(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5245906号
(P5245906)

(45)発行日　平成25年7月24日(2013.7.24)　(24)登録日　平成25年4月19日(2013.4.19)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 353B

請求項の数 13　(全 22 頁)

(21)出願番号　特願2009-39707(P2009-39707)
(22)出願日　平成21年2月23日(2009.2.23)
(65)公開番号　特開2010-198125(P2010-198125A)
(43)公開日　平成22年9月9日(2010.9.9)
審査請求日　平成24年1月26日(2012.1.26)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　永森　彰
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　▲高▼部　広大

最終頁に続く

(54)【発明の名称】機器管理装置、機器管理システム、機器管理方法、機器管理プログラム、及びそのプログラムを記録した記録媒体

(57)【特許請求の範囲】
【請求項１】
所定のデータ伝送路に接続された機器から送信される機器情報を取得し、取得した機器情報に基づき前記機器を管理する機器管理装置であって、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手段と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手段と、
前記機器特定手段により特定した前記送信元の機器が当該機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手段と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手段と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手段と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手段を、有し、

前記判定条件変換手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求することを特徴とする機器管理装置。
【請求項２】
前記管理対象機器判定手段は、
前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていると確認された場合に、
前記セキュリティレベル取得手段に、前記送信元の機器に設定されたセキュリティレベル情報の取得を要求することを特徴とする請求項１に記載の機器管理装置。
【請求項３】
前記機器特定手段は、
前記送信元の機器から取得した前記機器特定情報を基に前記機器照合情報を参照し、該当する管理対象機器の管理対象機器特定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、管理対象機器である前記送信元の機器を特定することを特徴とする請求項１又は２に記載の機器管理装置。
【請求項４】
前記機器特定手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていると確認された場合に、
前記送信元のネットワーク設定情報を基に前記機器照合情報から取得した前記管理対象機器特定情報と、前記送信元の機器から取得した前記機器特定情報とを照合し、照合結果に基づいて、管理対象機器である前記送信元の機器を特定することを特徴とする請求項３に記載の機器管理装置。
【請求項５】
前記機器特定手段は、
前記照合結果が一致した管理対象機器を前記送信元の機器であると特定することを特徴とする請求項４に記載の機器管理装置。
【請求項６】
前記機器特定手段は、
前記照合結果が一致せず、
かつ、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合、又は、前記機器照合情報に該当する管理対象機器の管理対象機器特定情報が含まれていないと確認された場合、
前記送信元の機器が管理対象機器でないと特定することを特徴とする請求項４又は５に記載の機器管理装置。
【請求項７】
前記機器特定手段は、
前記照合結果が一致せず、
かつ、前記機器照合情報に該当する管理対象機器の管理対象機器特定情報が含まれていると確認された場合、
前記管理対象機器である前記送信元の機器を特定し、
かつ、前記送信元の機器に割り当てられた前記ＩＰアドレスが変更されたと判断することを特徴とする請求項４ないし６のいずれか一項に記載の機器管理装置。
【請求項８】
当該機器管理装置が、
前記機器照合情報を更新する機器照合情報更新手段を、有し、
前記機器照合情報更新手段は、

前記機器特定手段により、前記管理対象機器である前記送信元の機器を特定し、
かつ、前記送信元の機器に割り当てられた前記ＩＰアドレスが変更されたと判断された場合、
前記機器照合情報を更新することを特徴とする請求項１ないし７のいずれか一項に記載の機器管理装置。
【請求項９】
前記ネットワーク設定情報は、
前記機器に割り当てられたＩＰアドレスを含むことを特徴とする請求項１ないし８のいずれか一項に記載の機器管理装置。
【請求項１０】
所定のデータ伝送路に接続された機器から送信される機器情報を機器管理装置が取得し、取得した機器情報に基づき前記機器を管理する機器管理システムであって、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手段と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手段と、
前記機器特定手段により特定した前記送信元の機器が前記機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手段と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手段と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手段と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手段を、有し、
前記判定条件変換手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求することを特徴とする機器管理システム。
【請求項１１】
所定のデータ伝送路に接続された機器から送信される機器情報を取得し、取得した機器情報に基づき前記機器を管理する機器管理装置における機器管理方法であって、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手順と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手順と、
前記機器特定手順により特定した前記送信元の機器が前記機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手順と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手順と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定

手順と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手順を、有し、
前記判定条件変換手順は、
前記管理対象機器判定手順により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手順を実行する管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求することを特徴とする機器管理方法。
【請求項１２】
所定のデータ伝送路に接続された機器から送信される機器情報を取得し、取得した機器情報に基づき前記機器を管理する機器管理装置における機器管理プログラムであって、
コンピュータを、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手段と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手段と、
前記機器特定手段により特定した前記送信元の機器が前記機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手段と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手段と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手段と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手段として機能させ、
前記判定条件変換手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求する機器管理プログラム。
【請求項１３】
請求項１２に記載のプログラムを記憶した、コンピュータが読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークなどのデータ伝送路を介して接続される１又は複数の機器を管理する機器管理装置、機器管理システムに関し、特に、受信した機器情報が、管理対象の機器のうち、どの機器のものかを特定する技術に関するものである。
【背景技術】
【０００２】
ネットワークなどの所定のデータ伝送路を介して複合機（ＭＦＰ：Multifunction Peripheral）やプリンタと言った画像処理装置などの状態を機器管理装置により監視するシステムはすでに知られており、ユーザは管理対象の機器（以下、「管理対象機器」と言う。）に自ら出向くことなく、管理対象機器の異常を検知する（知る）ことが可能となっている。

【０００３】
例えば特許文献１には、機器管理システムにおいて、機器管理装置が管理対象機器からの機器情報を取得する方法であるＴｒａｐとポーリングとを使い分けることで、情報取得に係る通信負荷を軽減することができる機器管理装置が開示されている。
【０００４】
上述のとおり、機器管理装置が機器情報を取得する方法には、Ｔｒａｐとポーリングの２つがある。
【０００５】
Ｔｒａｐとは、管理対象機器自らが、予め決められた条件（例えば「発生エラー」や「機器状態」など）を満たした場合に機器情報を送信することで、機器管理装置が機器情報を取得するものである。つまり、エージェントが自発的にマネージャへ情報を通知する。一方、ポーリングとは、機器管理装置が、管理対象機器に対して機器情報の取得要求を行うことで、管理対象機器からの応答を受信し、機器管理装置が機器情報を取得するものである。つまり、マネージャが定期的に要求を送信し、これにエージェントが応答する。
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来の機器管理では、機器管理装置が、Ｔｒａｐにより機器情報を取得する場合に、受信した機器情報が、どの機器から送信された情報かを正しく特定することができない場合があった。
【０００７】
ＤＨＣＰ（Dynamic Host Configuration Protocol）によるネットワーク環境は、多数のクライアントをネットワークに接続する際、クライアントごとにネットワーク設定（例えば「ＩＰアドレスの割り当て」など）を手動で行う必要がない。また、モバイル端末（例えば「ノート型ＰＣ（Personal Computer）」など）を複数の場所でネットワークに接続する場合にも、ネットワーク設定を手動で切り替える必要がない。このように、ネットワーク管理の手間を削減できるメリットがある。
【０００８】
このようなことから、上述したような機器管理システムにおいても、管理対象機器の増減などに対して、各機器のネットワーク設定が自動的に行われ、ネットワーク管理の手間を削減できることから、ＤＨＣＰによるネットワーク環境を構築する場合がある。
【０００９】
このようなネットワーク環境下では、機器に対して自動的にＩＰアドレスが割り当てられる。そのため、各機器に割り当てられたＩＰアドレスと、機器管理装置側で管理する各機器のＩＰアドレスとが異なる可能性がある。
【００１０】
もし、ＩＰアドレスが異なる場合には、機器管理装置が、Ｔｒａｐにより機器から機器情報を受信しても、どの機器から送信された情報かを正しく特定することができない。
【００１１】
そのため、機器管理装置が、機器情報を送信した機器が、管理対象機器なのか又は非管理対象機器なのかを判断することができず、受信した機器情報を機器管理用データとして取り扱えない。その結果、機器管理が正常に行えないこととなる。
【００１２】
そこで、機器管理装置は、管理対象機器なのか又は非管理対象機器なのかを判断するために、機器と所定のデータ通信を行い、機器を特定可能な情報（例えば「ネットワーク機器のハードウェア固有の物理アドレス：ＭＡＣ（Media Access Control）アドレス」など）を取得する必要がある。さらに、機器管理装置と機器とにおいて、互いの通信時におけるセキュリティレベルの設定が異なることも考えられるため、機器とのデータ通信の際には、適切なセキュリティレベル（機器にあったセキュリティレベル）で通信を行う必要がある。

【００１３】
本発明は上記従来技術の問題点を鑑み提案されたものであり、その目的とするところは、ネットワーク設定が自動的に行われる環境下において機器のネットワーク設定が変更されても、セキュリティを意識した通信方法で情報送信元の機器を特定し、機器管理を正常に行うことができる機器管理装置、機器管理システム、機器管理方法、機器管理プログラム、及びそのプログラムを記録した記録媒体を提供することにある。
【課題を解決するための手段】
【００１４】
上記目的を達成するため、本発明に係る機器管理装置にあっては、所定のデータ伝送路に接続された機器から送信される機器情報を取得し、取得した機器情報に基づき前記機器を管理する機器管理装置であって、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手段と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手段と、
前記機器特定手段により特定した前記送信元の機器が当該機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手段と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手段と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手段と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手段を、有し、
前記判定条件変換手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求するように、している。
【００１５】
このような構成によって、本発明に係る機器管理装置は、送信元のＩＰアドレスを基に該機器に設定された通信時のセキュリティレベルを示す情報（以下、「セキュリティレベル情報」を言う。）を取得し、取得した情報に示されるセキュリティレベルに従って機器を特定する情報（以下、「機器特定情報」と言う。）を取得する。続いて、取得した機器特定情報を基に、機器情報を送信した機器を特定する。その結果、特定した機器が管理対象機器であった場合、受信した機器情報を基に該当する管理対象機器の機器情報を更新する。
【００１６】
これによって、本発明に係る機器管理装置は、ネットワーク設定が自動的に行われる環境下において機器のネットワーク設定が変更されても、セキュリティを意識した通信方法で情報送信元の機器を特定することができる。その結果、受信した機器情報を機器管理データとして取り扱うことができ、機器管理を正常に行うことができる。
【００１７】
上記目的を達成するため、本発明に係る機器管理システムは、所定のデータ伝送路に接続された機器から送信される機器情報を機器管理装置が取得し、取得した機器情報に基づき前記機器を管理する機器管理システムであって、

送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手段と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手段と、
前記機器特定手段により特定した前記送信元の機器が前記機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手段と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手段と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手段と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手段を、有し、
前記判定条件変換手段は、
前記管理対象機器判定手段により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求するように、している。

【００１８】

上記目的を達成するため、本発明に係る機器管理方法は、所定のデータ伝送路に接続された機器から送信される機器情報を取得し、取得した機器情報に基づき前記機器を管理する機器管理装置における機器管理方法であって、
送信元のネットワーク設定情報を基に、前記機器に設定された通信時のセキュリティレベルを示すセキュリティレベル情報を取得するセキュリティレベル取得手順と、
前記セキュリティレベル情報に示されるセキュリティレベルに従って前記機器から取得した、前記機器を特定する機器特定情報に基づいて、前記送信元の機器を特定する機器特定手順と、
前記機器特定手順により特定した前記送信元の機器が前記機器管理装置で管理する管理対象機器であった場合、受信した前記機器情報に基づいて、１又は複数の管理対象機器の機器情報のうち、該当した機器情報を更新する機器情報更新手順と、
前記管理対象機器のネットワーク設定情報及び前記管理対象機器を特定する管理対象機器特定情報を含む機器照合情報を保持する機器照合情報保持手順と、
前記送信元のネットワーク設定情報を基に前記機器照合情報を参照し、該当する管理対象機器のネットワーク設定情報が前記機器照合情報に含まれているかを確認し、確認結果に基づいて、前記送信元の機器が管理対象機器であるか否かを判定する管理対象機器判定手順と、
前記送信元のネットワーク設定情報に含まれるＩＰアドレスをホスト名に変換する判定条件変換手順を、有し、
前記判定条件変換手順は、
前記管理対象機器判定手順により、前記機器照合情報に該当する管理対象機器のネットワーク設定情報が含まれていないと確認された場合に、前記ＩＰアドレスを前記ホスト名に変換し、
前記管理対象機器判定手順を実行する管理対象機器判定手段に対して、前記送信元の機器が管理対象機器であるか否かの判定を要求するように、している。

【００１９】

このような手順によって、本発明に係る機器管理方法は、送信元のＩＰアドレスを基に

機器から該機器に設定された通信時のセキュリティレベル情報を取得し、取得した情報に示されるセキュリティレベルに従って機器特定情報を取得し、取得した機器特定情報を基に機器情報を送信した機器を特定し、特定した機器が管理対象機器であった場合、受信した機器情報を基に該当する管理対象機器の機器情報を更新すると言う動作を実現する。

【００２０】

これによって、本発明に係る機器管理方法は、ネットワーク設定が自動的に行われる環境下において機器のネットワーク設定が変更されても、セキュリティを意識した通信方法で情報送信元の機器を特定し、機器管理を正常に行うことが可能な環境を提供できる。

【発明の効果】

【００２１】

本発明によれば、ネットワーク設定が自動的に行われる環境下において機器に割り当てられるＩＰアドレスが変更されても、セキュリティを意識した通信方法で機器を特定し、機器管理が正常に行える機器管理装置、機器管理システム、機器管理方法、機器管理プログラム、及びそのプログラムを記録した記録媒体を提供することができる。

【図面の簡単な説明】

【００２２】

【図１】本発明の第１の実施形態に係る機器管理システムの構成例を示す図である。

【図２】本発明の第１の実施形態に係る機器管理装置のハードウェア構成例を示す図である。

【図３】本発明の第１の実施形態に係る機器管理装置が有する機能構成例を示す図である。

【図４】本発明の第１の実施形態に係る機器照合情報のデータ例を示す図である。

【図５】本発明の第１の実施形態に係るＳＮＭＰ通信を行う処理手順例を示すフローチャートである。

【発明を実施するための形態】

【００２３】

以下、本発明の好適な実施の形態（以下、「実施形態」と言う。）について、図面を用いて詳細に説明する。

【００２４】

［第１の実施形態］

＜システム構成＞

本実施形態に係る機器管理システムの構成について説明する。

【００２５】

図１は、本実施形態に係る機器管理システム１の構成例を示す図である。

図１に示すように、機器管理システム１は、例えば、ＭＦＰやＬＰ（Laser Printer）と言った画像処理装置である複数の機器２００、ユーザ端末などの複数のクライアントＰＣ３００（以下、単に「ＰＣ」と言う。）、及び機器管理装置１００が、ネットワークなどのデータ伝送路９０で相互に接続されている。

【００２６】

このようなシステム構成により、機器管理装置１００は、機器２００から各種ログ（例えば「ジョブログ」や「アクセスログ」など）を含む機器情報を取得し、機器状態を監視することで機器管理を行う。また、ＰＣ３００に対しては、管理対象機器２００の状態に関する各種情報を提供する。

【００２７】

また、図１に示す機器管理システム１には、ＤＨＣＰ・ＤＮＳ（Domain Name System）サーバであるネットワーク管理装置４００が接続されている。

【００２８】

ＤＨＣＰは、コンピュータがネットワーク接続する際に必要な情報（例えば「ＩＰアドレス」などのネットワーク設定情報）を自動的に割り当てるプロトコルのことを言う。また、ＤＮＳは、ホスト名の入力があるとＤＮＳサーバと呼ばれるコンピュータを参照し、

そのホストのもつＩＰアドレスを検索するシステムである。ＤＮＳでは、ホスト名からＩＰアドレスを検索する順引きと、ＩＰアドレスからホスト名を検索（名前解決）する逆引きが行える。

【００２９】

ここで、ホスト名とは、ネットワークに接続された機器２００に付けられた人間が可読可能なユニークな名前である。

【００３０】

このようなネットワーク管理装置４００では、ＤＨＣＰにより機器２００にＩＰアドレスが割り当てられると、それに連動してＤＮＳのエントリ（「ＩＰアドレス」と「ホスト名」との対応付け）が動的に更新される。

【００３１】

このようなシステム構成により、機器管理システム１における機器２００やＰＣ３００など増減に対して柔軟に対応することができ、ネットワーク管理の手間を削減できる。

【００３２】

なお、図１に示すシステム構成は、機器２００に割り当てられたＩＰアドレスが変更される（手動／自動問わず）可能性があるネットワーク環境の一例であって、上記構成に本発明が限定されるものではない。

【００３３】

＜ハードウェア構成＞

次に、本実施形態に係る機器管理装置１００のハードウェア構成について説明する。

【００３４】

図２は、本実施形態に係る機器管理装置１００のハードウェア構成例を示す図である。

図２に示すように、機器管理装置１００は、入力装置１０１、表示装置１０２、ドライブ装置１０３、ＲＡＭ（Random Access Memory）１０４、ＲＯＭ（Read Only Memory）１０５、ＣＰＵ１０６、インタフェース装置１０７、及びＨＤＤ（Hard Disk Drive）１０８などを含むハードウェアを備え、それぞれがバスで相互に接続されている。

【００３５】

入力装置１０１は、キーボード及びマウスなどを含み、機器管理装置１００に各操作信号を入力するのに用いられる。表示装置１０２は、ディスプレイなどを含み、機器管理装置１００による処理結果（例えば「機器の状態情報」）などを表示する。

【００３６】

インタフェース装置１０７は、機器管理装置１００をネットワークなどの所定のデータ伝送路９０に接続するインタフェースである。よって、機器管理装置１００は、インタフェース装置１０７を介して、機器２００、ＰＣ３００、及びネットワーク管理装置４００とデータ通信を行うことができる。

【００３７】

ＨＤＤ１０８は、各種プログラムやデータを格納している不揮発性の記憶装置である。格納されるプログラムやデータには、例えば、機器管理装置１００全体を制御する情報処理システム（例えば「Ｗｉｎｄｏｗｓ（登録商標）」や「ＵＮＩＸ（登録商標）」などの基本ソフトウェアであるＯＳ（Operating System））、及び情報処理システム上において各種機能（例えば「機器管理機能」）を提供するアプリケーションなどがある。また、ＨＤＤ１０８は、格納している上記プログラムやデータを、所定のファイルシステム及び／又はＤＢ（Data Base）により管理している。

【００３８】

ドライブ装置１０３は、着脱可能な記録媒体１０３ａとのインタフェースである。よって、機器管理装置１００は、ドライブ装置１０３を介して、記録媒体１０３ａの読み取り及び／又は書き込みを行うことができる。

【００３９】

ＲＯＭ１０５は、電源を切っても内部データを保持することができる不揮発性の半導体メモリ（記憶装置）である。ＲＯＭ１０５には、機器管理装置１００が起動されるときに

実行されるＢＩＯＳ（Basic Input/Output System）や、機器管理装置１００のシステム設定やネットワーク関連の設定などのデータが格納されている。

【００４０】

ＲＡＭ１０４は、上記各種記憶装置から読み出されたプログラムやデータを一時保持する揮発性の半導体メモリ（記憶装置）である。

【００４１】

ＣＰＵ１０６は、上記ＲＡＭ１０４上に読み出したプログラムを実行することにより、機器管理装置１００の全体制御や機器管理装置１００が搭載する各種機能を動作させる。

【００４２】

このようなハードウェア構成により、機器管理装置１００は、例えば、ＨＤＤ１０８からＲＡＭ１０４上に読み出したプログラム（機器管理プログラム）をＣＰＵ１０６により実行し、機器管理機能を実現することができる。

【００４３】

＜機器特定機能＞

次に、本実施形態に係る機器管理機能について説明する。

【００４４】

本実施形態に係る機器管理装置１００では、送信元のＩＰアドレスを基に機器２００から機器２００に設定された通信時のセキュリティレベル情報を取得する。続いて、取得した情報に示されるセキュリティレベルに従って、機器２００から機器特定情報を取得する。続いて、取得した機器特定情報を基に機器情報を送信した機器２００を特定する。その結果、特定した機器２００が管理対象機器であった場合、受信した機器情報を基に該当する管理対象機器の機器情報を更新する。機器管理装置１００は、このような機器管理機能を有している。

【００４５】

例えば、ＩＰアドレスが自動的に割り当てられるネットワーク環境では、各機器２００に割り当てられたＩＰアドレスと、機器管理装置１００で管理する各管理対象機器のＩＰアドレスとが異なる可能性がある。

【００４６】

もし、ＩＰアドレスが異なる場合には、機器管理装置１００が、機器２００からＳＮＭＰのＴｒａｐにより送信された機器情報を受信しても、どの機器２００から送信された情報かを正しく特定することができない。そのため、受信した機器情報を機器管理用データとして取り扱えず、機器管理が正常に行えないこととなる。

【００４７】

そのため、機器管理装置１００は、送信元の機器２００が管理対象機器なのか又は非管理対象機器なのかを判断しなければならない。このとき、機器２００と所定のデータ通信を行い、機器２００の機器特定情報を取得する必要がある。さらに、機器管理装置１００と機器２００とにおいて、互いの通信時におけるセキュリティレベルの設定が異なることも考えられる。機器２００とのデータ通信の際には、適切なセキュリティレベル（機器２００にあったセキュリティレベル）で通信を行う必要がある。

【００４８】

そこで、本実施形態に係る機器管理装置１００は、送信元の機器２００に応じたセキュリティレベルに従って機器２００から機器特定情報を取得し、取得した情報を基に機器情報を送信した機器２００を特定し、特定した機器２００が管理対象機器か又は非管理対象機器かを判断する。その結果、機器管理装置１００は、特定した機器２００が管理対象機器であった場合、受信した機器情報を基に該当する管理対象機器の機器情報を更新する。

【００４９】

これによって、機器管理装置１００では、ネットワーク設定が自動的に行われる環境下において機器２００に割り当てられるＩＰアドレスが変更されても、セキュリティを意識した通信方法で情報送信元の機器２００を特定し、機器管理が正常に行える。

【００５０】

《機能構成》
以下に、上記ログ管理機能の構成とその動作について説明する。
【００５１】
図３は、本実施形態に係る機器管理機能の構成例を示す図である。
図３に示すように、機器管理装置１００は、機器照合用データ取得部２１、機器照合情報保持部２２、機器情報取得部２３、管理対象機器判定部２４、判定情報変換部２５、セキュリティレベル取得部２６、機器特定部２７、受信データ処理部２８、及び機器照合情報更新部２９などを有している。
【００５２】
機器照合用データ取得部２１は、機器２００及びネットワーク管理装置４００から、機器２００を特定するための各種照合用データを取得する。ここで取得するデータは、機器特定情報である。機器特定情報には、例えば、ネットワーク機器のハードウェア固有の物理アドレス（以下、「ＭＡＣ（Media Access Control）アドレス」と言う。）などが挙げられる。
【００５３】
また、上記照合用データの取得は、機器２００及びネットワーク管理装置４００のＩＰアドレスを基に、ＳＮＭＰのコマンド（Ｇｅｔコマンドなど）を用いて、情報取得要求を行い、機器２００及びネットワーク管理装置４００から応答を受信することで取得できる。
【００５４】
このように、機器照合用データ取得部２１で取得した各種照合用データは、機器照合情報３１として、例えば、機器管理装置１００が備える記憶装置（例えば「ＨＤＤ１０８」）の所定の記憶領域に格納され保持される。よって、機器照合情報３１を保持する記憶領域が、機器照合情報保持部２２にあたる。
【００５５】
（機器照合情報）
ここで、上記機器照合情報３１について、図４を用いて説明する。
【００５６】
図４は、本実施形態に係る機器照合情報３１のデータ例を示す図である。
図４に示すように、機器照合情報３１は、「ＩＰアドレス」、「ホスト名」、「ＭＡＣアドレス」、及び「ＳＮＭＰ通信設定」の各情報項目を含み、機器２００ごとに各情報項目が対応付けられている。つまり、いずれか１つの項目データが明らかであれば、このデータを基に、他の項目データを特定することができる。
【００５７】
「ＩＰアドレス」は、後述する機器情報取得部２３により取得される機器照合用データである。「ＩＰアドレス」は、機器２００に割り当てられたＩＰアドレスを示すデータである。
【００５８】
また、「ホスト名」及び「ＭＡＣアドレス」は、上述したように機器照合用データ取得部２１により取得された機器照合用データである。「ホスト名」は、機器２００のホスト名を示すデータであり、「ＭＡＣアドレス」は、機器２００が備えるネットワークＩ／Ｆ装置（非図示）の物理アドレスを示すデータである。例えば、ＮＩＣ（Network I/F Card）などが保有するデータである。
【００５９】
また、「ＳＮＭＰ通信設定」は、ＳＮＭＰを用いたデータ通信に関する各種制御情報があるか否か（制御情報の有無）を示すデータである。上記各種制御情報とは、通信時のＳＮＭＰのバージョン情報（ｖ１，ｖ２，ｖ３）や、各バージョンにおけるＳＮＭＰコマンドの各種パラメータなどである。
【００６０】
ＳＮＭＰ通信設定項目には、上記各種制御情報があるか否かを設定することができる。

【００６１】
また、上記各設定項目は、管理者を含むユーザが、当該機器管理装置１００が備える入力装置１０１を介して、所定のツール（ブラウザなど）又は所定のコマンドを用いて設定・変更を行うことができる。
【００６２】
なお、上記機器照合用情報３１に登録される機器２００は、機器管理装置１００で管理する管理対象機器である。よって、上記「ＩＰアドレス」及び上記「ホスト名」は、管理対象機器のネットワーク設定情報にあたり、上記「ＭＡＣアドレス」は、管理対象機器を特定する情報（管理対象機器特定情報）にあたる。
【００６３】
本実施形態では、後述する機器特定部２４が、上記機器照合情報３１を用いて、機器２００の特定を行う。
【００６４】
次に、機器情報取得部２３は、機器２００から機器情報を取得する。上述したように、機器２００からの機器情報の取得は、主に、ポーリングとＴｒａｐの２つがある。本実施形態では、Ｔｒａｐにより機器２００から機器情報が送信される場合を想定している。よって、機器情報取得部２３は、機器２００から送信されたメッセージを受信することで、メッセージ内の機器情報を取得する。また、機器情報取得部２３は、機器情報取得時に、機器２００から送信されたメッセージ内のＩＰアドレスも取得する。このＩＰアドレスは、ネットワーク管理装置４００から機器２００に割り当てられたアドレスである。すなわち、送信元のネットワーク設定情報である。
【００６５】
このようにして、機器管理装置１００は、機器２００から機器情報を取得するが、ポーリングによる情報取得と異なり、機器管理装置１００から情報取得要求を行い、その応答として機器２００から情報を受信しているわけではない。
【００６６】
そのため、ＩＰアドレスが変更される可能性のあるネットワーク環境下では、受信した機器情報を、どの機器２００の機器管理用データとして取り扱えばよいか判断できない。そのため、正しく判断するためには、機器管理装置１００において、送信元の機器２００を特定する必要がある。そこで、機器管理装置１００は、管理対象機器判定部２４、判定情報変換部２５、セキュリティレベル取得部３６、及び機器特定部２７を有している。
【００６７】
管理対象機器判定部２４は、機器２００が管理対象機器であるか否かの可能性を判定する。管理対象機器判定部２４は、機器照合情報保持部２２で保持する機器照合情報３１にアクセスし、機器情報取得部２３により取得したＩＰアドレスを基に、該当した登録ＩＰアドレスが存在するか否かを確認する。すなわち、送信元のネットワーク設定情報を基に、該当する管理対象機器のネットワーク設定情報が機器照合情報３１に含まれているかを確認する。このとき、該当ＩＰアドレスが存在した場合に、機器２００が管理対象機器の可能性があると判断する。一方、該当ＩＰアドレスが存在しない場合に、機器２００が非管理対象機器の可能性（管理対象機器でない可能性）があると判断する。
【００６８】
また、管理対象機器判定部２４は、ＩＰアドレス以外でも、ホスト名を基に、該当した登録ホスト名が存在するか否かを確認できる。これは、ＩＰアドレスを基に、機器２００が管理対象機器であるか否かの可能性を判断し、非管理対象機器の可能性があると判断された場合、次の段階として、ホスト名を基に、再び判断する。これら２つの判定条件を基に、機器２００が管理対象機器であるか否かの可能性を判定する。
【００６９】
そのため、本実施形態では、判定条件であるＩＰアドレスをホスト名へ変換する判定情報変換部２５を有している。
【００７０】

判定情報変換部２５は、ＩＰアドレスをホスト名に変換する。その変換方法は、例えば、ＤＮＳ逆引きにより変換できる。つまり、ＩＰアドレスの入力があるとＤＮＳサーバと呼ばれるコンピュータを参照し、ＩＰアドレスに対応する登録ホスト名を検索する。これにより、ホスト名を取得する。

【００７１】

このようにして、判定情報変換部２５により変換されたホスト名は、管理対象機器判定部２４に渡され、管理対象機器判定部２４が、再び管理対象機器か否かの可能性を確認する。

【００７２】

続いて、管理対象機器判定部２４により、機器２００が管理対象機器であると判断された場合には、機器２００に合わせたセキュリティレベルに従って、情報送信元である機器２００を特定するための機器特定情報を取得する。

【００７３】

そのため、本実施形態では、機器２００に設定されているセキュリティレベル情報を取得するセキュリティレベル取得部２６を有している。

【００７４】

セキュリティレベル取得部２６は、管理対象機器判定部２４により管理対象機器と判断された機器２００から、現在機器２００に設定されているセキュリティレベル情報を取得する。その取得方法は、機器２００からの取得ＩＰアドレスを基に、ＳＮＭＰのコマンド（Ｇｅｔコマンドなど）を用いて情報取得要求を行い、機器２００からの応答を受信することで取得する。

【００７５】

このようにして、セキュリティレベル取得部２６により取得されたセキュリティレベル情報は、後述する機器特定部２７に渡され、機器特定部２７が、セキュリティレベル情報に示すセキュリティレベルに従って、情報送信元である機器２００から機器特定情報を取得する。

【００７６】

機器特定部２７は、情報送信元の機器２００が管理対象機器であるか又は非管理対象機器であるかを特定する。また、情報送信元の機器２００が管理対象機器であった場合に、管理対象機器として登録されてから以降に割り当てられたＩＰアドレス（送信元のネットワーク設定情報）が変更されているか否かを判断する。

【００７７】

なお、上述したように、管理対象機器判定部２４では、ＩＰアドレス又はホスト名によって、情報送信元の機器２００が管理対象機器であるか否かの可能性を判定している。しかし、判定の際に用いる情報が、ネットワーク環境下において必ずしも不変な情報でないことから、あくまでもこの段階では管理対象機器であるか否かの可能性を判定している。

【００７８】

そこで、機器２００が管理対象機器であるか否かの特定は、機器特定部２７により行う。このように段階的な判定機能を有する理由として、情報送信元の機器２００から機器特定情報を取得することなく、非管理対象機器を特定できる点が挙げられる。具体的には、情報送信元である機器２００のＩＰアドレス及びホスト名両方のデータが、機器照合情報３１内に存在しなければ、機器２００が非管理対象機器２００であると特定できるためである。

【００７９】

（機器の特定）

機器特定部２７は、まず、機器情報取得部２３により取得した送信元のＩＰアドレスを基に、情報送信元の機器２００から機器特定情報を取得する。機器特定情報は、例えば、ＳＮＭＰのコマンド（Ｇｅｔコマンド）を用いて情報取得要求を行うことで、機器２００から取得することができる。

【００８０】

続いて、機器特定部２７は、取得した機器特定情報（例えば「機器２００の取得ＭＡＣアドレス」）と、上述した機器照合情報保持部２２で保持する管理対象機器特定情報（例えば「管理対象機器の登録ＭＡＣアドレス」）とを基に、機器情報を送信した機器２００を特定する。機器照合情報３１には、現在、機器管理装置１００が管理する管理対象機器のＭＡＣアドレスが含まれており、ＩＰアドレス（管理対象機器のネットワーク設定情報）に対応付けられている。

【００８１】

よって、機器情報取得部２３により取得した送信元のＩＰアドレスを基に、機器照合情報３１のＭＡＣアドレス項目を参照し、該当した登録ＭＡＣアドレスと、機器２００の取得ＭＡＣアドレスとを照合（比較）する。

【００８２】

このとき、ＭＡＣアドレス同士が一致すれば、たとえＩＰアドレスが異なっていても、機器２００が管理対象機器であると特定できる。一方、ＭＡＣアドレス同士が不一致であれば、機器照合情報３１の中に、機器２００の取得ＭＡＣアドレスと一致する該当ＭＡＣアドレスが存在するか否かを判定する。その結果、一致するＭＡＣアドレスが存在しなければ、情報送信元の機器２００が非管理対象機器（現在、管理対象となっていない機器）であると特定できる。また、上記機器照合情報３１参照において、取得ＩＰアドレスに対応付けられた該当ＭＡＣアドレスが存在しなかった場合には、情報送信元である機器２００の取得ＭＡＣアドレスと一致する該当ＭＡＣアドレスが存在するか否かを判定する。

【００８３】

このように、機器管理装置１００は、機器２００（又は機器２００が備えるネットワークＩ／Ｆ装置）においてハードウェア固有の不変な情報に基づき、情報送信元の機器２００を特定する。

【００８４】

（ＩＰアドレスの変更）

また、機器特定部２７では、上記照合においてＭＡＣアドレス同士が不一致であった場合に、機器２００に割り当てられるＩＰアドレス（送信元のネットワーク設定情報）が変更されたものと判断する。

【００８５】

以上のように、機器管理装置１００は、機器特定部２７により、機器２００の管理対象機器又は非管理対象機器を特定し、さらに管理対象機器であった場合には、割り当てられたＩＰアドレスが変更されているか否かも判断する。これにより、管理対象機器でＩＰアドレスが変更されている場合には、機器情報の更新とともに機器照合情報３１も更新する。また、非管理対象機器であった場合には、新たな管理対象とするか否かを確認後、管理者を含むユーザからの指示に従って、機器情報及び機器照合情報３１を追加・更新する。

【００８６】

機器特定部２７からの指示に従って、これらの情報更新や更新確認などを以下の各機能部が行う。

【００８７】

機器照合情報更新部２９は、機器照合情報保持部２２が保持する機器照合情報３１を更新する。機器照合情報３１は、ＩＰアドレス、ホスト名、ＭＡＣアドレス、及びＳＮＭＰ通信設定が含まれている。よって、機器照合情報更新部２９は、機器特定部２７により、管理対象機器のＩＰアドレスが変更されたと判断された場合、ＩＰアドレスとＭＡＣアドレスとの対応付けを更新する。また、機器特定部２７により、非管理対象機器として特定された場合、ＩＰアドレスやＭＡＣアドレスなどを含む新たな機器照合用データを追加する。

【００８８】

また、機器特定部２７により機器２００が管理対象機器と特定された場合や、機器照合情報更新部２９により機器照合用データの追加・更新が行われた場合などには、受信データ処理部２８に、機器２００に対応する機器管理データの更新が各機能部から指示される

。
【００８９】
受信データ処理部２８は、当該機器管理装置１００が管理する機器管理用データを更新する。機器管理装置１００では、管理対象機器から取得した機器情報を機器管理用データとして管理することで、各管理対象機器の動作状態を監視する。よって、受信データ処理部２８は、機器特定部２７により管理対象機器として特定した機器２００からの機器情報を基に、対応する機器管理用データを更新する。また、受信データ処理部２８は、機器２００が非管理対象機器と特定された場合には、機器２００からの機器情報である受信データを破棄する。
【００９０】
このように、本実施形態に係る機器管理機能は、上記各機能部が連係動作することにより実現される。
【００９１】
《機能動作》
以下に、機器管理機能の詳細な動作（機能部群の連係動作）について、処理手順を示すフローチャートを用いて説明する。
【００９２】
機器管理機能は、機器管理装置１００に搭載（インストール）される機器管理プログラム（ソフトウェア部品）が、ＣＰＵ１０６により、格納先（例えば「ＲＯＭ１０５」など）からＲＡＭ１０４上に読み出され、以下の処理が実行されることで実現される。
【００９３】
図５は、本実施形態に係るＳＮＭＰ通信を行う処理手順例を示すフローチャートである。つまり、Ｔｒａｐにより機器２００から機器管理装置１００に対して機器情報が送信された場合の処理手順である。
【００９４】
図５に示すように、機器管理装置１００は、機器情報取得部２３により、機器２００からのＴｒａｐを受信する（ステップＳ１０１）。このとき受信するメッセージが機器２００からの機器情報にあたり、Ｔｒａｐにより送信される機器情報は、主に、機器２００で発生した障害についてのエラー通知である。
【００９５】
また、機器情報取得部２３は、機器情報受信時のメッセージに含まれる送信元のＩＰアドレスを取得する（ステップＳ１０２）。つまり、Ｔｒａｐにより機器情報を送信した機器２００のＩＰアドレスを取得する。これにより、機器照合用データである機器２００のＩＰアドレスを取得することができる。
【００９６】
このように、機器情報取得部２３は、機器２００から機器情報及びＩＰアドレスを受信すると、管理対象機器判定部２４に受信した旨を通知する。
【００９７】
続いて、機器管理装置１００は、管理対象機器判定部２４が、機器照合情報保持部２２が保持する機器照合情報３１を参照し、ステップＳ１０２において取得したＩＰアドレスを基に、機器２００が管理対象機器か否かを確認する（ステップＳ１０３）。具体的には、機器照合情報３１のＩＰアドレス項目を参照し、取得ＩＰアドレスが、項目内に存在するか否かを判定する。つまり、取得ＩＰアドレスに対応する機器２００が、管理対象機器として機器照合情報３１に登録されているか否かを判定する。項目内に存在すれば、取得ＩＰアドレスは管理対象機器のＩＰアドレスとして登録されていることから、機器２００が管理対象機器であると判断できる。一方、項目内に存在しなければ、取得ＩＰアドレスは管理対象機器のＩＰアドレスとして登録されていないことから、機器２００が管理対象機器でない可能性があると判断できる。
【００９８】
ステップＳ１０３において、機器２００が管理対象機器であることが確認されると（ス

テップＳ１０４：ＹＥＳ）、機器管理装置１００は、セキュリティレベル取得部２６により、機器２００からＳＮＭＰ通信時のセキュリティレベルに関する情報を取得する（ステップＳ１０５）。具体的には、取得ＩＰアドレスを基にＳＮＭＰのコマンドを用いて、管理対象機器と判断した機器２００から、現在、機器２００に設定されているＳＮＭＰ通信時のセキュリティレベルに関する情報を取得する。

【００９９】

ＳＮＭＰでは、バージョンによって、通信時のセキュリティレベルが異なる。よって、ステップＳ１０５において取得する情報は、バージョンによって異なる。

【０１００】

そこで、セキュリティレベル取得部２６は、まず、機器２００がサポートするＳＮＭＰのうち、最も新しいバージョンに関する情報を取得する。その結果、取得したバージョンからＳＮＭＰで主に用いられている３つのバージョン（ｖ１，ｖ２ｃ，ｖ３）のうち、どのバージョンかを特定する。

【０１０１】

このとき、特定したバージョンがＳＮＭＰｖ１又はｖ２ｃであった場合には、コミュニティ名などの情報を取得する。なお、ここで言う「コミュニティ」とは、ＳＮＭＰが管理するネットワークシステムの範囲を表し、コミュニティ名は、そのコミュニティの権限に紐づいたパスワードの役割を果たす。例えば、ＳＮＭＰマネージャ及びエージョンは、コミュニティ名が一致していないと通信することができない。

【０１０２】

また、特定したバージョンがＳＮＭＰｖ３であった場合には、noAuthNoPriv（認証も暗号化もしない）、authNoPriv（認証するが暗号化はしない）、authPriv（認証も暗号化もする）などの各セキュリティレベルの設定値を取得する。また、これらのセキュリティレベルに応じて、認証方法（ＭＤ５（Message Digest Algorithm 5）又はＳＨＡ（Secure Hash Algorithm））や暗号化プロトコル（ＤＥＳ（Data Encryption Standard）又はＡＥＳ（Advanced Encryption Standard））などの情報を取得する。

【０１０３】

このように、セキュリティレベル取得部２６は、機器管理装置１００と機器２００との間のデータ通信を、機器２００がサポートするＳＮＭＰバージョンのうち、最もセキュリティレベルの高いバージョンを用いて行うための情報を取得する。

【０１０４】

続いて、機器管理装置１００は、機器特定部２７が、取得ＩＰアドレスを基にＳＮＭＰのコマンドを用いて、管理対象機器と判断した機器２００から、ＭＡＣアドレス（機器２００の機器特定情報）を取得する（ステップＳ１０６）。具体的には、機器２００に、ＭＡＣアドレスの取得要求を行い、機器２００からの応答を受信することでＭＡＣアドレスを取得する。例えば、ＳＮＭＰのＧｅｔコマンドにより、ＩＰグループ又はＩｎｔｅｒｆａｃｅグループに定義されるＭＡＣアドレスのＭＩＢオブジェクト値のＯＩＤを指定し、情報取得要求を行うことで応答を受信する。これにより、機器照合用データである機器２００のＭＡＣアドレスを取得することができる。

【０１０５】

続いて、機器特定部２７は、機器照合情報３１を参照し、ステップＳ１０６において取得したＭＡＣアドレスを基に、該当するＭＡＣアドレスを検索する（ステップＳ１０７）。つまり、検索結果に基づき、取得ＭＡＣアドレスに対応する機器２００が、管理対象機器として機器照合情報３１に登録されているか否かを判定する。

【０１０６】

ステップＳ１０７において、該当データがある場合には（ステップＳ１０８：ＹＥＳ）、機器特定部２７が、機器２００からの取得ＭＡＣアドレスと、機器照合情報３１において取得ＩＰアドレスに対応付けられた該当ＭＡＣアドレスとが一致するか否かを確認する（ステップＳ１０９）。

【０１０７】

ステップＳ１０９において、一致することが確認されると（ステップＳ１１０：ＹＥＳ）、機器特定部２７が、機器２００が管理対象機器であると特定する。さらに、管理対象機器のＩＰアドレスが変更されていないと判断する。

【０１０８】

その結果、機器管理装置１００は、受信データ処理部２８により、Ｔｒａｐを受信した機器２００を管理対象機器として処理する（ステップＳ１１１）。具体的には、受信データ処理部２８が、取得ＩＰアドレスに対応する機器２００の機器情報を、受信した機器情報（最新情報）に基づき更新する。

【０１０９】

一方、ステップＳ１０３において、機器２００が管理対象機器でない可能性があることが確認された場合（ステップＳ１０４：ＮＯ）、又は、ステップＳ１０９において、ＭＡＣアドレスが一致しないことが確認された場合には（ステップＳ１１０：ＮＯ）、機器管理装置１００が、判定情報変換部２５により、取得ＩＰアドレスを対応ホスト名に変換する（ステップＳ１１２）。

【０１１０】

上記処理の中では、機器２００が管理対象機器か否かの判定を、機器情報受信時の取得ＩＰアドレスに基づき行っていた。しかし、ステップＳ１０４のＩＰアドレス登録確認やステップＳ１１０のＭＡＣアドレス照合確認などを行っても、機器２００が管理対象機器と特定できない場合がある。そのため、管理対象機器か否かの判定条件、つまり、判定時に用いる取得ＩＰアドレスを、同様に判定時に用いることが可能な他の情報に変換し、改めて、機器２００が管理対象機器か否かの判定を行う。

【０１１１】

そこで、判定情報変換部２５は、ネットワーク管理装置４００へアクセスし、取得ＩＰアドレスを基に、ＩＰアドレスに対応するホスト名を取得する。例えば、ＤＮＳ逆引きにより、ＩＰアドレスに対応するホスト名を調査する（名前解決する）。これにより、機器照合用データである機器２００のホスト名を取得することができる。

【０１１２】

機器管理装置１００は、管理対象機器判定部２４が、機器照合情報３１を参照し、ステップＳ１１２において変換したホスト名を基に、機器２００が管理対象機器か否かを確認する（ステップＳ１１３）。具体的には、機器照合情報３１のホスト名項目を参照し、変換後ホスト名が、項目内に存在するか否かを判定する。つまり、変換後ホスト名に対応する機器２００が、管理対象機器として機器照合情報３１に登録されているか否かを判定する。項目内に存在すれば、変換後ホスト名は管理対象機器のホスト名として登録されていることから、機器２００が管理対象機器であると判断できる。一方、項目内に存在しなければ、変換後ホスト名は管理対象機器のホスト名として登録されていないことから、機器２００が管理対象機器でない可能性があると判断できる。

【０１１３】

ステップＳ１１３において、機器２００が管理対象機器であることが確認されると（ステップＳ１１４：ＹＥＳ）、機器管理装置１００では、ステップＳ１１５からＳ１２０までの各処理手順が実行される。なお、ステップＳ１１５からＳ１２０の各処理手順は、上述したステップＳ１０５からＳ１１０の各処理手順と同様である。よって、詳細な説明は便宜省略し、ステップＳ１２０以降の処理手順について説明する。

【０１１４】

ステップＳ１１９において、一致することが確認されると（ステップＳ１２０：ＹＥＳ）、機器特定部２７が、機器２００が管理対象機器であると特定する。さらに、管理対象機器のＩＰアドレスが変更されていると判断する。

【０１１５】

その結果、機器管理装置１００は、機器照合情報更新部２９により、機器照合情報保持部２２にアクセスし、機器照合情報３１を更新する（ステップＳ１２１）。具体的には、機器照合情報３１を参照後に、取得ＩＰアドレス、変換後ホスト名、及び取得ＭＡＣアド

レスなどの各データを基に、機器照合情報３１における機器２００の該当照合用データを更新する。

【０１１６】

機器管理装置１００は、機器照合情報３１を最新状態に更新すると、ステップＳ１１１の処理手順へ移行する。

【０１１７】

また、ステップＳ１０８及ぶＳ１１８において、機器参照情報３１に該当データ（取得ＭＡＣアドレス）がない場合（ステップＳ１０８及びＳ１１８：ＮＯ）、又は、ステップＳ１１９において、ＭＡＣアドレスが一致しないことが確認された場合には（ステップＳ１２０：ＮＯ）、機器管理装置１００が、機器特定部２７により、機器２００が管理対象機器でない（非管理対象機器である）と特定する。

【０１１８】

その結果、機器管理装置１００は、受信データ処理部２８により、Ｔｒａｐを受信した機器２００を非管理対象機器として処理する（ステップＳ１２２）。具体的には、受信データ処理部２８が、受信した機器情報を破棄し、管理対象機器の機器情報を更新しない。

【０１１９】

＜まとめ＞

以上のように、本実施形態に係る機器管理装置１００によれば、送信元のＩＰアドレスから機器特定情報を取得し、取得した機器特定情報に基づき、機器情報を送信した機器２００を特定し、特定した機器２００が管理対象機器であった場合、受信した機器情報を基に該当する管理対象機器の機器情報を更新する。

【０１２０】

その中で、機器管理装置１００では、送信元のＩＰアドレスを基に機器２００から機器２００に設定された通信時のセキュリティレベルを示す情報を取得し、取得した情報に示されるセキュリティレベルに従って、機器特定情報を取得している。

【０１２１】

これによって、機器管理装置１００は、ネットワーク設定が自動的に行われる環境下において機器２００に割り当てられるＩＰアドレスが変更されても、セキュリティを意識した通信方法で、機器情報を送信した機器２００を特定することができる。その結果、受信した機器情報を機器管理用データとして取り扱うことができ、機器管理を正常に行うことができる。

【０１２２】

ここまで、上記実施形態の説明を行ってきたが、上記実施形態に係る機器管理装置１００が有する「機器管理機能」は、図を用いて説明を行った各処理手順を、動作環境（プラットフォーム）にあったプログラミング言語でコード化したプログラムが、ＣＰＵ１０６により実行されることで実現される。

【０１２３】

上記プログラムは、コンピュータが読み取り可能な記録媒体１０３ａに格納することができる。記録媒体１０３ａには、例えば、フロッピー（登録商標）ディスク、ＣＤ（Compact Disk）、及びＤＶＤ（Digital Versatile Disk）、ならびにＳＤメモリカード（SD Memory Card）及びＵＳＢ（Universal Serial Bus）メモリなどがある。

【０１２４】

よって、上記プログラムは、記録媒体１０３ａを読み取り可能なドライブ装置１０３や外部記憶Ｉ／Ｆ（非図示）などを介して機器管理装置１００にインストールすることができる。また、機器管理装置１００は、インタフェース装置１０７を備えていることから、インターネットなどの電気通信回線を用いて上記プログラムをダウンロードし、インストールすることもできる。

【０１２５】

また、上記実施形態では、機器管理装置１００と異なる装置（ネットワーク管理装置４００）が、ＤＨＣＰ・ＤＮＳの各機能を搭載している構成を例に説明を行ったが、この限

りでない。例えば、機器管理装置１００が、上記ＤＨＣＰ・ＤＮＳの各機能を搭載する構成であってもよい。

【０１２６】

また、上記実施形態では、機器特定情報３１を、機器管理装置１００が備える記憶装置（例えば「ＨＤＤ１０８」など）に保持する構成（機器特定情報保持部２２を有する構成）について説明を行ったが、この限りでない。例えば、機器管理装置１００が外部記憶Ｉ／Ｆ装置（非図示）を備えていれば、上記ＳＤメモリカード（SD Memory Card）及びＵＳＢ（Universal Serial Bus）メモリなどを含む記録媒体１０３ａが保持する構成であってもよい。さらに、機器管理装置１００が備えるインタフェース装置１０７を介して、所定のデータ伝送路９０により接続される外部装置が保持する構成であってもよい。

【０１２７】

最後に、上記実施形態に挙げた形状や構成に、その他の要素との組み合わせなど、ここで示した要件に、本発明が限定されるものではない。これらの点に関しては、本発明の主旨をそこなわない範囲で変更することが可能であり、その応用形態に応じて適切に定めることができる。

【符号の説明】

【０１２８】

１　機器管理システム
２１　機器照合用データ取得部
２２　機器照合情報保持部
２３　機器情報取得部
２４　管理対象機器判定部
２５　判定情報変換部
２６　セキュリティレベル取得部
２７　機器特定部
２８　受信データ処理部
２９　機器照合情報更新部
３１　機器照合情報
９０　データ伝送路
１００　機器管理装置（機器管理サーバ）
１０１　入力装置
１０２　表示装置
１０３　ドライブ装置（ａ：記録媒体）
１０４　ＲＡＭ（揮発性の半導体メモリ）
１０５　ＲＯＭ（不揮発性の半導体メモリ）
１０６　ＣＰＵ（中央処理装置）
１０７　インタフェース装置（ＮＩＣ：Network I/F Card）
１０８　ＨＤＤ（不揮発性の記憶装置）
２００　機器（画像処理装置：管理対象／非管理対象を含む）
３００　クライアントＰＣ（情報処理装置）
４００　ネットワーク管理装置（ＤＨＣＰ・ＤＮＳサーバ）

【先行技術文献】

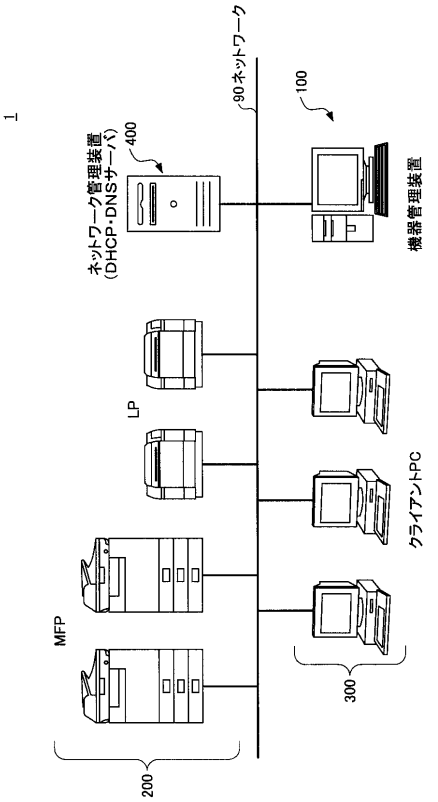
【特許文献】

【０１２９】

【特許文献１】特開２００３－２９６２０６号公報

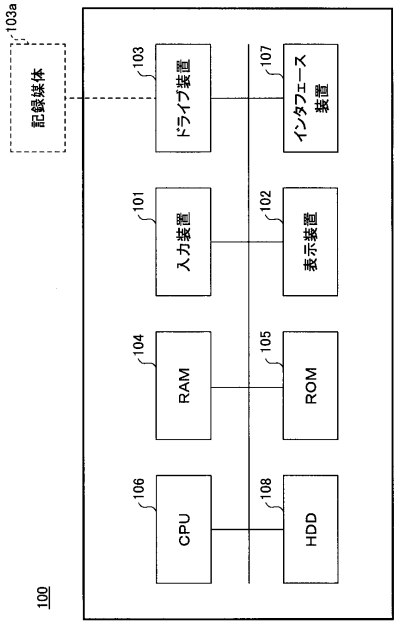
【図１】

本発明の第1の実施形態に係る機器管理システムの構成例を示す図



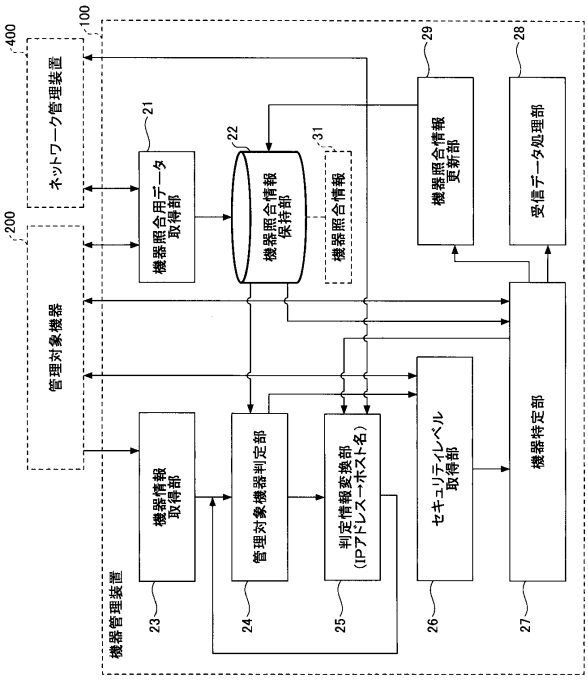
【図２】

本発明の第1の実施形態に係る機器管理装置のハードウェア構成例を示す図



【図３】

本発明の第1の実施形態に係る機器管理装置が有する機能構成例を示す図



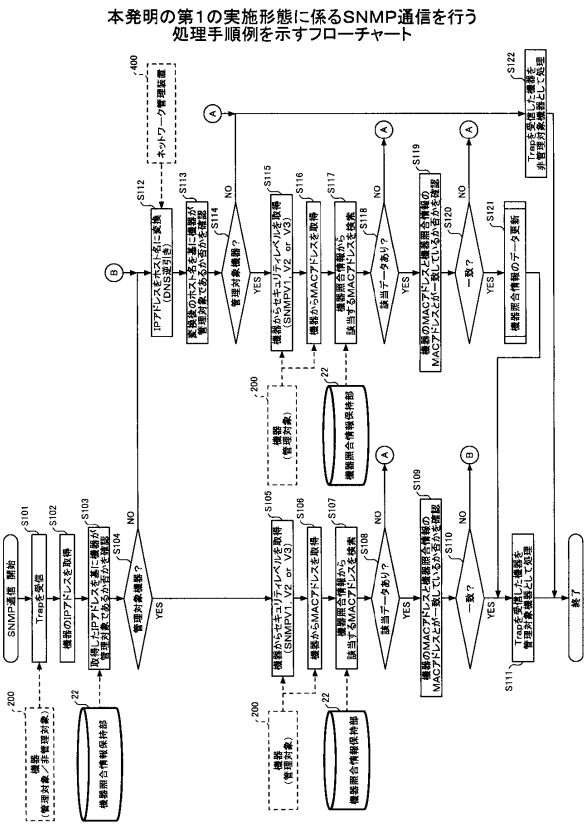
【図４】

本発明の第1の実施形態に係る機器照合情報のデータ例を示す図

31

IPアドレス	ホスト名	MACアドレス
192. 168. 11. 1	MFP01	00:d0:50:XX:XX:XX
192. 168. 11. 2	MFP02	0a:50:b7:XX:XX:XX
192. 168. 11. 3	MFP03	00:a1:23:XX:XX:XX
192. 168. 11. 4	MFP04	00:a0:c9:XX:XX:XX
.....	.....	.....

【図５】


本発明の第1の実施形態に係るSNMP通信を行う
処理手順例を示すフローチャート
SNMP通信 開始
Trapを受信
機器のIPアドレスを取得
取得したIPアドレスを基に機器が管理対象であるか否かを確認
管理対象機器？
YES
NO
機器（管理対象／非管理対象）
機器照合情報保持部
機器からセキュリティレベルを取得（SNMPV1、V2 or V3）
機器からSNMPアドレスを取得
機器照合情報から該当するMACアドレスを検索
該当データあり？
機器（管理対象）
IPアドレスをホスト名に変換（DNS逆引き）
ネットワーク管理装置
実機器のホスト名を基に機器が管理対象であるか否かを確認
機器のMACアドレスと機器照合情報のMACアドレスが一致しているか否かを確認
一致？
機器照合情報のデータ更新
Trapを受信した機器を管理対象機器として処理
Trapを受信した機器を非管理対象機器として処理
終了
A
B

フロントページの続き

(56)参考文献 特開２００５－２９３１１０（ＪＰ，Ａ）
特開２００３－１２２６５０（ＪＰ，Ａ）
特開２００４－０９４９１９（ＪＰ，Ａ）
特開２００４－３６４１９０（ＪＰ，Ａ）
特開２００７－２５７５２５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００