

(19)대한민국특허청(KR) (12) 등록특허공보(B1)

(51) 。 Int. Cl.⁷
H04L 9/32

(45) 공고일자 2004년09월30일
(11) 등록번호 10-0450570
(24) 등록일자 2004년09월17일

(21) 출원번호	10-2002-7010391	(65) 공개번호	10-2003-0019313
(22) 출원일자	2002년08월10일	(43) 공개일자	2003년03월06일
번역문 제출일자	2002년08월10일		
(86) 국제출원번호	PCT/JP2001/010834	(87) 국제공개번호	WO 2002/48893
(86) 국제출원출원일자	2001년12월11일	(87) 국제공개일자	2002년06월20일

(81) 지정국 국내특허 : 오스트레일리아, 브라질, 캐나다, 중국, 일본, 대한민국, 노르웨이, 뉴질랜드, 폴란드, 미국, 싱가포르,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투갈, 스웨덴, 핀란드, 사이프러스, 터키,

(30) 우선권주장 JP-P-2000-00376630 2000년12월11일 일본(JP)

(73) 특허권자 엔티티 도꼬모 인코퍼레이티드
일본 도쿄도 치요다쿠 나가타초 2초메 11-1

(72) 발명자 야마모토마사아키
일본국가나가와켄요코하마시이소고쿠스기타9초메2-10-107

히라마츠요시아키
일본국가나가와켄요코스카시후나구라2초메5-20

와카바야시다츠아키
일본국가나가와켄요코하마시아사히쿠혼주쿠초18-24

간토히로시
일본국도쿄도오오타쿠하네다4초메4-22

(74) 대리인 한양특허법인

심사관 : 문태진

(54) 사용자 인증을 위한 방법 및 장치

요약

IP 서버(W)나 게이트웨이 서버(GWS)는 이동국(MS)으로부터의 요구에 응하여 HTML 형식의 데이터를 송신한다. 여기서, 이 HTML 데이터에서 사용자 인증이 필요한 서비스에 관련하는 페이지의 URL에는 개인 식별정보 요구 데이터 열이 부가된다. 이 HTML 데이터가 이동국(MS)에 의해 수신되면, 그 HTML 데이터에 대응하는 화면이 액정표시부에 표시된 상태에서 사용자가 해당 URL을 지정하는 입력조작을 한다. 그리고, 이동국(MS)은 개인 식별정보를 ROM으로부터 독출하여 이동 패킷 통신망(MPN)에 송신한다. IP 서버(W)는 이와 같이 이동국(MS)으로부터 송신된 개인 식별정보에 따라 사용자 인증을 한다.

대표도

도 1

명세서

기술분야

본 발명은 상이한 네트워크 사이에서 엔드 투 엔드(end-to-end)의 사용자 인증을 실행하기 위한 방법 및 장치에 관한 것이다.

배경기술

근년, 휴대전화기 등의 이동국의 고기능화에 따라, 이동국에 WWW(World Wide Web) 브라우저(이하, 'WWW 브라우저'라 한다)를 탑재하여, 이동국 단독으로 WWW 브라우징을 가능하게 하는 제품이 시판되고 있다. 이러한 이동국을 이용함으로써, 사용자는 인터넷상의 정보 제공자(이하, 'IP'라 한다)로부터 각종 서비스의 제공을 받는 것이 가능해지고 있다.

여기서, IP가 제공하는 서비스 중에는 계약 사용자에게 대해서만 제공되는 것이나 비화성을 필요로 하는 것이 존재한다. 이 때문에, 이러한 종류의 서비스를 제공하는 IP는 제삼자에 의한 부정사용을 방지할 목적으로, 서비스 제공 시에 사용자 인증을 하고 있다. 이 사용자 인증방법으로서, 종래 일반적으로 쓰이고 있는 방법은 패스워드를 이용하는 방법이다. 그러나, 패스워드에 의한 사용자 인증방법으로는 패스워드가 악의를 가진 제삼자에게 누설될 위험이 있고, 또한 패스워드가 일단 누설되면 누구나 부정사용을 할 수 있게 되어 버린다. 이 때문에, 예컨대, 네트워크를 이용한 은행거래 서비스(이하, '넷 뱅킹'이라 한다)와 같이 보안의 확보가 불가결한 서비스를 제공하는 데에는, 보다 신뢰성을 확보할 수 있는 사용자 인증방법을 이용할 필요가 있다.

그래서, 이러한 서비스를 제공하는 IP에서는 이동통신망이 보유하는 발신 ID 등의 이동국을 특정할 수 있는 고유한 정보(이하, '개인 식별정보'라 한다)를 이용하여 사용자 인증을 하고 있다. 이 사용자 인증방법에 관해 간단히 설명하면 다음과 같다:

i. 이동국의 사용자에게 서비스를 제공하는 경우, 우선, IP가 보유하는 서버(이하, 'IP 서버'라 한다)는 이동통신망에 대해 개인 식별정보의 송신을 요구한다.

ii. 이 송신요구에 따라서 이동통신망이 개인 식별정보를 IP 서버로 회신한다.

iii. IP 서버는 이동통신망으로부터 회신된 개인 식별정보에 따라 사용자 인증을 한다.

종래에는 상기 설명한 사용자 인증방법에 의해, 제삼자에 의한 부정사용을 효과적으로 방지하고 있었다.

그러나, 개인 식별정보는 사용자의 프라이버시나 재산에 관계하는 중요한 정보이다. 이 때문에, 이동통신 사업자가 아무런 제한 없이 사용자의 개인 식별정보를 IP에 제공하게 되면, 이동국의 사용자에게 예기치 못한 불이익을 줄 수 있는 위험이 있다. 이동통신 사업자는 이러한 예기치 못한 불이익을 방지하기 위해, 자신이 보유하는 개인 식별정보를 제공할 IP와 사전에 계약하여, 이것에 의해 개인 식별정보가 제공되는 목적지의 신뢰성을 확보하고 있다. 이와 같이, 이러한 방법에서는 사전의 계약이 필요하기 때문에, 이동통신 사업자와 계약을 맺고 있지 않은 IP가 사용자 인증에 개인 식별정보를 이용하는 것은 불가능하여, 해당 IP에서는 개인 식별정보를 이용한 인증을 할 수 없다는 문제가 있었다.

발명의 상세한 설명

본 발명의 목적은 이동통신 사업자와 특별한 계약을 맺지 않고도, 모든 IP에서 개인 식별정보를 이용한 사용자 인증을 가능하게 하는 사용자 인증방법 및 통신 시스템을 제공하는 것이다.

상기 목적을 달성하기 위해 본 발명은, 제1 네트워크에 수용된 휴대단말이 상기 제1 네트워크로부터 데이터를 수신하는 수신과정; 상기 휴대단말이 상기 수신과정에서 수신한 데이터 중에 소정의 데이터열이 존재하는지 여부를 검출하는 검출과정; 상기 검출과정에서 상기 데이터열이 존재하는 것으로 검출된 경우에만, 상기 휴대단말이 미리 이 휴대단말에 기억되어 있는 사용자를 일의적으로 특정하기 위한 개인 식별정보를 송신하는 송신과정; 상기 제1 네트워크와 제2 네트워크 사이의 데이터 송수신을 중계하는 중계장치가 상기 휴대단말에서 송신된 개인 식별정보를 상기 제2 네트워크로 전송하는 전송과정; 및 상기 제2 네트워크에 접속된 서버가 상기 개인 식별정보에 따라 상기 휴대단말의 사용자를 인증하는 인증과정을 구비하는 것을 특징으로 하는 사용자 인증방법을 제공한다.

이러한 구성에 있어서, 상기 송신과정에서 상기 휴대단말이 송신하는 식별정보는 상기 서버 이외의 장치에 의해 해독 불가능한 형식으로 송신될 수 있다. 이 경우, 상기 인증과정에서 상기 서버는 상기 휴대단말로부터 송신된 개인 식별정보를 해독하여, 그 개인 식별정보에 따라 상기 휴대단말의 사용자를 인증한다.

또한, 상기 수신과정에 앞서, 상기 중계장치가 상기 휴대단말로부터의 요구에 따라 상기 제2 네트워크에 있어서의 상기 서버의 어드레스를 검색하는 검색과정을 갖출 수 있다. 이 경우, 상기 수신과정에서 상기 휴대단말이 수신하는 상기

데이터는 상기 검색과정에서 상기 중계장치가 검색한 검색결과에 대응하는 데이터이다. 바람직한 실시형태에 있어서, 상기 데이터는 마크업 언어로 기술될 수 있고; 상기 데이터열은 상기 데이터 내에 있어서 소정의 식별자의 마크업이 되도록 할 수 있다.

또한, 상기 송신과정에 앞서, 상기 휴대단말은 상기 검출과정에서 상기 데이터열이 존재하는 것으로 검출된 경우에만, 상기 휴대단말이 이 휴대단말의 사용자에게 대하여 상기 개인 식별정보의 송신 여부에 관해 판단을 재촉하는 판단촉진 과정을 실행하는 기능을 구비할 수 있고, 상기 송신과정에서 상기 휴대단말은 상기 판단촉진과정에서 상기 사용자의 허가가 얻어진 경우에만, 상기 개인 식별정보를 송신할 수 있다. 이 경우, 상기 판단촉진과정에서는 사용자의 판단을 재촉하기 위한 화상을 표시할 뿐 아니라, 사용자에게 대하여 입력 식별정보의 입력을 재촉하여, 사용자가 입력한 입력 식별정보를 상기 송신과정에서 상기 개인 식별정보와 함께 송신하는 것도 가능하다.

또한, 상기 인증과정 후에 상기 서버가 상기 휴대단말에 대하여 입력 식별정보의 입력을 재촉하는 입력 데이터를 송신하는 송신과정; 상기 송신과정에서 송신된 상기 입력 데이터를 수신한 상기 휴대단말이 상기 입력 데이터에 근거하여 사용자에게 대해 상기 입력 식별정보의 입력을 재촉하는 과정; 상기 입력을 재촉하는 과정에서 입력된 입력 식별정보를 송신하는 제2 송신과정; 및 상기 제2 송신과정에서 송신된 상기 입력 식별정보에 따라 상기 휴대단말의 사용자를 인증하는 제2 인증과정을 더 설정할 수 있다.

바람직하게는, 상기 개인 식별정보로서 상기 휴대단말의 제조번호가 사용되어야 한다.

이 경우, 개인 식별정보로서 상기 휴대단말의 제조번호와 상기 휴대단말에 접속된 사용자 식별모듈에 저장된 정보와의 조합을 사용하면, 인증의 신뢰성을 향상시킬 수 있다. 또한, 제1 네트워크로서 이동통신망을 이용할 수도 있다. 본 발명은 또한 제1 네트워크로부터 데이터를 수신하여, 그 데이터 중에 소정의 데이터열이 존재하는지 여부를 검출하고, 상기 데이터열이 존재하는 것으로 검출된 경우에만, 미리 단말에 기억되어 있는 사용자를 일의적으로 특정하기 위한 개인 식별정보를 상기 제1 네트워크에 송신하는 휴대단말; 상기 제1 네트워크와 중계장치를 통해 상호 접속된 제2 네트워크; 및 상기 제2 네트워크에 접속되어, 상기 개인 식별정보에 따라 인증을 하는 서버를 구비하는 것을 특징으로 하는 통신 시스템을 제공한다.

또한, 본 발명은 제1 네트워크를 통해 타자와 통신하는 통신부; 및 상기 통신부에 의해 상기 제1 네트워크 및 이 제1 네트워크에 접속된 제2 네트워크를 통해 상기 제2 네트워크내의 서버와 통신하여, 상기 서버로부터 소정의 데이터열을 포함하는 데이터를 수신하였을 때, 상기 휴대단말에 설치된 메모리 또는 상기 휴대단말에 접속된 메모리로부터 개인 식별정보를 독출하여, 상기 접속을 통해 상기 개인 식별정보를 상기 서버에 송신하는 제어부를 구비하는 것을 특징으로 하는 휴대단말을 제공한다.

또한, 본 발명은 이와 같은 휴대단말로서 기능하기 위한 프로그램을 네트워크를 통해 사용자에게 배포하거나, CD나 FD 등의 기록매체에 저장하여 사용자에게 배포하는 형태로도 실행될 수 있다.

도면의 간단한 설명

- 도 1은 본 실시형태에 있어서의 통신 시스템(1)의 전체 구성을 나타내는 블록도이다.
- 도 2는 상기 실시형태에 있어서의 IP 서버(W)의 구성을 나타내는 블록도이다.
- 도 3은 상기 실시형태에 있어서의 HTML 데이터의 예를 나타내는 도면이다.
- 도 4는 도 3에 나타난 데이터에 대응하는 화상의 일례를 나타내는 도면이다.
- 도 5는 상기 실시형태에 있어서의 개인 식별정보 데이터베이스(113)의 기억내용을 나타내는 도면이다.
- 도 6은 상기 실시형태에 있어서의 검색용 데이터베이스(GWS1)의 기억내용을 나타내는 도면이다.
- 도 7은 상기 실시형태에 있어서의 이동국(MS)의 구성을 나타내는 블록도이다.
- 도 8은 상기 실시형태에 있어서의 입력 저장 테이블(TBL)의 기억내용을 나타내는 도면이다.
- 도 9는 상기 실시형태에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 10은 상기 실시형태에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 11은 상기 실시형태에 있어서의 이동국(MS)의 CPU(211)가 실행하는 처리를 나타내는 순서도이다.
- 도 12는 상기 실시형태에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 13은 상기 실시형태에 있어서의 통신 시스템(1)에서 신호의 흐름을 나타내는 시퀀스도이다.
- 도 14는 상기 실시형태에 있어서의 통신 시스템(1)에서 신호의 흐름을 나타내는 시퀀스도이다.
- 도 15는 상기 실시형태에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 16은 상기 실시형태에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 17은 변형예 1에 있어서의 개인 식별정보 데이터베이스(113)의 기억내용을 나타내는 도면이다.
- 도 18은 변형예 2에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 19는 상기 변형예에 있어서의 이동국(MS)의 액정표시부(24)에 표시된 화면의 일례를 나타내는 도면이다.
- 도 20은 변형예 3에 있어서의 이동국(MS)의 구성을 나타내는 블록도이다.
- 도 21은 상기 변형예에 있어서의 UIM(2000)의 구성을 나타내는 블록도이다.
- 도 22는 상기 변형예에 있어서의 개인 식별정보 데이터베이스(113)의 기억내용을 나타내는 도면이다.

실시예

이하, 도면을 참조하여 본 발명의 실시형태에 관해 설명한다. 본 실시형태는 본 발명을 인터넷에 접속된 이동통신망에 적용함으로써 실현된다.

<1-1. 실시형태의 구성>

<A. 시스템 전체의 구성>

도 1은 본 실시형태에 있어서의 통신 시스템의 구성을 나타내는 블록도이다.

이 도면에 도시한 바와 같이, 본 실시형태의 통신 시스템(1)은 다수의 이동국(MS), 다수의 기지국(BS), 이동 패킷 통신망(MPN), 게이트웨이 서버(GWS), 인터넷(INET), 다수의 IP 서버(W)로 구성된다. 도 1에서는 도면이 복잡해지는 것을 피하기 위해, 통신 시스템(1)에 수용되는 다수의 이동국(MS), 기지국(BS) 및 IP 서버(W) 중에서 소정의 이동국, 기지국 및 IP 서버만이 도시되고 있다.

이동국(MS)은 휴대전화기 등의 휴대형 전자기기이고, 도 1에 나타난 이동 패킷 통신망(MPN)을 통해 데이터 통신이 가능하며, 이동전화망(도시 없음)을 통해 음성통화를 한다. 이동국(MS)은 이동 패킷 통신망(MPN)을 통한 데이터 통신에 의해 IP 서버(W)에서 각종 서비스의 제공을 받는다. 또한, 이동국(MS)은 개인 식별정보를 기억하여, 사용자 인증이 필요한 서비스의 제공을 받는 데 있어서 IP 서버(W)에 개인 식별정보를 송신한다. 여기서, 개인 식별정보에는 사용자를 일의적으로 특정할 수 있는 고유한 정보라면 어떤 정보를 이용하더라도 상관없지만, 본 실시형태에서는 이동국(MS)의 제조번호를 이용하는 것으로 한다.

IP 서버(W)는 IP가 보유하는 WWW(World Wide Web) 서버이고, 이동국(MS)에 대하여 '넷 बैं킹'(예컨대, '송금'이나 '잔액조회' 등)이나 회원제 서비스 등의 각종 서비스를 제공한다.

도 2는 IP 서버(W)의 구성을 나타낸 블록도이다. 이 도면에 나타난 바와 같이 IP 서버(W)는 데이터 전송 관리부(111), 인증부(112), 개인 식별정보 데이터베이스(113), 통신부(114)로 구성된다.

데이터 전송 관리부(111)는 예컨대 CPU(Central Processing Unit), ROM(Read Only Memory), RAM(Random Access Memory), 하드디스크(도시하는 모두 생략)로 구성된다. 하드디스크에는 홈페이지나 웹페이지 등의 자원에 대응하는 HTML(Hyper Text Markup Language) 형식의 데이터(이하, 'HTML 데이터'라 한다)가 저장되어 있고, 그 각각에는 URL이 설정되어 있다. ROM에는 이동국(MS)으로부터 GET 방법을 이용한 HTTP(Hyper Text Transfer Protocol)나 HTTPS의 메시지(이하, 'GET 요구'라 한다)를 받은 경우에, 이 GET 요구에 따라 데이터를 전송하기 위한 제어 프로그램이 저장되어 있다. CPU는 이들 프로그램에 따라 각종 처리를 실행한다. RAM은 CPU의 작업영역으로 쓰인다.

여기서, 본 실시형태에서 데이터 전송 관리부(111)로부터 인터넷(INET)으로 송신되는 HTML 데이터 중에는 종래에 있던 특징적인 구성이 존재한다.

도 3은 본 실시형태에 있어서의 HTML 데이터의 소스의 예를 게시한 것이고, 도 4는 도 3에 나타난 데이터에 대응하는 화상의 일례를 나타낸 도면이다. 도 3에서, 는 앵커 태그이고, 이 앵커 태그에 의해 IP 서버(W)가 이동국(MS)에 제공 가능한 서비스에 관련하는 페이지에 대응하는 URL이 지정된다.

도 4에 나타난 '송금' 메뉴항목에는, 도 3에 나타난 앵커 태그 가 첨부되지만, 이 앵커 태그에 의해 지정된 URL의 말미에는 'utn'으로 된 데이터열이 부가되어 있다. 이 데이터열 'utn'은 IP 서버(W)가 개인 식별정보의 송신을 요구하고 있는 것을 나타내는 데이터열이다 (이하, 이 'utn'으로 된 문자열을 '개인 식별정보 요구 데이터열'이라 한다).

상술한 바와 같이, IP 서버(W)가 이동국(MS)에 제공하는 서비스 중에는 '넷 बैं킹' 서비스나 회원제 서비스 등의 사용자 인증이 필요한 것이 존재한다. 상술한 HTML 데이터 중에는 이러한 종류의 서비스에 관련하는 페이지의 URL에 개인 식별정보 요구 데이터열 'utn'이 부가된 것이 있다. 그리고, 개인 식별정보 요구 데이터열 'utn'이 부가된 URL을 포함하는 HTML 데이터가 이동국(MS)에 수신되어, 이동국(MS)에서 그 URL이 지정되면, 이동국(MS)은 그 URL을 포함하는 GET 요구에 대해 이동국(MS)이 기억하고 있는 개인 식별정보를 부가하여 송출한다. 이렇게 하여, 이동국(MS)으로부터 개인 식별정보를 포함하는 GET 요구가 송신되면, 데이터 전송 관리부(111)는 GET 요구에 포함되어 있는 URL을 추출하여 인증부(112)로 보낸다.

인증부(112)는 데이터 전송 관리부(111)로부터 송신된 개인 식별정보와 개인 식별정보 데이터베이스(113)에 저장된 정보에 따라 사용자 인증을 한다.

도 5는 개인 식별정보 데이터베이스(113)의 기억내용을 나타내는 도면이다. 이 도면에 나타난 바와 같이, 개인 식별정보 데이터베이스(113)에는 각 사용자 ID에 대응하여 개인 식별정보가 저장되어 있다. 여기서, 개인 식별정보 데이터베이스(113)에 저장되어 있는 사용자 ID는 각 사용자가 IP 서버(W)에 자신의 개인 식별정보를 등록할 때, IP 서버(W)가 각 사용자에게 부여한 ID이다. IP 서버(W)가 사용자에게 제공하는 서비스가, 예컨대, '넷 बैं킹' 서비스인 경우, 이 사용자 ID는 그 사용자의 은행구좌를 특정하기 위해 쓰인다. 한편, IP 서버(W)가 제공하는 서비스가 콘텐츠 전송인 경우, 사용자 ID는 서비스 요금 산출에 쓰인다.

또한, 개인 식별정보 데이터베이스(113)에 대한 개인 식별정보나 사용자 ID의 등록은 여러 가지 방법으로 실현 가능하다. 예컨대, 사용자가 IP 서버(W)를 보유하는 IP의 서비스 창구에서 이동국(MS)의 제조번호를 창구 종업원에게 제시함으로써 등록을 하는 구성도 가능하다. 또한, IP 측에서 SSL(Security Sockets Layer)에 의한 통신이 가능한 사이트를 개설하고, 사용자가 이동국(MS)을 이용하여 그 사이트에 액세스하여 개인 식별정보를 등록하는 구성도 가능하다. 이러한 방법을 채용하는 경우, 해당 사이트의 페이지에 대응하는 HTML 데이터에 개인정보 요구 데이터열을 부가한 후, 이동국(MS)에 기억되어 있는 제조번호 등의 개인 식별정보를 송신하도록 해야 한다.

데이터 전송 관리부(111)로부터 개인 식별정보가 송신되면, 인증부(112)는 그 개인 식별정보에 따라 개인 식별정보 데이터베이스(113)를 검색한다. 그리고, 개인 식별정보와 일치하는 정보가 개인 식별정보 데이터베이스(113)에 저장되어 있는 경우, 그 개인 식별정보에 대응하는 사용자 ID를 독출한다. 그리고, 그 사용자 ID에 따라 각종 서비스를 제공한다. 한편, 개인 식별정보에 일치하는 정보가 개인 식별정보 데이터베이스(113)에 존재하지 않는 경우, 인증부(112)는 해당 이동국(MS)의 사용자가 정당한 권한을 갖는 사용자가 아닌 것으로 판정하여 서비스의 제공을 거부한다.

통신부(114)는 인터넷(INET)과 데이터 전송 관리부(111) 사이의 데이터의 송수신을 중개한다. 구체적으로는, 통신부(114)는 인터넷(INET)에서 송신된 데이터를 데이터 전송 관리부(111)에 보내는 동시에, 데이터 전송 관리부(111)로부터 송신된 데이터를 인터넷(INET)으로 송출한다.

다음에, 이동 패킷 통신망(MPN)은 이동국(MS)에 대해 패킷 통신 서비스를 제공하기 위한 통신망으로서, 게이트웨이 서버(GWS)나 다수의 기지국(BS)으로 구성되며, 패킷 가입자 처리장치(도시 생략)를 구비한다.

게이트웨이 서버(GWS)는 인터넷(INET)과 이동 패킷 통신망(MPN)을 접속하는 이동 패킷 게이트웨이 중계 교환국에 설치된 컴퓨터 시스템이고, 상이한 네트워크 사이의 데이터의 송수신을 중개한다. 구체적으로는, 게이트웨이 서버(GWS)는 이동 패킷 통신망(MPN) 측의 이동국(MS)에서 송신된 데이터를 인터넷(INET)이 따르는TCP/IP(Transmission Control Protocol/Internet Protocol)에 적합하게 하기 위한 프로토콜 변환을 한 후 인터넷(INET) 측으로 송신한다. 또한, 게이트웨이 서버(GWS)는 인터넷(INET) 측에서 송신된 데이터를 이동 패킷 통신망(MPN)용의 전송 프로토콜로 변환하여 이동 패킷 통신망(MPN) 측에 송신한다.

또한, 게이트웨이 서버(GWS)는 이동국(MS)에서 송신된 HTTP의 GET 요구를 수신하면, 이 GET 요구에 포함되는 URL을 조사하여, 그 URL이 인터넷(INET)상에서 일반적인 URL인 경우에는 그 GET 요구를 인터넷(INET) 측에 전송한다. 그리고, 이 GET 요구에 응하여 인터넷(INET) 측에서 회신된 데이터를 이동 패킷 통신망(MPN)에 전송한다. 또한, 게이트웨이 서버(GWS)는 이동국(MS)으로부터 HTTPS의 GET 요구를 받으면, 이 GET 요구에 포함되는 URL을 조사하여, 그 URL에 대응하는 SSL 사이트와 이동국(MS)이 직접 통신할 수 있도록 한다.

더욱이, 게이트웨이 서버(GWS)는 이동국(MS)에서의 요구에 응하여, 예컨대, 홈페이지나 웹페이지 등에 대응하는 HTML 데이터를 생성한다. 게이트웨이 서버(GWS)는 이 HTML 데이터를 이동국(MS)에 송신함으로써, 이동국(MS)에 각종 서비스를 제공한다. 게이트웨이 서버(GWS)가 이동국(MS)에 제공하는 서비스로서는 예컨대 IP 서버(W)의 검색 서비스 등이 있다. 이 검색 서비스를 제공하기 위해 게이트웨이 서버(GWS)는 검색용 데이터베이스(GWS1)를 구비한다.

도 6은 검색용 데이터베이스(GWS1)의 기억내용을 나타내는 도면이다. 이 도면에 나타난 바와 같이, 검색용 데이터베이스(GWS1)에는 IP 서버(W)에 저장된 각 페이지의 타이틀에 대응하는 검색용 키워드와, 해당 페이지에 대응하는 URL이 저장되어 있다. 여기서, 검색용 데이터베이스(GWS1)에 저장되어 있는 URL 중 사용자 인증을 필요로 하는 서비스에 관련하는 페이지의 URL에는 개인 식별정보 데이터열(즉, 'utn')이 부가되어 있다. 예컨대, 이 도면에 나타난 예에서, '00 은행'이나 '△△ 은행'에 대응하여 미리 저장되어 있는 URL(즉, 'http://www.00bank.co.jp/index.html#utn'이나 'http://www.△△bank.co.jp/index.html#utn')이 이것에 대응한다.

게이트웨이 서버(GWS)는 이동국(MS)에서의 요구에 따라 검색용 데이터베이스(GWS1)의 검색을 한다. 그리고, 게이트웨이 서버(GWS)는 그 검색 결과 찾아낸 URL을 앵커 태그에 의해 지정된 HTML 데이터를 생성하여 인터넷(INET)으로 송출한다. 예컨대, 도 6에 나타난 경우에 있어서, '00 은행'으로 된 타이틀이 선택된 경우, 게이트웨이 서버(GWS)는 검색용 데이터베이스로부터 URL 'https://www.00bank.co.jp/index.html#utn'을 독출하고, 그 URL을 포함하는 HTML 데이터를 생성하여 이동 패킷 통신망(MPN)으로 송출한다.

<B. 이동국(MS)의 구성>

도 7은 본 실시형태에 있어서의 이동국(MS)의 구성을 나타내는 블록도이다.

이 도면에 나타난 바와 같이, 이동국(MS)은 제어부(21), 송수신부(22), 지시 입력부(23), 액정표시부(24) 및 각 요소 사이에서의 데이터의 송수신을 중개하는 버스(25)를 갖는다.

송수신부(22)는 이동 패킷 통신망(MPN)의 기지국(BS)과 무선통신을 한다.

지시 입력부(23)는 PB(푸시버튼) 등의 각종 버튼 및 커서 키로 이루어져, 사용자에게 의해 입력조작이 행해지면, 그 입력조작에 대응하는 조작 데이터를 제어부(21)의 CPU(211)에 공급한다. CPU(211)는 이 조작 데이터로부터 사용자의 입력지시를 판정하여, 그 지시를 실행한다.

액정표시부(24)는 액정패널 등의 표시장치로 구성되어, 제어부(21)의 제어 하에 각종 정보를 표시한다.

제어부(21)는 CPU(211), ROM(212), RAM(213), 플래시 메모리(214)로 구성되어, 이동국(MS)의 각 부를 제어한다. ROM(212)에는 개인 식별정보로서의 이동국(MS)의 제조번호나 이동국(MS) 전체를 제어하기 위한 제어 프로그램, 각종 제어정보 외에도, 다른 통신장치(예컨대, IP 서버(W))로부터 원하는 데이터를 취득하여, 그 취득한 데이터에 대응하는 화상을 표시하기 위한 WWW 브라우저가 기억되어 있다. RAM(213)은 CPU(211)의 작업영역으로 쓰인다.

CPU(211)는 ROM(212)에 기억된 각종 제어 프로그램에 따라 각종 처리를 실행한다. 예컨대, CPU(211)가 ROM(212)에 기억된 WWW 브라우저를 독출하여 실행하면, 그 실행과정에서 다음 처리가 행해진다. 즉, 사용자가 지시 입력부(23)에 의해 원하는 URL을 지정하면, CPU(211)는 지시 입력부(23)로부터의 입력지시에 따라, 상기 URL을 포함하는 HTTP나 HTTPS의 GET 요구를 이동 패킷 통신망(MPN)에 송출하기 위한 처리를 한다.

또한, 이 때 지시 입력부(23)로부터 지정된 URL에 개인 식별정보 요구 데이터열 'utn'이 부가되는 경우가 있다. 이러한 경우에, CPU(211)는 ROM(212)에 저장된 개인 식별정보(제조번호)를 독출하여, 이 개인 식별정보 요구 데이터열 'utn'을 부가한 GET 요구를 송신한다. 그리고, 이 GET 요구에 대응하는 HTML 데이터가 IP 서버(W)나 게이트웨이 서버(GWS)에서 회신되면, CPU(211)는 그 HTML 데이터를 RAM(213)에 기입하는 동시에, 그 HTML 데이터에 대응하는 화상을 액정표시부(24)에 표시하게 한다.

플래시 메모리(214)는 액세스 이력을 등록하기 위해, 도 8에 나타난 이력 저장 테이블(TBL)을 구비하고 있다. 이 도면에 나타난 바와 같이, 이력 저장 테이블(TBL)에는 사용자가 이동국(MS)을 이용하여 실제로 액세스한 자원의 URL이 액세스 이력으로서 저장되어 있다(이하, 이 액세스 이력으로서의 URL을 '이력 URL'이라 한다). 또한, 각 이력 URL에 대응하여 해당 URL에 개인 식별정보 요구 데이터열 'utn'이 부가되어 있는지 여부를 나타내는 요구 데이터열 플래그(F)가 저장되어 있다. 이 요구 데이터열 플래그(F)가 '1'인 경우, 해당 URL에는 요구 데이터열이 부가되어 있는

것을 나타내고, 요구 데이터열 플래그(F)가 '0'인 경우에는 요구 데이터열이 URL에 부가되지 않은 것을 나타내고 있다.

이동국(MS)이 IP 서버(W)에서 HTML 데이터의 다운로드에 실패하여, 그 HTML 데이터를 다시 다운로드 하려고 하는 경우가 있다. 이러한 경우에, 이동국(MS)은 이력 저장 테이블(TBL)에서 요구 데이터열 플래그(F)를 독출하여, 개인 식별정보를 송신하는지 여부를 결정한다. 구체적으로는, 다시 독출할 페이지에 대응하는 URL의 요구 데이터열 플래그(F)가 '1'인 경우, 제어부(21)는 IP 서버(W)에 개인 식별정보를 부가하여 GET 요구를 송신한다. 한편, 요구 데이터열 플래그(F)가 '0'인 경우, 제어부(21)는 개인 식별정보를 부가하지 않고, 단지 해당 페이지에 대응하는 URL을 포함하는 GET 요구를 송신한다.

<1-2. 실시형태의 동작>

이하, 도면을 참조하여, 본 실시형태에 있어서의 통신 시스템의 동작에 관해 설명한다. 또, 이하의 설명에서는 설명을 보다 구체적으로 하기 위해, 개인 식별정보 데이터베이스(113) 및 검색용 데이터베이스(GWS1)의 기억내용은 도 5 및 도 6에 나타난 것과 동일한 것으로 하고, 이동국(MS)의 제조번호는 '△△△△△△'인 것으로 한다.

우선, 외출 시에 자신의 아파트 집세의 송금을 잊은 것을 깨달은 사용자는 게이트웨이 서버(GWS)의 검색 서비스를 이용하여 자신이 구좌를 개설하고 있는 'OO 은행'의 홈페이지를 검색하여, '넷 뱅킹' 서비스를 받도록 이동국(MS)의 지시 입력부(23)에 대해 브라우저를 하기 위한 입력조작을 한다. 이 지시 입력부(23)에 대한 입력에 따라, CPU(211)는 ROM(212)으로부터 WWW 브라우저를 독출하여, 패킷 가입자 처리장치(도시 생략)에 패킷 등록을 한다. 이 패킷 등록은 이동국(MS)이 이동 패킷 통신망(MPN)과의 패킷 교환을 하기 위한 등록 절차이다. 이렇게 하여, 패킷 등록이 행해지면, 이동국(MS)은 게이트웨이 서버(GWS)와의 패킷 교환이 가능해진다.

그 후, 사용자가 이동국(MS)의 지시 입력부(23)에 대해, 게이트웨이 서버(GWS)의 검색 서비스에 대응하는 URL을 입력하면, 이동국(MS)은 그 URL을 포함하는 GET 요구를 이동 패킷 통신망(MPN)으로 송신한다. 게이트웨이 서버(GWS)는 이 GET 요구를 수신하면, 검색화면에 대응하는 HTML 데이터를 이동 패킷 통신망(MPN)에 송출한다. 또, 이 검색화면의 구성은 임의이지만, 본 실시형태에서는 도 9에 나타난 바와 같이 '키워드'로 된 문자열 밑에 있는 박스 부분에 검색용 문자열을 입력하는 구성으로 되어있다.

다음에, 이 검색화면에 대응하는 HTML 데이터는 이동국(MS)의 송수신부(22)에 의해 수신되어 CPU(211)로 전송된다. 이 결과, 해당 HTML 데이터에 대응하는 검색화면(도 9 참조)이 액정표시부(24)에 표시된다. 이 상태에서, 사용자는 이동국(MS)의 지시 입력부(23)에 대해, 자신이 검색하고 싶은 서비스에 대응하는 검색용 문자열(즉, '넷 뱅킹'으로 된 검색용 문자열)을 입력하여, 결정을 위한 입력조작을 한다. 이 결과, 이동국(MS)의 CPU(211)는 해당 문자열을 부가한 GET 요구를 이동 패킷 통신망(MPN)에 송출한다.

그리고, 이 GET 요구가 게이트웨이 서버(GWS)에 의해 수신되면, 게이트웨이 서버(GWS)는 그 GET 요구에 포함되어 있는 검색용 문자열(즉, '넷 뱅킹'으로 된 검색용 문자열)을 추출한다. 게이트웨이 서버(GWS)는 이 '넷 뱅킹'으로 된 검색용 문자열에 근거하여 검색용 데이터베이스(GWS1)를 검색한다. 이 결과, 검색용 데이터베이스(GWS1)에서 '넷 뱅킹'이라는 키워드에 따라 'OO 은행'이나 '△△ 은행'에 대응하는 URL이 찾아진다(도 6 참조).

다음에, 게이트웨이 서버(GWS)는 이들 'OO 은행'이나 '△△ 은행'에 대응하는 URL 'https://www.OObank.co.jp/index.html#utn'이나

'http://www.△△bank.co.jp/index.html#utn'을 검색용 데이터베이스(GWS1)로부터 독출한다. 여기서, '넷 뱅킹'은 상술한 바와 같이 보안을 필요로 하는 서비스이기 때문에, 이들 서비스에 관련하는 페이지의 URL에는 개인 식별정보 요구 데이터열 'utn'이 포함되어 있다. 그리고, 게이트웨이 서버(GWS)는 검색용 데이터베이스(GWS1)로부터 독출한 'OO 은행'이나 '△△ 은행'에 대응하는 URL을 앵커 태그에 의해 지정한 HTML 데이터를 생성하여 이동 패킷 통신망(MPN)으로 송출한다.

다음에, 이 HTML 데이터는 이동국(MS)의 송수신부(22)에 의해 수신되어 CPU(211)로 송신된다. CPU(211)는 이 송신된 HTML 데이터에 대응하는 화상을 액정표시부(24)에 표시하게 한다. 이 결과, 이동국(MS)의 액정표시부(24)에는 도 10에 나타난 바와 같이, 게이트웨이 서버(GWS)에서의 검색의 결과, 찾아된 타이틀(예컨대, 'OO 은행'이나 '△△ 은행' 등)이 메뉴항목으로서 표시된다.

이 상태에서, 사용자가 이동국(MS)의 지시 입력부(23)에 대해 자신이 구좌를 갖고 있는 은행 명에 대응하는 메뉴항목(즉, 'OO 은행')을 찾아하는 입력조작을 하면, 그 메뉴항목에 대응하는 문자열이 반전 표시된다. 이 반전 표시된 상태에서, 사용자가 지시 입력부(23)에 결정을 위한 입력조작을 하면, 이동국(MS)의 CPU(211)는 도 11에 나타난 처리를 실행한다.

이 처리에서 CPU(211)는 우선, 찾아된 메뉴항목 'OO 은행'에 대응하는 URL 'https://www.OObank.co.jp/index.html#utn'을 추출하여, 그 URL에 개인 식별정보 요구 데이터열(즉, 'utn')이 포함되어 있는지 여부를 판정한다(단계 S1, S2).

그리고, 추출한 URL에 개인정보 요구 데이터열이 포함되어 있지 않은 경우(단계 S2 'No'), CPU(211)는 그 URL이 SSL에 의한 통신을 지정하고 있는지 여부를 판단한다(단계 S9). 이 때, CPU(211)는 이 URL이 'http'로 시작되는 것인지, 'https'로 시작되는 것인지에 따라, 이 URL이 SSL에 의한 통신을 지정하고 있는지 여부를 판정한다. 그리고, 그 URL이 SSL에 의한 통신을 지정하고 있는 경우(단계 S9 'Yes'), CPU(211)는 SSL에 의한 통신을 시작하기 위한 처리를 실행하여(단계 S10), GET 요구를 송신한다(단계 S11). 한편, 상기 URL이 SSL에 의한 통신을 지정하지 않은 경우(단계 S9 'No'), CPU(211)는 SSL 핸드셰이크를 확립하지 않고 GET 요구를 송신한다(단계 S11). 그리고, CPU(211)는 플래시 메모리(214)의 이력 저장 테이블(TBL)에 해당 URL을 액세스 이력으로서 저장하는 동시에, 요구 데이터열 플래그(F)로서 '0'을 저장한다(단계 S12).

또, 이 때의 처리의 차이에 관해서는 뒤에 상세히 설명한다.

한편, 이 경우, 메뉴항목 'OO 은행'이 찾아되어 있다. 이 때문에, CPU(211)에 의해 추출되는 URL에는 개인정보 요구 데이터열이 포함되어 있다(단계 S2 'Yes'). 이러한 경우, CPU(211)는 도 12에 나타난 화면을 액정표시부(24)에 표시하게 한다(단계 S3). 즉, 이동국(MS)의 액정표시부(24)에는 '개인 식별정보가 요구됩니다. 송신하시겠습니까?' 등의 사용자의 판단을 재촉하는 문자와 함께 'Yes'와 'No' 버튼이 표시되는 것이다. 이 상태에서, 사용자가 'No' 버튼을 찾아 한 경우, CPU(211)는 단계 S4에서 'No'라고 판정하고, 처리를 종료한다.

한편, 사용자가 'Yes'를 찾아하는 입력조작을 하면, CPU(211)는 단계 S4에서 'Yes'라고 판정하여, 단계 S1에서 추출한 URL이 SSL에 의한 통신을 지정하고 있는지 여부를 판정한다(단계 S5). 이 때, CPU(211)는 이 URL이 'http'로 시작되는 것인지, 'https'로 시작되는 것인지에 따라, 이 URL이 SSL에 의한 통신을 지정하고 있는지 여부를 판정한다. 그리고, 이 단계 S5에서의 판단 결과에 따라 통신 시스템(1)에서는 다음과 같은 2개의 다른 처리가 실행된다.

(i) 처리 1

이 처리는 URL이 SSL에 의한 통신을 지정하고 있는 것으로 판정된 경우(즉, 단계 S5 'Yes'인 경우)에 행해지는 처리이다. 예컨대, 메뉴항목 'OO 은행'에 대응하는 URL 'https://www.OObank.co.jp/index.html#utn'과 같이 'https'로 시작하는 URL이 지정된 경우에는 이 처리 1이 실행되는 것이다.

이 처리 1에서는, CPU(211)에 의해 SSL에 의한 통신을 시작하기 위한 처리가 실행되므로(단계 S6), 통신 시스템(1)에서는 도 13에 나타난 데이터의 송수신이 실행된다. 이 과정에서는 우선, 이동국(MS)의 CPU(211)가 'connect' 신호(DS1)를 송수신부(22)를 통해 게이트웨이 서버(GWS)로 송신한다. 이 신호(DS1)가 수신되면, 게이트웨이 서버(GWS)는 IP 서버(W)에 'TCP Connect' 신호(DS2)를 송신한다. 이렇게 하여 IP 서버(W)에 대한 신호(DS2)의 송신이 종료하면, 게이트웨이 서버(GWS)는 이동국(MS)에 'Connection established' 신호(DS3)를 송신한다.

한편, 이 'Connection established' 신호(DS3)를 수신하면, 이동국(MS)의 CPU(211)는 IP 서버(W)에 'Client hello' 신호(DS4)를 송신한다. 이렇게 하여, 이동국(MS)에서 송신된 'Client hello' 신호(DS4)가 IP 서버(W)의 통신부(114)에 의해 수신되면, 데이터 전송 관리부(111)는 'Server hello' 신호(DS5)를 이동국(MS)에 송신한다. 이상 설명한 신호(DS1 ~ DS5)의 송수신 결과, 이동국(MS)과 IP 서버(W) 사이에서 SSL 핸드셰이크가 행해져, 이동국(MS)과 IP 서버(W) 사이에서 엔드 투 엔드의 SSL 통신이 가능해진다.

다음에, 이동국(MS)의 CPU(211)는 단계 S7을 실행하여, 메뉴항목 'OO 은행'에 대응하는 URL 'https://www.OObank.co.jp/index.html'을 포함하는 GET 요구(DS6)에 개인 식별정보(즉, 제조번호) '△△△△△△'를 부가하여 이동 패킷 통신망(MPN)에 송출한다(단계 S7). 그리고, CPU(211)는 플래시 메모리(214)의 이력 저장 테이블(TBL)에 대해 URL 'http://www.OObank.co.jp/index.html'을 액세스 이력으로서 저장하는 동시에, 요구 데이터열 플래그(F)로서 '1'을 저장한다(단계 S8).

한편, 이동국(MS)에서 송신된 GET 요구(DS6)가 IP 서버(W)의 통신부(114)에 의해 수신되면, 데이터 전송 관리부(111)는 이 GET 요구(DS6)에 부가되어 있는 URL 'https://www.OObank.co.jp/index.html'을 추출하여 RAM에 저장한다. 다음에, 데이터 전송 관리부(111)는 RAM에 저장된 URL에 따라, 이동국(MS)의 사용자가 원하는 서비스가 사용자 인증을 필요로 하는 것인지 여부를 판정한다. 그리고, 이 판정 결과, 사용자 인증이 필요 없다고 판정한 경우, 데이터 전송 관리부(111)는 RAM에 저장한 URL에 대응하는 HTML 데이터를 회신하고, 처리를 종료한다.

한편, 이러한 경우, 이동국(MS)의 사용자가 원하는 서비스는 '넷 뱅킹' 서비스이다. 이 때문에, 이러한 판정 처리에서, 데이터 전송 관리부(111)는 사용자 인증이 필요한 것으로 판정하고, GET 요구(DS6)에 부가된 개인 식별정보 '△△△△△△'를 추출하여 인증부(112)로 보낸다. 이렇게 하여, 데이터 전송 관리부(111)로부터 개인 식별정보가 송신되면, 인증부(112)는 이 개인 식별정보 '△△△△△△'를 검색키로 하여 개인 식별정보 데이터베이스(113)를 검색한다. 그리고, 이 검색 결과, 개인 식별정보 '△△△△△△'가 찾아지지 않은 경우, 인증부(112)는 GET 요구(DS6)의 송신원인 이동국(MS)의 사용자가 정당한 사용자가 아닌 것으로 간주하고, 데이터 전송 관리부(111)로 처리를 종료하라는 명령을 보낸다.

한편, 도 5에서 개인 식별정보 데이터베이스(113)에는 개인 식별정보 '△△△△△△'가 저장되어 있다. 이러한 경우, 인증부(112)는 개인 식별정보 데이터베이스(113)로부터 개인 식별정보 '△△△△△△'에 대응하는 사용자 ID 'user.a'를 독출하여 데이터 전송 관리부(111)에 보낸다. 그리고, 데이터 전송 관리부(111)는 이동국(MS)의 사용자가 정당한 사용자인 것으로 판정하여, RAM에 저장되어 있는 URL 'https://www.OObank.co.jp/index.html'에 대응하는 HTML 데이터(DS7)를 인터넷(INET)으로 송출하는 것이다.

(ii) 처리 2

이 처리는 해당 URL이 SSL에 의한 통신을 지정하지 않고 있다고 판정된 경우(즉, 단계 S5 'No')에 행해지는 것이다. 이동국(MS)의 CPU(221)가 이 처리 2를 실행하면, 통신 시스템(1)에서는 도 14에 나타난 데이터의 송수신이 실행된다. 예컨대, 메뉴항목 '△△ 은행'에 대응하는 URL 'http://www.△△bank.co.jp/index.html#utn'과 같이 'http'로 시작하는 URL이 지정된 경우에는 이 처리 2가 실행된다.

이 처리 2에서, CPU(211)는 메뉴항목 '△△ 은행'에 대응하는 URL 'http://www.△△bank.co.jp/index.html#utn'을 포함하는 GET 요구(D1)에 개인 식별정보(즉, 제조번호) '△△△△△△'를 부가하여 이동 패킷 통신망(MPN)에 송출한다(단계 S7). 다음에, CPU(211)는 플래시 메모리(214)의 이력 저장 테이블(TBL)에 URL 'http://www.△△bank.co.jp/index.html'을 액세스 이력으로서 저장하는 동시에, 요구 데이터열 플래그(F)로서 '1'을 저장한다(단계 S8). 이렇게 하여, 이동국(MS)에서 송출된 GET 요구(D1)는 그 후에 게이트웨이 서버(GWS)에 의해서 수신되어 프로토콜 변환된 다음, GET 요구(D2)로서 인터넷(INET)으로 전송된다.

다음에, GET 요구(D2)가 통신부(114)에 의해 수신되면, 데이터 전송 관리부(111)에 의해 상술한 처리 1과 같은 처리가 실행되고, URL 'http://www.△△bank.co.jp/index.html'에 대응하는 HTML 데이터(D3)가 인터넷(INET)으로 송출되어, 게이트웨이 서버(GWS)에 의해 HTML 데이터(D4)로서 전송된다.

이상 설명한 처리 1 또는 처리 2를 통해 송신된 HTML 데이터(D4 또는 DS7)가 이동국(MS)에 의해 수신되면, 이동국(MS)의 액정표시부(24)에는 도 15에 나타난 화면이 표시된다. 여기서, 이 도면에 나타난 각 메뉴항목에는 각 메뉴항목에 대응하는 서비스의 제공을 받기 위한 페이지로 이동하기 위한 URL이 대응되어 있다. 또, 이들 각 메뉴항목에 대응하는 URL에 대해서는, 개인 식별정보 요구 데이터열 'utn'이 부가된 URL을 이용하는지 여부는 임의이다. 또 사용자 인증을 필요로 하는 경우에는, 개인 식별정보 요구 데이터열 'utn'이 부가된 URL을 이용하는 것이 좋고, 사용자 인증을 필요로 하지 않는 경우에는 개인 식별정보 요구 데이터열 'utn'이 부가되지 않은 URL을 이용하는 것이 좋다. 이 상태에서, 집세를 송금하고자 하는 사용자가 이동국(MS)의 이지 입력부(23)에 대해 '은행 송금'을 선택하는 입력 조작을 한다. 그렇게 하면, 이동국(MS)에서는 상술한 도 11과 같은 처리가 실행되어, '은행 송금'에 대응하는 URL을 포함하는 GET 요구에 대해 개인 식별정보 '△△△△△△'를 부가하여 이동 패킷 통신망(MPN)에 송출한다. 또, 이 때 메뉴항목에 대응하는 URL이 SSL에 의한 통신을 지정하고 있는지 여부에 따라, 상술한 처리 1 또는 처리 2 중 어느 한 처리와 같은 처리가 실행된다.

그리고, IP 서버(W)에서 GET 요구에 대응하는 HTML 데이터가 송신되면, 이동국(MS)의 액정표시부(24)에는 도 16에 나타난 은행 송금용 화면이 표시된다. 그 후, 사용자가 송금할 계좌번호와 집세에 해당하는 금액 등을 입력하고 결정을 하는 입력조작을 한다. 그렇게 하면, 이동국(MS)은 이들 정보와, 개인 식별정보 '△△△△△△'를 포함하는 GET 요구를 송신한다. 이렇게 하여, 이동국(MS)에서 GET 요구가 송신되면, IP 서버(W)는 수신한 GET 요구로부터 각종 정보를 추출하여 은행 송금을 실행한다.

한편, 이동국(MS)이 도 16의 화면에 대응하는 HTML 데이터의 다운로드 중에 통신상태가 악화하여, HTML 데이터의 다운로드에 실패한 경우, 이동국(MS)은 다시 도 16의 화면에 대응하는 HTML 데이터를 다운로드 해야 한다. 이러한 경우에, 이동국(MS)은 이력 저장 테이블(TBL)에서 요구 데이터열 플래그(F)를 독출한다. 그리고, 요구 데이터열 플래그(F)가 '0'인지 '1'인지에 따라 다음과 같이 처리를 변경한다.

(a) 요구 데이터열 플래그(F) = '1'일 때

이 경우, 이동국(MS)의 CPU(211)는 재독출을 위한 화면에 대응하는 GET 요구를 송신할 때, 이 GET 요구에 개인 식별정보 '△△△△△△'를 부가하여 송신한다. 예컨대, 상술한 도 10의 메뉴항목 'OO 은행'이나 '△△ 은행'에 대응하는 URL과 같이 URL에 개인정보 송신요구 데이터열 'utn'이 부가되어 있는 경우, 상술한 도 11의 단계 S8에서의 처리 결과, 이동국(MS)의 이력 저장 테이블(TBL)에는 요구 데이터열 플래그(F)로서 '1'이 저장되어 있다. 이 경우, 해당 화면에 대응하는 HTML 데이터를 재독출할 때, 이동국(MS)의 CPU(211)는 IP 서버(W)에 대해 개인 식별정보를 부가하여 GET 요구를 송신한다. 이 결과, 이동국(MS)의 액정표시부(24)에는 도 16에 나타난 화면이 표시된다. 그리고, 마찬가지로 '은행 송금' 등의 서비스가 제공된다.

(b) 요구 데이터열 플래그(F) = '0'일 때

이 경우, 이동국(MS)의 CPU(211)는 재독출을 위한 화면에 대응하는 URL을 포함하는 GET 요구를 송신할 때, 이 GET 요구에 개인 식별정보 '△△△△△△'를 부가하지 않는다.

이상, 사용자가 은행 송금을 하는 경우를 예로 하여 본 실시형태의 동작을 설명하였지만, 이동국(MS)의 사용자가 회원제 서비스를 받을 때에도 완전히 동일한 처리가 통신 시스템(1)에서 실행된다.

이렇게 하여, 본 실시형태에의 사용자 인증방법은 HTML 데이터에 포함된 URL에 개인 식별정보 요구 데이터열이 부가되어 있는 경우에, 이동국이 사용자의 승낙을 얻어 개인 식별정보를 IP 서버에 송신하고, IP 서버가 개인 식별정보에 따라 사용자 인증을 하는 구성으로 되어있다. 이 때문에, 이동통신 사업자와 특별한 계약을 맺지 않고도 모든 IP에서 개인 식별정보를 이용한 사용자 인증을 하는 것이 가능해진다.

또한, 본 실시형태에의 이동국은 개인 식별정보를 송신하는 데 있어서, 사용자의 승인을 얻기 위한 화상을 액정표시부에 표시하여, 사용자의 승낙이 얻어진 경우에만 개인 식별정보를 송신하는 구성으로 하고 있다. 이 때문에, 사용자가 의도하지 않은 경우에도 개인 식별정보가 송신되어, 개인 식별정보가 부정 사용되는 것을 효과적으로 방지하는 것이 가능해진다.

또한, 본 실시형태에서는 게이트웨이 서버의 검색 서비스를 이용한 경우에도, 사용자 인증을 필요로 하는 서비스를 제공하는 페이지의 URL에는 개인 식별정보 요구 데이터열이 부가되어 송신된다. 이 때문에, 검색 서비스를 이용하여 IP 서버에 액세스한 경우에도, 확실히 개인 식별정보를 부가한 GET 요구가 송신되기 때문에, 보다 확실히 사용자 인증을 하는 것이 가능해진다.

또한, 본 실시형태에서는 IP 서버 등으로부터 송신되는 데이터의 형식으로서 HTML 형식의 데이터를 사용하기 때문에, 기존의 설비를 이용하여 본 발명의 효과를 달성하는 것이 가능해진다.

또, 본 실시형태에서는 개인 식별정보에 이용하는 고유한 정보로서 이동국(MS)의 제조번호를 이용하는 구성에 관해 설명하였지만, 이동국(MS)의 전화번호 등의 정보를 이용하는 것도 물론 가능하다.

또, 본 실시형태에서는 개인 식별정보로서 데이터열 'utn'을 이용했지만, 다른 데이터열을 이용하는 것도 물론 가능하다.

또, 본 실시형태에서는 이동국(MS)이 이동 패킷 통신망(MPN)을 통해 통신하는 경우에 관해 설명하였다. 그러나, 본 발명은 이것에 한하지 않고, 고정전화망에 수용되는 퍼스널 컴퓨터 등의 단말을 이용하여 통신하는 경우에도 적용 가능하다. 이 경우, 퍼스널 컴퓨터에 상기 실시형태의 이동국(MS)과 같은 기능을 갖게 함으로써, 상기 실시형태와 같은 처리를 실행하는 것이 가능하다.

또, 본 실시형태에서 IP 서버(W)나 게이트웨이 서버(GWS)로부터 이동국(MS)으로 송신되는 데이터는 HTML 형식의 데이터인 것으로 하고 설명하고 있다. 그러나, 본 발명은 이것에 한하지 않고, XML(eXtensive Markup Language) 등의 다른 마크업 언어를 사용해도 상관없다.

<1-3. 변형예>

<변형예 1>

본 실시형태에서는 게이트웨이 서버(GWS)에 검색기능을 마련하여, 이동국(MS)에 검색 서비스를 제공하는 구성으로 하고 있다. 그러나, 검색 서비스의 제공원은 게이트웨이 서버(GWS)가 아니라 인터넷(INET)상의 검색 엔진으로 할 수도 있다. 이 경우, 검색 엔진에 검색용 데이터베이스를 갖게 함으로써, 본 실시형태와 같은 효과를 달성하는 것이 가능해진다.

<변형예 2>

본 실시형태에서는 게이트웨이 서버(GWS)가 이동국(MS)에서 송신된 키워드에 따라 검색용 데이터베이스의 검색을 하는 구성으로 하고 있다. 그러나, 게이트웨이 서버(GWS)가 이동국(MS)에 대해 각종 서비스를 송신하는 방법은 다른 방법으로 실행될 수도 있다. 예컨대, 게이트웨이 서버(GWS)의 홈페이지 상에 '넷 뱅킹'이나 '게임' 등의 각종 서비스에 대응하는 메뉴항목을 마련하여, 각 메뉴항목마다 대응하는 페이지를 작성하는 구성도 가능하다. 이 경우, 이 각 메뉴항목마다 대응하는 페이지에는, 예컨대, 'OO 은행' 등의 메뉴항목을 마련한다. 그리고, 메뉴항목에 대응하는 URL을 앵커 태그에 의해 지정할 때 개인 식별정보 요구 데이터열 'utn'을 부가한다. 이러한 구성으로 하면, 본 실시형태와 같이 이동국(MS)의 사용자가 게이트웨이 서버(GWS)상에서 원하는 사이트를 찾는 것이 가능해진다.

<변형예 3>

본 실시형태에서 IP 서버(W)는 이동국(MS)에서 송신된 개인 식별정보에만 따라 사용자 인증을 하는 구성으로 되어 있다. 그러나, 보다 확실한 사용자 인증을 하기 위해 다른 정보를 병용하는 구성으로 해도 상관없다. 예컨대, 다음과 같은 방법이 있다.

i) 방법 a

이 방법은 개인 식별정보에 따라 사용자 인증을 한 후에 사용자에게 패스워드를 입력하게 하는 방법이다.

이 방법을 채용하는 경우, IP 서버(W)의 개인 식별정보 데이터베이스(113)의 기억내용을 도 17과 같이 변경한다. 즉, 각 사용자 ID에 대응하여 개인 식별정보와 패스워드를 저장한다. 여기서, 이 패스워드는 IP와 이동국(MS)의 사용자가 서비스의 제공계약을 맺었을 때 IP에 의해 부여되는 패스워드이다.

그리고, IP 서버(W)의 데이터 전송 관리부(111)는 이동국(MS)으로부터 개인 식별정보를 부가한 GET 요구(DS6 또는 D2)(도 13, 도 14)가 송신되면, 그 GET 요구(DS6 또는 D2)에 부가된 URL을 추출하여 RAM에 저장하는 동시에, GET 요구(DS6 또는 D2)로부터 개인 식별정보를 추출하여 인증부(112)에 송신한다. 인증부(112)는 이 개인 식별정보에 따라 개인 식별정보 데이터베이스(113)를 검색하여, 그 개인 식별정보에 대응하는 사용자 ID를 독출하여 데이터 전송 관리부(111)에 송신한다.

그리고, 인증부(112)로부터 사용자 ID가 송신되면, 데이터 전송 관리부(111)는 그 사용자 ID를 RAM에 저장하는 동시에, 도 18에 나타난 것과 같은 패스워드 등을 입력하기 위한 화면(이하, '패스워드 입력화면'이라 한다)에 대응하는 HTML 데이터를 인터넷(INET)으로 송출한다.

이 HTML 데이터가 이동국(MS)에 의해 수신되어, 액정표시부(24)상에 도 18에 나타난 패스워드 입력화면이 표시되어 있는 상황에서, 이동국(MS)의 지시 입력부(23)에 패스워드와 사용자 ID를 입력하여 결정하기 위한 입력조작을 하면, 이동국(MS)의 제어부(21)는 이동 패킷 통신망(MPN)에 대해, 패스워드 등을 포함하는 GET 요구를 송출한다. IP 서버(W)의 데이터 전송 관리부(111)는 이 GET 요구를 수신하면, 그 GET 요구로부터 패스워드와 사용자 ID를 추출하여 인증부(112)로 송신한다.

인증부(112)는 데이터 전송 관리부(111)로부터 송신된 사용자 ID에 대응하는 패스워드를 개인 식별정보 데이터베이스(113)로부터 독출한다. 그리고, 인증부(112)는 독출한 패스워드와 데이터 전송 관리부(111)로부터 송신된 패스워드가 일치하는지 여부를 판정하여, 그 인증 결과를 데이터 전송 관리부(111)에 보낸다. 다음에, 데이터 전송 관리부(111)는 이 사용자 인증 결과, 해당 사용자가 정당한 사용자인 것으로 판단한 경우에만 서비스를 제공한다.

또, 이 경우, IP 서버(W)가 제공하는 서비스마다 보안 확보의 필요성에 따라 인증방법을 변경할 수도 있고, 개인 식별정보에 의해서만 사용자 인증이 실행될 수도 있다. 또한, 패스워드 대신, 지문정보 등의 바이오 매트릭스 정보를 송신하는 구성으로 할 수도 있다.

ii) 방법 b

이 방법은 이동국(MS)이 개인 식별정보를 송신할 때, 사용자에게 사용자 ID의 입력을 재촉하여, 사용자가 입력한 사용자 ID와 개인 식별정보를 IP 서버(W)에 송신함으로써 사용자 인증을 하는 방법이다.

이 경우, 상술한 도 11의 단계 S3에서 이동국(MS)의 액정표시부(24)에 표시되는 화면(도 12)에 사용자 ID를 입력하는 박스를 추가한다. 도 19는 이 경우에 이동국(MS)의 액정표시부(24)에 표시되는 화면의 일례를 나타낸 도면이다. 여기서, 이 도면에 나타난 화면이 표시된 상태에서 사용자가 자신의 사용자 ID를 입력하고 송신 버튼을 누르면, 이동국(MS)의 제어부(21)는 입력된 사용자 ID와 개인 식별정보를 부가한 GET 요구(DS6 또는 D2)(도 13, 도 14)를 이동 패킷 통신망(MPN)에 송신한다.

한편, IP 서버(W)에서는 데이터 전송 관리부(111)가 GET 요구(DS6 또는 D2)로부터 개인 식별정보와 사용자 ID를 추출하여 인증부(112)로 송신한다. 인증부(112)는 이 송신된 정보에 따라 사용자 인증을 한다. 구체적으로는, 인증부(112)는 데이터 전송 관리부(111)로부터 송신된 사용자 ID에 대응하는 개인 식별정보를 개인 식별정보 데이터베이스(113)로부터 독출하여, 해당 개인 식별정보와 데이터 전송 관리부(111)로부터 송신된 개인 식별정보가 일치하는지 여부를 판정한다. 그리고, 인증부(112)는 그 인증 결과를 데이터 전송 관리부(111)에 보낸다. 데이터 전송 관리부(111)는 이 사용자 인증 결과, 해당 사용자가 정당한 사용자인 것으로 판단한 경우에만 서비스를 제공하는 것이다.

이와 같이 개인 식별정보에 의한 사용자 인증뿐만 아니라, 다른 인증방법을 병용함으로써 사용자 인증의 확실성을 보장하는 것이 가능해진다. 특히, '넷 뱅킹'과 같이 사용자의 재산에 관계하는 서비스에 관해서는, 개인 식별정보에 의한 사용자 인증뿐만 아니라, 다른 인증방법을 병용하는 것에 의한 효과는 대단히 큰 것이 된다.

<변형예 4>

도 20은 본 변형예에 있어서의 이동국(MS2)의 구성을 나타낸 블록도이다. 또, 이 도면에서 상술한 도 7과 같은 요소에 관해서는 동일한 부호를 부여한다.

본 변형예에 있어서의 특징적인 구성으로서, 이동국(MS2)은 UIM(User Identity Module)(2000)을 접속하기 위한 UIM 인터페이스부(26)(이하, '인터페이스'를 'I/F'라 약칭한다)를 구비하여, UIM(2000)과 접속된 상태로 사용된다. 여기서, UIM(2000)은 사용자의 가입자 번호 등의 사용자 고유의 정보를 갖는 모듈이다. 이동국(MS2)의 제어부(21)는 UIM I/F부(26)에 의해 UIM(2000)과 데이터를 교환하고, 이동 패킷 통신망(MPN)의 패킷 교환 서비스를 받는다. 또한, 본 변형예에서는 이동 패킷 통신망(MPN)에서의 패킷 교환 서비스의 제공을 받을 때, 예컨대, GSM(Global System for Mobile Communications)에서의 SIM과 같이 각 UIM(2000) 단위로 가입자 번호가 발행되어, 과금도 각 UIM(2000) 단위로 행해진다.

다음에, UIM(2000)에 관해 보다 상세히 설명한다. 도 21은 UIM(2000)의 구성을 나타낸 블록도이다. 이 도면에 나타낸 바와 같이, UIM(2000)은 CPU(2001), 외부 I/F부(2002), ROM(2003), RAM(2004), EEPROM(2005)으로 구성된다.

외부 I/F부(2002)는 CPU(2001)와 이동국(MS2)의 UIM I/F부(26) 사이의 데이터의 송수신을 중개한다. ROM(2003)은 불휘발성 메모리이고, 제어 프로그램 외에 도, 이동국(MS2)으로부터 공급되는 제어지시의 해석, 실행, 응답, 데이터 관리 등을 위한 프로그램이 기억되어 있다. CPU(2001)는 ROM(2003)에 저장되어 있는 프로그램을 실행함으로써 UIM(2000)의 각 부를 제어한다. RAM(2004)은 CPU(2001)의 작업영역으로 쓰인다. EEPROM(2005)에는 가입자 정보 등의 사용자 고유의 정보 외에도, UIM(2000)의 제조번호 등의 정보가 저장되어 있다.

여기서, IP 서버(W)가 이동국(MS2)에 제공하는 서비스 중에는 캐릭터 콘텐츠나, 음악 콘텐츠 등을 송신하는 것이 존재한다. 이들 서비스에 대해서는 콘텐츠 단위로 과금이 행해지기 때문에, 동일한 서비스에 대해 송신요구가 두 번째 수신된 경우에는 과금을 하지 않은 것이 많다. 이 때문에, 본 변형예와 같이 UIM(2000) 단위로 과금을 하는 통신 시스템에서는, 동일한 UIM(2000)을 사용함으로써 일회의 과금으로 다수의 이동국(MS2)에 동일한 콘텐츠를 다운로드 하는 부정사용이 가능해지게 된다. 그래서, 본 변형예에서는 개인 식별정보로서 이동국(MS2)의 제조번호뿐만 아니라, UIM(2000)에 고유한 정보(본 변형예에서는 'UIM(2000)의 제조번호')를 이용함으로써 사용자 인증을 하는 구성으로 되어있다.

이하, 본 변형예의 동작에 대해 상술한 실시형태와 다른 부분에 관해 설명한다.

우선, 본 변형예에 있어서의 이동국(MS2)에서는 도 11의 단계 S1 S6과 같은 처리가 실행된다. 그리고, 도 11의 단계 S7에서 이동국(MS2)이 GET 요구를 송신할 때, CPU(211)는 UIM(2000)에 대해 그 UIM(2000)의 제조번호의 송신을 요구한다. UIM(2000)의 CPU(2001)는 이동국(MS2)으로부터 제조번호에 대한 송신요구가 보내지면, EEPROM(2005)으로부터 제조번호를 독출하여, 외부 I/F부(2002)를 통해 이동국(MS2)으로 송신한다.

그리고, 이동국(MS2)의 CPU(211)는 ROM(212)으로부터 독출한 이동국(MS2)의 제조번호와 함께 이 UIM(2000)으로부터 취득한 UIM의 제조번호를 개인 식별정보로서 부가한 GET 요구를 이동 패킷 통신망(MPN)으로 송출한다. IP 서버(W)는 이 GET 요구에 부가된 이동국(MS2)의 제조번호와 UIM(2000)의 제조번호에 따라 사용자 인증을 한다. 이것에 따라, IP 서버(W)의 개인 식별정보 데이터베이스(113)는 도 22에 나타낸 바와 같이 그 기억내용이 변경된다. 즉, 각 사용자 ID에 대응하는 개인 식별정보로서 이동국(MS2)의 제조번호와 UIM의 제조번호가 저장되어 있다. 인증부(112)는 이동국(MS2)으로부터 송신된 2개의 제조번호와 개인 식별정보 데이터베이스(113)에 저장되어 있는 정보가 일치하는지 여부를 판정하여, 일치하는 경우에 인증이 성공한 것으로 한다.

이렇게 하여, 본 변형예에 의하면, 이동국의 제조번호뿐만 아니라 UIM의 제조번호도 개인 식별정보로서 이용하여 사용자 인증을 하는 구성으로 하고 있다. 이 때문에, 이동국 단위로 과금이 행해질 수 있는 경우뿐만 아니라, UIM 등의 모듈 단위로 과금이 행해지는 시스템에서도 간단하고 확실한 사용자 인증을 하는 것이 가능해지는 동시에, 인증의 신뢰성을 확보하는 것이 가능해진다.

산업상 이용 가능성

이상 설명한 바와 같이, 본 발명에 의하면 이동통신 사업자와 특별한 계약을 맺지 않고도, 모든 IP에서 개인 식별정보를 이용한 사용자 인증을 가능하게 하는 사용자 인증방법 및 통신 시스템을 제공하여, 간단하고 확실한 사용자 인증을 하는 것이 가능한 동시에, 인증의 신뢰성을 확보하는 것이 가능하다.

(57) 청구의 범위

청구항 1.

제1 네트워크에 수용된 휴대단말이 상기 제1 네트워크로부터 하나 이상의 데이터 항목을 포함하는 데이터를 수신하는 수신과정;

상기 휴대단말이 상기 수신과정에서 수신한 데이터 중에서 사용자가 데이터 항목을 선택한 경우에, 상기 데이터 항목에 소정의 데이터열이 존재하는지 여부를 검출하는 검출과정;

상기 검출과정에서 상기 데이터열이 존재하는 것으로 검출된 경우에만, 상기 휴대단말이 미리 이 휴대단말에 기억되어 있는 사용자를 일의적으로 특정하기 위한 개인 식별정보를 송신하는 송신과정;

상기 제1 네트워크와 제2 네트워크 사이의 데이터 송수신을 중계하는 중계장치가 상기 휴대단말에서 송신된 개인 식별정보를 상기 제2 네트워크로 전송하는 전송과정; 및

상기 제2 네트워크에 접속된 서버로서, 상기 데이터 항목에 대응하는 서버가 상기 개인 식별정보에 따라 상기 휴대단말의 사용자를 인증하는 인증과정을 구비하는 것을 특징으로 하는 사용자 인증방법.

청구항 2.

제1항에 있어서,
상기 송신과정에서 상기 휴대단말은 상기 서버 이외의 장치에 의해 해독 불가능한 형식으로 상기 개인 식별정보를 송신하고;
상기 인증과정에서 상기 서버는 상기 개인 식별정보를 해독하여, 그 개인 식별정보에 따라 상기 휴대단말의 사용자를 인증하는 것을 특징으로 하는 사용자 인증방법.

청구항 3.

제1항에 있어서,
상기 중계장치가 상기 휴대단말로부터의 요구에 따라 상기 제2 네트워크에 있어서의 상기 서버의 어드레스를 검색하는 검색과정을 더 포함하고;
상기 수신과정에서 상기 휴대단말이 수신하는 상기 데이터는 상기 검색과정에서 상기 중계장치가 검색한 검색결과에 대응하는 데이터인 것을 특징으로 하는 사용자 인증방법.

청구항 4.

제1항에 있어서,
상기 데이터는 마크업 언어로 기술되고;
상기 데이터열은 상기 데이터 내에 포함되는 소정의 식별자인 것을 특징으로 하는 사용자 인증방법.

청구항 5.

제1항에 있어서,
상기 검출과정에서 상기 데이터열이 존재하는 것으로 검출된 경우에만, 상기 휴대단말이 이 휴대단말의 사용자에 대하여, 상기 개인 식별정보의 송신 여부에 관해 판단을 재촉하는 판단촉진과정을 더 포함하고;
상기 송신과정에서 상기 휴대단말은 상기 판단촉진과정에서 상기 사용자의 허가가 얻어진 경우에만, 상기 개인 식별정보를 송신하는 것을 특징으로 하는 사용자 인증방법.

청구항 6.

제5항에 있어서,
상기 판단촉진과정에서 상기 휴대단말은 사용자의 판단을 재촉하기 위한 화상을 표시하는 동시에, 사용자에게 대하여 입력 식별정보의 입력을 재촉하고;
상기 송신과정에서 상기 휴대단말은 상기 개인 식별정보와 함께 사용자가 입력한 입력 식별정보를 송신하며;
상기 인증과정에서 상기 서버는 상기 송신과정에서 송신된 개인 식별정보와 상기 입력 식별정보에 따라 사용자 인증을 하는 것을 특징으로 하는 사용자 인증방법.

청구항 7.

제1항에 있어서,
상기 인증과정 후에 상기 서버가 상기 휴대단말에 대하여 입력 식별정보의 입력을 재촉하는 입력 데이터를 송신하는 송신과정;
상기 송신과정에서 송신된 상기 입력 데이터를 수신한 상기 휴대단말이 상기 입력 데이터에 근거하여 사용자에게 대해 상기 입력 식별정보의 입력을 재촉하는 과정;
상기 입력을 재촉하는 과정에서 입력된 입력 식별정보를 송신하는 제2 송신과정; 및
상기 제2 송신과정에서 송신된 상기 입력 식별정보에 따라 상기 휴대단말의 사용자를 인증하는 제2 인증과정을 더 포함하는 것을 특징으로 하는 사용자 인증방법.

청구항 8.

제1항에 있어서,
상기 개인 식별정보는 상기 휴대단말의 제조번호인 것을 특징으로 하는 사용자 인증방법.

청구항 9.

제1항에 있어서,
상기 개인 식별정보는 상기 휴대단말의 제조번호와 상기 휴대단말에 접속된 사용자 식별모듈에 저장된 정보와의 조합으로 구성되는 것을 특징으로 하는 사용자 인증방법.

청구항 10.

제1항에 있어서,
상기 제1 네트워크는 이동통신망이고;
상기 휴대단말은 상기 이동통신망을 통해 통신하는 이동국인 것을 특징으로 하는 사용자 인증방법.

청구항 11.

제1 네트워크로부터 하나 이상의 데이터 항목을 포함하는 데이터를 수신하여, 그 데이터 중에서 사용자가 데이터 항목을 선택한 경우에, 상기 데이터 항목에 소정의 데이터열이 존재하는지 여부를 검출하고, 상기 데이터열이 존재하는 것으로 검출된 경우에만, 미리 단말에 기억되어 있는 사용자를 일의적으로 특정하기 위한 개인 식별정보를 상기 제1 네트워크에 송신하는 휴대단말;
상기 제1 네트워크와 중계장치를 통해 상호 접속된 제2 네트워크; 및

상기 제2 네트워크에 접속되고, 상기 데이터 항목에 대응하는 서버로서, 상기 개인 식별정보에 따라 인증을 하는 서버를 구비하는 것을 특징으로 하는 통신 시스템.

청구항 12.

제1 네트워크를 통해 타자와 통신하는 통신부; 및

상기 통신부에 의해 상기 제1 네트워크 및 이 제1 네트워크에 접속된 제2 네트워크를 통해 상기 제2 네트워크내의 서버와 통신하여, 상기 서버로부터 수신한 하나 이상의 데이터 항목을 포함하는 데이터 중에서 사용자가 데이터 항목을 선택한 경우에, 상기 데이터 항목 중에 소정의 데이터열의 존재가 검출되었을 때, 상기 휴대단말에 설치된 메모리 또는 상기 휴대단말에 접속된 메모리로부터 개인 식별정보를 독출하여, 상기 접속을 통해 상기 개인 식별정보를 상기 서버에 송신하는 제어부를 구비하는 것을 특징으로 하는 휴대단말.

청구항 13.

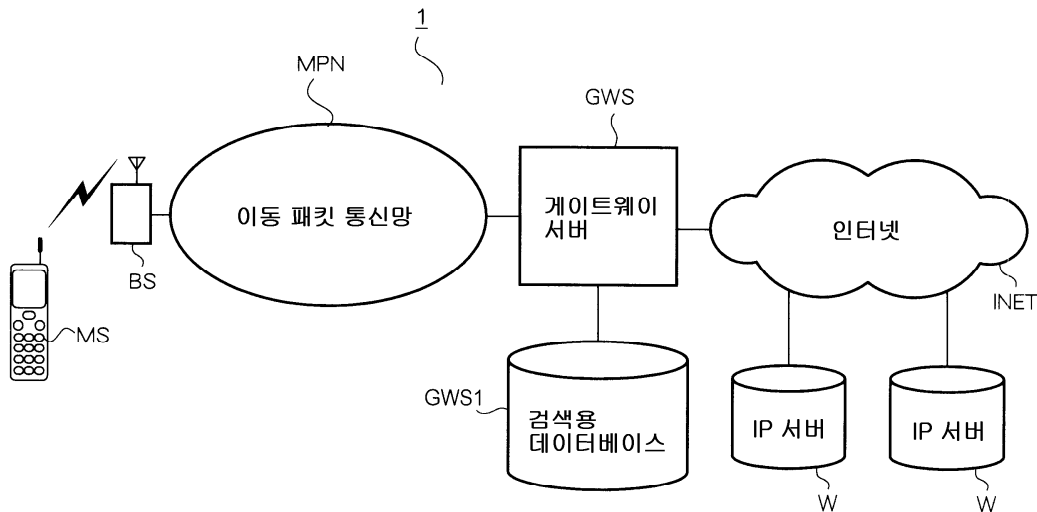
삭제

청구항 14.

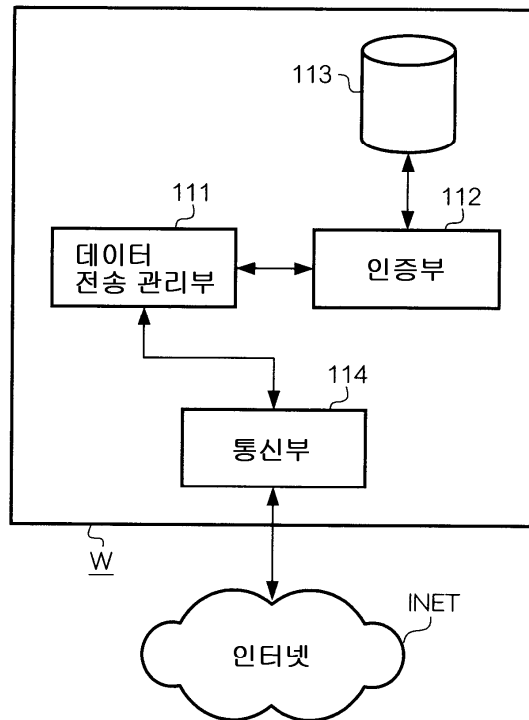
통신부에 의해 제1 네트워크 및 이 제1 네트워크에 접속된 제2 네트워크를 통해 상기 제2 네트워크내의 서버와 통신하여, 상기 서버로부터 수신한 하나 이상의 데이터 항목을 포함하는 데이터 중에서 사용자가 데이터 항목을 선택한 경우에, 상기 데이터 항목 중에 소정의 데이터열의 존재가 검출되었을 때, 휴대단말에 설치된 메모리 또는 상기 휴대단말에 접속된 메모리로부터 개인 식별정보를 독출하여, 상기 통신부에 의해 상기 서버에 송신하는 처리를 컴퓨터에 실행시키는 프로그램을 기억한 기록매체.

도면

도면1



도면2



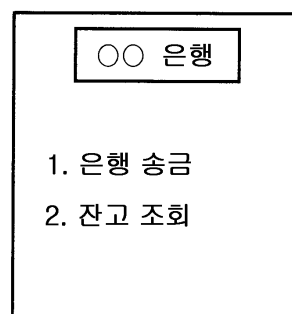
도면3

```

<HTML>
<HEAD>
<TITLE>〇〇 은행 </TITLE>
<META name="△△" content="△△">
</HEAD>
<CENTER>
<H2><IMG src="△△GIF" alt="〇〇 은행 "
height="30" width="200"><FONT color="#004000">
〇〇 은행 </FONT></H2>
</CENTER>
<BODY>
<BR>
<A href="http://www.〇〇bank.co.jp/△△#utn">
1. 은행 송금 </A>
<FONT size="-1"><BR>
<BR>
<A href="http://www.〇〇bank.co.jp/××#utn">
2. 잔고 조회 </A>
<FONT size="-1"><BR>
</BODY>

```

도면4



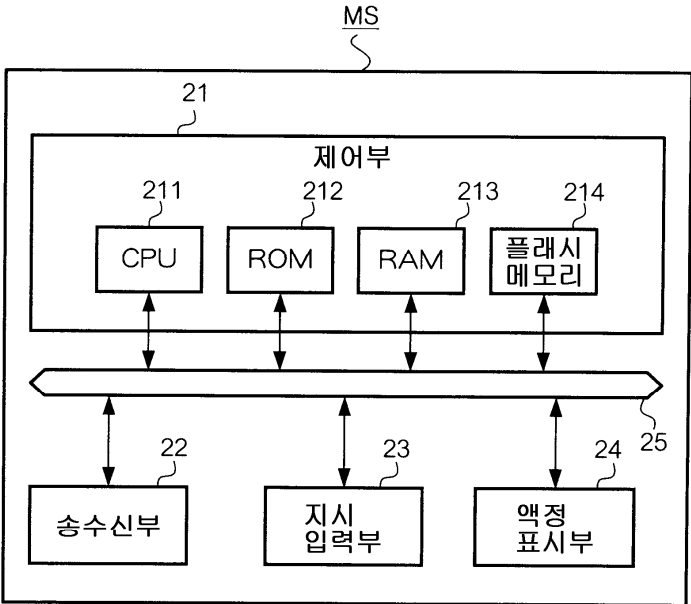
도면5

사용자 ID	개인 식별 정보
user.a	△△△△△△
user.b	■ ■ ■ ■ ■ ■
...	...

도면6

타이틀	키 워드	URL
○○ 은행	넷 뱅킹	https://www.○○ bank.co.jp/index.html#utn
	...	
×× 상사	넷 옥션	http://www.××.co.jp
	...	
△△ 은행	넷 뱅킹	http://www.△△ bank.co.jp/index.html#utn
	...	
...	...	...

도면7



도면8

F
└─┘

URL	요구 데이터열 플래그
http://△△.co.jp	1
http://■■.co.jp	0
...	...

└─┘
TBL

도면9

검색 서비스

키 워드

도면10

검색 결과

키 워드 "넷 뱅킹"

1

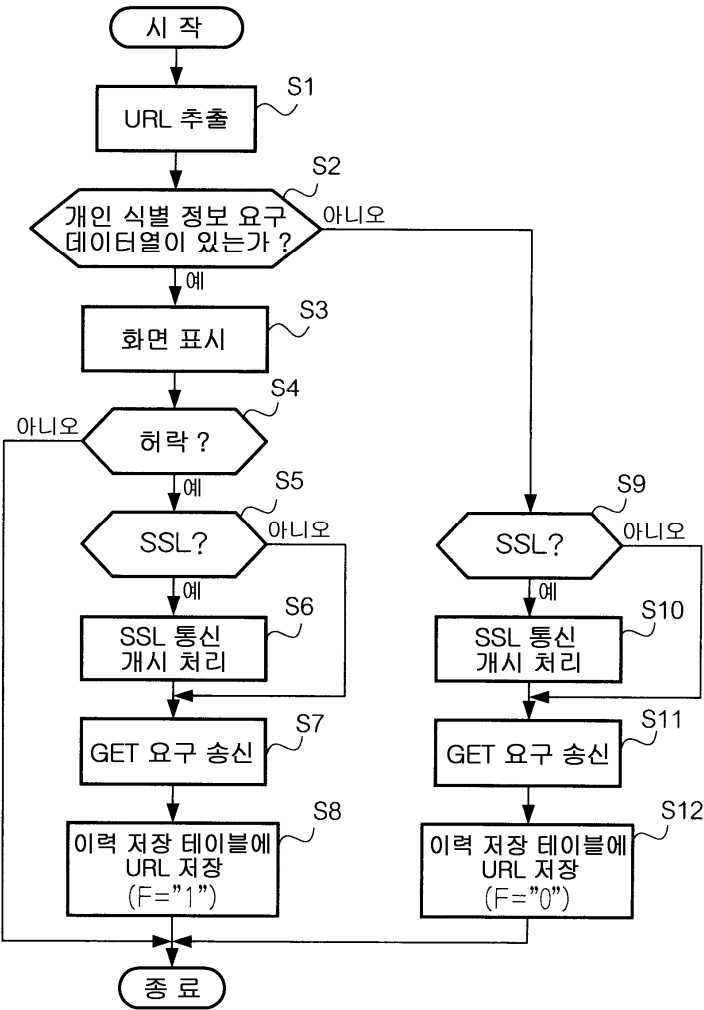
○○ 은행

2

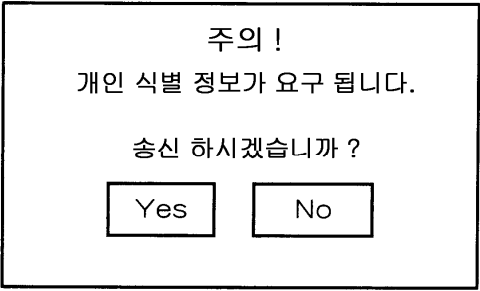
△△ 은행

...

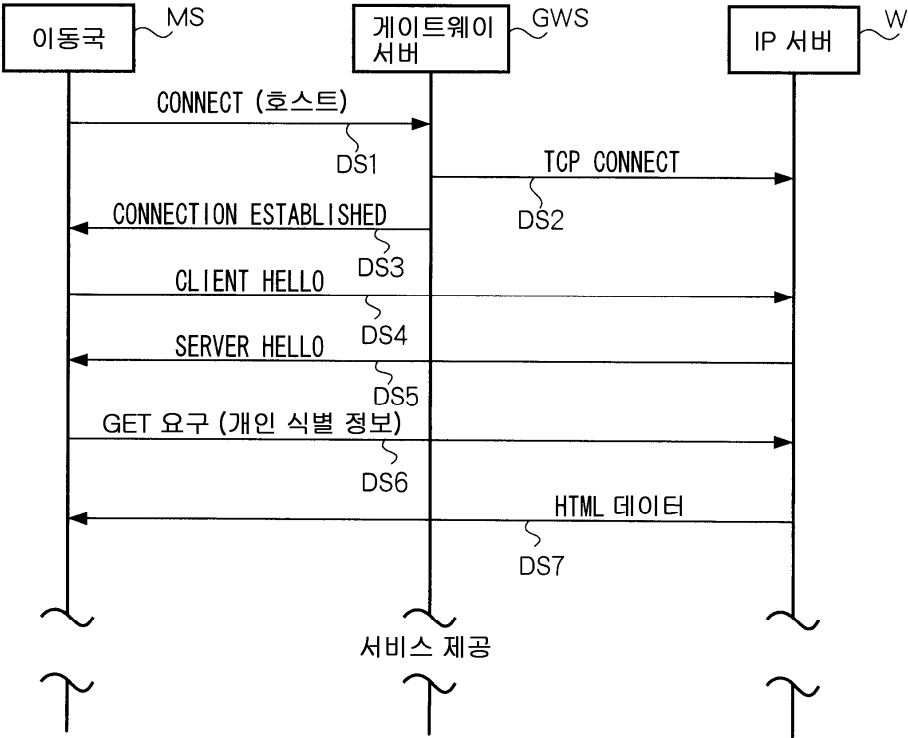
도면11



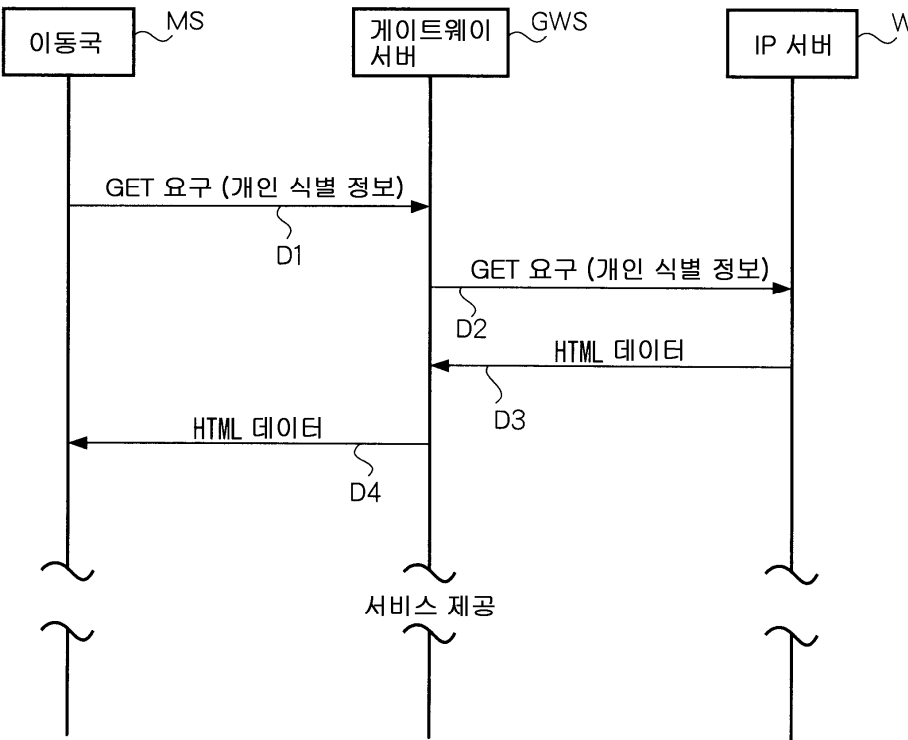
도면12



도면13



도면14



도면15

○○ 은행

1

은행 송금

2

잔고 조회

...

도면16

은행 송금 페이지

.....

.....

.....

.....

.....

돌아가기

도면17

사용자 ID	개인 식별 정보	패스워드
user.a	△△△△△△	△△△△
user.b	■ ■ ■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■
...	...	...

도면18

서비스 로그인

사용자 ID

패스워드

도면19

주의 !

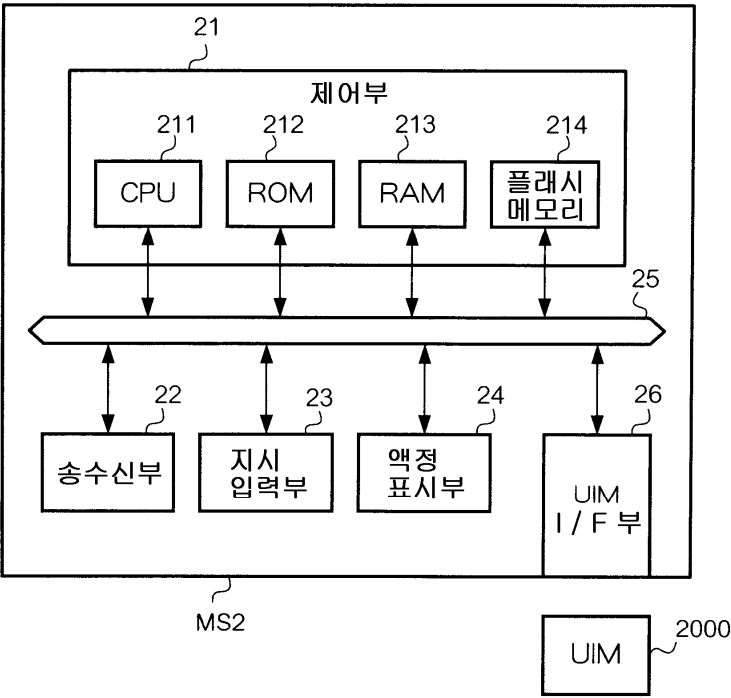
개인 식별 정보가 요구됩니다.

송신하시려면 사용자 ID를
입력하세요.

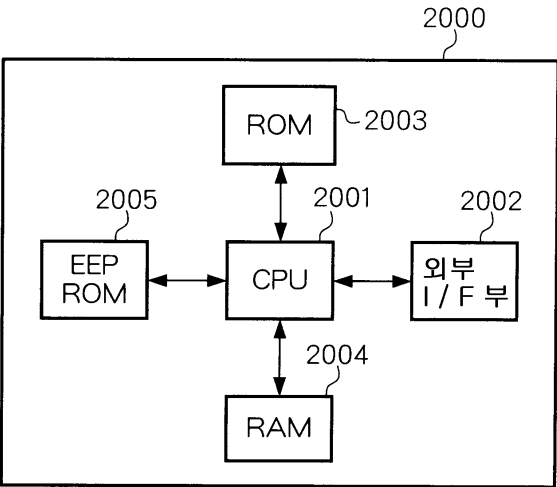
사용자 ID

송신

도면20



도면21



도면22

사용자 ID	개인 식별 정보	
	이동국	UIM
user.a	△△△△△△	△△△△
user.b	■ ■ ■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■
...	...	...