(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년12월06일
(11) 등록번호 10-1804966
(24) 등록일자 2017년11월29일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 21/31* (2013.01)
G06F 21/60 (2013.01) *H04N 1/44* (2006.01)
(21) 출원번호 10-2014-0112133
(22) 출원일자 2014년08월27일
심사청구일자 2015년08월27일
(65) 공개번호 10-2015-0026900
(43) 공개일자 2015년03월11일
(30) 우선권주장
JP-P-2013-181564 2013년09월02일 일본(JP)
(56) 선행기술조사문헌
KR1020050119751 A*
KR1020030081878 A*
KR100739245 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
캐논 가부시끼가이샤
일본 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고
(72) 발명자
호소다 야스히로
일본국 도쿄도 오오따꾸 시모마루꼬 3쪼메 30방 2고 캐논 가부시끼가이샤 나이
(74) 대리인
권태복

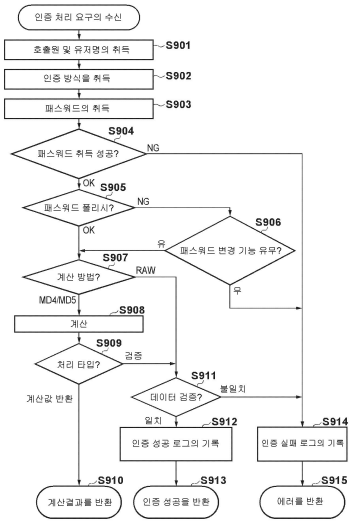
전체 청구항 수 : 총 17 항 심사관 : 양종필

(54) 발명의 명칭 **정보처리장치 및 그 제어방법**

(57) 요 약

복수의 프로토콜 중의 한 프로토콜에 따라 인증 요구를 수신할 수 있는 정보처리장치와 그 제어방법이 제공된다. 정보처리장치는, 각 유저에 대한 패스워드 및 유저 식별자와 각 프로토콜에 대한 계산 방법을 저장하고, 이 장치가 상기 복수의 프로토콜 중의 한 프로토콜에 따라 리모트 컴퓨터로부터 인증 데이터를 포함하는 인증 요구를 수신한 경우에, 이 장치는 상기 인증 요구에 포함되어 있는 인증 데이터에 대응하는 저장된 패스워드를 취득하고, 상기 프로토콜에 대응하는 저장된 계산 방법을 취득하며, 상기 취득한 계산 방법에 따라 취득한 패스워드를 해쉬로 변환하고, 상기 해쉬로 상기 인증 데이터를 검증한다.

대 표 도 - 도9



명 세 서

청구범위

청구항 1

정보처리장치로서,

복수의 서버들에 대한 인증 처리 방법을 상기 정보처리장치에 저장하도록 구성된 인증 정보 저장 유닛과,

상이한 종류의 서버들을 제공하도록 구성된 제공 유닛과,

유저 식별자와 관련된 적어도 하나의 패스워드를 저장하도록 구성된 유저 정보 저장 유닛과,

상기 서버들 중 하나에 대한 유저의 인증 처리 요구를 수신하도록 구성된 수신 유닛과,

상기 인증 정보 저장 유닛으로부터, 인증 처리가 요구된 상기 서버에 대한 인증 처리 방법을 취득하고, 상기 유저 정보 저장 유닛에 저장되고 상기 요구에 포함된 유저 식별자와 관련된 패스워드를 취득하도록 구성된 취득 유닛과,

상기 취득된 패스워드를 이용하여, 상기 서버에 대한 상기 취득된 인증 처리 방법에 따라 상기 인증 처리를 행하는 제어 유닛을 구비하고,

상기 상이한 종류의 서버들의 각각은, 다른 서버들과는 상이한 통신 프로토콜을 사용하여 상기 다른 서버들과 상이한 애플리케이션과 통신하며,

상기 수신 유닛이 상기 복수의 서버들 중 제 1 서버로부터 상기 요구를 수신한 경우, 상기 제어 유닛은 상기 제 1 서버에 인증 처리의 결과를 응답하기 위하여 패스워드 폴리시를 확인하고,

상기 수신 유닛이 상기 복수의 서버들 중 제 2 서버로부터 상기 요구를 수신한 경우, 상기 제어 유닛은 패스워드 폴리시를 확인하고, 상기 제 2 서버가 인증 처리를 수행하는 데 필요한 인증 데이터를 생성하며, 상기 인증 데이터를 상기 제 2 서버에 응답하는, 정보처리장치.

청구항 2

제 1 항에 있어서,

상기 제어 유닛은, 상기 인증 처리의 결과에 의거해서, 상기 정보처리장치에 유저가 로그 인하는 것을 허용하도록 구성된, 정보처리장치.

청구항 3

제 1 항에 있어서,

상기 통신 프로토콜은, HTTP, SMB, 및 SNMP 중의 어느 하나인, 정보처리장치.

청구항 4

제 1 항에 있어서,

상기 통신 프로토콜이, 상기 제어 유닛에 의한 상기 인증 처리를 실행할 수 없는 프로토콜인 경우, 인증 유닛에 변환된 패스워드를 전송하도록 구성된 전송 유닛을 더 구비하고,

상기 변환된 패스워드는, 상기 취득된 인증처리 방법에 따라 상기 취득된 패스워드를 변환함으로써 획득되는, 정보처리장치.

청구항 5

제 1 항에 있어서,

상기 유저 정보 저장 유닛으로부터 패스워드를 취득할 수 없는 경우에 인증 에러를 리모트 컴퓨터에 통지하도록 구성된 통지 유닛을 더 구비하는, 정보처리장치.

청구항 6

제 1 항에 있어서,

상기 취득된 패스워드의 유효기한이 만료된 경우, 인증 에러를 리모트 컴퓨터에 통지하도록 구성된 통지 유닛을 더 구비하는, 정보처리장치.

청구항 7

제 1 항 내지 제 6 항 중 어느 한 항에 있어서,

유저로부터 인증 데이터를 수신하도록 구성된 조작 유닛을 더 구비하고,

상기 제어 유닛은, 상기 유저 정보 저장 유닛으로부터, 상기 조작 유닛이 수신한 상기 인증 데이터에 대응하는 패스워드를 취득하고, 상기 취득한 패스워드를 해쉬로 변환하지 않고, 상기 취득한 패스워드로 상기 인증 데이터를 검증하도록 구성되는, 정보처리장치.

청구항 8

제 1 항에 있어서,

상기 제어 유닛의 인증의 결과를 기록하도록 구성된 로그 기록 유닛을 더 구비하는, 정보처리장치.

청구항 9

복수의 서버들에 대한 인증 처리 방법을 정보처리장치에 저장하는 인증 정보 저장 유닛과, 상이한 종류의 서버들을 갖고, 상기 상이한 종류의 서버들의 각각은, 다른 서버들과는 상이한 통신 프로토콜을 사용하여 상기 다른 서버들과 상이한 애플리케이션과 통신하는, 정보처리장치의 제어방법으로서,

유저 식별자와 관련된 적어도 하나의 패스워드를 유저 정보 저장 유닛에 저장하는 저장 단계와,

상기 서버들 중 하나에 대한 유저의 인증 처리 요구를 수신하는 수신 단계와,

상기 인증 정보 저장 유닛으로부터, 인증 처리가 요구된 상기 서버에 대한 인증 처리 방법을 취득하고, 상기 유저 정보 저장 유닛에 저장되고 상기 요구에 포함된 유저 식별자와 관련된 패스워드를 취득하는 단계와,

상기 취득된 패스워드를 이용하여, 상기 서버에 대한 상기 취득된 인증 처리 방법에 따라 상기 인증 처리를 행하는 제어 단계를 포함하고,

상기 수신 단계에서, 상기 복수의 서버들 중 제 1 서버로부터 상기 요구를 수신한 경우, 상기 제어 단계에서는 상기 제 1 서버에 인증 처리의 결과를 응답하기 위하여 패스워드 폴리시를 확인하고,

상기 수신 단계에서, 상기 복수의 서버들 중 제 2 서버로부터 상기 요구를 수신한 경우, 상기 제어 단계에서는 패스워드 폴리시를 확인하고, 상기 제 2 서버가 인증 처리를 수행하는 데 필요한 인증 데이터를 생성하며, 상기 인증 데이터를 상기 제 2 서버에 응답하는, 정보처리장치의 제어방법.

청구항 10

제 1 항에 있어서,

상기 상이한 종류의 서버들은, 적어도 HTTP 서버 및 SNMP 서버를 포함하는, 정보처리장치.

청구항 11

제 1 항에 있어서,

상기 서버들의 각각은, 서로 상이한 기능을 제공하는, 정보처리장치.

청구항 12

제 1 항에 있어서,

상기 서버들 중 하나는, HTTP를 사용하여 클라이언트의 웹 브라우저와 통신하고,

상기 서버들 중 또 다른 하나는, HTTP와 상이한 통신 프로토콜을 사용하여 상기 클라이언트의 설정 관리 툴과 통신하는, 정보처리장치.

청구항 13

제 1 항에 있어서,

상기 정보처리장치는 변환 유닛을 더 포함하고,

상기 인증 처리 방법은 상기 패스워드로부터 해쉬 값을 계산하는 계산 방법을 포함하고,

상기 변환 유닛은 상기 인증 처리 방법에 포함된 계산 방법에 따라 상기 취득된 패스워드를 상기 해쉬 값으로 변환하도록 구성되는, 정보처리장치.

청구항 14

제 1 항에 있어서,

상기 정보처리장치는 복합기인, 정보처리장치.

청구항 15

제 1 항에 있어서,

상기 유저 정보 저장 유닛은 상기 패스워드의 최종 갱신 일시를 저장하고,

인증 처리의 실행에 있어서, 상기 최종 갱신 일시에 의거하여, 상기 취득된 패스워드의 유효 기한이 만료되었는지의 여부를 판정하며,

상기 취득된 패스워드의 유효 기한이 만료되는 경우에, 에러가 상기 요구에 대응하는 상기 서버에 반환되는, 정보처리장치.

청구항 16

제 1 항에 있어서,

상기 인증 처리의 실행에 있어서, 상기 취득된 패스워드가 상기 패스워드의 소정의 복잡함의 설정을 충족시키고

있는지 아닌지를 판정하며,

상기 취득된 패스워드가 소정의 복잡함의 설정을 충족시키고 있지 않은 경우에, 에러가 상기 요구에 대응하는 상기 서버에 반환되는, 정보처리장치.

청구항 17

컴퓨터에게 청구항 제9항에 따른 방법을 실행시키기 위한 프로그램을 기억하는, 컴퓨터 판독 가능한 기억 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은, 정보처리장치 및 그 제어방법에 관한 것이다.

배 경 기 술

[0002] 스캐닝, 프린팅, 통신 등의 기능을 가진 복합기(MFP:Multi Function Peripheral)이 알려져 있다. MFP는 본체에 조작 패널(operation panel)을 구비하고, 유저는 그 조작패널을 조작해서 MFP의 카피 기능, 스캔 기능 등을 이용할 수 있다. 또, 최근에, MFP는, 파일 공유 서버, 웹 서버 등의 기능을 가지고 있고, 네트워크상의 단말은, SMB(Server Message Block), HTTP 등의 통신 프로토콜을 사용해서 MFP의 서버 기능에 액세스할 수 있다. 또, MFP는, MIB(Management Information Base)을 구비하고 있고, 네트워크상의 단말은, 네트워크 기기의 관리 프로토콜로서 알려져 있는 SNMP v3(RFC3414(User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3))을 이용해 MFP의 MIB에 액세스할 수 있다.

[0003] 또한, 최근에, MFP는, 그 MFP을 이용하는 유저를 특정하기 위한 유저 인증 기구를 구비한다. 일반적으로, 1개의 MFP가 복수의 기능, 통신 프로토콜 등을 구비하는 경우, MFP는 각 기능, 통신 프로토콜 등에 대응하는 복수의 유저 인증 기구를 구비한다. 예를 들면, 조작 패널용, 웹 서버용, 파일 공유 서버용, SNMP v3용의 유저 인증 기구는 각각 다른 경우가 있다.

[0004] 이렇게 하나의 MFP가 복수의 유저 인증 기구를 구비하고 있는 경우에, 인증 기구들을 연계시키기 위한 것으로서 이하의 기술이 있다. 주로 조작 패널용의 인증에 사용하는 유저 정보와, SNMP v3의 USM(User based Security Model)으로 관리되는 유저 정보를 관련지어 동기시키는 방법이 알려져 있다(예를 들면, 일본국 공개특허공보 특개2006-195755호).

[0005] 또, 최근에는, MFP에 대해서 퍼스널 컴퓨터 등의 네트워크 단말과 같은 시큐리티가 필요하다고 여겨지고 있다. 이 때문에, 패스워드 방법(패스워드의 유효기한, 패스워드의 복잡성, 록아웃(lockout)의 설정/제어), 인증 로그(인증 성공/실패 로그의 기록) 등에 대응하는 유저 인증 기구를 구비하는 MFP도 출현하고 있다.

[0006] 하나의 기기 내에 복수의 유저 인증 기구가 존재할 경우, 이하와 같은 과제가 있다.

[0007] - 각각의 유저 인증 기구에 대하여, 같은 유저의 어카운트(account)를 등록할 경우가 있어, 유저 정보의 관리가 번거롭다. 유저에게 부담을 주지 않고, 복수의 유저 인증 기구에 대하여 같은 어카운트를 이용가능하게 하기 위해서는, 일본국 공개특허공보 특개2006-195755호에 기재된 발명과 같이, 유저의 인증을 행하는 기구 사이에서의 연계가 필요하게 된다.

[0008] - 한 개의 기기에, 패스워드 방법, 인증 로그 등을 서포트하고 있는 유저 인증 기구와, 패스워드 방법, 인증 로그 등을 서포트하고 있지 않은 유저 인증 기구가 혼재하는 것은 시큐리티의 관점에서도 바람직하지 않다. 이 때문에, 기기를 제조하는 벤더는, 복수의 유저 인증 기구에 대하여 동등의 시큐리티 기능을 제공하기 위해서 개발 비용을 발생시킬 필요가 있다고 하는 과제가 있다.

[0009] 하나의 기기에 복수의 유저 인증 기구가 존재할 경우에, 상기와 같은 과제로 인해, 통신 프로토콜이나 기능이 다른 경우에도, 단일의 유저 인증 기구를 공통으로 사용하는 구성이 바람직하다. 그렇지만, 각종 통신 프로토콜의 각 유저 인증 방법에는 사양의 차이가 있어, 단일의 유저 인증 기구에서 모든 통신 프로토콜의 유저 인증과 관련된 처리를 서포트하는 것은 곤란하다. 예를 들면, SNMP v3의 USM에서 규정된 방식은, 유저의 패스워드를 사

용하여 유저의 인증뿐만 아니라, 패스워드에 근거해 생성한 열쇠로, 암호처리, 서명/위조 검출 처리 등도 행하고 있기 때문에, 그 처리는 복잡하다.

[0010] 또한, RFC에 의해 규정된 일반적으로 잘 알려져 있는 프로토콜에 대해서는, 그 프로토콜을 설치한 소프트웨어 모듈이나 소스 코드가 일반적으로 공개되어 있다. 이 때문에, 서버를 설치하는 벤더는, 이들 기존의 소프트웨어 모듈, 소스 코드 등을 이용할 수 있다. 그러나, 기기를 제조하는 벤더가 프로토콜마다 다른 기존의 소프트웨어 모듈 및 소스 코드와 유저 인증에 관해서 기기의 모든 부분에 공통인 유저 인증 기구를 교체하기 위해서는 매우 많은 수고와 공수가 걸린다. 또한, 패스워드 방법의 체크, 패스워드의 변경, 및 인증 로그의 기록에 관한 사양이 프로토콜에 규정되어 있지 않은 경우에는, 공개된 기존의 소프트웨어 모듈과 소스 코드도 그러한 기능을 가지고 있지 않다. 따라서, 기기를 제조하는 벤더가, 기존의 소프트웨어 모듈과 소스 코드에, 패스워드 정책의 체크, 패스워드의 변경, 및 인증 로그의 기록 등의 기능을 추가/실장하지 않으면 안 되고, 거기에는 매우 많은 수고와 공수가 걸린다고 하는 문제가 있다.

발명의 내용

[0011] 본 발명의 국면은, 상술한 종래기술의 문제점을 해결하는 것에 있다.

[0012] 본 발명의 특징은, 유저의 인증에 관한 관리를 통합할 수 있는 기술을 제공하는 것이다.

[0013] 제1 국면에 있어서의 본 발명은, 복수의 프로토콜 중의 한 프로토콜에 따라 인증 요구를 수신할 수 있는 정보처리장치를 제공하고, 상기 장치는 각 유저에 대한 패스워드 및 유저 식별자와 각 프로토콜에 대한 계산 방법을 저장하도록 구성된 저장 유닛; 상기 복수의 프로토콜 중의 한 프로토콜에 따라 리모트 컴퓨터로부터 인증 데이터를 포함하는 인증 요구를 수신하도록 구성된 수신 유닛; 및

[0014] (i) 상기 저장 유닛으로부터, 상기 인증요구에 포함되어 있는 인증 데이터에 대응하는 패스워드를 취득하고,

[0015] (ii) 상기 저장 유닛으로부터 상기 프로토콜에 대응하는 계산 방법을 취득하며,

[0016] (iii) 상기 취득한 계산 방법에 따라 상기 취득한 패스워드를 해쉬로 변환하고,

[0017] (iv) 상기 해쉬로 상기 인증 데이터를 검증하도록 구성된 제어유닛을 구비한다.

[0018] 제2 국면에 있어서의 본 발명은, 복수의 프로토콜 중의 한 프로토콜에 따라 인증 요구를 수신할 수 있는 정보처리장치의 제어방법을 제공하고, 상기 방법은, 각 유저에 대한 패스워드 및 유저 식별자와 각 프로토콜에 대한 계산 방법을 메모리에 저장하는 저장 단계; 상기 복수의 프로토콜 중의 한 프로토콜에 따라 리모트 컴퓨터로부터 인증 데이터를 포함하는 인증 요구를 수신하는 수신 단계; 및

[0019] (i) 상기 메모리로부터, 상기 인증요구에 포함되어 있는 인증 데이터에 대응하는 패스워드를 취득하고,

[0020] (ii) 상기 메모리로부터, 상기 프로토콜에 대응하는 계산 방법을 취득하며,

[0021] (iii) 상기 취득한 계산 방법에 따라 상기 취득한 패스워드를 해쉬로 변환하고,

[0022] (iv) 상기 해쉬로 상기 인증 데이터를 검증하는 제어 단계를 포함한다.

[0023] 본 발명의 그 외의 특징들은 첨부도면을 참조하면서 이하의 예시적인 실시예의 설명으로부터 밝혀질 것이다.

도면의 간단한 설명

[0024] 도 1은, 본 발명의 제1 실시예에 따른 네트워크 구성을 나타내는 간략도이다.

도 2는, 제1 실시예에 따른 MFP의 하드웨어 구성을 나타내는 블럭도이다.

도 3은, 제1 실시예에 따른 MFP와 PC의 소프트웨어 및 소프트웨어가 관리하는 데이터의 구성을 설명하는 블럭도이다.

도 4a 내지 도 4d는, 제1 실시예에 따른 로컬 UI가 조작부에 표시되는 유저 인터페이스의 예를 나타내는 도면이다.

도 5a 내지 도 5f는, 설정 유저 인터페이스를 설명하는 도면이다.

도 6은, 제1 실시예에 따른 유저 데이터베이스의 데이터 구성의 예를 도시한 도면이다.

도 7a 내지 도 7c는, 제1 실시예에 따른 유저 인증 시스템이 구비하는 API의 예를 나타내는 도면이다.

도 8은, 제1 실시예에 따른 인증 처리 테이블의 내용 예를 도시한 도면이다.

도 9는, 제1 실시예에 따른 MFP에 있어서, 도 7a의 API가 호출되었을 때의 유저 인증 시스템의 동작을 설명하는 플로차트이다.

도 10a 내지 10d는, 제1 실시예에 따른 MFP이 유저 인증을 행할 때의 소프트웨어 모듈과의 관계를 데이터의 흐름과 함께 도시한 도면이다.

도 11은, 본 발명의 제2 실시예에 따른 유저 인증 시스템을 인증 서버로서 구성한 시스템 구성의 예를 도시한 도면이다.

도 12는, 제2 실시예에 따른 MFP과 인증 서버의 소프트웨어 구성을 나타내는 블럭도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 자세하게 설명한다. 한편, 이하의 실시예는 본 발명의 특허청구범위를 한정하는 것이 아니며, 또 본 실시예에서 설명되어 있는 국면들의 조합의 모두가 본 발명에 따른 문제를 해결하는 수단에 필수적인 것이라고는 할 수 없다.

[0026] 도 1은, 본 발명의 제1 실시예에 따른 네트워크 구성을 나타내는 간략도다.

[0027] 네트워크(LAN)(100)에는, 본 발명에 따른 정보처리장치의 일례인 MFP(101)와 퍼스널 컴퓨터(PC)(102)가 접속되어 있다. MFP(101)와 PC(102)는, LAN(100)을 통해서 서로 통신을 행할 수 있다. 여기에서, MFP(101)는, 스캐닝, 프린팅, 및 통신 등의 복수의 기능을 가진 복합기다.

[0028] 도 2는, 제1 실시예에 따른 MFP(101)의 하드웨어 구성을 나타내는 블럭도다.

[0029] CPU(201)을 포함하는 제어부(200)는, MFP(101) 전체의 동작을 제어한다. CPU(201)는, ROM(202)에 기억된 부트 프로그램(boot program)에 따라 HDD(204)에 인스톨되어 있는 OS, 제어프로그램 등을 RAM(203)에 전개하고, 이 프로그램을 실행하는 CPU(201)의 제어하에서 MFP(101)가 동작한다. RAM(203)은, CPU(201)의 주메모리, 워크 에어리어(work area) 등의 일시기억영역(temporary storage)으로서 사용된다. HDD(204) 는, 화상 데이터, 각종 프로그램 등을 기억한다. 조작부 인터페이스(console unit interface)(205)는, 조작부(209)와 제어부(200)를 접속한다. 조작부(209)는, 터치 패널로서 동작하는 표시부를 구비한다. 프린터 인터페이스(206)는, 프린터부(210)와 제어부(200)를 접속한다. 프린터부(210)가 인쇄해야 하는 화상 데이터는, 프린터 인터페이스(206)를 통해서 제어부(200)로부터 프린터부(210)에 전송되고, 프린터부(210)에 의해 시트 등의 기록 매체에 인쇄된다. 스캐너 인터페이스(207)는, 스캐너부(211)와 제어부(200)를 접속한다. 스캐너부(211)는, 원고 위의 화상을 스캔해서 화상 데이터를 생성하고, 이 화상 데이터를 스캐너 인터페이스(207)를 통해서 제어부(200)에 공급한다. 네트워크 인터페이스(208)는, 제어부(200)(MFP 101)를 LAN(100)에 접속한다. 네트워크 인터페이스(208)는, LAN(100)에 접속된 외부장치(예를 들면, 웹 서버 등)에 화상 데이터, 정보 등을 송신하고, LAN(100) 상의 외부장치로부터 각종 정보를 수신한다.

[0030] 한편, PC(102)는, 일반적으로 알려져 있는 범용 컴퓨터의 하드웨어 구성으로 구성되기 때문에, 그 구성의 설명을 생략한다.

[0031] 도 3은, 제1 실시예에 따른 MFP(101)와 PC(102)의 소프트웨어 및 소프트웨어가 관리하는 데이터를 설명하는 블럭도다. 한편, 도 3의 화살표는, 메인 유스 케이스(main use cases)에 있어서의 기능의 호출원(caller)과 호출처(call target)를 나타낸다. 소프트웨어의 기능과 소프트웨어가 관리하는 데이터에 대해서, 이하에 설명한다.

[0032] MFP(101)의 소프트웨어는, MFP(101)의 HDD(204)에 프로그램으로서 기억되어 있고, 그 프로그램을 RAM(203)에 전개해서 CPU(201)가 그 프로그램을 실행함으로써 이하에 설명하는 기능을 실현한다.

[0033] 로컬 UI(유저 인터페이스)(301)는, 유저가 조작가능한 유저 인터페이스를 조작부(209)에 표시하고, MFP(101)가 가지는 기능을 유저에게 제공한다.

[0034] 도 4a 내지 도 4d는, 제1 실시예에 따른 로컬 UI(301)가 조작부(209)에 표시하는 유저 인터페이스의 예를 나타

내는 도면이다.

[0035] 예를 들면, 도 4a는, 조작부(209)를 이용하는 유저를 인증하기 위한 유저 인증 화면의 일례를 도시한 도면이다. 도 4b는, 도 4a의 유저 인증 화면에서 인증한 유저가 패스워드의 변경을 요구하기 위한 패스워드 변경 화면의 일례를 나타낸다. 도 4c는, 조작부(209)를 이용하는 유저에게 제공하는 기능의 기능일람을 나타내는 메뉴 화면의 일례를 나타낸다. 도 4d는, MFP(101)의 박스 기능을 이용하기 위한 유저 인터페이스 화면의 일례를 나타낸다. 예를 들면, 유저는, 도 4d의 유저 인터페이스 화면을 이용하여 스캐너부(211)로부터 취득한 화상 데이터를, 전자 도큐먼트(electronic document)로서 HDD(204)에 보존할 수 있다. 또, HDD(204)로부터 취득한 전자 도큐먼트를 프린터부(210)를 사용해서 프린트할 수 있다.

[0036] PC(102)는, 웹 브라우저(317), 파일 관리 툴(319), MFP 관리 툴(321) 등의 소프트웨어를 구비한다.

[0037] 웹 브라우저(317)는, MFP(101)의 HTTP 서버(302)와 웹 브라우저(317)가 통신하기 위한 HTTP 클라이언트(318)로서의 기능을 갖는다. HTTP 서버(302)는, 웹 브라우저(317)로부터 요구를 수신할 때 리모트 UI(303)을 호출한다. 리모트 UI(303)는, 웹 브라우저(317)를 조작하는 유저에 대하여, HTML에 기재된 유저 인터페이스를 제공한다. HTTP 서버(302)는, 웹 브라우저(317)로부터의 요구의 응답으로서, 리모트 UI(303)로부터 취득한 HTML 데이터를 웹브라우저(317)로 반환한다.

[0038] 파일 관리 툴(319)은, MFP(101)의 SMB/CIFS 서버(304)와 파일 관리 툴(319)이 통신하기 위한 SMB/CIFS 클라이언트(320)로서의 기능을 갖는다. SMB/CIFS 서버(304)는, NTLM(NT LAN Manager) 인증 프로토콜을 처리하는 NTLM 인증 처리부(305)를 구비한다. SMB/CIFS 서버(304)는, 파일 관리 툴(319)로부터, 파일의 열람, 파일 보존 등의 요구를 수신하면, 문서 관리 서비스(306)를 호출한다. 문서 관리 서비스(306)는, HDD(204)에 보존된 전자 도큐먼트(PDF, JPEG, PNG, DOC 등의 파일 확장자를 가지는 파일)의 열람이나 갱신을 행하고, 신규 파일의 보존 등을 행하는 기능을 갖는다.

[0039] MFP 관리 툴(321)은, MFP(101)의 SNMP 서버(307)에 액세스하여 MFP(101)가 구비하는 MIB(309)에 액세스하기 위한 SNMP 클라이언트(322)로서의 기능을 갖는다. SNMP 서버(307)는, SNMP version 3의 USM에 의해 규정되어 있는 유저 인증 프로토콜을 처리하는 USM 인증 처리부(308)를 구비한다. SNMP 서버(307)가 PC(102)의 MFP 관리 툴(321)로부터의 액세스 요구를 받으면, SNMP 서버(307)는 MIB(309)에 보존된 데이터를 참조해서 설정을 행한다.

[0040] 유저 인증 시스템(310)은, MFP(101)을 이용하는 유저를 인증하기 위한 기구를 구비한다. 이 유저 인증 시스템(310)이 가지는 기능의 상세를 이하에 설명한다.

[0041] 유저 인증 시스템(310)은, MFP(101)을 관리하는 유저가, MFP(101)의 유저 인증에 관한 설정을 행하기 위한 설정 UI(311)을 구비한다. 설정 UI(311)는, 리모트 UI(303)와 마찬가지로, PC(102)의 웹 브라우저(317)로부터 이용 가능한 HTML에 기재된 유저 인터페이스로서 구성할 수 있다.

[0042] 도 5a 내지 도 5f는, 설정 UI(311)의 유저 인터페이스를 설명하는 도면이다.

[0043] 도 5a는 메뉴 화면 예를 나타낸다. 도 5a의 화면에서 숫자 502-505로 나타낸 항목 중 어느 하나가 지시되면, 처리는 그 지시된 기능의 화면으로 천이한다. 유저 인증 설정(502)은, MFP(101)의 유저 인증 기능의 ON 혹은 OFF를 설정하는 유저 인터페이스다. 도 5a의 화면에서 유저 인증 설정(502)이 지시되면, 처리는 도 5b의 화면으로 천이한다. 도 5b의 화면에서는, 유저가 유저 인증의 ON 혹은 OFF를 설정할 수 있고, 유저 인증 시스템(310)은 여기에서 설정된 내용을 HDD(204)에 인증 설정(312)으로서 기억한다. 각 소프트웨어 모듈은, 이 인증 설정(312)에 액세스해서 유저 인증의 ON/OFF 설정을 참조할 수 있다. 도 5b의 예에서는, 유저 인증이 ON으로 설정되어 있다.

[0044] 도 5c의 화면은, 도 5a의 화면에서 유저 어카운트 관리(user account management)(503)가 지시됨으로써 표시된다. 도 5c의 화면에서는, 유저가 유저명과 그 유저의 권한을 등록 및 편집할 수 있다. 도 5d의 화면은, 도 5c의 화면에서 등록 또는 편집이 지시되었을 때에 표시되는 화면의 예를 나타낸다. 유저는, 도 5c와 도 5d에 나타낸 유저 인터페이스 화면을 통해서 유저 어카운트의 등록, 편집 등을 행할 수 있다. 유저 인증 시스템(310)은, 도 5d의 화면을 사용해서 등록된 유저 어카운트와 관련된 정보를, HDD(204)의 유저 데이터베이스(313)에 기억해서 관리한다. 도 5d의 화면에서는, 유저명 "Alice"가 관리자로 등록되고, 그것과 함께 그 유저명에 대응하는 패스워드가 등록된다.

[0045] 도 6은, 제1 실시예에 따른 유저 데이터베이스(313)의 데이터 구성의 예를 도시한 도면이다.

[0046] 여기에는, 도 5c와 도 5d에 나타낸 유저 인터페이스 화면을 통해서 등록된 유저 명(601), 패스워드(602), 및 권한(603)이 등록되어 있다. 패스워드 최종 갱신 일시(604)는, 도 5d의 화면을 통해서 패스워드가 등록 또는 갱신된 일시를 나타낸다.

[0047] 도 5e의 화면은, 도 5a의 화면에서, 패스워드 폴리시 설정(password policy setting)(504)이 지시됨으로써 표시된다. 도 5e는, 패스워드와 관련된 폴리시를 설정하기 위한 유저 인터페이스 화면의 예를 나타낸다. 예를 들면, 패스워드의 유효기한으로서, "유효기한 없음", "30일", 및 "90일"을 선택할 수 있다. 또한, 패스워드의 복잡함의 설정으로서, "3문자 이상" (3문자 이상의 패스워드를 강제하는 설정), "기호를 포함시킨다" (패스워드에 기호를 포함시키는 것을 강제하는 설정) 등의 유효/무효를 선택할 수 있다. 유저 인증 시스템(310)은 도 5e의 화면을 통해서 설정된 사항을, HDD(204)에 패스워드 폴리시 설정(314)으로서 기억한다.

[0048] 도 5f의 화면은, 도 5a의 화면에서, 인증 로그 관리(505)가 지시됨으로써 표시된다. 도 5f는, 인증 결과의 로그 기록을 관리하는 유저 인터페이스 화면을 나타낸다. 도 5f에서는, 유저 인증 시스템(310)이 HDD(204)에 기록한 인증 로그(316)를 열람할 수 있다. 이 화면에는, 인증 로그(316)에 등록되어 있는 유저명, 인증 방식, 그 인증을 행하는 일시, 및 인증 결과(OK 또는 NG(no good))가 표시된다.

[0049] 도 7a 내지 도 7c는, 제1 실시예에 따른 유저 인증 시스템(310)이 구비하는 A PI(Application Programming Interface)의 예를 나타내는 도면이다.

[0050] 다른 소프트웨어 모듈이 도 7a의 API(701)을 호출함으로써, 유저 인증 시스템(310)에, 유저의 인증을 요구하는 인증 요구를 발행할 수 있다. 유저 인증 시스템(310)은, 호출원(702)의 정보에 근거한 인증 처리 테이블(315)을 참조하여 API(701)의 동작을 결정한다.

[0051] 도 8은, 제1 실시예에 따른 인증 처리 테이블(315)의 내용 예를 도시한 도면이다.

[0052] 인증 처리 테이블(315)은, 호출원의 정보(801), 호출원의 패스워드 변경 기능 유무(802), 계산 방법(803), 인증 처리 타입(804) 등의 결합을 기억한다. 호출원의 정보(801)에는, 인증 요구의 발행원인 호출원 통신 프로토콜이 등록되어 있다. 호출원 패스워드의 변경 기능 유무(802)는, 호출원의 소프트웨어 모듈이, 패스워드의 변경 기능을 포함하는지 아닌지를 나타낸다. 예를 들면, 유저와의 인터페이스를 제어하는 로컬 UI(301)에 대해서는, 호출원 패스워드의 변경 기능 유무(802)가 "유(exist)"이기 때문에, 도 4b의 패스워드 변경 화면을 조작 화면에 표시하는 기능이 존재한다.

[0053] 한편, HTTP, SMB/CIFS, SNMP v3 등의 통신 프로토콜에 대해서는, 패스워드를 변경하기 위한 프로토콜이 규정되어 있지 않다. 이 때문에, HTTP 서버(302), SMB/CIFS 서버(304), 및 SNMP v3 서버(307)는, 패스워드 변경을 요구하는 기능이 없다. 계산 방법(803)은, API(701)가 패스워드로부터 다른 값으로 변환하기 위해서 사용하는 계산 알고리즘을 나타낸다. "RAW"는, 패스워드를 가공하지 않고 그대로 사용하는 것을 나타낸다."MD4"은, 패스워드로부터 MD4(Message Digest Algorithm 4)의 다이제스트(Hash 값)을 산출하는 것을 나타낸다. "MD5"은, 패스워드로부터의 MD5(Message Digest Algorithm 5)의 다이제스트(해쉬(Hash)값)를 산출하는 것을 나타낸다. 계산 방법(803)은, "MD4", "MD5" 등에 한정되지 않고, 유저 인증 시스템(310)이 실장하고 있는 공지된 계산 방법이면 어떤 계산 방법이라도 된다. 예를 들면, HMAC(Keyed-Hashing for Message Authentication code)(RFC2104), SHA(Secure Hash Algorithm) 등 계산 알고리즘이 일반적으로 알려져 있다. 유저 인증 시스템(310)은, NTLM이나 SNMP version 3의 USM의 계산 알고리즘을 계산 방법으로서 구비하는 구성을 취해도 된다. 인증 처리 타입(804)은, API(701)의 동작을 "검증(verify)" 혹은 "산출값 반환" 중 어느 하나로 분류한다. "검증"은, API(701)가, 패스워드로부터 산출한 값과, 호출원으로부터 수신한 인증 데이터(704)를 검증해서 검증 결과를 반환하는 동작을 행하는 것을 나타낸다. "산출값 반환"은, API(701)가, 패스워드로부터 "계산 방법"(803)으로 나타낸 알고리즘으로 패스워드와 다른 값을 산출하고, 그 산출한 값을 반환하는(도 7a의 숫자 705로 나타낸 출력 데이터) 동작을 행하는 것을 나타낸다.

[0054] 다음에, API(701)가 반환하는 반환값(706)의 의미를 이하에 설명한다.

[0055] - SUCCESS

[0056] SUCCESS는 API(701)의 처리가 성공한 것을 나타낸다. 인증 처리 타입(804)이 "검증(verify)"인 경우에는, SUCCESS는 유저의 인증 처리가 성공한 것을 나타낸다. 인증 처리 타입(804)이 "산출값 반환"인 경우에는, 패스워드로부터 산출한 값을 아웃풋 데이터(705)에 기억해서 반환한다.

[0057] - SUCCESS_NEED_PWD_CHANGE

[0058] SUCCESS_NEED_PWD_CHANGE는 API(701)의 처리는 성공했지만, 패스워드가 패스워드 폴리시를 충족시키지 않기 때문에, 유저가 패스워드의 변경을 행할 필요가 있다는 것을 나타낸다. 호출원의 패스워드 변경 기능이 있는 경우에는, 이값을 반환한다.

[0059] - ERROR

[0060] ERROR는 API(701)의 처리를 중단한 것을 나타낸다. 인증 처리 타입(804)이 "검증"인 경우에는, ERROR는 유저의 인증 처리가 실패한 것을 나타낸다. 인증 처리 타입(804)이 "산출값 반환"인 경우에는, 패스워드로부터 산출한 값을 반환하지 않는다.

[0061] - ERROR_NEED_PWD_CHANGE

[0062] ERROR_NEED_PWD_CHANGE는 패스워드가 패스워드 폴리시를 충족시키지 않기 때문에, API(701)의 처리를 중단한 것을 나타낸다. 호출원 패스워드의 변경 기능이 없는 경우에는, 이값을 반환한다.

[0063] 이상에서 설명한 API(701)의 사양은, 어디까지나 일례이며, 본 발명을 한정하는 것이 아니다. 예를 들면, 도 8에 나타낸 인증 처리 테이블(315)의 정보의 일부 혹은 모두를 API의 호출원으로부터 취득하도록 구성해도 된다. 일부의 정보만을 호출원으로부터 취득하는 경우에는, API의 동작을 결정하는 데에 필요한 정보만을 인증 처리 테이블(315)로부터 취득하도록 구성한다. 이렇게 해서 인증 처리 테이블(315)을 외부로부터 편집 가능하게 구성함으로써, API를 사용하는 소프트웨어 모듈의 변경이나 추가에 유연하게 대응하는 것이 가능해 진다.

[0064] 그 밖의 API의 예를 도 7b에 나타낸다. 도 7b의 API는, 파라미터 708을 사용하고, 도 8에 나타낸 바와 같이 인증 처리 테이블(315)의 모든 정보를 호출원으로부터 취득 가능하게 하고 있다. 이렇게, 모든 정보를 호출원으로부터 취득하도록 구성한 경우에는, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조할 필요가 없다. 또한, 인증 처리용의 API는 1개의 API에 한정할 필요는 없고, 미리 상정되는 처리의 결합마다 복수의 API를 준비해도 된다. 이후의 설명에서는, 인증 처리용의 API로서, 도 7a에 나타낸 API(701)을 사용하는 것으로서 설명한다.

[0065] 도 7c의 API는, 소프트웨어 모듈이 실행하는 유저 인증의 결과를 취득하고, 인증 로그(316)에 로그를 기록한다.

[0066] 도 9는, 제1 실시예에 따른 MFP(101)에 있어서, 소프트웨어 모듈이 도 7a의 API(701)을 호출했을 때의 유저 인증 시스템(310)의 동작을 설명하는 플로차트다. 한편, 이 처리를 실행하는 프로그램은, 실행시에는 RAM(203)에 전개되고, CPU(201)의 제어 하에서 실행된다.

[0067] 이 처리는, 도 7a의 API(701)가 호출되고, 유저 인증 시스템(310)이 유저 인증과 관련된 처리의 요구를 수신하는 것에 의해 개시된다. 우선, 스텝 S901에서, 유저 인증 시스템(310)은, API(701)의 파라미터로부터 호출원(702)의 정보와 유저명(703)(유저 식별자)을 취득한다. 다음에, 처리는 스텝 S902로 진행되고, 유저 인증 시스템(310)은, 호출원(702)의 정보에 근거한 인증 처리 테이블(315)을 참조하여, 인증 방식(패스워드 변경 기능의 유무, 계산 방법, 인증 처리 타입)을 취득한다. 다음에, 처리는 스텝 S903로 진행되고, 유저 인증 시스템(310)은, 스텝 S901에서 취득한 유저명이 유저 데이터베이스(도 6)에 등록되어 있는지 아닌지를 판정한다. 그 유저명이 등록되어 있는 경우에는, 그 유저명과 관련지어서 등록된 패스워드(602) 및 패스워드 최종 갱신 일시(604)를 취득한다. 한편, 스텝 S903에서 유저명이 유저 데이터베이스에 등록되어 있지 않고 패스워드를 취득할 수 없는 경우에는, 스텝 S904에서 유저 인증 시스템(310)은 패스워드를 취득할 수 없기 때문에, 인증 실패라고 판단하고, 처리는 스텝 S914로 진행된다. 스텝 S914에서, 유저 인증 시스템(310)은 인증 실패 로그를 기록한다. 그리고, 처리는 스텝 S915로 진행되고, 유저 인증 시스템(310)은, API(701)의 호출원에 에러(ERROR)를 반환하고, 이 처리를 종료한다.

[0068] 한편, 스텝 S904에서 패스워드의 취득에 성공한 경우에는, 처리는 스텝 S905로 진행되고, 유저 인증 시스템(310)은, 패스워드 폴리시 설정(314)을 참조하여, 그 취득한 패스워드가 유효기한, 복잡함의 설정 등을 충족시키고 있는지 아닌지를 판정한다. 여기에서, 패스워드의 유효기한이 만료되었거나 복잡함이 충족되지 않은 경우에는, 처리는 스텝 S906로 진행되고, 유저 인증 시스템(310)은, 또한 호출원의 패스워드 변경 기능의 유무를 판정한다. 여기에서, 패스워드 변경 기능이 존재하는 경우에는, 처리가 스텝 S907로 진행되고, 처리를 계속한다. 그러나, 스텝 S906에서 패스워드 변경 기능이 존재하지 않는다고 판정한 경우에는, 처리는 스텝 S914로 진행되고, 인증 실패 로그를 기록하고, 스텝 S915에서, API(701)의 호출원으로 에러(ERROR_NEED_PWD_CHANGE)를 반환하고, 이 처리를 종료한다.

[0069] 스텝 S905에서, 유저 인증 시스템(310)이 취득한 패스워드가 유효기한과 복잡함의 설정을 충족시키고 있다고 판

정했을 경우, 또는 스텝 S906에서, 호출원 패스워드 변경 기능이 있다고 판정한 경우에는, 처리가 스텝 S907로 진행된다. 스텝 S907에서, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조하여, 그 호출원에 대해서 설정되어 있는 계산 방법(803)을 확인한다. 여기에서, 계산 방법이 "RAW"가 아닌 경우(예를 들면, "MD4"이나 "MD5"인 경우)에는, 처리가 스텝 S908로 진행되고, 그 계산 방법에 따라, 취득한 패스워드에 의거해 계산 처리를 행한다. 여기에서는, 예를 들면 MD4나 MD5의 알고리즘에 따라 MD4 다이제스트나 MD5 다이제스트를 산출한다. 그리고, 처리는 스텝 S909로 진행되고, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조하여, 그 호출원에 대해서 설정되어 있는 인증 처리 타입(804)을 확인한다. 여기에서, 인증 처리 타입(804)이 "산출값 반환"인 경우에는, 처리는 스텝 S910로 진행되고, 유저 인증 시스템(310)은, 산출한 값을 아웃풋 데이터(705)에 저장하고, 처리 성공(SUCCESS)을 반환하며, 이 처리를 종료한다. 또한, 이때 스텝 S905의 패스워드 폴리시 체크가 실패인 경우에는, 그 취지(SUCCESS_NEED_PWD_CHANGE)를 반환한다.

[0070] 한편, 스텝 S909에서, 유저 인증 시스템(310)이 인증 처리 타입(804)이 "검증(verify)"이라고 판정한 경우에는, 처리가 스텝 S911로 진행되고, 유저 인증 시스템(310)은, 인증 데이터(704)(도 7a)와, 스텝 S908에서 산출한 값을 검증한다. 이 검증의 결과, 인증 데이터(704)와 산출한 값이 일치한 경우에는, 처리가 스텝 S912로 진행되고, 유저 인증 시스템(310)은, 인증 성공의 로그를 기록하고, 처리는 스텝 S913로 진행되며, API의 호출원으로 처리 성공(SUCCESS)을 반환하고, 이 처리를 종료한다. 이 경우, 스텝 S905의 패스워드 폴리시 체크가 NG인 경우에는, 그 취지(SUCCESS_NEED_PWD_CHANGE)를 반환한다.

[0071] 한편, 스텝 S911의 검증 결과, 인증 데이터(704)와 산출한 값이 일치하지 않는다고 판정한 경우에는, 인증 실패라고 판단하고, 처리는 스텝 S914로 진행되고, 유저 인증 시스템(310)은 인증 실패 로그를 기록한다. 그리고, 스텝 S915에서, API의 호출원으로 에러(ERROR)를 반환하고, 이 처리를 종료한다.

[0072] 다음에, MFP(101)의 유저 인증이 ON으로 설정되어 있고, 각종 소프트웨어 모듈이 유저 인증 시스템(310)을 이용해서 유저 인증을 실행할 때의 동작 예를 설명한다. 여기에서는, 소프트웨어 모듈이, 로컬 UI(301), HTTP 서버(302), SMB/CIFS 서버(304), 및 SNMP 서버(307)인 경우에 대해서 설명한다.

[0073] 도 10a 내지 도 10d는, 제1 실시예에 따른 MFP(101)가 유저 인증을 실행할 때의 소프트웨어 모듈과의 관계를 데이터의 흐름과 함께 도시한 도면이다.

[0074] 도 10a는 로컬 UI(301)가 유저 인증 시스템(310)을 이용해서 유저 인증을 실행하는 경우를 설명하는 도면이다. 도 10a에 있어서, 유저 인증 화면을 조작 화면에 표시하고, MFP(101)을 이용하는 유저에게 유저 인증을 요구한다. 로컬 UI(301)는 스텝 S1001에서, 유저가 도 4a의 유저 인증 화면에 입력한 유저명 및 패스워드를 취득한다. 또, 스텝 S1002에서, 로컬 UI(301)는, 도 7a의 API(701)을 통해서, 유저명과 패스워드를 유저 인증 시스템(310)에 건네주어서 인증 처리를 요구한다. 이것에 의해, 유저 인증 시스템(310)은 인증 처리 테이블(315)을 참조하여 패스워드 폴리시 체크, 패스워드의 검증, 및 인증 로그의 기록을 행하고, 스텝 S1003에서, 처리 결과를 로컬 UI(301)에 응답한다.

[0075] 여기에서, 로컬 UI(301)는, 결과가 성공(SUCCESS)인 경우에는, 예를 들면 도 4c의 메뉴 화면을 표시하고, 유저에게 MFP(101)의 기능의 이용을 허가한다. 한편, 인증 결과가 NG(SUCCESS_NEED_PWD_CHANGE)인 경우에는, 패스워드 폴리시 체크가 NG이었기 때문에 조작 화면에, 도 4b의 패스워드 변경 화면을 표시하고, 유저에게 패스워드의 변경을 요구한다. 또한, 인증 결과가 에러(ERROR)인 경우에는, 도 4a의 유저 인증 화면을 표시하고, 유저에게 인증 정보의 재입력을 요구한다.

[0076] 다음에, MFP(101)의 HTTP 서버(302)의 동작을 도 10b를 참조하여 설명한다. 도 10b는, HTTP 서버(302)가 유저 인증 시스템(310)을 이용해서 유저 인증을 실행하는 경우를 설명하는 도면이다.

[0077] HTTP 서버(302)는, 스텝 S1004에서, 웹 브라우저(317)로부터 HTTP 다이제스트 인증(RFC 2617)을 포함하는 HTML 취득 요구를 수신한다. 이에 따라, HTTP 서버(302)는, 유저명과 MD5 다이제스트를 패킷으로부터 취득하고, 스텝 S1005에서, API(701)을 통해서 유저 인증 시스템(310)에 인증 처리를 요구한다. 이것에 의해, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조하여, 패스워드 폴리시 체크와, MD5 다이제스트 산출에 대해 검증하는 검증 처리를 실행하고, 인증 로그의 기록을 행하며, 스텝 S1006에서, 인증 결과를 응답한다. HTTP 서버(302)는, 그 인증 결과가 성공(SUCCESS)인 경우에는, 스텝 S1007에서 HTML 취득 요구를 리모트 UI(303)에 송신한다. 이것에 의해, 리모트 UI(303)는, 인증한 유저의 정보를 HTTP 서버(302)로부터 취득하고, 그 유저에 따라 HTML 제공 및 액세스 제어를 행한다. 한편, 결과가 실패(ERROR/ERROR_NEED_PWD_CHANGE)인 경우에는, HTTP 서버(302)는 웹 브라우저(317)에 에러를 통지한다.

[0078] 다음에, MFP(101)의 SMB/CIFS 서버(304)의 동작을 도 10c를 참조하여 설명한다. 도 10c는, SMB/CIFS 서버(304)가 유저 인증 시스템(310)을 이용해서 유저 인증을 행하는 경우를 설명하는 도면이다.

[0079] SMB/CIFS 서버(304)는, 스텝 S1008에서 PC(102)의 파일 관리 툴(319)로부터 NTLM 데이터 포맷의 인증 데이터를 포함하는 패킷을 수신한다. 이에 따라, SMB/CIFS 서버(304)는, 유저명을 패킷으로부터 취득하고, 스텝 S1009에서, API(701)을 통해서, 유저 인증 시스템(310)에 인증 처리를 요구한다. 이것에 의해, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조하여, 패스워드 폴리시 체크와 MD4 다이제스트 산출을 행하고, 스텝 S1010에서, 그 처리 결과와 함께, MD4 다이제스트를 반환한다. 이에 따라, SMB/CIFS 서버(304)에서는, NTLM 인증 처리부(305)는, 유저 인증 시스템(310)으로부터 취득한 MD4 다이제스트와 패킷으로부터 취득한 NTLM 인증 데이터를 사용해서 NTLM 인증 처리를 행한다. 그리고, SMB/CIFS 서버(304)는, NTLM 인증 처리부(305)에 의해 처리된 인증 결과를 취득하고, 스텝 S1011에서, 도 7c의 API을 통해서 유저명과 인증 결과를 유저 인증 시스템(310)에 통지한다.

[0080] 여기에서 유저의 인증에 성공한 경우에는, SMB/CIFS 서버(304)는, 그 후의 PC(102)의 파일 관리 툴(319)로부터 문서 관리 서비스(306)에의 액세스를 허가한다. 문서 관리 서비스(306)는, 스텝 S1012에서 SMB/ CIFS 서버(304)로부터 유저 정보를 취득하고, 그 유저에 따라 서비스 제공, 액세스 제어 등을 행한다. 한편, 유저의 인증이 실패했을 경우에는, SMB/CIFS 서버(304)는, PC(102)의 파일 관리 툴(319)에 에러를 통지한다.

[0081] 다음에, MFP(101)의 SNMP 서버(307)의 동작을 도 10d를 참조하여 설명한다. 도 10d는, SNMP 서버(307)가 유저 인증 시스템(310)을 이용해서 유저 인증을 행하는 경우를 설명하는 도면이다.

[0082] SNMP 서버(307)는, 스텝 S1013에서, PC(102)의 MFP 관리 툴(321)로부터 SNMP v3의 USM(RFC3414)에 따라 인증 데이터를 포함하는 패킷을 수신한다. 그리고, SNMP 서버(307)는, 그 패킷으로부터 유저명을 취득하고, 스텝 S1014에서, API(701)을 통해서 유저 인증 시스템(310)에 인증 처리를 요구한다. 이것에 의해, 유저 인증 시스템(310)은, 인증 처리 테이블(315)을 참조하여, 패스워드 폴리시 체크, 및 MD5 다이제스트 산출을 행하고, 스텝 S1015에서, 그 처리 결과와 함께 MD5 다이제스트를 반환한다. 이에 따라, SNMP 서버(307)에서는, USM 인증 처리부(308)는, 유저 인증 시스템(310)으로부터 취득한 MD4 다이제스트와 패킷으로부터 취득한 NTLM 인증 데이터를 사용해서 NTLM 인증 처리를 행한다. 그리고, SNMP 서버(307)는, USM 인증 처리부(308)의 인증 결과를 취득하고, 스텝 S1016에서, 도 7c의 API을 통해서 유저명과 인증 결과를 유저 인증 시스템(310)에 통지한다. 여기에서, 유저 인증이 성공한 경우에는, SNMP 서버(307)는, 스텝S1017에서, MFP 관리 툴(321)이 요구하는 MIB(309)에의 액세스를 행한다. SNMP 서버(307)는, 유저에 따라 MIB(309)에의 액세스 제어를 행한다. 한편, 유저의 인증이 실패했을 경우, SNMP 서버(307)는, PC(102)의 MFP 관리 툴(321)에 에러를 통지한다.

[0083] 이상에서 설명한 바와 같이, 제1 실시예에 의하면, MFP(101)의 유저 인증 기구를 단일의 유저 인증 시스템(310)으로 실현하기 때문에, 유저 인증에 관한 설정의 관리와 유저 어카운트의 관리의 부담을 경감할 수 있다.

[0084] 또, 제1 실시예에 의하면, 모든 액세스 경로에 대하여, 패스워크 시큐리티 폴리시(password security policy) 및 인증 로그의 인쇄기능을 제공하기 때문에, 모든 액세스 경로에 동등한 시큐리티 기능을 적용할 수 있다.

[0085] 또, MFP(101)의 유저 인증 시스템(310)을 이용하는 소프트웨어 모듈은, 패스워드 시큐리티 폴리시, 인증 로그의 기록 등에 반드시 대응할 필요가 없어, 기존의 소프트웨어 모듈이나 소스 코드의 개조 비용이 들지 않는다고 하는 이점이 있다.

[0086] 또한, 제1 실시예 에 의하면, 유저 인증 시스템(310)과 유저 인증 시스템(310)을 이용하는 소프트웨어 모듈이 유저 인증과 관련된 처리를 분산 처리할 수 있다. 이 때문에, 기존의 소프트웨어 모듈 및 소스 코드를 최대한 이용하면서, 유저 인증과 관련된 관리가 통합된 기기를 구성할 수 있다고 하는 효과가 있다.

[0087] [제2 실시예]

[0088] 이전에 기술한 유저 인증 시스템(310)은, 반드시 MFP(101) 내부에 있을 필요는 없고, 이 유저 인증 시스템(310)은 네트워크상의 별도의 노드로 구성해도 된다.

[0089] 도 11은, 본 발명의 제2 실시예에 따른 유저 인증 시스템을 인증 서버로서 구성한 시스템 구성의 예를 나타내는 도면이다.

[0090] 여기에서는, MFP(1101), PC(1102), 및 인증 서버(1103)가 LAN(1100)을 통해서 접속되어 있다. 한편, MFP(1101)와 PC(1102)의 하드웨어 구성은 전술한 제1 실시예에 따른 MFP(101)와 PC(102)의 하드웨어 구성과 같기 때문

에, 그 설명을 생략한다.

[0091] 도 12는, 제2 실시예에 따른 MFP(1101)와 인증 서버(1103)의 소프트웨어 구성을 나타내는 블럭도다. PC(1102)의 구성은, 전술한 제1 실시예의 PC(102)와 같은 구성이기 때문에, 그 설명을 생략한다. 한편, 전술한 도 3과 공통되는 부분은 같은 참조번호로 나타내고, 그들의 설명을 생략한다. 또, 유저 인증 서버(1103)의 참조번호 1211-1216로 나타내는 구성은, 전술한 도 3의 참조번호 311-316로 나타내는 구성과 같은 기능을 갖기 때문에, 그 설명을 생략한다.

[0092] MFP(1101)는, 인증 서버(1103)와 통신하기 위한 에이전트(1201)를 구비한다. 인증 서버(1103)는, 유저 인증 시스템(1202)을 구비한다. MFP(1101)와 인증 서버(1103)는, 사전에 통신에 사용하는 비밀의 암호 열쇠를 교환함으로써 신뢰 관계를 구축할 수 있다. PKI 기술을 사용한 클라이언트 증명서, 서버 증명서 등 제3자가 발행한 증명서를 교환해도 된다.

[0093] 에이전트(1201)는, 유저 인증 시스템(1202)이 가지는 API와 동등한 API(도 7a의 번호 701 혹은 도 7c 등)을 구비한다. 에이전트(1201)는, 다른 소프트웨어 모듈로부터 API가 호출되면, 네트워크상의 통신을 통해서 유저 인증 시스템(1202)의 API를 호출해서 처리 결과를 취득한다. 이때 네트워크상에 흐르는 정보는 은닉할 필요가 있기 때문에, 사전에 교환한 열쇠를 이용해서 암호화를 행한다. 이렇게 유저 인증 시스템(1202)을 네트워크상의 독립된 노드(인증 서버)로 구성함으로써, 복수의 MFP으로부터 이용 가능한 유저 인증 시스템(1202)을 제공할 수 있다.

[0094] 이상에서 설명한 바와 같이 본 실시예에 의하면, 이하의 같은 효과를 취득할 수 있다.

[0095] - 유저 인증 기구를 단일의 유저 인증 시스템으로서 실현 가능하게 한 것에 의해, 유저 인증과 관련된 설정의 관리와 유저 어카운트의 관리의 부담을 경감할 수 있다.

[0096] - 유저 인증 시스템을 이용하는 기기에 대한 모든 액세스 경로에, 같은 유저 인증 기구를 적용할 수 있다.

[0097] - 기존의 소프트웨어 모듈과 소스 코드를 재이용할 수 있고, 비교적 적은 수고와 공수로, 유저의 인증을 행할 수 있는 기기를 구성할 수 있다.

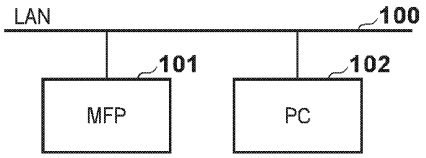
[0098] 그 밖의 실시예

[0099] 본 발명의 실시예들은, 상술한 본 발명의 실시예(들) 중의 하나 또는 그 이상의 기능을 행하도록 기억매체(예를 들면, 비일시 컴퓨터 판독가능한 기억매체) 상에 기록된 컴퓨터 실행가능한 명령들을 판독 및 실행하는 시스템 또는 장치의 컴퓨터에 의해서 실현될 수 있고, 또 예를 들면, 상술한 실시예(들) 중의 하나 또는 그 이상의 기능을 행하도록 기억매체로부터 컴퓨터 실행가능한 명령들을 판독 및 실행함으로써 시스템 또는 장치의 컴퓨터에 의해 행해지는 방법에 의해서도 실현될 수 있다. 이 컴퓨터는 CPU(Central Processing Unit), MPU(Micro Processing Unit), 또는 다른 회로 중 하나 또는 그 이상을 구비할 수도 있고, 독립된 컴퓨터 또는 독립된 컴퓨터 프로세서의 네트워크를 포함할 수도 있다. 이 컴퓨터 실행가능한 명령들은 예를 들면, 네트워크 또는 기억매체로부터 컴퓨터에 제공될 수도 있다. 이 기억매체는 예를 들면, 하드 디스크, RAM(random-access memory), ROM(read only memory), 분산 컴퓨팅 시스템의 스토리지, 광디스크(컴팩트 디스크(CD), DVD(digital versatile disc), Blue-ray Disc(BD)TM 등), 플래시 메모리 디바이스, 메모리 카드 중 어느 하나 또는 그 이상을 포함할 수도 있다.

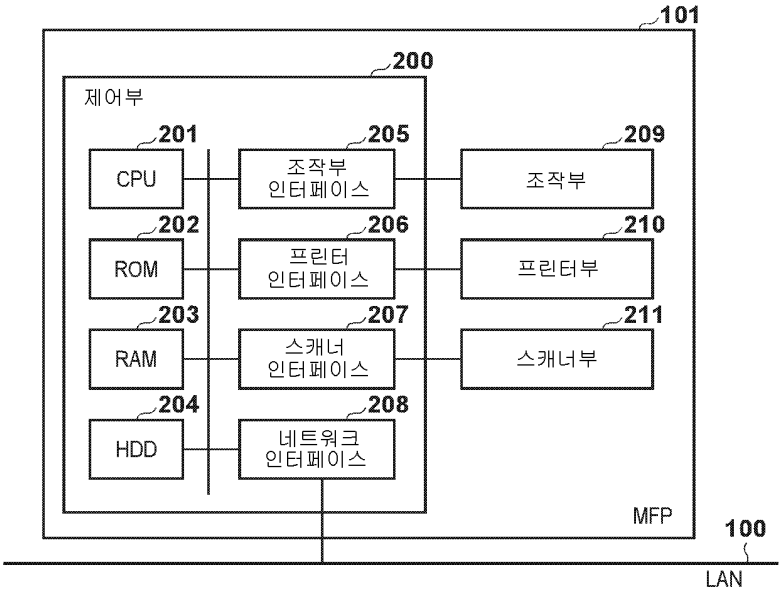
[0100] 본 발명은 예시적인 실시 예를 참조하면서 설명되었지만, 본 발명은 이 개시된 예시적인 실시 예에 한정되는 것이 아니라는 것이 이해될 것이다. 이하의 특허청구범위의 범주는 모든 변형 및 균등구조 및 기능을 포함하도록 가장 넓게 해석되어야 할 것이다.

도면

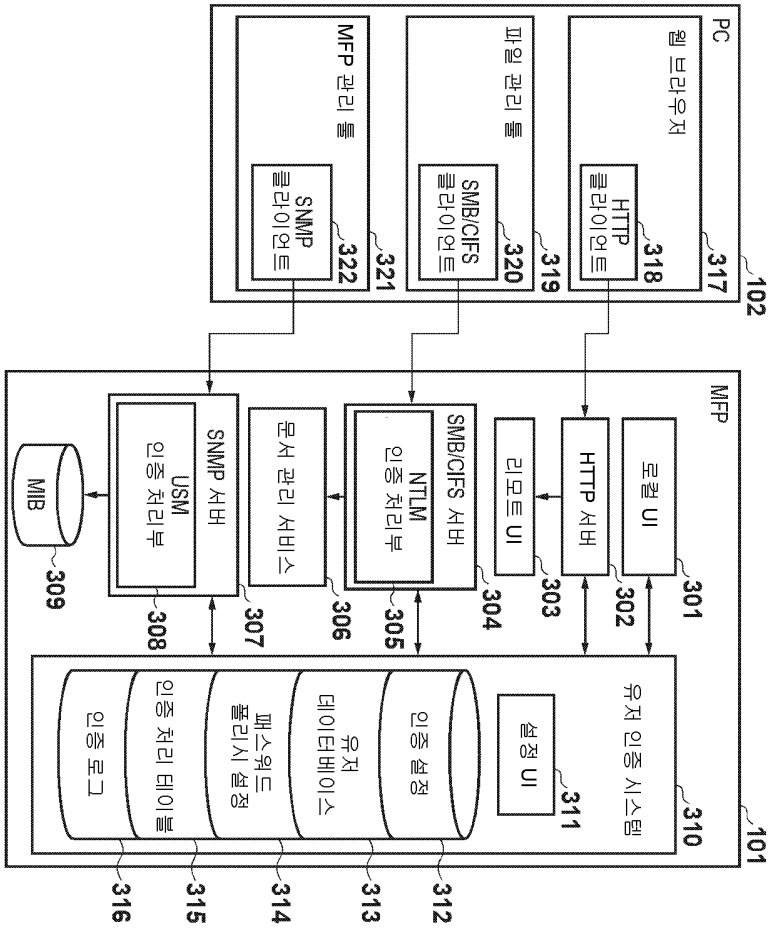
도면1



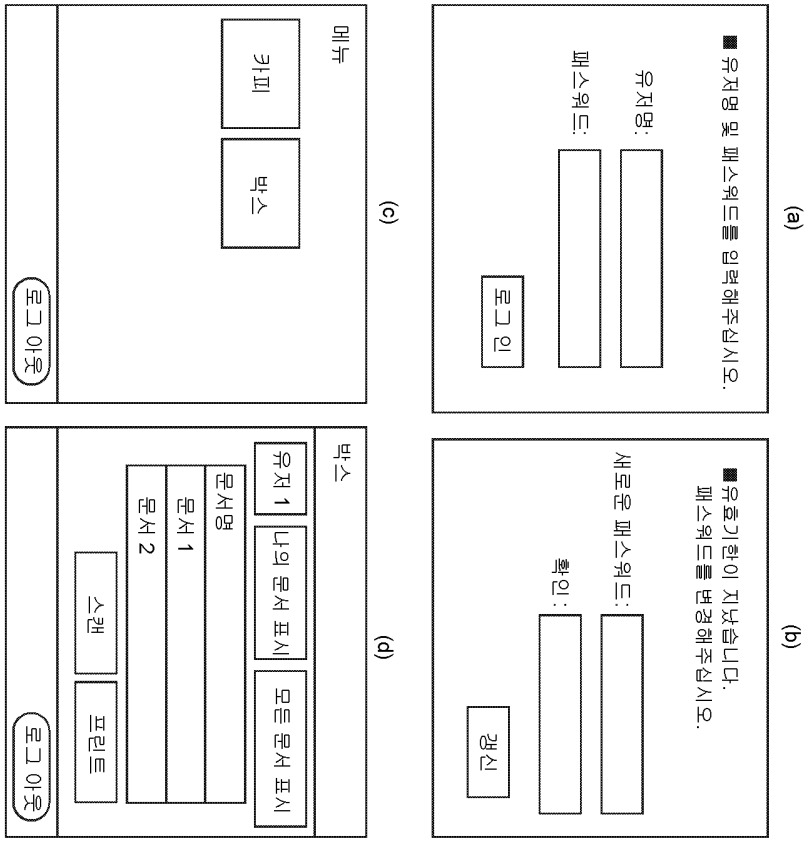
도면2


101
200
제어부
201
CPU
202
ROM
203
RAM
204
HDD
205
조작부 인터페이스
206
프린터 인터페이스
207
스캐너 인터페이스
208
네트워크 인터페이스
209
조작부
210
프린터부
211
스캐너부
MFP
100
LAN

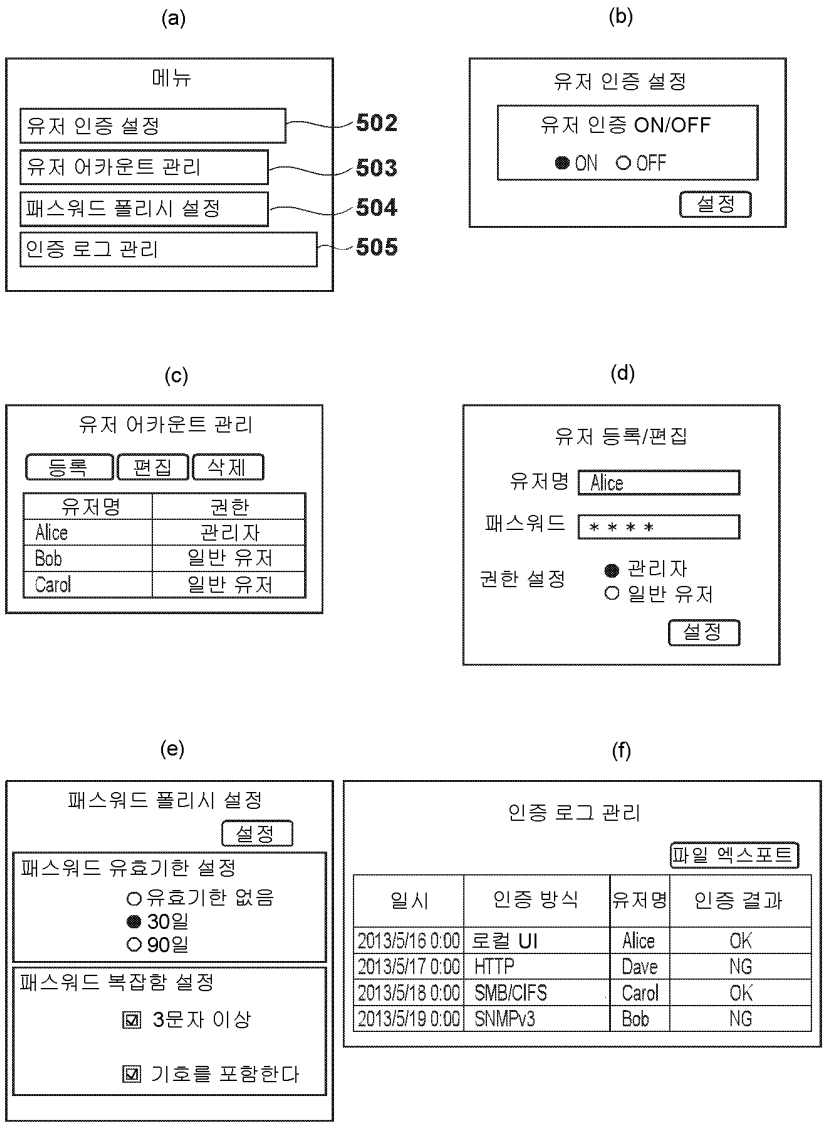
도면3


PC
웹 브라우저
HTTP 클라이언트
317
318
파일 관리 툴
SMB/CIFS 클라이언트
319
320
MFP 관리 툴
SNMP 클라이언트
321
322
102
MFP
로컬 UI
301
HTTP 서버
302
리모트 UI
303
SMB/CIFS 서버
NTLM 인증 처리부
304
305
문서 관리 서비스
306
SNMP 서버
USM 인증 처리부
307
308
MIB
309
유저 인증 시스템
310
설정 UI
311
인증 설정
유저 데이터베이스
패스워드 폴리시 설정
인증 처리 테이블
인증 로그
312
313
314
315
316
101

도면4


(a)
■ 유저명 및 패스워드를 입력해주십시오.
유저명:
패스워드:
로그 인
(b)
■ 유효기한이 지났습니다.
패스워드를 변경해주십시오.
새로운 패스워드:
확인 :
갱신
(c)
메뉴
카피
박스
로그 아웃
(d)
박스
유저 1
나의 문서 표시
모든 문서 표시
문서명
문서 1
문서 2
스캔
프린트
로그 아웃

도면5



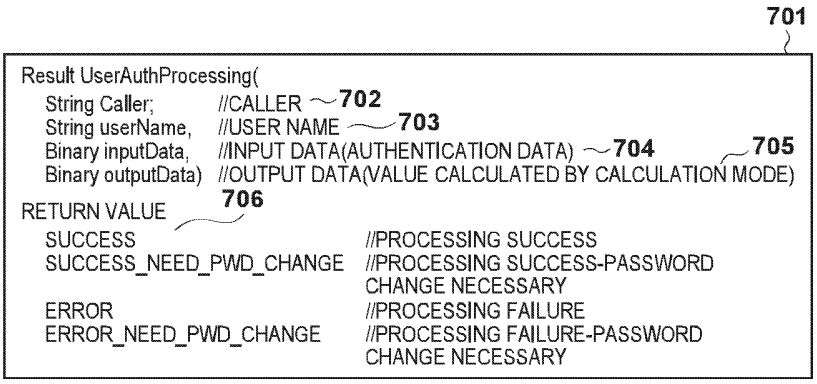
도면6

601 602 603 604

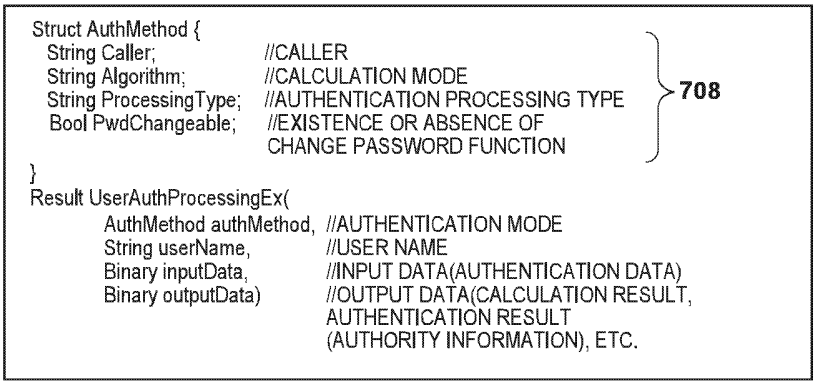
유저명	패스워드	권한	패스워드 최종 갱신 일시
Alice	****	관리자	2013/2/1 10:00
Bob	****	일반 유저	2013/2/2 10:00
Carol	****	일반 유저	2013/2/3 10:00

도면7

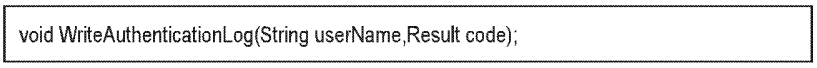
(a)


701
Result UserAuthProcessing(
String Caller; //CALLER 702
String userName, //USER NAME 703
Binary inputData, //INPUT DATA(AUTHENTICATION DATA) 704
Binary outputData) //OUTPUT DATA(VALUE CALCULATED BY CALCULATION MODE) 705
RETURN VALUE 706
SUCCESS //PROCESSING SUCCESS
SUCCESS_NEED_PWD_CHANGE //PROCESSING SUCCESS-PASSWORD CHANGE NECESSARY
ERROR //PROCESSING FAILURE
ERROR_NEED_PWD_CHANGE //PROCESSING FAILURE-PASSWORD CHANGE NECESSARY

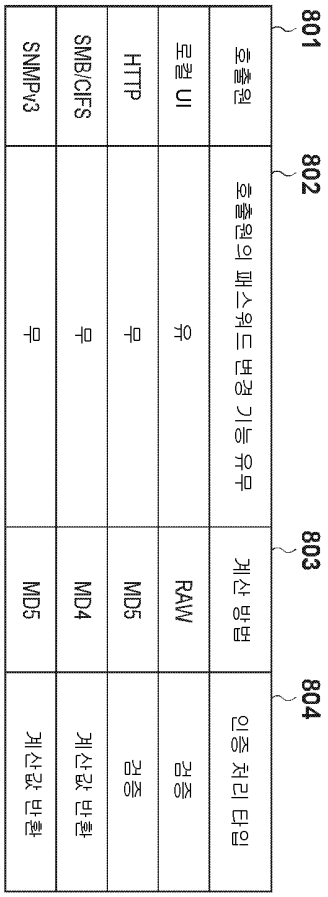
(b)


Struct AuthMethod {
String Caller; //CALLER
String Algorithm; //CALCULATION MODE
String ProcessingType; //AUTHENTICATION PROCESSING TYPE
Bool PwdChangeable; //EXISTENCE OR ABSENCE OF CHANGE PASSWORD FUNCTION
708
}
Result UserAuthProcessingEx(
AuthMethod authMethod, //AUTHENTICATION MODE
String userName, //USER NAME
Binary inputData, //INPUT DATA(AUTHENTICATION DATA)
Binary outputData) //OUTPUT DATA(CALCULATION RESULT, AUTHENTICATION RESULT (AUTHORITY INFORMATION), ETC.

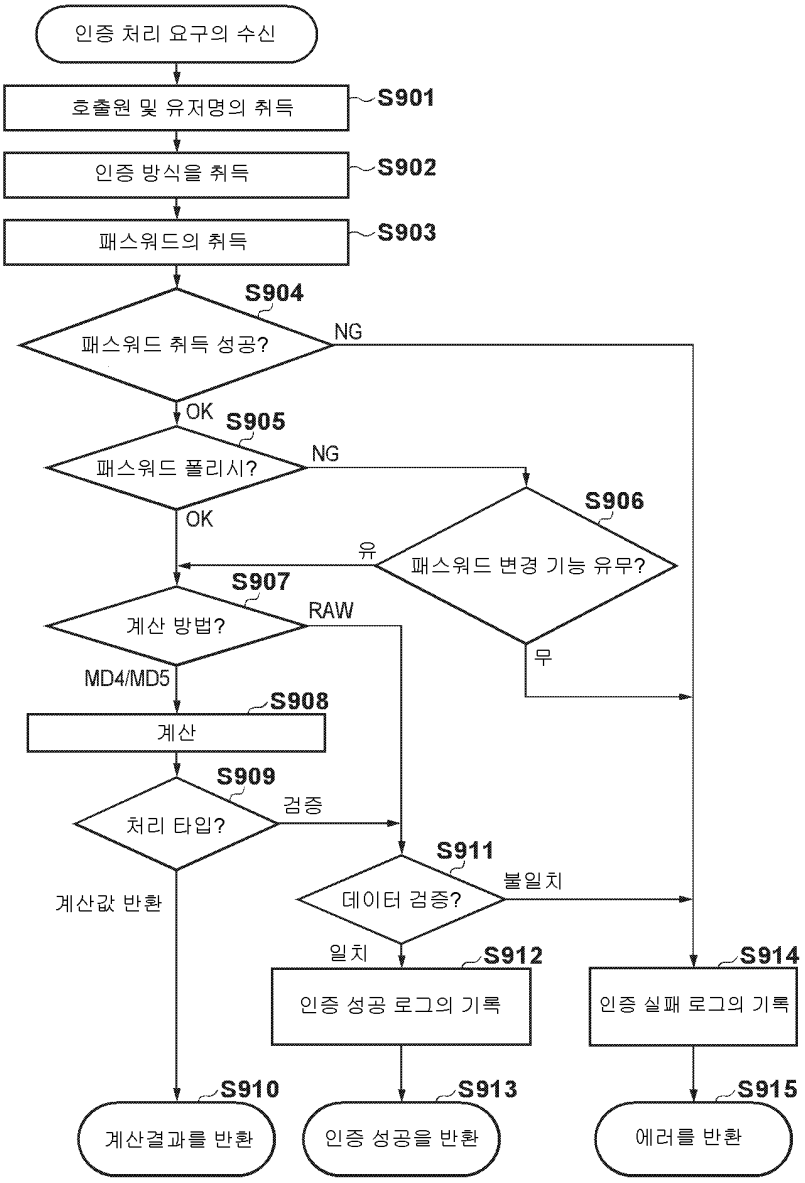
(c)


void WriteAuthenticationLog(String userName,Result code);

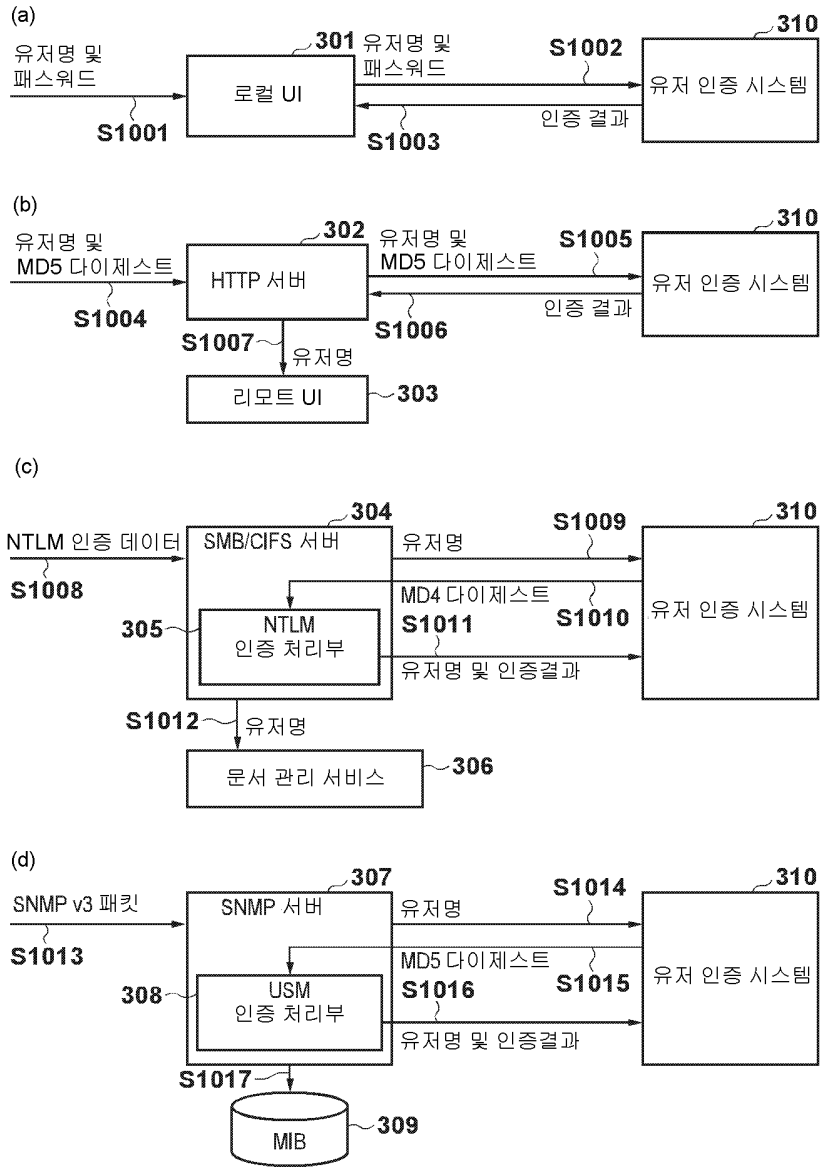
도면8


801
802
803
804
호출원
로컬 UI
HTTP
SMB/CIFS
SNMPv3
호출원의 패스워드 변경 기능 유무
유
무
무
계산 방법
RAW
MD5
MD4
MD5
인증 처리 타입
검증
검증
계산값 반환
계산값 반환

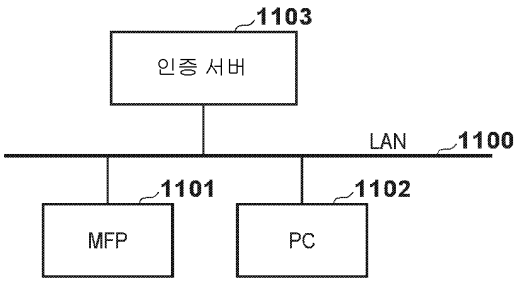
도면9


인증 처리 요구의 수신
호출원 및 유저명의 취득
S901
인증 방식을 취득
S902
패스워드의 취득
S903
S904
패스워드 취득 성공?
NG
OK
S905
패스워드 폴리시?
NG
OK
S906
패스워드 변경 기능 유무?
유
무
S907
계산 방법?
RAW
MD4/MD5
S908
계산
S909
처리 타입?
검증
계산값 반환
S911
데이터 검증?
불일치
일치
S912
인증 성공 로그의 기록
S914
인증 실패 로그의 기록
S910
계산결과를 반환
S913
인증 성공을 반환
S915
에러를 반환

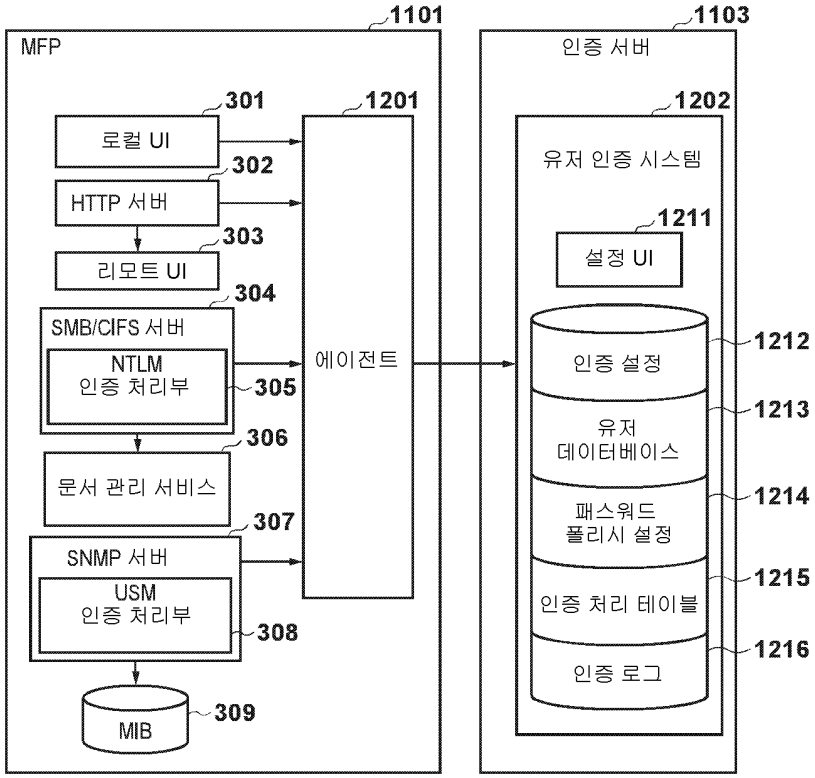
도면10


(a)
유저명 및
패스워드
S1001
301
로컬 UI
유저명 및
패스워드
S1002
310
유저 인증 시스템
인증 결과
S1003
(b)
유저명 및
MD5 다이제스트
S1004
302
HTTP 서버
유저명 및
MD5 다이제스트
S1005
310
유저 인증 시스템
인증 결과
S1006
S1007
유저명
리모트 UI
303
(c)
NTLM 인증 데이터
S1008
304
SMB/CIFS 서버
유저명
S1009
310
유저 인증 시스템
MD4 다이제스트
S1010
305
NTLM
인증 처리부
S1011
유저명 및 인증결과
S1012
유저명
문서 관리 서비스
306
(d)
SNMP v3 패킷
S1013
307
SNMP 서버
유저명
S1014
310
유저 인증 시스템
MD5 다이제스트
S1015
308
USM
인증 처리부
S1016
유저명 및 인증결과
S1017
MIB
309

도면11


1103
인증 서버
LAN
1100
1101
1102
MFP
PC

도면12


1101
MFP
301
로컬 UI
302
HTTP 서버
303
리모트 UI
304
SMB/CIFS 서버
NTLM
인증 처리부
305
306
문서 관리 서비스
307
SNMP 서버
USM
인증 처리부
308
MIB
309
1201
에이전트
1103
인증 서버
1202
유저 인증 시스템
1211
설정 UI
1212
인증 설정
1213
유저
데이터베이스
1214
패스워드
폴리시 설정
1215
인증 처리 테이블
1216
인증 로그