(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년10월07일
(11) 등록번호 10-1314512
(24) 등록일자 2013년09월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04B 10/85* (2013.01)
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2006-0072204
(22) 출원일자 2006년07월31일
심사청구일자 2011년08월01일
(65) 공개번호 10-2007-0015880
(43) 공개일자 2007년02월06일
(30) 우선권주장
JP-P-2005-00223084 2005년08월01일 일본(JP)
(56) 선행기술조사문헌
US06393127 B2*
JP2003018148 A
KR1020050000673 A
US6393127 B2
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
소니 주식회사
일본국 도쿄도 미나토쿠 코난 1-7-1
(72) 발명자
스기야마 도시노부
일본 도쿄도 시나가와꾸 기따시나가와 6쪼메 7-35 소니 가부시끼가이샤 내
(74) 대리인
구영창, 이중희, 장수길

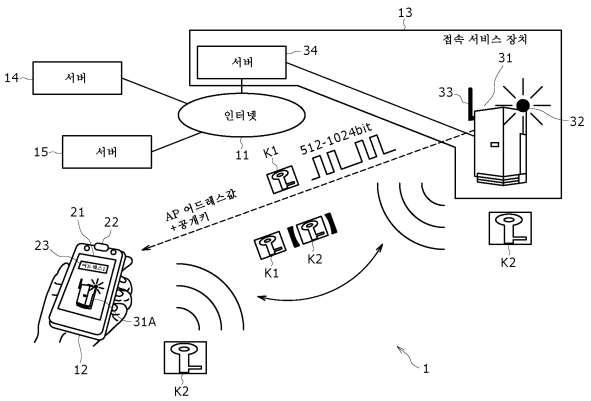
전체 청구항 수 : 총 5 항 심사관 : 양종필

(54) 발명의 명칭 **정보 처리 방법 및 기록 매체**

(57) 요 약

광원으로부터 방출된 광선의 변화에 의해 제1 키를 공개적으로 배신하고, 상기 광원으로부터 방출된 광선으로부터 상기 제1 키를 추출하고, 추출된 상기 제1 키로 제2 키를 암호화하여, 암호화된 상기 제2 키를 근거리 통신으로 송신하고, 암호화된 상기 제2 키를 수신해서 복호화하고, 상기 제2 키를 공통 키를 사용하여, 정보를 전송하도록 구성된 정보 처리 시스템이 제공된다.

대 표 도 - 도2



특허청구의 범위

청구항 1

배신(配信) 수단, 추출 수단, 표시 수단, 송신 수단, 수신 수단, 복호 수단 및 전송 수단을 포함하는 정보 처리 장치의 정보 처리 방법으로서,

상기 배신 수단에 의해, 광원으로부터 방출된 광선의 변화에 의해 광 점멸(flash) 신호로서 제1 키와 함께 액세스 포인트의 어드레스 값을 공개적으로 배신하는 단계,

상기 추출 수단에 의해, 상기 광원으로부터 방출된 상기 광선이 촬상되는 상기 액세스 포인트의 촬상 화상을 이용하여, 상기 광원으로부터 방출된 상기 광선으로부터 상기 제1 키 및 상기 액세스 포인트의 상기 어드레스 값을 추출하는 단계,

상기 표시 수단에 의해, 상기 액세스 포인트의 촬상 화상으로 상기 액세스 포인트의 상기 어드레스 값에 대응하는 심볼을 표시하는 단계,

상기 송신 수단에 의해, 상기 심볼이 선택되었는지에 기초하여, 추출된 상기 제1 키로 제2 키를 암호화하여, 암호화된 상기 제2 키를 근거리 통신으로 송신(transmit)하는 단계,

상기 수신 수단에 의해 암호화된 상기 제2 키를 수신하여 상기 복호 수단에 의해 복호화하는 단계, 및

상기 전송 수단에 의해, 상기 제2 키를 공통 키로서 이용하여 정보를 전송(transfer)하는 단계

를 포함하고,

상기 광원으로부터 방출된 상기 광선은, 상기 액세스 포인트의 상기 촬상 화상을 촬상하는데 이용되는 수광부가 상기 액세스 포인트를 향하여 미리 정해진 방향으로 배열되는 경우, 상기 액세스 포인트의 상기 촬상 화상에 촬상되는, 정보 처리 방법.

청구항 2

배신 수단 및 수신 수단을 포함하는 제1 정보 처리 장치와 상기 제1 정보 처리 장치와는 다른 제2 정보 처리 장치 사이의 정보 처리 방법으로서,

상기 제1 정보 처리 장치의 상기 배신 수단에 의해, 광원으로부터 방출된 광선의 변화에 의해 광 점멸 신호로서 제1 키와 함께 상기 제1 정보 처리 장치의 어드레스 값을 배신하는 단계,

상기 제1 정보 처리 장치의 상기 수신 수단에 의해, 배신된 상기 제1 키로 암호화된 정보를 수신하는 단계

를 포함하고,

배신된 상기 제1 키는, 상기 제2 정보 처리 장치의 수광부가 상기 제1 정보 처리 장치를 향하여 미리 정해진 방향으로 배열될 때, 상기 광원으로부터 방출된 광선이 촬상되어 얻어진 상기 제1 정보 처리 장치의 촬상 화상을 이용하여, 상기 제2 정보 처리 장치에 의해 수신되며,

배신된 상기 제1 키로 암호화된 상기 정보는, 상기 제2 정보 처리 장치의 표시부가 상기 제1 정보 처리 장치의 상기 촬상 화상으로 심볼을 표시하는 경우에, 상기 제1 정보 처리 장치의 상기 어드레스 값에 대응하는 상기 심볼이 선택되는지에 기초하여, 상기 제2 정보 처리 장치로부터 송신되는, 정보 처리 방법.

청구항 3

배신 수단 및 수신 수단을 포함하는 제1 정보 처리 장치와 상기 제1 정보 처리 장치와는 다른 제2 정보 처리 장치 사이의 정보 처리 방법을 컴퓨터에서 실행시키는 프로그램이 저장된 기록 매체로서,

상기 방법은,

상기 제1 정보 처리 장치의 상기 배신 수단으로 하여금, 광원으로부터 방출된 광선의 변화에 의해 광 점멸 신호로서 제1 키와 함께 상기 제1 정보 처리 장치의 어드레스 값을 배신하는 단계; 및

상기 제1 정보 처리 장치의 상기 수신 수단으로 하여금, 배신된 상기 제1 키로 암호화된 정보를 수신하는 단계

를 포함하고,

배신된 상기 제1 키는, 상기 제2 정보 처리 장치의 수광부가 상기 제1 정보 처리 장치를 향하여 미리 정해진 방향으로 배열될 때, 상기 광원으로부터 방출된 광선이 촬상되어 얻어진 상기 제1 정보 처리 장치의 촬상 화상을 이용하여, 상기 제2 정보 처리 장치에 의해 수신되며,

배신된 상기 제1 키로 암호화된 상기 정보는, 외부의 상기 제2 정보 처리 장치의 표시부가 상기 제1 정보 처리 장치의 상기 촬상 화상으로 심볼을 표시하는 경우에, 상기 제1 정보 처리 장치의 상기 어드레스 값에 대응하는 상기 심볼이 선택되는지에 기초하여, 상기 제2 정보 처리 장치로부터 송신되는, 기록 매체.

청구항 4

수신 수단, 판독 수단, 표시 수단, 송신 수단 및 전송 수단을 포함하는 정보 처리 장치의 정보 처리 방법으로서,

상기 수신 수단에 의해, 광원으로부터 공개적으로 방출되는 변화된 광선을 수신하는 단계 - 상기 광원에 의해 액세스 포인트의 어드레스 값이 광 점멸 신호로서 제1 키와 함께 송신됨 - ;

상기 판독 수단에 의해, 상기 광원으로부터 방출된 상기 광선이 촬상되는 상기 액세스 포인트의 촬상 화상을 이용하여, 수신된 상기 광선으로부터 상기 액세스 포인트의 상기 어드레스 값 및 상기 제1 키를 판독하는 단계;

상기 표시 수단에 의해, 상기 액세스 포인트의 촬상 화상으로 상기 액세스 포인트의 상기 어드레스 값에 대응하는 심볼을 표시하는 단계;

상기 송신 수단에 의해, 상기 심볼이 선택되었는지에 기초하여, 판독된 상기 제1 키로 제2 키를 프로세서에 의해 암호화하여, 암호화된 상기 제2 키를 근거리 통신에 의해 송신하는 단계; 및

상기 전송 수단에 의해, 상기 제2 키를 공통 키로서 이용하여 정보를 전송하는 단계

를 포함하고,

상기 광원으로부터 방출된 상기 광선은, 상기 액세스 포인트의 상기 촬상 화상을 촬상하는데 이용되는 수광부가 상기 액세스 포인트를 향하여 미리 정해진 방향으로 배열되는 경우, 상기 액세스 포인트의 상기 촬상 화상에 촬상되는, 정보 처리 방법.

청구항 5

정보 처리 방법을 컴퓨터에서 실행시키는 프로그램이 저장된 기록 매체로서,

상기 방법은,

액세스 포인트의 어드레스 값이 광 점멸 신호로서 제1 키와 함께 송신됨에 의해, 광원으로부터 공개적으로 방출되는 변화된 광선을 수신하는 단계;

상기 광원으로부터 방출된 상기 광선이 촬상되는 상기 액세스 포인트의 촬상 화상을 이용하여, 수신된 상기 광선으로부터 상기 액세스 포인트의 상기 어드레스 값 및 제1 키를 판독하는 단계;

상기 액세스 포인트의 촬상 화상으로 상기 액세스 포인트의 상기 어드레스 값에 대응하는 심볼을 표시하는 단계;

상기 심볼이 선택되었는지에 기초하여, 판독된 상기 제1 키로 제2 키를 프로세서에 의해 암호화하여, 암호화된 상기 제2 키를 근거리 통신에 의해 송신하는 단계; 및

상기 제2 키를 공통 키로서 이용하여 정보를 전송하는 단계

를 포함하고,

상기 광원으로부터 방출된 상기 광선은, 상기 액세스 포인트의 상기 촬상 화상을 촬상하는데 이용되는 수광부가 상기 액세스 포인트를 향하여 미리 정해진 방향으로 배열되는 경우, 상기 액세스 포인트의 상기 촬상 화상에 촬상되는, 기록 매체.

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

명 세 서

발명의 상세한 설명

발명의 목적

종래기술의 문헌 정보

[0036] 비특허문헌 1: "802.11 High-Speed Wireless LAN Textbook" (제334 페이지 및 제335페이지)

발명이 속하는 기술 및 그 분야의 종래기술

[0037] 상호 참조

[0038] 본 발명은 2005년 8월 1일에 일본특허청에 제출된 일본특허출원 JP 2005-223084와 관련된 특허 대상을 포함하며, 그 전체 내용이 본 명세서에 참조로 편입된다.

[0039] 본 발명은 정보 처리 시스템, 정보 처리 장치 및 방법, 컴퓨터 프로그램 및 기록 매체에 관한 것으로, 특히, 신속하고 자유롭게, 그리고 안전하게 정보를 전송할 수 있도록 한 정보 처리 시스템, 정보 처리 장치 및 방법, 컴퓨터 프로그램 및 기록 매체에 관한 것이다.

[0040] 최근, 사용자가 임의의 출장지에서 인터넷에 액세스할 수 있도록 액세스 포인트가 많이 배치되어 있다. 사용자는, 출장지의 액세스 포인트로부터 인터넷에 접속하는 것이 가능하다. 액세스 포인트에 있어서 패스워드와 사용자 ID를 이용해서 인증하는 방식이 제안되어 있다(예를 들면, 비특허문헌 1).

[0041] 패스워드와 사용자 ID를 이용해서 인증하는 액세스 포인트의 동작에 대해서, 도 1을 참조하여 설명한다. 또한, 도 1의 시스템에서는, 클라이언트(1)와 액세스 포인트(2) 사이의 통신은 무선 전파에 의해 행해지고, 액세스 포인트(2)와 인증 서버(3) 사이의 통신은 유선 통신에 의해 행해진다.

[0042] 각 사용자는, 출장지의 액세스 포인트를 이용해서 인터넷에 액세스할 경우, 사전에 사용자 등록을 끝마치고, 패스워드와 사용자 ID의 교부를 받아 둔다. 그 후, 단계 S1에서, 클라이언트(1)는 액세스 포인트(2)에 대하여 접속 요구를 송신한다.

[0043] 액세스 포인트(2)는 단계 S21에서, 클라이언트(1)로부터의 접속 요구를 수신하면, 단계 S22에서, 그 접속 요구를 인증 서버(3)에 전송한다. 단계 S51에서, 인증 서버(3)는 이 접속 요구를 수신하면, 지금 응답이 가능인가 아닌가를 판정하고, 단계 S52에서, 그 판정 결과에 대응하는 접속 응답을 액세스 포인트(2)에 출력한다. 액세스 포인트(2)는, 단계 S23에서 이 접속 응답을 수신하면, 단계 S24에서 이것을 클라이언트(1)에 전송한다. 단계 S2에서, 클라이언트(1)는 접속 응답을 수신한다.

[0044] 또한, 단계 S53에서, 인증 서버(3)는, 도시하지 않는 인증 기관으로부터 미리 발행을 받은 공개 키와 증명서를 액세스 포인트(2)로 송신한다. 액세스 포인트(2)는, 단계 S25에서 이 공개 키와 증명서를 수신하면, 단계 S26에서 이것을 클라이언트(1)에 송신한다. 클라이언트(1)는, 단계 S3에서, 액세스 포인트(2)로부터 송신되어 온 공개 키와 증명서를 수신한다.

[0045] 증명서에는, 규격 버젼, 일련 번호, 공개 키 소유자, 공개 키 등의 평문의 데이터 외에, 이들에 기초하는 디지털 서명이 부여되어 있다. 클라이언트(1)는, 공개 키에 의해 디지털 서명을 복호하여 얻은 내용을, 이미 얻은 평문의 규격 버젼, 일련 번호, 공개 키소유자, 공개 키 등과 비교함으로써, 수신한 공개 키와 그 증명서가 진정한 인증 서버로부터, 즉, 인증국에 의해 인증된 관리자로부터 송부된 것을 확인할 수 있다. 따라서, 사용자는 안심하고 그 인증 서버를 통해서 인터넷에 접속할 수 있다.

[0046] 단계 S4에서, 클라이언트(1)는 인증 서버(3)와 정보를 전송하는데도 공통 키로서 이용하는 암호키를 생성하고, 액세스 포인트(2)로부터 수신한 공개 키로 암호화하고, 액세스 포인트(2)에 송신한다. 액세스 포인트(2)는, 단계 S27에서 암호키를 수신하면, 단계 S28에서 이것을 인증 서버(3)에 송신한다. 단계 S54에서, 인증 서버(3)는 암호키를 수신하고, 이 암호키를 공개 키에 대응하는 비밀키로 복호화하고, 암호키를 공통 키로 한다.

[0047] 한편, 단계 S5에서, 클라이언트(1)는 사용자 ID를 암호키에 의해 암호화하고, 그 암호화된 사용자 ID를 액세스 포인트(2)에 송신한다. 그리고, 클라이언트(1)는, 단계 S6에서 패스워드를 암호키에 의해 암호화해서 액세스

포인트(2)에 송신한다. 액세스 포인트(2)는, 단계 S29에서 사용자 ID를 수신하고, 단계 S31에서 패스워드를 수신한다. 액세스 포인트(2)는, 단계 S30에서 사용자 ID를 인증 서버(3)로 송신하고, 단계 S32에서 패스워드를 인증 서버(3)에 송신한다. 인증 서버(3)는, 단계 S55에서 사용자 ID를 수신하고, 단계 S56에서 패스워드를 수신한다. 인증 서버(3)는 수신한 사용자 ID와 패스워드를 단계 S54에서 수신하고 있는 암호키로 복호화함으로써, 사용자 ID와 패스워드가 이미 등록되어 있는 사용자의 것임을 확인한다.

[0048] 클라이언트(1)가 정규 사용자임을 사용자 ID와 패스워드로부터 확인한 경우, 클라이언트(1)는 단계 S7에서, 또한, 인증 서버(3)는 단계 S57에서, 서로 액세스 포인트(2)를 통해 접속 수속을 완료한다. 따라서, 이후, 클라이언트(1)는 액세스 포인트(2)와 인증 서버(3)를 통해서 인터넷에 접속하고, 적절히 필요한 정보에 액세스할 수 있다.

[0049] 액세스 포인트(2)는, 많은 장소에 분산되어서 배치되어서 있기 때문에, 사용자는 필요에 따라 출장지에서 액세스 포인트(2)와 인증 서버(3)를 통해 인터넷에 접속하고, 거기에서 각종의 서비스의 제공을 받는 것이 가능하게 된다.

[0050] 그러나, 종래의 시스템에서는, 사용자가 액세스 포인트를 이용해서 인터넷에 접속하기 위해서는, 사전에 등록해 두어, ID와 패스워드의 교부를 받아 놓아야 한다. 따라서, 제공자가 신속하고 자유롭게 정보를 제공하는 것이 곤란해져서, 사용자도 신속하고 자유롭게 정보의 제공을 받는 것이 곤란하였다.

[0051] 따라서, 사전의 등록과 증명서의 이용을 생략하는 것도 생각된다. 그러나, 그 경우, 무선 LAN 피싱 사기의 피해를 입는 우려가 있다. 즉, 피싱 사기를 행하려고 하는 자가 액세스 포인트의 서비스 범위 내에서 부정한 전파를 발신하고, 그 부정한 전파를 수신한 사용자의 클라이언트에 가짜의 웹페이지를 표시시켜, 사용자가 그 가짜의 웹페이지의 어디를 클릭해도 자동적으로 바이러스를 다운로드시키는 사건이 발생하고 있다.

발명이 이루고자 하는 기술적 과제

[0052] 본 발명은, 이러한 상황을 감안하여 이루어진 것으로, 신속하고 자유롭게, 그리고 안전하게 정보를 전송할 수 있도록 하는 것이다.

발명의 구성 및 작용

[0053] 본 발명의 제1 측면은, 광원으로부터 방출된 광선의 변화에 의해 제1 키를 공개적으로 배신하고, 상기 광원의 광으로부터 상기 제1 키를 추출하고, 추출된 상기 제1 키에 의해 제2 키를 암호화해서 암호화된 제2 키를 근거리 통신에 의해 송신하고, 암호화되어 있는 상기 제2 키를 수신해서 복호화하고, 상기 제2 키를 공통 키로서 정보를 전송하는 정보 처리 시스템 및 정보 처리 방법이다.

[0054] 본 발명의 측면에서는, 광원으로부터 방출된 광선의 변화에 의해 제1 키가 공개적으로 배신되어, 광원의 광으로부터 제1 키가 추출된다. 추출된 제1 키에 의해 암호화해서 제2 키가 근거리 통신에 의해 송신되어, 암호화되어 있는 제2 키가 수신해서 복호화되어, 제2 키가 공통 키로서 정보가 전송된다.

[0055] 본 발명의 다른 측면은, 광원으로부터 방출된 광선의 변화에 의해 제1 키를 공개적으로 배신하는 배신 수단과, 배신된 상기 제1 키에 의해 암호화된 정보를 수신하는 수신 수단을 구비하는 정보 처리 장치다.

[0056] 상기 배신 수단은, 상기 제1 키로서 인증 기관에 의해 발행된 공개 키를 배신할 수 있다.

[0057] 상기 수신 수단은, 상기 제1 키에 의해 암호화된 정보로서 제2 키를 수신하고, 상기 정보 처리 장치는, 수신된 상기 제2 키를 복호화하고, 공통 키를 얻는 복호 수단을 더 구비할 수 있다.

[0058] 상기 배신 수단은 액세스 포인트에 설치되고, 상기 제1 키를 클라이언트에 공개적으로 배신하고, 상기 수신 수단은 상기 액세스 포인트에 설치되고, 상기 클라이언트로부터 근거리 통신에 의해 송신된 상기 제2 키를 수신할 수 있다.

[0059] 상기 배신 수단은, 상기 제1 키로서 인증 기관에 의해 발행된 공개 키를 배신하고, 상기 액세스 포인트에는, 상기 인증 기관에 의해 증명되어 있는 것을 나타내는 정보를 게시시킬 수 있다.

[0060] 또한, 상기 배신 수단은, 상기 광원으로부터 방출된 광선의 변화에 의해 어드레스 값을 배신할 수 있다.

[0061] 상기 광원은, 제공하는 정보에 관계되는 물체를 조명하는 조명 기구로 할 수 있다.

[0062] 상기 액세스 포인트는, 상기 조명 기구의 점멸을 제어하는 신호를 전력선을 통해서 송신할 수 있다.

[0063] 상기 광원은, 가시광 또는 적외광을 발생하는 LED로 할 수 있다.

[0064] 본 발명의 다른 측면은, 광원으로부터 방출된 광선의 변화에 의해 키를 공개적으로 배신하고, 배신된 상기 키에 의해 암호화된 정보를 수신하는 단계을 구비하는 정보 처리 방법, 컴퓨터에 실행시키는 프로그램, 및 기록 매체다.

[0065] 본 발명의 다른 측면에서는, 광원으로부터 방출된 광선의 변화에 의해 키가 공개적으로 배신되고, 배신된 키에서 암호화된 정보가 수신된다.

[0066] 본 발명의 또 다른 측면은, 광원이 공개적으로 발생하는 변화하는 광을 수광하는 수광 수단과, 수광된 광으로부터 제1 키를 판독하는 판독 수단과, 판독된 상기 제1 키에 의해 암호화해서 제2 키를 근거리통신에 의해 송신하는 송신 수단과, 상기 제2 키를 공통 키로서 정보를 전송하는 전송 수단을 구비하는 정보 처리 장치다.

[0067] 또한, 상기 판독 수단은, 수광된 광으로부터 어드레스 값을 판독할 수 있다.

[0068] 상기 어드레스 값에 대응하는 심볼을 표시하는 표시 수단과, 상기 심볼의 선택을 판정하는 판정 수단을 더 구비할 수 있다.

[0069] 본 발명의 또 다른 측면은, 광원이 공개적으로 발생하는 변화하는 광을 수광하고, 수광된 광으로부터 제1 키를 판독하고, 판독된 상기 제1 키에 의해 암호화해서 제2 키를 근거리 통신에 의해 송신하고, 상기 제2 키를 공통 키로서 정보를 전송하는 단계를 구비하는 정보 처리 방법, 컴퓨터에 실행시키는 프로그램 또는 기록 매체다.

[0070] 본 발명의 또 다른 측면에서는, 광원이 공개적으로 발생하는 변화하는 광이 수광되고, 수광된 광으로부터 제1 키를 판독되고, 판독된 상기 제1 키에 의해 암호화해서 제2 키가 근거리 통신에 의해 송신되고, 상기 제2 키를 공통 키로서 정보가 전송된다.

[0071] 이상과 같이, 본 발명에 따르면, 정보를 전송 및 수신할 수 있다. 특히, 본 발명에 따르면, 신속하고 자유롭게, 그리고 안전하게 정보를 전송 및 수신할 수 있다.

[0072] 이하에 본 발명의 실시예를 설명하지만, 본 발명의 구성 요건과, 발명의 상세한 설명에 기재된 실시예와의 대응관계를 예시하면, 다음과 같이 된다. 이 기재는, 본 발명을 서포트하는 실시예가, 발명의 상세한 설명에 기재되어 있는 것을 확인하기 위한 것이다. 따라서, 발명의 상세한 설명 중에는 기재되어 있지만, 본 발명의 구성 요건에 대응하는 실시예로서, 여기에는 기재되지 않고 있는 실시예가 있다고 해도, 그것은, 그 실시예가, 그 구성 요건에 대응하지 것은 아닌 것을 의미하는 것은 아니다. 반대로, 실시예가 구성 요건에 대응하는 것으로서 여기에 기재되어 있어도, 그것은, 그 실시예가 그 구성 요건 이외의 구성 요건에는 대응하지 않는 것을 의미하는 것이 아니다.

[0073] 본 발명의 제1 측면은, 광원(예를 들면, 도 2의 LED(32))으로부터 방출된 광선의 변화에 의해 제1 키(예를 들면, 도 2의 공개 키 K1)를 공개적으로 배신해(예를 들면, 도 11의 단계 S42, 도 19의 단계 S147의 처리), 상기 광원의 광으로부터 상기 제1 키를 추출하고(예를 들면, 도 10의 단계 S12, 도 18의 단계 S108), 추출된 상기 제1 키에 의해 암호화해서 제2 키(예를 들면, 도 2의 암호키 K2)를 근거리 통신에 의해 송신하고(예를 들면, 도 10의 단계 S19, 도 18의 단계 S110의 처리), 암호화되어 있는 상기 제2 키를 수신해서 복호화하고(예를 들면, 도 12의 단계 S78, 도 20의 단계의 처리), 상기 제2 키를 공통 키로서 정보를 전송하는(예를 들면, 도 10의 단계 S20, 도 18의 단계 S111의 처리, 도 12의 단계 S79, 도 20의 단계 S179의 처리) 정보 처리 시스템 (예를 들면, 도 2의 정보 제공 시스템(1)) 또는 정보 처리 방법(예를 들면, 도 2의 정보 제공 시스템(1)의 정보 처리 방법)이다.

[0074] 본 발명의 다른 측면은, 광원(예를 들면, 도 2의 LED(32))으로부터 방출된 광선의 변화에 의해 제1 키(예를 들면, 도 2의 공개 키 K1)를 공개적으로 배신하는 배신 수단(예를 들면, 도 11의 단계 S42, 도 19의 단계 S147의 처리를 실행하는 도 7의 송신부(122))과, 배신된 상기 제1 키에 의해 암호화된 정보(예를 들면, 도 2의 암호키 K2)를 수신하는 수신 수단(예를 들면, 도 11의 단계 S47, 도 19의 단계 S146의 처리를 실행하는 도 7의 수신부(121))을 구비하는 정보 처리 장치(예를 들면, 도 2의 접속 서비스 장치(13))이다.

[0075] 상기 배신 수단은, 상기 제1 키로서 인증 기관에 의해 발행된 공개 키(예를 들면, 도 2의 공개 키 K1)를 배신할 수 있다.

[0076] 상기 수신 수단은, 상기 제1 키에 의해 암호화된 정보로서 제2 키(예를 들면, 도 2의 암호키 K2)를 수신하고, 상기 정보 처리 장치는, 수신된 상기 제2 키를 복호화하고, 공통 키를 얻는 복호 수단(예를 들면, 도 12의 단계

S78, 도 20의 단계 S178의 처리를 실행하는 도 8의 복호부(144))를 더 구비할 수 있다.

[0077] 상기 배신 수단은 액세스 포인트(예를 들면, 도 2의 액세스 포인트(31))에 설치되고, 상기 제1 키를 클라이언트(예를 들면, 도 2의 클라이언트(12))에 공개적으로 배신하고(예를 들어, 도 11의 단계 S42, 도 19의 단계 S147의 처리), 상기 수신 수단은 상기 액세스 포인트에 설치되고, 상기 클라이언트로부터 근거리 통신에 의해 송신된 상기 제2 키를 수신(예를 들면, 도 11의 단계 S47, 도 19의 단계 S148의 처리)할 수 있다.

[0078] 상기 배신 수단은, 상기 제1 키로서 인증 기관에 의해 발행된 공개 키(예를 들면, 도 2의 공개 키 K2)를 배신하고, 상기 액세스 포인트에는, 상기 인증 기관에 의해 증명되어 있는 것을 나타내는 정보를 게시(예를 들면, 도 15의 게시부(171)의 게시)할 수 있다.

[0079] 또한, 상기 배신 수단은, 상기 광원으로부터 방출된 광선의 변화에 의해 어드레스 값을 배신(예를 들면, 도 11의 단계 S42, 도 19의 단계 S141의 처리)할 수 있다.

[0080] 상기 광원은, 제공하는 정보에 관계되는 물체(예를 들면, 도 16의 포스터(204, 205))를 조명하는 조명 기구(예를 들면, 도 16의 조명 기구(202, 203))로 할 수 있다.

[0081] 상기 액세스 포인트는, 상기 조명 기구의 점멸을 제어하는 신호를 전력 선(예를 들면, 도 16의 전력선(201))을 통해서 송신할 수 있다.

[0082] 상기 광원은, 가시광 또는 적외광을 발생하는 LED(예를 들면, 도 2의 LED(32))로 할 수 있다.

[0083] 또한, 본 발명의 다른 측면은, 광원(예를 들면, 도 2의 LED(32))으로부터 방출된 광선의 변화에 의해 키(예를 들면, 도 2의 공개 키 K1)를 공개적으로 배신하고(예를 들면, 도 11의 단계 S42, 도 19의 단계 S147), 배신된 상기 키에 의해 암호화된 정보(예를 들면, 도 2의 암호키 K2)를 수신 하는(예를 들면, 도 11의 단계 S47, 도 19의 단계 S146) 단계를 구비하는 정보 처리 방법(예를 들면, 도 2의 접속 서비스 장치(13)의 정보 처리 방법), 컴퓨터에 실행시키는 프로그램, 또는 기록 매체다.

[0084] 본 발명의 또 다른 측면은, 광원이 공개적으로 발생하는 변화하는 광을 수광하는 수광 수단(예를 들면, 도 10의 단계 S11, 도 18의 단계 S108의 처리를 실행하는 도 6의 촬상부(101))과, 수광된 광으로부터 제1 키(예를 들면, 도 2의 공개 키 K1)를 판독하는 판독 수단(예를 들면, 도 10의 단계 S12, 도 18의 단계 S108의 처리를 실행하는 도 6의 판독부(102))과, 판독된 상기 제1 키에 의해 암호화해서 제2 키(예를 들면, 도 2의 암호키 K2)를 근거리 통신에 의해 송신하는 송신 수단(예를 들면, 도 10의 단계 S19, 도 18의 단계 S110의 처리를 실행하는 도 6의 송신부(107))과 상기 제2 키를 공통 키로서 정보를 전송하는 전송 수단(예를 들면, 도 10의 단계 S20, 도 18의 단계 S111의 처리를 실행하는 도 6의 전송 처리부(108))를 구비하는 정보 처리 장치다.

[0085] 또한, 상기 판독 수단은, 수광된 광에서 어드레스 값을 판독(예를 들면, 도 10의 단계 S12, 도 18의 단계 S102)할 수 있다.

[0086] 상기 어드레스 값에 대응하는 심볼(예를 들면, 도 2의 아이콘(23))을 표시하는 표시 수단(예를 들면, 도 6의 표시부(103))과, 상기 심볼의 선택을 판정하는 판정 수단(예를 들면, 도 10의 단계 S14, 도 18의 단계 S104의 처리를 실행하는 도 6의 판정부(104))를 더 구비할 수 있다.

[0087] 본 발명의 또 다른 측면은, 광원이 공개적으로 발생하는 변화하는 광을 수광하고(예를 들면, 도 10의 단계 S11, 도 18의 단계 S108), 수광된 광으로부터 제1 키(예를 들면, 도 2의 공개 키 K1)를 판독하고(예를 들면, 도 10의 단계 S12, 도 18의 단계 S108), 판독된 상기 제1 키에 의해 암호화해서 제2 키(예를 들면, 도 2의 암호키 K2)를 근거리 통신에 의해 송신하고(예를 들면, 도 10의 단계 S19, 도 18의 단계 S110), 상기 제2 키를 공통 키로서 정보를 전송하는(예를 들면, 도 10의 단계 S20, 도 18의 단계 S111) 단계를 구비하는 정보 처리 방법, 컴퓨터에 실행시키는 프로그램 또는 기록 매체다.

[0088] 이하, 본 발명의 실시예에 대해서 도면을 참조하여 설명한다.

[0089] 도 2는 본 발명의 실시예의 정보 처리 시스템으로서의 정보 제공 시스템의 구성을 나타내고 있다. 이 정보 제공 시스템(1)은, 인터넷(11), 클라이언트(12), 접속 서비스 장치(13), 서버(14, 15)로 구성되어 있다. 도 2에는, 클라이언트(12)가 1대만 나타나 있지만, 1개의 액세스 포인트(31)에 대하여 복수대의 클라이언트(12)가 접속되어도 좋다. 또한, 액세스 포인트(31)는, 필요한 개소에 분산되어서 임의의 대수가 배치된다.

[0090] PDA인 클라이언트(12)는 LCD(21)를 갖고 있다. 이 LCD(21)에는 필요한 화상이 적당히 표시된다. 클라이언트(12)의 카메라(22)는 피사체를 촬상하고, LCD(21)에 그 피사체의 화상을 표시한다.

[0091] 접속 서비스 장치(13)는 액세스 포인트(31)와 서버(34)로 구성되어 있다. 액세스 포인트(31)는, 광(가시광 또는 적외광)을 점멸해서 광 신호를 송신하는 LED(32)와, 무선으로 근거리 통신을 행할 경우에 이용되는 안테나(33)를 갖고 있다. 액세스 포인트(31)와 서버(34)는, 유선 또는 무선에 의해 서로 접속되어 있다. 또한, 서버(34)는 인터넷(11)에 접속되어 있다. 또한, 인터넷(11)에는 각종의 정보를 제공하는 서버(14, 15) 등이 접속되어 있다.

[0092] 또한, 클라이언트(12)와 액세스 포인트(31) 사이의 근거리 통신은, 예를 들면, IEEE 802.11b/a/g, UWB, Bluetooth, ZigBee 등을 이용하는 것이 가능하다. 여기에서 말하는 근거리 통신은, 광선의 변화에 의한 신호를 수광하여, 복호화할 수 있는 거리의 통신을 말한다. 구체적으로는, 몇 미터 내지 수십 미터의 거리의 무선에 의한 통신을 말한다.

[0093] 상세한 동작은 도 9와 도 11을 참조해서 후술하지만, 액세스 포인트(31)의 LED(32)는, 광을 점멸함으로써 액세스 포인트(31)의 어드레스와 공개 키 K1을 송신한다. 이 공개 키 K1은, 소정의 인증 기관에 의해 대응하는 비밀 키 와 함께, 접속 서비스 장치(13)의 관리자에 발행된 것, 또는 액세스 포인트의 사업자에 의해 독자적으로 작성된 것이다. 클라이언트(12)는, 이 액세스 포인트(31)의 화상을 카메라(22)로 촬상하고, 그 화상을 LCD(21)에 표시시킨다. 사용자는, 화상에 표시된, 공개 키 K1을 발하고 있는 액세스 포인트의 존재를 나타내는 아이콘(23)을 지시함으로써 액세스 포인트를 선택한다. 클라이언트(12)는, 수신한 화상으로부터 공개 키 K1을 추출하면, 스스로 발생한 암호키 K2를 그 공개 키 K1에 의해 암호화하고, 액세스 포인트(31)에 전파(근거리 통신)로 송신한다.

[0094] 액세스 포인트(31)는, 공개 키 K1에 의해 암호화되어 있는 암호키 K2를 서버(34)에 전송한다. 이에 따라 서버(34)는, 클라이언트(12) 사이에서 암호키 K2를 공유 키로서 공유할 수가 있어, 상호 간에 정보를 전송할 때 이용할 수 있다.

[0095] 도 3은 클라이언트(12)의 구성을 나타내고 있다. 촬상부(51)는 카메라(22)에 대응하고, 피사체를 촬상하며, 대응하는 화상 신호를 출력한다. 화상 처리부(52)는, 촬상부(51)에서 출력된 화상 신호를 처리하고, 표시부(53)에 출력하여, 표시시킨다. 표시부(53)는 LCD(21)에 대응한다.

[0096] 제어부(55)는, 예를 들면, 마이크로 컴퓨터(microcomputer) 등으로 구성되어, 촬상부(51), 화상 처리부(52), 표시부(53), 그 밖의 그 동작을 제어한다. 입력부(54)는, 스위치, 각종의 버튼 등으로 구성되어, 사용자에 의해 조작되면, 그 조작에 대응한 신호를 제어부(55)에 출력한다. 통신부(56)는, 액세스 포인트(31)와 전파로 통신을 행한다.

[0097] 탈착형 미디어(57)는 클라이언트(12)에 적당히 장착되어, 필요한 프로그램이나 데이터 등을 제어부(55)에 공급한다.

[0098] 도 4는 액세스 포인트(31)의 구성을 나타내고 있다. 발광부(73)는 LED(32)에 대응하고, 제어부(72)로 제어되어, 광의 레벨을 변화시키는 것으로 신호를 출력 한다(예를 들면, 광의 점멸 신호를 출력한다). 통신부(71)는, 안테나(33)를 통해서 클라이언트(12)와 무선으로 통신을 행한다. 또 통신부(71)는, 서버(34)와의 통신도 행한다. 기억부(74)에는, 클라이언트(12)에 대하여 송신하는 어드레스나 공개 키 K1이 기억된다.

[0099] 예를 들면, 마이크로 컴퓨터 등으로 구성되는 제어부(72)에는, 탈착형 미디어(75)가 적당히 접속된다. 탈착형 미디어(75)에는, 제어부(72)가 동작하는데도 필요한 프로그램이나 데이터 등이 기억되어 있다.

[0100] 도 5는 서버(34)의 구성을 나타내고 있다. 통신부(81)는, 액세스 포인트(31)나 인터넷(11)을 통해서 다른 장치와 통신을 행한다. 기억부(82)는, 액세스 포인트(31)에 공급하는 공개 키 등을 기억하고 있다. 표시부(83)는 필요한 화상이나 정보를 표시한다. 마이크로 컴퓨터 등으로 구성되는 제어부(85)는, 각 부의 동작을 제어한다. 입력부(84)는, 키보드나 마우스 등으로 구성되어, 사용자에 의해 조작되었을 때, 그 조작에 대응하는 신호를 제어부(85)에 공급한다.

[0101] 탈착형 미디어(86)는, 필요에 따라 서버(34)에 접속되어, 프로그램이나 데이터 등을 적당히 제어부(85)에 공급한다.

[0102] 클라이언트(12)의 제어부(55)는, 도 6에 나타내지는 것 같은 기능적 구성을 갖고있다. 또한, 도시는 생략하지만, 각 부는 필요에 따라 신호를 전송하는 것이 가능하게 되어 있다. 이것은, 후술하는 도 7과 도 8에 있어서도 마찬가지다.

[0103] 촬상부(101)는, 피사체의 화상을 촬상한다. 판독부(102)는, 촬상해서 얻을 수 있은 화상으로부터 어드레스 값

과 공개 키를 판독한다. 표시부(103)는, 표시부(53)에 대한 화상의 표시를 제어한다. 판정부(104)는 각종의 판정 처리를 행한다. 요구부(105)는, 액세스 포인트에 대하여 접속을 요구한다. 판독부(106)는 암호키를 판독하는 처리를 실행한다. 송신부(107)는, 공개 키에 의해 암호화된 암호 키를 액세스 포인트(31)에 송신하는 처리를 실행한다. 전송 처리부(108)는, 액세스 포인트(31)와 서버(34)를 통해서 서버(14, 15) 간에 정보를 전송하는 처리를 실행한다.

[0104] 도 7은 액세스 포인트(31)의 제어부(72)의 기능적 구성을 나타내고 있다. 수신부(121)는 공개 키를 서버(34)로부터 수신한다. 송신부(122)는 어드레스 값과 공개 키를 송신하거나, 접속 요구를 서버(34)에 송신하거나, 클라이언트(12)에 접속 응답을 송신한다. 또한, 송신부(122)는 암호키를 서버(34)에 송신한다. 판정부(123)는 각종의 판정 처리를 실행한다. 기억부(124)는 어드레스 값과 공개 키를 기억한다. 전송 처리부(125)는, 클라이언트(12)와 서버(34) 사이의 정보의 전송를 중개한다.

[0105] 도 8은 서버(34)의 제어부(85)의 기능적 구성을 나타내고 있다. 송신부(141)는, 공개 키를 액세스 포인트(31)에 송신하거나, 접속 응답을 액세스 포인트(31)에 송신한다. 수신부(142)는, 액세스 포인트(31)로부터 접속 요구를 수신한다. 판정부(143)는 각종의 판정 처리를 실행한다. 복호부(144)는, 암호 키를 비밀 키에 의해 복호화하는 처리를 실행한다. 전송 처리부(145)는, 액세스 포인트(31)와 서버(14, 15) 사이의 정보의 전송를 중개하는 처리를 실행한다.

[0106] 다음으로, 도 9 내지 도 12의 플로우차트를 참조하여, 클라이언트(12)가 액세스 포인트(31)를 통해서 서버(34)에 접속하고, 인터넷(11)을 통해서 서버(14, 15)로부터 필요한 정보의 제공을 받을 경우의 처리에 대해서 설명한다. 또한, 도 9는 클라이언트(12), 액세스 포인트(31),및 서버(34)의 전체의 동작을 나타내고, 도 10은 클라이언트(12)의 동작을 나타내고, 도 11은 액세스 포인트(31)의 동작을 나타내고, 도 12는 서버(34)의 동작을 나타내고 있다.

[0107] 단계 S71에서, 서버(34)의 송신부(141)는, 공개 키를 액세스 포인트에 송신한다. 구체적으로는, 통신부(81)는 기억부(82)에 기억되어 있는 공개 키를 판독하고, 액세스 포인트(31)에 송신한다.

[0108] 단계 S41에서, 액세스 포인트(31)의 수신부(121)는 공개 키를 수신한다. 그리고, 단계 S42에서, 송신부(141)는, 단계 S41에서 수신한 공개 키를 어드레스 값과 함께 클라이언트(12)에 송신한다.

[0109] 구체적으로는, 액세스 포인트(31)의 제어부(72)는, 통신부(71)에 의해 수신한 서버(34)로부터 송신되어 온 공개 키와, 기억부(74)로부터 판독한, 미리 기억되어 있는 어드레스 값(액세스 포인트(31)에 액세스하기 위한 어드레스 값)을, 발광부(73)를 제어함으로써 광의 점멸 신호로서 송신(브로드캐스트(broadcast)) 시킨다.

[0110] 송신되는 신호는 도 13에 도시된 바와 같이 맨체스터 부호화되어 있다. 이 맨체스터 부호화에서는, 상승 엣지(LED(32)가 소등하고 있는 상태로부터 점등하고 있는 상태로의 천이)가 0이라고 하고, 하강 엣지(LED(32)가 점등하고 있는 상태로부터 소등하고 있는 상태로의 천이)가 1이라고 한다. 이에 의해, 예를 들면 도 14에 도시된 바와 같이, 「010011」과 같은 데이터의 부호열이, 광의 점멸 신호로서 송신 된다(물론, 소등이라고 해도 완전하게 광이 발생하지 않는 상태일 필요는 없고, 광의 레벨이 보다 높은 레벨보다 낮은 레벨 사이에서 변화하면 된다. 즉, 수신측에서 검출이 가능한 정도에 광을 변화시키면 좋다).

[0111] 이렇게, 액세스 포인트(31)는, LED(32)를 점멸시킴으로써 자기 자신의 어드레스 값과 공개 키를 항상 브로드캐스트하고 있다(광, 따라서 어드레스 값과 공개 키를 공개적으로 배신하고 있다).

[0112] 그리고, 사용자는 클라이언트(12)의 카메라(22)를, 액세스를 희망하는 액세스 포인트(31)에 지향시켜, 입력부(54)를 조작하고, 액세스를 희망하는 액세스 포인트(31)의 촬상을 지시한다. 이때, 단계 S11에서, 촬상부(101)는 촬상하는 처리를 실행한다. 구체적으로는, 촬상부(51)에 의해 액세스 포인트(31)가 촬상되고, 그 화상 신호가 화상 처리부(52)에 의해 처리된 후, 표시부(53)(LCD(21))에 출력되어 표시된다.

[0113] 광은 직진성을 갖기 때문에, 지향시킨 방향의 액세스 포인트(31)만이 카메라(22)에 의해 촬상되고, 카메라(22)가 지향되지 않고 있는 방향에 액세스 포인트가 만났다고 한들, 그 액세스 포인트는 촬상되지 않는다. 따라서, 사용자는 의도하지 않는 액세스 포인트로부터의 광을 수광하므로, 피싱 사기의 피해를 받는 것이 억제된다.

[0114] 액세스 포인트의 사업자가 공개 키로서 소정의 인증국에 의해 발행된 것을 이용할 경우, 예를 들면, 도 15에 도시된 바와 같이, 액세스 포인트(31)의 게시부(171)에는, 이 액세스 포인트(31)가 소정의 인증 기관으로부터 인증을 받은 것을 나타내는 정보로서의 심벌 마크(172)가 게시되어 있다(도 15의 예에서는, "인증(Certification)"의 문자가 표시되어 있다). 또한, 이 게시부(171)에는, 심벌 마크(172)와 함께 인증일 "2005

년 6월 28일", 그리고 유효 기한 "2006년 6월 27일"이 게시되어 있다. 따라서, 사용자는, 표시된 화상으로부터 이 심벌 마크(172)와 인증일과 유효 기한을 확인함으로써, 그 액세스 포인트(31)가 적정하게 인증을 받은 진정인 액세스 포인트인 것을 확인할 수 있다. 이에 따라 안전성을 확보할 수 있다.

[0115] 판독부(102)는, 단계 S12에서, 촬상부(101)에 의해 촬상된 화상을 분석 함으로써(점멸 신호(맨체스터 부호)을 복호화함으로써), 어드레스 값과 공개 키를 점멸 신호로부터 판독한다. 그리고, 단계 S13에서, 표시부(103)는, 단계 S12의 처리에서 판독된 어드레스 값에 대응하는 심볼로서의 아이콘을 LCD(21)에 표시시킨다. 이에 의해, 예를 들면 도 2에 도시된 바와 같이, 액세스 포인트(31)의 화상(31A)의 근방에, 거기에 대응하는 어드레스 "어드레스1"이 아이콘(23)으로서 LCD(21)에 표시된다.

[0116] 사용자는, 이 어드레스(아이콘)로부터, 그 액세스 포인트가 액세스를 희망하는 액세스 포인트인 것인지를 다시 확인하고, 확인한 아이콘을 손가락 등으로 지정함으로써, 액세스하는 액세스 포인트를 지정한다. 따라서, 단계 S14에서, 판정부(104)는, 아이콘이 사용자에 의해 선택되었는지를 판정한다. 아이콘이 선택되지 않은 경우에는, 단계 S15에서, 판정부(104)는 종료가 지시되었는지를 판정한다. 사용자에 의해 종료가 아직 지시되지 않고 있을 경우에는, 처리는 단계 S11로 되돌아가고, 그 이후의 처리가 반복해 실행된다. 즉, 아이콘(23)이 선택될 때까지 단계 S11 내지 단계 S15의 처리가 반복해 실행되게 된다.

[0117] 사용자에 의해 아이콘(23)이 선택되면, 단계 S16에서, 요구부(105)는 액세스 포인트에 접속을 요구한다. 즉, 통신부(56)는 제어부(55)에 의해 제어되어, 근거리 통신에 의해 무선에서 액세스 포인트(31)에 대하여 접속을 요구하는 신호를 송신한다.

[0118] 액세스 포인트(31)는, 단계 S43에서, 접속 요구를 수신했는지를 판정부(123)가 판정한다. 수신부(121)에 의해 접속 요구가 아직 수신되지 않은 경우에는, 처리는 단계 S41으로 되돌아가고, 그 이후의 처리가 반복해 실행된다.

[0119] 단계 S43에서, 수신부(121)에 의해 접속 요구가 수신되었다고 판정되었을 경우, 단계 S44에서, 송신부(122)는 접속 요구를 서버에 전송한다. 즉, 액세스 포인트(31)의 통신부(71)는, 클라이언트(12)로부터 수신한 접속 요구를 서버(34)에 전송한다.

[0120] 서버(34)에서는, 판정부(143)가 단계 S72에서 액세스 포인트로부터 접속 요구를 수신했는지를 판정하고, 아직 수신하지 않은 경우에는, 처리는 단계 S71로 되돌아가고, 액세스 포인트로부터 접속 요구를 수신할 때까지 단계 S71, S72의 처리가 반복해 실행된다.

[0121] 액세스 포인트(31)로부터 접속 요구를 수신했다고 판정되었을 경우, 단계 S73에서, 판정부(143)는 응답 가능인가를 판정한다. 즉, 지금, 많은 클라이언트로부터 액세스가 요구되어 있는지 등과 같이, 응답이 곤란할지를 판정한다. 응답이 가능할 경우, 단계 S74에서, 송신부(141)는 OK의 접속 응답을 액세스 포인트(31)에 송신하는 처리를 실행한다. 이것에 대하여, 단계 S73에서, 응답이 가능하지 않다고 판정되었을 경우에는, 단계 S75에서, 송신부(141)는 NG의 접속 응답을 액세스 포인트에 송신하는 처리를 실행한다.

[0122] 액세스 포인트(31)의 판정부(123)는, 단계 S45에서, 서버로부터 접속 응답을 수신했는지를 판정하고, 접속 응답을 수신할 때까지 대기한다. 서버(34)로부터 접속 응답을 수신했을 경우, 단계 S46에서, 송신부(122)는 액세스해 온 클라이언트에 접속 응답을 송신한다.

[0123] 클라이언트(12)의 판정부(104)는, 단계 S17에서, 액세스 포인트로부터 응답이 있는지 판정하고, 액세스 포인트로부터 응답이 있을 때까지 대기한다. 그리고, 액세스 포인트(31)로부터 응답이 있을 경우에는, 단계 S18에서, 판독부(106)는 암호키를 판독한다. 이 암호키는, 이미 생성된 것이어도 좋고, 할 때마다 판독부(106)가 생성하는 것 이어도 된다.

[0124] 다음으로, 단계 S19에서, 송신부(107)는 단계 S18에서 판독한 암호키를 공개 키를 사용하여 암호화해서 송신하는 처리를 실행한다. 즉, 단계 S12에서 판독된 공개 키에 의해 단계 S18에서 판독된 암호키가 암호화되어, 액세스 포인트(31)에 송신된다.

[0125] 액세스 포인트(31)의 판정부(123)는, 단계 S47에서, 암호키를 수신했는지를 판정하고, 수신할 때까지 대기한다. 암호키를 수신했을 경우, 단계 S48에서, 송신부(122)는 단계 S47에서 수신한 암호키를 서버(34)에 송신한다.

[0126] 서버(34)의 판정부(143)는, 단계 S76에서, 암호키를 수신했는지를 판정하고, 암호키를 아직 수신하지 않고 있을 경우에는, 단계 S77에서 타임 오버코트(overcoat)인가를 판정한다. 즉, 단계 S74, S75에서, 접속 응답을 송신한 후, 미리 설정해 있는 소정의 시간이 경과했는지가 판정되어, 아직 설정한 소정의 시간이 경과하지 않고 있

을 경우에는, 단계 S76에 되돌아가고, 그 이후의 처리가 반복해 실행된다. 미리 설정한 소정의 시간이 경과했다고 판정되었을 경우, 처리는 종료된다.

[0127] 단계 S76에서 암호키가 수신되었다고 판정되었을 경우, 단계 S78에서, 복호부(144)는, 암호 키를 비밀 키와 복합하는 처리를 실행한다. 즉, 단계 S76에서 수신부(142)에 의해 수신된 암호키가, 단계 S71에서 송신된 공개키에 대응하는 비밀키로 복호화된다. 이에 의해, 클라이언트(12)과 서버(34) 사이에서 공통 키로서의 암호키가 공유된 것으로 된다.

[0128] 따라서, 서버(34)의 전송 처리부(145)는 단계 S79에서, 또한, 클라이언트(12)의 전송 처리부(108)는 단계 S20에서, 또한 액세스 포인트(31)의 전송 처리부(125)는 단계 S49에서, 각각 정보 전송 처리를 실행한다. 구체적으로는, 클라이언트(12)의 전송 처리부(108)는, 단계 S20에서 액세스 포인트(31)에 필요한 정보를 송신한다. 액세스 포인트(31)의 전송 처리부(125)는, 단계 S49에서 클라이언트(12)로부터의 신호를 서버(34)에 전송한다. 서버(34)의 전송 처리부(145)는 단계 S79에서, 액세스 포인트(31)를 통해서 클라이언트(12)로부터 송신되어 온 액세스 정보에 기초하여, 인터넷(11)을 통해, 예를 들면 서버(14)에 액세스하고, 거기에 접속시킨다.

[0129] 서버(14)로부터 송신된, 예를 들면, 홈 페이지 등의 데이터는, 인터넷(11)을 통해서 서버(34)의 전송 처리부(145)에 의해 수신되어, 단계 S79에서 액세스 포인트(31)에 송신된다. 액세스 포인트(31)의 전송 처리부(125)는, 단계 S49에서 서버(34)로부터의 데이터를 수신하면, 이것을 클라이언트(12)에 전송한다. 클라이언트(12)의 전송 처리부(108)는 단계 S20에서, 서버(34)와 액세스 포인트(31)를 통해서 서버(14)로부터 수신한 데이터를, 예를 들면, LCD(21)에 출력하여 표시시킨다.

[0130] 이상과 같이 하면, 사용자는 ID나 패스워드를 필요로 하지 않기 때문에 사전의 등록이 불필요해진다. 그리고, 사용자는 사전의 등록 없이, 필요에 응해서 액세스 포인트(31)를 통해서 서버(34)로부터 인터넷(11)에 액세스하는 것이 가능하게 된다. 따라서, 사용자는, 임의의 장소에서(단, 액세스 포인트(31)가 존재하는 장소에서) 신속하고 자유롭게 인터넷(11)을 통해서 소정의 서버(14, 15)에 액세스하고, 필요한 정보의 제공을 받는 것이 가능하게 된다. 정보 제공자도 임의인 장소에 액세스 포인트를 설치함으로써, 신속하고 자유롭게 정보를 제공하는 것이 가능하게 된다.

[0131] 또한, 사용자가 실제로 점멸하는 LED(32)를 촬상한 화상으로부터 검출된 어드레스 값과 공개 키가 이용되므로, 숨은 위치에서 발생된 부정한 전파를 수신해서 무선 LAN 피싱 피해를 받는 것 같은 것이 억제된다. 따라서, 정보의 안전한 전송이 가능하게 된다. 또한 액세스 포인트(31)를 통해서 행해지는 클라이언트(12)와 서버(34)의 통신은, 암호키 K2로 암호화되기 때문에, 비밀성을 확보 할 수 있다.

[0132] 또한, 접속 서비스 장치(13)를 구성하는 액세스 포인트(31)와 서버(34)는, 떨어진 위치에 배치된 구성으로 했지만, 양자를 일체적으로 구성하는 것도 물론 가능하다.

[0133] 이상에서는, 광원으로서의 LED(32)와 액세스 포인트(31)가 일체화되어 있었지만, 광원을 액세스 포인트(31)로부터 떨어진 위치에 배치하는 것도 가능하다. 도 16은, 이 경우의 실시예를 나타내고 있다. 즉, 이 실시예에서는, LED로 이루어지는 조명 기구(202)가 포스터(204)를 조명하고 있고, LED로 이루어지는 조명 기구(203)가 포스터(205)를 조명하고 있다. 또한, LED로 이루어지는 조명 기구(206)가, 각종의 상품을 진열하고 있는 진열장(207)을 조명하고 있다. 조명 기구(202, 203, 206)에는, 전력선(201)을 통해서 필요한 전력이 공급되고 있다. 액세스 포인트(31)도 이 전력선(201)에 접속되고 있고, 액세스 포인트(31)는 이 전력선(201)을 통해, 조명 기구(202, 203, 206)를 제어하고, 그것들을 점멸시킨다.

[0134] 도 16의 실시예에서는, 클라이언트(12)의 카메라(22)에 의해, 포스터(204, 205)가 촬상되고 있다. 따라서, 그 LCD(21)에는, 포스터(204)의 화상(204A)와 포스터(205)의 화상(205A)가 표시되고, 각각에 대응하는 아이콘(23-1, 23-2)가 표시되어 있다. 사용자는, 그 어느 한쪽의 아이콘을 손가락 등으로 선택함으로써, 한쪽의 아이콘을 선택할 수 있다.

[0135] 이 경우, 조명 기구(202)는, 그 점멸 신호에 의해 포스터(204)에 관한 정보를 제공하는 URL을 제공하고, 조명 기구(203)도 마찬가지로 그 점멸 신호에 의해 포스터(205)에 관련되는 URL을 제공하고 있다. 조명 기구(206)는, 그 점멸 신호에 의해 진열장(207)에 진열되어 있는 상품에 관한 정보를 제공하는 URL을 제공한다.

[0136] 도 17 내지 도 20은 또 다른 실시예의 동작을 나타내고 있다. 이 실시예에서는, 액세스 포인트(31)가, 통상은 어드레스만을 브로드캐스트하고 있고, 적어도 1개의 클라이언트(12)가 액세스해 왔을 때 공개 키가 송신된다. 그 밖의 처리는, 도 9 내지 도 12에 있어서의 처리와 기본적으로 마찬가지다.

[0137] 즉, 보다 상세하게는, 우선 도 12의 단계 S71 내지 단계 S79에 대응하는 도 20의 단계 S171 내지 S179의 처리 중, 도 12의 단계 S71에서 행해지고 있었던 공개 키의 액세스 포인트에 대한 송신 처리가, 도 20의 실시예에서는, 단계 S173, S174의 액세스 포인트에 대한 접속 응답의 송신 처리의 다음 단계 S175에서 행해진다. 그 밖의 처리는, 도 12에 있어서의 경우와 마찬가지이다.

[0138] 도 11의 단계 S41 내지 S49에 대응하는 도 19의 단계 S141 내지 S150의 액세스 포인트(31)의 처리에 있어서도, 도 11에 있어서의 경우에는, 단계 S41에서 공개 키가 수신되어 있었지만, 도 19의 실시예에서는, 단계 S145에서 액세스해 온 클라이언트에 접속 응답을 송신하는 처리가 행해진 후, 단계 S146에서 행해진다. 그 밖의 처리는, 도 11에서의 경우와 마찬가지이다.

[0139] 또한, 도 10의 단계 S11 내지 S20에 대응하는 도 18의 단계 S101 내지 S111의 클라이언트(12)의 처리에서는, 도 18에 도시된 바와 같이, 도 10의 단계 S12에서는 어드레스 값과 공개 키의 양방이 판독되어 있었지만, 도 18의 단계 S102에서는 어드레스 값만이 판독된다. 그 대신에, 도 18의 단계 S107에서, 액세스 포인트로부터 응답이 있다고 판정되었을 경우, 다음 단계 S108에서 액세스 포인트로부터 송신되어 온 광의 점멸 신호가 촬상부(101)에 의해 수신(촬상)되어, 수신된 신호로부터 판독부(102)에 의해 공개 키를 판독하는 처리가 실행된다. 그 밖의 처리는, 도 10에서의 경우와 마찬가지이다.

[0140] 이 실시예에서도, 도 9의 실시예와 마찬가지의 효과를 발휘할 수 있다.

[0141] 이상에서는, 광의 검출을 면에서 행하도록 했지만(카메라에서 촬상하도록 했지만), 점에서 행하도록 해도 된다. 예를 들면, 1개의 적외광 수광 소자에서 적외광을 수광하고, 그 레벨의 변화를 검출하도록 하여도 된다. 이 경우에도, 광은 직진성을 가지므로, 사용자는, 적외광 수광부가 지향하는 방향을 확인함으로써, 지금 어느 액세스 포인트의 발생하는 적외광을 수광하고 있는 것인지를 인식할 수 있다. 따라서, 숨은 위치로부터 발생되는 광을 수광하여, 피싱 사기의 피해를 받는 것이 억제된다.

[0142] 도 21은 전술한 일련의 처리를 프로그램에 의해 실행하는 퍼스널 컴퓨터의 구성을 도시하는 블록도다. CPU(221)는, ROM(222), 또는 기억부(228)에 기억되어 있는 프로그램에 따라서 각종의 처리를 실행한다. RAM(223)에는, CPU(221)가 실행하는 프로그램이나 데이터 등이 적당히 기억된다. 이것들의 CPU(221), ROM(222), 및 RAM(223)은, 버스(224)에 의해 서로 접속되어 있다.

[0143] 또한, CPU(221)에는, 버스(224)를 통해서 입출력 인터페이스(225)가 접속되어 있다. 입출력 인터페이스(225)에는, 키보드, 마우스, 마이크로폰 등으로 이루어진 입력부(226), 디스플레이, 스피커 등으로 이루어지는 출력부(227)가 접속되어 있다. CPU(221)는, 입력부(226)로부터 입력되는 명령에 대응해서 각종의 처리를 실행한다. 그리고, CPU(221)은, 처리의 결과를 출력부(227)에 출력한다.

[0144] 입출력 인터페이스(225)에 접속되어 있는 기억부(228)는, 예를 들면, 하드 디스크로 이루어지고, CPU(221)가 실행하는 프로그램이나 각종의 데이터를 기억한다. 통신부(229)는, 인터넷이나 LAN 등의 네트워크를 통해서 외부의 장치와 통신한다. 또한, 통신부(229)를 통해서 프로그램을 취득하고, 기억부(228)에 기억하여도 된다.

[0145] 입출력 인터페이스(225)에 접속되어 있는 드라이브(230)는, 자기 디스크, 광 디스크, 광 자기 디스크, 혹은 반도체 메모리 등의 탈착형 미디어(231)가 장착되었을 때, 그것들을 구동하고, 거기에 기록되어 있는 프로그램이나 데이터 등을 취득한다. 취득된 프로그램이나 데이터는, 필요에 따라, 기억부(228)에 전송되어 기억된다.

[0146] 전술한 일련의 처리는, 하드웨어에 의해 실행시키는 것도 할 수 있고, 소프트웨어에 의해 실행시킬 수도 있다. 일련의 처리를 소프트웨어에 의해 실행시킬 경우에는, 그 소프트웨어를 구성하는 프로그램이, 전용의 하드웨어에 내장되어 있는 컴퓨터, 또는, 각종의 프로그램을 인스톨하는 것으로, 각종의 기능을 실행하는 것이 가능한, 예를 들면 범용의 퍼스널 컴퓨터 등에, 프로그램 저장 매체로부터 인스톨된다.

[0147] 컴퓨터에 인스톨되어, 컴퓨터에 의해 실행 가능한 상태로 되는 프로그램을 저장하는 프로그램 저장 매체는, 도 21에 도시한 바와 같이 자기 디스크(플렉시블 디스크를 포함함), 광 디스크(CD-ROM, MD 등을 포함함), 혹은 반도체 메모리 등으로 이루어지는 패키지 미디어인 탈착형 미디어(231), 또는, 프로그램이 일시적 혹은 영속적으로 저장되는 ROM(222)이나, 기억부(228)를 구성하는 하드 디스크 등으로 구성된다. 프로그램 저장 매체에의 프로그램의 저장은, 필요에 따라, 라우터, 모뎀 등의 인터페이스인 통신부(229)를 통해, LAN, 인터넷, 디지털 위성 방송과 같은, 유선 또는 무선의 통신 매체를 이용해서 행해진다.

[0148] 또한, 본 명세서에서, 프로그램 저장 매체에 저장되는 프로그램을 기술하는 단계는, 기재된 순서에 따라 시계열적으로 행해지는 처리는 물론, 반드시 시계열적으로 처리되지 않더라도, 병렬적 혹은 개별로 실행되는 처리도

포함하는 것이다.

[0149] 또한, 본 명세서에서, "시스템"은 복수의 장치로 구성되는 장치 전체를 나타내는 것이다.

[0150] 또한, 본 발명의 실시예는, 전술한 실시예에 한정되는 것은 아니고, 본 발명의 요지를 일탈하지 않는 범위에 있어서 다양한 변경이 가능하다.

발명의 효과

[0151] 이상과 같이, 본 발명의 제1 측면에 따르면, 정보를 전송 및 수신할 수 있다. 특히, 본 발명의 제1 측면에 따르면, 신속하고 자유롭게, 그리고 안전하게 정보를 전송 및 수신할 수 있다.

도면의 간단한 설명

[0001] 도 1은 종래의 액세스 포인트의 동작을 설명하는 플로우차트다.

[0002] 도 2는 본 발명의 실시예의 정보 제공 시스템의 구성을 나타내는 도면이다.

[0003] 도 3은 클라이언트의 구성을 도시하는 블록도다.

[0004] 도 4는 액세스 포인트의 구성을 도시하는 블록도다.

[0005] 도 5는 서버의 구성을 도시하는 블록도다.

[0006] 도 6은 클라이언트의 제어부의 기능적 구성을 도시하는 블록도다.

[0007] 도 7은 액세스 포인트의 제어부의 기능적 구성을 도시하는 블록도다.

[0008] 도 8은 서버의 제어부의 기능적 구성을 도시하는 블록도다.

[0009] 도 9는 도 2의 정보제공 시스템의 동작을 설명하는 플로우차트다.

[0010] 도 10은 클라이언트의 처리를 설명하는 플로우차트다.

[0011] 도 11은 액세스 포인트의 동작을 설명하는 플로우차트다.

[0012] 도 12는 서버의 동작을 설명하는 플로우차트다.

[0013] 도 13은 맨체스터 부호화의 0과 1을 설명하는 도면이다.

[0014] 도 14는 데이터 부호화 열의 예를 도시하는 도면이다.

[0015] 도 15는 인증 기관의 심벌 마크의 게시 예를 도시하는 도면이다.

[0016] 도 16은 본 발명의 실시예의 다른 구성을 나타내는 도면이다.

[0017] 도 17은 도 16의 실시예의 처리를 설명하는 플로우차트다.

[0018] 도 18은 클라이언트의 처리를 설명하는 플로우차트다.

[0019] 도 19는 액세스 포인트의 처리를 설명하는 플로우차트다.

[0020] 도 20은 서버의 처리를 설명하는 플로우차트다.

[0021] 도 21은 퍼스널 컴퓨터의 구성을 도시하는 블록도다.

[0022] <도면의 주요 부분에 대한 부호의 설명>

[0023] 1: 정보 제공 시스템

[0024] 11: 인터넷

[0025] 12: 클라이언트

[0026] 13: 접속 서비스 장치

[0027] 14, 15: 서버

[0028] 21: LCD

[0029] 22: 카메라

[0030] 23: 아이콘

[0031] K1, K2: 암호키

[0032] 31: 액세스 포인트

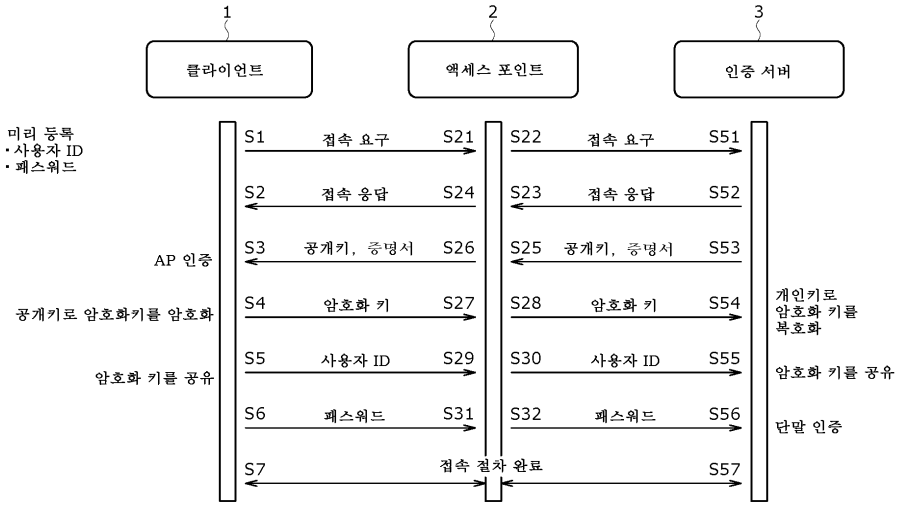
[0033] 32: LED

[0034] 33: 안테나

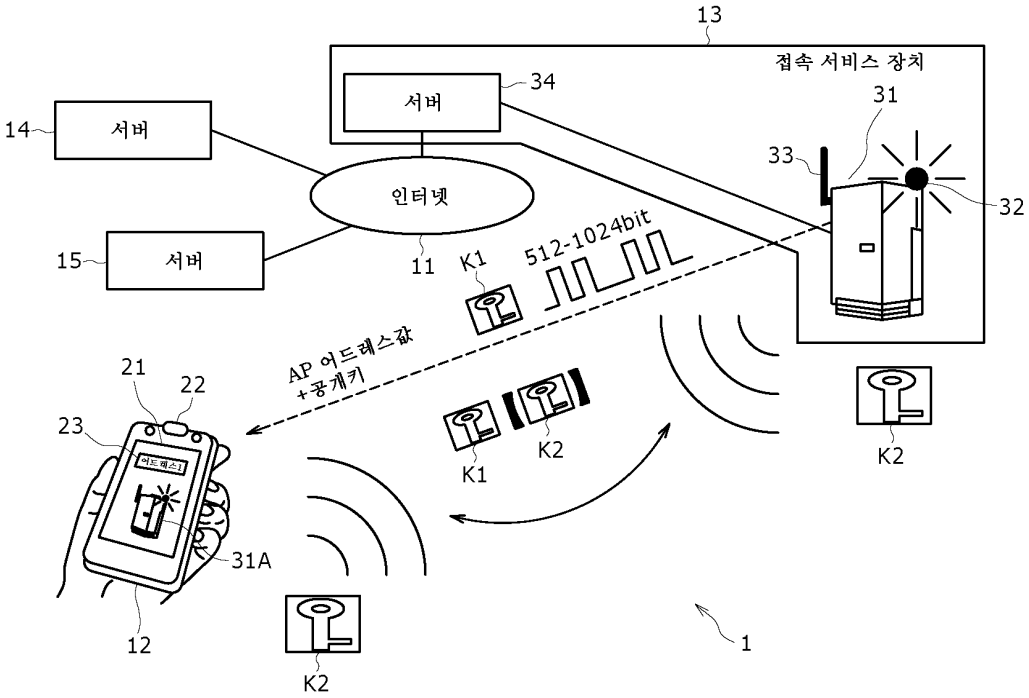
[0035] 34: 서버

도면

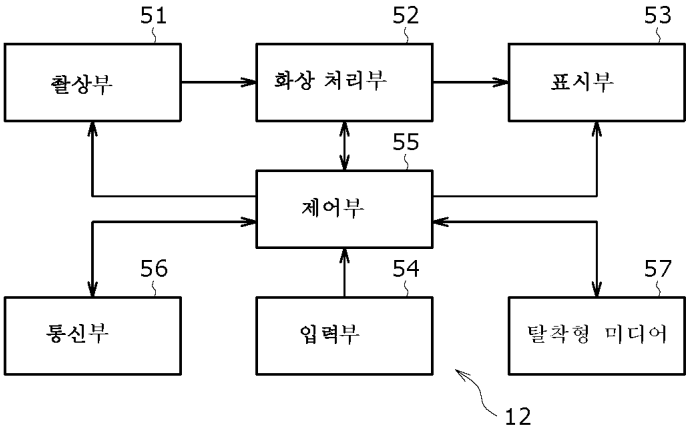
도면1



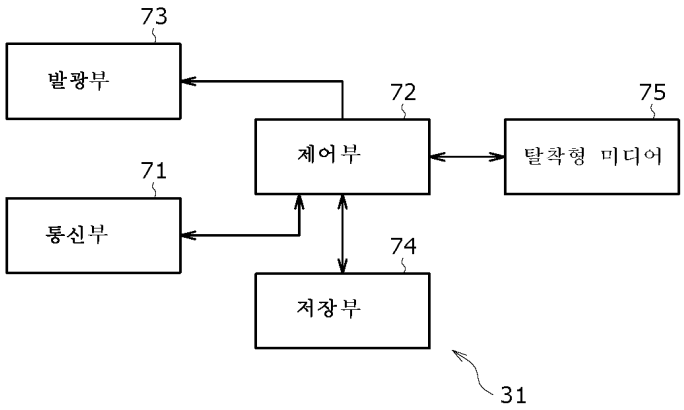
도면2


13
접속 서비스 장치
34
서버
14
서버
31
33
32
인터넷
15
서버
11
K1
512-1024bit
AP 어드레스값
+공개키
21
22
23
31A
12
K1
K2
K2
K2
1

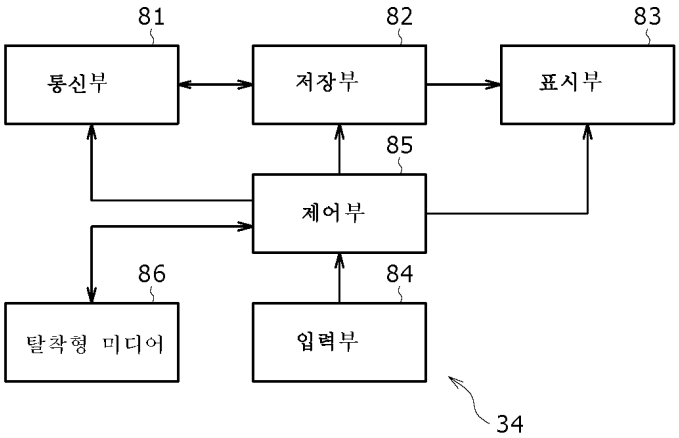
도면3


51
52
53
촬상부
화상 처리부
표시부
55
제어부
56
54
57
통신부
입력부
탈착형 미디어
12

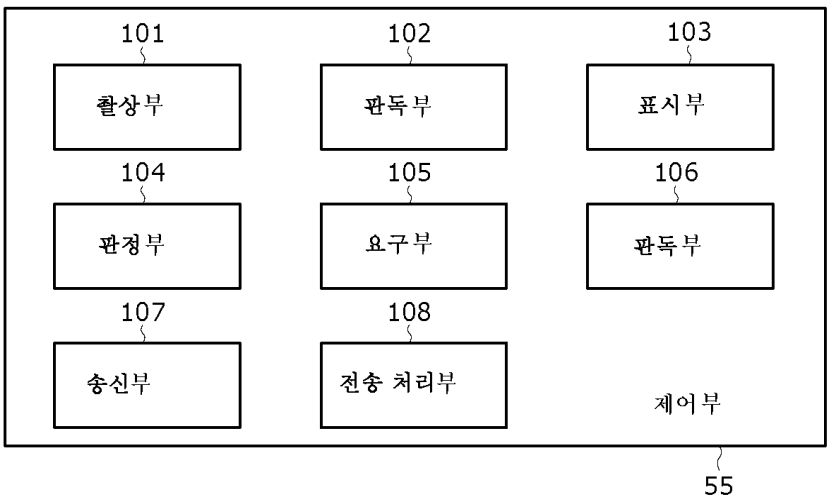
도면4


73
발광부
72
제어부
75
탈착형 미디어
71
통신부
74
저장부
31

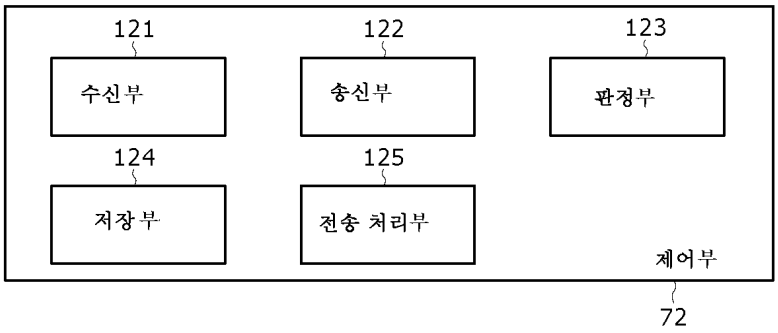
도면5


81
통신부
82
저장부
83
표시부
85
제어부
86
탈착형 미디어
84
입력부
34

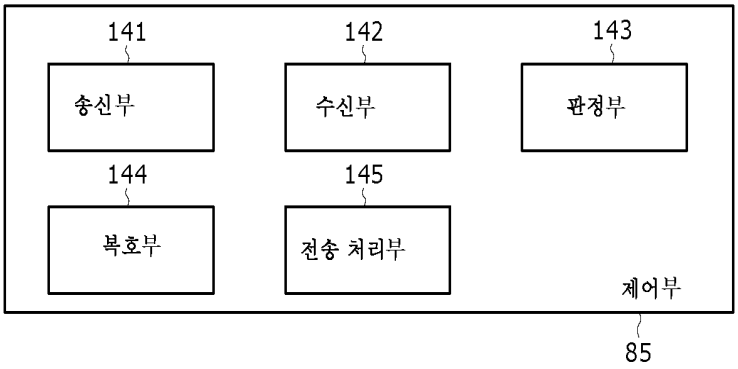
도면6


101
촬상부
102
판독부
103
표시부
104
판정부
105
요구부
106
판독부
107
송신부
108
전송 처리부
제어부
55

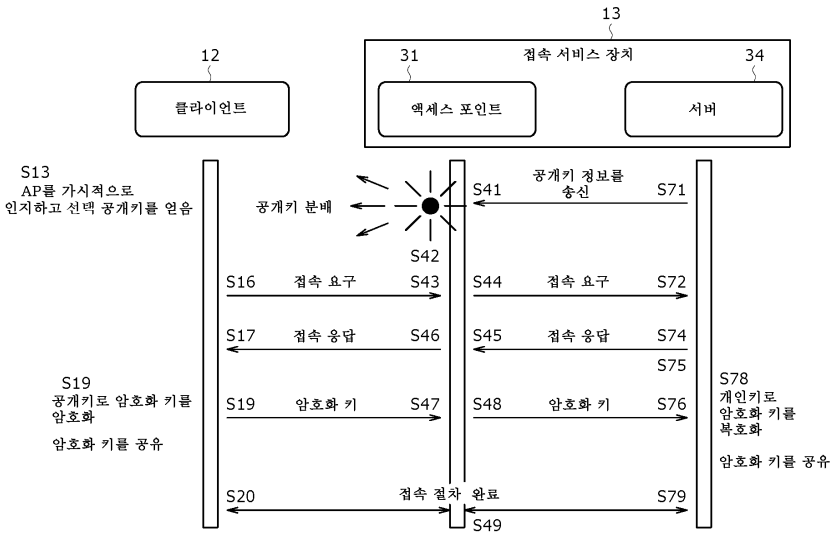
도면7


121
수신부
122
송신부
123
판정부
124
저장부
125
전송 처리부
제어부
72

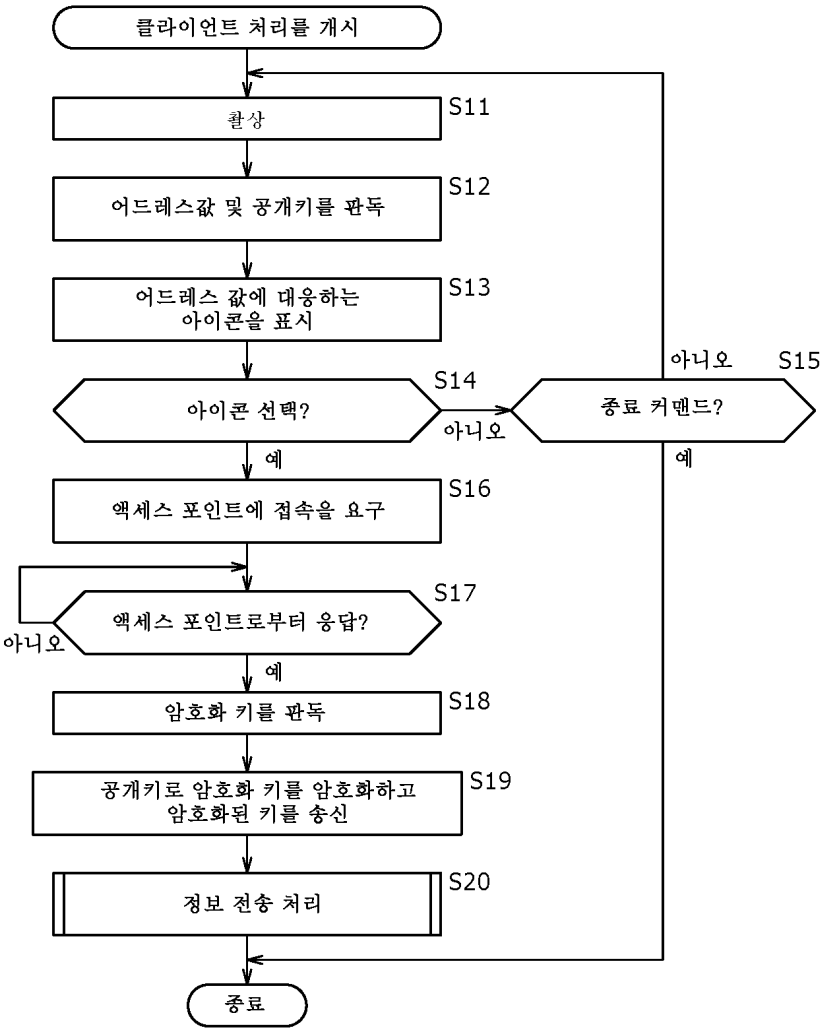
도면8


141
송신부
142
수신부
143
판정부
144
복호부
145
전송 처리부
제어부
85

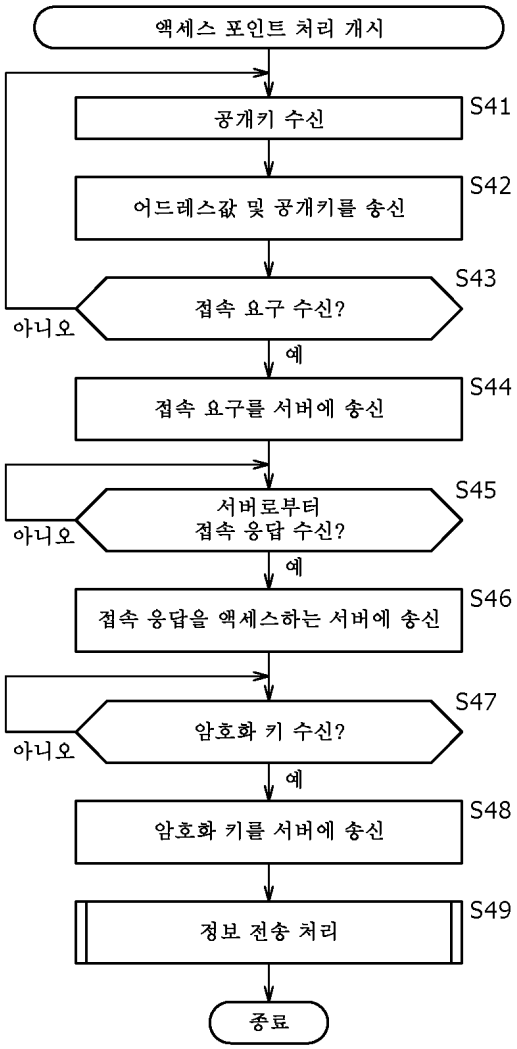
도면9


13
12
31
접속 서비스 장치
34
클라이언트
액세스 포인트
서버
S13
AP를 가시적으로
인지하고 선택 공개키를 얻음
공개키 분배
S41
공개키 정보를
송신
S71
S42
S16
접속 요구
S43
S44
접속 요구
S72
S17
접속 응답
S46
S45
접속 응답
S74
S75
S19
공개키로 암호화 키를
암호화
암호화 키를 공유
S19
암호화 키
S47
S48
암호화 키
S76
S78
개인키로
암호화 키를
복호화
암호화 키를 공유
S20
접속 절차 완료
S79
S49

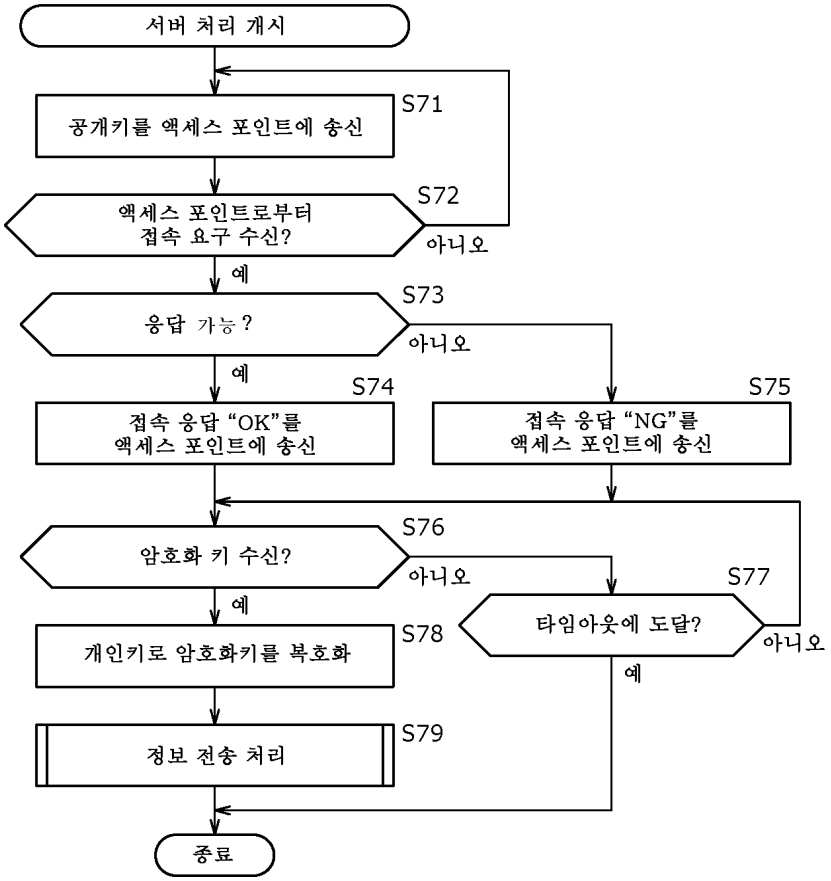
도면10


클라이언트 처리를 개시
촬상
S11
어드레스값 및 공개키를 판독
S12
어드레스 값에 대응하는
아이콘을 표시
S13
아이콘 선택?
S14
아니오
종료 커맨드?
S15
아니오
예
액세스 포인트에 접속을 요구
S16
액세스 포인트로부터 응답?
S17
아니오
예
암호화 키를 판독
S18
공개키로 암호화 키를 암호화하고
암호화된 키를 송신
S19
정보 전송 처리
S20
종료

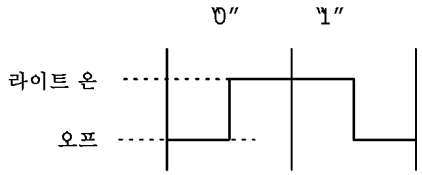
도면11


액세스 포인트 처리 개시
공개키 수신
S41
어드레스값 및 공개키를 송신
S42
접속 요구 수신?
S43
아니오
예
접속 요구를 서버에 송신
S44
서버로부터
접속 응답 수신?
S45
아니오
예
접속 응답을 액세스하는 서버에 송신
S46
암호화 키 수신?
S47
아니오
예
암호화 키를 서버에 송신
S48
정보 전송 처리
S49
종료

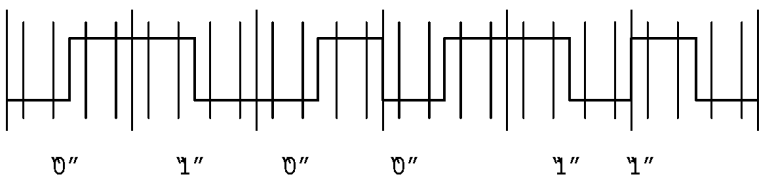
도면12



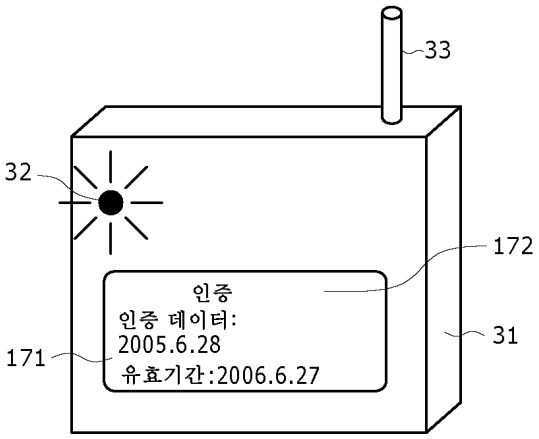
도면13



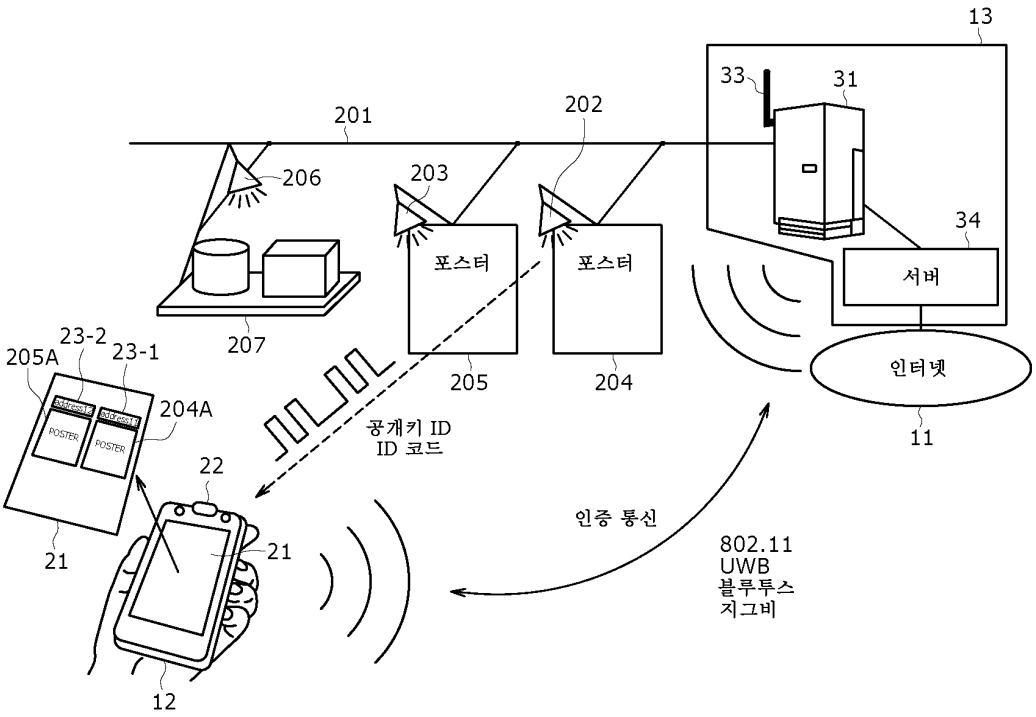
도면14



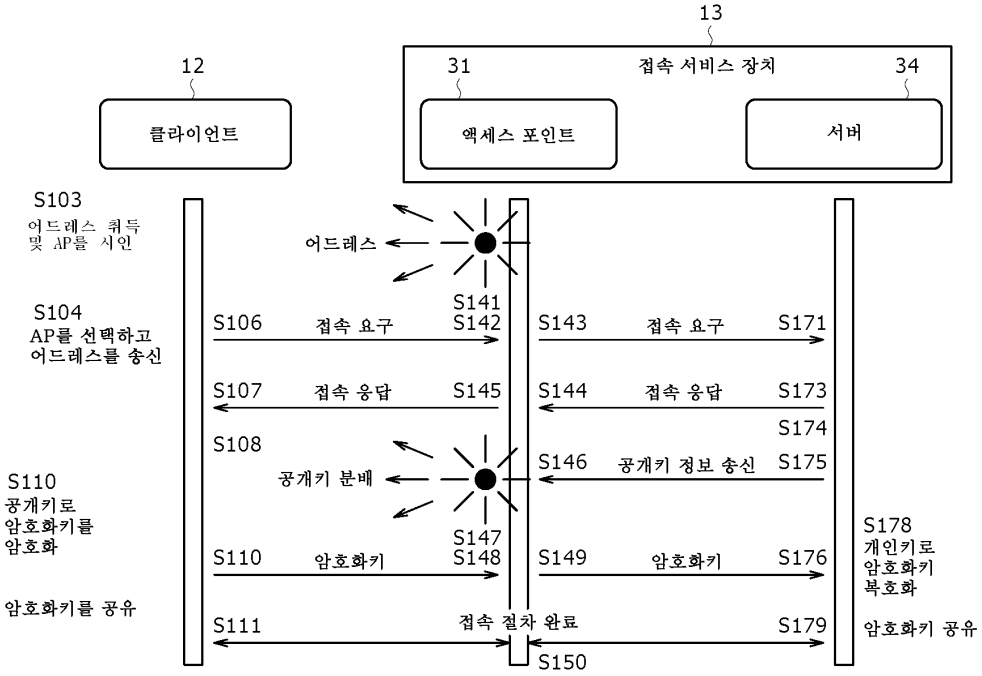
도면15


33
32
172
인증
인증 데이터:
2005.6.28
유효기간:2006.6.27
171
31

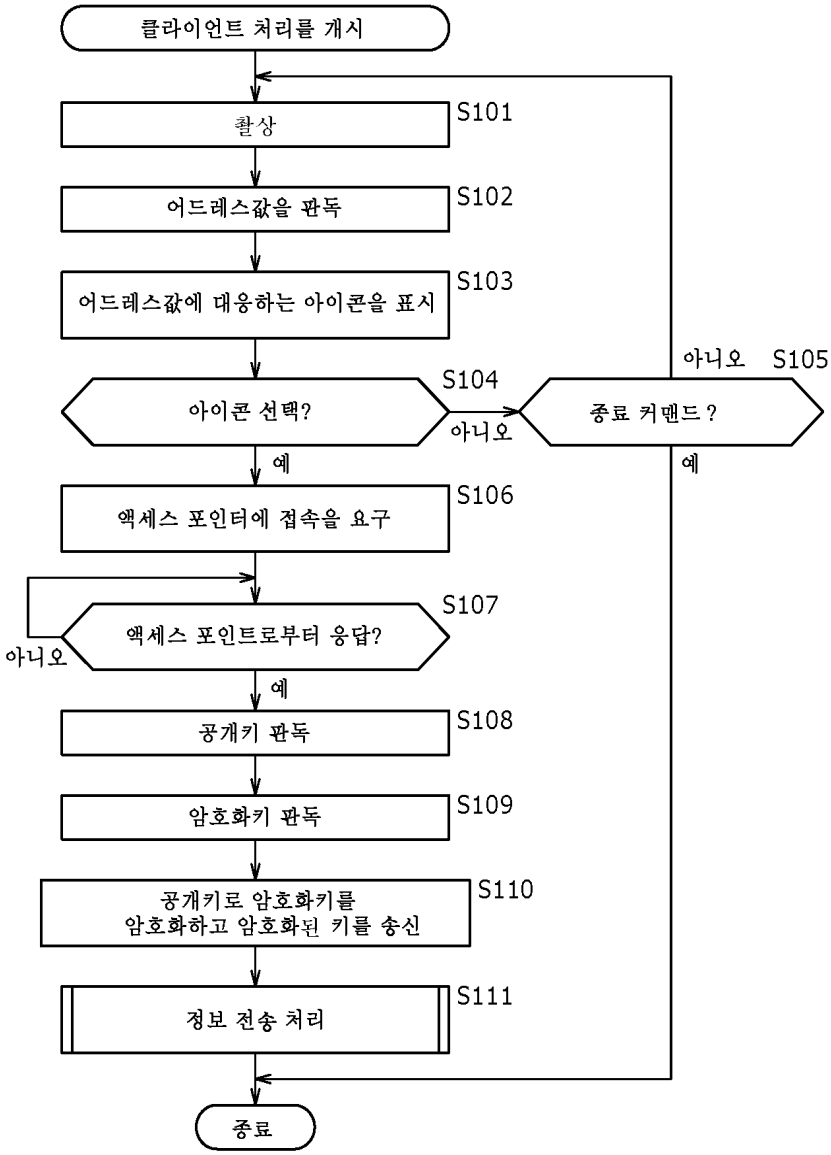
도면16


13
33
31
201
202
206
203
34
포스터
포스터
서버
23-2
205A
23-1
207
205
204
인터넷
11
204A
공개키 ID
ID 코드
22
인증 통신
802.11
UWB
블루투스
지그비
21
21
12

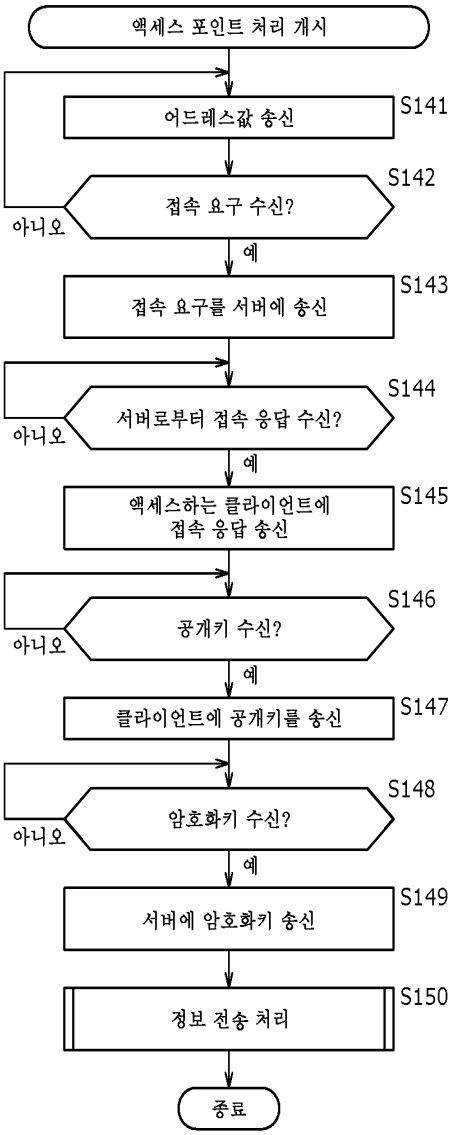
도면17


13
12
31
접속 서비스 장치
34
클라이언트
액세스 포인트
서버
S103
어드레스 취득
및 AP를 시인
어드레스
S141
S104
AP를 선택하고
어드레스를 송신
S106
접속 요구
S142
S143
접속 요구
S171
S107
접속 응답
S145
S144
접속 응답
S173
S174
S108
S146
공개키 정보 송신
S175
S110
공개키로
암호화키를
암호화
공개키 분배
S147
S178
개인키로
암호화키
복호화
S110
암호화키
S148
S149
암호화키
S176
암호화키를 공유
S111
접속 절차 완료
S179
암호화키 공유
S150

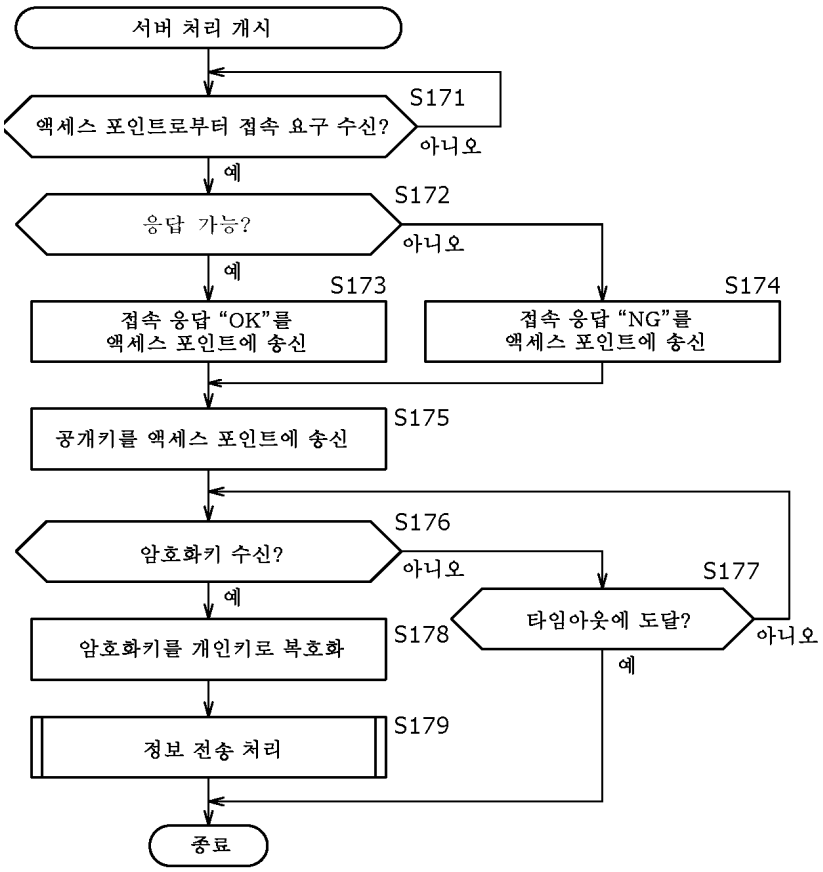
도면18


클라이언트 처리를 개시
촬상
S101
어드레스값을 판독
S102
어드레스값에 대응하는 아이콘을 표시
S103
아이콘 선택?
S104
아니오
종료 커맨드 ?
아니오
S105
예
예
액세스 포인터에 접속을 요구
S106
액세스 포인트로부터 응답?
S107
아니오
예
공개키 판독
S108
암호화키 판독
S109
공개키로 암호화키를
암호화하고 암호화된 키를 송신
S110
정보 전송 처리
S111
종료

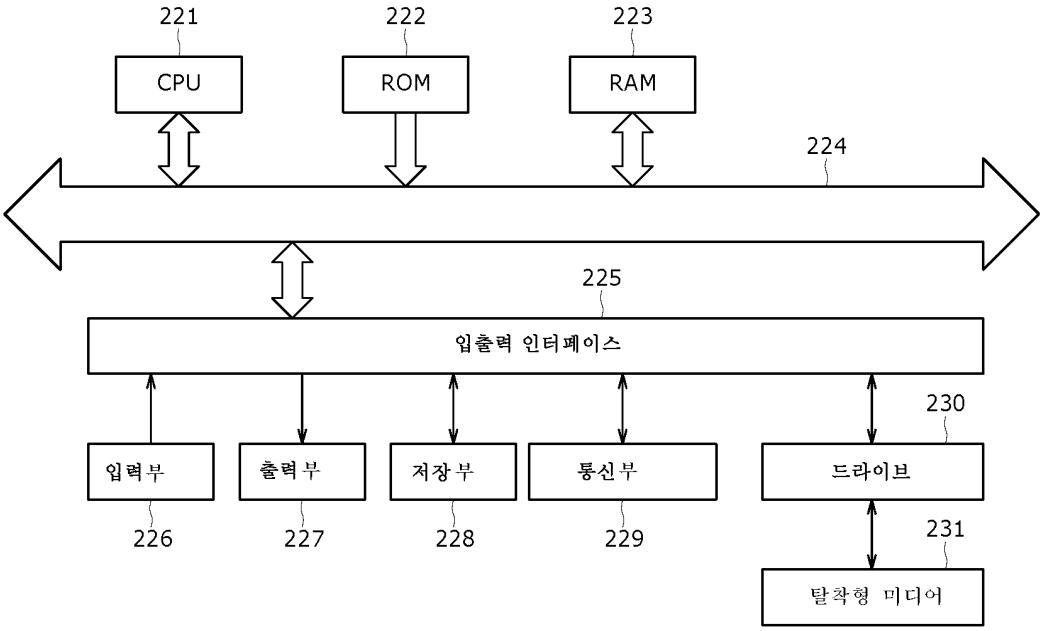
도면19


액세스 포인트 처리 개시
어드레스값 송신
S141
접속 요구 수신?
S142
아니오
예
접속 요구를 서버에 송신
S143
서버로부터 접속 응답 수신?
S144
아니오
예
액세스하는 클라이언트에
접속 응답 송신
S145
공개키 수신?
S146
아니오
예
클라이언트에 공개키를 송신
S147
암호화키 수신?
S148
아니오
예
서버에 암호화키 송신
S149
정보 전송 처리
S150
종료

도면20


서버 처리 개시
액세스 포인트로부터 접속 요구 수신?
S171
아니오
예
응답 가능?
S172
아니오
예
S173
접속 응답 "OK"를 액세스 포인트에 송신
S174
접속 응답 "NG"를 액세스 포인트에 송신
공개키를 액세스 포인트에 송신
S175
암호화키 수신?
S176
아니오
예
타임아웃에 도달?
S177
아니오
예
암호화키를 개인키로 복호화
S178
정보 전송 처리
S179
종료

도면21


221
CPU
222
ROM
223
RAM
224
225
입출력 인터페이스
230
입력부
출력부
저장부
통신부
드라이브
226
227
228
229
231
탈착형 미디어