

明 細 書

発明の名称： 機器保守管理システム

技術分野

[0001] 本開示は、複数の機器の情報を集積する遠隔処理装置を備えた機器保守管理システムに関する。

背景技術

[0002] 従来、機器保守管理システムは、複数の機器（例えば、空調機器）の情報を、管理センタで一元管理し、機器の故障が発生する前に修理又は交換を行う。このような機器保守管理システムにおいて、クラウドサービスを提供するサーバにより、複数の建物に設置された複数の機器の消費電力又は電力波形のデータを取得するものがある（例えば、特許文献 1 参照）。特許文献 1 に開示される機器保守管理システムのサーバは、取得した機器毎のデータから機器の劣化状況を評価し、修理又は交換の優先度を設定する構成とされる。

先行技術文献

特許文献

[0003] 特許文献 1：国際公開第 2 0 1 7 / 0 4 7 7 2 1 号

発明の概要

発明が解決しようとする課題

[0004] 特許文献 1 に開示される機器保守管理システムでは、複数の機器の情報は管理センタで一括管理されている。このため、機器の使用者又は保守業者といった特定の機器の情報を使用する者が、他の機器の情報を閲覧できてしまう場合があり、情報セキュリティを担保できないという課題があった。

[0005] 本開示は、上記のような課題を解決するためになされたもので、情報セキュリティを担保しつつ、特定の機器の情報使用者に必要な情報を提供できる機器保守管理システムを提供することを目的とする。

課題を解決するための手段

[0006] 本開示に係る機器保守管理システムは、自己の運転及び異常の有無に関する情報を送信する複数の機器と、複数の前記機器のそれぞれの前記情報を取得して記憶する遠隔処理装置と、を備え、前記遠隔処理装置は、主従関係を有する少なくとも一種類の認証鍵を用いて通信を制限するものであり、複数の前記機器の少なくとも一部の機器について主となる前記認証鍵が予め付与された第一の通信機器、及び、前記第一の通信機器の従となる前記認証鍵が予め付与された第二の通信機器のそれぞれを通信相手として通信を行い、通信を行う際、前記通信相手が有する前記認証鍵の種類及び前記主従関係に応じて、提供する前記情報の範囲を決定する。

発明の効果

[0007] 本開示によれば、遠隔処理装置の通信相手が有する認証鍵の種類、特定の認証鍵の有無、及び認証鍵の主従関係に応じて、通信相手に情報を提供する対象機器、及び情報の開示レベルを違えることができる。したがって、情報セキュリティを担保しつつ、通信相手に必要な情報を提供できる。

図面の簡単な説明

[0008] [図1]実施の形態1に係る機器保守管理システムを示す概略構成図である。
[図2]実施の形態1に係る機器保守管理システムの一例を示す図である。
[図3]実施の形態1に係る機器保守管理システムの遠隔処理装置の機能を示す機能ブロック図である。
[図4]図2の例において所有者及び使用者が有する認証鍵と機器との関係を示す図である。
[図5]図2の例において認証鍵で取得可能な情報の範囲を示す図である。
[図6]実施の形態2に係る機器保守管理システムの一例を示す図である。
[図7]図6の例において使用者と提供先と管理者がそれぞれ有する認証鍵の関係を示す図である。
[図8]図6の例において認証鍵で取得可能な情報の範囲を示す図である。
[図9]実施の形態3に係る機器保守管理システムにおける認証鍵交換の様子を示す図である。

[図10]図9に示す認証鍵交換の前及び後における所有者及び使用者が有する認証鍵と機器との関係を示す図である。

[図11]実施の形態3に係る機器保守管理システムにおける認証鍵置換の様子を示す図である。

[図12]図11に示す認証鍵置換の前及び後における所有者及び使用者が有する認証鍵と機器との関係を示す図である。

[図13]実施の形態3に係る交換要求の処理を示すフローチャートである。

[図14]実施の形態3に係る置換要求の処理を示すフローチャートである。

[図15]実施の形態4に係る機器保守管理システムにおける変更認否設定を説明する図である。

[図16]実施の形態5に係る機器保守管理システムの一例を示す図である。

[図17]図16の機器保守管理システムにおける視覚化手段の一例を示す図である。

[図18]図16の機器保守管理システムにおいて検索符号と認証鍵と各種情報との関係を示す図である。

発明を実施するための形態

[0009] 実施の形態1.

図1は、実施の形態1に係る機器保守管理システムを示す概略構成図である。機器保守管理システム100は、例えば複数の店舗を有するコンビニエンスチェーン、又は多様な施設を含む商業ビル等に設置された複数の機器1の情報を収集し、収集した情報を、一定の条件のもとで提供するものである。図1に示されるように、機器保守管理システム100は、複数の機器1と、クラウド等の遠隔処理装置2とを備える。図1を参照して、機器保守管理システム100の概略構成について説明する。

[0010] 機器1は、例えば、ルームエアコン、給湯器、テレビ、及び冷蔵庫といった家庭用家電、又は、業務用空調機及びチラーといった業務用機器である。図1に示される例では、機器保守管理システム100には、ルームエアコン及び給湯器といった複数の種類の機器1が含まれる。なお、機器保守管理シ

ステム１００は、単一の種類の機器を複数台備える構成であってもよい。

[0011] 機器１は、通信手段を備え、予め決められた時間ごとに遠隔処理装置２にデータを送信する定期通信を行う。また機器１は、遠隔処理装置２及び通信機器２０ｂ（例えば、スマートフォン）といった外部からの要求に応じて通信を実施する。具体的には、機器１は、遠隔処理装置２に対して、自己の運転及び異常の有無に関する情報を送信する。機器１の通信手段は、例えば、Wi-Fi、LTE（Long Term Evolution）、5G、又はBluetooth（登録商標）といった規格に従って無線通信を行う通信インターフェース等で構成される。なお、機器１の通信手段は上記のものに限定されず、例えば、ADSLといった電話回線、有線LAN（Local Area Network）又はPLC（Programmable Logic Controller）等でもよい。

[0012] 遠隔処理装置２は、機器１の情報を収集し、収集した情報の分析及び提供を行うものである。遠隔処理装置２は、例えば、クラウドサービスを提供するクラウドサーバ等で構成される。より具体的には、遠隔処理装置２は、一台又は複数台のコンピュータで構成される。遠隔処理装置２を構成するコンピュータの台数は、必要とされる演算処理及び通信負荷等に応じて決定されるとよい。

[0013] 遠隔処理装置２は、複数の機器１と通信し、各機器１の情報を収集する。機器１の情報には、例えば、機器１の運転情報、及び機器１の異常の有無といった情報が含まれる。また遠隔処理装置２は、遠隔処理装置２の管理者６が所有する通信機器２０ａ（図６）と通信し、複数の機器１の情報を送信する。また遠隔処理装置２は、機器１の所有者３及び機器１の使用者４がそれぞれ所有する通信機器２０ｂと通信し、収集した複数の機器１に関する情報を、例えば保守業者又はサービス業者といった提供先５に、一定の制限のもとで開示する。

[0014] 遠隔処理装置２は、認証機能を有し、複数の機器１から収集した情報を、遠隔処理装置２の管理者６、機器１の使用者４、及び機器１の所有者３、及

び提供先 5 といった通信相手がそれぞれ有する認証鍵 30 に応じて開示する。遠隔処理装置 2 による認証には、主従関係を有する認証鍵 30 が使用される。情報開示の対象となる機器 1、及び、情報の開示レベルといった提供する情報の範囲は、遠隔処理装置 2 の通信相手に予め付与されている認証鍵 30 の種類及び主従関係に基づいて決定される。遠隔処理装置 2 には、遠隔処理装置 2 の管理者 6、機器 1 の使用者 4、及び機器 1 の所有者 3、及び提供先 5 の情報が記憶されている。遠隔処理装置 2 は、遠隔処理装置 2 の管理者 6、機器 1 の使用者 4、及び機器 1 の所有者 3、及び提供先 5 の情報を記憶する際に、これらの者に対して認証鍵 30 を付与する。

[0015] 遠隔処理装置 2 は、収集した各機器 1 の情報を分析し、分析結果に応じて、その機器 1 に運転の中断、再開又は非常停止等を行わせる指令を送信する。例えば、特定の機器 1 の情報を分析して、不良又は故障が生じていると判定された場合には、遠隔処理装置 2 は、その機器 1 に対して運転の中断の指令を送信する。

[0016] 所有者 3 は、機器 1 の所有者であって、機器 1 が設置された場所にいなくてもよい。所有者 3 は、複数の機器 1 の所有者となり得る。図 1 に示される例では、所有者 3 は、4 台の機器 1 の所有者とされている。

[0017] 使用者 4 は、機器 1 の使用者であって、所有者 3 と同一人物でもよい。また、使用者 4 は、複数の所有者 3 が所有する複数の機器 1 の所有者となり得る。

[0018] 提供先 5 は、遠隔処理装置 2 から機器 1 に関する情報を取得して活用する、例えば、保守業者又はサービス業者である。保守業者とは、機器 1 の保守及び点検等を実施する業者である。サービス業者とは、機器 1 に関する情報を元に、機器 1 とサービス業者のサービス（例えば、消費電力のマネジメントサービス、又は、健康に関するライフサポートサービス）とを連携させるものである。保守業者及びサービス業者はそれぞれ、ギグワークのような個人事業主でも構わない。

[0019] 本開示において、機器 1 について主となる認証鍵 30 が予め付与された通

信機器 20 a 又は 20 b を第一の通信機器と称し、第一の通信機器の従となる認証鍵 30 が予め付与された通信機器 20 a 又は 20 b を第二の通信機器と称する。すなわち、同じ種類の認証鍵 30 が割り当てられた第一の通信機器及び第二の通信機器のうち、第一の通信機器は、第二の通信機器よりも強い権限を有する。

[0020] 一般的には、遠隔処理装置 2 の管理者 6 及び機器 1 の所有者 3 に対して、機器 1 の使用者 4 及び情報の提供先 5 よりも上位の権限が与えられる。この場合、管理者 6 が有する通信機器 20 a 及び所有者 3 が有する通信機器 20 b 等を第一の通信機器とし、使用者 4 が有する通信機器 20 b 及び提供先 5 が有する通信機器 20 b 等を第二の通信機器とすることができる。

[0021] ところで、機器 1 の使用者 4 が長期に渡って機器 1 を使用する場合、機器 1 の情報から使用者 4 の生活リズム又は消費動向等が特定される懸念があり、一部の情報については、機器 1 の所有者 3 及び遠隔処理装置 2 の管理者 6 に開示することが好まれない場合がある。この場合においても、提供先 5 に対しては、保守等のために情報の開示が必要とされることがある。本開示では、主従関係を有する認証鍵 30 を用いて通信を行うことで提供される情報の範囲が決定されるので、認証鍵 30 の主従関係により、機器 1 の使用者 4 に対して所有者 3 よりも強い権限を割り当てることも可能である。

[0022] 認証鍵 30 は、主従関係を有しており、通信に認証鍵 30 が用いられることで、認証鍵 30 の種類及び主従関係に応じて通信が制限される。具体的には、機器 1 と遠隔処理装置 2 との通信、遠隔処理装置 2 と、提供先 5、所有者 3 又は使用者 4 が所有する通信機器 20 b との通信、遠隔処理装置 2 と、管理者 6 が所有する通信機器 20 a との通信に対し、認証鍵 30 に応じて制限が設けられる。なお、通信機器 20 a、20 b 同士、あるいは通信機器 20 a、20 b と機器 1 とが直接通信しても構わない。

[0023] 主従関係とは、主となる認証鍵 30 で得られる権限には、従となる認証鍵 30 で得られる権限が全て含まれる、という関係である。主従関係を有する認証鍵 30 は、認証鍵 30 において開示レベルと権限に差がある主と従とを

構成する。以下の説明において、主となる認証鍵30を主鍵と称し、従となる認証鍵を従鍵と称する場合がある。また、主となる認証鍵30を有する者を主鍵所有者と称し、従となる認証鍵30を有する者を従鍵所有者と称する場合がある。

[0024] 図2は、実施の形態1に係る機器保守管理システムの一例を示す図である。図2に示される例では、2つの機器1aから成る機器群Gaを所有者3aが所有し、2つの機器1bから成る機器群Gbを所有者3bが所有し、機器群Ga及び機器群Gbから成る機器群Gtの4つの機器1a、1bを使用者4が使用する。図2に示されるように、所有者3a及び使用者4に、主従関係を有する認証鍵30aが予め付与され、所有者3b及び使用者4に、主従関係を有する認証鍵30bが予め付与されている。

[0025] 図3は、実施の形態1に係る機器保守管理システムの遠隔処理装置の機能を示す機能ブロック図である。図3に示されるように、遠隔処理装置2は、通信部21と、情報取得部22と、通信設定部23と、情報管理部24と、制御部25と、記憶部26とを備えている。

[0026] 遠隔処理装置2は、専用のハードウェア、又はメモリに格納されるプログラムを実行するCPU (Central Processing Unit) で構成されている。なお、CPUは、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、又はプロセッサともいう。

[0027] 遠隔処理装置2が専用のハードウェアである場合、遠隔処理装置2は、例えば、単回路、複合回路、ASIC (application specific integrated circuit)、FPGA (field-programmable gate array)、又はこれらを組み合わせたものが該当する。遠隔処理装置2が実現する各機能部のそれぞれを、個別のハードウェアで実現してもよいし、各機能部を一つのハードウェアで実現してもよい。

[0028] 遠隔処理装置2がCPUの場合、遠隔処理装置2が実行する各機能は、ソフトウェア、ファームウェア、又はソフトウェアとファームウェアとの組み

合わせにより実現される。ソフトウェア及びファームウェアはプログラムとして記述され、メモリに格納される。CPUは、メモリに格納されたプログラムを読み出して実行することにより、遠隔処理装置2の各機能を実現する。ここで、メモリは、例えば、RAM、ROM、フラッシュメモリ、EPROM、又はEEPROM等の、不揮発性又は揮発性の半導体メモリである。

[0029] 遠隔処理装置2の機能の一部を専用のハードウェアで実現し、一部をソフトウェア又はファームウェアで実現するようにしてもよい。

[0030] 図3に基づいて、遠隔処理装置2の機能部を構成する通信部21と、情報取得部22と、通信設定部23と、情報管理部24と、制御部25と、記憶部26とについて説明する。制御部25は、情報取得部22、通信設定部23、及び情報管理部24の動作を制御する。また制御部25は、複数の機器1の情報を分析し、分析結果に応じて機器1に指令を送信する。

[0031] 通信部21は、複数の機器1それぞれと、インターネット等のネットワーク10を介して接続され、データの送受信をする。通信部21は、同様に、機器群Ga（図2）の所有者3a及び機器群Gb（図2）の所有者3bそれぞれの通信機器20b（不図示）と、ネットワーク10を介して接続され、データの送受信をする。また通信部21は、機器群Gt（図2）の使用者4が保有する通信機器20b（図1）と、ネットワーク10を介して接続され、データの送受信を行う。また通信部21は、遠隔処理装置2の管理者6が所有する通信機器20a（図6）と、ネットワーク10を介して接続され、データの送受信をする。なお、図3では、説明のために通信機器20a、20bを省略し、遠隔処理装置2の通信相手を、それらを保有する所有者3a、所有者3b、使用者4、提供先5、又は管理者6と表している。

[0032] 情報取得部22は、複数の機器1の情報を取得する。情報取得部22は、各機器1から予め決められたタイミングで送信される機器1の情報を、通信部21を介して受信する。なお、情報取得部22は、予め決められたタイミングで、機器1の情報を送信するように通信部21を介して各機器1に要求を送信し、要求に応じて機器1から送信される情報を受信する構成とされて

もよい。情報取得部 2 2 が受信した複数の機器 1 の情報は、記憶部 2 6 に記憶される。

[0033] 通信設定部 2 3 は、外部から受信した設定要求に基づいて、通信に対する制限を設定及び変更する。記憶部 2 6 には、通信相手ごとに、通信に対する制限が記憶されている。

[0034] 情報管理部 2 4 は、外部との通信で送受信するデータを管理する。例えば、通信相手から情報開示の要求を受信した場合に、情報管理部 2 4 は、通信相手の認証鍵 3 0 a、3 0 b（図 2）に基づいて、開示する情報の範囲を決定する。情報管理部 2 4 は、開示する情報の範囲を認証鍵 3 0 a、3 0 b（図 2）に基づいて決定する際、予め記憶部 2 6 に記憶された設定を参照する。情報管理部 2 4 は、決定した範囲の情報を記憶部 2 6 から抽出し、通信部 2 1 を介して通信相手に送信する。

[0035] 記憶部 2 6 には、情報取得部 2 2 が取得した複数の機器 1 の情報が、機器 1 ごとに記憶されている。また、記憶部 2 6 には、制限について規定した第一の制限テーブル 8 1 及び第二の制限テーブル 8 2 が記憶されている。

[0036] 図 4 は、図 2 の例において所有者及び使用者が有する認証鍵と機器との関係を示す図である。所有者 3 a は、対象を機器 1 a とする認証鍵 3 0 a（図 2）の主鍵所有者であり、機器 1 a の主とされている。所有者 3 b は、対象を機器 1 b とする認証鍵 3 0 b（図 2）の主鍵所有者であり、機器 1 b の主とされている。使用者 4 は、2 つの認証鍵 3 0 a、3 0 b（図 2）の従鍵所有者であり、機器 1 a について所有者 3 a よりも下位の権限を有し、機器 1 b について所有者 3 b よりも下位の権限を有する。このような主鍵所有者及び従鍵所有者と、情報開示される機器 1 との関係は、第一の制限テーブル 8 1 に規定されている。

[0037] 図 5 は、図 2 の例において認証鍵で取得可能な情報の範囲を示す図である。以下、機器 1 の情報には、複数の情報 A～情報 C が含まれるものとして説明する。認証鍵 3 0 a（図 2）の主鍵に対しては、機器 1 a に関する情報 A～情報 C の全てが取得可能とされ、認証鍵 3 0 a（図 2）の従鍵に対しては

、機器 1 a に関する情報 A～C のうち情報 C のみが取得可能とされている。
また、認証鍵 3 0 b (図 2) の主鍵に対しては、機器 1 b に関する情報 A～C の全てが取得可能とされ、認証鍵 3 0 b (図 2) の従鍵に対しては、機器 1 b に関する情報 A～C のうち情報 C のみが取得可能とされている。このような主鍵及び従鍵と、情報の開示レベルとの関係は、第二の制限テーブル 8 2 に規定されている。

[0038] 次に、図 2～3 を参照して、機器保守管理システム 1 0 0 の動作について説明する。図 3 に示されるように、機器 1 は、自己の運転及び異常の有無といった情報を、遠隔処理装置 2 に、定期的に送信する。また、機器 1 は定期通信の他、遠隔処理装置 2、所有者 3 a、3 b、使用者 4、提供先 5、又は管理者 6 からの要求に基づき自己の情報を送信する。また機器 1 は、自己の情報又は遠隔処理装置 2 から受信した指令に基づき、運転の中断、再開又は非常停止を実施する。

[0039] 遠隔処理装置 2 は、ネットワークを介して接続された複数の機器 1 の情報を収集する。また遠隔処理装置 2 は、図 2 に示されるように、収集した複数の機器 1 の情報を、認証鍵 3 0 a、3 0 b に基づき、所有者 3 a、3 b 及び使用者 4 に送信する。

[0040] 遠隔処理装置 2 は、認証鍵 3 0 a の主鍵を有する所有者 3 a に、機器 1 a の情報 A～情報 C 全てを送信する。なお、認証鍵 3 0 a を有していない所有者 3 b には、機器 1 a の情報が送信されない。また遠隔処理装置 2 は、認証鍵 3 0 b の主鍵を有する所有者 3 b に、機器 1 b の情報 A～情報 C 全てを送信する。なお、認証鍵 3 0 b を有していない所有者 3 a には、機器 1 b の情報が送信されない。また遠隔処理装置 2 は、認証鍵 3 0 a 及び認証鍵 3 0 b の従鍵を有する使用者 4 に、機器 1 a 及び機器 1 b の情報 C のみを送信する。

[0041] なお、図 1 のように、提供先 5 に認証鍵 3 0 が付与されている場合には、提供先 5 もまた、自己が有する認証鍵 3 0 に応じて機器 1 の情報を取得することができ、取得した情報に基づき保守等のサービスを提供することができ

る。また、図5に示す第二の制限テーブル82は一例であって、開示が制限される情報（例えば、情報A～情報C）の種類及び数は制限されず、図1に示される機器1の使用者4又は所有者3に関する個人情報も、制限の対象とできる。

[0042] 図2に基づき、所有者3a、3bが主鍵所有者であり、使用者4が従鍵所有者である場合について説明したが、主鍵所有者及び従鍵所有者の組み合わせは特にこれに限定されない。図1に示されるように、機器1の種類又は使用者4の希望等に応じて、付与する認証鍵30の種類及び従属関係が決定されるとよい。図2において、例えば、使用者4を主鍵所有者とし、所有者3a、3bを従鍵所有者とすることができる。また例えば、所有者3aが所有する機器群Gaについて、所有者3aを認証鍵30aの主鍵所有者とし、提供先5を認証鍵30aの従鍵所有者とすることができる。また例えば、使用者4が使用する機器群Gtについて、使用者4を認証鍵30a、30bの主鍵所有者とし、提供先5を認証鍵30a、30bの従鍵所有者とすることができる。また例えば、管理者6が管理する遠隔処理装置2によって情報が収集される機器群Gtについて、所有者3、使用者4、又は提供先5を認証鍵30a、30bの従鍵所有者とすることができる。

[0043] 以上のように、実施の形態1に係る機器保守管理システム100は、自己の運転及び異常の有無に関する情報を送信する複数の機器1と、複数の機器1のそれぞれの情報を取得して記憶する遠隔処理装置2と、を備える。遠隔処理装置2は、主従関係を有する少なくとも一種類の認証鍵30を用いて通信を制限するものである。遠隔処理装置2は、複数の機器1の少なくとも一部の機器1aについて主となる認証鍵30aが予め付与された第一の通信機器、及び、第一の通信機器の従となる認証鍵30aが予め付与された第二の通信機器のそれぞれを通信相手として通信を行う。遠隔処理装置2は、通信を行う際、通信相手が有する認証鍵30の種類及び主従関係に応じて、提供する情報の範囲を決定する。

[0044] これにより、遠隔処理装置2の通信相手が有する認証鍵30の種類、特定

の認証鍵 30 の有無、及び認証鍵 30 の主従関係に応じて、通信相手に情報を提供する対象機器、及び情報の開示レベルを違えることができる。したがって、情報セキュリティを担保しつつ、通信相手に必要な情報を提供できる。

[0045] また、第一の通信機器及び第二の通信機器には、管理者 6 が有する通信機器 20 a、一部の機器 1 の所有者 3、使用者 4 又は保守業者（提供先 5）が有する通信機器 20 b の少なくとも二つが含まれる。

[0046] これにより、通信相手により個別設定がされない従来の構成と比べ、二以上の通信相手に対して認証鍵 30 を付与することで、より柔軟に、通信相手に適した情報を提供する設定とできる。例えば、1 つの建物内に複数の施設が設けられた商業ビルでは、建物内に、互いに異なる機器群を所有する複数の所有者が存在し、機器群ごとに定期点検が行われるが、この場合においても、所有者ごとに対象機器を制限でき、管理が容易となる。

[0047] また、一以上の第一の通信機器（例えば、所有者 3 a 及び所有者 3 b それぞれの通信機器 20 b）に対し、異なる種類の認証鍵 30 a、30 b であって、複数の機器 1 a、1 b のうち異なる機器群 G a、G b の主となる認証鍵が予め付与されている。また、一以上の第二の通信機器（例えば、使用者 4 の通信機器 20 b）に対し、異なる種類の認証鍵 30 a、30 b であって、複数の機器 1 a、1 b のうち異なる機器群 G a、G b の従となる認証鍵が予め付与されている。また、機器 1 の情報には、第一の情報（例えば、情報 C）及び第二の情報（例えば、情報 A 及び情報 B）が含まれる。遠隔処理装置 2 は、第一の機器群（機器群 G a）の主となる認証鍵 30 a が付与された第一の通信機器（例えば、所有者 3 a の通信機器 20 b）に対しては、第一の機器群（機器群 G a）に関する第一の情報及び前記第二の情報を開示する。また遠隔処理装置 2 は、第一の機器群（機器群 G a）の従となる認証鍵 30 a が付与された第二の通信機器（例えば、使用者 4 の通信機器 20 b）に対しては、第一の機器群（機器群 G a）に関する第一の情報を開示し、第二の情報を開示しない。また遠隔処理装置 2 は、第二の機器群（機器群 G b）の

主となる認証鍵 30b が付与された第一の通信機器（例えば、所有者 3b の通信機器 20b）に対しては、第二の機器群（機器群 Gb）の第一の情報及び第二の情報を開示する。また遠隔処理装置 2 は、第二の機器群（機器群 Gb）の従となる認証鍵 30b が付与された第二の通信機器（例えば、使用者 4 の通信機器 20b）に対しては、第二の機器群（機器群 Gb）の第一の情報を開示し、第二の情報を開示しない。

[0048] 実施の形態 2.

図 6 は、実施の形態 2 に係る機器保守管理システムの一例を示す図である。図 7 は、図 6 の例において使用者と提供先と管理者がそれぞれ有する認証鍵の関係を示す図である。図 8 は、図 6 の例において認証鍵で取得可能な情報の範囲を示す図である。図 6～図 8 に基づいて実施の形態 2 に係る機器保守管理システム 100 について説明する。

[0049] 実施の形態 2 の機器保守管理システム 100 は、主従関係を有する認証鍵 30（30a、30b、30c）が階層構造を有する点が、実施の形態 1 の場合とは異なる。その他の構成及び動作については、実施の形態 1 と同様であるため、ここでは詳細な説明を省略する。

[0050] 図 6 及び図 7 に示されるように、同一の機器 1 に対して、管理者 6 が主となる認証鍵 30a を有し、使用者 4 が管理者 6 の従となる認証鍵 30b を有し、提供先 5 が使用者 4 の従となる認証鍵 30c を有する。すなわち、実施の形態 2 では、主従関係を有する 2 組の認証鍵の組み合わせにより、認証鍵 30a、30b 及び 30c に、3 階層の階層構造が構築されている。なお、3 組以上の認証鍵を組み合わせると 4 階層以上の階層構造を形成してもよい。

[0051] ここで、最上位の認証鍵 30a の開示レベルを 0 とし、その配下のレベルを 1、2・・・と定義し、レベルが大きくなるにつれ、情報の取得制限が厳しくなるものとする。図 8 に示されるように、第二の制限テーブル 82 には、各開示レベルに対し、開示される情報の範囲が規定されている。レベルが 0 の認証鍵 30a に対して情報 A～情報 C 全てが取得可とされ、レベルが 1 の認証鍵 30b に対して情報 B～情報 C が取得可とされ、レベルが 2 の認証

鍵 3 0 c に対して情報 C のみが取得可と設定されている。

[0052] なお、図 8 に示される第二の制限テーブル 8 2 は一例であって、開示が制限される情報（図 8 では、情報 A ～ 情報 C）の種類及び数は、これに限定されない。また、図 6 において、階層構造を有する認証鍵 3 0 a、3 0 b 及び 3 0 c が、管理者 6、使用者 4 及び提供先 5 に付与されている場合について説明したが、所有者 3 に対しても同様に扱うことができる。

[0053] 以上のように、実施の形態 2 に係る機器保守管理システム 1 0 0 において、主従関係を有する認証鍵 3 0 a、3 0 b 及び 3 0 c は、一部の機器 1 に関する情報について開示レベルの異なる 3 階層以上の階層構造を構成する。

[0054] これにより、同一の機器 1 の情報について従来よりも細分化して通信相手ごとに開示範囲を設定することができるので、不要な情報の開示を低減でき、情報セキュリティの機密性を高めることができる。

[0055] 実施の形態 3.

図 9 は、実施の形態 3 に係る機器保守管理システムにおける認証鍵交換の様子を示す図である。図 1 0 は、図 9 に示す認証鍵交換の前及び後における所有者及び使用者が有する認証鍵と機器との関係を示す図である。図 1 1 は、実施の形態 3 に係る機器保守管理システムにおける認証鍵置換の様子を示す図である。図 1 2 は、図 1 1 に示す認証鍵置換の前及び後における所有者及び使用者が有する認証鍵と機器との関係を示す図である。図 9 ～ 図 1 2 に基づいて実施の形態 3 に係る機器保守管理システム 1 0 0 について説明する。

[0056] 実施の形態 3 の機器保守管理システム 1 0 0 は、主となる認証鍵 3 0 a、3 0 b を有する者すなわち主鍵所有者の許可を得ることで、その認証鍵 3 0 a、3 0 b の主鍵所有者及び従鍵所有者の少なくとも一方を変更できる点が、実施の形態 1 の場合とは異なる。その他の構成については、実施の形態 1 と同様であるため、ここでは詳細な説明を省略する。

[0057] 所有者 3、使用者 4、提供先 5、及び管理者 6 間において（図 1）、認証鍵 3 0 a、3 0 b の主従関係を交換することができる。ここで、認証鍵 3 0

aの主従関係を交換するとは、図9に示されるように、その認証鍵30aについて予め設定された主鍵所有者と従鍵所有者とを入れ替えることをいう。図9に示される例では、認証鍵30aの主従関係が交換されている。具体的には、図10に示されるように、遠隔処理装置2の記憶部26（図3）に記憶された第一の制限テーブル81において、交換前には機器1aの主であった所有者3aと従であった使用者4との間で主従関係が入れ替えられる。交換後には、機器1aの主が使用者4とされ、従が所有者3aとされる。認証鍵30aの主従関係が交換される際、遠隔処理装置2の通信設定部23により、記憶部26に記憶された第一の制限テーブル81が更新されるとともに（図3）、設定が変更された者に対し、変更後の主従関係に応じて認証鍵30aが付与される。

[0058] また、主となる認証鍵30a、30bを有する者すなわち主鍵所有者、又は従となる認証鍵30a、30bを有する者すなわち従鍵所有者を置換することができる。ここで、主鍵所有者を置換するとは、予め設定された主鍵所有者を別の者にするをいい、従鍵所有者を置換するとは、予め設定された従鍵所有者を別の者にするをいう。図11に示される例では、認証鍵30bの主鍵所有者が置換されている。具体的には、図12に示されるように、遠隔処理装置2の記憶部26（図3）に記憶された第一の制限テーブル81において、機器1bの主が、所有者3bから別の所有者3cに置き換えられる。機器1bの従は、置換の前後で変更されない。認証鍵30bの主鍵所有者の置換後には、機器1bの主は所有者3cとされ、機器1bの従は使用者4とされる。認証鍵30bの主鍵所有者又は従鍵所有者が別の者と置換される際、遠隔処理装置2の通信設定部23により、記憶部26に記憶された第一の制限テーブル81が更新されるとともに（図3）、変更後の主従関係に応じて認証鍵30bが付与される。

[0059] 次に、上記のような通信設定の変更が外部から要求された場合に遠隔処理装置2が行うステップについて説明する。その他の基本的な動作については、実施の形態1と同じであるため、ここでは詳細な説明を省略する。

[0060] 図13は、実施の形態3に係る交換要求の処理を示すフローチャートである。図11を参照しつつ、図13に基づき、認証鍵30aの交換要求を受信した場合に遠隔処理装置2が行うステップについて説明する。

[0061] 遠隔処理装置2は、外部（例えば、従となる者又はそれ以外の者）から、機器1aの主従関係の交換要求を受信すると（ステップS1）、その機器1aの主となる者（所有者3a）により交換が許可されたか否かを判定する（ステップS2）。遠隔処理装置2は、ステップS2の判定に際し、交換要求がされた機器1aの主となる者に対して交換要求を送信し、主となる者から交換を許可する旨を受信した場合に、交換要求が許可されたと判定する（ステップS2：YES）。遠隔処理装置2は、交換が許可されたと判定した場合には（ステップS2：YES）、その機器1aに対する認証鍵30aについて主従関係の交換を行う（ステップS3）。このとき、遠隔処理装置2は、上述したように、記憶部26（図3）に記憶された第一の制限テーブル81を更新するとともに（図10）、交換要求に従って認証鍵30aを付与する。一方、ステップS2の判定において、交換が許可されなかったと遠隔処理装置2が判定した場合には（ステップS2：NO）、要求された交換を行わず、終了する。遠隔処理装置2は、交換要求を送信した者に対し、許可判定の結果、すなわち交換要求が許可されたか拒否されたか、を通知する構成とされてもよい。

[0062] 図14は、実施の形態3に係る置換要求の処理を示すフローチャートである。図11を参照しつつ、図14に基づき、認証鍵の置換要求を受信した場合に遠隔処理装置2が行うステップについて説明する。

[0063] 遠隔処理装置2は、機器1bの主又は従を置換する置換要求を受信すると（ステップS11）、その機器1bの主となる者により置換が許可されたか否かを判定する（ステップS2）。遠隔処理装置2は、ステップS2の判定に際し、置換要求の送信元がその機器1bの主となる者（所有者3b）である場合には、主となる者により交換要求が許可されたと判定する（ステップS2：YES）。また遠隔処理装置2は、置換要求の送信元がその機器1の

主となる者でない場合には、その機器 1 の主となる者に対して置換要求を送信し、置換を許可する旨を受信した場合に、置換要求が許可されたと判定する（ステップ S 2 : Y E S）。遠隔処理装置 2 は、主となる者により置換が許可されたと判定した場合には（ステップ S 2 : Y E S）、その機器 1 について主又は従を置換する（ステップ S 3）。このとき、遠隔処理装置 2 は、上述したように、記憶部 2 6 に記憶された第一の制限テーブル 8 1 を更新するとともに、置換要求に従って認証鍵 3 0 b を付与する。一方、遠隔処理装置 2 は、置換要求の送信元がその機器 1 の主となる者でない場合に、主となる者により置換が許可されなかったと判定した場合には（ステップ S 2 : N O）、要求された置換を行わず、終了する。遠隔処理装置 2 は、置換要求を送信した者に対し、許可判定の結果、すなわち置換要求が許可されたか拒否されたか、を通知する構成とされてもよい。

[0064] 図 9 及び図 1 1 に示されるように、認証鍵 3 0 a、3 0 b が変更された後では、遠隔処理装置 2 の情報管理部 2 4（図 3）は、変更後の認証鍵 3 0 a、3 0 b に基づいて、通信相手に対する情報の開示範囲を決定する。そして、遠隔処理装置 2 の記憶部 2 6（図 3）に記憶された複数の機器 1 の情報が、決定した開示範囲で、通信相手に提供される。

[0065] 以上のように、実施の形態 3 に係る保守システムにおいて、遠隔処理装置 2 は、認証鍵 3 0 b について予め設定された主鍵所有者又は従鍵所有者を置換する置換要求が、主鍵所有者により許可された場合に、置換要求に従って認証鍵 3 0 b を付与する。また遠隔処理装置 2 は、認証鍵 3 0 a について予め設定された主鍵所有者と従鍵所有者とを交換する交換要求が、主鍵所有者により許可された場合に、交換要求に従って認証鍵 3 0 a を付与する。

[0066] これにより、例えば機器 1 が故障した場合等のように、通常よりも情報の開示が必要とされるときに、機器 1 に対する認証鍵 3 0 の主鍵所有者に対し、通信機器 2 0 a、2 0 b 上で置換要求又は交換要求を送信し、簡単な作業で開示範囲を広げることができる。また、通常時には下位の権限に戻し、不要な情報の流出を防ぐことができる。

[0067] 実施の形態４．

図１５は、実施の形態４に係る機器保守管理システムにおける変更認否設定を説明する図である。図１５に基づいて実施の形態４に係る機器保守管理システム１００について説明する。

[0068] 実施の形態４の機器保守管理システム１００は、変更要求に対する可否を、予め決められた認否設定に基づいて自動で実行する点が、実施の形態３の場合とは異なる。その他の構成及び動作については、実施の形態３と同様であるため、ここでは詳細な説明を省略する。

[0069] 遠隔処理装置２の記憶部２６には（図３）、図１５に示されるように、各機器１ａ、１ｂについて交換及び置換といった変更の認否を規定した第三の制限テーブル８３が記憶されている。図１５に示される例では、機器１ａについての交換要求及び置換要求はいずれも拒否される設定とされ、一方、機器１ｂについての交換要求及び置換要求はいずれも許可される設定とされている。

[0070] 実施の形態４の遠隔処理装置２は、図１３に示されるステップＳ２、及び図１４に示されるステップＳ１２の判定を行う際、予め決められた認否設定に基づき自動で判定を行う。

[0071] 以上のように、実施の形態４に係る機器保守管理システム１００において、遠隔処理装置２には、認証鍵３０の主鍵所有者又は従鍵所有者を置換する置換要求、及び、主鍵所有者と従鍵所有者とを交換する交換要求に対する認否が機器１毎に予め設定されている。遠隔処理装置２は、置換要求が許可されている機器１ｂについて主又は従の置換要求があった場合に、置換要求に従って認証鍵３０を付与する。また遠隔処理装置２は、交換要求が許可されている機器１ｂについて主従関係の交換要求があった場合に、交換要求に従って認証鍵３０を付与する。これにより、遠隔処理装置２は、機器１の主となる者に対して変更要求の認否を問い合わせる必要が無く、また、機器１の主となる者は、変更要求の都度、応答する必要が無い。したがって、通信負荷及び作業負荷を軽減できる。

[0072] 実施の形態 5.

図 1 6 は、実施の形態 5 に係る機器保守管理システムの一例を示す図である。図 1 7 は、図 1 6 の機器保守管理システムにおける視覚化手段の一例を示す図である。図 1 8 は、図 1 6 の機器保守管理システムにおいて検索符号と認証鍵と各種情報との関係を示す図である。図 1 6 ～図 1 8 に基づいて実施の形態 5 に係る機器保守管理システム 1 0 0 について説明する。

[0073] 実施の形態 5 の機器保守管理システム 1 0 0 は、認証鍵に対し 1 つ以上の検索符号 S S 1、S S 2 を割り当て可能である点、及び、検索符号 S S 1、S S 2 と関連する情報群を管理者 6 に対して報知する報知手段を備える点が、実施の形態 1 の場合とは異なる。その他の構成及び動作は、実施の形態 1 と同様であるため、ここでは詳細な説明を省略する。

[0074] 図 1 6 に示されるように、機器保守管理システム 1 0 0 は、検索結果を管理者 6 に対して報知する報知手段として、遠隔処理装置 2 の管理者 6 が所有する通信機器 2 0 a（例えば、スマートフォン）を備える。以下、管理者 6 が所有する通信機器 2 0 a を、使用者 4 等の通信機器 2 0 b と区別して、管理用通信機器と称する場合がある。通信機器 2 0 a は、遠隔処理装置 2 に集積された複数の機器 1 の情報を通信により取得して報知する。図 1 7 に示されるように、通信機器 2 0 a は、情報を表示する表示画面 2 0 1 を備える。なお、通信機器 2 0 a は、上記のスマートフォンに限定されず、遠隔処理装置 2 から取得した情報を、管理者 6 に対して聴覚的に又は視覚的に報知する機能を有していればよい。

[0075] 図 1 6 に示される例では、管理者 6 が主となる認証鍵 3 0 a ～ 3 0 e を有し、また、使用者 4 a が主となる認証鍵 3 0 a ～ 3 0 c を有し、使用者 4 b が主となる認証鍵 3 0 d ～ 3 0 e を有する。なお、説明の都合上、管理者 6 と使用者 4 a、4 b との主従関係は無いものとし、管理者 6 は、使用者 4 a の認証鍵 3 0 a ～ 3 0 c と同一の認証鍵と、使用者 4 b の認証鍵 3 0 d ～ 3 0 e と同一の認証鍵とを有する構成とする。また、使用者 4 a が使用する 3 つの機器 1 はそれぞれ、所有者 3 a 1、3 a 2、3 a 3 が 1 台ずつ所有して

いる。また、使用者4 bが使用する2つの機器1はそれぞれ、所有者3 b 1、3 b 2が1台ずつ所有している。所有者3 (3 a 1、3 a 2、3 a 3、3 b 1及び3 b)は、自己が所有する機器1について従となる認証鍵3 0 (3 0 a、3 0 b、3 0 c、3 0 d又は3 0 e)を有している。したがって、図1 6に示される例では、各認証鍵3 0 a～3 0 eに、所有者3 a 1、3 a 2、3 a 3、3 b 1及び3 bが、1対1で対応する。

[0076] 遠隔処理装置2の記憶部2 6 (図3)には、認証鍵3 0 a～3 0 eと、各認証鍵3 0 a～3 0 eに対応づけられた一種以上の検索符号SS 1、SS 2と、所有者3と、所有者3が所有する機器1に関する複数の情報D 1、D 2とを含む対応テーブル8 4が記憶される。図1 8に示される例では、2つの検索符号SS 1、SS 2が使用され、検索符号SS 1は使用者4 ごとに設定されている。具体的には、使用者4 aが有する3つの認証鍵3 0 a～3 0 cに対して同一の検索符号SS 1 (例えば、3 3 a)が割り当てられ、使用者4 bが有する2つの認証鍵3 0 d～3 0 eに対しては同一の検索符号SS 1 (例えば、3 3 b)が割り当てられている。また、検索符号SS 2は、所有者3 ごとに設定されている。

[0077] 検索符号SS 1、SS 2は、上記のように英数文字列、又は記号を含む英数字文字列で構成される。なお、検索符号SS 1、SS 2を、認証鍵3 0自体、又は認証鍵3 0の所有者3の情報とすることも可能である。また、認証鍵3 0と関連する機器1の複数の情報D 1、D 2として、データが無い場合には検索結果は空白でも構わない。

[0078] 次に、認証鍵3 0 a～3 0 eを有する管理者6が、自己の通信機器2 0 aで検索符号SS 1として3 3 bを使用して検索した場合に、通信機器2 0 aの表示画面2 0 1 (図1 7)に表示される情報について説明する。管理者6が通信機器2 0 aにおいて検索符号SS 1を選択又は入力し、検索ボタン2 0 1 aを押すと、選択された検索符号SS 1 (図1 7では、3 3 b)と関連する情報の送信を求める検索要求が、遠隔処理装置2へ送信される (図1 6)。遠隔処理装置2は、検索要求に含まれる検索符号SS 1、及び通信相手

(管理者6)が有する認証鍵30a~30eに基づいて記憶部26(図3)から検索結果となる情報を抽出し送信する。通信機器20aは、遠隔処理装置2から検索結果を受信し、図17に示されるように、通信機器20aの表示画面201に検索結果を表示する。具体的には、通信機器20aの表示画面201に、選択された検索符号SS1(図17では、33b)と、検索符号SS1に対応する認証鍵30と、その認証鍵30と関連する所有者3の情報及び機器1の情報D1、D2が表示される。

[0079] なお、検索符号SS1、S2は完全一致の他、部分検索でも構わない。管理者6が、33bの検索符号SS1を元に検索した結果、図17に示されるように、管理者6が有する認証鍵30a~30eと対応した5台の機器1のうち、使用者4bが有する認証鍵30d~30eと対応した2台の機器1の情報が表示画面201に表示される。つまり、認証鍵30dに対応する機器1の所有者3b1、並びに、その機器1の情報D1(100a(4))及び情報D2(100b(4))が表示される。また、認証鍵30eに対応する機器1の所有者3b2、並びに、その機器1の情報D1(100a(5))及び情報D2(100b(5))が表示される。

[0080] なお、表示項目及び項目数は、図17の一例に限定されない。また、検索欄201bへの入力、検索可能な項目を一覧表示して選択させることで入力してもよく、あるいは、手動での入力でもよい。

[0081] なお、音声等により報知する報知手段を用いる場合には、検索項目を音声認識により入力する構成とできる。また、検索結果を、表示画面201に表示する代わりに読み上げにより報知する構成とできる。この場合において、使用する言語は日本語に限定されない。

[0082] また、図16に示されるように、使用者4aは、主となる認証鍵30a~30cを用いて自己の通信機器20b(不図示)により遠隔処理装置2と通信を行い、認証鍵30a~30cと関連する情報を取得することができる。具体的には、使用者4aは、使用する3台の機器1について、情報D1(100a(1)、100a(2)及び100a(3))、情報D2(100b

(1)、100b(2)及び100b(3))、及び所有者3(3a1、3a2及び3a3)の情報を取得できる。

[0083] 使用者4bは、主となる認証鍵30d～30eを用いて自己の通信機器20b(不図示)により遠隔処理装置2と通信を行い、認証鍵30d～30eと関連する情報を取得することができる。具体的には、使用者4bは、使用する2台の機器1について、情報D1(100a(4)及び100a(5))、情報D2(100b(4)及び100b(5))、及び所有者3(3b1及び3b2)の情報を取得できる。

[0084] また使用者4a、4bは、自己の通信機器20b(不図示)により検索符号SS2を用いて検索し、自己が所有する認証鍵30a～30cのうち特定の認証鍵(例えば認証鍵30a)と関連する情報のみを自己の通信機器20b(不図示)に表示させることができる。

[0085] 所有者3(3a1、3a2、3a3、3b1及び3b)は、従となる認証鍵30(30a、30b、30c、30d又は30e)を用いて自己の通信機器20b(不図示)により遠隔処理装置2と通信を行い、認証鍵30と関連する情報を取得することができる。例えば、所有者3a1は、所有する1台の機器1について、情報D1(100a(1))及び情報D2(100b(1))の情報を取得できる。

[0086] 以上のように、実施の形態5に係る機器保守管理システム100は、遠隔処理装置2から情報を取得して報知する管理用通信機器(通信機器20a)を備える。遠隔処理装置2には、認証鍵30a～30bに対して一種以上の検索符号SS1、S2が対応づけて記憶されている。通信機器20aは、検索符号SS1、S2が入力された場合に、検索符号SS1、S2とともに、検索符号SS1、S2に対応する認証鍵30、及び認証鍵30と関連する情報を含む情報群(例えば、情報D1及び情報D2)を報知する。

[0087] これにより、膨大なデータ群から検索した情報が報知されるので、作業負荷を回避しつつ、簡単に必要な情報を入手でき、機器1の管理及び保守等における利便性を向上させることができる。

[0088] なお、各実施の形態を組み合わせたり、各実施の形態を適宜、変形、又は省略したりすることが可能である。

符号の説明

[0089] 1 機器、2 遠隔処理装置、3 所有者、4 使用者、5 提供先、6 管理者、10 ネットワーク、20a、20b 通信機器、21 通信部、22 情報取得部、23 通信設定部、24 情報管理部、25 制御部、26 記憶部、30 認証鍵、81 第一の制限テーブル、82 第二の制限テーブル、83 第三の制限テーブル、84 対応テーブル、100 機器保守管理システム、201 表示画面、201a 検索ボタン、201b 検索欄、A、B、C、D1、D2 情報、Ga、Gb、Gt 機器群、SS1、SS2 検索符号。

請求の範囲

- [請求項1] 自己の運転及び異常の有無に関する情報を送信する複数の機器と、
複数の前記機器のそれぞれの前記情報を取得して記憶する遠隔処理装置と、を備え、
前記遠隔処理装置は、
主従関係を有する少なくとも一種類の認証鍵を用いて通信を制限するものであり、
複数の前記機器の少なくとも一部の機器について主となる前記認証鍵が予め付与された第一の通信機器、及び、前記第一の通信機器の従となる前記認証鍵が予め付与された第二の通信機器のそれぞれを通信相手として通信を行い、
通信を行う際、前記通信相手が有する前記認証鍵の種類及び前記主従関係に応じて、提供する前記情報の範囲を決定する
機器保守管理システム。
- [請求項2] 前記第一の通信機器及び前記第二の通信機器には、前記遠隔処理装置の管理者が有する通信機器、前記一部の機器の所有者が有する通信機器、前記一部の機器の使用人が有する通信機器、及び前記一部の機器の保守業者が有する通信機器の少なくとも二つが含まれる
請求項1に記載の機器保守管理システム。
- [請求項3] 主従関係を有する前記認証鍵は、前記一部の機器に関する前記情報について開示レベルの異なる3階層以上の階層構造を構成する
請求項1又は2に記載の機器保守管理システム。
- [請求項4] 前記遠隔処理装置は、
前記認証鍵について予め設定された主鍵所有者又は従鍵所有者を置換する置換要求が、前記主鍵所有者により許可された場合に、前記置換要求に従って前記認証鍵を付与し、
前記認証鍵について予め設定された前記主鍵所有者と前記従鍵所有者とを交換する交換要求が、前記主鍵所有者により許可された場合に

、前記交換要求に従って前記認証鍵を付与する

請求項 1 ～ 3 のいずれか一項に記載の機器保守管理システム。

[請求項5]

前記遠隔処理装置には、

前記認証鍵の主鍵所有者又は従鍵所有者を置換する置換要求、及び、前記主鍵所有者と前記従鍵所有者とを交換する交換要求に対する認否が前記機器毎に予め設定され、

前記遠隔処理装置は、

前記置換要求が許可されている前記機器について前記置換要求があった場合に、前記置換要求に従って前記認証鍵を付与し、

前記交換要求が許可されている前記機器について前記交換要求があった場合に、前記交換要求に従って前記認証鍵を付与する

請求項 1 ～ 3 のいずれか一項に記載の機器保守管理システム。

[請求項6]

前記遠隔処理装置から前記情報を取得して報知する管理用通信機器を備え、

前記遠隔処理装置には、前記認証鍵に対して一種以上の検索符号が対応づけて記憶されており、

前記管理用通信機器は、前記検索符号が入力された場合に、前記検索符号とともに、前記検索符号に対応する前記認証鍵、及び前記認証鍵と関連する前記情報を含む情報群を報知する

請求項 1 ～ 5 のいずれか一項に記載の機器保守管理システム。

[請求項7]

一以上の前記第一の通信機器に対し、異なる種類の前記認証鍵であって、複数の前記機器のうち異なる機器群の主となる前記認証鍵が予め付与され、

一以上の前記第二の通信機器に対し、異なる種類の前記認証鍵であって、複数の前記機器のうち異なる前記機器群の従となる前記認証鍵が予め付与され、

前記機器の前記情報には、第一の情報及び第二の情報が含まれ、

前記遠隔処理装置は、一以上の前記第一の通信機器及び一以上の前

記第二の通信機器それぞれと通信する際、

第一の機器群の主となる前記認証鍵が付与された前記第一の通信機器に対しては、前記第一の機器群に関する前記第一の情報及び前記第二の情報を開示し、

前記第一の機器群の従となる前記認証鍵が付与された前記第二の通信機器に対しては、前記第一の機器群に関する前記第一の情報を開示し、前記第二の情報を開示せず、

第二の機器群の主となる前記認証鍵が付与された前記第一の通信機器に対しては、前記第二の機器群の前記第一の情報及び前記第二の情報を開示し、

前記第二の機器群の従となる前記認証鍵が付与された前記第二の通信機器に対しては、前記第二の機器群の前記第一の情報を開示し、前記第二の情報を開示しない

請求項 1 ～ 6 のいずれか一項に記載の機器保守管理システム。