(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-284985
(P2005-284985A)
(43)公開日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/00	G06F 13/00	351N	2C061
B41J 29/38	B41J 29/38	Z	2H027
G03G 21/00	G03G 21/00	396	5B021
G06F 3/12	G03G 21/00	510	5B089
H04N 1/00	G06F 3/12	D	5C062

審査請求 未請求　請求項の数 24　OL　（全 26 頁）　最終頁に続く

(21)出願番号　特願2004-101063 (P2004-101063)
(22)出願日　平成16年3月30日 (2004.3.30)

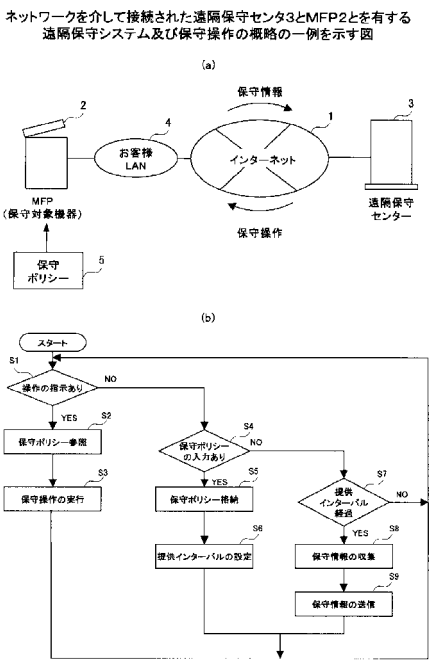
(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　2C061 AP01 AP07 HJ08 HQ17 HV19 HV35 HV60
2H027 EJ08 EJ13 EJ15 HB17
5B021 AA01 BB01 BB04 CC05 EE02 NN00
5B089 JA35 JB22 KA12 KC28 KC58 KC59 KH30 LB01

最終頁に続く

(54)【発明の名称】ネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システム

(57)【要約】
【課題】　ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システムを提供すること。
【解決手段】　保守操作を指示する保守センタ３とネットワーク１を介して接続されたネットワーク対応機器２であって、保守センタ３による当該ネットワーク対応機器２の保守操作又は当該ネットワーク対応機器２の保守に係る保守情報の送信、について規定する保守ポリシー５が格納された保守ポリシーデータベースと、保守ポリシーデータベースを参照して、保守情報を前記保守センタ３に送信する保守情報送信手段と、保守センタ３から指示された操作を受信する保守操作指示受信手段と、保守ポリシーデータベースを参照して、保守操作指示受信手段により受信した操作を行う保守操作制御手段と、を有することを特徴とするネットワーク対応機器、を提供する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
保守操作を指示する保守センタとネットワークを介して接続されたネットワーク対応機器であって、
前記保守センタによる当該ネットワーク対応機器の保守操作又は当該ネットワーク対応機器の保守に係る保守情報の送信、について規定する保守ポリシーが格納された保守ポリシーデータベースと、
前記保守ポリシーデータベースを参照して、前記保守情報を前記保守センタに送信する保守情報送信手段と、
前記保守センタから指示された操作を受信する保守操作指示受信手段と、
前記保守ポリシーデータベースを参照して、前記保守操作指示受信手段により受信した操作を行う保守操作制御手段と、
を有することを特徴とするネットワーク対応機器。
【請求項２】
前記保守ポリシーは、
前記保守情報のうち、前記保守センタに自動的に送信する定期提供保守情報と、
前記定期提供保守情報を前記保守センタに送信するタイミングと、
を規定することを特徴とする請求項１記載のネットワーク対応機器。
【請求項３】
前記定期提供保守情報を収集する保守情報収集手段を、有し、
前記保守情報送信手段は、前記保守情報収集手段により収集された前記定期提供保守情報を、前記タイミングで、前記保守センタに送信する、
ことを特徴とする請求項２記載のネットワーク対応機器。
【請求項４】
前記保守センタに操作の指示を問い合わせる操作問い合わせ手段を有し、
前記保守操作指示受信手段は、前記操作問い合わせ手段による操作の指示の問い合わせ、又は、前記保守情報送信手段による前記定期提供保守情報の送信、に応答して前記保守センタから送信された操作の指示を受信する、
ことを特徴とする請求項１又は３記載のネットワーク対応機器。
【請求項５】
保守操作指示受信手段により前記操作の指示を受信した場合に前記保守センタを認証し、又は、
前記保守情報送信手段により前記定期提供保守情報を前記保守センタに送信する場合に前記保守センタを認証する、保守センタ認証手段を有する、
ことを特徴とする請求項１又は３記載のネットワーク対応機器。
【請求項６】
前記保守情報送信手段により送信される前記保守情報又は前記定期提供保守情報が、暗号化されていることを特徴とする請求項１又は３記載のネットワーク対応機器。
【請求項７】
当該ネットワーク対応機器を管理する管理者を認証する管理者認証処理手段と、
前記管理者認証処理手段より認証された管理者により入力された保守ポリシーで、前記保守ポリシーデータベースを更新する保守ポリシー更新手段と,
を有することを特徴とする請求項１記載のネットワーク対応機器。
【請求項８】
前記保守ポリシー更新手段は、前記管理者により入力された保守ポリシーをＸＭＬに変換して、前記保守ポリシーデータベースを更新することを特徴とする請求項７記載のネットワーク対応機器。
【請求項９】
前記保守ポリシー更新手段は、ＸＭＬで記述された前記保守ポリシーが記録された記録媒体を用いて前記保守ポリシーデータベースを更新する、ことを特徴とする請求項７記載

のネットワーク対応機器。
【請求項１０】
前記保守ポリシー更新手段は、ネットワークに接続された端末から入力された保守ポリシーにより前記保守ポリシーデータベースを更新することを特徴とする請求項７記載のネットワーク対応機器。
【請求項１１】
ネットワークを介して保守センタと接続された、保守ポリシーデータベースを備えるネットワーク対応機器を保守する保守方法であって、
前記保守ポリシーデータベースは、前記保守センタによる当該ネットワーク対応機器の保守操作又はネットワーク対応機器の保守に係る保守情報の送信、について規定した保守ポリシーが格納されたデータベースであり、
前記保守ポリシーデータベースを参照して、前記保守情報を前記保守センタに送信する保守情報送信ステップと、
前記保守センタから指示された操作を受信する保守操作指示受信ステップと、
前記保守ポリシーデータベースを参照して、前記保守操作指示受信ステップで受信した操作を行う保守操作制御ステップと、
を有することを特徴とするネットワーク対応機器を保守する保守方法。
【請求項１２】
前記保守ポリシーは、
前記保守情報のうち、前記保守センタに自動的に送信する定期提供保守情報と、
前記定期提供保守情報を前記保守センタに提供するタイミングと、
を規定することを特徴とする請求項１１記載のネットワーク対応機器を保守する保守方法。
【請求項１３】
前記定期提供保守情報を収集する保守情報収集ステップと、
前記保守情報収集ステップにより収集された前記定期提供保守情報を、前記タイミングで、前記保守センタに送信する定期提供情報送信ステップと、
を更に有することを特徴とする請求項１２記載のネットワーク対応機器を保守する保守方法。
【請求項１４】
前記保守センタに操作の指示を問い合わせる操作問い合わせステップを有し、
前記保守操作指示受信ステップは、前記操作問い合わせステップによる操作の指示の問い合わせ、又は、前記定期提供情報送信ステップによる前記定期提供保守情報の送信、に応答して前記保守センタから送信された操作の指示を受信する、
ことを特徴とする請求項１１又は１３記載のネットワーク対応機器。
【請求項１５】
前記保守センタから保守操作の指示を受信した場合に、前記保守センタを認証する第１の保守センタ認証ステップを、更に有することを特徴とする請求項１１記載のネットワーク対応機器を保守する保守方法。
【請求項１６】
前記定期提供情報送信ステップにより前記定期提供保守情報を前記保守センタに送信する場合に、前記保守センタを認証する第２の保守センタ認証ステップを、更に有する、
ことを特徴とする請求項１３記載のネットワーク対応機器を保守する保守方法。
【請求項１７】
前記保守情報送信ステップにより送信される前記保守情報又は前記定期提供情報送信ステップにより送信される前記定期提供保守情報を暗号化する保守情報暗号化ステップを、更に有することを特徴とする請求項１１又は１３記載のネットワーク対応機器を保守する保守方法。
【請求項１８】
当該ネットワーク対応機器を管理する管理者を認証する管理者認証ステップと、

前記管理者認証ステップにより認証された管理者により入力された保守ポリシーで、前記保守ポリシーデータベースを更新する保守ポリシー更新ステップと，
を有することを特徴とする請求項１１記載のネットワーク対応機器を保守する保守方法。
【請求項１９】
前記保守ポリシー更新ステップは、前記管理者により入力された保守ポリシーをＸＭＬに変換して前記保守ポリシーデータベースを更新する、ことを特徴とする請求項１８記載のネットワーク対応機器を保守する保守方法。
【請求項２０】
前記保守ポリシー更新ステップは、ＸＭＬで記述された前記保守ポリシーが記録された記録媒体を用いて前記保守ポリシーデータベースを更新する、ことを特徴とする請求項１８記載のネットワーク対応機器を保守する保守方法。
【請求項２１】
前記保守ポリシー更新ステップは、ネットワークに接続された端末から入力された保守ポリシーにより前記保守ポリシーデータベースを更新する、ことを特徴とする請求項１８記載のネットワーク対応機器を保守する保守方法。
【請求項２２】
請求項１１から２１に記載の方法をコンピュータに実行させるためのプログラム。
【請求項２３】
請求項２２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項２４】
ネットワークを介して接続されたネットワーク対応機器と、当該ネットワーク対応機器の保守操作を行う保守センタとを有する保守システムであって、
前記ネットワーク対応機器は、前記保守センタによる当該ネットワーク対応機器の保守操作又は当該ネットワーク対応機器の保守に係る保守情報の送信、について規定された保守ポリシーが記憶された保守ポリシーデータベースと、
前記保守ポリシーデータベースを参照して、保守情報を前記保守センタに送信する保守情報送信手段と、を有し、
前記保守センタは、前記保守情報送信手段により送信された保守情報を受信する保守情報受信手段と、
前記保守情報受信手段により受信した保守情報に基づいて、前記ネットワーク対応機器に操作を指示する保守操作指示手段を有し、
前記ネットワーク対応機器は、前記保守ポリシーデータベースを参照して、前記保守センタから指示された操作を行う保守操作制御手段と、
を有することを特徴とする保守システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システムに関し、特に、ユーザの設定した保守の方針に従って遠隔から保守が可能なネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システムに関する。
【背景技術】
【０００２】
デジタル複合機や電子文書管理システムなどの製品は，ユーザがその製品を導入してから障害発生を防ぐために状態を監視することや，ソフトウェアのアップデートを行うことなど定期的な保守（メンテナンス）が必要となる。保守作業を製品の設置場所で実施するのは効率的でないため、従来から遠隔保守サービスが行われている。
【０００３】

従来の遠隔保守サービスでは、電話回線を保守対象のデジタル複合機に接続するなどして、回線を通じて対象機器から保守操作を行う。例えば、サービスマンがユーザ先まで行かなくても適切な保守のできるリモートシステムができる発明が提案されている（例えば、特許文献１参照）。当該発明のリモートシステムは、機器の異常を遠隔地で検知して、当該機器の異常の内容を分類し、分類された異常の内容に応じて適切な保守を行うことができる。

【０００４】

近年のネットワークの普及に伴って，保守対象機器もネットワークに接続されるようになり，電話回線だけでなくネットワーク経由で遠隔保守を行えるようにすることが求められる。ネットワークから保守対象機器の保守操作を行うことができれば障害対応を即時に行えるなど利点が多い。

【０００５】

しかしながら、ネットワークを介してユーザの機器にアクセスすることを自由に認めてしまうと、セキュリティの観点から不都合が多い。また、セキュリシー意識や要求されるセキュリシーの程度は、ユーザによって異なる。したがって、保守対象機器の保守をいかに行うかについて一様に定めることは困難である。このため、保守対象機器のユーザ毎に保守の方針（ポリシー）を定め、当該ポリシーに従いネットワークを介して保守がどのように行われるかを定めることが要望される。すなわち、遠隔保守が可能な機器において、保守をどのように実行するかは、機器を使用するユーザのポリシーに従うことが望ましい。

【０００６】

本出願人は、上記の要望に鑑み、保守可能な範囲を保守対象機器に予め設定しておき、保守対象機器を遠隔から保守する際に、保守可能な範囲を制限する発明を提案している。当該発明によれば、認証されたユーザにより保守可能な範囲を設定しておくことができ、遠隔から保守する場合には、設定された以外の保守操作を防止できる。

【特許文献１】特開２０００－１３２３６４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、本願出願人の発明は、保守可能な範囲の記述方法について説明がされておらず、ユーザの保守のポリシーに柔軟に対応して、保守可能な範囲を設定する方法が明らかでない。

【０００８】

また、本願出願人の発明では、遠隔した場所から保守を行う遠隔保守センタ側から保守対象の保守対象機器にアクセスする保守形態しか記載されていない。保守対象機器から、コピー枚数やトナー残量など保守情報を遠隔保守センタに送信することが想定されておらず、遠隔保守センタが保守情報を取得するためには、遠隔保守センタが管理する全ての保守対象機器にアクセスを行わなければならない。

【０００９】

加えて、遠隔保守センタが保守対象機器にアクセスする場合には、いわゆるファイアウォールを通過する必要がある場合が多いが、通常は、外部のネットワークから保守対象機器にアクセスすることは困難である。したがって、遠隔保守センタ側から保守対象機器にアクセスする保守形態では、保守対象の保守対象機器へアクセスできないという不都合がある。

【００１０】

すなわち、従来、ユーザの保守のポリシーに従って、ネットワークを介して保守対象機器の遠隔保守を行えるようにする技術は考案されていなかった。

【００１１】

本発明は、上記問題に鑑み、ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器、ネットワーク対応機器を保守する保守方法、

プログラム、プログラムが記録された媒体及び保守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】

【００１２】

上記問題を解決するため、本発明は、保守操作を指示する保守センタとネットワークを介して接続されたネットワーク対応機器であって、保守センタによる当該ネットワーク対応機器の保守操作又は当該ネットワーク対応機器の保守に係る保守情報の送信、について規定する保守ポリシーが格納された保守ポリシーデータベースと、保守ポリシーデータベースを参照して、保守情報を保守センタに送信する保守情報送信手段と、保守センタから指示された操作を受信する保守操作指示受信手段と、保守ポリシーデータベースを参照して、保守操作指示受信手段により受信した操作を行う保守操作制御手段と、を有することを特徴とするネットワーク対応機器を提供する。本発明によれば、ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器を提供することができる。

【００１３】

また、本発明の一形態において、保守ポリシーは、保守情報のうち、保守センタに自動的に送信する定期提供保守情報と、定期提供保守情報を前記保守センタに送信するタイミングと、を規定することを特徴とする。本発明によれば、ユーザの保守のポリシーに従って、保守センタに自動的に送信する定期提供保守情報と送信するタイミングを、保守ポリシーに規定することができる。

【００１４】

また、本発明の一形態において、ネットワーク対応機器は、定期提供保守情報を収集する保守情報収集手段を有し、保守情報送信手段が、保守情報収集手段により収集された定期提供保守情報を前記タイミングで、保守センタに送信する、ことを特徴とする。本発明によれば、ユーザが保守ポリシーに設定した自動的に送信する定期提供保守情報を、所定のタイミングで、保守センタに送信することができる。

【００１５】

また、本発明の一形態において、ネットワーク対応機器は、保守センタに操作の指示を問い合わせる操作問い合わせ手段を有し、保守操作指示受信手段は、操作問い合わせ手段による操作の指示の問い合わせ、又は、保守情報送信手段による定期提供保守情報の送信、に応答して保守センタから送信された操作の指示を受信することを特徴とする。本発明によれば、ネットワーク対応機器から保守センタとの通信を開始して、その応答として保守センタから送信された操作の指示を受信する。したがって、ファイアウォールにより保守センタからネットワーク対応機器への通信がブロックされていても、保守センタから操作の指示を送信することができる。なお、操作の指示の問い合わせや定期提供保守情報の送信に対しては、保守センタから応答がなくともよい。

【００１６】

また、本発明の一形態において、ネットワーク対応機器は、保守操作指示受信手段により操作の指示を受信した場合に保守センタを認証し、又は、保守情報送信手段により定期提供保守情報を保守センタに送信する場合に保守センタを認証する、保守センタ認証手段を有する、ことを特徴とする。保守センタを認証することで、保守の契約を結んだ保守センタから操作の指示を受信し、また、保守の契約を結んだ保守センタに定期提供保守情報を送信することができる。

【００１７】

また、本発明の一形態において、保守情報送信手段により送信される前記保守情報又は前記定期提供保守情報が、暗号化されていることを特徴とする。前記保守情報又は前記定期提供保守情報が、暗号化されることで改ざんや漏洩が防止できる。

【００１８】

また、本発明の一形態において、ネットワーク対応機器は、当該ネットワーク対応機器を管理する管理者を認証する管理者認証処理手段と、管理者認証処理手段より認証された

管理者により入力された保守ポリシーで、保守ポリシーデータベースを更新する保守ポリシー更新手段と，を有することを特徴とする。管理者を認証することで、管理者以外のユーザ等による保守ポリシーデータベースの更新を防止できる。

【００１９】

また、保守ポリシー更新手段は、管理者により入力された保守ポリシーをＸＭＬに変換して、保守ポリシーデータベースを更新することとしてもよい。ＸＭＬのデータ形式で保存しておくことで、ＳＯＡＰメッセージの利用が容易となり、また、ネットワーク対応機器のＯＳ等に関わらず遠隔保守が可能となる。

【００２０】

また、保守ポリシー更新手段は、ＸＭＬで記述された保守ポリシーが記録された記録媒体を用いて前記保守ポリシーデータベースを更新する、こととしてもよい。ＸＭＬに変換又はＸＭＬで記述された保守ポリシを記録媒体に記録し、当該機録媒体から保守ポリシデータベースを更新することで、ネットワーク対応機器等から入力する作業を省略できる。記録媒体に記録された保守ポリシは、電子署名されていることが好適である。電子署名によりＸＭＬファイルの改ざんを防止できる。

【００２１】

また、ポリシー更新手段は、ネットワークに接続された端末から入力された保守ポリシーにより前記保守ポリシーデータベースを更新することとしてもよい。ネットワーク対応機器ではなく端末から保守ポリシーデータベースを更新できるので、複数のネットワーク対応機器の保守ポリシーデータベースを共通の保守ポリシーで更新したり、同時に複数のネットワーク対応機器の保守ポリシーデータベースを更新できる。

【００２２】

また、上記問題に鑑み、本発明は、ネットワークを介して保守センタと接続された、保守ポリシーデータベースを備えるネットワーク対応機器を保守する保守方法であって、保守ポリシーデータベースは、保守センタによる当該ネットワーク対応機器の保守操作又はネットワーク対応機器の保守に係る保守情報の送信、について規定した保守ポリシーが格納されたデータベースであり、保守ポリシーデータベースを参照して、保守情報を保守センタに送信する保守情報送信ステップと、保守センタから指示された操作を受信する保守操作指示受信ステップと、保守ポリシーデータベースを参照して、保守操作指示受信ステップで受信した操作を行う保守操作制御ステップと、を有することを特徴とする。

【００２３】

本発明によれば、ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器を保守する保守方法を提供することができる。

【００２４】

また、本発明の一形態において、保守ポリシーは、記保守情報のうち、保守センタに自動的に送信する定期提供保守情報と、定期提供保守情報を保守センタに提供するタイミングと、を規定することを特徴とする。

【００２５】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、定期提供保守情報を収集する保守情報収集ステップと、保守情報収集ステップにより収集された前記定期提供保守情報を、所定のタイミングで、保守センタに送信する定期提供情報送信ステップと、を更に有することを特徴とする。

【００２６】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、保守センタに操作の指示を問い合わせる操作問い合わせステップを有し、保守操作指示受信ステップは、操作問い合わせステップによる操作の指示の問い合わせ、又は、定期提供情報送信ステップによる前記定期提供保守情報の送信、に応答して前記保守センタから送信された操作の指示を受信する、ことを特徴とする。

【００２７】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、保守セ

ンタから保守操作の指示を受信した場合に、保守センタを認証する第１の保守センタ認証ステップを、更に有することを特徴とする。

【００２８】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、定期提供情報送信ステップにより定期提供保守情報を保守センタに送信する場合に、保守センタを認証する第２の保守センタ認証ステップを、更に有する、ことを特徴とする。

【００２９】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、保守情報送信ステップにより送信される保守情報又は定期提供情報送信ステップにより送信される定期提供保守情報を暗号化する保守情報暗号化ステップを、更に有することを特徴とする。

【００３０】

また、本発明の一形態において、ネットワーク対応機器を保守する保守方法は、当該ネットワーク対応機器を管理する管理者を認証する管理者認証ステップと、管理者認証ステップにより認証された管理者により入力された保守ポリシーで、保守ポリシーデータベースを更新する保守ポリシー更新ステップと，を有することを特徴とする。

【００３１】

また、本発明の一形態において、保守ポリシー更新ステップは、管理者により入力された保守ポリシーをＸＭＬに変換して保守ポリシーデータベースを更新する、ことを特徴とする。また、本発明の一形態において、保守ポリシー更新ステップは、ＸＭＬで記述された保守ポリシーが記録された記録媒体を用いて保守ポリシーデータベースを更新する、ことを特徴とする。また、本発明の一形態において、保守ポリシー更新ステップは、ネットワークに接続された端末から入力された保守ポリシーにより前記保守ポリシーデータベースを更新する、ことを特徴とする。

【００３２】

また、上記問題に鑑み、本発明は、請求項１１から２１に記載の方法をコンピュータに実行させるためのプログラムを提供する。本発明によれば、ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器のプログラムを提供することができる。

【００３３】

また、上記問題に鑑み、本発明は、請求項２２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【００３４】

また、上記問題に鑑み、本発明は、ネットワークを介して接続されたネットワーク対応機器と、当該ネットワーク対応機器の保守操作を行う保守センタとを有する保守システムであって、ネットワーク対応機器は、保守センタによる当該ネットワーク対応機器の保守操作又は当該ネットワーク対応機器の保守に係る保守情報の送信、について規定された保守ポリシーが記憶された保守ポリシーデータベースと、保守ポリシーデータベースを参照して、保守情報を前記保守センタに送信する保守情報送信手段と、を有し、保守センタは、保守情報送信手段により送信された保守情報を受信する保守情報受信手段と、保守情報受信手段により受信した保守情報に基づいて、ネットワーク対応機器に操作を指示する保守操作指示手段を有し、ネットワーク対応機器は、保守ポリシーデータベースを参照して、保守センタから指示された操作を行う保守操作制御手段とを有することを特徴とする。

【発明の効果】

【００３５】

ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システムを提供することができる。

【発明を実施するための最良の形態】

【００３６】

以下、本発明の好ましい最良の形態について実施例に基づいて図面を参照しながら説明する。本実施例では、保守対象のネットワーク対応機器としてコピー、ファクス、プリント、スキャンの機能を併せ持ち、画像の形成が可能な画像形成装置の機能を有するデジタル複合機（以下、ＭＦＰと称す）を例にして説明する。

【００３７】

図１（ａ）は、ネットワークを介して接続された遠隔保守センタ３とＭＦＰ２とを有する遠隔保守システムの一例を示す。遠隔保守センタ３は、外部のネットワーク１及び内部のネットワーク４を介してＭＦＰ２と接続されている。遠隔保守センタ３は、ＭＦＰ２に設定されている保守ポリシー５に従い、ＭＦＰ２の保守を行う。外部のネットワーク１は主にインターネットであり、内部のネットワーク４は、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）などである。

【００３８】

始めに、保守作業の概略について説明する。本実施例では、ユーザが使用するＭＦＰ２について、ユーザにより定められた保守のセキュリティ方針（以下、保守ポリシーという）に従い、ＭＦＰ２の保守が行われる。また、ＭＦＰ２は、保守に係る情報である保守情報を保有する。保守情報とは、トナー残量やコピー枚数など当該ＭＦＰの保守に関する情報をいう。

【００３９】

本実施例の遠隔保守は、保守ポリシー５に従って行われる。ＭＦＰ２には、保守ポリシー５が格納されている。保守ポリシー５について詳しくは後述するが、保守ポリシー５は、どのような保守情報をどのようなタイミングで遠隔保守センタに送信するのかを規定する部分（保守情報提供ポリシー）と，遠隔保守センタからどのような保守操作を許可するのかを規定する部分（保守操作許可ポリシー）で構成される。保守情報提供ポリシーは，遠隔保守センタ３に提供する保守情報の内容や提供の頻度等を規定する。例えば、トナー残量やコピー枚数の累計は保守情報として30分に一回提供してよいが、ファクス送信のログは提供しないなどである。また，保守操作許可ポリシーは、遠隔保守センタ３が、ＭＦＰ２に対して行うことができる保守の内容を定める。例えば、保守操作許可ポリシーとしては，例えばコピーカウンタのリセットは許可するが、再起動は許可しない、などが設定できる。

【００４０】

図1（ｂ）は、本実施例のＭＦＰ２における遠隔保守操作の概略を示すフローチャート図の一例を示す。ＭＦＰ２は、遠隔保守センタ３により保守操作を指示されると（ステップＳ１のＹｅｓ）、当該保守操作が許可されているかどうか保守ポリシー５を参照する（ステップＳ２）。ＭＦＰ２は、指示された操作のうち許可されている保守操作を実行する（ステップＳ３）。なお、操作の指示として、保守情報の取得、という指示があった場合は、保守情報のうち、保守情報提供ポリシーで許可されていない保守情報については、遠隔保守センタに提供されない。

【００４１】

遠隔保守センタ３から操作の指示がない場合には（ステップＳ１のＮｏ）、新しい保守ポリシーの入力があるか否かが判断される（ステップＳ４）。ＭＦＰ２に保守ポリシー５を設定することができるのは、ＭＦＰ２の管理者であり、例えばユーザＩＤお及びパスワードにより管理者を認証する。保守ポリシー５を設定する権限のある管理者であることと認証されると、ＭＦＰ２は保守ポリシー５を設定する画面を表示してユーザに保守ポリシーを入力させる。新しい保守ポリシーは、保守ポリシーを格納する保守ポリシーデータベースに格納される（ステップＳ５）。ＭＦＰ２は、格納された保守ポリシーから、遠隔保守センタ３に送信するタイミングを抽出する（ステップＳ６）。

【００４２】

保守操作や新しい保守ポリシーの入力がなされない場合には（ステップＳ４のＮｏ）、遠隔保守センタ３に送信するタイミングを待って（ステップＳ７のＹｅｓ）、保守情報が定期的に遠隔保守センタに送信される。ＭＦＰ２は、保守ポリシー５を参照して、保守ポ

リシー５で規定されている定期的に送信する保守情報を収集する（ステップＳ８）。ＭＦＰ２は、収集された保守情報を、遠隔保守センタ３に送信する（ステップＳ９）。なお、操作の指示の判定（ステップＳ１）や保守ポリシーの入力の判定（ステップＳ４の）の処理は、割り込みにより行われるとしてもよい。

【００４３】

〔遠隔保守センタのハードウェア及び機能構成〕

遠隔保守センタ３のハードウェア構成について図２（ａ）に基づき説明する。遠隔保守センタ３は、例えばコンピュータであり、それぞれバスを介して相互に接続されたＣＰＵ４１（中央処理装置）、Ｉ／Ｏ制御部４２（入出力制御装置）、ドライブ装置４３、通信部４４，主記憶装置４５、記憶装置４６、を有するように構成される。

【００４４】

ＣＰＵ４１は、遠隔保守センタ３が行う処理を統括的に制御する。Ｉ／Ｏ制御装置は、記憶装置４６やドライブ装置４３とのデータの入出力を制御する。ドライブ装置４３は、記録媒体４７からプログラムやデータを読み込み、又、記録媒体４７にプログラムやデータを書き込む。通信部４４は、ネットワーク１に接続する為のインターフェースであり、例えばモデム，ルータ等で構成される。主記憶装置４５は、オペレーティングシステムやプログラム、データを一時保管する記憶領域である。記憶装置４６は、プログラム、データの保管装置である。記録媒体４７は、遠隔保守センタ３の各種機能を提供するプログラムが記録された記録媒体であり、例えばＣＤ－ＲＯＭ等である。記録媒体４７は、ドライブ装置４３にセットされ、遠隔保守センタ用プログラムがドライブ装置４３を介して記憶装置４６にインストールされる。

【００４５】

遠隔保守センタ用プログラムを記録した記録媒体４７は、ＣＤ－ＲＯＭ、フレキシブルディスク、光磁気ディスク（ＭＯ）等の様に情報を光学的，電気的或いは磁気的に記録する記録媒体、ＲＯＭ、フラッシュメモリ等の様に情報を電気的に記録する半導体メモリ等、様々なタイプの記録媒体を用いることが可能である。

【００４６】

続いて、遠隔保守センタ３の機能について説明する。図２（ｂ）は、遠隔保守センタ３の機能構成図の一例を示す。遠隔保守センタ３は、通信手段１１、保守情報受信手段１２及び保守操作指示手段１３を有するように構成される。通信手段１１は、主にＭＦＰ２とネットワーク１を介して通信を行う。保守情報受信手段１２は、通信手段１１を介して、ＭＦＰ２から保守情報を受信する。受信した保守情報は保守操作指示手段１３に出力される。保守操作指示手段１３は、ＭＦＰ２が送信した保守情報に基づき、通信手段１１を介して、当該ＭＦＰ２に適切な保守操作を指示する。

【００４７】

〔ＭＦＰ２の機能構成〕

次に、ＭＦＰ２の機能について図３に基づき説明する。ＭＦＰ２は、保守処理部２０、ポリシー判定処理部２１、センタ認定処理部２２、保守情報管理部２３、主機能制御部２４、ポリシー管理部２５、ユーザ認証処理部２６、ポリシー設定処理部２７、を有するように構成される。

【００４８】

ポリシー設定処理部２７は、ユーザとＭＦＰ２とのインターフェイスを提供し、ユーザにより入力される内容に応じて、当該内容を他の機能に出力する。ユーザ認証処理部２６は、ユーザにより入力されポリシー設定処理部２７から受け取ったユーザＩＤ及びパスワードに基づき、ユーザを認証する。したがって、ユーザ認証処理部２６は、管理者認証手段の機能を提供する。

【００４９】

ポリシー管理部２５は、現在設定されている現保守ポリシーを呼び出し、また、保守ポリシー５をユーザにより設定された新しい新保守ポリシーで更新する。ポリシー管理部２５は、保守ポリシーが格納された保守ポリシーデータベース２９を有する。したがって、

ポリシー管理部２５は、保守ポリシー更新手段の機能を提供する。

【００５０】

保守処理部２０は、保守情報を保守ポリシーに設定されたタイミングで、遠隔保守センタ３に送信し、また、遠隔保守センタ３からの保守操作の指示を受信する。ファイアウォールにより遠隔保守センタ３から保守操作の指示ができない場合にも、保守操作が行われるように定期的に、保守操作の指示の有無を遠隔保守センタ３に問い合わせる。したがって、保守処理部２０は、保守情報送信手段、保守操作指示受信手段及び操作問い合わせ手段の機能を提供する。

【００５１】

ポリシー判定処理部２１は、遠隔保守センタ３に指示された保守操作が、保守ポリシーにおいて許可されているか否かを判定する。センタ認証処理部２２は、所定の認証方式を用い、遠隔保守センタ３が、保守契約をしている遠隔保守センタであるか否かなどの認証を行う。したがって、センタ認証処理部２２は、保守センタ認証手段の機能を提供する。

保守情報管理部２３は、保守情報の読み出しや更新などを管理する。主機能制御部２４は、マシンの再起動やＨＤＤフォーマットなどの保守操作を行う。したがって、主機能制御部２４は、保守操作制御部の機能を提供する。

【００５２】

〔保守ポリシーについて〕

保守ポリシーについて詳細に説明する。上述のとおり、保守ポリシーは、保守情報提供ポリシーと保守操作許可ポリシーとで構成される。保守情報提供ポリシーは、保守情報の種別に対応づけて、当該保守情報の遠隔保守センタ３への提供の許可／禁止と、提供のタイミングを規定する。保守操作許可ポリシーは、各保守操作に対応づけて、遠隔保守センタ３による保守操作の許可／禁止を規定する。

【００５３】

図４（ａ）は、保守情報提供ポリシーの一例を、図４（ｂ）は、保守操作許可ポリシーの一例を、それぞれ示す。保守情報提供ポリシーは、自動提供インターバル、単位、定期提供保守情報の種別、保守情報の種別、の項目を有する。自動提供インターバルは、保守情報を自動的に提供するタイミングを規定する。単位は、自動提供インターバルで設定されたタイミングの単位であり、例えば、時間や分、秒で表される。定期提供保守情報の種別は、自動的に遠隔保守センタ３に提供される保守情報である。例えば、図４（ａ）では、機種番号、コピーカウンタ、トナー残量が設定されている。定期提供保守情報の種別に何も設定しておかなくともよい。保守情報の種別は、例えば、機種番号、ＩＰアドレス、ＭＡＣアドレス、ファームウェアバージョン、コピーカウンタ、トナー残量、等である。機種番号は、当該ＭＦＰを識別する番号である。ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレスにより、外部のネットワークから通信可能となり、ＭＡＣ（Media Access Control）アドレスによりＬＡＮ内のアドレスが特定できる。ファームウェアバージョンは、当該ＭＦＰにインストールされているファームウェアのバージョンを表す。コピーカウンタは、当該ＭＦＰが納入されてからや最後の保守からのコピー枚数である。トナー残量は、トナーの残量である。各保守情報の種別毎に許可／禁止を設定でき、許可と設定された種別の保守情報は、遠隔保守センタの指示により、遠隔保守センタ３へ送信される。

【００５４】

保守操作許可ポリシーは、マシンの再起動、ＨＤＤフォーマット、アドレス帳クリア、管理者パスワードクリア、保守情報取得、等の保守操作を有し、各保守操作毎に許可／禁止を設定できる。許可と設定された保守操作は、遠隔保守センタ３の指示のより操作されることが可能となる。

【００５５】

管理者は、例えばＭＦＰのタッチパネルなどから各項目を設定する。図５（ａ）は、保守情報ポリシーの設定画面の一例を、図５（ｂ）は、保守操作許可ポリシーの設定画面の一例を、それぞれ示す。保守情報ポリシー及び保守操作許可ポリシーの設定画面は、キーボードに触れることで数値を入力でき、許可／禁止の項目は、触れることで選択できる。

例えば、自動提供インターバルは、キーボードの３と０に触れると３０と入力され、自動提供インターバルの単位は、「分」の部分を触れるたびに、時間、分、秒と切り替わる。定期提供保守情報の種別は、保守情報種別の番号を、キーボードに触れることで入力する。また、許可／禁止のうち、選択されたいずれか一方は、四角で囲まれる。管理者が、終了ボタンに触れると設定が終了する。

【００５６】

また、図５（ａ）又は（ｂ）のように項目を個別に操作するのではなく、保守ポリシーの各項目を一回の操作で設定できるようにしてもよい。図６（ａ）はスライダ式の保守ポリシーの設定画面を、図６（ｂ）はプルダウン選択式の保守ポリシーの選択画面の、それぞれ一例を示す。図６（ａ）又は（ｂ）の設定画面では、例えば、「全て禁止」、「高」、「中ー高」、「中」、「低」、「全て許可」のように、保守ポリシーのセキュリティレベルを選択できる。各セキュリティレベルに対応づけられて、予め、各保守ポリシーを許可／禁止のいずれに設定するかの組み合わせ、定期提供保守情報の種別、自動提供インターバル、が定められている。したがって、管理者がいずれかのセキュリティレベルを選択することで、保守ポリシーの各項目が自動的に設定される。なお、各セキュリティレベルと、各保守ポリシーの許可／禁止の対応づけ等を、管理者が行えるようにしてもよい。

【００５７】

管理者により入力された保守ポリシーは、ＸＭＬ形式のＸＭＬデータとして生成される。図７は、図５又は６の画面から入力された保守ポリシーに基づき生成されたＸＭＬデータの一例を示す。終了ボタンに触れられると、図３のポリシー設定処理部２７は、入力された保守ポリシーの設定内容から図７のようにＸＭＬデータを生成する。ＸＭＬデータは、ポリシー管理部２５へ出力され、ポリシー管理部２５は、ＸＭＬデータをファイルとして保守ポリシーデータベース２９に格納する。

【００５８】

また、保守ポリシーは、ＭＦＰ２のタッチパネル等ではなく、内部のネットワーク４やインターネット１に接続された端末から入力してもよい。図８（ａ）は、端末１０が接続された遠隔保守システムの一例を示す。図８（ａ）において、図１と同一構成部分には同一の符号を付しその説明は省略する。端末１０は例えば、コンピュータである。端末１０から保守ポリシーを入力する場合には、保守ポリシーを設定するためのプログラムを立ち上げ、入力する。図８（ｂ）は、端末１０に表示された保守ポリシーを設定するための画面の一例を示す。保守ポリシーの各項目は、認証された管理者により設定される。保守ポリシーの設定が終了したら、終了ボタンが押下されることで、保守ポリシーがＸＭＬに変換される。図８（ｂ）の保守ポリシー５は、ＸＭＬで記述されている。ＸＭＬで記述された保守ポリシー５は、ＭＦＰ２へ送信され、保守ポリシーデータベース２９に格納されている現行の保守ポリシーを更新する。

【００５９】

なお、保守ポリシー５は、ＭＦＰ２や端末１０から入力しなくともよい。例えば、管理者が予めＸＭＬデータを作成しておき、ＭＦＰ２に設定するようにしてもよい。管理者はＸＭＬで記述した保守ポリシーをファイルとしてＦＤやスマートカードのような記録媒体に格納しておく。ＭＦＰ２に保守ポリシーを設定する際には、保守ポリシーの各項目（許可／禁止）を入力するのではなく、ＸＭＬデータが記録されたＦＤやスマートカードをＭＦＰ２にセットする。ＭＦＰ２のポリシー設定処理部２７は、ＭＦＰ２にセットされたＦＤやスマートカードからそのXMLファイルを読み取って保守ポリシーとして保守ポリシーデータベース２９に格納する。

【００６０】

また、ＦＤに記録した保守ポリシーを他者に渡して、ＭＦＰ２に保守ポリシーを設定するような場合、ＦＤ内の保守ポリシー（ＸＭＬデータ）が不正に改ざんされる可能性がある。これを防ぐために、ＸＭＬデータには例えば管理者が電子署名を付与しておくことが好適である。ポリシー設定処理部２７はＭＦＰにセットされたＦＤやスマートカードからそのＸＭＬデータを読み取って保守ポリシーとしてポリシー管理部２５に設定する際に、

その付与されている電子署名を参照し、ＸＭＬデータの正当性が確認されたらポリシー管理部２５に当該ＸＭＬデータを設定する。

【００６１】

ＸＭＬファイルへ電子署名を付与する方式としては、例えばＸＭＬ Signature（IETF RFC3275）のようにＸＭＬ構造にあわせた電子署名方式を用いてもよいし、ＸＭＬファイルを単にデータとして扱ってPKCS（Public Key Cryptography Standards）＃7のような電子署名方式を用いてもよい。

【００６２】

（通信のインターフェイスについて）

以降では、これまで説明した構成及び機能に基づき、遠隔保守センタ３によるＭＦＰ２の保守について詳細に説明する。

【００６３】

ところで、遠隔保守センタ３とＭＦＰ２とは、複数の通信を繰り返す。例えば、保守情報を送信するだけでなく、保守契約をしている保守対象機器であるかどうかの確認を行うことや、正しい遠隔保守センタ３へ接続しているかどうかの認証を行うことなどである。このような通信を行うためには、ＨＴＴＰ上でＳＯＡＰ（Simple Object Access Protocol）を用いることが好適である。

【００６４】

ＳＯＡＰは、ＸＭＬで記述されたメッセージを使用して、ネットワーク上のコンピュータのオブジェクト（データ）にアクセスを可能とする。ＳＯＡＰは、ＯＳやプログラム言語に依存しないでデータにアクセス可能であるので、種々の保守対象機器やコンピュータであっても、アーキテクチャの相違に影響されずにデータの加工や処理ができる。

【００６５】

以下の説明では、遠隔保守センタ３による保守操作を、ＳＯＡＰメッセージにより行う。遠隔保守センタ３からＭＦＰ２に送信されるＳＯＡＰメッセージには、ＭＦＰ２の処理で使用される複数のＳＯＡＰインターフェイスが含まれているので、保守処理部２０は処理の内容に応じてＳＯＡＰインターフェイスを図３に示される各機能構成部に振り分けて出力する。

【００６６】

〔保守ポリシーの入力における管理者の認証〕

保守ポリシーは、保守情報の送信や保守操作の許可又は禁止を規定するものであるので、保守ポリシーを管理する管理者以外のものが更新できないことが好ましい。保守ポリシーを入力する際の認証について説明する。

【００６７】

図９は、管理者によりＭＦＰ２に保守ポリシー５が設定される際のシーケンスを表すシーケンス図の一例を示す。保守ポリシーを設定する場合、ユーザは、ユーザＩＤ及びパスワードを入力する（Ｓ１０１）。例えば、「authenticateAdmin(String name, String password): String session」というＳＯＡＰインターフェイスが呼び出され、nameにはユーザＩＤ、passwordにはパスワードが格納される。ユーザＩＤ及びパスワードが入力されると、ポリシー設定処理部２７が、ユーザＩＤ等をユーザ認証処理部２６に出力する（Ｓ１０２）。

【００６８】

ユーザ認証処理部２６は、ユーザＩＤとパスワードの整合性に基づき、ユーザを認証する（Ｓ１０３）。ユーザＩＤとパスワードの整合性がある場合には、ユーザ認証がされた旨の信号がポリシー設定処理部２７に出力される（Ｓ１０４）。ユーザ認証がされた旨の信号は、戻り値sessionに格納される。

【００６９】

認証された場合には、ポリシー設定処理部２７は、ポリシー管理部２５に現保守ポリシーを要求する（Ｓ１０５）。例えば、「getCurrentRemoteMaintenancePolicy(String session): byte[] policy」というＳＯＡＰインターフェイスが呼び出される。ポリシー管理

部２５は、現保守ポリシーを読み出して（Ｓ１０６）、policyに現保守ポリシーを格納し、ポリシー設定処理部２７に出力する（Ｓ１０７）。ポリシー設定処理部２７は、保守ポリシー設定画面を表示すると共に、現保守ポリシーを保守ポリシー設定画面に表示する（Ｓ１０８）。ユーザは、保守ポリシー設定画面に表示された現保守ポリシーを参照して、新しい保守ポリシーを入力できる。

【００７０】

ユーザにより入力された新保守ポリシー（Ｓ１０９）は、ポリシー設定処理部２７によりポリシー管理部２５へ出力される（Ｓ１１０）。ポリシー設定処理部２７により、例えば、「setNewRemoteMaintenancePolicy(String session, byte[] policy): String error」というＳＯＡＰインターフェイスが呼び出される。Policyに格納された新保守ポリシーは、ポリシー管理部２５へ出力される。ポリシー管理部２５は、新保守ポリシーで現保守ポリシーを更新する（Ｓ１１１）。また、ポリシー管理部２５は、保守ポリシーの更新が完了した旨の信号をerrorに格納し、ポリシー設定処理部２７に出力する（Ｓ１１２）。

【００７１】

次いで、ポリシー設定処理部２７は、新保守ポリシーの設定が完了した旨を保守ポリシー設定画面に表示する（Ｓ１１５）。また、ポリシー設定処理部２７は、保守処理部２０に、新しい保守ポリシーが設定された旨の信号を出力する（Ｓ１１３）。

【００７２】

新しい保守ポリシーが設定されると、保守情報を定期的に遠隔保守センタ３へ提供する自動提供インターバルなどが変更されるため、保守処理部２０は、新保守ポリシーに基づき保守情報の提供処理を開始する（Ｓ１１４）。保守情報の提供処理について詳しくは後述する。

【００７３】

以上で、ユーザの保守のポリシーに基づき、保守ポリシーが設定された。なお、ユーザ認証の方式は指紋などを用いた生体認証方式やスマートカードを用いたＰＫＩ（Public Key Infrastructure）ベースの認証方式でも良い。

【００７４】

保守ポリシーは、ユーザにおけるＭＦＰ２の保守の方針を定めるものであるため、管理者以外により保守ポリシーが設定されようとした場合や、遠隔保守センタ３から保守ポリシーが設定されようとした場合などは保守ポリシーが設定されない。

【００７５】

図１０は、ＭＦＰ２に管理者以外の者が保守ポリシー５を設定する場合、したがってユーザ認証が失敗する場合のシーケンスを表すシーケンス図の一例を示す。ユーザは、ユーザＩＤ及びパスワードを入力する（Ｓ２０１）。ポリシー設定処理部２７は、入力されたユーザＩＤ等をユーザ認証処理部２６に出力する（Ｓ２０２）。

【００７６】

ユーザＩＤ及びパスワードを取得したユーザ認証処理部２６は、ユーザＩＤとパスワードの整合性に基づき、ユーザを認証する（Ｓ２０３）。ユーザＩＤとパスワードの整合性がとれない場合には、ユーザ認証ができない旨の信号がポリシー設定処理部２７に出力される（Ｓ２０４）。ポリシー設定処理部２７は、認証エラー画面を表示して処理を終了する（Ｓ２０５）。ユーザが認証されなかった場合、保守ポリシー設定画面は表示されない。

【００７７】

図１１は、遠隔保守センタ３から保守ポリシーが設定されようとした場合のシーケンスを表すシーケンス図の一例を示す。まず、遠隔保守センタ３が、ＭＦＰ２に認証要求を行う（Ｓ３０１）。本実施例では、認証方式として、チャレンジ／レスポンス方式を用いる。保守処理部２０は、センタ認証処理部２２にチャレンジを要求する（Ｓ３０２）。センタ認証処理部２２は、チャレンジを生成し（Ｓ３０３）、生成したチャレンジを守処理部２０へ出力する（Ｓ３０４）。

【００７８】

保守処理部２０は、チャレンジを遠隔保守センタ３へ送信する（Ｓ３０５）。遠隔保守センタ３は、チャレンジを受信し、次いで、当該チャレンジに秘密（Secret）を用いて演算を施し、認証データを生成する。遠隔保守センタ３は、生成した認証データを保守処理部２０に送信する（Ｓ３０６）。

【００７９】

保守処理部２０は、受信した認証データをセンタ認証処理部２２に出力する（Ｓ３０７）。センタ認証処理部２２は、遠隔保守センタ３と共有している秘密（Secret）によりチャレンジに施した演算の演算結果と、遠隔保守センタ３から送信された認証データとが等しいか否かにより、遠隔保守センタ３を認証する。演算結果と認証データとが等しい場合には、認証された旨の信号が保守処理部２０に出力される（Ｓ３０９）。保守処理部２０は、当該信号を、遠隔保守センタ３に送信する（Ｓ３１０）。

【００８０】

認証された遠隔保守センタ３は、保守ポリシーの設定の指示を保守処理部２０に行う（Ｓ３１１）。しかしながら、保守ポリシーの設定は、管理者のみが行えるように予め設定されているため、保守処理部２０は、管理者以外からの保守ポリシーの設定指示に対し、保守操作のエラー信号を遠隔保守センタ３に送信する（Ｓ３１３）。

【００８１】

遠隔保守センタ３は、後述するように、保守操作を行う場合にも認証されることが必要だが、認証されても保守ポリシーを更新する権限は与えられない。図１０及び図１１のシーケンス図に示されるように、管理者以外は保守ポリシーを設定できないので、セキュリシーが守られる。

【００８２】

なお、保守ポリシーにおいて、遠隔保守センタ３による保守ポリシーの書き換えの許可／禁止を規定してもよい。管理者が保守ポリシーにおいて保守ポリシーの書き換えを「許可」に設定していた場合には、遠隔保守センタ３により保守ポリシーの書き換えが可能となる。保守ポリシーの書き換えが「禁止」に設定されていた場合には、管理者が「許可」に設定しない限り、保守ポリシーの書き換えはできない。ユーザに自由度を与えることにより、ユーザの保守ポリシーにしたがって、外部のネットワーク１から機器を保守できる。

【００８３】

〔遠隔保守センタによる保守操作〕

続いて、遠隔保守センタ３が、ＭＦＰ２に対して保守操作を行う処理について説明する。図１２は、遠隔保守センタ３が、保守ポリシーで許可されている範囲の保守情報の保守操作を行うシーケンス図を示す。

【００８４】

最初に、遠隔保守センタ３は、保守処理部２０に認証要求を行う（Ｓ４０１）。認証は、管理者の認証の場合と同様に、チャレンジ／レスポンス方式を用いる。保守処理部２０は、センタ認証処理部２２にチャレンジを要求する（Ｓ４０２）。チャレンジを要求する場合、例えば、「getChallenge(): byte[] challenge」というＳＯＡＰインターフェイスが呼び出される。

【００８５】

チャレンジを要求されたセンタ認証処理部２２は、チャレンジを生成して戻り値challengeに格納し（Ｓ４０３）、保守処理部２０に出力する（Ｓ４０４）。チャレンジを取得した保守処理部２０は、チャレンジを遠隔保守センタ３へ送信する（Ｓ４０５）。

【００８６】

チャレンジを受信した遠隔保守センタ３は、当該チャレンジに秘密（Secret）を用いて演算を施すことで認証データを生成し、認証データを保守処理部２０に送信する（Ｓ４０６）。　次いで、保守処理部２０は、認証データをセンタ認証処理部２２に出力する（Ｓ４０７）。認証を要求する場合、例えば「internalAuthenticate(byte[] authCode): String session」というＳＯＡＰインターフェイスが呼び出される。authCodeには、遠隔保

守センタ３が秘密（Secret）によりチャレンジに施した演算により得られる認証データが格納されている。

センタ認証処理部２２は、遠隔保守センタ３と共有している秘密（Secret）によりチャレンジに演算した演算結果と、遠隔保守センタ３から送信された認証データとが等しいかどうかにより、遠隔保守センタ３を認証する（Ｓ４０８）。認証結果に応じて戻り値sessionに数値が格納され、保守処理部２０へ出力される（Ｓ４０９）。

【００８７】

認証された場合には（Ｓ４１０）、遠隔保守センタ３は、保守処理部２０に、保守操作を指示する（Ｓ４１１）。図１３は、保守操作を指示する場合のＳＯＡＰインターフェイスの一例を示す。段落４５１では、保守操作を指定するためにsession、operation、parameterが用いられ、保守操作の結果が戻り値resultに格納される。例えば、sessionにセッションＩＤを格納して当該保守操作を特定する。operationには保守操作の種別を格納し、parameterには当該種別の保守操作を行うためのパラメータが格納される。段落４５１の３，４行目では、parameterの型を定義している。nameにはパラメータの名前が格納され、valueにはパラメータの値が格納される。段落４５２では、保守操作の結果が格納されるresultの型が定義されている。保守操作が正常に終了しなかった場合には、errorにエラーコードが格納され、resultには保守操作の操作結果が格納される。

【００８８】

段落４５３及び４５４では、operationの内容が定義されている。一例として、段落４５３では、保守操作としてマシンの再起動させるMachine Rebootingが、段落４５４では、保守操作として保守情報を取得させるMaintenance Info Retrievalが、それぞれ定義されている。マシンの再起動の場合は、段落４５３の２，３行目で、何分後に再起動するのかが定義されている。保守情報を取得させる場合は、段落４５４の２，３行目で、取得する情報が定義されている。

【００８９】

図１２に戻り、ＳＯＡＰインターフェイスを受信した保守処理部２０は、ポリシー判定処理部２１に、当該保守操作が認められているか否かの判定を依頼する（Ｓ４１２）。判定を依頼されたポリシー判定処理部２１は、まず、ポリシー管理部２５に、現保守ポリシーの取得を依頼する（Ｓ４１３）。ポリシー管理部２５は、現保守ポリシーを読み出し（Ｓ４１４）、ポリシー判定処理部２１に出力する（Ｓ４１５）。

【００９０】

現保守ポリシーを取得したポリシー判定処理部２１は、現保守ポリシーと遠隔保守センタ３により指示された保守操作の内容を比較して、許可された保守操作であるか否かを判定する（Ｓ４１６）。図１４（ａ）及び（ｂ）は、ポリシー判定処理部２１が行う保守ポリシーの判定処理におけるＳＯＡＰインターフェイスの擬似コードの一例を示す。まず、図１４（ａ）のOperationResult performRemoteOperationにより、sessionが有効かどうか判定する。sessionが有効でない場合には、エラーコード として"BAD_SESSION_ERROR"が返り、処理が終了する。

【００９１】

sessionが有効である場合には、ポリシー判定結果としてisAllowedOperation(operation, params)のoperationに保守操作の種別が，paramsに当該保守操作のためのパラメータが格納される。現保守ポリシーでは、遠隔保守センタ３から指示された保守操作が許可されていない場合には、エラーコード として"NOT_PERMITTED"が返され、終了する。

【００９２】

sessionが有効である場合、より詳細には、図１４（ｂ）に示される処理が行われる。isAllowedOperation(operation, params)が呼び出されると、ポリシー判定処理部２１は、保守ポリシーファイル（ＸＭＬデータ）を開いて保守ポリシーをメモリ上に読み込む。次いで、図７で説明したＸＭＬデータにおいて、<RemoteMaintenancePolicy>要素の下の<PolicyElement>要素における<Name>要素の内容がoperationに一致するものを探す。一致する<Name>要素が一つもない場合には、false（「禁止」）が返されて終了する。一致する<

Name>要素が存在した場合には、当該<Name>要素の<Permission>要素を参照して、allowed又はdeniedかに応じて、保守操作が許可されているか否かを判定する。

【００９３】

図１２に戻り、ポリシー判定処理部２１は、現保守ポリシーを参照した結果、保守操作が許可されているか否かの判定結果を保守処理部２０へ出力する（Ｓ４１７）。保守処理部２０は、許可された保守操作について、主機能制御部２４に保守操作の処理を依頼する（Ｓ４１８）。保守操作を依頼された主機能制御部２４は、依頼された保守操作を行う（Ｓ４１９）。

【００９４】

図１５は、保守操作処理部２４が保守操作を行う際のＳＯＡＰインターフェイスの擬似コードの一例を示す。OperationResult performOperationが呼び出されると、operationの内容に応じて保守操作の内容が指定される。paramsには、保守操作に必要なパラメータが格納されている。図１５の擬似コードでは、一例として、マシン再起動（Machine Rebooting）、ＨＤＤフォーマット（HDD Formatting）、保守情報の取得（Maintenance Info Retrieval）について記述されている。operationが、Machine Rebootingであった場合は、paramsを参照して再起動の時刻を取得する。次いで、再起動の時刻をＭＦＰ２のタッチパネル等に表示し、ＭＦＰの主機能制御部に時刻を指定した再起動の指示を出す。operationが、HDD Formattingであった場合は、ＭＦＰの主機能制御部にＨＤＤのフォーマットを指示する。operationが、Maintenance Info Retrievalであった場合は、保守情報を取得する。いずれの処理の場合も、処理結果を返して終了する。

【００９５】

図１２に戻り、保守操作処理部２４は、戻り値などを保守処理部２０へ出力する（Ｓ４２０）。保守処理部２０は、当該戻り値などを遠隔保守センタ３へ送信する（Ｓ４２１）。以上で、遠隔保守センタ３による保守操作が完了する。

【００９６】

なお、図１２のシーケンス処理では、遠隔保守センタ３の認証方式としてチャレンジ／レスポンス方式を示しているが、認証方式はいかなる方式であってもよい。上述したように，遠隔保守センタ３と保守対象のＭＦＰ２との間で、SSLのセッションを確立できるネットワーク環境がある場合には、SSLを用いて遠隔保守センタ３を認証すると共に、その後にやり取りする保守操作の改ざん、盗聴を防ぐ方式にしてもよい。また、図１２では保守操作を行う機能を主機能制御部２４としたが，例えばＭＦＰ２のコピー枚数カウンタのクリアといった保守操作の場合は、保守操作の対象が保守情報管理部２３となることもある。遠隔保守センタ３の認証に失敗した場合は、保守操作の指示は受け付けず、遠隔保守センタ３にエラーが通知されて処理を終了する。

【００９７】

〔ＭＦＰから遠隔保守センタへの保守情報の送信〕

ＭＦＰ２は、保守ポリシーの自動提供インターバルに設定されたタイミングで、定期提供保守情報を保守情報を遠隔保守センタ３へ送信する。これにより、遠隔保守センタ３は、例えばトナー残量やコピー枚数の累計などの保守情報を取得でき、保守情報に応じて遠隔保守を行うことができる。図１６は、保守対象のＭＦＰ２が、保守ポリシーに規定された定期提供保守情報を、自動提供インターバルに設定されたタイミングで遠隔保守センタ３へ送信するシーケンス図を示す。最初に、保守処理部２０は、ポリシー判定処理部２１に、定期提供保守情報の種別を問い合わせる（Ｓ５０１）。

問い合わせを受けたポリシー判定処理部２１は、ポリシー管理部２５に現保守ポリシーの取得を依頼する（Ｓ５０２）。ポリシー管理部２５は、現保守ポリシーを読み出し（Ｓ５０３）、ポリシー判定処理部２１に現保守ポリシーを出力する（Ｓ５０４）。

現保守ポリシーを取得したポリシー判定処理部２１は、保守ポリシーのうち、定期提供保守情報の種別に記録されている保守情報の種別を抽出する（Ｓ５０５）。また、ポリシー判定処理部２１は、保守ポリシーの自動提供インターバルに設定されている時間間隔を抽出する（Ｓ５０５）。抽出された定期提供保守情報及び自動提供インターバルは、保守処

理部２０へ出力される（Ｓ５０６）。
【００９８】
保守処理部２０は、定期提供保守情報を取得するように、保守情報管理部２３へ依頼する（Ｓ５０７）。保守情報管理部２３は、保守処理部２０から依頼された定期提供保守情報を取得し（Ｓ５０８）、保守管理部２１へ出力する（Ｓ５０９）。
【００９９】
保守処理部２０は、保守情報管理部２３から取得した定期提供保守情報を、自動提供インターバルに従って遠隔保守センタ３へ送信する（Ｓ５１０）。保守情報を受信した遠隔保守センタ３は、正常に保守情報が受信された旨の信号を保守処理部２０へ送信する（Ｓ５１１）。以上で、ＭＦＰ２から遠隔保守センタ３へ、保守情報を送信する処理が終了する。ＭＦＰ２は、自動提供インターバルに従い、図１６のシーケンスに示される処理を繰り返す。自動提供インターバルの抽出は、保守ポリシーが更新された場合にのみ行うようにしてもよい。
【０１００】
図１７は、保守処理部２０が、定期提供保守情報を保守ポリシーの自動提供インターバルで規定されているタイミングで遠隔保守センタ３へ送信する処理を行うＳＯＡＰインターフェイスの擬似コードの一例を示す。保守処理部２０は、新しい保守ポリシーが設定された旨の信号を受けて、例えば図１７のような処理を開始する。
まず、保守処理部２０は、ＳＯＡＰインターフェイスAutoProvisionを呼び出す。ポリシー管理部２５は、保守ポリシーファイル（ＸＭＬデータ）を保守ポリシーデータベースから開き保守ポリシーをメモリ上に読み込む。次いで、図７で説明したＸＭＬデータにおいて、<InfoProvisionPolicy>要素の下位の<AutoProvision>要素にある<Interval>要素から、保守ポリシーの自動提供インターバルを抽出する。
【０１０１】
続いて、ポリシー管理部２５は、<InfoList>要素の下に列挙されている情報種別のリストを取得する。これにより、保守情報を提供する自動提供インターバル、定期提供保守情報の種別が取得された。保守処理部２０は、自動提供インターバル毎に、定期提供保守情報を保守情報管理部２３から取得し、取得した保守情報を遠隔保守センタ３に送信する。保守ポリシーを自動提供インターバル毎に送信する処理は、管理者により保守ポリシーが更新されるまで繰り返し行われる。
【０１０２】
ＭＦＰ２が、保守情報を遠隔保守センタ３へ送信するＳＯＡＰインターフェイスについて説明する。ＭＦＰ２は、定期提供保守情報を遠隔保守センタ３へ送信するため、遠隔保守センタ３が提供する、例えば、sendMaintenanceInfo(byte[] random, byte[] authCode, String targetId, Parameter[] params): String error、のようなＳＯＡＰインターフェイスを、呼び出す。呼び出した当該ＳＯＡＰインターフェイスの、randomとauthCodeには保守対象となるＭＦＰを認証するためのパラメータを格納し、targetIdには保守対象のＭＦＰの識別情報を格納する。
【０１０３】
また、paramsには、提供される保守情報を格納する。例えば、params[0].name を "Machine Number"として、params[0].value に製品番号 "23094203-777635"を格納し、また、params[1].nameを "Firmware Versions"として、params[1].valueにファームウェアバージョン "OS: 5.05, Main: 2.00, Sub: 1.01"を格納する。ＭＦＰ２が呼び出したＳＯＡＰインターフェイスを用い遠隔保守センタ３と通信することで、遠隔保守センタ３は、当該ＭＦＰの識別のための情報と保守情報を受信できる。
【０１０４】
なお、これらのＳＯＡＰメッセージは、保守操作や保守情報の改ざん、盗聴を防ぐため、ＳＳＬ上のＨＴＴＰプロトコル（HTTPS）で行うことが好適である。
【０１０５】
図１６のシーケンスに示される処理では、保守対象のＭＦＰ２が自動提供インターバル

に従い保守情報を送信することから処理が開始するため、遠隔保守センタ３の認証を行っていないが、遠隔保守センタ３でないコンピュータ等に保守情報を送付してしまうのを防ぐために遠隔保守センタ３を認証するようにしてもよい。

【０１０６】

また、認証するのではなく、遠隔保守センタ３でのみ復号可能な保守情報を一時鍵で（ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの高速暗号アルゴリズムを用いて）暗号化して送付し、暗号化に使った一時鍵を遠隔保守センタ３の公開鍵で（ＲＳＡなどの公開鍵暗号アルゴリズムを用いて）暗号化して保守情報とともに送付するようにしても良い。そのようにすれば遠隔保守センタは自身の持つ秘密鍵を用いて復号することで一時鍵を得て保守情報の復号ができる。また、遠隔保守センタと保守対象機器との間でＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）のセッションを確立することができるネットワーク環境であれば、ＳＳＬを用いることで一連の暗号処理ができ、保守情報を第三者に盗聴されることなく遠隔保守センタに送付することができる。

【０１０７】

〔ファイアウォールが設定されている場合について〕

ＭＦＰ２は、ユーザの内部ネットワークに接続されていることが想定され、インターネット１と内部ネットワーク４との間にはファイアウォールが設置されていることが想定される。したがって、ＭＦＰ２から保守情報を送信する方法としてはHTTPやSMTPをプロトコルとして用いるようにしておけばファイアウォールに特別な設定をしなくとも保守情報の送信が可能であるため好適である。

【０１０８】

また、内部のネットワークからインターネットに向けて通信を開始するのはファイアウォールで許可されているが、インターネットから内部のネットワークに対する通信は、ファイアウォールによりブロックされ得る。係る場合には、保守対象のＭＦＰ２から遠隔保守センタ３に操作の指示があるか否かを問い合わせ、当該問い合わせに対する返信で保守操作の指示を受け取るようにする。内部のネットワークから通信を開始することで、ファイアウォールの設定を変えずに，外部のネットワークからの通信が可能となり、ユーザのポリシーに従って保守操作の指示を処理できるようになる

ＭＦＰ２は、遠隔保守センタ３が提供する、例えば、getRequest(byte[] random, byte[] authCode, String targetId): String soapRequestEnvelopeというＳＯＡＰインターフェイスを、遠隔保守センタ３から呼び出す。呼び出した当該ＳＯＡＰインターフェイスの、randomとauthCodeには保守対象となるＭＦＰを認証するためのパラメータを格納し、targetIdには保守対象のＭＦＰの識別情報を格納する。

【０１０９】

ＭＦＰ２が呼び出したＳＯＡＰインターフェイスを遠隔保守センタ３へ送信すると、遠隔保守センタ３は、soapRequestEnvelopeに、遠隔保守センタ３側からの指示であるgetChallengeやinternalAuthenticate、performRemoteOperationを格納して、ＭＦＰ２へ送信する。

【０１１０】

getChallenge等にチャレンジ等を格納したら、ＭＦＰ２は、putResult(String soapResultEnvelope): String errorというＳＯＡＰインターフェイスを用い、遠隔保守センタ３と通信する。soapResultEnvelopeには、getChallengeやinternalAuthenticate, performRemoteOperationの戻り値及びout引数のSOAPエンベロープを格納する。

【０１１１】

保守操作の対象となるＭＦＰ２から、定期的に遠隔保守センタ３に問い合わせることにより、ファイアウォールがあっても、遠隔保守センタ３は保守操作を所定のタイミングで行うことができる。所定のタイミングは、自動提供インターバル毎であってもよいし、毎日、所定時間に一回送信しても、また、１分毎に送信してもよい。

【０１１２】

〔遠隔保守の機能を提供するプログラム〕

保守対象機器はＭＦＰであるとして説明したが、対象機器はプリンタなど単一の機能を有する機器や電子文書管理サーバなど所定の機能を提供するコンピュータでもよい。保守対象機器が変われば保守情報や保守操作の内容が変わるが、遠隔保守を保守ポリシーに従って制御する点でＭＦＰと同様である。

【０１１３】

これらの遠隔保守の機能は、ソフトウェアとして提供できる。ソフトウェアとして提供する場合にはＦＤやＣＤ－ＲＯＭ、メモリーカード、等の記録媒体に遠隔保守のプログラムを格納して提供する。特に、電子文書管理サーバのように製品がソフトウェアの場合には、遠隔保守の機能をプログラムで提供されることが好適である。これにより、電子文書管理サーバのソフトウェアにおいて、アップグレードなどの遠隔保守が可能となる。

【０１１４】

遠隔保守のプログラムを単体で提供できれば、遠隔保守の機能を購入後に追加できるため、遠隔保守の機能をＭＦＰや電子文書管理サーバにインストールされた状態で譲渡するのではなく、遠隔保守の機能を後から追加導入できるようになる。図１８は、ソフトウェアで追加できる機能の一例を示す。点線Ａで囲まれた機能は、オプションのプログラムで提供される機能の一例を示す。ＭＦＰの場合にはソフトウェアを後からオプションとして提供する場合にはメモリーカードやＤＩＭＭ（Dual Inline Memory Module）モジュールといった媒体に格納して提供することが好適である。

【０１１５】

本実施例によれば、ユーザの保守のポリシーにしたがって、外部のネットワークから保守が可能なネットワーク対応機器、ネットワーク対応機器を保守する保守方法、プログラム、プログラムが記録された媒体及び保守システムを提供することができる。

【０１１６】

ユーザの定めた保守ポリシーに従って、定期的に保守情報を遠隔保守センタ３に送信できる。保守情報は暗号化して送信できるので、盗聴や改ざんを防止できる。遠隔保守センタから、操作の指示を受信した場合には、保守ポリシーで許可されている操作を行う。また、保守ポリシーは、ＭＦＰ２毎に設定できるので、ユーザの保守のポリシーに従った保守を実現できる。保守ポリシーの入力の際には管理者が認証され、また、保守ポリシを記録媒体で入力する場合には、電子署名をすることで保守ポリシーの第三者による設定や改ざんを防止できる、また、ファイアウォールがあっても、ＭＦＰ２は、ＭＦＰ２からの問い合わせや定期的な保守情報の送信に対する応答として、操作の指示を受信できる。ＭＦＰ２と遠隔保守センタ３との通信には、ＸＭＬやＳＯＡＰメッセージを用いることで、ＯＳやアーキテクチャに依存しないで遠隔から保守操作が可能となる。

【図面の簡単な説明】

【０１１７】

【図１】ネットワークを介して接続された遠隔保守センタ３とＭＦＰ２とを有する遠隔保守システム及び保守操作の概略の一例を示す図である。

【図２】遠隔保守センタ３のハードウェア構成図及び機能構成図の一例である。

【図３】ＭＦＰ２の機能構成図の一例である。

【図４】保守ポリシーの一例を示す図である。

【図５】保守ポリシーの設定画面の一例を示す図である。

【図６】保守ポリシーの設定画面の一例を示す図である。

【図７】保守ポリシーに基づき生成されたＸＭＬデータの一例である。

【図８】端末１０が接続された遠隔保守システムの一例である。

【図９】ＭＦＰ２に保守ポリシー５が設定される際のシーケンスを表すシーケンス図の一例である。

【図１０】管理者の認証が失敗した場合のシーケンスを表すシーケンス図の一例である。

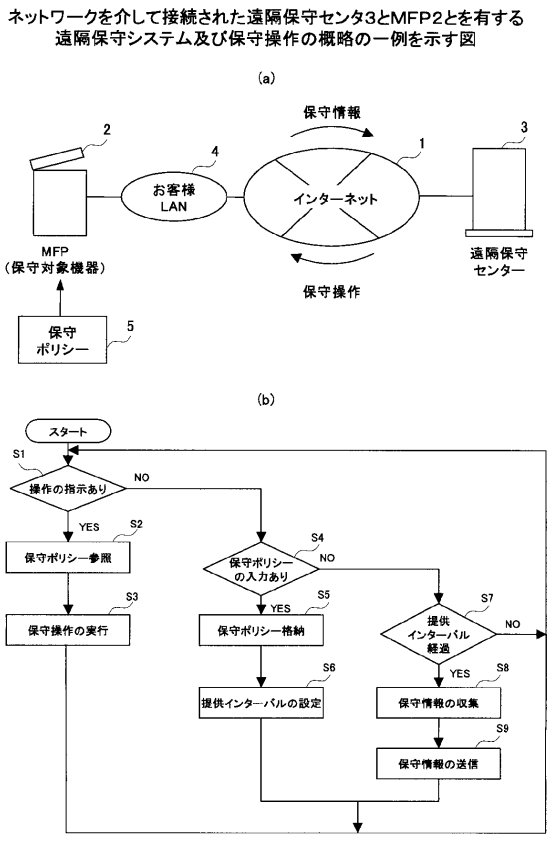
【図１１】遠隔保守センタ３から保守ポリシーが設定されようとした場合のシーケンスを表すシーケンス図の一例である。

【図１２】遠隔保守センタ３が保守ポリシーで許可されている範囲の保守操作を行うシー

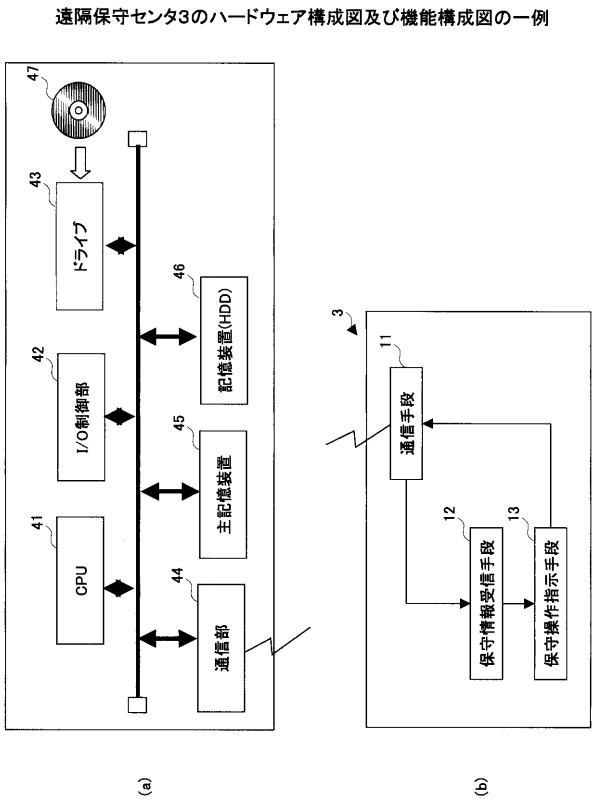
ケンス図の一例である。
【図１３】保守操作を指示する場合のＳＯＡＰインターフェイスの一例である。
【図１４】保守ポリシーの判定処理におけるＳＯＡＰインターフェイスの一例である。
【図１５】保守操作を行う際のＳＯＡＰインターフェイスの擬似コードの一例である。
【図１６】定期提供保守情報を自動提供インターバルで遠隔保守センタ３へ送信するシーケンス図の一例である。
【図１７】保守処理部が保守情報を自動提供インターバルで遠隔保守センタ３へ送信する処理を行うＳＯＡＰインターフェイスの擬似コードの一例である。
【図１８】ソフトウェアで追加できる遠隔保守の機能の一例を示す図である。
【符号の説明】
【０１１８】

２	ＭＦＰ（デジタル複合機）
３	遠隔保守センタ
１２	保守情報受信手段
１３	保守操作指示手段
２０	保守処理部
２１	ポリシー判定処理部
２２	センタ認証処理部
２３	保守情報管理部
２４	主機能制御部
２５	ポリシー管理部
２６	ユーザ認証処理部
２７	ポリシー設定処理部
２９	保守ポリシーデータベース

【図１】

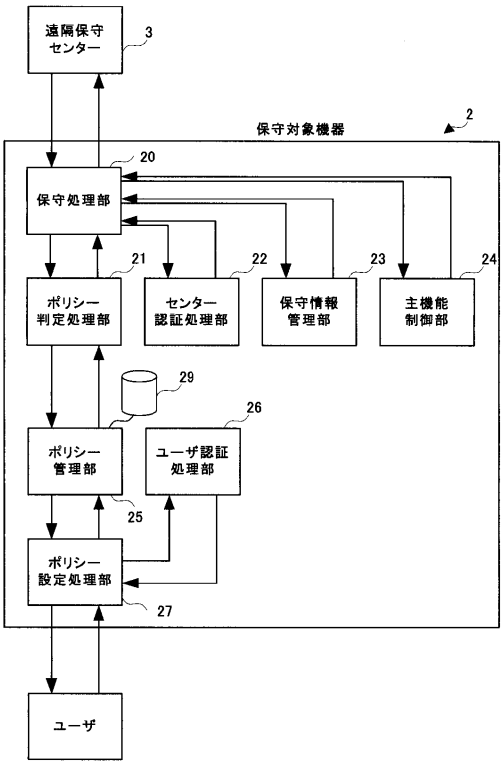


【図２】



【図３】

MFP2の機能構成図の一例



【図４】

保守ポリシーの一例を示す図

保守情報提供ポリシー

(a)

自動提供インターバル	30
単位	分
定期提供保守情報の種別	機種番号
	コピーカウンタ
	トナー残量
保守情報種別	許可／禁止
機種番号	許可
IP アドレス	禁止
MAC アドレス	禁止
ファームウェアバージョン	許可
コピーカウンタ	許可
トナー残量	許可
・・・	

保守操作許可ポリシー

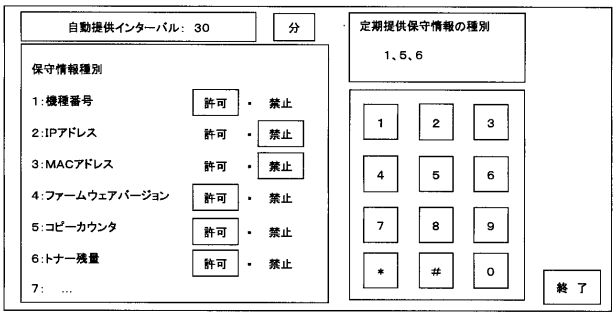
(b)

保守操作種別	許可／禁止
マシン再起動	許可
HDD フォーマット	禁止
アドレス帳クリア	禁止
管理者パスワードクリア	禁止
保守情報取得	許可
・・・	

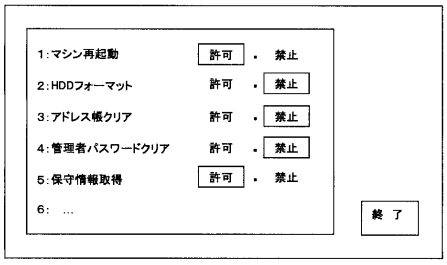
【図５】

保守ポリシーの設定画面の一例を示す図

(a)



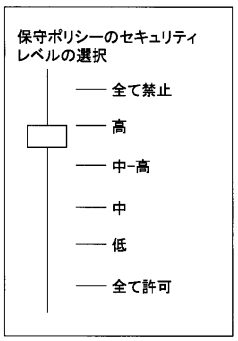
(b)



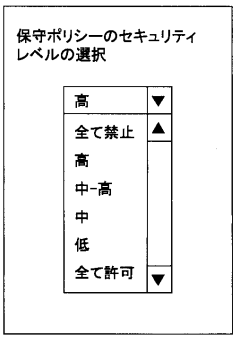
【図６】

保守ポリシーの設定画面の一例を示す図

(a)



(b)



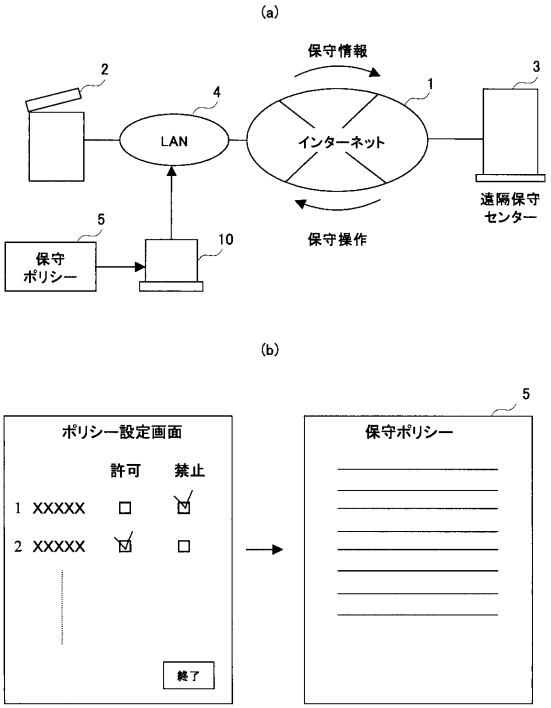
【図７】

保守ポリシーに基づき生成されたXMLデータの一例

```
<?xml version="1.0" encoding="UTF-8" ?>
- <RemoteMaintenancePolicy>
- <InfoProvisionPolicy>
- <AutoProvision>
- <Interval>
<Value>30</Value>
<Unit>min</Unit>
</Interval>
- <InfoList>
<Name>Machine Number</Name>
<Name>Copy Counter</Name>
<Name>Toner Amount</Name>
</InfoList>
</AutoProvision>
- <PolicyElement>
<Name>Machine Number</Name>
<Permission>allowed</Permission>
</PolicyElement>
- <PolicyElement>
<Name>IP Address</Name>
<Permission>denied</Permission>
</PolicyElement>
- <PolicyElement>
<Name>MAC Address</Name>
<Permission>denied</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Firmware Versions</Name>
<Permission>allowed</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Copy Counter</Name>
<Permission>allowed</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Toner Amount</Name>
<Permission>allowed</Permission>
</PolicyElement>
</InfoProvisionPolicy>
- <RemoteOperationPolicy>
- <PolicyElement>
<Name>Machine Rebooting</Name>
<Permission>allowed</Permission>
</PolicyElement>
- <PolicyElement>
<Name>HDD Formatting</Name>
<Permission>denied</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Address Book Initialization</Name>
<Permission>denied</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Administrator Password Initialization</Name>
<Permission>denied</Permission>
</PolicyElement>
- <PolicyElement>
<Name>Maintenance Info Retrieval</Name>
<Permission>allowed</Permission>
</PolicyElement>
</RemoteOperationPolicy>
</RemoteMaintenancePolicy>
```

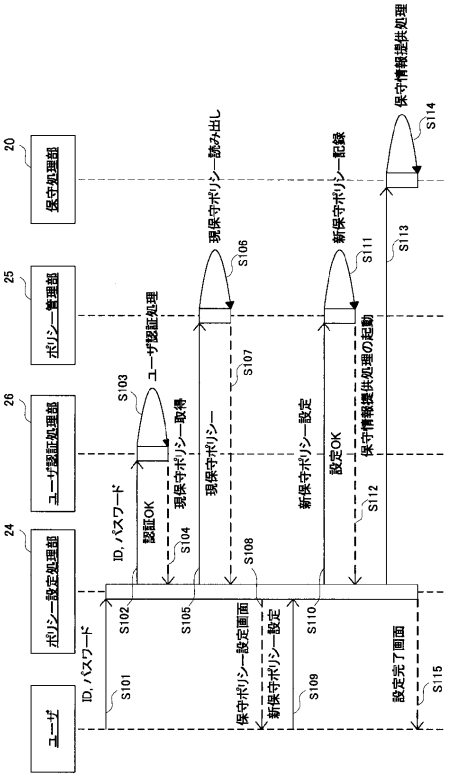
【図８】

端末10が接続された遠隔保守システムの一例



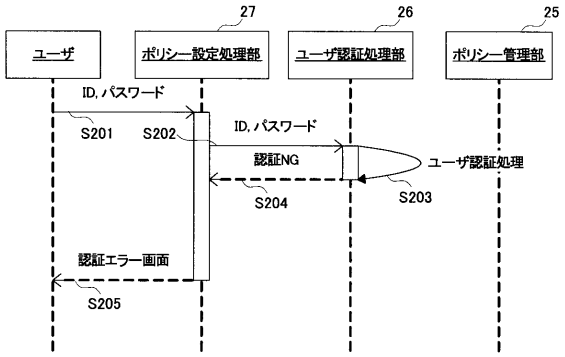
【図９】

MFP2に保守ポリシー5が設定される際のシーケンスを表すシーケンス図の一例



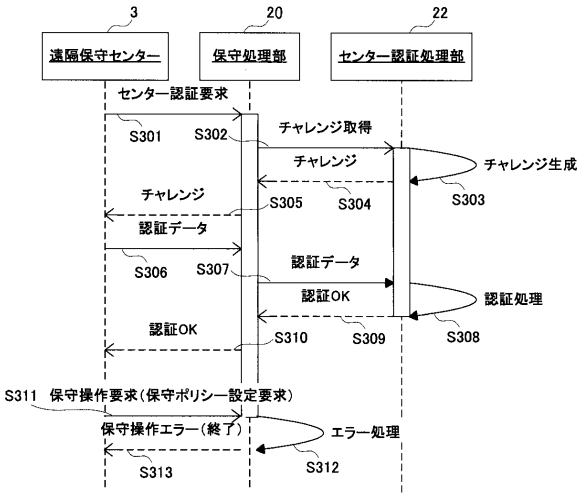
【図１０】

管理者の認証が失敗した場合のシーケンスを表すシーケンス図の一例



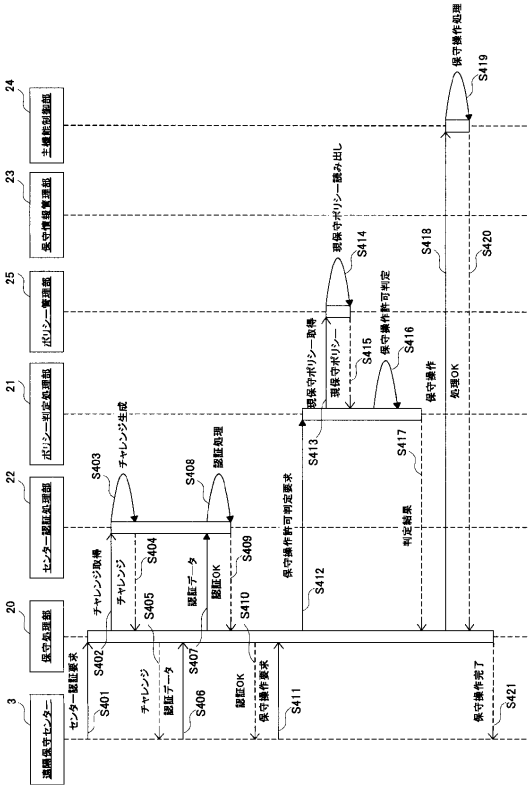
【図１１】

遠隔保守センタ3から保守ポリシーが設定されようとした場合の
シーケンスを表すシーケンス図の一例



【図１２】

遠隔保守センタ3が保守ポリシーで許可されている範囲の
保守操作を行うシーケンス図の一例



【図１３】

保守操作を要求する場合のSOAPインターフェイスの一例

```
■保守操作要求
performRemoteOperation(String session, String operation, Parameter[] params): OperationResult result
Paramter型 {
        String name; ←パラメータの名前
        String value; ←パラメータの値
};
OperationResult型 {
        String error; ←エラーの場合にはエラーコードが格納される.
        Parameter[] results; ←様々な操作結果が格納される.
};

operation = "Machine Rebooting";
params[0].name = "TIME";
params[0].value = "NOW";
```

という形で，保守操作の名前と，その保守操作に必要なパラメータを渡して，保守操作要求をする．

```
operation = "Maintenance Info Retrieval";
params[0].name = "INFO TYPE";
params[0].value = "ALL";
```

【図１４】

保守ポリシーの判定処理におけるSOAPインターフェイスの一例

(a)

```
OperationResult performRemoteOperation(String session, String operation, Parameter[] params) {
        session が有効かどうか判定する.
        if(有効でない){
                エラーコード = "BAD_SESSION_ERROR";
                エラーコードを返して終了;
        }
        ポリシー判定結果＝isAllowedOperation(operation, params);
        if(ポリシー判定結果が「不許可」){
                エラーコード = "NOT_PERMITTED";
                エラーコードを返して終了;
        }
        result = performOperation(operation, params);
        return result;
}
```

(b)

```
boolean isAllowedOperation(String operation, Parameter[] params) {
        保守ポリシーファイルを開いて保守ポリシーデータ(XML データ)をメモリ上に読み込む
        XML データ内の<RemoteMaintenancePolicy>要素の下の,
        <RemoteOperationPolicy>要素の下の,
        <PolicyElement>要素で, 下に<Name>要素の内容が operation に一致するものを探す
        if(一致する要素がない){
                false(「不許可」)を返して終了;
        }
        if(一致する要素があった){
                その要素の下の<Permission>要素の内容を参照する
                if(allowed){
                        true(「許可」)を返して終了;
                }
                else{
                        false(「不許可」)を返して終了
                }
        }
}
```

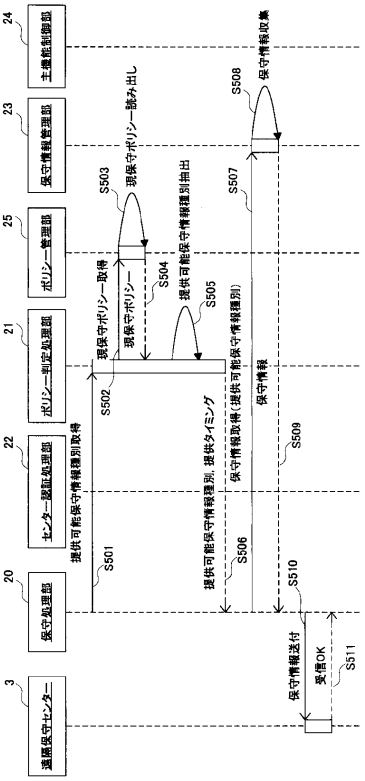
【図１５】

保守操作を行う際のSOAPインターフェイスの擬似コードの一例

```
OperationResult performOperation(String operation, Parameter[] params){
        if(operation が"Machine Rebooting"なら){
                params を参照し，再起動の時刻を取得する
                再起動の時刻をオペパネに表示する
                MFP の主制御部に時刻を指定した再起動の指示を出す
                処理結果を返して終了;
        }
        else if(operation が"HDD Formatting"なら){
                MFP の主制御部に HDD フォーマットの指示を出す
                処理結果を返して終了;
        }
        else if(operation が"Maintenance Info Retrieval"){
                保守情報の取得(getMaintenanceInfo(params))
                取得した保守情報を返して終了;
        }
        else if(. . . ){
                . . .
        }
        エラーコード = "INVALID_OPERATION"
        エラーコードを返して終了
}
```

【図１６】

定期提供保守情報を提供インターバルで
遠隔保守センタ3へ送信するシーケンス図の一例



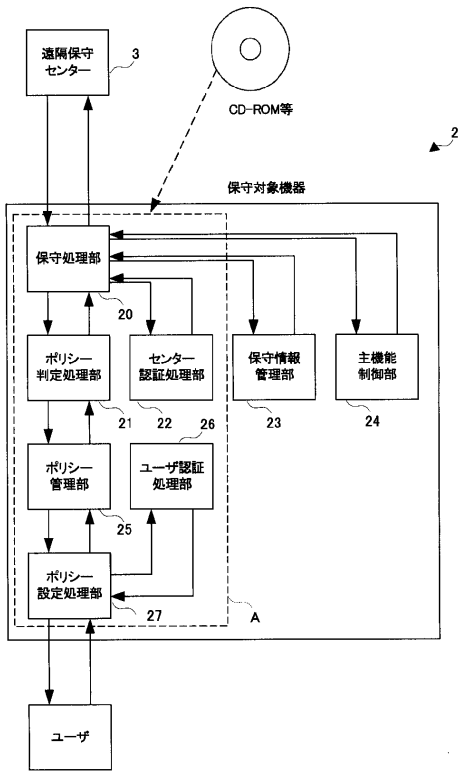
【図１７】

保守処理部が保守情報を提供インターバルで遠隔保守センタ3へ送信する
処理を行うSOAPインターフェイスの擬似コードの一例

```
AutoProvision(){
        保守ポリシーファイルを開いて保守ポリシーデータ(XML データ)をメモリ上に読み込む
        XML データ内の<InfoProvisionPolicy>要素の下の，
        <AutoProvision>要素の下の，
        <Interval>要素の下から自動提供インターバルを取得する
        <InfoList>要素の下に列挙されている情報種別のリストを取得する
        while(保守ポリシーの変更があるまで){
                for(取得した情報種別リストの情報種別ごとに){
                        情報種別に対応する保守情報を保守情報管理部から取得する
                }
                取得した保守情報を遠隔保守センターに送付する(sendMaintenanceInfo())
                自動提供インターバルの分だけ待機する
        }
}
```

【図１８】

ソフトウェアで追加できる遠隔保守の機能の一例を示す図



フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｇ０６Ｆ 3/12	Ｋ	
	Ｈ０４Ｎ 1/00	１０６Ｃ	
	Ｈ０４Ｎ 1/00	１０７Ｚ	

Ｆターム(参考) 5C062 AA02 AA05 AA13 AA29 AA35 AB20 AB23 AB38 AB42 AC02
AC22 AC34 AC51 AC56 AF00 BA00 BD09

【要約の続き】