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

特許第4185661号
(P4185661)

(45)発行日　平成20年11月26日(2008.11.26)　(24)登録日　平成20年9月12日(2008.9.12)

(51)Int.Cl.　　F I
G06Q 50/00 (2006.01)　　G06F 17/60　138
G06Q 30/00 (2006.01)　　G06F 17/60　318Z

請求項の数 26　(全 40 頁)

(21)出願番号　特願2000-351263 (P2000-351263)
(22)出願日　平成12年11月17日 (2000.11.17)
(65)公開番号　特開2002-157357 (P2002-157357A)
(43)公開日　平成14年5月31日 (2002.5.31)
審査請求日　平成16年12月15日 (2004.12.15)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090538
弁理士　西山　恵三
(74)代理人　100096965
弁理士　内尾　裕一
(72)発明者　片山　康二朗
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　中村　真一
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

最終頁に続く

(54)【発明の名称】機器管理装置、機器管理プログラム、機器管理プログラムが格納された記録媒体、及び機器管理方法

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して機器を管理する機器管理装置であって、
前記機器の障害を示すデータを受信する障害検知手段と、
前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、
ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、
前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、
前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する作成手段と、
予め決められた宛先に、前記作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段とを有することを特徴とする機器管理装置。
【請求項２】
前記送信制御手段により送信された復旧作業要求データに対する、作業報告データを前記復旧作業要求データが送信された宛先から受信する受信手段を有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】

前記作成手段により復旧作業要求データが作成される際に、当該復旧作業要求データに対する識別子を発行する発行手段と、
前記発行手段により発行された識別子と共に、当該復旧作業要求データに対応する復旧作業の状態を管理する管理手段とを有することを特徴とする請求項２に記載の機器管理装置。
【請求項４】
前記送信制御手段は、前記復旧作業要求データとともに、前記発行手段により発行された識別子を送信するように制御し、
前記受信手段は、前記作業報告データとともに、前記送信制御手段により送信された識別子を受信し、
前記管理手段は、前記受信手段により受信された前記作業報告データに基づいて、前記受信手段により受信された識別子に対応する復旧作業の状態を変更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】
複数の宛先のうち、前記機器の復旧作業要求データを送信すべき宛先を選択する選択手段を有し、
前記障害検知手段は、障害が検知された機器を識別する機器情報を受信し、
前記選択手段は、受信された前記機器情報に基づいて、前記機器の復旧作業要求データを送信すべき宛先を選択することを特徴とする請求項１乃至４のいずれかに記載の機器管理装置。
【請求項６】
前記障害検知手段は、検知された障害を識別する障害情報を受信し、前記作成手段は、受信された障害情報を、前記作業依頼書用テンプレートに埋め込むことを特徴とする請求項１乃至５のいずれかに記載の機器管理装置。
【請求項７】
前記作成手段は、受信された障害情報により識別される障害の対応方法を示すデータを、前記作業依頼書用テンプレートに埋め込むことを特徴とする請求項１乃至６のいずれかに記載の機器管理装置。
【請求項８】
前記障害検知手段により検知された障害の対応者を判断する判断手段と、
前記対応者が前記機器を有する顧客であると判断されるのに応じて、前記顧客に関する顧客情報と、検知された障害の対処方法を示すメッセージを表示部に表示させる表示制御手段とを有することを特徴とする請求項１乃至７のいずれかに記載の機器管理装置。
【請求項９】
前記機器の復旧作業の緊急度を示す情報は、前記機器の復旧作業の対応期限を示す情報を含むことを特徴とする請求項１乃至請求項８のいずれかに記載の機器管理装置。
【請求項１０】
前記決定手段は、複数ある、機器の復旧作業の緊急度を示す情報のうち、前記作業依頼書用テンプレートに埋め込むべき緊急度を示す情報を、前記障害検知手段によって受信されるデータによって示される機器に対応する顧客の契約レベルに応じて決定することを特徴とする請求項１乃至請求項８のいずれかに記載の機器管理装置。
【請求項１１】
ネットワークを介して機器を管理する機器管理プログラムを格納したコンピュータにより読み取り可能な記録媒体であって、前記機器管理プログラムは、
前記機器の障害を示すデータを受信する障害検知ステップと、
前記障害検知ステップにより受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別ステップと、
ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別ステップにより識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定ステップと、

前記障害検知ステップにより障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別ステップにより識別されたユーザを示す情報と前記決定ステップにより決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する作成ステップと、

予め決められた宛先に、前記作成ステップにより作成された復旧作業要求データを送信するよう制御する送信制御ステップとをコンピュータに実行させることを特徴とする記録媒体。

【請求項１２】

ネットワークを介して機器を管理する機器管理装置の制御方法であって、

前記機器の障害を検知する障害検知ステップと、

前記障害検知ステップにより受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別ステップと、

ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別ステップにより識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定ステップと、

前記障害検知ステップにより障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別ステップにより識別されたユーザを示す情報と前記決定ステップにより決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する作成ステップと、

予め決められた宛先に、前記作成ステップにより作成された復旧作業要求データを送信するよう制御する送信制御ステップとを有することを特徴とする機器管理装置の制御方法。

【請求項１３】

送信された復旧作業要求データに対する、作業報告データを前記復旧作業要求データが送信された宛先から受信する受信ステップを有することを特徴とする請求項１２に記載の機器管理装置の制御方法。

【請求項１４】

前記作成ステップにより復旧作業要求データが作成される際に、当該復旧作業要求データに対する識別子を発行する発行ステップと、

前記発行ステップにより発行された識別子と共に、当該復旧作業要求データに対応する復旧作業の状態を管理する管理ステップとを有することを特徴とする請求項１３に記載の機器管理装置の制御方法。

【請求項１５】

前記送信制御ステップは、前記復旧作業要求データとともに、前記発行ステップにより発行された識別子を送信するように制御し、

前記受信ステップは、前記作業報告データとともに、前記送信制御ステップにより送信された識別子を受信し、

前記管理ステップは、前記受信ステップにより受信された前記作業報告データに基づいて、前記受信ステップにより受信された識別子に対応する復旧作業の状態を変更することを特徴とする請求項１４に記載の機器管理装置の制御方法。

【請求項１６】

前記送信制御ステップは、電子メールにおいて前記復旧作業要求データを送信することを特徴とする請求項１２乃至１５のいずれかに記載の機器管理装置の制御方法。

【請求項１７】

複数の宛先のうち、前記機器の復旧作業要求データを送信すべき宛先を選択する選択ステップを有し、

前記障害検知ステップは、障害が検知された機器を識別する機器情報を取得し、

前記選択ステップは、受信された前記機器情報に基づいて、前記機器の復旧作業要求データを送信すべき宛先を選択することを特徴とする請求項１２乃至１６のいずれかに記載の機器管理装置の制御方法。

【請求項１８】
前記障害検知ステップは、検知された障害を識別する障害情報を取得し、
前記作成ステップは、受信された障害情報を、前記作業依頼書用テンプレートにデータに埋め込むことを特徴とする請求項１２乃至１７のいずれかに記載の機器管理装置の制御方法。
【請求項１９】
前記作成ステップは、受信された障害情報により識別される障害の対応方法を示すデータを、前記作業依頼書用テンプレートに埋め込むことを特徴とする請求項１２乃至１８のいずれかに記載の機器管理装置の制御方法。
【請求項２０】
前記障害検知ステップにより検知された障害の対応者を判断する判断ステップと、
前記対応者が前記機器を有する顧客であると判断されるのに応じて、前記顧客に関する顧客情報と、検知された障害の対処方法を示すメッセージを表示部に表示させる表示制御ステップとを有することを特徴とする請求項１２乃至１９のいずれかに記載の機器管理装置の制御方法。
【請求項２１】
前記対応者が顧客ではないと判断されるのに応じて、前記送信制御ステップは、前記予め決められた宛先に、前記作成ステップにより作成された復旧作業要求データを送信するよう制御することを特徴とする請求項２０に記載の機器管理装置の制御方法。
【請求項２２】
前記機器の復旧作業の緊急度を示す情報は、前記機器の復旧作業の対応期限を示す情報を含むことを特徴とする請求項１２乃至請求項２１のいずれかに記載の機器管理装置の制御方法。
【請求項２３】
前記決定ステップは、複数ある、機器の復旧作業の緊急度を示す情報のうち、前記作業依頼書用テンプレートに埋め込むべき緊急度を示す情報を、前記障害検知ステップによって受信されるデータによって示される機器に対応する顧客の契約レベルに応じて決定することを特徴とする請求項１２乃至請求項２２のいずれかに記載の機器管理装置の制御方法。
【請求項２４】
ネットワークを介して機器を管理する機器管理装置であって、
前記機器の障害を示すデータを受信する障害検知手段と、
前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、
ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、
前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、
前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と、前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、
前記機器の障害ごとに前記復旧作業要求データを送信すべき宛先を記憶する記憶手段と、
前記記憶手段に記憶された、前記復旧作業要求データを送信すべき宛先のうち、前記障害検知手段によって受信されたデータによって示される障害に対応する宛先に、前記第１の作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段と、
前記機器のカウント情報を取得するカウンタ取得手段と、
前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告

データを作成する第２の作成手段と、
障害が発生すると、障害が発生した機器を示す機器情報を含む障害情報を保存する保存手段とを有し、
前記第２の作成手段は、前記保存手段に保存された障害情報に基づいて、障害が複数回発生した機器を示す機器情報を特定し、特定した機器情報を前記稼動報告データに埋め込むことを特徴とする機器管理装置。
【請求項２５】
ネットワークを介して機器を管理する機器管理装置であって、
前記機器の障害を示すデータを受信する障害検知手段と、
前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、
ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、
前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、
前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、
予め決められた宛先に、前記第１の作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段と、
当該復旧作業要求データに対応し、復旧作業がなされた場合に受信する復旧作業報告データを受信したか否かを示す情報を管理する管理手段と、
前記機器のカウント情報を取得するカウンタ取得手段と、
前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告データを作成する第２の作成手段とを有し、
前記第２の作成手段は、前記管理手段により管理されている復旧作業要求データに対応する復旧作業報告データを受信したか否かを示す情報に基づいて、当該復旧作業がなされていない機器を示す機器情報を、前記稼動報告データに埋め込むことを特徴とする機器管理装置。
【請求項２６】
ネットワークを介して機器を管理する機器管理装置であって、
前記機器の障害を示すデータを受信する障害検知手段と、
前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、
ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、
前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、
前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と、前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、
前記機器の障害ごとに前記復旧作業要求データを送信すべき宛先を記憶する記憶手段と、
前記記憶手段に記憶された、前記復旧作業要求データを送信すべき宛先のうち、前記障害検知手段によって受信されたデータによって示される障害に対応する宛先に、前記第１の作成手段により作成された作業依頼データを送信するよう制御する送信制御手段と、
前記機器のカウント情報を取得するカウンタ取得手段と、
前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告データを作成する第２の作成手段と、

障害が発生すると、障害が発生した機器を示す機器情報を含む障害情報を保存する保存手段を有し、

前記第２の作成手段は、前記保存手段に保存された障害情報に基づいて、障害が発生していない機器を示す機器情報を特定し、特定した障害情報を前記稼動報告データに埋め込むことを特徴とする機器管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、たとえばコンピュータネットワークを介して接続された、汎用性のあるパーソナルコンピュータ（ＰＣ）やサーバコンピュータといったＰＣ・サーバ系機器と、専用の機能、特にプリンタや複写機、スキャンといった入出力機能に特化した周辺機器（デバイス）系機器の状態を、包括的に遠隔監視する遠隔サイト管理システムに関するものである。

【０００２】

【従来の技術】

従来、オフィス内の機器に関する稼動情報、エラー情報、ログ情報などをオフィス内で収集するような監視・管理システムは存在していた。また、そのようにオフィスで収集された情報をネットワークを介してオフィスの外部に設置・接続されたセンタサーバに収集し監視・管理するようなシステムも存在していた。

【０００３】

しかしながら、それらの管理・監視システムはＰＣ・サーバ系すなわち汎用コンピュータのみを監視・管理するようなシステムであったり、プリンタや複写機などのデバイス系のみを監視・管理するようなシステムであった。

【０００４】

このように、汎用コンピュータとデバイスとが別個に管理されていたのは、汎用コンピュータとデバイスとを管理する手順等が全く異なるためである。すなわち、汎用コンピュータを管理する場合には、コンピュータのオペレーティングシステム等の環境に応じて所望の機能を果たすプログラムを作成し、管理対象のコンピュータで実行させることが必要であるのに対して、周辺機器を管理する場合には、機能の後付や変更が実際上ほとんど不可能であった。

【０００５】

加えて、周辺機器を管理する場合、監視・管理システムが周辺機器とやりとりするデータ形式や交換の手順（プロトコル）に標準的なものが存在しなかった。そのため、周辺機器ごとに対応した管理手順を開発しなければならず、個々の周辺機器がそれぞれ管理サイトに接続され、管理されていた。

【０００６】

このようにデバイス系の管理システムはＰＣ・サーバ系の管理システムとは相容れず、それぞれ全く別個に存在していた。

【０００７】

【発明が解決しようとする課題】

その一方、デバイス系の周辺機器とＰＣ・サーバ系のコンピュータが共にオフィス環境で普及するにつれて、それらを統括的に監視・管理する保守サービスが望まれている。

【０００８】

しかし、従来の方法では、保守サービス会社（管理サイト）が、あるオフィスのデバイス系とＰＣ・サーバ系との両方を監視・管理するためには、両方のシステムをオフィスに設置して、別々の回線を通じて情報を収集し、別々に監視・管理しなければならなかった。そのため、保守サービス会社における管理の煩雑化、システムの運用費・維持費の高価格化が生じた。

【０００９】

そこで、本発明は、上記問題点を鑑みてなされたものであり、管理サイトが、オフィスに

おけるＰＣ・サーバ系の機器とデバイス系の機器との双方を、一元的に管理できる遠隔サイト管理システムを提供することを目的とする。

【００１０】

特に、管理サイトが、オフィスのＰＣ・サーバ系の機器とデバイス系の機器との障害情報及び予兆情報を自動的に受信し、顧客になにも意識させることなく、メンテナンスサービスを提供し、更に、実際にメンテナンスサービスを行なうサービス会社への依頼書の送付、サービス会社からの作業報告書を一本化することを目的とする。

【００１１】

また、カウンタ情報と障害履歴を用いて、オフィス環境での機器の稼動報告書を顧客に提供することを目的とする。

【００１２】

【課題を解決するための手段】

本発明に係る機器管理装置は、ネットワークを介して機器を管理する機器管理装置であって、前記機器の障害を示すデータを受信する障害検知手段と、前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する作成手段と、予め決められた宛先に、前記作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段とを有することを特徴とする。

【００１３】

また、本発明では、送信された復旧作業要求データに対する、作業報告データを前記復旧作業要求データが送信された宛先から受信することを特徴とする。

【００１４】

さらに、本発明では、前記復旧作業要求データが作成される際に、当該復旧作業要求データに対する識別子を発行し、発行された識別子と共に、当該復旧作業要求データに対する復旧作業の状態を管理する管理手段とを有することを特徴とする。

【００１５】

さらに、本発明では、前記復旧作業要求データとともに、発行された識別子を送信するように制御し、前記作業報告書を示すデータとともに、前記送信制御手段により送信された識別子を受信し、受信された前記作業報告データに基づいて、受信された識別子に対応する復旧作業の状態を変更することを特徴とする。

【００１６】

さらに、本発明では、電子メールにおいて前記復旧作業要求データを送信することを特徴とする。

【００１７】

さらに、本発明では、障害が検知された機器を識別する機器情報を受信し、受信された前記機器情報に基づいて、前記機器の復旧作業要求データを送信すべき宛先を選択することを特徴とする。

【００１８】

さらに、本発明では、検知された障害を識別する障害情報を受信し、受信された障害情報を、前記作業依頼書用テンプレートに埋め込むことを特徴とする。

【００１９】

さらに、本発明では、受信された障害情報により識別される障害の対応方法を示すデータを、前記作業依頼用テンプレートに埋め込むことを特徴とする。

【００２０】

さらに、本発明では、検知された障害の対応者を判断し、前記対応者が前記機器を有する

顧客であると判断されるのに応じて、前記顧客に関する顧客情報と、検知された障害の対処方法を示すメッセージを表示部に表示させることを特徴とする。

【００２１】

さらに、本発明では、前記対応者が顧客ではないと判断されるのに応じて、予め決められた宛先に、前記復旧作業要求データを送信するよう制御することを特徴とする。

【００２２】

また、本発明に係る機器管理装置は、ネットワークを介して機器を管理する機器管理装置であって、前記機器の障害を示すデータを受信する障害検知手段と、前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と、前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、前記機器の障害ごとに前記復旧作業要求データを送信すべき宛先を記憶する記憶手段と、前記記憶手段に記憶された、前記復旧作業要求データを送信すべき宛先のうち、前記障害検知手段によって受信されたデータによって示される障害に対応する宛先に、前記第１の作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段と、前記機器のカウント情報を取得するカウンタ取得手段と、前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告データを作成する第２の作成手段と、障害が発生すると、障害が発生した機器を示す機器情報を含む障害情報を格納する格納手段とを有し、前記第２の作成手段は、前記格納手段に格納された障害情報に基づいて、障害が複数回発生した機器を示す機器情報を特定し、特定した機器情報を前記稼動報告書を示すデータに埋め込むことを特徴とする。

【００２３】

また、本発明に係る機器管理装置は、ネットワークを介して機器を管理する機器管理装置であって、前記機器の障害を示すデータを受信する障害検知手段と、前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、予め決められた宛先に、前記第１の作成手段により作成された復旧作業要求データを送信するよう制御する送信制御手段と、当該復旧作業要求データに対応し、復旧作業がなされた場合に受信する復旧作業報告データを受信したか否かを示す情報を管理する管理手段と、前記機器のカウント情報を取得するカウンタ取得手段と、前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告データを作成する第２の作成手段とを有し、前記第２の作成手段は、前記管理手段により管理されている復旧作業要求データに対応する復旧作業報告データを受信したか否かを示す情報に基づいて、当該復旧作業がなされていない機器を示す機器情報を、前記稼動報告データに埋め込むことを特徴とする。

【００２４】

また、本発明に係る機器管理装置は、ネットワークを介して機器を管理する機器管理装置であって、前記機器の障害を示すデータを受信する障害検知手段と、前記障害検知手段によって受信されたデータに含まれる情報に基づいて特定される機器に対応するユーザを識別する識別手段と、ユーザごとに機器の復旧作業の緊急度を示す情報を格納する格納手段と、前記格納手段に格納された、機器の復旧作業の緊急度を示す情報のうち、前記識別

手段によって識別されたユーザに対応する緊急度を示す情報に基づいて緊急度を決定する決定手段と、前記障害検知手段により障害が検知されるのに応じて、作業依頼書用テンプレートに、前記識別手段によって識別されたユーザを示す情報と、前記決定手段により決定された緊急度を示す情報を埋め込むことにより、復旧作業要求データを作成する第１の作成手段と、前記機器の障害ごとに前記復旧作業要求データを送信すべき宛先を記憶する記憶手段と、前記記憶手段に記憶された、前記復旧作業要求データを送信すべき宛先のうち、前記障害検知手段によって受信されたデータによって示される障害に対応する宛先に、前記第１の作成手段により作成された作業依頼データを送信するよう制御する送信制御手段と、前記機器のカウント情報を取得するカウンタ取得手段と、前記カウンタ取得手段により取得されたカウンタ情報に基づいて、前記機器の稼動報告データを作成する第２の作成手段と、障害が発生すると、障害が発生した機器を示す機器情報を含む障害情報を格納する格納手段を有し、前記第２の作成手段は、前記格納手段に格納された障害情報に基づいて、障害が発生していない機器を示す機器情報を特定し、特定した障害情報を前記稼動報告データに埋め込むことを特徴とする。

【００２５】

【発明の実施の形態】

＜第１の遠隔サイト管理システムの構成＞

図を参照して本発明に係る遠隔サイト管理システムを説明する。

【００２６】

図１は、遠隔サイト管理システムにおける被管理サイト（オフィス側）と管理サイト（保守サービス会社側）の構成を示すブロック図である。被管理サイトでは、汎用コンピュータであるＰＣ１０３、デバイス監視サーバ２０３ａ（オフィスのローカルネットワーク上に接続されたデバイス系の周辺機器を管理する情報機器）、周辺機器である複写機１０１、プリンタ１０５、プリンタ１０４がＬＡＮ（ローカルエリアネットワーク）で接続されている。

【００２７】

なお、ここでいう汎用コンピュータは、パーソナルコンピュータやサーバコンピュータのほか、ゲートウエイ、ルータなどのコンピュータネットワークに欠かせないネットワーク機器をも含むものとする。周辺機器は、複写機、プリンタ、スキャナー、ＦＡＸ、複合機等を含むものとする。

【００２８】

ＰＣ１０３では、後述するＰＣ監視クライアントモジュールが実行され、これは、オフィスのローカルネットワーク上に接続された汎用コンピュータ機器等を管理することができる。また、デバイス監視サーバ２０３ａとＰＣ監視クライアントモジュールは物理的に別々のコンピュータで実行されてもよく、また一つのコンピュータで実行されても良い。

【００２９】

また、図１に記載はされてはいないが、この遠隔サイト管理システムには、データフォーマット変換装置がある。これは、デバイス監視サーバ２０３ａとＰＣ監視クライアントモジュールとの間のデータフォーマット形式を変換・調整する装置である。

【００３０】

また、管理サイトには、被管理サイトの機器を一元的に管理するためのセンタサーバ１１０、管理情報等を蓄積するためのインベントリデータベース１０９、被管理サイトにおける周辺機器の管理を専門に行うためのデバイスセンタサーバ２１０が、それぞれＬＡＮに接続されている。また、このシステムでは、サーバ・ＰＣ１１１といったその他のコンピュータが接続されている。このコンピュータ１１１では、管理情報を用いて、オフィス機器を統括管理するアプリケーションプログラムが実行されている。

【００３１】

また、図１に記載はされてはいないが、管理サイトには、被管理サイトから通知されてくる情報を表示させる表示装置や、センタサーバ１１０とデバイスセンタサーバ２１０との間でデータフォーマット形式を変換・調整する変換装置もある。

【００３２】
また、複数の管理サイトを統合的に管理するサービスセンタ（図２のアプリケーションシステム２０５に相当）もあり、これは、管理サイトと外部ネットワークまたはＬＡＮを介して接続さている。
【００３３】
これら被管理サイトと管理サイトは、互いにゲートウエイ１０６，１０７で接続されている。この接続は、汎用のルータやモデム等を用いても良い。また、ＰＣ１０３においてＰＣ監視クライアントモジュールが実行されている場合には、ＰＣ１０３とセンタサーバ１１０との間の回線と、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０との間の回線が、それぞれ別々に設けられ、それぞれ独立していてもよい。
【００３４】
図３は、ＰＣ及びサーバコンピュータの構成を示すブロック図である。図３において、コンピュータ３０００は、ＣＰＵ１、ＲＡＭ２、ＲＯＭ３、システムバス４、ＫＢＣ５、ＣＲＴＣ６、ＭＣ７、ＬＡＮ制御部８、ＫＢ９、ＣＲＴ１０、外部メモリ１１とを備える。
【００３５】
ＣＰＵ１は、ＲＯＭ３のプログラム用ＲＯＭに記憶された通信制御プログラムを実行して、それに基づいて、指定されたデータの外部への送信を制御したり、あるいは外部からのデータの受信を制御したりする。また、ＣＰＵ１は、システムバス４に接続される各デバイスを統括的に制御する。
【００３６】
ＲＡＭ２は、ＣＰＵ１の主メモリ、ワークエリア等として機能する。ＲＯＭは、それぞれフォント（フォントＲＯＭ）、プログラム（プログラムＲＯＭ）、データ（データＲＯＭ）を記憶する。キーボードコントローラ（ＫＢＣ）５は、キーボード９や不図示のポインティングデバイスからのキー入力を制御する。ＣＲＴコントローラ（ＣＲＴＣ）６は、ＣＲＴディスプレイ１０の表示を制御する。メモリコントローラ（ＭＣ）７は、外部メモリ１１へのアクセスを制御する。ハードディスク（ＨＤ）やフロッピーディスク（ＦＤ）等の外部メモリ１１は、ブートプログラム、種々のアプリケーション、フォントデータ、ユーザファイル、後述する編集ファイル等を記憶する。ＬＡＮ制御部８は、ネットワークに接続されて、ネットワークに接続された他の機器との通信処理を実行する。
【００３７】
図２は本遠隔サイト管理システムのソフトウエアモジュールの構成を示すブロック図である。ユーザ拠点システム（被管理サイトを指す）では、デバイス系機器（複写機、プリンタ、複合機、スキャナ、ＦＡＸ等の周辺機器）と、ＰＣ・サーバ系機器（汎用コンピュータなど）が混在している。が、デバイス系機器はデバイス監視サーバ２０３ａによって、ＰＣ・サーバ系機器はＰＣ監視クライアントモジュール２０３ｄによってぞれぞれローカルで管理される。これらを総称して、拠点側管理システム２０３と呼ぶことにする。デバイス監視サーバ２０３ａは、管理情報を蓄積するためのデータベース２０３ａ－１を有する。
【００３８】
一方、センターシステム（管理サイトを指す）は、デバイス監視サーバ２０３ａとの間でデータを交換するデバイスセンタサーバ２１０と、ＰＣ監視クライアントモジュール２０３ｄとの間でデータを交換するセンタサーバ１１０とを含む。デバイス系機器の管理情報はインベントリデータベース１０９に蓄積される。また、センタサーバ１１０によって管理される管理情報もインベントリデータベース１０９に蓄積される。これらインベントリデータベース１０９に蓄積される管理情報は、アプリケーションシステム２０５等により利用される。なお、インベントリデータベース１０９はデバイス系とＰＣ・サーバ等の汎用コンピュータ系とで、それぞれ論理的に分かれていればよく、無論、物理的に分かれていてもよい。
【００３９】
デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とは、データ形式や手順を必

要に応じて変換するための拠点プラグインモジュール２０３ｂとサーバプラグインモジュールを介して接続されている。これら拠点プラグインモジュールとサーバプラグインモジュールとによって、拠点側とセンタ側とで使用ＯＳが異なる場合などでも、お互いの通信が可能になる。また、電気的には、ルータ２０４を介する。この回線は、ＰＣ監視クライアント２０３ｄとセンタサーバ１１０とを接続する回線と物理的または論理的に共用されている。

【００４０】

デバイスセンタサーバ２１０とデバイス監視サーバ２０３ａを接続する回線は、監視クライアント２０３ｄとセンタサーバ間を接続する回線と共用されない場合も想定される。その場合には、モデムやルータを介して、監視クライアント２０３ｄ－センタサーバ１１０とは独立した回線で接続されても良い。

【００４１】

センタサーバ１１０には、イベントモニタ１１０ａが含まれており、センタサーバ１１０に対して発行されたイベントを監視し、障害の発生等を伝えるイベントであればモニタ上に表示する。管理者はその表示を見ることで、被管理サイトにおいて発生した障害の状況を知ることができる。センタサーバ１１０に対してイベントを発行するのは、イベントアダプタ２１０ａと、ＰＣ監視クライアント２０３ｄと、アプリケーションシステム２０５である。センタサーバ１１０は、受け取ったイベントを、それが示す内容に従って所定の処理を実行する。イベントとしては例えば、障害通知等がある。

【００４２】

デバイスセンタサーバ２１０には、イベントアダプタモジュール２１０ａが含まれている。イベントアダプタ２１０ａは、デバイス監視サーバ２０３ａからデバイスセンタサーバ２１０に対して送られてきて受信した情報を定期的に検索する機能をもち、その検索された情報の内から、周辺機器において発生した障害に関する情報を判別してより分けて、センタサーバ１１０において処理可能な形式（ファイル形式、プロトコル形式等）に変換してから、センタサーバ１１０に対して障害の発生を示すイベントを発行する。あるいは、イベントアダプタモジュール２１０ａによってセンタサーバに処理化能な形式に変換する機能をセンタサーバ１１０に持たせてもよい。障害関連のイベント（障害イベント）には、障害の起きた装置やその内容、発生時刻等が含まれる。このイベントアダプタ２１０ａを本システム及び装置に設けることによって、デバイス専用に想定されたプロトコル・フォーマットを使用した管理ソフトによって得られたデバイス固有の情報、例えば、紙詰まり、ステープル機能チェック等を別の種別のシステム・装置（実施例では汎用コンピュータ・サーバ等）を監視するソフトと一元化して管理することが可能となる。

【００４３】

イベントモニタ１１０ａはそれを受けて、障害の起きた装置やその内容、発生時刻等を、イベントのリストに加えて表示する。表示の方法としては、たとえば、１行に１イベントを表示し、時系列的にイベントのリストを表示する。図２ではイベントモニタ１１０ａはセンタサーバ１１０に含まれる形で記載されているが、このイベントモニタ１１０ａをセンタサーバ１１０からネットワーク等を介して外部に接続することで、例えば、デバイスセンタサーバ２１０側やアプリケーションシステム２０５側でデバース系、ＰＣ・サーバ系を包括管理することが可能となる。

【００４４】

ここで注意すべきなのは、イベントモニタ１１０ａは、イベントの発生元を意識することなく、障害系のイベントであればそれを表示することで、管理者の注意を喚起できる、ということである。すなわち、イベントモニタ１１０ａにおいては、ＰＣ監視クライアント２０３ｄから発行された、汎用コンピュータ系の障害イベントと、デバイスセンタサーバ２１０のイベントアダプタ２１０ａを介してデバイス監視サーバ２０３ａから発行された、周辺機器系の障害イベントとを、同一画面上のイベントリストにたとえば時系列的に表示する。

【００４５】

次に、デバイスセンタサーバ２１０と、デバイス監視サーバ２０３ａとの間でなされるデータ交換の手順の例を、図４を参照しつつ、（１）デバイスへの、デバイスセンタサーバ２１０からの設定値のダウンロード、（２）デバイス監視サーバ２０３ａからデバイスセンタサーバ２１０へのログデータのアップロード、（３）デバイスセンタサーバ２１０からデバイス監視サーバ２０３ａへのカウンタデータの要求、という３つのケースで説明する。その前に、データフォーマットについて簡単に説明する。

【００４６】

図８は、デバイスセンタサーバ２１０とデバイス監視サーバ２０３ａとの間で交換されるメッセージフォーマットの一例を示す図である。１つのメッセージは、フラグフィールド，データ種別フィールド，ジョブＩＤフィールド，リターン値フィールド，データ長フィールド，データフィールドを含む。フラグフィールドには、通信手段を示すビット群と、そのメッセージがデータの最終フレームであるか否かを示すビットが含まれる。

【００４７】

データ種別フィールドでは、たとえば認証要求データ（セッションの先頭に送信されるデータ）であることや、ダウンロードされる設定値データであること、後述するデバイス情報要求であること、イベント情報の通知であること、ログデータ処理要求であることなどが示される。たとえば障害の通知などは、イベント情報であることがデータ種別として示され、データフィールドで具体的な内容が示される。

【００４８】

ジョブＩＤは、そのセッションの種類を示すもので、パラメータ設定やデバイス情報の取得、イベント通知などがこれによって示される。データ長には後続するデータの長さが示され、データフィールドには、データ長で示された長さのデータが格納される。設定値のダウンロードやログデータの処理要求には、データフィールドにデータが載せられる。また、カウンタアップロードにおいては、デバイス情報要求に対する応答のデータフィールドに、デバイス情報が載せられる。

【００４９】

以下の手順をはじめ、デバイスセンタサーバ２１０やデバイス監視サーバ２０３ａは、このメッセージを交換しつつ処理を遂行する。なお、以下の説明では、イベントとは、イベントの発生を伝えるためのメッセージという意味で使用している。

【００５０】

＜設定値ダウンロード手順＞

図４は、拠点システムとセンタシステムとの間で行われる、データの交換の手順を説明するためのブロック図である。

【００５１】

設定値のダウンロードは次のようにして行われる。

【００５２】

（１）アプリケーションシステム２０５において、手作業などで、設定対象のデバイスの指定やデバイスのＩＰアドレス、デバイスの拠点デバイスサーバに対するエラー等のアラーム通知の時の閾値の設定値等を入力し、設定値情報ファイル４０１を作成する。

【００５３】

（２）アプリケーションシステム２０５よりデバイスセンタサーバ２１０との間のセッションを確立し、設定値情報ファイル４０１に含まれる設定値データを送信する。

【００５４】

（３）デバイスセンタサーバ２１０は、設定値データを受信すると、デバイス監視サーバ２０３ａとの間でセッションを確立し、デバイス監視サーバ２０３ａに対して設定値データを送信する。

【００５５】

（４）デバイス監視サーバ２０３ａは、設定値データを受信するとデバイスに設定値を送りつける。この手順は、デバイスごとに定まった手順で行われる。

【００５６】

（５）デバイスの設定が終了すると、デバイス監視サーバ２０３ａは、デバイスセンタサーバ２１０に対して設定終了を送信する。

【００５７】

（６）デバイスセンタサーバ２１０は、アプリケーションシステム２０５に対して設定終了通知を送信する。

【００５８】

その後、アプリケーションシステム２０５はデバイスセンタサーバ２１０との間のセッションを解放し、デバイスセンタサーバ２１０は、デバイス監視サーバ２０３ａとの間のセッションを解放する。

【００５９】

以上のようにして、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とは直接通信することで、デバイスの設定情報をデバイス４０２にダウンロードする事ができる。

【００６０】

なお、障害に関しては次のようになる。

【００６１】

（７）ＰＣ監視クライアント２０３ｄがサーバやＰＣにおいて何らかの障害を検出し、障害イベントを発行する際には、センタサーバ１１０に対して直接イベントを発行する。

【００６２】

（８）また、デバイス監視サーバ２０３ａがデバイス４０２の障害を検出した場合には、その情報をデバイスセンタサーバ２１０に送信する。

【００６３】

（９）デバイスセンタサーバ２１０は、デバイス４０２における障害の通報を受信すると、それを基に、センタサーバ１１０に対して障害発生を知らせるイベントを発行する。図４のデバイスセンタサーバ２１０には図２のイベントアダプタ２１０ａが含まれる形で記載されおり、イベントアダプタ２１０ａから図４に記載される障害系イベントが発行されることになる。

【００６４】

（１０）イベントモニタ１１０ａは、そのイベントが障害系イベントであるので、イベントコンソールにその障害情報を表示させ、イベントリストを更新する。

【００６５】

このように、障害を通知するイベントは、被管理サイトのどのデバイス系または汎用コンピュータ系で生じても、センタサーバ１１０を通ることになり、管理者は、センタサーバのイベントコンソールを監視するだけで、被管理サイトのすべてのデバイス系の情報または汎用コンピュータ系の情報を監視できる。また、イベントコンソールに表示される情報は、印刷出力されたり、サービスマンの所持する形態端末等に表示されるような処理を施されることも考えられる。印刷された情報は、被管理者宛に郵送で送られたり、サービスマンの形態端末に表示された情報はサービスマンの派遣等に利用することができる。このようにデバイス系と汎用ＰＣ・サーバ系を一元管理された情報を様々な形態で応用する場面が想定される。

【００６６】

前述の記載では、デバイス系の障害を図４中のイベントモニタ１１０ａを介してイベントコンソール１１０ｂに表示させることについて説明してきたが、本名発明の特徴として、デバイス系で発生した全ての障害情報をイベントコンソール１１０ｂに表示するわけではないことが挙げられる。すなわちデバイス機器の障害のレベルによってデバイスセンタサーバ２１０に情報を送信するか否かの判断処理を行う機能を本システムは有する。

【００６７】

例えば、複写機等におけるドアオープンエラー、デバイス機器のパワーオン・オフ機能によるリセットで回復できるようなエラーに関してはデバイス監視サーバ２０３ａはデバイスセンタサーバ２１０にエラー通知を行わない。一方、センタサーバに通知されてくる情報のうちでも、顧客先で顧客による対応がとれるエラー、例えば、デバイスの温度上昇等

の現状動作に支障の無いエラー、ジャムエラー）に関しては、サービスマンの呼び出し等を行わない。

【００６８】

これら、センタサーバへ障害を通知するか否かの判断機能データベースは監視データベース２０３ａ－１、デバイス４０２、等のデバイス側の機器のいずれかに記憶されていれば、デバイス側からセンタ側に情報を通知するか否かの判断を行うことができる。

【００６９】

また、センタサーバ１１０に通知されてきた障害情報をイベントコンソール１１０ｂに表示するか否か、または、サービスマンに連絡するか否かの判断機能データベースはセンタサーバ側のアプリケーションシステム２０５、インベントリデータベース１０９、センタサーバ１１０等の機器のいずれかに記憶されていれば、本発明の機能を達成することはできる。

【００７０】

これらの情報伝達に伴うフィルタリング機能を本システムは有することにより、拠点側－センタ側間のトラフィック量の軽減、また、センタ側で管理する管理者にとって、重大なエラー情報をより明確且つ容易に認識することが可能となる。

【００７１】

＜カウンタアップロード手順＞

カウンタ値のアップロード、すなわちデバイス情報の収集は次のようにして行われる。カウンタ値とは、複写機やプリンタにおいて印刷したページ数を示す値、デバイスの各種モードがどれほど使用されたかを示すモードカウンタ等であり、保守料金算定の基本となる値である。これをセンタシステムからの要求に応じてアップロードすることで、遠隔サイトからのカウンタ値をはじめとするデバイス情報の取り込みを可能とする。カウンタのアップロードはアプリケーションからの要求に応じて行われるために、センタシステム（管理サイト）がイニシエータとなる。

【００７２】

（１）アプリケーションシステム２０５よりセッションを確立し、デバイス情報要求をデバイスセンタサーバ２１０に対して送信する。デバイス情報要求には、拠点システムにおける対象デバイスを指定する情報等が含まれている。

【００７３】

（２）デバイスセンタサーバ２１０は、デバイス情報要求を受信すると、デバイス監視サーバ２０３ａとの間でセッションを確立し、デバイス監視サーバ２０３ａに対してデバイス情報要求を送信する。

【００７４】

（３）デバイス監視サーバ２０３ａは、デバイス情報要求を受信すると、デバイス情報を指定されたデバイスから取得する。この手順は、デバイスごとに定まった手順で行われ、デバイスごとに定まった情報、あるいは指定された情報が取得される。

【００７５】

（４）デバイス情報を取得すると、デバイス監視サーバ２０３ａは、デバイスセンタサーバ２１０に対して取得したデバイス情報を含むデバイス情報応答を送信する。

【００７６】

（５）デバイスセンタサーバ２１０は、アプリケーションシステム２０５に対してデバイス情報応答を送信する。

【００７７】

その後、アプリケーションシステム２０５はデバイスセンタサーバ２１０との間のセッションを解放し、デバイスセンタサーバ２１０は、デバイス監視サーバ２０３ａとの間のセッションを解放する。

【００７８】

以上のようにして、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とは直接通信することで、デバイス情報を取得することができる。

【００７９】
なお、障害に関しては設定値のダウンロードと同じ要領で行われる。
【００８０】
＜ログデータアップロード手順＞
ログデータのアップロードは次のようにして行われる。ログデータとは、たとえば周辺機器において発生した警告やリトライの情報などが履歴で、それらの警告が所定回数以上に達するなど、エラーに至らないまでも、何らかの異常事態が発生しつつあることが予想される場合にそれを管理サイトに自発的に送信する。したがって、ログデータのアップロードはカウンタのアップロードとは異なり、被管理サイト（拠点システム）がイニシエータとなる。
【００８１】
（１）デバイス監視サーバ２０３ａがデバイスのログを収集する。その量が所定値を越えたり、警告の発生頻度が所定の率を超えた場合には、デバイス監視サーバ２０３ａはログデータのアップロードを開始する。
【００８２】
（２）まず、デバイス監視サーバ２０３ａよりセッションを確立し、ログデータを含むログデータ処理要求をデバイスセンタサーバ２１０に対して送信する。
【００８３】
（３）デバイス監視サーバ２０３ａは、ログデータ処理要求を受信すると、デバイスセンタサーバ２１０との間でセッションを確立し、デバイスセンタサーバ２１０に対してログ処理要求を送信する。
【００８４】
（４）デバイスセンタサーバ２１０は、ログデータ処理要求を受信すると、アプリケーションシステム２０５との間にセッションを確立し、ログデータ処理要求を、ログデータを処理するアプリケーションシステム２０５に対して送信する。
【００８５】
（５）アプリケーションシステム２０５は、ログデータ処理要求を受信すると、それと共に受信したログデータを処理し、ログデータ処理応答を、デバイスセンタサーバ２１０に対して送信する。
【００８６】
（６）デバイスセンタサーバ２１０は、デバイス監視サーバ２０３ａに対してログデータ処理応答を送信する。
【００８７】
（７）デバイス監視サーバ２０３ａは、デバイスセンタサーバ２１０との間のセッションを解放し、後処理を行う。後処理においては、ログデータ処理応答が、ログデータの処理が正常に完了したことを示すものであれば、ログデータ消去などを行う。
【００８８】
その後、デバイスセンタサーバ２１０はアプリケーションシステム２０５との間のセッションを解放する。
【００８９】
以上のようにして、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とは直接通信することで、ログ情報をアップロードすることができる。
【００９０】
なお、障害に関しては設定値のダウンロードと同じ要領で行われる。
【００９１】
＜デバイスセンタサーバによる処理手順＞
次に、デバイスセンタサーバ２１０、デバイス監視サーバ２０３ａそれぞれにおける処理手順を簡単に示す。図５は、デバイスセンタサーバにおけるメッセージ受信時の処理手順を示すフローチャートである。なお、このメッセージはデバイス監視サーバからのものとは限らず、アプリケーションシステム２０５からも受信する。このメッセージのフォーマ

ットは、図８と異なるものでも良い。いずれにしても、メッセージの発信元を識別可能にできているか、あるいは、発信元に応じて異なるプロセスが実行される。本実施形態では、前者を採用する。

【００９２】

メッセージを受信すると、図５の処理が開始される。まず、受信したメッセージを解析し（ステップＳ５０１）、その発行元が判定される（ステップＳ５０２）。発行元は、アドレス等をメッセージに付加しても良いが、その内容によっても識別できる。たとえば、ログ処理要求であれば、その発行元はデバイス監視サーバであり、設定値ダウンロード要求であればアプリケーションシステム（フローチャートではバックエンドと示している）である。

【００９３】

発行元がデバイス監視サーバ２０３ａであれば、それが障害イベントであるか判定し（ステップＳ５０３）、障害イベントであれば、センタサーバ１１０へ処理可能な形式に変換してから転送する（ステップＳ５０４）。センタサーバ１１０においては障害の場所や内容、時刻などがそのメッセージに含まれたデータから読み出され、表示される（ステップＳ５０５）。障害イベントでない場合には、データをアプリケーションシステムに渡してメッセージに応じた処理をさせ、メッセージ待ちとなる。アプリケーションシステムに渡す処理には、たとえばログデータ処理要求や、収集されたデバイス情報が含まれる。

【００９４】

一方、発行元がアプリケーションシステムであれば、そのメッセージがデバイス情報の収集要求であるか判定する（ステップＳ５０６）。そうであれば、デバイス情報収集要求をデバイス監視サーバ２０３ａに対して発行し、メッセージ待ちとなる。

【００９５】

デバイス情報収集要求でなければ設定値のダウンロード要求であるかが判定される（ステップＳ５０８）。ダウンロード要求であれば、受信したダウンロード情報を取得し（ステップＳ５０９）、それをデバイス監視サーバ２０３ａに対して発呼する（ステップＳ５１０）。

【００９６】

＜デバイス監視サーバによる処理手順＞

図６は、デバイス監視サーバ２０３ａにおいて発生したイベントに対する処理手順を示すフローチャートである。

【００９７】

何らかのイベントが発生すると、発生したイベントを解析し（ステップＳ６０１）、それがデバイスからの警告であり、所定の閾値を越えていれば（ステップＳ６０２）、それまでに蓄積したログデータを取得してログデータ処理要求のメッセージを作成し（ステップＳ６０３）デバイスセンタサーバ２１０に対してログ処理要求を発行する。閾値を超えていなければログに蓄積する。

【００９８】

一方、警告でなければ本実施例ではエラーの発生であるとみなして障害イベントを示すメッセージを作成し（ステップＳ６０５）、ステップＳ６０４でデバイスセンタサーバ２１０に送信する。

【００９９】

図７は、デバイス監視サーバ２０３ａが、デバイスセンタサーバ２１０から受信したメッセージを受信する手順を示すフローチャートである。

【０１００】

まず、受信したメッセージが設定値のダウンロード要求であるか判定する（ステップＳ７０１）。ダウンロードであれば、受信した設定値データに基づく設定をデバイス監視サーバ２０３ａとデバイス間でう。（ステップＳ７０２）、拠点プラグイン２０３ｂがそのデータを削除し（ステップＳ７０３）、デバイスセンタサーバ２１０に対してダウンロードが完了した旨の応答メッセージを発行する（ステップＳ７０４）。なお、拠点プラグイン

２０３ｂはデバイス監視サーバ２０３ａに論理的に接続されていればよく、接続されていれば物理的に分かれていてもよい。

【０１０１】

ダウンロードでなければ、デバイス情報収集要求であるか判定し（ステップＳ７０６）、そうであれば指定されたデバイスから情報を収集して（ステップＳ７０７）、デバイスセンタサーバにそのデバイス情報を送信する（ステップＳ７０８）。

【０１０２】

以上の手順により、汎用コンピュータのための管理システムと、周辺機器のための管理システムとによる障害イベントを、管理サイト側においては統合された情報として一元的に管理できる。また、本発明はＰＣ・サーバ系の管理ソフトにデバイス系の管理情報を適合させるものに限定されるものではなく、その逆、即ちデバイス系の管理ソフトにＰＣ・サーバ系の管理情報を適合させるものにすることも可能である。例えば、図２中のイベントアダプタ２１０ａをセンタサーバ１１０に設けて、デバイスサーバで発生したイベントをデバイスセンタサーバ２１０に通知するようにしてもよい。

【０１０３】

また、図２に示したように、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とを接続する回線と、ＰＣ監視クライアント２０３ｄとセンタサーバ１１０とを接続する回線とを同じ回線とし、ルータ等で共用することで、回線数の節約を図ることもできる。これは回線として専用回線を使用する場合などに有効である。

【０１０４】

＜第２の遠隔サイト管理システムの構成＞

図を参照して本発明の第２の実施形態である遠隔サイト管理システムを説明する。本実施形態のシステムは、第１の実施形態のそれと比較して、管理サイトと被管理サイトとの間における論理的なチャネルの持ち方において相違する。第１の実施形態においては、通信回線を共用することは可能であるものの、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とを接続するチャネルと、ＰＣ監視クライアント２０３ｄとセンタサーバ１１０とを接続するチャネルとは、論理的には互いに独立した別個のチャネルである。デバイスセンタサーバ２１０が障害イベントの通知をデバイス監視サーバ２０３ａから受信した場合に、障害の発生を通知するイベントをセンタサーバ１１０に送信することで、イベントモニタにおける障害イベントの一元化が図れられている。

【０１０５】

これに対して本実施形態では、デバイスセンタサーバ２１０も、デバイス監視サーバ２０３ａとデバイスセンタサーバ２１０とを接続するチャネルも存在しない。デバイスセンタサーバの代わりに、デバイス情報処理モジュール９０１がセンタサーバ１１０におかれ（図では別体として示した）、センタサーバ１１０が受信したデバイス系の情報を処理している。この構成においては、市販のＰＣ監視クライアント２０３ｄとセンタサーバ１１０とを用いた場合に、その間に確立されるチャネルに、デバイス系のメッセージも流してしまう。こうすることで、第１実施例で説明したように回線を共通に使用できるメリットの他に、デバイス系の情報のために独立した通信チャネルを用意する必要がなく、デバイスセンタサーバを別途設ける必要もなくなるという効果を得ることができる。

【０１０６】

＜システム構成＞

図９は、本実施形態の遠隔サイト管理システムのソフトウエアモジュールの構成を示すブロック図である。ユーザ拠点システム（被管理サイトを指す）は、デバイス系機器（プリンタ、複写機、スキャナー、ＦＡＸ、複合機等の周辺機器）と、ＰＣ・サーバ系機器（汎用コンピュータ）が混在しているが、デバイス系機器はデバイス監視サーバ２０３ａによって、ＰＣ・サーバ系機器はＰＣ監視クライアント２０３ｄによって管理される。この点は第１の実施形態と同様である。

【０１０７】

センターシステム（管理サイトを指す）は、デバイス監視サーバ２０３ａとの間でデータ

を交換するデバイス情報処理モジュール９０１と、ＰＣ監視クライアント２０３ｄとの間でデータを交換するセンタサーバ１１０とを含む。デバイス系機器およびＰＣ・サーバ系の管理情報はインベントリデータベース１０９に蓄積される。図９では一つのデータベースとして図示されているが、論理的または物理的にデバイス系とＰＣ・サーバ系のデータベースが分かれていればよい。この情報はアプリケーションシステム２０５、センタサーバ１１０等により利用される。これも第１の実施形態と同様である。

【０１０８】

管理サイトと被管理サイトとは、ルータ２０４同士で接続された一本の回線で接続されている。このＰＣ監視クライアント２０３ｄとセンタサーバ１１０とは市販のサイト管理システムで実現できる。すべてのメッセージは、この市販の管理システムにより提供される、ＰＣ監視クライアント２０３ｄとセンタサーバ１１０とで構成されるチャネルを通して送受信される。なお、図９ではデバイス情報処理モジュール９０１が独立してあるものとして（図２のデバイスセンタサーバ２１０に相当）いるが、この機能をセンタサーバ１１０に組み込んで実現することもできる。

【０１０９】

デバイス監視サーバ２０３ａとＰＣ監視クライアント２０３ｄとは、データ形式（フォーマット）や手順（プロトコル）を必要に応じて変換するための拠点プラグインモジュール２０３ｂを介して接続されている。すなわち、デバイス監視サーバの情報をＰＣ監視クライアント２０３ａのフォーマット（またはプロトコル）に変換する機能、その逆の変換の機能を拠点プラグインモジュール２０３ｂは有している。また、センタ側でセンタサーバ１１０とデバイス処理モジュール９０１間でのデータを受け渡しを行うセンタ側のプラグイン（図２のサーバプラグインに相当）に、この拠点プラグインモジュール２０３ｂと同等の機能を持たせることも考えられる。

【０１１０】

この拠点プラグインモジュール２０３ｂは、後述するように、ＰＣ監視クライアント２０３ｄに対してデバイス監視サーバ２０３ａからのメッセージを渡して指定した宛先に送信させると共に、ＰＣ監視クライアント２０３ｄが書き込む所定のデータ領域の内容を定期的にポーリングし検索を行い、デバイス監視サーバ２０３ａ宛のメッセージがあればそれをデバイス監視サーバ２０３ａに渡す役割を有する。

【０１１１】

また、センタサーバ１１０は、受信したメッセージに応じて、そのメッセージの内容がデバイスに係る情報であればデバイス情報処理モジュールに渡して処理をさせるし、イベントの発生を知らせるメッセージであれば、イベントモニタ１１０ａにより発生したイベントをデバイス系のイベントかＰＣ・サーバ系のイベントかを識別可能な表示形態にしてイベントリストとして表示させる。デバイス系のイベントについてはデバイス情報処理モジュール９０１から発生されることになる。

【０１１２】

このように、デバイス系とＰＣ・サーバ系間のフォーマット変換機能を有するプラグインを設ける事により、市販されているＰＣ・サーバ系の管理ソフトの機能を流用することが可能となり、デバイス系の情報を拠点側と管理センタ側で送受信をすることができる。また、市販のＰＣ・サーバ系の管理ソフトでは詳細に管理できないような、デバイス固有の情報に関しても、センタ側で送信されてきたデバイス系のない様にに係るデータをＰＣ・サーバ系のフォーマットからデバイス系のフォーマットに変換してからデバイス情報処理モジュールで処理をすればよく、デバイスの情報を詳細に管理したい場合には、デバイす情報処理モジュールのみを独自に開発すればよく、開発・設計の効率を上げる効果を得ることができる。

【０１１３】

次に、拠点システム（被管理サイト）と、センタシステム（管理サイト）との間でなされるメッセージ交換の手順の例を、図１０乃至図１２を参照しつつ、（１）デバイスへの、デバイスセンタサーバ２１０からの設定値のダウンロード、（２）デバイス監視サーバ２

０３ａからデバイスセンタサーバ２１０へのログデータのアップロード、（３）デバイスセンタサーバ２１０からデバイス監視サーバ２０３ａへのカウンタデータの要求、という３つのケースで説明する。

【０１１４】

＜設定値ダウンロード手順＞

図１０は、拠点システムとセンタシステムとの間で行われる、デバイスへの設定値のダウンロードの手順を説明するためのブロック図である。設定値のダウンロードは次のようにして行われる。

【０１１５】

まずアプリケーションシステム２０５において、手作業などで、設定対象のデバイスの指定や設定値等を入力し、設定値情報ファイル１００２を作成しておく。

【０１１６】

（１）アプリケーションシステム２０５よりセンタサーバ１１０との間のセッションを確立する。

【０１１７】

（２）センタサーバ１１０において配布モジュール１００１を起動し、設定値情報ファイル１００２から配布用ファイルパッケージ１００１ａを作成する。

【０１１８】

（３）配布モジュール１００１ａは、配布用パッケージファイルをＰＣ監視クライアント２０３ｄに送信し、ワークファイルとして格納させる。

【０１１９】

（４）拠点プラグイン２０３ｂは、ＰＣ監視クライアント２０３ｄが格納するデータファイルを定期的に監視しており、ＰＣ監視クライアントによりワークファイルが作成されたことを検知すると、デバイス監視サーバに設定値の到着を通知すると共に、設定値データをデバイス監視サーバ２０３ａに渡す。デバイス監視サーバ２０３ａは、指定されたデバイスに、設定された値を設定する。

【０１２０】

（４－２）拠点プラグイン２０３ｂは、ＰＣ監視クライアント２０３ｄを介してセンタサーバに設定が終了したことを通知する。

【０１２１】

（５）センタサーバ１１０では、配布モジュール１００１により、配布用パッケージファイル１００１ａを削除させる。

【０１２２】

（６）センタサーバ１１０は、アプリケーションシステム２０５に対して設定の終了を通知する。

【０１２３】

以上のようにして、デバイス監視サーバ２０３ａに設定データを渡すことで、デバイスの設定情報をデバイスにダウンロードすることができる。

【０１２４】

なお、デバイス系で発生した障害に関しては、上記手順（４－２）と同様にして拠点プラグイン２０３ｂからＰＣ監視クライアント２０３ｄを介してセンタサーバ１１０に障害イベントとして送信する。このために、障害を通知するイベントは、センタサーバ１１０のイベントモニタ１１０ａで処理され、イベントのリストに表示される。

【０１２５】

＜カウンタアップロード手順＞

図１１は、拠点システムとセンタシステムとの間で行われる、カウントデータのアップロード、すなわちデバイス情報収集の手順を説明するためのフローチャートである。デバイス情報のアップロードは次のようにして行われる。

【０１２６】

（１）アプリケーションシステム２０５は情報要求コマンドをファイルに格納し、センタ

サーバ１１０に対して情報収集のきっかけとなるメッセージ（イベント）を発行する。
【０１２７】
（２）アプリケーションシステム２０５からのイベントをイベントモニタが解析し、配布モジュール１００１を起動して、情報要求コマンドの配布用ファイルパッケージ１００１ａを作成する。
【０１２８】
（３）センタサーバ１１０は、作成した情報要求コマンドを含む配布用パッケージをＰＣ監視クライアント２０３ｄに対して送信する。ＰＣ監視サーバ２０３ｄは受信したファイルをワークファイルとして格納する。なお、ワークファイルはＰＣ・サーバ管理システムでの汎用ファイルなるもので、配布用ファイルパッケージ１００１ａの実態に該当するものである。
【０１２９】
（４）拠点プラグイン２０３ｂは、ＰＣ監視サーバ２０３ｄがファイルを格納したことを検知すると、それを呼んでデバイス監視サーバ２０３ａに渡す。デバイス監視サーバ２０３ａは、それを受けて指定されたデバイスから、デバイス情報を収集して拠点プラグイン２０３ｄに渡す。
【０１３０】
（５）拠点プラグイン２０３ｂは、受信したデバイス情報を、所定の形式のファイル２０３ｅとして格納する。本実施例では以下に所定の形式としてＭＩＦ形式を例に説明を進めていくが、ＭＩＦ形式とは情報管理系の一般的なファイル形式を指す。
【０１３１】
（６）拠点プラグイン２０３ｂは、ワークファイルを削除する。
【０１３２】
（７）拠点プラグインは、ＭＩＦファイルを作成した旨のイベントを作成してセンタサーバ１１０に送信する。
【０１３３】
（８）センタサーバ１１０はそのイベントを受け、配布用ファイルパッケージを削除する。
【０１３４】
（９）また、センタサーバ１１０は、拠点プラグイン２０３ｂから受信したイベントが、正常な情報収集の完了を通知するものであれば、共通情報収集モジュール１１０１を起動し、拠点プラグインの作成したＭＩＦファイルを読み込ませてデバイス情報を収集させる。
【０１３５】
（１０）共通情報収集モジュール１１０１は、ＭＩＦファイル２０３ｅを読み、収集したデバイス情報を獲得する。
【０１３６】
（１１）共通情報収集モジュール１１０１は獲得したデバイス情報をインベントリデータベースに格納する。なお、インベントリデータベースは物理的または論理的にデバイス機器系とＰＣ・サーバ機器系のデータベースとをそれぞれ有しており、対象機器に応じて柔軟な処理を行うことができる。
【０１３７】
（１２）センタサーバは拠点側のＭＩＦファイル２０３ｅを削除させる。
【０１３８】
（１３）アプリケーションに完了通知を送信する。
【０１３９】
以上のようにして、デバイス監視サーバ２０３ａが収集したデバイス情報をセンタサーバ１１０に取得することができる。
【０１４０】
＜ログデータアップロード手順＞

図１２は、拠点システムからセンタシステムへのログデータのアップロード手順を説明するためのフローチャートである。ログデータのアップロードは本実施形態では次のようにして行われる。

【０１４１】

（１）デバイス監視サーバ２０３ａは、拠点プラグインに２０３ｂに対して、エラーや警告、それらの回数が閾値を超えたことを検知した旨の通知を発行する。

【０１４２】

（２）デバイス監視サーバ２０３ａは、拠点プラグインに２０３ｄに対して前述した警告のイベントデータ発行する。

【０１４３】

（３）拠点プラグイン２０３ｂは、ログデータを、ＭＩＦ形式のファイル２０３ｅとして格納する。ＭＩＦ形式とは、前述で説明したとおり、情報管理系の一般的なファイル・データ形式である。

【０１４４】

（４）拠点プラグイン２０３ｂは、ＭＩＦファイルを作成した旨のイベントを作成してセンタサーバ１１０に送信する。

【０１４５】

（５）センタサーバ１１０はそのイベントを受け、共通情報収集モジュール１２０１を起動する。

【０１４６】

（６）共通情報収集モジュール１２０１は、拠点プラグイン２０３ｂの作成したＭＩＦファイル２０３ｅを読み込ませてログファイルを読む。

【０１４７】

（７）共通情報収集モジュール１２０１は、獲得したデバイス情報をインベントリデータベース１０９に格納する。

【０１４８】

（８）センタサーバは拠点側のＭＩＦファイル２０３ｅを削除させる。

【０１４９】

（９）アプリケーションに完了通知を送信する。

【０１５０】

以上のようにして、デバイス監視サーバ２０３ａが作成したログデータファイルをセンタサーバ１１０は取得することができる。

【０１５１】

＜デバイスセンタサーバによる処理手順＞

次に、センタサーバ１１０、デバイス情報処理モジュール９０１、拠点プラグイン２０３ｂ、ＰＣ監視クライアント２０３ｄによる処理手順を簡単に示す。図１３は、センタサーバ１１０におけるイベント受信時の処理手順を示すフローチャートである。イベントを受信すると、図１３の処理が開始される。なお、以下の説明において、メッセージとイベントは厳密に区別されていない。イベントとは、イベントの発生を伝えるメッセージ、という意味で使用している。

【０１５２】

まず、受信したイベントを解析し（ステップＳ１３０１）、その発行元が判定される（ステップＳ１３０２）。発行元がＰＣ監視クライアント２０３ｄであれば、イベントモニタにより処理されて、障害イベントであればイベントリストに表示される（ステップＳ１３０３）。

【０１５３】

そのあとで、イベントがデバイス系であるか否か、すなわちそれが拠点プラグイン２０３ｂから発行されたものか否かが判定され（ステップＳ１３０４）、デバイス系であれば、イベントごとに応じてデバイス情報処理モジュールにより処理が行われる。この手順が図１４乃至図１６に示されている。デバイス系でなければ、センタサーバ１１０によりイベ

ントに応じた処理が行われる。
【０１５４】
一方、イベントの発行元がバックエンド、すなわちアプリケーションシステムであれば、そのイベントが情報収集を行わせるためのものかが判定され（ステップＳ１３０５）、そうであれば、情報収集要求を拠点プラグインモジュール２０３ｂに対して発行する（ステップＳ１３０９）。情報収集要求は、その要求を行うための配布モジュール１００１に配布用ファイルパッケージを作成し、それを配布させて行わせる。
【０１５５】
情報収集要求のイベントでなければ、ダウンロードを要求するためのイベントであるか判定する（ステップＳ１３０６）。そのイベントでもなければ、イベントに応じた処理をおこなってイベント待ちとなる。
【０１５６】
ダウンロード要求の場合には、ダウンロードするデータをバックエンドから獲得し（ステップＳ１３０７）、ダウンロードデータを拠点プラグイン２０３ｂに対して配布する（ステップＳ１３０８）。
【０１５７】
＜デバイス情報処理モジュールによる処理手順＞
図１３のステップＳ１３０４でデバイス系と判定されたイベントは、更に詳細に分析されて、（１）ダウンロード終了の通知イベント、（２）デバイス情報収集終了のイベント、（３）ログデータアップロードの要求のイベント、という３種の処理に分岐する。これらの処理は、ぞれぞれ図１４乃至図１６のフローチャートの手順となる。
【０１５８】
（ダウンロード終了）
図１４は、デバイス情報処理モジュール９０１による、ダウンロード終了イベントに対する処理手順を示すフローチャートである。ダウンロードの終了が通知されると、まず配布ファイルパッケージ１００１ａを削除し（ステップＳ１４０１）、ダウンロードが終了したことをバックエンドに通知する（ステップＳ１４０２）。
【０１５９】
（デバイス情報の取得）
図１５は、デバイス情報処理モジュール９０１による、デバイス情報取得（カウンタアップロード）の通知に対する処理手順を示すフローチャートである。
【０１６０】
まず、情報収集要求のために作成した配布用ファイルパッケージ１００１ａを削除する（ステップＳ１５０１）。次に、データの取得が正常に行われていれば、情報収集モジュール１１１０１を起動し（ステップＳ１５０３）、デバイス監視サーバ２０３ａに対してデバイス情報の格納されたＭＩＦファイルを要求し、それに対する応答であるＭＩＦファイルを受信する（ステップＳ１５０４）。
【０１６１】
そして受信したファイルをインベントリデータベース１０９に格納し（ステップＳ１５０５）、デバイス監視サーバ２０３ａに対してＭＩＦファイルの削除を要求する（ステップＳ１５０６）。最後にバックエンドに対してデバイス情報の収集が終了したことを通知する（ステップＳ１５０７）。
【０１６２】
一方、ステップ１５０２で正常でないと判定された場合には、その旨をバックエンドに対して通知する（ステップＳ１５０８）。
【０１６３】
以上のようにして、ＭＩＦファイルとして作成されたデバイス情報をデバイス監視サーバ２０３ａから取得する。
【０１６４】
（ログデータアップロード）

図１６は、デバイス情報処理モジュール９０１による、ログデータアップロードの通知に対する処理手順を示すフローチャートである。

【０１６５】

ログデータをアップロードする通知を受けると、共通情報収集モジュール１２０１を起動し（ステップＳ１６０１）、ログデータを含むＭＩＦファイルの送付要求をデバイス監視モジュール２０３ａに発行する（ステップＳ１６０２）。

【０１６６】

その要求への応答であるＭＩＦファイルを受信し（ステップＳ１６０３）、それをインベントリデータベース１０９へ格納する（ステップＳ１６０４）。ＭＩＦファイルの削除要求をデバイス監視サーバ２０３ａに対して発行し（ステップＳ１６０５）、それらの処理が終了すると処理終了の旨をバックエンドに通知する（ステップＳ１６０６）。

【０１６７】

＜デバイス監視サーバによる処理手順＞

図１７は、拠点プラグイン２０３ｂにおいて、プラグインに対して発行されたメッセージあるいはイベントに対する処理手順を示すフローチャートである。なお、センタサーバ１１０から拠点プラグイン２０３ｂにあって発行されたメッセージは、監視クライアント２０３ｄにより所定の領域に格納されるために、拠点プラグイン２０３ｂはそれを常時あるいは一定時間おきに監視し続けている。

【０１６８】

メッセージがあると、それがデバイス監視サーバ２０３ａからのメッセージであるか判定し（ステップＳ１７０１）、そうであれば、メッセージを解析して（ステップＳ１７０２）、警告や閾値越えであれば、ログデータをＭＩＦファイルとして書き出し、ＰＣ監視クライアント２０３ｄを介して、ログファイルのアップロードを行う旨、センタサーバ１１０にあててイベントを発行する（ステップＳ１７０５）。

【０１６９】

警告や閾値越えではない場合には、エラーであるか判定し（ステップＳ１７０６）、エラーであれば障害イベントを示すメッセージを作成してステップＳ１７０５へ分岐する。（ステップＳ１７０７）。

【０１７０】

デバイス監視サーバ２０３ａからのメッセージでない場合には、センタサーバ１１０からのメッセージであると判定して、ＰＣ監視クライアント２０３ｄにより書き出された所定の領域を読み出し（ステップＳ１７０８）、そのデータを解析して内容に応じた処理を遂行する。この解析した内容に応じた処理の詳細が図１８に示されている。

【０１７１】

図１８は、拠点プラグイン２０３ｂによる、センタサーバ１１０から受信したメッセ維持に応じた処理の手順を示すフローチャートである。

【０１７２】

まず、それがダウンロードデータであるか判定し（ステップＳ１８０１）、ダウンロードデータであれば、デバイス監視サーバ２０３ａに対してダウンロードデータの受信を通知し（ステップＳ１８０２）そのデータを渡す（ステップＳ１８０３）。そして、渡し終えたデータを削除し（ステップＳ１８０４）、センタサーバにあててダウンロード完了イベントを発行する（ステップＳ１８０５）。

【０１７３】

ダウンロードデータでない場合には、デバイス情報の収集要求であるか判定し（ステップＳ１８０６）、そうであれば、デバイス監視サーバ２０３ａに対してデバイｓじょうほうの収集を要求する（ステップＳ１８０７）。

【０１７４】

それに応えてデバイス監視サーバ２０３ａからデバイス情報を受信すると（ステップＳ１８０８）、それをＭＩＦファイルとして格納し（ステップＳ１８０９）、デバイス情報を収集した旨のメッセージをセンタサーバ１１０にあてて発行する。

【０１７５】
＜ＰＣ監視クライアントによる処理手順＞
図１９は、ＰＣ監視クライアントがメッセージを受信した場合の処理手順を示すフローチャートである。
【０１７６】
図１９において、受信データの宛先がどこであるか判定し（ステップＳ１９０１）、ＰＣ・サーバといった汎用コンピュータにあてたデータであれば、指定されたプロセスへとそのデータを渡し（ステップＳ１９０２）、拠点プラグインであれば、前述した所定の領域へとデータを書き込む。
【０１７７】
以上のように、本実施形態のシステムでは、汎用コンピュータ用の監視システムを用いて、監視対象の汎用コンピュータと同じ被管理サイトに設置された周辺機器をも管理することができる。これにより、管理サイトにおいては、汎用コンピュータと周辺機器とを同様な方法で一元的に監視することができる。さらに、周辺機器に関する情報の収集や、パラメータの設定等を、その監視システムを通して管理サイト側から行える。また、被管理サイト側から、ログを管理サイトに対して送信することができる。
【０１７８】
さらに、汎用コンピュータ用の監視システムに対して、周辺機器を管理するために付加するモジュールは、すべてソフトウエア的に実現できるために、そのためのハードウエアを必要とせず、設置面積や機器の費用、維持作業等、ハードウエア的な規模の増大を防止できる。
【０１７９】
また、本発明は汎用コンピュータ（ＰＣ・サーバ系）の管理ソフトにデバイス系の管理情報を適合させるものに限定されるものではなく、その逆、即ち周辺機器（デバイス系）の管理ソフトにＰＣ・サーバ系の管理情報を適合させるものにすることも可能である。例えば、図９中のデバイス系２０１とＰＣ・サーバ系２０２とを、デバイス監視サーバ２０３ａとＰＣ監視クライアントモジュール２０３ｄとを、それぞれ入れ替え、ＭＩＦファイル２０３ｅをデバイス固有のファイル形式にし、拠点プラグイン２０３ｂにはＰＣ・サーバ系のフォーマット形式をデバイス系のフォーマット形式に変換させる機能を持たせ、また、センタサーバにデバイス系の処理をさせ、デバイス処理モジュール９０１にＰＣ・サーバ系の情報を処理させデバイスセンタにイベントを発行させるなどの形態が考えられる。
【０１８０】
＜サービス作業依頼＞
上記で説明した第１の遠隔サイト管理システム或いは第２の遠隔サイト管理システムにおいて、顧客先のオフィスで機器に障害が発生したときに、センタシステムが、その旨を通知を受け、それに対処する処理を説明する。特に、発生した障害が顧客によって対応できない場合に、作業依頼書を作成し、サービス会社へメンテナンスサービスを依頼する処理について説明する。
【０１８１】
図２０は、障害発生の通知を受けて、メンテナンスサービスを遂行するために、管理サイト（センタシステム）で使用されるアプリケーションシステムが処理する内容を示すフローチャートである。
【０１８２】
まず、被管理サイトのＰＣ・サーバ系の機器やデバイス系の機器において障害発生すると、障害イベントが、デバイス監視サーバやＰＣ監視クライアントからデバイスセンタサーバやセンタサーバに通知される。そして、更に、アプリケーションシステムは、その障害イベントを受ける（ステップＳ２００１）。図２１は、障害イベントのデータ構造を示す図である。障害イベントのデータには、障害が発生した機器の機番（シリアル番号）、障害が発生した発生日時、障害の内容を示す障害コード、障害が発生した機器の機器区分を示すＰＣ／デバイス区分（ＰＣ系であるか、デバイス系であるか）が含まれる。

【０１８３】
すると、障害に含まれている、機番（或いはシリアル番号）、発生日時、障害コード、ＰＣ／デバイス区分を取得する（ステップＳ２００２）。そして、必要に応じて、図２１や図２２のような表示画面を表示部に表示する。
【０１８４】
図２２は、障害リストを示す表示画面である。発生した障害ごとに、その障害が発生した日時、その障害が発生した機器のＰＣ／デバイス区分（ＰＣ系であるか、デバイス系であるか）、その障害の内容を示す障害コード、その障害が発生した機器の機番（或いはシリアル番号）をリスト表示している。
【０１８５】
図２３は、顧客の機器ごとに発生した障害を示す表示画面である。まず、左上には、顧客の情報としてユーザ情報が表示される。また、右上には、対象となる機器に関する機器情報が表示される。そして、下には、その顧客のオフィスに設置されたその機器において発生した障害の履歴が表示される。履歴情報には、発生した障害ごとに、その障害が発生した日時、その障害の内容を示す障害コード、その障害の種別、その障害が発生した機器における箇所（位置）、その障害に関する備考が表示される。
【０１８６】
つぎに、障害コードとＰＣ／デバイス区分とに基づいて、その障害に対応すべき対応者を判定する。判定する際には、図２４のテーブルを用いる。なお、図２４のテーブルは、図２のインベントリデータベース１０９に格納されている。
【０１８７】
図２４は、障害コードマスタテーブルを示す図である。このテーブルには、障害のタイプ別に、その障害の障害コード、その障害が発生した機器のＰＣ／デバイス区分、その障害に対応すべき対応者区分（顧客であるか、サービスマンであるか）、その招待に対する対応方法が格納されている。
【０１８８】
従って、ステップＳ２００３では、障害コードとＰＣ／デバイス区分を検索キーにして、その障害に対する対応者を割り出す。対応者が「顧客」になっている場合にはステップＳ２００４に進み、対応者が「サービス」になっている場合には、ステップＳ２００６に進む。
【０１８９】
ステップＳ２００４では、障害イベントに含まれていた機番（シリアル番号）から顧客情報を所得する。顧客情報を所得する際には、まず、図２５のテーブルを用いて、機番（シリアル番号）に対応する顧客コード、顧客サブコードを割り出す。図２５は、機番（シリアル番号）マスタテーブルを示す図である。ここには、機器ごとに、その機器の機番（シリアル番号）、その機器のメーカ名、その機器を所有する顧客の顧客コード及び顧客サブコード、その機器の設置場所、その機器のメンテナンスサービスを行なっているサービス会社コードが格納されている。
【０１９０】
そして、障害コードと顧客サブコードが割り出されると、つぎに、図２６のテーブルを用いて、顧客コードと顧客サブコードとに対応する顧客情報を引き出す。図２６は、顧客マスタテーブルを示す図である。ここには、顧客ごとに、その顧客の顧客コード、その顧客の顧客サブコード、その顧客の会社名、その顧客の部署名、その顧客の住所、その顧客の電話番号、その顧客のＦＡＸ番号、その顧客の電子メールアドレス、その顧客の担当者、その顧客の契約レベル、その顧客のＰＣ系機器のメンテナンスサービスを行なうサービス会社コード、その顧客のデバイス系機器のメンテナンスサービスを行なうサービス会社コードが格納されている。なお、顧客コードと顧客サブコードとは、同じ会社の違う部署を区別するために使われ、その場合には、顧客コードは会社を示し、顧客サブコードは部署を示す。
【０１９１】

最後に、先ほどの図２４の障害コードマスタテーブルを用いて、障害コードに対応する対処方法を引き出す。そして、図２７のような表示画面をディスプレイに表示する（ステップＳ２００５）。図２７は、対応方法表示画面を示す図である。この画面には、顧客のユーザ情報、障害が発生した機器の機器情報、発生した障害に対する対処方法が表示されている。従って、センタシステムのオペレータが、この画面を見ながら、顧客先に電話をかけ、機器に障害が発生していること、その障害の対処方法を伝える。

【０１９２】

一方、ステップＳ２００６以降では、作業依頼を作成する処理に進む。そのためにまず、トラブルチケットＩＤ（トラブルＩＤとも言う）を発行する（ステップＳ２００６）。トラブルチケットＩＤとは、作業依頼を識別するＩＤであり、作業以来ごとに発行される。そして、新しいトラブルチケットＩＤが発行されるたびに、図２８のようなテーブルに登録され、その作業依頼の依頼内容や作業経過を管理するために使用される。なお、トラブルチケットＩＤは、一例としては、“日付＋連番”で付けられる。

【０１９３】

図２８は、トラブルチケットテーブルを示す図である。ここでは、作業依頼ごとに、その作業依頼のトラブルチケットＩＤ、その作業依頼の状態（経過状況）、その作業依頼の発生日時、その作業依頼に対する対応日時（作業日時）、その作業依頼の顧客コード及び顧客サブコード、その作業依頼の機器の機番（シリアル番号）、その作業依頼に対する作業を実施する実施サービス会社のサービス会社コード、その作業依頼に対する作業の実施者名、その作業依頼における障害原因、その作業依頼に対する対処内容が格納されている。

【０１９４】

つぎに、作業依頼書を作成する（ステップＳ２００７）。作業依頼書を作成する処理は、後に説明する。作業依頼書を作成した後は、それを電子メールでサービス会社に送付する（ステップＳ２００８）。このとき、電子メールの内容そのものが作業依頼書になっていてもいいし、作業依頼書を示すファイルが電子メールに添付されていてもよい。

【０１９５】

その後、サービス会社が、サービスを行なって、作業報告書を送付してくるのを待って、作業報告書を電子メールで受信する（ステップＳ２００８）。このときも、電子メールの内容そのものが作業報告書になっていてもいいし、作業報告書を示すファイルが電子メールに添付されていてもよい。

【０１９６】

いずれにしても、電子メールの件名（Ｓｕｂｊｅｃｔ）欄には、この作業依頼に対するトラブルチケットＩＤが記載されているので、そのトラブルチケットＩＤを認識する（ステップＳ２００９）。そして、図２８のトラブルチケットテーブルにおいて、認識したトラブルチケットＩＤに対応する状態を「対応済み」に変更する。また、作業報告書の原因、対処の欄に記載されているメッセージ（テキストデータ）を、トラブルチケットテーブルの原因、対処の欄に格納する。

【０１９７】

＜作業依頼書作成・送付＞

図２９は、図２０のステップＳ２００７の、作業依頼書を作成・送付する処理を示すフローチャートである。まず、作業依頼書兼作業報告書のテンプレートファイルを読み出す（ステップＳ２９０１）。この実施例では、作業依頼書と作業報告書を一枚のシートにまとめることとしたが、別々のシートで実装されてもよい。

【０１９８】

図３０は、作業依頼書兼作業報告書のテンプレートファイルを示す図である。このテンプレートファイルには、トラブルチケットＩＤ（トラブルＩＤ）、障害の発生時刻、顧客のユーザ情報、故障が発生した機器の機器情報、障害コード、障害に対する対処内容、原因、対処が埋め込まれるようになっている。

【０１９９】

従って、図２０のステップＳ２００６で発行したトラブルチケットＩＤを埋め込む（ステ

ップＳ２９０２）。つぎに、図２０のＳ２００２で得た発行日時を埋め込む（ステップＳ２９０３）。つぎに、図２０のＳ２００４と同様にして顧客情報（ユーザ情報）を引き出し、それを埋め込む（ステップＳ２９０４）。つぎに、図２０のＳ２００４と同様にして機器情報を引き出し、それを埋め込む（ステップＳ２９０５）。つぎに、図２０のステップＳ２００５同様にして対処内容を引き出し、ステップＳ２００２で得た障害コードと対処内容を埋め込む（ステップＳ２９０６）。

【０２００】

つぎに、図２６を用いて得た顧客情報に含まれる契約レベルがいずれかを判断する（ステップＳ２９０７）。レベル１の場合には、緊急に対処すべく、対応期限を２時間後に設定し、それを埋め込む（ステップＳ２９０８）。レベル２の場合には、対応期限を４時間後に設定し、それを埋め込む（ステップＳ２９０９）。レベル４の場合には、対応期限を翌日に設定し、それを埋め込む（ステップＳ２９１０）。

【０２０１】

つぎに、図３１のテーブルを用いて、サービス会社の電子メールアドレス（Ｅｍａｉｌアドレス）を引き出す（ステップＳ２９１１）。そのためにまず、サービス会社コードを特定する。図２６の顧客マスターテーブルを用いて、図２０のＳ２００２で得たＰＣ／デバイス区分が「ＰＣ」の場合には、ＰＣ系サービス会社コードを読み出し、ＰＣ／デバイス区分が「デバイス」の場合には、デバイス系サービス会社コードを読み出す。そして、図３１のテーブルを用いて、そのサービス会社コードに対応する会社の電子メールアドレスを引き出す。

【０２０２】

図３１は、サービス会社マスターテーブルを示す図である。ここには、サービス会社ごとに、その会社のサービス会社コード、その会社のサービス区分、その会社の会社名、その会社の部署名、その会社の住所、その会社の電話番号、その会社のＦＡＸ番号、その会社のＥｍａｉｌアドレス、その会社の担当者が格納されている。なお、この実施例では、各会社の部署ごとに異なるサービス会社コードを割り当てている。

【０２０３】

最後に、電子メールの件名にトラブルチェックＩＤを記入し、情報が埋められた作業依頼書兼作業報告書のテンプレートファイルを電子メールに添付して、ステップＳ２９１１で得た電子メールアドレス宛てに電子メールを送付する（ステップＳ２９１２）。

【０２０４】

＜作業報告書作成・送付＞

一方、サービス会社に設置されているコンピュータは、作業依頼書付の電子メールを受信する（ステップＳ２０５０）。そして、添付されている作業依頼書兼作業報告書の内容をディスプレイに表示する。すると、サービス会社のサービスマンが、その作業依頼書の中身を見て、顧客先に向い、作業を行なう。

【０２０５】

つぎに、サービス会社のコンピュータは、作業報告書の作成・送付の処理を行なう。図３２は、作業報告書作成・送付の処理を示すフローチャートである。まず、図２０のＳ２０５０で受信した作業依頼書兼作業報告書のファイルを読み出す（ステップＳ３２０１）。そして、キーボードから入力された原因に関するメッセージ、対処に関するメッセージ、担当者を作業依頼書兼作業報告書のファイルに埋め込む（ステップＳ３２０２）。そして、電子メールの件名にこの作業依頼に対するトラブルチケットＩＤを記載し、作成した作業依頼書兼作業報告書のファイルを電子メールに添付して、電子メールを送付する。

【０２０６】

＜稼動報告書作成＞

もうひとつ、遠隔サイトシステムのもう一つの機能として、稼動報告の処理を説明する。図３５は、稼動報告書のテンプレートファイルを示す図である。ここには、当月使用枚数、用途別使用枚数、用紙別使用枚数率、障害履歴などが埋め込まれるようになっている。

【０２０７】

図３３は、顧客に対して機器の稼動報告を行なうために、管理サイト（センタシステム）で使用されるアプリケーションシステムが処理する内容を示すフローチャートである。

【０２０８】

まず、月次に、所定の機器のカウンタ情報を取得要求するコマンドを、被管理サイトのデバイス監視サーバに送信する（ステップＳ３３０１）。そして、カウンタ情報を受信し、図３４に示すテーブルに格納する。図３４は、カウンタテーブルを示す図である。ここでは、機器の月別の稼動情報、具体的には、機器の機番（シリアル番号）、どの年月の稼動情報であるか、その月時点でのカウンタ値、両面の印刷枚数、多重の印刷枚数、２ｉｎ１の印刷枚数、４ｉｎ１の印刷枚数、ＦＡＸ出力枚数、ホストコンピュータからの印刷データのプリント枚数、スキャン送信数、電子メール送信数、あと、コピーやプリントで使用された用紙の用紙サイズごとの枚数などが格納されている。そして、カウンタ情報には、それぞれの値が含まれている。

【０２０９】

つぎに、当月時点でのカウンタ値から先月時点でのカウンタ値を引き算し、当月だけの使用枚数を算出し、それを稼動報告書用のテンプレートファイルに埋め込む。次に、用途別の印刷枚数をそれぞれ埋め込む（ステップＳ３３０４）。つぎに、用紙別の印刷枚数を使用枚数で割った％を用紙別の用紙枚数率として、テンプレートファイルに埋め込む（ステップＳ３３０５）。

【０２１０】

つぎに、図２８のトラブルチケットテーブルにおいて、顧客コード、顧客サブコード、発生日時＝当月をキーにして、それに該当するトラブルチケットＩＤを引き出し、そのトラブルチケットＩＤに対応する情報を障害履歴に埋め込む（ステップＳ３３０６）。

【０２１１】

そして、そのトラブルチケットＩＤの中で、機番が同一のトラブルチケットＩＤが２こ以上あるかを判定する（ステップＳ３３１０）。また、作業依頼の状態が「未対応」になっているトラブルチケットＩＤがあるかを判定する（ステップＳ３３０８）。また、障害があるかないかを判定する（ステップＳ３３０９）。

【０２１２】

その結果に従って、ステップＳ３３１０では、「故障の頻度が高くなっています。しばらく観察が必要です」の欄に、障害が２回以上発生している機番、或いは、「未対応」になっているトラブルチケットＩＤの機番を埋め込む。また、ステップＳ３３１１では、「全く問題ありません。快適にお使いいただいています」の欄に、機番を埋め込む。ステップＳ３３１２では、「障害がありましたが、対処済みなので問題ありません」の欄に機番を埋め込む。

【０２１３】

そして、現在の日付をテンプレートファイルに埋め込む（ステップＳ３３１３）。最後に、テンプレートファイルをＨＴＭＬ形式で保存し、顧客に送付する（ステップＳ３３１４）。ステップＳ３３１４では、ＨＴＭＬ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式の稼動報告書のファイルを電子メールに添付して送ってもよいし、また、このＨＴＭＬ形式の稼動報告書ファイルのＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｉｏｎ）を電子メールで知らせ、顧客がＷＷＷブラウザで閲覧するときに稼動報告書ファイルを送ってもよい。

【０２１４】

＜その他の実施の形態＞

なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。

【０２１５】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現

することになり、そのプログラムコードに記憶した記憶媒体は本発明を構成することになる。

【０２１６】

また、デバイス情報データは、画像処理装置及び画像データ展開装置に内蔵されているＨＤＤ、外部接続されている記憶媒体、画像データ展開装置からアクセス可能なサーバ等に保持されていても構わない。さらに、デバイス情報データはユーザが任意に設定したものを使用することが可能であっても構わない。

【０２１７】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【０２１８】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが、実際の処理の一部または全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれる。

【０２１９】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【０２２０】

本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明した（図５乃至図７、図１３乃至図１９、図２０、図２９、図３２、）フローチャートに対応するプログラムコードが格納されることになる。

【０２２１】

【発明の効果】

本発明は、管理サイトが、オフィスにおけるＰＣ・サーバ系の機器とデバイス系の機器との双方を一元的に管理できる。

【０２２２】

特に、管理サイトが、オフィスのＰＣ・サーバ系の機器とデバイス系の機器との障害情報及び予兆情報を自動的に受信し、顧客になにも意識させることなく、メンテナンスサービスを提供し、更に、実際にメンテナンスサービスを行なうサービス会社への依頼書の送付処理、サービス会社からの作業報告書の受信処理を一本化することができる。それにより、顧客は、各サービス会社と個別に契約することなく、１つの管理サイトと契約するだけで様々な機器のメンテナンスサービスを受けることができる。

【０２２３】

また、カウンタ情報と障害履歴を用いて、オフィス環境での機器の稼動報告書を自動的に顧客に提供することができる。

【図面の簡単な説明】

【図１】被管理サイトと管理サイトの構成を示すブロック図である。

【図２】本遠隔サイト管理システムのソフトウエアモジュールの構成を示すブロック図である。

【図３】各ＰＣ及びサーバであるコンピュータの構成を示すブロック図である。

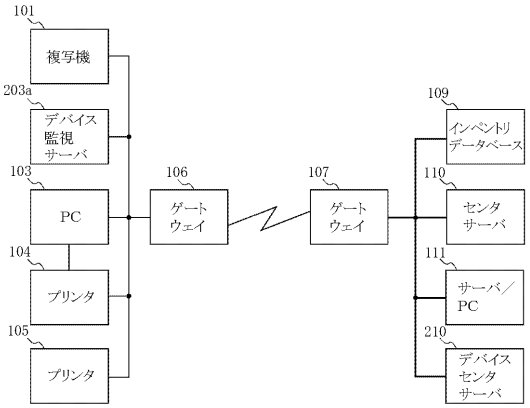
【図４】拠点システムとセンタシステムとの間で行われる、データの交換の手順を説明するためのブロック図である。

【図５】デバイスセンタサーバにおけるメッセージ受信時の処理手順を示すフローチャートである。

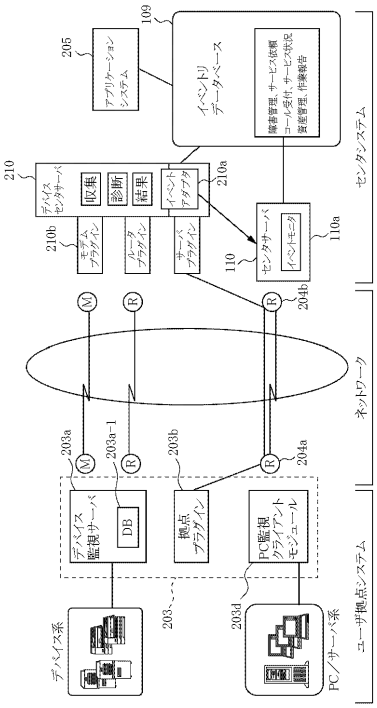
【図６】デバイス監視サーバ２０３ａにおいて発生したイベントに対する処理手順を示す

フローチャートである。
【図７】デバイス監視サーバ２０３ａが、デバイスセンタサーバ２１０から受信したメッセージを受信する手順を示すフローチャートである。
【図８】デバイスセンタサーバ２１０とデバイス監視サーバ２０３ａとの間で交換されるメッセージフォーマットの一例を示す図である。
【図９】本実施形態の遠隔サイト管理システムのソフトウエアモジュールの構成を示すブロック図である。
【図１０】拠点システムとセンタシステムとの間で行われる、デバイスへの設定値のダウンロードの手順を説明するためのフローチャートである。
【図１１】拠点システムとセンタシステムとの間で行われる、カウントデータのアップロード、すなわちデバイス情報収集の手順を説明するためのフローチャートである。
【図１２】拠点システムからセンタシステムへのログデータのアップロード手順を説明するためのフローチャートである。
【図１３】センタサーバ１１０におけるイベント受信時の処理手順を示すフローチャートである。
【図１４】デバイス情報処理モジュール９０１による、ダウンロード終了イベントに対する処理手順を示すフローチャートである。
【図１５】デバイス情報処理モジュール９０１による、デバイス情報取得（カウンタアップロード）の通知に対する処理手順を示すフローチャートである。
【図１６】デバイス情報処理モジュール９０１による、ログデータアップロードの通知に対する処理手順を示すフローチャートである。
【図１７】拠点プラグイン２０３ｂにおいて、プラグインに対して発行されたメッセージあるいはイベントに対する処理手順を示すフローチャートである。
【図１８】拠点プラグイン２０３ｂによる、センタサーバ１１０１から受信したメッセ維持に応じた処理の手順を示すフローチャートである。
【図１９】ＰＣ監視クライアントがメッセージを受信した場合の処理手順を示すフローチャートである。
【図２０】管理サイト（センタシステム）で使用されるアプリケーションシステムが処理する内容を示すフローチャートである。
【図２１】障害イベントのデータ構造を示す図である。
【図２２】障害リストを示す表示画面である。
【図２３】顧客の機器ごとに発生した障害を示す表示画面である。
【図２４】障害コードマスタテーブルを示す図である。
【図２５】機番（シリアル番号）マスタテーブルを示す図である。
【図２６】顧客マスタテーブルを示す図である。
【図２７】対応方法表示画面を示す図である。
【図２８】トラブルチケットテーブルを示す図である。
【図２９】作業依頼書を作成・送付する処理を示すフローチャートである。
【図３０】作業依頼書兼作業報告書のテンプレートファイルを示す図である。
【図３１】サービス会社マスターテーブルを示す図である。
【図３２】作業報告書作成・送付の処理を示すフローチャートである。
【図３３】管理サイト（センタシステム）で使用されるアプリケーションシステムが処理する内容を示すフローチャートである。
【図３４】カウンタテーブルを示す図である。
【図３５】稼動報告書のテンプレートファイルを示す図である。

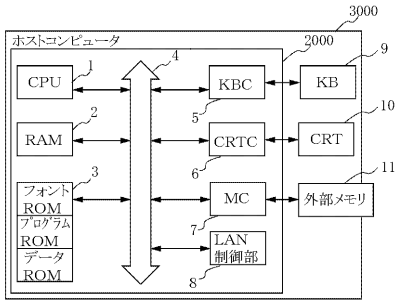
【図１】


101
複写機
203a
デバイス
監視
サーバ
103
PC
104
プリンタ
105
プリンタ
106
ゲート
ウェイ
107
ゲート
ウェイ
109
インベントリ
データベース
110
センタ
サーバ
111
サーバ／
PC
210
デバイス
センタ
サーバ

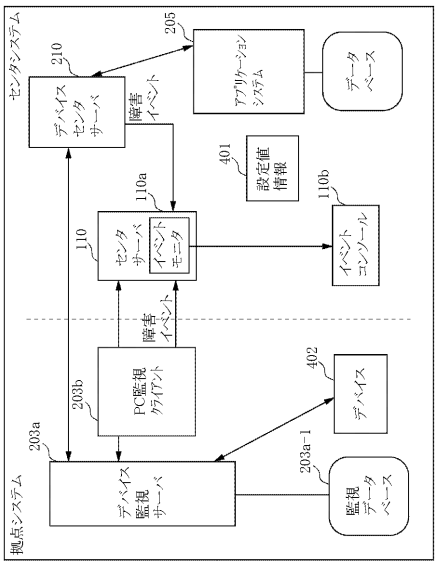
【図２】


センタシステム
ネットワーク
ユーザ拠点システム
PC／サーバ系
デバイス系
109
205
アプリケーション
システム
インベントリ
データベース
障害管理：サービス依頼
コール受付：サービス状況
変更管理：作業報告
210
デバイス
センタサーバ
収集
診断
結果
イベント
アダプタ
210a
210b
モデム
プラグイン
ルータ
プラグイン
サーバ
プラグイン
110
センタサーバ
イベントモニタ
110a
204b
203a
203a−1
203b
204a
デバイス
監視サーバ
DB
拠点
プラグイン
PC監視
クライアント
モジュール
203
203d

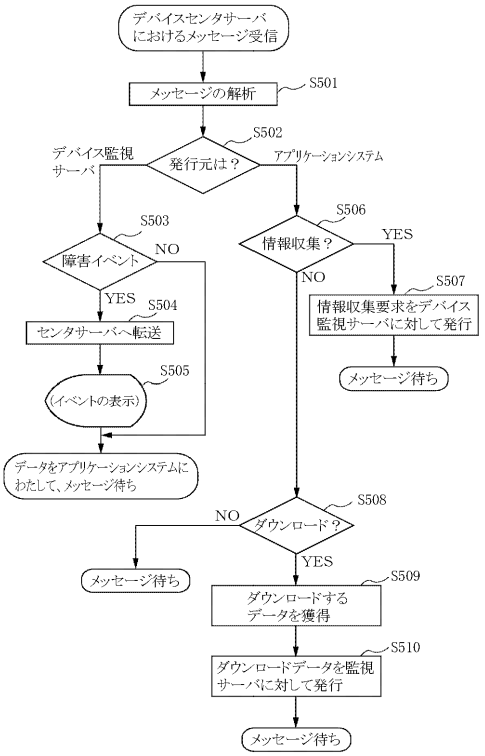
【図３】


3000
ホストコンピュータ
2000
CPU
1
RAM
2
フォント
ROM
プログラム
ROM
データ
ROM
3
4
KBC
5
CRTC
6
MC
7
LAN
制御部
8
KB
9
CRT
10
外部メモリ
11

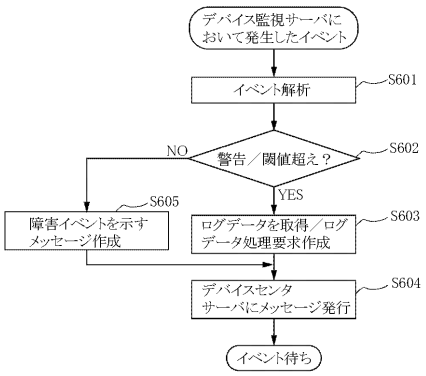
【図４】


センタシステム
拠点システム
205
アプリケーション
システム
データ
ベース
210
デバイス
センタ
サーバ
障害
イベント
401
設定値
情報
110a
110b
110
センタ
サーバ
イベント
モニタ
イベント
コンソール
障害
イベント
402
デバイス
203b
PC監視
クライアント
203a
203a−1
デバイス
監視
サーバ
監視
データ
ベース

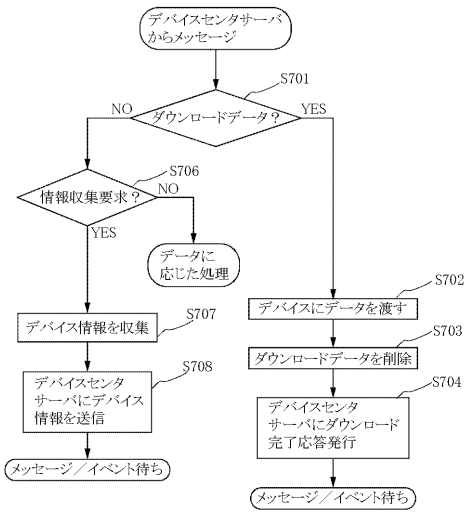
【図５】



【図６】



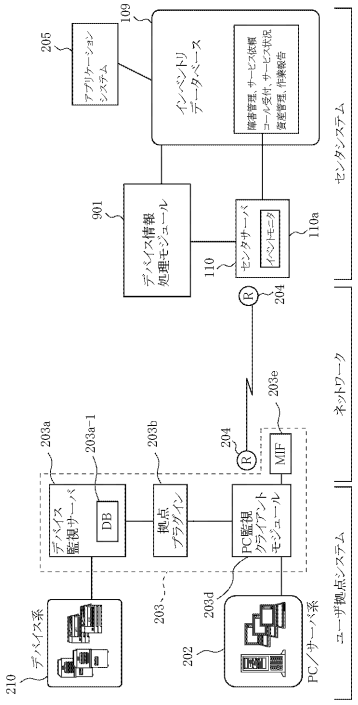
【図７】



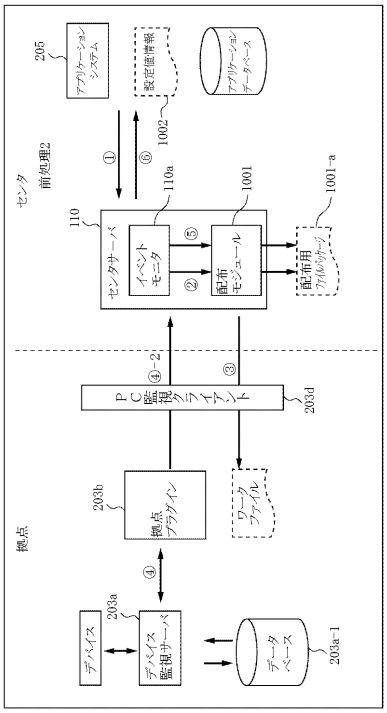
【図８】

フィールド	長さ(Byte)	用途
タグ		
フラグ	1	各種情報をビットで表わす。ビットの内容は以下のとおりである xxx..... :通信手段を示す B'100'＝TCP／IP B'010'＝ダイヤルアップ B'001'＝Eメール ....x　データが連続しているかを表わす B'0'＝単純データまたは最終データ B'1'＝連続データあり 上記以外のビットは予備とする
データ種別	1	データの種類を表わす X'01':認証要求データ X'02':パラメータ設定要求データ X'04':デバイス情報取得要求データ X'08':イベント情報通知データ X'10':応答データ X'80':切断要求データ
ジョブID	1	シーケンスを区別する セッション中、ジョブIDは同一である必要がある X'00':パラメータ設定 X'01':デバイス情報取得 X'02':イベント情報通知
リターン値	1	データ種別が応答データ(X'10')の場合はリターン値を表わす。データ種別が切断要求データ(X'80')の場合は切断理由を表わす。データ種別が応答データ(X'10')、切断要求データ(X'80')以外の場合はX'00'をセットする
データ長	4	データ長の長さをバイト数で示す(Network Byte Order)
データ	可変長	データ

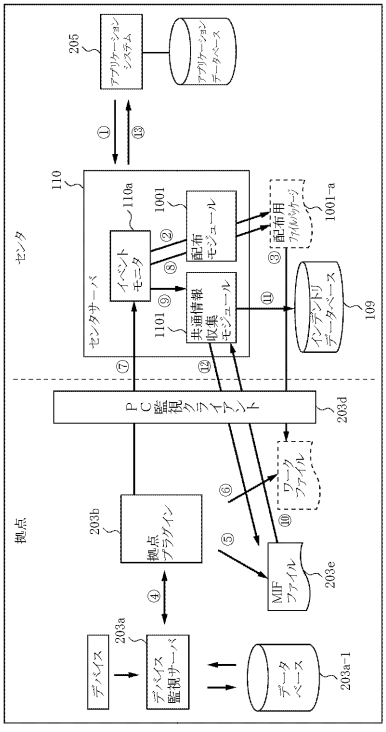
【図９】



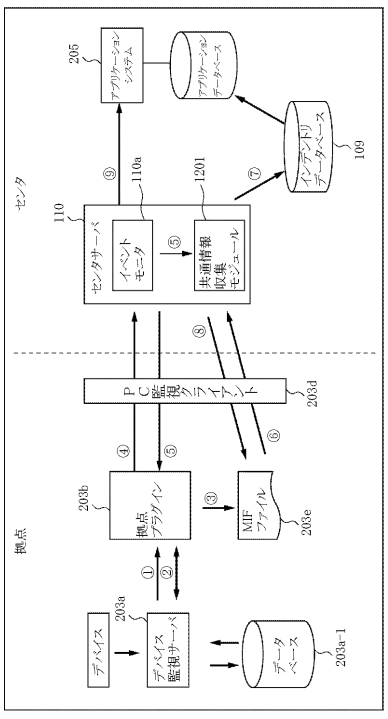
【図１０】



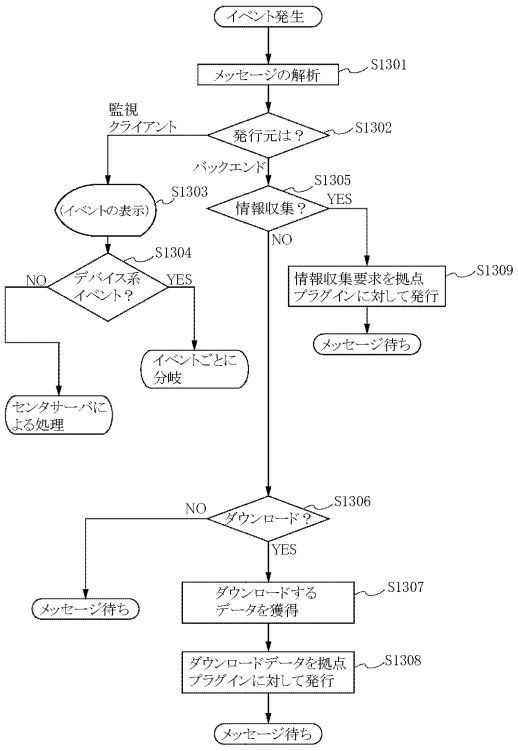
【図１１】



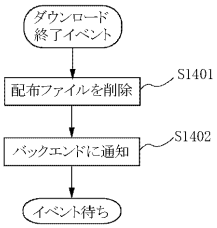
【図１２】



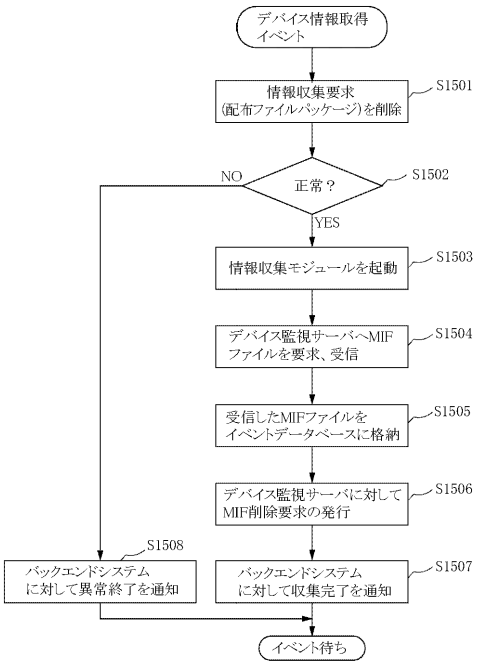
【図１３】



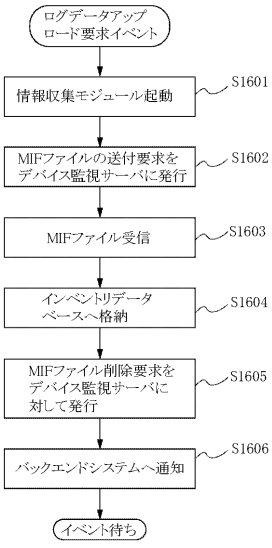
【図１４】



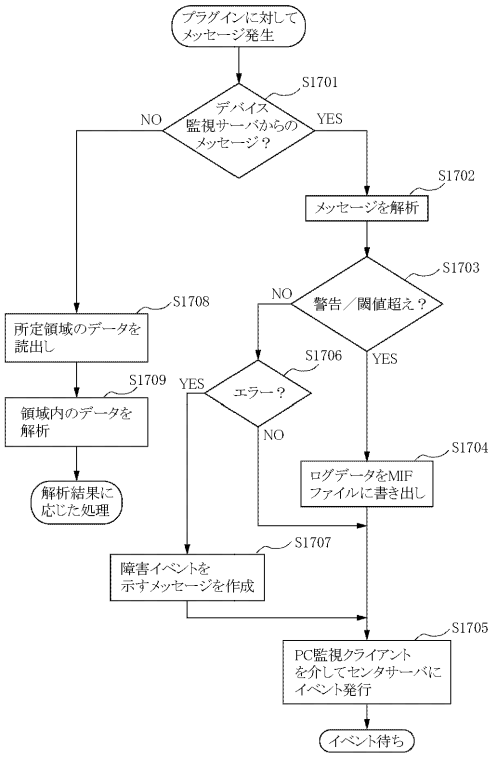
【図１５】



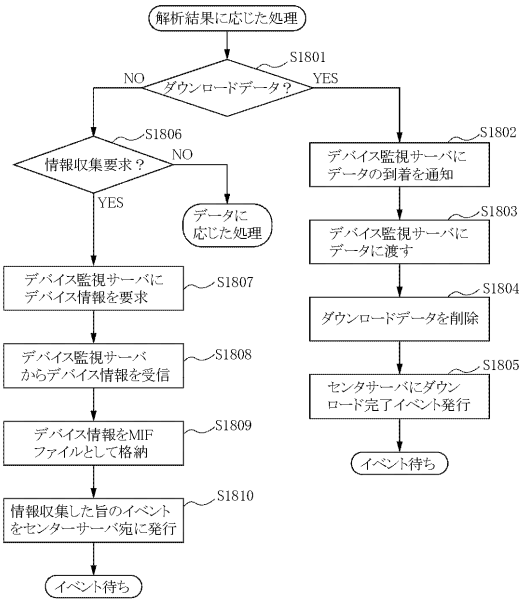
【図１６】



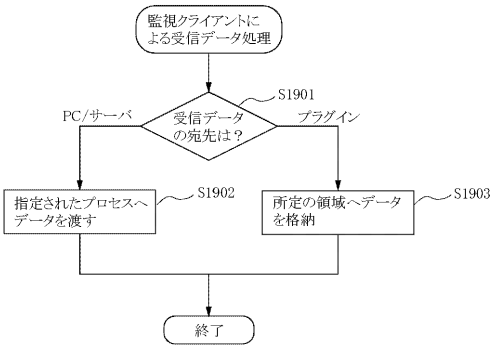
【図１７】



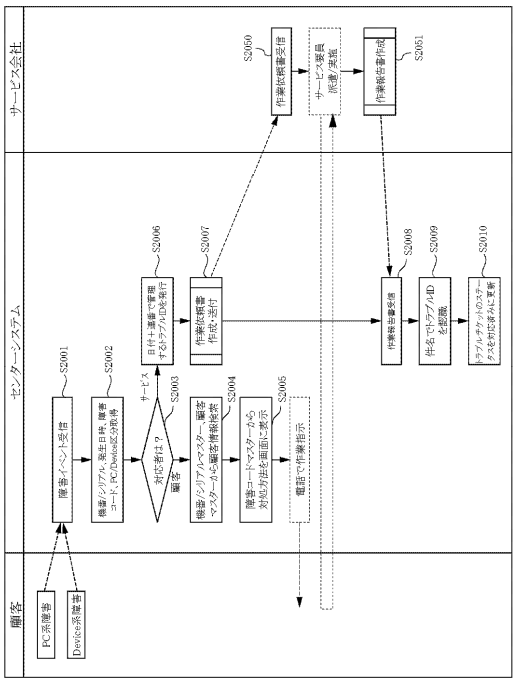
【図１８】



【図１９】



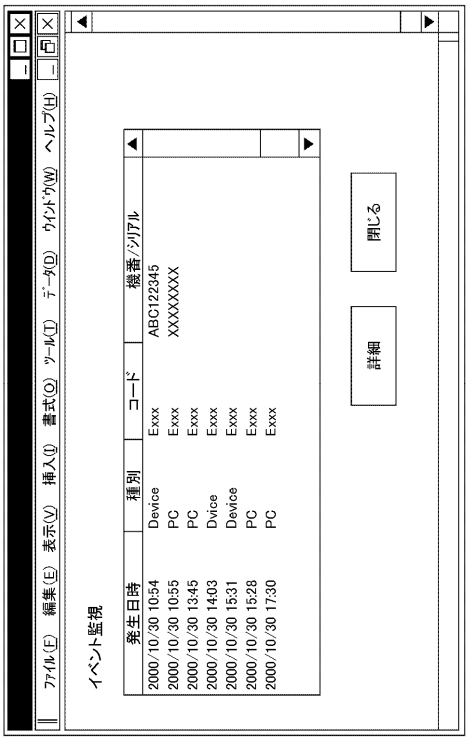
【図２０】



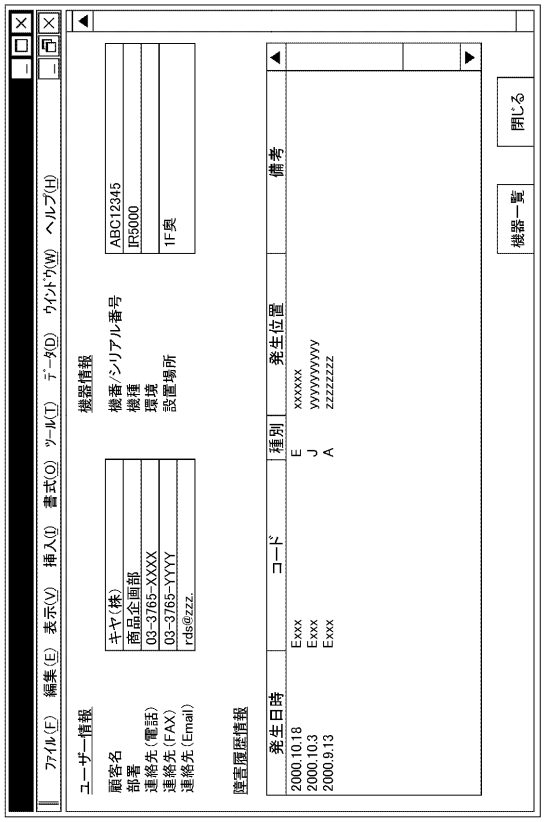
【図２１】

機番/シリアル	発生日時	障害コード	PC/Device区分

【図２２】



【図２３】



【図２４】

障害ｺｰﾄﾞ	区分	対応者区分	対処方法
E001	Device	顧客	電源のOFF/ON
Exxx	Device	サービス	部品xxxxの交換
Exxx	Device	サービス	現地で要調査
-1000	PC	顧客	ディスクの
-1001	PC	サービス	ハードディスク交換

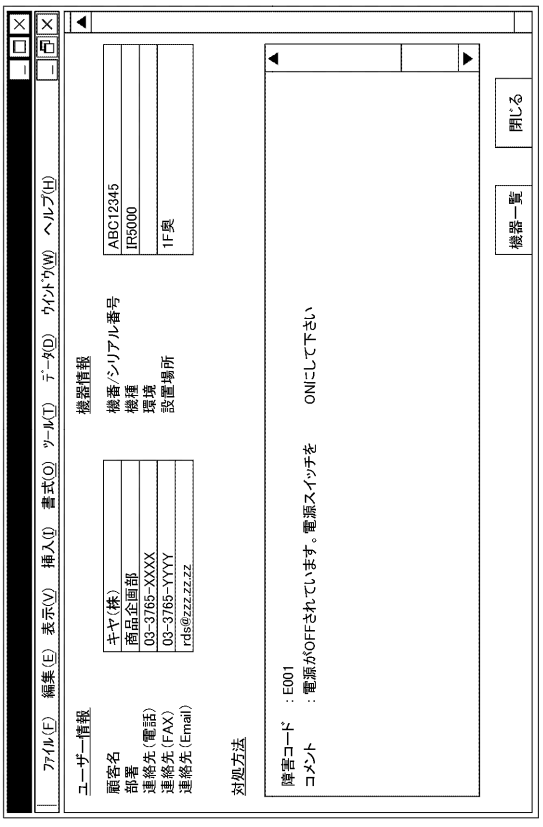
【図２５】

機番/シリアル	メーカー	顧客コード	顧客サブコード	設置場所	サービス会社コード
ABC12345	Caa	0001	01	1F奥	300
12345678	IBB	0001	01	マシン室	500

【図２６】

顧客コード	顧客サブコード	会社名	部署名	住所	電話	FAX	Email	担当者	契約レベル	PC系サービス会社コード	ディバス系サービス会社コード
0001	01	ABC(株)	東京本社	千代田区丸の内・・・	03-3555-xxxx		xxx@yyy.co.jp		1		
0001	02	ABC(株)	横浜支社	横浜市西区・・・	045-312-xxxx				2		
0002	01	日本産業		千代田区霞が関・・・					3		
0003	01	千商事	東京本社	大田区下丸子・・・							
0003	02	千商事	神奈川支社	横浜市戸塚区・・・							
0003	03	千商事	千葉支社	千葉市美浜区・・・							

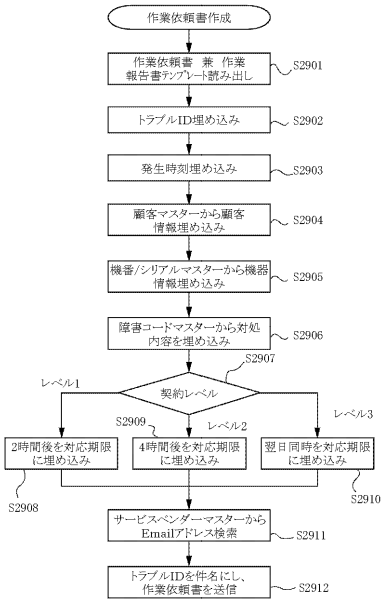
【図２７】



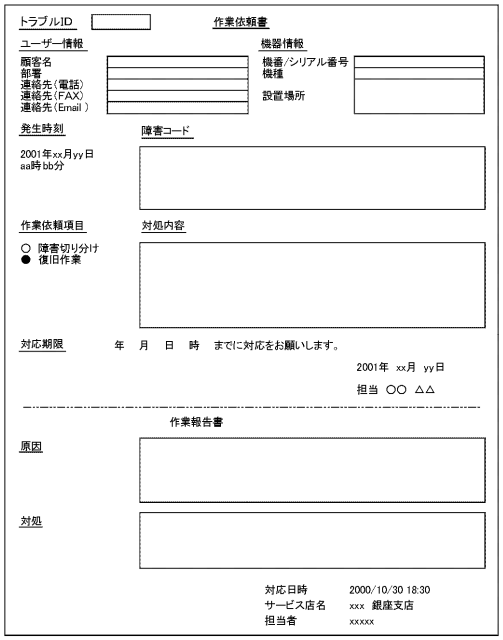
【図２８】

トラブルチケットID	ステータス	発生日時	対応日時	顧客コード	顧客サブコード	機番/シリアル	実施サービス会社	実施者	原因	対処内容
0010300001	対処済み	2000/10/30 10:21	2000/10/30 11:18	0001	02	ABC12345	3001	xxx	xxx部品寿命	xxxx交換
0010300002	対応中	2000/10/30 11:54		0003	01	xxxxx	3002	oooo		
0010300003	対応中	2000/10/30 15:09		0001	01	xxxxxx	3001	yyyyy		

【図２９】



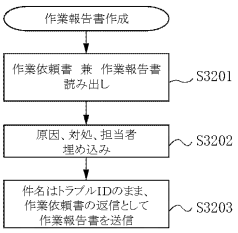
【図３０】



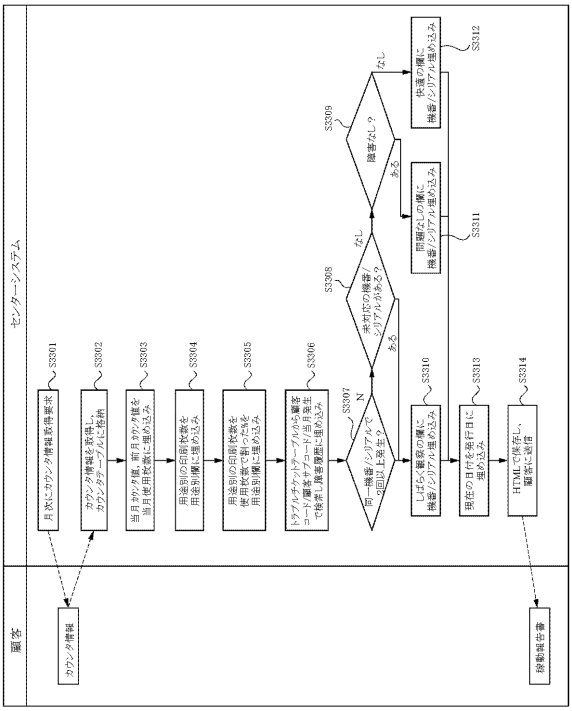
【図３１】

サービス会社コード	区分	会社名	部署名	住所	電話	FAX	Email	担当者
3001	Device,PC	CSS	銀座支店	中央区銀座…	03-3555-XXXX			
3002	Device	CSS	横浜支店	横浜市…				
3003	Device	CSS	千葉支店	千葉市…				

【図３２】



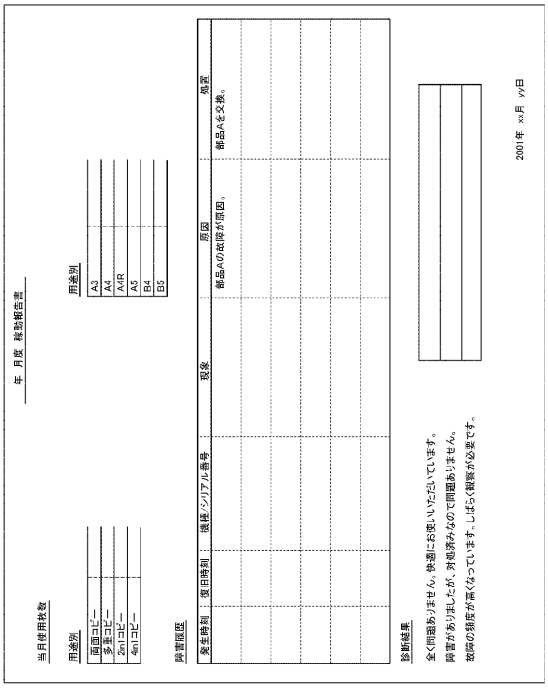
【図３３】



【図３４】

機番/シリアル	年月	カウンタ値	両面	多重	2in1	4in1	FAX出力	プリント出力	スキャン送信	eMail送信	A3	A4	A4R	A5	B4	B5	B5R	LET	LETR	LGL	その他
ABC12345	0008																				
ABC12345	0009																				
ABC12345	0010																				

【図３５】



フロントページの続き

(72)発明者　原　寛行
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　廣瀬　淳一
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　大森　和志
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
(72)発明者　川島　真
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

審査官　須田　勝巳

(56)参考文献　特開平０８－１６６９９８（ＪＰ，Ａ）
特開平０９－１０１９８７（ＪＰ，Ａ）
特開平１１－３３８３１８（ＪＰ，Ａ）
特開２０００－２８７０１８（ＪＰ，Ａ）
特開２０００－２７０１４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q 10/00-50/00