에 관한 것이다.

근래에 있어서는, 설치된 디스플레이로 알려진 공공의 환경(장소)에 설치된 디스플레이 장치 상에 표시되는 정보를, 그 디스플레이 장치에 근접해 온 유저에 따라 퍼스널라이즈(personalize)하고, 그 유저에게 적합한 정보를 제공하는 퍼스널라이즈 시스템의 연구가 행해지고 있다.

예를 들면, 비특허 문헌1에 있어서는 퍼스널 서버의 필요성을 강조하는 한편, 퍼스널 서버로부터 개인의 정보를 읽어내어(리드해서), 공공의 환경에 있는 디스플레이에 표시함으로써, 작은 모바일 단말이 아니라 시청하고 작동시키기에 충분히 쾌적한 디스플레이 장치 상에 자신의 정보를 시청하는 것을 가능하게 하는 방법이 제안되어 있다.

또, 예를 들면 특허 문헌1에 있어서는 표시 장치와 유저 사이의 거리에 따라, 표시 장치에 표시할 화상을 확대 또는 축소하는 방법이 제안되어 있다. 단, 이 방법에서는 유저가 누구인지에 관계없이 표시 장치와 유저 사이의 거리에 따라, 표시 장치에 표시되는 화상이 확대되거나 축소될 뿐이기 때문에, 엄밀하게는 표시 장치에 표시되는 화상이 유저에 따라 퍼스널라이즈 되고 있다고는 말하기 어렵다.

현재 실시되고 있는 퍼스널라이즈 시스템에 있어서는 예를 들면, 유저에게 RF 태그(Radio Frequency Tag)를 갖게 하고, 그 RF 태그를 이용한 무선 통신(RF 통신)에 의해 유저와 디스플레이 사이의 거리를 검출함으로써, 유저가 디스플레이에 가까운 위치에 있는지 어떤지가 검출된다.

그러나, RF 태그를 이용한 무선 통신에 의한 거리의 검출은 유도 전자계의 전달 강도를 이용해서 행해지는 것이기 때문에, 유저와 디스플레이 사이의 거리를 안정적으로 정밀도 좋게 검출하는 것이 곤란했다.

즉, 유도 전자계의 전달 강도는 무선 통신이 행해지는 환경 등의 여러 가지 요인에 의해서 변화되기 때문에, 그 범위를 정밀도 좋게 검출하는 것은 곤란했다.

이 때문에, 유저가 서있는 위치를 정밀도 좋게 특정할 수 없어, 어느 정도 대략적인 서있는 위치에 따라, 디스플레이 상의 화상을 퍼스널라이즈하지 않을 수 없었다.

따라서, 유저가 그 화상을 보기 위해서가 아니라, 단지 그 디스플레이의 근처를 지나는 바와 같은 경우라도, 디스플레이 상의 화상이 그 지나가려고 하고 있던 유저에 따라 퍼스널라이즈되는 경우가 발생할 수 있었다.

또, 복수의 디스플레이를 설치하는 경우에는, 예를 들면 다른 2개 이상의 디스플레이의 표시가 어느 1명의 유저에 따라 동일한 화상으로 되지 않도록 하기 위해, 복수의 디스플레이 각각과 유저 사이의 거리를 검출하는 장치를 간격을 충분히 띄우고 설치할 필요가 있었다.

또 만일, RF 통신이 행해지는 환경 등이 변화하지 않는 경우라도, RF 태그를 이용한 RF 통신에서는 소위 멀티 패스가 형성되기 때문에, 그 멀티 패스에 기인해서 RF 태그를 가지고 있는 유저의 위치를 특정하는 메커니즘이 복잡하게 되고, 또 그 위치를 특정하기 위한 기기의 설정(캘리브레이션)도 필요해진다.

한편, 퍼스널라이즈 시스템에 있어서, 상시 디스플레이에 근접해 온 유저에 따라 그 디스플레이의 화상을 항상 퍼스널라이즈하면, 유저는 상시 감시 받고 있는 것과 같은 인상을 받을 수도 있어, 기분이 상하게 된다.

또, 퍼스널라이즈 시스템에 있어서 유저에게 적합한 정보를 제공하기 위해서는, 유저가 자신에 관한 정보를 시스템에 제공할 필요가 있다. 즉, 퍼스널라이즈 시스템에 있어서, 디스플레이 장치 상의 표시를 퍼스널라이즈하는 것에 의해, 유저에게 적합한 정보를 제공하는 장치를 서비스 시스템이라는 것으로 하면, 서비스 시스템에서는 예를 들면 유저가 소지하고 있는 RF 태그로부터 그 유저에 관한 정보의 제공을 받고, 그 정보에 따라 유저에게 적합한 정보를 선택하여 디스플레이에 표시함으로써, 그 디스플레이 장치 상의 표시를 퍼스널라이즈한다.

그러나, RF 태그에서는 그 RF 태그가 기억하고 있는 유저에 관한 정보 전부가 서비스 시스템에 제공되어 버려, 서비스 시스템에 대해서 제공되는 유저에 관한 정보를 제한하는 것이 곤란했다. 이 때문에, 역시 유저는 상시 감시 받고 있는 것과 같은 인상을 받을 수도 있어, 기분이 상하게 된다.

본 발명은 이러한 상황을 감안해서 이루어진 것으로서, 유저에 대해서 최적한 정보를 확실하게 제공하는 것 등이 가능하도록 하는 것이다.

발명이 이루고자 하는 기술적 과제

본 발명의 제 1 양상에 따라, 제 1 정보 처리 장치와 제 2 정보 처리 장치를 구비하는 정보 처리 시스템이 제공되며,

제 1 정보 처리 장치는, 사용자와 관련된 개인 관련 정보를 기억하기 위한 개인 관련 정보 기억 수단과, 개인 관련 정보중의 제2 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단과, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보를 제2 정보 처리 장치에 송신하는 송신 수단을 가지고, 제2 정보 처리 장치가 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 제1 정보 처리 장치로부터 송신되어 오는 허가 정보를 수신하는 수신 수단과, 외부에 제공할 정보중에서 유저에게 제공할 정보를 허가 정보에 따라 취득하는 정보 취득 수단과, 정보 취득 수단에 있어서 취득된 정보를 유저에게 제공하는 제공 수단을 갖는다.

본 발명의 제 2 양상에 따라, 다른 장치와 통신을 수행하기 위한 정보 처리 장치가 제공되며, 이 장치는, 유저와 관련된 개인 관련 정보를 기억하기 위한 개인 관련 정보 기억 수단과, 개인 관련 정보중의 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단과, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보를 다른 장치에 송신하는 송신 수단과, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 다른 장치가 허가 정보에 따라 송신해 오는 정보를 수신하는 수신 수단을 갖는다.

본 발명의 제 3 양상에 따라, 다른 장치와 통신을 수행하기 위한 정보 처리 방법이 제공되며, 이 방법은, 개인 관련 정보 기억 수단에 기억된 개인 관련 정보중의 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보를 다른 장치에 송신하는 송신 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보에 따라 다른 장치로부터 허가 정보를 수신하는 수신 단계를 포함한다.

본 발명의 제 4 양상에 따라, 다른 장치와 통신을 수행하는 컴퓨터가 다음의 단계, 즉 개인 정보 기억 수단에 기억된 개인 관련 정보중의 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보를 다른 장치에 송신시키는 송신 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보에 따라 다른 장치로부터 허가 정보를 수신하는 수신 단계를 수행하도록 하는 프로그램을 제공한다.

본 발명의 제 5 양상에 따라, 다른 장치와 통신을 수행하기 위해 컴퓨터에 의해 수행될 프로그램을 기록하는 기록 매체가 제공되며, 상기 프로그램은, 개인 정보 기억 유닛에 기억된 개인 관련 정보중의 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보를 다른 장치에 송신시키는 송신 단계와, 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 허가 정보에 따라 다른 장치로부터 허가 정보를 수신하는 수신 단계를 포함하는 것을 특징으로 한다.

본 발명의 제 6 양상에 따라, 다른 장치와 통신을 수행하기 위한 정보 처리 장치가 제공되며, 상기 장치는 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 다른 장치로부터 송신되어 오는 유저에 관련된 정보인 개인 관련 정보중의 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 수단과, 외부에 제공할 정보중에서 유저에게 제공할 정보를 허가 정보에 따라 취득하는 정보 취득 수단과, 정보 취득 수단에 있어서 취득된 정보를 유저에게 제공하는 제공 수단을 포함한다.

본 발명의 제 7 양상에 따라, 다른 장치와 통신을 수행하기 위한 정보 처리 방법이 제공되며, 상기 방법은, 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 다른 장치로부터 송신되어 오는 유저에 관련된 정보인 개인 관련 정보중의 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 단계와, 외부에 제공할 정보중에서 유저에게 제공할 정보를 허가 정보에 따라 취득하는 정보 취득 단계와, 정보 취득 단계에 있어서 취득된 정보를 유저에게 제공하는 제공 단계를 포함한다.

본 발명의 제 8 양상에 따라, 다른 장치와 통신을 수행하기 위해 컴퓨터로 하여금 다음의 단계, 즉 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 다른 장치로부터 송신되어 오는 유저에 관련된 정보인 개인 관련 정보중의 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신시키는 수신 단계와, 외부에 제공할 정보중에서 유저에게 제공할 정보를 허가 정보에 따라 취득하는 정보 취득 단계와, 정보 취득 단계에 있어서 취득된 정보를 유저에게 제공하는 제공 단계를 실행하게 하는 프로그램이 제공된다.

본 발명의 제 9 양상에 따라, 다른 장치와 통신을 수행하기 위해 컴퓨터에 의해 수행될 프로그램을 기록한 기록 매체가 제공되며, 상기 프로그램은, 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 다른 장치로부터 송신되어 오는 유저에 관련된 정보인 개인 관련 정보중의 컴퓨터에 대해서 제공하는 것이 허가된 허가 정보를 수신시키는 수신 단계와, 외부에 제공할 정보중에서 유저에게 제공할 정보를 허가 정보에 따라 취득하는 정보 취득 단계와, 정보 취득 단계에 있어서 취득된 정보를 유저에게 제공하는 제공 단계를 포함한다.

본 발명의 상기 및 다른 목적, 특성 및 장점이 수반하는 도면과 연계하여 취해진 다음의 설명 및 첨부된 청구항으로부터 명백해질 것이며, 이러한 도면에서 동일한 부분 또는 요소는 동일한 참조부호로 표기된다.

발명의 구성 및 작용

이하에 본 발명의 실시의 형태를 설명하지만, 청구항에 기재된 구성 요건과 발명의 실시의 형태에 있어서의 구체예의 대응 관계를 예시하면, 다음과 같이 된다. 이 기재는 청구항에 기재되어 있는 발명을 서포트하는 구체예가, 본 명세서에서 기재되어 있는 것을 확인하기 위한 것이다. 따라서, 발명의 실시의 형태중에는 기재되어 있지만, 본 발명에 대응하는 것으로서 여기에는 기재되어 있지 않은 구체예가 있다고 해도, 그것은 그 구체예가 본 발명에 대응하는 것이 아님을 의미하는 것은 아니다. 반대로, 구체예가 본 발명에 대응하는 것으로서 여기에 기재되어 있다고 해도, 그것은 그 구체예가 본 발명이외의 다른 발명에 대응하지 않는 것임을 의미하는 것도 아니다.

또, 이 기재는 전체 발명이 여기에 기술되어 있음을 의미하는 것은 아니다. 바꾸어 말하면, 이 기재는 발명의 실시의 형태에 기재되어 있는 구체예에 대응하는 발명이며, 이 출원의 청구항에는 기재되지 않은 발명의 존재, 즉 장래 분할 출원되거나 보정에 의해 추가될 발명의 존재를 부정하는 것은 아니다.

청구항 1에 기재된 정보 처리 시스템으로서,

제 1과 제 2 정보 처리 장치(예를 들면, 도 27의 PK(22)와 서비스 시스템(24))를 포함하는 정보 처리 시스템(예를 들면, 도 27의 서비스 제공 시스템)에 있어서,

상기 제1 정보 처리 장치는

유저에 관련된 정보인 개인 관련 정보를 기억하는 개인 관련 정보 기억 수단(예를 들면, 도 8의 기억부(38))과,

상기 개인 관련 정보중의 상기 제 2 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단(예를 들면, 도 30의 단계 S701의 처리)과,

상기 유저의 인체와 안테나(예를 들면, 도 27의 안테나(121)) 사이의 거리에 의해 제어되는 통신에 의해서 상기 허가 정보를 상기 제 2 정보 처리 장치에 송신하는 송신 수단(예를 들면, 도 30의 단계 S702의 처리)을 포함하고,

상기 제 2 정보 처리 장치는

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 제 1 정보 처리 장치로부터 송신되어 오는 상기 허가 정보를 수신하는 수신 수단(예를 들면, 도 29의 단계 S681의 처리)과,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 수단(예를 들면, 도 29의 단계 S683의 처리)과,

상기 정보 취득 수단에 있어서 취득된 정보를 상기 유저에게 제공하는 제공 수단(예를 들면, 도 29의 단계 S684의 처리)을 포함한다.

청구항 2에 기재된 정보 처리 장치는 다른 장치(예를 들면, 도 27의 서비스 시스템(24))와 통신을 행하는 정보 처리 장치(예를 들면, 도 27의 PK(22))에 있어서,

유저에 관련된 정보인 개인 관련 정보를 기억하는 개인 관련 정보 기억 수단(예를 들면, 도 8의 기억부(38))과,

상기 개인 관련 정보중의 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단(예를 들면, 도 30의 단계 S701의 처리)과,

상기 유저의 인체와 안테나(예를 들면, 도 27의 안테나(121)) 사이의 거리에 의해 제어되는 통신에 의해서 상기 허가 정보를 상기 다른 장치에 송신하는 송신 수단(예를 들면, 도 30의 단계 S702의 처리)과,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 다른 장치가 상기 허가 정보에 따라 송신해 오는 정보를 수신하는 수신 수단(예를 들면, 도 30의 단계 S703의 처리)을 포함한다.

청구항 3에 기재된 정보 처리 장치는 출력 수단(예를 들면, 도 30의 단계 S704의 처리)을 더 포함한다.

청구항 4에 기재된 정보 처리 장치는 상기 다른 장치와의 사이에서 인증을 행하는 인증 수단(예를 들면, 도 28의 단계 S663 내지S665의 처리)을 더 포함하고,

상기 인증이 성공한 경우에, 상기 허가 정보가 상기 다른 장치에 송신된다.

청구항 6에 기재된 정보 처리 방법은

개인 관련 정보 기억 수단에 기억되어 있는 개인 관련 정보중의 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계(예를 들면, 도 30의 단계 S701)와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 허가 정보를 상기 다른 장치에 송신하는 송신 단계(예를 들면, 도 30의 단계 S702)와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 다른 장치가 상기 허가 정보에 따라 송신해 오는 정보를 수신하는 수신 단계(예를 들면, 도 30의 단계 S703)를 포함한다.

청구항 7에 기재된 프로그램 및 청구항 8에 기재된 기록 매체에 기록되어 있는 프로그램은,

개인 관련 정보 기억 수단에 기억되어 있는 개인 관련 정보중의 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계(예를 들면, 도 30의 단계 S701)와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 허가 정보를 상기 다른 장치에 송신시키는 송신 단계(예를 들면, 도 30의 단계 S702)와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서 상기 다른 장치가 상기 허가 정보에 따라 송신해 오는 정보를 수신시키는 수신 단계(예를 들면, 도 30의 단계 S703)를 포함한다.

다른 장치{예를 들면, 도 27의 PK(22)}와 통신을 행하기 위한, 청구항 9에 기재된 정보 처리 장치{예를 들면, 도 27의 서비스 시스템(24)}는,

상기 다른 장치의 유저의 인체와 안테나(예를 들면, 도 27의 안테나(121)) 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 정보인 개인 관련 정보중의 상기 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 수단(예를 들면, 도 29의 단계 S681의 처리)과,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 수단(예를 들면, 도 29의 단계 S683의 처리)과,

상기 정보 취득 수단에 있어서 취득된 정보를 상기 유저에게 제공하는 제공 수단(예를 들면, 도 29의 단계 S684의 처리)을 포함한다.

청구항 12에 기재된 정보 처리 장치는,

상기 유저가 존재하는 위치인 유저 위치를 취득하는 유저 위치 취득 수단(예를 들면, 도 29의 단계 S682의 처리)을 더 포함하고,

상기 정보 취득 수단은 상기 유저에게 제공할 정보를 상기 유저 위치에 따라서도 취득한다.

청구항 13에 기재된 정보 처리 장치는,

상기 다른 장치와의 사이에서 인증을 행하는 인증 수단(예를 들면, 도 28의 단계 S643 내지 S645의 처리)을 더 포함하고,

상기 인증이 성공한 경우에, 상기 정보 취득 수단에 있어서 취득된 정보가 상기 유저에게 제공된다.

청구항 15에 기재된 정보 처리 방법은,

상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 정보인 개인 관련 정보중의 상기 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 단계(예를 들면, 도 29의 단계 S681)와,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 단계(예를 들면, 도 29의 단계 S683)와,

상기 정보 취득 단계에 있어서 취득된 정보를 상기 유저에게 제공하는 제공 단계(예를 들면, 도 29의 단계 S684)를 포함한다.

청구항 16에 기재된 프로그램 및 청구항 17에 기재된 기록 매체에 기록되어 있는 프로그램은,

상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 정보인 개인 관련 정보중의 상기 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신시키는 수신 단계(예를 들면, 도 29의 단계 S681)와,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 단계(예를 들면, 도 29의 단계 S683)와,

상기 정보 취득 단계에 있어서 취득된 정보를 상기 유저에게 제공하는 제공 단계(예를 들면, 도 29의 단계 S684)를 수행한다.

다음에, 본 발명의 실시예에 대해 설명한다.

본 발명의 각 실시예는 예를 들면 개인 네트워크 통신과 PK(Personal Key) 시스템을 이용할 수가 있다. 그래서, 우선, 개인 네트워크 통신과 PK 시스템에 대해 설명한다.

개인 네트워크 통신이란 인체가 개재하는 통신으로서, 인체의 근방에서 행해지는 안정적인 통신(인체 근방 통신)이다. 인체가 개재하는 개인 네트워크 통신중에는 인체와 안테나와의 거리에 의해 제어되는 통신이 있고, 그러한 통신으로서는 예를 들면 준정전계 통신이 있다.

준정전계 통신은 인체 근방에 원격 전파하지 않고 폐역에만 성립하는 물리적 성질{에버네센트성(evanescence)}을 가지는 폐쇄된 정전적인 정보 공간을 형성하는 통신이며, 이 통신에 의하면 인체가 미약한 정전기의 안테나로 되어, 인체 주위의 수센티미터 또는 수미터의 한정된 공간에서 통신하는 것이 가능해진다.

준정전계 통신의 원리는 다음과 같다.

즉, 예를 들면 전기 쌍극자(다이폴 안테나)에 전류를 흘린 경우, 그 다이폴 안테나로부터 발생되는 전계는 맥스웰 방정식에 따라, 식 (1)로 나타낼 수가 있다.

수학식 1

$$E_r = \frac{A\cos\omega t\cdot\cos\theta}{2\pi\varepsilon r^3}\cdot(1+jkr)\cdot\exp(-jkr)$$

$$E_\theta = \frac{A\cos\omega t\cdot\sin\theta}{4\pi\varepsilon r^3}\cdot(1+jkr+(jkr)^2)\cdot\exp(-jkr)$$

... (1)

식 (1)에 있어서, E_r은 반경 r방향의 전계 성분을 나타내고, E_Θ는 각도Θ방향의 전계 성분을 나타낸다. 또, cosωt는 각(角)주파수ω에서의 전하의 진동을 나타내고, t는 시각을 나타낸다. 또, A는 진동하는 2개의 전하의 전하량과, 그 2개의 전하끼리 사이의 거리로 정의되는 전계의 출력(진폭)(파워)을 나타내는 계수이다. 또, Θ는 다이폴 안테나의 중심 주위의 각도를 나타내고, r은 다이폴 안테나의 중심으로부터의 거리(단위는 [m])를 나타낸다. 또, ε는 유전율을 나타내고, k는 파수(단위는 [ℓ/m])를 나타낸다. 또, j는 그 후에 계속되는 값이 허수임을 나타낸다.

식 (1)에 의해서 나타내지는 전계 E_r과 E_Θ 각각중, 거리(반경) r에 선형으로 반비례하는 성분인 방사 전계 E_{1r}과 $E_{1\Theta}$는 식 (2)로 나타내진다.

수학식 2

$$E_{1r} = 0$$

$$E_{1\theta} = \frac{A\cos\omega t\cdot\sin\theta}{4\pi\varepsilon r^3}\cdot(jkr)^2\cdot\exp(-jkr)$$

... (2)

또, 식 (1)에 의해 나타내지는 전계 E_r과 E_Θ 각각중, 거리 r의 2승에 반비례하는 성분인 유도 전자계 E_{2r}과 $E_{2\Theta}$는 식 (3)으로 나타내진다.

수학식 3

$$E_{2r} = \frac{A\cos\omega t \cdot \cos\theta}{2\pi\varepsilon r^3} \cdot (jkr) \cdot \exp(-jkr)$$

$$E_{2\theta} = \frac{A\cos\omega t \cdot \sin\theta}{4\pi\varepsilon r^3} \cdot (jkr) \cdot \exp(-jkr)$$

... (3)

또, 식 (1)에 의해 나타내지는 전계 E_r과 E_Θ 각각중, 거리 r의 3승에 반비례하는 성분 E_{3r}과 $E_{3\Theta}$는 식 (4)로 나타내진다.

수학식 4

$$E_{3r} = \frac{A\cos\omega t \cdot \cos\theta}{2\pi\varepsilon r^3} \cdot \exp(-jkr)$$

$$E_{3\theta} = \frac{A\cos\omega t \cdot \sin\theta}{4\pi\varepsilon r^3} \cdot \exp(-jkr)$$

... (4)

식 (4)로 나타내지는 성분 E_{3r}과 $E_{3\Theta}$가 준정전계이다.

여기서, 도 1은 맥스웰 방정식을 다이폴 안테나에 적용해서 얻어지는 방사 전계 E_{1r} 및 $E_{1\Theta}$, 유도 전자계 E_{2r} 및 $E_{2\Theta}$, 준정전계 E_{3r} 및 $E_{3\Theta}$ 각각의 전계 강도와 거리 r의 관계를 도시하고 있다.

또한, 도 1에서는 주파수 f(=ω / (2π))는 1[㎒]로 하고 있다.

도 1에 있어서, 방사 전계, 유도 전자계, 준정전계 각각의 전계 강도가 동일해지는 거리인 강도 경계 거리가 존재하지만, 이 강도 경계 거리보다 먼 곳에서는 방사 전계가 지배적으로 되고, 강도 경계 거리보다 근방에서는 준정전계가 지배적으로 된다.

맥스웰 방정식에 의하면, 식 (5)를 충족시키는 r이 강도 경계 거리로 된다.

수학식 5

$$k \cdot r = 1$$

... (5)

식 (5)에 있어서의 파수 k는 광속을 c($c=3\times10^8$[m/s])로 함과 동시에, 주파수를 f(=ω / (2π))로 하면, 식 (6)으로 나타내진다.

수학식 6

$$k = \frac{2\pi f}{c}$$

... (6)

식 (5)와 식 (6)으로부터, 강도 경계 거리 r은 아래에서 식 (7)로 나타내진다.

수학식 7

$$r = \frac{c}{2\pi f}$$

... (7)

도 2에는 식 (7)에 의해 나타내지는 강도 경계 거리 r과 주파수 f의 관계를 도시하고 있다.

강도 경계 거리 r은 주파수 f에 대해서 일의적으로 구해진다.

따라서, 지금 도 3에 도시하는 바와 같이, 송신 단말 TX로부터 복수인 N개의 강도 경계 거리 r_1, r_2,…r_N을 설정하면, 그 강도 경계 거리 r_1, r_2,…r_N 각각 대해서, 식 (7)을 충족시키는 주파수 f_1, f_2,…f_N에서 각각 진동하는 N개의 준정전계(도면 중 파선으로 표시되어 있는 부분)가 지배적으로 되는 공간을 형성할 수가 있다. 단, $r_1 < r_2 < \cdots < r_N$이라고 하면, $f_1 > f_2 > \cdots > f_N$이다

여기서, 강도 경계 거리 r_n과 그 강도 경계 거리 r_n에 대해서 식 (7) 식을 충족시키는 주파수 f_n의 관계에 의해(n=1, 2,…, N), 준정전계 통신을 행하는 송신 단말 TX와 수신 단말 RX 사이의 거리를 구할 수가 있다.

즉, 예를 들면 송신 단말 TX에 있어서, 2종류의 주파수 각각에서 진동하는 2개의 전계를 동일 출력(파워)으로 형성하고, 그 전계내를 소정의 레벨 TH 이상의 전계 강도를 수신할 수 있는 수신 단말 RX가 이들 2개의 전계에서 이동한다고 한다. 이 경우, 수신 단말 RX는 송신 단말 TX가 형성한 전계내의 소정의 레벨 TH 이상의 전계 강도를 수신할 수 있는 범위(거리)에 있어서, 송신 단말 TX와 통신할 수가 있다.

도 4는 송신 장치 TX가 형성하는 2개의 전계의 주파수를 각각, 예를 들면 5[㎒]와 50[㎒]로 하고, 그 2개의 전계 각각의 방사 전계, 유도 전자계 및 준정전계의 전계 강도와 거리 r의 관계를 도시하고 있다.

도 4에서는 5[㎒]의 주파수의 전계에 대해서는, 수신 단말 RX가 수신할 수 있는 소정 레벨 TH(도 4에서는 10^{-2}으로 되어 있다) 이상의 전계 강도가 얻어지는 거리(도 4에서는 10[m]로 되어 있다) 내에 있어서, 준정전계가 지배적으로 되고 있다.

한편, 50[㎒]의 주파수의 전계에 대해서는, 수신 단말 RX가 수신할 수 있는 소정 레벨 TH 이상의 전계 강도가 얻어지는 거리중의 1[m]까지는 준정전계가 지배적으로 되고 있지만, 1[m]를 넘으면 방사 전계가 지배적으로 되고 있다.

그래서, 송신 단말 TX에 있어서, 도 4에 있어서의 5[㎒]의 주파수의 전계와 마찬가지로, 수신 단말 RX가 수신할 수 있는 소정 레벨 TH 이상의 전계 강도가 얻어지는 거리내에 있어서만 준정전계가 지배적으로 되도록 50[㎒]의 전계의 출력을 조정하면, 도 4에 도시한 전계 강도와 거리 r의 관계는 도 5에 도시하는 바와 같이 된다.

송신 단말 TX에 있어서, 상술한 바와 같이 전계의 출력을 조정함으로써, 5[㎒] 및 50[㎒]의 어느 주파수에서도 수신 단말 RX가 수신할 수 있는 소정의 레벨 TH 이상의 전계 강도의 전계내에서는, 준정전계가 지배적으로 된다.

따라서, 송신 단말 TX에 있어서, 그 송신 단말 TX(의 안테나)로부터 강도 경계 거리 r_n의 위치에서, 그 강도 경계 거리 r_n에 대해서 식 (7)을 충족시키는 주파수 f_n의 전계의 전계 강도가 수신 단말 RX가 수신할 수 있는 소정 레벨 TH로 되도록 주파수 f_n의 전계의 출력을 조정함으로써, 송신 단말 TX와 수신 단말 RX가 서로 통신 가능한 공간으로서 주파수 f_n에서 진동하는 준정전계가 지배적으로 되는 공간을 확실하게 형성할 수가 있다.

또 이 경우, 수신 단말 RX에서 수신할 수 있었던 준정전계의 주파수에 근거해서, 송신 단말 TX와 수신 단말 RX 사이의 거리를 검출할 수가 있다.

지금, 송신 단말 TX에 있어서, 주파수 f_n의 전계의 출력을 상술한 바와 같이 조정하기 위한 계수로서 출력 조정 계수 A_n을 도입하고, 식 (1)~식 (4)의 계수 A를 출력 조정 계수 A_n으로 치환한다. 이 경우, 주파수 f_n의 전계의 강도 경계 거리 r_n에 있어서의 전계 강도의 절대값 E_n은 식 (8)로 나타내진다.

수학식 8

$$E_n = \left| \frac{A_n \sin^2\theta + 4\cos^2\theta}{4\pi\varepsilon} \cdot \left(\frac{2\pi f_n}{c}\right)^3 \cdot \exp(-j) \right| \quad \cdots (8)$$

또한, 식 (8)에 있어서의 출력 조정 계수 A_n은 강도 경계 거리 r_n에 있어서 전계 강도의 절대값 E_n이 소정의 레벨 TH가 되는 값으로 하면 좋다.

준정전계의 전계 강도는 거리 r의 3승에 반비례하기 때문에, 강도 경계 거리 r_n의 범위에 있어서 주파수 f_n의 준정전계가 지배적으로 되는 공간을 방사 전계나 유도 전자계에 비해 명확하게 형성할 수가 있다.

따라서, 송신 단말 TX에 있어서, 주파수 f_n의 전계의 출력을 출력 조정 계수 A_n에 의해서 조정한 경우, 수신 단말 RX가 주파수 f_n의 준정전계의 신호를 수신할 수 있는지 어떤지에 따라서, 송신 단말 TX와 수신 단말 RX 사이의 거리를 고정밀도로 검출할 수가 있다.

즉, 예를 들면 지금 도 6에 도시하는 바와 같이, 송신 단말 TX가 상술한 바와 같이 출력을 조정한 3개의 주파수 f_1, f_2, f_3의 전계를 출력하는 것으로 하면, 수신 단말 RX가 주파수 f_1 내지 f_3의 모든 준정전계를 수신할 수 있는 경우, 송신 단말 TX와 수신 단말 RX 사이의 거리 r은 주파수 f_1에 대응하는 강도 경계 거리 r_1 이하인 것을 검출할 수가 있다.

또, 수신 단말 RX가 주파수 f_2와 f_3의 양쪽의 준정전계만을 수신할 수 있는 경우, 송신 단말 TX와 수신 단말 RX 사이의 거리 r은 주파수 f_1에 대응하는 강도 경계 거리 r_1보다 크고, 또한 주파수 f_2에 대응하는 강도 경계 거리 r_2 이하인 것을 검출할 수가 있다.

또, 수신 단말 RX가 주파수 f_3의 준정전계만을 수신할 수 있는 경우, 송신 단말 TX와 수신 단말 RX 사이의 거리 r은 주파수 f_2에 대응하는 강도 경계 거리 r_2보다 크고, 또한 주파수 f_3에 대응하는 강도 경계 거리 r_3 이하인 것을 검출할 수가 있다.

그리고, 수신 단말 RX가 주파수 f_1 내지 f_3의 어떠한 준정전계도 수신할 수 없는 경우, 송신 단말 TX와 수신 단말 RX 사이의 거리 r은 주파수 f_3에 대응하는 강도 경계 거리 r_3보다 큰 것을 검출할 수가 있다.

이상과 같은 준정전계가 지배적으로 되는 공간에 있어서, 그 전계 강도의 변화를 검출하는 것에 의해 행해지는 통신이 준정전계 통신이다.

그리고, 상술한 것으로부터, 준정전계가 지배적으로 되는 공간은 전계를 출력하는 송신 단말 TX(의 안테나)로부터 그 전계의 주파수 f_n에 대응하는 강도 경계 거리 r_n내의 공간으로서 명확하게 형성되므로, 준정전계 통신에 의하면 준정전계가 지배적으로 되는 공간에 있어서 확실하고 또한 안정되게 통신을 행할 수가 있다.

그런데, 인체가 방사 전계나 유도 전자계를 발생시키기 위해서는, 인체에 전류를 흘릴 필요가 있다. 그러나, 인체의 임피던스는 높으므로, 인체에 전류를 효율적으로 흘리는 것은 곤란하다.

한편, 일상생활에 있어서 정전기를 체감하도록 인체는 대전하기 쉽다. 그리고, 인체 표면의 대전에 의해 준정전계가 발생한다. 인체는 매우 적은 전하의 이동에 의해 정전기적으로 대전하고, 그 대전의 변화는 순간적으로 인체 표면 주위로 전해지며, 그 주위로부터 거의 등방향으로 준정전계의 등전위면이 형성된다. 그리고, 준정전계가 지배적으로 되는 공간내에서는 방사 전계나 유도 전자계의 영향이 최적화되므로, 인체는 안테나로서 효율적으로 기능한다.

이와 같이, 인체 표면에 형성되는 준정전계가 지배적으로 되는 공간에 있어서, 그 전계 강도의 변화를 검출하는 것에 의해 행해지는 통신이 인체 근방 통신으로서의 준정전계 통신이다.

따라서, 예를 들면 유저가 송신 단말 TX를 휴대한 경우, 그 유저의 인체 표면에는 송신 단말 TX가 출력하는 전계중의 준정전계가 지배적으로 되는 공간(이하, 적절히 '준정전계 공간'이라고 함)이, 그 인체 표면으로부터 준정전계의 주파수에 대응하는 강도 경계 거리의 범위에 형성된다. 그리고, 수신 단말 RX와 유저가 휴대하고 있는 송신 단말 TX 사이에서는, 수신 단말 RX의 안테나가 유저의 인체 표면에 형성된 준정전계 공간 내에 존재하는 경우에만, 즉 수신 단말 RX의 안테나가 인체 표면으로부터 강도 경계 거리의 범위에 존재하는 경우에만, 유저의 인체를 거쳐서 준정전계 통신을 행할 수가 있다.

이 때문에, 인체 근방 통신 중 하나로서의 준정전계 통신은 유저의 인체와 수신 단말 RX의 안테나와의 거리에 따라 (통신의 가부가) 제어되는 통신이라고 할 수 있다.

인체 근방 통신 중 하나로서의 준정전계 통신에 의하면, 송신 단말 TX에 의한 전계의 출력(파워)과 주파수를 적절히 설정하는 것에 의해, 송신 단말 TX를 휴대하고 있는 유저의 인체와 수신 단말 RX(의 안테나)가 근방에 위치하고 있을 때에만, 즉 예를 들면 수 센티미터 내지 수십 센티미터 이내에 근접했을 때, 혹은 접촉할 정도로 근접했을 때, 또는 접촉했을 때에만 준정전계 통신이 행해지도록 할 수가 있다.

따라서, 송신 단말 TX를 휴대하고 있는 유저가, 예를 들면 IC카드와 리더/라이터 사이의 통신과 달리, 송신 단말 TX는 수신 단말 RX에 꽂지(달지) 않아도, 수신 단말 RX과 통신을 행할 수가 있다.

즉, 유저가 IC 카드를 의복의 포켓에 넣는 등해서 휴대하고 있는 경우에, 유저는 IC 카드를 포켓에서 꺼내어 리더/라이터에 꽂아서, IC카드와 리더/라이터 사이에서 통신을 행하도록 하기 위한 명시적인 행위를 행한다.

이것에 대해서, 준정전계 통신에 의하면, 송신 단말 TX를 휴대하고 있는 유저 자신이 수신 단말(의 안테나)에 근접하면, 송신 단말 TX와 수신 단말 RX 사이에서 통신을 행하도록 하기 위한 명시적인 행위를 행하지 않더라도, 송신 단말 TX와 수신 단말 RX 사이에서 통신을 행하는 것이 가능해진다.

또한, 송신 단말 TX와 수신 단말 RX를 바꿔넣어도(교체해도), 즉 유저가 송신 단말 TX 대신에 수신 단말 RX를 휴대하고 있는 경우에도 상술한 경우와 마찬가지이다.

다음에, 본 발명의 실시예에서 이용하는 PK(개인 관련 키) 시스템에 대해 설명한다.

도 7은 PK 시스템의 구성예를 도시하는 블록도이다.

네트워크(21)는 예를 들면 인터넷이나 LAN(Local Area Network) 및 그밖의 유선 또는 무선의 네트워크이다. 도 7에서는 네트워크(21)에는 pBase(23)나 서비스 시스템(24)(도 7에서는 4개의 서비스 시스템(24-1), (24-2), (24-3), (24-4))이 접속되어 있다.

PK(Personal Key)(22)는 그 소유자인 유저에 관한 정보인 개인 관련 정보를 기억하는 휴대 가능한 소형의 컴퓨터 등으로 구성된다. 도 7에 있어서, 유저는 PK(22)를 예를 들면 의복의 포켓에 휴대하고 있다.

여기서, 개인 관련 정보란, 단지 이름, 주소 등 그 유저의 개인 관련 정보를 특정하기 위한 정보 뿐만 아니라, 기호 정보, 인증 정보, 점수 정보, 다른 사람으로부터 받은 정보 등을 포함하는 그 유저에 관련된 여러가지 정보를 의미한다. 이하에 있어서는 개인 관련 정보를 PMD(Personal Meta Data)라고도 한다.

PK(22)는 서비스 시스템(24) 주위의 영역 R에 있어서, 그 서비스 시스템(24)과 통신한다. 또, PK(22)는 근방의 도시하지 않은 정보 기기와의 사이에서도 통신을 행할 수가 있다.

또한, PK(22)와 서비스 시스템(24)과의 사이에서는 예를 들면 RF(Radio Frequency) 통신, 준정전계 통신, 광통신 등의 무선 통신 및 유선 통신을 행할 수 있음을 주의해야 한다. 여기에서는 예를 들면 상술한 인체 근방 통신 중 하나로서의 준정전계 통신이 행해지는 것으로 한다. 따라서, PK(22) 및 서비스 시스템(24)은 모두, 도 3 및 도 6에서 설명한 송신 단말 TX와 수신 단말 RX와 동일한 통신 기능을 가지고 있다. 이 경우, 도 7의 영역 R은 유저의 인체 표면으로부터 근방의 영역이다.

또, PK(22)는 암호키에 근거해서 정보를 암호화하는 암호화 기능을 가지고 있으며, 서비스 시스템(24) 등과 통신하는 경우, 나아가서는 후술하는 바와 같이 서비스 시스템(24)을 거쳐서 pBase(23) 등과 통신하는 경우에는 정보를 암호화해서 송신한다. PK(22)의 통신 상대가 되는 pBase(23)나 서비스 시스템(24)도 마찬가지이다.

pBase(23)는 컴퓨터로 구성되고, PK(22)의 유저의 PMD(Personal Meta Data)를 기억한다. 또, pBase(23)는 네트워크(21)에 접속되어 있고, 서비스 시스템(24), 나아가서는 서비스 시스템(24)을 거쳐서 PK(22)와 통신할 수가 있다.

또한, pBase(23)는 예를 들면 PK(22)의 유저의 유저 집의 홈 서버(도시하지 않음) 등으로 구성할 수가 있다. 또, pBase(23)는 그밖에 예를 들면 인터넷 상의 서버로 구성할 수도 있으며, 이 경우 pBase(23)에는 다른 유저의 PMD도 기억시킬 수가 있다.

서비스 시스템(24)은 컴퓨터에 의해 구성되고, 네트워크(21)를 거쳐서 pBase(23)와 통신할 수가 있다. 또, 서비스 시스템(24)은 준정전계 통신용의 안테나(25)를 가지고, 그 안테나(25) 및 유저의 인체를 거쳐서 PK(22)와의 사이에서 준정전계 통신을 행한다. 서비스 시스템(24)은 PK(22)와의 사이에서 준정전계 통신을 행하는 것에 의해, 예를 들면 정보 제공, 쇼핑 대금의 결제(payment settlement) 등의 서비스를 유저에게 제공한다. 또, 서비스 시스템(24)은 PK(22)와의 사이에서 준정전계 통신을 행하는 것에 의해, 네트워크(21)를 거친 PK(22)와 pBase(23) 사이의 통신의 중계를 행한다. 즉 이 경우, 서비스 시스템(24)은 PK(22)와 pBase(23) 사이의 통신의 소위 액세스 포인트로서 기능한다.

또한, 안테나(25)는 서비스 시스템(24)의 근처에 설치할 수도 있고, 서비스 시스템(24)으로부터 떨어진 위치에 설치할 수도 있다.

여기서, 서비스 시스템(24)은 예를 들면 web(웹) 페이지나 음악 정보 등을 제공하는 컨텐츠 서버, 크레디트 카드에 의한 결제 등을 행하는 크레디트 카드 처리 서버, 채팅 등의 커뮤니케이션을 제어하는 커뮤니케이션 서버 등으로서, 서비스를 제공하는 것으로 할 수가 있다.

또, 도 7에서는 서비스 시스템(24)으로서 4개의 서비스 시스템(24-1) 내지 (24-4)을 도시하고 있지만, 서비스 시스템의 수는 4개에 한정되는 것은 아니다.

또, 서비스 시스템(24)은 서버에 한정되는 것은 아니며, 퍼스널 컴퓨터나 콘솔 단말, 각종 컨슈머(consumer) 일렉트로닉스 기기(CE 기기) 등이어도 좋다.

또, 서비스 시스템(24)은 네트워크(21)에 접속되어 있지 않아도 좋다.

또, 서비스 시스템(24-i)(도 7에서는 i=1, 2, 3, 4)은, 다른 서비스 시스템(24-j)(도 7에서는 j=1, 2, 3, 4이며, j≠i)가 PK(22)와 준정전계 통신을 행하고 있는 경우에는, 네트워크(21)를 거쳐서 다른 서비스 시스템(24-j)과 통신하고, PK(22)의 유저에 대해서 서비스를 제공할 수가 있다.

다음에, 도 8은 도 7의 PK(22)의 하드웨어 구성예를 도시하는 블록도이다.

CPU(Central Processing Unit)(31)은 ROM(Read Only Memory)(32)에 기억되어 있는 프로그램 또는 기억부(38)로부터 RAM(Random Access Memory)(33)에 로드된 프로그램에 따라 각종 처리를 실행한다. RAM(33)에는 또, CPU(31)가 각종 처리 동작을 실행하는데 있어서 필요한 데이터 등도 적절히 기억된다.

CPU(31), ROM(32) 및 RAM(33)은 버스(34)를 거쳐서 서로 접속되어 있다. 이 버스(34)에는 또, 입출력 인터페이스(35)도 접속되어 있다.

입출력 인터페이스(35)에는 스위치, 버튼, 터치 민감성 패널, 마이크(마이크로폰) 등으로 이루어지는 입력부(36), 및 도트 매트릭스 디스플레이, 스피커, 진동 모터 등에 의해 구성되고, 화상, 음성, 점자 또는 진동 등에 의해 유저에게 제시할 정보를 출력하는 출력부(37)가 접속되어 있다. 또, 입출력 인터페이스(35)에는 하드 디스크 또는 EEPROM(Electrically Erasable and Programmable Read Only Memory) 등에 의해 구성되는 기억부(38), 적어도 준정전계 통신을 행하는 기능(도 3 및 도 6의 송신 단말 TX 및 수신 단말 RX의 기능)을 가지는 통신부(39)가 접속되어 있다. 또한, 통신부(39)는 그 밖에 RF통신(전자파 통신)이나 광통신, 네트워크(21)를 거친 통신 등을 행하는 기능을 가지고 있어도 좋다.

입출력 인터페이스(35)에는 필요에 따라서 드라이브(40)가 접속된다. 드라이브(40)에는 후술하는 각종 처리 동작을 CPU(31)에 실행시키는 프로그램이 기록된 기록 매체로서, 예를 들면 리무버블(소거가능한) 미디어(41)가 장착된다. 리무버블 미디어(41)에 기록된 프로그램은 필요에 따라서 읽어내져(리드되어), 기억부(38)에 인스톨(설치)된다.

다음에, 도 9는 도 7의 pBase(23)의 하드웨어 구성예를 도시하는 블록도이다.

pBase(23)는 도 8에 도시한 PK(22)와 마찬가지로 구성되어 있다. 즉, 도 9의 CPU(51) 내지 리무버블 미디어(61)는 도 8의 CPU(31) 내지 리무버블 미디어(41)에 대응하고 있다. 각 부의 기능은 도 8의 경우와 마찬가지이며, 상세한 설명은 생략한다. 단, 통신부(59)는 준정전계 통신이 아니라, 네트워크(21)를 거친 통신을 행하는 기능을 적어도 가지고 있다.

또, 서비스 시스템(24)도 도 9와 마찬가지의 구성이며, 동일 도면을 적용한다. 단, 서비스 시스템(24)의 통신부(59)는 적어도 준정전계 통신과 네트워크(21)를 거친 통신을 행하는 기능을 가지고 있다.

다음에, 도 10에는 PK(22)의 기억부(38)의 기억 내용을 도시하고 있다.

PK(22)의 기억부(38)에는 적어도 복수의 프로그램인 모듈군(71)과 PMDB(72)가 기억된다.

모듈군(71)은 서비스 시스템(24)으로부터 서비스의 제공을 받는 것 등을 위해서, PK(22)의 CPU(31)가 실행하는 프로그램(모듈)인 통신 모듈(81), 유저 제어 허가 입력 모듈(82), 허가 항목 확인 모듈(83), 위장 방지 모듈(84), PMD 변경 모듈(85) 및 DB 액세스 모듈(86)을 가지고 있다.

통신 모듈(81)은 도 8의 통신부(39)를 제어해서 통신을 행한다. 유저 제어 허가 입력 모듈(82)은 PMD에 대한 액세스의 허가의 유저의 명령을 접수한다. 허가 항목 확인 모듈(83)은 서비스 시스템(24)으로부터 액세스 요구가 있었던 PMD에 대해서, 그 액세스 가부를 판단한다. 위장 방지 모듈(83)은 서비스 시스템(24)의 소위 위장을 방지한다. 처리(위장 방지 처리)를 행하는 PMD 변경 모듈(85)은 PMD의 변경을 제어한다. DB액세스 모듈(86)은 유저 제어 허가 입력 모듈(82) 내지 PMD 변경 모듈(85)의 명령(요구)에 근거해서, PMDB(72)에 액세스하여 PMD의 읽기(리드) 또는 변경을 행한다.

PMDB(72)는 PMD에 의해 구성되는 데이터베이스이다. PMDB(72)에는 서비스 시스템(24)(또는 서비스 시스템(24)에 의해서 제공되는 서비스) 고유의 ID(Identification)인 서비스 ID에 대응하는 디렉토리가 구성되고, 각 디렉토리에 PMD가 기억된다.

도 10에 있어서는 서비스 ID1에 대응하는 디렉토리, 서비스 ID2에 대응하는 디렉토리 등이 구성되어 있다.

서비스 ID1에 대응하는 디렉토리에는 PMD로서의 액세스 허가 정보, 메타데이터 A－1, 메타데이터 A－2, 메타데이터 A－3 등이 기억되어 있다.

액세스 허가 정보는 그 디렉토리에 기억되어 있는 정보에 대한 서비스 시스템(24)으로부터의 액세스의 가부를 나타내는 정보로서, 유저에 의해 설정된다. 메타데이터 A－1, 메타데이터 A－2 및 메타데이터 A－3 등은 서비스 ID1에 대응하는 서비스 시스템(24)에 있어서 이용되는 메타데이터로서, 예를 들면 서비스 ID1에 대응하는 서비스 시스템이 영화나 텔레비전 프로그램 등의 컨텐츠를 제공하는 컨텐츠 서버인 경우, 메타데이터 A－1, 메타데이터 A－2 및 메타데이터 A－3 등으로서는 예를 들면 유저가 시청한 영화나 프로그램을 나타내는 메타데이터가 기억된다.

그밖에, PMD로서는 서비스 시스템(24)이 PK(22)(유저)를 특정하기 위한 유저 ID, 후술하는 위장 방지 처리에 있어서 필요로 되는 암호 또는 암호키 등의 인증 정보, 시청된 프로그램에 근거하는 유저의 기호 정보 등이 기억된다.

서비스 ID2에 대응하는 디렉토리에도, 서비스 ID1에 대응하는 디렉토리와 마찬가지로, 액세스 허가 정보, 메타데이터 B－1, 메타데이터 B－2, 메타데이터 B－3 등의 PMD가 기억되어 있다.

여기서, PK(22)가 새로운 서비스 시스템(24)을 이용하는 경우, PMDB(72)에는 그 새로운 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리가 생성되고, 그 생성된 디렉토리에 필요한 PMD가 기억된다.

도 11은 PK(22)의 PMDB(72)에 새로운 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리가 생성될 때에 PK(22)와 서비스 시스템(24)에서 행해지는 처리, 즉 PK(22)에 새로운 서비스 시스템(24)에 대응하는 서비스 ID를 등록(초기 등록)할 때에 행해지는 처리를 도시하는 화살표도(흐름도)이다.

또한, 상술한 바와 같이 PK(22)와 서비스 시스템(24) 사이에서는 준정전계 통신이 행해진다. 따라서, PK(22)와 서비스 시스템(24) 사이의 통신은 PK(22)를 휴대하고 있는 유저가 서비스 시스템(24)에 근접해 있을 때, 즉 유저의 인체 표면에 형

성된 준정전계가 지배적으로 되는 공간 내에 서비스 시스템(24)의 안테나(25)(도 7)가 존재할 때에, 거꾸로 말하면 서비스 시스템(24)의 안테나(25) 표면에 형성된 준정전계가 지배적으로 되는 공간 내에 유저의 인체의 적어도 일부가 존재할 때에 행해진다.

우선, 최초로 단계 S1에 있어서, 서비스 시스템(24)은 PK(22)에 대해서 서비스 요구, 서비스 ID 및 그 서비스 시스템(24)에서 읽기 변경 대상이 되는 메타데이터와 같은 정보를 송신하고, 단계 S21에 있어서 PK(22)의 통신 모듈(81)에 의해 이것이 수신된다.

여기서, 서비스 시스템(24)에서 읽기 변경 대상이 되는 전술된 메타데이터(읽기 변경 대상 메타데이터)는, 서비스 시스템(24)이 참조만 행하는 메타데이터와 내용의 변경을 행하는 메타데이터의 둘 모두를 포함한다.

그 후, 단계 S22에 있어서, PK(22)의 통신 모듈(81)은 허가 항목 확인 모듈(83)에 서비스 시스템(24)으로부터 수신한 정보를 전송하고, 허가 항목 확인 모듈(83)은 단계 S41에 있어서 PK(22)의 통신 모듈(81)로부터의 정보를 수신하고, 단계 S42로 진행한다.

단계 S42에서는 허가 항목 확인 모듈(83)은 통신 모듈(81)로부터 수신한 정보에 근거해서, 읽기 변경 대상 메타데이터를 유저에게 제시한다. 즉, 예를 들면 읽기 변경 대상 메타데이터의 내용이 도트 매트릭스 디스플레이 디바이스에 문자 또는 도형으로 표시되거나, 스피커를 통해서 소리내어 읽어내질 수 있다.

그리고, 단계 S43에 있어서 허가 항목 확인 모듈(83)은 유저 제어 허가 입력 모듈(82)에 대해서 확인 요구를 출력하고, 유저 제어 허가 입력 모듈(82)은 단계 S61에 있어서 확인 요구를 수신한다. 그리고, 유저 제어 허가 입력 모듈(82)은 단계 S62에 있어서, 단계 S42에서 유저에게 제시된 읽기 변경 대상 메타데이터에 대한 액세스를 유저가 거부했는지의 여부를 판정하고, 거부했다고 판정된 경우, 거부 신호를 통신 모듈(81)에 출력한다. 이 경우, 통신 모듈(81)은 단계 S23에 있어서, 유저 제어 허가 입력 모듈(82)로부터의 거부 신호를 수신하고, 단계 S24로 진행해서, 그 거부 신호를 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S2에 있어서, 통신 모듈(81)로부터의 거부 신호를 수신하고, 그 후 PK(22)와 서비스 시스템(24)은 처리를 종료한다. 이 경우, PK(22)에 있어서, 서비스 시스템(24)에 대응하는 서비스 ID의 등록은 행해지지 않는다.

한편, 단계 S42에서 제시된 읽기 변경 대상 메타데이터에 대한 액세스를 유저가 거부하고 있지 않다고 판정된 경우, 단계 S63으로 진행하고, 유저 제어 허가 입력 모듈(82)은 읽기 변경 대상 메타데이터의 각각에 대해 예를 들면 "읽기와 변경을 허가", "읽기만 허가"의 정보를 설정한다. 이들 정보는 액세스 허가 정보(도 10)로서 PMDB(72)에 기억된다.

또한, 읽기 변경 대상 메타데이터에 대한 "읽기와 변경을 허가"나 "읽기만 허가"와 같은 정보의 설정은 유저의 지정에 근거해서 행해짐을 주목해야 한다.

그리고, 단계 S64에 있어서, 유저 제어 허가 입력 모듈(82)은 액세스 허가 정보가 설정된 것을 허가 항목 확인 모듈(83)에 통지하고, 허가 항목 확인 모듈(83)은 단계 S44에 있어서 이 통지를 수신한다. 단계 S45에 있어서, 허가 항목 확인 모듈(83)은 위장 방지 모듈(84)에 대해서 확인 코드의 생성 요구를 송신하고, 위장 방지 모듈(84)은 단계 S81에 있어서 그 생성 요구를 수신한다.

위장 방지 모듈(84)은 확인 코드의 생성 요구를 수신하면, 단계 S81에서 S82로 진행해서, 확인 코드를 생성한다.

여기서, 확인 코드는 PK(22)와 서비스 시스템(24)이 다음 번의 통신을 행할 때에 사용되는 위장 방지 방법을 나타내는 코드이다. 즉, 부정한 유저 또는 PK(22)와 서비스 시스템(24) 사이의 통신을 도청한 제3자가, PK(22) 또는 서비스 시스템(24)으로 위장하고 있지 않은지를 PK(22)와 서비스 시스템(24) 사이에서 상호 확인하기 위한 방법을 나타내는 코드가 확인 코드이다.

위장 방지 방법으로서는 예를 들면 암호에 의한 인증(암호 방식), 공개키에 의해 암호화된 정보에 의한 인증(공개키 방식), 공통키에 의해 암호화된 정보에 의한 인증(공통키 방식) 등을 채용할 수가 있다. PK(22), 서비스 시스템(24) 또는 PK(22)의 유저는 예를 들면 PK(22)와 서비스 시스템(24)과의 통신에 있어서, 어느 정도의 안전성이 요구되는지, 어느 정도 빈번

하게 위장 방지를 위한 체크를 행하는지, 암호키의 관리 방법의 안전성과 평이함, 암호화와 복호에 있어서의 연산량 등을 고려해서 최적한 위장 방지 방법을 선택할 수 있으며, 위장 방지 모듈(84)은 그 선택된 위장 방지 방법에 대응하는 확인 코드를 생성한다. 또한, 위장 방지의 처리에 대해서는 도 12와 도 13을 참조해서 후술한다.

단계 S82에 있어서, 위장 방지 모듈(84)은 확인 코드를 생성하면, 그 생성된 확인 코드를 통신 모듈(81)에 대해서 출력하고, 통신 모듈(81)은 단계 S25에 있어서 그 확인 코드를 수신한다. 단계 S26에 있어서, 통신 모듈(81)은 단계 S25에서 수신한 확인 코드를 서비스 시스템(24)에 송신하고, 서비스 시스템(24)은 단계 S3에 있어서 통신 모듈(81)로부터의 확인 코드를 수신하여 기억하고, 처리를 종료한다.

또한, PK(22)의 통신 모듈(81)은 확인 코드 이외에, 서비스 시스템(24)이 PK(22)(의 유저)를 특정하기 위한 유저 ID도 서비스 시스템(24)에 송신한다. 서비스 시스템(24)은 통신 모듈(81)로부터의 확인 코드를 마찬가지로 통신 모듈(81)로부터의 유저 ID와 대응시켜 기억한다.

여기서, 유저 ID는 서비스 시스템(24)이 PK(22)(의 유저)를 특정할 수 있는 것이면 어떠한 형식이라도 좋다. 또, PK(22)의 유저 ID는 서비스 시스템마다 달라도 좋고, 또 하나의 서비스 시스템이 복수의 서비스를 제공하는 경우에는 서비스마다 달라도 좋다.

한편, 허가 항목 확인 모듈(83)은 단계 S45에 있어서, 확인 코드의 생성 요구를 위장 방지 모듈(84)에 송신한 후, 단계 S46으로 진행해서, DB 액세스 모듈(86)에 대해서 서비스 ID 등록 요구를 단계 S41에서 수신한 서비스 시스템(24)으로부터의 서비스 ID와 함께 출력한다. DB 액세스 모듈(86)은 단계 S101에 있어서, 허가 항목 확인 모듈(83)로부터의 서비스 ID 등록 요구 및 서비스 ID를 수신하고, 단계 S102로 진행해서, 도 14를 참조하여 후술하는 서비스 ID 등록 처리를 실행하고 처리를 종료한다.

DB 액세스 모듈(86)이 서비스 ID 등록 처리를 실행하는 것에 의해, 서비스 시스템(24)으로부터의 서비스 ID가 등록되는 디렉토리, 즉 그 서비스 ID에 대응하는 디렉토리가 생성된다.

이상과 같이, PK(22)에 있어서 서비스 시스템(24)에 대응하는 서비스 ID가 등록될 때, 그 서비스 시스템(24)이 읽기 또는 변경을 요구하는 PMD인 읽기 변경 대상 메타데이터가 유저에게 제시되고, 유저의 지정에 근거해서 "읽기와 변경을 허가"하는 메타데이터나 "읽기만 허가"하는 메타데이터가 설정되므로, 유저는 서비스 시스템(24)에 대해서 제공하는 PMD(서비스 시스템(24)이 참조할 수 있는 PMD)나 서비스 시스템(24)이 변경할 수 있는 PMD를 제한할 수가 있다.

따라서, 예를 들면 유저가 모르는 사이에 유저가 공개하고 싶지 않은 PMD가 서비스 시스템(24)에 제공되는 것을 방지할 수 있어, 유저는 안심하고 서비스를 받을 수가 있다.

다음에, PK(22)는 도 11에서 설명한 바와 같이, 서비스 시스템(24)과 최초로 통신을 행할 때, 그 서비스 시스템(24)의 서비스 ID를 등록하고, 확인 코드를 생성한다. 또, 서비스 시스템(24)도 PK(22)와 최초로 통신을 행할 때, 그 PK(22)에서 생성된 확인 코드와 PK(22)의 유저 ID를 적절하게 기억한다.

서비스 시스템(24)의 서비스 ID가 등록된 후, 서비스 시스템(24)으로부터 서비스의 제공을 받기 위해서 서비스 시스템(24)과 통신할 때는, PK(22)는 그 서비스 ID를 등록했을 때에 생성된 확인 코드에 근거해서 위장 방지 처리를 행할 수가 있다.

마찬가지로 PK(22)의 유저 ID와 확인 코드를 적절하게 기억한 후, PK(22)의 유저에게 서비스를 제공하기 위해서 PK(22)와 통신할 때, 서비스 시스템(24)은 그 PK(22)의 유저 ID와 관련된 확인 코드에 근거해서 위장 방지 처리를 행할 수가 있다.

그래서, 도 12 및 도 13의 화살표도를 참조해서, PK(22)와 서비스 시스템(24)이 통신할 때에 행해지는 위장 방지 처리에 대해 설명한다.

도 12는 암호에 의한 인증을 이용한 위장 방지 처리를 포함하는 PK(22)와 서비스 시스템(24)의 처리를 설명하는 화살표도이다.

도 12의 위장 방지 처리에서, PK(22)는, 서비스 시스템(24)이 위장인지를 확인하고, 그 후 서비스 시스템(24)은 PK(22)가 위장인지를 확인한다. 그리고, PK(22)와 서비스 시스템(24) 모두가 위장이 아닌 것을 확인할 수 있었던 후, PMD의 읽기 또는 변경의 처리가 행해진다.

여기서, 도 12의 인증에서 이용되는 암호는 예를 들면 소정의 코드 이다. PK(22)는, 서비스 시스템(24)의 서비스 ID의 등록시에, 그 서비스 ID에 대응하는 암호로서 서비스 시스템(24)을 인증하기 위한 암호(서비스 암호)와 PK(22)를 인증하기 위한 암호(PK 암호)를 생성하고, 이들 생성된 암호를 PMDB(72)에 기억시킨다. 또, PK(22)는, 서비스 ID 등록시에, PMDB(72)에 기억시킨 서비스 암호와 PK 암호를 서비스 시스템(24)에 송신한다. 그리고, 서비스 시스템(24)은 PK(22)의 유저 ID를 서비스 암호와 PK 암호에 관련시켜, 관련된 정보를 기억시킨다.

우선 최초로 단계 S121에 있어서, 서비스 시스템(24)은 자신의 서비스 ID와 PK(22)의 유저 ID에 관련된 서비스 암호를 PK(22)에 송신하고, PK(22)의 통신 모듈(81)은 단계 S141에 있어서, 서비스 시스템(24)으로부터의 서비스 ID 및 서비스 암호를 수신한다.

여기서, 단계 S121에서는 서비스 시스템(24)은 이미 PK(22)로부터 PK(22)의 유저 ID를 수신하고 있으며, PK(22)의 유저 ID에 관련된 서비스 암호를 PK(22)에 송신한다.

PK(22)의 통신 모듈(81)은 단계 S142에 있어서, 단계 S141에서 수신한 서비스 시스템(24)으로부터의 서비스 ID와 서비스 암호를 위장 방지 모듈(84)로 전송하고, 위장 방지 모듈(84)은 단계 S171에 있어서 이들 ID 및 암호를 수신하고, 단계 S172로 진행한다.

단계 S172에 있어서, 위장 방지 모듈(84)은 도 15를 참조해서 후술하는 서비스 ID 매칭 처리를 실행하고 단계 S173으로 진행하며, DB 액세스 모듈(86)에 대해서 서비스 시스템(24)으로부터의 서비스 ID에 관련된 PMDB(72)에 기억되어 있는 서비스 암호 및 PK 암호와 유저 ID의 요구를 통지한다. DB 액세스 모듈(86)은 단계 S191에 있어서, 위장 방지 모듈(84)로부터의 요구를 수신하고, 단계 S192로 진행한다.

단계 S192에서는 DB 액세스 모듈(86)은 위장 방지 모듈(84)로부터 요구된 서비스 암호 및 PK 암호와 유저 ID를 PMDB(72)로부터 읽어내어, 이들 정보를 위장 방지 모듈(84)로 출력한다.

위장 방지 모듈(84)은 단계 S174에 있어서, DB 액세스 모듈(86)로부터의 서비스 암호 및 PK 암호와 유저 ID를 수신한다. 단계 S175에서는 위장 방지 모듈(84)은 서비스 시스템(24)으로부터의 서비스 암호와 PMDB(72)에 기억된 서비스 암호(단계 S174에서 수신한 서비스 암호)를 비교하고, 그들이 일치하는지 어떤지를 판정한다.

단계 S175에 있어서, 서비스 시스템(24)으로부터의 서비스 암호와 PMDB(72)에 기억된 서비스 암호가 일치하지 않는다고 판정된 경우, 위장 방지 모듈(84)은 서비스 시스템(24)이 위장일 가능성이 있다고 판정하고, 통신 모듈(81)에 대해서 통신의 거부를 나타내는 거부 신호를 출력한다.

통신 모듈(81)은 단계 S143에 있어서, 위장 방지 모듈(84)로부터의 거부 신호를 수신하고, 단계 S144로 진행해서, 그 수신된 거부 신호를 서비스 시스템(24)에 송신한다. 그리고, 서비스 시스템(24)은 단계 S122에 있어서, 통신 모듈(81)로부터의 거부 신호를 수신한다.

PK(22)는 이상과 같이 거부 신호를 서비스 시스템(24)에 송신한 후에는 서비스 시스템(24)으로부터의 액세스를 거부한다. 즉, PK(22)는 서비스 시스템(24)과의 통신을 거부한다.

한편, 단계 S175에 있어서 비교가 일치한다고 판정된 경우, 단계 S176에서, 위장 방지 모듈(84)은 서비스 시스템(24)이 위장이 아니라고 해서, 유저 ID와 PMDB(72)에 서비스 시스템(24)의 서비스 ID에 관련된 PK 암호(단계 S174에서 수신된 PK 암호)를 통신 모듈(81)에 출력한다.

통신 모듈(81)은 단계 S145에 있어서 위장 방지 모듈(84)로부터의 유저 ID와 PK 암호를 수신하고, 단계 S146으로 진행해서, 그 유저 ID와 PK 암호를 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S123에 있어서 PK(22)(의 통신 모듈(81))로부터의 유저 ID와 PK 암호를 수신한다. 단계 S124에서는 서비스 시스템(24)은 PK(22)로부터의 유저 ID에 관련된 PK 암호와 PK(22)로부터의 PK 암호(단계 S123에서 수신한 PK 암호)를 비교하고, 일치하는지의 여부를 판정한다.

단계 S124에 있어서, PK 암호가 일치하지 않는다고 판정된 경우, 서비스 시스템(24)은 PK(22)가 위장일 가능성이 있음을 결정하고, 서비스 시스템(24)은 통신의 거부를 나타내는 거부 신호를 PK(22)에 송신한다. PK(22)에서는 단계 S177에 있어서, 위장 방지 모듈(84)이 통신 모듈(81)을 거쳐서 서비스 시스템(24)으로부터의 거부 신호를 수신한다.

서비스 시스템(24)은 이상과 같이, 거부 신호를 PK(22)에 송신한 후에는 PK(22)로부터의 액세스를 거부한다. 즉, 서비스 시스템(24)은 PK(22)와의 통신을 거부한다.

한편, 단계 S124에 있어서, PK 암호가 일치한다고 판정된 경우, 서비스 시스템(24)은 PK(22)가 위장이 아님을 결정하고, 단계 S125로 진행하고, PK(22)에 대해서 PMD의 읽기 요구를 송신한다.

PK(22)의 통신 모듈(81)은 단계 S147에 있어서, 서비스 시스템(24)으로부터의 읽기 요구를 수신하고, 단계 S148로 진행해서, 그 수신된 읽기 요구를 DB액세스 모듈(86)에 대해서 출력한다.

DB 액세스 모듈(86)은 단계 S193에 있어서, 통신 모듈(81)로부터의 읽기 요구를 수신하고, 단계 S194로 진행해서, 요구되고 있는 PMD를 PMDB(72)의 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리로부터 읽어낸다.

여기서, 단계 S194에서는 DB 액세스 모듈(86)은 요구되고 있는 PMD의 읽기가 허가되고 있는지 어떤지를, 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도 10)를 참조하는 것에 의해 확인한다. 요구되고 있는 PMD중 읽기가 허가되고 있는 PMD만을 PMDB(72)로부터 읽어낸다.

그 후, 단계 S195에서, DB 액세스 모듈(86)은 PMDB(72)로부터 읽어낸 PMD를 통신 모듈(81)에 대해서 출력한다. 통신 모듈(81)은 단계 S149에 있어서 그 PMD를 수신하고, 단계 S150으로 진행한다.

단계 S150에서는, 통신 모듈(81)은 단계 S149에서 수신한 PMD를 서비스 시스템(24)에 대해서 송신하고, 서비스 시스템(24)은 단계 S126에 있어서 그 PMD를 수신하고, 단계 S127로 진행한다.

단계 S127에서는 서비스 시스템(24)은 PK(22)로부터 수신한 PMD에 근거해서, 각종 처리(서비스 대응 처리)를 실행한다. 단계 S127의 서비스 대응 처리의 결과, PK(22)로부터의 PMD의 변경이 필요해지는 경우, 서비스 시스템(24)은 단계 S128로 진행해서, PK(22)로부터 수신한 PMD를 변경하고, 변경된 PMD를 PK(22)에 대해서 송신한다.

통신 모듈(81)은 단계 S151에 있어서, 서비스 시스템(24)으로부터의 PMD를 수신하고, 단계 S152로 진행해서, 그 수신된 PMD를 DB 액세스 모듈(86)에 대해서 출력한다.

DB 액세스 모듈(86)은 단계 S196에 있어서, 통신 모듈(81)로부터의 PMD, 즉 서비스 시스템(24)에 의해 변경된 PMD를 수신하고, 단계 S197로 진행해서, 그 PMD의 변경이 허가되고 있는지 어떤지를 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도 10)를 참조하는 것에 의해 확인한다. 또, 단계 S197에서는 DB 액세스 모듈(86)은 서비스 시스템(24)에 의해 변경된 PMD에 대응하는 변경이 허가되고 있는 것을, 서비스 시스템(24)에 의해 변경된 PMD에 따라 변경하고(PMD의 갱신을 행하고), 처리를 종료한다.

이상과 같이, PK(22)는, 서비스 암호의 일치성에 의한 서비스 시스템(24)의 위장의 확인을 행하고, 서비스 시스템(24)은 PK 암호의 일치성에 의한 PK(22)의 위장의 확인을 행하여, 안전한 서비스의 제공을 행할 수가 있다.

또한, 상술한 경우에는 PK(22)는 서비스 암호의 일치성을 확인하고, 그 후 서비스 시스템(24)은 PK 암호의 일치성을 확인함을 주목해야 한다. PK(22)가 서비스 암호의 일치성을 확인하기 이전에 서비스 시스템(24)은 PK 암호의 일치성을 확인하는 것은 가능하다.

다음에, 도 13은 공개키에 의해 암호화된 정보에 의한 인증을 이용한 위장 방지 처리를 포함하는 PK(22)와 서비스 시스템(24)의 처리를 설명하는 화살표도이다.

도 13의 위장 방지 처리에서는, PK(22)는 서비스 시스템(24)이 위장이 아닌 것을 확인하고, 그 후 서비스 시스템(24)은 PK(22)가 위장이 아닌 것을 확인한다. 그리고, PK(22)와 서비스 시스템(24)이 각각이 위장이 아닌 것을 확인한다면, PMD의 읽기 또는 변경의 처리가 행해진다.

또한, PK(22)와 서비스 시스템(24)은 예를 들면 RSA(Rivest, Shamir, Adeleman) 등의 공개키 방식의 암호 알고리즘에 의한 정보의 암호화 또는 복호의 처리를 실행하는 기능을 가지고 있는 것으로 가정됨을 주목해야 한다.

그리고, PK(22)에 있어서 서비스 시스템(24)의 서비스 ID가 등록될 때, PK(22)에서는 서비스 시스템(24)의 공개키가 예를 들면 서비스 시스템(24)으로부터 취득되고, 서비스 시스템(24)의 서비스 ID에 관계된 것으로 PMDB(72)에 이러한 취득된 공개키가 기억되어 있는 것으로 한다. 마찬가지로, 서비스 시스템(24)에서도 PK(22)의 공개키가 취득되고, 이 취득된 공개키는 PK(22)의 유저 ID에 관계된 것으로 기억되어 있는 것으로 한다.

또, PK(22)와 서비스 시스템(24) 각각은 자신의 비밀키를 기억하고 있는 것으로 한다.

우선 최초로 단계 S211에 있어서, 서비스 시스템(24)은 자신의 서비스 ID를 PK(22)에 송신한다. PK(22)의 통신 모듈(81)은 단계 S241에 있어서, 서비스 시스템(24)으로부터의 서비스 ID를 수신하고, 단계 S242로 진행해서, 그 수신된 서비스 ID를 위장 방지 모듈(84)에 전송한다.

위장 방지 모듈(84)은 단계 S281에 있어서, 통신 모듈(81)로부터 전송 되어 오는 서비스 시스템(24)으로부터의 서비스 ID를 수신하고, 단계 S282로 진행해서, 도 15를 참조하여 후술하는 서비스 ID 매칭 처리를 실행하고, 단계 S283으로 진행한다.

단계 S283에서는 위장 방지 모듈(84)은 DB 액세스 모듈(86)에 대해서 유저 ID, PK(22)의 비밀키 및 서비스 시스템(24)의 서비스 ID에 대응하는 공개키의 요구를 송신하고, DB 액세스 모듈(86)은 단계 S311에 있어서 그 요구를 수신한다.

단계 S312에서, DB 액세스 모듈(86)은 유저 ID, PK(22)의 비밀키 및 서비스 시스템(24)의 서비스 ID에 대응하는 공개키를 PMDB(72)로부터 읽어내어, 이러한 유저 ID 및 키들을 위장 방지 모듈(84)에 공급한다.

위장 방지 모듈(84)은 단계 S284에 있어서, DB 액세스 모듈(86)로부터의 유저 ID, PK(22)의 비밀키 및 서비스 시스템(24)의 서비스 ID에 대응하는 공개키(서비스 시스템(24)의 공개키)를 수신하고, 단계 S285로 진행한다.

단계 S285에서, 위장 방지 모듈(84)은 서비스 시스템(24)을 인증하기 위한 소위 챌린지(challenge) 코드를 생성한다. 또, 단계 S285에서, 위장 방지 모듈(84)은 생성된 챌린지 코드를 서비스 시스템(24)의 공개키로 암호화하고, 그 결과 얻어지는 암호화 챌린지 코드를 유저 ID와 함께 통신 모듈(81)에 출력한다.

통신 모듈(81)은 단계 S243에 있어서, 위장 방지 모듈(84)로부터의 암호화 챌린지 코드와 유저 ID를 수신하고, 단계 S244로 진행해서, 그 수신된 암호화 챌린지 코드와 유저 ID를 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S212에 있어서, PK(22)(의 통신 모듈(81))로부터의 암호화 챌린지 코드와 유저 ID를 수신하고, 단계 S213으로 진행한다.

단계 S213에서는 서비스 시스템(24)은 PK(22)로부터의 암호화 챌린지 코드를 자신의 비밀키에 의해 평문(plaintext) 챌린지 코드로 복호한다. 또, 단계 S213에서는 서비스 시스템(24)은 그 챌린지 코드를 소위 응답 코드로 하고, 그 응답 코드를 단계 S212에서 PK(22)로부터 수신한 유저 ID와 관계하여 기억하고 있는 공개키(PK(22)의 공개키)로 암호화하고, 그 결과 얻어지는 암호화 응답 코드를 PK(22)에 대해서 송신한다.

통신 모듈(81)은 단계 S245에 있어서, 서비스 시스템(24)으로부터의 암호화 응답 코드를 수신하고, 단계 S246으로 진행해서, 그 수신된 암호화 응답 코드를 위장 방지 모듈(84)에 출력한다.

위장 방지 모듈(84)은 단계 S286에 있어서, 통신 모듈(81)로부터의 암호화 응답 코드를 수신하고, 그 암호화 응답 코드를 자신의 비밀키에 의해 복호하고, 단계 S287로 진행한다.

단계 S287에서는 위장 방지 모듈(84)은 응답 코드와 단계 S285에서 생성한 챌린지 코드를 비교하고, 그 챌린지 코드와 응답 코드가 일치하고 있는지의 여부를 판정한다.

단계 S287에 있어서, 챌린지 코드와 응답 코드가 일치하지 않는다고 판정된 경우, 위장 방지 모듈(84)은 서비스 시스템(24)이 위장일 가능성이 있다고 인식하여, 통신 모듈(81)에 대해서, 통신의 거부를 나타내는 거부 신호를 통지한다.

통신 모듈(81)은 단계 S247에 있어서, 위장 방지 모듈(84)로부터의 거부 신호를 수신하고, 단계 S248로 진행해서, 그 수신된 거부 신호를 서비스 시스템(24)에 송신한다. 그리고, 서비스 시스템(24)은 단계 S214에 있어서, 통신 모듈(81)로부터의 거부 신호를 수신한다.

PK(22)는 이상과 같이, 거부 신호를 서비스 시스템(24)에 송신한 후에는 서비스 시스템(24)으로부터의 액세스를 거부한다. 즉, PK(22)는 서비스 시스템(24)과의 통신을 거부한다.

한편, 단계 S287에 있어서 챌린지 코드와 응답 코드가 일치한다고 판정된 경우, 위장 방지 모듈(84)은 서비스 시스템(24)이 위장이 아닌 것을 확인할 수 있었던 것을 나타내는 OK 코드를 통신 모듈(81)을 거쳐서 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S215에 있어서, PK(22)로부터의 OK 코드를 수신하고, 단계 S216으로 진행해서, PK(22)를 인증하기 위한 챌린지 코드를 생성한다. 또, 단계 S216에 있어서, 서비스 시스템(24)은 그 생성된 챌린지 코드를 PK(22)의 유저 ID에 관계된 것으로 기억하고 있는 공개키(PK(22)의 공개키)로 암호화하고, 그 암호화 챌린지 코드를 PK(22)에 대해서 송신한다.

PK(22)의 통신 모듈(81)은 단계 S249에 있어서, 서비스 시스템(24)으로부터의 암호화 챌린지 코드를 수신하고, 단계 S250으로 진행해서, 그 수신된 암호화 챌린지 코드를 위장 방지 모듈(84)에 대해서 출력한다.

위장 방지 모듈(84)은 단계 S289에 있어서, 통신 모듈(81)로부터의 암호화 챌린지 코드를 수신하고, 단계 S290으로 진행한다. 단계 S290에서는 위장 방지 모듈(84)은 단계 S289에서 수신한 암호화 챌린지 코드를, 단계 S284에서 얻은 PK(22)의 비밀키에 의해 복호한다. 또, 단계 S290에서는 위장 방지 모듈(84)은 PK(22)의 비밀키에 의한 복호의 결과 얻어진 챌린지 코드를 응답 코드로 하고, 그 응답 코드를 서비스 시스템(24)의 서비스 ID에 대응시켜 기억되어 있는 공개키(단계 S284에서 얻은 서비스 시스템(24)의 공개키)로 암호화하고, 그 결과 얻어지는 암호화 응답 코드를 통신 모듈(81)에 대해서 출력한다.

통신 모듈(81)은 단계 S251에 있어서, 위장 방지 모듈(84)로부터의 암호화 응답 코드를 수신하고, 단계 S252로 진행해서, 그 수신된 암호화 응답 코드를 서비스 시스템(24)에 대해서 송신한다.

서비스 시스템(24)은 단계 S217에 있어서 PK(22)(의 통신 모듈(81))로부터의 암호화 응답 코드를 수신하고, 그 수신한 암호화 응답 코드를 자신의 비밀키에 의해 복호하고, 단계 S218로 진행한다.

단계 S218에서는 서비스 시스템(24)은 단계 S217에서 복호한 응답 코드와 단계 S216에서 생성한 챌린지 코드를 비교하고, 양자가 일치하는지의 여부를 판정한다.

단계 S218에 있어서, 챌린지 코드와 응답 코드가 일치하지 않는다고 판정된 경우, 서비스 시스템(24)은 PK(22)가 위장일 가능성이 있다고 인식하여, PK(22)에 대해서 통신의 거부를 나타내는 거부 신호를 송신한다.

PK(22)의 통신 모듈(81)은 단계 S253에 있어서 서비스 시스템(24)으로부터의 거부 신호를 수신하고, 단계 S254로 진행해서, 그 수신된 거부 신호를 위장 방지 모듈(84)에 대해서 송신한다. 위장 방지 모듈(84)은 단계 S291에 있어서, 통신 모듈(81)로부터의 거부 신호를 수신하고, 전술된 처리를 종료한다.

서비스 시스템(24)은 이상과 같이, 거부 신호를 PK(22)에 송신한 후에는 PK(22)로부터의 액세스를 거부한다. 즉, 서비스 시스템(24)은 PK(22)와의 통신을 거부한다.

한편, 단계 S218에 있어서 챌린지 코드와 응답 코드가 일치한다고 판정된 경우, 즉 PK(22)와 서비스 시스템(24)에 있어서 상호 인증에 성공한 경우, 서비스 시스템(24)은 PK(22)가 위장이 아님을 인식하고, 단계 S219로 진행하고, PK(22)에 대해서 PMD의 읽기 요구를 송신한다.

PK(22)의 통신 모듈(81)은 단계 S255에 있어서 서비스 시스템(24)으로부터의 읽기 요구를 수신하고, 단계 S256으로 진행해서, 그 수신된 요구를 DB 액세스 모듈(86)에 대해서 출력한다.

DB 액세스 모듈(86)은 단계 S313에 있어서 통신 모듈(81)로부터의 읽기 요구를 수신하고, 단계 S314로 진행해서, 요구되고 있는 PMD를 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리로부터 읽어낸다.

여기서, 단계 S314에서는 도 12의 단계 S194에 있어서의 경우와 마찬가지로, DB 액세스 모듈(86)은 읽기 요구에 의해 요구되고 있는 PMD의 읽기가 허가되고 있는지 어떤지를, 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도 10)를 참조하는 것에 의해 확인하고, 읽기 요구에 의해 요구되고 있는 PMD중 읽기가 허가되고 있는 PMD만을 PMDB(72)로부터 읽어낸다.

그 후, 단계 S315에서, DB 액세스 모듈(86)은 PMDB(72)로부터 읽어낸 PMD를 통신 모듈(81)에 대해서 출력하고, 통신 모듈(81)은 단계 S257에 있어서 그 PMD를 수신하고, 단계 S258로 진행한다.

단계 S258에서는 통신 모듈(81)은 수신한 PMD를 서비스 시스템(24)에 대해서 송신하고, 서비스 시스템(24)은 단계 S220에 있어서 그 PMD를 수신하고, 단계 S221로 진행한다.

단계 S221에서는 서비스 시스템(24)은 단계 S220에서 PK(22)로부터 수신한 PMD에 근거해서, 서비스 처리동작으로서의 각종 처리 동작을 실행한다. 단계 S221의 서비스 관련 처리의 결과, PK(22)로부터 수신된 PMD의 변경이 필요하게 되는 경우, 서비스 시스템(24)은 단계 S222로 진행해서, PK(22)로부터 수신된 PMD를 변경하고, 변경된 PMD를 PK(22)에 송신한다.

통신 모듈(81)은 단계 S259에 있어서, 서비스 시스템(24)으로부터의 PMD를 수신하고, 단계 S260으로 진행해서, 수신된 PMD를 DB 액세스 모듈(86)에 대해서 출력한다.

DB 액세스 모듈(86)은 단계 S316에 있어서, 통신 모듈(81)로부터의 PMD, 즉 서비스 시스템(24)에 의해 변경된 PMD를 수신하고, 단계 S317로 진행해서, 그 PMD의 변경이 허가되고 있는지 어떤지를 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도 10)를 참조하는 것에 의해 확인한다. 또, 단계 S317에서는 DB 액세스 모듈(86)은 서비스 시스템(24)에 의해 변경된 PMD에 대응하는 PMDB(72)의 PMD중 변경이 허가되고 있는 것을, 서비스 시스템(24)에 의해 변경된 PMD에 따라 변경하고(또는 갱신하고), 처리를 종료한다.

이상과 같이, PK(22) 및 서비스 시스템(24)에 있어서, 소위 챌린지 및 응답 방식에 의한 인증을 행하는 경우에도, 안전한 서비스의 제공을 행할 수가 있다.

또한, 상술한 경우에는 PK(22)는 먼저 서비스 시스템(24)의 인증을 행하고, 그 후 서비스 시스템(24)에 있어서 PK(22)의 인증을 행하도록 했지만, 먼저 서비스 시스템(24)에 있어서 PK(22)의 인증을 행하고, 그 후 PK(22)에 있어서 서비스 시스템(24)의 인증을 행하는 것도 가능하다.

또, 상술한 경우에는, 챌린지 코드와 응답 코드는 공개키에 의해 암호화/복호화된다. 챌린지 코드와 응답 코드의 암호화/복호는 공통키 방식으로 행하는 것도 가능하다.

또, 도 12 또는 도 13에 있어서 상호 인증이 성공한 후에 수행되는 PK(22)와 서비스 시스템(24) 사이의 통신에서는, 정보는 예를 들면 공개키 방식 등으로 암호화되어 수수(주고받음)된다. 즉, 도 12에 있어서의 단계 S126과 S150의 통신 및, 도 12에 있어서의 단계 S128과 S151의 통신과 도 13에 있어서의 단계 S220과 S258의 통신 및, 도 13에 있어서의 단계 S222와 S259의 통신에서는 정보가 암호화되어 수수된다.

다음에, 도 14를 참조해서 도 11의 단계 S102의 서비스 ID 등록 처리의 상세한 것에 대해서 설명한다.

여기서, 이하에서는 서비스 시스템(24)의 서비스 ID로서, 예를 들면 URI(Uniform Resource Identifiers)가 채용되고 있는 것으로 한다.

우선 최초로 단계 S331에 있어서, DB 액세스 모듈(86)은 마스크 정보가 설정되어 있는지의 여부를 판정한다.

여기서, 마스크 정보는 각 URI의 일부를 마스크하기 위한 정보로서, 예를 들면 유저가 미리 설정할 수가 있다.

또, URI는 예를 들면 스킴명(scheme name), 호스트명, 포트 번호 및 패스명으로 구성된다. 또한, URI에 있어서 포트 번호는 생략할 수가 있다.

포트 번호가 생략된 URI는 예를 들면 "http://aaa.bbb.ccc/ddd"와 같이 기술된다. 이 URI "http://aaa.bbb.ccc/ddd"중 "http"가 스킴명이며, "aaa.bbb.ccc"가 호스트명이며, "ddd"가 패스명이다.

예를 들면, 하나의 서비스 제공자가 복수의 서비스 시스템(24)을 운용하고 있는 경우, 서비스 시스템(24)의 어느것에 대해서도 동일한 PMD의 읽기나 변경을 허가할 때에는, PK(22)에 있어서 이들 서비스 시스템(24)의 서비스 ID를 따로 따로 등록하는 것은 번거롭다(귀찮다). 또, 이 경우, PK(22)에 있어서 이들 서비스 시스템(24) 각각을 구별할 필요도 없다.

한편, 서비스 시스템(24)의 서비스 ID로서 URI를 채용한 경우, 동일한 서비스 제공자가 운용하는 복수의 서비스 시스템(24)의 URI 중 스킴명과 호스트명(예를 들면, "http://aaa.bbb.ccc") 또는 스킴명과 호스트명의 일부(예를 들면, "http://aaa.bbb")는 일반적으로 동일한 것이 채용된다.

이 경우, 동일한 서비스 제공자가 운용하는 복수의 서비스 시스템(24)은 URI중 스킴명과 호스트명 또는 스킴명과 호스트명의 일부에 의해 특정할 수가 있다.

마스크 정보는 동일한 서비스 제공자가 운용하는 복수의 서비스 시스템(24)을 구별하지 않고 특정할 수 있는 URI의 스킴명과 호스트명, 또는 스킴명과 호스트명의 일부를 제외한 부분을 마스크하기 위해서 설정된다.

단계 S331에 있어서, 마스크 정보가 설정되어 있다고 판정된 경우, 단계 S332로 진행하고, DB 액세스 모듈(86)은 도 11의 단계 S101에서 수신한 서비스 ID로서의 URI의 일부를 마스크 정보에 따라 마스크하고, 그 마스크 정보에 의해 마스크된 URI를 서비스 ID로서 PMDB(72)에 등록하고, 단계 S334로 진행한다. 즉, DB 액세스 모듈(86)은 예를 들면 PMDB(72)에, 마스크 정보에 의해서 마스크된 URI를 디렉토리명으로 하는 디렉토리를 생성한다.

또, 단계 S331에 있어서 마스크 정보가 설정되어 있지 않다고 판정된 경우, 단계 S333으로 진행하고, DB 액세스 모듈(86)은 도 11의 단계 S101에서 수신한 서비스 ID로서의 URI를 직접 PMDB(72)에 등록하고, 단계 S334로 진행한다. 즉, DB 액세스 모듈(86)은 도 11의 단계 S101에서 수신한 서비스 ID로서의 URI를 디렉토리명으로 하는 디렉토리를 생성한다.

단계 S334에서는 DB 액세스 모듈(86)은 서비스 시스템(24)이 도 11의 단계 S1에서 송신한 정보에 의해 나타내지는 읽기 변경 대상 메타데이터인 PMD를, 단계 S332 또는 S333에서 생성한 디렉토리에 기억시키고, 서비스 ID 등록 처리를 종료한다.

다음에, 도 15를 참조해서 도 12의 단계 S172 또는 도 13의 단계 S282에서 위장 방지 모듈(84)이 행하는 서비스 ID 매칭 처리의 상세한 것에 대하여 설명한다.

단계 S351에 있어서, 위장 방지 모듈(84)은 PMDB(72)(도 10)에 등록되어 있는 최초의 서비스 ID를 주목 서비스 ID로 하고, 그 주목 서비스 ID와 도 12의 단계 S171 또는 도 13의 단계 S281에서 수신한 서비스 시스템(24)으로부터의 서비스 ID인 (서비스 시스템(24)의) URI를 이들 서비스 ID의 선두의 문자부터 비교하고, 단계 S352로 진행한다.

여기서, 위장 방지 모듈(84)은 DB 액세스 모듈(86)을 거쳐서, PMDB(72)(도 10)에 등록되어 있는 서비스 ID를 취득함을 주목해야 한다.

단계 S352에서는 위장 방지 모듈(84)은 서비스 시스템(24)의 URI와 주목 서비스 ID를 비교한 결과, URI가 그 URI의 선두로부터 주목 서비스 ID와 일치하는 부분을 가지는지 어떤지를 판정한다.

단계 S352에 있어서, 서비스 시스템(24)의 URI가 주목 서비스 ID와 일치하는 부분을 가진다고 판정된 경우, 단계 S353으로 진행하고, 위장 방지 모듈(84)은 주목 서비스 ID를 서비스 시스템(24)을 특정하는 서비스 ID로서 인식하고, 서비스 ID 매칭 처리를 종료한다.

또, 단계 S352에 있어서, 서비스 시스템(24)의 URI가 주목 서비스 ID와 일치하는 부분을 가지고 있지 않다고 판정된 경우, 단계 S354로 진행하고, 위장 방지 모듈(84)은 PMDB(72)에 등록되어 있는 서비스 ID 전체를 주목 서비스 ID로 해서, 서비스 시스템(24)의 URI와 비교했는지 어떤지를 판정한다.

단계 S354에 있어서, PMDB(72)에 등록되어 있는 서비스 ID 전체를 아직 주목 서비스 ID로 하고 있지 않다고 판정된 경우, 단계 S355로 진행하고, 위장 방지 모듈(84)은 PMDB(72)에 등록되어 있는 서비스 ID중 아직 주목 서비스 ID로 하고 있지 않은 것의 1개를 서비스 시스템(24)의 URI와 비교한다. 그리고, 단계 S352로 진행해서, 이하 마찬가지의 처리가 반복된다.

한편, 단계 S354에 있어서, PMDB(72)에 등록되어 있는 서비스 ID 전체를 주목 서비스 ID로 했다고 판정된 경우, 즉 서비스 시스템(24)의 URI와 일치하는 서비스 ID가 PMDB(72)에 등록되어 있지 않은 경우, 단계 S356으로 진행하고, 위장 방지 모듈(84)은 통신 모듈(81)을 거쳐서 서비스 시스템(24)에 대해서 서비스의 제공의 거부를 통지하고, 서비스 ID 매칭 처리를 종료한다.

또한, 상술한 바와 같이, 단계 S356에 있어서 서비스 시스템(24)에 대해서 서비스의 제공의 거부가 통지되고, 도 12의 단계 S172 또는 도 13의 단계 S282의 서비스 ID 매칭 처리가 종료한 경우, 도 12 또는 도 13에서는 이후의 처리는 행해지지 않는다.

다음에, 도 16을 참조해서 PK(22), pBase(23) 및 서비스 시스템(24)에 의한 PMD의 수수(授受)를 설명한다.

PK(22)는 상술한 바와 같이, 서비스 시스템(24)을 액세스 포인트로 해서, 네트워크(21)를 거쳐 pBase(23)와 통신할 수가 있다.

도 16의 맨 위에 도시하는 바와 같이, PK(22)와 pBase(23) 사이에서 통신이 행해지는 것에 의해, PK(22)에 기억되어 있는 PMD와 pBase(23)에 기억되어 있는 PMD를 비교하여, PMD의 동기를 행할 수가 있다. PK(22)의 PMD의 내용이 갱신되고 있는 경우, 이 PMD의 동기에 의하면, pBase(23)의 PMD도 마찬가지로 갱신된다. 또한, PMD의 동기의 상세한 것에 대해서는 후술한다.

또, 예를 들면 pBase(23)에는 PK(22)에 다 기억할 수 없는 PMD를 기억시켜 둘 수가 있다. 이 경우, 도 16의 중앙에 도시하는 바와 같이, 서비스 시스템(24)은 pBase(23)의 PMD를 참조해서, PK(22)의 유저에 대해 서비스를 제공할 수가 있다.

또, 도 16의 맨 밑에 도시하는 바와 같이, pBase(23)와 서비스 시스템(24) 사이에서 네트워크(21)를 거쳐서 통신을 행하는 것에 의해, pBase(23)로부터 서비스 시스템(24)에 대해서 PMD를 제공하고, 제공된 PMD에 따른 서비스를 서비스 시스템(24)으로부터 받을 수도 있다.

다음에, 도 17과 도 18을 참조해서, 도 16의 맨 밑에 도시한 pBase(23)와 서비스 시스템(24) 사이의 처리의 흐름을 설명한다.

또한, 도 17에서는 PK(22)(의 유저)에 기억되어 있는 것과 동일한 PMDB(72)가 pBase(23)에 기억되어 있는 것으로 하고, 또 서비스 시스템(24)과의 사이에서 행해지는 위장 방지 처리로서 도 12에서 설명한 암호에 의한 인증을 이용한 처리가 채용되고 있다.

또, 도 17에서는 pBase(23)는 도 12에서 설명한 PK(22)와 마찬가지로, PK 암호, 서비스 암호, PK(22)의 유저 ID 및 서비스 시스템(24)의 서비스 ID를 기억하고 있는 것으로 한다.

우선 최초로 단계 S371에 있어서, 서비스 시스템(24)은 자신의 서비스 ID와 PK(22)의 유저 ID에 관계하여 기억하고 있는 서비스 암호를 pBase(23)에 송신하고, pBase(23)는 단계 S391에 있어서 서비스 시스템(24)으로부터의 서비스 ID 및 서비스 암호를 수신한다.

여기서, 단계 S371에서는 서비스 시스템(24)은 이미 PK(22) 또는 pBase(23)로부터 PK(22)의 유저 ID를 수신하고 있고, 그 유저 ID에 관련하여 기억하고 있는 서비스 암호를 pBase(23)에 송신한다.

pBase(23)는 단계 S392에 있어서, 단계 S391에서 수신한 서비스 시스템(24)으로부터의 서비스 ID를 이용하여, 도 15를 참조해서 설명한 서비스 ID매칭 처리를 실행하고, 단계 S393으로 진행한다.

단계 S393에서는 pBase(23)는 서비스 시스템(24)으로부터의 서비스 ID에 관련하여 기억하고 있는 서비스 암호 및 PK 암호를 인식하고, 서비스 시스템(24)으로부터 수신된 서비스 암호와 자신이 기억하고 있는 서비스 암호를 비교하는 것에 의해, 그들이 일치하는지 어떤지를 판정한다.

단계 S393에 있어서, 서비스 시스템(24)으로부터의 서비스 암호와 자신이 기억하고 있는 서비스 암호(서비스 시스템(24)으로부터의 서비스 ID에 관련되어 기억하고 있는 서비스 암호)가 일치하지 않는다고 판정된 경우, pBase(23)는 서비스 시스템(24)이 위장일 가능성이 있다고 판정하고, 서비스 시스템(24)에 대해서 통신의 거부를 나타내는 거부 신호를 출력한다.

서비스 시스템(24)은 단계 S372에 있어서, pBase(23)로부터의 거부 신호를 수신한다.

pBase(23)는 이상과 같이, 거부 신호를 서비스 시스템(24)에 송신한 후에는 서비스 시스템(24)으로부터의 액세스를 거부한다. 즉, pBase(23)는 서비스 시스템(24)과의 통신을 거부한다.

한편, 단계 S393에 있어서, 서비스 암호가 일치한다고 판정된 경우, 단계 S394로 진행하고, pBase(23)는 서비스 시스템(24)이 위장이 아니라고 판정하고, PK(22)의 유저 ID와 서비스 시스템(24)의 서비스 ID에 관련하여 기억하고 있는 PK 암호를 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S373에 있어서, pBase(23)로부터의 유저 ID와 PK 암호를 수신하고, 단계 S374로 진행한다. 단계 S374에서는 서비스 시스템(24)은 pBase(23)로부터의 유저 ID에 관련하여 기억하고 있는 PK 암호와 pBase(23)로부터의 PK 암호(단계 S373에서 수신한 PK 암호)를 비교하고, 일치하는지의 여부를 판정한다.

단계 S374에 있어서, PK 암호가 일치하지 않는다고 판정된 경우, pBase(23)가 위장일 가능성이 있다고 판정하여, 서비스 시스템(24)은 통신의 거부를 나타내는 거부 신호를 pBase(23)에 송신한다. pBase(23)는 단계 S395에 있어서, 서비스 시스템(24)으로부터의 거부 신호를 수신한다.

서비스 시스템(24)은 이상과 같이, 거부 신호를 pBase(23)에 송신한 후에는 pBase(23)로부터의 액세스를 거부한다. 즉, 서비스 시스템(24)은 pBase(23)와의 통신을 거부한다.

한편, 단계 S374에 있어서, PK 암호가 일치한다고 판정된 경우, 서비스 시스템(24)은 pBase(23)가 위장이 아님을 판정하고, 단계 S375로 진행하고, pBase(23)에 대해서 PMD의 읽기 요구를 송신한다.

pBase(23)는 단계 S396에 있어서, 서비스 시스템(24)으로부터의 PMD 읽기 요구를 수신하고, 단계 S397로 진행해서, 그 수신된 읽기 요구에 명시되어 있는 PMD를 읽어낸다.

여기서, 단계 S397에서는 pBase(23)는 도 12의 단계 S194에 있어서의 경우와 마찬가지로, 읽기 요구에 명시되어 있는 PMD의 읽기가 허가되고 있는지 어떤지를 판정하고, 읽기 요구에 의해 명시되고 있는 PMD중 읽기가 허가되고 있는 PMD만을 읽어낸다.

그 후, 단계 S398로 진행해서, pBase(23)는 자신으로부터 읽어낸 PMD를 서비스 시스템(24)에 대해서 송신하고, 서비스 시스템(24)은 단계 S376에 있어서 PBase(23)로부터 PMD를 수신하고, 단계 S377로 진행한다.

단계 S377에서는 서비스 시스템(24)은 단계 S376에서 pBase(23)로부터 수신한 PMD에 근거해서 각종 처리 동작(서비스 대응 처리)을 실행한다. 단계 S377의 서비스 대응 처리의 결과, pBase(23)로부터의 PMD의 변경이 필요하게 되는 경우, 서비스 시스템(24)은 단계 S378로 진행해서, pBase(23)로부터의 PMD를 변경하고, 변경된 PMD를 pBase(23)에 대해서 송신한다.

pBase(23)는 단계 S399에 있어서, 서비스 시스템(24)으로부터 변경된 PMD를 수신하고, 단계 S400로 진행해서, 그 PMD의 변경이 허가되고 있는지 어떤지를 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도 10)를 참조하는 것에 의해 확인한다. 또, 단계 S400에서는 pBase(23)는 pBase(23)에 기억하고 있는 PMD 중 서비스 시스템(24)에 의해 변경된 PMD에 대응하는 것 중에서, 그 변경이 허가되고 있는 PMD를 서비스 시스템(24)에 의해 변경된 PMD에 따라 변경하고(갱신하고), 처리를 종료한다.

이상과 같이, pBase(23)에 있어서 서비스 암호를 비교하여, 서비스 시스템(24)의 위장의 확인을 행함과 동시에, 서비스 시스템(24)에 있어서 PK 암호를 비교하여 pBase(23)의 위장의 확인을 행하므로, 안전한 서비스의 제공을 행할 수가 있다.

또한, 상술한 경우에는 pBase(23)에 있어서 서비스 암호의 일치성을 확인하고, 그 후 서비스 시스템(24)에 있어서 PK 암호의 일치성을 확인하도록 했지만, 먼저 서비스 시스템(24)에 있어서 PK 암호의 일치성을 확인하고, 그 후 pBase(23)에 있어서 서비스 암호의 일치성을 확인하는 것도 가능함을 주목해야 한다.

다음에, 도 18을 참조해서, 도 16의 맨 밑에 있어서의 pBase(23)와 서비스 시스템(24) 사이의 처리의 흐름의 다른 예를 설명한다.

도 18에서도 도 17에 있어서의 경우와 마찬가지로, PK(22)에 기억되어 있는 것과 동일한 PMDB(72)가 pBase(23)에 기억되어 있는 것으로 한다.

또, 도 18에서는 서비스 시스템(24)과의 사이에서 행해지는 위장 방지 처리로서 도 13에 있어서의 경우와 마찬가지로 공개키에 의해 암호화된 정보에 의한 인증이 채용되고 있는 것으로 한다.

또, 도 18에서는 pBase(23)와 서비스 시스템(24)이 예를 들면 공개키 방식의 암호 알고리즘에 의한 정보의 암호화 또는 복호의 처리를 실행하는 기능을 가지고 있는 것으로 하고, 따라서 pBase(23)는 PK(22)의 공개키에 대한 비밀키를 기억하고 있으며, 서비스 시스템(24)은 자신의 공개키에 대한 비밀키를 기억하고 있는 것으로 한다. 또, pBase(23)에서는 서비스 시스템(24)의 공개키가 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있고, 서비스 시스템(24)에서도 PK(22)의 공개키가 PK(22)의 유저 ID에 대응시켜 기억되어 있는 것으로 한다.

우선 최초로 단계 S421에 있어서, 서비스 시스템(24)은 자신의 서비스 ID를 pBase(23)에 송신한다. pBase(23)는 단계 S451에 있어서, 서비스 시스템(24)으로부터의 서비스 ID를 수신하고, 단계 S452로 진행해서, 그 수신된 서비스 ID를 이용하여 도 15를 참조해서 설명한 서비스 ID매칭 처리를 실행하고, 단계 S453으로 진행한다.

단계 S453에서는 pBase(23)는 PK(22)의 유저 ID 및 비밀키와 서비스 시스템(24)의 서비스 ID에 대응하는 공개키를 인식하고, 서비스 시스템(24)을 인증하기 위한 챌린지 코드를 생성한다. 또, 단계 S453에서는 pBase(23)는 생성된 챌린지 코드를 서비스 시스템(24)의 공개키로 암호화하고, 그 결과 얻어지는 암호화 챌린지 코드를 유저 ID와 함께 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S422에 있어서, pBase(23)로부터의 암호화 챌린지 코드와 유저 ID를 수신하고, 단계 S423으로 진행한다.

단계 S423에서는 서비스 시스템(24)은 pBase(23)로부터의 암호화 챌린지 코드를 자신의 비밀키에 의해 챌린지 코드로 복호한다. 또, 단계 S423에서는 서비스 시스템(24)은 그 챌린지 코드를 응답 코드로 하고, 그 응답 코드를 단계 S422에서 pBase(23)로부터 수신한 유저 ID와 대응시켜 기억하고 있는 공개키(PK(22)의 공개키)로 암호화하며, 그 결과 얻어지는 암호화 응답 코드를 pBase(23)에 대해서 송신한다.

pBase(23)는 단계 S454에 있어서, 서비스 시스템(24)으로부터의 암호화 응답 코드를 수신하고, 단계 S455로 진행해서, 그 암호화 응답 코드를 PK(22)의 비밀키에 의해 평문 응답 코드로 복호한다. 또, 단계 S455에서는 pBase(23)는 응답 코드와 단계 S453에서 생성한 챌린지 코드를 비교하고, 그 챌린지 코드와 응답 코드가 일치하고 있는지의 여부를 판정한다.

단계 S455에 있어서, 챌린지 코드와 응답 코드가 일치하지 않는다고 판정된 경우, 서비스 시스템(24)이 위장일 가능성이 있다고 판정하여, pBase(23)는 통신의 거부를 나타내는 거부 신호를 서비스 시스템(24)에 송신한다. 그리고, 서비스 시스템(24)은 단계 S424에 있어서, pBase(23)로부터의 거부 신호를 수신한다.

pBase(23)는 이상과 같이, 거부 신호를 서비스 시스템(24)에 송신한 후에는 서비스 시스템(24)으로부터의 액세스를 거부한다. 즉, pBase(23)는 서비스 시스템(24)과의 통신을 거부한다.

한편, 단계 S455에 있어서, 챌린지 코드와 응답 코드가 일치한다고 판정된 경우, 단계 S456으로 진행하고, pBase(23)는 서비스 시스템(24)이 위장이 아닌 것을 확인할 수 있었던 것을 나타내는 OK코드를 서비스 시스템(24)에 송신한다.

서비스 시스템(24)은 단계 S425에 있어서, pBase(23)로부터의 OK 코드를 수신하고, 단계 S426으로 진행해서, pBase(23)를 인증하기 위한 챌린지 코드를 생성한다. 또, 단계 S426에 있어서, 서비스 시스템(24)은 그 생성된 챌린지 코드를 PK(22)의 유저 ID에 관련되어 기억하고 있는 공개키(PK(22)의 공개키)로 암호화하고, 그 결과 얻어지는 암호화 챌린지 코드를 pBase(23)에 대해서 송신한다.

pBase(23)는 단계 S457에 있어서, 서비스 시스템(24)으로부터의 암호화 챌린지 코드를 수신하고, 단계 S458로 진행해서, 그 수신된 암호화 챌린지 코드를 PK(22)의 비밀키에 의해 평문 챌린지 코드로 복호한다. 또, 단계 S458에서는 pBase(23)는 PK(22)의 비밀키에 의한 복호의 결과 얻어진 챌린지 코드를 응답 코드로 하고, 그 응답 코드를 서비스 시스템(24)의 서비스 ID에 대응시켜 기억하고 있는 공개키(서비스 시스템(24)의 공개키)로 암호화하고, 그 결과 얻어지는 암호화 응답 코드를 서비스 시스템(24)에 대해서 송신한다.

서비스 시스템(24)은 단계 S427에 있어서, pBase(23)로부터의 암호화 응답 코드를 수신하고, 그 수신한 암호화 응답 코드를 자신의 비밀키에 의해 복호하고, 단계 S428로 진행한다.

단계 S428에서는 서비스 시스템(24)은 단계 S427에서 복호한 응답 코드와 단계 S426에서 생성한 챌린지 코드를 비교하고, 양자가 일치하는지의 여부를 판정한다.

단계 S428에 있어서, 챌린지 코드와 응답 코드가 일치하지 않는다고 판정된 경우, 서비스 시스템(24)은 pBase(23)가 위장일 가능성이 있다고 판정하여, pBase(23)에 대해서 통신의 거부를 나타내는 거부 신호를 송신한다.

pBase(23)는 단계 S459에 있어서, 서비스 시스템(24)으로부터의 거부 신호를 수신하고, 전술된 처리를 종료한다.

서비스 시스템(24)은 이상과 같이, 거부 신호를 pBase(23)에 송신한 후에는 pBase(23)로부터의 액세스를 거부한다. 즉, 서비스 시스템(24)은 pBase(23)와의 통신을 거부한다.

한편, 단계 S428에 있어서, 챌린지 코드와 응답 코드가 일치한다고 판정된 경우, 즉 pBase(23)와 서비스 시스템(24)에 있어서 상호 인증에 성공한 경우, 서비스 시스템(24)은 pBase(23)가 위장이 아니라고 판정하고, 단계 S429로 진행하고, pBase(23)에 대해서 PMD의 읽기 요구를 송신한다.

pBase(23)는 단계 S460에 있어서, 서비스 시스템(24)으로부터의 PMD 읽기 요구를 수신하고, 단계 S461로 진행해서, 그 수신된 PMD 읽기 요구에 의해 명시되어 PMD를 읽어낸다.

여기서, 단계 S461에서는 pBase(23)는 도 12의 단계 S194에 있어서의 경우와 마찬가지로, 읽기 요구에서 명시된 PMD의 읽기가 허가되고 있는지 어떤지를 판정하고, 읽기 요구에서 명시된 PMD중 읽기가 허가되고 있는 PMD만을 읽어낸다.

그 후, 단계 S462로 진행해서, pBase(23)는 자신으로부터 읽어낸 PMD를 서비스 시스템(24)에 대해서 송신하고, 서비스 시스템(24)은 단계 S430에 있어서 그 PMD를 pBase(23)로부터 수신하고, 단계 S431로 진행한다.

단계 S431에서는 서비스 시스템(24)은 단계 S430에서 pBase(23)로부터 수신한 PMD에 근거해서, 서비스 관련 처리로서의 각종 처리 동작을 실행한다. 단계 S431의 서비스 대응 처리의 결과, pBase(23)로부터의 PMD의 변경이 필요하게 되는 경우, 서비스 시스템(24)은 단계 S432로 진행해서, pBase(23)로부터 수신된 PMD를 변경하고, pBase(23)에 대해서 변경된 PMD를 송신한다.

pBase(23)는 단계 S463에 있어서, 서비스 시스템(24)으로부터의 변경된 PMD를 수신하고, 단계 S464로 진행해서, 그 PMD의 변경이 허가되고 있는지 어떤지를 서비스 시스템(24)의 서비스 ID에 대응하는 디렉토리의 액세스 허가 정보(도

10)를 참조하는 것에 의해 확인한다. 또, 단계 S464에서는 pBase(23)는 자신이 기억하고 있는 PMD 중 서비스 시스템(24)에 의해 변경된 PMD에 대응하는 것 중에서, 그 변경이 허가되고 있는 PMD를 서비스 시스템(24)에 의해 변경된 PMD에 따라 변경하고(갱신하고), 처리를 종료한다.

이상과 같이, pBase(23) 및 서비스 시스템(24)에 있어서, 소위 챌린지&응답 방식에 의한 인증을 행하는 경우에도, 안전한 서비스의 제공을 행할 수가 있다.

또한, 상술한 경우에는 pBase(23)에 있어서 먼저 서비스 시스템(24)의 인증을 행하고, 그 후 서비스 시스템(24)에 있어서 pBase(23)의 인증을 행하도록 했지만, 먼저 서비스 시스템(24)에 있어서 pBase(23)의 인증을 행하고, 그 후 pBase(23)에 있어서 서비스 시스템(24)의 인증을 행하는 것도 가능하다.

또, 상술한 경우에는 공개키 방식으로 챌린지 코드와 응답 코드의 암호화/복호를 행하는 것으로 했지만, 챌린지 코드와 응답 코드의 암호화/복호는 공통키 방식으로 행하는 것도 가능하다.

또, 도 17 또는 도 18에 도시된 예에서, 상호 인증이 성공한 후의 pBase(23)와 서비스 시스템(24) 사이의 통신에서는, 정보는 예를 들면 공개키 방식 등으로 암호화되어 수수된다. 즉, 도 17에 있어서의 단계 S376과 S398의 통신, 및 도 17에 있어서의 단계 S378과 S399의 통신 및, 도 18에 있어서의 단계 S430과 S462의 통신, 및 도 18에 있어서의 단계 S432와 S463의 통신에서는 정보가 암호화되어 수수된다.

다음에, 도 19 내지 도 21에는 PMD의 내용의 예를 도시하고 있다.

각 PMD는 서비스 ID에 관련된 메타데이터의 세트로서, 그 메타데이터의 식별 정보인 프로퍼티(속성)와 그 프로퍼티의 내용(속성값)을 포함하고 있다.

도 19에서는 메타데이터의 속성으로서 "name", "위장 방지 방법", "서비스 공개키", "PK 비밀키", "action" 및 "프로그램 기호 정보"가 마련되어 있다.

도 19의 PMD(메타데이터)가 예를 들면 서비스 ID1에 관련되어있는 경우, 속성 "name"은 서비스 ID1에 대응하는 서비스 시스템(24)에 대해서 제공된 유저 ID를 나타내고, 도 19에서는 그 속성값은 "foo"로 되어 있다.

도 19에 있어서, 속성 "위장 방지 방법"은 서비스 ID1에 대응하는 서비스 시스템(24)과의 사이에서 행해지는 위장 방지 처리의 방법을 나타내고, 그 속성값은 "공개키 방식"으로 되어 있다.

여기서, PK(22)와 예를 들면 서비스 ID1에 대응하는 서비스 시스템(24) 사이에서 도 11의 처리가 행해지고, 단계 S82에 있어서 "공개키 방식"을 나타내는 코드가 확인 코드로서 생성된 경우, 도 19에 도시한 바와 같이, 속성 "위장 방지 방법"의 속성값은 "공개키 방식"으로 된다.

또, 도 19에서는 속성 "위장 방지 방법"의 속성값이 "공개키 방식"으로 되어 있기 때문에, 그 공개키 방식의 암호화/복호에서 이용되는 키를 나타내는 속성 "서비스 공개키" 및 "PK 비밀키"가 PMD에 마련되어 있다.

즉, 속성 "서비스 공개키"는 서비스 ID1에 대응하는 서비스 시스템(24)의 공개키를 나타내고, 도 19에서는 그 속성값으로서 서비스 시스템(24)의 공개키의 데이터가 기술되어 있다.

속성 "PK 비밀키"는 PK(22)의 비밀키를 나타내고, 도 19에서는 그 속성값으로서 PK(22)의 비밀키의 데이터가 기술되어 있다.

속성 "action"는 서비스 ID1에 대응하는 서비스 시스템(24)으로부터의 서비스를 받을 때에 실행되는 프로그램을 나타내고, 그 속성값으로서 프로그램의 실행 형식 파일(명)이 기술된다.

속성 "프로그램 기호 정보"는 서비스 ID1에 대응하는 서비스 시스템(24)으로부터의 서비스를 받을 때에 이용되는 유저의 기호 정보를 나타내고, 도 19에서는 그 속성값으로서 "스포츠 10, 버라이어티 7, 음악 5, 기타 3"이 기술되어 있다.

액세스 허가 정보는 각 속성의 속성값에 대한 액세스 제어를 하기 위한 정보로서, 각 속성에 대해서는 액세스 허가 정보로서 소정의 비트수로 구성되는 제어 코드가 설정되어 있다.

임의의 속성에 주목하면, 그 주목하고 있는 속성(주목 속성)에 대한 제어 코드의 예를 들면 제 1 비트에 의하면, 서비스 ID1에 대응하는 서비스 시스템(24)에 의한 주목 속성의 속성값의 읽기의 가부가 설정된다. 또, 제 2 비트에 의하면, 서비스 ID1에 대응하는 서비스 시스템(24)에 의한 주목 속성의 속성값의 변경의 가부가 설정된다. 또, 제 3 비트에 의하면, 서비스 ID1에 대응하는 서비스 시스템(24) 이외에 다른 서비스 시스템에 의한 주목 속성의 속성값의 읽기의 가부가 설정되고, 제 4 비트에 의하면, 서비스 ID1에 대응하는 서비스 시스템(24) 이외의 다른 서비스 시스템에 의한 주목 속성의 속성값의 변경의 가부가 설정된다.

그밖에, 제어 코드에는 프로그램의 실행의 가부를 설정하는 비트를 마련할 수가 있다.

다음에, 도 20에서는 메타데이터의 속성으로서 "name", "위장 방지 방법", "공통키", "action" 및 "프로그램 기호 정보"가 마련되어 있다. 또, 도 21에서는 메타데이터의 속성으로서 "name", "위장 방지 방법", "서비스 암호", "PK 암호", "action" 및 "프로그램 기호 정보"가 마련되어 있다.

도 20 및 도 21에 있어서, 속성 "name", "action" 및 "프로그램 기호 정보"에 대해서는, 도 19에 있어서의 경우와 동일한 속성값이 기술되어 있다. 또, 도 20 및 도 21에 있어서, 액세스 허가 정보(제어 코드)는 도 19에 있어서의 경우와 마찬가지의 것이다.

그리고, 도 20에서는 속성 "위장 방지 방법"의 속성값이 "공통키 방식"으로 되어 있다. PK(22)와 서비스 ID1에 대응하는 서비스 시스템(24) 사이에서 도 11의 처리가 행해지고, 단계 S82에 있어서 "공통키 방식"을 나타내는 코드가 확인 코드로서 생성된 경우, 도 20에 도시한 바와 같이, 속성 "위장 방지 방법"의 속성값은 "공통키 방식"으로 된다.

또, 도 20에서는 속성 "위장 방지 방법"의 속성값이 "공통키 방식"으로 되어 있기 때문에, 그 공통키 방식의 암호화/복호에서 이용되는 키를 나타내는 속성 "공통키"가 PMD에 마련되어 있다.

즉, 속성 "공통키"는 공통키 방식의 암호화/복호에서 이용되는 공통키(비밀키)를 나타내고, 도 20에서는 그 속성값으로서 그 공통키의 데이터가 기술되어 있다.

한편, 도 21에서는 속성 "위장 방지 방법"의 속성값이 "암호 방식"으로 되어 있다. PK(22)와 예를 들면 서비스 ID1에 대응하는 서비스 시스템(24) 사이에서 도 11의 처리가 행해지고, 단계 S82에 있어서 "암호 방식"을 나타내는 코드가 확인 코드로서 생성된 경우, 도 21에 도시한 바와 같이, 속성 "위장 방지 방법"의 속성값은 "암호 방식"으로 된다.

또, 도 21에서는 속성 "위장 방지 방법"의 속성값이 "암호 방식"으로 되어 있기 때문에, 그 암호 방식에서의 인증에 이용되는 암호를 나타내는 속성 "서비스 암호" 및 "PK 암호"가 PMD에 마련되어 있다.

그리고, 도 21에서는 속성 "서비스 암호"의 속성값으로서 상술한 서비스 암호의 데이터가 기술되어 있고, 속성 "PK 암호"의 속성값으로서 상술한 PK 암호의 데이터가 기술되어 있다.

다음에, 도 22를 참조해서 PMD를 갱신하는 PMD 갱신 처리에 대해 설명한다.

도 22의 PMD 갱신 처리는 예를 들면 서비스 시스템(24)에 의해, 컨텐츠의 시청 서비스가 제공된 경우, 도 12의 단계 S127 또는 도 13의 단계 S221의 서비스 대응 처리의 하나로서 서비스 시스템(24)에 의해 실행된다.

또한, 여기에서는 서비스 시스템(24)으로부터 컨텐츠의 시청 서비스를 받은 유저의 PK(22)에, 예를 들면 도 19 내지 도 21에 도시한 바와 같은 "프로그램 기호 정보"를 포함하는 PMD가 기억되어 있고, 그 "프로그램 기호 정보"(의 속성값)가 PK(22)로부터 서비스 시스템(24)에 대해서 이미 제공되고 있는 것으로 한다.

단계 S481에 있어서, 서비스 시스템(24)(의 CPU(51)(도 9))은 유저가 시청(유저에게 제공)한 프로그램(컨텐츠)의 메타데이터를 취득하고, 단계 S482로 진행한다. 단계 S482에 있어서, 서비스 시스템(24)은 단계 S481에서 취득한 메타데이터로부터 유저가 시청한 프로그램의 장르를 분석하고, 단계 S483으로 진행한다.

단계 S483에 있어서, 서비스 시스템(24)은 단계 S482에서의 분석에 의해 얻어진 장르가 스포츠인지의 여부를 판정한다. 단계 S483에 있어서 장르가 스포츠라고 판정된 경우, 단계 S484로 진행하고, 서비스 시스템(24)은 PMD중의 속성 "프로

그램 기호 정보"(도 19 내지 도 21)의 속성값에 있어서의 스포츠의 포인트를 증가시키고, 처리를 종료한다. 예를 들면, 도 19 내지 도 21에 있어서 "스포츠 10, 버라이어티 7, 음악 5, 기타 3"으로 되어 있던 것이, "스포츠 11, 버라이어티 7, 음악 5, 기타 3"으로 된다.

또, 단계 S483에 있어서, 단계 S482에서의 분석에 의해 얻어진 장르가 스포츠가 아니라고 판정된 경우, 서비스 시스템(24)은 단계 S485로 진행해서, 장르가 버라이어티인지의 여부를 판정한다.

단계 S485에 있어서 장르가 버라이어티라고 판정된 경우, 단계 S486으로 진행하고, 서비스 시스템(24)은 버라이어티의 포인트를 증가시키고, 처리를 종료한다. 예를 들면, 도 19 내지 도 21에 있어서 "스포츠 10, 버라이어티 7, 음악 5, 기타 3"으로 되어 있던 것이, "스포츠 10, 버라이어티 8, 음악 5, 기타 3"으로 된다.

한편, 단계 S485에 있어서, 단계 S482에서의 분석에 의해 얻어진 장르가 버라이어티가 아니라고 판정된 경우, 서비스 시스템(24)은 단계 S487로 진행해서, 장르가 음악인지의 여부를 판정한다.

단계 S487에 있어서, 장르가 음악이라고 판정된 경우, 단계 S488로 진행하고, 서비스 시스템(24)은 PMD중의 속성 "프로그램 기호 정보"의 속성값에 있어서의 음악의 포인트를 증가시키고, 처리를 종료한다. 예를 들면, 도 19 내지 도 21에 있어서 "스포츠 10, 버라이어티 7, 음악 5, 기타 3"으로 되어 있던 것이, "스포츠 10, 버라이어티 7, 음악 6, 기타 3"으로 된다.

단계 S487에 있어서, 단계 S482에서 얻어진 장르가 음악이 아니라고 판정된 경우, 서비스 시스템(24)은 단계 S489로 진행해서, PMD중의 속성 "프로그램 기호 정보"의 속성값에 있어서의 기타 포인트를 증가시키고, 처리를 종료한다. 예를 들면, 도 19 내지 도 21에 있어서 "스포츠 10, 버라이어티 7, 음악 5, 기타 3"으로 되어 있던 것이, "스포츠 10, 버라이어티 7, 음악 5, 기타 4"로 된다.

이와 같이 해서, 서비스 시스템(24)에 있어서 PMD가 갱신된다. 갱신된 PMD는 PK(22)에 송신되어, PK(22)의 PMD가 갱신된다.

다음에, PK(22)에 의하면, PMD를 이용하여 특정한 정보 기기에 그 PK(22)의 유저에 대응하는 처리를 실행시킬 수 있다. 이와 같이, 정보 기기가 그 유저용으로 퍼스널라이즈(personalize)되었다고 할 수 있다.

도 23에는 정보 처리 기기 중 하나인 PC(Personal Computer)를 퍼스널라이즈하는 PK 시스템의 구성예를 도시하고 있다. 도 23을 참조하면, 또한, 도면중 도 7에 있어서의 경우와 대응하는 부분에 대해서는 동일한 부호를 붙이고 있다.

도 23에 있어서, 공공 PC(101)는 예를 들면 소위 인터넷 카페나 도서관 등의 공공의 장소, 회사의 회의실 등에 설치되어 있는 PC이며, 네트워크(21)에 접속되어 있다. 또한, 공공 PC(101)는 도 7의 서비스 시스템(24)이기도 하며, 준정전계 통신을 행할 수가 있음을 주목해야 한다.

또, 도 23에 있어서, 유저 PC(102)는 예를 들면 PK(22)의 유저의 자택이나 회사에 있는 그 유저 전용의 PC(유저가 소유하는 PC)이며, 공공 PC(101)와 마찬가지로 네트워크(21)에 접속되어 있다.

여기서, 유저는 예를 들면 자택에서 사용하는 유저 PC(102)에 대해서는 일반적으로 자신이 사용하기 쉽게 동작 환경 설정을 행한다. 한편, 공공 PC(101)에는 일반적으로 유저 PC(102)와는 다른 환경 설정이 행해져 있다. 따라서, 종래에 있어서는 유저는 외출지 등에 설치되어 있는 공공 PC(101)를, 유저 PC(102)에 있어서의 환경(예를 들면, 유저 PC(102)의 데스크탑의 표시 상태나 디렉토리 구성)과 동일한 동작 환경에서 사용할 수 없다.

그래서, 도 23의 PK 시스템에서는 유저가 공공 PC(101)를, 유저 PC(102)에 있어서의 환경과 동일한 동작 환경에서 사용할 수 있도록 되어 있다.

즉, 서비스 시스템인 공공 PC(101)를 유저가 사용하는 경우, PK 시스템은 그 공공 PC(101)를 PK(22)의 유저용으로 퍼스널라이즈 하는 퍼스널라이즈 처리를 행한다.

도 24는 서비스 시스템인 공공 PC(101)가 행하는 퍼스널라이즈 처리의 예를 도시하는 흐름도이다.

도 24의 퍼스널라이즈 처리는 예를 들면 PK(22)를 휴대하는 유저가 공공 PC(101)를 사용하고자 하면 행해진다.

즉, PK(22)와 공공 PC(101)는 상술한 바와 같이, 준정전계 통신을 행할 수 있도록 되어 있다. 그리고, 공공 PC(101)의 최근방 위치(예를 들면, 공공 PC(101)가 놓여 있는 테이블이나 바로 아래의 마루(바닥) 부분, 공공 PC(101)의 하우징 등)에, 공공 PC(101)가 준정전계 통신을 행하기 위한 안테나가 마련되어 있으며, 따라서 유저가 공공 PC(101)를 사용하고자 해서, 공공 PC(101)에 근접하여 그 안테나에 대해서 접촉하거나 혹은 근접한 상태로 되면, 유저가 휴대하고 있는 PK(22)와 공공 PC(101) 사이에서는 유저의 인체 및 공공 PC(101)의 안테나를 거쳐서 준정전계 통신이 가능해진다.

공공 PC(101)는 PK(22)와의 사이에서 준정전계 통신이 가능해지면, 단계 S501에 있어서 PK(22)로부터 PMD를 취득한다. 즉, 공공 PC(101)는 준정전계 통신에 의해서 PK(22)에 대해서 PMD를 요구하고, PK(22)는 요구된 PMD를 준정전계 통신에 의해서 공공 PC(101)에 송신한다. 이것에 의해, 공공 PC(101)는 PK(22)로부터 PMD를 취득한다.

여기서, PK(22)에는 유저 PC(102)에 있어서의 동작 환경을 나타내는 동작 환경 데이터가 PMD로서 기억되어 있고, 단계 S501에 있어서 공공 PC(101)는 이 PMD를 취득하는 것으로 한다.

공공 PC(101)는 단계 S501에 있어서, PK(22)로부터 동작 환경 데이터인 PMD를 취득한 후 단계 S502로 진행해서, 그 취득한 동작 환경 데이터에 따라 자신의 환경 설정을 행한다. 즉, 이것에 의해, 공공 PC(101)는 PK(22)의 유저용으로 퍼스널라이즈되고, PK(22)의 유저는 공공 PC(101)를 자신이 소유하는 유저 PC(102)에 있어서의 환경과 동일한 환경에서 사용할 수가 있다.

그 후, PK(22)의 유저가 공공 PC(101)를 조작하고, 예를 들면 유저가 워드 프로세서의 어플리케이션으로 작성한 데이터 파일을 여는(오픈하는) 것을 요구하면, 공공 PC(101)는 단계 S503으로 진행해서, 여는 것이 요구된 데이터 파일을 유저 PC(102)로부터 취득한다.

즉, 단계 S503에서는 공공 PC(101)는 네트워크(21)를 거쳐서 유저 PC에 액세스하고, 여는 것이 요구된 데이터 파일을 다운로드한다. 그리고, 공공 PC(101)는 그 데이터 파일을 열어 표시 동작을 행한다.

그 후, PK(22)의 유저가 공공 PC(101)를 조작하여, 단계 S503에서 취득된 데이터 파일을 편집, 갱신하며, 그 갱신된 데이터 파일을 닫는(클로우즈하는) 것을 요구하면, 공공 PC(101)는 단계 S504로 진행해서, 갱신된 데이터 파일을 네트워크(21)를 거쳐서 유저 PC(102)에 전송하고 기억시킨다.

그리고, PK(22)의 유저가 공공 PC(101)를 조작해서 로그 오프를 요구하면, 단계 S505로 진행하고, 공공 PC(101)는 현재의 자신에 있어서의 동작 환경을 나타내는 동작 환경 데이터를 준정전계 통신에 의해서 PK(22)에 송신한다.

여기서, PK(22)의 유저가 공공 PC(101)를 사용하기 시작할 때는, 단계 S502에서 설명한 바와 같이 공공 PC(101)는 유저 PC(102)에 있어서의 환경과 동일한 환경으로 되어 있지만, 그 후 유저가 공공 PC(101)를 사용함으로써 초기 동작 환경과는 다른 환경으로 되는 경우가 있다. 이 경우, 공공 PC(101)에 있어서의 동작 환경은 PK(22)에 기억되어 있는 동작 환경 데이터에 따라 설정되는 환경과 다르기 때문에, 단계 S505에서는 공공 PC(101)는 PK(22)에 기억되어 있는 동작 환경 데이터를 갱신하기 위해서, 현재의 자신에 있어서의 동작 환경을 나타내는 동작 환경 데이터를 준정전계 통신에 의해서 PK(22)에 송신한다.

이 경우, PK(22)는 공공 PC(101)로부터의 환경 데이터를 수신하고, 그 수신된 동작 환경 데이터에 의해서 자신이 기억하고 있는 PMD로서의 동작 환경 데이터를 갱신한다.

공공 PC(101)는 단계 S505에 있어서, 동작 환경 데이터를 PK(22)에 송신한 후에는 단계 S506로 진행해서, 그 동작 환경 데이터나 단계 S501에서 취득한 동작 환경 데이터, 유저 PC(102)로부터 다운로드한 데이터 파일 등을 삭제하고, 도 24의 퍼스널라이즈 처리가 개시되기 전의 상태로 되어, 단계 S507로 진행한다.

단계 S507에서는 공공 PC(101)는 로그 오프 시퀀스를 행하고, 퍼스널라이즈 처리를 종료한다.

이상과 같이, 도 24의 퍼스널라이즈 처리에 의하면, 공공 PC(101)가 유저 PC(102)에 있어서의 환경과 동일한 동작 환경으로 퍼스널라이즈되므로, 유저는 유저 PC(102)와 동일한 동작 환경에서 공공 PC(101)를 사용할 수가 있다.

또, 공공 PC(101)를 퍼스널라이즈하기 위해서는, PK(22)와 공공 PC(101) 사이에서 통신을 행할 필요가 있지만, PK(22)를 휴대하는 유저는 의식적으로 PK(22)와 공공 PC(101)를 통신시키는 바와 같은 행위, 즉 예를 들면 PK(22)를 포켓 등으로부터 꺼내어, 공공 PC(101)의 안테나를 향해 꽂는 바와 같은 행위를 행하지 않아도 좋다.

즉, PK(22)와 공공 PC(101) 사이의 준정전계 통신은 상술한 바와 같이, PK(22)를 휴대하고 있는 유저가 공공 PC(101)의 안테나에 대해서 접촉하거나 혹은 근접한 상태로 되면, 유저의 인체 및 공공 PC(101)의 안테나를 거쳐서 행하는 것이 가능해진다.

따라서, PK(22)를 휴대하고 있는 유저는 단지 공공 PC(101)를 사용할 용도로 공공 PC(101) 앞에 앉거나, 혹은 공공 PC(101)의 키보드나 마우스에 접촉하면된다. 이것에 의해 PK(22)와 공공 PC(101) 사이에서 통신이 행해지고, 공공 PC(101)가 퍼스널라이즈된다.

또한, PK(22)와 서비스 시스템인 공공 PC(101) 사이의 통신, 및 네트워크(21)를 거친 공공 PC(101)와 유저 PC(102)와의 통신은 모두, 예를 들면 SSL(Secure Sockets Layer)을 이용하는 것에 의해서 안전하게(확실하게) 행해진다.

다음에, 도 23의 PK 시스템에 있어서 예를 들면 유저의 PK(22)와 pBase(23)에 동일한 PMD가 기억되어 있었다고 해도, 도 24의 퍼스널라이즈 처리가 행해진 경우, 공공 PC(101)가 단계 S505에 있어서 PK(22)에 송신하는 PMD에 의해서 PMD(22)가 기억하고 있는 PMD가 갱신되면, PK(22)와 pBase(23)에 기억되어 있는 PMD는 다른 것으로 된다.

그래서, PK(22)와 pBase(23) 사이에서는 pBase(23)에 기억되어 있는 PMD를 PK(22)에 기억되어 있는 PMD에 일치시키기 위해서, 도 16에서 개략적으로 설명한 PMD의 동기 처리가 행해진다.

도 25는 PK(22)와 pBase(23) 사이에서 행해지는 PMD의 동기의 처리를 설명하는 화살표도이다.

이 PMD의 동기의 처리는 PK(22)가 공공 PC(101) 등의 서비스 시스템 및 네트워크(21)를 거쳐서, pBase(23)와의 사이에서 통신을 행할 수 있는 경우에 행해진다.

또한, 여기서는 PK(22)가 서비스 시스템인 공공 PC(101)와의 사이에서 준정전계 통신이 가능한 상태에 있는 것으로 한다.

단계 S521에 있어서, PK(22)는 자신이 기억하고 있는 PMD를 공공 PC(101)에 송신하고, 공공 PC(101)는 단계 S541에 있어서 PK(22)로부터의 PMD를 수신한다.

그리고, 단계 S542로 진행해서, 공공 PC(101)는 단계 S541에서 수신한 PMD를 네트워크(21)를 거쳐서 pBase(23)에 송신하고, pBase(23)는 단계 S561에서 공공 PC(101)로부터의 PMD를 수신하고, 단계 S562로 진행한다.

단계 S562에서는 pBase(23)는 도 26을 참조해서 후술하는 PMD 동기 처리를 실행한다. 이것에 의해, pBase(23)에 기억되어 있는 PMD가 갱신됨과 동시에, PK(22)에 기억된 PMD를 갱신하는 동기 데이터가 생성된다.

그리고, pBase(23)는 단계 S563으로 진행해서, 단계 S562의 동기 처리에 의해 생성한 동기 데이터를 네트워크(21)를 거쳐서 공공 PC(101)에 송신하고, 공공 PC(101)는 단계 S543에서 pBase(23)로부터의 동기 데이터를 수신하고, 단계 S544로 진행한다.

단계 S544에 있어서, 공공 PC(101)는 단계 S543에서 수신한 동기 데이터를 PK(22)에 송신하고, PK(22)는 단계 S522에서 공공 PC(101)로부터의 동기 데이터를 수신하고, 단계 S523으로 진행한다.

단계 S523에 있어서, PK(22)는 단계 S522에서 수신한 동기 데이터에 근거해서 자신의 PMD를 갱신하고, 동기 처리를 종료한다.

다음에, 도 26을 참조해서 도 25의 단계 S562의 PMD 동기 처리의 상세한 것에 대하여 설명한다.

단계 S581에 있어서, pBase(23)는 도 25의 단계 S561에서 수신한 PK(22)로부터 수신한 PMD와 pBase(23)에 기억되어 있는 PMD를 비교한다. 즉, 단계 S581에 있어서, pBase(23)는 PK(22)로부터 수신한 PMD의 속성의 속성값 중 아직 주목

속성값으로 선택되지 않은 것을 주목 속성값으로 선택한다. 또, 단계 S581에서는 pBase(23)는 자신이 기억하고 있는 PMD중에서 주목 속성값에 대응하는 속성값을 읽어내고(리드하고), 그 판독된 속성값이 마지막에 갱신된 시간을 나타내는 갱신 시간 정보와 주목 속성값의 갱신 시간 정보를 비교한다.

여기서, PMD에는 갱신 시간 정보가 포함되는 것으로 한다.

그리고, 단계 S581에서 S582로 진행하고, pBase(23)는 단계 S581의 비교 결과에 근거해서 주목 속성값의 갱신 시간이 그 주목 속성값에 대응하는 속성값(이하, 적절히 대응 속성값이라고 함)의 갱신 시간보다 새로운지의 여부를 판정한다.

단계 S582에 있어서, 주목 속성값의 갱신 시간이 pBase(23)에 기억되어 있는 대응 속성값의 갱신 시간보다 새롭다고 판정된 경우, 단계 S583으로 진행하고, pBase(23)는 자신이 기억하고 있는 대응 속성값을 주목 속성값으로 갱신하고, 단계 S585로 진행한다.

또, 단계 S582에 있어서, 주목 속성값의 갱신 시간이 대응 속성값의 갱신 시간보다 새롭지 않다고 판정된 경우, 단계 S584로 진행하고, pBase(23)는 대응 속성값을 동기 데이터로 하고, 단계 S585로 진행한다.

여기서, 동기 데이터는 도 26에 도시된 PMD 동기 처리의 종료후, 도 25에 도시된 단계 S563에서 공공 PC(101)를 거쳐서 PK(22)에 송신된다. 그리고, PK(22)에서는 도 25의 단계 S523에 있어서 동기 데이터에 따라 자신이 기억하고 있는 PMD가 갱신된다.

또한, 여기에서는 주목 속성값의 갱신 시간보다 새로운 갱신 시간으로 되어 있는 대응 속성값 이외에, 주목 속성값의 갱신 시간과 동일한 갱신 시간의 대응 속성값도 동기 데이터로 되게 되지만, 주목 속성값의 갱신 시간보다 새로운 갱신 시간의 대응 속성값만으로 동기 데이터로서 처리된다.

단계 S585에서는 pBase(23)는 PK(22)로부터 수신된 PMD의 모든 속성값의 갱신 시간을 주목 속성값으로 체크했는지 어떤지를 판정한다.

단계 S585에 있어서, 임의의 속성값이 아직 주목 속성값으로 하고 있지 않다고 판정된 경우, 단계 S581로 되돌아가서, 이하 마찬가지의 처리가 반복된다.

또, 단계 S585에 있어서, PK(22)로부터 수신된 PMD의 속성값 전체를 주목 속성값으로 했다고 판정된 경우, PMD 동기 처리를 종료한다.

다음에, 도 27에는 도 7 및 도 23에 도시한 PK시스템을 이용한 서비스 제공 시스템의 일실시예의 구성예를 도시하고 있다. 도 27을 참조하여, 도면중 도 7 및 도 23을 참조하여 전술된 바와 유사한 부분은 동일한 부호를 붙이고 있다.

도 27에 있어서, 서비스 시스템(24)은 PK(22)를 휴대하고 있는 유저에 대해서, 그 유저용으로 퍼스널라이즈된 정보를 제공한다.

즉, 서비스 시스템(24)에는 안테나(121) 및 출력장치(122)가 접속되어 있다.

안테나(121)는 준정전계 통신용의 안테나인 도체 시트이며, 그 근방에는 준정전계가 형성되어 있다. PK(22)와 서비스 시스템(24)은 PK(22)를 휴대하는 유저의 인체의 표면에 형성되는 준정전계 또는 안테나(121)의 근방에 형성되는 준정전계의 범위 내에 있어서, 준정전계 통신을 행할 수가 있다.

또한, 안테나(121)는 예를 들면 마루 등에 설치할 수가 있다.

또, 여기서는 유저의 인체 주위에 형성되는 준정전계와 안테나(121)의 근방에 형성되는 준정전계는 그 두께(상술한 강도 경계 거리 r)가 미소한 것으로 한다. 즉, PK(22)와 서비스 시스템(24)은 PK(22)를 휴대하는 유저의 인체의 일부가 안테나(121)에 접촉하거나 또는 그것에 매우 가까운 상태로 되었을 때에만, 준정전계 통신이 가능해지는 것으로 한다.

이 경우, PK(22)와 서비스 시스템(24)이 준정전계 통신을 행할 수 있는 상태일 때는, 그 PK(22)를 휴대하는 유저는 안테나(121)의 위치에 있다고 특정할 수가 있다.

출력장치(122)는 예를 들면 디스플레이 장치나 스피커로 구성되고, 서비스 시스템(24)으로부터 공급되는 정보를 화상으로 표시하거나 또는 음성으로 출력한다.

도 27에 있어서, 서비스 시스템(24)은 기능적으로는 유저 정보 취득 모듈(131), 최적화 엔진(132), 컨텐츠 DB(Data Base)(133) 및 유저 DB(134)로 구성되어 있다.

유저 정보 취득 모듈(131)은 안테나(121) 및 PK(22)를 휴대하는 유저의 인체를 거쳐서 준정전계 통신을 행하는 것에 의해, PK(22)로부터 송신되어 오는 PMD를 수신하고, 또 PK(22)에 대해서 후술하는 컨텐츠 DB로부터 취득된 정보를 송신한다.

최적화 엔진(132)은 유저 정보 취득 모듈(131)이 PK(22)로부터 수신한 PMD에 따라, 컨텐츠 DB(133)에 기억되어 있는 컨텐츠(정보)중에서 PK(22)의 유저에게 제공하는데 최적한 것을 인식한다.

컨텐츠 DB(133)는 PK(22)의 유저의 서비스 시스템(24)의 외부에 제공하는 여러가지 컨텐츠를 기억하고 있다. 또, 컨텐츠 DB(133)는 자신이 기억하고 있는 컨텐츠의 메타데이터인 컨텐츠 메타데이터도 기억하고 있다.

유저 DB(134)는 상술한 PK(22)의 유저의 유저 ID, 서비스 암호, PK 암호, 공개키 방식의 암호화/복호에서 이용되는 비밀키 및 공개키, 공통키 방식의 암호화/복호에서 이용되는 공통키와 같은, PK(22)와의 사이의 통신에 필요한 데이터를 기억한다. 여기서, 유저 DB(134)의 기억 정보의 갱신은 예를 들면 유저 정보 취득 모듈(131)에 의해 행해진다.

또한, 컨텐츠 DB(133) 및 유저 DB(134)는 서비스 시스템(24)에 마련하는 것이 아니라, 서비스 시스템(24)과는 독립적으로 네트워크(21)상에 있어도 좋다는 점을 주목해야 한다.

다음에, 도 28을 참조해서, PK(22)와 서비스 시스템(24)에서 행해지는 처리에 대해 설명한다.

단계 S641에 있어서, 유저 정보 취득 모듈(131)은 안테나(121)를 거쳐서 일정 간격으로 자신의 서비스 ID(서비스 시스템(24)이 제공하는 서비스를 특정하는 정보인 서비스 ID)로서의 URI를 준정전계 통신에 의해 송신하고 있다.

또한, 이 URI의 송신은 예를 들면 IP(Internet Protocol) 프로토콜을 이용한 브로드캐스트에 의해 행할 수가 있다는 점을 주목해야 한다.

그리고, PK(22)를 소지한 유저가 예를 들면 안테나(121) 위를 통과하거나 또는 안테나(121) 위에 서면, PK(22)와 서비스 시스템(24)은 안테나(121) 및 PK(22)의 유저의 인체를 거쳐서 준정전계 통신을 행하는 것이 가능해지고, 이것에 의해 단계 S661에 있어서 PK(22)는 서비스 시스템(24)의 유저 정보 취득 모듈(131)이 안테나(121)를 거쳐서 송신하고 있는 URI를 수신하고, 단계 S662로 진행한다.

단계 S662에서는 PK(22)는 서비스 시스템(24)으로부터 수신한 URI인 서비스 ID가 PMDB(72)(도 10)에 등록되어 있는지 어떤지를 판정한다.

단계 S662에 있어서, 서비스 시스템(24)으로부터 수신한 URI인 서비스 ID가 PMDB(72)에 등록되어 있지 않다고 판정된 경우, PK(22)는 서비스 시스템(24)으로부터의 서비스의 제공을 거부하는 것을 나타내는 거부 신호를 준정전계 통신에 의해서 송신한다.

PK(22)가 송신한 거부 신호는 단계 S642에 있어서, 안테나(121)를 거쳐서 유저 정보 취득 모듈(131)에서 수신된다.

거부 신호가 수신된다면, 서비스 시스템(24)은 PK(22)에 대해서 서비스를 제공하지 않는다.

한편, 단계 S662에 있어서, 서비스 시스템(24)으로부터 수신한 URI인 서비스 ID가 PMDB(72)에 등록되어 있다고 판정된 경우, 단계 S663로 진행하고, PK(22)는 그 서비스 ID와 관계되어 기억하고 있는 상술한 PK 암호와 유저 ID를 준정전계 통신에 의해서 송신한다.

또한, 이 PK 암호와 유저 ID의 송신은 예를 들면 IP 기반 싱글캐스트에 의해, 타겟으로 하는 서비스 시스템(24)에 대해서 행해진다는 점을 주목해야 한다. PK(22)에 있어서 행해지는 그 이후의 통신도 마찬가지이다.

또, 서비스 시스템(24)에 있어서 행해지는 그 이후의 통신도 마찬가지로, IP 기반 한 싱글캐스트에 의해, 타겟으로 하는 PK(22)에 대해서 행해진다.

PK(22)가 송신한 PK 암호 및 유저 ID는 단계 S643에 있어서, 안테나(121)를 거쳐서 유저 정보 취득 모듈(131)에 의해 수신된다.

그리고, 유저 정보 취득 모듈(131)은 단계 S644로 진행해서, PK(22)로부터 수신한 유저 ID에 관련하여 기억되어 있는 PK 암호를 유저 DB(134)로부터 읽어내고, 그 읽어낸 PK 암호와 PK(22)로부터 수신된 PK 암호가 일치하는지 어떤지를 판정한다.

단계 S644에 있어서, PK(22)로부터 수신된 유저 ID에 관련되어 기억되어 있는 PK 암호와 PK(22)로부터 수신된 PK 암호가 일치하지 않는다고 판정된 경우, 즉 PK(22)가 위장일 가능성이 있음을 지시하고, 유저 정보 취득 모듈(131)은 처리를 종료한다.

이 경우, 서비스 시스템(24)은 PK(22)에 대해서 서비스를 제공하지 않는다.

한편, 단계 S644에 있어서, PK(22)로부터 수신된 유저 ID에 관련되어 기억되어 있는 PK 암호와 PK(22)로부터 수신된 PK 암호가 일치한다고 판정된 경우, 유저 정보 취득 모듈(131)은 PK(22)로부터 수신된 유저 ID에 관련되어 기억되어 있는 서비스 암호를 유저 DB(134)로부터 읽어내고, 이 서비스 암호를 안테나(121)를 거쳐서 준정전계 통신에 의해서 송신한다.

서비스 시스템(24)(의 유저 정보 취득 모듈(131))이 송신한 서비스 암호는 단계 S664에 있어서 PK(22)에 의해 수신된다.

그리고, PK(22)는 단계 S665로 진행해서, 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있는 서비스 암호를 PMDB(72)(도 10)로부터 읽어내고, 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있는 서비스 암호와 서비스 시스템(24)으로부터 수신된 서비스 암호가 일치하는지 어떤지를 판정한다.

단계 S665에 있어서, 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있는 서비스 암호와 서비스 시스템(24)으로부터 수신된 서비스 암호가 일치하지 않는다고 판정된 경우, 서비스 시스템(24)이 위장일 가능성이 있음을 지시하고, PK(22)는 서비스 시스템(24)으로부터의 서비스의 제공을 거부하는 것을 나타내는 거부 신호를 준정전계 통신에 의해서 송신한다.

PK(22)가 송신한 거부 신호는 단계 S645에 있어서, 안테나(121)를 거쳐서 유저 정보 취득 모듈(131)에 의해 수신된다.

이 경우, 서비스 시스템(24)은 PK(22)에 대해서 서비스를 제공하지 않는다.

한편, 단계 S665에 있어서, 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있는 서비스 암호와 서비스 시스템(24)으로부터 수신된 서비스 암호가 일치한다고 판정된 경우, 즉 PK(22)와 서비스 시스템(24) 사이에서 상호 인증에 성공함을 지시하고, 단계 S666로 진행하고, PK(22)는 PMDB(72)로부터 서비스 시스템(24)의 서비스 ID에 관련되어 기억되어 있는 PMD중 읽기가 허가되고 있는 것, 즉 서비스 시스템(24)에 대해서 제공하는 것이 허가되고 있는 PMD(허가 정보)를 읽어내고, PMD를 준정전계 통신에 의해서 서비스 시스템(24)에 송신한다.

또한, PK(22)와 서비스 시스템(24) 사이에서 상호 인증에 성공한 후의 PK(22)와 서비스 시스템(24) 사이의 통신은 예를 들면 SSL을 이용하는 것에 의해서, 안전하게 행해진다는 점을 주목해야 한다.

PK(22)가 송신한 PMD는 단계 S646에 있어서, 안테나(121)를 거쳐서 유저 정보 취득 모듈(131)에 의해 수신된다. 그리고, 유저 정보 취득 모듈(131)은 단계 S647로 진행해서, PK(22)로부터 수신된 PMD를 최적화 엔진(132)에 전송하고, 최적화 엔진(132)은 단계 S622에 있어서 그 PMD를 수신한다.

또, 유저 정보 취득 모듈(131)은 단계 S648에 있어서, 예를 들면 PK(22)와의 사이의 준정전계 통신을 행하는데 사용되고 있는 안테나(121)의 설치 위치를, PK(22)를 휴대하고 있는 유저가 있는 위치(유저 위치)로서 인식하고, 그 유저 위치를 최적화 엔진(132)에 전송한다. 최적화 엔진(132)은 단계 S623에 있어서, 유저 정보 취득 모듈(131)로부터의 유저 위치를 수신한다.

한편, 컨텐츠 DB(133)는 단계 S601에 있어서, 자신이 기억하고 있는 컨텐츠 메타데이터를 최적화 엔진(132)에 공급하고, 최적화 엔진(132)은 단계 S621에 있어서 컨텐츠 DB(133)로부터 메타데이터를 수신하고, 그 수신된 메타데이터에 의해 컨텐츠 DB(133)에 기억되어 있는 컨텐츠(의 내용 등)를 인식한다.

그리고, 최적화 엔진(132)은 단계 S624에 있어서, PK(22)로부터의 PMD와 PK(22)를 휴대하고 있는 유저의 유저 위치에 따라, PK(22)를 휴대하고 있는 유저에 대해서 제공하는 것이 최적한 컨텐츠를 단계 S621에서 인식한 컨텐츠 중에서 특정(인식)하고, 그 컨텐츠를 요구하는 리퀘스트 신호를 컨텐츠 DB(133)에 공급한다.

컨텐츠 DB(133)는 단계 S602에 있어서, 최적화 엔진(132)으로부터의 리퀘스트 신호를 수신하고, 단계 S603으로 진행한다.

단계 S603에서는 컨텐츠 DB(133)는 자신이 기억하고 있는 컨텐츠중에서, 최적화 엔진(132)으로부터 수신된 리퀘스트 신호에 의해서 요구되고 있는 컨텐츠를 검색(선택)하고, 그 컨텐츠(이하, 적절히 '최적 컨텐츠'라고 함)를 출력장치(122)에 공급한다.

출력장치(122)는 단계 S631에 있어서, 컨텐츠 DB(133)로부터의 최적 컨텐츠를 수신하고, 예컨대, 수신된 컨텐츠를 디스플레이한다.

또한, 도 28에서는 위장 방지 처리로서 암호 방식을 이용한 처리를 행하도록 했지만, 위장 방지 처리는 그밖에 상술한 공개키 방식이나 공통키 방식을 이용한 처리여도 좋다.

단, 위장 방지 처리를 행하는 것은 본 발명에서 필수는 아님을 주목해야 한다. 즉, PK(22)를 휴대하는 유저측 혹은 서비스 시스템(24)을 제공하는 서비스 제공자측중의 한쪽 또는 양쪽이 불요하다고 인정하는 경우에는, 위장 방지 처리는 스킵할(건너뛸) 수가 있다. 구체적으로는, 예를 들면 PK(22)를 휴대하는 유저의 성별이 남자 또는 여자이다와 같은 공개하는 PMD가 유저의 정보로서 그다지 중요하지 않은 것인 경우에는 위장 방지의 요청은 낮다. 따라서, 이러한 경우에는 위장 방지 처리를 스킵해도 문제는 없다. 또 위장 방지 처리가 스킵되면, 전체 시스템의 처리 시간은 단축될 수 있다.

또, 도 28에서는 서비스 시스템(24)에 대해서 PK(22)로부터 유저의 PMD를 제공하도록 했지만, 유저의 PMD는 그밖에 예를 들면 pBase(23)(도 27)로부터 제공하는 것도 가능하다. 즉, 예를 들면 PK(22)에서는 서비스 시스템(24)에 대해 PMD로서 pBase(23)의 URI를 제공하도록 하고, 서비스 시스템(24)에서는 PK(22)로부터의 PMD가 URI였던 경우에는 수신된 URI가 나타내는 pBase(23)에 대해 네트워크(21)를 거쳐서 액세스하고, 그 pBase(23)로부터 PK(22)의 유저의 PMD를 취득하도록 할 수가 있다. 이 경우, pBase(23)와 서비스 시스템(24) 사이의 통신은 안전하게 행하는 것이 바람직하다.

또, 도 28에서는 단계 S603에 있어서 컨텐츠 DB(133)로부터 출력장치(122)에 대해서 최적 컨텐츠를 공급하도록 했지만, 단계 S603에서는 도 28에 있어서 점선으로 나타내는 바와 같이, 컨텐츠 DB(133)는 최적 컨텐츠를 안테나(121)를 거쳐서 준정전계 통신에 의해서 PK(22)에 송신할 수가 있다.

그리고, 이 경우, PK(22)에서는 단계 S667에 있어서, 최적 컨텐츠를 수신해서 수신된 최적 컨텐츠를 출력(디스플레이)하거나 또는 기억할 수가 있다.

다음에, 도 29의 흐름도를 참조해서, 도 27의 서비스 시스템(24)의 처리에 대해 더욱더 설명한다.

서비스 시스템(24)에서는 PK(22)와의 사이에서 상호 인증이 성공하면, 단계 S681에 있어서 유저 정보 취득 모듈(131)은 PK(22)로부터 준정전계 통신에 의해서 송신되어 오는 PMD를 수신하고, 수신된 PMD를 최적화 엔진(132)에 전송하며, 단계 S682로 진행한다.

단계 S682에서는 유저 정보 취득 모듈(131)은 PK(22)를 휴대하고 있는 유저가 있는 유저 위치를 취득하고, 최적화 엔진(132)에 전송하며, 단계 S683으로 진행한다.

단계 S683에서는 최적화 엔진(132)은 유저 정보 취득 모듈(131)로부터 수신된 PMD와 유저 위치에 따라, PK(22)를 휴대하고 있는 유저에 대해서 제공하는 것이 최적한 최적 컨텐츠를 특정하고, 컨텐츠 DB(133)에 자신이 기억하고 있는 컨텐츠 중에서 최적 컨텐츠를 선택시키는 것에 의해 취득시키고, 단계 S684로 진행한다.

단계 S684에서는 컨텐츠 DB(133)는 최적 컨텐츠를 출력장치(122)에 공급해서 출력시키거나, 또는 안테나(121)를 거쳐서 준정전계 통신에 의해서 송신하는 것에 의해, PK(22)로 출력하고 처리를 종료한다.

다음에, 도 30에 도시된 흐름도를 참조해서, 도 27에 도시된 PK(22)의 처리에 대해 더욱더 설명한다.

PK(22)는 서비스 시스템(24)과의 사이에서 상호 인증이 성공하면, 단계 S701에 있어서 PMDB(72)(도 10)에 기억되어 있는 PMD중 서비스 시스템(24)에 대해서 제공하는 것(읽기)이 허가되고 있는 PMD를 읽어내고, 단계 S702로 진행한다.

단계 S702에서는 PK(22)는 단계 S701에서 취득한 PMD를 준정전계 통신에 의해서 서비스 시스템(24)에 송신한다.

그 후, 서비스 시스템(24)으로부터 최적 컨텐츠가 준정전계 통신에 의해서 송신되어 온 경우에는, PK(22)는 단계 S703으로 진행해서, 그 최적 컨텐츠를 수신하고, 단계 S704로 진행한다.

단계 S704에서는 PK(22)는 단계 S703에서 수신한 최적 컨텐츠를 기억하거나 또는 화상 또는 음성 등으로 출력하며, 처리를 종료한다.

이상과 같이, 도 27의 서비스 제공 시스템에 의하면, PK(22)에 있어서 PMDB(72)(도 10)에 기억되어 있는 PMD중 서비스 시스템(24)에 대해서 제공하는 것이 유저에 의해서 허가된 PMD만을, 유저의 인체와 안테나(121) 사이의 거리에 의해 제어되는 준정전계 통신에 의해서 서비스 시스템(24)에 송신한다. 한편, 서비스 시스템(24)에 있어서, 유저에게 제공하는 최적 컨텐츠가 PK(22)로부터 수신된 PMD에 따라 컨텐츠 DB(133)에서 선택되고 검색된 최적 컨텐츠가 유저에게 제공된다. 따라서, 유저에 대해서 최적한 정보를 확실하게 제공하는 것 등이 가능하다.

즉, RF 통신과 같이 멀티 패스가 생기는 통신에서는, 유저 위치를 특정하기 위한 구조는 복잡하게 되고, 각 서비스 시스템이 설치되는 환경에 있어서, 유저 위치를 특정하기 위한 기기 설정이나 캘리브레이션이 필요해진다.

이것에 대해서, 도 27에 도시된 서비스 제공 시스템에서는 준정전계 통신을 채용하고 있으므로, 유저를 검출하기 위한 위치에 안테나(121)로서의 도체 시트를 설치하는 것만으로, 유저 위치를 간단하고 또한 정확하게 특정할 수 있고, 그 유저 위치에 있는(서 있는) 유저에 대해서 최적한 정보를 확실하게 제공하는 것이 가능해진다.

또, PK(22)로부터 서비스 시스템(24)에 대해서는 유저가 허가한 PMD만이 제공되고, 서비스 시스템(24)은 그 PMD에 따라 유저에게 정보를 제공하므로, 유저는 상시 시스템에 의해 감시받고 있는 바와 같은 인상을 받지 않고 서비스를 받을 수가 있다.

또, 예를 들면 과금 처리를 행하는 서비스 시스템에 대해서만, 유저의 크레디트 카드의 번호나 은행 계좌의 계좌 번호 등의 PMD를 제공하는 것을 허가함으로써, 과금 처리를 수행하지 않는 서비스 시스템에 그와 같은 PMD가 누설되는 것을 방지할 수가 있다.

또, 유저 위치를 정확하게 파악할 수 있으므로, 예를 들면 출력장치(122)의 화면에 있어서 유저 위치에 가까운 부분에 그 유저에 대한 최적 컨텐츠를 디스플레이하는 것이 가능해진다.

또, 안테나(121)는 1개에 한정되지 않고, 복수 설치할 수가 있다. 안테나(121)를 복수 개소에 설치한 경우에는 복수의 유저 위치는 동시에 특정할 수 있다. 이러한 구성으로 인해 예를 들면 출력장치(122)의 화면에 있어서 복수의 유저 위치 각각에 가까운 부분에, 그 유저 위치에 있는 유저에 대한 최적 컨텐츠를 동시에 표시하는 것이 가능해진다.

이상과 같은 서비스 제공 시스템(도 27)은 예를 들면 공공의 장소에 놓여진 정보 제시(디스플레이 출력, 음성 출력을 기초한 정보의 전달 또는 디지털 정보의 전달) 시스템에 적용할 수가 있다. 이 경우, 정보 제시 시스템에서는 누구나 균일한 정보 제시를 행하는 것이 아니라, 유저마다 그 유저에게 적합한 정보 제시를 행할 수가 있다.

정보 제시는 공공의 장소에 있는 디스플레이나 스피커, 유저의 PDA(Personal Digital Assistant) 등의 단말을 이용해서 행할 수가 있다.

또, 정보 제시는 유저가 정보 제시 시스템으로부터 일정한 거리에 있는지 어떤지에 따라 행할 수도 있고, 또 유저가 어느 곳(위치나 영역)에 있는지에 따라 행할 수도 있다.

유저와 정보 제시 시스템과의 거리에 따른 정보 제시에 있어서는, 예를 들면 정보로서의 컨텐츠의 디테일(detail)의 정도나, 문자의 크기, 문장의 요약의 정도, 음성 신호의 크기를 필요에 따라 변화시킬 수가 있다.

또, 정보 제시는 유저가 소지하고 있는 PK(22) 및 그밖의 장치에 대해서 정보를 전송함으로써 행할 수도 있다. 이 경우, 유저가 소지하고 있는 각 장치에서는 정보의 디스플레이의 최적화나 음성 출력되는 정보의 내용의 최적화를 행하는 것이 가능하다.

또, 유저는 정보 제시 시스템에 대해서 적절한 PMD를 제공하는 것에 의해, 가는 곳마다 자신에게 의미가 있는 정보 제시를 받을 수가 있다.

즉, PMD로서는 예를 들면 도 19 내지 도 21에 도시한 프로그램 기호 정보 및 그밖의 유저 기호 정보, 유저의 스케줄 정보, 성별, 국적, 연령, 신체의 장해 정보, 건강 데이터, 흥미가 있는 대상을 나타내는 키워드 및 그밖의 것을 채용할 수 있으며, 이러한 PMD를 PK(22)로부터 정보 제시 시스템에 제공할 수가 있다.

정보 제시 시스템은 PK(22)로부터 예를 들면 유저의 국적 정보가 제공된 경우, 그 유저의 모국어로 정보를 제시할 수가 있다.

또, 정보 제시 시스템은 PK(22)로부터 예를 들면 유저가 시각 장해를 가지는 것을 나타내는 정보가 제공된 경우, 정보를 음성 출력에 의해서 제시할 수가 있다.

또, 정보 제시 시스템은 PK(22)로부터 예를 들면 스케줄 정보가 제공된 경우, 그 수신된 스케줄 정보로부터 유저가 지금부터 가고자 하는 행선지를 인식하고, 그 행선지를 안내하는 메시지의 제시를 행할 수가 있다. 이러한 메시지의 제시는 예를 들면 빌딩 등의 비교적 대규모 건물 내에서의 특정 장소로의 유도나, 역 구내에서의 전철의 환승지로의 유도에 이용할 수가 있다.

또, 정보 제시 시스템은 PK(22)로부터 예를 들면 키워드가 제공된 경우, 그 제공된 키워드가 나타내는 정보를 제시할 수가 있다. 구체적으로는, 제공된 키워드가 브랜드명인 경우, 정보 제시 시스템은 그 브랜드와 관련된 상품 정보를 제시할 수가 있다.

이 경우, 유저는 예를 들면 좋아하는 브랜드의 상품 정보를 모르는 사이에 수집할 수가 있다.

즉, 유저는 예를 들면 백화점에서 윈도우쇼핑을 행하는 경우, 디스플레이윈도우에 근접해서 디스플레이 윈도우에 진열된 상품을 자세히 보려고 한다. 따라서, 유저가 디스플레이윈도우에 근접했을 때에, 준정전계 통신을 행하는 것이 가능하도록 정보 제시 시스템을 설치해 둠과 동시에, PK(22)로부터 정보 제시 시스템에 대해서 유저가 좋아하는 브랜드의 브랜드명을 제공하도록 함으로써, 정보 제시 시스템은 디스플레이윈도우에 진열되어 있는 상품중 유저가 좋아하는 브랜드의 상품의 상품 정보를 제시할 수가 있다. 이 경우, PK(22)에 있어서, 정보 제시 시스템이 제시하는 상품 정보를 데이터로서 기억해 두도록 함으로써, 유저는 윈도우쇼핑을 하고 있는 동안에 좋아하는 브랜드의 상품 정보만을 수집할 수가 있다.

또한, 본 실시의 형태에서는 PK(22)와 서비스 시스템(24) 사이에서 준정전계 통신을 행한다. PK(22)와 서비스 시스템(24) 사이에서 그 밖의 통신을 행하는 것도 가능하다. 단, 인체 근방에서 통신을 수행하는 것이 바람직하다.

또, 본 발명의 전술된 실시예에서는, 유저가 PK(22)를 휴대하는 것으로 하고, 그 PK(22)를 이용해서 서비스 시스템(24)으로부터 서비스의 제공을 받는다. 유저는 PK(22)의 기능과 동일한 기능을 갖는다면 임의의 디바이스를 휴대할 수 있다. 즉, 유저가 휴대하는 장치는 예를 들면 PK(22)의 기능을 가지는 휴대 전화기 등이라도 좋다.

여기서, 본 명세서에 있어서, 컴퓨터에 각종 처리를 실행시키기 위한 프로그램을 기술하는 처리 단계는 반드시 플로차트로서 기재된 순서에 따라 시계열적으로 처리할 필요는 없고, 병렬적 혹은 개별적으로 실행되는 처리(예를 들면, 병렬 처리 혹은 오브젝트에 의한 처리)도 포함하는 것이다.

또, 본 발명에 따른 프로그램은 1개의 컴퓨터에 의해 처리되는 것이어도 좋고, 복수의 컴퓨터에 의해서 분산 처리되는 것이어도 좋다. 또, 본 발명에 따른 프로그램은 먼 곳의 컴퓨터에 전송되어 실행되는 것이어도 좋다. 설명된 본 발명에 따라, 사용자에게 최적인 정보는 확실히 사용자에게 제공된다.

본 발명의 바람직한 실시예는 특정한 용어를 사용하여 기술되었지만, 이러한 설명은 단지 예시적인 용도이며, 다음의 청구항의 사상과 범주에서 벗어나지 않고 변경 및 변형이 있을 수 있음을 이해해야 한다.

발명의 효과

본 발명에 의하면, 유저에 대해서 최적한 정보를 확실하게 제공하는 것 등이 가능해진다.

(57) 청구의 범위

청구항 1.

제1과 제2 정보 처리 장치를 포함하는 정보 처리 시스템에 있어서,

상기 제1 정보 처리 장치는

유저에 관련된 개인 관련 정보를 기억하는 개인 관련 정보 기억 수단과,

상기 개인 관련 정보중의 상기 제2 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단과,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보를 상기 제2 정보 처리 장치에 송신하는 송신 수단을 포함하고,

상기 제2 정보 처리 장치는

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 제1 정보 처리 장치로부터 송신되어 오는 상기 허가 정보를 수신하는 수신 수단과,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 수단과,

상기 정보 취득 수단에 의해 취득된 정보를 상기 유저에게 제공하는 제공 수단을 포함하는, 정보 처리 시스템.

청구항 2.

다른 장치와 통신을 행하는 정보 처리 장치에 있어서,

유저에 관련된 정보인 개인 관련 정보를 기억하는 개인 관련 정보 기억 수단과,

상기 개인 관련 정보중의 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 수단과,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보를 상기 다른 장치에 송신하는 송신 수단과,

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보에 따라 상기 다른 장치로부터 상기 허가 정보를 수신하는 수신 수단을 포함하는, 정보 처리 장치.

청구항 3.

제 2항에 있어서,

상기 수신 수단에 의해 수신된 상기 정보를 출력하는 출력 수단을 더 포함하는, 정보 처리 장치.

청구항 4.

제 2항에 있어서,

상기 다른 장치와의 사이에서 인증을 행하는 인증 수단을 더 구비하고,

상기 인증이 성공한 경우에, 상기 허가 정보가 상기 다른 장치에 송신되는, 정보 처리 장치.

청구항 5.

제 2항에 있어서,

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 상기 통신은 준정전계 통신인, 정보 처리 장치.

청구항 6.

다른 장치와 통신을 행하는 정보 처리 방법에 있어서,

개인 관련 정보 기억 수단에 기억되어 있는 개인 관련 정보중의, 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보를 상기 다른 장치에 송신하는 송신 단계와,

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 상기 통신에 의해서, 상기 다른 장치로부터의 상기 허가 정보에 상기 허가 정보를 수신하는 수신 단계를 포함하는, 정보 처리 방법.

청구항 7.

프로그램에 있어서,

다른 장치와 통신을 행하는 컴퓨터로 하여금,

개인 관련 정보 기억 수단에 기억되어 있는 개인 관련 정보중의 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와,

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보를 상기 다른 장치에 송신시키는 송신 단계와,

상기 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보에 따라 상기 다른 장치로부터 상기 허가 정보를 수신시키는 수신 단계를 수행하도록 하는, 프로그램.

청구항 8.

다른 장치와 통신을 행하는 컴퓨터에 의해 실행될 프로그램이 기록되어 있는 기록 매체에 있어서, 상기 프로그램은,

개인 관련 정보 기억 수단에 기억되어 있는 개인 관련 정보중의, 상기 다른 장치에 대해서 제공하는 것이 허가된 허가 정보를 취득하는 허가 정보 취득 단계와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보를 상기 다른 장치에 송신시키는 송신 단계와,

상기 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 허가 정보에 따라 상기 다른 장치로부터 상기 허가 정보를 수신하는 수신 단계를 포함하는, 기록 매체.

청구항 9.

다른 장치와 통신을 행하는 정보 처리 장치에 있어서,

상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 정보인 개인 관련 정보중의 상기 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 수단과,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 수단과,

상기 정보 취득 수단에 의해 취득된 정보를 상기 유저에게 제공하는 제공 수단을 포함하는, 정보 처리 장치.

청구항 10.

제 9항에 있어서,

상기 제공 수단은 상기 정보 취득 수단에 의해 취득된 정보를, 출력장치에서 출력하는 것에 의해, 상기 유저에게 제공하는, 정보 처리 장치.

청구항 11.

제 9항에 있어서,

상기 제공 수단은 상기 정보 취득 수단에 의해 취득된 정보를, 상기 다른 장치에 송신하는 것에 의해, 상기 유저에게 제공하는, 정보 처리 장치.

청구항 12.

제 9항에 있어서,

상기 유저가 존재하는 위치인 유저 위치를 취득하는 유저 위치 취득 수단을 더 구비하고,

상기 정보 취득 수단은 상기 유저에게 제공할 정보를 상기 유저 위치에 따라서도 취득하는, 정보 처리 장치.

청구항 13.

제 9항에 있어서,

상기 다른 장치와의 사이에서 인증을 행하는 인증 수단을 더 구비하고,

상기 인증이 성공한 경우에, 상기 정보 취득 수단에 의해 취득된 상기 정보가 상기 유저에게 제공되는, 정보 처리 장치.

청구항 14.

제 9항에 있어서,

상기 다른 장치의 유저의 인체와 상기 안테나 사이의 거리에 의해 제어되는 통신은 준정전계 통신인, 정보 처리 장치.

청구항 15.

다른 장치와 통신을 행하는 정보 처리 방법에 있어서,

상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 개인 관련 정보중의 상기 정보 처리 장치에 대해서 제공하는 것이 허가된 허가 정보를 수신하는 수신 단계와,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 단계와,

상기 정보 취득 단계에 의해 취득된 상기 정보를 상기 유저에게 제공하는 제공 단계를 포함하는 것을 특징으로 하는 정보 처리 방법.

청구항 16.

프로그램으로서,

다른 장치와 통신을 행하는 컴퓨터로 하여금,

상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 개인 관련 정보중의 상기 컴퓨터에 대해서 제공하는 것이 허가된 허가 정보를 수신시키는 수신 단계와,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 단계와,

상기 정보 취득 단계에 의해 취득된 정보를 상기 유저에게 제공하는 제공 단계를 포함하는 것을 특징으로 하는 프로그램.

청구항 17.

다른 장치와 통신을 행하는 컴퓨터에 의해 실행되는 프로그램이 기록되어 있는 기록 매체에 있어서,

상기 프로그램은,

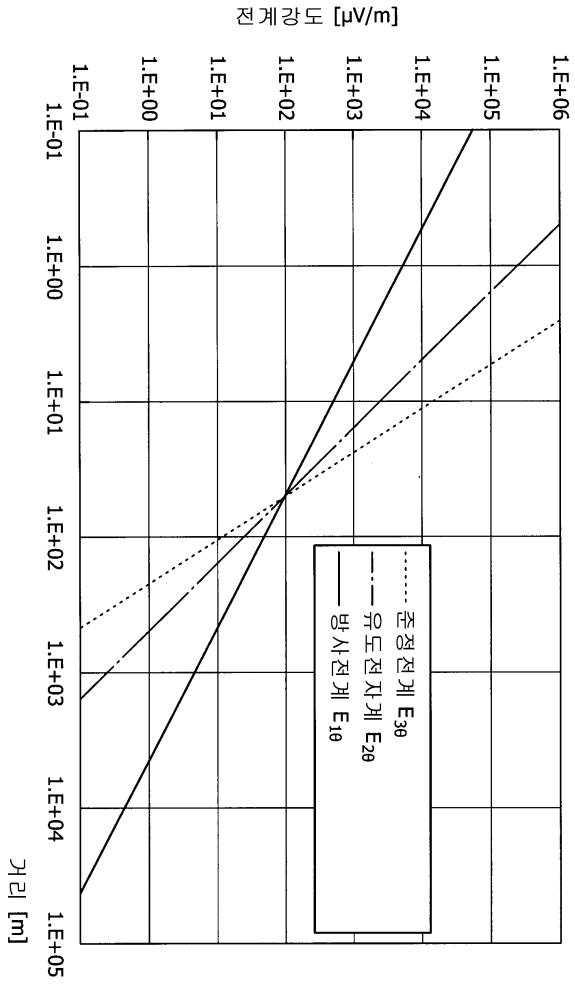
상기 다른 장치의 유저의 인체와 안테나 사이의 거리에 의해 제어되는 통신에 의해서, 상기 다른 장치로부터 송신되어 오는 상기 유저에 관련된 개인 관련 정보중의 상기 컴퓨터에 대해서 제공하는 것이 허가된 허가 정보를 수신시키는 수신 단계와,

외부에 제공할 정보중에서 상기 유저에게 제공할 정보를 상기 허가 정보에 따라 취득하는 정보 취득 단계와,

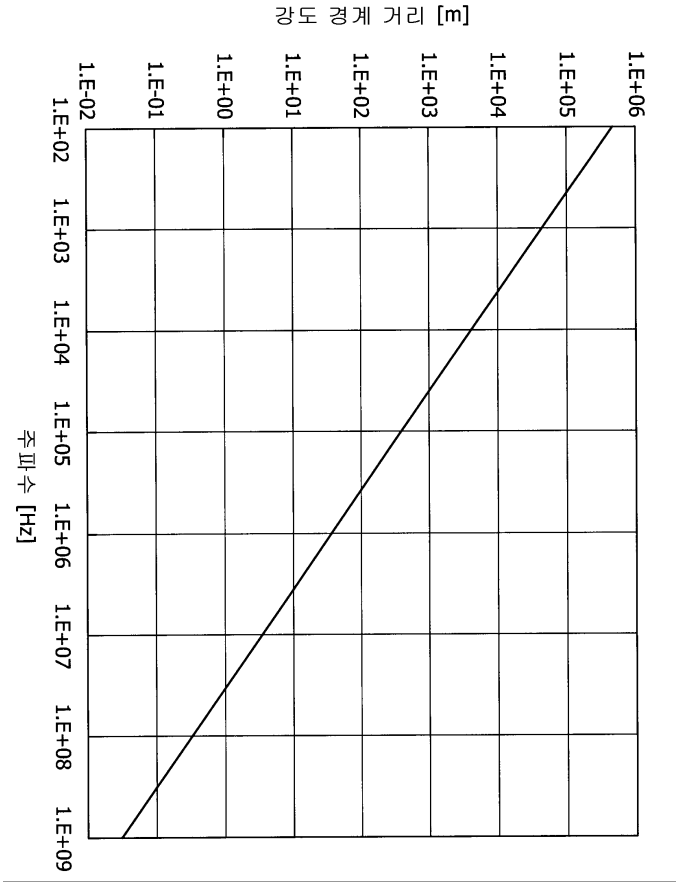
상기 정보 취득 단계에 의해 취득된 정보를 상기 유저에게 제공하는 제공 단계를 포함하는, 기록 매체.

도면

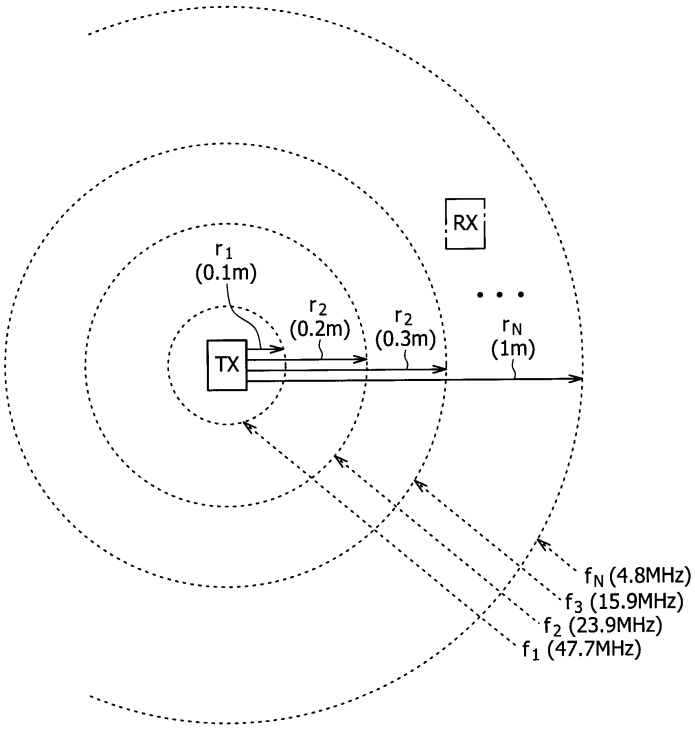
도면1



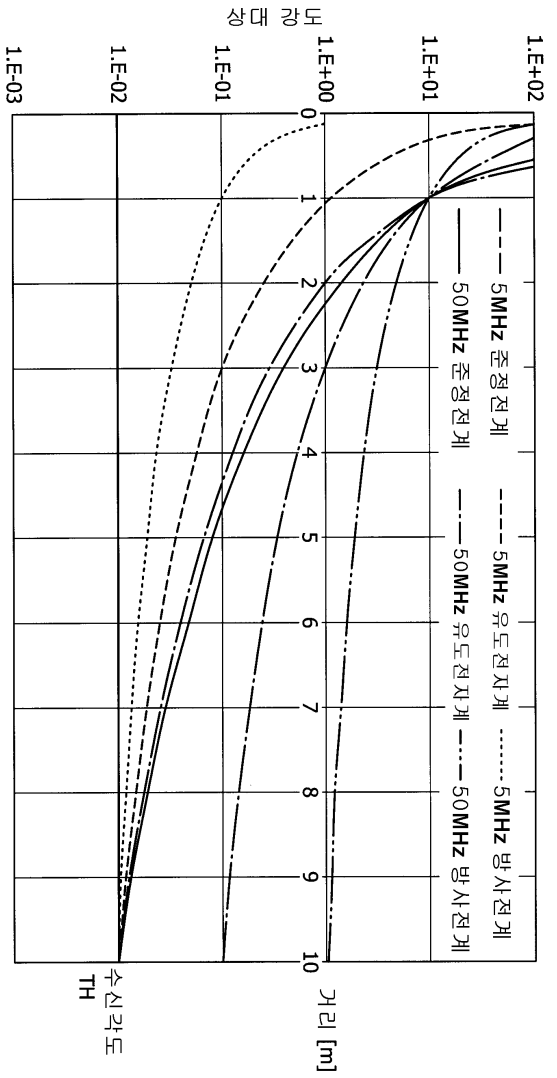
도면2


강도 경계 거리 [m]
1.E-02
1.E-01
1.E+00
1.E+01
1.E+02
1.E+03
1.E+04
1.E+05
1.E+06
주파수 [Hz]
1.E+02
1.E+03
1.E+04
1.E+05
1.E+06
1.E+07
1.E+08
1.E+09

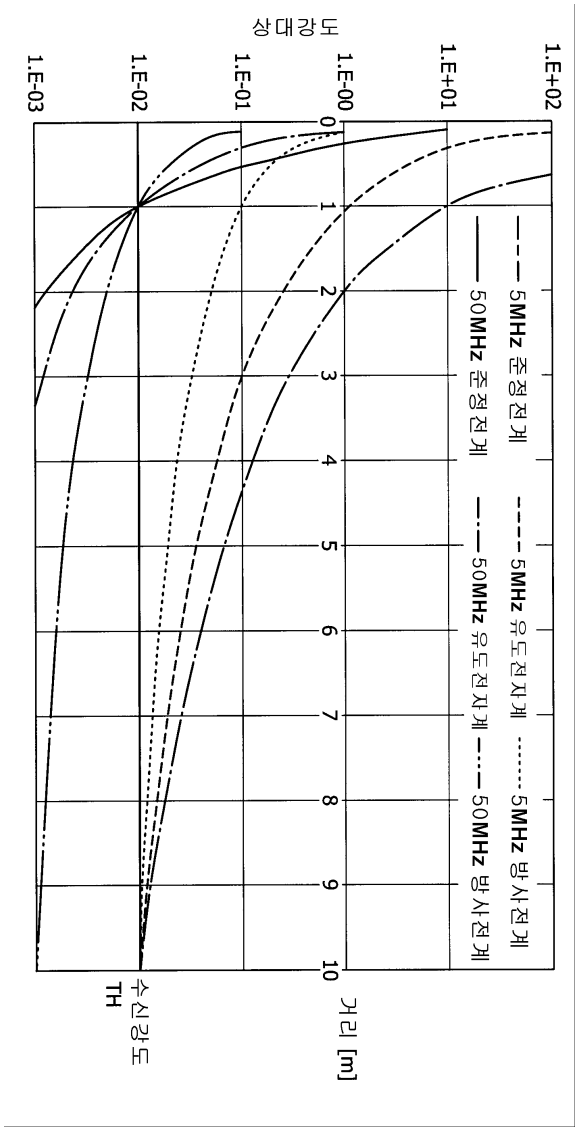
도면3


RX
TX
r1 (0.1m)
r2 (0.2m)
r2 (0.3m)
rN (1m)
fN (4.8MHz)
f3 (15.9MHz)
f2 (23.9MHz)
f1 (47.7MHz)

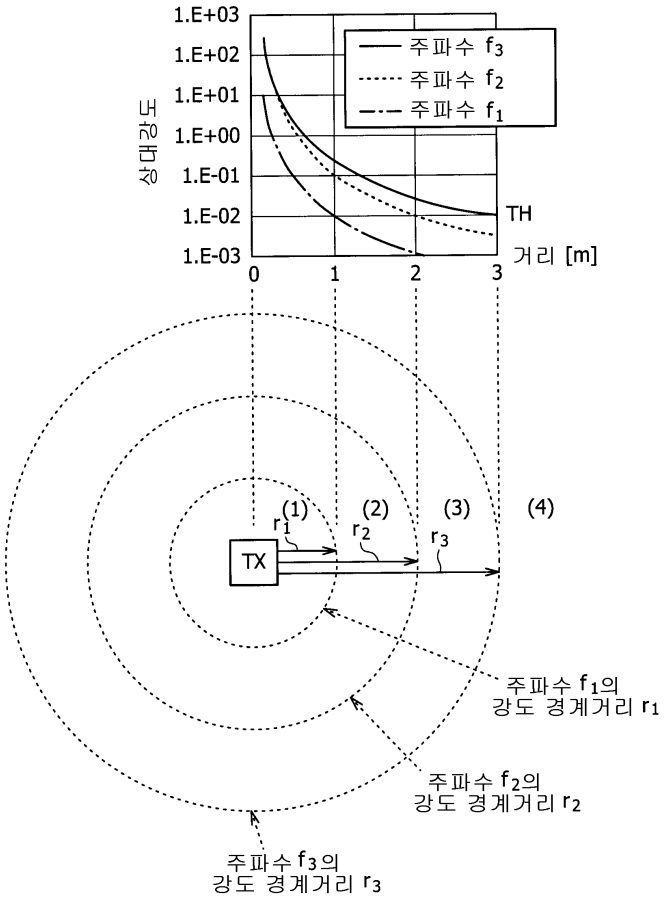
도면4


상대 강도
1.E+02
1.E+01
1.E+00
1.E-01
1.E-02
1.E-03
0
1
2
3
4
5
6
7
8
9
10
거리 [m]
수신각도
TH
5MHz 준정전계
5MHz 유도전자계
5MHz 방사전계
50MHz 준정전계
50MHz 유도전자계
50MHz 방사전계

도면5

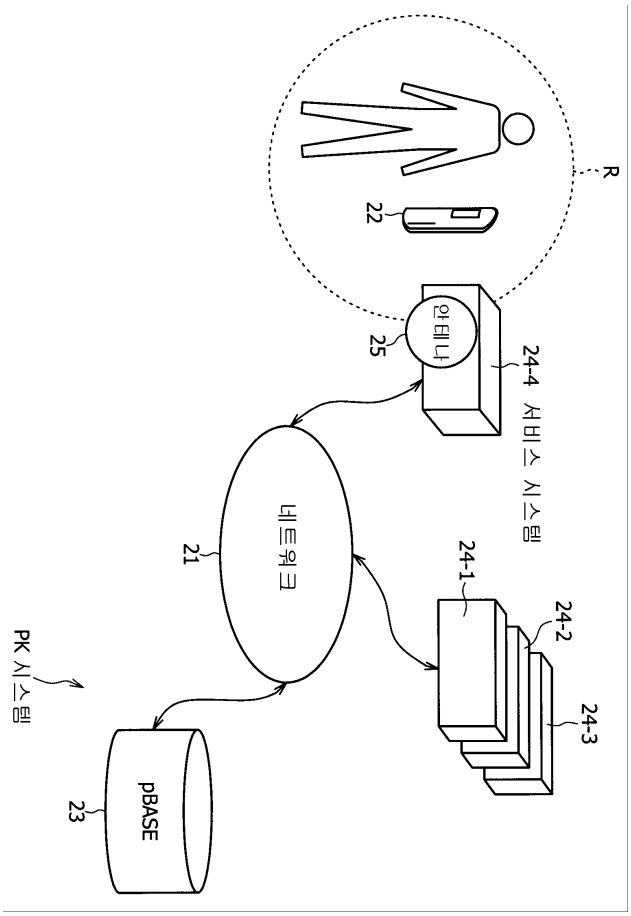

상대강도
1.E+02
1.E+01
1.E-00
1.E-01
1.E-02
1.E-03
0
1
2
3
4
5
6
7
8
9
10
거리 [m]
수신강도 TH
5MHz 준정전계
5MHz 유도전자계
5MHz 방사전계
50MHz 준정전계
50MHz 유도전자계
50MHz 방사전계

도면6

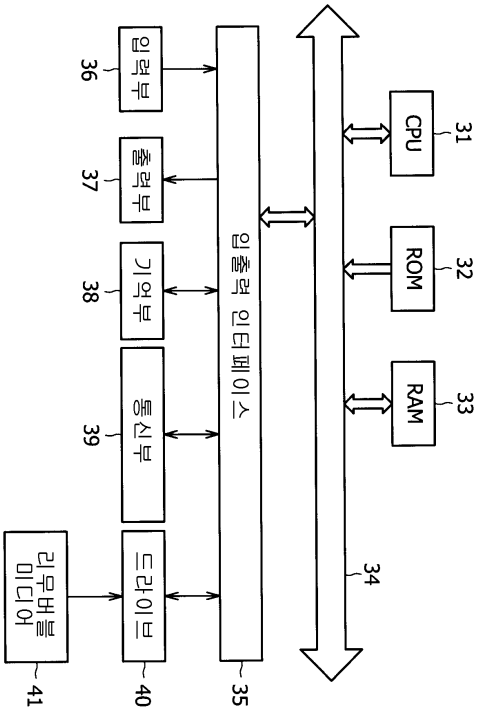


수신상태	거리 r
f_1와 f_2와 f_3를 수신가능	$r \geq r_1$ (1)
f_2와 f_3를 수신가능	$r_1 < r \leq r_2$ (2)
f_3만을 수신가능	$r_2 < r \leq r_3$ (3)
수신불가	$r > r_3$ (4)

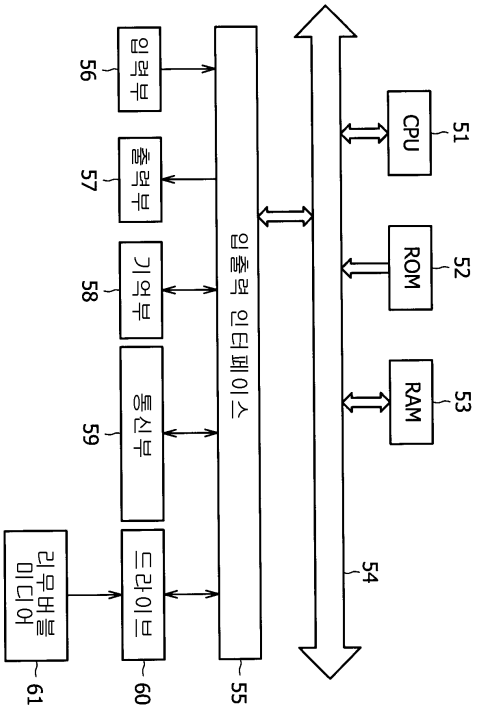
도면7


R
22
안테나
25
24-4 서비스 시스템
네트워크
21
24-1
24-2
24-3
PK 시스템
pBASE
23

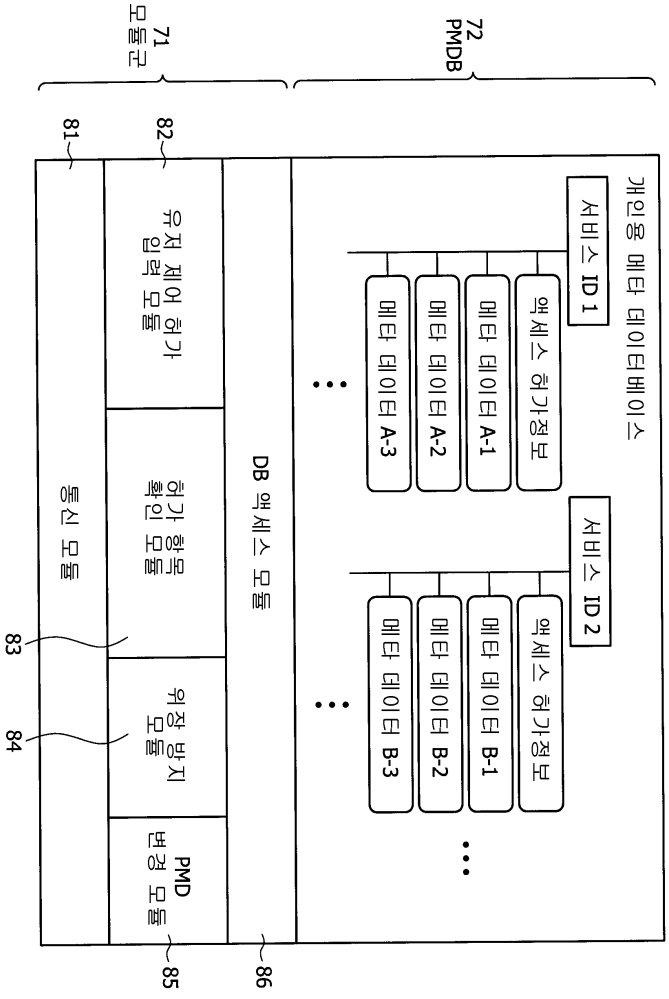
도면8


CPU
31
ROM
32
RAM
33
34
입출력 인터페이스
35
입력부
36
출력부
37
기억부
38
통신부
39
드라이브
40
리무버블 미디어
41

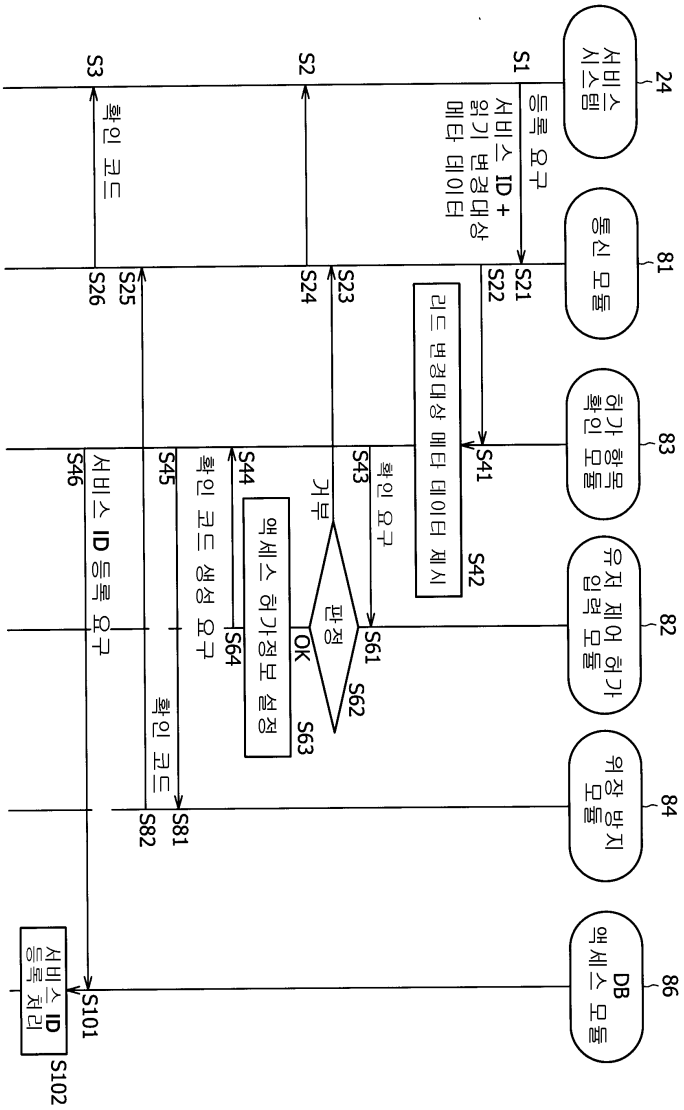
도면9


CPU
51
ROM
52
RAM
53
54
입출력 인터페이스
55
입력부
56
출력부
57
기억부
58
통신부
59
드라이브
60
리무버블 미디어
61

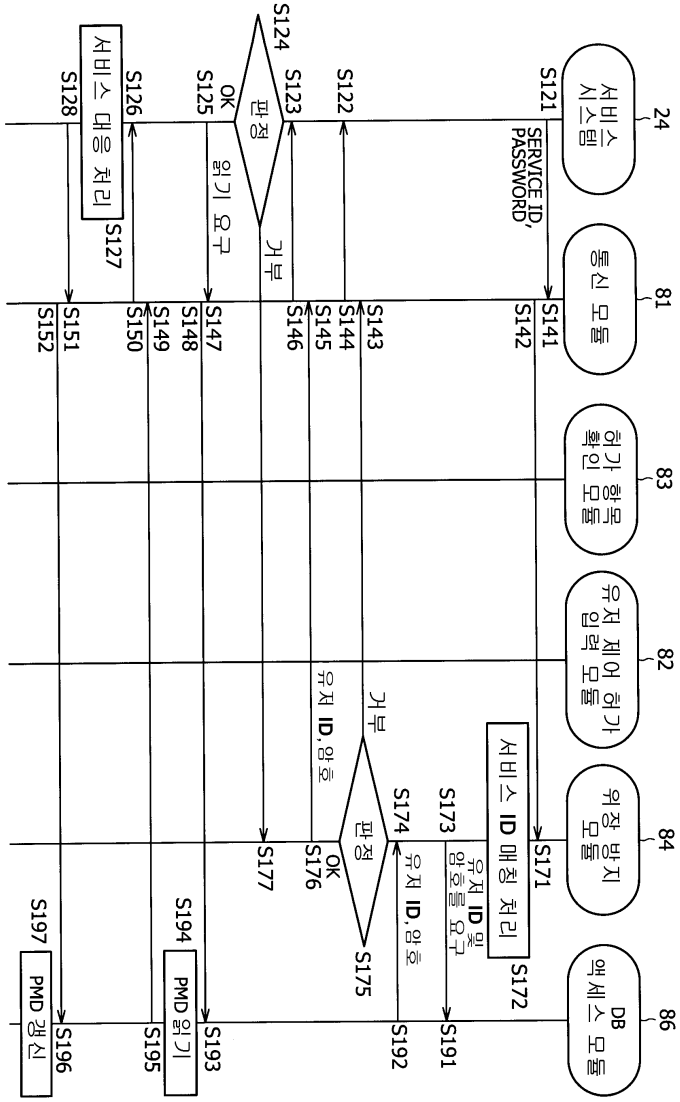
도면10


71 모듈군
72 PMDB
개인용 메타 데이터베이스
서비스 ID 1
액세스 허가정보
메타 데이터 A-1
메타 데이터 A-2
메타 데이터 A-3
서비스 ID 2
액세스 허가정보
메타 데이터 B-1
메타 데이터 B-2
메타 데이터 B-3
DB 액세스 모듈
86
81
82
유저 제어 허가 입력 모듈
허가 항목 확인 모듈
83
위장 방지 모듈
84
PMD 변경 모듈
85
통신 모듈

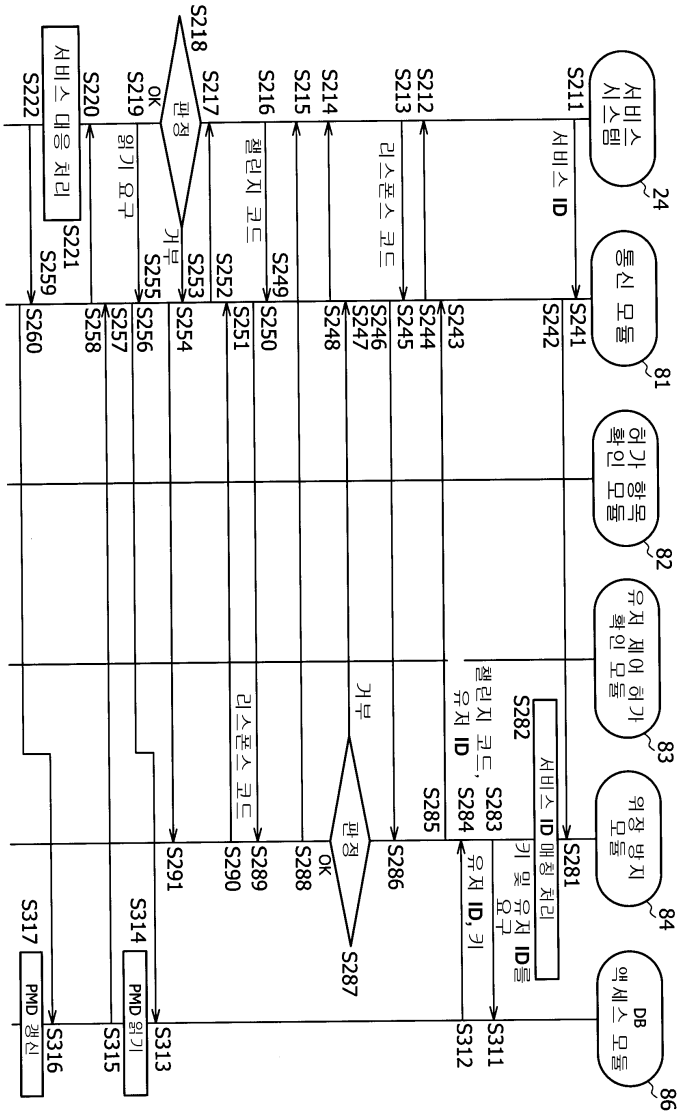
도면11


서비스 시스템
24
통신 모듈
81
허가 항목 확인 모듈
83
유저 제어 허가 입력 모듈
82
위장 방지 모듈
84
DB 액세스 모듈
86
S1
등록 요구
서비스 ID + 읽기 변경대상 메타 데이터
S2
S3
확인 코드
S21
S22
S23
S24
S25
S26
리드 변경대상 메타 데이터 제시
S41
S42
확인 요구
S43
거부
판정
OK
S61
S62
S63
액세스 허가정보 설정
S64
확인 코드 생성 요구
S44
S45
확인 코드
S81
S82
서비스 ID 등록 요구
S46
서비스 ID 등록 처리
S101
S102

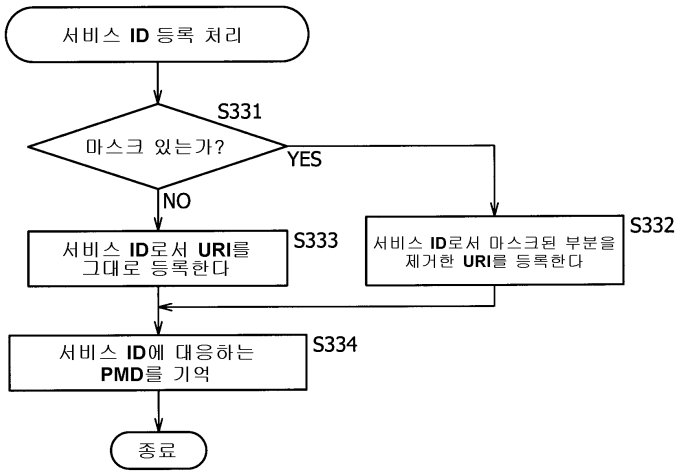
도면12


서비스 시스템
24
통신 모듈
81
허가 항목 확인 모듈
83
유저 제어 허가 입력 모듈
82
위장 방지 모듈
84
DB 액세스 모듈
86
S121
SERVICE ID, PASSWORD
S122
S123
판정
거부
S124
OK
S125
읽기 요구
S126
서비스 대응 처리
S127
S128
S141
S142
S143
S144
S145
S146
S147
S148
S149
S150
S151
S152
서비스 ID 매칭 처리
S171
S172
S173
유저 ID 및 암호를 요구
S174
유저 ID, 암호
S175
판정
거부
OK
S176
유저 ID, 암호
S177
S191
S192
S193
PMD 읽기
S194
S195
PMD 갱신
S196
S197

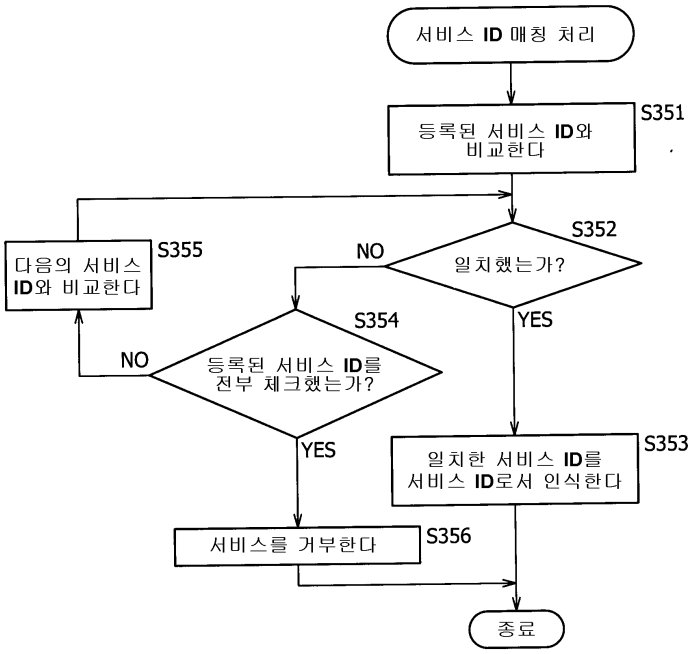
도면13


서비스 시스템
24
통신 모듈
81
허가 항목 확인 모듈
82
유저 제어 허가 확인 모듈
83
위장 방지 모듈
84
DB 액세스 모듈
86
서비스 ID
리스폰스 코드
챌린지 코드
읽기 요구
서비스 대응 처리
판정
OK
거부
서비스 ID 매칭 처리
챌린지 코드, 유저 ID
키 및 유저 ID를 요구
유저 ID, 키
PMD 갱신
PMD 읽기
S211
S212
S213
S214
S215
S216
S217
S218
S219
S220
S221
S222
S241
S242
S243
S244
S245
S246
S247
S248
S249
S250
S251
S252
S253
S254
S255
S256
S257
S258
S259
S260
S281
S282
S283
S284
S285
S286
S287
S288
S289
S290
S291
S311
S312
S313
S314
S315
S316
S317

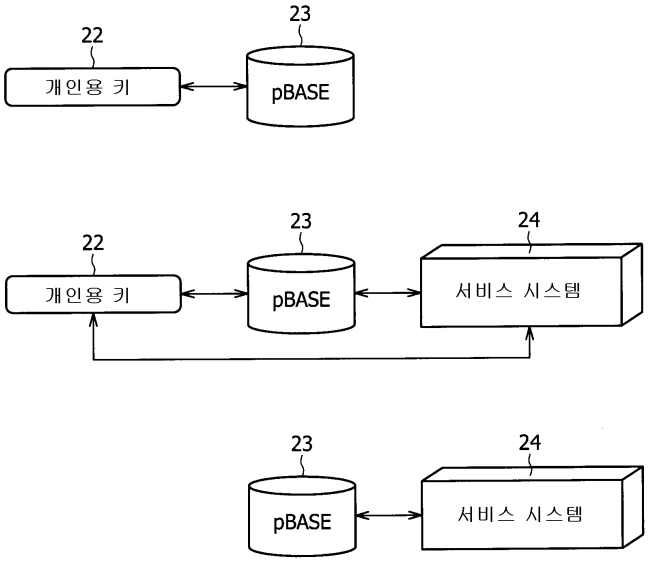
도면14


서비스 ID 등록 처리
S331
마스크 있는가?
YES
NO
서비스 ID로서 URI를 그대로 등록한다
S333
서비스 ID로서 마스크된 부분을 제거한 URI를 등록한다
S332
서비스 ID에 대응하는 PMD를 기억
S334
종료

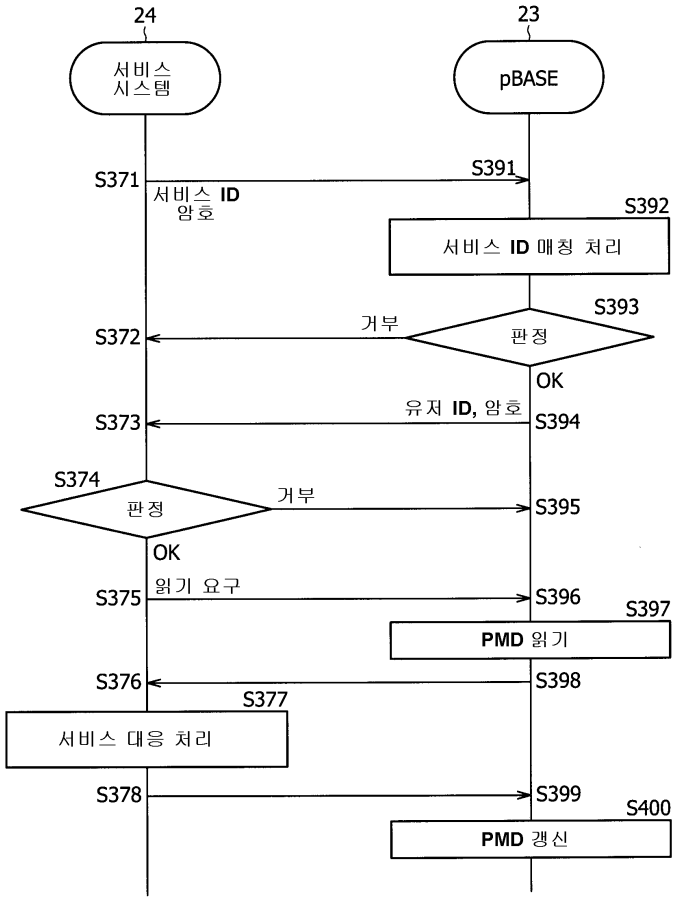
도면15


서비스 ID 매칭 처리
등록된 서비스 ID와 비교한다
S351
S352
일치했는가?
NO
YES
다음의 서비스 ID와 비교한다
S355
S354
등록된 서비스 ID를 전부 체크했는가?
NO
YES
일치한 서비스 ID를 서비스 ID로서 인식한다
S353
서비스를 거부한다
S356
종료

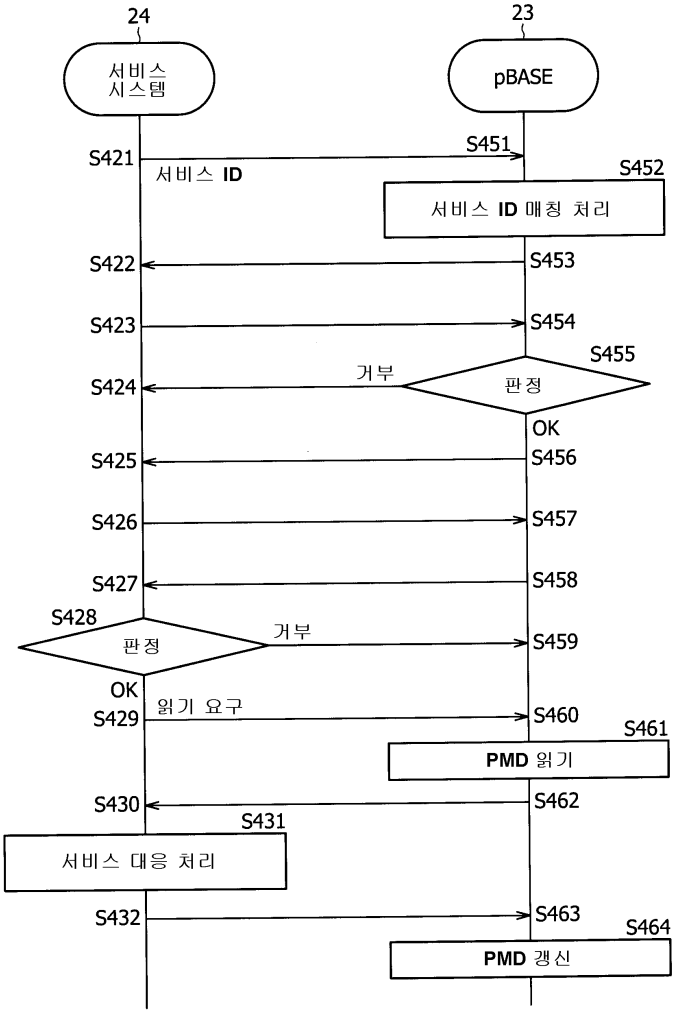
도면16


22
개인용 키
23
pBASE
22
개인용 키
23
pBASE
24
서비스 시스템
23
pBASE
24
서비스 시스템

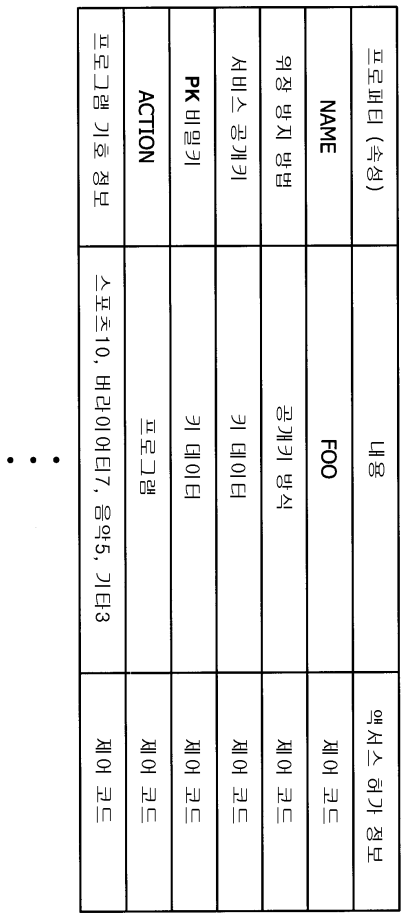
도면17


24
서비스 시스템
23
pBASE
S371
서비스 ID 암호
S391
S392
서비스 ID 매칭 처리
S393
판정
거부
S372
OK
유저 ID, 암호
S373
S394
S374
판정
거부
S395
OK
읽기 요구
S375
S396
S397
PMD 읽기
S376
S398
S377
서비스 대응 처리
S378
S399
S400
PMD 갱신

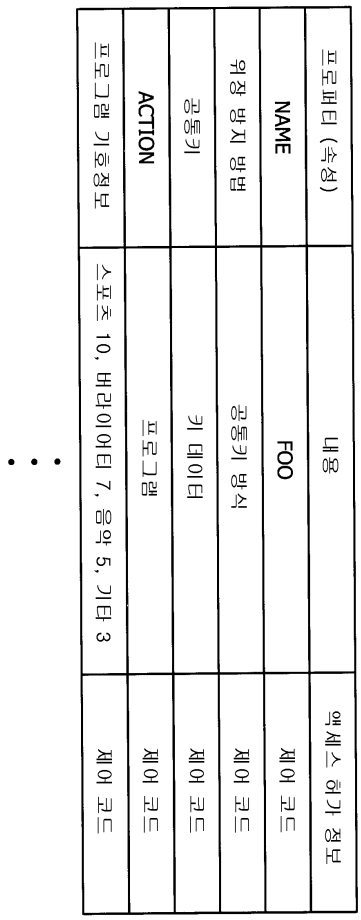
도면18


24
서비스 시스템
23
pBASE
S421
서비스 ID
S451
S452
서비스 ID 매칭 처리
S422
S453
S423
S454
S455
S424
거부
판정
OK
S425
S456
S426
S457
S427
S458
S428
판정
거부
S459
OK
S429
읽기 요구
S460
S461
PMD 읽기
S430
S462
S431
서비스 대응 처리
S432
S463
S464
PMD 갱신

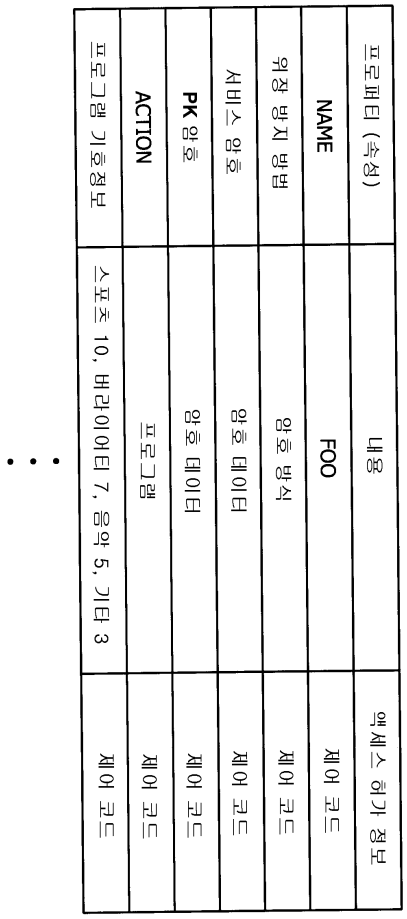
도면19


프로퍼티 (속성)
내용
엑서스 허가 정보
NAME
FOO
제어 코드
위장 방지 방법
공개키 방식
제어 코드
서비스 공개키
키 데이터
제어 코드
PK 비밀키
키 데이터
제어 코드
ACTION
프로그램
제어 코드
프로그램 기호 정보
스포츠10, 버라이어티7, 음악5, 기타3
제어 코드

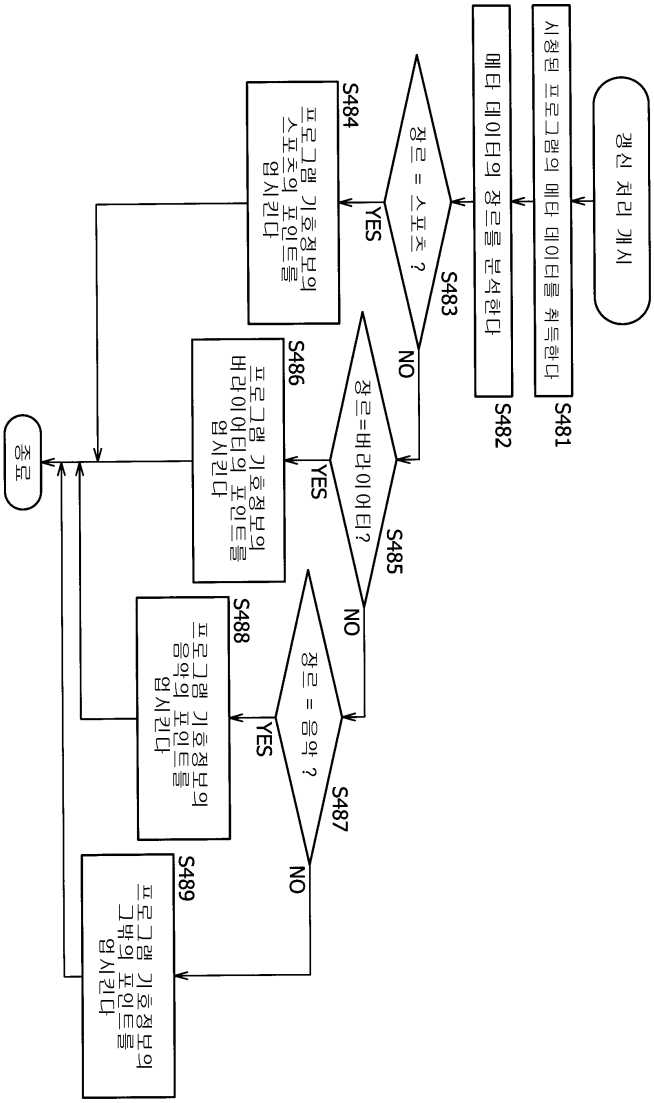
도면20


프로퍼티 (속성)
내용
액세스 허가 정보
NAME
FOO
제어 코드
워징 방지 방법
공통키 방식
제어 코드
공통키
키 데이터
제어 코드
ACTION
프로그램
제어 코드
프로그램 기호정보
스포츠 10, 버라이어티 7, 음악 5, 기타 3
제어 코드

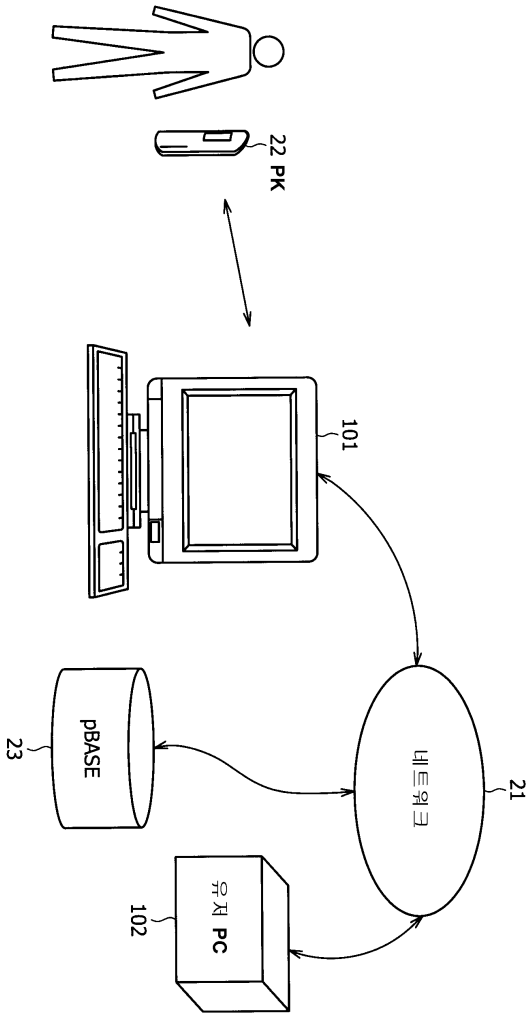
도면21


프로퍼티 (속성)
NAME
위장 방지 방법
서비스 암호
PK 암호
ACTION
프로그램 기술정보
내용
FOO
암호 방식
암호 데이터
암호 데이터
프로그램
스프즈 10, 버라이어티 7, 음악 5, 기타 3
액세스 허가 정보
제어 코드
제어 코드
제어 코드
제어 코드
제어 코드

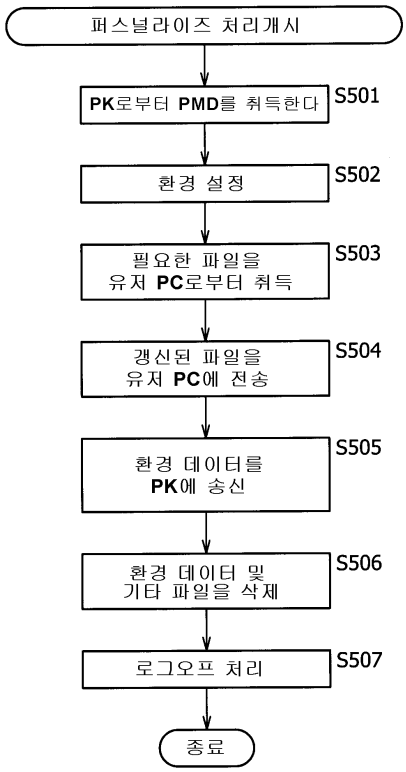
도면22


갱신 처리 개시
시청된 프로그램의 메타 데이터를 취득한다
S481
메타 데이터의 장르를 분석한다
S482
장르 = 스포츠 ?
S483
YES
프로그램 기호정보의 스포츠의 포인트를 업 시킨다
S484
NO
장르=바라이어티?
S485
YES
프로그램 기호정보의 바라이어티의 포인트를 업 시킨다
S486
NO
장르 = 음악 ?
S487
YES
프로그램 기호정보의 음악의 포인트를 업 시킨다
S488
NO
프로그램 기호정보의 그밖의 포인트를 업 시킨다
S489
종료

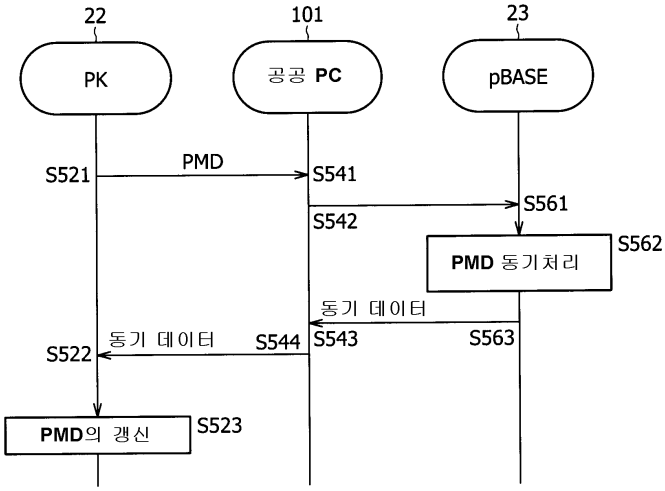
도면23



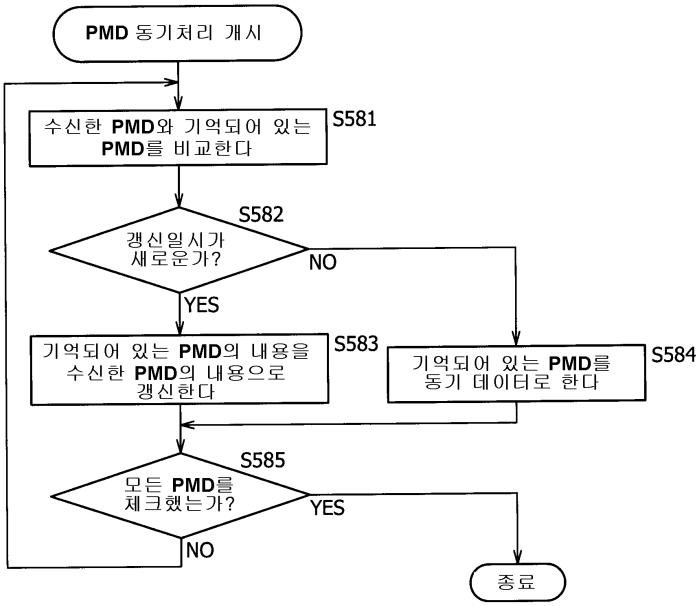
도면24


퍼스널라이즈 처리개시
PK로부터 PMD를 취득한다
S501
환경 설정
S502
필요한 파일을
유저 PC로부터 취득
S503
갱신된 파일을
유저 PC에 전송
S504
환경 데이터를
PK에 송신
S505
환경 데이터 및
기타 파일을 삭제
S506
로그오프 처리
S507
종료

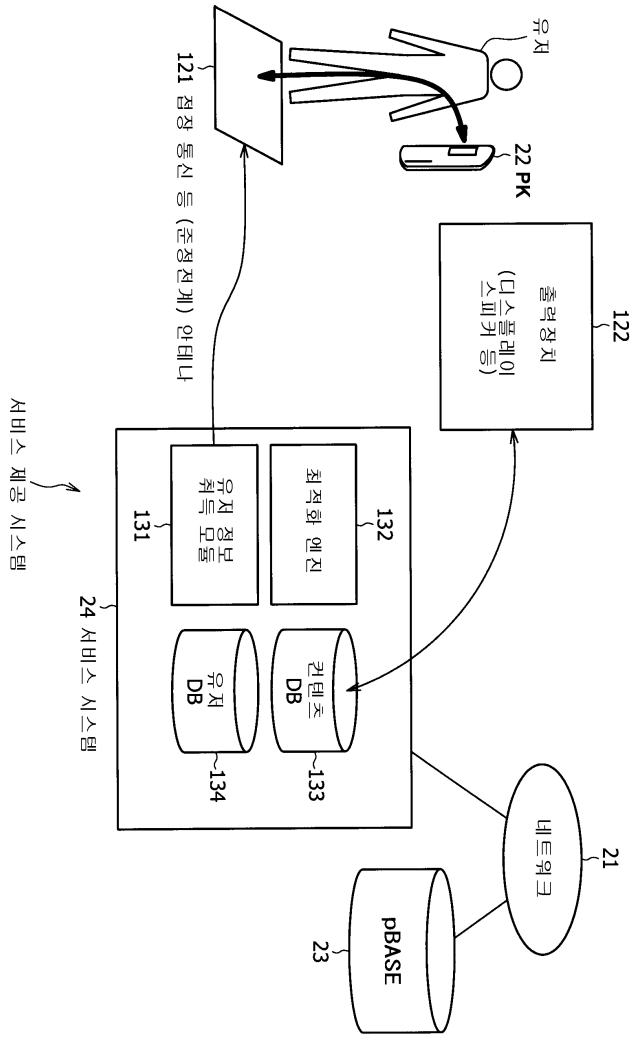
도면25


22
101
23
PK
공공 PC
pBASE
PMD
S521
S541
S561
S542
PMD 동기처리
S562
동기 데이터
동기 데이터
S522
S544
S543
S563
PMD의 갱신
S523

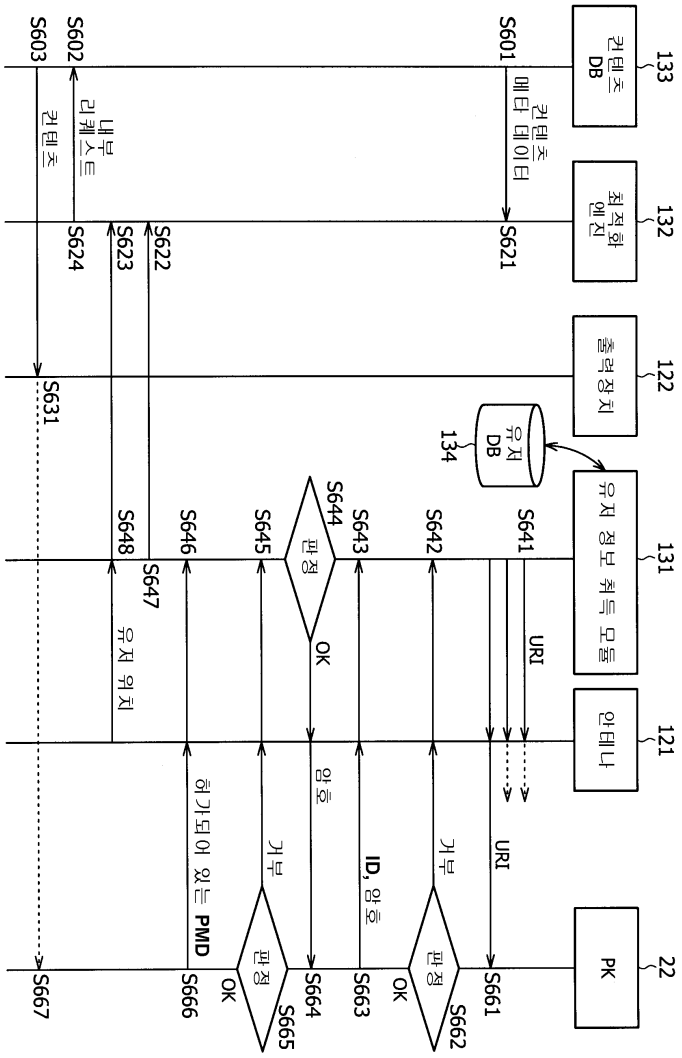
도면26


PMD 동기처리 개시
수신한 PMD와 기억되어 있는 PMD를 비교한다
S581
S582
갱신일시가 새로운가?
NO
YES
기억되어 있는 PMD의 내용을 수신한 PMD의 내용으로 갱신한다
S583
기억되어 있는 PMD를 동기 데이터로 한다
S584
S585
모든 PMD를 체크했는가?
YES
NO
종료

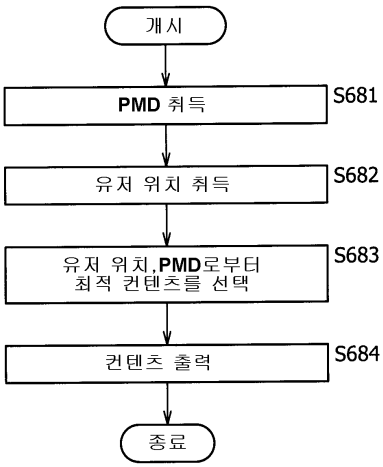
도면27


유저
121 접장 통신 등 (준정전계) 안테나
22 PK
출력장치 (디스플레이 스피커 등)
122
서비스 제공 시스템
131 유저 정보 취득 모듈
132 최적화 엔진
24 서비스 시스템
유저 DB
134
컨텐츠 DB
133
네트워크
21
pBASE
23

도면28


컨텐츠 DB
133
최적화 엔진
132
출력장치
122
유저 DB
134
유저 정보 취득 모듈
131
안테나
121
PK
22
S601
S602
S603
S621
S622
S623
S624
S631
S641
S642
S643
S644
S645
S646
S647
S648
S661
S662
S663
S664
S665
S666
S667
컨텐츠 메타 데이터
내부 리퀘스트
컨텐츠
판정
OK
URI
유저 위치
암호
ID, 암호
거부
허가되어 있는 PMD

도면29


개시
PMD 취득
S681
유저 위치 취득
S682
유저 위치,PMD로부터 최적 컨텐츠를 선택
S683
컨텐츠 출력
S684
종료

도면30