(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년03월26일
(11) 등록번호 10-0890287
(24) 등록일자 2009년03월17일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2007-0060471
(22) 출원일자 2007년06월20일
심사청구일자 2007년06월20일
(65) 공개번호 10-2007-0120909
(43) 공개일자 2007년12월26일
(30) 우선권주장
JP-P-2006-00170247 2006년06월20일 일본(JP)
(56) 선행기술조사문헌
KR1020060048552 A
전체 청구항 수 : 총 11 항

(73) 특허권자
캐논 가부시끼가이샤
일본 도꾜도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
기시모또 히로아끼
일본 도꾜도 오오따꾸 시모마루꼬 3-30-2 캐논 가부시끼가이샤 내
(74) 대리인
박충범, 장수길

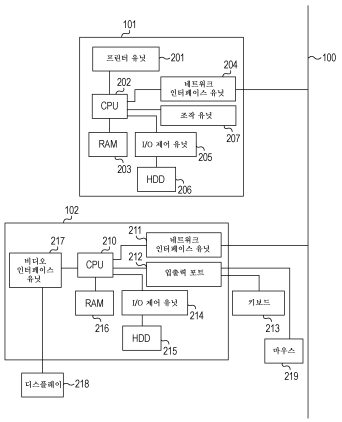
심사관 : 안철용

(54) 외부 인증 장치와 통신 가능한 정보 처리 장치

(57) 요 약

외부 인증 장치에서 인증 처리에 필요한 인증 정보가 암호 없이 사용자 단말로부터 정보 처리 장치에 송신되는 것이 제한된다. 정보 처리 장치는 암호화 정보를 통신하도록 구성된 암호화 통신을 사용하지 않는 경우 사용자가 외부 인증 장치에서 인증 처리를 선택할 수 있게 하는 정보 송신을 제한한다.

대 표 도 - 도2



특허청구의 범위

청구항 1

정보 처리 장치에 있어서,

암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하도록 구성된 송신 유닛; 및

상기 송신 유닛에 의해 송신된 상기 화면 정보에 기초하여, 상기 복수의 선택지 중 상기 외부 인증 장치에서의 인증 처리에 대응하는 선택지가 상기 사용자에 의해 선택된 경우, 상기 사용자 단말로부터 사용자가 입력한, 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 유닛

을 포함하며,

상기 송신 유닛은, 상기 암호화 통신을 사용하는 경우, 사용자가 상기 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하고, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 상기 사용자 단말에 송신하는 것을 제한하는 정보 처리 장치.

청구항 2

제1항에 있어서,

상기 송신 유닛은, 상기 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 입력할 수 있게 하고, 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하는 화면을, 웹 브라우저가 디스플레이할 수 있게 하는 정보를 송신하는 정보 처리 장치.

청구항 3

제1항 또는 제2항에 있어서,

상기 송신 유닛은, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 상기 정보 처리 장치에서의 인증 처리에 필요한 인증 정보를 입력할 수 있게 하고, 상기 정보 처리 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하는 화면을, 웹 브라우저가 디스플레이할 수 있게 하는 정보를 송신하는 정보 처리 장치.

청구항 4

제1항 또는 제2항에 있어서,

사용자가 상기 암호화 통신을 사용할지 사용하지 않을 지를 선택하게 할 수 있도록 구성된 설정 유닛을 더 포함하는 정보 처리 장치.

청구항 5

제1항 또는 제2항에 있어서,

사용자가 외부 인증 장치를 등록할 수 있도록 구성된 등록 유닛을 더 포함하며;

상기 송신 유닛은, 상기 암호화 통신을 사용하는 경우, 상기 등록 유닛에 의해 등록된 복수의 외부 인증 장치들의 리스트를 나타내는 정보를 송신하는 정보 처리 장치.

청구항 6

정보 처리 장치의 제어 방법에 있어서,

암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를

선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하도록 구성된 송신 단계; 및

상기 송신 단계에서 송신된 상기 화면 정보에 기초하여, 상기 복수의 선택지 중 상기 외부 인증 장치에서의 인증 처리에 대응하는 선택지가 상기 사용자에 의해 선택된 경우, 상기 사용자 단말로부터 사용자가 입력한, 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 단계

를 포함하며,

상기 송신 단계에서는, 상기 암호화 통신을 사용하는 경우, 사용자가 상기 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하고, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 상기 사용자 단말에 송신하는 것이 제한되는 정보 처리 장치의 제어 방법.

청구항 7

제6항에 있어서,

상기 송신 단계는, 상기 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 입력할 수 있게 하고, 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하는 화면을, 웹 브라우저가 디스플레이할 수 있게 하는 정보를 송신하도록 구성되는 정보 처리 장치의 제어 방법.

청구항 8

제6항 또는 제7항에 있어서,

상기 송신 단계는, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 상기 정보 처리 장치에서의 인증 처리에 필요한 인증 정보를 입력할 수 있게 하고, 상기 정보 처리 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하는 화면을, 웹 브라우저가 디스플레이할 수 있게 하는 정보를 송신하도록 구성되는 정보 처리 장치의 제어 방법.

청구항 9

제6항 또는 제7항에 있어서,

사용자가 상기 암호화 통신을 사용할지 사용하지 않을 지를 선택할 수 있도록 구성된 설정 단계를 더 포함하는 정보 처리 장치의 제어 방법.

청구항 10

제6항 또는 제7항에 있어서,

사용자가 외부 인증 장치를 등록할 수 있도록 구성된 등록 단계를 더 포함하며;

상기 송신 단계는, 상기 암호화 통신을 사용하는 경우, 상기 등록 단계에서 등록된 복수의 외부 인증 장치들의 리스트를 나타내는 정보를 송신하도록 구성되는 정보 처리 장치의 제어 방법.

청구항 11

정보 처리 장치인 컴퓨터가 판독할 수 있고 실행할 수 있는 컴퓨터 프로그램을 저장하는 기록 매체로서,

상기 컴퓨터가,

암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하도록 구성된 송신 단계; 및

상기 송신 단계에서 송신된 상기 화면 정보에 기초하여, 상기 복수의 선택지 중 상기 외부 인증 장치에서의 인증 처리에 대응하는 선택지가 상기 사용자에 의해 선택된 경우, 상기 사용자 단말로부터 사용자가 입력한 외부

인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 단계

를 실행하도록 하며,

상기 송신 단계에서는, 상기 암호화 통신을 사용하는 경우, 사용자가 상기 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 사용자 단말에 송신하고, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 선택지를 포함하는 복수의 선택지를 표시하기 위한 화면 정보를 상기 사용자 단말에 송신하는 것이 제한되도록 하는 컴퓨터 프로그램을 저장하는 기록 매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<17> 본 발명은 외부 인증 장치와 통신 가능한 정보 처리 장치에 관한 것이다.

<18> 인증 기능을 구비한 정보 처리 장치는 사용자가 네트워크를 통해 정보 처리 장치를 조작하는 경우 인증 처리를 실행한다. 예를 들어, 사용자가 웹 브라우저를 사용하여 사용자 모드로 이행할 것을 인쇄 장치에 명령할 때, 인쇄 장치는 웹 브라우저로부터 사용자 식별 번호 입력을 요구하고, 사용자가 입력한 사용자 식별 번호에 기초하여 인증 처리를 실행한다(예를 들어, 일본 특허 공개 번호 제2002-359718호).

<19> 사용자 식별 번호에 기초하여 인증이 성공한 경우, 인쇄 장치는 사용자 모드의 웹 페이지를 웹 브라우저에 송신한다. 따라서, 사용자는 사용자 모드의 웹 페이지로부터 인쇄 장치를 동작할 수 있다.

<20> 네트워크 환경에서, 인증 처리에 사용되는 인증 정보는 대부분의 경우 복수의 정보 처리 장치들 각각에 의해 관리되지 않고, 외부 인증 장치(이후, 인증 서버라고 함)에 의해 통합적으로 관리된다.

<21> 예를 들어, 사용자명, 패스워드 등과 같은 인증 정보는 인증 서버에서 보유되고, 정보 처리 장치는 인증 서버에게 사용자가 입력한 인증 정보에 기초하여 인증 처리를 실행할 것을 요구한다. 사용자가 네트워크를 통해 사용자 단말로부터 정보 처리 장치를 조작하는 경우, 정보 처리 장치는 네트워크를 통해 사용자 단말로부터 인증 정보를 수신하고, 수신된 인증 정보에 기초하여 인증 처리를 실행할 것을 인증 서버에 요구한다.

<22> 이 때에, 정보 처리 장치는 사용자 단말에서 사용자가 입력한 인증 정보 자체를 수신할 필요가 있다. 정보 처리 장치가 인증 처리를 실행하기 위한 인증 정보를 보유한 경우, 몇몇 인증 방법들에 따라, 사용자가 입력한 인증 정보 자체를 네트워크를 통해 정보 처리 장치에 송신할 필요는 없다. 한편, 정보 처리 장치가 사용자 단말 대신 동작하거나 인증 서버에 대한 인증 처리 요구에 관해 사용자 단말과 인증 서버 간에서 조정하는 경우, 정보 처리 장치는 사용자가 입력한 인증 정보 자체를 수신할 필요가 있다.

<23> 그러나, 인증 서버에서의 인증 처리에 필요한 인증 정보가 사용자 단말로부터 네트워크를 통해 정보 처리 장치에 송신되는 경우, 인증 정보는 제3자에 의해 쉽게 도청될 수 있으며, 쉽게 누설된다.

<24> 암호화 통신은 사용자 단말과 정보 처리 장치 사이에서 실행되어서, 인증 정보는 도청으로부터 보호될 수 있다. 그러나, 정보 처리 장치는 항상 암호 처리를 실행할 수는 없다. 예를 들어, 암호화 통신 사용이 사용자에 의해 설정되지 않은 경우, 정보 처리 장치는 암호화 통신을 실행할 수 없다.

<25> 정보 처리 장치가 의도한 바와는 달리 암호화 통신을 실행할 수 없는 상태에서 인증 서버에서 인증 처리를 선택할 수 있으면, 사용자 단말은 보안 구현 없이 인증 정보를 정보 처리 장치에 송신할 수 있다.

발명이 이루고자 하는 기술적 과제

<26> 결국, 본 발명은 외부 인증 장치에서 인증 처리에 필요한 인증 정보가 암호 없이 사용자 단말로부터 정보 처리 장치에 송신되는 것을 방지한다.

<27> 본 발명의 일 양태에 따라, 정보 처리 장치는 암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하도록 구성된 송

신 유닛; 및 상기 사용자 단말로부터 사용자가 입력한 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 유닛을 포함하며; 상기 송신 유닛은, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 상기 사용자 단말에 송신하는 것을 제한한다.

<28> 또한, 본 발명의 다른 양태에 따라, 정보 처리 방법은 암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하도록 구성된 송신 단계; 및 상기 사용자 단말로부터 사용자가 입력한 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 수신하도록 구성된 수신 단계를 포함하며; 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 상기 사용자 단말에 송신하는 것이 제한된다.

<29> 또한, 본 발명의 다른 양태에 따라, 컴퓨터가 판독할 수 있고 실행할 수 있는 컴퓨터 프로그램으로서, 암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하도록 구성된 송신 단계; 및 상기 사용자 단말로부터 사용자가 입력한 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 단계를 컴퓨터가 실행하도록 하며, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하는 것이 제한된다.

<30> 또한, 본 발명의 다른 양태에 따라, 컴퓨터가 판독할 수 있고 실행할 수 있는 컴퓨터 프로그램을 저장한 기록매체로서, 암호화 정보를 통신하도록 구성된 암호화 통신을 사용하는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하도록 구성된 송신 단계; 및 상기 사용자 단말로부터 사용자가 입력한 외부 인증 장치에서의 인증 처리에 필요한 인증 정보를 상기 암호화 통신을 사용하여 수신하도록 구성된 수신 단계를 컴퓨터가 실행하도록 하며, 상기 암호화 통신을 사용하지 않는 경우, 사용자가 외부 인증 장치에서의 인증 처리를 선택할 수 있게 하는 정보를 사용자 단말에 송신하는 것이 제한된다.

<31> 본 요약이 본 발명의 모든 양태들을 포함하지 않으며, 청구항에 기술된 바들 및 그 특징들의 결합들이 본 발명에 포함될 수 있음을 유의해야 한다.

<32> 본 발명의 다른 특징들 및 장점들은 첨부 도면과 함께 기술된 이하의 설명으로부터 명백해질 것이며, 도면들에서, 유사한 참조 부호들은 동일하거나 유사한 파트들을 나타낸다.

발명의 구성 및 작용

<33> 본 발명의 실시예들은 이제부터 첨부 도면을 참조하여 상세히 설명될 것이다. 이하의 실시예들은 청구항들에서 기술된 본 발명을 제한하지 않으며 실시예들에서 설명된 특징들의 모든 결합들이 본 발명의 목적들을 달성하기 위한 수단에 반드시 필수적인 것은 아님을 유의해야 한다.

<34> 도면들을 참조하여 이제부터 본 발명의 실시예가 후술될 것이다.

<35> 도 1은 네트워크 시스템의 구성을 도시한 도면이다. 네트워크 시스템을 통해, 정보 처리 장치(101), 사용자 단말(102), 인증 서버(103) 및 인증 서버(104)는 네트워크(100)를 통해 서로 통신할 수 있다. 상기 네트워크는 유선일 수도 무선일 수도 있다.

<36> 인증 서버(103) 및 인증 서버(104)는 사용자명 및 패스워드에 기초하여 인증 처리를 실행하도록 구성된 인증 장치들이다. 정보 처리 장치(101)는 사용자명 및 패스워드 자체에 기초하여 인증 처리를 실행할 수 있으며, 또한, 인증 서버(103) 및 인증 서버(104)에게 인증 처리 실행을 요구할 수 있다. 인증 처리에 필요한 정보가 사용자명 및 패스워드에 제한되는 것은 아님을 유의해야 한다.

<37> 정보 처리 장치(101), 인증 서버(103) 및 인증 서버(104) 각각에 식별 정보로서 이름이 제공된다. 정보 처리 장치(101)의 이름은 "Printer000"이고, 인증 서버(103)의 이름은 "Auth1.domain.net"이며, 인증 서버(104)의 이름은 "Auth2.domain.net"이다.

<38> 도 2는 정보 처리 장치(101) 및 사용자 단말(102)의 하드웨어 구성을 도시한 도면이다. 이제부터, 정보 처리 장치(101)의 일례로서 인쇄 장치가 기술될 것이다. 또한, 정보 처리 장치(101)는 스캐너, 디지털 다기능 장치, 복사기 등일 수도 있다. 정보 처리 장치(101)는 프린터 유닛(201), 중앙 처리 장치(이후, CPU라고 함)(202), RAM(203), 네트워크 인터페이스 유닛(204), I/O 제어 유닛(205), HDD(206) 및 조작 유닛(207)을 포함한다.

<39> CPU(202)는 HDD(206)에 저장된 프로그램을 판독하고, 프로그램을 RAM(203)에 저장한다. 이어서, CPU(202)는

RAM(203)에 저장된 프로그램을 실행하여, 전체 정보 처리 장치(101)의 동작을 제어한다. 프린터 유닛(201)은 인쇄 데이터에 기초하여 용지에 인쇄한다. RAM(203)은 CPU(202)에 의해 실행되는 프로그램을 저장하고, 프로그램 실행에 필요한 다양한 형태의 변수 값들을 저장하며, 인쇄 데이터를 저장한다. 네트워크 인터페이스 유닛(204)은 네트워크(100)를 통해 정보의 송수신을 실행한다. I/O 제어 유닛(205)은 HDD(206)로부터의 정보 판독을 제어하고, HDD(206)로의 정보 기록을 제어한다. HDD(206)는 대용량 기억 장치이며, 프로그램, 인쇄 데이터 및 다양한 형태의 정보를 저장한다. 조작 유닛(207)은 조작 패널 및 조작 키들을 포함한다. 사용자는 조작 패널에 디스플레이된 다양한 형태의 정보를 브라우징하고, 조작 키들을 사용하여 다양한 형태의 정보를 입력한다.

<40> 사용자 단말(102)의 한 일례로서 퍼스널 컴퓨터가 기술될 것이다. 사용자 단말(102)은 워크스테이션, 휴대형 단말 등일 수도 있다. 사용자 단말(102)은 중앙 처리 장치(이후, CPU라고 함)(210), 네트워크 인터페이스 유닛(211), 입출력 포트(212), I/O 제어 유닛(214), HDD(215), RAM(216) 및 비디오 인터페이스 유닛(217)을 포함한다. 또한, 사용자 단말(102)은 입출력 포트를 통해 키보드(213) 및 마우스(219)에 접속되고, 비디오 인터페이스 유닛(217)을 통해 디스플레이(218)에 접속된다.

<41> CPU(210)는 HDD(215)에 저장된 프로그램을 판독하고, 프로그램을 RAM(216)에 저장한다. 이어서, CPU(210)는 RAM(216)에 저장된 프로그램을 실행하여, 전체 사용자 단말(102)의 동작을 제어한다. 네트워크 인터페이스 유닛(211)은 네트워크(100)를 통해 정보의 송수신을 실행한다. 입출력 포트(212)는 키보드(213), 마우스(219) 등과 같은 입력 장치에 접속되고, 입력 장치가 아닌 외부 장치(도시되지 않음)에 접속된다. 입출력 포트(212)는 입력 장치 또는 외부 장치와의 정보 송수신을 실행한다. 사용자는 키보드(213) 또는 마우스(219)를 사용하여 다양한 형태의 정보를 입력한다. I/O 제어 유닛(214)은 HDD(215)로부터의 정보 판독을 제어하고, HDD(215)로의 정보 기록을 제어한다. HDD(215)는 대용량 기억 장치이며, 프로그램 및 다양한 형태의 정보를 저장한다. RAM(216)은 CPU(210)에 의해 실행되는 프로그램을 저장하고, 프로그램 실행에 필요한 다양한 형태의 변수 값들을 저장한다. 비디오 인터페이스 유닛(217)은 디스플레이(218)에 디스플레이될 정보를 디스플레이(218)에 송신한다. 디스플레이(218)는 다양한 형태의 정보를 디스플레이하도록 구성된 디스플레이 장치이고, 사용자는 디스플레이 유닛(218)에 디스플레이된 정보를 브라우징한다.

<42> 인증 서버(103) 및 인증 서버(104)의 하드웨어 구성은 사용자 단말(102)의 하드웨어 구성과 동일하다.

<43> 사용자 단말(102)의 경우, 웹 브라우저(이후, WWW 브라우저라고 함)의 프로그램은 HDD(215)에 저장된다. WWW 브라우저의 프로그램은 판독되어 RAM(216)에 기록되고, 사용자로부터의 명령에 따라 CPU(210)에 의해 실행됨으로써, WWW 브라우저가 활성화된다. 정보 처리 장치(101)의 경우, WWW 서버의 프로그램은 HDD(206)에 저장된다. 정보 처리 장치(101)의 파워가 턴온된 후에, WWW 서버의 프로그램은 판독되어 RAM(203)에 기록되고, CPU(202)에 의해 실행됨으로써, WWW 서버가 활성화된다.

<44> WWW 브라우저는 어드레스, URL(Uniform Resource Locator) 또는 사용자가 지정한 이름에 기초하여 WWW 서버에 접속되고, WWW 서버와의 통신을 개시한다. 이 때에 통신 프로토콜로서 HTTP(Hyper Text Transfer Protocol)가 사용된다. WWW 브라우저는 HTTP를 사용하여 WWW 서버에 액세스하고, WWW 서버로부터의 명령 실행을 요구한다. WWW 서버는 명령을 실행하고, 그 결과를 나타내는 문서 정보를 WWW 브라우저에 송신한다. 이 때에 문서 정보는 HTML(Hyper Text Markup Language) 등으로 기술된다. WWW 브라우저는 문서 정보에 기초하여 화면을 렌더링하고, 그 화면을 디스플레이(218)에 디스플레이한다.

<45> 본 발명에 따른 정보 처리에 관한 설명이 후술될 것이다. 도 3은 정보 처리 장치(101)에 의해 실행되는 정보 처리를 도시한 플로우차트이다. 도 3에 도시된 플로우차트에 기초하여 프로그램이 CPU(202)에 의해 실행되어서, 정보 처리가 실행된다.

<46> 정보 처리 장치(101)는 사용자 단말(102)의 WWW 브라우저로부터 액세스를 수신한다(단계(S301)). 이에 응답해서, 정보 처리 장치(101)는 SSL 설정들(Secure Socket Layer)이 유효한지 무효한지를 판정한다(단계(S302)).

<47> 도 4는 SSL 설정을 인에이블 또는 디스에이블하도록 구성된 관리 화면을 도시한 도면이다. 관리자 권한을 가진 사용자가 WWW 브라우저를 사용하여 정보 처리 장치(101)에 액세스하고, 관리자로서의 인증이 성공할 때, WWW 브라우저는 관리 화면을 디스플레이한다. 또한, 관리 화면은 조작 유닛(207)에 의해 디스플레이될 수도 있다.

<48> 도 4에서, 옵션 스위치(401)는 SSL 설정들을 인에이블 또는 디스에이블하도록 구성된다. SSL 설정들이 유효한 경우, SSL에 기초하여 암호화 통신이 사용될 수 있으며, SSL 설정들이 무효한 경우, SSL에 기초하여 암호화 통신이 사용될 수 없다. SSL은 암호 기술을 사용하여 WWW 브라우저와 WWW 서버 간의 HTTP에 의한 통신을 보호하기 위해 사용되는 프로토콜이다. SSL을 사용하는 암호화 통신을 실행하기 위해, SSL 설정들은 WWW 서버(정보

처리 장치(101))에서 유효할 필요가 있으며, WWW 브라우저는 SSL에 의한 암호화 통신을 실행할 필요가 있다. 정보 처리 장치(101)의 초기 값들에 있어서, SSL 설정들은 무효로 설정된다.

<49> 정보 처리 장치(101) 자체는 자신의 사용자 인증 방법을 지원함으로써, 정보 처리 장치(101)에서의 인증 처리에 필요한 패스워드가 보호되므로, SSL에 의한 암호화 통신이 반드시 요구되는 것은 아니다. 따라서, SSL 설정들은 무효로 설정될 수도 있다.

<50> 옵션 스위치(402)는, SSL 설정이 유효한 경우 인증 서버에서의 인증 처리를 허용하거나, SSL 설정이 유효한 경우에도 인증 서버에서의 인증 처리를 금지하도록 구성된 스위치이다.

<51> 통상의 환경에서는, SSL을 사용하는 암호화 통신의 경우, 송수신되는 정보는 암호화되며, 안전성이 보장된다. 즉, 인증 서버에서의 인증 처리에 필요한 패스워드가 사용자 단말(102)로부터 정보 처리 장치(101)에 송신되는 경우에도, SSL 설정들이 유효한 한, 패스워드의 안전성이 보장되며, 패스워드는 도청으로부터 보호된다. 그러나, 인증 서버에서의 인증 처리에 사용되는 인증 정보가 보다 엄격하게 관리되는 환경에서는, 인증 정보 자체는 네트워크를 통해 송신되는 것이 방지되며, 따라서, 인증 처리가 인증 서버에서 실행되는 것이 바람직하지 않은 경우가 존재한다. 옵션 스위치(402)는 이러한 경우를 위해 제공된다.

<52> 필드(403)는 관리자가 인증 서버를 등록할 수 있도록 구성된다. 관리자는 인증 서버의 명칭을 입력해서, 복수의 인증 서버들을 등록할 수 있다. 도 4에 도시된 일례의 경우, 인증 서버(103) 및 인증 서버(104)가 등록된다.

<53> 도 4에 도시된 일례에서는 인증 서버의 명칭이 입력되어 있지만, 인증 서버를 식별하도록 구성된 다른 식별 정보가 입력될 수도 있다. 예를 들어, 네트워크가 도메인이라고 하는 인크리먼트로 관리되는 환경에서, 인증 서버는 각각의 도메인을 위해 존재한다. 따라서, 각 도메인의 명칭(이후, 도메인명이라 함)이 인증 서버를 식별하도록 구성된 인증 정보로서 사용될 수도 있다.

<54> 또한, 사용자가 인증 서버의 명칭을 입력할 뿐만 아니라 관리 서버로부터 인증 서버들의 리스트를 나타내는 정보를 자동으로 획득하도록 구성될 수도 있는데, 여기서 관리 서버로 그 리스트에 포함된 인증 서버의 명칭을 등록하기 위해 네트워크 상에 존재한다. 예를 들어, 네트워크에 존재하는 장치들의 명칭들로부터 장치의 IP 어드레스를 탐색하도록 구성된 DNS 서버는 SRV 레코드들로서 복수의 인증 서버들의 명칭들을 저장한다. 정보 처리 장치(101)는 DNS 서버의 서비스 (SRV) 레코드들로부터 복수의 인증 서버들의 명칭들을 자동으로 획득하고, 필드(403)에 디스플레이한다.

<55> 단계(S302)에서 SSL 설정들이 무효하다고 판정되면, SSL을 사용하지 않고 통신이 계속된다. 정보 처리 장치(101)는 로그인 목적지로서 정보 처리 장치(101)만을 열거하며, 로그인 화면을 나타내는 문서 정보를 생성한다(단계(S303)). 이어서, 정보 처리 장치(101)는 로그인 화면을 나타내는 문서 정보를 사용자 단말(102)에 송신한다(단계(S304)).

<56> SSL 설정들이 무효한 경우, 정보 처리 장치(101)에서의 인증 처리만이 허용된다. 인증 서버에서의 인증 처리에 있어서, 정보 처리 장치(101)는 사용자 단말(102)을 대리하고, 인증 서버에게 인증 처리를 실행할 것을 요구한다. 따라서, 정보 처리 장치(101)는 사용자가 입력한 패스워드 자체를 필요로 하며, 사용자 단말(102)로부터 사용자가 입력한 패스워드 자체를 정보 처리 장치(101)에 송신할 필요가 있다. SSL을 사용하는 암호화 통신이 실행되는 경우, 패스워드는 암호화되어, 패스워드가 도청으로부터 보호되지만, SSL을 사용하는 암호화 통신이 실행되지 않는 경우, 패스워드는 쉽게 도청될 수 있다. 따라서, SSL 설정들이 무효한 경우, 인증 서버에서의 인증 처리는 실행되지 않도록 구성된다.

<57> 한편, 정보 처리 장치(101)에서의 인증 처리의 경우, 사용자가 입력한 패스워드 자체는 이하의 방법에 따라 송신되지 않는다.

<58> 도 5는 단계(S304)에서 송신된 문서 정보에 기초하여 WWW 브라우저에 의해 디스플레이되는 로그인 화면을 도시한 도면이다. 입력 영역(501)은 사용자명을 입력하도록 구성되고, 입력 영역(502)은 패스워드를 입력하도록 구성된다. 풀다운 메뉴(503)는 로그인 목적지를 선택하도록 구성된다. 사용자명 및 패스워드에 기초하여 인증 처리는 로그인 목적지에서 실행된다. 도 5에 도시된 로그인 화면의 경우, 정보 처리 장치(101)만이 로그인 목적지로서 선택될 수 있다.

<59> 사용자가 사용자명, 패스워드를 입력하고, 로그인 목적지를 선택하며, OK 버튼을 누를 때, 사용자 단말(102)은 인증 처리 실행 요구 명령(인증 요구 명령)을 정보 처리 장치(101)에 송신한다.

<60> 정보 처리 장치(101)에서의 인증 처리에 있어서, 사용자가 입력한 패스워드 자체를 정보 처리 장치(101)에 송신할 필요는 없다. WWW 브라우저는 단방향 속성을 갖는 특정 함수(예를 들어, 해시 함수)를 사용하여 사용자가 입력한 패스워드가 처리되게 한다. 특정 함수에 의해 생성된 값은 고유 패스워드로 역으로 변환될 수는 없다.

<61> 인증 요구 명령은 사용자가 입력한 사용자명, 특정 함수에 의해 생성된 값(이후, 제2 패스워드라고 함) 및 사용자가 선택된 로그인 목적지를 나타낸다.

<62> 정보 처리 장치(101)는 사용자 단말(102)로부터 인증 요구 명령을 수신한다(단계(S305)). 수신된 인증 요구 명령이 나타내는 로그인 목적지는 항상 정보 처리 장치(101)이다. 따라서, 정보 처리 장치(101)의 인증 처리가 실행된다(단계(S306a)).

<63> 도 6은 정보 처리 장치(101)에 의해 실행되는 인증 처리를 도시한 플로우차트이다. 도 6에 도시된 플로우차트에 기초하여 하는 프로그램은 CPU(202)에 의해 실행되어서, 인증 처리가 실행된다.

<64> 정보 처리 장치(101)의 HDD(206)는 사용자 데이터베이스(이후, 사용자 DB라고 함)를 보유한다. 사용자 DB는 정보 처리 장치(101) 로그인이 허용된 사용자를 위한 사용자명과 패스워드로 된 적어도 하나의 집합을 저장한다.

<65> 정보 처리 장치(101)는 사용자 DB로부터 인증 요구 명령이 나타내는 사용자명을 탐색한다(단계(S601)). 이어서, 정보 처리 장치(101)는 탐색 결과에 기초하여 인증 요구 명령이 나타내는 사용자명이 사용자 DB 내에 존재하는지를 판정한다(단계(S602)).

<66> 인증 요구 명령이 나타내는 사용자명이 사용자 DB 내에 존재하지 않는 경우, 정보 처리 장치(101)는 인증 실패를 나타내는 문서 정보를 사용자 단말(102)에 송신한다(단계(S603)). WWW 브라우저는 문서 정보에 기초하여 인증이 실패했다고 디스플레이(218)에 디스플레이한다.

<67> 한편, 인증 요구 명령이 나타내는 사용자명이 사용자 DB 내에 존재하는 경우, 정보 처리 장치(101)는 인증 요구 명령이 나타내는 제2 패스워드를 사용자 DB 내의 패스워드와 매칭(matching)하고, 그들이 일치하는지를 판정한다(단계(S604)). 단계(S604)에서, 정보 처리 장치(101)는 먼저 사용자 DB 내에서 발견된 패스워드를 상술된 특정 기능을 사용하여 처리하여 제2 패스워드를 생성한다. 이어서, 정보 처리 장치(101)는 인증 요구 명령이 나타내는 제2 패스워드가 사용자 DB 내의 패스워드로부터 생성된 제2 패스워드와 동일한지를 판정한다.

<68> 두개의 제2 패스워드들이 일치하지 않을 때, 정보 처리 장치(101)는 인증이 실패했다는 문서 정보를 사용자 단말(102)에 송신한다(단계(S603)). 두개의 제2 패스워드들이 일치할 때, 정보 처리 장치(101)는 인증이 성공한 경우에만 송신되는 문서 정보를 사용자 단말(102)에 송신한다(단계(S605)). 예를 들어, 도 5에 도시된 로그인 화면을 나타내는 문서 정보, 사용자가 정보 처리 장치(101)에서의 인쇄 처리를 할 수 있도록 구성된 오퍼레이팅 화면을 나타내는 문서 정보 등이 단계(S605)에서 송신된다.

<69> 상술된 사용자명 및 패스워드에 기초한 인증 방법은 단지 한 일례이며, 다른 방법으로 인증이 실행될 수도 있음은 물론이다.

<70> 도 3의 단계(S302)에서 SSL 설정이 유효하다고 판정되면, 정보 처리 장치(101)는 사용자 단말(102)에게 SSL에 의한 액세스를 방향 전환(redirect)하라는 명령을 송신하여, SSL에 의한 암호화 통신을 실행한다(단계(S306b)). 방향 전환 명령에 따라, WWW 브라우저는 WWW 서버 액세스를 위해 사용되는 포트를 HTTP 통신을 위해 일반적으로 사용되는 포트로부터 SSL에 의해 보호되는 HTTP 통신용 포트로 스위칭한다. 일반적으로 HTTP 통신을 위해 사용되는 포트의 일례는 Port 80이고, SSL에 의해 보호되는 HTTP 통신용 포트는 Port 443이다. 이어서, WWW 브라우저는 다시 SSL을 사용하여 Port 443에 액세스한다.

<71> 정보 처리 장치(101)는 사용자 단말(102)의 WWW 브라우저로부터 액세스(Port 443 액세스)를 수신한다(단계(S307)). 단계(S307)에서의 통신에서는 SSL이 사용된다.

<72> 다음으로, 정보 처리 장치(101)는 인증 서버에서의 인증 처리가 허용되는지 금지되는지를 판정한다(단계(S308)). 인증 서버에서의 인증 처리 허용 또는 금지는 관리 화면의 옵션 스위치(402)에 의해 설정된다.

<73> SSL 설정이 유효한 경우에라도, 인증 서버에서의 인증 처리가 금지될 때, 정보 처리 장치(101)는 단계(S303)로 진행한다. 이러한 경우, 정보 처리 장치(101)에서의 인증 처리만이 실행된다.

<74> 인증 서버에서의 인증 처리가 허용되는 경우, 정보 처리 장치(101)는 등록된 인증 서버가 존재하는지를 판정한다(단계(S309)). 등록된 인증 서버가 없을 때, 정보 처리 장치(101)는 단계(S303)로 진행한다.

<75> 등록된 인증 서버가 존재하면, 정보 처리 장치(101)는 정보 처리 장치(101) 뿐만 아니라 로그인 목적지로서 등록된 인증 서버들을 열거하고, 로그인 화면을 나타내는 문서 정보를 생성한다(단계(S310)). 이어서, 정보 처리 장치(101)는 로그인 화면을 나타내는 문서 정보를 사용자 단말(102)에 송신한다(단계(S311)).

<76> 도 7은 단계(S311)에서 송신된 문서 정보에 기초하여 WWW 브라우저에 의해 디스플레이되는 로그인 화면을 도시한 도면이다. 입력 영역(701)은 사용자명을 입력하도록 구성되고, 입력 영역(702)은 패스워드를 입력하도록 구성된다. 풀다운 메뉴(703)는 로그인 목적지를 선택하도록 구성된다. 도 7에 도시된 로그인 화면의 경우, 정보 처리 장치(101) 뿐만 아니라 인증 서버(103) 및 인증 서버(104)도 로그인 목적지로서 선택될 수 있다.

<77> 사용자가 사용자명, 패스워드를 입력하고, 로그인 목적지를 선택하여, OK 버튼을 누를 때, 사용자 단말(102)은 인증 요구 명령을 정보 처리 장치(101)에 송신한다.

<78> 사용자가 로그인 목적지로서 정보 처리 장치(101)를 선택하는 경우, 인증 요구 명령은 사용자가 입력한 사용자명, 사용자가 입력한 패스워드로부터 생성된 제2 패스워드 및 사용자가 선택한 로그인 목적지를 나타낸다. 사용자가 로그인 목적지로서 인증 서버를 선택하는 경우, 인증 요구 명령은 사용자가 입력한 사용자명, 사용자가 입력한 패스워드 및 사용자가 선택한 로그인 목적지를 나타낸다.

<79> 정보 처리 장치(101)는 사용자 단말(102)로부터 인증 요구 명령을 수신한다(단계(S312)). 이어서, 정보 처리 장치(101)는 인증 요구 명령이 나타내는 로그인 목적지가 정보 처리 장치(101)인지 인증 서버인지를 판정한다(단계(S313)). 로그인 목적지가 정보 처리 장치(101)인 경우, 정보 처리 장치(101)는 단계(S306a)로 진행한다. 이 경우, 정보 처리 장치(101)에서의 인증 처리가 실행된다. 로그인 목적지가 인증 서버인 경우, 인증 서버에서의 인증 처리가 실행된다(단계(S314)).

<80> 도 8은 인증 서버에게 인증 처리를 실행할 것을 요구하도록 구성된 정보 처리를 도시한 플로우차트이다. CPU(202)는 도 8에 도시된 플로우차트에 기초하여 프로그램을 실행하여, 상기 정보 처리가 실행된다.

<81> 정보 처리 장치(101)는 사용자 단말(102)로부터 수신된 인증 요구 명령이 나타내는 사용자명 및 패스워드에 기초하여 로그인 목적지로서 선택된 인증 서버에 소정의 프로토콜을 사용하여 인증 처리 실행을 요구한다(단계(S801)). 소정의 프로토콜은 로그인 목적지로서 선택된 인증 서버에 의해 지원되는 프로토콜이다. 예를 들어, NTLM, 케르베로스(Kerberos) 등과 같은 유용한 프로토콜들이 있다. 상기 프로토콜들의 경우, 사용자명 및 패스워드는 정보 처리 장치(101)로부터 인증 서버로 송신되지 않으며, 일련의 안전한 절차에 따라 인증 처리가 실행된다.

<82> 인증 서버에 의한 인증 처리 실행에 이어, 정보 처리 장치(101)는 인증 서버로부터 인증 결과들을 수신한다(단계(S802)). 이어서, 정보 처리 장치(101)는 수신된 인증 결과들에 기초하여 인증이 성공했는지를 판정한다(단계(S803)).

<83> 인증이 실패했다고 판정되면, 정보 처리 장치(101)는 인증이 실패했다는 문서 정보를 사용자 단말(102)에 송신한다(단계(S804)). WWW 브라우저는 문서 정보에 기초하여 인증이 실패했다고 디스플레이(218)에 디스플레이한다.

<84> 인증이 성공했다고 판정되면, 정보 처리 장치(101)는 인증이 성공한 경우에만 송신되는 문서 정보를 사용자 단말(102)에 송신한다(단계(S805)).

<85> <다른 실시예들>

<86> 본 발명의 실시예에 관해 상세히 설명되었지만, 본 발명이 상술된 실시예에 제한되는 것은 아님을 이해해야 한다. 예를 들어, 본 발명은 복수의 장치들로 구성된 시스템에 적용될 수 있으며, 또는 단일 디바이스로 구성된 장치에 적용될 수도 있다.

<87> 본 발명이 시스템 또는 장치에 상술된 실시예의 기능들을 실현하도록 구성된 소프트웨어 프로그램을 직접 지원하거나 또는 원격으로 지원함으로써 달성될 수 있으며, 시스템 또는 장치가 제공된 프로그램을 판독 및 실행함을 유의해야 한다. 이러한 경우, 그 형태는 프로그램에 제한되는 것이 아니며, 프로그램의 기능들을 갖는 한 가능하다.

<88> 따라서, 컴퓨터를 사용하여 본 발명의 기능 처리를 구현하기 위해, 컴퓨터에 설치되는 프로그램 코드 자체도 본 발명을 구현한다. 즉, 본 발명의 범위는 본 발명의 기능 처리를 구현하는 컴퓨터 프로그램 자체도 포함한다. 이러한 경우, 객체 코드, 인터프리터에 의해 실행되는 프로그램, 운영 체제(OS)에 제공되는 스크립트 데이터 등

과 같은 임의의 프로그램 형태가 프로그램의 기능들을 포함하는 한 사용될 수도 있다.

<89> 프로그램을 제공하도록 구성된 기록 매체에 있어서, 다양한 형태들이 사용될 수도 있다. 예를 들어, 플로피 디스크, 하드 디스크, 광 디스크, 광자기 디스크, MO, CD-ROM, CD-R, CD-RW, 자기 테이프, 비휘발성 메모리 카드, ROM, DVD(DVD-ROM, DVD-R) 등이 유용하다.

<90> 또한, 프로그램을 지원하도록 구성된 방법에 있어서, 프로그램이 클라이언트 컴퓨터의 브라우저를 사용하여 인터넷의 홈페이지에 액세스하고, 홈페이지로부터 프로그램을 하드 디스크 등과 같은 기록 매체에 다운로드함으로써 제공될 수 있다. 이러한 경우, 본 발명에 따른 컴퓨터 프로그램 자체 또는 자동 설치 기능을 포함하는 압축 파일이 다운로드될 수도 있다.

<91> 또한, 본 발명의 프로그램을 구성하는 프로그램 코드가 복수의 파일들로 분할될 수도 있으며, 각각의 파일이 상이한 홈페이지로부터 다운로드되어서, 프로그램이 제공될 수 있다. 다시 말해서, 복수의 사용자들이 컴퓨터에서 본 발명의 기능 처리를 구현하도록 구성된 프로그램 파일을 다운로드할 수 있도록 구성된 WWW 서버가 본 발명의 범위 내에 포함된다.

<92> 또한, 본 발명에 따른 프로그램이 암호화되어, CD-ROM 등과 같은 기록 매체에 저장되어 사용자들에게 분배되는 구성이 사용될 수도 있다. 이러한 경우, 소정의 조건들을 만족시키는 사용자가 인터넷을 통해 홈페이지로부터 암호를 해독하도록 구성된 키 정보를 다운로드할 수 있으며, 키 정보를 사용하여 암호 프로그램을 실행 가능 형태로 설치할 수 있다.

<93> 또한, 상술된 실시예의 기능들은 판독된 프로그램을 실행하는 컴퓨터에 의해 상술된 구성외의 구성으로 구현될 수 있다. 예를 들어, 컴퓨터를 운영하는 운영 체제 등이 프로그램의 명령에 기초하여 실제 프로세싱 전부 혹은 일부를 실행할 수도 있으며, 상술된 실시예의 기능들이 프로세싱에 의해 구현된다.

<94> 또한, 기록 매체로부터 판독된 프로그램이 컴퓨터에 삽입된 기능 확장 보드 또는 컴퓨터에 접속된 기능 확장 유닛에 포함된 메모리에 기록되는 구성이 이루어질 수도 있다. 이러한 경우, 기능 확장 보드 또는 기능 확장 유닛에 포함된 CPU 등은 프로그램 명령에 기초하여 실제 프로세싱 전부 혹은 일부를 실행하며, 상술된 실시예의 기능들이 프로세싱에 의해 구현된다.

<95> 본 발명에 따라, 암호화 정보를 통신하도록 구성된 암호화 통신이 사용되지 않는 경우, 외부 인증 장치에서의 인증 처리를 사용자가 선택하는 것이 방지될 수 있다.

<96> 또한, 암호화 통신이 사용되지 않는 경우, 사용자는 정보 처리 장치에서의 인증 처리를 선택할 수 있어서, 인증 서버에서의 인증 처리에 필요한 인증 정보가 사용자 단말로부터 정보 처리 장치에 송신되는 것이 방지될 수 있다.

<97> 본 발명이 일례의 실시예들을 참조하여 기술되었지만, 본 발명이 기술된 실시예들에 제한되는 것이 아님을 이해해야 한다. 이하의 청구범위는 모든 변경들, 등가 구조들 및 기능들을 포함하도록 가장 넓은 범위로 해석되어야 한다.

발명의 효과

<98> 외부 인증 장치에서 인증 처리에 필요한 인증 정보가 암호 없이 사용자 단말로부터 정보 처리 장치에 송신되는 것을 방지할 수 있다.

도면의 간단한 설명

<1> 도 1은 네트워크 시스템의 구성을 도시한 도면.

<2> 도 2는 정보 처리 장치(101) 및 사용자 단말(102)의 하드웨어 구성을 도시한 도면.

<3> 도 3은 정보 처리 장치(101)에 의해 실행되는 정보 처리를 도시한 플로우차트.

<4> 도 4는 SSL 설정을 인에이블 또는 디스에이블하도록 구성된 관리 화면을 도시한 도면.

<5> 도 5는 WWW 브라우저에 의해 디스플레이되는 로그인 화면을 도시한 도면.

<6> 도 6은 정보 처리 장치(101)에 의해 실행되는 인증 처리를 도시한 플로우차트.

<7> 도 7은 WWW 브라우저에 의해 디스플레이되는 로그인 화면을 도시한 도면.

<8> 도 8은 인증 서버에게 인증 처리를 실행할 것을 요구하도록 구성된 정보 처리를 도시한 플로우차트.

<9> <도면의 주요 부분에 대한 부호의 설명>

<10> 101 : 정보 처리 장치

<11> 102 : 사용자 단말

<12> 103, 104 : 인증 서버

<13> 202, 210 : CPU

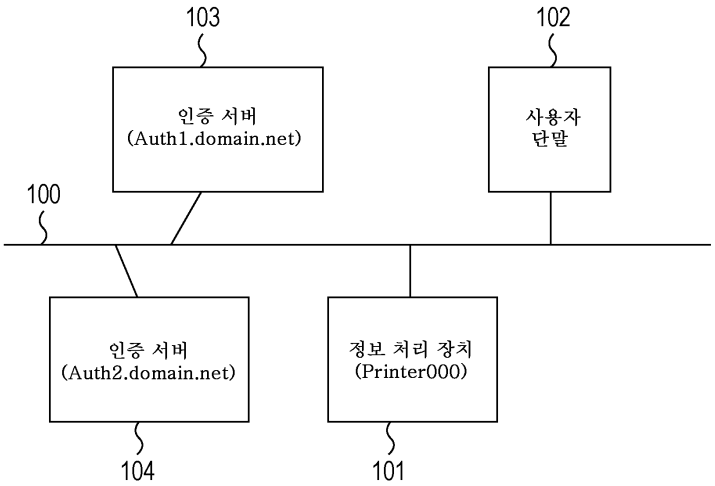
<14> 203, 216 : RAM

<15> 206, 215 : HDD

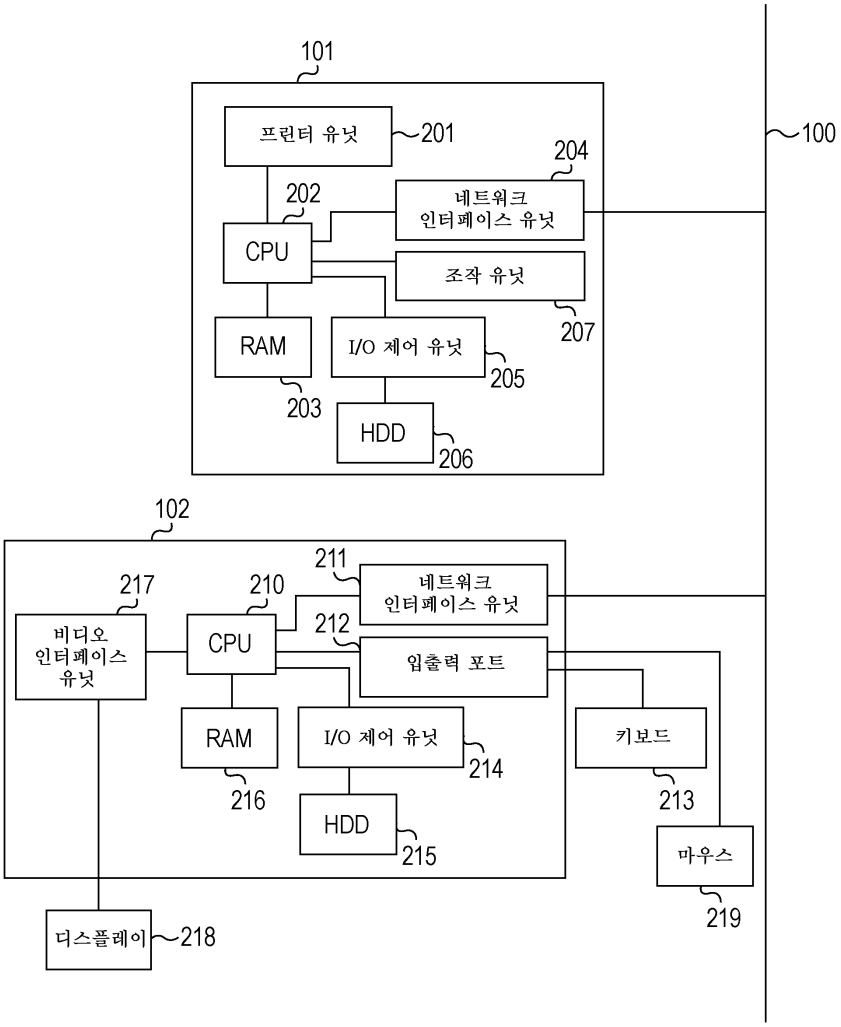
<16> 218 : 디스플레이

도면

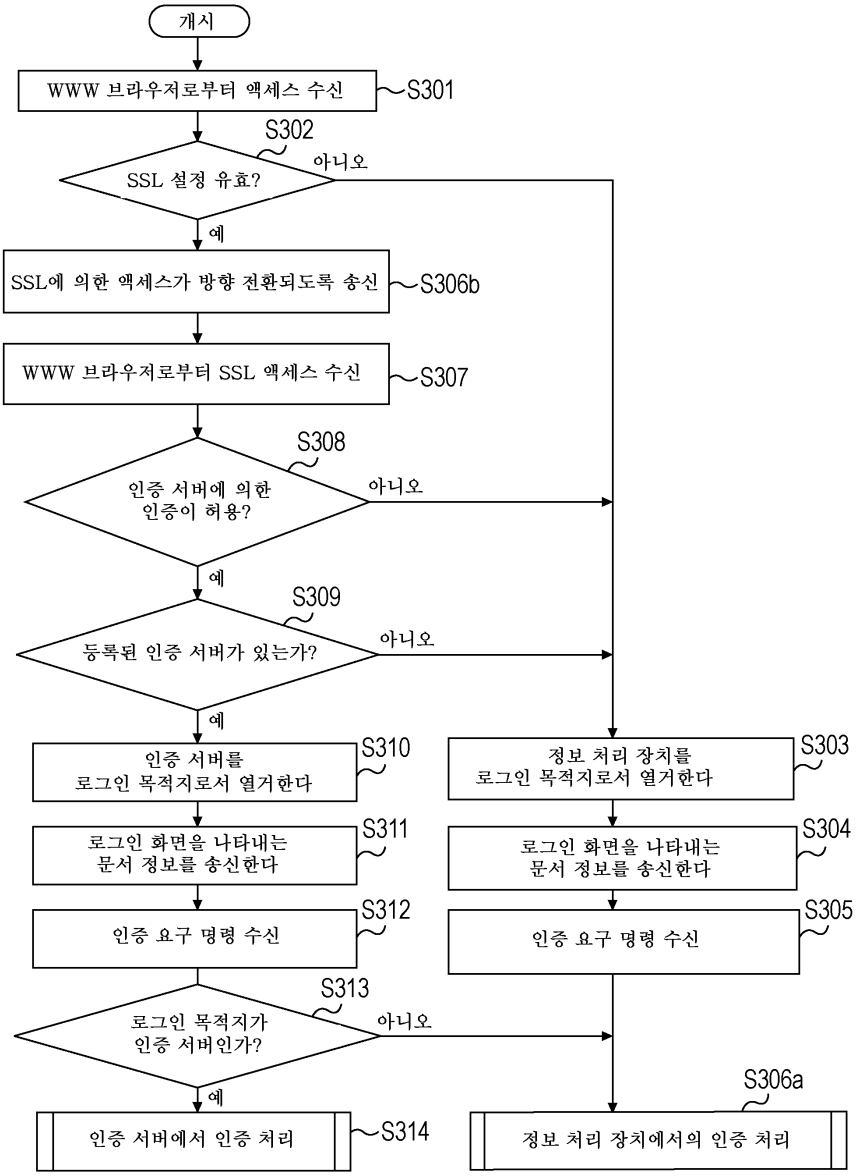
도면1



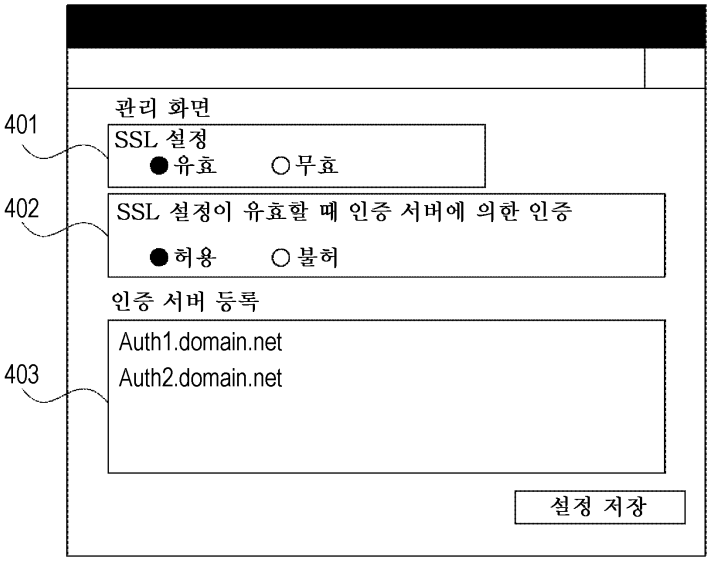
도면2


101
프린터 유닛
201
204
네트워크
인터페이스 유닛
202
CPU
조작 유닛
207
RAM
I/O 제어 유닛
205
203
HDD
206
100
102
211
네트워크
인터페이스 유닛
217
210
212
비디오
인터페이스
유닛
CPU
입출력 포트
RAM
I/O 제어 유닛
214
키보드
216
213
HDD
215
마우스
219
디스플레이
218

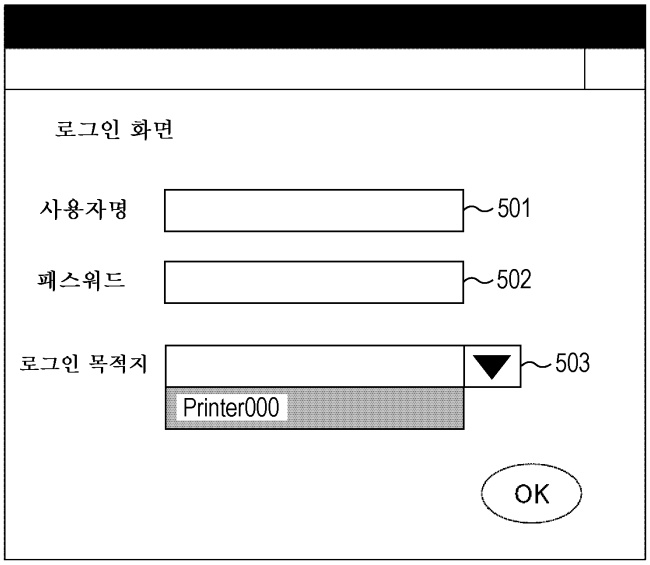
도면3


개시
WWW 브라우저로부터 액세스 수신
S301
S302
SSL 설정 유효?
아니오
예
SSL에 의한 액세스가 방향 전환되도록 송신
S306b
WWW 브라우저로부터 SSL 액세스 수신
S307
S308
인증 서버에 의한 인증이 허용?
아니오
예
S309
등록된 인증 서버가 있는가?
아니오
예
인증 서버를 로그인 목적지로서 열거한다
S310
로그인 화면을 나타내는 문서 정보를 송신한다
S311
인증 요구 명령 수신
S312
S313
로그인 목적지가 인증 서버인가?
아니오
예
인증 서버에서 인증 처리
S314
정보 처리 장치를 로그인 목적지로서 열거한다
S303
로그인 화면을 나타내는 문서 정보를 송신한다
S304
인증 요구 명령 수신
S305
S306a
정보 처리 장치에서의 인증 처리

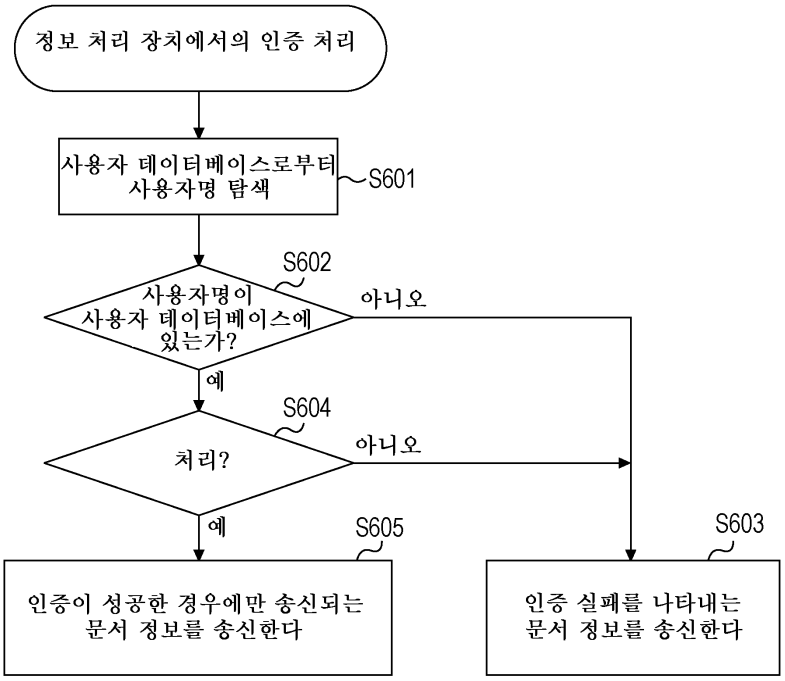
도면4


관리 화면
401
SSL 설정
●유효 ○무효
402
SSL 설정이 유효할 때 인증 서버에 의한 인증
●허용 ○불허
인증 서버 등록
403
Auth1.domain.net
Auth2.domain.net
설정 저장

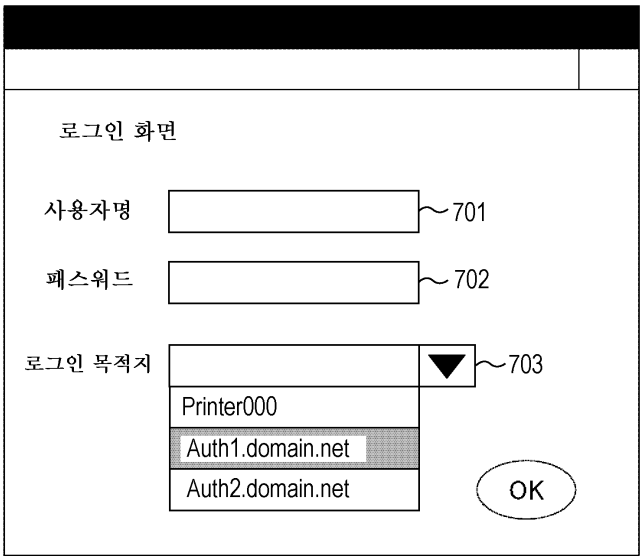
도면5


로그인 화면
사용자명
501
패스워드
502
로그인 목적지
503
Printer000
OK

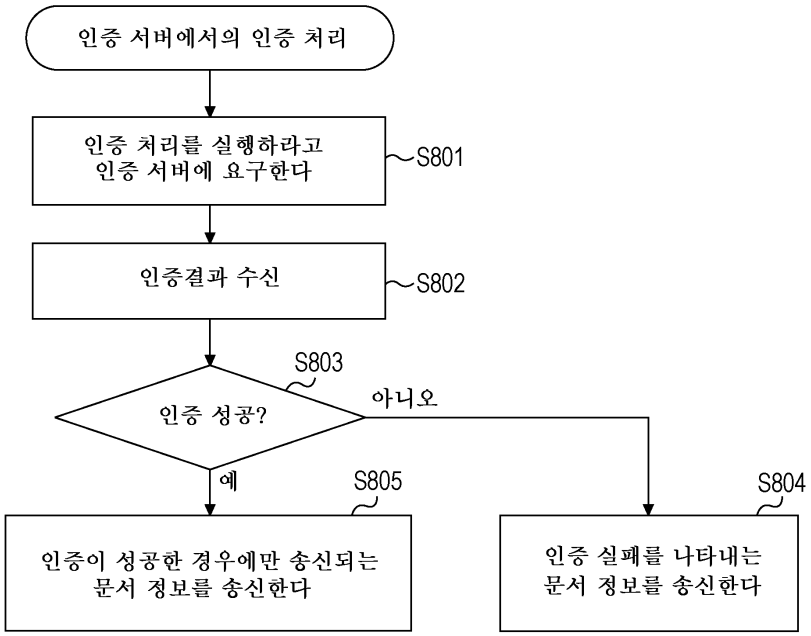
도면6


정보 처리 장치에서의 인증 처리
사용자 데이터베이스로부터 사용자명 탐색
S601
S602
사용자명이 사용자 데이터베이스에 있는가?
아니오
예
S604
처리?
아니오
예
S605
S603
인증이 성공한 경우에만 송신되는 문서 정보를 송신한다
인증 실패를 나타내는 문서 정보를 송신한다

도면7


로그인 화면
사용자명
701
패스워드
702
로그인 목적지
703
Printer000
Auth1.domain.net
Auth2.domain.net
OK

도면8


인증 서버에서의 인증 처리
인증 처리를 실행하라고
인증 서버에 요구한다
S801
인증결과 수신
S802
S803
인증 성공?
아니오
예
S805
인증이 성공한 경우에만 송신되는
문서 정보를 송신한다
S804
인증 실패를 나타내는
문서 정보를 송신한다