(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6180149号
(P6180149)
(45)発行日　平成29年8月16日(2017.8.16)　(24)登録日　平成29年7月28日(2017.7.28)

(51)Int.Cl.　F I
G06Q 10/00 (2012.01)　G06Q 10/00 300

請求項の数 3　(全 16 頁)

(21)出願番号　特願2013-67676(P2013-67676)
(22)出願日　平成25年3月27日(2013.3.27)
(65)公開番号　特開2014-191665(P2014-191665A)
(43)公開日　平成26年10月6日(2014.10.6)
審査請求日　平成28年1月8日(2016.1.8)

前置審査

(73)特許権者　598057291
株式会社富士通エフサス
神奈川県川崎市中原区中丸子１３番地２
(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　伊藤　昌彦
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内
(72)発明者　浅沼　広樹
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内

最終頁に続く

(54)【発明の名称】端末装置および制御方法

(57)【特許請求の範囲】
【請求項１】
近距離ネットワークを介して、サーバへの送信を許可されていない、電子機器の利用状態の情報を含む第１情報および前記サーバへの送信を許可された第２情報を前記電子機器から取得する取得部と、
前記電子機器の障害に関する情報を含む前記第２情報を、遠距離ネットワークを介して前記サーバに送信する送信部と、
前記第２情報の前記電子機器の障害に関する複数の対応方法に関する情報を含む第３情報を前記サーバから受信する受信部と、
前記第１情報および前記第３情報を分析して、前記複数の対応方法の優先順位を特定する分析部と、
前記取得部、前記送信部、前記受信部の処理の履歴情報を生成し、生成した前記履歴情報を、前記サーバに送信する履歴送信部と、
を有することを特徴とする端末装置。
【請求項２】
前記端末装置は、情報を記憶する記憶装置としてＲＡＭ（Random Access Memory）を有することを特徴とする請求項１に記載の端末装置。
【請求項３】
端末装置が、近距離ネットワークを介して、サーバへの送信を許可されていない第１情報および前記サーバへの送信を許可された第２情報を電子機器から取得し、

前記端末装置が、前記第２情報を、遠距離ネットワークを介して前記サーバに送信し、
前記サーバが、前記第２情報に対応する第３情報を前記端末装置に送信し、
前記端末装置が、前記サーバから前記第３情報を受信し、
前記端末装置が、前記第１情報、前記第２情報、第３情報に対する処理の履歴情報を生成し、生成した履歴情報を前記サーバに送信し、
前記サーバが、前記履歴情報をハッシュ化して他のサーバに送信する
各処理を実行することを特徴とする制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、端末装置等に関する。

【背景技術】

【０００２】

顧客電子機器に対して保守作業を実施する場合には、保守作業員が保守ノウハウの格納された保守端末を携帯して顧客先において当該ネットワークに接続して顧客電子機器のＲＡＳ情報を取得し、保守作業を実施する。近年では、保守センターが顧客電子機器のＲＡＳ情報等各種情報をネットワーク経由で受信し、受信した情報と保守センター内の保守ノウハウをもとに、保守作業を実施する場合もある。

【０００３】

この方法によれば顧客電子機器の詳細情報と保守センター内の膨大な保守ノウハウを突き合わせることができ、的確な保守作業が実施できる。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００５－３２１９５５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかしながら、上述した従来技術を適用しようとすると顧客側からセキュリティの問題で接続を許可されないケースが多い。本発明は顧客のセキュリティを確保しつつ、ネットワーク経由で保守端末と保守センターを接続することにより適切な保守作業を実現しようとするものである。

【０００６】

１つの側面では、上記に鑑みてなされたものであって、顧客のセキュリティを確保しつつ、ネットワーク経由で保守端末と保守センターを接続することにより適切な保守作業を実現できる端末装置および制御方法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】

【０００７】

第１の案では、端末装置は、取得部と、送信部と、受信部と、履歴送信部とを有する。取得部は、近距離ネットワークを介して、サーバへの送信を許可されていない第１情報およびサーバへの送信を許可された第２情報を電子機器から取得する。送信部は、第２情報を、遠距離ネットワークを介してサーバに送信する。受信部は、第２情報に対応する第３情報を前記サーバから受信する。履歴送信部は、取得部、送信部、受信部の処理の履歴情報を生成し、生成した履歴情報を、サーバに送信する。

【発明の効果】

【０００８】

本発明の１実施態様によれば、顧客のセキュリティを確保しつつ、ネットワーク経由で保守端末と保守センターを接続することにより適切な保守作業を実現できる。

【図面の簡単な説明】

【０００９】

【図１】図１は、本実施例に係るシステムの構成を示す図である。
【図２】図２は、本実施例に係る保守端末の構成を示す図である。
【図３】図３は、保守ナレッジ情報のデータ構造の一例を示す図である。
【図４】図４は、交換順位情報の一例を示す図（１）である。
【図５】図５は、交換順位情報の一例を示す図（２）である。
【図６】図６は、交換順位情報を表示する表示画面の一例を示す図である。
【図７】図７は、作業完了情報を表示する表示画面の一例を示す図である。
【図８】図８は、本実施例に係る保守サーバの構成を示す図である。
【図９】図９は、被疑部品判定テーブルのデータ構造の一例を示す図である。
【図１０】図１０は、保守端末の処理手順を示すフローチャート（１）である。
【図１１】図１１は、保守端末の処理手順を示すフローチャート（２）である。
【図１２】図１２は、保守サーバの処理手順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】
【００１０】
以下に、本願の開示する端末装置および制御方法の実施例を図面に基づいて詳細に説明する。なお、この実施例によりこの発明が限定されるものではない。
【実施例】
【００１１】
例えば、保守作業を行う場合には、ＲＡＳ情報を電子機器からネットワークを介して入手し、保守端末に内蔵されている診断機能によって障害情報を判断する。しかしながら保守作業員にとってＲＡＳ情報のみでは的確な判断が下せない。また、保守端末に内蔵される診断機能は限定されているため、保守センター内に蓄積された保守ノウハウを参照したい場合がある。この二つを実現するためには顧客電子機器内の運用情報を前記ネットワークによって入手し、また、保守センターとネットワークによって接続して保守センター内の保守ナレッジを入手する必要がある。この場合、顧客からみると保守端末を経由して顧客電子機器と保守センターがネットワークで接続されているようにみえる。ここにセキュリティ上の顧客の疑義が発生する。その疑義の内容は保守端末を経由して顧客の運用情報が保守センターに流れる。もう一点は保守センター内から何らかの操作が顧客電子機器に行われる可能性がある。しかし、上記にみたように保守作業において必要なのは、顧客電子機器から保守端末が情報を入手、かつ、保守センターから保守端末が情報を入手するの二点のみである。よって、顧客に対して保守端末経由で顧客電子機器と保守センターが接続されているようにみえてもその内実が保守端末から顧客電子機器にも保守センターにも情報送出が行われないことが保証されれば上記接続が許諾される可能性がある。
【００１２】
さらには保守センターとしては保守ナレッジ蓄積のために顧客電子機器のＲＡＳ情報は蓄積したい。また、保守作業の履歴も蓄積したい。また、当然保守センターの保守ナレッジに対する問い合わせの電文は保守端末から保守センターに送出される。上記３種の限定された情報については例外として保守端末から保守センターへの情報の送出が許諾される必要がある。そのためには、保守端末から保守センターに送出される情報が上記３種の情報に限定されることを保証する必要がある。
【００１３】
上記の点に鑑みて、本実施例に示すシステムでは、顧客のセキュリティを確保しつつ、ネットワーク経由で保守端末と保守センターを接続することにより適切な保守作業を実現可能とする。
【００１４】
本実施例に係るシステムの構成について説明する。図１は、本実施例に係るシステムの運用概要を示す図である。図１に示すように、このシステムは、顧客システム１０と、保守端末１００と、保守センター３００とを有する。顧客システム１０は、社内ＬＡＮ（Local Area Network）、無線等のネットワークを介して、保守端末１００に接続される。また、保守端末１００および保守センター３００は、社外のネットワーク５０を介して相

互に接続される。保守センター３００は、保守サーバ２００を有する。また、保守センター３００は、ＥＭＡ（環境管理）局４００にネットワークを介して接続される。

【００１５】

顧客システム１０は、電子機器２０を有する。電子機器２０は、例えば、ＰＣ（Personal Computer）、サーバ、プリンタ、ネットワーク機器、外部ストレージ、冷蔵庫、洗濯機、テレビ、ステレオコンポ、医療機器または工作機器等に対応する。

【００１６】

電子機器２０は、エージェントプログラムを有している。例えば、電子機器２０は、保守端末１００に接続されると、エージェントプログラムを実行してエージェント（agent）を起動する。エージェントは、運用情報とＲＡＳ情報を取得し、保守端末１００に送信する。

【００１７】

運用情報は、社外のネットワーク５０を介して保守センター３００への送信が許可されていない情報である。運用情報の内容は、顧客の業務にかかる情報や履歴、また医療機器等にあっては、医療にかかる情報、体温、血圧、服薬、医療行為等である。

【００１８】

ＲＡＳ（Reliability Availability Serviceability）情報とは、ハードウェア、ソフトウェアの障害の予兆検知のために、また、障害発生時の対応を迅速かつ的確に行うために当該ハードウェアやソフトウェアの動作の履歴を取得蓄積した情報等である。例えば、ハードウェアの軽微なエラー発生時のエラーコード、ハードウェアが自動修復した軽微な障害の履歴等である。この情報は顧客の業務情報を含まないので、ＲＡＳ情報は、社外のネットワーク５０を介して保守センター３００への送信が許可されている情報である。その他にも、ＲＡＳ情報には、エラーの発生した電子機器を特定する情報、エラーの発生した日時などを含んでいても良い。このＲＡＳ情報は顧客業務に依存しないので保守センター内に汎用的に保守ナレッジとして蓄積可能である。

【００１９】

保守端末１００は、顧客システム１０から取得する運用情報およびＲＡＳ情報と、保守センター３００から得られる最新の保守ナレッジ情報を基にして、顧客の業務状況に応じた適切な保守を行う装置である。

【００２０】

例えば、保守ナレッジ情報には、ＲＡＳ情報に対応する複数種類の障害被疑部品の情報が含まれる。障害対応にあたる保守員が携帯する保守端末１００は、当該電子機器から取得した運用情報（この運用情報は保守端末内にとどまり保守センターには送られない）と、当該電子機器から取得した当該電子機器のＲＡＳ情報と、当該電子機器のＲＡＳ情報を保守センターが受信することにより保守センター側が必要と判定し、保守端末に送信した保守センター内の保守ナレッジ情報との３つの情報によって適切な障害被疑部品を特定する。なお、保守端末１００は、保守作業が完了した時点で保守端末１００内に記録されている障害対処履歴情報を保守センターに送信する。保守センターは障害対処履歴情報を保守ナレッジに蓄積する。また、作業完了情報も併せて保守センターに送信する。そののち、保守端末１００は端末内のデータの初期化を行い、顧客システム１０から取得した運用情報とＲＡＳ情報と保守ナレッジおよび障害対処履歴等の記憶部の情報を消去する。なお、これは例示であって定期保守時等においても同様の保守作業を行う。

【００２１】

保守センター３００は、保守端末１００から送信されるＲＡＳ情報と障害対処履歴等を保守センター内の保守ナレッジに蓄積し、保守作業実施ごとに最新化を図る。また、当然のことながら、適宜送られてくる技術情報に基づくナレッジの最新化も行う。また、保守センター３００は、保守端末１００から送られてくる保守端末１００と電子機器２０との間のすべての通信内容を含む通信履歴と、保守端末１００と保守サーバ２００との間のすべての通信内容を含む通信履歴を保存するとともに、それぞれの通信履歴のハッシュ値を計算して保守サーバ２００内に保存して、または保存せずに、それぞれのハッシュ値をＥ

ＭＡ局４００に送信する。このハッシュ値には通信履歴に関する属性情報、例えば通信機器対の名称、通信機器ＩＤ、通信時刻等が付随してもよい。ＥＭＡ局４００は、保守センター３００から送付されてきたハッシュ値をその属性情報とともに保存する。また、このハッシュ値とそれに付随する属性情報は電子署名を付してもよい。なお、このハッシュ値の算出にあたっては、適宜ポリシーを定め、そのポリシーにしたがって実行する。

【００２２】

ＥＭＡ局４００は、特許第４８１８６６４号公報に開示される環境管理局に類するものである。ＥＭＡ局４００は、図２で示される保守端末を構成するＴＰＭチップに類するものを局内に含む。ＥＭＡ局４００は、例えば、電子機器２０等の顧客の機器に組み込まれているソフトウェアやハードウェアの正規品情報を管理し、必要に応じ保守端末や保守センター等の監査を行う機能を有する。なお、保守端末や保守センター等の認証にかかる行為は従来技術であるＰＫＩシステムに従う。その際に、署名鍵管理等については、ＩＥＴＦ　ＲＦＣ５７９２／５７９３に開示されているＴＣＧ技術を応用してもよい。

【００２３】

ところで、図１に示した保守端末１００および保守センター３００の保守サーバ２００、ＥＭＡ局４００は、例えば、ＴＣＧ（Trusted Computing Group）技術を利用して、セキュアにデータ通信を実行することを前提とする。

【００２４】

本実施例で利用するＴＣＧ技術の一例について説明する。インターネットに接続される端末、デバイスは常にセキュリティの脅威に曝され、ウィルス、スパイウェア、その他悪質なスクリプト、不正アクセス等により、プラットフォームを構成するソフトウェア構造に予期せぬ改変が加えられる場合がある。このようなリスクに対して、ＴＣＧでは、プラットフォームの信頼性を保障することにより、安全なコンピューティング環境を実現する。ここで、プラットフォームとは、ハードウェア、ＯＳ、アプリケーション等を示す。

【００２５】

例えば、ソフトウェアの改竄という脅威に対して、従来のソフトウェアのみに依存するセキュリティ対策には限界がある。このため、ＴＣＧでは、ＴＰＭ（Trusted Platform Module）チップをプラットフォームに埋め込み、かかるＴＰＭチップを信頼のルートとして、改竄が極めて困難な、信頼できるコンピューティング環境を構築している。また、ＴＰＭチップを利用することで、ハードウェアベースのデータ・証明書の保護、安全な暗号処理環境を実現できる。

【００２６】

次に、ＴＰＭチップについて説明する。ＴＰＭチップは、電子機器にバインドされるハードウェアのチップであり、耐タンパー性を持つ。ＴＰＭチップは電子機器から取り外しができないように、電子機器の主要な構成パーツに物理的にバインドされる。例えば、電子機器の構成パーツは、マザーボード等に対応する。ＴＰＭチップは、実装される機能、メモリ領域、プロセッサ・パワーを極力抑えて設計されているため、低コストで製造でき、様々な電子機器やプラットフォームに適用できる。

【００２７】

例えば、ＴＰＭの機能には、ＲＳＡ（Rivest Shamir Adleman）秘密鍵の生成・保管する機能、ＲＳＡ秘密鍵による署名、暗号化、復号する機能が含まれる。ＲＳＡでは、秘密鍵と公開鍵とのペアを作成する。また、ＴＰＭの機能には、ＳＨＡ－１（Secure Hash Algorithm 1）のハッシュ演算する機能、電子機器の環境情報を保持する機能が含まれる。ＴＰＭは、バインドされた電子機器が起動した時点で、ＢＩＯＳ、ＯＳｌｏａｄｅｒ、ＯＳカーネルへのブートプロセスにおけるソフトウェアコードを計測し、計測したソフトウェアコードをハッシュ化して、ＴＰＭ内部のレジスタに登録する。また、ＴＰＭは、バインドされた電子機器のハードウェアの情報を収集し、ハードウェアの情報をハッシュ化して、ＴＰＭ内部のレジスタに登録する。

【００２８】

ＴＣＧ技術では、上位のアプリケーションやライブラリからハードウェア・デバイスで

あるＴＰＭチップを利用するためソフトウェア・スタックとソフトウェアインターフェースを規定する。このソフトウェア・スタックはＴＳＳ（TCG Software Stack）と呼ばれ、リソースが制限されるＴＰＭチップの機能を保管するソフトウェアモジュールから構成されている。電子機器のアプリケーションは、ＴＳＳの提供するインタフェースを利用して、上述したＴＰＭチップの機能にアクセスすることができる。ＴＰＭチップは、顧客システム側のＴＰＭチップでハッシュ値を採取する際のルールをハッシュ化及び署名付与して管理することで、ハッシュ値採取の正当性を担保するものである。しかも、ＴＰＭチップは、必要に応じて、現時点でのルール及び署名をチェックすることで、ルールの非改竄性を証明する。その結果、ＴＰＭチップは、ＴＰＭチップ側で非改竄性が証明されたルールを参照しながら運用することでハッシュ値を採取する際のルールに改竄がないことを保証する。

【００２９】

次に、図１に示した保守端末１００の構成について説明する。図２は、本実施例に係る保守端末の構成を示す図である。図２に示すように、この保守端末１００は、通信部１１０、入力部１２０、表示部１３０、インタフェース部１４０、ＴＰＭチップ１５０、記憶部１６０、制御部１７０を有する。各部１１０～１７０は、バス１８０によって相互に接続される。

【００３０】

通信部１１０は、社外のネットワーク５０を介して他の装置とデータ通信を行う処理部である。例えば、通信部１１０は、ネットワーク５０を介して、保守サーバ２００とデータをやり取りする。また、通信部１１０は、社内のネットワークを介して、顧客システム１０とデータ通信を行う。後述する制御部１７０は、通信部１１０を介して、電子機器２０ａ、保守サーバ２００とデータをやり取りする。

【００３１】

入力部１２０は、各種の情報を保守端末１００に入力する入力装置である。例えば、入力部１２０は、キーボードやマウス、タッチパネルなどに対応する。表示部１３０は、制御部１７０から出力される各種の情報を表示する表示装置である。例えば、表示部１３０は、液晶ディスプレイやタッチパネル等に対応する。インタフェース部１４０は、各種の外部装置と接続するインタフェースである。

【００３２】

ＴＰＭチップ１５０は、上述したＴＣＧ技術に準拠するＴＰＭチップである。例えば、ＴＰＭチップ１５０は、後述する制御部１７０が保守サーバ２００に送信する情報に、ＴＰＭチップ１５０に格納された秘密鍵によって電子署名を付与する。

【００３３】

記憶部１６０は、運用情報１６１、ＲＡＳ情報１６２、保守ナレッジ情報１６３、交換順位情報１６４、障害対処履歴情報１６５を記憶する記憶装置である。例えば、記憶部１６０は、ＲＡＭ（Random Access Memory）に対応する。すなわち、電源供給が停止されると、記憶部１６０に記憶された情報は消去される。

【００３４】

記憶部１６０は、情報エリア１６０ａ、保守エリア１６０ｂ、分析エリア１６０ｃを有する。情報エリア１６０ａには、保守サーバ２００に送信することが許可されていない情報が格納される。例えば、情報エリア１６０ａには、運用情報１６１が格納される。保守エリア１６０ｂには、保守サーバ２００に送信することが許可されている情報が格納される。例えば、保守エリア１６０ｂには、ＲＡＳ情報１６２が格納される。また、保守エリア１６０ｂには、交換順位情報１６４および障害対処履歴情報１６５が格納される。

【００３５】

分析エリア１６０ｃは、後述する分析部１７５が作業を行う作業領域である。例えば、分析エリア１６０ｃには、保守ナレッジ情報１６３が格納される。また、情報エリア１６０ａの運用情報１６１は読み出されて分析エリア１６０ｃに格納される。保守エリア１６０ｂのＲＡＳ情報１６２は読み出されて分析エリア１６０ｃに格納される。

【００３６】
運用情報１６１は、顧客システム１０の電子機器２０から取得する情報である。上記のように、運用情報１６１は、業務ログ、機器構成、ソフト構成、ＩＰアドレス等の構成情報等を含む。また、業務ログは、例えば、顧客システム１０の各電子機器２０の稼働実績の履歴を含む情報である。この業務ログは、社外のネットワーク５０を介して保守センター３００への送信が許可されていない情報である。
【００３７】
ＲＡＳ情報１６２は、顧客システム１０の電子機器２０から取得する情報である。ＲＡＳ情報１６２は、上記のように、ハードウェア、ソフトウェアの障害の予兆検知のために、また、障害発生時の対応を迅速かつ的確に行うために当該ハードウェアやソフトウェアの動作の履歴を取得蓄積した情報である。
【００３８】
保守ナレッジ情報１６３は、ＲＡＳ情報に対応する複数の障害被疑部品の情報が含まれる。図３は、保守ナレッジ情報のデータ構造の一例を示す図である。図３に示す例では、この保守ナレッジ情報１６３は、被疑部品と、被疑確率と、交換時間とを対応付ける。被疑部品は、障害を引き起こした可能性のある部品を一意に特定する情報である。被疑確率は、障害を引き起こした部品であることを示す確からしさを示す値であり、数値が高い部品ほど、より障害を引き起こした可能性が高いことを示す。交換時間は、該当する部品を交換するのに要する時間を示す。
【００３９】
図３において、例えば、被疑部品「部品Ａ」は、被疑部品である可能性が「５０％」であり、部品Ａを交換するのに要する時間が「６０分」となる。
【００４０】
交換順位情報１６３は、被疑部品の交換順位を示す情報である。交換順位情報の具体的な説明は後述する。
【００４１】
障害対処履歴情報１６５は、保守端末１００が実行した処理の履歴の情報を含む。例えば、障害対処履歴情報１６５には、送受信したデータの方向やデータの実体、情報の種別、情報の出所、情報の行き先、情報を処理したタイミング、作業者の情報が含まれる。すなわち、後述する制御部１７０が実行する処理の履歴が全て、障害対処履歴情報１６５に含まれることとなる。制御部１７０に関する詳しい説明は後述する。
【００４２】
次に、制御部１７０について説明する。制御部１７０は、取得部１７１、格納処理部１７２、送信部１７３、受信部１７４、分析部１７５、履歴生成部１７６、判定部１７７、初期化部１７８を有する。制御部１７０は、例えば、ＡＳＩＣ（Application Specific Integrated Circuit）や、ＦＰＧＡ（Field Programmable Gate Array）などの集積装置に対応する。また、制御部１７０は、例えば、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）等の電子回路に対応する。
【００４３】
取得部１７１は、電子機器２０ａのエージェントとデータ通信を実行して、エージェントから運用情報およびＲＡＳ情報を取得する処理部である。取得部１７１は、運用情報およびＲＡＳ情報を、格納処理部１７２に出力する。
【００４４】
格納処理部１７２は、運用情報を記憶部１６０の情報エリア１６０ａに格納し、ＲＡＳ情報を記憶部１６０の保守エリア１６０ｂに格納する。情報エリア１６０ａに格納された運用情報を、運用情報１６１と表記する。保守エリア１６０ｂに格納されたＲＡＳ情報をＲＡＳ情報１６２と表記する。
【００４５】
送信部１７３は、保守エリア１６０ｂに格納されたＲＡＳ情報１６２を、保守サーバ２００に送信する処理部である。送信部１７３は、ＴＰＭチップ１５０に電子署名付与の依

頼を行うことで、ＲＡＳ情報１６２に電子署名を付与し、ＲＡＳ情報１６２を保守サーバ２００に送信する。送信部１７３は、保守サーバ２００のＴＰＭチップの秘密鍵と対になる公開鍵を用いて、ＲＡＳ情報１６２を暗号化し、保守サーバ２００にＲＡＳ情報を送信しても良い。

【００４６】

受信部１７４は、保守サーバ２００から、ＲＡＳ情報１６２に対応する保守ナレッジ情報１６３を受信する処理部である。受信部１７４は、受信した保守ナレッジ情報を、記憶部１６０の分析エリア１６０ｃに格納する。分析エリア１６０ｃに格納された保守ナレッジ情報を、保守ナレッジ情報１６３と表記する。

【００４７】

保守サーバ２００から送信される保守ナレッジ情報には、保守サーバ２００のＴＰＭチップによって生成された電子署名が付与されている。受信部１７４は、保守サーバ２００のＴＰＭチップの秘密鍵と対になる公開鍵と、保守ナレッジ情報１６３と、保守ナレッジ情報１６３に付与された電子署名を基にして、保守ナレッジ情報１６３が適切であるか否かを判定する。受信部１７４は、保守ナレッジ情報１６３が適切である場合に、保守ナレッジ情報１６３を、分析エリア１６０ｃに格納する。

【００４８】

また、受信部１７４は、保守ナレッジ情報１６３が暗号化されている場合には、ＴＰＭチップ１５０に保守ナレッジ情報１６３の復号を要求し、復号された保守ナレッジ情報１６３を、分析エリア１６０ｃに格納する。

【００４９】

分析部１７５は、情報エリア１６０ａの運用情報１６１を分析エリア１６０ｃに移動する。分析部１７５は、保守エリア１６０ｂのＲＡＳ情報１６２を分析エリア１６０ｃに移動する。そして、分析部１７５は、運用情報１６１、ＲＡＳ情報１６２、保守ナレッジ情報１６３を基にして、障害被疑部品の最適な交換順位を判定する。

【００５０】

ここで、分析部１７５が、被疑部品の最適な交換順序を判定する処理の一例について説明する。まず、分析部１７５は、運用情報１６１を基にして、各時刻の各電子機器２０の平均稼働率を求める。分析部１７５は、求めた各時刻の各電子機器２０の平均稼働率を参照し、平均稼働率が閾値以上となる時刻を特定する。以下の説明において、現在時刻よりも後の時刻であり、現時時刻に最も近い平均稼働率が閾値以上となる時刻を目標時刻と表記する。

【００５１】

続いて、分析部１７５は、現在時刻と目標時刻との差を算出する。以下の説明では、現在時刻と目標時刻との差を、差分時間と表記する。分析部１７５は、保守ナレッジ情報１６３に含まれる各被疑部品の交換時間をそれぞれ合計した合計時間と、差分時間との関係から、最適な交換順序を判定する。なお、分析部１７５は、ＲＡＳ情報１６２を基にして、被疑部品のうち、障害の発生していない被疑部品を取り除いた上で、下記の処理を実行する。例えば、被疑部品のうち、エラーコードが発生していない被疑部品は、障害が発生した部品ではないため、分析部１７５は、被疑部品から取り除く。

【００５２】

合計時間が差分時間よりも大きい場合について説明する。この場合、分析部１７５は、交換時間の少ない被疑部品を優先させて、交換順位を判定し、交換順位情報を生成する。例えば、保守ナレッジ情報１６３を図３に示すものとすると、分析部１７５は、図４に示す交換順位情報１６４を生成する。図４は、交換順位情報の一例を示す図（１）である。図４に示すように、交換順位情報１６４は、交換時間が最も少ない被疑部品「部品Ｂ」が交換順位「１位」となり、次いで、被疑部品「部品Ｃ」が「２位」、被疑部品「部品Ａ」が「３位」となる。

【００５３】

合計時間が差分時間以上の場合について説明する。この場合、分析部１７５は、被疑確

率の高い被疑部品を優先させて、交換順位を判定し、交換順位情報を生成する。例えば、保守ナレッジ情報１６３を、図３に示すものとすると、分析部１７５は、図５に示す交換順位情報を生成する。図５は、交換順位情報の一例を示す図（２）である。図５に示すように、交換順位情報１６４は、日日確率が最も高い被疑部品「部品Ａ」が交換順位「１位」となり、ついで、被疑部品「部品Ｂ」が「２位」、被疑部品「部品Ｃ」が「３位」となる。

【００５４】

分析部１７５は、生成した交換順位情報１６４を表示部１３０に表示させる。図６は、交換順位情報を表示する表示画面の一例を示す図である。分析部１７５は、目標時刻の情報も合わせて表示部１３０に表示させても良い。例えば、図６の補足情報が、目標時刻に対応する。また、分析部１７５は、交換順位情報を、保守エリア１６０ｂに格納する。

【００５５】

履歴生成部１７６は、取得部１７１、格納処理部１７２、送信部１７３、受信部１７４、分析部１７５の処理を監視し、各部１７１～１７５が実行した処理の履歴を、障害対処履歴情報１６５として生成する処理部である。例えば、履歴生成部１７６は、受信部１７１が受信した、運用情報１６１、ＲＡＳ情報１６２の実体、各情報を受信した時刻、各情報の出所、各情報に対して処理を行った時刻の情報を、障害対処履歴情報１６５に残す。また、履歴生成部１７６は、送信部１７３が送信したＲＡＳ情報１６２の実体、ＲＡＳ情報１６２を送信した時刻、ＲＡＳ情報１６２の出所、ＲＡＳ情報１６２に対して処理を行った時刻の情報を、障害対処履歴情報１６５に残す。また、履歴生成部１７６は、受信部１７５が受信した保守ナレッジ情報１６３の実体、保守ナレッジ情報１６３を送信した時刻、保守ナレッジ情報１６３の出所、保守ナレッジ情報１６３に対して処理を行った時刻の情報を、障害対処履歴情報１６５に残す。履歴生成部１７６は、障害対処履歴情報１６５を、保守エリア１６０ｂに格納する。なお、保守作業員の情報は、入力部１２０を介して取得するものとする。

【００５６】

判定部１７７は、保守作業が完了したか否かを判定する処理部である。例えば、判定部１７７は、入力部１２０を介して、保守作業員から、交換作業が完了した旨の情報を取得した場合に、電子機器２０ａとデータ通信を行って、顧客システム１０が正常に動作しているか否かの情報を取得する。

【００５７】

判定部１７７は、顧客システム１０が正常に動作している場合には、保守情報を生成し、生成した保守情報を、保守サーバ３００に送信する。保守情報には、交換順位情報１６４、障害対処履歴情報１６５が含まれる。また、保守情報は、ＴＰＭチップ１５０によって電子署名が付与される。判定部１７７は、保守情報を保守サーバ２００に送信した後に、初期化依頼を、初期化部１７８に出力する。

【００５８】

初期化部１７８は、判定部１７７から初期化依頼を受け付けた場合に、記憶部１６０の情報エリア１６０ａ、保守エリア１６０ｂ、分析エリア１６０ｃに格納された情報を全て消去する。初期化部１７８は、初期化が完了した旨を示す初期化完了情報を、保守サーバ２００に送信する。初期化完了情報は、ＴＰＭチップ１５０によって電子署名が付与される。

【００５９】

初期化部１７８は、初期化完了情報を送信した後、保守サーバ２００から、作業完了報告情報を受信した場合には、受信した作業完了報告情報を、表示部１３０に表示させる。図７は、作業完了情報を表示する表示画面の一例を示す図である。

【００６０】

次に、図１に示した保守センター３００に含まれる保守サーバ２００の構成について説明する。図８は、本実施例に係る保守サーバの構成を示す図である。図８に示すように、この保守サーバ２００は、通信部２１０、入力部２２０、表示部２３０、インタフェース

部２４０、ＴＰＭチップ２５０、記憶部２６０、制御部２７０を有する。各部２１０～２７０は、バス２８０によって相互に接続される。

【００６１】

通信部２１０は、社外のネットワーク５０を介して他の装置とデータ通信を行う処理部である。例えば、通信部２１０は、ネットワーク５０を介して、保守端末１００とデータをやり取りする。後述する制御部２７０は、通信部２１０を介して、保守端末１００とデータをやり取りする。

【００６２】

入力部２２０は、各種の情報を保守サーバ２００に入力する入力装置である。例えば、入力部２２０は、キーボードやマウス、タッチパネルなどに対応する。表示部２３０は、制御部２７０から出力される各種の情報を表示する表示装置である。例えば、表示部２３０は、液晶ディスプレイやタッチパネル等に対応する。インタフェース部２４０は、各種の外部装置と接続するインタフェースである。

【００６３】

ＴＰＭチップ２５０は、上述したＴＣＧ技術に準拠するＴＰＭチップである。例えば、ＴＰＭチップ２５０は、後述する制御部２７０が保守端末１００に送信する情報に、ＴＰＭチップ２５０に格納された秘密鍵によって電子署名を付与する。また、ＴＰＭチップ２５０は、制御部１７０によって情報の復号を要求された場合には、ＴＰＭチップ２５０の秘密鍵を用いて、情報を復号する。

【００６４】

記憶部２６０は、保守ナレッジ２６０ａを記憶する記憶装置である。保守ナレッジ２６０ａは、被疑部品判定テーブル２６１と、保守情報テーブル２６２と、初期化完了情報テーブル２６３を有する。例えば、記憶部２６０は、ハードディスク装置、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、フラッシュメモリ（Flash Memory）などの半導体メモリ素子などの記憶装置に対応する。

【００６５】

被疑部品判定テーブル２６１は、各種のＲＡＳ情報と障害の原因となる被疑部品の情報とを対応付けたテーブルである。図９は、被疑部品判定テーブルのデータ構造の一例を示す図である。図９に示すように、この被疑部品判定テーブル２６１は、ＲＡＳ情報、被疑部品、被疑確率、交換時間を対応付ける。このうちＲＡＳ情報は、障害等を一意に特定する情報である。被疑部品、被疑確率、交換時間に関する説明は、図３に示した被疑部品、被疑確率、交換時間に関する説明と同様である。

【００６６】

例えば、図９に示す例では、ＲＡＳ情報が「ＲＡＳ情報Ｘ１」である場合には、係る障害を引き起こした可能性のある被疑部品は「部品Ａ、部品Ｂ、部品Ｃ」であることが示されている。また、被疑部品「部品Ａ、部品Ｂ、部品Ｃ」の被疑確率はそれぞれ「５０％、３０％、２０％」であり、交換時間はそれぞれ「６０分、５分、１０分」である。

【００６７】

保守情報テーブル２６２は、保守端末１００から受信する保守情報を格納するテーブルである。保守情報には、上記のように、交換順位情報１６４、障害対処履歴情報１６５が含まれる。初期化完了情報テーブル２６３は、保守端末１００から受信する初期化完了情報を格納するテーブルである。

【００６８】

制御部２７０は、管理部２７１を有する。制御部２７０は、例えば、ＡＳＩＣや、ＦＰＧＡなどの集積装置に対応する。また、制御部２７０は、例えば、ＣＰＵ等の電子回路に対応する。

【００６９】

管理部２７１は、保守端末１００からＲＡＳ情報、保守情報、初期化完了情報を受信し、各種の処理を実行する処理部である。以下では、管理部２７１が、ＲＡＳ情報、保守情報、初期化完了情報を受信した場合の処理について順に説明する。なお、情報が暗号化さ

れている場合には、管理部２７１は、ＴＰＭチップ２５０に復号を依頼するものとする。また、管理部２７１は、情報に電子署名が付与されている場合には、保守端末１００のＴＰＭチップと対になる公開鍵を用いて、電子署名が適切であるか否かを判定し、適切である場合に、下記の処理を実行するものとする。

【００７０】

管理部２７１が、保守端末１００からＲＡＳ情報を受信した場合の処理について説明する。管理部２７１は、ＲＡＳ情報と、被疑部品判定テーブル２６１とを比較して、ＲＡＳ情報に対応する被疑部品、被疑確率、交換時間を含む保守ナレッジ情報を生成する。管理部２７１は、保守ナレッジ情報を、保守端末１００に送信する。

【００７１】

管理部２７１は、ＴＰＭチップ２５０に電子署名付与の依頼を行うことで、保守ナレッジ情報に電子署名を付与し、保守ナレッジ情報を保守端末１００に送信する。また、管理部２７１は、保守端末１００のＴＰＭチップの秘密鍵と対になる公開鍵を用いて、保守ナレッジ情報を暗号化し、保守端末１００に送信しても良い。

【００７２】

管理部２７１が、保守端末１００から保守情報を受信した場合の処理について説明する。管理部２７１は、保守情報を、保守情報テーブル２６２に格納する。管理部２７１は、保守情報の内容に応じて、被疑部品判定テーブル２６１を更新しても良い。

【００７３】

管理部２７１が、初期化完了情報を受信した場合の処理について説明する。管理部２７１は、初期化完了情報を受信した場合には、初期化完了情報を、初期化完了情報テーブル２６３に格納する。管理２７１は、完了報告書情報を生成し、完了報告書情報を、保守端末１００に送信する。

【００７４】

管理部２７１は、ＴＰＭチップ２５０に電子署名付与の依頼を行うことで、完了報告書情報に電子署名を付与し、完了報告書情報を保守端末１００に送信する。また、管理部２７１は、保守端末１００のＴＰＭチップ１５０の秘密鍵と対になる公開鍵を用いて、完了報告書情報を暗号化し、保守端末１００に送信しても良い。

【００７５】

更に、管理部２７１は、保守情報に含まれる障害対処履歴情報を、ハッシュ化して、ＥＭＡ局４００に送信する。管理部２７１は、例えば、ＴＰＭチップ２５０にハッシュ化を依頼する。ハッシュ化した障害対処履歴情報に、ＴＰＭ２５０の電子署名を付与しても良い。ＥＭＡ局４００に送信された、ハッシュ化された障害対処履歴情報は、ＥＭＡ局４００に保管される。

【００７６】

次に、本実施例に係る保守端末１００および保守サーバ２００の処理手順について説明する。図１０および図１１は、保守端末の処理手順を示すフローチャートである。図１０に示すように、保守端末１００は、保守端末１００と顧客システム１０の電子機器２０とが接続された場合に（ステップＳ１０１）、電子機器２０のエージェントプログラムを起動させる（ステップＳ１０２）。

【００７７】

保守端末１００は、エージェントを経由して運用情報およびＲＡＳ情報を取得する（ステップＳ１０３）。保守端末１００は、運用情報を、情報エリア１６０ａに格納し、ＲＡＳ情報を保守エリア１６０ｂに格納する（ステップＳ１０４）。保守端末１００は、ＴＰＭチップ１５０による電子署名を付与したＲＡＳ情報を保守サーバ２００に送信する（ステップＳ１０５）。

【００７８】

保守端末１００は、保守ナレッジ情報を受信し、分析エリア１６０ｃに保存する（ステップＳ１０６）。保守端末１００は、情報エリア１６０ａの運用情報１６１および保守エリア１６０ｂのＲＡＳ情報１６２を、分析エリア１６０ｃに移動させる（ステップＳ１０

７）。保守端末１００は、交換順位情報を生成し（ステップＳ１０８）、図１１のステップＳ１０９に移行する。

【００７９】

図１１の説明に移行する。保守端末１００は、交換順位情報を表示する（ステップＳ１０９）。保守端末１００は、交換作業完了を受付（ステップＳ１１０）、顧客システム１０が正常に動作するか否かを判定する（ステップＳ１１１）。保守端末１００は、顧客システム１０が正常に動作しない場合には（ステップＳ１１１，Ｎｏ）、エラーを出力し（ステップＳ１１２）、ステップＳ１１０に移行する。

【００８０】

保守端末１００は、顧客システム１０が正常に動作した場合には（ステップＳ１１１，Ｙｅｓ）、ＴＰＭチップ１５０による電子署名を付与した保守情報を保守サーバ２００に送信する（ステップＳ１１３）。例えば、保守情報には、交換順位情報１６４、障害対処履歴情報１６５が含まれる。保守端末１００は、初期化を行い（ステップＳ１１４）、ＴＰＭチップ１５０による電子署名を付与した初期化完了情報を保守サーバ２００に送信する（ステップＳ１１５）。保守端末１００は、保守サーバ２００から、完了報告書情報を受信し、表示する（ステップＳ１１６）。

【００８１】

図１２は、保守センターの処理手順を示すフローチャートである。図１２に示すように、保守端末１００からＲＡＳ情報を受信し（ステップＳ２０１）、ＲＡＳ情報に対応する保守ナレッジ情報を保守端末１００に送信する（ステップＳ２０２）。

【００８２】

保守サーバ２００は、保守端末１００から保守情報を受信し、保守情報を保存する（ステップＳ２０３）。保守サーバ２００は、保守端末１００から初期化完了情報を受信し、初期化完了情報を保存する（ステップＳ２０４）。保守サーバ２００は、完了報告書情報を保守端末１００に送信する（ステップＳ２０５）。

【００８３】

次に、本実施例に係る保守端末１００の効果について説明する。保守端末１００は、近距離ネットワークを介して、保守センター３００への送信を許可されていない運用情報および保守センター３００への送信を許可されたＲＡＳ情報を電子機器２０から取得する。保守端末１００は、ＲＡＳ情報を、ネットワーク５０を介して保守センター３００に送信する。保守端末１００は、ＲＡＳ情報に対応する保守ナレッジ情報を保守センター３００から受信する。そして、保守端末１００は、制御部１７０の処理履歴を障害対処履歴情報１６５として残し、障害対処履歴情報を、保守センター３００に送信する。保守センター側では、保守端末１００から送られてくる保守端末１００と電子機器２０との間のすべての通信内容を含む通信履歴と、保守端末１００と保守サーバー２００との間のすべての通信内容を含む通信履歴を保存するとともに、それぞれの通信履歴のハッシュ値を計算して保守サーバー内に保存して、または保存せずに、それぞれのハッシュ値をＥＭＡ局４００に送信する。このハッシュ値には通信履歴に関する属性情報、例えば通信機器対の名称、通信機器ＩＤ、通信時刻等が付随してもよい。ＥＭＡ局４００は、保守センター３００から送付されてきたハッシュ値をその属性情報とともに保存する。また、このハッシュ値とそれに付随する属性情報は電子署名を付してもよい。保守センターは通信履歴を改ざんした場合、そのハッシュ値がＥＭＡ局に保存されているハッシュ値と異なるものになるため、改ざんが検知されてしまう。したがって、保守センター側が少なくとも故意に通信履歴を改ざんすることはない。これによって、顧客がセキュリティ上の疑義を抱くことなく、保守端末１００が取得した顧客電子機器のＲＡＳ情報等各種情報と、保守センター内の膨大な保守ノウハウをもとに、的確な保守作業を実施することができる。

【００８４】

また、保守端末１００は社内のネットワークを介して、電子機器２０から運用情報およびＲＡＳ情報を取得し、情報エリア１６０ａに運用情報を格納し、保守エリア１６０ｂにＲＡＳ情報を格納する。保守端末１００は、保守エリア１６０ｂのＲＡＳ情報を、保守サ

ーバ２００に送信し、保守サーバ２００からＲＡＳ情報に対応する保守ナレッジ情報を受信する。このため、保守端末１００は、保守サーバ２００から得られた保守ナレッジ情報を利用して、適切な保守作業を実行するための情報を保守作業員に通知することができる。

【００８５】

また、保守端末１００は、運用情報および保守ナレッジ情報を基にして、交換順位情報を生成し、表示部１３０に表示させるので、顧客の業務状況によって、顧客装置に対して作業を行える時間が限られている場合であっても、最適な被疑部品の交換順位を提案することができる。例えば、顧客システム１０の利用ピーク時が迫っている場合などでも、保守作業員のスキルによらず、一定品質以上の保守サービスを提供することができる。

【００８６】

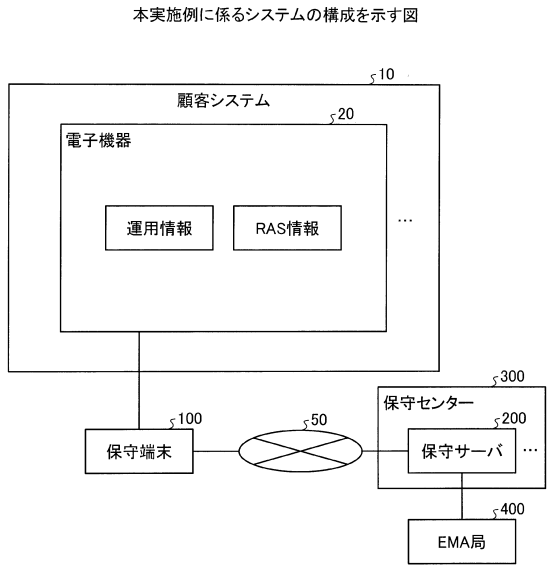
また、保守端末１００は、記憶部１６０としてＲＡＭを用いる。このため、保守端末１００の電源を落とすことで、記憶部１６０に記憶された顧客の情報を消去することができ、情報漏洩を防止することができる。

【符号の説明】

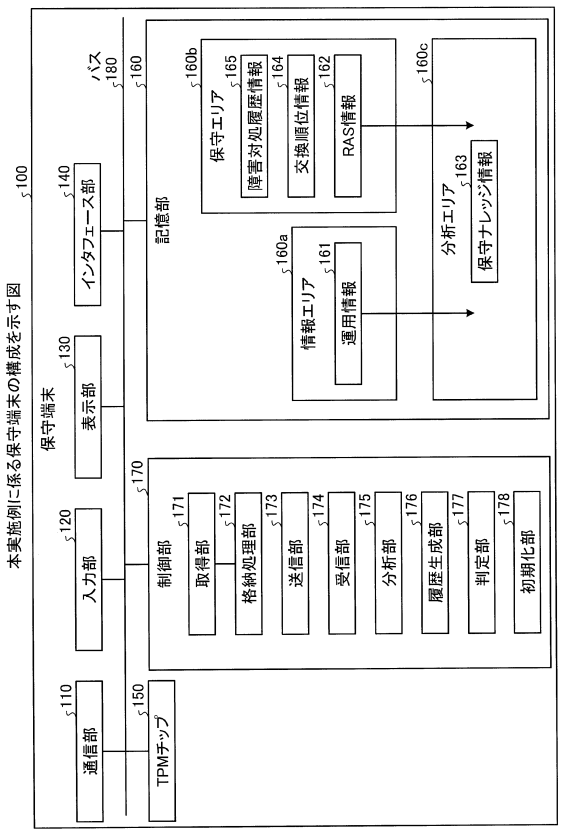
【００８７】

１０　顧客システム
５０　ネットワーク
１００　保守端末
２００　保守サーバ

【図１】



【図２】



【図３】

保守ナレッジ情報のデータ構造の一例を示す図

163

被疑部品	被疑確率	交換時間
部品A	50%	60分
部品B	30%	5分
部品C	20%	10分

【図４】

交換順位情報の一例を示す図(1)

被疑部品	被疑確率	交換時間	交換順位
部品B	30%	5分	1位
部品C	20%	10分	2位
部品A	50%	60分	3位

【図５】

交換順位情報の一例を示す図(2)

被疑部品	被疑確率	交換時間	交換順位
部品A	50%	60分	1位
部品B	30%	5分	2位
部品C	20%	10分	3位

【図６】

交換順位情報を表示する表示画面の一例を示す図

以下の順番で部品を交換し、システムを稼働してから、本装置をシステムに接続してください。

1、部品B(予想交換時間5分)
2、部品C(予測交換時間10分)
3、部品A(予想交換時間60分)
の順に、部品を交換してください。

補足情報:顧客の利用ピーク時刻は、12時です。

【図７】

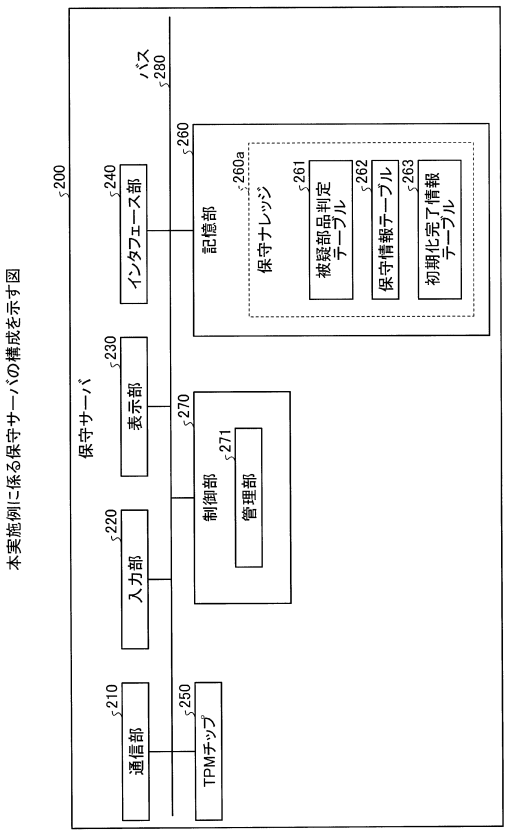
作業完了情報を表示する表示画面の一例を示す図

作業完了報告書

保守作業が完了し、本端末が初期化されたことを証明致します。

日時…1012/12/21
対象装置…顧客システム
現場保守作業員…甲
保守完了番号…A12991Z2243

【図８】



【図９】

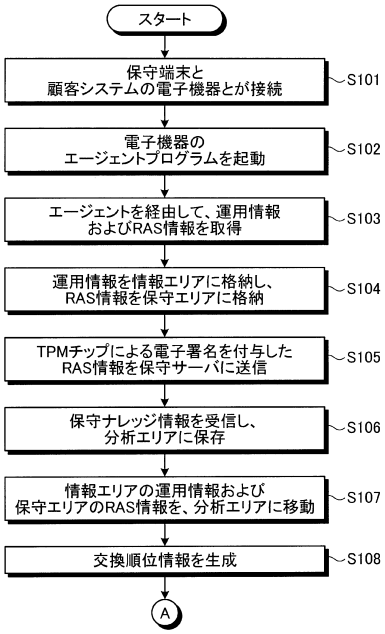
被疑部品判定テーブルのデータ構造の一例を示す図

261

RAS情報	被疑部品	被疑確率	交換時間
RAS情報X1	部品A	50%	60分
	部品B	30%	5分
	部品C	20%	10分
RAS情報X2	部品D	70%	20分
	部品E	30%	10分
…	…	…	…

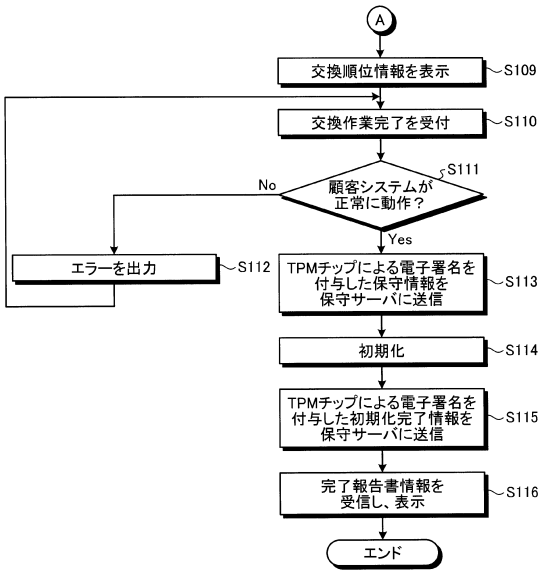
【図１０】

保守端末の処理手順を示すフローチャート（1）



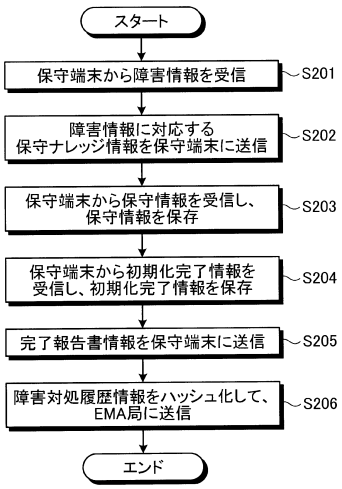
【図１１】

保守端末の処理手順を示すフローチャート（2）



【図１２】

保守サーバの処理手順を示すフローチャート



フロントページの続き

(72)発明者　今野　淳
東京都港区浜松町一丁目５番１号　株式会社富士通エフサス内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　藤野　明夫
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　杉浦　孝光

(56)参考文献　特開２００６－１７８７９４（ＪＰ，Ａ）
特開２００３－０３２７６４（ＪＰ，Ａ）
特開２００５－２５８８５５（ＪＰ，Ａ）
米国特許出願公開第２００４／０２５５００４（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９０／００
Ｇ０６Ｆ　１１／３０