

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第3979413号
(P3979413)

(45) 発行日 平成19年9月19日(2007.9.19)

(24) 登録日 平成19年7月6日(2007.7.6)

(51) Int.C1.

F 1

H04L 12/24 (2006.01)
G06F 13/00 (2006.01)H04L 12/24
G06F 13/00 353V

請求項の数 23 (全 52 頁)

(21) 出願番号 特願2004-289130 (P2004-289130)
 (22) 出願日 平成16年9月30日 (2004.9.30)
 (65) 公開番号 特開2006-108800 (P2006-108800A)
 (43) 公開日 平成18年4月20日 (2006.4.20)
 審査請求日 平成17年9月27日 (2005.9.27)

(73) 特許権者 000005267
 プラザー工業株式会社
 愛知県名古屋市瑞穂区苗代町15番1号
 (74) 代理人 100082500
 弁理士 足立 勉
 (72) 発明者 田川 典生
 愛知県名古屋市瑞穂区苗代町15番1号
 プラザー工業株式会社内

審査官 衣鳩 文彦

最終頁に続く

(54) 【発明の名称】設定管理プログラムおよび設定管理システム

(57) 【特許請求の範囲】

【請求項1】

ネットワーク経由で所定の通信手順に従ってデータ通信可能なデバイスとして動作させるために必要な通信パラメータを複数種類の設定機能にて設定可能であり、該設定したときにおける設定機能を設定した通信パラメータと対応づけて登録するように構成された被管理デバイスを含む1以上のネットワーク接続されたデバイスのうち、いずれかのデバイスに前記通信パラメータを管理するための各種処理手順を実行させるための設定管理プログラムであって、

前記被管理デバイスにおける通信パラメータのうち、変更すべき通信パラメータをユーザに指定させる変更指定手順と、

該変更指定手順により指定された通信パラメータに対応づけて登録された設定機能に基づき、該通信パラメータと共に変更すべき設定機能に関する機能パラメータを推定するパラメータ推定手順と、

該パラメータ推定手順にて推定された機能パラメータが、前記変更指定手順にて指定された通信パラメータと共に変更すべきパラメータとして存在する旨を報知する存在報知手順と、が含まれている

ことを特徴とする設定管理プログラム。

【請求項2】

前記パラメータ推定手順においては、前記変更指定手順にてユーザが前記複数種類の通信パラメータのうちのいずれかを削除すべき通信パラメータとして指定した場合、該指定

された通信パラメータに対応づけて登録された設定機能について、該設定機能の一部または全部による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、

前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能の一部または全部による通信パラメータの設定を無効にすべき旨、または、前記機能パラメータに対応する設定機能の一部または全部以外の設定機能による通信パラメータの設定を有効にすべき旨を報知する

ことを特徴とする請求項1に記載の設定管理プログラム。

【請求項3】

前記パラメータ推定手順においては、前記変更指定手順にて指定された通信パラメータに対応づけて登録された設定機能と同種の設定機能について、該同種の設定機能による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定する

ことを特徴とする請求項2に記載の設定管理プログラム。

【請求項4】

前記複数種類の設定機能の中に、ネットワーク接続された他のデバイスから取得した前記通信パラメータを設定する機能が含まれてあり、

前記パラメータ推定手順においては、前記変更指定手順にて指定された通信パラメータに対応づけて登録された設定機能として他のデバイスから取得した前記通信パラメータを設定する機能について、該機能により前記他のデバイスと同じデバイスから取得した通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、

前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能による前記他のデバイスから取得した前記通信パラメータの設定を無効にすべき旨を報知する

ことを特徴とする請求項2または請求項3に記載の設定管理プログラム。

【請求項5】

前記変更指定手順においては、前記被管理デバイスにおいて追加的に設定すべき通信パラメータの少なくとも一部および設定機能を指定可能であり、

さらに、前記変更指定手順にて通信パラメータおよび設定機能が指定された際、該通信パラメータを設定すると共に、該通信パラメータに対応づけて前記設定機能を登録する設定登録手順が含まれており、

前記パラメータ推定手順においては、前記変更指定手順にてユーザが前記被管理デバイスにおいて追加的に設定すべき通信パラメータおよび設定機能を指定した場合、該指定された設定機能の一部または全部による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、

前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づき、該機能パラメータに対応する設定機能の一部または全部以外の設定機能による通信パラメータの設定を無効にすべき旨、または、前記機能パラメータに対応する設定機能の一部または全部による通信パラメータの設定を有効にすべき旨を報知する

ことを特徴とする請求項1から4のいずれかに記載の設定管理プログラム。

【請求項6】

前記パラメータ推定手順においては、前記変更指定手順にて指定された設定機能と同種の設定機能について、該同種の設定機能による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定する

ことを特徴とする請求項5に記載の設定管理プログラム。

【請求項7】

前記複数種類の設定機能の中に、ネットワーク接続された他のデバイスから取得した前記通信パラメータを設定する機能が含まれてあり、

前記パラメータ推定手順においては、前記変更指定手順にて指定された設定機能が、前

10

20

30

40

50

記他のデバイスから取得した前記通信パラメータを設定する機能について、該機能により前記他のデバイスと同じデバイスから取得した通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、

前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能が前記他のデバイスから取得した前記通信パラメータを設定する機能であれば、該機能による前記他のデバイスから取得した前記通信パラメータの設定を有効にすべき旨を報知する

ことを特徴とする請求項 5 または請求項 6 に記載の設定管理プログラム。

【請求項 8】

前記通信パラメータは、ネットワーク接続されたデバイスに割り当てられる識別情報の一部または全部を示すパラメータである 10

ことを特徴とする請求項 1 から 7 のいずれかに記載の設定管理プログラム。

【請求項 9】

前記複数種類の設定機能には、少なくとも、ユーザの操作を受けて前記通信パラメータを設定可能な手動設定機能、および、ユーザの操作とは無関係に前記通信パラメータを設定可能な自動設定機能が含まれている

ことを特徴とする請求項 1 から 8 のいずれかに記載の設定管理プログラム。

【請求項 10】

前記変更指定手順にて通信パラメータが指定された際、該指定された通信パラメータに基づき、該通信パラメータが通信パラメータとして適切であるか否かを判定するパラメータ判定手順が含まれており、 20

前記パラメータ推定手順においては、前記パラメータ判定手順にて適切なパラメータであると判定された場合にのみ前記機能パラメータの推定を行う

ことを特徴とする請求項 1 から 9 のいずれかに記載の設定管理プログラム。

【請求項 11】

前記存在報知手順にてパラメータの報知が行われた以降に、該報知内容に従ってパラメータを変更するか否かをユーザに選択させる変更選択手順と、

該変更選択手順にて前記機能パラメータを変更すべき旨が選択されたら、該機能パラメータと共に前記変更指定手順にて指定された通信パラメータを前記報知内容に従って変更する一方、前記機能パラメータを変更しない旨が選択されたら、前記変更指定手順にて指定された通信パラメータのみを前記報知内容に従って変更するパラメータ変更手順と、が含まれている 30

ことを特徴とする請求項 1 から 10 のいずれかに記載の設定管理プログラム。

【請求項 12】

前記被管理デバイスが同一設定機能により複数の通信パラメータを設定可能であって、

前記変更選択手順においては、前記変更指定手順にて指定された通信パラメータと同一の設定機能による他の通信パラメータが設定されていなければ、パラメータを変更するか否かの選択を行わせる一方、他の通信パラメータが設定されていれば、パラメータを変更するか否かの選択を行わせず、

前記パラメータ変更手順においては、前記変更選択手順によりパラメータを変更するか否かの選択を行わせない場合、前記変更指定手順にて指定された通信パラメータのみを変更する 40

ことを特徴とする請求項 11 に記載の設定管理プログラム。

【請求項 13】

前記被管理デバイスにおいて設定可能な設定機能それぞれによる通信パラメータの設定を許可するか否かをユーザの操作を受けて決定する第 1 設定許可手順が含まれており、

前記機能パラメータに対応する設定機能による通信パラメータの設定を許可する旨が前記第 1 設定許可手順にて決定されているか否かを判定する決定判定手順が含まれており、

前記変更選択手順においては、前記決定判定手順により決定されていると判定された場合に、パラメータを変更するか否かの選択を行わせ、 50

前記パラメータ変更手順においては、前記判定手順にて前記第1許可手順が決定されていない場合、前記変更指定手順にて指定された通信パラメータのみを変更することを特徴とする請求項11または請求項12に記載の設定管理プログラム。

【請求項14】

前記第1設定許可手順においては、ユーザの操作を受けて決定された設定するか否かを示す設定許可情報を前記被管理デバイスにおける記憶部に記憶させて、

前記変更選択手順においては、前記被管理デバイスの記憶部から読み出した設定許可情報が、前記機能パラメータに対応する設定機能による通信パラメータの設定を許可する旨の情報であれば、前記機能パラメータを変更するか否かの選択を行わせる

ことを特徴とする請求項13に記載の設定管理プログラム。 10

【請求項15】

前記変更指定手順にてユーザが前記複数の通信パラメータのうちのいずれかを削除すべき通信パラメータとして指定した際に、前記被管理デバイスを前記データ通信可能なデバイスとして動作させることを停止すべき停止条件が満たされたか否かを判定する条件判定手順が含まれてあり、

前記存在報知手順においては、前記条件判定手順にて停止条件が満たされたと判定された場合、前記被管理デバイスを前記データ通信可能なデバイスとして動作させるか否かを示すパラメータについて、動作させない旨に変更すべき旨を報知する

ことを特徴とする請求項1から14のいずれかに記載の設定管理プログラム。 20

【請求項16】

前記条件判定手順においては、前記被管理デバイスにおいて設定可能な通信パラメータのうち、前記データ通信可能なデバイスとして動作させるために必須の通信パラメータが、前記変更指定手順にて削除すべき通信パラメータとして指定された場合に、前記停止条件が満たされたと判定する

ことを特徴とする請求項15に記載の設定管理プログラム。 20

【請求項17】

前記条件判定手順においては、前記変更指定手順にて指定された通信パラメータ以外の通信パラメータが設定されていない場合に、前記停止条件が満たされたと判定する

ことを特徴とする請求項15に記載の設定管理プログラム。 20

【請求項18】

前記被管理デバイスを前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可するか否かをユーザの操作を受けて決定する第2設定許可手順が含まれてあり、

前記条件判定手順においては、前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可する旨が前記第2設定許可手順にて決定されていることを前提に前記停止条件が満たされたとの判定を行う

ことを特徴とする請求項15から17のいずれかに記載の設定管理プログラム。 30

【請求項19】

前記第2設定許可手順においては、ユーザの操作を受けて決定された許可するか否かを示す変更許可情報を前記被管理デバイスにおける記憶部に記憶させて、 40

前記条件判定手順においては、前記被管理デバイスの記憶部から読み出した変更許可情報が、前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可する旨の情報である場合、前記停止条件が満たされたと判定する

ことを特徴とする請求項18に記載の設定管理プログラム。 40

【請求項20】

前記変更指定手順により指定された通信パラメータが特定の設定機能により設定された通信パラメータである場合、該通信パラメータの変更を制限する変更制限手順が含まれている

ことを特徴とする請求項10から19のいずれかに記載の設定管理プログラム。 50

【請求項21】

前記被管理デバイスにおける設定機能により設定された通信パラメータそれぞれの変更を制限するか否かをユーザの操作を受けて決定する第3設定許可手順が含まれてあり、

前記変更制限手順においては、前記第3設定許可手順にて変更を制限すべき旨が前記第3設定許可手順にて決定されている設定機能について、該設定機能による通信パラメータの変更を制限する

ことを特徴とする請求項20に記載の設定管理プログラム。

【請求項22】

前記第3設定許可手順においては、ユーザの操作を受けて決定された制限するか否かを示す変更制限情報を前記被管理デバイスにおける記憶部に記憶させて、

前記変更制限手順においては、前記変更指定手順により指定された通信パラメータに対応する設定機能が、前記被管理デバイスの記憶部から読み出した変更制限情報で変更を制限すべき設定機能として示される設定機能である場合、該通信パラメータの変更を制限する

ことを特徴とする請求項20または請求項21に記載の設定管理プログラム。

【請求項23】

請求項1から22のいずれかに記載の設定管理プログラムに含まれる全ての処理手順と同様に機能する手段を備えてなる設定管理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワーク経由で所定の通信手順に従ってデータ通信可能なデバイスとして動作させるために必要な通信パラメータを管理するための設定管理プログラムに関する。

【背景技術】

【0002】

従来から、ネットワークデバイス（以降、単に「デバイス」という）をネットワーク経由でデータ通信可能に動作させるためには、例えば、デバイス自身の識別情報（IPアドレス）、ゲートウェイ（いわゆるデフォルトゲートウェイ）やDNS（Domain Name System）サーバの識別情報など各種のパラメータ（以降、「通信パラメータ」という）を設定する必要があり、このような設定は、例えば、ユーザの操作に基づき手動設定する機能、所定の通信手順（例えば、DHCP；Dynamic Host Configuration Protocol、NDP；Neighbor Discovery Protocolなど）に従って自動設定する機能など複数種類の設定機能それぞれにより実現されるように構成されていることが一般的である。

【0003】

ただ、このように設定機能により設定された通信パラメータは、その使用状態に合わせて任意に変更することはできるが、場合によっては、通信パラメータと共に特定の設定機能に関する他のパラメータを併せて変更しなければ、デバイスの正常な動作が維持できなくなってしまう虞がある。

【0004】

例えば、通信パラメータの設定を自動設定により実現する場合、こうして設定された通信パラメータは、通常、その使用期間（リース期間）が定められ、この使用期間毎に新たな通信パラメータに更新されていくことになる。このように、自動設定が有効になっているままの状態で、通信パラメータを手動設定する機能により変更してしまうと、上述の使用期間中であれば問題なくデータ通信を行うことができたとしても、使用期間が経過することにより通信パラメータが自動的に更新されてしまうため、以降のデータ通信が正常に行えなくなってしまう。より具体的には、デバイス自身の識別情報をユーザが任意に変更したのにも拘わらず、ユーザの意図しないタイミングで不用意に更新されてしまうと、それまで受信できていたデータが適切に受信できなくなってしまい、また、ゲートウェイサーバやDNSサーバの識別情報をユーザが任意に変更したのにも拘わらず、ユーザの意図しないタイミングで不用意に更新されてしまうと、それまで送信できていたデータが適切

10

20

30

40

50

に送信できなくなってしまう。

【0005】

近年、このような不具合を是正するための技術として、特定の設定機能に関する機能パラメータ（DHCPの有効または無効を示す情報）を変更（有効を示す情報に変更）するための操作が行われた際、この変更により正常な動作を妨げる要因（DHCP下で動作しないI/F）があるか否かをチェックし、あると判定した場合に、その旨を報知（パネルに表示）する、といった技術が提案されている（特許文献1参照）。

【0006】

この技術によれば、特定の設定機能に関する機能パラメータを変更する操作が行われた際に、この変更により正常な動作が妨げられることをユーザに知らせることができ、さらには、この機能パラメータと共に関連する他のパラメータ（I/Fの有効または無効を示すパラメータ）を併せて変更することもできる（特許文献1カッコ書参照）。

【特許文献1】特開2001-34434号公報（例えば、段落[0043]など）

【発明の開示】

【発明が解決しようとする課題】

【0007】

ただ、上述した技術において、正常な動作を妨げる要因があるか否かをチェックする際に参照されるのは、機能パラメータが通信パラメータを設定する設定機能に関するパラメータであるにも拘わらず、通信パラメータではなく、デバイスのI/Fといったハードウェア構成の設定に関するものである。つまり、上述した技術においては、機能パラメータと通信パラメータとが互いに密接な関係にあるにも拘わらず、両者を連携して変更すべきことまで報知することはできない。

【0008】

このように、両者を連携して変更すべきことを報知することは、通信パラメータがデバイスのハードウェア構成よりも頻繁に変更されうるものであることを考慮すると、デバイスのハードウェア構成に基づいて正常な動作を妨げる要因があることを報知するよりも必要性が高いと考えられ、このような報知を行うことのできる技術が要望されていた。

【0009】

本発明は、上記課題を解決するためになされたものであり、その目的は、機能パラメータと通信パラメータとを連携して変更すべきことを報知するための技術を提供することである。

【課題を解決するための手段】

【0010】

上記課題を解決するため請求項1に記載の設定管理プログラムは、ネットワーク経由で所定の通信手順に従ってデータ通信可能なデバイスとして動作させるために必要な通信パラメータを複数種類の設定機能にて設定可能であり、該設定したときにおける設定機能を設定した通信パラメータと対応づけて登録するように構成された被管理デバイスを含む1以上のネットワーク接続されたデバイスのうち、いずれかのデバイスに前記通信パラメータを管理するための各種処理手順を実行させるための設定管理プログラムである。そして、前記被管理デバイスにおける通信パラメータのうち、変更すべき通信パラメータをユーザに指定させる変更指定手順と、該変更指定手順により指定された通信パラメータに対応づけて登録された設定機能に基づき、該通信パラメータと共に変更すべき設定機能に関する機能パラメータを推定するパラメータ推定手順と、該パラメータ推定手順にて推定された機能パラメータが、前記変更指定手順にて指定された通信パラメータと共に変更すべきパラメータとして存在する旨を報知する存在報知手順と、が含まれている。

【0011】

このようなプログラムにより制御されるデバイスであれば、変更すべき通信パラメータがユーザにより指定された際、この通信パラメータに対応する設定機能（つまり、この通信パラメータを登録したときにおける設定機能）に基づいて、通信パラメータと共に変更すべき機能パラメータを推定し、その存在を報知することができる。これにより、ユーザ

10

20

30

40

50

が変更すべきものとして指定した通信パラメータと、この通信パラメータと密接な関係にある機能パラメータとを連携して変更すべきことを報知することができる。

【0012】

また、上述した変更指定手順は、被管理デバイスにおいて設定可能な通信パラメータのうち、変更すべき通信パラメータをユーザに指定させる手順であるが、ここでいう「変更すべき」とは、例えば、登録済みの通信パラメータの中から「削除すべき」場合が考えられる。このように、特定の通信パラメータが削除すべきものとして指定されることは、ユーザが、この通信パラメータを使用しなくてもよいと考えており、つまり、この通信パラメータを登録したときにおける設定機能を無効にしても問題ない、または、この通信パラメータを登録したときにおける設定機能以外の設定機能を有効にしたい、と考えていると推測することもできる。よって、登録済みの通信パラメータの中から「削除すべき」通信パラメータが指定される場合には、この通信パラメータを登録したときにおける設定機能による通信パラメータの設定について無効にすべき旨、または、この通信パラメータを登録したときにおける設定機能以外の設定機能による通信パラメータの設定について有効にすべき旨を報知するように構成することが考えられる。10

【0013】

このためには、例えば、請求項2に記載のように、前記パラメータ推定手順においては、前記変更指定手順にてユーザが前記複数種類の通信パラメータのうちのいずれかを削除すべき通信パラメータとして指定した場合、該指定された通信パラメータに対応づけて登録された設定機能について、該設定機能の一部または全部による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能の一部または全部による通信パラメータの設定を無効にすべき旨、または、前記機能パラメータに対応する設定機能の一部または全部以外の設定機能による通信パラメータの設定を有効にすべき旨を報知する、ように構成するとよい。20

【0014】

このように構成すれば、ユーザが削除すべきものとして通信パラメータを指定した際、ユーザの意図を推測して、こうして指定された通信パラメータを登録したときにおける設定機能を無効にすべき旨、または、この設定機能以外の設定機能を有効にすべき旨を報知することができる。30

【0015】

また、この構成において、パラメータ推定手順は、設定機能による通信パラメータの設定を有効にするか無効にするかを示すパラメータを機能パラメータとして推定する手順であって、このとき推定するパラメータに対応する設定機能は、変更指定手順にてユーザに指定された通信パラメータに対応づけて登録された設定機能だけとすればよい。

【0016】

なお、ここでいう「設定機能」には、複数種類の設定機能の中に、例えば、ユーザにより手入力された通信パラメータを自身に設定する種類の機能、他のデバイスから取得された通信パラメータを自身に設定する種類の機能などにおいて、それぞれ同種の機能が複数存在している場合であれば、この同種の設定機能についても含むものとしてもよい。40

【0017】

このような同種の設定機能による通信パラメータの設定については、無効にしたとしても問題はなく、むしろユーザの意図をより反映したものとすることが期待できる。このためには、例えば、請求項3に記載のように、前記パラメータ推定手順においては、前記変更指定手順にて指定された通信パラメータに対応づけて登録された設定機能と同種の設定機能について、該同種の設定機能による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定する、ように構成すればよい。

【0018】

このように構成すれば、ユーザが削除すべきものとして通信パラメータを指定した際、50

こうして指定された通信パラメータを登録したときにおける設定機能と同種の設定機能について無効にすべき旨を報知することができる。

【0019】

また、上述した存在報知手順が無効または有効にすべき旨を報知する「設定機能の全部による通信パラメータの設定」とは、この設定機能により通信パラメータを設定することそのものである。また、「設定機能の一部による通信パラメータの設定」とは、例えば、この設定機能により通信パラメータの一部分を設定すること、この設定機能が他のデバイスから取得した通信パラメータ（または、取得したパラメータに基づいて生成した通信パラメータ）を設定する機能である場合において、特定のデバイス（または、特定のデバイス以外）からのパラメータに基づいて通信パラメータを設定すること、などのことである
10。

【0020】

この後者のように、「他のデバイスから取得した通信パラメータの設定」を「前記設定機能の一部による通信パラメータの設定」とした場合、特定の通信パラメータが削除すべきものとして指定されることは、ユーザが、この通信パラメータを使用しなくてもよいと考えており、つまり、この通信パラメータの取得元であるデバイスからの以降の通信パラメータの設定を無効にしても問題ないと考えていると推測できることから、存在報知手順にて報知すべき旨としては、例えば、特定のデバイスから取得した通信パラメータの設定を無効にすべき旨とするように構成することが考えられる。
20

【0021】

このように、特定のデバイスから取得した通信パラメータの設定を無効にすべき旨を報知するための構成としては、例えば、請求項4に記載のように、前記複数種類の設定機能の中に、ネットワーク接続された他のデバイスから取得した前記通信パラメータを設定する機能が含まれてあり、前記パラメータ推定手順においては、前記変更指定手順にて指定された通信パラメータに対応づけて登録された設定機能として他のデバイスから取得した前記通信パラメータを設定する機能について、該機能により前記他のデバイスと同じデバイスから取得した通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能による前記他のデバイスから取得した前記通信パラメータの設定を無効にすべき旨を報知する、
30 ように構成すればよい。

【0022】

このように構成すれば、ユーザが削除すべきものとして通信パラメータを指定した際、こうして指定された通信パラメータを登録したときにおける設定機能が、他のデバイスから取得した通信パラメータを設定する機能である場合には、この機能により他のデバイスと同じデバイス（特定のデバイス）から取得した通信パラメータの設定を無効にすべき旨を報知することができる。

【0023】

なお、この構成において、通信パラメータの取得元となるデバイスが同一の設定機能に対して複数存在する場合には、設定機能を通信パラメータと対応づけて登録するにあたり、この取得元となるデバイスを識別可能な情報を登録するようにしておき、以降、こうして登録されたデバイスからの通信パラメータの登録を行わないように構成すればよい。
40

【0024】

また、上述した変更指定手順における「変更すべき」としては、例えば、新たな通信パラメータを「追加すべき」場合が考えられる。このように、特定の通信パラメータが追加すべきものとして指定されることは、ユーザが、この通信パラメータを使用したいと考えており、つまり、この通信パラメータを登録するときにおける設定機能を有効にすべき、または、この通信パラメータを登録するときにおける設定機能以外の設定機能を無効にしても問題ない、と考えていると推測することもできる。よって、「追加すべき」通信パラメータが指定された場合には、この通信パラメータを登録するときにおける設定機能によ
50

る通信パラメータの設定について有効にすべき旨、または、この通信パラメータを登録するときにおける設定機能以外の設定機能による通信パラメータの設定について無効にすべき旨を報知するように構成することが考えられる。

【0025】

このためには、例えば、請求項5に記載のように、前記変更指定手順においては、前記被管理デバイスにおいて追加的に設定すべき通信パラメータの少なくとも一部および設定機能を指定可能であり、さらに、前記変更指定手順にて通信パラメータおよび設定機能が指定された際、該通信パラメータを設定すると共に、該通信パラメータに対応づけて前記設定機能を登録する設定登録手順が含まれており、前記パラメータ推定手順においては、前記変更指定手順にてユーザが前記被管理デバイスにおいて追加的に設定すべき通信パラメータおよび設定機能を指定した場合、該指定された設定機能の一部または全部による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づき、該機能パラメータに対応する設定機能の一部または全部以外の設定機能による通信パラメータの設定を無効にすべき旨、または、前記機能パラメータに対応する設定機能の一部または全部による通信パラメータの設定を有効にすべき旨を報知する、ように構成するとよい。10

【0026】

このように構成すれば、ユーザが追加（追加的に設定）すべきものとして通信パラメータおよび設定機能を指定した際、ユーザの意図を推測して、こうして指定された通信パラメータを登録するときにおける設定機能を有効にすべき旨、または、この設定機能以外の設定機能を無効にすべき旨を報知することができる。20

【0027】

また、この構成において、パラメータ推定手順は、設定機能によるパラメータの設定を有効にするか無効にするかを示すパラメータを機能パラメータとして推定する手順であって、このとき推定するパラメータに対応する設定機能は、変更指定手順にてユーザに通信パラメータと共に指定された設定機能だけとすればよい。

【0028】

なお、ここでいう「設定機能」には、複数種類の設定機能の中に、例えば、ユーザにより手入力された通信パラメータを自身に設定する種類の機能、他のデバイスから取得された通信パラメータを自身に設定する種類の機能など、同種の機能が複数存在している場合であれば、この同種の設定機能についても含むものとしてもよい。30

【0029】

このような同種の設定機能による通信パラメータの設定については、有効にしたとしても問題はなく、むしろユーザの意図をより反映したものとすることが期待できる。このためには、例えば、請求項6に記載のように、前記パラメータ推定手順においては、前記変更指定手順にて指定された設定機能と同種の設定機能について、該同種の設定機能による通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定する、ように構成すればよい。

【0030】

このように構成すれば、ユーザが追加すべきものとして通信パラメータおよび設定機能を指定した際、こうして指定された設定機能と同種の設定機能について有効にすべき旨を報知することができる。40

【0031】

また、上述したように、「設定機能の一部による通信パラメータの設定」とは、例えば、この設定機能により通信パラメータの一部分を設定すること、この設定機能が他のデバイスから取得した通信パラメータを設定する機能である場合において、特定のデバイスからのパラメータに基づいて通信パラメータを設定すること、などのことである。

【0032】

このように、「他のデバイスから取得した通信パラメータの設定」を「前記設定機能の50

一部による通信パラメータの設定」とした場合、特定の通信パラメータが追加すべきものとして指定されることは、ユーザが、この通信パラメータを使用したいと考えてあり、つまり、この通信パラメータの取得元であるデバイスからの以降の通信パラメータの設定を有効にすべきと考えていると推測できることから、存在報知手順にて報知すべき旨としては、例えば、特定のデバイスから取得される通信パラメータの設定を有効にすべき旨とするように構成することが考えられる。

【0033】

このように、特定のデバイスから取得した通信パラメータの設定を無効にすべき旨を報知するための構成としては、例えば、請求項7に記載のように、前記複数種類の設定機能の中に、ネットワーク接続された他のデバイスから取得した前記通信パラメータを設定する機能が含まれてあり、前記パラメータ推定手順においては、前記変更指定手順にて指定された設定機能が、前記他のデバイスから取得した前記通信パラメータを設定する機能について、該機能により前記他のデバイスと同じデバイスから取得した通信パラメータの設定を有効にするか無効にするかを示すパラメータを前記機能パラメータとして推定して、前記存在報知手順においては、前記パラメータ推定手順にて推定された機能パラメータに基づいて、該機能パラメータに対応する設定機能が前記他のデバイスから取得した前記通信パラメータを設定する機能であれば、該機能による前記他のデバイスから取得した前記通信パラメータの設定を有効にすべき旨を報知する、ように構成すればよい。10

【0034】

このように構成すれば、ユーザが追加すべきものとして通信パラメータおよび設定機能を指定した際、こうして指定された通信パラメータを登録したときにおける設定機能が、他のデバイスから取得した通信パラメータを設定する機能であれば、この機能により他のデバイスから取得される通信パラメータの設定を有効にすべき旨を報知することができる。20

【0035】

なお、この構成において、通信パラメータの取得元となるデバイスが同一の設定機能に対して複数存在する場合には、変更指定手順にて、設定機能において取得元となるデバイスを識別可能な情報をユーザに指定させておき、こうして指定されたデバイスからの通信パラメータの登録を行うように構成すればよい。

【0036】

ところで、上述した通信パラメータとは、ネットワーク経由で所定の通信手順に従ってデータ通信可能なデバイスとして動作させるために必要なパラメータであり、例えば、請求項8に記載のように、ネットワーク接続されたデバイスに割り当てられる識別情報の一部または全部を示すパラメータのことである。30

【0037】

これによれば、通信パラメータにより被管理デバイスに識別情報の一部または全部を設定することができる。

ここでいう「デバイスに割り当てられる識別情報」としては、例えば、被管理デバイスに割り当てられる識別情報、被管理デバイスのデータ通信を中継する中継装置（例えば、ルータ、ゲートウェイサーバ、DNSサーバ、メールサーバなど）に割り当てられる識別情報（または、識別情報の一部分）などのことである。40

【0038】

また、上述した複数種類の設定機能は、どのような種類の設定機能が含まれていてもよく、例えば、請求項9に記載のように、前記複数種類の設定機能には、少なくとも、ユーザの操作を受けて前記通信パラメータを設定可能な手動設定機能、および、ユーザの操作とは無関係に前記通信パラメータを設定可能な自動設定機能が含まれていればよい。

【0039】

これによれば、少なくとも、通信パラメータを手動設定機能および自動設定機能それにより設定することができる。

また、上述したパラメータ推定手順においては、変更指定手順により指定された通信パ50

ラメータに対応する設定機能に基づいて機能パラメータを推定するが、このとき、変更指定手順にて通信パラメータとして不適切なパラメータが指摘されると、不適切なパラメータに基づいて不適切な機能パラメータが推定されてしまい、結果、被管理デバイスにおいて不適切な設定がなされてしまう虞がある。

【0040】

このようなことを防止するためには、例えば、請求項10に記載のように、前記変更指定手順にて通信パラメータが指定された際、該指定された通信パラメータに基づき、該通信パラメータが通信パラメータとして適切であるか否かを判定するパラメータ判定手順が含まれており、前記パラメータ推定手順においては、前記パラメータ判定手順にて適切なパラメータであると判定された場合にのみ前記機能パラメータの推定を行う、ように構成することが考えられる。10

【0041】

このように構成すれば、パラメータ推定手順による推定は、変更指定手順にて指定された通信パラメータが適切なものでなければ行われることがないため、これにより、不適切な機能パラメータが推定されて、被管理デバイスにおいて不適切な設定がなされてしまう虞もない。

【0042】

この構成において、パラメータ判定手順では、指定されたパラメータが通信パラメータとして適切であるか否かを判定することができれば、その判定方法については特に限定されない。例えば、通信パラメータとして想定される形式（例えば、使用可能な文字列、文字数、文字の構成など）が適切なパラメータであれば、適切な通信パラメータであると判定する、などといったように構成すればよい。20

【0043】

以上説明した設定管理プログラムとしては、存在報知手順にて報知が行われるように構成されたものを示したが、こうして報知を行った後、ユーザによるパラメータの変更を実際に行わせるように構成すればよく、この場合、ユーザの操作負担を軽減するために、例えば、請求項11に記載のように構成することが考えられる。

【0044】

請求項11に記載の設定管理プログラムは、前記存在報知手順にてパラメータの報知が行われた以降に、該報知内容に従ってパラメータを変更するか否かをユーザに選択させる変更選択手順と、該変更選択手順にて前記機能パラメータを変更すべき旨が選択されたら、該機能パラメータと共に前記変更指定手順にて指定された通信パラメータを前記報知内容に従って変更する一方、前記機能パラメータを変更しない旨が選択されたら、前記変更指定手順にて指定された通信パラメータのみを前記報知内容に従って変更するパラメータ変更手順と、が含まれている、ことを特徴とする。30

【0045】

このように構成すれば、存在報知手順にて報知が行われた後、報知内容に従ってユーザがパラメータを変更すべき旨を選択するだけで、存在報知手順による報知内容に従って通信パラメータと共に機能パラメータを変更することができる。

【0046】

この構成における変更選択手順は、存在報知手順にて報知が行われた以降、この報知内容に従ってパラメータを変更するか否かをユーザに選択させる手順であり、ユーザの選択に従ってパラメータ変更手順にて機能パラメータを変更させるように構成すればよい。また、必要に応じてユーザに選択させることを行わず、パラメータ変更手順において機能パラメータを変更させないように構成してもよい。40

【0047】

例えば、被管理デバイスが同一設定機能により複数の通信パラメータを設定可能な場合、同一の設定機能による他の通信パラメータが既に設定されている状態であれば、この時点で機能パラメータが適切な内容になっている可能性が高いため、この場合、ユーザに選択させなくても問題はない。このためには、例えば、請求項12に記載のように、前記被

管理デバイスが同一設定機能により複数の通信パラメータを設定可能であって、前記変更選択手順においては、前記変更指定手順にて指定された通信パラメータと同一の設定機能による他の通信パラメータが設定されていなければ、パラメータを変更するか否かの選択を行わせる一方、他の通信パラメータが設定されていれば、パラメータを変更するか否かの選択を行わせない、ように構成することが考えられる。

【0048】

このように構成すれば、同一の設定機能による他のパラメータが設定されている状態であれば、変更選択手順によりパラメータを変更するか否かの選択が行われることではなく、これにより、パラメータ変更手順において変更指定手順にて指定された通信パラメータのみを変更させ、機能パラメータについて変更させないようにすることができる。 10

【0049】

また、必要に応じてユーザに選択させることを行わず、パラメータ変更手順において機能パラメータを変更させないようにするためには、請求項13に記載のように、前記被管理デバイスにおいて設定可能な設定機能それぞれによる通信パラメータの設定を許可するか否かをユーザの操作を受けて決定する第1設定許可手順が含まれており、前記機能パラメータに対応する設定機能による通信パラメータの設定を許可する旨が前記第1設定許可手順にて決定されているか否かを判定する決定判定手順が含まれており、前記変更選択手順においては、前記決定判定手順により決定されると判定された場合に、パラメータを変更するか否かの選択を行わせ、前記パラメータ変更手順においては、前記判定手順にて前記第1許可手順が決定されていない場合、前記変更指定手順にて指定された通信パラメータのみを変更する、ように構成することが考えられる。 20

【0050】

このように構成すれば、第1設定許可手順により通信パラメータの設定を許可しない旨を決定しておけば、パラメータ変更手順において機能パラメータを変更させないようにすることができる。

【0051】

なお、この構成において、第1設定許可手順にて決定された通信パラメータの設定を許可するか否かを示す情報については、全て本設定管理プログラムを実行するデバイスが管理（記憶）するように構成してもよいが、被管理デバイス側で管理するように構成してもよい。この後者のためには、例えば、請求項14に記載のように、前記第1設定許可手順においては、ユーザの操作を受けて決定された設定するか否かを示す設定許可情報を前記被管理デバイスにおける記憶部に記憶させて、前記変更選択手順においては、前記被管理デバイスの記憶部から読み出した設定許可情報が、前記機能パラメータに対応する設定機能による通信パラメータの設定を許可する旨の情報であれば、前記機能パラメータを変更するか否かの選択を行わせる、ように構成することが考えられる。 30

【0052】

このように構成すれば、本設定管理プログラムを実行するデバイスが複数存在する環境で、1つの本設定管理プログラムを実行するデバイスで変更指定手順を実行すれば、他のデバイスでは変更指定手順を実行せずにすむ。また、設定許可情報を被管理デバイス側に記憶させることができるために、本設定管理プログラムを実行するデバイスに設定許可情報を記憶するための記憶領域を確保する必要がない。 40

【0053】

また、請求項15に記載の設定管理プログラムは、前記変更指定手順にてユーザが前記複数の通信パラメータのうちのいずれかを削除すべき通信パラメータとして指定した際に、前記被管理デバイスを前記データ通信可能なデバイスとして動作させることを停止すべき停止条件が満たされたか否かを判定する条件判定手順が含まれており、前記存在報知手順においては、前記条件判定手順にて停止条件が満たされたと判定された場合、前記被管理デバイスを前記データ通信可能なデバイスとして動作させるか否かを示すパラメータについて、動作させない旨に変更すべき旨を報知する、ことを特徴とする。

【0054】

このように構成すれば、変更指定手順にて削除すべき通信パラメータが指定された際、停止条件が満たされていれば、被管理デバイスをデータ通信可能なデバイスとして動作させるか否かを示すパラメータを、動作させない（つまり停止させることを示す）内容に変更すべき旨を報知することができる。

【0055】

この構成における「停止条件」としては、例えば、データ通信可能なデバイスとして動作させるために必須の通信パラメータが、変更指定手順にて削除すべき通信パラメータとして指定されたこと、を考えることができ、この場合には、請求項16に記載のように構成すればよい。

【0056】

請求項16に記載の設定管理プログラムのうち、前記条件判定手順においては、前記被管理デバイスにおいて設定可能な通信パラメータのうち、前記データ通信可能なデバイスとして動作させるために必須の通信パラメータが、前記変更指定手順にて削除すべき通信パラメータとして指定された場合に、前記停止条件が満たされたと判定する、ことを特徴とする。

【0057】

これによれば、データ通信可能なデバイスとして動作させるために必須の通信パラメータが削除すべきものとして指定された場合に、停止条件が満たされたと判定され、上述した報知を行うことができる。

【0058】

このように、必須の通信パラメータが削除すべきものとして指定された状態は、ユーザが被管理デバイスのデータ通信可能なデバイスとしての動作を停止させても問題ないと考えていることが推測されるため、この状態を停止条件が満たされたと判定して上述した報知を行うことにより、ユーザの意図を反映させた報知を行うことができる。

【0059】

また、上述した「停止条件」としては、変更指定手順にて指定された通信パラメータ以外の通信パラメータが設定されていないこと、を考えることもでき、この場合には、請求項17に記載のように構成すればよい。

【0060】

請求項17に記載の設定管理プログラムのうち、前記条件判定手順においては、前記変更指定手順にて指定された通信パラメータ以外の通信パラメータが設定されていない場合に、前記停止条件が満たされたと判定する、ことを特徴とする。

【0061】

これによれば、変更指定手順にて指定された通信パラメータ以外の通信パラメータが設定されていない場合に、停止条件が満たされたと判定され、上述した報知を行うことができる。

【0062】

このように、変更指定手順にて指定された通信パラメータ以外の通信パラメータが設定されていない状態は、ユーザが被管理デバイスのデータ通信可能なデバイスとしての動作を停止させようとしていることが推測されるため、この状態を停止条件が満たされたと判定して上述した報知を行うことにより、ユーザの意図を反映させた報知を行うことができる。

【0063】

また、上述した「停止条件」については、例示した状態となった場合であれば、常に満たされたと判定されるものとすればよいが、必要に応じて停止条件が満たされたと判定されなくなるように構成してもよい。この場合、例えば、請求項18に記載のように、前記被管理デバイスを前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可するか否かをユーザの操作を受けて決定する第2設定許可手順が含まれており、前記条件判定手順においては、前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可する旨が前記第2設定許可手順にて決定されているこ

10

20

30

40

50

とを前提に前記停止条件が満たされたとの判定を行う、ように構成すればよい。

【0064】

このように構成すれば、第2設定許可手順にてパラメータの変更を許可しない旨を決定しておけば、停止条件が満たされるような状態になったとしても、停止条件が満たされたと判定されないようにすることができる。

【0065】

なお、この構成において、第2設定許可手順にて決定されたパラメータの変更を許可するか否かを示す情報については、全て本設定管理プログラムを実行するデバイスが管理（記憶）するように構成してもよいが、被管理デバイス側で管理するように構成してもよい。この後者のためには、例えば、請求項19に記載のように、前記第2設定許可手順においては、ユーザの操作を受けて決定された許可するか否かを示す変更許可情報を前記被管理デバイスにおける記憶部に記憶させて、前記条件判定手順においては、前記被管理デバイスの記憶部から読み出した変更許可情報が、前記データ通信可能なデバイスとして動作させるか否かを示すパラメータの変更を許可する旨の情報である場合、前記停止条件が満たされたと判定する、ように構成すればよい。10

【0066】

このように構成すれば、被管理デバイスが複数存在する環境において、本設定管理プログラムを実行するデバイスにより全ての被管理デバイスそれぞれの設定を管理することができる。また、変更許可情報を被管理デバイス側に記憶させることができるために、本設定管理プログラムを実行するデバイスに変更許可情報を記憶するための記憶領域を確保しておく必要がない。20

【0067】

また、上述したパラメータ変更手順による通信パラメータの変更は、何ら制限なく行われるように構成すればよいが、任意に制限できるように構成してもよい。このためには、例えば、請求項20に記載のように、前記変更指定手順により指定された通信パラメータが特定の設定機能により設定された通信パラメータである場合、該通信パラメータの変更を制限する変更制限手順が含まれている、ように構成することが考えられる。

【0068】

このように構成すれば、変更制限手順により変更が制限された通信パラメータについては、パラメータ変更手順による変更を制限することができる。30

この構成における変更制限手順は、通信パラメータの変更を制限する手順であって、例えば、変更を制限すべき通信パラメータをユーザに選択させ、こうして選択された通信パラメータを登録するように構成すればよい。そして、パラメータ変更手順については、変更すべき通信パラメータが、変更制限手段により登録されたものであれば、変更を制限するように構成すればよい。なお、ここでいう「変更の制限」とは、例えば、変更そのものを禁止することや、通信パラメータの一部分のみの変更を認めるなどといったことである。

【0069】

また、この構成において、変更制限手順により変更を制限する通信パラメータについては、あらかじめ定められたものとしてもよいが、ユーザが任意に指定できるように構成してもよい。この後者のためには、例えば、請求項21に記載のように、前記被管理デバイスにおける設定機能により設定された通信パラメータそれぞれの変更を制限するか否かをユーザの操作を受けて決定する第3設定許可手順が含まれており、前記変更制限手順においては、前記第3設定許可手順にて変更を制限すべき旨が前記第3設定許可手順にて決定されている設定機能について、該設定機能による通信パラメータの変更を制限する、ように構成することが考えられる。40

【0070】

このように構成すれば、第3設定許可手順にて変更を制限する旨を決定しておけば、その通信パラメータについては、パラメータ変更手順において変更を制限することができる。50

【0071】

なお、この構成において、第3設定許可手順にて決定されたパラメータの変更を制限するか否かを示す情報については、全て本設定管理プログラムを実行するデバイスが管理（記憶）するように構成してもよいが、被管理デバイス側で管理するように構成してもよい。この後者のためには、例えば、請求項22に記載のように、前記第3設定許可手順においては、ユーザの操作を受けて決定された制限するか否かを示す変更制限情報を前記被管理デバイスにおける記憶部に記憶させて、前記変更制限手順においては、前記変更指定手順により指定された通信パラメータに対応する設定機能が、前記被管理デバイスの記憶部から読み出した変更制限情報で変更を制限すべき設定機能として示される設定機能である場合、該通信パラメータの変更を制限する、ように構成することが考えられる。

10

【0072】

このように構成すれば、変更制限情報を被管理デバイス側に記憶させることができるために、本設定管理プログラムを実行するデバイスに設定許可情報を記憶するための記憶領域を確保しておく必要がない。

【0073】

ここまでに説明した各設定管理プログラムは、コンピュータによる処理に適した命令の順番付けられた列からなるものであって、例えば、FD, CD-ROM, メモリーカードなどの記録媒体やインターネットなどの通信回線網を介して、デバイス、または、デバイスを利用するユーザに提供されるものである。また、これらプログラムをユーザに提供する形態としては、デバイスのハードディスクやメモリにプレインストールされた状態で提供する形態であってもよい。

20

【0074】

また、請求項23に記載の設定管理システムは、請求項1から22のいずれかに記載の設定管理プログラムに含まれる全ての処理手順と同様に機能する手段を備えてなる設定管理システムである。

【0075】

このように構成された設定管理システムによれば、請求項1～22のいずれかに記載の設定管理プログラムを実行するデバイスの一部を構成することができる。

なお、この設定管理システムについては、1のデバイスからなるものであってもよいし、複数のデバイスが協調して動作するように構成したものであってもよい。また、この後者の場合においては、上述した設定管理プログラムの一部分がそれぞれ別のデバイスにより実行されるように構成すればよい。

30

【発明を実施するための最良の形態】**【0076】**

以下に、複数のパーソナルコンピュータ（以降、「PC」という）10（10_1～10_n）、複数のプリンタ20（20_1～20_m）、ゲートウェイ30、メールサーバ40、プライマリDNS（Domain Name System）サーバ50_1、セカンダリDNSサーバ50_2などが、図1に示すように、それぞれネットワーク経由でデータ通信可能に接続されてなる設定管理システムについて説明する。

【0077】

40

PC10は、CPU11、ROM12、RAM13、ハードディスク14、プロトコルスタック15、ネットワークインターフェース（ネットワークI/F）16、表示部17、入力部18などがバス19を介して接続され、ネットワークI/F16によりネットワークと接続された状態でネットワークデバイスとして機能する周知のコンピュータシステムである。

【0078】

これらのうち、プロトコルスタック15は、図1において、ネットワークI/F16をバス19に接続する構成要素として示しているが、これは、ネットワークI/F16によるデータ通信がプロトコルスタック15に従った処理を経て行われる状態を概念的に示したものであり、実際は、IPv4（Internet Protocol version 4）およびIPv6（In

50

ternet Protocol version 6) 両方に従ったデータ通信を実現するために実装 (ハードディスク 14 に記憶) されたプログラムモジュールである。

【 0079 】

また、ハードディスク 14 には、 S N M P (Simple Network Management Protocol) エージェントとして機能するデバイスに対する情報の通知、更新などを S N M P に従って指令するマネージャプログラムが記憶されており、これにより、 P C 10 を S N M P マネージャとして機能させることができる。

【 0080 】

また、この P C 10 のうち、 P C 10 _ 1 には、後述する各種処理を実行するための設定管理プログラムがインストールされている。

プリンタ 20 は、 C P U 21 , R O M 22 , R A M 23 , N V R A M (Non Volatile R A M) 24 , プロトコルスタック 25 , ネットワークインターフェース (ネットワーク I / F) 26 , ユーザインターフェース (ユーザ I / F) 27 , 印刷部 28 などがバス 29 を介して接続され、ネットワーク I / F 26 によりネットワークと接続された状態でネットワークデバイスとして機能する周知のネットワークプリンタである。

【 0081 】

これらのうち、 N V R A M 24 には、プリンタ 20 をネットワークデバイスとして機能させるための設定値が登録されるデータベース (M I B : Management Information Base) と、 S N M P マネージャとして機能するデバイスからの指令を受けてのデータベースに登録された情報の通知、更新などを S N M P に従って行うエージェントプログラムと、が記憶されており、この両者により、プリンタ 20 を S N M P エージェントとして機能させることができる。こうして、 S N M P マネージャからの指令を受けてデータベースを更新した際、プリンタ 20 は、後述するように、この更新内容に対応する自身の設定内容も併せて変更するように構成されている。また、プロトコルスタック 25 については、 P C 10 のプロトコルスタック 15 と同様、 N V R A M 24 に記憶されたプログラムモジュールである。

【 0082 】

また、これらプリンタ 20 は、エラーなどを電子メールによりあらかじめ定められた宛先に通知する機能や、印刷データが添付された電子メールをネットワーク経由で受信し、この電子メールに添付された印刷データを印刷する機能 (ネットワーク印刷機能) を有している。

【 0083 】

上述した P C 10 およびプリンタ 20 について、ネットワークを介してデータ通信可能な状態とするためには、そのネットワークにおいてデバイスを識別するための I P アドレスを設定する必要がある。なお、こうして設定する I P アドレスは、 I P v 4 であれば 1 つで十分であるのに対し、 I P v 6 では、通常複数の I P アドレスが設定される。

【 0084 】

また、 I P アドレスは、 I P v 4 であるか I P v 6 であるかに拘わらず、手動および自動の設定機能にて設定することができる。この設定機能のうち、手動の設定機能 (手動設定、スタティック) は、後述するように、 P C 10 の設定管理プログラムに従って行われるものである。また、自動の設定機能 (自動設定) については、 I P v 4 であれば、ネットワーク上に設置された D H C P (Dynamic Host Configuration Protocol) サーバから取得したものを自身の I P アドレスとして設定するものだけであるが、 I P v 6 であれば、 D H C P サーバから取得したものを自身の I P アドレスとして設定するもの (以降、「ステートフル」という) の他、ネットワーク上に設けられた図示しないルータなどから取得またはあらかじめ定められた情報 (プリフィックス) , および、自身のネットワーク I / F 16 , 26 に割り当てられた M A C アドレスから I P アドレスを生成して自身の I P アドレスとして設定するもの (以降、「ステートレス」という) がある。こうして、 I P アドレスが設定された際には、設定された I P アドレス、および、この I P アドレスを設定したときの設定機能が対応づけられた状態でデータベース (M I B) へ登録される。

10

20

30

40

50

【0085】

ここで、プリンタ20のデータベースに登録される情報のうち、本発明の特徴部分を説明するうえで必要なものについて説明する。

(1) プリンタ20自身のIPアドレス：これについては、設定したときにおける設定機能を示す情報が対応づけられた状態で登録される。

(2) デフォルトルータのIPアドレス：これについても、設定したときにおける設定機能が対応づけられた状態で登録される。

(3) プリフィックスの取得元デバイスのIPアドレス：これは、ステートレスによりIPアドレスを設定する際に、このIPアドレスを生成する元となるプリフィックスの取得先であるルータのIPアドレスであって、後述のようにリストとして登録されている。そして、こうして登録されたルータ以外からのRAは受信されなくなる（破棄される）。 10

(4) 自動設定有効情報：これは、プリンタ20において、ステートレスおよびステートフルによる設定それぞれを有効とするか否かを示す情報であって、この情報に基づいて有効であることを示す設定機能によるIPアドレスの設定のみが可能な状態となる。

(5) RA無視情報：これは、プリンタ20において、ルータから送信されるプリフィックスを含む情報（RA：Router Advertisement）を無視するか否かを示す情報であって、この情報が無視することを示す内容となっている間、ルータからプリフィックスが取得されなくなる。

(6) IPv6停止情報：これは、プリンタ20がIPv6によるデータ通信を停止させるか否かを示す情報であって、この情報が停止することを示す内容となっている間、IPv6によるデータ通信が行われなくなる。 20

【0086】

以下、上記構成のネットワークにおいて、PC10またはプリンタ20による処理内容が異なる実施形態について、それぞれ説明する。

[第1実施形態]

手動設定処理

以下に、PC10_1（のCPU11）により実行される手動設定処理の処理手順を図2に基づいて説明する。この手動設定処理は、上述した設定管理プログラムに従って実行される処理である。

【0087】

まず、ユーザがプログラムを起動するための操作を入力部18により行うと、ネットワーク上のデバイスを検索し、その結果を表示部17に一覧表示する（s102）。詳述すると、ネットワーク上のデバイスに対して一般情報を要求するための要求データを、IPv4およびIPv6それぞれにより送信（ブロードキャストおよびマルチキャスト）する。ここでいう「一般情報」とは、各デバイスに対して設定された情報であり、例えば、デバイス名（Node Name）などの情報である。そして、この要求データを受信したデバイスそれぞれから送信された情報を一定時間収集した後、図3に示すように、これらの情報をデバイス（デバイス名；Node Name）毎に配列した表形式の一覧表示画面を表示部17に表示する。このように一覧表示画面が表示された後、ユーザは、入力部18により、一覧表示されたうちのいずれかのデバイスを指定する操作などを行うことができる。 40

【0088】

こうして、一覧表示画面が表示されたら、ユーザによる操作が行われるまで待機する（s104：NO）。

その後、ユーザによる操作が行われた際（s104：YES）、その操作がいずれかのデバイスを指定する操作であれば（s106：YES）、こうして指定されたデバイス（以降、「被管理デバイス」という；本実施形態ではいずれかのプリンタ20）に対して設定情報を問い合わせる（s110）。ここでは、被管理デバイスの設定情報として、以降の処理で表示される設定画面のうちの表示対象となる画面に対応する情報、および、データベースの登録情報を問い合わせるために、この被管理デバイスに問合データを送信する。この問合データを受信した被管理デバイスからは、設定情報および登録情報を示す設定 50

データが返信されてくる。このとき、被管理デバイスは、問い合わせを受けた情報が自身に設定されていない情報である場合、設定されていない旨を特定可能な状態（例えば、空のパラメータなど）で設定データを返信してくる。なお、一覧表示画面が表示された以降、ユーザにより行われた操作が上述したいずれの操作でもない場合（s106：NO）、この操作に対応する処理（その他の処理）を行った後（s108）、s104の処理へ戻る。

【0089】

次に、s110の処理による問い合わせに対して返信されてきた設定データに基づいて、この被管理デバイスに対してパラメータを設定（リモートセットアップ）するための設定画面を表示部に表示する（s112、図4（a）（b）参照）。ここでは、複数の画面それぞれに対応するタブ201を選択する操作を行うことで表示対象となる画面が切り替えられ、それぞれの画面毎に異なる機能に対応するパラメータを入力するための入力欄の設けられてなる設定画面が表示される。10

【0090】

ここで、各画面のうち、本発明に関係のある画面について説明する。被管理デバイス固有の情報を表示させるための第1の画面として、s110の処理が最初に実行された場合に、図4（a）の画面が表示される。また、この画面は、他の画面から「General」タブ201aを選択することによって切り替えられる。ここでいう「固有の情報」とは、上述したs102の処理で収集したデバイス名（Node Name），被管理デバイスのインターフェース部に割り当てられたMACアドレス（MAC Address）などのことである。また、この第1の画面には、この被管理デバイスのユーザ名を入力するための入力欄202およびOKボタン302が設けられており、ここにユーザ名を入力し、OKボタン302を選択する操作を行うことにより、後述のように、この入力されたユーザ名が被管理デバイスに対して設定されることとなる。なお、この第1の画面に対応する情報は、被管理デバイスのデバイス名（Node Name）などであり、上述したs110の処理で送信する問合データにおいては、このデバイス名などのパラメータを問い合わせることとなる。20

【0091】

この第1の画面や他の画面から「TCP/IP」タブ201bを選択することで、図4（b）に示す画面（他のタグを省略した状態）が表示される。この図4（b）に示す画面（以下、「第2の画面」という）では、デバイスをIPv4およびIPv6のいずれか一方または両方によるデータ通信を可能な状態とするIP_Mode，デバイスに割り当てられたIPv4に対応するIPアドレス，ゲートウェイ30のIPアドレス（いわゆるデフォルトゲートウェイ；Gateway），DNSサーバ50（プライマリおよびセカンダリDNSサーバ；Primary DNS Server，Secondary DNS Server）のIPアドレスなど、ネットワークを介してのデータ通信を実現するために必要なパラメータを設定することができる。この第2の画面には、上述した各IPアドレスなどを入力するための入力欄210～218などが設けられており、これら入力を行った後で、OKボタン310を選択する操作を行うことにより、後述のように、この入力された情報が被管理デバイスに対して設定されることとなる。また、この第2の画面には、デバイスにおけるIPv6に関する設定を行う「IPv6_Settings」画面を表示させるための「IPv6_Settings」ボタン410が設けられており、この「IPv6_Settings」ボタン410を選択する操作を行うことにより、後述する「IPv6_Setting」処理が行われることとなる。なお、この第2の画面に対応する情報は、上述した各IPアドレスなどのパラメータ（「IPv6_Setting」に関するパラメータを含む）であり、上述したs110の処理で送信する問合データにおいては、これらパラメータを問い合わせることになる。3040

【0092】

なお、その他、設定画面における画面としては、「POP3/SMTP」タブ201cを選択することにより切り替えられる画面であって、上述したネットワーク印刷機能を実現するために必要なメールサーバ40のIPアドレスなどが表示される画面などがある（50

図4(c)参照)。

【0093】

このように、設定画面が表示された後、ユーザは、入力部18により、タブ201を選択する操作、各入力欄にパラメータを入力する操作、「IPV6_Settings」ボタン410を選択する操作、OKボタンを選択する操作などを行うことができる。

【0094】

こうして、s112の処理で設定画面が表示された以降、ユーザによる操作が行われるまで待機する(s114: NO)。

その後、ユーザによる操作が行われたら(s114: YES)、その操作が入力欄への入力を行う操作であれば(s116: YES)、こうして入力された内容を入力欄に表示(反映)させた後(s118)、s114の処理へ戻る。

10

【0095】

また、ユーザによる操作が設定画面(第2の画面)における「IPV6_Settings」ボタン410を選択する操作であれば(s116: NO, s120: YES)、後述する「IPV6_Setting処理」を行った後、s114の処理へ戻る。この「IPV6_Setting処理」は、デバイスに割り当てられたIPV6に対応するIPアドレスなど、ユーザにIPV6に関連するパラメータを指定させる処理であり、詳細な処理手順については後述する。

【0096】

また、ユーザによる操作が設定画面における表示対象となる画面を切り替えるための操作、つまりタブを選択する操作であれば(s120: NO, s124: YES)、s110の処理へ戻り、このs110の処理にて、上述したように、選択されたタブの画面に対応する設定情報を被管理デバイスに対して問い合わせたうえ、s112の処理で設定画面を表示する。

20

【0097】

こうして、s110～s124の処理を繰り返した後、s114の処理によるユーザの操作が、設定画面におけるいずれかの画面のOKボタンを選択する操作であれば(s124: NO, s126: YES)、「IPV6_Setting処理」にて指定されたパラメータを除き、設定画面における全ての画面の入力欄に入力されているパラメータそれぞれの設定を被管理デバイスに指令するための設定指令データを、この設定デバイスに送信した後(s128)、本手動設定処理を終了する。この設定指令データを受信した被管理デバイスは、この設定指令データに基づいて自身に対してパラメータを設定、または、自身に設定されているパラメータを更新する。なお、本実施形態においては、設定指令データを送信した後、手動設定処理を終了するように構成されたものを例示したが、複数の被管理デバイスに対する設定指令を繰り返し行うことを利用するために、s128の処理で設定指令データを送信した後、s102の処理へ戻るように構成してもよい。

30

【0098】

また、s114の処理によるユーザの操作が上述した操作以外の操作である場合には(s124: NO, s126: NO)、その操作に対応する処理(他の処理)を行った後(s130)、s114の処理へ戻る。また、本手動設定処理では、設定画面におけるいずれかの画面の「キャンセル」ボタンを選択する操作が行われた際には、設定画面および一覧表示画面の表示を消去して、s102の処理へ戻るように構成されているが、本発明を理解する上では重要ではないため、ここでは省略する。

40

IPV6_Setting処理

以下に、図2におけるs122の処理であるIPV6_Setting処理の詳細な処理手順について、図5～図8に基づいて説明する。

【0099】

まず、IPV6_Settings画面を表示部17に表示させる(s202)。このIPV6_Settings画面は、図9(a)に示すように、被管理デバイスに割り当てられたIPV6に対応するIPアドレスの設定に関するデバイス設定領域610、デフ

50

オルトルートに関するルート設定領域 620、より詳細な設定を行う Advanced_Settings 画面を表示させるための Advanced_Settings ボタン 632、Hide ボタン 634 などが設けられている。

【0100】

これらのうち、デバイス設定領域 610 は、被管理デバイスに対して設定されている IP アドレス（図 2 における s110 の処理で取得された IPv6 に対応する IP アドレス；以降、「デバイス IP アドレス」という）をプルダウンメニュー形式で指定可能に一覧表示する選択欄 612、デバイス IP アドレスを追加的に設定するための追加ボタン 614、選択欄 612 から選択的に指定したデバイス IP アドレスを削除するための削除ボタン 616 などからなる。なお、選択欄 612 には、被管理デバイス側で設定されているデバイス IP アドレスのうち、最先に設定されたデバイス IP アドレスが入力された状態となっており、また、選択欄 612 に入力されたデバイス IP アドレスには、その設定時ににおける設定機能（図 2 における s110 の処理で取得された IP アドレスに対応する設定機能）を示す文字列が併せて表示された状態となっている。10

【0101】

また、ルート設定領域 620 についても、デフォルトルータの IP アドレス（図 2 における s110 の処理で取得された IPv6 に対応する IP アドレス；以降、「ルータ IP アドレス」という）をプルダウンメニュー形式で指定可能に一覧表示する選択欄 622、被管理デバイスに対してルータ IP アドレスを追加的に設定するための追加ボタン 624、選択欄 622 から選択的に指定したルータ IP アドレスを削除するための削除ボタン 626 などからなる。なお、選択欄 622 には、実際のルータ IP アドレスとして被管理デバイス側で設定されているものが入力された状態となっており、また、選択欄 622 に入力されたルータ IP アドレスには、デバイス設定領域 612 における選択欄 612 と同様、その設定時ににおける設定機能を示す文字列が併せて表示された状態となっている。20

【0102】

こうして、IPv6_Settings 画面が表示部 17 に表示された以降、ユーザは、入力部 18 により、選択欄 612、622 により選択的に IP アドレスを指定する操作、追加ボタン 614、624 を選択する操作、削除ボタン 616、626 を選択する操作、Advanced_Settings ボタン 632 を選択する操作、Hide ボタン 634 を選択する操作などを行うことができる。30

【0103】

こうして、s202 の処理により IPv6_Settings 画面が表示された後、ユーザによる操作が行われるまで待機する（s204：NO）。

その後、ユーザによる操作が行われたら（s204：YES）、その操作が選択欄 612 により選択的に IP アドレスを指定する操作であれば（s206：YES）、こうして指定された IP アドレスが選択欄 612 に入力された状態として表示した後（s208）、s204 の処理へ戻る。

【0104】

また、ここからは、上述した s204 の処理で行われたユーザの操作が、追加ボタン 614 を選択する操作である場合（s206：NO、s210：YES）の処理を図 6 に基づいて説明する。40

【0105】

まず、図 9(b) に示すような追加すべき IP アドレスの入力を促すための入力用ダイアログを表示部 17 に表示させた後（s212）、この入力用ダイアログに設けられた入力欄 65 に IP アドレスが入力され、OK ボタン 653 を選択する操作が行われるまで待機する（s214：NO）。

【0106】

この後、入力欄 651 に IP アドレスが入力され、さらに OK ボタン 653 を選択する操作が行われたら（s214：YES）、こうして入力された IP アドレスを示す文字列を読み込む（s216）。50

【0107】

次に、読み込んだ文字列の中に、設定機能を示す文字列が含まれているか否かをチェックする(s218)。上述したs212の処理で表示される入力用ダイアログでは、単にIPアドレスのみを示す文字列に続けて、以降のIPアドレスを自動設定(ステートレスまたはステートフル)により設定するか否かを示す文字列、さらには、ステートレスによる場合においてプレフィックスの取得元とすべきルータのIPアドレスを示す文字列も入力することができる。そして、このs218の処理では、IPアドレスを示す文字列の後に、ステートレスにより設定する旨の文字列(例えば、Statelessなど)やステートフルにて設定する旨の文字列(例えば、DHCP, Statefulなど)が付けられていれば、設定機能を示す文字列が含まれていると判定する。

10

【0108】

このs218の処理で、設定機能を示す文字列が含まれていると判定された場合(s218: YES)、この文字列で示される設定機能を有効なものとすべき旨を被管理デバイスに指令する(s220)。被管理デバイスのデータベース(MIB)には、ステートレスおよびステートフルによる設定それぞれを有効とするか否かを示す自動設定有効情報が登録されているため、このs220の処理では、この自動設定有効情報について、いずれかまたは両方の自動設定を有効とさせるための設定要求をSNMPに従って行う。この設定要求を受けた被管理デバイスは、後述のように、設定要求に基づく情報の更新を行い、これに応じて、自動設定が有効な状態に設定変更する。

【0109】

20

次に、s216の処理で読み込んだ文字列の中に、ルータのIPアドレスを示す文字列が含まれているか否かをチェックする(s222)。上述したように、s212の処理で表示される入力用ダイアログでは、ステートレスによる場合においてルータのIPアドレスを示す文字列をも入力することができる。そのため、このs222の処理では、ステートレスにより設定する旨の文字列の後、さらに、IPアドレスを示す文字列が付けられていれば、ルータのIPアドレスが含まれていると判定する。

【0110】

このs222の処理で、ルータのIPアドレスを示す文字列が含まれていると判定された場合(s222: YES)、このIPアドレスに基づいてルータリストを更新すべき旨を被管理デバイスに指令する(s224)。被管理デバイスのデータベースには、プリフィックスの取得元とすべきでないルータのIPアドレスがリスト(Inhibit router list: 図10参照)として登録されているため、このs224の処理では、このリストからs216の処理で読み込んだ文字列(IPアドレス)を削除すべき旨の設定要求をSNMPに従って行う。この設定要求を受けた被管理デバイスは、後述のように、設定要求に基づく情報の更新を行い、以降、リストから削除されたルータからのプリフィックスを取得するようになる。

30

【0111】

こうして、s224の処理を終えた後、または、s222の処理でルータのIPアドレスを示す文字列が含まれていないと判定された場合(s222: NO)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

40

【0112】

また、上述したs218の処理で、設定機能を示す文字列が含まれていないと判定された場合(s218: NO)、s216の処理で読み込まれたIPアドレスが有効なものであるか否かをチェックする(s226)。ここでは、s216の処理で読み込まれた文字列が、IPアドレスを示す文字列として適切な文字列であるかについて、不適切な文字が用いられていないか、適切な文字数により構成されているか、といった点からIPv6のIPアドレスとして適切か否かのチェックを行う。

【0113】

このs226の処理で有効なものではないと判定された場合には(s226: NO)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

50

一方、s 2 2 6 の処理で有効なものであると判定された場合には(s 2 2 6 : Y E S)、s 2 1 6 の処理で読み込まれた I P アドレスについて、手動で設定された(スタティックの) I P アドレスとして設定すべき旨をデバイスに指令する(s 2 2 8)。被管理デバイスのデータベースには、I P アドレスが、それぞれ設定機能と対応づけた状態で登録されているため、この s 2 2 8 の処理では、s 2 1 6 の処理で読み込まれた I P アドレスを、手動で設定された旨の情報と対応づけて登録する旨の設定要求を S N M P に従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じて手動設定としての I P アドレスが設定される。

【 0 1 1 4 】

次に、自動設定を禁止するか否かの確認メッセージを表示部 1 7 に表示させる(s 2 3 0)。ここでは、s 2 2 8 の処理で手動の設定機能により I P アドレスの設定が行われたことから、ユーザが自動の設定機能を使用しなくともよい(または、無効にしても問題ない)と考えていると推測し、図 1 1 (a)に示すように、自動設定を禁止するか否かの確認メッセージを通知するための自動設定禁止確認画面を表示部 1 7 に表示させる。この自動設定禁止確認画面には、確認メッセージだけでなく、禁止する、禁止しないを選択するための選択ボタン 7 0 2 , 7 0 4 が設けられており、この自動設定禁止確認画面が表示された後、ユーザは、入力部 1 8 により選択ボタン 7 0 2 , 7 0 4 のいずれかを選択する操作を行うことができる。

【 0 1 1 5 】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する(s 2 3 2 : N O)。

その後、ユーザによる操作が行われたら(s 2 3 2 : Y E S)、その操作が禁止しない旨の選択ボタン 7 0 4 を選択する操作であれば(s 2 3 4 : N O)、本 I P v 6 _ S e t t i n g 処理を終了し、図 2 における s 1 1 4 の処理へ戻る。

【 0 1 1 6 】

一方、ユーザによる操作が、禁止する旨の選択ボタン 7 0 2 を選択する操作であれば(s 2 3 4 : Y E S)、両方の自動設定を無効なものとすべき旨を被管理デバイスに指令する(s 2 3 6)。被管理デバイスのデータベースには、上述したように自動設定有効情報が登録されているため、この s 2 3 6 の処理では、この自動設定有効情報について、ステートフルおよびステートレスそれぞれを無効とすべき旨の設定要求を S N M P に従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じて自動設定が無効な状態に設定変更する。

【 0 1 1 7 】

そして、s 2 3 4 の処理で自動設定を禁止する旨が選択されたことから、自動設定による I P アドレスが不要になると推測して、自動設定により設定された全ての I P アドレスを削除すべき旨を被管理デバイスに指令した後(s 2 3 8)、本 I P v 6 _ S e t t i n g 処理を終了し、図 2 における s 1 1 4 の処理へ戻る。被管理デバイスのデータベースには、上述したように各 I P アドレスが設定機能を示す情報に対応づけられた状態で登録されているため、この s 2 3 8 の処理では、データベースに登録されている I P アドレスのうち、ステートレスおよびステートフルを示す情報と対応づけられた I P アドレスについて、これらすべてを削除すべき旨の設定要求を S N M P に従って指令する。この設定要求を受けた被管理デバイス側では、設定要求に基づく情報の更新が行われ、これに応じて、該当する I P アドレスの設定が解除(設定済みの I P アドレスが削除)される。

【 0 1 1 8 】

また、ここからは、上述した s 2 0 4 の処理で行われたユーザの操作が、削除ボタン 6 1 6 を選択する操作である場合(s 2 1 0 : N O , s 2 4 0 : Y E S)の処理を図 5 , 図 7 , 図 8 に基づいて説明する。

【 0 1 1 9 】

まず、削除ボタン 6 1 6 を選択する操作する操作が行われた時点で選択欄 6 1 2 に入力されている I P アドレスに対応する設定機能(図 2 における s 1 1 0 の処理で取得された

10

20

30

40

50

IPアドレスに対応する設定機能)が、ステートレスによるものであるか否かをチェックする(s242)。ここでは、s240の処理にて削除ボタン616が選択された時点で選択欄612に入力されているIPアドレスに、例えば、Statelessなどの情報、および、このIPアドレスを生成するにあたりプリフィックスを取得したルータのIPアドレスが対応づけられていれば、選択欄612に入力されているIPアドレスがステートレスによるものであると判定する。

【0120】

このs242の処理で、ステートレスによるものであると判定されたら(s242: YES)、自動設定されたものであることを確認させると共に、自動設定を禁止するか否かの確認メッセージを表示部17に表示させる(s244)。ここでは、削除しようとするIPアドレスが自動設定によるものであることから、ユーザが自動設定を無効にしてもよいと考えていると推測し、図11(b)に示すように、自動設定されたものであることを確認させると共に、自動設定を禁止するか否かの確認メッセージを通知するための自動設定禁止確認画面を表示部17に表示させる。この自動設定禁止確認画面には、確認メッセージだけでなく、自動設定を禁止する旨の禁止ボタン714、IPアドレスの削除のみを行うためのOKボタン712、および、Cancelボタン716が設けられており、この自動設定禁止確認画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行うことができる。

【0121】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する(s246: NO)。

その後、ユーザによる操作が行われたら(s246: YES)、その操作がCancelボタン716を選択する操作であれば(s248: NO, s250: NO)、本IPV6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0122】

また、ユーザによる操作がOKボタン712を選択する操作であれば(s248: NO, s250: YES)、被管理デバイス側において自動設定が有効となっているか否かをチェックする(s252)。ここでは、図2におけるs110の処理で取得された設定情報のうち、自動設定が有効であるか無効であるかを示す自動設定有効情報に基づいてチェックが行われる。

【0123】

このs252の処理で自動設定が有効になっていないと判定されたら(s252: NO)、選択欄612, 622に入力されているIPアドレスがリンクローカルアドレス以外のIPアドレスである場合(s254: YES)、かつ、選択欄612に入力されているIPアドレス以外のIPアドレスが被管理デバイス側に設定されている(つまり、削除しようとしているIPアドレスを除く他のIPアドレスも設定されている)場合(s256: YES)、削除ボタン616が選択された時点で選択欄612に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令した後(s258)、本IPV6_Setting処理を終了し、図2におけるs114の処理へ戻る。ここでは、まず、s254の処理でリンクローカルアドレスであるか否かをチェックしているが、このリンクローカルアドレスがIPV6によるデータ通信を実現するために必須のIPアドレスであって、これを削除することにより、IPV6によるデータ通信が正常に実現されなくなる虞がある。また、s256の処理においては、s110の処理で取得された情報のうち、被管理デバイス自身のIPアドレスとして設定されているIPアドレスが、削除しようとしているIPアドレス以外に存在すれば、設定されていると判定される。このチェックはリンクローカルアドレスか否かのチェックと同様の趣旨による。このため、リンクローカルアドレス以外のIPアドレスであり、かつ、他のIPアドレスも設定されている場合にのみ、s258の処理で該当するIPアドレスを削除することとしている。なお、このリンクローカルアドレスであるか否かのチェックについては、デバイス設定領域610の入力欄612に対してのみとしてもよい。

10

20

30

40

50

【0124】

また、s258の処理では、s110の処理で取得されたIPアドレスのうち、削除ボタン616が選択された時点で選択欄612に入力されているIPアドレスについて、これらを削除すべき旨の設定要求をSNMPに従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じて、該当するIPアドレスの設定を解除（設定済みのIPアドレスを削除）する。

【0125】

また、選択欄612, 622に入力されているIPアドレスがリンクローカルアドレスである場合（s254: NO）、または、選択欄612, 622に入力されているIPアドレス以外のIPアドレスが設定デバイス側に設定されていない（つまり、削除しようとしているIPアドレスのみしか設定されていない）場合は（s256: NO）、該当するIPアドレスを削除することにより正常なデータ通信が行えなくなる虞がある旨の確認メッセージを表示部17に表示させる（s260）。ここでは、図11(c)に示すように、IPアドレスを削除することにより正常なデータ通信が行えなくなる虞がある旨の確認メッセージを通知するための不通確認画面を表示部17に表示させる。この不通確認画面には、確認メッセージだけでなく、IPアドレスの削除を強行するためのOKボタン722、および、Cancelボタン724が設けられており、この不通確認画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行うことができる。

【0126】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する（s262: NO）。

その後、ユーザによる操作が行われたら（s262: YES）、その操作がOKボタン722を選択する操作であれば（s264: YES）、IPv6によるデータ通信を停止すべき旨を被管理デバイスに指令した後（s266）、s258の処理へ移行する。被管理デバイスのデータベースには、IPv6によるデータ通信を機能させるか停止するかを示すIPv6機能停止情報が登録されているため、このs266の処理では、この機能停止情報について停止を示す内容とすべき旨の設定要求をSNMPに従って指令する。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じてIPv6によるデータ通信が停止される。

【0127】

また、s262の処理で行われたユーザの操作がCancelボタン724を選択する操作であれば（s264: NO）、s258, s266の処理を行うことなく、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0128】

また、上述したs252の処理で自動設定が有効となっていると判定された場合については（s252: YES）、上述したs254, s256の処理を行うことなく、s258の処理へ移行し、IPアドレスの削除を指令する。

【0129】

また、上述したs246の処理におけるユーザの操作が自動設定禁止ボタン714を選択する操作である場合（s248: YES）、自動設定のうちいずれの設定機能を禁止にするかの選択をユーザに促す（s270）。ここでは、図12(a)に示すように、いずれの設定機能を禁止するかを選択させるための禁止選択画面を表示部17に表示させる。この禁止選択画面には、削除しようとするIPアドレスを生成した際のプリフィックスでの設定（の取得元ルータに基づく設定）を禁止にするための第1禁止ボタン732、ステートレスでの設定を全て禁止するための第2禁止ボタン734、ステートレスだけでなくステートフルでの設定も（全ての自動設定を）禁止するための第3禁止ボタン736、Cancelボタン738などが設けられており、この禁止選択画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行うことができる。

【0130】

10

20

30

40

50

こうして、禁止選択画面を表示させた後、ユーザによる操作が行われるまで待機する（s 272 : N O）。

その後、ユーザによる操作が行われたら（s 272 : Y E S）、その操作が第3禁止ボタン736を選択する操作であれば（s 274 : Y E S）、まず、ステートフルでの設定を無効なものとすべき旨を被管理デバイスに指令する（s 276）。被管理デバイスのデータベースには、ステートレスおよびステートフルによる設定それぞれを有効とするか否かを示す自動設定有効情報が登録されているため、このs 276の処理では、この自動設定有効情報のうち、ステートフルによる設定（D H C P 設定）を無効なものとすべき旨の設定要求をS N M P に従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じてステートフルによる設定を無効な状態に設定変更する。10

【0131】

次に、ステートフルにより設定された全てのI P アドレスを削除すべき旨を被管理デバイスに指令する（s 278）。被管理デバイスのデータベースには、上述したように各I P アドレスが設定機能を示す情報に対応づけられたりストとして登録されているため、このs 278の処理では、データベースに登録されているI P アドレスのうち、ステートフルに対応するI P アドレスについて、これらすべてを削除すべき旨の設定要求をS N M P に従って指令する。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じて、該当するI P アドレスの設定を解除（設定済みのI P アドレスを削除）する。20

【0132】

次に、ステートレスでの設定を無効なものとすべき旨を被管理デバイスに指令する（s 280）。ここでは、s 276の処理と同様、自動設定有効情報のうち、ステートレスによる設定を無効なものとすべき旨の設定要求をS N M P に従って行う。

【0133】

そして、ステートレスにより設定された全てのI P アドレスを削除すべき旨を被管理デバイスに指令した後（s 282）、本I P v 6 _ S e t t i n g 処理を終了し、図2におけるs 114の処理へ戻る。このs 282の処理では、s 278の処理と同様、データベースに登録されているI P アドレスのうち、ステートレスに対応するI P アドレスについて、これらすべてを削除すべき旨の設定要求をS N M P に従って行う。30

【0134】

また、s 272の処理により行われたユーザの操作が第2禁止ボタン734を選択する操作であれば（s 274 : N O , s 284 : Y E S）、上述したs 280の処理へ移行し、ステートレスによる設定の無効化、および、ステートレスにより設定されたI P アドレスの削除を行い、本I P v 6 _ S e t t i n g 処理を終了し、図2におけるs 114の処理へ戻る。

【0135】

また、s 272の処理により行われたユーザの操作が第1禁止ボタン732を選択する操作であれば（s 284 : N O , s 286 : Y E S）、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているルータのI P アドレスに基づいてルータリストを更新すべき旨を被管理デバイスに指令する（s 288）。被管理デバイスのデータベースには、上述したように、プリフィックスの取得元とすべきでないルータのI P アドレスがリスト（図10参照）として登録されているため、このs 288の処理では、上記ルータのI P アドレスをリストに登録すべき旨の設定要求をS N M P に従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、以降、こうして更新されたリストに登録されているルータからのプリフィックスが取得されなくなる。40

【0136】

このs 288の処理を終えた後は、上述したs 252の処理へ移行し、以降、s 258までの処理を終えたら、本I P v 6 _ S e t t i n g 処理を終了し、図2におけるs 1150

4の処理へ戻る。

【0137】

なお、s272の処理により行われたユーザの操作がCancelボタン738を選択する操作であれば(s286: NO)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0138】

また、図5に戻り、上述したs242の処理で、ステートレスによるものではないと判定されたら(s242: NO)、ステートフルによるものであるか否かをチェックする(s292)。ここでは、s240の処理にて削除ボタン616が選択された時点で選択欄612に入力されているIPアドレスに、ステートフルにより設定する旨の情報(例えば、DHCP, Statefulなど)が対応づけられていれば、選択欄612に入力されているIPアドレスがステートフルによるものであると判定する。10

【0139】

このs292の処理で、ステートフルによるものであると判定されたら(s292: YES)、自動設定されたものであることを確認させると共に、自動設定を禁止するか否かの選択をユーザに促すための確認メッセージを表示部17に表示させる(s294)。ここでは、削除しようとするIPアドレスが自動設定によるものであることから、ユーザが自動設定を無効にしてもよいと考えていると推測し、図12(b)に示すように、自動設定されたものであることを確認させると共に、ステートフルによる設定(DHCP設定)を禁止するか否かの確認メッセージを通知するための自動設定禁止確認画面を表示部17に表示させる。この自動設定禁止確認画面には、確認メッセージだけでなく、ステートフルによる設定を禁止(Disable DHCP)する旨の禁止ボタン742、IPアドレスの削除のみを行うためのOKボタン744、および、Cancelボタン746が設けられており、この自動設定禁止確認画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行うことができる。20

【0140】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する(s296: NO)。

その後、ユーザによる操作が行われたら(s296: YES)、その操作が禁止ボタン742を選択する操作であれば(s298: YES)、上述したs276, s278の処理と同様に、ステートフルでの設定を無効なものとすべき旨を被管理デバイスに指令し(s300)、ステートフルにより設定された全てのIPアドレスを削除すべき旨を被管理デバイスに指令した後(s302)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。30

【0141】

また、s296の処理でユーザにより行われた操作がOKボタン744を選択する操作であれば(s298: NO, s304: YES)、上述したs258の処理と同様、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令した後(s306)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。40

【0142】

また、s296の処理でユーザにより行われた操作がCancelボタン746を選択する操作であれば(s304: NO)、s306の処理を行うことなく、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0143】

また、図5に戻り、上述したs292の処理で、ステートフルによるものではないと判定されたら(s292: NO)、手動設定(スタティック)によるものであるか否かをチェックする(s312)。ここでは、s240の処理にて削除ボタン616, 626が選択された時点で選択欄612に入力されているIPアドレスを示す文字列の後に、何も付けられていなければ(または、ステートレス、ステートフルを示す以外の文字列が付けら50

れていれば）、選択欄 612 に入力されている IP アドレスが手動設定によるものであると判定する。

【0144】

この s312 の処理で、手動設定によるものでないと判定されたら (s312: NO) 、例えば、リンクローカルアドレスであった場合、図 7 に示す s252 の処理へ移行する (s252 以降の処理は上述したのでここでは省略する)。

【0145】

また、s312 の処理で、手動設定によるものであると判定されたら (s312: YES) 、手動設定されたものであることを確認させると共に、自動設定を有効にするか否かの選択を促すための確認メッセージを表示部 17 に表示させる (s314)。ここでは、削除しようとする IP アドレスが手動設定によるものであることから、ユーザが自動設定を有効にしてもよいと考えていると推測し、図 12 (c) に示すように、手動設定されたものであることを確認させると共に、自動設定を有効にするか否かを促すための自動設定有効確認画面を表示部 17 に表示させる。この自動設定有効確認画面には、確認メッセージだけでなく、自動設定を有効にする旨の有効ボタン 752, IP アドレスの削除のみを行うための OK ボタン 754, および, Cancel ボタン 756 が設けられており、この自動設定有効確認画面が表示された後、ユーザは、入力部 18 により各ボタンのいずれかを選択する操作を行うことができる。

【0146】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する (s316: NO)。

その後、ユーザによる操作が行われたら (s316: YES) 、その操作が有効ボタン 752 を選択する操作であれば (s318: YES) 、ステートフルによる設定を有効なものとすべき旨を被管理デバイスに指令し (s320) 、続いて、ステートレスによる設定を有効なものとすべき旨を被管理デバイスに指令する (s322)。被管理デバイスのデータベースには、上述したように、ステートレスおよびステートフルによる設定それぞれを有効とするか否かを示す自動設定有効情報が登録されているため、この s320, s322 の処理では、この自動設定有効情報のうち、ステートフルによる設定 (DHCP 設定) を有効なものとすべき旨の設定要求を SNMP に従って行うと共に、ステートレスによる設定を有効なものとすべき旨の設定要求を SNMP に従って行う。これら設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じて自動設定が有効な状態に設定変更する。

【0147】

そして、上述した s258 の処理と同様、削除ボタン 616 が選択された時点で選択欄 612 に入力されている IP アドレスを削除すべき旨を被管理デバイスに指令した後 (s324) 、本 IPv6_Setting 処理を終了し、図 2 における s114 の処理へ戻る。

【0148】

また、上述した s316 の処理により行われたユーザの操作が、OK ボタン 754 を選択する操作であれば (s318: NO, s326: YES) 、s324 の処理へ移行し、IP アドレスの削除を行った後、本 IPv6_Setting 処理を終了し、図 2 における s114 の処理へ戻る。

【0149】

そして、上述した s316 の処理により行われたユーザの操作が、Cancel ボタン 756 を選択する操作であれば (s326: NO) 、s324 の処理へ移行することなく、本 IPv6_Setting 処理を終了し、図 2 における s114 の処理へ戻る。

【0150】

また、s296 の処理でユーザにより行われた操作が Cancel ボタン 746 を選択する操作であれば (s304: NO) 、s306 の処理を行うことなく、本 IPv6_Setting 処理を終了し、図 2 における s114 の処理へ戻る。

10

20

30

40

50

【0151】

また、ここからは、上述した s204 の処理で行われたユーザの操作が、「Advanced_Settings」ボタン 632（図9（a）参照）を選択する操作である場合（s240：NO, s330：YES）の処理を図5に戻って説明する。

【0152】

まず、Advanced_Settings 画面を表示部 17 に表示させる（s332）。この Advanced_Settings 画面は、図13に示すように、ルータから送信されるプレフィックスを含む情報（RA：Router Advertisement）を無視（Ignore outer advertisement）するためのチェックボックス 762, ステートフルによる設定を無効（Disable DHCPv6）にするためのチェックボックス 764, ステートレスによる設定を無効（Ignore stateless address）にするためのチェックボックス 766, 正常な IPv6 の動作を損なう設定は無視（Always enable IPv6）するためのチェックボックス 770, 自動設定パラメータの変更を許可しない（Do not allow modifying auto-configuration parameter）ようにするためのチェックボックス 772, OK ボタン 768 などが設けられている。こうして、Advanced_Settings 画面が表示された後、ユーザは、入力部 18 により、各チェックボックスを選択（チェック）する操作, OK ボタン 768 を選択する操作などを行うことができる。10

【0153】

こうして、Advanced_Settings 画面が表示された後、ユーザによる操作が行われるまで待機する（s334：NO）。20

その後、ユーザによる操作が行われたら（s334：YES）、その操作がチェックボックスを選択する操作であれば（s336：YES）、そのチェックボックスが選択された状態（既に選択されたものであれば、選択されていない状態）とした後（s338）、s334 の処理へ戻る。

【0154】

そして、s334 の処理で行われたユーザの操作が、OK ボタン 768 を選択する操作であれば（s336：NO, s339：YES）、この時点でのチェックボックスの選択状況に基づく設定変更を被管理デバイスに指令した後（s340）、s204 の処理へ戻る。被管理デバイスのデータベースには、ルータから送信されるプリフィックスを含む情報（RA：Router Advertisement）を無視するか否かを示す RA 無視情報、自動設定を有効とするか無効とするかを示す自動設定有効情報が登録されているため、この s340 の処理では、これらの情報をチェックボックスの選択状況に応じた内容に変更すべき旨の設定要求を SNMP に従って行う。この設定要求を受けた被管理デバイスは、設定要求に基づく情報の更新を行い、これに応じてチェックボックスの選択状況に基づく設定変更を行う。なお、s334 の処理で行われたユーザの操作が、上述したいずれの操作でもなければ（s339：NO）、その操作に対応する処理（その他の処理）を行った後（s342）、s334 の処理へ戻る。30

【0155】

また、上述した s204 の処理で行われたユーザの操作が、Hide ボタン 634 を選択する操作である場合（s330：NO）、本 IPv6_Setting 処理を終了し、図2における s114 の処理へ戻る。40

プリンタ 20 による受信データ処理

以下に、プリンタ 20（の CPU 21）により実行される受信データ処理の処理手順を図14（a）に基づいて説明する。なお、この受信データ処理は、ネットワーク I/F 26 を介してデータが受信される毎に開始される。

【0156】

まず、受信したデータが SNMP に従った設定要求であるか否かをチェックし（s602）、SNMP に従った設定要求であれば（s602：YES）、それに従った処理（SNMP 処理）を行った後（s604）、本受信データ処理を終了する。この s604 の処理では、設定要求が、例えば、自動設定有効情報を有効または無効とすべきものであれば50

、自動設定有効情報を指令通りに更新する。また、ルータリストを更新（登録）すべきものであれば、該当するIPアドレスのリストへの登録を行う。また、IPアドレスを登録すべきものであれば、該当するIPアドレスの登録を行う。また、データベースに登録されたIPアドレスを削除すべきものであれば、該当するIPアドレスの削除を行う。また、IPv6機能停止情報を停止する、または、機能させるべきものであれば、IPv6機能停止情報を指令通りに更新する。また、これ以外に、SNMPに従った通常の処理についてもここで行うこととなる。

【0157】

また、受信したデータがSNMPに従った設定要求でなく（s602: NO）、ルータから送信されるRAである場合（s606: YES）、それに従った処理（RA処理）を行った後（s608）、本受信データ処理を終了する。10

【0158】

このRA処理では、図14（b）に示すように、RAを送信してきたルータのIPアドレスをデータベース中のリストから検索し（s612）、データベース中のリストから検出された場合（s614: YES）、受信したデータを破棄した後（s616）、受信データ処理と共に終了する。

【0159】

また、s614の処理で、データベース中のリストから検出されなかった場合（s614: NO）、さらに、データベース中のRA無視情報がRAを無視することを示す内容となつていなければ（s618: YES）、このRAに含まれるプリフィックスに基づくIPアドレスの生成および設定（プリフィックス処理）を行った後で（s620）、この処理以外のRAに基づく通常の処理を行って（s622）、受信データ処理と共に終了する。一方、データベース中のRA無視情報がRAを無視することを示す内容となつていれば（s618: NO）、プリフィックス処理を行うことなく、RAに基づく通常の処理を行って（s622）、受信処理と共に終了する。20

【0160】

そして、受信データ処理に戻り、受信したデータがRAでない場合には（s606: NO）、そのデータに応じた通常の処理を行った後（s610）、本受信データ処理を終了する。

ネットワーク印刷処理

以下に、上述したネットワーク印刷機能を有するプリンタ20により実行されるネットワーク印刷処理の処理手順を図26に基づいて説明する。なお、このネットワーク印刷処理は、ネットワーク印刷機能を有するプリンタ20が起動された以降、繰り返し実行される処理である。30

【0161】

まず、POPサーバへのポーリング周期が経過するまで待機する（s902: NO）。本実施形態において、プリンタ20は、自身宛の電子メールが届いているか否かを隨時チェックするために、POPサーバ（本実施形態においては、メールサーバ40）へ一定周期でアクセスするよう構成されており、このs902の処理では、この周期（ポーリング周期）が経過するまで待機する。40

【0162】

このs902の処理でポーリング周期が経過したら（s902: YES）、プリンタ20側において、POPサーバのIPアドレスが自身のIPモード（IPv4またはIPv6）に対応する形式の文字列で登録されているか否かをチェックする（s904）。

【0163】

このs904の処理でPOPサーバのIPアドレスが登録されていなければ、すなわち、IPアドレスではなくPOPサーバのサーバ名が登録されていた場合は（s904: NO）、POPサーバのサーバ名を元にDNSサーバ50からPOPサーバのIPアドレスを取得した後（s906）、次の処理（s908）へ移行する一方、POPサーバのIPアドレスが登録されていれば（s904: YES）、s406の処理を行うことなく次の50

処理 (s 9 0 8) へ移行する。

【 0 1 6 4 】

次に、登録されている I P アドレス、または、s 9 0 6 の処理で取得した I P アドレスで示される P O P サーバがプリンタ 2 0 自身と同一のネットワークに所属しているものであるか否かを、I P アドレスを元にえっとワークアドレスを比較することでチェックする (s 9 0 8) 。

【 0 1 6 5 】

この s 9 0 8 の処理で、P O P サーバがプリンタ 2 0 自身と同一のネットワークに所属しているものであれば (s 9 0 8 : Y E S) 、この P O P サーバに対して直接アクセスを行う一方 (s 9 1 0) 、P O P サーバがプリンタ 2 0 自身と同一のネットワークに所属しているものでなければ (s 9 0 8 : N O) 、ゲートウェイ 3 0 を介して P O P サーバに対してアクセスを行う (s 9 1 2) 。 10

【 0 1 6 6 】

こうして、P O P サーバへのアクセスを行った後、所定のタイムアウト時間を経過するまでの間で P O P サーバとの接続が完了するまで待機し (s 9 1 4 : N O , s 9 1 6 : N O) 、タイムアウト時間が経過したら (s 9 1 6 : Y E S) 、s 9 0 2 の処理へ戻る一方、タイムアウト時間が経過するまでの間に P O P サーバとの接続が完了したら (s 9 1 4 : Y E S) 、プリンタ 2 0 自身宛の電子メールが P O P サーバに受信されているかをチェックする (s 9 1 8) 。

【 0 1 6 7 】

この s 9 1 8 の処理で、プリンタ 2 0 自身宛の電子メールが P O P サーバに受信されていなければ (s 9 1 8 : N O) 、s 9 0 2 の処理へ戻る一方、プリンタ 2 0 自身宛の電子メールが P O P サーバに受信されていれば (s 9 1 8 : Y E S) 、この P O P サーバから自身宛の電子メールを受信する (s 9 2 0) 。 20

【 0 1 6 8 】

そして、こうして受信した電子メールに含まれる印刷データを抽出し (s 9 2 2) 、この印刷データで示される画像の印刷部 2 8 による印刷を行った後 (s 9 2 4) 、s 9 0 2 の処理へ戻る。

【 0 1 6 9 】

[第 1 実施形態の効果]

上述した P C 1 0 _ 1 であれば、図 5 における s 2 1 0 , s 2 4 0 の処理で、選択欄に入力された I P アドレスが追加または削除すべき I P アドレスとしてユーザに指定された際、図 6 における s 2 2 6 または図 5 における s 2 4 2 以降の処理で、この I P アドレスを設定すべき設定機能または設定したときの設定機能に基づき、この I P アドレスと共に変更すべき他のパラメータを推測し、その存在を表示部 1 7 に表示することにより報知できる。これにより、ユーザが変更すべきものとして指定した I P アドレスと、この I P アドレスと密接な関係にある他のパラメータとを連携して変更すべきことを報知することができる。さらに、ユーザは、これら処理による報知内容に沿って選択操作を行うことによって、その報知内容に従って他のパラメータを変更することができる。 30

【 0 1 7 0 】

また、図 7 における s 2 4 4 , 図 8 (a) における s 2 9 4 の処理では、ユーザの意図を推測して、指定された I P アドレスを設定したときにおける自動設定 (ステートレスまたはステートフル) を禁止するか否か、つまり自動設定を禁止 (無効) にすべき旨を報知することができる。また、図 8 (a) における s 3 1 4 の処理では、ユーザの意図を推測して、指定された I P アドレスを設定したときにおける手動設定以外の設定機能を有効にするか否か、つまり自動設定を有効にすべき旨を報知することができる。 40

【 0 1 7 1 】

また、図 5 における s 2 4 0 の処理で選択欄に入力された I P アドレスが削除すべき I P アドレスとしてユーザに指定された際、この I P アドレスがステートレスによるものである場合には、図 7 における s 2 4 4 の処理で、同種の設定機能であるステートフルにつ

いても併せて禁止（無効）にするか否かを報知することができる。

【0172】

また、図5におけるs210, s240の処理で、選択欄に入力されたIPアドレスが削除すべきIPアドレスとしてユーザに指定された際、このIPアドレスが設定されたときにおける設定機能がステートレスによるものである場合には、図7におけるs270の処理で、このルータからのプリフィックスを取得しないようにすべき旨を報知することができる。そして、ユーザが、その旨を選択した場合には、同図s288の処理で、プリンタ20側のルータリストを更新させることができ、これにより、以降プリンタ20側において上述したルータからのプリフィックスを取得しないようにすることができる。

【0173】

また、図6におけるs226の処理では、追加すべきものとして指定されたIPアドレスが有効（適切）なものであるか否かを判定し、有効である場合にのみ、IPアドレスの設定など同図s228以降の処理を行うことができる。そのため、ユーザが間違ってIPアドレスとしては不適切な文字列を選択欄に入力してしまった場合であっても、そのような不適切な文字列に基づく不適切な設定がプリンタ20側でなされてしまう虞がない。

【0174】

また、図7におけるs258の処理によるIPアドレスの削除は、同図s254, s256の処理にて「NO」と判定された場合、同図s266の処理によるIPv6によるデータ通信の停止を伴わなければ行われない。この場合、同図s262の処理によるユーザの確認操作を受けて、同図s258の処理へ移行することになるが、自動設定により設定された他のIPアドレスが設定されていれば、同図s252の処理で「YES」と判定され、直接s258の処理へ移行するため、この場合はユーザの確認操作を求める事はない。つまり、他のIPアドレスが設定されている状態であれば、ユーザの確認操作を求ることはなく、指定されたIPアドレスを削除することのみを行うため、これにより、必要に応じてユーザの確認操作を行わせることができる。

【0175】

また、図7におけるs260の処理では、指定されたIPアドレスがIPv6によるデータ通信を実現するために必須のIPアドレス（リンクローカルアドレス）である場合、または、指定された以外のIPアドレスが設定されていない場合に、ユーザの確認操作を受けてIPv6に従ったデータ通信を停止すべき旨を報知することができる。

【0176】

また、被管理デバイスに各種情報を登録するためのデータベースが備えられ、PC10は、このデータベースに登録された情報を問い合わせることにより、被管理デバイスの設定状況を確認できるように構成されている。このように、被管理デバイスの設定状況を示す情報については、被管理デバイスにて記憶されていることから、この情報をPC10側で記憶するための記憶領域を確保しておく必要がない。

[第2実施形態]

本実施形態においては、IPv6_Setting処理のうち、s242の処理とs244の処理との間、および、s292の処理とs294の処理との間に、以下に示すような処理が行われるように構成されたものであり、それ以外については、第1実施形態と同様であるため、この相違点についてのみ図15, 図16に基づいて説明する。すなわち、図7にs402の処理を、図8(a)にs404の処理をそれぞれ追加したフローとして図15, 図16を示している。

【0177】

まず、s242の処理で「YES」と判定された場合に、図15に示すように、ステートレスによる設定が禁止されているか否かをチェックする(s402)。ここでは、図2におけるs110の処理で取得した情報のうち、自動設定有効情報をチェックし、ステートレスによる設定を無効にすべき旨となつていれば、ステートレスによる設定が禁止されていると判定する。なお、この情報は、図5におけるs340の処理において変更される情報である。

10

20

30

40

50

【0178】

この s 4 0 2 の処理で禁止されていないと判定されたら (s 4 0 2 : N O) 、 s 2 4 4 の処理へ移行する一方、禁止されていると判定されたら (s 4 0 2 : Y E S) 、 s 2 5 8 の処理へ移行する。

【0179】

また、 s 2 9 2 の処理で「 Y E S 」と判定された場合に、図 1 6 に示すように、ステートフルによる設定が禁止されているか否かをチェックする (s 4 0 4) 。ここでは、図 2 における s 1 1 0 の処理で取得した情報のうち、自動設定有効情報をチェックし、ステートフルによる設定を無効にすべき旨となっていれば、ステートフルによる設定が禁止されていると判定する。なお、この情報についても、図 5 における s 3 4 0 の処理において変更される情報である。10

【0180】

この s 4 0 4 の処理で禁止されていないと判定されたら (s 4 0 4 : N O) 、 s 2 9 4 の処理へ移行する一方、禁止されていると判定されたら (s 4 0 4 : Y E S) 、 s 3 0 6 の処理へ移行する。

[第2実施形態の効果]

このような P C 1 0 においては、第1実施形態と同様の構成により得られる作用、効果の他に、以下に示すような作用、効果を得ることができる。

【0181】

例えば、図 1 5 、図 1 6 における s 4 0 2 、 s 4 0 4 の処理でステートレス、ステートフルによる設定が無効となつていれば、以降の処理によるユーザの選択操作を行わせることなく、指定された I P アドレスを削除することとなる。これら処理による設定が禁止となっているか否かの判定は、図 5 における s 3 3 2 ~ s 3 4 0 の処理にてユーザの操作を受けて変更した情報に基づいて行われるため、ユーザは、この処理にて任意にステートレス、ステートフルによる設定を禁止（無効）にすることを選択しておけば、 s 2 4 4 ~ s 2 6 6 、 s 2 9 4 ~ s 3 0 4 の処理にてパラメータを変更させないようにすることができます。20

[第3実施形態]

本実施形態においては、 I P v 6 _ S e t t i n g 処理のうち、 s 2 4 2 の処理と s 2 4 4 の処理との間、および、 s 2 9 2 の処理と s 2 9 4 の処理との間に、以下に示すような処理が行われるように構成されたものであり、それ以外については、第1実施形態と同様であるため、この相違点についてのみ図 1 7 、図 1 8 に基づいて説明する。すなわち、図 7 に s 4 1 2 の処理を、図 8 (a) に s 4 1 4 の処理をそれぞれ追加したフローとして図 1 7 、図 1 8 を示している。30

【0182】

まず、 s 2 4 2 の処理で「 Y E S 」と判定された場合、図 1 7 に示すように、選択欄 6 1 2 , 6 2 2 に入力されている I P アドレス以外に、ステートレスにより設定された他の I P アドレスが設定デバイス側に設定されているか否かをチェックする (s 4 1 2) 。ここでは、 s 1 1 0 の処理で取得された情報のうち、被管理デバイス自身の I P アドレスとして設定されている I P アドレスであつて、ステートレスを示す情報が対応づけられた I P アドレスが、削除しようとしている I P アドレス以外に存在すれば、設定されていると判定される。40

【0183】

この s 4 1 2 の処理で設定されていないと判定されたら (s 4 1 2 : N O) 、 s 2 4 4 の処理へ移行する一方、設定されていると判定されたら (s 4 1 2 : Y E S) 、 s 2 5 8 の処理へ移行する。

【0184】

また、 s 2 9 2 の処理で「 Y E S 」と判定された場合、図 1 7 に示すように、選択欄 6 1 2 , 6 2 2 に入力されている I P アドレス以外に、ステートフルにより設定された他の I P アドレスが設定デバイス側に設定されているか否かをチェックする (s 4 1 4) 。こ50

こでは、`s110`の処理で取得された情報のうち、被管理デバイス自身のIPアドレスとして設定されているIPアドレスであって、ステートフルを示す情報が対応づけられたIPアドレスが、削除しようとしているIPアドレス以外に存在すれば、設定されていると判定される。

【0185】

この`s414`の処理で設定されていないと判定されたら(`s414: NO`)、`s294`の処理へ移行する一方、設定されていると判定されたら(`s414: YES`)、`s306`の処理へ移行する。

[第3実施形態の効果]

このようなPC10においては、第1実施形態と同様の構成により得られる作用、効果の他に、以下に示すような作用、効果を得ることができる。10

【0186】

例えば、図17、図18における`s412`、`s414`の処理でステートレス、ステートフルにより他のIPアドレスが設定されていれば、以降の処理によるユーザの選択操作を行わせることなく、指定されたIPアドレスを削除することとなる。つまり、同一の設定機能により他のIPアドレスが既に設定されている状態であれば、以降の処理によりユーザの選択を受けて変更することとなる設定内容は、この時点で変更すべき設定内容となっている可能性が高いため、この場合、ユーザによる選択を行わせることなく、以降の処理を行ったとしても問題はない。よって、このように、既に変更すべき設定内容になつていて推定される場合に、ユーザによる選択を行わせないようにすることで、ユーザによる無用な操作を行わせないようにすることができる。20

[変形例]

以上、本発明の実施の形態について説明したが、本発明は、上記実施形態に何ら限定されることはなく、本発明の技術的範囲に属する限り種々の形態をとり得ることはいうまでもない。

【0187】

例えば、上記実施形態においては、PC10、プリンタ20を本発明におけるデバイスとした構成を例示したが、これら以外のデバイスを採用してもよい。例えば、スキャナ、ネットワークカメラ、ファクシミリ、コピー機、プロジェクタ、ソーディングマシン、ネットワーク電話、オーディオ・ビジュアル機器、ネットワークストレージなど、ネットワークに接続し、その機能を発揮する機器であれば何でもよく、それぞれの機器がもつ機能を統合した複合機でもよい。30

【0188】

また、上記実施形態においては、PC10がプリンタ20に対してリモートセットアップを行うことを前提に説明したが、PC10が自身に対して設定を行うように構成することも当然可能である。また、プリンタ20が自身のユーザI/F27経由で設定を行うように構成してもよい。

【0189】

また、上記実施形態のIPv6_Setting処理では、各自設定のための操作が行われた際にパラメータの設定が被管理デバイスに対して指令されるように構成されたものを例示した。しかし、IPv6_Setting処理において、各自設定のための操作が行われた際、これらの操作内容、つまりユーザに指定されたパラメータを記憶しておき、図2における`s128`の処理において、まとめて設定を指令するように構成してもよい。40

【0190】

また、上記実施形態においては、図5における`s240`の処理で選択欄に入力されたIPアドレスが削除すべきIPアドレスとしてユーザに指定された際、このIPアドレスがステートレスによるものである場合にのみ、図7における`s244`の処理で、同種の設定方法であるステートフルについても併せて禁止(無効)にするか否かを報知するように構成されたものを例示した。しかし、指定されたIPアドレスがステートフルによる場合においても、同様に、同種の設定方法であるステートレスについても併せて禁止にするか否50

かを報知するように構成することができる。この場合、例えば、図 8 における s 2 9 4 ~ s 3 0 6 の処理の替わりに、図 7 における s 2 4 4 ~ s 2 5 8 の処理と同様の処理が行われるように構成する、といったことが考えられる。

【0191】

また、上記実施形態において、図 7 における s 2 7 0 の処理では、特定のルータからのプリフィックスを取得しないようにすべき旨を、自動設定の一部を無効にすることとして報知するように構成されたものを例示した。しかし、この「自動設定の一部を無効にすること」としては、他の事項を採用してもよい。

【0192】

また、上記実施形態においては、図 5 における s 2 1 0 の処理で選択欄に入力された IP アドレスが追加すべき IP アドレスとしてユーザに指定された際、図 6 における s 2 2 0 の処理にて、この IP アドレスを設定すべき（IP アドレスに付加された文字列で示される）設定機能だけでなく、両方の自動設定を有効なものとするように構成されたものを例示した。しかし、この 2 2 0 の処理では、この IP アドレスを設定すべき設定機能についてのみ有効なものとするように構成してもよい。

10

【0193】

また、上記実施形態においては、図 5 における s 2 1 0 の処理で選択欄に入力された IP アドレスが追加すべき IP アドレスとしてユーザに指定された際、直ちに、図 6 における s 2 2 0 の処理にて、自動設定を有効なものとするように構成されたものを例示した。しかし、同図 s 2 1 8 の処理で設定機能を含むと判定した場合に、この設定機能と同種の設定機能についても有効にすべきものとして推定して、その旨を報知すると共に、ユーザの確認操作を受けてから、同図 s 2 2 0 の処理へ移行するように構成してもよい。

20

【0194】

このように構成すれば、ユーザが追加すべきものとして IP アドレスおよび設定機能を指定した際、こうして指定された設定機能と同種の設定機能についても有効にすべき旨を報知することができる。

【0195】

また、上記実施形態においては、図 5 における s 2 1 0 , s 2 4 0 の処理で、選択欄に入力された IP アドレスが削除すべき IP アドレスとしてユーザに指定された際、この IP アドレスが設定されたときにおける設定機能が、ルータからプリフィックスを取得して IP アドレスを生成するステートレスによるものであって、そのルータの IP アドレスについても指定されている場合に、図 6 における s 2 2 4 の処理により、プリンタ 2 0 側のルータリストを更新させるように構成されたものを例示した。しかし、ルータの IP アドレスについても指定されている場合、このルータからのプリフィックスを取得するようすべき旨を報知し、ユーザの確認操作を受けた後で、初めて同図 s 2 2 4 の処理へ移行するように構成してもよい。

30

【0196】

このように構成すれば、ユーザが追加すべきものとして IP アドレスおよび設定機能（ルータの IP アドレス含む）を指定した際、こうして指定された IP アドレス設定したときにおける設定機能がステートレスであれば、この設定機能と共に指定されたルータからのプリフィックスの取得を有効なものとすべきものを報知することができる。

40

【0197】

また、上記実施形態においては、図 6 における s 2 2 6 の処理で、ユーザに指定された IP アドレスが有効なものであるか否かについて判断しているが、このような判断は、他にユーザによる IP アドレスの入力が伴う箇所（例えば、s 2 2 2 と s 2 2 4 の間など）において同様に行われるよう構成してもよい。

【0198】

また、上記実施形態においては、図 7 における s 2 6 6 の処理で、IP v 6 によるデータ通信を停止するための条件（停止条件）として、削除すべき IP アドレスとして指定されたものが IP v 6 によるデータ通信を実現するために必須の IP アドレス（リンクロー

50

カルアドレス)であること、また、指定された以外のIPアドレスが設定されていないこと、を採用した構成を例示した。しかし、この「停止条件」としては、他の事項を採用してもよい。

【0199】

また、上記実施形態においては、被管理デバイス側に各種情報を記憶(データベースに登録)させておき、この情報を問い合わせることにより、被管理デバイス側の設定状況を特定できるように構成されたものを例示した。しかし、この被管理デバイス側に記憶させる情報全てをPC10側で収集して管理できるように構成してもよい。このためには、例えば、被管理デバイスに対してデータベースへの登録を伴わない形式で設定を指令すると共に、この指令内容をPC10自身の記憶領域(例えば、RAM13, ハードディスク14など)に記憶しておき、こうして記憶された内容を被管理デバイス側の設定状況をチェックする際に用いるように構成すればよい。10

【0200】

このように構成すれば、PC10側に設定許可情報を記憶させることができるために、被管理デバイスにデータベースを記憶するための記憶領域を確保しておく必要がない。

また、上記実施形態のIPv6_Setting処理においては(図5～図8)、Hideボタン634を選択する操作が行われた場合を除いて、全て図5におけるs204の処理へ戻るように構成してもよい。

【0201】

また、上記実施形態においては、リストにプリフィックスの取得元とすべきでないルータを登録しておき、このリストに登録されたルータからのプリフィックスを取得しないようにする構成を例示した。しかし、このリストに、プリフィックスの取得元とすべきルータのIPアドレスを登録しておき、こうして登録されているルータからのみプリフィックスを取得するように構成してもよい。この場合、図6におけるs224の処理では、同図s216の処理で読み込んだ文字列を登録すべき旨を指令するものとし、図7におけるs288の処理では、選択欄612に入力されているルータのIPアドレスを削除すべき旨を指令するものとすればよい。また、上述したリストとして、プリフィックスの取得元とすべきでないルータのIPアドレスが登録されるリストと、プリフィックスの取得元とすべきルータのIPアドレスが登録されるリストとの2つ用意しておき、両方のリストに基づいてプリフィックスを取得するか否かを決定するように構成してもよく、この場合、より確実に不要なプリフィックスを取得しないようにすることができる。2030

【0202】

また、上記実施形態では、図7におけるs254, s256の処理で「NO」と判定された場合に、同図s266の処理でIPv6によるデータ通信を停止させるように構成されたものを例示した。しかし、このs254, s256の処理による判定については、被管理デバイス側でIPv6によるデータ通信を停止させるか否かを設定しておき、停止させる旨の設定がなされている場合にのみ行うように構成してもよい。具体的な構成としては、まず、被管理デバイス側のデータベースに、IPv6によるデータ通信を停止させることを許可するか否かを示す情報を登録しておき、図2におけるs110の処理でこの情報についても取得するようにしておく。なお、この情報については、PC10側からSNMPに従って任意に変更可能なものとする。そして、図7におけるs252の処理で「YES」と判定された場合、s254の処理に移行する前に、図19に示すように、s110の処理で取得された情報に基づいて、被管理デバイス側でIPv6によるデータ通信を停止させているか否かをチェックし(s422)、停止させることが許可されていれば(s422: YES)、s254以降の処理へ移行する一方、停止させることが許可されていなければ(s422: NO)、s254～s266の処理を行うことなく、s258の処理(または、図2におけるs114の処理)へ移行するように構成すればよい。40

【0203】

このように構成しておけば、被管理デバイスに対してIPv6によるデータ通信を停止

させることを許可しないように設定しておくことにより、図7におけるs254, s256の処理で「NO」と判定されるような状態となっていたとしても、この処理を経てIP v6によるデータ通信が停止されないようにすることができる。

【0204】

また、上記実施形態においては、各種パラメータの変更（図5におけるs340, 図6におけるs220, s224, s236, s238, 図7におけるs258, s266, s276～s282, 図8(a)におけるs300, s302, s306, 図8(b)におけるs320, s322, s324の各処理）を行う際に、例えば、変更自体を禁止する、一部分のみの変更を認めるなどといった何らかの制限を課すことができるよう構成してもよい。例えば、ユーザが入力部18を操作することにより指定したパラメータであって、被管理デバイスに対して変更を制限すべきものとして通知（SNMPなどによる）した特定のパラメータについて変更が制限されるようにすることが考えられ、このためには、パラメータを変更する各処理を以下に示すようにするとよい。10

【0205】

まず、図2におけるs110の処理で上述した制限すべき旨のパラメータを取得しておき、これに基づいて、図20に示すように、変更が制限されているか否かチェックし（s430）、変更が制限されている場合には（s430：YES）、変更が制限されている旨の確認メッセージ（図21参照；ここでは、変更自体が禁止される場合のメッセージを例示）を表示部17に表示させた後（s432）、ユーザによる確認操作（OKボタンを選択する操作）が行われるまで待機し（s434：NO）、確認操作が行われたら（s434：YES）、その制限条件に応じた変更を行う一方（s436）、変更が制限されなければ（s430：NO）、上述したのと同様にパラメータを変更する（s438）、ように構成すればよい。20

【0206】

このように構成すれば、変更を制限すべきものとしてユーザが任意に指定し、かつ、被管理デバイスに対して通知したパラメータについては、この被管理デバイスにおいて変更を制限することができる。20

【0207】

また、上記実施形態におけるIPv6_Setting処理のうち、削除ボタンを選択する操作が行われた場合の処理については、以下に示すような簡略化したものとして構成することもできる。30

【0208】

具体的には、図22に示すように、s240の処理で「YES」と判定された際に、まず、削除ボタン616を選択する操作が行われた時点で選択欄612に入力されているIPアドレスに対応する設定機能（図2におけるs110の処理で取得されたIPアドレスに対応する設定機能）が、ステートレスによるものであるか否かをチェックする（s502）。この処理は、図2におけるs242の処理と同様である。

【0209】

このs502の処理で、ステートレスによるものであると判定されたら（s502：YES）、自動設定されたものであることを確認させるための確認メッセージを表示部17に表示させる（s504）。ここでは、図23(a)に示すように、自動設定されたものであることを確認させるための自動設定通知画面を表示部17に表示させる。この自動設定通知画面には、確認メッセージだけでなく、OKボタン802、および、Cancelボタン804が設けられており、この自動設定通知画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行なうことができる。40

【0210】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する（s506：NO）。

その後、ユーザによる操作が行われたら（s506：YES）、その操作がCancelボタン804を選択する操作であれば（s508：NO）、本IPv6_Setting

g処理を終了し、図2におけるs114の処理へ戻る。

【0211】

また、ユーザによる操作がOKボタン802を選択する操作であれば(s508: YES)、被管理デバイス側においてステートレスにより設定された他のIPアドレスが設定されているか否かをチェックする(s510)。この処理は、図17におけるs412の処理と同様の処理である。

【0212】

このs510の処理でステートレスにより設定された他のIPアドレスが設定されないと判定されたら(s510: YES)、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているルータのIPアドレスに基づいてルータリスト(図10参照)を更新すべき旨を被管理デバイスに指令する(s512)。この処理は、図7におけるs288の処理と同様の処理である。

10

【0213】

一方、s510の処理でステートレスにより設定された他のIPアドレスが設定されないと判定されたら(s510: NO)、ステートレスでの設定を無効なものとすべき旨を被管理デバイスに指令する(s514)。この処理は、図7におけるs280の処理と同様の処理である。

【0214】

こうして、s512, s514の処理を終えた後、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令したら(s516)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。このs516の処理は、図7におけるs258の処理と同様の処理である。

20

【0215】

また、s502の処理で、ステートレスによるものでないと判定されたら(s502: NO)、該当する設定機能(図2におけるs110の処理で取得されたIPアドレスに対応する設定機能)が、ステートフルによるものであるか否かをチェックする(s522)。この処理は、図2におけるs292の処理と同様である。

【0216】

このs522の処理でステートフルによるものと判定されたら(s522: YES)、上述したs504の処理と同様の確認メッセージ(図23(a)参照)を表示部17に表示させる(s524)。

30

【0217】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する(s526: NO)。

その後、ユーザによる操作が行われたら(s526: YES)、その操作がCancelボタン804を選択する操作であれば(s528: NO)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0218】

また、ユーザによる操作がOKボタン802を選択する操作であれば(s528: YES)、被管理デバイス側においてステートフルにより設定された他のIPアドレスが設定されているか否かをチェックする(s530)。この処理は、図18におけるs414の処理と同様の処理である。

40

【0219】

このs530の処理でステートフルにより設定された他のIPアドレスが設定されないと判定されたら(s530: NO)、ステートフルでの設定を無効なものとすべき旨を被管理デバイスに指令する(s534)。この処理は、図7におけるs276の処理と同様の処理である。

【0220】

こうして、s534の処理を終えた後、または、s530の処理でステートフルにより

50

設定された他のIPアドレスが設定されていると判定された場合(s530: YES)、s516の処理へ移行して、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令する。

【0221】

また、上述したs522の処理で、ステートフルによるものでないと判定されたら(s522: NO)、明示的に設定されたアドレスであることを確認させるための確認メッセージを表示部17に表示させる(s542)。ここでは、図23(b)に示すように、明示的に設定されたアドレスであることを確認させるための確認画面を表示部17に表示させる。この確認画面には、確認メッセージだけでなく、OKボタン812、および、Cancelボタン814が設けられており、この自動設定通知画面が表示された後、ユーザは、入力部18により各ボタンのいずれかを選択する操作を行うことができる。10

【0222】

こうして、確認メッセージを表示させた後、ユーザによる操作が行われるまで待機する(s546: NO)。

その後、ユーザによる操作が行われたら(s546: YES)、その操作がCancelボタン814を選択する操作であれば(s548: NO)、本IPv6_Setting処理を終了し、図2におけるs114の処理へ戻る。

【0223】

また、ユーザによる操作がOKボタン812を選択する操作であれば(s548: YES)、被管理デバイス側において手動により設定された他のIPアドレスが設定されているか否かをチェックする(s550)。ここでは、s110の処理で取得された情報のうち、被管理デバイス自身のIPアドレスとして設定されているIPアドレスであって、手動設定を示す情報が対応づけられたIPアドレスが、削除しようとしているIPアドレス以外に存在すれば、設定されていると判定される。20

【0224】

このs550の処理で手動により設定された他のIPアドレスが設定されていないと判定されたら(s550: NO)、ステートフルによる設定を有効なものとすべき旨を被管理デバイスに指令し(s552)、続いて、ステートレスによる設定を有効なものとすべき旨を被管理デバイスに指令した後(s554)、s516の処理へ移行して、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令する。このs552, s554の処理は、図8におけるs320, s322の処理と同様の処理である。30

【0225】

一方、s550の処理で手動により設定された他のIPアドレスが設定されていると判定されたら(s550: YES)、s552, s554の処理を行うことなく、s516の処理へ移行して、削除ボタン616, 626が選択された時点で選択欄612, 622に入力されているIPアドレスを削除すべき旨を被管理デバイスに指令する。

【0226】

また、上記実施形態の図2におけるs128の処理においては、設定画面における全ての画面の入力欄に入力された利用パラメータの設定を設定対象プリンタ20に指令するように構成されたものを例示した。しかし、このような設定指令は、設定対象プリンタ20がIPv4およびIPv6のいずれか、または、両方により通信を実現するように設定されているか(つまりIPモード)に応じたものについて行うように構成してもよい。このためには、例えば、図2におけるs128の処理の替わりに、以下に示すような処理を行うものとした構成を考えることができる。40

【0227】

まず、図2に示すように、s126の処理で「YES」と判定されたら、設定画面における全ての画面の入力欄に入力された利用パラメータそれぞれについて、設定対象IPモード(IPv4用のパラメータであるか、IPv6用のパラメータであるか、または、両方に対応するパラメータであるかを示す)，および、IPアドレス項目(IPアドレスで50

ある場合に「1」となることでIPアドレスを示すパラメータであるか否かを示す)を対応づけて登録したデータテーブルを作成する(s702)。

【0228】

次に、設定対象プリンタに対し、このプリンタのIPモードを確認する(s704)。ここでは、設定対象プリンタに対し、このプリンタのIPモードを問い合わせるための問合データを送信する。この問合データを受信したプリンタからは、後述するように、このプリンタのIPモードを通知するための通知データが送信されてくるため、この通知データで示されるIPモードを設定対象プリンタのIPモードとして確認する。なお、このIPモードについては、図2におけるs110の処理で他の情報と併せて問い合わせるように構成しておき、これをもってIPモードを確認することとしてもよい。

10

【0229】

こうして、設定対象プリンタのIPモードを確認したら、データテーブルに登録されている情報のうち、s702の処理で確認したIPモードに応じた情報をパラメータとして設定指令するための設定指令データを設定対象デバイスに送信する。

【0230】

具体的にいうと、まず、確認したIPバージョンがDualであれば(s708:YES)、データテーブルに登録されている全ての情報をパラメータとして設定対象デバイスに反映させるために、これらパラメータの設定を指令するための設定指令データを送信する(s710)。

【0231】

また、確認したIPバージョンがIPv4であれば(s708:NO, s712:YES)、データテーブルに登録されている情報のうち、設定対象IPモードが「IPv4」となっている情報、「Dual」となっている情報、および、IPアドレス項目が「1」以外つまりIPアドレスではない情報をパラメータとして設定対象デバイスに反映させるために、これらパラメータの設定を指令するための設定指令データを送信する(s714)。

20

【0232】

そして、確認したIPバージョンがIPv6であれば(s712:NO, s716:YES)、データテーブルに登録されている情報のうち、設定対象IPモードが「IPv6」となっている情報、「Dual」となっている情報、および、IPアドレス項目が「1」以外つまりIPアドレスではない情報をパラメータとして設定対象デバイスに反映させるために、このパラメータの設定を指令するための設定指令データを送信する(s718)。なお、確認したIPバージョンが上述したいずれでもなければ(s716:NO)、それに対応するためのエラー処理を行う。

30

【0233】

また、上記実施形態の図2におけるs128の処理においては、設定画面における全ての画面の入力欄に入力された利用パラメータの設定が設定対象プリンタ20に指令され、全ての利用パラメータについての設定がなされるように構成されたものを例示した。しかし、こうして設定を指令された利用パラメータのうち、設定対象プリンタ20側で対応可能な設定のなされたIPモードに応じたもののみを設定するように構成してもよい。このためには、例えば、図2におけるs128の処理による設定指令については、それぞれ設定を指令すべき利用パラメータに、上述したのと同様に、IPモードおよびIPアドレス項目を対応づけて行うこととしておき、このような設定指令を受けた設定対象プリンタ20が、以下に示すような設定反映処理を行うように構成するとよい。

40

【0234】

まず、図25に示すように、設定指令データを受信するまで待機し(s802:NO)、設定指令データを受信したら(s802: YES)、この設定指令データに対応するIPアドレス項目が「1」でない、つまりIPアドレスを示すパラメータでない場合(s808: NO)、この設定指令データで設定を指令されたパラメータ全てをプリンタ20自身の設定内容に反映させる(s810)。ここでは、プリンタ20に設定されているパラ

50

メータのうち、設定指令データで設定を指令されたパラメータ全てについての設定および設定変更を行う。

【0235】

また、設定指令データで特定可能なIPアドレス項目が「1」、つまりIPアドレスを示す情報である場合(s808:YES)、その情報がIPv4の形式で構成された文字列であれば(s812:YES)、プリンタ20自身のIPモードがIPv4またはDualに設定されていることを条件として(s814:YES)、この設定指令データで設定を指令されたパラメータをプリンタ20自身の設定内容に反映させた後(s816)、s802の処理へ戻る。つまり、ネットワーク経由で受信したデータがIPv4に対応するIPアドレスの設定を指令する旨の設定指令データである場合には、プリンタ20自身のIPモードがIPv4またはDualに設定されているときでなければ(s814:NO)、設定内容へのパラメータの反映を行うことなくs802の処理へ戻ることになる。10

【0236】

また、設定指令データで示される情報がIPv4の形式で構成された文字列でなくても(s812:NO)、IPv6の形式で構成された文字列であれば(s818:YES)、プリンタ20自身のIPモードがIPv6またはDualに設定されていることを条件として(s820:YES)、この設定指令データで設定を指令されたパラメータをプリンタ20自身の設定内容に反映させた後(s822)、s802の処理へ戻る。つまり、ネットワーク経由で受信したデータがIPv6に対応するIPアドレスの設定を指令する旨の設定指令データである場合には、プリンタ20自身のIPモードがIPv6またはDualに設定されているときでなければ(s820:NO)、設定内容へのパラメータの反映を行うことなくs802の処理へ戻ることになる。20

【0237】

[本発明との対応関係]

以上説明した実施形態において、被管理デバイスに対して設定すべきパラメータのうち、被管理デバイス自身のIPアドレスは、本発明における通信パラメータであり、これ以外で被管理デバイスに対して設定可能なパラメータが、本発明における機能パラメータである。

【0238】

また、図2におけるs112～s126の処理は本発明における変更指定手順である。30
また、図5におけるs210、s240、s242、s292、s312、図6におけるs218、s226、図7におけるs252からs256、s274、s284、s286、図8におけるs298、s318、図22におけるs502、s522、s508、s510、s528、s530、s548、s550の処理は、本発明におけるパラメータ推定手順である。

【0239】

また、図5におけるs340、図6におけるs220、s228、s224、s236、s238、図7におけるs258、s266、s276～s282、図8におけるs300、s302、s306、s320～s324、図22におけるs512、s514、s516、s534、s552、s554の処理は、本発明におけるパラメータ変更手順である。40

【0240】

また、図6におけるs230、図7におけるs244、s260、s270、図8におけるs294、s314、図22におけるs504、s524、s542の処理は、本発明における存在報知手順および変更選択手順である。

【0241】

また、図6におけるs226の処理は本発明におけるパラメータ判定手順であり、図7におけるs254、s256の処理は本発明における条件判定手順である。

また、図14におけるs604の処理(IPアドレスを設定機能と対応づけて登録する部分)は、本発明における設定登録手順である。50

【0242】

また、図19におけるs422の処理での判断を行うにあたり、被管理デバイス側でIPv6によるデータ通信を停止させるか否かを設定しておく処理については、本発明における第2設定許可手順である。

【0243】

また、図20におけるs430の処理での判断を行うにあたり、ユーザが入力部18を操作することにより指定したパラメータを被管理デバイスに対して変更を制限すべきものとして通知(SNMPなどによる)するまでの処理については、本発明における第1設定許可手順および第3設定許可手順である。

【0244】

また、図20におけるs430の処理は本発明における決定判定手順であり、s436の処理は本発明における変更制限手順である。

【図面の簡単な説明】

【0245】

【図1】ネットワーク構成および各デバイスの制御系統を示す図

【図2】手動設定処理の処理手順を示すフローチャート

【図3】一覧表示画面を示す図

【図4】設定画面における第2の画面を示す図

【図5】第1実施形態におけるIPv6_Setting処理の処理手順を示すフローチャート(1/4)

【図6】第1実施形態におけるIPv6_Setting処理の処理手順を示すフローチャート(2/4)

【図7】第1実施形態におけるIPv6_Setting処理の処理手順を示すフローチャート(3/4)

【図8】第1実施形態におけるIPv6_Setting処理の処理手順を示すフローチャート(4/4)

【図9】第1実施形態におけるIPv6_Settings画面を示す図

【図10】アドレスリストのデータ構造を示す図

【図11】自動設定禁止確認画面(a), (b)、不通確認画面(c)を示す図

【図12】禁止選択画面(a)、自動設定禁止確認画面(b)、自動設定有効確認画面(c)を示す図

【図13】Advanced_Settings画面を示す図

【図14】受信データ処理(メイン)(a)、受信データ処理(RA処理)(b)の処理手順を示すフローチャート

【図15】第2実施形態におけるIPv6_Setting処理の要部の処理手順を示すフローチャート(1/2)

【図16】第2実施形態におけるIPv6_Setting処理の要部の処理手順を示すフローチャート(2/2)

【図17】第3実施形態におけるIPv6_Setting処理の要部の処理手順を示すフローチャート(1/2)

【図18】第3実施形態におけるIPv6_Setting処理の要部の処理手順を示すフローチャート(2/2)

【図19】変形例におけるIPv6_Setting処理の要部

【図20】変形例におけるパラメータを変更する各処理の詳細な処理手順を示すフローチャート

【図21】変形例における変更が制限されている旨の確認メッセージを示す図

【図22】変形例におけるIPv6_Setting処理の要部の処理手順を示すフローチャート

【図23】自動設定通知画面(a)、確認画面(b)を示す図

【図24】別の実施形態における手動設定処理の処理手順を示すフローチャート

10

20

30

40

50

【図25】別の実施形態における設定反映処理の処理手順を示すフローチャート

【図26】ネットワーク印刷処理の処理手順を示すフローチャート

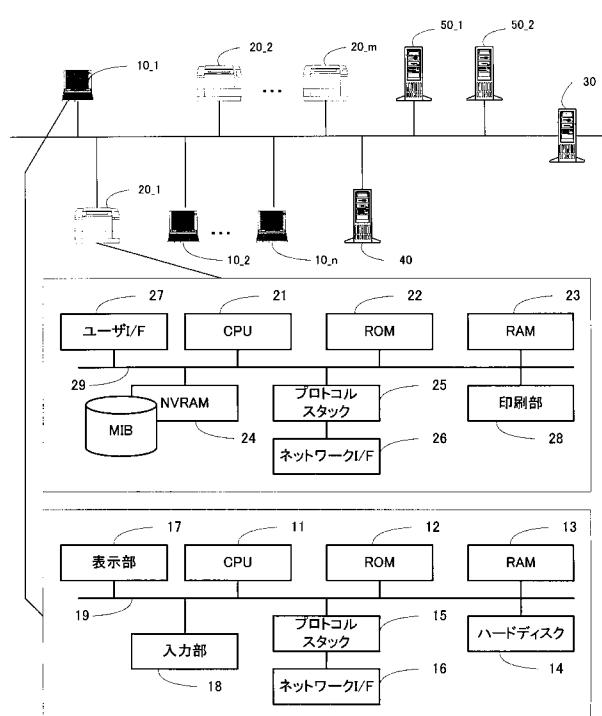
【符号の説明】

【0246】

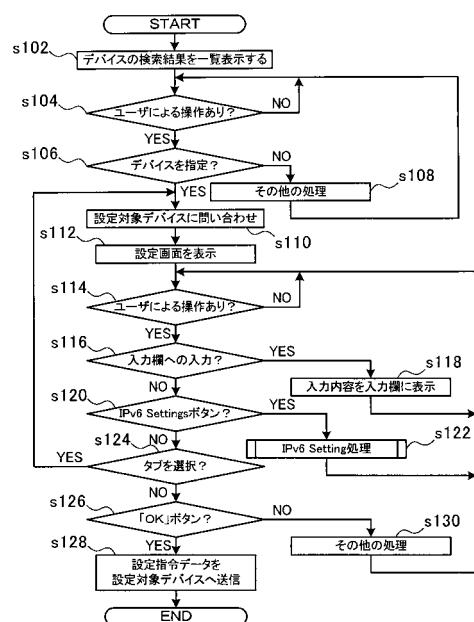
10...パーソナルコンピュータ、11...CPU、12...ROM、13...RAM、14...ハードディスク、15...プロトコルスタック、16...ネットワークインターフェース、17...表示部、18...入力部、19...バス、20...プリンタ、21...CPU、22...ROM、23...RAM、24...NVRAM、25...プロトコルスタック、26...ネットワークインターフェース、27...ユーザインターフェース、28...印刷部、29...バス、30...ゲートウェイ、40...メールサーバ、50...DNSサーバ。

10

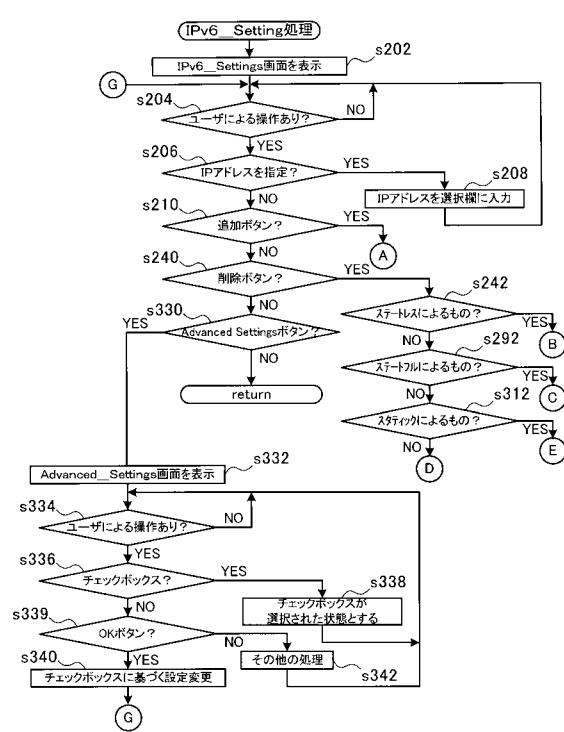
【図1】



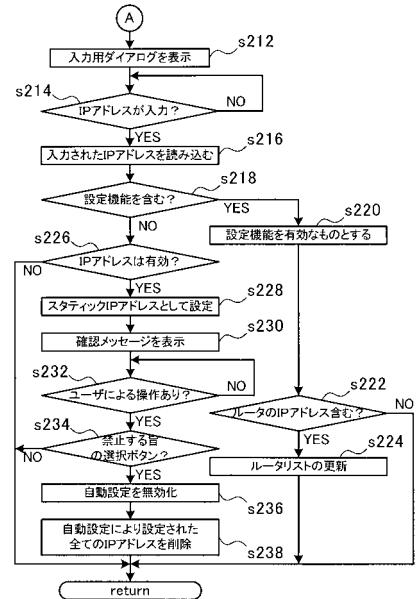
【図2】



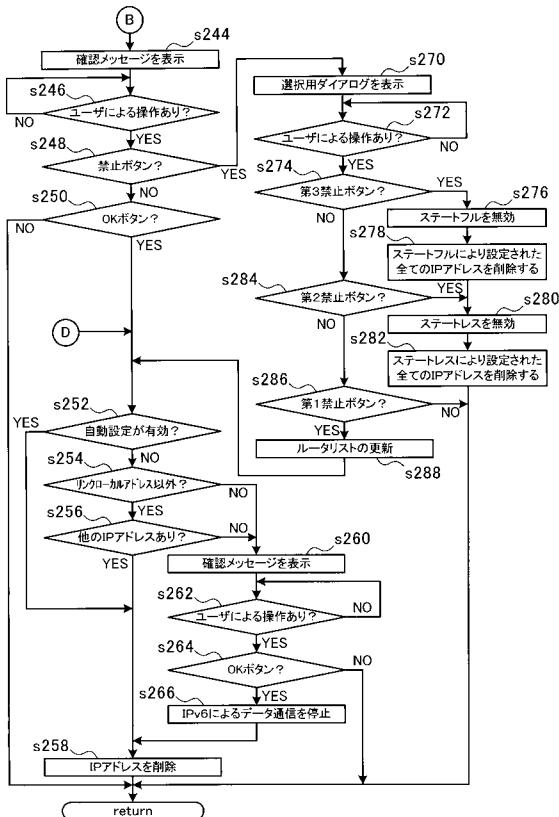
【 図 5 】



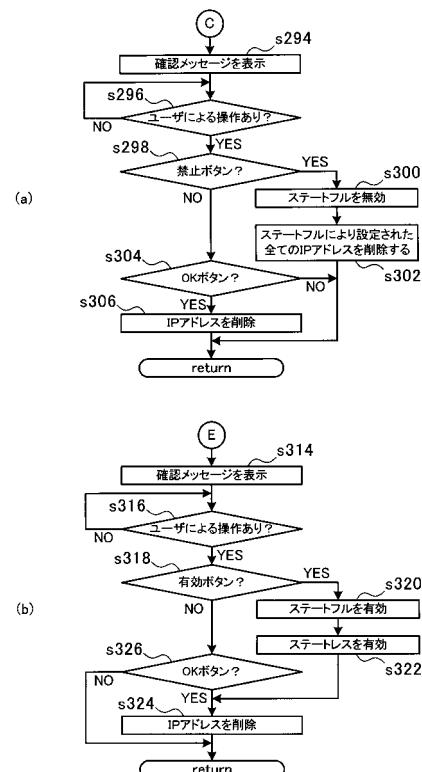
【 四 6 】



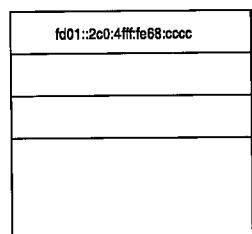
【 図 7 】



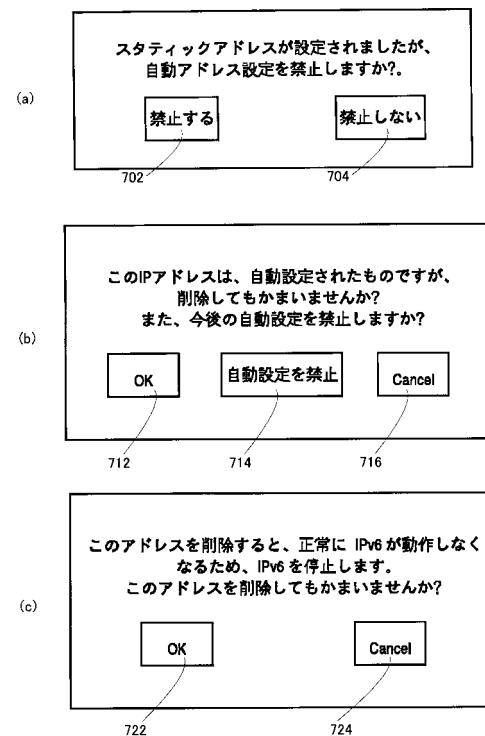
【 四 8 】



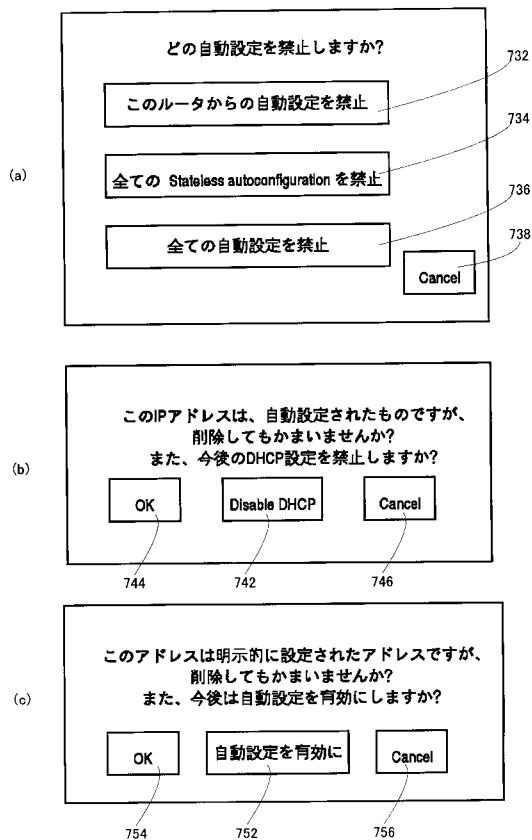
【図10】



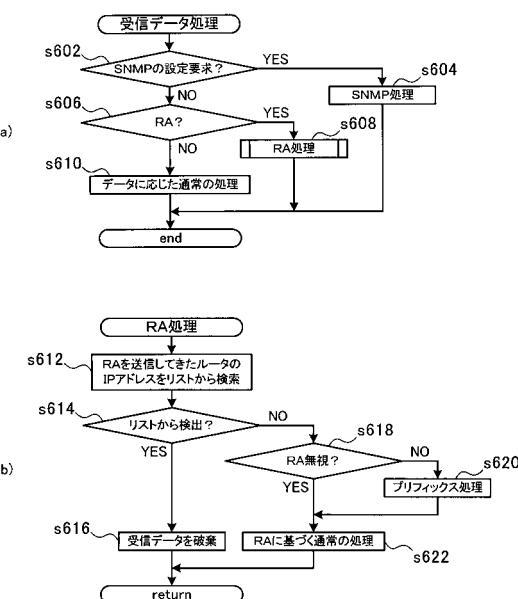
【図11】



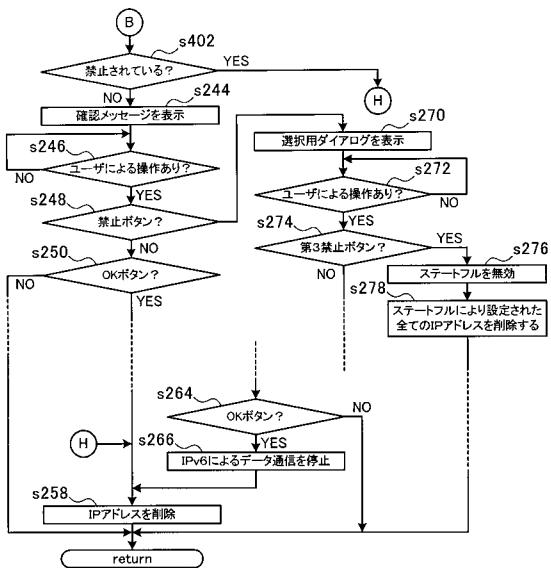
【図12】



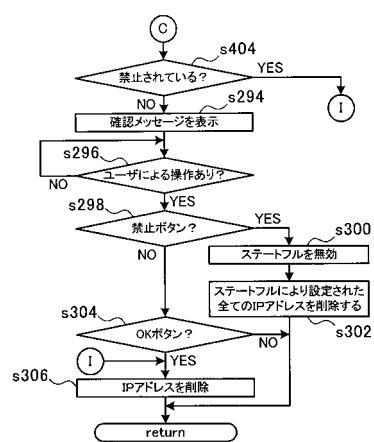
【図14】



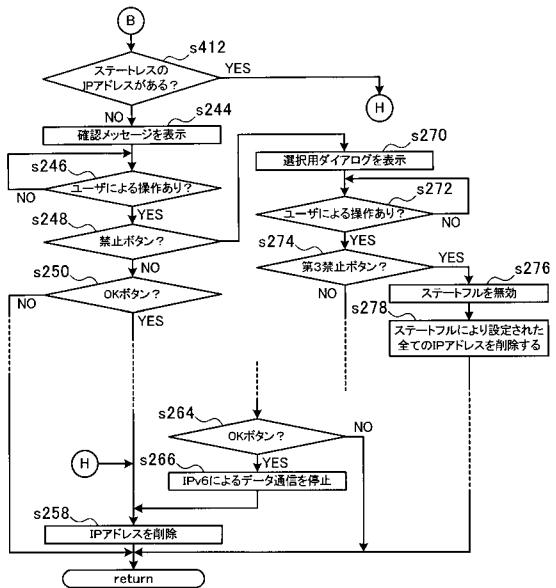
【図15】



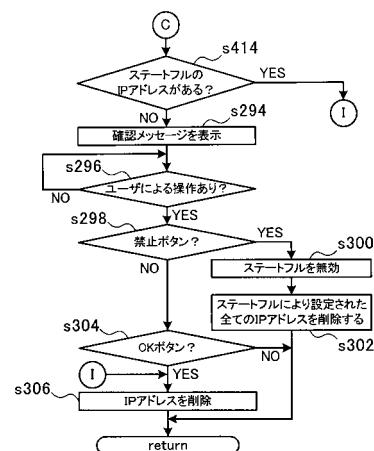
【図16】



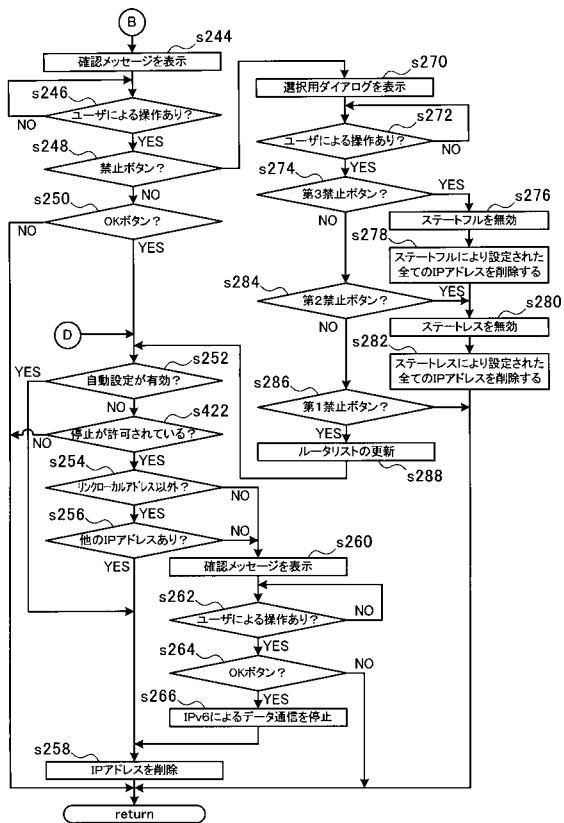
【図17】



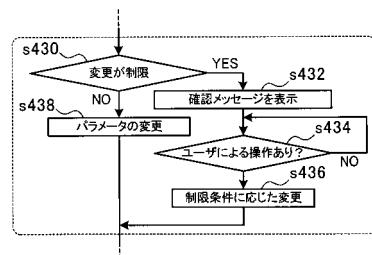
【図18】



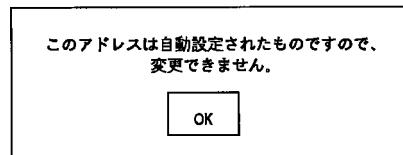
【図19】



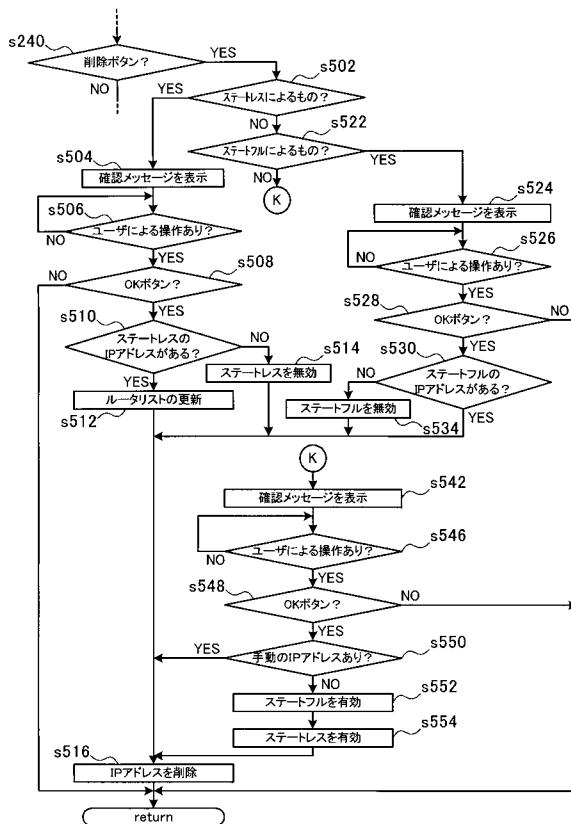
【図20】



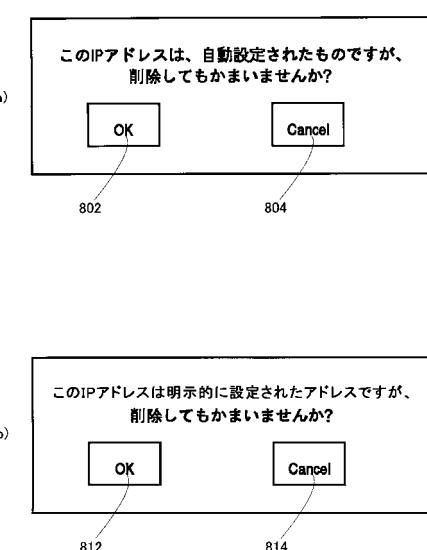
【図21】



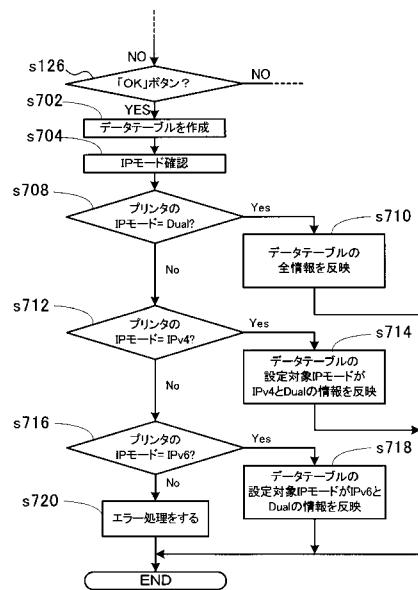
【図22】



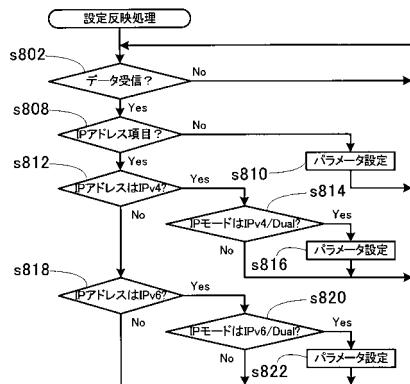
【図23】



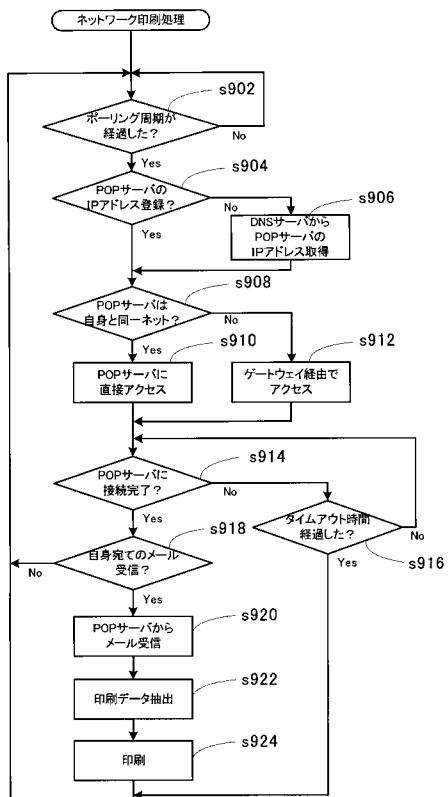
【図24】



【図25】



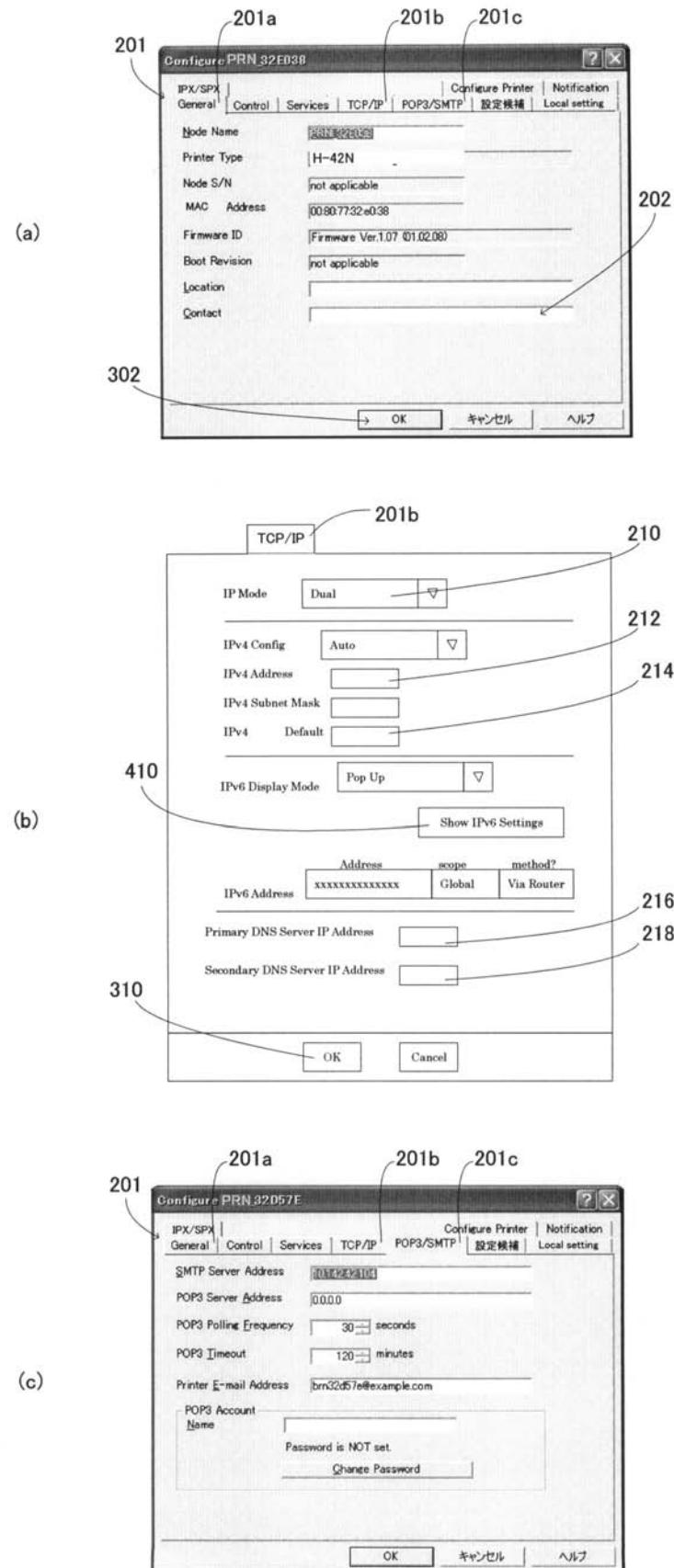
【図26】



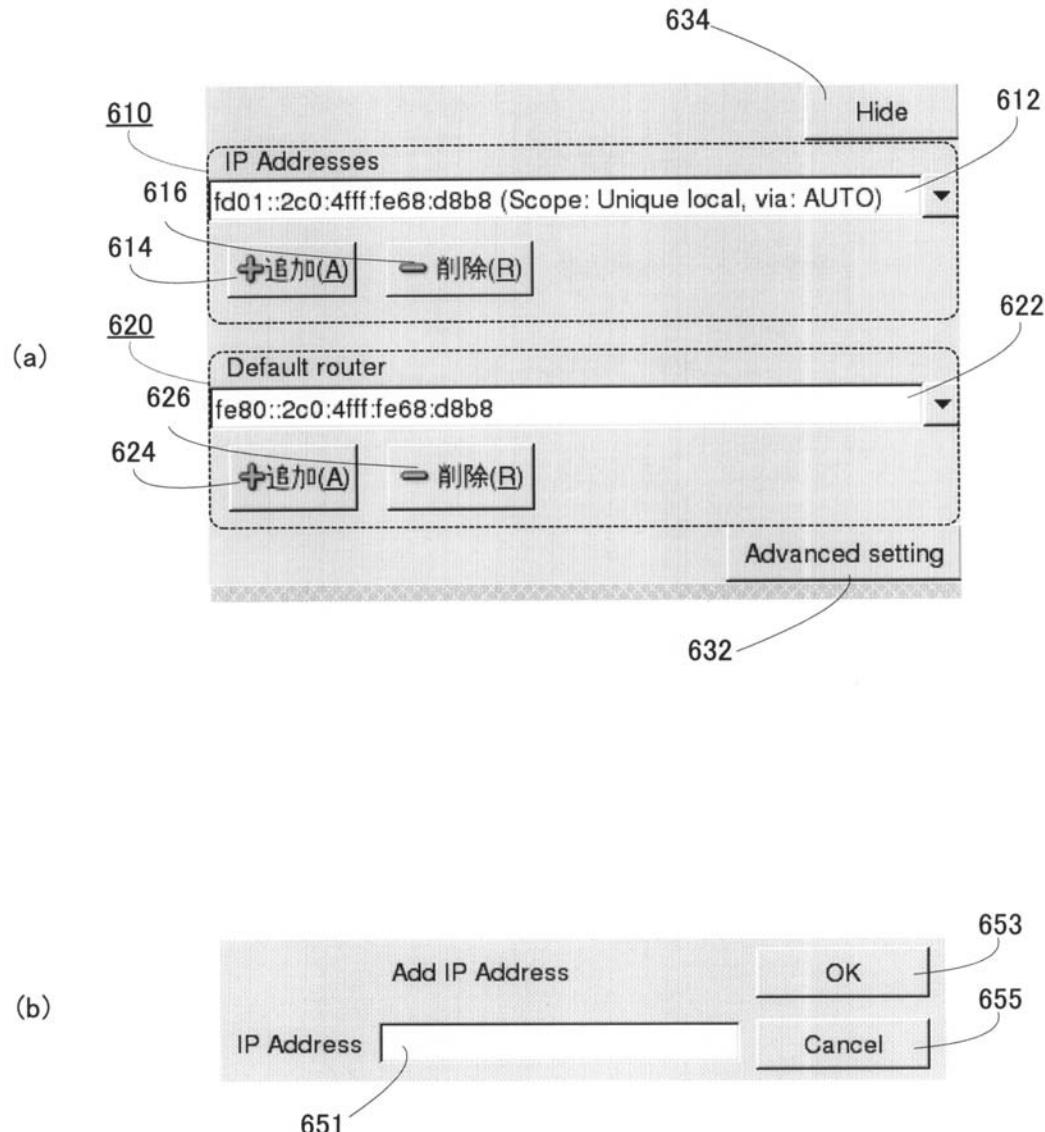
【図3】

Node Name	Log	IPv4 Address	IPv6 Address	Printer Status
PRN_200003		192.168.43.24		SLEEP
PRN_200310		192.168.41.236	2004:0:0:200:69FF:FE20:310	TONER LOW
PRN_220020			2004:0:0:200:69FF:FE20:20	08/08 13:57 FAX
PRN_220029			2004:0:0:200:69FF:FE20:29	READY
PRN_220045		192.168.41.216	2004:0:0:200:69FF:FE20:45	01/01/2002 03:51
PRN_220073			2004:0:0:200:69FF:FE20:73	BACK COVER OPEN
PRN_220077		192.168.150.10	2004:0:0:200:69FF:FE20:77	SLEEP
PRN_22008D		192.168.41.237		SLEEP
PRN_220098		192.168.43.88	2004:0:0:200:69FF:FE20:98	08/26/2004 09:52
PRN_220099			2004:0:0:200:69FF:FE20:99	08/31/2004 13:03
PRN_22009F			2004:0:0:200:69FF:FE20:9F	02/15/2005 15:27
PRN_2200A4		192.168.43.113	2004:0:0:200:69FF:FE20:A4	08/31/2004 13:01
PRN_2241B0		192.168.150.48	2004:0:0:200:69FF:FE20:41B0	2004/01/01 04:12
PRN_2241A8		192.168.41.210	2004:0:0:200:69FF:FE20:41A8	Check Paper
PRN_2241B4		192.168.44.81	2004:0:0:200:69FF:FE20:41B4	Check Paper #1
PRN_343509		192.168.43.40	2004:0:0:200:69FF:FE34:3509	READY
PRN_35AC43		192.168.100.19		SLEEP
PRN_35FAEF		192.168.150.133		02/08 14:07 Fax
PRN_420028			2004:0:0:200:69FF:FE42:28	SLEEP

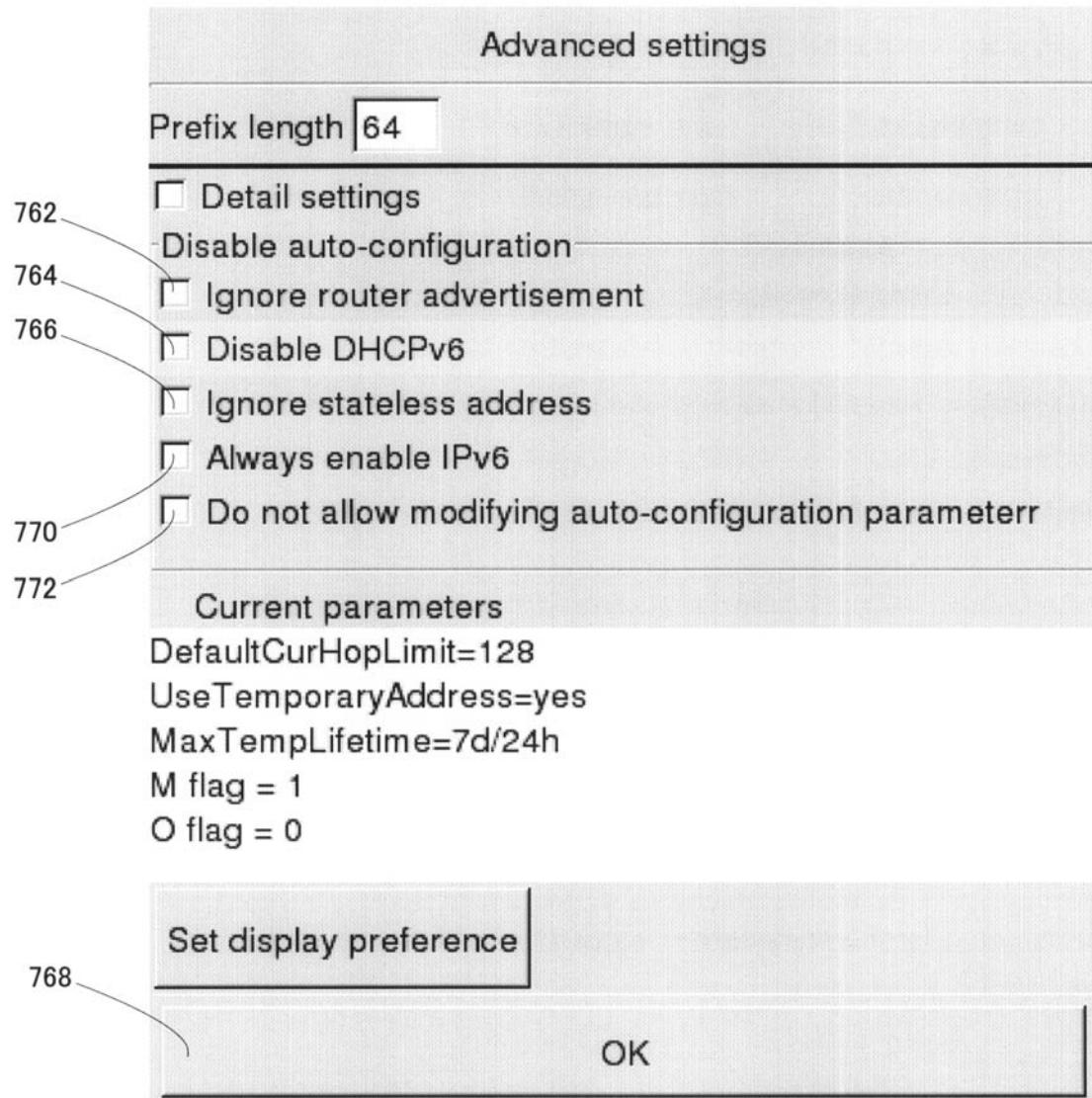
【図4】



【図9】



【図13】



フロントページの続き

(56)参考文献 特開平04-175852(JP,A)
国際公開第2004/071044(WO,A1)
特開2001-292191(JP,A)
特開2001-273220(JP,A)
特開平11-73487(JP,A)
島 康一, IPV6の実装 11 アドレス自動設定の実装(2), UNIX MAGAZINE, 2002年 9月 1日, 第17巻, 第9号, p.76~87

(58)調査した分野(Int.Cl., DB名)

H04L 12/24
G06F 13/00