(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4946302号
(P4946302)
(45)発行日　平成24年6月6日(2012.6.6)　(24)登録日　平成24年3月16日(2012.3.16)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 357A

請求項の数 11　(全 30 頁)

(21)出願番号　特願2006-256165(P2006-256165)
(22)出願日　平成18年9月21日(2006.9.21)
(65)公開番号　特開2007-299368(P2007-299368A)
(43)公開日　平成19年11月15日(2007.11.15)
審査請求日　平成21年6月4日(2009.6.4)
(31)優先権主張番号　特願2006-101294(P2006-101294)
(32)優先日　平成18年4月3日(2006.4.3)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　島　敏博
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内
(72)発明者　阿部　卓弥
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内
(72)発明者　松本　明
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内

最終頁に続く

(54)【発明の名称】ネットワークに接続されたデバイスの監視装置および監視方法

(57)【特許請求の範囲】
【請求項１】
ネットワークに接続された１つ以上のネットワークデバイスの監視装置であって、
前記ネットワークデバイスは、
個々のネットワークデバイスを識別可能な個体識別情報を格納する個体識別情報格納部と、
所定のネットワークプロトコルに従って、前記ネットワーク上にメッセージを送出するメッセージ送出部であって、前記ネットワークデバイスの時刻を前記ネットワークに接続された時刻サーバに同期させるための同期メッセージを送出する時刻同期部を有するメッセージ送出部と、
前記ネットワークデバイスに関する情報であって時間の経過とともに変化する管理情報を格納する管理情報格納部と、
を備えており、
前記監視装置は、
前記時刻サーバの機能を提供する時刻サーバ実行部と、
前記ネットワークデバイスの前記メッセージ送出部が前記ネットワーク上に送出するメッセージを伝送する通信データであって、前記時刻同期部が時刻の同期を行う際に前記時刻サーバ実行部に送信する同期メッセージを伝送する通信データから、前記ネットワークデバイスを前記ネットワーク上で特定するためのネットワーク識別子であって単一のネットワークデバイスに対して割り当てられる値が変更可能なネットワーク識別子を抽出する

ネットワーク識別子抽出部と、
前記ネットワーク識別子抽出部により抽出された前記ネットワーク識別子により特定されるネットワークデバイスである特定デバイス宛に、前記ネットワークデバイスの前記固体識別情報を要求することによって、前記メッセージを送信した前記ネットワークデバイスから前記個体識別情報を取得する個体識別情報取得部と、
前記個体識別情報取得部が取得した個体識別情報に基づいて前記特定デバイスが前記監視装置による監視対象となる監視対象デバイスであるか否かを判断する監視対象判定部と、
前記監視対象判定部により前記特定デバイスが監視対象デバイスであると判断された場合、前記特定デバイスの管理情報格納部から前記管理情報を取得する管理情報取得部と、
を備える、ネットワークデバイスの監視装置。
【請求項２】
前記固体識別情報は機種名および製造番号を含む、請求項１記載のネットワークデバイスの監視装置。
【請求項３】
請求項１または請求項２に記載のネットワークデバイスの監視装置であって、
前記ネットワークデバイスの前記時刻同期部は、前記ネットワークデバイスの起動の際に前記ネットワークデバイスと前記時刻サーバとの時刻の同期を行う、ネットワークデバイスの監視装置。
【請求項４】
請求項１ないし請求項３のいずれか一項に記載のネットワークデバイスの監視装置であって、
前記ネットワークデバイスの前記時刻同期部は、所定の時間間隔に少なくとも１回、前記ネットワークデバイスと前記時刻サーバとの時刻の同期を行う、ネットワークデバイスの監視装置。
【請求項５】
請求項１ないし請求項４のいずれか一項に記載のネットワークデバイスの監視装置であって、
前記メッセージ送出部により送出される前記メッセージは、前記ネットワークデバイスを前記ネットワーク上で使用可能とするために、前記ネットワークデバイスの存在を前記ネットワークに対して通知するメッセージを含む、ネットワークデバイスの監視装置。
【請求項６】
請求項１ないし５のいずれか記載のネットワークデバイスの監視装置であって、さらに、
前記監視対象デバイスに関する情報を前記監視対象デバイスの前記個体識別情報に対応付けて格納する監視対象情報格納部を有しており、
前記監視対象判定部は、前記個体識別情報取得部が取得した個体識別情報と、前記監視対象情報格納部に格納された監視対象情報とを照合することにより、前記特定デバイスが前記監視対象デバイスか否かを判断する、ネットワークデバイスの監視装置。
【請求項７】
請求項６記載のネットワークデバイスの監視装置であって、
前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスを監視対象に追加するか否かの前記監視装置のユーザからの指示に基づいて、前記特定デバイスに関する情報と前記特定デバイスの前記個体識別情報とを前記監視対象情報に登録する、ネットワークデバイスの監視装置。
【請求項８】
請求項６記載のネットワークデバイスの監視装置であって、
前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスが所定の監視対象追加条件に合致するか否かを判断し、前記監視対象追加条件に合致する場合、前記特定デバイスに関する情報と前記特定デバイスの

前記個体識別情報とを前記監視対象情報に登録する、ネットワークデバイスの監視装置。
【請求項９】
請求項６記載のネットワークデバイスの監視装置であって、
前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスの前記個体識別情報を前記ネットワークを介して管理サーバに送信し、前記管理サーバから受信した前記特定デバイスを監視対象に追加するか否かを表す情報に基づいて、前記特定デバイスに関する情報と前記特定デバイスの前記個体識別情報とを前記監視対象情報に登録する、ネットワークデバイスの監視装置。
【請求項１０】
ネットワークに接続された１つ以上のネットワークデバイスの監視方法であって、
前記ネットワークデバイスは、
個々のネットワークデバイスを識別可能な個体識別情報を格納する個体識別情報格納部と、
所定のネットワークプロトコルに従って、前記ネットワーク上にメッセージを送出するメッセージ送出部であって、前記ネットワークデバイスの時刻を前記ネットワークに接続された時刻サーバに同期させるための同期メッセージを送出する時刻同期部を有するメッセージ送出部と、
前記ネットワークデバイスに関する情報であって時間の経過とともに変化する管理情報を格納する管理情報格納部と、
を備えており、
前記監視方法は、
前記時刻サーバの機能を提供する時刻サーバ実行工程と、
（ａ）前記ネットワークデバイスの前記メッセージ送出部前記ネットワーク上に送出するメッセージを伝送する通信データであって、前記時刻同期部が時刻の同期を行う際に前記時刻サーバ実行部に送信する同期メッセージを伝送する通信データから、前記ネットワークデバイスを前記ネットワーク上で特定するためのネットワーク識別子であって単一のネットワークデバイスに対して割り当てられる値が変更可能なネットワーク識別子を抽出する工程と、
（ｂ）前記工程（ａ）において抽出された前記ネットワーク識別子により特定されるネットワークデバイスである特定デバイス宛に、前記ネットワークデバイスの前記固体識別情報を要求することによって、前記メッセージを送信した前記ネットワークデバイスから前記個体識別情報を取得する工程と、
（ｃ）前記工程（ｂ）において取得された個体識別情報に基づいて前記特定デバイスが前記監視装置による監視対象となる監視対象デバイスであるか否かを判断する工程と、
（ｄ）前記工程（ｃ）において前記特定デバイスが監視対象デバイスであると判断された場合、前記特定デバイスの管理情報格納部から前記管理情報を取得する工程と、
を備える、ネットワークデバイスの監視方法。
【請求項１１】
前記固体識別情報は機種名および製造番号を含む、請求項１０記載のネットワークデバイスの監視方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ネットワークに接続されたデバイスから管理情報を取得するデバイス監視技術に関する。
【背景技術】
【０００２】
ネットワークに接続されたプリンタを管理するプリンタ管理システムでは、プリンタの総印刷枚数、障害情報、印刷ジョブ数、印刷ジョブごとに使用された紙の枚数やトナー等の消耗品使用量などの管理情報に基づいて、プリンタのメンテナンスや課金管理等が行わ

れる。このような管理情報を取得するため、ネットワークにはプリンタを監視するためのプリンタ監視装置が接続され、プリンタ監視装置がプリンタからこれらの管理情報を取得する。

【０００３】

プリンタ監視装置による管理情報の取得には、多くの場合、ＳＮＭＰ（Simple Network Management Protocol）を用いて行われる。ＳＮＭＰによる管理情報の取得は、具体的には、プリンタ監視装置がプリンタに管理情報の送信を要求する要求メッセージを送信し、プリンタがプリンタ監視装置に要求メッセージに対して応答する応答メッセージを送信することにより行われる。

【０００４】

【特許文献１】特開２００５－１０８２４１号公報
【特許文献２】特開２００５－４７３５号公報
【特許文献３】特開２００４－１９３６８８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかしながら、ＳＮＭＰでは、メッセージの送受信先はＩＰアドレスによって特定されるためＩＰアドレスが変更されるような環境下においては不都合が生じる。例えば、ＮｅｔＢＩＯＳ名でプリンタ管理を行っている場合は、ＮｅｔＢＩＯＳ名によりプリンタを指定できるため、プリンタのＩＰアドレスがＤＨＣＰ（Dynamic Host Configuration Protocol）により動的に設定される場合がある。また、プリンタの移動で静的に設定されたプリンタのＩＰアドレスが変更された場合、プリンタ監視装置は、監視対象のプリンタにＳＮＭＰのメッセージを送信することができなくなり、管理情報の取得ができなくなるおそれがある。この問題は、ＩＰアドレスによってプリンタが特定される場合の他、一般に、プリンタを特定するための情報が変更される場合に共通する。この問題は、また、プリンタの管理情報を取得するプリンタ監視装置のみならず、ネットワークに接続される個々のデバイスの管理情報を取得するデバイス監視装置に共通する。

【０００６】

本発明は、上述した従来の課題を解決するためになされたものであり、ネットワークデバイスの管理情報をより確実に取得することを目的とする。

【課題を解決するための手段】

【０００７】

上記目的の少なくとも一部を達成するために、本発明のネットワークデバイスの監視装置は、ネットワークに接続された１つ以上のネットワークデバイスの監視装置であって、

前記ネットワークデバイスは、

個々のネットワークデバイスを識別可能な個体識別情報を格納する個体識別情報格納部と、

所定のネットワークプロトコルに従って、前記ネットワーク上にメッセージを送出するメッセージ送出部であって、前記ネットワークデバイスの時刻を前記ネットワークに接続された時刻サーバに同期させるための同期メッセージを送出する時刻同期部を有するメッセージ送出部と、

前記ネットワークデバイスに関する情報であって時間の経過とともに変化する管理情報を格納する管理情報格納部と、

を備えており、

前記監視装置は、

前記時刻サーバの機能を提供する時刻サーバ実行部と、

前記ネットワークデバイスの前記メッセージ送出部が前記ネットワーク上に送出するメッセージを伝送する通信データであって、前記時刻同期部が時刻の同期を行う際に前記時刻サーバ実行部に送信する同期メッセージを伝送する通信データから、前記ネットワークデバイスを前記ネットワーク上で特定するためのネットワーク識別子であって単一のネッ

トワークデバイスに対して割り当てられる値が変更可能なネットワーク識別子を抽出するネットワーク識別子抽出部と、

前記ネットワーク識別子抽出部により抽出された前記ネットワーク識別子により特定されるネットワークデバイスである特定デバイス宛に、前記ネットワークデバイスの前記固体識別情報を要求することによって、前記メッセージを送信した前記ネットワークデバイスから前記個体識別情報を取得する個体識別情報取得部と、

前記個体識別情報取得部が取得した個体識別情報に基づいて前記特定デバイスが前記監視装置による監視対象となる監視対象デバイスであるか否かを判断する監視対象判定部と、

前記監視対象判定部により前記特定デバイスが監視対象デバイスであると判断された場合、前記特定デバイスの管理情報格納部から前記管理情報を取得する管理情報取得部と、を備えることを特徴とする。

【０００８】

この構成によれば、ネットワークデバイスがネットワーク上に送出するメッセージに含まれるネットワーク識別子を抽出される。監視装置は、抽出されたネットワーク識別子を用いることにより、監視対象となるデバイスを特定することができる。そのため、監視装置は、より確実に、監視対象デバイスから管理情報を取得することが可能となる。

【００１０】

一般に、管理情報の取得対象となるネットワークデバイスでは、種々のイベントの発生時刻を正確に記録するため、ネットワークに接続された時刻サーバとの時刻の同期が行われる。そのため、ネットワークデバイスが監視装置と時刻の同期を行うための同期メッセージからネットワーク識別子を抽出することにより、ネットワークデバイスへの新たな機能の追加を抑制しつつ、より確実に、監視対象となるネットワークデバイスのネットワーク識別子を取得することが可能となる。

【００１１】

前記ネットワークデバイスの前記時刻同期部は、前記ネットワークデバイスの起動の際に前記ネットワークデバイスと前記時刻サーバとの時刻の同期を行うものとしても良い。

【００１２】

通常、ネットワーク識別子が変更された場合、ネットワークデバイスは再起動される。そのため、ネットワークデバイスがその起動の際に時刻の同期を行うようにすると、監視装置は、ネットワーク識別子の変更をより確実に把握することができる。そのため、監視装置は、より確実に監視対象デバイスを監視することが可能となる。

【００１３】

前記ネットワークデバイスの前記時刻同期部は、所定の時間間隔に少なくとも１回、前記ネットワークデバイスと前記時刻サーバとの時刻の同期を行うものとしても良い。

【００１４】

この構成によれば、監視装置は、所定の時間間隔に少なくとも１回ネットワーク識別子の変更を把握することができる。そのため、監視装置は、より確実に監視対象デバイスを監視することが可能となる。

【００１５】

前記メッセージ送出部により送出される前記メッセージは、前記ネットワークデバイスを前記ネットワーク上で使用可能とするために、前記ネットワークデバイスの存在を前記ネットワークに対して通知するメッセージであるものとしても良い。

【００１６】

ネットワークデバイスがその存在をネットワークに対して通知するメッセージは、ネットワークデバイスの起動時、あるいは、稼働中に少なくとも１回は送出される。そのため、この構成によれば、監視装置は、より確実にネットワークデバイスから送出されるメッセージを取得して、監視対象デバイスをより確実に監視することが可能となる。

【００１７】

前記監視装置は、さらに、前記監視対象デバイスに関する情報を前記監視対象デバイス

の前記個体識別情報に対応付けて格納する監視対象情報格納部を有しており、前記監視対象判定部は、前記個体識別情報取得部が取得した個体識別情報と、前記監視対象情報とを照合することにより、前記特定デバイスが前記監視対象デバイスか否かを判断するものとしても良い。

【００１８】

この構成によれば、特定デバイスが監視対象デバイスか否かを監視対象情報格納部に格納された情報に基づいて判断できる。そのため、特定デバイスが監視対象デバイスか否かを判断するための、監視装置によるネットワークからの情報の取得を省略できるので、ネットワークのトラフィックをより低減することができる。

【００１９】

前記監視装置は、前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスを監視対象に追加するか否かの前記監視装置のユーザからの指示に基づいて、前記特定デバイスに関する情報と前記特定デバイスの前記個体識別情報とを前記監視対象情報に登録するものとしても良い。

【００２０】

この構成によれば、予め監視対象情報に登録されていないネットワークデバイスを監視対象デバイスとすることができるので、より確実に監視対象となるネットワークデバイスを監視することが可能となる。

【００２１】

前記監視装置は、前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスが所定の監視対象追加条件に合致するか否かを判断し、前記監視対象追加条件に合致すると判断された場合、前記特定デバイスに関する情報と前記特定デバイスの前記個体識別情報とを前記監視対象情報に登録するものとしても良い。

【００２２】

この構成によっても、予め監視対象条件に登録されていないネットワークデバイスを監視対象デバイスとすることができるので、より確実に監視対象となるネットワークデバイスを監視することが可能となる。

【００２３】

前記監視装置は、前記監視対象判定部により前記特定デバイスが前記監視対象デバイスでないと判断された場合に、前記特定デバイスの前記個体識別情報を前記ネットワークを介して管理サーバに送信し、前記管理サーバから受信した前記特定デバイスを監視対象に追加するか否かを表す情報に基づいて、前記特定デバイスに関する情報と前記特定デバイスの前記個体識別情報とを前記監視対象情報に登録するものとしても良い。

【００２４】

この構成によっても、予め監視対象情報に登録されていないネットワークデバイスを監視対象デバイスとすることができるので、より確実に監視対象となるネットワークデバイスを監視することが可能となる。

【００２５】

なお、本発明は、種々の態様で実現することが可能である。例えば、ネットワークデバイス管理システムとネットワークデバイス管理方法、それらの管理システムおよび管理方法で使用されるネットワークデバイス監視装置およびネットワークデバイス監視方法、それらの管理システム、管理方法、監視装置または監視方法の機能を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記録媒体、そのコンピュータプログラムを含み搬送波内に具現化されたデータ信号、等の態様で実現することができる。

【発明を実施するための最良の形態】

【００２６】

次に、本発明の実施の形態を実施例に基づいて以下の順序で説明する。

Ａ．第１実施例：

Ｂ．第２実施例：
Ｃ．第３実施例：
Ｄ．変形例：
【００２７】
Ａ．第１実施例：
図１は、本発明の第１実施例を適用するプリンタ管理システム１０の構成を示す説明図である。このプリンタ管理システム１０では、第１のネットワークシステム１２と第２のネットワークシステム１４とがルータＲＴを介して互いに接続されている。また、第１のネットワークシステム１２と第３のネットワークシステム１６とは、ファイアウォールＦＷおよびインターネットＩＮＥＴを介して互いに接続されている。
【００２８】
これらの３つのネットワークシステム１２，１４，１６が有するコンピュータ２００，３００やプリンタ１００ａ～１００ｄ等の各ネットワークデバイス（以下、単に「デバイス」とも呼ぶ）間では、ＴＣＰ／ＩＰプロトコルに従ってデータの送受信が行われる。第１実施例では、ネットワークシステム１２，１４，１６のそれぞれにおいてデバイス間を接続するローカルエリアネットワークＬＡＮ１，ＬＡＮ２，ＬＡＮ３には、ＩＥＥＥ８０２．３で規定される有線ネットワークを使用している。但し、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２，ＬＡＮ３は、ＩＥＥＥ８０２．１１ｂ／ｇ／ａなどの無線ネットワークとしてもよい。
【００２９】
第１のネットワークシステム１２の各デバイスには、割り当てられる３２ビットのＩＰアドレスは、上位２４ビットが同一の値「１９２．１６８．１」となっている。このように、ネットワークシステムの各デバイスに同一の値が割り当てられるＩＰアドレスの上位所定数のビットの値は、「ネットワークアドレス」と呼ばれる。また、ネットワークアドレスが同一のネットワークシステムは、「サブネット」と呼ばれる。第２のネットワークシステム１４のネットワークアドレスは、「１９２．１６８．２」に設定されている。
【００３０】
ＩＰアドレスのネットワークアドレスを除いた下位ビットの値は、ホストアドレスと呼ばれる。異なるネットワークシステムのネットワークアドレスを互いに異なる値に設定することにより、各ネットワークシステムの範囲で一意のホストアドレスを個々のデバイスに設定すれば、複数のネットワークシステム全体で各デバイスに重複しないＩＰアドレスを設定できる。図１の例では、第１のネットワークシステム１２と、第２のネットワークシステム１４と、のネットワークアドレスが異なっている。そして、第１のネットワークシステム１２の各デバイスには、それぞれ異なるホストアドレスが割り当てられている。そのため、第１のネットワークシステム１２のデバイスと、第２のネットワークシステム１４のデバイスとのそれぞれには、２つのネットワークシステム１２，１４を通じて重複しないＩＰアドレスが割り当てられている。
【００３１】
このように、２つのネットワークシステム１２，１４の個々のデバイスには、重複しないＩＰアドレスが割り当てられているので、ルータＲＴを介して接続された２つのネットワークシステム１２，１４の個々のデバイスは、ＩＰアドレスにより特定される。そのため、第１のネットワークシステム１２のデバイスと、第２のネットワークシステム１４のデバイスとの間では、ＩＰアドレスの変換を行わないルータＲＴを介したＴＣＰ／ＩＰプロトコルによるデータの送受信を行うことができる。なお、ＩＰアドレスの変換を行わないルータは、一般に、ローカルルータと呼ばれる。
【００３２】
第１のネットワークシステム１２は、ローカルエリアネットワークＬＡＮ１に、３台のプリンタ１００ａ～１００ｃと、監視用パーソナルコンピュータ２００（以下、単に「監視用ＰＣ２００」とも呼ぶ）と、が接続された構成となっている。
【００３３】

３台のプリンタ１００ａ～１００ｃには、それぞれ、ローカルエリアネットワークＬＡＮ１あるいはローカルエリアネットワークＬＡＮ２に接続された図示しないクライアントから印刷ジョブが送信される。これらのプリンタ１００ａ～１００ｃは、クライアントから送信された印刷ジョブに従って印刷処理を実行する。

【００３４】

図１の例では、監視用ＰＣ２００とプリンタ１００ａ～１００ｃとのそれぞれには、ＩＰアドレスが固定的に割り当てられている。これらのＩＰアドレスは、例えば、各デバイスをローカルエリアネットワークＬＡＮ１に接続する前に設定される。なお、プリンタ１００ａ～１００ｃのそれぞれのＩＰアドレスは、プリンタ１００ａ～１００ｃが有する操作ユニット（図示しない）や、プリンタ１００ａ～１００ｃに直接接続されたパーソナルコンピュータ等を用いて設定することができる。また、各デバイスのＩＰアドレスは、ＤＨＣＰ（Dynamic Host Configuration Protocol）サーバにより自動的に割り当てられるものとしても良い。この場合、各デバイスは電源が投入された時点でＤＨＣＰサーバが割り当てるＩＰアドレスを取得する。取得されたＩＰアドレスは、各デバイスの電源が遮断されるまで各デバイスにより使用される。

【００３５】

第２のネットワークシステム１４は、ローカルエリアネットワークＬＡＮ２に、プリンタ１００ｄが接続された構成となっている。プリンタ１００ｄには、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２に接続された図示しないクライアントから印刷ジョブが送信される。図１の例では、第１のネットワークシステム１２のプリンタ１００ａ～１００ｃと同様に、第２のネットワークシステム１４のプリンタ１００ｄにも、ＩＰアドレスが固定的に割り当てられている。但し、プリンタ１００ｄのＩＰアドレスを、ＤＨＣＰサーバにより自動的に割り当てても良い。

【００３６】

なお、図１に示す第１実施例では、第１のネットワークシステム１２のローカルエリアネットワークＬＡＮ１には３台のプリンタ１００ａ～１００ｃが接続され、第２のネットワークシステム１４のローカルエリアネットワークＬＡＮ２には１台のプリンタ１００ｄが接続されているが、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２を通じて１台以上の任意の台数のプリンタを接続することが可能である。

【００３７】

第３のネットワークシステム１６は、ローカルエリアネットワークＬＡＮ３に、管理サーバ３００が接続された構成となっている。第２のネットワークシステム１６は、第１のネットワークシステム１６とは異なり、ファイアウォールを介さずにインターネットＩＮＥＴに接続されている。

【００３８】

監視用ＰＣ２００は、プリンタ１００ａ～１００ｃのそれぞれが保持している管理情報を、ローカルエリアネットワークＬＡＮ１を介してプリンタ１００ａ～１００ｃから取得する。同様に、プリンタ１００ｄが保持している管理情報を、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２とルータＲＴとを介して取得する。取得されたプリンタ１００ａ～１００ｄの管理情報は、監視用ＰＣ２００上に蓄積される。監視用ＰＣ２００に蓄積された管理情報は、管理サーバ３００に随時送信される。

【００３９】

図１に示すように、４台のプリンタ１００ａ～１００ｄには、それぞれ、プリンタＩＤが設定されている。図１の例では、プリンタ１００ａには、プリンタＩＤ「Ｐｒｔ＿００１」が設定されており、プリンタ１００ｂ，１００ｃには、それぞれ、プリンタＩＤ「Ｐｒｔ＿００２」と「Ｐｒｔ＿００３」が設定されている。また、プリンタ１００ｄにはプリンタＩＤ「Ｐｒｔ＿１０１」が設定されている。これらのプリンタＩＤは、監視用ＰＣ２００が管理サーバ３００に送信する管理情報に含まれている。

【００４０】

ここで、監視用ＰＣ２００が接続されているローカルエリアネットワークＬＡＮ１は、

ファイアウォールＦＷを介してインターネットＩＮＥＴに接続されている。このため、管理サーバ３００側からは、ファイアウォールＦＷを越えて監視用ＰＣ２００側へ接続を要求し、監視用ＰＣ２００が取得・蓄積した管理情報を取得することができない。そこで、第１実施例では、監視用ＰＣ２００は、管理サーバ３００にＨＴＴＰ（HyperText Transfer Protocol）を用いて接続して、管理サーバ３００に管理情報を通知する。なお、監視用ＰＣ２００および管理サーバ３００間では、セキュリティの観点から、ＨＴＴＰの一種であるＨＴＴＰＳプロトコルによる暗号化通信が行われるのが好ましい。

【００４１】

図２は、プリンタ１００ｄと、監視用ＰＣ２００と、管理サーバ３００と、のそれぞれの構成を示す説明図である。なお、図２では、ローカルエリアネットワークＬＡＮ１とインターネットＩＮＥＴとの間に設けられているファイアウォールＦＷの図示を省略している。また、第１のネットワークシステム１２のプリンタ１００ａ～１００ｃは、プリンタ１００ｄと同一の構成となっているので、ここではその図示と説明を省略する。

【００４２】

プリンタ１００ｄは、ネットワークボード１１０と、プリンタ制御部１２０と、プリントエンジン１３０と、を備えている。ネットワークボード１１０と、プリンタ制御部１２０は、それぞれ、図示しない中央処理装置（ＣＰＵ）とメモリとを備えるコンピュータとして構成されている。プリントエンジン１３０は、与えられた印刷データに応じて印刷を実行する印刷機構である。

【００４３】

ネットワークボード１１０は、通信制御部１１２と、受信データ処理部１１４と、ＳＮＭＰエージェント１１６と、ＮＴＰクライアント１１８と、を備えている。通信制御部１１２は、ネットワークボード１１０が備えるネットワークインタフェース（図示しない）を制御することにより、ローカルエリアネットワークＬＡＮ２に接続されたデバイスと、プリンタ１００ｄとの間でのＴＣＰ／ＩＰプロトコルに従った通信を行う機能を有している。プリンタ１００ｄとローカルエリアネットワークＬＡＮ１に接続されたデバイスとの間の通信は、ローカルエリアネットワークＬＡＮ２に接続されたルータＲＴを介して行われる。

【００４４】

通信制御部１１２は、クライアントＣＬからの印刷ジョブを含む通信データを受け取ると、受け取った通信データを受信データ処理部１１４に供給する。受信データ処理部１１４は、供給された通信データから印刷ジョブデータを抽出する。抽出された印刷ジョブデータは、プリンタ制御部１２０に供給される。プリンタ制御部１２０は、印刷ジョブデータに含まれる印刷コマンドに従って印刷データを生成し、生成された印刷データをプリントエンジン１３０に供給する。供給された印刷データに応じて、プリントエンジン１３０は印刷を実行する。

【００４５】

通信制御部１１２は、ローカルエリアネットワークＬＡＮ２とＳＮＭＰエージェント１１６との間で、ＳＮＭＰ（Simple Network Management Protocol）に従った通信データを受け渡す機能を有している。通信制御部１１２は、ＳＮＭＰマネージャ２２２（後述する）から受け取った情報送信を要求するＳＮＭＰメッセージ（要求メッセージ）をＳＮＭＰエージェント１１６に供給する。ＳＮＭＰエージェント１１６は、要求メッセージに従って、プリンタ制御部１２０が備えるデータベース１２２（ＭＩＢ：Management Information Base）から種々の情報を取得する。ＳＮＭＰエージェント１１６は、取得された情報からＳＮＭＰメッセージ（応答メッセージ）を生成し、応答メッセージを通信制御部１１２を介してＳＮＭＰマネージャ２２２に送信する。

【００４６】

プリンタ制御部１２０は、プリンタ１００ａに関する種々の情報を管理情報として収集して、ＳＮＭＰエージェント１１６により参照されるＭＩＢ１２２に格納する。ＭＩＢ１２２に格納される情報には、プリンタに関して予め規格で統一的に規定されている情報や

、製造者によって独自に定義されている情報がある。ＭＩＢ１２２に格納された各情報（「オブジェクト」あるいは「ＭＩＢ情報」と呼ばれる）は、情報の要素に割り振られたオブジェクトＩＤ（ＯＩＤ）により参照される。このオブジェクトＩＤは、「１．３．６．１．２．１．１」のようにピリオドで区切られた数字となっている。

【００４７】

図２に示すプリンタ１００ｄでは、プリンタ制御部１２０のＭＩＢ１２２には、時間の経過とともに変化する管理情報と、プリンタ１００ｄに固有の情報である識別情報とが、格納されている。ＭＩＢ１２２には、管理情報として、例えば、プリンタ１００ｄの総印刷枚数や障害情報等の印刷ジョブとは関係なく収集される情報と、個々の印刷ジョブに対応付けられた種々の情報とが格納される。また、プリンタ１００ｄの個体の識別に使用される識別情報として、例えば、プリンタ１００ｄの機種名および製造番号等がＭＩＢ１２２に格納される。なお、ＭＩＢ１２２のうち管理情報を格納する領域は、管理情報格納部とも呼ぶことができる。

【００４８】

通信制御部１１２は、ローカルエリアネットワークＬＡＮ２とＮＴＰクライアント１１８との間で、ＮＴＰ（Network Time Protocol）に従った通信データを受け渡す機能を有している。ＮＴＰクライアント１１８は、監視用ＰＣ２００のＮＴＰサーバ２５０（後述する）に現在時刻を問い合わせるＮＴＰメッセージを送信し、ＮＴＰサーバ２５０から返信されるメッセージから現在時刻を取得する。取得された現在時刻は、プリンタ制御部１２０が備える計時タイマ１２４に供給される。これにより、プリンタ１００ｄの各部は、監視用ＰＣ２００の時刻に同期した現在時刻を計時タイマ１２４から取得することが可能となる。なお、ＮＴＰクライアント１１８からＮＴＰサーバ２５０へのＮＴＰメッセージの送信と、ＮＴＰサーバ２５０からＮＴＰクライアント１１８への修正されたＮＴＰメッセージの送信とは、一連の処理として実行される。そのため、この一連の処理が行われている状態は、ＮＴＰクライアント１１８とＮＴＰサーバ２５０とが接続された状態とも言うことができる。

【００４９】

監視用ＰＣ２００は、通信制御部２１０と、管理エージェント２２０と、プリンタ情報格納部２３０と、リアルタイムクロック２４０と、ＮＴＰサーバ２５０と、を備えている。監視用ＰＣ２００は、これらの各部の機能によりプリンタ１００ｄのＭＩＢ情報を取得し、プリンタ１００ｄの状態を監視することができる。そのため、監視用ＰＣ２００は、プリンタ監視装置であるともいうことができる。

【００５０】

通信制御部２１０と管理エージェント２２０とＮＴＰサーバ２５０とのそれぞれの機能は、監視用ＰＣ２００が備える図示しないＣＰＵにより実現されている。また、プリンタ情報格納部２３０は、監視用ＰＣ２００が備える図示しないメモリの一部の領域である。

【００５１】

通信制御部２１０は、監視用ＰＣ２００が備えるネットワークインタフェース（図示しない）を制御することにより、ローカルエリアネットワークＬＡＮ１に接続されたデバイスと、監視用ＰＣ２００との間でのＴＣＰ／ＩＰプロトコルに従った通信を行う機能を有している。監視用ＰＣ２００とローカルエリアネットワークＬＡＮ２に接続されたデバイスとの間の通信は、ローカルエリアネットワークＬＡＮ１に接続されたルータＲＴを介して行われる。

【００５２】

リアルタイムクロック２４０は、バッテリによりバックアップされた現在時刻を格納する計時タイマである。なお、リアルタイムクロック２４０に格納される現在時刻は、図示しないＮＴＰクライアントにより、インターネットＩＮＥＴを介して接続された標準時刻サーバ（図示しない）の時刻に同期される。

【００５３】

ＮＴＰサーバ２５０は、ＮＴＰクライアント１１８からのＮＴＰメッセージを受信する

と、リアルタイムクロック２４０に格納された現在時刻を取得する。リアルタイムクロック２４０から取得した現在時刻と、ＮＴＰメッセージに含まれる情報とに基づいて、ＮＴＰサーバ２５０はＮＴＰメッセージを修正する。修正されたＮＴＰメッセージは、通信制御部２１０を介してＮＴＰクライアント１１８に返信される。これにより、プリンタ１００ｄの時刻は、リアルタイムクロック２４０の時刻に同期される。上述のように、リアルタイムクロック２４０の時刻は、標準時刻サーバに同期されているので、プリンタ１００ｄの時刻は、標準時刻サーバに同期される。

【００５４】

管理エージェント２２０は、ＳＮＭＰマネージャ２２２と、管理情報送受信部２２４と、アドレス監視部２２６と、を備えている。ＳＮＭＰマネージャ２２２は、プリンタ１００ｄのＭＩＢ１２２から管理情報を取得し、プリンタ情報格納部２３０の管理情報蓄積部２３４に格納・蓄積する。管理情報送受信部２２４は、管理情報蓄積部２３４に蓄積された情報を、通信制御部２１０を介して管理サーバ３００に送信する。

【００５５】

プリンタ情報格納部２３０は、監視対象情報格納部２３２と、管理情報蓄積部２３４と、を備えている。監視対象情報格納部２３２には、監視対象となっているプリンタのそれぞれについて、プリンタＩＤと、ＩＰアドレスと、識別情報と、が登録された監視対象情報が予め格納されている。

【００５６】

図３は、監視対象情報の一例を示す説明図である。図３の例では、第１のネットワークシステム１２および第２のネットワークシステム１４のプリンタ１００ａ～１００ｄの全てが監視対象となっている。そのため、図３に示すように、監視対象情報格納部２３２には、プリンタ１００ａ～１００ｄのそれぞれについて、プリンタＩＤと、ＩＰアドレスと、識別情報としての機種名および製造番号と、が格納されている。

【００５７】

図２のＳＮＭＰマネージャ２２２は、プリンタ１００ｄのほか、監視対象情報格納部２３２に登録された個々のプリンタ（監視対象プリンタ）から、管理情報を取得する。個々の監視対象プリンタから取得された管理情報は、プリンタＩＤに対応付けられて管理情報蓄積部２３４に格納される。

【００５８】

管理情報をプリンタ１００ｄから取得する場合、まず、ＳＮＭＰマネージャ２２２は、監視対象情報格納部２３２を参照し、プリンタ１００ｄ（プリンタＩＤ＝Ｐｒｔ＿１０１）のＩＰアドレスを取得する。図３の例では、ＳＮＭＰマネージャ２２２は、プリンタ１００ｄのＩＰアドレス「１９２．１６８．２．２１」を取得する。そして、取得したＩＰアドレス「１９２．１６８．２．２１」が設定されたプリンタに設けられたＳＮＭＰエージェント１１６に対し、ＭＩＢ情報を指定するオブジェクトＩＤを格納した要求メッセージを送信する。

【００５９】

要求メッセージを受信したＳＮＭＰエージェント１１６は、プリンタ制御部１２０が有するＭＩＢ１２２から、要求メッセージに格納されたオブジェクトＩＤで指定されるＭＩＢ情報を取得し、取得したＭＩＢ情報を格納した応答メッセージを生成する。生成された応答メッセージは、ＳＮＭＰエージェント１１６からＳＮＭＰマネージャ２２２に送信される。

【００６０】

ＳＮＭＰマネージャ２２２は、ＳＮＭＰエージェント１１６が送信した応答メッセージを受信し、応答メッセージに含まれるＭＩＢ情報を取得することにより、プリンタ制御部１２０のＭＩＢ１２２に格納された管理情報を取得することができる。

【００６１】

なお、ＳＮＭＰでは、メッセージの送受信にＴＣＰ／ＩＰプロトコルのうち、再送制御などを行わず、通信の信頼性が保証されないＵＤＰ（User Datagram Protocol）を使用し

ている。そのため、ＳＮＭＰマネージャ２２２は、ＳＮＭＰエージェント１１６に対する要求メッセージ送信の後、予め定められた待ち時間を経過してもＳＮＭＰエージェント１１６からの応答メッセージが受信できない場合、要求メッセージを再送する。所定の回数（例えば３回）要求メッセージを送信しても、ＳＮＭＰエージェント１１６からの応答メッセージが受信できない場合、要求メッセージの送信先が応答不能とである判断し、ＭＩＢ情報の取得は中止される。

【００６２】

アドレス監視部２２６は、ローカルエリアネットワークＬＡＮ１から通信制御部２１０に供給された通信データに基づいて、監視対象となるプリンタのＩＰアドレスを監視するこの、アドレス監視部２２６の機能とその動作については、後述する。

【００６３】

管理サーバ３００は、通信制御部３１０と、プリンタ管理データベース３２０と、データベース管理部３３０と、を備えている。通信制御部３１０は、図示しないネットワークインタフェースを制御することにより、インターネットＩＮＥＴを介した監視用ＰＣ２００との通信を行う。

【００６４】

データベース管理部３３０は、監視用ＰＣ２００から管理サーバ３００に送信された管理情報をプリンタＩＤに関連付けてプリンタ管理データベース３２０に蓄積する。データベース管理部３３０は、プリンタ管理データベース３２０に蓄積されたプリンタＩＤと管理情報とに基づいて、消耗品の使用量や印刷ジョブごとのプリンタの使用量等に応じた課金管理等を行う。なお、第１実施例において、管理サーバ３００は、個々のプリンタの管理をプリンタＩＤに基づいて行っているが、一般に、個々のプリンタの管理が可能であれば良い。例えば、管理サーバ３００は、識別情報に基づいて個々のプリンタを管理するものとしても良い。

【００６５】

図４は、監視用ＰＣ２００とプリンタ１００ｄとの間のデータ通信に関する機能の階層構造を示すブロック図である。図４に示すブロック図では、通信データは、送信側のデバイスでは上層から下層に伝達され、受信側のデバイスでは下層から上層に伝達される。

【００６６】

監視用ＰＣ２００では、管理エージェント２２０とＮＴＰサーバ２５０とがその最上層に位置している。管理エージェント２２０は、ＨＴＴＰクライアント２３１０とＳＮＭＰクライアント２４１０とを有している。ＨＴＴＰクライアント２３１０は、図２の管理情報送受信部２２４により実行される機能であり、ＳＮＭＰクライアント２４１０は、図２のＳＮＭＰマネージャ２２２およびアドレス監視部２２６により実行される機能である。

【００６７】

ＨＴＴＰクライアント２３１０の下層には、ＴＣＰ処理部２３００が設けられている。ＳＮＭＰクライアント２４１０およびＮＴＰサーバ２５０の下層には、ＵＤＰ処理部２４００が設けられている。ＴＣＰ処理部２３００とＵＤＰ処理部２４００との下層には、上から順番に、ＩＰ処理部２２００と、パケット監視部２２１０と、ネットワークインタフェース（Ｉ／Ｆ）２１００とが設けられている。パケット監視部２２１０は、通信制御部２１０により実行される機能である。パケット監視部２２１０の機能の詳細については、後述する。

【００６８】

ＴＣＰ処理部２３００と、ＵＤＰ処理部２４００と、ＩＰ処理部２２００とは、ＴＣＰ／ＩＰプロトコルの対応するプロトコルに関する処理を実行する機能モジュールであり、通信制御部２１０により実行される。これらの機能モジュールは、上層から供給されたデータを対応するプロトコルに従ったデータに変換して、変換後のデータを下層に供給する。また、各機能モジュールは、下層から供給されるデータを逆変換して上層に供給する。

【００６９】

プリンタ１００ｄは、その最上層に、プリントサーバ１３１０と、ＳＮＭＰサーバ１４

１０と、ＮＴＰクライアント１１８を有している。プリントサーバ１３１０は、印刷ジョブを受信し印刷を実行する印刷処理機能である。この印刷処理機能は、図２に示す受信データ処理部１１４と、プリンタ制御部１２０と、プリントエンジン１３０とによって実行される。また、ＳＮＭＰサーバ１４１０は、ＳＮＭＰエージェント１１６（図２）により実行される機能である。

【００７０】

プリントサーバ１３１０の下層には、ＴＣＰ処理部１３００が設けられている。また、ＳＮＭＰサーバ１４１０とＮＴＰクライアント１１８との下層には、ＵＤＰ処理部１４００が設けられている。ＴＣＰ処理部１３００とＵＤＰ処理部１４００との下層には、上から順番に、ＩＰ処理部１２００と、ネットワークインタフェース１１００とが設けられている。ＴＣＰ処理部１３００とＵＤＰ処理部１４００とＩＰ処理部１２００との機能および構成は、監視用ＰＣ２００のＴＣＰ処理部２３００とＵＤＰ処理部２４００とＩＰ処理部２２００と同様である。

【００７１】

ルータＲＴは、ローカルエリアネットワークＬＡＮ１に接続された第１のネットワークインタフェース４１００と、ローカルエリアネットワークＬＡＮ２に接続された第２のネットワークインタフェース４２００と、を備えている。これらの２つのネットワークインタフェース４１００，４２００とが接続されることにより、ローカルエリアネットワークＬＡＮ１とローカルエリアネットワークＬＡＮ２との間でデータが転送される。

【００７２】

図４に示すように、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２に接続されている４つのネットワークインタフェース１１００，２１００，４１００，４２００には、それぞれ、ＭＡＣ（Media Access Control）アドレスと呼ばれる４８ビットの固有の数字が割り当てられている。このＭＡＣアドレスは、ネットワークインタフェースを特定するために使用される。そのため、ＭＡＣアドレスは、通常、全てのネットワークインタフェースで重複しないように設定されている。ローカルエリアネットワークＬＡＮ１内で伝送される通信データの宛先は、ＭＡＣアドレスによって指定される。同様に、ローカルエリアネットワークＬＡＮ２内で伝送される通信データの宛先は、ＭＡＣアドレスによって指定される。

【００７３】

図５は、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２上でＮＴＰメッセージを伝送する際の通信データの構成を示す説明図である。なお、通常、ＮＴＰメッセージとしては、バージョン３のＮＴＰメッセージ（ＮＴＰ３メッセージ）が使用される。図５（ａ）は、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２上で伝送されるデータパケット（以下、単に「パケット」とも呼ぶ）の構成を示している。このパケットは、一般に、ＭＡＣフレームと呼ばれる。

【００７４】

ＭＡＣフレームは、１４オクテット（１オクテット＝８ビット）のＭＡＣヘッダと、４６～１５００オクテットのユーザデータ部と、２オクテットのチェックサムと、を含んでいる。ＭＡＣヘッダは、パケットの宛先となるネットワークインタフェースを特定するための宛先ＭＡＣアドレスと、パケットの送信元のネットワークインタフェースを特定するための送信元ＭＡＣアドレスと、プロトコル情報（タイプ）とを有している。

【００７５】

図４の例でプリンタ１００ｄから監視用ＰＣ２００にＮＴＰ３メッセージが伝送される場合、ローカルエリアネットワークＬＡＮ２で伝送されるＭＡＣフレームでは、宛先ＭＡＣアドレスには、ネットワークインタフェース４２００のＭＡＣアドレス「00:01:01:12:04:3B」が格納され、送信元ＭＡＣアドレスには、ネットワークインタフェース１１００のＭＡＣアドレス「00:00:6C:05:10:50」が格納される。一方、ローカルエリアネットワークＬＡＮ１で伝送されるＭＡＣフレームでは、宛先ＭＡＣアドレスには、ネットワークインタフェース２１００のＭＡＣアドレス「00:0C:C2:04:13:A4」が格納され、送信元Ｍ

ＡＣアドレスには、ネットワークインタフェース４１００のＭＡＣアドレス「00:01:01:12:04:3A」が格納される。

【００７６】

図５（ａ）のフレームチェックシーケンス（ＦＣＳ：Frame Check Sequence）と呼ばれるチェックサムには、ＭＡＣフレーム全体のデータに対してビット単位の特殊な演算で算出される３２ビットのＣＲＣ（Cyclic Redundancy Code：巡回冗長符号）が格納されている。この伝送されたＭＡＣフレーム中のフレームチェックシーケンスと、伝送されたＭＡＣフレームから算出されるＣＲＣとを比較することにより、ＭＡＣフレームの伝送が誤りなく行われたか否かが判断される。ＭＡＣフレームが正しく伝送されなかった場合には、そのＭＡＣフレームは廃棄される。一方、ＭＡＣフレームが正しく伝送された場合には、ユーザデータが抽出される。

【００７７】

プロトコル情報は、ユーザデータ部に格納されているデータが、どのプロトコルによって処理されるかを指定する。例えば、ユーザデータ部に格納されるデータが、インターネットプロトコル（ＩＰ：Internet Protocol）によって処理されるＩＰデータグラムである場合には、プロトコル情報には１６進数の「０８００」が格納される。図５（ａ）の例では、ユーザデータ部にはＩＰデータグラムが格納されているので、プロトコル情報には、１６進数「０８００」が格納されている。そのため、ＭＡＣフレームから抽出されたユーザデータであるＩＰデータグラムは、ＩＰを処理するモジュールに伝達される。

【００７８】

図４に示すプリンタ１００ｄの例では、ＩＰデータグラムは、ネットワークインタフェース１１００からＩＰ処理部１２００に伝達され、あるいは、ＩＰ処理部１２００からネットワークインタフェース１１００に伝達される。ＩＰ処理部１２００からネットワークインタフェース１１００に伝達されたＩＰデータグラムには、ＭＡＣヘッダとフレームチェックシーケンスとが付加され、ＭＡＣフレームが生成される。

【００７９】

一方、監視用ＰＣ２００では、ＩＰデータグラムは、パケット監視部２２１０を介してＩＰ処理部２２００に伝達される。パケット監視部２２１０は、ネットワークインタフェース２１００とＩＰ処理部２２００との間で授受されるＩＰデータグラムを監視する。そして、受信したＩＰデータグラムに含まれるデータのうち、送信元ＩＰアドレスおよび宛先ポート番号（これらのデータについては、後述する）を取得し、管理エージェント２２０のアドレス監視部２２６（図２）に供給する。但し、パケット監視部２２１０は、ＩＰ処理部２２００とネットワークインタフェース２１００との間で授受されるＩＰデータグラムに変更を加えることなく転送する。

【００８０】

なお、パケット監視部２２１０がアドレス監視部２２６に供給するデータは、ＩＰデータグラムに含まれる送信元ＩＰアドレス、宛先ＩＰアドレス、送信元ポート番号および宛先ポート番号の全てを含んでいても良い。また、パケット監視部２２１０がＩＰデータグラムに含まれるメッセージがＮＴＰメッセージであるか否かを判断し、ＮＴＰメッセージを含むＩＰデータグラムの送信元ＩＰアドレスのみをアドレス監視部２２６に供給するものとしても良い。

【００８１】

ルータＲＴでは、ＩＰデータグラムは、２つのネットワークインタフェース４１００，４２００間で伝達される。この際、ルータＲＴは、ＩＰデータグラムの内容に応じて、ＩＰデータグラムの伝達を行うか否かを判断する。

【００８２】

図５（ｂ）は、ＩＰデータグラムの構成を示している。ＩＰデータグラムは、制御情報と、送信元ＩＰアドレスと、宛先ＩＰアドレスと、オプションデータおよびパディングデータ（以下、「パディング等」とも呼ぶ）と、ＵＤＰデータグラムと、を含んでいる。図５は、ＵＤＰを伝送に使用するＮＴＰ３メッセージの例を示しているので、パディング等

の後にＵＤＰデータグラムが格納されているが、一般に、パディング等の後には、伝送に使用されるプロトコルに従ってデータが格納される。なお、パディング等の後に格納されるデータがいずれの上位プロトコルで処理されるかの情報は、制御情報に格納されている。

【００８３】

図５（ｃ）は、ＵＤＰデータグラムの構成を示している。ＵＤＰデータグラムは、送信元ポート番号と、宛先ポート番号と、データ長と、チェックサムと、ＮＴＰ３メッセージと、を含んでいる。宛先ポート番号は、チェックサムの後に格納されているデータがいずれの上位プロトコルで処理されるかを指定する値である。なお、図５の例では、チェックサムの後にはＮＴＰ３メッセージが格納されているが、一般に、格納されるデータは宛先ポート番号で指定される上位プロトコルに従ったメッセージが格納される。

【００８４】

図５（ｄ）は、ＮＴＰ３メッセージの構成を示している。ＮＴＰ３メッセージは、制御情報と、ネットワークでの伝送遅延に関する情報であるルート遅延およびルート拡散と、時刻に関する情報である参照クロックＩＤおよび４つのタイムスタンプと、を有している。ＮＴＰサーバ２５０（図４）は、図５（ｄ）に示すＮＴＰ３メッセージを受信すると、これらの情報を修正したＮＴＰ３メッセージを生成し、ＮＴＰクライアント１１８（図４）に返信する。

【００８５】

図４および図５に示すように、図４に示すローカルエリアネットワークＬＡＮ１，ＬＡＮ２を伝送されるＮＴＰ３メッセージの通信データでは、ルータＲＴによりＭＡＣアドレス（図５（ａ））が変更される。そのため、ルータＲＴを介して伝送されるＮＴＰ３メッセージの送信元を特定しうる情報は、ＩＰデータグラム（図５（ｂ））に含まれる送信元ＩＰアドレスとなる。

【００８６】

図６は、プリンタ１００ｄ（図２）のＮＴＰクライアント１１８により実行される時刻同期実行ルーチンを示すフローチャートである。この時刻同期実行ルーチンは、プリンタ１００ｄの起動の際に実行開始される。なお、プリンタ１００ｄは、ＮＴＰクライアント１１８を起動せず時刻同期実行ルーチンを実行しないようにすることも可能であるが、プリンタ１００ｄが監視用ＰＣ２００（図２）による監視対象のプリンタである場合には、プリンタ１００ｄの起動の際に、ＮＴＰクライアント１１８が起動され、時刻同期実行ルーチンが実行されるように設定される。この設定は、ユーザによる変更が禁止されている。

【００８７】

ステップＳ１１０において、ＮＴＰクライアント１１８は、監視用ＰＣ２００（図２）のＮＴＰサーバ２５０から現在時刻を取得する。この現在時刻の取得先である監視用ＰＣ２００は、予め設定されており、この設定のユーザによる変更は禁止されている。そのため、ＮＴＰクライアント１１８は、常に、監視用ＰＣ２００に対してＮＴＰメッセージ送信し、監視用ＰＣ２００から修正されたＮＴＰメッセージを受信する。そして、ステップＳ１２０において、ＮＴＰクライアント１１８は、取得した現在時刻をプリンタ１００ｄの計時タイマ１２４に設定する。

【００８８】

ステップＳ１３０において、ＮＴＰクライアント１１８は、前回の同期から所定の時間が経過したか否かを判断する。前回の同期から所定の時間が経過していないと判断された場合には、制御は戻され、ステップＳ１３０が繰り返し実行される。一方、前回の同期から所定の時間が経過していると判断された場合には、制御はステップＳ１４０に移される。なお、所定の時間は、プリンタ１００ｄのクロック精度等に応じて適宜設定される。

【００８９】

ステップＳ１４０では、ステップＳ１１０と同様に、現在時刻の取得が行われ、ステップＳ１５０では、ステップＳ１２０と同様に、取得された現在時刻の計時タイマ１２４へ

の設定が行われる。そして、ステップＳ１５０での現在時刻の設定後、制御はステップＳ１３０に戻される。このように、図６に示す時刻同期実行ルーチンが実行されることにより、所定の時間間隔で、プリンタ１００ｄから監視用ＰＣ２００にＮＴＰメッセージが送信される。

【００９０】

図７は、監視用ＰＣ２００（図２）のアドレス監視部２２６により実行されるプリンタアドレス監視ルーチンを示すフローチャートである。このプリンタアドレス監視ルーチンは、監視用ＰＣ２００の起動の際のＮＴＰサーバ２５０（図２）の起動に引き続いて実行開始される。

【００９１】

ステップＳ２１０において、アドレス監視部２２６は、ＮＴＰサーバ２５０へのＮＴＰメッセージの送信があったか否かを判断する。具体的には、アドレス監視部２２６は、パケット監視部２２１０（図４）により取得された受信データの宛先ポート番号から、ＮＴＰサーバ２５０へのＮＴＰメッセージの送信があったか否かを判断する。ＮＴＰメッセージの送信があったと判断された場合には、制御はステップＳ２２０に移される。一方、ＮＴＰメッセージの送信がなかったと判断された場合には、制御は戻され、ステップＳ２１０が繰り返し実行される。

【００９２】

ステップＳ２２０において、アドレス監視部２２６は、ＮＴＰメッセージの送信元のＩＰアドレスを取得する。ＮＴＰメッセージの送信元のＩＰアドレスは、パケット監視部２２１０（図４）により取得されたＮＴＰメッセージを含む受信データの送信元ＩＰアドレスから取得することが可能である。

【００９３】

ステップＳ２３０において、アドレス監視部２２６は、ステップＳ２２０で取得したＩＰアドレスで特定されるデバイス（特定デバイス）から識別情報を取得する。具体的には、ステップＳ２２０で取得したＩＰアドレスを指定して、識別情報の送信を要求する要求メッセージを特定デバイスに送信する。そして、特定デバイスからの、応答メッセージを取得することにより、プリンタの識別情報を取得する。但し、応答メッセージの取得に失敗した場合、所定の回数（例えば３回）要求メッセージを再送信する。再送信の後、応答メッセージが受信できない場合、識別情報の取得は中止される。

【００９４】

ステップＳ２４０において、アドレス監視部２２６は、取得した識別情報から特定デバイスが監視対象プリンタであるか否かを判断する。具体的には、アドレス監視部２２６は、監視対象情報格納部２３２（図２）に格納された監視対象情報を検索し、取得した識別情報である機種名および製造番号が一致するプリンタがあるか否かを判断する。識別情報が一致するプリンタがある場合、特定デバイスは監視対象プリンタであると判断され、制御はステップＳ２５０に移される。一方、識別情報が一致するプリンタがない場合には、特定デバイスは監視対象プリンタでないと判断され、制御はステップＳ２１０に戻される。また、ステップＳ２３０において、識別情報の取得が中止された場合も、特定デバイスは監視対象プリンタでないと判断され、制御はステップＳ２１０に戻される。

【００９５】

ステップＳ２５０において、アドレス監視部２２６は、ステップＳ２３０で取得した監視対象プリンタのＩＰアドレス（実アドレス）と、監視対象情報に登録されたプリンタのＩＰアドレス（登録アドレス）とが一致するか否かを判断する。実アドレスと登録アドレスが一致すると判断された場合、制御はステップＳ２１０に戻される。一方、実アドレスと登録アドレスが一致しないと判断された場合には、制御はステップＳ２６０に移される。なお、ステップＳ２５０を省略し、監視対象プリンタの実アドレスを取得した場合、監視対象情報に登録されたＩＰアドレスを常に更新するものとしても良い。

【００９６】

ステップＳ２６０において、アドレス監視部２２６は、監視対象情報格納部２３２を書

き換えることにより、プリンタの登録アドレスを実アドレスに更新する。登録アドレスの更新の後、制御はステップＳ２１０に戻される。

【００９７】

図８（ａ）は、プリンタ１００ｄのＩＰアドレス（ホストアドレス）の変更直後における監視対象情報の状態を示している。図８（ａ）は、図８（ａ）のハッチングで示すプリンタ１００ｄの実際のＩＰアドレスが、「１９２．１６８．２．３１」に変更されている点で、図３と異なっている。他の点は図３と同じである。

【００９８】

図８（ａ）に示す状態では、監視対象情報に登録されているＩＰアドレスは、実際のプリンタ１００ｄの実際のＩＰアドレスと異なっている。この状態では、監視用ＰＣ２００（図２）は、管理情報をＩＰアドレスによって宛先を特定するＳＮＭＰによって取得するので、監視用ＰＣ２００はプリンタ１００ｄの管理情報を取得することができない。

【００９９】

図８（ｂ）は、プリンタ１００ｄの登録アドレスが更新される際、監視用ＰＣ２００とプリンタ１００ｄとの間で授受される主要なメッセージを示している。

【０１００】

図８（ｂ）のステップ[S1]では、プリンタ１００ｄのＮＴＰクライアント１１８（図２）が図６に示す時刻同期実行ルーチンを実行することにより、監視用ＰＣ２００に対してＮＴＰメッセージが送信される（ステップＳ１１０，Ｓ１４０）。そして、監視用ＰＣ２００のアドレス監視部２２６（図２）が、図７に示すプリンタアドレス監視ルーチンを実行することにより、プリンタ１００ｄのＩＰアドレスを取得する（ステップＳ２１０，２２０）。

【０１０１】

図８（ｂ）のステップ[S2]では、監視用ＰＣ２００のアドレス監視部２２６から識別情報の送信を要求するＳＮＭＰメッセージがプリンタ１００ｄに送信される。次に、ステップ[S3]において、アドレス監視部２２６は、プリンタ１００ｄが返信した識別情報を含むＳＮＭＰメッセージを受信する。このプリンタ１００ｄから受信した識別情報と、ステップ[S1]において取得されたプリンタ１００ｄの実際のＩＰアドレスとから、上述のように、アドレス監視部２２６は、プリンタ１００ｄの登録アドレスを更新する。

【０１０２】

図８（ｃ）は、プリンタ１００ｄの登録アドレス更新後の監視対象情報を示している。図８（ｃ）は、監視対象情報に登録されているプリンタ１００ｄのＩＰアドレスが、実際のＩＰアドレスに更新されている点で、図８（ａ）と異なっている。他の点は、図８（ａ）と同じである。

【０１０３】

図８（ｃ）に示すように、登録アドレスを更新することにより、監視対象情報に登録されているＩＰアドレスは、実際のプリンタ１００ｄの実際のＩＰアドレスと同一になる。そのため、図８（ｃ）に示す状態では、監視用ＰＣ２００（図２）は、ＩＰアドレスによってプリンタ１００ｄを特定し、ＳＮＭＰによりプリンタ１００ｄの管理情報を取得することが可能になる。

【０１０４】

このように、第１実施例では、プリンタ１００ｄが時刻同期を行うことにより、監視用ＰＣ２００はプリンタ１００ｄを特定するＩＰアドレスを取得する。監視用ＰＣ２００は、取得したＩＰアドレスで特定される特定デバイスから識別情報を取得する。取得された識別情報により特定デバイスが監視対象プリンタであると判断された場合には、プリンタ１００ｄのＩＰアドレスにより監視対象情報が更新される。これにより、監視用ＰＣ２００は、プリンタ１００ｄのＩＰアドレスが変更された場合であっても、ＩＰアドレスにより特定されるプリンタ１００ｄの監視を行うことができる。

【０１０５】

一般に、ネットワークを介して管理が行われるプリンタでは、障害の発生や、ジョブの

開始時間および終了時間など種々のイベントの発生時刻が正確に記録されるのが好ましい。そのため、このようなプリンタにおいては、外部のＮＴＰサーバと時刻の同期を取るためのＮＴＰクライアントの機能を通常の機能として有している。第１実施例では、監視用ＰＣ２００が、このように監視の対象となるプリンタ１００ｄが通常有する機能であるＮＴＰクライアント１１８から送信されるＮＴＰメッセージを受信することにより、プリンタ１００ｄのＩＰアドレスを取得することができる。そのため、プリンタ１００ｄに新たな機能を付加することなくプリンタ１００ｄのＩＰアドレスを取得し、ＩＰアドレスにより特定されるプリンタの監視を行うことができる。また、プリンタ１００ｄが監視用ＰＣ２００と時刻同期を取ることによって、互いの時刻を合わせるという効果も併せて得ることができる。

【０１０６】

なお、第１実施例では、プリンタ１００ｄの時刻の同期は、図６に示すように、プリンタ１００ｄの起動時（ステップＳ１１０，Ｓ１２０）および所定の時間間隔（Ｓ１４０，Ｓ１５０）に行われるが、時刻の同期をプリンタ１００ｄの起動時もしくは所定の時間間隔毎のいずれか一方のみで行うものとしても良い。また、第１実施例では、プリンタ１００ｄの時刻の同期は、所定の時間間隔に１回行われているが、所定の時間間隔に少なくとも１回行われるものとしても良い。

【０１０７】

Ｂ．第２実施例：

図９は、第２実施例において、アドレス監視部２２６（図２）により実行されるプリンタアドレス監視ルーチンを示すフローチャートである。第２実施例は、図９に示すプリンタアドレス監視ルーチンにステップＳ２７０，Ｓ２８０が付加されている点と、ステップＳ２４０で特定デバイスが監視対象プリンタでないと判断された場合に制御がステップＳ２７０に移される点、とで図７に示す第１実施例のプリンタアドレス監視ルーチンと異なっている。他の点は、第１実施例と同じである。

【０１０８】

ステップＳ２７０において、アドレス監視部２２６は、特定デバイスを監視用ＰＣ２００（図２）による監視対象とするか否かを判断する。具体的には、監視用ＰＣ２００のユーザに特定デバイスを監視対象に追加するか否かの指示の入力を許容するダイアログボックスを監視用ＰＣ２００のディスプレイ（図示しない）に表示する。そして、ダイアログボックスから入力されたユーザからの指示に従って、特定デバイスを監視対象とするか否かを判断する。アドレス監視部２２６が特定デバイスを監視対象とすると判断した場合には、制御はステップＳ２８０に移される。一方、アドレス監視部２２６が特定デバイスを監視対象としないと判断した場合には、制御はステップＳ２１０に戻される。

【０１０９】

図１０（ａ）は、ステップＳ２７０において監視用ＰＣ２００のディスプレイに表示されるダイアログボックスＤＬＧの一例を示している。図１０（ａ）に示すように、ダイアログボックスＤＬＧには、ユーザに特定デバイスを監視対象とするか否かを問い合わせるメッセージＴＱＭと、特定デバイスに関する情報ＴＰＩとが表示される。図１０（ａ）の例では、特定デバイスに関する情報として、ＩＰアドレスと、識別情報である機種名および製造番号とがダイアログボックスＤＬＧに表示される。

【０１１０】

ユーザは、ダイアログボックスＤＬＧの表示内容ＴＱＭ，ＴＰＩに従ってダイアログボックスＤＬＧに設けられた２つのボタンＢＹＥＳ，ＢＮＯをクリックすることにより、特定デバイスを監視対象とするか否かの指示を入力する。図１０（ａ）の例では、ユーザがボタンＢＹＥＳをクリックすると特定デバイスが監視対象に追加され、ユーザがボタンＢＮＯをクリックすると特定デバイスの監視対象への追加は行われない。

【０１１１】

ステップＳ２８０において、アドレス監視部２２６は、特定デバイスであるプリンタにプリンタＩＤを付与し、プリンタＩＤとＩＰアドレスと機種名と製造番号とを監視対象情

報格納部２３２（図２）に格納されている監視対象情報に追加する。これにより、特定デバイスは監視用ＰＣ２００による監視の対象となり、管理情報が管理エージェント２２０（図２）により取得される。

【０１１２】

図１０（ｂ）は、図１０（ａ）の例においてユーザが特定デバイスを監視対象とする指示を与えることにより、ステップＳ２８０において特定デバイスが追加された監視対象情報を示している。図１０（ｂ）に示す監視対象情報は、図３に示す監視対象情報に追加されたプリンタに関する情報が付加されている。

【０１１３】

このように、第２実施例では、ＮＴＰメッセージの送信元である特定デバイスを監視対象とするか否かが判断され、必要に応じて特定デバイスが監視対象に追加される。そのため、ＮＴＰクライアント１１８（図２）が監視用ＰＣ２００のＮＴＰサーバ２５０（図２）と時刻の同期を行うように設定することにより、個々のプリンタに関する情報を監視対象情報に予め登録することなく、個々のプリンタを監視用ＰＣ２００で監視することが可能となる。

【０１１４】

なお、第２実施例では、ユーザからの指示に従って、特定デバイスを監視対象に追加するか否かを判断しているが、他の方法によって特定デバイスを監視対象に追加することも可能である。例えば、監視用ＰＣ２００が図９のステップＳ２３０で取得した識別情報を管理サーバ３００（図２）に送信し、管理サーバ３００から特定デバイスを監視対象とするか否かの情報を受信することにより、特定デバイスを監視対象に追加するか否かを判断することも可能である。この場合、管理サーバ３００は、監視用ＰＣ２００から受信した識別情報と、プリンタ管理データベース３２０に格納された監視対象プリンタに関する情報と、を対照することにより特定デバイスを監視対象とするか否かを判断することができる。

【０１１５】

また、監視用ＰＣ２００に予め監視対象追加条件を設定しておき、この監視対象追加条件に特定デバイスが合致する場合に、特定デバイスを自動的に監視対象に追加することもできる。このようにすれば、監視対象のプリンタが多い場合であっても、各プリンタを同一の監視用ＰＣ２００に対して時刻同期を行うように設定すれば、各プリンタを監視対象に追加することができる。そのため、個々のプリンタの監視対象への登録を省略できるので、監視対象の設定がより容易になる。また、監視対象追加条件を適宜設定することにより、ＮＴＰサーバにアクセス可能な装置であれば、既設のプリンタ、製造者が異なるプリンタ、あるいは、プリンタ以外のデバイスを監視対象に登録することができ、これらのプリンタあるいはデバイスの監視を行うことが可能になる。さらに、事後的に監視対象を変更する必要が生じた場合、監視対象追加条件を変更することにより、監視対象を変更することができる。この場合、監視対象のデバイスは、監視対象追加条件の変更の後、各デバイスの電源が再投入された段階で自動的に登録される。

【０１１６】

Ｃ．第３実施例：

図１１は、第３実施例のプリンタ管理システムを構成するネットワークデバイスの構成を示す説明図である。なお、図１１に示す第３実施例のプリンタ管理システムは、プリンタ１００ｄと監視用ＰＣ２００とが、それぞれプリンタ１０１００ｄと監視用ＰＣ１０２００に置き換えられている点と、ローカルエリアネットワークＬＡＮ１上にＤＮＳ（Domain Name System）サーバ５００が設けられている点とで、図２に示す第１実施例のプリンタ管理システムと異なっている。他の点においては、図２に示す第１実施例と同様である。

【０１１７】

図１１に示すプリンタ１０１００ｄは、デバイス登録部１４０を備えている点と、ＮＴＰクライアントおよび計時タイマが省略されている点とで、図２に示すプリンタ１００ｄ

と異なっている。図１１に示す監視用ＰＣ１０２００は、ＮＴＰサーバ２５０が省略されている点で、図２に示す監視用ＰＣ２００と異なっている。

【０１１８】

プリンタ１０１００ｄのデバイス登録部１４０は、プリンタ１０１００ｄのＩＰアドレスとホスト名とをＤＮＳサーバ５００に登録する。なお、デバイス登録部１４０によるＩＰアドレスとホスト名との登録については、後述する。ここでホスト名とは、ユーザがネットワークデバイスをより容易に認知できるように、個々のデバイスに対して設定される名前である。

【０１１９】

図１２は、監視用ＰＣ１０２００とプリンタ１０１００ｄとＤＮＳサーバ５００との間のデータ通信に関する機能の階層構造を示すブロック図である。図１２のブロック図は、プリンタ１０１００ｄと監視用ＰＣ１０２００と機能ブロックが変更されている点と、ＤＮＳサーバ５００が付加されている点と、で図４に示す第１実施例のブロック図と異なっている。他の点は、図４と同様である。

【０１２０】

図１２に示すプリンタ１０１００ｄは、ＵＤＰ処理部１４００の上位に設けられたＮＴＰクライアント１１８（図４）がデバイス登録部１４０に置き換えられている点で、図４のプリンタ１００ｄと異なっている。他の点は、図４のプリンタ１００ｄと同じである。

【０１２１】

図１２に示す監視用ＰＣ１０２００は、第１実施例の監視用ＰＣ２００（図４）からＮＴＰサーバ２５０の機能が除かれている。監視用ＰＣ１０２００のネットワークインターフェース２１００は、宛先ＭＡＣアドレスがネットワークインターフェース２１００のＭＡＣアドレス「00:0C:C2:04:13:A4」となっているＭＡＣフレームの他、宛先ＭＡＣアドレスがネットワークインターフェース２１００のＭＡＣアドレスとは異なるＭＡＣフレームも受信可能なように設定されている。

【０１２２】

ＤＮＳサーバ５００は、その最上層に、アドレス解決部５４１０を有している。アドレス解決部５４１０の下層には、上から順番に、ＵＤＰ処理部５４００と、ＩＰ処理部５２００と、ネットワークインターフェース５１００と、が設けられている。ＵＤＰ処理部５４００とＩＰ処理部５２００との機能および構成は、監視用ＰＣ１０２００のＵＤＰ処理部２４００とＩＰ処理部２２００と同様である。ネットワークインターフェース５１００についても、他のネットワークインターフェース１１００，２１００，４１００，４２００と同様に、ＭＡＣアドレスが割り当てられている。

【０１２３】

アドレス解決部５４１０は、ホスト名とＩＰアドレスとの対応表（アドレス解決テーブル）を有している。アドレス解決部５４１０は、このアドレス解決テーブルを参照することにより、ホスト名からＩＰアドレスを取得し、あるいは、ＩＰアドレスからホスト名を取得することができる。そのため、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２上のデバイスは、ホスト名を用いてＤＮＳサーバ５００にＩＰアドレスを問い合わせ、そのホスト名を有するデバイスを特定可能なＩＰアドレスを取得することができる。このようにホスト名等の名前（ネットワーク名）からＩＰアドレス等のネットワーク識別子を取得することは、一般に、「アドレス解決」と呼ばれる。

【０１２４】

アドレス解決部５４１０は、また、ローカルエリアネットワークＬＡＮ１を介して、ホスト名とＩＰアドレスとの組を受信し、受信したホスト名とＩＰアドレスとの組でアドレス解決テーブルを書き換えることが可能となっている。

【０１２５】

図１３は、プリンタ１０１００ｄのデバイス登録部１４０により実行されるデバイス登録実行ルーチンを示すフローチャートである。このデバイス登録実行ルーチンは、プリンタ１０１００ｄの起動時に実行される。

【０１２６】
ステップＳ３１０においてデバイス登録部１４０は、プリンタ１０１００ｄ自身のＩＰアドレスと、ＤＮＳサーバ５００のＩＰアドレスとを取得する。具体的には、デバイス登録部１４０は、ローカルエリアネットワークＬＡＮ２上に設けられたＤＨＣＰサーバ（図示しない）にＩＰアドレスの割り当てと、ＤＮＳサーバ５００のＩＰアドレスの通知と、を要求する。ＤＨＣＰサーバは、ローカルエリアネットワークＬＡＮ２で使用可能なＩＰアドレスをプリンタ１０１００ｄに割り当て、割り当てたＩＰアドレスと、ＤＮＳサーバ５００のＩＰアドレスと、をデバイス登録部１４０に通知する。
【０１２７】
ステップＳ３２０において、デバイス登録部１４０は、ステップＳ３１０において割り当てられたプリンタ１０１００ｄ自身のホスト名とＩＰアドレスとの組を、ＤＮＳサーバ５００に登録する。具体的には、デバイス登録部１４０は、自身のホスト名とＩＰアドレスとを所定の形式のメッセージ（以下、「登録メッセージ」とも呼ぶ）に格納してＤＮＳサーバ５００に送信する。
【０１２８】
図１２の例でプリンタ１０１００ｄからＤＮＳサーバ５００に登録メッセージが伝送される場合、ローカルエリアネットワークＬＡＮ１で伝送されるＭＡＣフレームの宛先ＭＡＣアドレスには、ネットワークインタフェース５１００のＭＡＣアドレス「11:00:AA:C5:41:0E」が格納される。そのため、ネットワークインターフェース５１００は、登録メッセージを伝送するＭＡＣフレームを受信し、ＩＰ処理部５２００とＵＤＰ処理部５４００とを介して登録メッセージをアドレス解決部５４１０に供給する。アドレス解決部５４１０は、このようにして受信したホスト名とＩＰアドレスとの組を用いて、アドレス解決テーブルを書き換える。
【０１２９】
上述のように、監視用ＰＣ１０２００のネットワークインターフェース２１００は、宛先ＭＡＣアドレスがネットワークインターフェース２１００に割り当てられたＭＡＣアドレス「00:0C:C2:04:13:A4」とは異なるＭＡＣフレームも受信する。そのため、ＤＮＳサーバ５００に登録メッセージを伝送するＭＡＣフレームは、ネットワークインターフェース２１００によっても受信される。
【０１３０】
図１３のステップＳ３３０において、デバイス登録部１４０は、前回の登録から所定の時間が経過したか否かを判断する。前回の登録から所定の時間が経過していないと判断された場合には、制御は戻され、ステップＳ３３０が繰り返し実行される。一方、前回の登録から所定の時間が経過していると判断された場合には、制御はステップＳ３４０に移される。ステップＳ３４０では、ステップＳ３２０と同様に、自身のホスト名とＩＰアドレスとを格納した登録メッセージがＤＮＳサーバ５００に送信される。ステップＳ３４０での登録メッセージの送信の後、制御はステップＳ３３０に戻される。これにより、ＤＮＳサーバ５００のアドレス解決テーブルは、所定の時間間隔で更新される。但し、ＤＮＳサーバ５００へのホスト名とＩＰアドレスとの登録は、プリンタ１０１００ｄの起動毎に１回のみ行うものとしても良い。
【０１３１】
図１４は、第３実施例において、監視用ＰＣ１０２００のアドレス監視部２２６（図１１）により実行されるプリンタアドレス監視ルーチンを示すフローチャートである。図１４に示す第３実施例のルーチンは、ステップＳ２１０とステップＳ２２０が、それぞれステップＳ２１２とステップＳ２２２に置き換えられている点で、図７に示す第１実施例のルーチンと異なっている。他の点は、図７に示す第１実施例のルーチンと同じである。
【０１３２】
ステップＳ２１２において、アドレス監視部２２６は、ＤＮＳサーバ５００への登録メッセージの送信が行われたか否かを判断する。具体的には、アドレス監視部２２６は、パケット監視部２２１０（図１２）が取得した受信データの宛先ポート番号を監視する。そ

して、宛先ポート番号が登録メッセージの伝送に使用されるポート番号であった場合には、ＤＮＳサーバ５００への登録メッセージの送信が行われたものと判断する。登録メッセージの送信があったと判断された場合には、制御はステップＳ２２２に移される。一方、登録メッセージの送信がなかったと判断された場合には、制御は戻され、ステップＳ２１２が繰り返し実行される。

【０１３３】

ステップＳ２２２において、アドレス監視部２２６は、登録メッセージの送信元のＩＰアドレスを取得する。登録メッセージの送信元のＩＰアドレスは、パケット監視部２２１０（図１２）により取得された登録メッセージを含む受信データの送信元ＩＰアドレスから取得することが可能である。ステップＳ２２２における登録メッセージの送信元のＩＰアドレスの取得の後は、図７に示す第１実施例と同様に処理が行われる。これにより、監視の対象となるプリンタ１０１００ｄのＩＰアドレスを取得し、取得したＩＰアドレスを用いてプリンタ１０１００ｄの監視をすることができる。

【０１３４】

第３実施例のプリンタ１０１００ｄのように、ＩＰアドレスが動的に割り当てられる場合、プリンタ１０１００ｄを使用するネットワークデバイスは、プリンタ１０１００ｄのホスト名から動的に割り当てられたＩＰアドレスを取得することが必要になる。そのため、プリンタ１０１００ｄは、一般に、割り当てられたＩＰアドレスとホスト名とをＤＮＳサーバ５００等に通知する。第３実施例では、監視用ＰＣ１０２００が、このようにプリンタ１０１００ｄがネットワークに対して通常送信するメッセージからプリンタ１０１００ｄのＩＰアドレスを取得することができる。そのため、プリンタ１０１００ｄに新たな機能を付加することなくプリンタ１０１００ｄのＩＰアドレスを取得し、取得したＩＰアドレスを用いてプリンタ１０１００ｄの監視を行うことができる。

【０１３５】

なお、第３実施例では、プリンタ１０１００ｄは、ＤＮＳサーバ５００にＩＰアドレスとホスト名とを通知しているが、ローカルエリアネットワークＬＡＮ１，ＬＡＮ２の構成によって、プリンタ１０１００ｄが送信し、監視用ＰＣ１０２００でのＩＰアドレス取得に使用されるメッセージとその送信先は適宜変更される。

【０１３６】

例えば、ネットワーク上でＮＢＴ（NetBIOS over TCP/IP）プロトコルが使用されており、アドレス解決がＷＩＮＳ（Windows Internet Name Service:Windowsは、Microsoft Corporationの商標）によって行われる場合、プリンタ１０１００ｄは、ＩＰアドレスおよびネットワーク名であるＮｅｔＢＩＯＳ名をＷＩＮＳサーバに対して通知する。監視用ＰＣ１０２００は、ＷＩＮＳサーバに対して送信されるメッセージからプリンタ１０１００ｄのＩＰアドレスを取得することができる。また、ネットワーク上でＢｏｎｊｏｕｒ（Apple Computer Incorporatedの商標）プロトコルが使用されている場合、プリンタ１０１００ｄは、ホスト名とＩＰアドレスとをネットワーク上の特定の複数のデバイスに通知する（このように、ネットワーク上の特定の複数のデバイスに同時にメッセージを送信することは、「マルチキャスト」とも呼ばれる）。監視用ＰＣ１０２００は、ネットワークに対してマルチキャストされたメッセージからプリンタ１０１００ｄのＩＰアドレスを取得することができる。

【０１３７】

さらに、監視用ＰＣ１０２００がプリンタのＩＰアドレスの取得に使用するメッセージは、上述のメッセージのようにアドレス解決のために使用されるメッセージでなくても良い。例えば、Ｂｏｎｊｏｕｒ、ＵＰｎＰ（Universal Plug and Play：ＵＰｎＰは、UPnP Implementers Corporationの商標）、あるいは、ＳＬＰ（Service Location Protocol）において、プリンタ１０１００ｄが提供するネットワークサービスをネットワーク上のデバイスに通知（アドバタイズ）するメッセージを使用して、プリンタ１０１００ｄのＩＰアドレスを特定することも可能である。一般に、監視用ＰＣ１０２００でのＩＰアドレス取得に使用されるメッセージは、所定のプロトコルに従ってプリンタ１０１００ｄからネ

ットワークに対して送信され、プリンタ１０１００ｄをネットワーク上で使用可能にするためのメッセージ、すなわち、プリンタ１０１００ｄの存在をネットワークに対して通知（登録）するためのメッセージであればよい。

【０１３８】

また、監視用ＰＣ１０２００がＩＰアドレスの取得に使用するメッセージとしては、上述の種々のメッセージの他、ＤＨＣＰやＡｕｔｏＩＰ等で使用されるメッセージのように、プリンタ１０１００ｄにＩＰアドレスを割り当てるためのメッセージを用いることも可能である。但し、これらのＩＰアドレスを割り当てるためのメッセージは、ネットワーク上の全てのデバイスに対して送信（ブロードキャスト）されるため、ネットワークの構成によって適用が困難な場合がある。

【０１３９】

Ｄ．変形例：

なお、この発明は上記実施例や実施形態に限られるものではなく、その要旨を逸脱しない範囲において種々の態様において実施することが可能であり、例えば次のような変形も可能である。

【０１４０】

Ｄ１．変形例１：

上記各実施例では、図３に示すように、監視対象情報には、監視対象プリンタのプリンタＩＤとＩＰアドレスと識別情報とが格納されているが、監視対象情報が含む情報は図３の例に限定されない。

【０１４１】

例えば、ＩＰアドレスのみが監視対象情報に含まれるものとしても良い。この場合、プリンタアドレス監視ルーチン（図７，図９，図１４）のステップＳ２４０では、ステップＳ２３０において取得された特定デバイスの識別情報を管理サーバ３００（図２）に送信する。そして、管理サーバ３００から受信した情報に基づいて、特定デバイスが監視対象プリンタであるか否かが判断される。但し、監視対象情報は、監視用ＰＣ２００，１０２００と管理サーバ３００とのトラフィックを低減するため、監視対象プリンタの識別情報を含むのがより好ましい。

【０１４２】

また、監視対象情報は、監視対象プリンタでない個々のデバイスに関する情報も含んでいても良い。この場合、監視対象プリンタか否かは、監視対象情報に個々のデバイスが監視対象か否かを表すフラグを含めることにより、そのフラグの値によって判断できる。

【０１４３】

Ｄ２．変形例２：

上記各実施例では、個々のプリンタを識別する識別情報として、機種名と製造番号とを使用しているが、識別情報は個々のプリンタによって異なる任意の情報とすることができる。例えば、製造番号が個々のプリンタで互いに異なるように設定されている場合、製造番号のみを識別情報とすることもできる。また、ネットワークボードごとに別個の値が設定されるＭＡＣアドレスを識別情報として使用することも可能である。

【０１４４】

Ｄ３．変形例３：

上記各実施例では、本発明をＳＮＭＰプロトコルを用いて管理情報を取得するプリンタ管理システムに適用しているが、本発明は、ＩＰアドレスにより監視対象プリンタを特定し、監視対象プリンタの管理情報を取得する任意のプリンタ管理システムに適用することが可能である。例えば、プリンタ１００ａ～１００ｄ，１０１００ｄが、ＨＴＴＰサーバの機能を備えている場合、監視用ＰＣ２００，１０２００は、管理情報の送信を要求するＨＴＴＰリクエスト（ＧＥＴリクエスト）をＨＴＴＰサーバに送信し、そのＨＴＴＰリクエストに対するＨＴＴＰレスポンスから管理情報を取得することも可能である。この場合においても、通常、ＨＴＴＰはＴＣＰ／ＩＰを使用してメッセージの授受が行われるため、監視用ＰＣ２００，１０２００は、ＮＴＰメッセージあるいは登録メッセージを伝送す

る転送データから取得したＩＰアドレスにより監視対象プリンタを特定することが可能となる。

【０１４５】

Ｄ４．変形例４：

上記各実施例では、管理エージェント２２０（図２）が種々の情報を取得するプリンタは、ＩＰアドレスにより特定されているが、情報の取得対象となるプリンタはネットワーク上でデバイスを特定する任意の識別子（ネットワーク識別子）によって特定することができる。このようなネットワーク識別子としては、例えば、ＡｐｐｌｅＴａｌｋ（登録商標）のノードＩＤを使用することも可能である。このノードＩＤの値も、ＩＰアドレスと同様に、プリンタに固有に割り当てられた値でなく、単一のプリンタに対して異なる値が割り当て可能（変更可能）な値である。なお、この場合、プリンタによる時刻の同期は、ＩＰアドレスを使用するＮＴＰに換えて、ネットワーク識別子としてノードＩＤを使用するプロトコルにより実行される。

【０１４６】

Ｄ５．変形例５：

上記各実施例では、監視用ＰＣ２００，１０２００が取得・蓄積した管理情報を受信する管理サーバ３００によりプリンタの管理を行っているが、監視用ＰＣ２００，１０２００自体でプリンタの管理を行うものとしても良い。この場合、監視用ＰＣ２００，１０２００には、プリンタ管理データベースと、データベース管理部とが設けられる。そして、監視用ＰＣ２００，１０２００に設けられたプリンタ管理データベースに蓄積された管理情報に基づいて、課金処理などの必要な処理が行われる。

【０１４７】

Ｄ６．変形例６：

上記各実施例では、本発明を、プリンタの管理システムに適用しているが、本発明は、任意のネットワークデバイスをから管理情報を取得するネットワーク管理システムに適用することができる。一般に、管理の対象となるネットワークデバイスが、ネットワークに接続された時刻サーバと時刻を同期させることが望ましいネットワークデバイスであれば、本発明を適用することができる。本発明は、例えば、このようなネットワークデバイスとして、制御用コンピュータや、ファクシミリ装置等に適用することができる。

【図面の簡単な説明】

【０１４８】

【図１】本発明の第１実施例を適用するプリンタ管理システム１０の構成を示す説明図。

【図２】プリンタ１００ｄと、監視用ＰＣ２００と、管理サーバ３００と、のそれぞれの構成を示す説明図。

【図３】監視対象情報格納部２３２に格納されている監視対象情報の一例を示す説明図。

【図４】監視用ＰＣ２００とプリンタ１００ｄとの間のデータ通信に関する機能の階層構造を示すブロック図。

【図５】ローカルエリアネットワークＬＡＮ１，ＬＡＮ２上でＮＴＰメッセージ伝送する際の通信データの構成を示す説明図。

【図６】ＮＴＰクライアント１１８により実行される現在時刻設定ルーチンを示すフローチャート。

【図７】アドレス監視部２２６により実行されるプリンタアドレス監視ルーチンを示すフローチャート。

【図８】監視対象情報に登録されたプリンタ１００ｄのＩＰアドレスが更新される様子を示す説明図。

【図９】第２実施例において、アドレス監視部２２６により実行されるプリンタアドレス監視ルーチンを示すフローチャート。

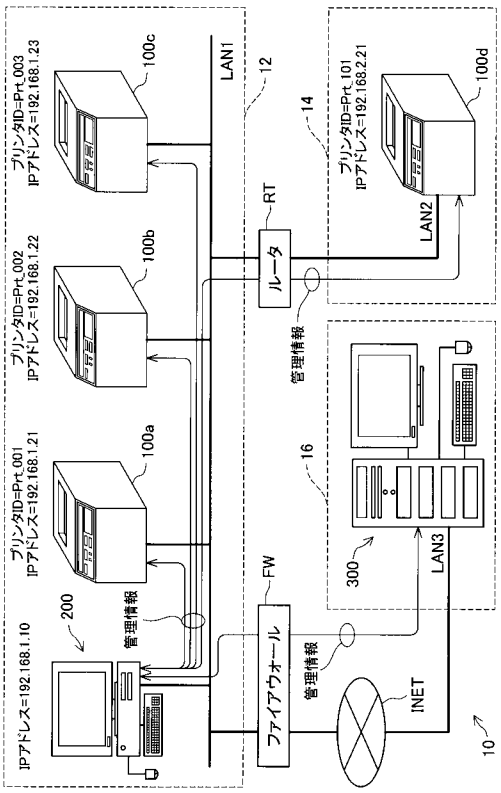
【図１０】第２実施例において、特定デバイスを監視対象に追加する様子を示す説明図。

【図１１】第３実施例のプリンタ管理システムを構成するネットワークデバイスの構成を示す説明図。

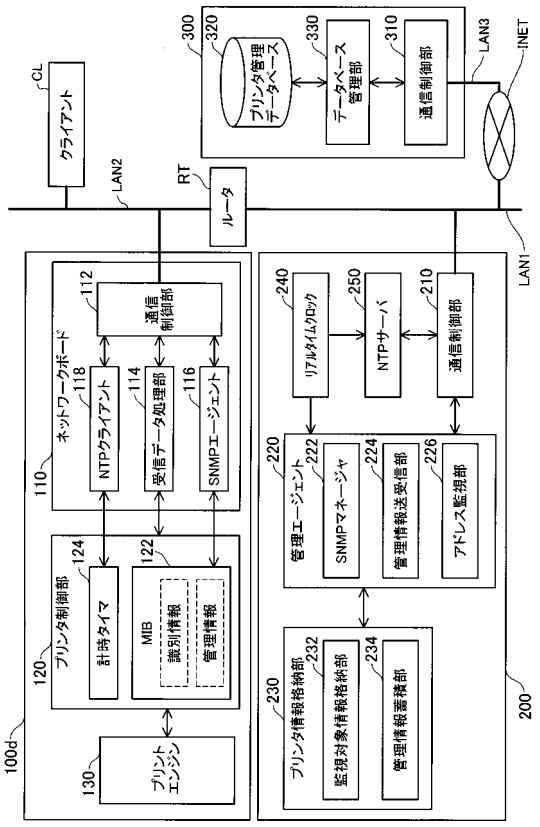
【図１２】監視用ＰＣ１０２００とプリンタ１０１００ｄとＤＮＳサーバ５００との間のデータ通信に関する機能の階層構造を示すブロック図。
【図１３】デバイス登録部１４０により実行されるデバイス登録実行ルーチンを示すフローチャート。
【図１４】第３実施例において、アドレス監視部２２６により実行されるプリンタアドレス監視ルーチンを示すフローチャート。
【符号の説明】
【０１４９】
１０…プリンタ管理システム
１２，１４，１６…ネットワークシステム
１００ａ～１００ｄ…プリンタ
１１０…ネットワークボード
１１２…通信制御部
１１４…受信データ処理部
１１６…ＳＮＭＰエージェント
１１８…ＮＴＰクライアント
１２０…プリンタ制御部
１２２…ＭＩＢ
１２４…計時タイマ
１３０…プリントエンジン
１４０…デバイス登録部
２００…監視用ＰＣ
２１０…通信制御部
２２０…管理エージェント
２２２…ＳＮＭＰマネージャ
２２４…管理情報送受信部
２２６…アドレス監視部
２３０…プリンタ情報格納部
２３２…監視対象情報格納部
２３４…管理情報蓄積部
２４０…リアルタイムクロック
２５０…ＮＴＰサーバ
３００…管理サーバ
３１０…通信制御部
３２０…プリンタ管理データベース
３３０…データベース管理部
５００…ＤＮＳサーバ
１１００…ネットワークインタフェース
１２００…ＩＰ処理部
１３００…ＴＣＰ処理部
１３１０…プリントサーバ
１４００…ＵＤＰ処理部
１４１０…ＳＮＭＰサーバ
２１００…ネットワークインタフェース
２２００…ＩＰ処理部
２２１０…パケット監視部
２３００…ＴＣＰ処理部
２３１０…ＨＴＴＰクライアント
２４００…ＵＤＰ処理部
２４１０…ＳＮＭＰクライアント

４１００，４２００…ネットワークインタフェース
５１００…ネットワークインタフェース
５２００…ＩＰ処理部
５４００…ＵＤＰ処理部
５４１０…アドレス解決部
１０１００ｄ…プリンタ
１０２００…監視用ＰＣ
ＣＬ…クライアント
ＦＷ…ファイアウォール
ＩＮＥＴ…インターネット
ＬＡＮ１，ＬＡＮ２，ＬＡＮ３…ローカルエリアネットワーク
ＲＴ…ルータ

【図１】



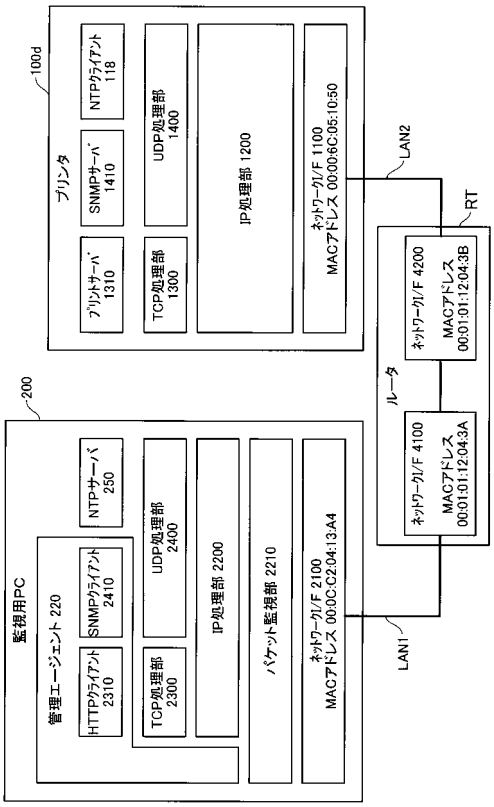
【図２】



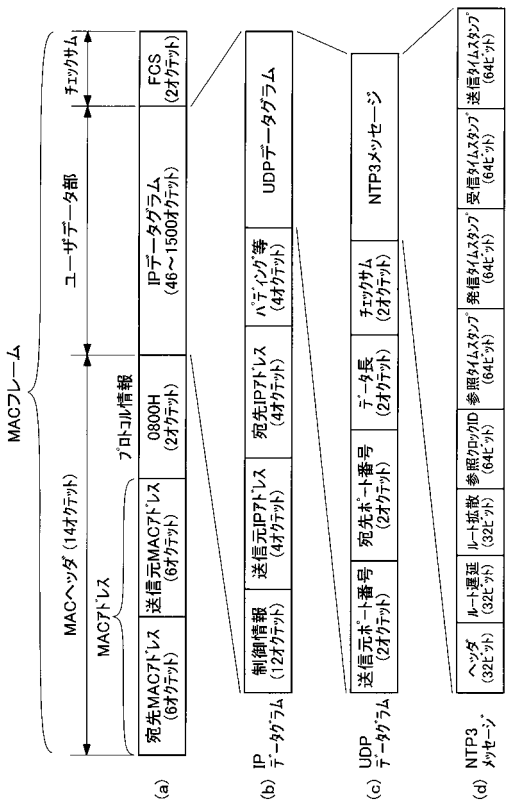
【図３】

監視対象情報				実際のIPアドレス	
ID	IPアドレス	機種名	製造番号		
Prt_001	192.168.1.21	LP-1234	1553182	192.168.1.21	←プリンタ100a
Prt_002	192.168.1.22	LP-1234	1552718	192.168.1.22	←プリンタ100b
Prt_003	192.168.1.23	LP-2345B	1581714	192.168.1.23	←プリンタ100c
Prt_101	192.168.2.21	LP-1234	1554176	192.168.2.21	←プリンタ100d

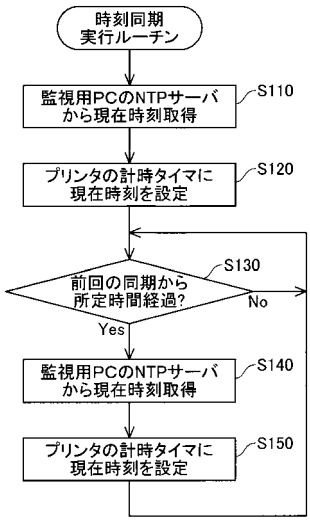
【図４】



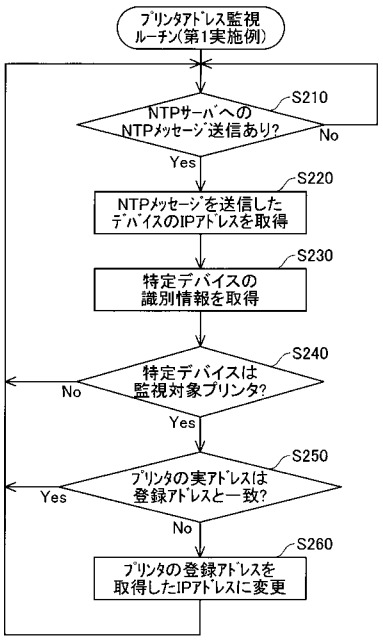
【図５】



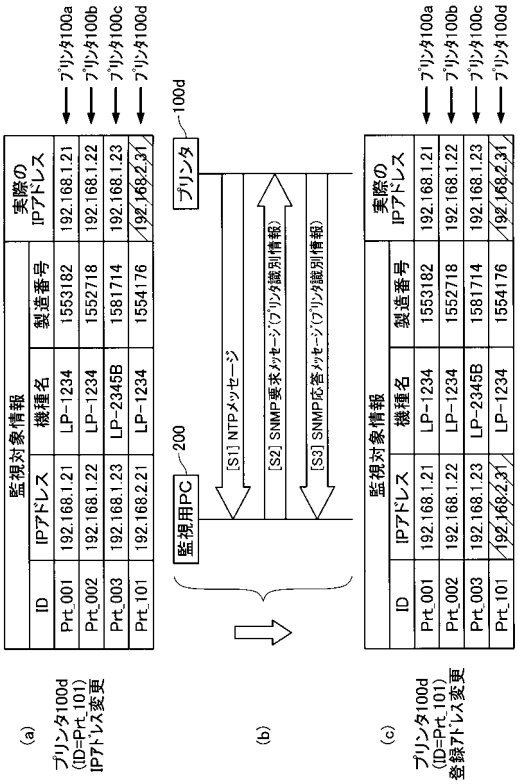
【図６】



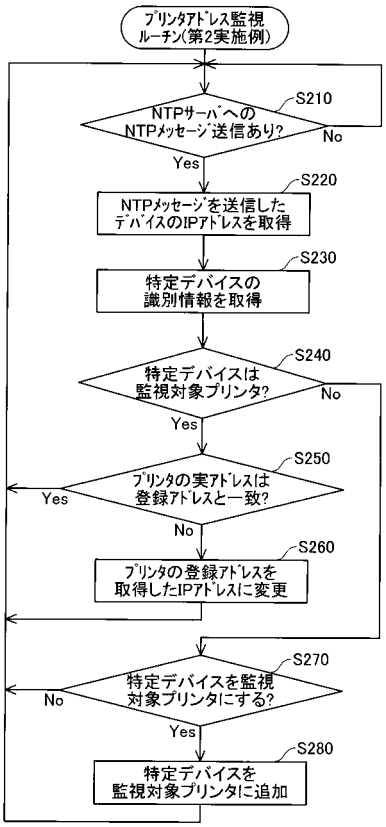
【図７】



【図８】

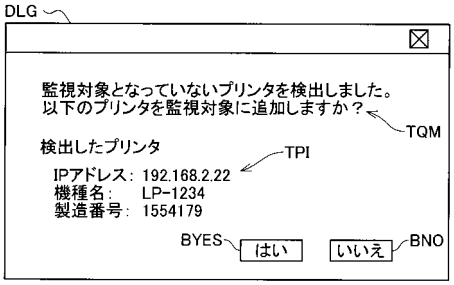


【図９】



【図１０】

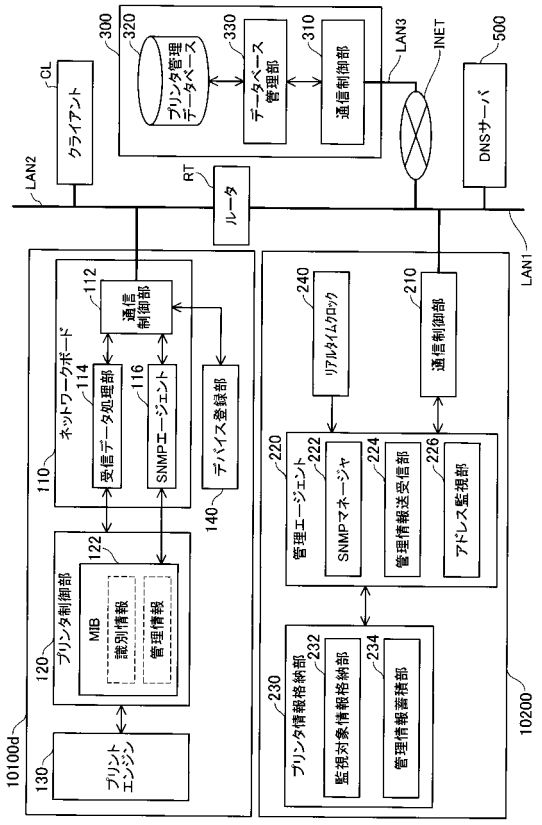
(a)



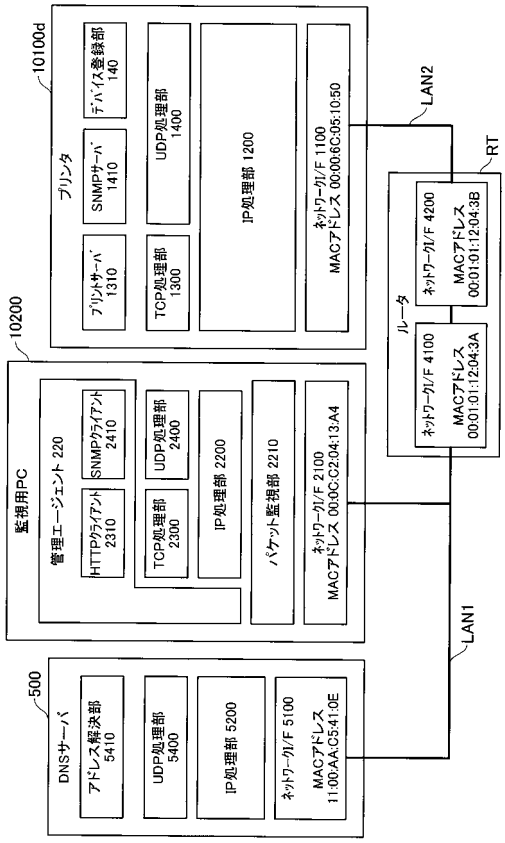
(b)

監視対象情報			
ID	IPアドレス	機種名	製造番号
Prt_001	192.168.1.21	LP-1234	1553182
Prt_002	192.168.1.22	LP-1234	1552718
Prt_003	192.168.1.23	LP-2345B	1581714
Prt_101	192.168.2.21	LP-1234	1554176
Prt_102	192.168.2.22	LP-1234	1554179

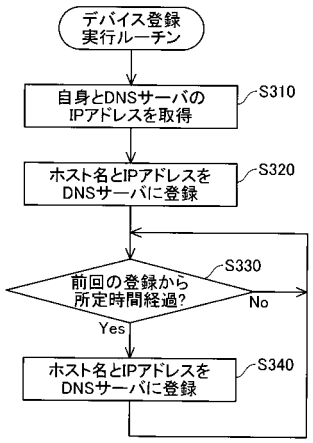
【図１１】



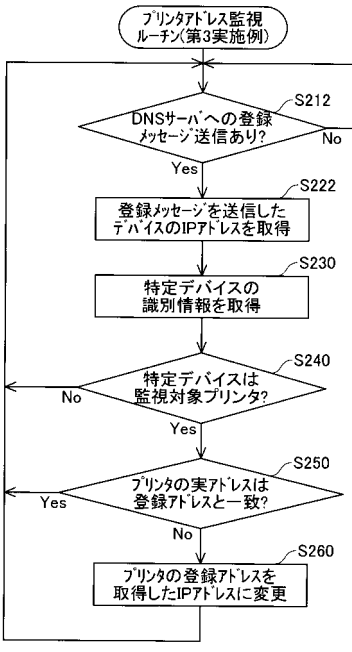
【図１２】



【図１３】



【図１４】



フロントページの続き

審査官　菅原　浩二

(56)参考文献　特開２００５－１７５６２５（ＪＰ，Ａ）
特開２００３－０９９３４０（ＪＰ，Ａ）
特開２００２－０７３４３８（ＪＰ，Ａ）
特開２００４－０５６５２１（ＪＰ，Ａ）
特開２００６－０８５６８９（ＪＰ，Ａ）
特開２００５－２４４７５３（ＪＰ，Ａ）
特開２００４－１９９４１０（ＪＰ，Ａ）
特開２００３－００８５７５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００