(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5383330号
(P5383330)
(45)発行日　平成26年1月8日(2014.1.8)　(24)登録日　平成25年10月11日(2013.10.11)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 353B
H04L 12/66 (2006.01)　　H04L 12/66 Z

請求項の数 8　(全 29 頁)

(21)出願番号　特願2009-138237(P2009-138237)
(22)出願日　平成21年6月9日(2009.6.9)
(65)公開番号　特開2010-286890(P2010-286890A)
(43)公開日　平成22年12月24日(2010.12.24)
審査請求日　平成24年6月11日(2012.6.11)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100125254
弁理士　別役　重尚
(72)発明者　五十嵐　敏明
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　田上　隆一

最終頁に続く

(54)【発明の名称】デバイス管理装置、制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
第１の通信プロトコルで運用される第１のネットワークに接続され、前記第１の通信プロトコルとは異なる第２の通信プロトコルで運用される第２のネットワークで稼動する情報取得装置と通信が可能で、前記第１のネットワークで稼動するデバイスの管理を行うデバイス管理装置であって、
前記情報取得装置からデバイス情報取得要求を受信した場合、前記デバイス情報取得要求から当該情報取得装置で利用が可能な通信プロトコルである前記第２の通信プロトコルを抽出する抽出手段と、
前記第１のネットワークに接続されたデバイスで、前記第２の通信プロトコルを起動させることが可能な場合は、前記デバイスに前記第２の通信プロトコルの起動を要求する第１の要求手段と、
前記第１の要求手段の要求により前記デバイスで前記第２の通信プロトコルの起動が成功した場合、前記デバイス情報取得要求に対する応答を作成する作成手段と、
前記作成手段により作成した前記応答を前記情報取得装置に送付する送付手段と、
を備えることを特徴とするデバイス管理装置。
【請求項２】
前記第１の要求手段の要求により前記デバイスで前記第２の通信プロトコルの起動が成功した場合、前記デバイスから情報を取得する際の前記デバイスへのアクセス設定の変更が必要か否かを判別するアクセス設定変更判別手段と、

前記アクセス設定変更判別手段により前記アクセス設定の変更が必要と判別された場合は、前記アクセス設定の変更を前記デバイスに要求する第２の要求手段を更に有し、
前記作成手段は、前記第２の要求手段の要求により前記デバイスで前記アクセス設定の変更が成功した場合に、前記情報取得装置に対する前記デバイス情報に関する応答を作成することを特徴とする請求項１記載のデバイス管理装置。
【請求項３】
前記第１のネットワークで稼働するデバイスの設定を変更することで前記通信プロトコルを前記デバイスで起動させることが可能か否かを判別する起動判別手段を更に備えることを特徴とする請求項２記載のデバイス管理装置。
【請求項４】
前記第１のネットワークに接続されたデバイスを探索することでデバイス情報を取得する取得手段を更に備え、
前記デバイス情報は、デバイス名、前記第１のネットワークにおけるアドレス、前記第２のネットワークにおけるアドレス、情報取得方法のいずれかを含むことを特徴とする請求項１乃至３の何れか１項に記載のデバイス管理装置。
【請求項５】
前記第１のネットワークに接続されたデバイスに対するアクセス設定の変更を指示する指示手段を更に備え、
前記第２の要求手段は、前記指示手段による前記アクセス設定の変更の指示に基づき、前記情報取得装置から前記デバイスへのアクセスの許可が必要か否かを判断し、必要な場合は、前記デバイスが有するアクセス許可リストに対して前記情報取得装置のアドレスを登録することを特徴とする請求項２記載のデバイス管理装置。
【請求項６】
前記第１のネットワークに接続されたデバイスにアクセスする際の認証情報を設定する設定手段を更に備え、
前記第２の要求手段は、前記設定手段による前記認証情報の設定に基づき、前記デバイスから情報を取得する際の前記デバイスへのアクセス設定の変更が必要か否かを判断し、必要な場合は、前記デバイスから情報を取得する際のアクセス方法を前記認証情報を用いて前記アクセス設定を変更することを前記デバイスに要求することを特徴とする請求項２記載のデバイス管理装置。
【請求項７】
第１の通信プロトコルで運用される第１のネットワークに接続され、前記第１の通信プロトコルとは異なる第２の通信プロトコルで運用される第２のネットワークで稼動する情報取得装置と通信が可能で、前記第１のネットワークで稼動するデバイスの管理を行うデバイス管理装置の制御方法であって、
前記情報取得装置からデバイス情報取得要求を受信した場合、前記デバイス情報取得要求から当該情報取得装置で利用が可能な通信プロトコルである前記第２の通信プロトコルを抽出する抽出工程と、
前記第１のネットワークに接続されたデバイスで、前記第２の通信プロトコルを起動させることが可能な場合は、前記デバイスに前記第２の通信プロトコルの起動を要求する第１の要求工程と、
前記第１の要求工程の要求により前記デバイスで前記第２の通信プロトコルの起動が成功した場合、前記デバイス情報取得要求に対する応答を作成する作成工程と、
前記作成工程で作成した前記応答を前記情報取得装置に送付する送付工程と、
を有することを特徴とする制御方法。
【請求項８】
請求項７に記載のデバイス管理装置の制御方法をコンピュータに実行させるためのコンピュータで読み取り可能なプログラムコードを有するプログラム。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、ネットワークに接続されているネットワークデバイスを管理するデバイス管理装置、制御方法、及びプログラムに関する。
【背景技術】
【０００２】
従来、ＳＮＭＰ（Simple Network Management Protocol）等のネットワーク管理技術を用いて、２つ以上のサブネットワークに接続されているネットワークデバイスを効率的に管理する方法が提案されている。先行技術文献としては、複数のサブネットワークに接続されている複数のネットワークデバイスを管理するために、各サブネットワーク内に代表デバイスを置くネットワーク接続デバイス管理システムが提案されている（例えば、特許文献１参照）。
【０００３】
特許文献１に記載のネットワーク接続デバイス管理システムでは、代表デバイスが各サブネットワーク内の他のデバイスの情報を収集する。次に、代表デバイスはサブネットワーク代表デバイスにデバイス情報を送付する。最後に、サブネットワーク代表デバイスは各サブネットワーク内の全てのデバイスのデバイス情報を取りまとめた上で、ネットワークデバイス管理装置に送付する。
【０００４】
一方、近年、セキュリティに関する関心が高まるに伴い、ＩＰｓｅｃ（Security Architecture for Internet Protocol）と相性のよいＩＰＶ６（Internet Protocol Ver.6）が広まりつつある。このような流れのもと、従来、ＩＰＶ４（Internet Protocol Ver.4）で運用していた環境の一部がＩＰＶ６に置き換えられつつある。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００３－１８６７６５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、ＩＰＶ６で運用しているサブネット（ＩＰＶ６環境と呼ぶ）と、ＩＰＶ４で運用しているサブネット（ＩＰＶ４環境と呼ぶ）が混在する環境で、特許文献１に記載のネットワークデバイス管理装置を稼動させた場合、次のような状況が発生しうる。即ち、ＩＰＶ６環境のデバイス情報を代表デバイスが収集し、ＩＰＶ４環境で稼動するネットワークデバイス管理装置に送付する、という状況である。
【０００７】
この場合、代表デバイスが収集したデバイス情報はＩＰＶ６に関する情報を含むため、ＩＰＶ４環境にあるネットワークデバイス管理装置はＩＰＶ６環境のネットワークデバイスの管理を行うことができない。また、仮にＩＰＶ６環境のネットワークデバイスが、ＩＰＶ６とＩＰＶ４の両方に対応したネットワークデバイス（デュアルスタックデバイスと呼ぶ）であった場合、代表デバイスが収集したデバイス情報には、ＩＰＶ６とＩＰＶ４の両方の情報が含まれる。
【０００８】
このため、ＩＰＶ４環境にあるネットワークデバイス管理装置は、ＩＰＶ４を使ってＩＰＶ６環境のネットワークデバイスの管理を行うことができるが、構築したセキュリティの高い環境の外でネットワークデバイスの管理を行うことになってしまう。
【０００９】
本発明の目的は、情報取得装置が接続されたネットワークと異なるネットワークに接続されたデバイス管理装置からデバイス情報を取得してデバイスの管理を行うことを可能としたデバイス管理装置、制御方法、及びプログラムを提供することにある。
【課題を解決するための手段】

【００１０】
上記目的を達成するために、本発明のデバイス管理装置は、第１の通信プロトコルで運用される第１のネットワークに接続され、前記第１の通信プロトコルとは異なる第２の通信プロトコルで運用される第２のネットワークで稼動する情報取得装置と通信が可能で、前記第１のネットワークで稼動するデバイス管理装置であって、前記情報取得装置からデバイス情報取得要求を受信した場合、前記デバイス情報取得要求から当該情報取得装置で利用が可能な通信プロトコルである前記第２の通信プロトコルを抽出する抽出手段と、前記第１のネットワークに接続されたデバイスで、前記第２の通信プロトコルを起動させることが可能な場合は、前記デバイスに前記第２の通信プロトコルの起動を要求する第１の要求手段と、前記第１の要求手段の要求により前記デバイスで前記第２の通信プロトコルの起動が成功した場合、前記デバイス情報取得要求に対する応答を作成する作成手段と、前記作成手段により作成した前記応答を前記情報取得装置に送付する送付手段と、を備えることを特徴とする。
【発明の効果】
【００１１】
本発明によれば、デバイス管理装置は情報取得装置のデバイス情報取得要求に基づき、デバイス情報に関する応答を作成して情報取得装置に送付する。これにより、第２のネットワークで稼動する情報取得装置は、第２のネットワークの外の異なる第１のネットワークに接続されたデバイス管理装置からデバイス情報を取得することが可能となり、情報取得装置でデバイスの管理を行うことが可能となる。
【図面の簡単な説明】
【００１２】
【図１】本発明の実施の形態に係るネットワークシステムの構成を示す図である。
【図２】ネットワークデバイス情報取得装置及びネットワークデバイス管理装置に共通の内部構成を示すブロック図である。
【図３】ネットワークデバイスの例である複合機の内部構成を示すブロック図である。
【図４】ネットワークデバイス情報取得装置がネットワークデバイス管理装置からデバイス情報を取得する際に実行する処理を示すフローチャートである。
【図５】ネットワークデバイス情報取得装置がネットワークデバイス管理装置に送信するデバイス情報取得要求コマンドの例を示す図である。
【図６】ネットワークデバイス情報取得装置がネットワークデバイス管理装置から受信するデバイス情報取得要求コマンドに対する応答の例を示す図である。
【図７】ネットワークデバイス情報取得装置で作成したデバイスリスト画面の例を示す図である。
【図８ａ】ネットワークデバイス管理装置がネットワークデバイス情報取得装置からデバイス情報取得要求を受信した際に実行する処理を示すフローチャートである。
【図８ｂ】ネットワークデバイス管理装置がネットワークデバイス情報取得装置からデバイス情報取得要求を受信した際に実行する処理を示すフローチャートである。
【図９】ネットワークデバイス管理装置がデバイス探索で取得したデバイス情報の例を示す図である。
【図１０】ネットワークデバイス管理装置で表示するデバイスに対するアクセス設定変更画面の例を示す図である。
【図１１ａ】ネットワークデバイスがネットワークデバイス管理装置とネットワークデバイス情報取得装置からの各種要求を受信した際に実行する処理を示すフローチャートである。
【図１１ｂ】ネットワークデバイスがネットワークデバイス管理装置とネットワークデバイス情報取得装置からの各種要求を受信した際に実行する処理を示すフローチャートである。
【図１２】ネットワークデバイスがネットワークデバイス管理装置からの要求に従ってデバイスのアクセス設定を変更した際のアクセス許可リストの例を示す図である。

【図１３】ネットワークデバイス管理装置からの要求に従ってデバイスのアクセス設定を変更した際のＳＮＭＰｖ３認証情報設定テーブルの例を示す図である。
【発明を実施するための形態】
【００１３】
以下、本発明の実施の形態を図面に基づいて説明する。
【００１４】
本実施の形態では、ＩＰＶ４ネットワーク環境のネットワークデバイス情報取得装置が、ＩＰＶ６ネットワーク環境のネットワークデバイス管理装置からデバイス情報を収集し、ＩＰＶ６環境のデバイスを管理する際の動作について説明する。
【００１５】
図１は、本実施の形態に係るネットワークシステムの構成を示す図である。
【００１６】
図１において、ネットワークシステムは、ネットワークデバイス情報取得装置１０１、ルータ１０２、ネットワークデバイス管理装置１１１、ルータ１１２、ネットワークデバイス１１３、１１４、１１５を備えている。ネットワーク１２０は、ＩＰＶ４ネットワーク環境１００（第１のネットワーク）と、ＩＰＶ６ネットワーク環境１１０（第２のネットワーク）とを繋ぐネットワークである。ネットワーク１２０には、ＩＰＶ４とＩＰｖ６の双方のデータの混在が可能である。尚、以後、ネットワークデバイス情報取得装置を情報取得装置、ネットワークデバイス管理装置を管理装置、ネットワークデバイスをデバイスと略記する。
【００１７】
情報取得装置１０１は、管理装置１１１が管理するデバイス１１３～１１５のデバイス情報を取得する。ルータ１０２は、ＩＰＶ４プロトコル及びＩＰＶ６プロトコルの電子データを転送する機能を有するネットワーク中継機器である。本実施の形態では、情報取得装置１０１及びルータ１０２は、ＩＰＶ４ネットワーク環境１００で稼動しているものとする。
【００１８】
管理装置１１１は、２つの役割を有する。１つ目の役割は、ＳＮＭＰを使用してデバイスが有するＭＩＢ（Management Information Base）の情報を取得し、デバイス情報として管理することである。２つ目の役割は、情報取得装置１０１が発行するデバイス情報取得要求を受け、自身が管理するデバイス１１３～１１５のデバイス情報を情報取得装置１０１に送付することである。ルータ１１２は、ルータ１０２と同等の機能を有するネットワーク中継機器である。デバイス１１３～１１５は、画像形成機能を有するデバイス（複合機、複写機、プリンタ等）として構成されている。
【００１９】
ＩＰＶ６ネットワーク環境１１０内では、各構成要素（管理装置１１１、ルータ１１２、デバイス１１３～１１５）は、ＩＰＶ６で相互に通信を行う。ただし、管理装置１１１は、情報取得装置１０１と通信するため、ＩＰＶ４及びＩＰＶ６のデュアルスタックで稼動している。また、各構成要素（管理装置１１１、ルータ１１２、デバイス１１３～１１５）は、自身の設定を変更することにより、ＩＰＶ４及びＩＰＶ６のデュアルスタックで稼動することも可能である。
【００２０】
図２は、情報取得装置及び管理装置に共通の内部構成を示すブロック図である。
【００２１】
図２において、情報取得装置１０１、管理装置１１１は、それぞれ、図示の構成要素を有するパーソナルコンピュータ（ＰＣ）上に実現される。情報取得装置１０１、管理装置１１１は、それぞれ、ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、システムバス２０４、キーボードコントローラ（ＫＢＣ）２０５、ディスプレイコントローラ（ＤＳＰＣ）２０６を備えている。更に、ディスクコントローラ（ＤＫＣ）２０７、インタフェースコントローラ（ＩＦＣ）２０８、キーボード２０９、ディスプレイ２１０、ハードディスク（

ＨＤ）２１１、フロッピー(登録商標)ディスクドライブ（以下ＦＤドライブ）２１２を備えている。

【００２２】

ＨＤ２１１には、後述の説明で動作主体となる本実施の形態に係る情報処理ソフトウェアのプログラム（情報処理プログラム）が格納されている。後述の説明で特に断りのない限り、実行の主体はハードウェア上はＣＰＵ２０１である。一方、ソフトウェア上の制御の主体は、例えばＨＤ２１１に格納された情報処理プログラムである。情報取得装置１０１のＣＰＵ２０１の制御の下で後述の図４のフローチャートに示す処理が実行される。また、管理装置１１１のＣＰＵ２０１の制御の下で後述の図８ａ及び図８ｂのフローチャートに示す処理が実行される。

【００２３】

ＲＯＭ２０２は、プログラム、固定データ等を記憶する。ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。キーボードコントローラ２０５は、キーボード２０９やポインティングデバイス（不図示）等からの指示入力を制御する。ディスプレイコントローラ２０６は、ディスプレイ２１０に対する表示（図７の画面及び図１０の画面の表示を含む）を制御する。

【００２４】

ディスクコントローラ２０７は、ＨＤ２１１、ＦＤドライブ２１２のＦＤ、ＣＤ－ＲＯＭ（不図示）等の記憶装置に対するアクセスを制御する。ＨＤ２１１及びＦＤドライブ２１２のＦＤには、ブートプログラム、オペレーティングシステム、データベース、情報処理アプリケーションプログラム及びそのデータ等が記憶される。インタフェースコントローラ２０８は、ＬＡＮ（Local Area Network）を介して他のネットワーク機器と情報を送受信する。

【００２５】

尚、本実施の形態では、情報処理プログラムは、ＦＤやＣＤ－ＲＯＭ等の記憶媒体に格納された形で供給されてもよい。その場合には、図２に示すＦＤドライブ２１２またはＣＤ－ＲＯＭドライブ等により記憶媒体からプログラムが読み取られ、ＨＤ２１１にインストールされる。

【００２６】

また、本実施の形態では、情報取得装置１０１及び管理装置１１１で動作するＯＳ（オペレーティングシステム）としては例えばウィンドウズ(登録商標)を想定しているが、これに限定されるものではない。

【００２７】

図３は、デバイス１１３の例である複合機の内部構成を示すブロック図である。

【００２８】

図３において、デバイス１１３は、スキャナ機能、プリンタ機能、コピー機能、ファクシミリ（ＦＡＸ）機能を備える複合機として構成されており、公衆回線網３１２を介して他のネットワーク機器に接続されている。尚、本実施の形態では、デバイス１１３として複合機を例示しているが、複合機に限定されず、デジタル複写機、コピー機能付プリンタ、単機能のプリンタのいずれでも構わない。

【００２９】

デバイス１１３は、主にリーダ部３０１、プリンタ部３０２、画像入出力制御部３０３、操作部３０４から構成されている。操作部３０４は、ユーザからの入力操作を受け付ける。リーダ部３０１は、プリンタ部３０２及び画像入出力制御部３０３に接続され、ユーザにより入力された操作部３０４からの指示に従って原稿の画像読み取りを行うと共に、読み取った画像データをプリンタ部３０２又は画像入出力制御部３０３に出力する。プリンタ部３０２は、リーダ部３０１及び画像入出力制御部３０３から出力された画像データを記録紙に印刷する。

【００３０】

画像入出力制御部３０３は、ＬＡＮと公衆回線網３１２に接続され、画像データの入出

力を行い、更にジョブの解析及び制御を行う。画像入出力制御部３０３は、ファクシミリ部３０５、ファイル部３０６、外部インタフェース部３０８、ＰＤＬ（Page Description Language）フォーマッタ部３０９、画像メモリ部３１０、コア部３１１から構成されている。

【００３１】

ファクシミリ部３０５は、コア部３１１及び公衆回線網３１２に接続され、公衆回線網３１２を介して他の機器から受信した圧縮された画像データの伸長を行い、伸長した画像データをコア部３１１へ送信する。また、ファクシミリ部３０５は、コア部３１１から送信された画像データの圧縮を行い、圧縮した画像データを公衆回線網３１２を介して他の機器に送信する。

【００３２】

ファイル部３０６は、コア部３１１及び外部記憶装置３０７に接続され、コア部３１１から送信された画像データや機器制御コマンドの実行結果を、これを検索するためのキーワードと共にハードディスク等で構成可能な外部記憶装置３０７に記憶させる。また、ファイル部３０６は、コア部３１１から送信されたキーワードに基づいて外部記憶装置３０７に記憶されている画像データや機器制御コマンドの実行結果を読み出し、コア部３１１へ送信する。

【００３３】

外部インタフェース部３０８は、他のネットワーク機器とコア部３１１との間のインタフェースをつかさどる。他のネットワーク機器との間におけるジョブ制御データ、画像データ、機器制御コマンドの送受信は、外部インタフェース部３０８を介して行う。

【００３４】

ジョブ制御データとしては、ＰＤＬデータと共に送信されるジョブ制御命令を含む。ジョブ制御データの例としては、例えば、ＰＤＬデータを展開して画像データとして印刷した後、ステイプルソートして排紙させるものが挙げられる。

【００３５】

また、機器制御コマンドの例としては、（１）デバイス１１３の製品名やネットワーク情報を取得するための情報取得コマンド、（２）デバイス１１３の通信プロトコルやネットワーク情報を変更する情報配信コマンド、等が挙げられる。

【００３６】

フォーマッタ部３０９は、コア部３１１に接続され、他の機器（例えばコンピュータ）から送信されたＰＤＬデータをプリンタ部３０２で印刷できる画像データに展開する。画像メモリ部３１０は、リーダ部３０１からの情報、外部インタフェース部３０８を介し他の機器（例えばコンピュータ）から送られてきた情報を一時的に蓄積する。コア部３１１は、リーダ部３０１、操作部３０４、ファクシミリ部３０５、ファイル部３０６、外部インタフェース部３０８、ＰＤＬフォーマッタ部３０９、画像メモリ部３１０のそれぞれの間を流れるデータ等の制御を行う。

【００３７】

次に、上記の構成を備える本実施の形態のネットワークシステムを構成する情報取得装置１０１、管理装置１１１、デバイス１１３でそれぞれ実行する処理について図４乃至図１３を参照しながら説明する。

【００３８】

＜情報取得装置の処理＞

まず、情報取得装置１０１が管理装置１１１からデバイス情報を取得する場合の処理を図４、図５、図６、図７に基づき説明する。

【００３９】

図４は、情報取得装置１０１が管理装置１１１からデバイス情報を取得する際に実行する処理を示すフローチャートである。本処理は情報取得装置１０１のＣＰＵ２０１の全体制御の下に実行される。

【００４０】

図４において、情報取得装置１０１のＣＰＵ２０１は、ユーザからの指示を操作部３０４を介して受け付けると、管理装置１１１が管理するデバイス情報の取得を要求するデバイス情報取得要求を管理装置１１１に送信する（ステップＳ４０１）。その際、情報取得装置１０１のＣＰＵ２０１は、情報取得装置自身が利用可能な通信プロトコルの情報を上記デバイス情報取得要求に付記して管理装置１１１に送信する。

【００４１】

図５に、情報取得装置１０１が発行するデバイス情報取得要求コマンドの例を示す。コマンドテーブル５００は、要求コマンド名５１０、拡張領域５２０を有する。要求コマンド名５１０は、要求するコマンドの名称を指定するための領域であり、コマンドの名称としてデバイス情報取得要求コマンド５０１が格納されている。拡張領域５２０は、要求コマンド名５１０に指定されたコマンドに応じて追加データを指定するための領域であり、情報取得装置１０１で利用可能な通信プロトコルの名称としてＩＰＶ４が格納されている。

【００４２】

尚、本実施の形態では、コマンドテーブル５００に拡張領域５２０を設け、拡張領域５２０を使用する場合を例に挙げているが、これに限定されるものではない。より単純に、情報取得装置１０１がデバイス情報取得要求コマンドを送信する際に使用した通信プロトコルを、利用可能な通信プロトコルとしてもよい。この場合、拡張領域５２０は不要となる。

【００４３】

図４に戻り、情報取得装置１０１のＣＰＵ２０１は、ステップＳ４０１で管理装置１１１に送信したデバイス情報取得要求コマンドに対する管理装置１１１からの応答を受信する（ステップＳ４０２）。受信した応答は、例えばＲＡＭ２０３またはＨＤ２１１に格納される。

【００４４】

図６に、情報取得装置１０１が管理装置１１１から受信するデバイス情報取得要求コマンドに対する応答の例を示す。応答テーブル６００は、デバイス情報取得要求コマンドに対する応答６０１を格納するものであり、取得結果６１０、結果詳細６２０、デバイス情報６３０を有する。

【００４５】

取得結果６１０は、管理装置１１１がデバイス情報取得要求コマンドを処理した結果を格納する領域である。本例では、取得結果６１０には、管理装置１１１がデバイス情報取得要求コマンドを処理した結果として「成功」が格納されている。尚、一般に、取得結果６１０が「失敗」である場合、後述のデバイス情報６３０の各要素の値は無効あるいは不定となる。

【００４６】

結果詳細６２０は、取得結果６１０の詳細情報を格納する領域である。特に、応答６０１の取得結果６１０の値が「失敗」である場合、その理由を格納するために結果詳細６２０が使用される。結果詳細６２０に格納される詳細情報の例としては、「指定された通信プロトコルの情報がデバイスから取得できなかった」、「指定されたデバイスが見つからなかった」等が想定される。あるいは、別途エラーコードを定義しておき、それを結果詳細６２０に格納してもよい。

【００４７】

デバイス情報６３０は、管理装置１１１から取得したデバイス情報を格納する領域であり、デバイス１１３、デバイス１１４、デバイス１１５のそれぞれのデバイス情報が列挙されている。デバイス情報６３０は、デバイス名６３１、製品名６３２、ＩＰＶ４アドレス６３３、ＩＰＶ６アドレス６３４、情報取得方法６３５から構成されている。

【００４８】

本実施の形態では、ＩＰＶ４ネットワーク環境で稼動している情報取得装置１０１ではＩＰＶ６を利用できないため、ＩＰＶ６アドレス６３４の値は空欄となっている。また、

情報取得方法６３５には、情報取得装置１０１がデバイス１１３～１１５にアクセスする際のアクセス方法としてＳＮＭＰｖ３が指定されている。尚、デバイス情報６３０の要素としては、上記以外に設置場所、ホスト名、デバイス状態等を加えてもよい。

【００４９】

図４に戻り、情報取得装置１０１のＣＰＵ２０１は、ステップＳ４０２でＲＡＭ２０３またはＨＤ２１１に格納したデバイス情報の取得結果６１０を調べる。更に、情報取得装置１０１のＣＰＵ２０１は、情報取得装置１０１がデバイス情報の受信に成功したかどうかを判別する（ステップＳ４０３）。

【００５０】

デバイス情報の受信に成功した場合は、情報取得装置１０１のＣＰＵ２０１は、ステップＳ４０２で受信したデバイス情報６３０のデバイス情報を用いてデバイスリスト画面を作成する。更に、情報取得装置１０１のＣＰＵ２０１は、作成したデバイスリスト画面をＤＳＰコントローラ２０６によりディスプレイ２１０に表示する（ステップＳ４０４）。デバイス情報の受信に失敗した場合は、ステップＳ４０６に進む。

【００５１】

図７に、情報取得装置１０１で作成したデバイスリスト画面の例を示す。デバイスリスト画面７００には、デバイスリストが表示されている。デバイスリストは、構成要素７０１、７０２、７０３（デバイス１１３、デバイス１１４、デバイス１１５）ごとに、デバイス名７１０、製品名７２０、ＩＰＶ４アドレス７３０、ＩＰＶ６アドレス７４０、情報取得方法７５０を列挙したものである。

【００５２】

デバイス名７１０は、デバイス情報６３０のデバイス名６３１の値と同一である。製品名７２０は、デバイス情報６３０の製品名６３２の値と同一である。ＩＰＶ４アドレス７３０は、デバイス情報６３０のＩＰＶ４アドレス６３３の値と同一である。ＩＰＶ６アドレス７４０は、デバイス情報６３０のＩＰＶ６アドレス６３４の値と同一である。情報取得方法７５０は、デバイス情報６３０の情報取得方法６３５の値と同一である。結果７６０は、取得結果６１０を表示したものである。詳細情報７７０は、結果詳細６２０を表示したものである。

【００５３】

図４に戻り、情報取得装置１０１のＣＰＵ２０１は、ステップＳ４０４でデバイスリスト画面７００を表示した後、デバイスリスト画面７００の構成要素７０１～７０３に対するユーザの操作を受け付ける。その後、情報取得装置１０１のＣＰＵ２０１は、デバイス１１３～１１５のうち該当するデバイスに対して情報取得方法７５０のアクセス方法で機器制御コマンドを発行する（ステップＳ４０５）。機器制御コマンドの例としては、上述したように、情報取得コマンド、情報配信コマンド、等が挙げられる。

【００５４】

他方、デバイス情報の受信に失敗した場合は（ステップＳ４０３でＮＯ）、情報取得装置１０１のＣＰＵ２０１は、ＲＡＭ２０３またはＨＤ２１１に格納されている取得結果６１０及び結果詳細６２０を読み出す。更に、情報取得装置１０１のＣＰＵ２０１は、デバイスリスト画面７００の結果７６０（表示例「成功」）及び詳細情報７７０（表示例「正常に取得できました」）として表示する（ステップＳ４０６）。これにより、本処理を終了する。

【００５５】

尚、ステップＳ４０６を実行する際には、結果６１０及び結果詳細６２０に格納されている内容をそのまま表示してもよいし、情報取得装置１０１でユーザが理解しやすい内容に変換してから表示してもよい。

【００５６】

＜管理装置の処理＞

次に、管理装置１１１が情報取得装置１０１からのデバイス情報取得要求を受信した際に実行する処理を図８ａ、図８ｂ、図９、図１０に基づき説明する。

【００５７】
図８ａ、図８ｂは、管理装置１１１が情報取得装置１０１からデバイス情報取得要求を受信した際に実行する処理を示すフローチャートである。本処理は管理装置１１１のＣＰＵ２０１の全体制御の下に実行される。
【００５８】
図８ａ、図８ｂにおいて、管理装置１１１のＣＰＵ２０１は、ＩＰＶ６ネットワーク環境１１０内のデバイスを探索し、探索結果をデバイス情報として管理装置１１１のＲＡＭ２０３またはＨＤ２１１に格納する（ステップＳ８０１：取得手段）。尚、デバイスを探索する方法の例としては、ＩＰＶ６のＳＬＰ（Service Location Protocol）マルチキャスト、ＳＮＭＰマルチキャストを利用する方法等が考えられるが、これに限定されるものではない。
【００５９】
図９に、管理装置１１１がステップＳ８０１で取得したデバイス情報の例を示す。デバイス情報テーブル９００は、構成要素９０１、９０２、９０３（デバイス１１３、１１４、１１５）ごとに、デバイス名９１０、製品名９２０、ＩＰＶ４アドレス９３０、ＩＰＶ６アドレス９４０、情報取得方法９５０を列挙したものである。
【００６０】
構成要素９０１、９０２、９０３には、管理装置１１１がステップＳ８０１で取得した、デバイス１１３、１１４、１１５のデバイス情報の値が格納されている。デバイス名９１０、製品名９２０、ＩＰＶ４アドレス９３０、ＩＰＶ６アドレス９４０、情報取得方法９５０は、それぞれ、図６のデバイス名６３１、製品名６３２、ＩＰＶ４アドレス６３３、ＩＰＶ６アドレス６３４、情報取得方法６３５に対応する。
【００６１】
本実施の形態では、ステップＳ８０１でＩＰＶ６のデバイス情報を取得しているため、ＩＰＶ４アドレス９３０は空欄となっている。また、情報取得方法９５０には、管理装置１１１がデバイスを管理する際に使用するアクセス方法として「ＳＮＭＰ」が格納されている。尚、情報取得方法９５０に格納する値は、ステップＳ８０１のデバイス探索時に使用したアクセス方法と異なる値が格納されていてもよい。また、図６のデバイス情報６３０と同様に、デバイス情報テーブル９００の要素として、上記以外に設置場所、ホスト名、デバイス状態等を加えてもよい。
【００６２】
図８ａに戻り、管理装置１１１のＣＰＵ２０１は、図４のステップＳ４０１で情報取得装置１０１から送信されたデバイス情報取得要求を受信する（ステップＳ８０２）。その後、管理装置１１１のＣＰＵ２０１は、デバイス情報取得要求を、情報取得装置１０１のＩＰアドレス情報（本実施の形態では、“１２３．１２３．１２３．１０１”と仮定する）と共にＲＡＭ２０３またはＨＤ２１１に格納する。
【００６３】
次に、管理装置１１１のＣＰＵ２０１は、ステップＳ８０２で情報取得装置１０１から受信したデバイス情報取得要求を解析する（ステップＳ８０３）。具体的には、デバイス情報取得要求から「情報取得装置１０１で利用可能なネットワークプロトコル」を抽出し（抽出手段）、情報取得装置１０１の通信プロトコル情報としてＲＡＭ２０３またはＨＤ２１１に格納する。
【００６４】
次に、管理装置１１１のＣＰＵ２０１は、ステップＳ８０１で取得したデバイス情報をテーブル化したデバイス情報テーブル９００に、ステップＳ８０３で抽出した通信プロトコル情報が含まれているかどうかを判別する（ステップＳ８０４）。本実施の形態では、通信プロトコル情報としてＩＰＶ４が抽出されているため、デバイス情報テーブル９００にＩＰＶ４の情報が存在するかどうかを確認することになる。
【００６５】
デバイス情報テーブル９００に管理装置１１１で利用可能な通信プロトコル情報が含ま

れている場合は、ステップＳ８１２に進む。デバイス情報テーブル９００に前記通信プロトコル情報が含まれていない場合は、管理装置１１１のＣＰＵ２０１は、デバイス１１３～１１５のそれぞれがステップＳ８０３で抽出した通信プロトコルで稼動しているかどうかを判別する（ステップＳ８０５）。本実施の形態では、デバイス１１３～１１５がＩＰＶ４で稼動しているかどうかを判別することになる。判別方法の例としては、管理装置１１１がデバイス１１３～１１５に対してＰＩＮＧコマンドを発行する方法等が考えられるが、これに限定されるものではない。

【００６６】

ステップＳ８０３で抽出した通信プロトコルが稼動しているデバイスに対する処理を続ける場合は、ステップＳ８１０に進む。ステップＳ８０３で抽出した通信プロトコルが稼動していないデバイスに対する処理を続ける場合は、管理装置１１１のＣＰＵ２０１は次の判別を行う。デバイスの設定を変更することにより情報取得装置１０１と同一の通信プロトコルをデバイスでも起動させることができるかどうかを判別する（ステップＳ８０６：第１の判別手段）。例えば、本実施の形態では、ＳＮＭＰを用いてＩＰＶ４の情報を示すＭＩＢオブジェクト（ipAdEntAddr等）を取得することができれば、デバイスはＩＰＶ４を有していると判断することができる。

【００６７】

デバイスの設定を変更することにより情報取得装置１０１と同一の通信プロトコルをデバイスでも起動させることができない場合は、ステップＳ８１７に進む。デバイスの設定を変更することにより情報取得装置１０１と同一の通信プロトコルをデバイスでも起動させることができる場合は、管理装置１１１のＣＰＵ２０１はデバイスに次の送信を行う。情報取得装置１０１と同一の通信プロトコルの起動要求をデバイスに送信する（ステップＳ８０７：第１の要求手段）。本実施の形態では、ＳＮＭＰを用いて通信プロトコルの起動要求を送信することを想定しているが、それ以外の方法を用いてもよい。

【００６８】

次に、管理装置１１１のＣＰＵ２０１は、デバイスからステップＳ８０７の情報取得装置１０１と同一の通信プロトコルの起動要求に対する実行結果を受信し、実行結果をＲＡＭ２０３またはＨＤ２１１に格納する（ステップＳ８０８）。更に、管理装置１１１のＣＰＵ２０１は、ステップＳ８０８で受信した実行結果を解析し、ステップＳ８０７で要求した通信プロトコルの起動が成功したかどうかを判別する（ステップＳ８０９）。

【００６９】

通信プロトコルの起動が失敗した場合は、ステップＳ８１７に進む。通信プロトコルの起動が成功した場合は、管理装置１１１のＣＰＵ２０１は、情報取得装置１０１と同一の通信プロトコルが稼動しているデバイスに対して、この通信プロトコルに関するデバイス情報を取得するための要求を発行する（ステップＳ８１０）。更に、管理装置１１１のＣＰＵ２０１は、デバイスからステップＳ８１０のデバイス情報取得要求に対する実行結果を受信し、ＲＡＭ２０３またはＨＤ２１１に格納する（ステップＳ８１１）。

【００７０】

次に、管理装置１１１のＣＰＵ２０１は、情報取得装置１０１が図４のステップＳ４０５の処理（デバイスリスト画面に対するユーザ操作の受け付け）を実行するためにアクセス設定の変更が必要かどうかを判別する（ステップＳ８１２：第２の判別手段）。本実施の形態では、管理装置１１１が保持するデバイス情報を情報取得装置１０１に送付し、情報取得装置１０１がデバイス１１３～１１５にアクセスすることを想定している。

【００７１】

本ネットワークシステムでは、ＩＰＶ６ネットワーク環境１１０内で閉じていた管理作業が、ＩＰＶ４ネットワーク環境１００とＩＰＶ６ネットワーク環境１１０を跨いで行われることになるため、通信のセキュリティを確保することが重要となる。そこで、ステップＳ８１２では、ＩＰＶ４ネットワーク環境１００とＩＰＶ６ネットワーク環境１１０を跨いでもセキュリティを維持できる設定をデバイスに対して行う。

【００７２】

図１０に、管理装置１１１で表示するデバイスに対するアクセス設定変更画面１０００の例を示す。管理装置１１１のＣＰＵ２０１は、ステップＳ８１２の処理を実行する前にアクセス設定変更画面１０００をディスプレイ２１０に表示し、ユーザからの入力を受け付ける必要がある。ユーザからアクセス設定変更画面１０００で受け付けた入力値は、ＲＡＭ２０３またはＨＤ２１１に格納しておく。

【００７３】

アクセス設定変更画面１０００には、アクセス設定変更対象デバイス一覧１０１０、チェックボックス１０２０、１０３０、ユーザ名１０３１、認証パスワード１０３２、暗号化パスワード１０３３、コンテキスト名１０３４、ＯＫボタン１０４０が表示されている。

【００７４】

アクセス設定変更対象デバイス一覧１０１０は、デバイス１１３～１１５ごとに、デバイス名１０１１、製品名１０１２、ＩＰＶ４アドレス１０１３、ＩＰＶ６アドレス１０１４を列挙したものである。デバイス名１０１１、製品名１０１２、ＩＰＶ４アドレス１０１３、ＩＰＶ６アドレス１０１４は、それぞれ、図９のデバイス名９１０、製品名９２０、ＩＰＶ４アドレス９３０、ＩＰＶ６アドレス９４０と同一である。

【００７５】

尚、図１０では、ステップＳ８０１で取得した全てのデバイス情報がアクセス設定変更対象となっているが、アクセス設定変更対象デバイス一覧１０１０にチェックボックスを設け、ユーザが選択した任意のデバイスをアクセス設定変更対象としてもよい。

【００７６】

アクセス許可リスト追加チェックボックス１０２０（指示手段）がユーザによりチェックされると、管理装置１１１のＣＰＵ２０１は次の処理を行う。ステップＳ８０２でＲＡＭ２０３またはＨＤ２１１に格納しておいた情報取得装置１０１のＩＰアドレスをデバイスに送付し、デバイスが持つアクセス許可リストに情報取得装置１０１のＩＰアドレスを追加（登録）する。

【００７７】

ＳＮＭＰｖ３認証情報設定チェックボックス１０３０（設定手段）がユーザによりチェックされると、管理装置１１１のＣＰＵ２０１は次の処理を行う。ＳＮＭＰｖ３認証を行うために必要な情報の設定を行う。即ち、デバイスから情報を取得する際のアクセス方法をＳＮＭＰｖ３認証を用いたアクセス方法に変更することをデバイスに要求する。ユーザ名１０３１、認証パスワード１０３２、暗号化パスワード１０３３、コンテキスト名１０３４は、ＳＮＭＰｖ３認証を行うために必要な情報である。

【００７８】

尚、ＳＮＭＰｖ３認証を行うために必要な情報としては、上記のユーザ名１０３１～コンテキスト名１０３４以外にも、例えばユーザによる情報参照範囲を規定するための「スコープ」等を持たせることも可能である。また、図１０では、全てのデバイスに同一のＳＮＭＰｖ３認証情報を設定するような構成となっているが、デバイスごとに異なる値を設定することも可能である。

【００７９】

ユーザがＯＫボタン１０４０を押下すると、アクセス設定変更画面１０００に入力された値がＲＡＭ２０３またはＨＤ２１１に格納される。デバイスにおけるアクセス許可リストへの追加手順、ＳＮＭＰｖ３認証情報設定手順については、後述する。

【００８０】

図８ｂに戻り、管理装置１１１のＣＰＵ２０１は、ユーザによりアクセス設定変更画面１０００から入力されたアクセス設定変更情報を確認するために、ＲＡＭ２０３またはＨＤ２１１の格納情報を確認する（ステップＳ８１２）。アクセス許可リスト追加チェックボックス１０２０、ＳＮＭＰｖ３認証情報設定チェックボックス１０３０が共にチェックされていないと判断した場合は、ステップＳ８１６に進む。

【００８１】

アクセス許可リスト追加チェックボックス１０２０またはＳＮＭＰｖ３認証情報設定チェックボックス１０３０がチェックされていると判断した場合は、管理装置１１１のＣＰＵ２０１は次の送信を行う。ユーザにより入力されたアクセス設定変更画面１０００に対する入力値に従って、デバイスに対してアクセス設定の変更要求（アクセス許可リストに対する情報取得装置１０１のＩＰアドレスの登録）を送信する（ステップＳ８１３：第２の要求手段）。更に、管理装置１１１のＣＰＵ２０１は、ステップＳ８１３で送信したアクセス設定の変更要求の結果をデバイスから受信し、ＲＡＭ２０３またはＨＤ２１１に格納する（ステップＳ８１４）。

【００８２】

次に、管理装置１１１のＣＰＵ２０１は、ステップＳ８１４でデバイスから受信したアクセス設定の変更要求の結果を解析し、デバイスでのアクセス設定の変更が成功したかどうかを判別する（ステップＳ８１５）。デバイスでのアクセス設定の変更が失敗した場合は、ステップＳ８１７に進む。デバイスでのアクセス設定の変更が成功した場合は、管理装置１１１のＣＰＵ２０１は、デバイス情報テーブル９００を用いて、ステップＳ８０２で受信した情報取得装置１０１からのデバイス情報取得要求に対する応答を作成する（ステップＳ８１６：作成手段）。作成する応答の例は図６で説明した通りである。その後、ステップＳ８１８に進む。

【００８３】

ＳＮＭＰｖ３認証情報設定チェックボックス１０３０がチェックされた状態でステップＳ８１３の処理が実施された場合、図９の情報取得方法９５０の値「ＳＮＭＰ」が「ＳＮＭＰｖ３」に書き換えられている。このため、ステップＳ８１６で作成される応答の情報取得方法６３５の値も「ＳＮＭＰｖ３」となる。図６のデバイス情報６３０に格納されるデバイス情報は、情報取得装置１０１と通信可能なデバイスの情報のみとなる。

【００８４】

ステップＳ８０６の判定がＮＯの場合、或いはステップＳ８０９の判定がＮＯの場合、或いはステップＳ８１５の判定がＮＯの場合は、管理装置１１１のＣＰＵ２０１は、発生したエラー情報を明記した応答を作成する（ステップＳ８１７）。エラーの明記方法は図６を用いて説明済みである。その後、ステップＳ８１８に進む。

【００８５】

管理装置１１１のＣＰＵ２０１は、ステップＳ８１６またはステップＳ８１７で作成した応答を情報取得装置１０１に送付する（ステップＳ８１８：送付手段）。情報取得装置１０１は、図４のステップＳ４０２で管理装置１１１からステップＳ８１８で送付される応答を受信する。これにより、本処理を終了する。

【００８６】

＜デバイスの処理＞

次に、デバイスが管理装置１１１と情報取得装置１０１からの各種要求を受信した際に実行する処理を図１１ａ、図１１ｂ、図１２、図１３に基づき説明する。

【００８７】

図１１ａ、図１１ｂは、デバイスが管理装置１１１と情報取得装置１０１からの各種要求を受信した際に実行する処理を示すフローチャートである。本処理はデバイス１１３～１１５のコア部３１１の全体制御の下に実行される。尚、本実施の形態ではデバイス１１３が本処理を実行すると仮定して説明する。

【００８８】

図１１ａ、図１１ｂにおいて、デバイス１１３のコア部３１１は、管理装置１１１が図８ａのステップＳ８０１で発行するデバイス探索要求を受信する（ステップＳ１１０１）。次に、デバイス１１３のコア部３１１は、デバイス探索要求に対する応答を管理装置１１１に返信する（ステップＳ１１０２）。返信する応答は図９で説明済みである。次に、デバイス１１３のコア部３１１は、管理装置１１１が図８ａのステップＳ８０７で送信する通信プロトコルの起動要求を受信する（ステップＳ１１０３）。

【００８９】

次に、デバイス１１３のコア部３１１は、ステップＳ１１０３で受信した起動要求があった通信プロトコルを起動可能かどうかを判別する（ステップＳ１１０４）。起動要求があった通信プロトコルを起動することができない場合は、ステップＳ１１０６に進む。起動要求があった通信プロトコルをデバイス１１３がサポートしており起動することが可能である場合は、デバイス１１３のコア部３１１は、起動要求があった通信プロトコルを起動する（ステップＳ１１０５）。

【００９０】

次に、デバイス１１３のコア部３１１は、ステップＳ１１０３で受信した起動要求に対する返信として、ステップＳ１１０４、ステップＳ１１０５の実行結果を管理装置１１１に返信する（ステップＳ１１０６）。具体的には、ステップＳ１１０３で受信した起動要求があった通信プロトコルを起動することができた場合は、実行結果として「成功」を管理装置１１１に返信する。それ以外の場合は、実行結果として「失敗」を管理装置１１１に返信する。

【００９１】

次に、デバイス１１３のコア部３１１は、管理装置１１１が図８ｂのステップＳ８１０で発行する、通信プロトコルに関するデバイス情報取得要求を受信する（ステップＳ１１０７）。次に、デバイス１１３のコア部３１１は、取得要求があった、通信プロトコルに関するデバイス情報を管理装置１１１に返信する（ステップＳ１１０８）。次に、デバイス１１３のコア部３１１は、管理装置１１１が図８ｂのステップＳ８１３で送信する、アクセス設定変更要求を受信する（ステップＳ１１０９）。次に、デバイス１１３のコア部３１１は、デバイス１１３自身のアクセス設定を変更し、設定変更結果を管理装置１１１に返信する。

【００９２】

図１２に、管理装置１１１からの要求に従ってデバイス１１３のアクセス設定を変更した際のアクセス許可リストの例を示す。アクセス許可リスト１２００は、例えば外部記憶装置３０７に格納され、アクセス許可ＩＰアドレス１２１０（ＩＰアドレス１２０１、１２０２、１２０３）を有する。ＩＰアドレス１２０１、１２０２、１２０３は、デバイス１１３へのアクセスが許可されているＩＰアドレスの例である。

【００９３】

本実施の形態では、図８ａのステップＳ８０２で説明したように、ＩＰアドレス１２０２として情報取得装置１０１のＩＰＶ４アドレス（“１２３．１２３．１２３．１０１”）が格納されている。尚、本実施の形態では、ＩＰＶ４アドレスとＩＰＶ６アドレスが混在したアクセス許可リストを例示しているが、これに限定されるものではない。ＩＰＶ４アドレス、ＩＰＶ６アドレスごとにアクセス許可リストを用意してもよい。

【００９４】

図１３に、管理装置１１１からの要求に従ってデバイス１１３のアクセス設定を変更した際のＳＮＭＰｖ３認証情報設定テーブルを示す。ＳＮＭＰｖ３認証情報設定テーブル１３００は、例えば外部記憶装置３０７に格納され、ユーザ名１３０１、認証パスワード１３０２、暗号化パスワード１３０３、コンテキスト名１３０４を有する。ユーザ名１３０１、認証パスワード１３０２、暗号化パスワード１３０３、コンテキスト名１３０４は、それぞれ、図１０のユーザ名１０３１、認証パスワード１０３２、暗号化パスワード１０３３、コンテキスト名１０３４に対応する。

【００９５】

尚、ＳＮＭＰｖ３認証情報設定テーブル１３００の構成要素としては、上記のユーザ名１３０１～コンテキスト名１３０４以外にも、例えばユーザによる情報参照範囲を規定するための「スコープ」等を持たせることも可能である。また、図１３では、デバイス１１３に対してＳＮＭＰｖ３認証情報を１つだけ設定できるような構成になっているが、複数のＳＮＭＰｖ３認証情報を設定できるような構成となっていてもよい。

【００９６】

図１１ｂに戻り、デバイス１１３のコア部３１１は、情報取得装置１０１が図４のステ

ップＳ４０５で発行する機器制御コマンドを受信する（ステップＳ１１１１）。デバイス１１３が受信する機器制御コマンドの例は図４のステップＳ４０５で記載済みである。次に、デバイス１１３のコア部３１１は、デバイス１１３が機器制御コマンドを実行できるどうかを判別する（ステップＳ１１１２）。

【００９７】

具体的には、デバイス１１３のコア部３１１が、アクセス許可リスト１２００、ＳＮＭＰｖ３認証情報設定テーブル１３００を参照する。その後、デバイス１１３のコア部３１１は、情報取得装置１０１からデバイス１１３へのアクセスが可能かどうかを判定し、その上で機器制御コマンドの処理を実施できるかどうかを判別する。

【００９８】

デバイス１１３が機器制御コマンドを実行できる場合は、デバイス１１３のコア部３１１は、機器制御コマンドを実行し、その実行結果を情報取得装置１０１へ返信する（ステップＳ１１１３）。ステップＳ４０５で説明した機器制御コマンド（１）の例ではデバイス１１３の情報を返信し、機器制御コマンド（２）の例ではデバイス１１３の設定値を変更した上で、その変更結果を返信する。デバイス１１３が機器制御コマンドを実行できない場合は、デバイス１１３のコア部３１１は、機器制御コマンドを実行せず、情報取得装置１０１へエラーを返信する（ステップＳ１１１４）。これにより、本処理を終了する。

【００９９】

以上詳細に説明したように、本実施の形態によれば以下の効果を奏する。ＩＰＶ４ネットワーク環境１００で稼動する情報取得装置は、情報取得装置自身が所属するサブネットワークの外の異なるサブネットワーク（ＩＰＶ６ネットワーク環境１１０）に存在する管理装置が有するデバイス情報を取得することが可能となる。

【０１００】

また、情報取得装置は、管理装置から取得したデバイス情報を用いて、情報取得装置自身が所属するサブネットワークの外の異なるサブネットワークに存在するデバイスを適正に管理することが可能となる。

【０１０１】

〔他の実施の形態〕

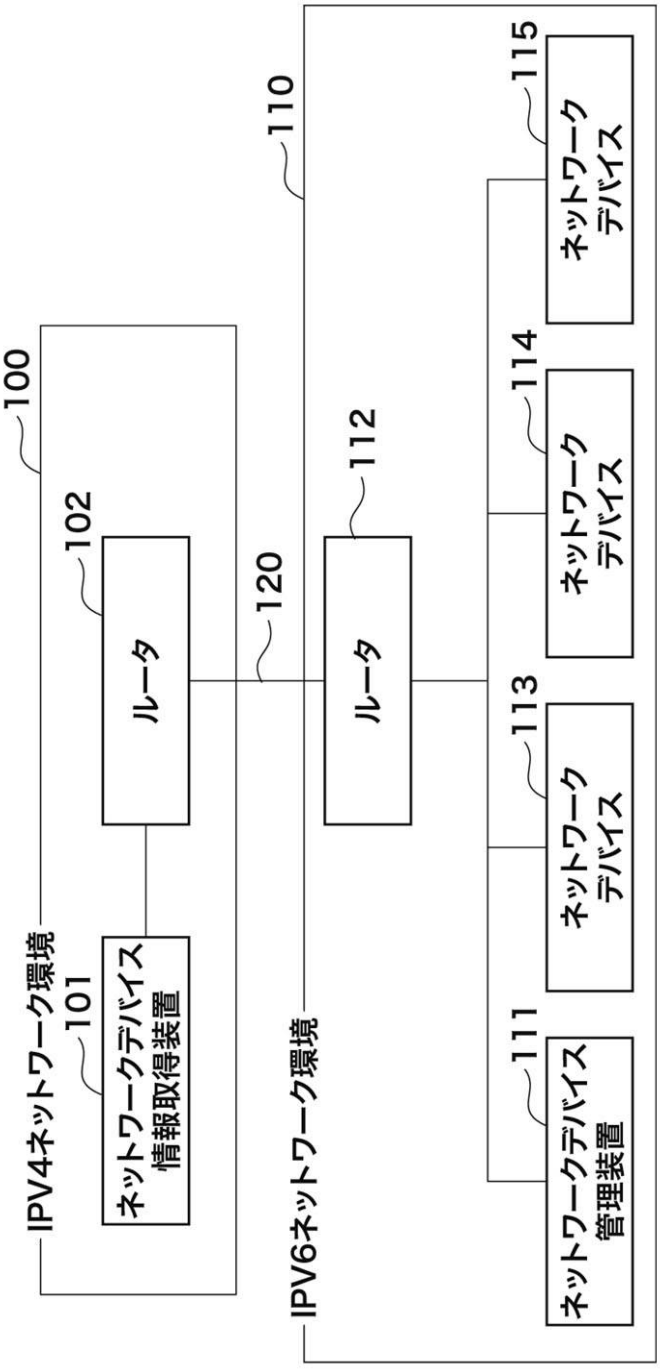
本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。この場合、そのプログラム、及び該プログラムを記憶した記憶媒体は本発明を構成することになる。

【符号の説明】

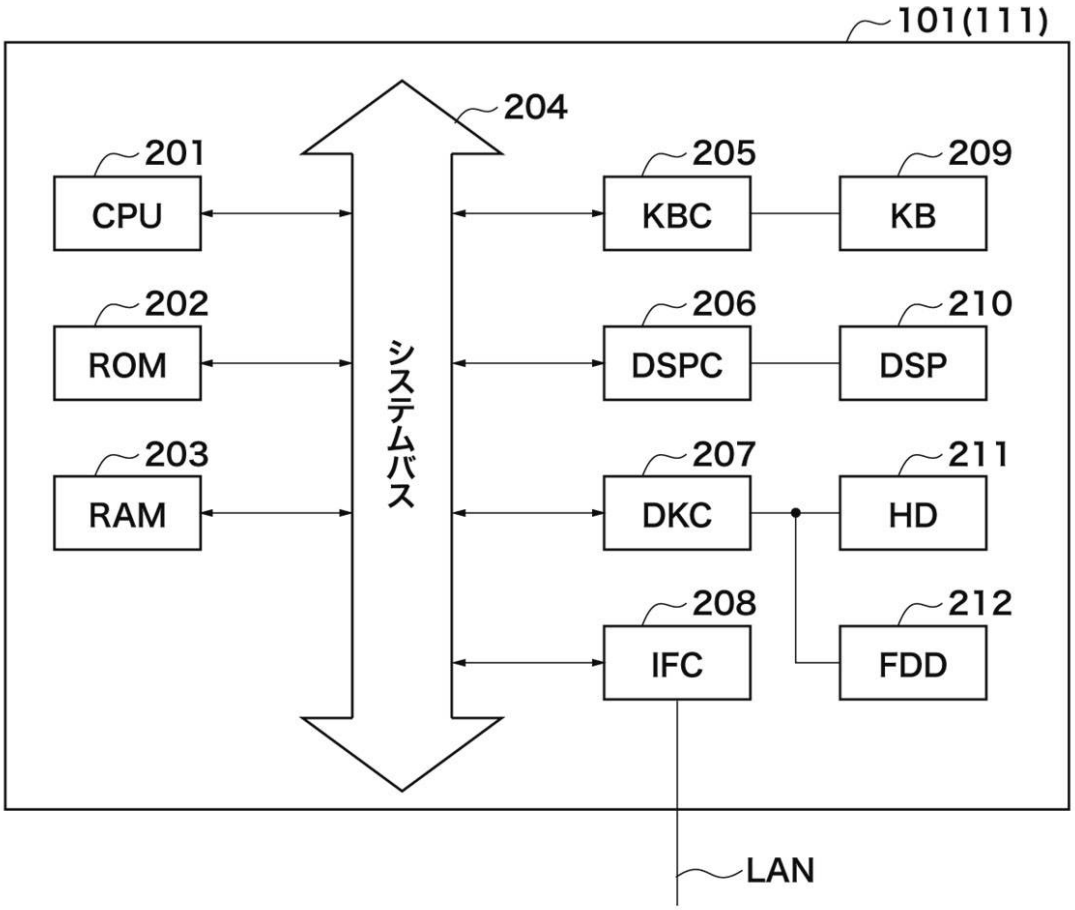
【０１０２】

１００　ＩＰＶ４ネットワーク環境
１０１　ネットワークデバイス情報取得装置
１１３、１１４、１１５　ネットワークデバイス
１１０　ＩＰＶ６ネットワーク環境
１１１　ネットワークデバイス管理装置

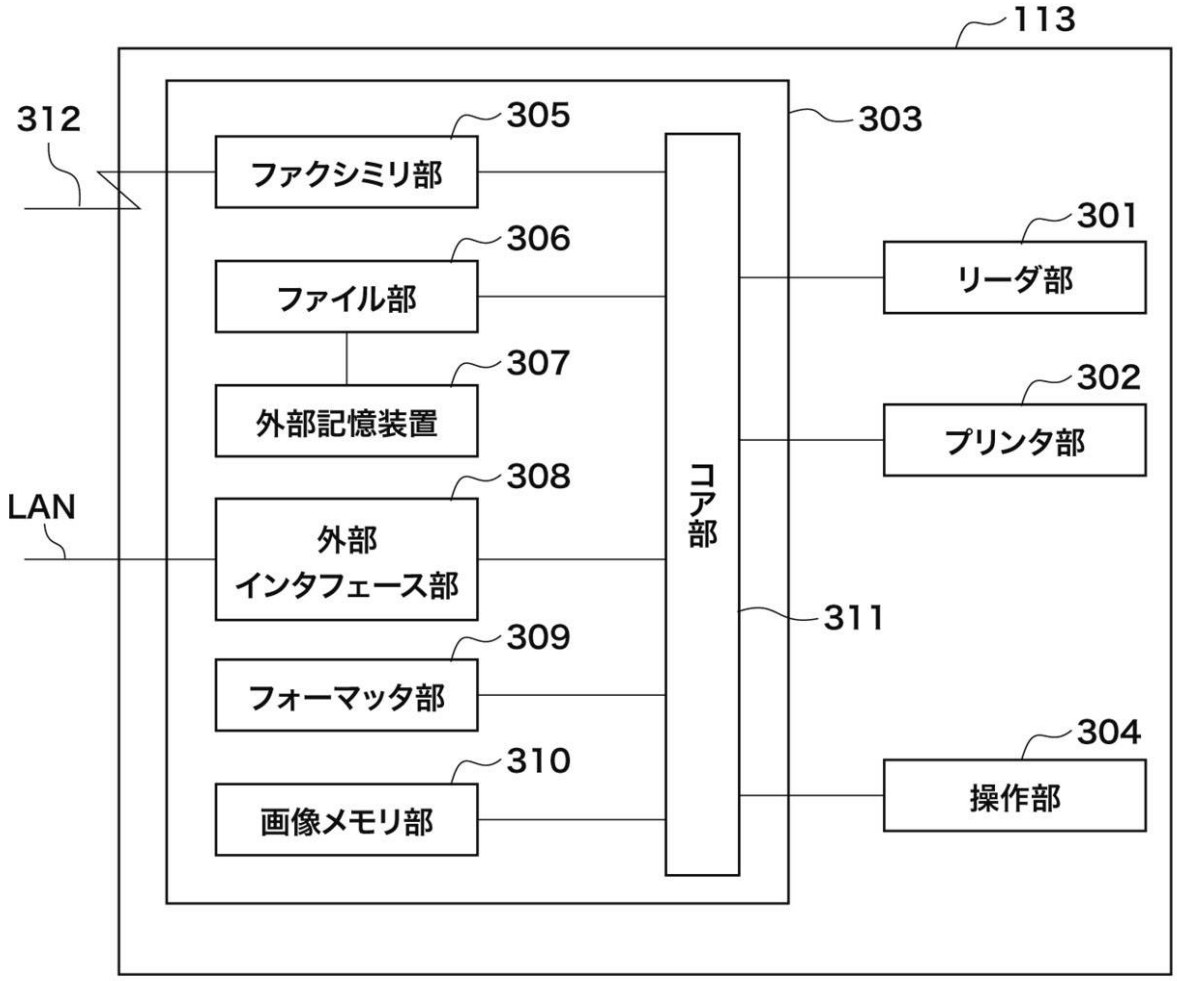
【図１】


IPV4ネットワーク環境
100
ネットワークデバイス
情報取得装置
101
ルータ
102
120
IPV6ネットワーク環境
110
ルータ
112
ネットワーク
デバイス
111
ネットワーク
デバイス
113
ネットワーク
デバイス
114
ネットワーク
デバイス
115

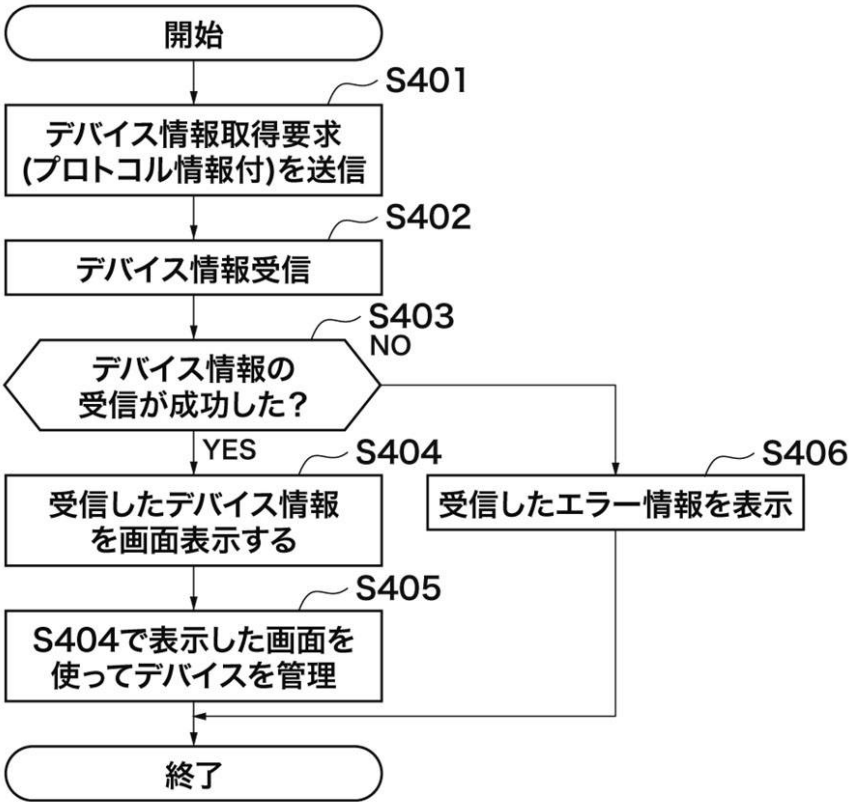
【図２】


101(111)
204
201
CPU
202
ROM
203
RAM
システムバス
205
KBC
206
DSPC
207
DKC
208
IFC
209
KB
210
DSP
211
HD
212
FDD
LAN

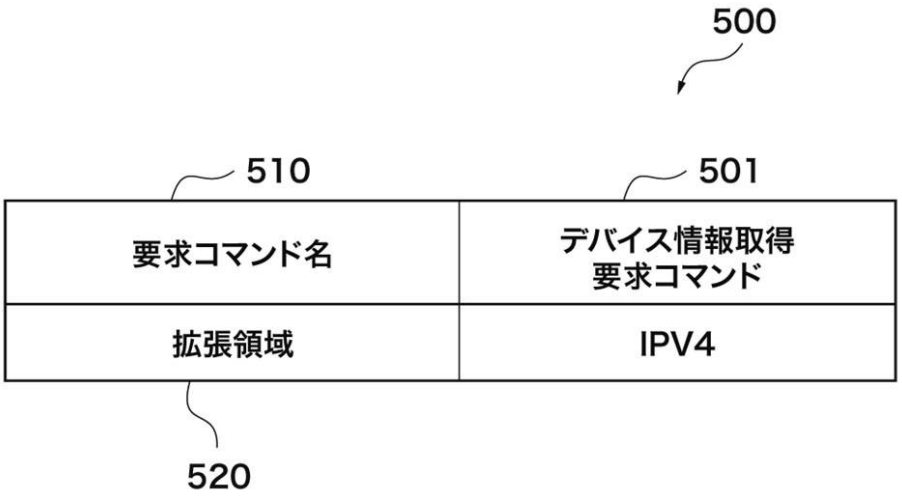
【図３】


113
312
305
ファクシミリ部
303
306
ファイル部
301
リーダ部
307
外部記憶装置
302
プリンタ部
LAN
308
外部
インタフェース部
コア部
311
309
フォーマッタ部
304
310
画像メモリ部
操作部

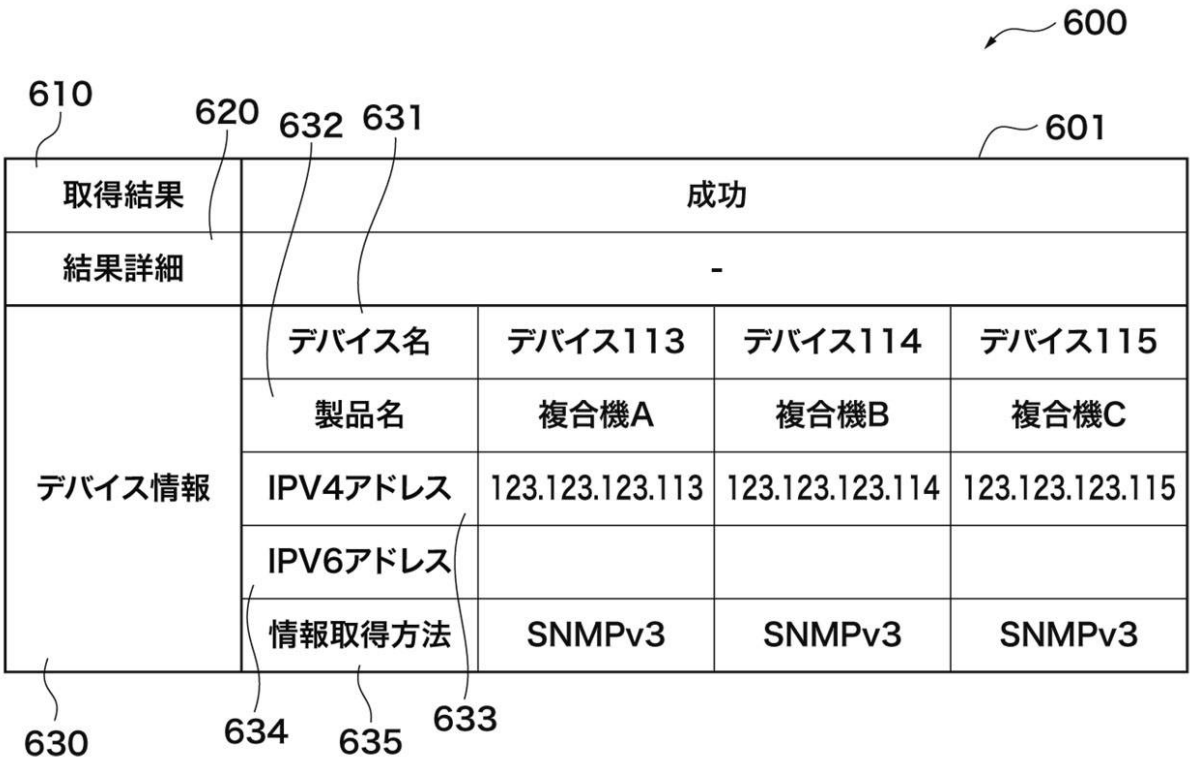
【図４】


開始
S401
デバイス情報取得要求
(プロトコル情報付)を送信
S402
デバイス情報受信
S403
NO
デバイス情報の
受信が成功した？
YES
S404
受信したデバイス情報
を画面表示する
S405
S404で表示した画面を
使ってデバイスを管理
S406
受信したエラー情報を表示
終了

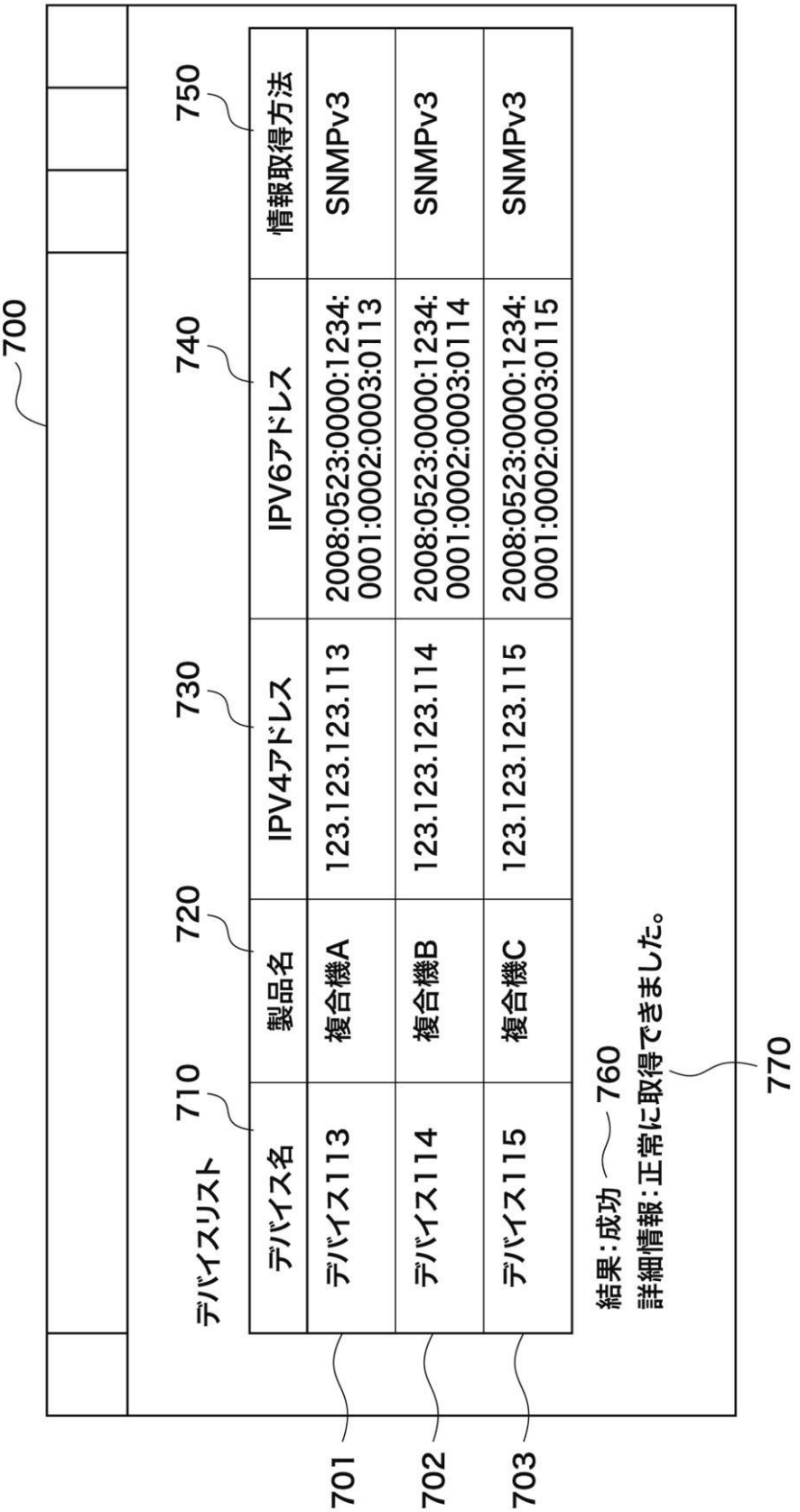
【図５】


500
510
501
要求コマンド名
デバイス情報取得
要求コマンド
拡張領域
IPV4
520

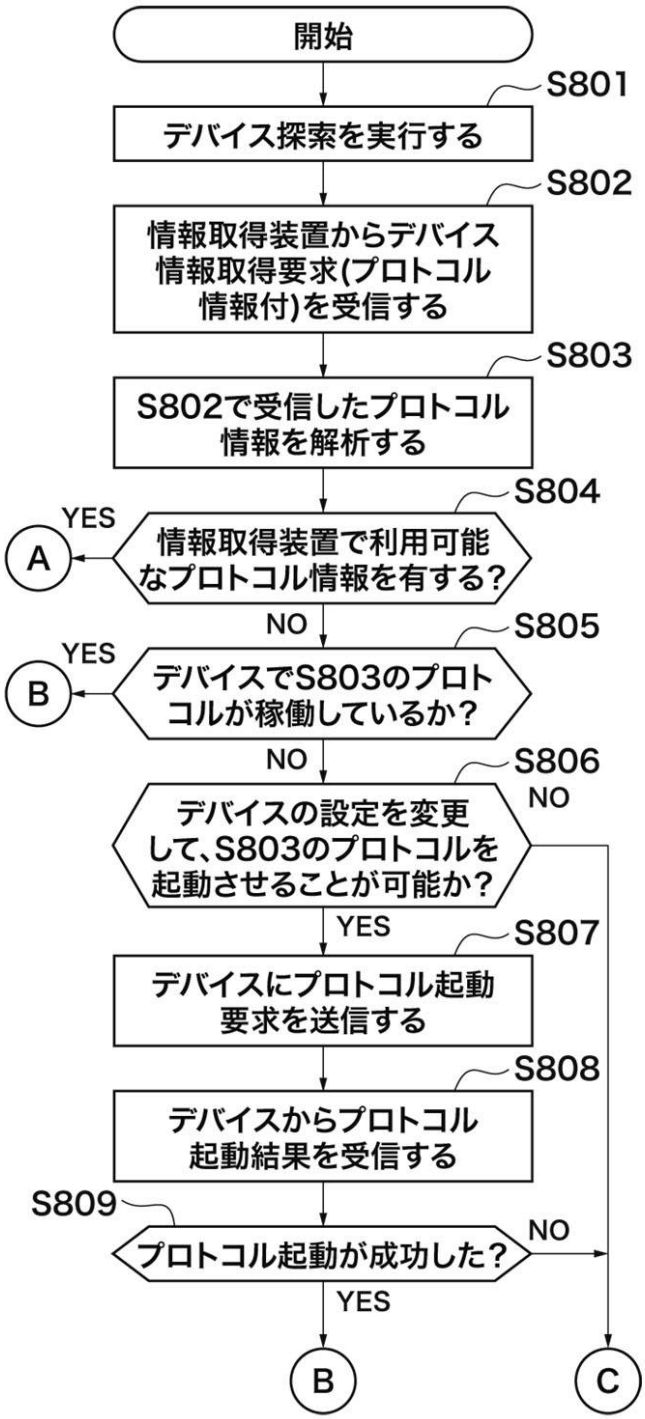
【図６】


600
601
610
620
632
631
取得結果
成功
結果詳細
-
デバイス情報
デバイス名
デバイス113
デバイス114
デバイス115
製品名
複合機A
複合機B
複合機C
IPV4アドレス
123.123.123.113
123.123.123.114
123.123.123.115
IPV6アドレス
情報取得方法
SNMPv3
SNMPv3
SNMPv3
630
634
635
633

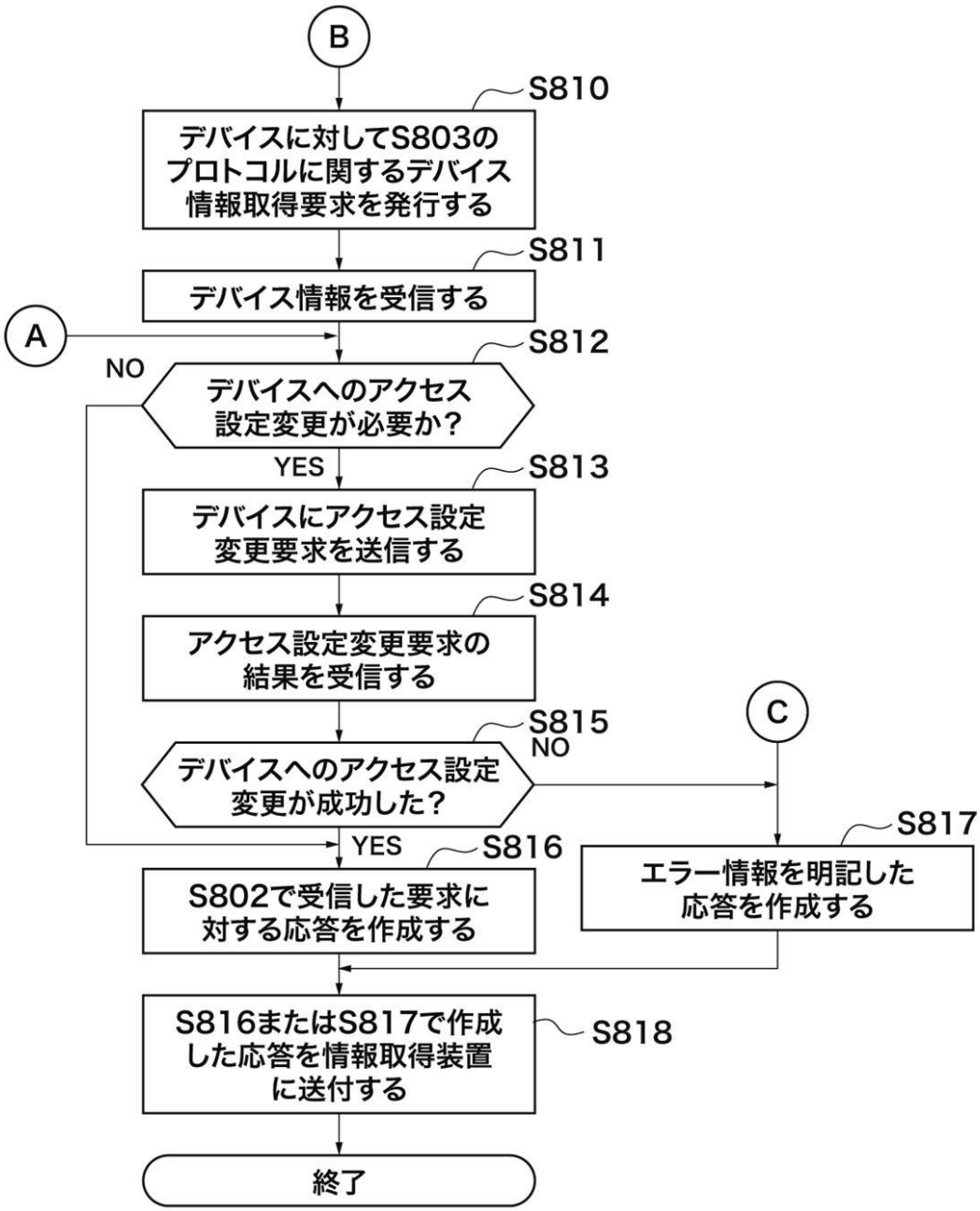
【図７】


700
デバイスリスト
710
720
730
740
750
デバイス名
製品名
IPV4アドレス
IPV6アドレス
情報取得方法
デバイス113
複合機A
123.123.123.113
2008:0523:0000:1234:0001:0002:0003:0113
SNMPv3
デバイス114
複合機B
123.123.123.114
2008:0523:0000:1234:0001:0002:0003:0114
SNMPv3
デバイス115
複合機C
123.123.123.115
2008:0523:0000:1234:0001:0002:0003:0115
SNMPv3
701
702
703
結果：成功
760
詳細情報：正常に取得できました。
770

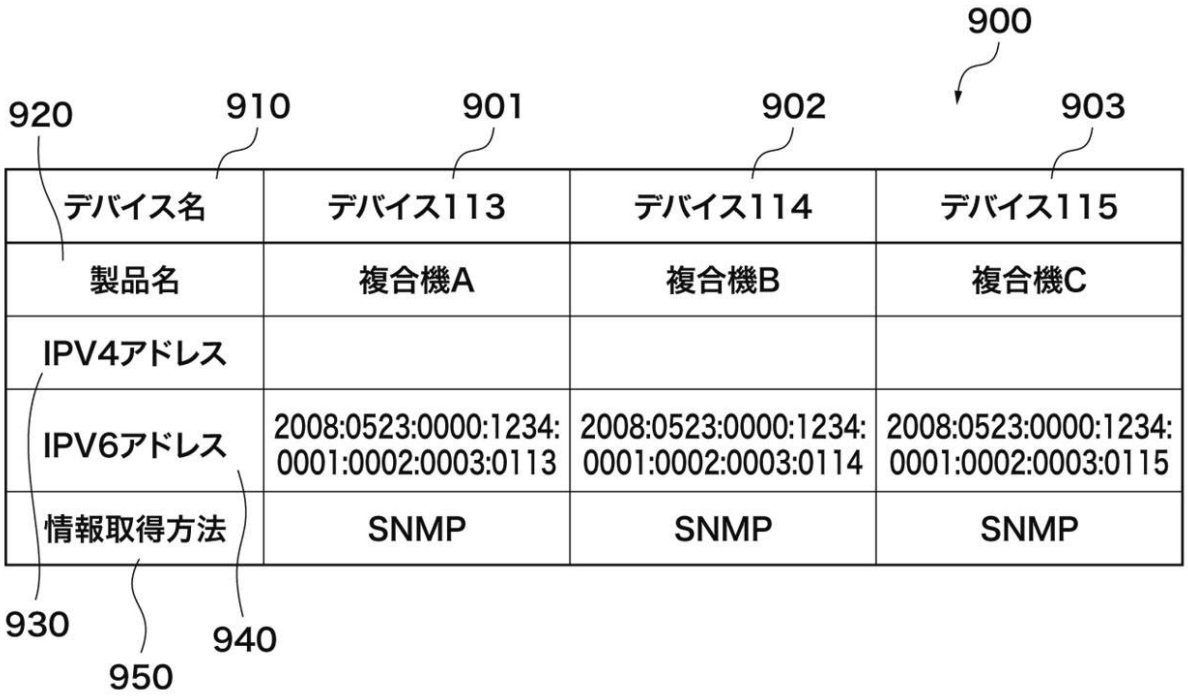
【図８ａ】


開始
S801
デバイス探索を実行する
S802
情報取得装置からデバイス情報取得要求(プロトコル情報付)を受信する
S803
S802で受信したプロトコル情報を解析する
S804
情報取得装置で利用可能なプロトコル情報を有する?
YES
A
NO
S805
デバイスでS803のプロトコルが稼働しているか?
YES
B
NO
S806
デバイスの設定を変更して、S803のプロトコルを起動させることが可能か?
NO
YES
S807
デバイスにプロトコル起動要求を送信する
S808
デバイスからプロトコル起動結果を受信する
S809
プロトコル起動が成功した?
NO
YES
B
C

【図８ｂ】

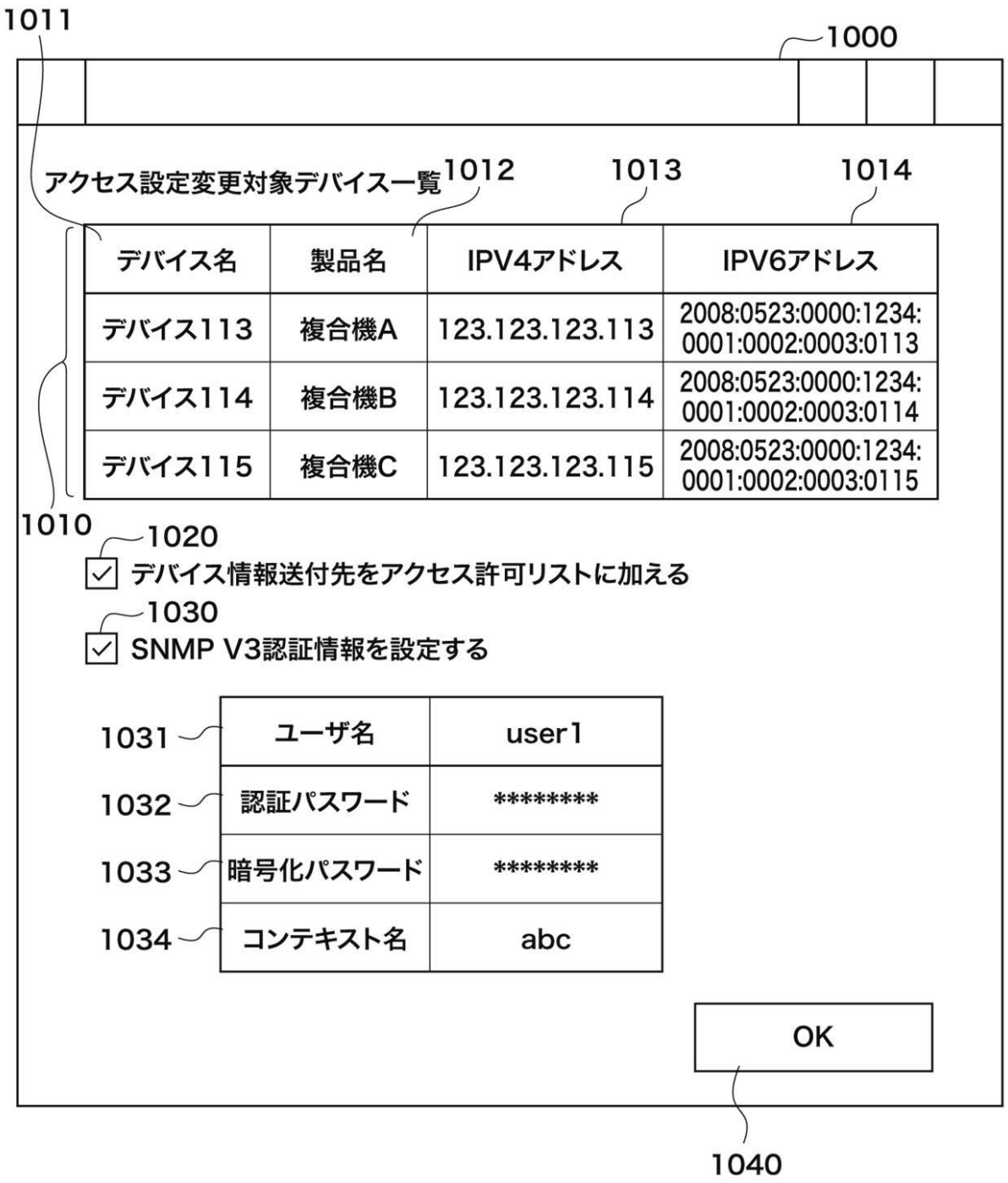

B
S810
デバイスに対してS803のプロトコルに関するデバイス情報取得要求を発行する
S811
デバイス情報を受信する
A
S812
NO
デバイスへのアクセス設定変更が必要か？
YES
S813
デバイスにアクセス設定変更要求を送信する
S814
アクセス設定変更要求の結果を受信する
C
S815
NO
デバイスへのアクセス設定変更が成功した？
YES
S816
S802で受信した要求に対する応答を作成する
S817
エラー情報を明記した応答を作成する
S816またはS817で作成した応答を情報取得装置に送付する
S818
終了

【図９】

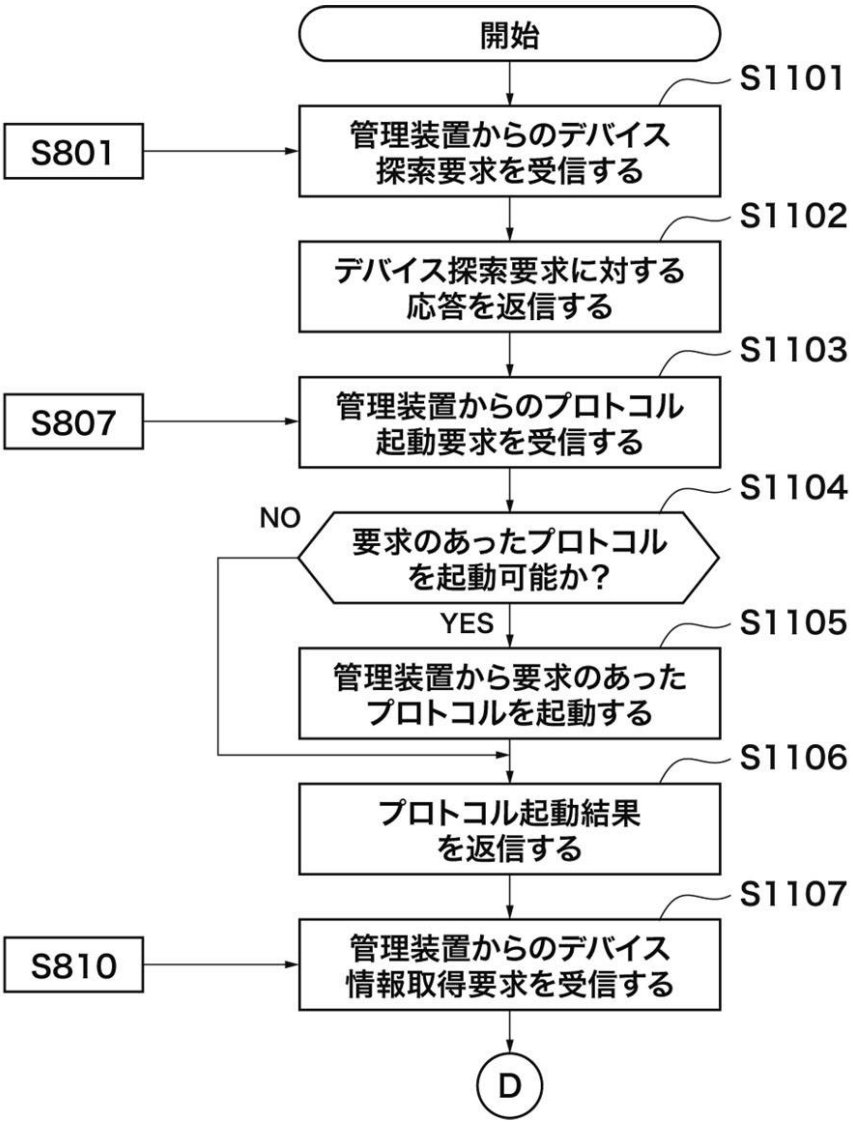


デバイス名	デバイス113	デバイス114	デバイス115
製品名	複合機A	複合機B	複合機C
IPV4アドレス			
IPV6アドレス	2008:0523:0000:1234:0001:0002:0003:0113	2008:0523:0000:1234:0001:0002:0003:0114	2008:0523:0000:1234:0001:0002:0003:0115
情報取得方法	SNMP	SNMP	SNMP

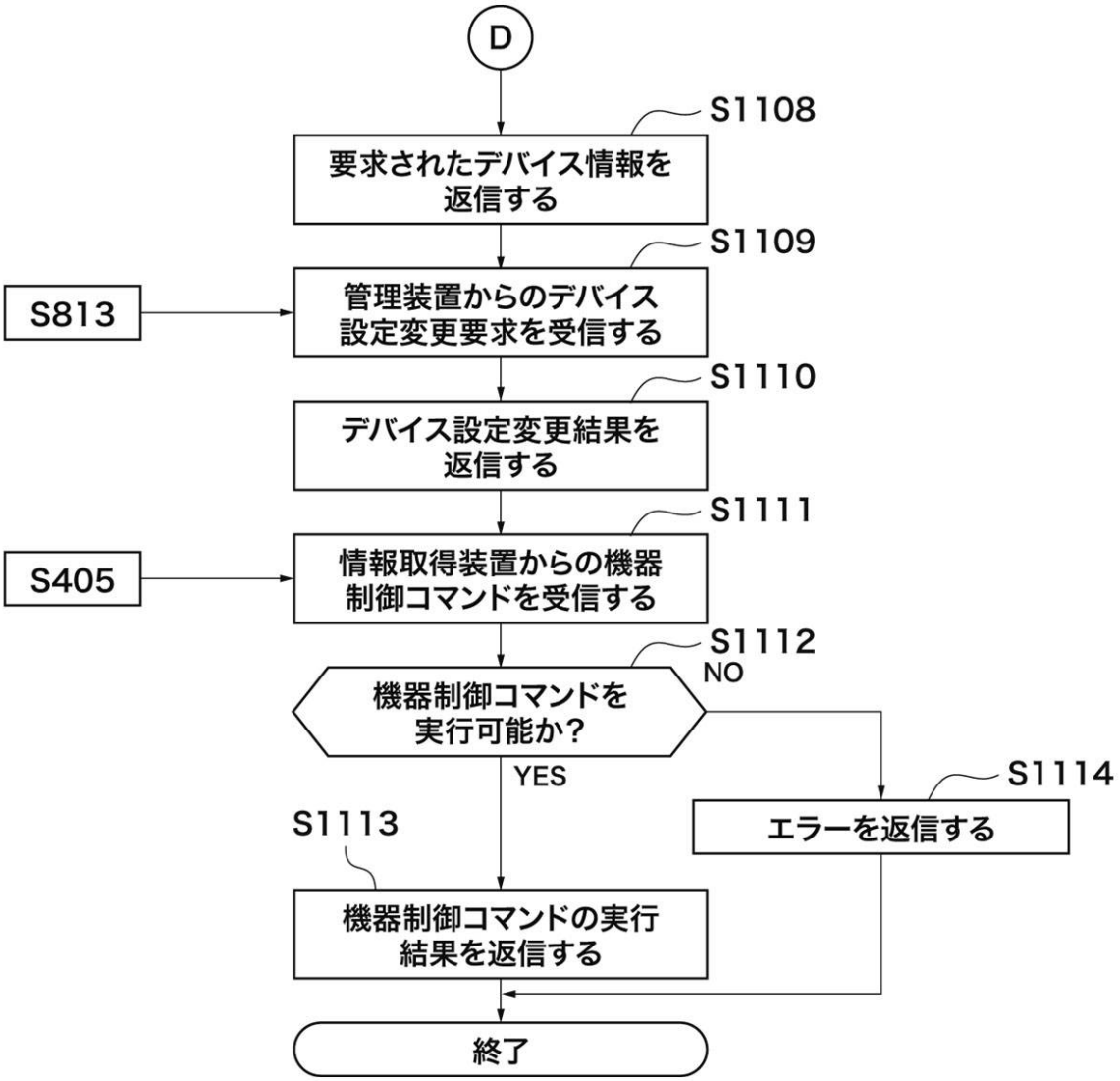
【図１０】


1011
1000
アクセス設定変更対象デバイス一覧
1012
1013
1014
デバイス名
製品名
IPV4アドレス
IPV6アドレス
デバイス113
複合機A
123.123.123.113
2008:0523:0000:1234:0001:0002:0003:0113
デバイス114
複合機B
123.123.123.114
2008:0523:0000:1234:0001:0002:0003:0114
デバイス115
複合機C
123.123.123.115
2008:0523:0000:1234:0001:0002:0003:0115
1010
1020
デバイス情報送付先をアクセス許可リストに加える
1030
SNMP V3認証情報を設定する
1031
ユーザ名
user1
1032
認証パスワード
****
1033
暗号化パスワード
****
1034
コンテキスト名
abc
OK
1040

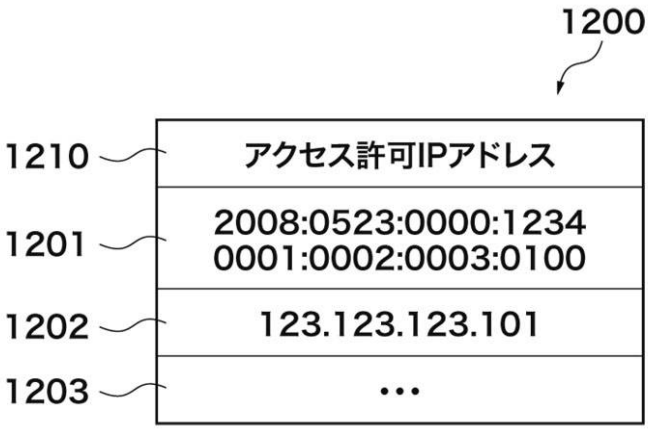
【図１１ａ】


開始
S1101
S801
管理装置からのデバイス
探索要求を受信する
S1102
デバイス探索要求に対する
応答を返信する
S1103
S807
管理装置からのプロトコル
起動要求を受信する
S1104
NO
要求のあったプロトコル
を起動可能か？
YES
S1105
管理装置から要求のあった
プロトコルを起動する
S1106
プロトコル起動結果
を返信する
S1107
S810
管理装置からのデバイス
情報取得要求を受信する
D

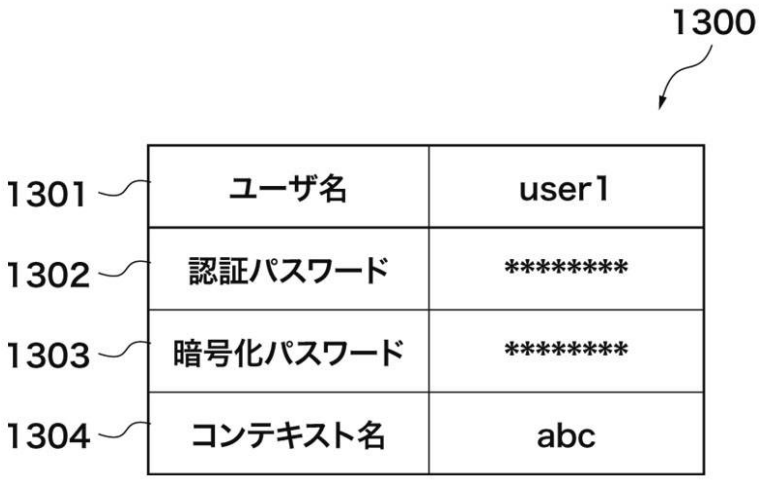
【図１１ｂ】


D
S1108
要求されたデバイス情報を返信する
S1109
S813
管理装置からのデバイス設定変更要求を受信する
S1110
デバイス設定変更結果を返信する
S1111
S405
情報取得装置からの機器制御コマンドを受信する
S1112
NO
機器制御コマンドを実行可能か？
YES
S1114
エラーを返信する
S1113
機器制御コマンドの実行結果を返信する
終了

【図１２】


1200
1210
アクセス許可IPアドレス
1201
2008:0523:0000:1234
0001:0002:0003:0100
1202
123.123.123.101
1203
・・・

【図１３】


1300
1301
ユーザ名
user1
1302
認証パスワード
****
1303
暗号化パスワード
****
1304
コンテキスト名
abc

フロントページの続き

(56)参考文献 特開２００７－３００６９０（ＪＰ，Ａ）
特開２００６－０１１７０３（ＪＰ，Ａ）
特開２００５－３５１９５８（ＪＰ，Ａ）
特開２００８－１０２８７２（ＪＰ，Ａ）
特開２００６－０８５６４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００