



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0137239
(43) 공개일자 2012년12월20일

(51) 국제특허분류(Int. Cl.)
G06F 15/16 (2006.01) G06F 3/12 (2006.01)
(21) 출원번호 10-2012-0058007
(22) 출원일자 2012년05월31일
심사청구일자 없음
(30) 우선권주장
JP-P-2011-129545 2011년06월09일 일본(JP)
JP-P-2011-272755 2011년12월13일 일본(JP)

(71) 출원인
캐논 가부시끼가이샤
일본 도쿄도 오오따꾸 시모마루쵸 3쵸메 30방 2고
(72) 발명자
가와나 요시마사
일본 도쿄도 오오따꾸 시모마루쵸 3쵸메 30방 2고
캐논 가부시끼가이샤 내
히라하라 아끼코
일본 도쿄도 오오따꾸 시모마루쵸 3쵸메 30방 2고
캐논 가부시끼가이샤 내
(74) 대리인
박충범, 장수길

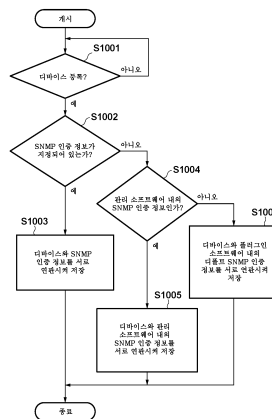
전체 청구항 수 : 총 19 항

(54) 발명의 명칭 관리 장치, 관리 방법, 및 컴퓨터 판독가능한 매체

(57) 요약

본 발명의 네트워크 상의 복수의 디바이스를 관리하기 위한 제1 관리 소프트웨어가 제어 수단에 의해 실행되는 관리 장치는, 상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과; 신규 기능을 추가하기 위해 상기 제1 관리 소프트웨어에 추가된 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단과; 상기 제2 관리 소프트웨어에 의해 관리되어야 하는 디바이스를 등록하는 등록 수단과; 상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제2 설정 수단을 포함한다.

대표도 - 도10



특허청구의 범위

청구항 1

네트워크 상의 복수의 디바이스를 관리하기 위한 제1 관리 소프트웨어가 제어 수단에 의해 실행되는 관리 장치이며,

상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과,

신규 기능을 추가하기 위해 상기 제1 관리 소프트웨어에 추가된 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단과,

상기 제2 관리 소프트웨어에 의해 관리되어야 하는 디바이스를 등록하는 등록 수단과,

상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제2 설정 수단을 포함하고,

상기 제2 설정 수단이 인증 정보를 설정한 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 상기 디바이스에 액세스하는데 이용되는 정보로서 저장하고,

상기 제2 설정 수단이 인증 정보를 설정하지 않고 또한 상기 제1 저장 수단이 등록된 상기 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 상기 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 장치.

청구항 2

제1항에 있어서,

상기 제2 설정 수단이 인증 정보를 설정하지 않고 또한 상기 제1 저장 수단이 등록된 상기 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있지 않은 경우, 상기 제2 저장 수단은, 상기 제2 관리 소프트웨어에 의해 디폴트로서 관리되고 있는 인증 정보를, 등록된 상기 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 장치.

청구항 3

제1항에 있어서,

상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제1 설정 수단을 더 포함하고,

상기 제1 설정 수단이 인증 정보를 설정한 경우, 상기 제1 저장 수단은 설정된 인증 정보를, 디바이스에 액세스하는데 이용되는 정보로서 저장하고,

상기 제1 설정 수단이 인증 정보를 설정하지 않은 경우, 상기 제1 저장 수단은 복수의 디바이스에 공통으로 이용되도록 관리되는 인증 정보를, 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 장치.

청구항 4

제1항에 있어서,

상기 제2 관리 소프트웨어의 기능으로서 상기 등록 수단에 의해 등록된 디바이스의 상세 정보를 표시하는 표시 수단을 더 포함하고,

상기 디바이스의 상세 정보로서 디바이스에 액세스하는데 이용되는 정보를 표시할 때, 상기 제2 저장 수단이 상기 제1 저장 수단에 저장되는 인증 정보를 저장하고 있는 경우, 상기 표시 수단은 인증 정보를 표시하지 않고 인증 정보가 설정되어 있음을 나타내는 통지를 표시하는 것을 특징으로 하는, 관리 장치.

청구항 5

제1항에 있어서,

상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보의 갱신 요구를 수신했을 때에,

상기 제1 저장 수단이 상기 갱신 요구에 의해 지정된 인증 정보를 저장하고 있지 않은 경우에는, 상기 제2 저장 수단에 저장된 인증 정보는 상기 갱신 요구에 따라 갱신되지 않고,

상기 제1 저장 수단이 상기 갱신 요구에 의해 지정된 인증 정보를 이미 저장하고 있는 경우에는, 상기 제2 저장 수단은 상기 갱신 요구에 따라, 상기 갱신 요구에 의해 지정된 인증 정보를, 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 장치.

청구항 6

제1항에 있어서,

상기 제2 관리 소프트웨어가 상기 제2 저장 수단에 저장된 인증 정보를 이용하여 디바이스로 액세스하는 것이 실패한 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장된, 상기 디바이스로의 액세스를 가능하게 하는 인증 정보를 취득하고, 저장되어 있는 인증 정보를 취득된 인증 정보로 갱신하는 것을 특징으로 하는, 관리 장치.

청구항 7

제1항에 있어서,

디바이스에 액세스하는데 이용되는 인증 정보는 SNMP(Simple Network Management Protocol)의 인증 정보인 것을 특징으로 하는, 관리 장치.

청구항 8

제7항에 있어서,

상기 SNMP의 인증 정보는 SNMP 버전 1의 커뮤니티명 또는 SNMP 버전 3의 유저명 및 패스워드를 포함하는 것을 특징으로 하는, 관리 장치.

청구항 9

네트워크 상의 복수의 디바이스를 관리하기 위한 제1 관리 소프트웨어가 제어 수단에 의해 실행되는 관리 장치로서, 상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과, 신규 기능을 추가하기 위해 상기 제1 관리 소프트웨어에 추가된 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단을 포함하는 관리 장치의 관리 방법이며,

상기 제2 관리 소프트웨어에 의해 관리되어야 하는 디바이스를 등록하는 등록 단계와,

상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제2 설정 단계를 포함하고,

상기 제2 설정 단계에서 인증 정보가 설정된 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하고,

상기 제2 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 방법.

청구항 10

제9항에 있어서,

상기 제2 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는

데 이용되는 인증 정보를 저장하고 있지 않은 경우, 상기 제2 저장 수단은 상기 제2 관리 소프트웨어에 의해 디폴트로서 관리되고 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 방법.

청구항 11

제9항에 있어서,

상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제1 설정 단계를 더 포함하고,

상기 제1 설정 단계에서 인증 정보가 설정된 경우, 상기 제1 저장 수단은 설정된 인증 정보를, 디바이스에 액세스하는데 이용되는 정보로서 저장하고,

상기 제1 설정 단계에서 인증 정보가 설정되지 않은 경우, 상기 제1 저장 수단은 복수의 디바이스에 공통으로 이용되도록 관리되는 인증 정보를, 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 관리 방법.

청구항 12

제9항에 있어서,

상기 제2 관리 소프트웨어가 상기 제2 저장 수단에 저장된 인증 정보를 이용하여 디바이스로 액세스하는 것이 실패한 경우, 상기 제1 저장 수단에 저장된, 상기 디바이스로의 액세스를 가능하게 하는 인증 정보로, 상기 제2 저장 수단에 저장된 인증 정보가 갱신되는 것을 특징으로 하는, 관리 방법.

청구항 13

제9항에 있어서,

디바이스에 액세스하는데 이용되는 인증 정보는 SNMP의 인증 정보인 것을 특징으로 하는, 관리 방법.

청구항 14

제13항에 있어서,

상기 SNMP의 인증 정보는 SNMP 버전 1의 커뮤니티명 또는 SNMP 버전 3의 유저명 및 패스워드를 포함하는 것을 특징으로 하는, 관리 방법.

청구항 15

네트워크 상의 복수의 디바이스를 관리하기 위한 관리 소프트웨어에 신규 기능을 추가하기 위해 컴퓨터에 의해 실행되는 프로그램을 저장하는 컴퓨터 판독가능한 매체로서, 상기 컴퓨터는, 상기 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과, 상기 관리 소프트웨어에 추가된 상기 프로그램의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단을 포함하는, 컴퓨터 판독가능한 매체이며,

상기 프로그램은,

상기 프로그램에 의해 관리되어야 하는 디바이스를 등록하는 등록 단계와,

상기 프로그램의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 설정 단계를 컴퓨터가 실행하도록 하고,

상기 설정 단계에서 인증 정보가 설정된 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하고,

상기 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 컴퓨터 판독가능한 매체.

청구항 16

제15항에 있어서,

상기 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있지 않은 경우, 상기 제2 저장 수단은 상기 프로그램의 기능에 의해 디폴트로서 관리되고 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 하는, 컴퓨터 판독가능한 매체.

청구항 17

제15항에 있어서,

상기 프로그램의 기능이 상기 제2 저장 수단에 저장된 인증 정보를 이용하여 디바이스로 액세스하는 것이 실패한 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장된, 상기 디바이스로의 액세스를 가능하게 하는 인증 정보를 취득하고, 저장되어 있는 인증 정보를 취득된 인증 정보로 갱신하는 것을 특징으로 하는, 컴퓨터 판독가능한 매체.

청구항 18

제15항에 있어서,

디바이스에 액세스하는데 이용되는 인증 정보는 SNMP의 인증 정보인 것을 특징으로 하는, 컴퓨터 판독가능한 매체.

청구항 19

제18항에 있어서,

상기 SNMP의 인증 정보는 SNMP 버전 1의 커뮤니티명 또는 SNMP 버전 3의 유저명 및 패스워드를 포함하는 것을 특징으로 하는, 컴퓨터 판독가능한 매체.

명세서

기술분야

[0001] 본 발명은 관리 장치, 관리 방법, 및 컴퓨터 판독가능 매체에 관한 것이다. 본 발명은 네트워크 상의 디바이스를 관리하는 기술에 관한 것이며, 특히 SNMP를 이용하여 디바이스를 관리할 때 인증 정보를 관리하는 기술에 관한 것이다.

배경기술

[0002] 종래에 프린터 등의 화상 형성 장치(이하, 디바이스로서 지칭됨)를 관리하는 관리 소프트웨어는, 통신 프로토콜로서 SNMP(Simple Network Management Protocol)를 이용하고 있다. 관리 소프트웨어는 SNMP를 이용하여 디바이스 관리에 필요한 정보를 취득한다. 이 때, 관리 소프트웨어는 디바이스로부터 정보를 취득하는데 이용되는 SNMP 인증 정보[SNMP 버전 1에 있어서의 커뮤니티명(community name)을 포함함]을 관리한다. 인증 정보를 관리하는 종래 기술에는, 관리 대상 디바이스의 타입에 따라 복수의 후보로부터 적절한 인증 정보가 결정되는 것이 개시되어 있다(예를 들면, 일본 특허 공개 제2009-110261호 공보).

[0003] 한편, 관리 소프트웨어로서, 시스템 관리자가 디바이스의 동작 상태를 확인하는데 이용되는 소프트웨어와, 유지보수를 행하는 외부의 서비스맨이 원격 지점으로부터 디바이스의 수리 또는 부품의 배송을 위한 관리를 행하는데 이용되는 소프트웨어가 존재한다. 다른 목적에 대응하기 위해, 1개의 관리 소프트웨어에 대하여 다른 목적의 기능을 추가하거나 그 기능을 확장하는데 이용되는 플러그인 소프트웨어가 존재한다. 플러그인 소프트웨어를 이용하여 각각의 목적에 따라 네트워크 상의 디바이스가 관리되는 것으로 가정한다.

[0004] 그러나, 종래 기술에서는, 인증 정보를 다른 관리 목적의 소프트웨어 각각에 대해 관리하는 방법은 가정하고 있지 않다. 예를 들면, 일본 특허 공개 제2009-110261호 공보에서는, 관리 소프트웨어와 플러그인 소프트웨어 각각이 디바이스의 인증 정보를 관리한다. 이러한 종래 기술은, 플러그인 소프트웨어가 관리 소프트웨어에서 관리되는 인증 정보를 이용할 수 있게 하는 방법에 대해서는 전혀 가정하고 있지 않다.

발명의 내용

해결하려는 과제

[0005] 본 발명은, 다른 관리 목적을 위해 플러그인 소프트웨어에 의해 확장된 관리 소프트웨어도, 네트워크 상의 디바이스를 관리하는데 이용되는 인증 정보를 각각의 관리 목적에 따라 관리할 수 있게 한다.

과제의 해결 수단

[0006] 본 발명의 일 양태에 따르면, 네트워크 상의 복수의 디바이스를 관리하기 위한 제1 관리 소프트웨어가 제어 수단에 의해 실행되는 관리 장치가 제공되며, 상기 관리 장치는, 상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과; 신규 기능을 추가하기 위해 상기 제1 관리 소프트웨어에 추가된 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단과; 상기 제2 관리 소프트웨어에 의해 관리되어야 하는 디바이스를 등록하는 등록 수단과; 상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제2 설정 수단을 포함하고, 상기 제2 설정 수단이 인증 정보를 설정한 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 상기 디바이스에 액세스하는데 이용되는 정보로서 저장하고, 상기 제2 설정 수단이 인증 정보를 설정하지 않고 또한 상기 제1 저장 수단이 등록된 상기 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 상기 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 한다.

[0007] 본 발명의 다른 양태에 따르면, 네트워크 상의 복수의 디바이스를 관리하기 위한 제1 관리 소프트웨어가 제어 수단에 의해 실행되는 관리 장치로서, 상기 제1 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과, 신규 기능을 추가하기 위해 상기 제1 관리 소프트웨어에 추가된 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단을 포함하는 관리 장치의 관리 방법이 제공되며, 상기 관리 방법은, 상기 제2 관리 소프트웨어에 의해 관리되어야 하는 디바이스를 등록하는 등록 단계와; 상기 제2 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 제2 설정 단계를 포함하고, 상기 제2 설정 단계에서 인증 정보가 설정된 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하고, 상기 제2 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 한다.

[0008] 본 발명의 다른 양태에 따르면, 네트워크 상의 복수의 디바이스를 관리하기 위한 관리 소프트웨어에 신규 기능을 추가하기 위해 컴퓨터에 의해 실행되는 프로그램을 저장하는 컴퓨터 판독가능한 매체로서, 상기 컴퓨터는, 상기 관리 소프트웨어의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제1 저장 수단과, 상기 관리 소프트웨어에 추가된 상기 프로그램의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 저장하는 제2 저장 수단을 포함하는, 컴퓨터 판독가능한 매체가 제공되며, 상기 컴퓨터 판독가능한 매체는, 상기 프로그램이, 상기 프로그램에 의해 관리되어야 하는 디바이스를 등록하는 등록 단계와; 상기 프로그램의 기능을 이용하여 디바이스에 액세스하는데 이용되는 인증 정보를 설정하는 설정 단계를 컴퓨터가 실행하도록 하고, 상기 설정 단계에서 인증 정보가 설정된 경우, 상기 제2 저장 수단은 설정된 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하고, 상기 설정 단계에서 인증 정보가 설정되지 않고 또한 상기 제1 저장 수단이 등록된 디바이스에 액세스하는데 이용되는 인증 정보를 저장하고 있는 경우, 상기 제2 저장 수단은 상기 제1 저장 수단에 저장되어 있는 인증 정보를, 등록된 디바이스에 액세스하는데 이용되는 정보로서 저장하는 것을 특징으로 한다.

발명의 효과

[0009] 본 발명에 따르면, 다른 관리 목적을 위해 플러그인 소프트웨어에 의해 확장된 관리 소프트웨어도, 네트워크 상의 디바이스를 관리하는데 이용되는 인증 정보를 각각의 관리 목적에 따라 관리할 수 있게 한다.

[0010] 본 발명의 추가적인 특징은 (첨부된 도면을 참조하여) 하기의 예시적인 실시형태의 상세한 설명으로부터 명백해질 것이다.

도면의 간단한 설명

- [0011] 도 1은 디바이스와 관리 장치(101) 사이의 네트워크 접속 관계의 일례를 도시하는 도면.
 도 2는 디바이스의 하드웨어 구성의 일례를 도시하는 블록도.
 도 3은 디바이스의 소프트웨어 기능 구성의 일례를 도시하는 블록도.
 도 4는 관리 장치(101)의 하드웨어 구성의 일례를 도시하는 블록도.
 도 5는 관리 장치(101)의 소프트웨어 기능 구성의 일례를 도시하는 블록도.
 도 6은 관리 소프트웨어 내에서 관리되는 인증 정보 데이터를 도시하는 표.
 도 7은 플러그인 소프트웨어 내에서 관리되는 인증 정보 데이터를 도시하는 표.
 도 8은 갱신 지시가 수신된 후의, 플러그인 소프트웨어 내에서 관리되는 인증 정보 데이터를 도시하는 표.
 도 9는 관리 소프트웨어에서의 디바이스 등록시의 동작의 일례를 도시하는 플로우차트.
 도 10은 플러그인 소프트웨어에서의 디바이스 등록시의 동작의 일례를 도시하는 플로우차트.
 도 11은 플러그인 소프트웨어에서의 디바이스 정보 갱신시의 동작의 일례를 도시하는 플로우차트.
 도 12a, 도 12b 및 도 12c는 플러그인 소프트웨어에서의 디바이스 등록 화면의 일례를 도시하는 도면.
 도 13a 및 도 13b는 플러그인 소프트웨어에서의 상세한 디바이스 정보 표시의 일례를 도시하는 도면.
 도 14는 디바이스의 커뮤니티명의 갱신 처리를 도시하는 플로우차트.

발명을 실시하기 위한 구체적인 내용

- [0012] 이제, 본 발명의 실시형태에 대해서 첨부한 도면을 참조하여 설명한다.
- [0013] <디바이스 관리 시스템의 구성예>
- [0014] 도 1은, 본 발명의 실시형태에 따른 복사기와 관리 장치(101) 사이의 접속 관계를 도시하는 도면이다. 도 1을 참조하면, 디바이스(100)는 고객의 인트라넷에 접속된 MFP(Multi Function Printer) 또는 SFP(Single Function Printer)를 나타내고 있다. 인쇄/복사 기능을 갖는 이들 디바이스는, 본원에서 총칭하여 "디바이스"로 지칭될 것이다. 본 실시형태에 있어서, 도 1에는 일례로서 4개의 디바이스가 도시되어 있다. 그러나, 디바이스의 개수는 이에 한정되지 않으며, 보다 많은 개수의 디바이스가 접속될 수 있다. 본 명세서에 있어서, 디바이스는, 처리와 관련하여 개별적으로 설명해야 할 필요가 있을 때에만 디바이스 A 내지 D로서 지칭될 것이다. 일반적인 설명에 대해서는, 디바이스는 디바이스(100)로서 지칭될 것이다.
- [0015] 관리 장치(101)는 도 1에 도시된 복수의 디바이스(100)를 관리한다. 관리 장치(101)에는, 디바이스(100)를 관리하는데 이용되는 관리 소프트웨어가 인스톨되어 있다. 관리 장치(101)는 디바이스들과 통신을 행하여 디바이스들로부터 정보를 취득하거나 또는 설정값을 변경함으로써 디바이스들을 관리한다. 관리 장치(101)는 각종 정보를 관리하기 위한 데이터 베이스(DB)를 포함한다. 네트워크(102)는 디바이스(100)와 관리 장치(101)가 접속되는 네트워크를 나타낸다. 본 실시형태에 있어서, 네트워크(102)는 기업용 또는 캠퍼스용의 LAN(Local Area Network)으로서 설명한다. 그러나, 네트워크의 구성은 이에 한정되지 않으며, 인터넷 등의 네트워크 상에서의 접속이 채용될 수 있다.
- [0016] 각각의 디바이스(100)는 SNMP(Simple Network Management Protocol)를 이용한 자기 관리 기능(self-management function)을 갖고 있다. SNMP는 디바이스(100)의 네트워크 통신 상태, 시스템 명칭, 기동 이후의 시간 등의 시스템에 관련된 각종 정보의 문의에 대한 응답을 반환한다. 디바이스(100)는, 프로토콜을 이용하여 문의와 인증 정보(예를 들면, SNMP 버전 1에서의 커뮤니티명)를 수신한다. 디바이스(100)는, 문의와 함께 인증 정보를 수신하면, 인증 정보를 검증하고, 인증 정보가 맞다고 판단했을 경우에 문의에 대해 응답한다. 커뮤니티명은 SNMP에 의해 관리되는 네트워크의 범위를 나타낸다는 점에 유의한다. 관리 장치(101)는 상기 범위에 속하는 디바이스들을 관리한다. 이 경우에, 커뮤니티명은 디바이스가 커뮤니티에 속하기 위한 인증 정보(패스워드)로서 제공된다.
- [0017] 관리 장치(101)는 일반적인 PC(퍼스널 컴퓨터)로서 도면에 도시되어 있지만, 관리 소프트웨어를 실행할 수 있는

디바이스를 나타낸다. 따라서, 관리 소프트웨어는 PC 뿐만 아니라 전용의 하드웨어 또는 디바이스(100)에 인스톨될 수 있다. 여기에서는, 관리 장치(101)의 형태가 특별히 한정되지 않는다.

[0018] 관리 장치(101)에 인스톨되는 관리 소프트웨어는 SNMP를 이용한 디바이스 관리 기능을 가지며, 네트워크에 접속되어 있는 각각의 디바이스로부터 관리 정보를 취득할 수 있다. 디바이스를 관리하는 시스템 관리자는, 관리 소프트웨어에 디바이스를 등록할 때 SNMP 인증 정보를 설정한다. 관리 소프트웨어는, 디바이스(100)로부터 관리 정보를 취득하기 위해, SNMP 인증 정보를 이용하여 디바이스(100)에 문의를 발행한다.

[0019] 플러그인 소프트웨어(플러그인 프로그램)를 추가함으로써, 관리 소프트웨어에 기능을 추가하거나 또는 관리 소프트웨어를 확장시키는 것이 가능하다. 플러그인 소프트웨어의 일례로는, 디바이스(100)의 유지 보수 서비스를 행하는 서비스맨용의 플러그인 소프트웨어가 있다. 보다 구체적으로, 플러그인 소프트웨어는, 인쇄되는 페이지 매수와 부품의 사용 횟수를 포함하는 카운터 정보와, 장애 정보 등의 동작 정보를 디바이스로부터 수집하고, 인터넷 등의 외부 네트워크의 유지 보수용의 원격 서버에 상기 정보를 송신한다. 또한, 플러그인 소프트웨어는, 원격 서버에 액세스하여 디바이스로부터 수집되어야 할 동작 정보를 변경하거나 또는 디바이스의 장애를 복구하기 위한 커맨드를 취득하는 기능을 구현한다. 당연히, 이러한 원격 유지 보수 서비스는, 다른 관리 기능의 디바이스와 상이한 디바이스를 대상으로 할 수 있다.

[0020] 플러그인 소프트웨어는, 관리 대상의 디바이스를 등록할 때에, 디바이스의 인증 정보를 설정할 수 있다. 관리 소프트웨어의 유저(예를 들면, 시스템 관리자)와 플러그인 소프트웨어의 유저(예를 들면, 유지 보수 서비스의 서비스맨)는 상이하기 때문에, 각각의 소프트웨어에 대응하여 단일 디바이스에 대해 상이한 인증 정보가 설정될 수 있다. 또한, 플러그인 소프트웨어는, 페어런트(parent) 소프트웨어로서 제공되는 관리 소프트웨어에 설정되어 있는 인증 정보를 참조하여, 이를 디바이스 관리 정보로서 설정할 수 있다.

[0021] 엄격한 시큐리티 제어 하의 유저 환경에서는, 디바이스 유지 보수 서비스를 위해 이용되는 서비스 인증 정보가 각각의 디바이스에 설정되고, 플러그인 소프트웨어에 대해 고유한 인증 정보를 이용하여 각각의 디바이스로부터 정보가 취득된다. 한편, 엄격하지 않은 시큐리티 제어 하의 유저 환경에서는, 플러그인 소프트웨어는 인증 정보를 설정할 필요가 없다. 대신에, 플러그인 소프트웨어는 관리 소프트웨어 내의 인증 정보를 참조하여 인증 정보를 설정할 수 있다. 엄격하지 않은 시큐리티 제어 하의 유저 환경은, 예를 들면 복수의 감시 대상 디바이스에 대해 똑같은 인증 정보가 설정되는 환경을 가리킨다.

[0022] <디바이스의 제어 유닛의 구성예>

[0023] 도 2는 도 1에 도시된 디바이스(100)의 제어 유닛에 관한 하드웨어 구성의 일례를 도시하는 블록도이다. 디바이스(100)의 제어 유닛은 주로 디바이스(100)의 인쇄 또는 스캐닝 기능 등의 화상 처리 기능을 구현하도록 구성된 프로그램을 제어한다. 또한, 제어 유닛은 관리 시스템의 처리 기능을 구현하도록 구성된 SNMP 서비스 프로그램 등의 프로그램을 제어한다. 디바이스(100)는, 관리 장치(101)로부터 SNMP에 의해 관리 정보에 관한 문의를 수신하면, SNMP 통신 포맷에 기초하여 제어 유닛 내에서 디바이스(100)의 관리 정보의 데이터를 생성하고, 관리 장치(101)에 상기 정보를 반환한다.

[0024] 본 실시형태에 따른 디바이스의 제어 유닛은 시스템 관리를 행하는 부분과, 화상 처리를 행하는 부분을 포함하고 있다. 시스템 관리를 위한 제어 유닛의 구성 요소는 조작 유닛(201), 네트워크 I/F(202), 회선 I/F(203), ROM(Read Only Memory)(204), RAM(Random Access Memory)(205), 저장 디바이스(206) 및 CPU(Central Processing Unit)(207)를 포함한다. 화상 처리를 위한 구성 요소는 IO 제어 유닛(208), 화상 처리 유닛(209), 화상 회전 유닛(210), 디지털 I/F(211), 압축/압축 해제 유닛(212) 및 화소 밀도 변환 유닛(213)을 포함한다. 이들 구성 요소는 시스템 버스(216) 및 화상 버스(217)에 접속된다.

[0025] 시스템 버스(216)에는 이하에 설명되는 구성요소가 배치된다. 조작 유닛(201)은 표시 수단과 키 입력 수단을 내장하고 있고, 이들은 CPU(207)에 의해 제어된다. 조작자는 키 입력 수단을 통해 스캐너 판독과 인쇄 출력에 관한 각종 설정 및 지시와, 동작 및 정지 지시를 입력한다. 또한, 조작자는 조작 유닛(201)을 통해 SNMP 인증 정보를 변경하고 설정할 수 있다.

[0026] 네트워크 I/F(202)는 디바이스(100)를 LAN에 접속하기 위한 인터페이스 유닛이다. 네트워크 I/F(202)는 LAN을 통해 관리 장치(101)와 통신한다. 예를 들면, 디바이스(100)는, 네트워크 I/F(202)를 통해 관리 장치(101)로부터 SNMP로 디바이스 관리 정보에 관한 문의를 수신하고, 대응하는 응답을 반환한다.

[0027] 회선 I/F(203)는 ISDN(Integrated Services Digital Network) 또는 공중 전화망에 접속되어, 원격 단말기로 데이터를 송신하고 원격 단말기로부터 데이터를 수신한다. 회선 I/F(203)는 통신 제어 프로그램에 의해 제어되어

팩시밀리 데이터 등을 송신/수신한다.

- [0028] ROM(204)은 디바이스(100)의 각종 제어 프로그램 및 SNMP 서비스 프로그램을 저장하고 있다. 이들의 각종 프로그램은 CPU(207)에 의해 실행된다. RAM(205)은 각종 프로그램을 실행하기 위한 워크(work) 메모리 영역으로서 제공된다. RAM(205)은, 예를 들면 SNMP 서비스 프로그램이 디바이스 정보를 관리하는데 필요한 상황 정보 또는 네트워크 I/F(202)로부터 수신된 화상 데이터를 일시적으로 저장한다.
- [0029] 저장 유닛으로서 제공되는 저장 디바이스(206)는, 디바이스(100)의 재기동 후에도 저장될 필요가 있는 각종 동작 모드 설정, 카운터값(예를 들면, 각각의 사이즈에 대해 인쇄되는 페이지 매수와, 원고 판독 횟수), 상황 정보(상황 플래그를 포함함) 등을 저장하는 비휘발성 메모리 디바이스이다. 저장 디바이스(206)에 저장되는 설정 정보는 조작 유닛(201)에 의해 설정된 SNMP 인증 정보를 포함한다. 디바이스의 오퍼레이팅 시스템(OS)과, 다른 어플리케이션 프로그램도 저장 디바이스(206)에 저장된다.
- [0030] CPU(207)는, ROM(204) 또는 저장 디바이스(206)에 저장되어 있는 제어 프로그램 및 SNMP 서비스 프로그램을 RAM(205)으로 판독해내어, 이를 실행한다. CPU(207)는 제어 프로그램을 실행하여 저장 디바이스(206)로부터 카운터값과 동작 로그(operation log) 등의 동작 정보와 장해 정보를 판독해내고, 디바이스(100)의 상황 정보로서 네트워크 I/F(202)를 통해 관리 장치(101)에 이들 정보를 송신한다.
- [0031] CPU(207)에 의해 실행되는 SNMP 서비스 프로그램은, 인증 정보와 함께 네트워크 I/F(202)로부터 디바이스 관리 정보에 관한 문의를 수신한다. SNMP 서비스 프로그램은, 저장 디바이스(206)로부터 판독해낸 SNMP 인증 정보에 기초하여, 수신된 인증 정보가 맞다고 판단하면, 디바이스 관리 정보에 관한 문의에 대응하는 응답을 반환한다.
- [0032] IO 제어 유닛(208)은 화상 데이터를 고속으로 전송하는 화상 버스(217)와 시스템 버스(216)를 접속하기 위한 버스 브릿지이다. 화상 버스(217)는 IEEE1394 등의 버스로 형성된다.
- [0033] 화상 버스(217) 상에는 이하에 설명되는 구성요소가 배치된다. 디지털 I/F(211)는 디바이스(100)의 리더 유닛(215) 및 프린터 유닛(214)을 제어 유닛에 접속하여 화상 데이터의 동기 시스템과 비동기 시스템 사이의 변환을 행한다. 리더 유닛(215) 또는 프린터 유닛(214)의 여러 위치에 배치된 상술한 각종 센서에 의해 검출된 정보는 디지털 I/F(211) 및 IO 제어 유닛(208)을 통해 시스템 버스(216)로 공급된다.
- [0034] 화상 처리 유닛(209)은 입력 및 출력 화상 데이터를 보정, 가공 및 편집한다. 화상 회전 유닛(210)은 화상 데이터를 회전시킨다. 화상 압축/압축 해제 유닛(212)은 다치(multilevel) 화상 데이터에 대해서는 JPEG, 2차 화상 데이터에 대해서는 JBIG/MMR/MR/MH 등의 압축/압축 해제 처리를 행한다. 화상 밀도 변환 유닛(213)은 출력 화상 데이터의 해상도를 변환한다. 압축 해제 처리의 방법은 단지 일례이며, 이에 한정되지 않는다는 점에 유의한다.
- [0035] <디바이스의 소프트웨어 모듈 구성>
- [0036] 도 3은 도 1에 도시된 디바이스(100)에 있어서의 외부 시스템과 통신 가능한 디바이스의 소프트웨어 모듈 구성의 일례를 도시하는 블록도이다. 본 발명에 관련된 관리 장치(101)에 대한 SNMP 설정 처리에 있어서의 기능을 주로 설명한다.
- [0037] 도 3에 도시된 구성요소(301 내지 310 및 312 내지 315)는 디바이스(100)의 소프트웨어 모듈에 대응한다. 디바이스(100)의 소프트웨어 모듈로서, 상황 감시 매니저(302), 조작 UI 시스템(307), SNMP 서비스(312)가 도시된다. 디바이스 인터페이스(301)는 도 2에 도시된 IO 제어 유닛(208)을 나타낸다. 프린터 유닛(214)에서 검출되는 에러(장해라고도 함)를 포함하는 화상 형성 장치 상황은 인터페이스를 통해 상황 감시 매니저(302)로 보내진다. 화상 형성 장치의 에러는 하드 디스크 에러 및 과금 카운터 에러 등의 서비스 콜 에러, 용지 잼 및 토너 부족 경고 등의 에러를 포함한다. 또한, 도어 개방과 배지 트레이 상의 시트 초과 적재도 포함된다.
- [0038] 상황 이벤트 모듈(303)은, 디바이스 인터페이스(301)로부터 보내진 에러 정보를 매니저(304)에게 통지한다. 디바이스 인터페이스(301)로부터 보내진 에러 정보는 도 2에 도시된 프린터 유닛(214)의 각종 센서에 의해 검출된 화상 형성 장치의 상황에 기초한다. 이 에러 정보는 시계열적으로 변화한다.
- [0039] 비휘발성 저장 디바이스(305)는 도 2의 ROM(204)과 저장 디바이스(206)에 대응한다. 비휘발성 저장 디바이스(305)는 디바이스 관리에 필요한 펌웨어 정보 및 디바이스 식별 번호 등의 디바이스 관리 정보를 저장하고 있다. 비휘발성 저장 디바이스(305)는, 디바이스 관리 정보 뿐만 아니라 프로그램으로부터 출력되는 로그 정보, 카운터 정보 및 장해 정보도 저장하고 있다. 또한, 위기 관리 정보로서, 본 발명에 관련된 SNMP의 인증

정보도 여기에 저장되어 있다.

- [0040] 조작 유닛 UI(306)는 도 2에 도시된 조작 유닛(201)을 나타낸다. 조작자는 조작 유닛 UI(306)를 통해 디바이스(100)의 각종 프로토콜을 온/오프 제어하고 다른 디바이스 설정을 행할 수 있다. 디바이스(100)는, 적절한 권한을 갖는 조작자만이 디바이스(100)의 설정을 변경할 수 있도록 하는 인증 기능을 갖는다. 조작자는 조작 유닛 UI(306)를 통해 인증 정보를 입력함으로써 디바이스의 설정을 변경할 수 있다.
- [0041] 입력 관리 매니저(308)는 조작 유닛 UI(306)로부터 조작자의 입력 정보를 수신하고, 적절한 프로그램에 요구를 발행한다. 입력 관리 매니저(308)는, 조작 유닛 UI(306)를 통해 디바이스에 대한 설정 정보 변경 화면을 출력할 것이 요구되면, 조작자가 적절한 권한을 가진 유저인지 여부를 확인하기 위해, 조작 유닛 UI(306)를 통해 인증 정보를 요구한다. 조작자로부터 인증 정보를 수신하면, 입력 관리 매니저(308)는 수신된 인증 정보와 함께 인증 요구를 인증 프로그램(309)으로 보낸다. 입력 관리 매니저(308)는, 인증 프로그램(309)으로부터 인증 성공의 결과를 수신하면, 조작자에게 설정 변경 프로그램(310)으로의 액세스를 허용한다. 보다 구체적으로, 입력 관리 매니저(308)는 설정 변경 프로그램(310)에 의해 제공되는 설정 메뉴를 조작 유닛 UI(306)에 반환하고, 조작자로부터의 요구를 수신한다. 또한, 입력 관리 매니저(308)는, 적절한 권한을 가진 조작자로부터 디바이스에 대한 설정 변경 요구를 수신하면, 설정 변경 프로그램(310)에 설정 변경 요구를 발행한다.
- [0042] 인증 프로그램(309)은 조작자가 적절한 권한을 갖고 있는 지 여부를 검증한다. 인증 프로그램(309)은 조작자가 적절한 권한을 갖고 있는 지 여부를 판정하여, 입력 관리 매니저(308)에 인증 결과를 반환한다.
- [0043] 설정 변경 프로그램(310)은 디바이스의 설정 변경을 수신하여, 각각의 프로그램에 통지하거나 또는 비휘발성 저장 디바이스(305)에 저장한다. 설정 변경 프로그램(310)은, 입력 관리 매니저(308)에 의해 발행된 설정 변경 요구를 수신하면, 비휘발성 저장 디바이스(305)에 새로운 설정 정보를 기입하고, 처리 결과를 입력 관리 매니저(308)에 반환한다.
- [0044] 예를 들면, SNMP 인증 정보를 변경하기 위해, 조작자는 먼저 조작 유닛 UI(306)를 통해 성공적으로 인증을 행하고, 설정 변경 프로그램(310)으로의 액세스 권한을 취득한다. 다음에, 조작자는 설정 변경 프로그램(310)에 의해 제공되는 설정 메뉴로부터 SNMP 인증 정보 변경 지시를 선택한다. 설정 변경 프로그램(310)에 의해 제공되는 UI 상에서 조작자가 SNMP 인증 정보 변경을 지정하면, 입력 관리 매니저(308)는 조작 유닛 UI(306)를 통해 설정 변경 요구를 수신한다. 입력 관리 매니저(308)는 설정 변경 프로그램(310)에 대해 SNMP 인증 정보 변경 요구를 발행한다. 설정 변경 프로그램(310)은 실제로 SNMP 인증 정보가 저장되어 있는 비휘발성 저장 디바이스(305)에 새로운 인증 정보를 기입한다. 올바르게 변경 요구가 처리되면, 프로그램을 통해 변경이 완료된 것이 조작자에게 통지된다.
- [0045] SNMP 서비스(312)는 디바이스(100) 상에서 작동하는 SNMP 서비스를 나타낸다. SNMP 서비스(312)는 디바이스의 상황과 설정값 및 네트워크 I/F의 상황을 포함하는 디바이스의 각종 관리 정보를 설정하고 반환한다. 디바이스(100)는 관리 장치(101)에 의해 발행되는 SNMP 문의를 SNMP 서비스(312)가 수신하도록 한다. SNMP 문의는 관리 정보의 타입을 나타내는 식별자인 OID(Object ID)와 인증 정보를 포함한다. SNMP 서비스(312)는 수신된 문의를 해석하고, 인증 정보와 요구로 나누고, 인증 정보가 맞는지 여부를 판정한다. 인증이 성공했을 경우에, SNMP 서비스(312)는 요구에 대한 응답을 다른 저장 장소로부터 취득하여, SNMP 요구에 대한 응답으로서 관리 장치(101)에 반환한다.
- [0046] SNMP 서비스 매니저(315)는 외부 네트워크(311)로부터 관리 정보 요구를 수신하는 프로그램이다. SNMP 서비스 매니저(315)는 수신된 SNMP 요구를 해석하고, SNMP 요구에 포함되는 OID 부분과 인증 정보를 분리한다. 그리고, SNMP 서비스 매니저(315)는 해석에 의해 취득된 인증 정보를 이용하여 인증 프로그램(314)에 인증 요구를 보내고, 그 응답으로서 인증 결과를 수신한다. 인증 결과가 인증 성공을 나타내는 경우에는, SNMP 서비스 매니저(315)는 인증 정보와 함께 수신된 SNMP 요구에 기초하여 필요한 관리 정보를 정보 참조 프로그램(313)에 요구한다. 정보 참조 프로그램(313)이 요구에 대응하는 관리 정보를 반환하면, SNMP 서비스 매니저(315)는 SNMP의 응답 포맷으로 관리 정보를 변환하여, 관리 장치(101)에 SNMP 응답을 반환한다.
- [0047] 인증 프로그램(314)은 SNMP 요구가 올바른 발행자에 의해 발행되었는지 여부를 검증한다. 인증 프로그램(314)은 SNMP 요구가 올바른 발행자에 의해 발행되었는지 여부를 판정하여, SNMP 서비스 매니저(315)에 인증 결과를 반환한다.
- [0048] 정보 참조 프로그램(313)은 SNMP 서비스 매니저(315)로부터 디바이스 관리 정보 또는 설정 정보 문의를 수신한다. 이 때, 정보 참조 프로그램(313)은 수신된 문의에 응답하여 비휘발성 저장 디바이스(305) 또는 다른 프로

그램으로부터 설정 정보를 취득하여, SNMP 서비스 매니저(315)에 응답으로서 반환한다.

[0049] <관리 장치(101)의 제어 유닛의 구성예>

[0050] 도 4는 도 1에 도시된 관리 장치(101)의 하드웨어 구성의 일례를 도시하는 블록도이다. 관리 장치(101)는 SNMP를 이용하여 디바이스(100)로부터 취득되는 디바이스 관리 정보를 수집하기 위한 어플리케이션을 실행한다. 관리 장치(101)는 일반적인 정보 처리 장치의 구성을 갖는다. 즉, 관리 장치(101)는, 버스(401), CPU(402), ROM(403) 및 RAM(404) 외에, 네트워크 I/F(405), 표시 제어 유닛(406), 표시 디바이스(409), 입력 제어 유닛(407), 입력 디바이스(410, 411) 및 저장 디바이스(408)를 포함한다.

[0051] 버스(401)는 도 1에 도시된 관리 장치(101)의 구성부품들 사이에서 데이터를 전송하는 공통 신호 경로로서 제공된다. RAM(404)은 재기입 가능한 저장 수단이며, 디바이스의 관리 소프트웨어를 실행하기 위한 워크 메모리 영역으로서 제공된다. 디바이스의 관리 소프트웨어는, 예를 들면 SNMP를 이용하여 디바이스(100)로부터 관리 데이터를 취득하는 프로그램을 포함한다. 디바이스(100)로부터 취득된 관리 데이터는 RAM에서 전개되어 소정의 포맷으로 변환된다.

[0052] 저장 디바이스(408)는 비휘발성 저장 디바이스이다. 저장 디바이스(408)는 하드웨어를 제어하는 OS를 저장하고 있다. 또한, 관리되어야 하는 디바이스(100)의 리스트와, 관리 소프트웨어와 플러그인 소프트웨어를 구성하는 프로그램이 저장되어 있다. 프로그램 이외에, SNMP 요구를 발행할 때의 인증 정보 등의, 프로그램을 처리하는데 이용되는 설정 정보도 저장 디바이스(408)에 저장된다.

[0053] 네트워크 I/F(405)는 장치를 LAN에 접속시키는 인터페이스이며, LAN을 통해 디바이스(100)와 통신한다. CPU(402)는 구성부품(403 내지 411)을 개별적으로 또는 조직적으로 제어하고, 저장 디바이스(408)에 저장된 프로그램과 스케줄에 기초하여 네트워크 I/F(405)를 통해 디바이스(100)의 관리 정보를 수집한다.

[0054] <관리 장치(101)의 소프트웨어 구성예>

[0055] 도 5는 관리 장치(101)에 인스톨되는 관리 소프트웨어(제1 관리 소프트웨어) 및 플러그인 소프트웨어(제2 관리 소프트웨어)에 있어서의 SNMP 인증 정보를 저장하는 어플리케이션 프로그램의 기능을 도시하는 블록도이다. 관리 소프트웨어를 이용하는 유저는 "유저 A"로서 정의되고, 플러그인 소프트웨어를 이용하는 유저는 "유저 B"로서 정의된다. 여러 소프트웨어의 상이한 입력 처리를 가정하여 설명한다. 각각의 소프트웨어의 유저는 시스템 관리 또는 유지 보수 서비스 등의 상술한 목적을 갖는 유저에 대응한다. 관리 소프트웨어(500)와 플러그인 소프트웨어(520)는 SNMP 인증 정보 입력/출력 유닛(502)과 SNMP 인증 정보 결정 로직 유닛(507)이 각종 정보를 송신/수신하도록 함으로써 협동할 수 있다. 또한, SNMP 클라이언트(512)와 플러그인 매니저(511) 사이에서도 각종 정보의 송신/수신이 행해진다.

[0056] 각각의 어플리케이션 프로그램은 각각의 유저로부터 관리 디바이스 등록을 수신하기 위한 UI를 갖는다. 관리 소프트웨어(500)에 있어서의 디바이스 등록 화면은 관리 소프트웨어 UI 디바이스 등록 유닛(501)이고, 플러그인 소프트웨어(520)에 있어서의 디바이스 등록 화면은 플러그인 UI 디바이스 등록 유닛(506)이다.

[0057] 유저 A는 관리 소프트웨어 UI 디바이스 등록 유닛(501)을 통해 SNMP 인증 정보의 디폴트값을 설정 및 변경할 수 있다. SNMP 인증 정보는, 개별의 디바이스 등록시 SNMP 인증 정보가 설정되지 않은 경우에, 디폴트값으로서 할당된다. 유저 A는 디폴트값으로서의 SNMP 인증 정보의 설정을 의도적으로 생략(설정 없음)할 수 있다. 관리 소프트웨어 UI 디바이스 등록 유닛(501)은, 유저 A로부터 SNMP 인증 정보의 디폴트값 등록 요구를 수신하면, SNMP 인증 정보 입력/출력 유닛(502)에 등록 요구를 발행한다. SNMP 인증 정보 입력/출력 유닛(502)은, SNMP 인증 정보의 디폴트값 등록 요구를 수신하면, 관리 소프트웨어 공통 인증 정보 저장 유닛(503)에 디폴트값으로서의 SNMP 인증 정보를 등록한다. SNMP 인증 정보 입력/출력 유닛(502)은 제1 설정 수단을 구현한다. 관리 소프트웨어 공통 인증 정보 저장 유닛(503)은, 예를 들면 저장 디바이스(408)로 구성된다. 또한, SNMP 인증 정보 입력/출력 유닛(502)은 관리 소프트웨어 공통 인증 정보 저장 유닛(503)을 이용하여 제3 설정 수단을 구현한다.

[0058] 또한, 유저 A는, 관리 소프트웨어 UI 디바이스 등록 유닛(501)을 통해, 관리되어야 하는 디바이스를 SNMP 인증 정보와 함께 등록할 수 있다. 이 때, 디바이스의 IP 어드레스, 디바이스를 고유하게 식별하기 위한 식별 정보(예를 들면, MAC 어드레스) 등도 등록된다. 이러한 처리는 본 발명의 특징과는 직접적으로 관계가 없으며 설명을 생략한다는 점에 유의한다. 여기에서 입력되는 SNMP 인증 정보는 필수 항목이 아니며 항상 등록될 필요는 없다. 관리 디바이스 등록 요구를 수신하면, 관리 소프트웨어 UI 디바이스 등록 유닛(501)은 SNMP 인증 정보 입력/출력 유닛(502)에 디바이스 정보 및 SNMP 인증 정보를 전달한다.

- [0059] SNMP 인증 정보 입력/출력 유닛(502)은 관리 소프트웨어 UI 디바이스 등록 유닛(501)으로부터 디바이스 등록 요구를 수신한다. 등록 요구에 의해 디바이스 정보와 함께 SNMP 인증 정보가 등록되는 경우, SNMP 인증 정보 입력/출력 유닛(502)은 디바이스(100)와 SNMP 인증 정보를 서로 연관시켜 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 등록한다.
- [0060] 디바이스 정보와 함께 SNMP 인증 정보가 등록되지 않는 경우, SNMP 인증 정보 입력/출력 유닛(502)은, 관리 소프트웨어 전체에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값을 관리 소프트웨어 공통 인증 정보 저장 유닛(503)으로부터 취득한다. SNMP 인증 정보 입력/출력 유닛(502)은, 디바이스와 SNMP 인증 정보의 디폴트값을 서로 연관시켜 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 등록한다. 관리 소프트웨어 공통 인증 정보 저장 유닛(503)에 SNMP 인증 정보의 디폴트값이 설정되지 않은 경우, 디바이스(100)는 SNMP 인증 정보 없이 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 등록된다. 관리 소프트웨어 디바이스 정보 저장 유닛(504)은, 예를 들면 저장 디바이스(408)로 구성된다.
- [0061] 관리 소프트웨어 매니저(505)는 독자적인 스케줄 또는 유저의 지시에 기초하여 네트워크를 통해 디바이스(100)로부터 디바이스 관리 정보를 취득한다. 관리 소프트웨어 매니저(505)는 대상 디바이스와 그 SNMP 인증 정보를 관리 소프트웨어 디바이스 정보 저장 유닛(504)으로부터 추출하고, SNMP 클라이언트(512)에 디바이스 관리 정보의 취득 요구를 발행한다. 디바이스(100)에 대응하는 SNMP 인증 정보가 등록되지 않은 경우, 관리 소프트웨어 매니저(505)는 디바이스(100)로부터 SNMP를 이용하여 디바이스 관리 정보를 취득하지 않는다.
- [0062] 다음으로, 플러그인 소프트웨어(520)에 있어서의 SNMP 인증 정보의 관리를 설명한다.
- [0063] 유저 B는, 플러그인 UI 디바이스 등록 유닛(506)을 통해, 관리되어야 하는 디바이스를 SNMP 인증 정보와 함께 등록할 수 있다. 이 때, 디바이스의 IP 어드레스, 디바이스를 고유하게 식별하기 위한 식별 정보(예를 들면, MAC 어드레스) 등도 등록된다. 이러한 처리는 본 발명의 특징과는 직접적으로 관계가 없으며 설명을 생략한다. 여기에서 입력되는 SNMP 인증 정보는 필수 항목이 아니며 항상 등록될 필요는 없다. 관리 디바이스 등록 요구를 수신하면, 플러그인 UI 디바이스 등록 유닛(506)은 SNMP 인증 정보 결정 로직 유닛(507)에 디바이스 정보 및 SNMP 인증 정보를 전달한다.
- [0064] SNMP 인증 정보 결정 로직 유닛(507)은 플러그인 UI 디바이스 등록 유닛(506)으로부터 디바이스 등록 요구를 수신한다. 등록 요구에 의해 디바이스 정보와 함께 SNMP 인증 정보가 등록되는 경우, SNMP 인증 정보 결정 로직 유닛(507)은 디바이스와 SNMP 인증 정보를 서로 연관시켜서 플러그인 SNMP 인증 정보 입력/출력 유닛(508)에 등록 요구를 발행한다. SNMP 인증 정보 결정 로직 유닛은 제2 설정 수단을 구현한다.
- [0065] 디바이스 정보와 함께 SNMP 인증 정보가 등록되지 않는 경우, SNMP 인증 정보 결정 로직 유닛(507)은 SNMP 인증 정보 입력/출력 유닛(502)에 대상 디바이스의 SNMP 인증 정보 요구를 발행한다. 요구의 결과로서 SNMP 인증 정보 입력/출력 유닛(502)으로부터 대상 디바이스의 SNMP 인증 정보가 취득되는 경우, SNMP 인증 정보 결정 로직 유닛(507)은 대상 디바이스와 취득된 SNMP 인증 정보를 서로 연관시킨다. 그리고, SNMP 인증 정보 결정 로직 유닛(507)은 플러그인 SNMP 인증 정보 입력/출력 유닛(508)에 등록 요구를 발행한다.
- [0066] 요구의 결과로서 관리 소프트웨어(500)로부터 SNMP 인증 정보가 취득되지 않은 경우, SNMP 인증 정보 결정 로직 유닛(507)은 플러그인 디폴트 인증 정보 저장 유닛(509)으로부터 플러그인 소프트웨어(520)에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값을 취득한다. 그리고, SNMP 인증 정보 결정 로직 유닛(507)은 디바이스와 SNMP 인증 정보의 디폴트값을 서로 연관시켜서 플러그인 SNMP 인증 정보 입력/출력 유닛(508)에 등록 요구를 발행한다. 플러그인 디폴트 인증 정보 저장 유닛(509)에 저장되어 있는 디폴트값은 미리 정의되어 설정되어 있다는 점에 유의한다. 플러그인 디폴트 인증 정보 저장 유닛(509)은, 예를 들면 저장 디바이스(408)로 구성된다. 이에 의해, 플러그인 디폴트 인증 정보 저장 유닛(509)은 플러그인 소프트웨어(520)에 있어서의 인증 정보 저장 수단을 구현한다.
- [0067] 플러그인 SNMP 인증 정보 입력/출력 유닛(508)은, SNMP 인증 정보와 연관된 디바이스의 등록 요구를 수신하면, 디바이스와 SNMP 인증 정보를 플러그인 SNMP 인증 정보 저장 유닛(510)에 등록한다.
- [0068] 플러그인 매니저(511)는, 독자적인 스케줄 또는 유저의 지시에 기초하여 네트워크를 통해 디바이스(100)로부터 디바이스 관리 정보를 취득한다. 플러그인 매니저(511)는 대상 디바이스와 그 SNMP 인증 정보를 플러그인 SNMP 인증 정보 저장 유닛(510)으로부터 추출하고, SNMP 클라이언트(512)에 디바이스 관리 정보 취득 요구를 발행한다. 플러그인 SNMP 인증 정보 저장 유닛(510)은, 예를 들면 저장 디바이스(408)로 구성된다는 점에 유의한다.

- [0069] 또한, 플러그인 UI 디바이스 등록 유닛(506)은 이미 등록되어 있는 디바이스에 대한 SNMP 인증 정보 갱신 지시를 발행할 수 있다. 본 실시형태에 있어서, SNMP 인증 정보를 갱신하는 방법은 2가지가 있다. 하나의 갱신 방법에서는, 플러그인 소프트웨어(520)가 신규 SNMP 인증 정보를 덮어쓴다. 다른 갱신 방법에서는, 기존의 디바이스와 연관되어 있는 SNMP 인증 정보를 삭제하고, 관리 소프트웨어(500)로부터 SNMP 인증 정보를 취득한다.
- [0070] 플러그인 소프트웨어가 신규 SNMP 인증 정보를 덮어쓰게 하는 갱신 방법은 디바이스 등록시의 처리와 동일하며, 그 설명은 생략한다. 플러그인 소프트웨어(520)가 관리 소프트웨어(500)로부터 SNMP 인증 정보를 취득하게 하는 갱신 방법에서는, 플러그인 UI 디바이스 등록 유닛(506)이 이미 등록되어 있는 디바이스의 SNMP 인증 정보를 갱신하기 위한 요구를 수신한다. 플러그인 UI 디바이스 등록 유닛(506)은, 갱신 요구를 수신하면, 갱신 요구가 관리 소프트웨어(500)로부터 SNMP 인증 정보의 취득을 요구한다는 것과 대상 디바이스 정보를 SNMP 인증 정보 결정 로직 유닛(507)에 통지한다. SNMP 인증 정보 결정 로직 유닛(507)은 SNMP 인증 정보 입력/출력 유닛(502)에 대상 디바이스의 SNMP 인증 정보 취득 요구를 발행한다.
- [0071] 요구의 결과로서 SNMP 인증 정보 입력/출력 유닛(502)으로부터 대상 디바이스의 SNMP 인증 정보가 취득되는 경우, SNMP 인증 정보 결정 로직 유닛(507)은 대상 디바이스와 취득된 SNMP 인증 정보를 서로 연관시킨다. 그리고, SNMP 인증 정보 결정 로직 유닛(507)은 플러그인 SNMP 인증 정보 입력/출력 유닛(508)에 등록 요구를 발행한다. 요구의 결과로서 관리 소프트웨어(500)로부터 SNMP 인증 정보가 취득되지 않은 경우, SNMP 인증 정보 결정 로직 유닛(507)은 현재 등록되어 있는 SNMP 인증 정보를 변경하지 않고 갱신 처리를 종료한다.
- [0072] 관리 소프트웨어(500)의 관리 소프트웨어 디바이스 정보 저장 유닛(504)은 제1 저장 유닛으로서 정의되고, 플러그인 소프트웨어(520)의 플러그인 SNMP 인증 정보 저장 유닛(510)은 제2 저장 유닛으로서 정의된다는 점에 유의한다. 이들 저장 유닛은 소프트웨어 구성의 설명을 위해 분리되었지만, 물리적인 구성의 관점으로부터는 동일한 하드웨어일 수 있다.
- [0073] <관리 소프트웨어의 비휘발성 영역의 구성>
- [0074] 도 6은 도 5에 도시된 관리 소프트웨어 공통 인증 정보 저장 유닛(503)과 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 기록되어 있는 정보의 일부를 도시하는 표이다. 관리 소프트웨어(500)는, SNMP를 이용하여 디바이스로부터 관리 정보 취득하기 위해서, 비휘발성 영역에 저장된 정보를 확인하여, 디바이스에 액세스하기 위한 인증 정보를 취득한다. 비휘발성 영역은, 예를 들면 도 4에 도시된 저장 디바이스(408)로 구성된다.
- [0075] 디바이스 ID(601)는 디바이스(100)를 고유하게 식별하기 위한 식별자이다. 예를 들면, 각각의 디바이스의 시리얼 번호 또는 MAC 어드레스가 이용된다. 이러한 식별자를 이용함으로써, 관리 장치(101)는 디바이스를 고유하게 식별할 수 있다.
- [0076] 커뮤니티명(Community Name)(602)은, 관리 소프트웨어에 의해 네트워크를 통해서 디바이스로부터 관리 정보를 취득하는데 이용되는 SNMP의 인증 정보이다.
- [0077] 타입(Type)(603)은 디바이스 ID(601)와 커뮤니티명(602) 사이의 관계를 나타낸다. 예를 들면, 표 내의 "디바이스 A"의 타입 항목에는 "공통 커뮤니티명"이 기록되어 있다. 이는, 디바이스 A가 등록될 때에, 개별의 SNMP 인증 정보가 지정되지 않고 관리 소프트웨어(500)에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값(public-parent)이 적용된 것을 나타내고 있다.
- [0078] 또한, 표 내의 "디바이스 B"의 타입 항목에는 "개별 커뮤니티명"이 기록되어 있다. 이는, 디바이스 B가 등록될 때에, 개별의 SNMP 인증 정보(dev-group1)가 지정된 것을 나타내고 있다.
- [0079] "디바이스 D"의 커뮤니티명 항목에는 엔트리가 없고, 타입 항목에는 "커뮤니티명 없음"이 기록되어 있다. 이러한 엔트리는, 관리 소프트웨어에 공통으로 이용되는 SNMP 인증 정보의 디폴트값이 설정되어 있지 않을 때에 디바이스를 등록함으로써 작성된다. "디폴트값이 설정되어 있지 않을 때"는 관리 소프트웨어(500)를 관리 장치(101)에 인스톨한 후 디폴트 SNMP 인증 정보를 설정할 때까지의 시간을 가리킨다.
- [0080] 마지막으로, 표 내의 "디폴트 디바이스"의 타입 항목에는 "공통 커뮤니티명"이 기록되어 있다. 이는, 도 5에 도시된 관리 소프트웨어 공통 인증 정보 저장 유닛(503)에 저장되어 있는 정보를 나타내며, 관리 소프트웨어(500)에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값(public-parent)을 나타내고 있다. 이 표에서는, 타입의 정보의 의미를 문자열로 나타내고 있다. 실제로, 정보는 플래그 등을 이용하여 구별되며, 그 설정이 DB에 저장되는 것이 일반적이다.

- [0081] <플러그인 소프트웨어의 비휘발성 영역의 구성>
- [0082] 도 7은 도 5에 도시된 플러그인 디폴트 인증 정보 저장 유닛(509)과 플러그인 SNMP 인증 정보 저장 유닛(510)에 기록되어 있는 정보의 일부를 도시하는 표이다. 플러그인 소프트웨어(520)는, SNMP를 이용하여 디바이스(100)로부터 관리 정보를 취득하기 위해서, 비휘발성 영역에 저장된 정보를 확인하여, 디바이스에 액세스하기 위한 인증 정보를 취득한다. 비휘발성 영역은, 예를 들면 도 4에 도시된 관리 장치(101)의 저장 디바이스(408)로 구성된다.
- [0083] 디바이스 ID(701)와 커뮤니티명(702)의 설명은 도 6에 도시된 디바이스 ID(601)와 커뮤니티명(602)의 설명과 동일하여, 생략한다.
- [0084] 타입(703)은 디바이스 ID(701)와 커뮤니티명(702) 사이의 관계를 나타낸다. 예를 들면, 표 내의 "디바이스 A"의 타입 항목에는 "관리 소프트웨어의 커뮤니티명"이 기록되어 있다. 이는, 플러그인 소프트웨어(520)에 디바이스가 등록될 때에, 플러그인 UI 디바이스 등록 유닛(506)을 통해 SNMP 인증 정보가 지정되지 않고, 관리 소프트웨어 디바이스 정보 저장 유닛(504)에서 관리되고 있는 정보(public-parent)가 취득되는 것을 나타낸다. 표에 "디바이스 B"의 엔트리가 없는 것은, 디바이스 B가 플러그인 소프트웨어(520)의 관리 대상이 아니기 때문이다. 이는, 관리 소프트웨어(500)와 플러그인 소프트웨어(520) 각각이 관리 대상 디바이스를 선택할 수 있다는 것을 의미한다.
- [0085] 표 내의 "디바이스 C"의 타입 항목에는 "플러그인에 대해 개별인 커뮤니티명"이 기재되어 있다. 이는, 플러그인 소프트웨어(520)에 디바이스가 등록될 때, SNMP 인증 정보가 지정되지 않고, 관리 소프트웨어(500)에서도 인증 정보를 관리하지 않기 때문에, 플러그인 소프트웨어(520)가 관리하고 있는 SNMP 인증 정보의 디폴트값(maintenance-group1)이 적용된 것을 의미한다.
- [0086] 마지막으로, 표 내의 "디폴트 디바이스"의 타입 항목에는 "플러그인에 대해 공통인 커뮤니티명"이 기록된다. 이는 도 5에 도시된 플러그인 디폴트 인증 정보 저장 유닛(509)에 저장되어 있는 정보가, 플러그인 소프트웨어(520)에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값(public-plugin)임을 나타낸다. 또한 이러한 표에서는, 타입 항목의 정보의 의미를 도 6과 같이 문자열로 나타내고 있다. 실제로는, 이러한 정보는 플래그 등을 이용하여 구별되고, 그 설정이 DB에 저장된다.
- [0087] <플러그인 소프트웨어의 비휘발성 영역의 구성>
- [0088] 도 8은, 도 5에 도시된 플러그인 디폴트 인증 정보 저장 유닛(509)과 플러그인 SNMP 인증 정보 저장 유닛(510)에 기록되어 있는 정보의 일부를 나타내는 표이다. 플러그인 소프트웨어(520)는, 디바이스 등록시에 SNMP 인증 정보가 지정되지 않으면, 관리 소프트웨어(500)의 SNMP 인증 정보를 참조하여, 대상 디바이스와 SNMP 인증 정보를 서로 연관시켜 저장한다. 그러나, 관리 소프트웨어(500)에서 SNMP 인증 정보가 갱신되었을 경우, 플러그인 소프트웨어(520)를 사용하는 유저가 다르기 때문에 플러그인 소프트웨어(520)에서 자동 갱신은 행해지지 않는다. 따라서, 디바이스(100) 및 관리 소프트웨어(500)에서 SNMP 인증 정보가 갱신되었을 경우, 플러그인 소프트웨어(520)는 통신을 행할 수 없다. 이러한 문제를 회피하기 위해서, 유저 B가 커뮤니티명의 취득 갱신 지시를 발행하면, 플러그인 소프트웨어(520)는 지정한 디바이스의 커뮤니티명을 관리 소프트웨어(500)로부터 재차 요구한다.
- [0089] 예를 들면, 유저 B가 도 7에 도시된 상태에서 표 내의 "디바이스 C"의 커뮤니티명을 취득하여 갱신할 것을 지시하면, 플러그인 소프트웨어는 도 5의 관리 소프트웨어(500)에서 관리되는 "디바이스 C"의 커뮤니티명을 취득한다. "디바이스 C"의 커뮤니티명 항목의 정보의 취득이 성공하면, 플러그인 소프트웨어(520)는, 도 7의 "디바이스 C"에서 나타난 바와 같이 도 7의 "maintenance-group1"으로부터 도 8의 "dev-group1"로 커뮤니티명 항목을 갱신한다. 커뮤니티명 항목의 정보가 관리 소프트웨어(500)로부터 취득될 수 없으면, 플러그인 소프트웨어(520)는 관리 소프트웨어(500)가 갱신된 정보를 저장할 수 없기 때문에, 관리하의 커뮤니티명 항목의 정보를 계속 사용한다.
- [0090] <관리 소프트웨어의 동작예>
- [0091] 본 실시형태에 따른 관리 소프트웨어(500)의 동작예를 상술한 구성에 기초하여 설명한다.
- [0092] 도 9는 관리 소프트웨어(500)에 디바이스(100)를 등록할 때에, 디바이스와 커뮤니티명을 연관시킬 때까지의 처리를 도시하는 플로우차트이다. 이러한 플로우차트의 처리는, 도 4에 도시된 ROM(403)과 저장 디바이스(408) 중 하나의 저장 수단에 저장된 프로그램을 필요에 따라 RAM(404)에 전개하고, CPU(402)에 의해 이를 실행함으로써

써 구현된다. 여기에 도시된 플로우차트의 처리는 도 5에 도시된 관리 소프트웨어(500)의 처리를 나타낸다.

- [0093] 도 9를 참조하면, 사용자가 관리 소프트웨어(500)의 디바이스 등록 화면을 요구하면, 플로우차트의 처리가 개시된다. 관리 소프트웨어(500)는, 스텝 S901에서 디바이스 등록 요구를 수신했는지 여부를 판정한다. 디바이스 등록 요구를 수신했으면(스텝 S901에서, 예), 처리는 스텝 S901로부터 스텝 S902로 진행한다.
- [0094] 관리 소프트웨어(500)는, 스텝 S902에서 디바이스 등록 요구의 상세 정보를 확인한다. 디바이스 등록 요구의 상세 정보에 SNMP 인증 정보가 지정되어 있는 경우(스텝 S902에서, 예), 처리는 스텝 S902로부터 스텝 S903으로 진행한다. 또한, 디바이스 등록 요구의 상세 정보에 SNMP 인증 정보가 지정되지 않은 경우(스텝 S902에서, 아니오), 처리는 스텝 S902로부터 스텝 S904로 진행한다.
- [0095] 관리 소프트웨어(500)는, 스텝 S903에서 등록 대상의 디바이스와 지정된 SNMP 인증 정보를 연관시키고, 도 5에 도시된 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 디바이스와 SNMP 인증 정보를 저장하고, 처리를 종료한다.
- [0096] 관리 소프트웨어(500)는, 스텝 S904에서 관리 소프트웨어에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값이 설정되어 있는지의 여부를 확인한다. 관리 소프트웨어에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값이 설정되어 있으면(스텝 S904에서, 예), 처리는 스텝 S904로부터 스텝 S905로 진행한다. 관리 소프트웨어에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값이 설정되지 않은 경우에는(S904에서, 아니오), 처리는 S904로부터 S906으로 진행한다.
- [0097] 관리 소프트웨어(500)는, 스텝 S905에서 등록 대상의 디바이스와, 관리 소프트웨어에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값을 연관시키고, 도 5에 도시된 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 디바이스와 SNMP 인증 정보를 저장하고, 처리를 종료한다.
- [0098] 관리 소프트웨어(500)는, 스텝 S906에서 등록 대상 디바이스에 연관되어야 할 SNMP의 인증 정보 없이, 도 5에 도시된 관리 소프트웨어 디바이스 정보 저장 유닛(504)에 디바이스 정보만을 저장하고, 처리를 종료한다.
- [0099] <플러그인 소프트웨어의 디바이스 등록에 있어서의 동작예>
- [0100] 상술한 구성에 기초하여, 본 실시형태에 따른 플러그인 소프트웨어(520)의 디바이스 등록에 있어서의 동작예를 설명한다.
- [0101] 도 10은, 플러그인 소프트웨어(520)에 디바이스(100)를 등록할 때, 디바이스와 커뮤니티명을 연관시킬 때까지의 처리를 도시하는 플로우차트이다. 이 플로우차트의 처리는, 도 4에 도시된 ROM(403)과 저장 디바이스(408) 중 하나의 저장 수단에 저장된 프로그램을 필요에 따라 RAM(404)에 전개하고, CPU(402)에 의해 이를 실행시킴으로써 구현된다. 여기에 도시된 플로우차트의 처리는, 도 5에 도시된 플러그인 소프트웨어(520)의 처리를 나타낸다.
- [0102] 도 10을 참조하면, 사용자가 플러그인 소프트웨어(520)의 디바이스 등록 화면을 요구하면, 플로우차트의 처리가 개시된다. 플러그인 소프트웨어(520)는, 스텝 S1001에서 디바이스 등록 요구를 수신했는지 여부를 판정한다. 디바이스 등록 요구를 수신했으면(스텝 S1001에서, 예), 처리는 스텝 S1001로부터 스텝 S1002로 진행한다.
- [0103] 플러그인 소프트웨어(520)는, 스텝 S1002에서 디바이스 등록 요구의 상세 정보를 확인한다. 디바이스 등록 요구의 상세 정보에 SNMP 인증 정보가 지정되어 있으면(스텝 S1002에서, 예), 처리는 스텝 S1002로부터 스텝 S1003으로 진행한다. 디바이스 등록 요구의 상세 정보에 SNMP 인증 정보가 지정되지 않았으면(스텝 S1002에서, 아니오), 처리는 스텝 S1002로부터 스텝 S1004로 진행한다.
- [0104] 플러그인 소프트웨어(520)는, 스텝 S1003에서 등록 대상 디바이스와 지정된 SNMP 인증 정보를 연관시키고, 도 5에 도시된 플러그인 SNMP 인증 정보 저장 유닛(510)에 디바이스와 SNMP 인증 정보를 저장하고, 처리를 종료한다.
- [0105] 플러그인 소프트웨어(520)는, 스텝 S1004에서 등록 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어(500)에 등록되어 있는지 여부를 확인한다. 등록 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어에 이미 등록되어 있는 경우(스텝 S1004에서, 예), 처리는 스텝 S1004로부터 스텝 S1005로 진행한다. 등록 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어에 등록되지 않은 경우(스텝 S1004에서, 아니오), 처리는 스텝 S1004로부터 스텝 S1006으로 진행한다. 스텝 S1004에서, SNMP 인증 정보가 관리 소프트웨어(500)에 등록되어 있어도, 해당 SNMP 인증 정보를 취득할 수 없을 경우에는, "아니오"로 판정을 종료한다는 점에 유의한다.

- [0106] 플러그인 소프트웨어(520)는, 스텝 S1005에서 등록 대상 디바이스와, 관리 소프트웨어(500)에 등록되어 있는 등록 대상 디바이스의 SNMP 인증 정보를 연관시킨다. 그리고, 플러그인 소프트웨어(520)는 도 5에 도시된 플러그인 SNMP 인증 정보 저장 유닛(510)에 디바이스와 SNMP 인증 정보를 저장하고, 처리를 종료한다.
- [0107] 플러그인 소프트웨어(520)는, 스텝 S1006에서 등록 대상의 디바이스와, 플러그인 소프트웨어(520)에서 공통으로 이용되는 SNMP 인증 정보의 디폴트값을 연관시킨다. 그리고, 플러그인 소프트웨어(520)는 도 5에 도시된 플러그인 SNMP 인증 정보 저장 유닛(510)에 디바이스와 SNMP의 인증 정보를 저장하고, 처리를 종료한다.
- [0108] 상술한 바와 같이, 관리 소프트웨어에 저장되는 정보에 따라, 플러그인 소프트웨어의 SNMP 인증 정보의 등록 우선 순위를 설정하면, 이하의 경우에 있어서의 인증 정보 관리가 적절하게 행해질 수 있다. 즉, 본 실시형태에서 SNMP 인증 정보는 (1) 플러그인 설정 화면 등을 통해 지정된 커뮤니티명(유저 등에 의해 지정된 디바이스의 커뮤니티명), (2) 관리 소프트웨어에 저장된 커뮤니티명, (3) 플러그인 소프트웨어의 디폴트(공통) 커뮤니티명의 우선 순위에 기초하여 플러그인 소프트웨어에 설정된다.
- [0109] SNMP 인증 정보는 (1) 관리 소프트웨어의 커뮤니티명(유저 등에 의해 지정된 디바이스의 커뮤니티명, (2) 관리 소프트웨어의 (공통) 커뮤니티명, (3) 설정 없음의 우선 순위에 기초하여 관리 소프트웨어에 설정된다.
- [0110] 예를 들면, 엄격한 시큐리티 제어 하의 기업을 가정한다. 관리 소프트웨어와 플러그인 소프트웨어는 다른 유저에 의해 사용되고 독립적으로 디바이스를 관리한다. 이와 같은 경우, 각각의 소프트웨어는 하나의 디바이스에 대하여 개별의 SNMP 인증 정보를 정의하여 관리할 수 있다. 이에 의해, 관리 소프트웨어와 플러그인 소프트웨어의 독립성을 유지하고, 높은 시큐리티 제어를 보장하게 한다.
- [0111] 한편, 디바이스의 엄격한 시큐리티 제어가 불필요하다고 판단되는 기업이 있다. 이와 같은 경우는, 디바이스에 대해 하나의 SNMP 인증 정보(예를 들면 "public")가 설정된다. 관리 소프트웨어에서 SNMP 인증 정보의 디폴트값을 설정한다. 이 설정에 의해, 관리 소프트웨어 및 플러그인 소프트웨어에 개별적으로 SNMP 인증 정보를 입력하지 않고 디폴트 SNMP 인증 정보를 공통으로 이용할 수 있도록 된다.
- [0112] 각각의 소프트웨어는, 각각의 디바이스에 대하여 SNMP의 인증 정보의 디폴트값을 이용할지 개별의 설정값을 이용할지 여부를 결정할 수 있다. 따라서, 그 때 상황에 따라서 SNMP의 인증 정보를 선택적으로 사용할 수 있다.
- [0113] <플러그인 소프트웨어의 SNMP 인증 정보 갱신에 있어서의 동작예>
- [0114] 상술한 구성에 기초하여, 본 실시형태에 따른 플러그인 소프트웨어(520)의 SNMP 인증 정보 갱신에 있어서의 동작예를 설명한다.
- [0115] 도 11은 플러그인 소프트웨어(520)에 등록된 디바이스(100)의 SNMP 인증 정보를 갱신할 때에, 디바이스와 커뮤니티명을 연관시킬 때까지의 처리를 도시하는 플로우차트이다. 이 플로우차트의 처리는 도 4에 도시된 ROM(403) 및 저장 디바이스(408) 중 하나의 저장 수단에 저장된 프로그램을 필요에 따라 RAM(404)에 전개하고, CPU(402)에 의해 이를 실행함으로써 구현된다. 여기에 도시된 플로우차트의 처리는 도 5에 도시된 플러그인 소프트웨어(520)의 처리를 나타낸다.
- [0116] 도 11을 참조하면, 유저가 플러그인 소프트웨어(520)에 등록되어 있는 디바이스용 SNMP 인증 정보 갱신 화면을 요구하면, 플로우차트의 처리가 개시된다. 플러그인 소프트웨어(520)는, 스텝 S1101에서 예를 들면, 조작 유닛 UI(306)를 통해서 유저로부터 관리하의 디바이스의 SNMP 인증 정보의 갱신 요구를 수신했는지 여부를 판정한다. SNMP 인증 정보의 갱신 요구를 수신하면(스텝 S1101에서, 예), 처리는 스텝 S1101로부터 스텝 S1102로 진행한다.
- [0117] 플러그인 소프트웨어(520)는, 스텝 S1102에서 갱신 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어(500)에 등록되어 있는지의 여부를 확인한다. 갱신 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어(500)에 등록되어 있을 경우(스텝 S1102에서, 예), 처리는 스텝 S1102로부터 스텝 S1103으로 진행한다. 갱신 대상 디바이스의 SNMP 인증 정보가 관리 소프트웨어(500)에 등록되지 않은 경우(스텝 S1102에서, 아니오), 처리는 스텝 S1102로부터 스텝 S1104로 진행한다.
- [0118] 플러그인 소프트웨어(520)는, 스텝 S1103에서 갱신 대상 디바이스와, 관리 소프트웨어(500)에 등록되어 있는 갱신 대상 디바이스의 SNMP 인증 정보를 연관시킨다. 그리고, 플러그인 소프트웨어(520)는 도 5에 도시된 플러그인 SNMP 인증 정보 저장 유닛(510)에 디바이스의 정보와 SNMP 인증 정보를 저장하고, 처리를 종료한다.
- [0119] 플러그인 소프트웨어(520)는, 스텝 S1104에서 SNMP 인증 정보를 변경하지 않고 그대로 처리를 종료한다.

- [0120] <플러그인 소프트웨어의 디바이스 등록에 있어서의 유저 인터페이스 예>
- [0121] 도 12a 내지 도 12c는 플러그인 소프트웨어(520)의 디바이스(100)용 등록 화면에서의 디바이스 등록 방법을 도시한다. 플러그인 소프트웨어(520)가 관리 소프트웨어(500)에 등록된 디바이스를 플러그인 소프트웨어(520)의 관리 대상으로 설정하는 경우의 표시 방법의 일례에 대해서 도 12a 내지 도 12c를 이용하여 설명한다.
- [0122] 도 12a는 플러그인 소프트웨어(520)의 디바이스 등록 화면의 예를 도시한다. 이러한 화면은 도 5에 도시된 플러그인 UI 디바이스 등록 유닛(506)에 의해 유저에게 제공된다. 유저는 화면에 직접 디바이스 정보를 입력해서 디바이스 등록을 행할 수 있다. 유저는 관리 소프트웨어(500)에 등록되어 있는 디바이스를 참조하기 위해, 도 12a의 상부의 "디바이스 리스트로부터 추가" 버튼(1201)을 누른다. 이어서, 표시는 도 12b에 도시된 화면으로 천이한다.
- [0123] 도 12b는 관리 소프트웨어(500)의 디바이스 리스트를 표시하는 화면의 예를 도시한다. 플러그인 소프트웨어(520)의 유저는, 이 디바이스 리스트에서 관리 대상 디바이스를 체크 박스를 이용하여 선택하고 결정한다. 유저가 화면 하부의 "추가" 버튼(1202)을 누르면, 표시는 도 12c에 도시된 화면으로 천이한다. 디바이스 리스트의 상측의 2개의 디바이스가 선택된 것으로 가정하여 설명한다.
- [0124] 도 12c는 플러그인 소프트웨어(520)의 원래의 디바이스 등록 화면의 예를 도시한다. 화면 구성은 도 12b에서 선택된 디바이스가 이미 등록된 디바이스로 표시된다는 점을 제외하고는 도 12a와 동일하다. 디바이스의 SNMP 인증 정보로서 제공되는 커뮤니티명의 설정값(1203)으로서, 관리 소프트웨어의 정보를 참조하고 있지만, 유저에게는 구체적인 값은 표시되지 않는다. 이는 동일한 설정값이 사용되더라도 구체적인 값을 유저가 인식하는 것을 방지하기 위해서이다. SNMP 인증 정보를 변경할 때, 유저는 이 화면의 인증 정보를 편집할 수 있다. 디바이스 정보가 완료되면, 유저는 화면 하부의 "추가" 버튼(1204)을 눌러서 플러그인 소프트웨어(520)의 디바이스 등록을 완료한다.
- [0125] 상술한 바와 같이 플러그인 소프트웨어의 유저는, 관리 소프트웨어에 등록된 디바이스의 SNMP 인증 정보를 이용할 수 있다. 유저가 SNMP 인증 정보를 그/그녀 자신에게 지정하고 싶을 경우에는, 그/그녀는 우선적으로 SNMP 인증 정보를 편집할 수 있다.
- [0126] <플러그인 소프트웨어의 SNMP 인증 정보 표시에 있어서의 유저 인터페이스의 예>
- [0127] 도 13a 및 도 13b는, 플러그인 소프트웨어(520)의 디바이스(100)의 SNMP 인증 정보를 표시하는 방법을 도시한다. 플러그인 소프트웨어(520)가 관리 소프트웨어(500)로부터 취득된 디바이스의 SNMP 인증 정보를 표시하는 방법과, 플러그인 소프트웨어(520)의 관리 화면으로부터 직접 입력된 디바이스의 SNMP 인증 정보를 표시하는 방법에는 차이가 있다고 생각된다.
- [0128] 도 13a는 플러그인 소프트웨어(520)에서 관리되는 디바이스의 상세 정보 표시 화면의 일례를 도시한다. 이 디바이스의 SNMP 인증 정보는 관리 소프트웨어(500)를 참조함으로써 설정된다. 이 디바이스의 SNMP 인증 정보(1301)(도 13a의 SNMP 커뮤니티명)로서 문자열 "(set)"이 표시되고, 실제의 인증 정보는 표시하지 않는다.
- [0129] 도 13b는 유사하게 플러그인 소프트웨어(520)에서 관리되는 디바이스의 상세 정보의 표시 화면의 일례를 도시한다. 이 디바이스의 SNMP 인증 정보는 플러그인 소프트웨어(520)의 UI를 통해 설정된다. 이 디바이스의 SNMP 인증 정보(1302)(도 13b의 SNMP 커뮤니티명)로서, 실제로 입력한 문자열(본 예에서는, "maintenance-group1")이 표시된다.
- [0130] 이는, 플러그인 소프트웨어(520)의 유저가 SNMP 인증 정보를 알지 못하더라도, SNMP 인증 정보가 관리 소프트웨어(500)에 설정되어 있는 한, 관리 소프트웨어(500)와 같은 디바이스로부터 정보를 취득하는 것을 가능하게 한다.
- [0131] 또한, 플러그인 소프트웨어(520)의 유저에게 시큐리티 정보, 즉 SNMP 인증 정보를 통지하지 않고 디바이스로부터 정보를 취득할 수 있다. 예를 들어, 관리 소프트웨어(500)의 유저가 시스템 관리자이며, 플러그인 소프트웨어(520)의 유저가 유지 보수를 맡은 서비스맨으로, 유저가 상이한 경우를 가정한다. 이러한 경우에는, 시스템 관리자는 인증 정보를 공유하지 않고 액세스 권한을 공유할 수 있다.
- [0132] <디바이스 커뮤니티명의 자동 갱신 처리>
- [0133] 상술한 구성에 기초하여, 본 실시형태에 따른 플러그인 소프트웨어(520)와 디바이스(100) 사이의 통신의 동작예를 설명한다.

- [0134] 도 14는, 플러그인 소프트웨어(520)와 디바이스(100)가 통신하는 경우, 통신 대상인 디바이스(100)의 커뮤니티명을 자동으로 갱신하는 처리를 도시하는 플로우차트이다. 이 플로우차트의 처리는, 도 4에 도시된 ROM(403) 및 저장 디바이스(408) 중 하나의 저장 수단에 저장된 프로그램을 필요에 따라 RAM(404)에 전개하고, CPU(402)에 의해 실행함으로써 구현된다. 여기에 도시된 플로우차트의 처리는 도 5에 도시된 플러그인 소프트웨어(520)의 처리를 나타낸다.
- [0135] 플러그인 소프트웨어(520)의 플러그인 매니저(511)는, 미리 정의된 독자적인 스케줄 또는 유저 지시에 기초하여, 네트워크(102)를 통해 디바이스(100)로부터 디바이스 관리 정보를 취득하기 위해서 통신을 행한다. 이러한 통신의 처리 수준은 도 14에 도시된다. 이하의 설명에 있어서, 플러그인 소프트웨어(520) 자신의 SNMP 인증 정보는 "SNMP 인증 정보 X"로 지칭하고, 관리 소프트웨어(500)에 등록된 디바이스의 SNMP 인증 정보는 "SNMP 인증 정보 Y"로 지칭한다는 점에 유의한다.
- [0136] 플러그인 소프트웨어(520)와 디바이스(100) 사이의 통신 처리가 개시되면, 도 14에 도시된 플로우차트의 처리가 개시된다. 플러그인 소프트웨어(520)는, 스텝 S1401에서, 예를 들면 스케줄 송신 또는 유저 지시에 의해 트리거되어, 플러그인 소프트웨어(520) 자신의 SNMP 인증 정보 X를 이용하여 디바이스(100)와 통신한다.
- [0137] 통신 처리가 실패하면(스텝 S1402에서, 예), 처리는 스텝 S1403으로 진행한다. 통신 처리가 성공하면(스텝 S1402에서, 아니오), 플러그인 소프트웨어(520)는 SNMP 인증 정보를 변경하지 않고 이러한 수순을 종료한다. 스텝 S1402의 통신의 성공 또는 실패 판정시에, SNMP 인증 정보 이외의 원인에 기인하여 에러가 발생하면, 플러그인 소프트웨어(520)는 통신 성공으로 판정하고(스텝 S1402에서, 아니오), SNMP 인증 정보를 변경하지 않고, 이러한 수순을 종료한다.
- [0138] 스텝 S1403에서, 플러그인 소프트웨어(520)는 통신 대상 디바이스의 SNMP 인증 정보 Y를 관리 소프트웨어(500)로부터 취득한다. 스텝 S1404에서, 플러그인 소프트웨어(520)는 SNMP 인증 정보 Y가 관리 소프트웨어(500)에 등록되고, 스텝 S1401에서 통신에 사용한 SNMP 인증 정보 X와 SNMP 인증 정보 Y가 상이한지 여부를 판정한다. SNMP 인증 정보 Y가 관리 소프트웨어(500)에 등록되고, SNMP 인증 정보 X와 상이한 경우(스텝 S1404에서, 예), 처리는 스텝 S1405로 진행한다. 그 외의 경우에는(스텝 S1404에서, 아니오), 플러그인 소프트웨어(520)는 SNMP 인증 정보 X의 값을 변경하지 않고, 이러한 수순을 종료한다. 통신 대상 디바이스의 SNMP 인증 정보 Y가 관리 소프트웨어(500)에 등록되지 않은 경우에는, 스텝 S1403에서 SNMP 인증 정보 Y를 취득할 수 없다는 점에 유의한다.
- [0139] 스텝 S1405에서, 플러그인 소프트웨어(520)는 스텝 S1403에서 취득된 SNMP 인증 정보 Y를 사용하여 통신 대상인 디바이스(100)와 통신한다. 통신 내용으로서, 예를 들면, 스텝 S1401에서 실행된 통신 데이터의 재송을 행한다. 통신 처리가 성공하면(스텝 S1406에서, 예), 처리는 스텝 S1407로 진행한다. 통신 처리가 실패하면(스텝 S1406에서, 아니오), 이러한 수순을 종료한다.
- [0140] 스텝 S1407에서는, 플러그인 소프트웨어(520)는 도 5에 도시된 플러그인 SNMP 인증 정보 저장 유닛(510)에 관리 소프트웨어(500)로부터 취득된 SNMP 인증 정보 Y를 저장한다. 그리고, 이러한 수순을 종료한다.
- [0141] 본 실시형태에서는, 최초의 통신 실패 후 관리 소프트웨어(500)의 SNMP 인증 정보 Y를 이용하는 통신 시도(스텝 S1405)가 1회 행해진다는 점에 유의한다. 그러나, 이러한 시도는 복수 회 행해질 수 있다.
- [0142] 본 실시형태에서는, 최초의 통신후 재송 처리시에, 관리 소프트웨어(500)의 SNMP 인증 정보 Y를 이용하여 통신 시도(스텝 S1405)가 행해진다. 그러나, 이러한 시도는 다른 타이밍에서 실시될 수 있다. 이 경우, 플러그인 소프트웨어(520)는 통신 결과를 저장하고, 예를 들어 소정 간격의 정기 처리에서 그 통신 결과를 참조하여, 관리 소프트웨어(500)의 SNMP 인증 정보 Y를 이용한 통신을 시도할지 여부를 판정한다. 여기서 시도되는 통신 내용은 이전에 실패한 통신과 동일한 것일 수 있다. 대안적으로는, 통신 테스트용의 소량의 데이터를 이용한 데이터 통신이 행해질 수 있다.
- [0143] 본 실시형태에서는, 플러그인 소프트웨어(520)의 SNMP 인증 정보를 갱신할 때, 통신 실패에 의해 트리거되어, 관리 소프트웨어(500)의 SNMP 인증 정보가 통신에 성공하는 유효 인증 정보일 때에만 SNMP 인증 정보는 자동으로 갱신된다. 그 때문에, 유저의 SNMP 인증 정보 갱신 지시는 불필요해지고, 관리 소프트웨어(500)의 SNMP 인증 정보 설정 에러의 경우에도 무효한 값이 저장되는 것을 방지할 수 있다.
- [0144] 상술한 실시형태는 디바이스 관리를 위한 인증 정보로서 SNMP 인증 정보를 이용하는 것을 설명하였다. 그러나, 프로토콜은 SNMP로 한정되지 않고, 임의의 다른 인증 정보가 사용 가능하다. HTTP(HyperText Transfer

Protocol)를 이용하는 기본 인증 또는 다른 프로토콜의 인증 정보가 적용될 수 있다.

[0145] 또한, 관리 소프트웨어에서 개별로 SNMP 인증 정보를 설정하지 않는 경우, 관리 소프트웨어 공통의 SNMP 인증 정보가 설정된다. 그러나, 관리 소프트웨어는 공통 SNMP 인증 정보를 설정하는 수단을 항상 가질 필요는 없다.

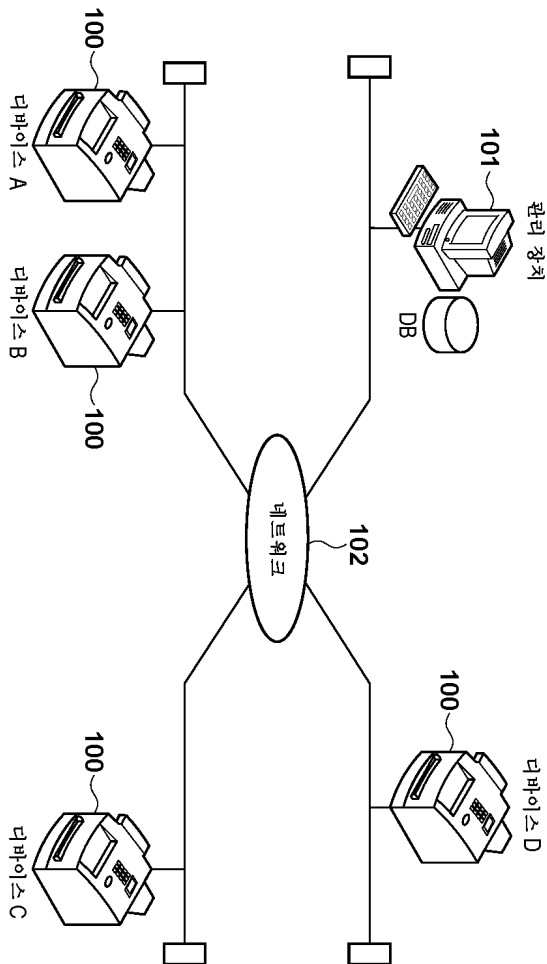
[0146] 본 실시형태에서, SNMP 버전 1이 이용된다. 그러나, 버전은 이에 한정되지 않고, 임의의 다른 버전의 SNMP가 적용 가능하다. 예를 들어, SNMP 버전 3의 유저명과 패스워드가 SNMP 인증 정보로서 이용될 수 있다.

[0147] 본 발명의 양태는 또한 상술한 실시형태(들)의 기능을 행하기 위해 메모리 디바이스에 기록된 프로그램을 판독하여 실행하는 시스템 또는 장치의 컴퓨터(또는 CPU 또는 MPU와 같은 디바이스)에 의해 구현될 수 있고, 상술한 실시형태(들)의 기능을 행하기 위해 예를 들어 메모리 디바이스에 기록된 프로그램을 판독하고 실행함으로써 시스템 또는 장치의 컴퓨터에 의해 단계들이 행해지는 방법에 의해 구현될 수 있다. 이를 위해, 프로그램은 예를 들어 메모리 디바이스(예를 들어, 컴퓨터 판독가능한 매체)로서 제공되는 다양한 종류의 기록 매체로부터 또는 네트워크를 통해 컴퓨터에 제공될 수 있다.

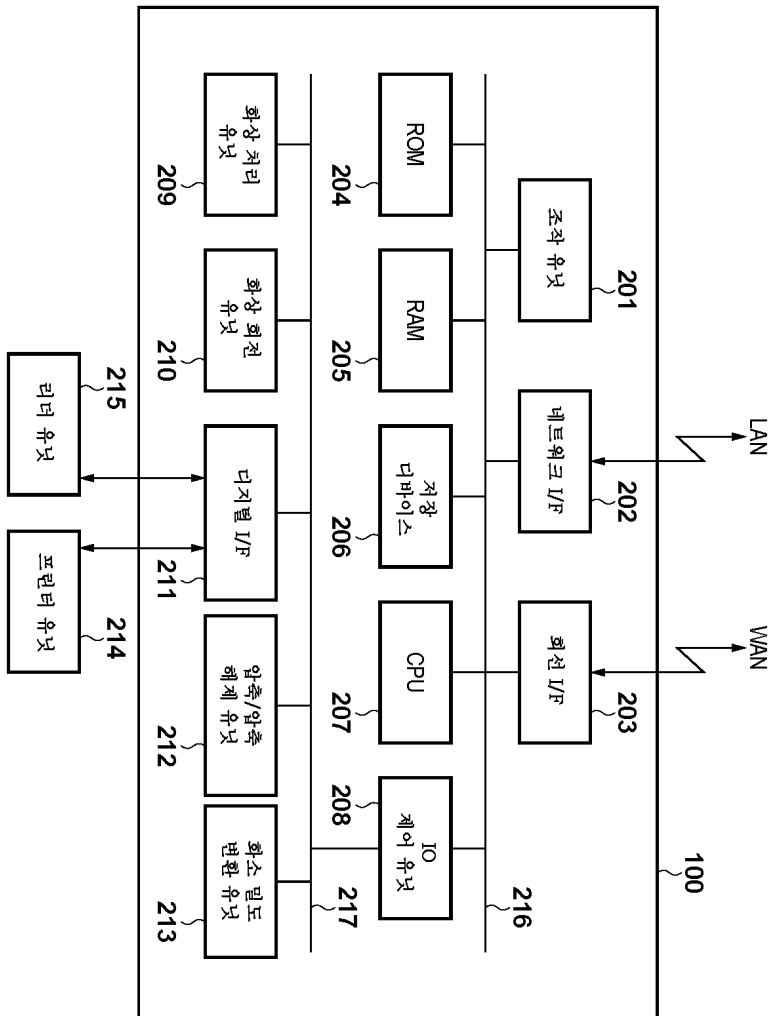
[0148] 본 발명은 예시적인 실시형태를 참조하여 설명되었지만, 본 발명은 개시된 예시적인 실시형태에 의해 제한되지 않는다는 점이 이해될 것이다. 이하의 청구범위의 범주는 이러한 모든 변경, 등가 구조 및 기능을 포함하도록 광의의 해석에 따라야 한다.

도면

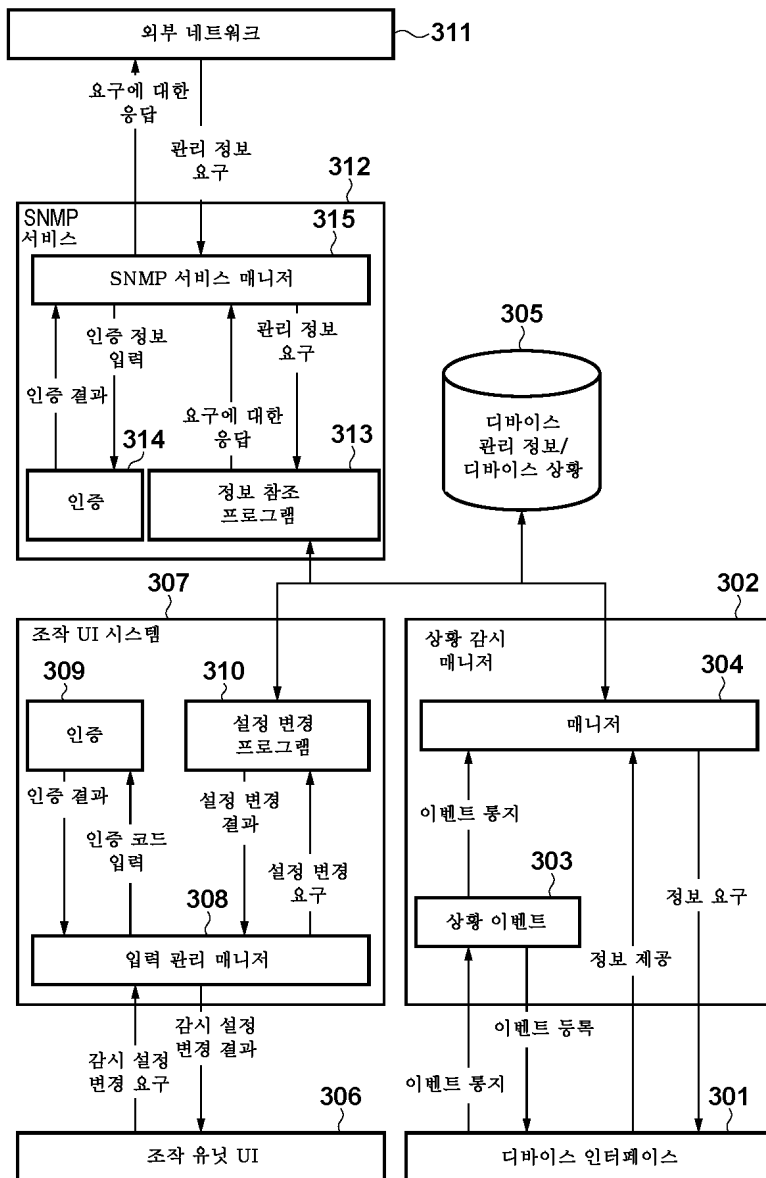
도면1



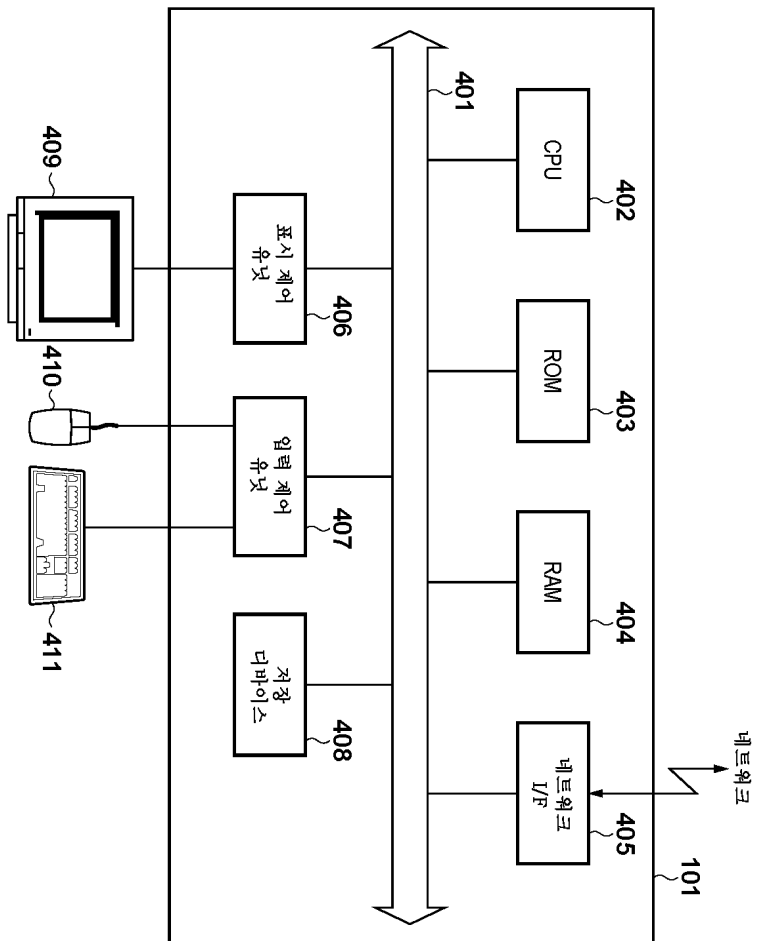
도면2



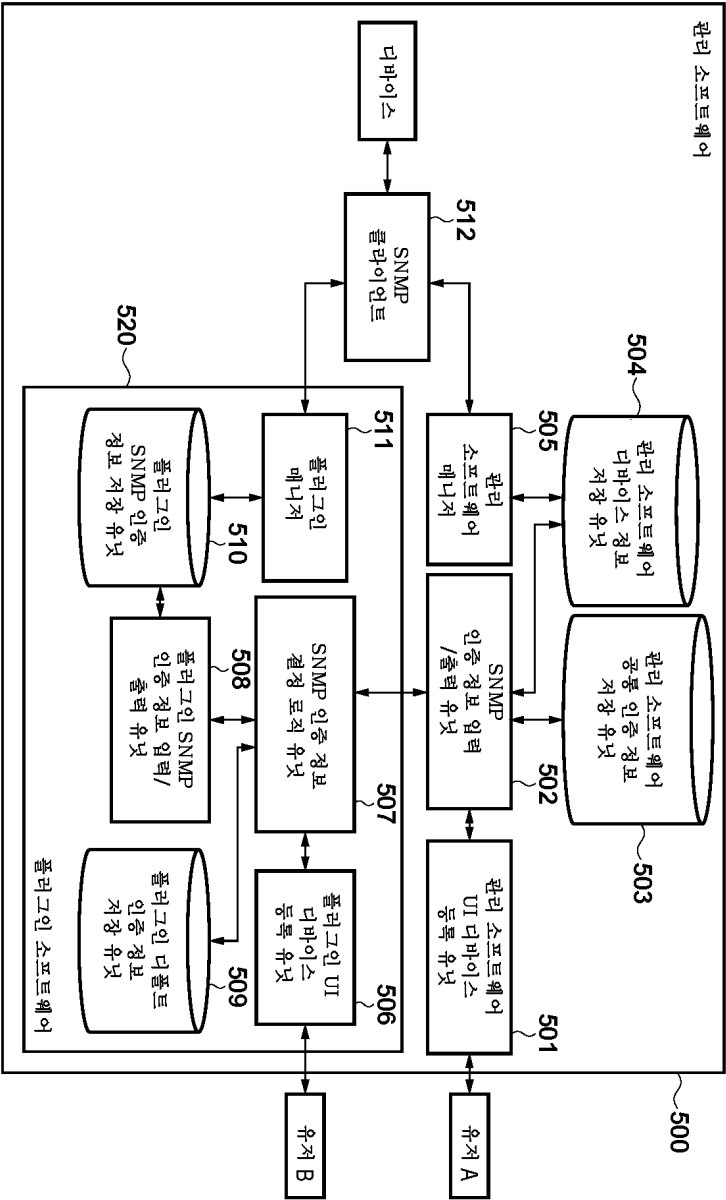
도면3



도면4



도면5



도면6

601	602	603
장치 ID	커뮤니티명	타입
장치 A	public-parent	공통 커뮤니티명
장치 B	dev-group1	개별 커뮤니티명
장치 C	dev-group1	개별 커뮤니티명
장치 D		커뮤니티명 없음
...	...	...
장치 X	dev-groupZ	개별 커뮤니티명
디폴트 장치	public-parent	공통 커뮤니티명

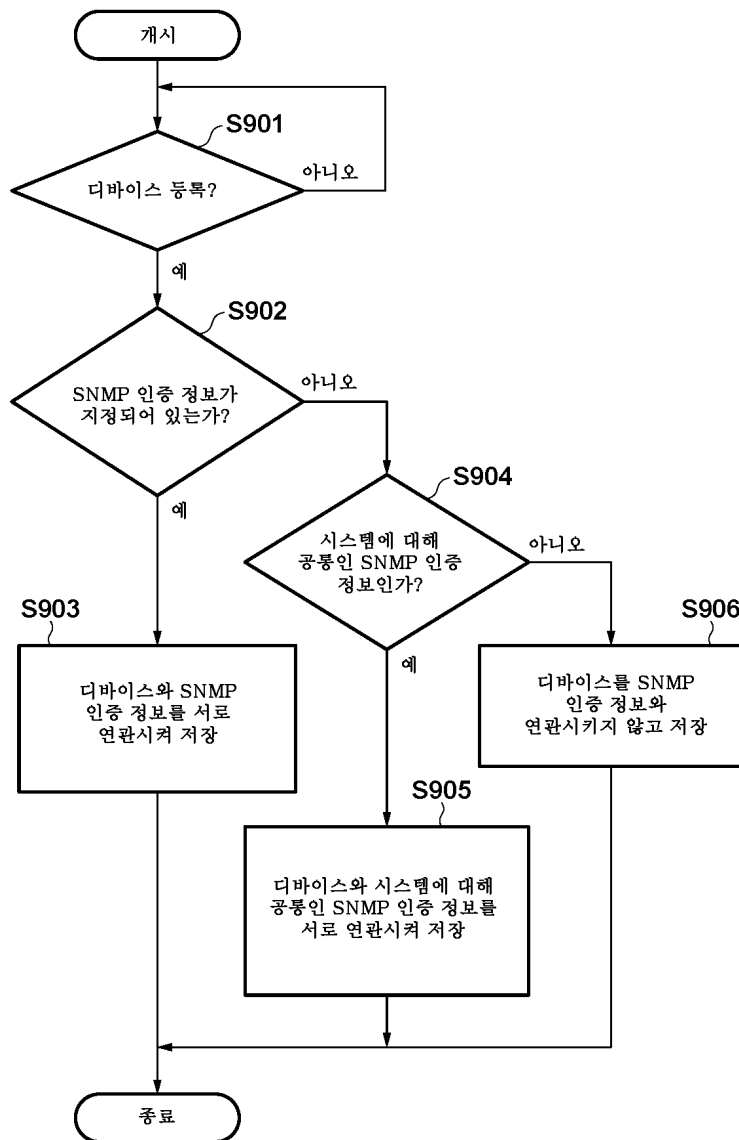
도면7

701		702	703
커뮤니티명		타입	
더바이스 ID	커뮤니티명	관리 소프트웨어의 커뮤니티명을 취득	
더바이스 A	public-parent	플러그인에 대해 개별인 커뮤니티명을 부여	
더바이스 C	maintenance-group1	플러그인에 대해 공통인 커뮤니티명을 취득	
더바이스 D	public-plugin	...	
...	...	관리 소프트웨어의 커뮤니티명을 취득	
더바이스 X	dev-groupZ	플러그인에 대해 공통인 커뮤니티명	
더폴트 더바이스	public-plugin		

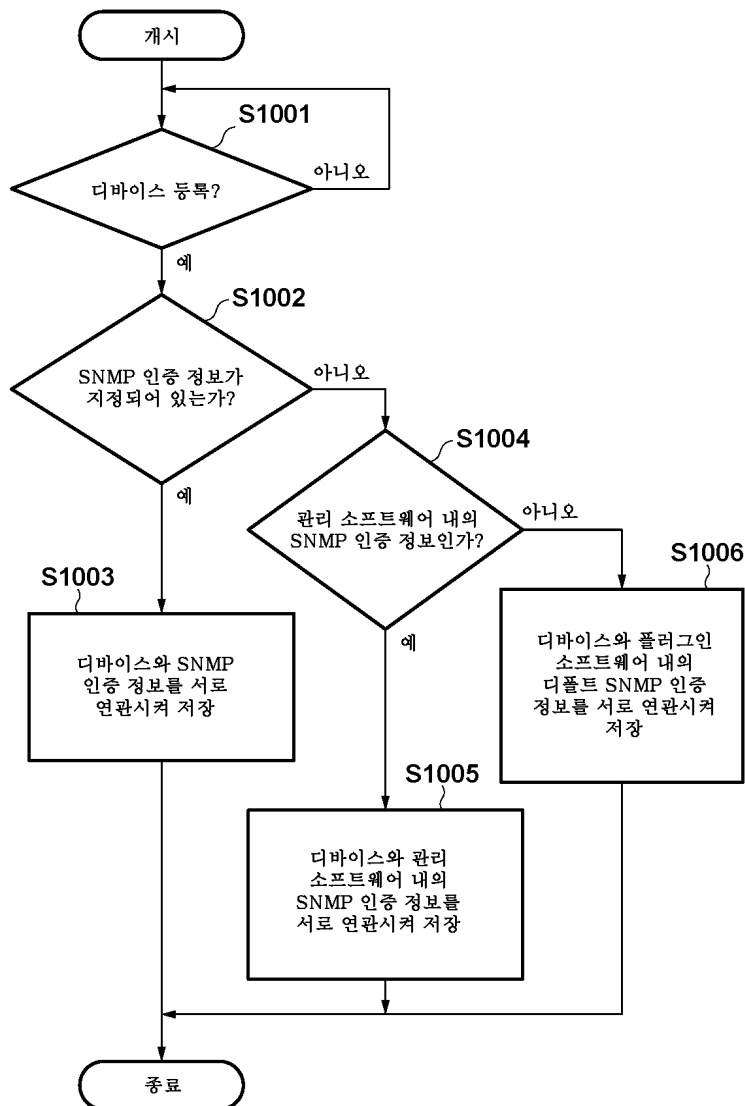
도면8

801		802		803	
더파이스 ID	커뮤니티명	코멘트			
더파이스 A	public-parent	관리 소프트웨어의 커뮤니티명을 취득			
더파이스 C	dev-group1	관리 소프트웨어의 커뮤니티명을 취득			
더파이스 D	public-plugin	플러그인에 대해 공통인 커뮤니티명을 취득			
...	...	...			
더파이스 X	dev-groupZ	개별 커뮤니티명			
더플트 더파이스	public-parent	공통 커뮤니티명			

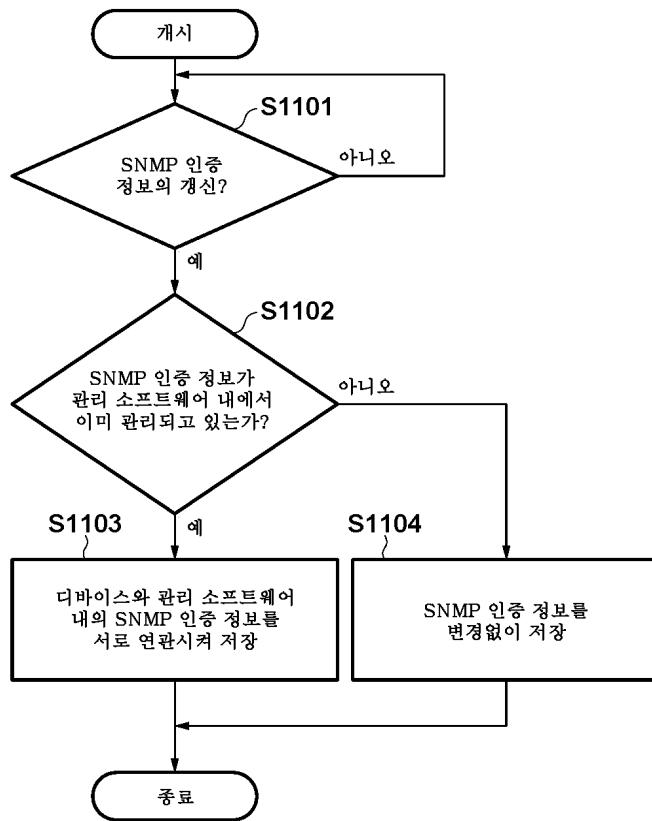
도면9



도면10



도면11



도면12a

관리할 디바이스를 추가

1201

전체 선택

전체 취소

X 삭제

디바이스 ID 검색

디바이스 리스트로부터 추가

빈 행 추가

No.

IP 어드레스/호스트명

디바이스명

제품명

디바이스 ID

커뮤니티명

타입

1-1 / 1

20 행

1 / 1 페이지

1

1-1 / 1

추가

철회

?

도면12b

전체 디바이스

전체 선택

전체 취소

대상 디바이스에 추가

1-5 / 1121

5행

1페이지

12345

디바이스명	제품명	▲	IPv4 어드레스	시리얼 번호	MAC 어드레스	갱신
☒  iPR C1PLUS	Canon iPR C1PLUS	192.168.0.1		00:00:85:C4:95:9D	2011/02/10 14:54:24	
☒  iPR C1PLUS	Canon iPR C1PLUS	192.168.0.2		00:00:85:18:9C:97	2011/02/10 14:54:24	
☐  iPR C1PLUS	Canon iPR C1PLUS	192.168.0.6		00:00:85:18:9C:99	2011/02/10 14:54:24	
☐  iPR C1PLUS	Canon iPR C1PLUS	192.168.0.8		00:00:85:18:9C:9A	2011/02/10 14:53:52	
☐  iPR C1PLUS	Canon iPR C1PLUS	192.168.0.9		00:00:85:18:9C:9B	2011/02/10 14:53:52	

1-5 / 1121

12345

추가

재설정

?

1202

도면12c

관리할 디바이스를 추가

전체 선택 전체 취소 X 삭제 디바이스 ID 검색 디바이스 리스트로부터 추가 빈 행 추가

1-2 / 2 20 행 1 / 1 페이지

No.	IP 어드레스/호스트명	디바이스명	제품명	디바이스 ID	커뮤니티명	타입
1	192.168.0.1	iPR C1PLUS	Canon iPR C1PLUS		●●●●	Canon Device
2	192.168.0.2	iPR C1PLUS	Canon iPR C1PLUS		●●●●	Canon Device

1-2 / 2

1203 1204

추가 취소 ?

도면13a

디바이스 정보	
디바이스명	iR-ADV C5051
제품명	Oanon iR-ADV C5051
MAC 어드레스	00:1E:8F:2E:CB:21
위치	
IPv4 어드레스	172.24.93.173
IPv6 어드레스	
호스트명	
시리얼 번호	DZJ01302
SNMP 커뮤니티명	(set)

1301

도면13b

디바이스 정보	
디바이스명	iR-ADV C5051
제품명	Canon iR-ADV C5051
MAC 어드레스	00:1E:8F:2E:CB:21
위치	
IPv4 어드레스	172.24.93.173
IPv6 어드레스	
호스트명	
시리얼 번호	DZJ01302
SNMP 커뮤니티명	maintenance-group1

1302

도면14

