(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/32 (2006.01)

(45) 공고일자 2007년01월22일
(11) 등록번호 10-0672922
(24) 등록일자 2007년01월16일

(21) 출원번호 10-2005-0082609
(22) 출원일자 2005년09월06일
심사청구일자 2005년09월06일

(65) 공개번호 10-2006-0051040
(43) 공개일자 2006년05월19일

(30) 우선권주장 JP-P-2004-00260196 2004년09월07일 일본(JP)

(73) 특허권자 가부시키가이샤 엔.티.티.도코모
일본 도쿄도 지요다쿠 나가타쵸 2쵸메 11반 1고

(72) 발명자 노구치 가쓰히로
일본 도쿄도 지요다쿠 나가타쵸 2쵸메 11반 1고 가부시키가이샤엔.티.티.도코모 지적재산부 내

(74) 대리인 유미특허법인

심사관 : 양종필

전체 청구항 수 : 총 6 항

(54) 중계 장치, 인증 서버 및 인증 방법

(57) 요약

본 발명은, 단말 장치로부터 상기 단말 장치의 사용자의 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 수신하는 제1 시큐리티 정보 수신부와, 상기 제1 시큐리티 정보에 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성하는 시큐리티 정보 처리부와, 제2 시큐리티 정보를 인증 서버에 송신하는 시큐리티 정보 송신부를 포함하는 중계 장치를 제공한다.

대표도

도 5

특허청구의 범위

청구항 1.

단말 장치로부터, 상기 단말 장치의 사용자의 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 수신하는 제1 시큐리티 정보 수신부와;

상기 제1 시큐리티 정보에 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성하는 시큐리티 정보 처리부와;

제2 시큐리티 정보를 인증 서버에 송신하는 시큐리티 정보 송신부

를 포함하는 중계 장치.

청구항 2.

제1항에 있어서,

상기 인증 서버로부터, 상기 제2 시큐리티 정보에 기초하여 생성된, 상기 단말 장치의 사용자용의 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 수신하는 제2 시큐리티 정보 수신부를 더 포함하는 것을 특징으로 하는 중계 장치.

청구항 3.

단말 장치의 사용자에 대한 사용자 인증 처리 및 중계 장치에 대한 중계 장치 인증 처리를 행하는 인증 서버에 있어서,

상기 중계 장치로부터 수신한, 상기 사용자의 사용자 ID 및 사용자 인증 정보와 상기 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 포함하는 제2 시큐리티 정보에 기초하여, 상기 단말 장치의 사용자가 정규의 사용자인지의 여부를 판단하는 사용자 인증 처리를 행하는 제1 인증 처리부와;

상기 제2 시큐리티 정보에 기초하여, 상기 중계 장치가 정규의 중계 장치인지의 여부를 판단하는 중계 장치 인증 처리를 행하는 제2 인증 처리부

를 포함하는 인증 서버.

청구항 4.

제3항에 있어서,

상기 제2 시큐리티 정보에 기초하여, 상기 단말 장치의 사용자용의 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 생성하는 시큐리티 정보 생성부와;

상기 제3 시큐리티 정보를 상기 중계 장치에 송신하는 시큐리티 정보 송신부를 더 포함하는 것을 특징으로 하는 인증 서버.

청구항 5.

단말 장치의 사용자에 대한 사용자 인증 처리 및 중계 장치에 대한 중계 장치 인증 처리를 행하는 인증 방법에 있어서,

상기 단말 장치가, 상기 사용자의 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 상기 중계 장치에 송신하는 단계와;

상기 중계 장치가 상기 제1 시큐리티 정보에 상기 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성하는 단계와;

상기 중계 장치가 상기 제2 시큐리티 정보를 인증 서버에 송신하는 단계와;

상기 인증 서버가, 상기 제2 시큐리티 정보에 기초하여, 상기 단말 장치의 사용자가 정규의 사용자인지의 여부를 판단하는 사용자 인증 처리를 행하는 단계와;

상기 인증 서버가, 상기 제2 시큐리티 정보에 기초하여, 상기 중계 장치가 정규의 중계 장치인지의 여부를 판단하는 중계 장치 인증 처리를 행하는 단계

를 포함하는 인증 방법.

청구항 6.

제5항에 있어서,

상기 인증 서버가 상기 단말 장치의 사용자용의 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 생성하는 단계와;

상기 인증 서버가 상기 제3 시큐리티 정보를 상기 중계 장치에 송신하는 단계를 더 포함하는 것을 특징으로 하는 인증 방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 중계 장치, 인증 서버 및 인증 방법에 관한 것이다.

종래, 중계 장치가 사업자에 의해 관리되어 있는 경우, 인증 서버가 데이터 은닉, 데이터 완전성 확보 등을 행하기 위해 필요한 시큐리티 정보를, 사업자에 의해 관리되고 있는 중계 장치(이하에서는 "사업자 관리 중계 장치"로 지칭함)에 통지하고, 단말 장치와 사업자 관리 중계 장치 사이에서 데이터의 은닉과 완전성 확보를 행한다. 도 1은 단말 장치(100)와 사업자 관리 중계 장치(200a) 간에 보안성의 통신로가 확보되어 있는 것을 나타내고 있다.

한편, 사업자 관리 중계 장치뿐만 아니라, 사업자에 의해 관리되고 있지 않은 중계 장치(이하에서는 "사업자 관리 외의 중계 장치"로 지칭함)도 수용하지 않으면 안되는 것이 상정된다(예를 들면, H. Yumida 등의 "IP-Based IMT Network Platform, IEEE Personal Communication Magazine, Oct. 2001, pp. 18-23 참조). 사업자 관리 외의 중계 장치로서는 예를 들면, 사용자 가정이나 사무실에 설치하는 액세스 포인트가 거론된다. 이와 같이, 사업자 관리 외의 중계 장치를 수용하는 경우, 단말 장치와 인증 서버 간에 있어서, 데이터의 은닉과 완전성 확보를 행하는 것이 필요하다. 도 1은 단말 장치(100), 사업자 관리 외의 중계 장치(200b) 및 인증 서버(300) 간에 보안성의 통신로가 확보되어 있는 것을 나타내고 있다.

그러나, 사업자 관리 외의 중계 장치가 사업자 관리 중계 장치의 ID를 사용하여, 사업자 관리 중계 장치가 되어 버려, 데이터 도청이나 데이터 무단변조에 의한 사용자의 프라이버시 침해라는 위협을 일으킨다는 문제가 발생한다. 도 2는 사업자 관리 외의 중계 장치(200b)가 사업자 관리 중계 장치(200a)의 ID(ID#1)를 사용하여 사업자 관리 중계 장치(200a)가 되는 것을 나타내고 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상기의 문제점을 감안하여, 사업자 관리 외의 중계 장치가 사업자 관리 중계 장치가 되어 버려, 데이터 도청이나 데이터 무단변조에 의한 사용자의 프라이버시 침해라는 위협을 야기하는 것을 방지하는 중계 장치, 인증 서버 및 인증 방법을 제공하는 것을 목적으로 한다.

본 발명에 따르면, 단말 장치로부터 상기 단말 장치의 사용자의 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 수신하는 제1 시큐리티 정보 수신부와, 상기 제1 시큐리티 정보에 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성하는 시큐리티 정보 처리부와, 제2 시큐리티 정보를 인증 서버에 송신하는 시큐리티 정보 송신부를 포함하는 중계 장치가 제공된다.

또한, 본 발명에 따르면, 단말 장치의 사용자에 대한 사용자 인증 처리 및 중계 장치에 대한 중계 장치 인증 처리를 행하는 인증 서버로서, 상기 중계 장치로부터 수신한, 상기 사용자의 사용자 ID 및 사용자 인증 정보와 상기 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 포함하는 제2 시큐리티 정보에 기초하여, 상기 단말 장치의 사용자가 정규의 사용자인지의 여부를 판단하는 사용자 인증 처리를 행하는 제1 인증 처리부와, 상기 제2 시큐리티 정보에 기초하여, 상기 중계 장치가 정규의 중계 장치인지의 여부를 판단하는 중계 장치 인증 처리를 행하는 제2 인증 처리부를 포함하는 인증 서버가 제공된다.

또한, 본 발명에 따르면, 단말 장치의 사용자에 대한 사용자 인증 처리 및 중계 장치에 대한 중계 장치 인증 처리를 행하는 인증 방법으로서, 상기 단말 장치가, 상기 사용자의 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 상기 중계 장치에 송신하는 단계와, 상기 중계 장치가 상기 제1 시큐리티 정보에 상기 중계 장치의 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성하는 단계와, 상기 중계 장치가 상기 제2 시큐리티 정보를 인증 서버에 송신하는 단계와, 상기 인증 서버가, 상기 제2 시큐리티 정보에 기초하여, 상기 단말 장치의 사용자가 정규의 사용자인지의 여부를 판단하는 사용자 인증 처리를 행하는 단계와, 상기 인증 서버가, 상기 제2 시큐리티 정보에 기초하여, 상기 중계 장치가 정규의 중계 장치인지의 여부를 판단하는 중계 장치 인증 처리를 행하는 단계를 포함하는 인증 방법이 제공된다.

발명의 구성

본 발명의 여러 실시예를 첨부 도면을 참조하여 설명한다. 도면에 걸쳐 동일하거나 유사한 부분 및 구성요소에는 동일하거나 유사한 도면부호가 부여되어 있으며, 동일 또는 유사한 부분 및 구성요소에 대해서는 그 설명을 생략하거나 간략히 설명할 것이다.

또한, 본 출원은 2004년 9월 7일자 출원된 일본 특허 출원 제2004-260196호를 기초로 하고, 이를 우선권 주장하는 출원으로서, 상기 일본 출원의 내용은 본 명세서에서 참조되어 그 일부를 이룬다.

(인증 시스템)

본 실시예에 따른 인증 시스템은 도 3에 나타낸 바와 같이 단말 장치(100), 중계 장치(200) 및 인증 서버(300)를 구비한다.

인증 서버(300)는 단말 장치(100)의 사용자에 대한 사용자 인증 처리를 행한다. 또한, 인증 서버(300)는 중계 장치(200)의 중계 장치 ID에 대한 중계 장치 인증 처리를 행한다.

또, 본 실시예에 따른 인증 시스템에서는, 단말 장치(100)는 무선을 통하여 중계 장치(200)에 접속되고, 중계 장치(200)는 인증 서버(300)에 접속되어 있다.

단말 장치(100)는 도 4에 나타낸 바와 같이, 사용자 ID 기억부(101) 및 시큐리티 정보 송신부(102)를 구비한다. 단말 장치(100)로서는 예를 들면 휴대용 통신 단말기 등이 사용된다.

사용자 ID 기억부(101)는 단말 장치(100)의 사용자를 식별하기 위한 사용자 ID와 사용자 인증에 필요한 사용자 인증 정보를 기억한다. 예를 들면, 사용자 ID로서 휴대 전화기 번호 등이 사용된다. 또, 사용자 인증 정보로서는 디지털 서명이나 패스워드 등이 사용된다.

시큐리티 정보 송신부(102)는 사용자 인증 처리시에 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 중계 장치(200)에 송신한다.

중계 장치(200)는 도 5에 나타낸 바와 같이, 시큐리티 정보 수신부(201), 중계 장치 ID 기억부(202), 시큐리티 정보 처리부(203) 및 시큐리티 정보 송신부(204)를 구비한다. 중계 장치(200)로서는 예를 들면 무선 액세스 포인트 등이 사용된다.

시큐리티 정보 수신부(201)는 단말 장치(100)로부터 제1 시큐리티 정보를 수신한다. 또, 시큐리티 정보 수신부(201)는 인증 서버(300)로부터, 후술하는 제2 시큐리티 정보에 기초하여 생성된, 단말 장치(100)의 사용자용의 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 수신한다.

중계 장치 ID 기억부(202)는 중계 장치 ID와 중계 장치의 인증에 필요한 중계 장치 인증 정보를 기억한다. 예를 들면, 중계 장치 ID로서 IP 어드레스 등이 사용된다. 또, 중계 장치 인증 정보로서 디지털 서명이나 패스워드 등이 사용된다.

시큐리티 정보 처리부(203)는 제1 시큐리티 정보에 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성한다. 즉, 제2 시큐리티 정보에는 사용자 ID, 사용자 인증 정보, 중계 장치 ID 및 중계 장치 인증 정보가 포함된다.

시큐리티 정보 송신부(204)는 제2 시큐리티 정보를 인증 서버(300)에 송신한다.

인증 서버(300)는 도 6에 나타낸 바와 같이 시큐리티 정보 수신부(301), 사용자 인증 처리부(302), 중계 장치 인증 처리부(303), 시큐리티 정보 생성부(304) 및 시큐리티 정보 송신부(305)를 구비한다. 인증 서버(300)로서는 예를 들면, AAA (Application Authorization Accounting) 서버 등이 사용된다.

시큐리티 정보 수신부(301)는 중계 장치(200)로부터 제2 시큐리티 정보를 수신한다.

사용자 인증 처리부(302)는 제2 시큐리티 정보에 포함되는 사용자 ID와 사용자 인증 정보에 의하여 사용자가 정규의 사용자인지의 여부를 인증한다.

중계 장치 인증 처리부(303)는 제2 시큐리티 정보에 포함되는 중계 장치 ID와 중계 장치 인증 정보에 의하여 중계 장치가 정규의 중계 장치인지의 여부를 인증한다.

시큐리티 정보 생성부(304)는 제2 시큐리티 정보에 포함되는 사용자 ID와 사용자 인증 정보로부터 사용자용의 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 생성한다.

시큐리티 정보 송신부(305)는 제3 시큐리티 정보를 중계 장치(200)에 송신한다.

그리고, 단말 장치(100)의 사용자 ID 기억부(101), 중계 장치(200)의 중계 장치 ID 기억부(202)는 RAM 등의 내부 기억 장치에 있어도 되고, HD 또는 FD 등의 외부 기억 장치에 있어도 된다.

또, 본 실시예에 따른 인증 서버(300)는 처리 제어 장치(CPU)를 가지며, 전술한 사용자 인증 처리부(302), 중계 장치 인증 처리부(303) 등을 모듈로서 CPU에 내장하는 구성으로 할 수 있다. 마찬가지로, 중계 장치(200)는 처리 제어 장치(CPU)를 가지며, 전술한 시큐리티 정보 처리부(203) 등을 모듈로서 CPU에 내장하는 구성으로 할 수 있다. 이들 모듈은, 퍼스널 컴퓨터 등의 범용 컴퓨터에 있어서, 소정의 프로그램 언어를 이용하기 위한 전용 프로그램을 실행함으로써 실현할 수 있다.

또, 도시하지는 않았지만, 인증 서버(300) 및 중계 장치(200)는 사용자 인증 처리, 중계 장치 인증 처리, 시큐리티 정보 처리 등을 CPU에서 실행시키기 위한 프로그램을 저장하는 프로그램 유지부를 각각 구비하여도 된다. 프로그램 유지부는 예를 들면, RAM, ROM, 하드 디스크, 플렉서블 디스크, 컴팩트 디스크, IC 칩, 카세트 테이프 등의 기록 매체이다. 이와 같은 기록 매체에 의하면, 프로그램의 저장, 운반, 판매 등을 용이하게 행할 수 있다.

(인증 방법)

다음으로, 본 실시예에 따른 인증 방법에 대하여 도 7을 참조하여 설명한다.

먼저, 단계 S101에서, 사용자 인증 처리를 희망하는 단말 장치(100)는 사용자 ID와 사용자 인증 정보를 포함하는 제1 시큐리티 정보를 중계 장치(200)에 송신한다.

다음에, 단계 S102에서, 중계 장치(200)는 제1 시큐리티 정보에 중계 장치 ID와 중계 장치 인증 정보를 부가하여 제2 시큐리티 정보를 생성한다.

다음에, 단계 S103에서, 중계 장치(200)는 제2 시큐리티 정보를 인증 서버(300)에 송신한다.

다음에, 단계 S104에서, 인증 서버(300)는 수신한 제2 시큐리티 정보에 기초하여 단말 장치(100)의 사용자 ID에 대하여 사용자 인증 처리를 행한다.

다음에, 단계 S105에서, 인증 서버(300)는 수신한 제2 시큐리티 정보에 기초하여 중계 장치(200)의 ID에 대하여 중계 장치 인증 처리를 행한다.

다음에, 인증 서버(300)는 사용자 인증 및 중계 장치 인증에 성공한 경우, 데이터 은닉과 데이터 완전성 확보에 필요한 제3 시큐리티 정보를 생성한다. 그리고, 단계 S106에 있어서, 인증 서버(300)는 제3 시큐리티 정보를 중계 장치(200)에 송신한다.

또, 중계 장치(200)는 제3 시큐리티 정보를 단말 장치(100)에 송신한다.

발명의 효과

본 실시예에 따른 중계 장치(200), 인증 서버(300) 및 인증 방법에 의하면, 사업자 관리 외의 중계 장치가 사업자 관리 중계 장치가 되어, 데이터 도청이나 데이터 변조에 의한 사용자의 프라이버시 침해라는 위협을 야기하는 것을 방지할 수 있다.

구체적으로는, 중계 장치(200) 및 단말 장치(100)가 제3 시큐리티 정보를 사용하여 데이터 은닉 처리를 행하기 때문에, 사업자 관리 외의 중계 장치가 사업자 관리 중계 장치가 되어 버리는 것 등에 의해 데이터 도청을 행하는 것을 방어할 수 있다.

또, 중계 장치(200) 및 단말 장치(100)가 제3 시큐리티 정보를 사용하여, 데이터 완전성을 확보(Integrity Check)하기 때문에, 사업자 관리 외의 중계 장치가 사업자 관리 중계 장치가 되어 버리는 것 등에 의해 데이터 변조를 행하는 것을 방어할 수 있다.

(그 외의 실시예)

본 발명은 상기의 실시예에 따라서 기재하였지만, 이 개시 내용의 일부를 이루는 설명 및 도면은 본 발명을 한정하는 것으로 이해하여서는 안된다. 이 개시 내용으로부터 당업자는 다양한 대체 실시예, 실시예 및 운용 기술을 유추할 수 있다.

예를 들면, 본 실시예에 있어서, 중계 장치(200)는 무선 액세스 포인트인 것으로 가정하여 설명을 행하였으나, 중계 장치(200)로는 액세스 라우터가 사용될 수도 있다. 예를 들면, 사업자 관리 외의 중계 장치를 수용하는 경우, 사업자 관리 외의 중계 장치와 인증 서버(300) 사이에 액세스 라우터를 설치한다. 그리고, 액세스 라우터는 인증 서버(300)로부터 수신한 제3 시큐리티 정보에 기초하여 데이터 은닉과 데이터 완전성의 확보를 행한다.

본 기술분야의 당업자라면 본 명세서의 교시를 참조하여 본 발명의 범위에서 벗어남이 없이 다양한 변경이 가능할 것이다.

도면의 간단한 설명

도 1은 종래의 인증 시스템의 일구성에 대한 블록도.

도 2는 종래의 인증 시스템의 다른 구성에 대한 블록도.

도 3은 본 발명의 실시예에 따른 인증 시스템의 구성에 대한 블록도.

도 4는 본 발명의 실시예에 따른 단말 장치의 구성에 대한 블록도.

도 5는 본 발명의 실시예에 따른 중계 장치의 구성에 대한 블록도.

도 6은 본 발명의 실시예에 따른 인증 서버의 구성에 대한 블록도.

도 7은 본 발명의 실시예에 따른 인증 방법을 나타낸 플로차트.

<도면의 주요 부분에 대한 부호의 설명>

100 : 단말 장치

101 : 사용자 ID 기억부

102 : 시큐리티 정보 송신부

200 : 중계 장치

201 : 시큐리티 정보 수신부

202 : 중계 장치 ID 기억부

203 : 시큐리티 정보 처리부

204 : 시큐리티 정보 송신부

300 : 인증 서버

301 : 시큐리티 정보 수신부

302 : 사용자 인증 처리부

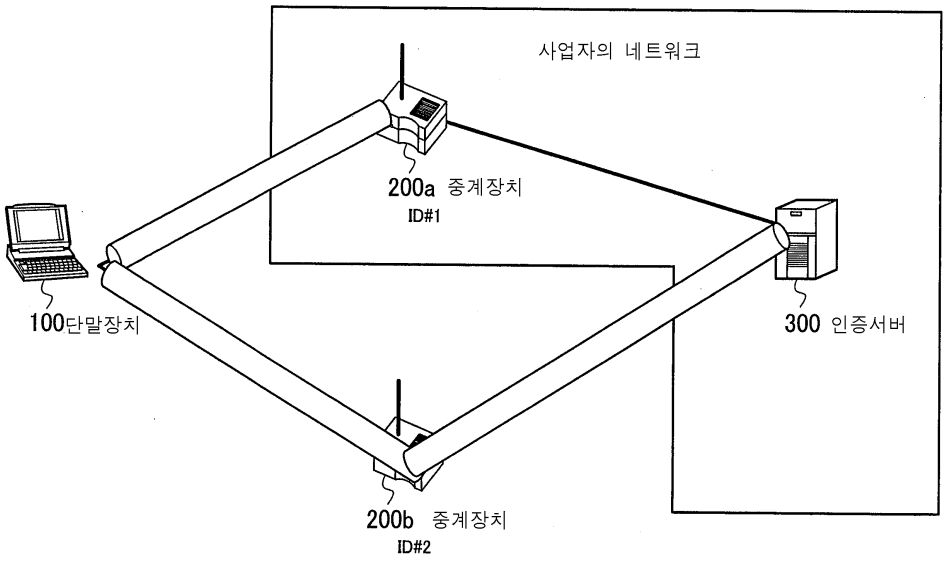
303 : 중계 장치 인증 처리부

304 : 시큐리티 정보 생성부

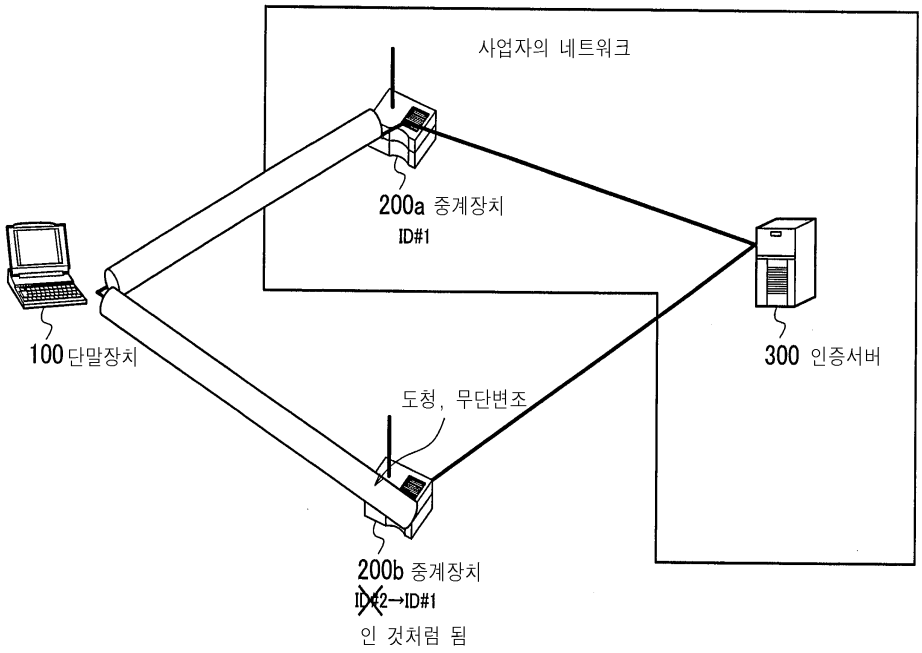
305 : 시큐리티 정보 송신부

도면

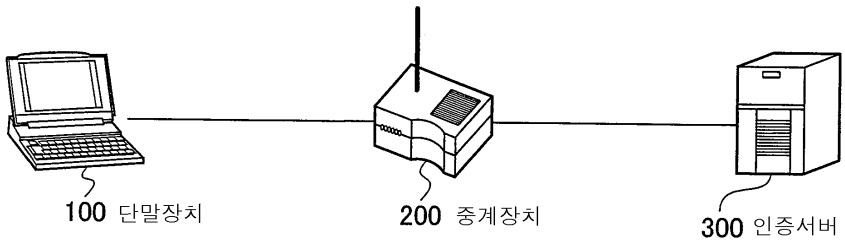
도면1


사업자의 네트워크
200a 중계장치
ID#1
100단말장치
300 인증서버
200b 중계장치
ID#2

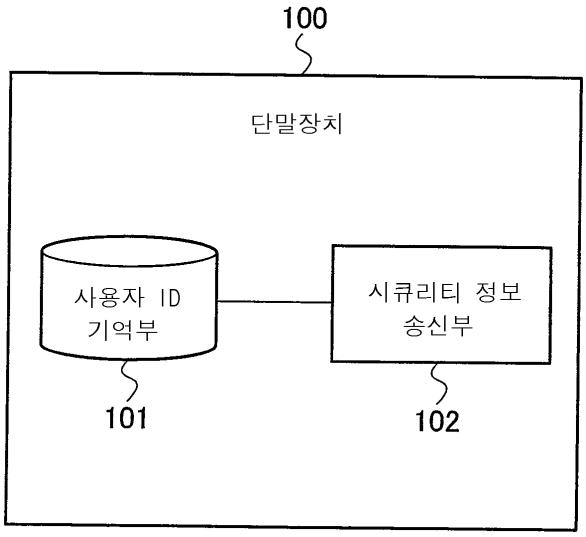
도면2


사업자의 네트워크
200a 중계장치
ID#1
100 단말장치
300 인증서버
도청, 무단변조
200b 중계장치
ID#2→ID#1
인 것처럼 됨

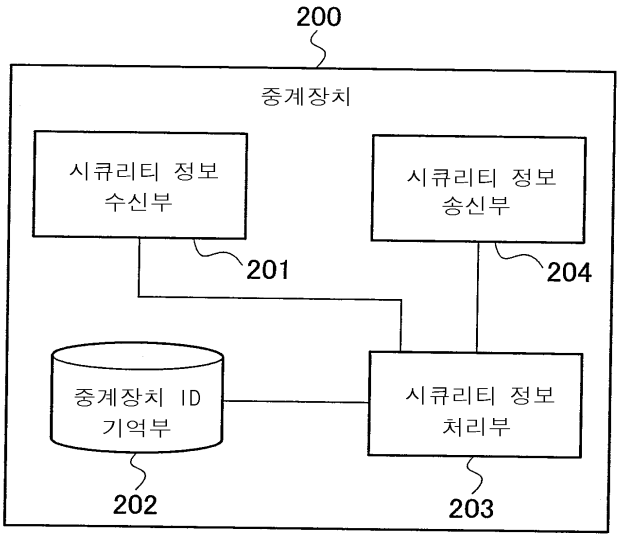
도면3


100 단말장치
200 중계장치
300 인증서버

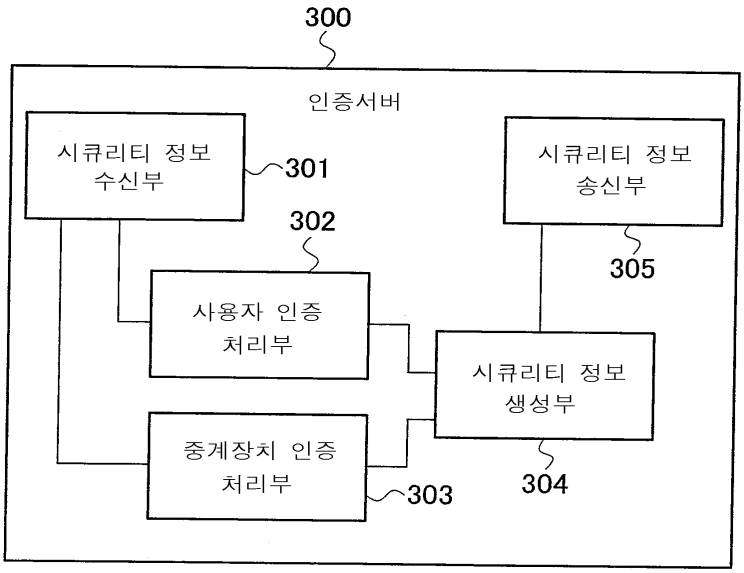
도면4


100
단말장치
사용자 ID
기억부
시큐리티 정보
송신부
101
102

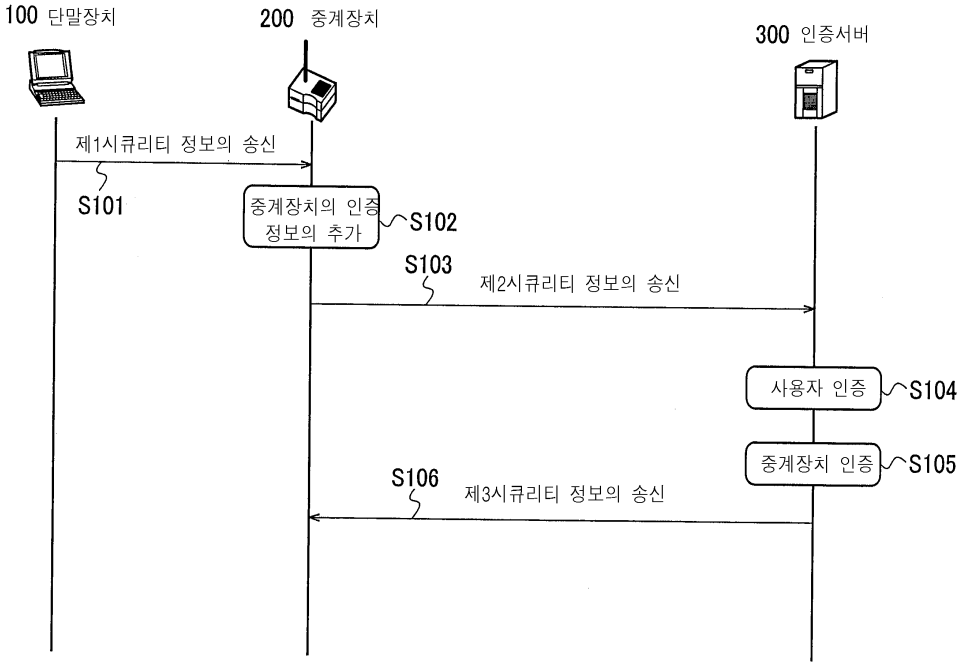
도면5


200
중계장치
시큐리티 정보
수신부
201
시큐리티 정보
송신부
204
중계장치 ID
기억부
202
시큐리티 정보
처리부
203

도면6


300
인증서버
시큐리티 정보
수신부
301
302
사용자 인증
처리부
중계장치 인증
처리부
303
시큐리티 정보
송신부
305
시큐리티 정보
생성부
304

도면7


100 단말장치
200 중계장치
300 인증서버
제1시큐리티 정보의 송신
S101
중계장치의 인증 정보의 추가
S102
S103
제2시큐리티 정보의 송신
사용자 인증
S104
중계장치 인증
S105
S106
제3시큐리티 정보의 송신