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

特許第4829822号
(P4829822)

(45)発行日　平成23年12月7日(2011.12.7)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.		F I		
G06F 3/12	(2006.01)	G06F	3/12	K
H04N 1/00	(2006.01)	H04N	1/00	107Z
H04M 11/00	(2006.01)	H04M	11/00	301
G03G 21/00	(2006.01)	G03G	21/00	396
G03G 21/04	(2006.01)	G03G	21/00	390

請求項の数 9　(全 32 頁)

(21)出願番号　特願2007-71223(P2007-71223)
(22)出願日　平成19年3月19日(2007.3.19)
(65)公開番号　特開2008-234180(P2008-234180A)
(43)公開日　平成20年10月2日(2008.10.2)
審査請求日　平成21年10月19日(2009.10.19)

(73)特許権者　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100080931
弁理士　大澤　敬
(74)代理人　100123881
弁理士　大澤　豊
(72)発明者　大西　一喜
東京都大田区中馬込１丁目３番６号　株式会社リコー内

審査官　田中　友章

最終頁に続く

(54)【発明の名称】遠隔機器管理システム

(57)【特許請求の範囲】
【請求項１】
管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、
前記電子機器に、
遠隔管理用機種機番等のメンテナンス用機器情報を保持するメンテナンス用機器情報保持手段と、前記通信アダプタからの要求に対し、前記メンテナンス用機器情報を変更するメンテナンス用機器情報変更手段とを設け、
前記通信アダプタに、
管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されているメンテナンス用機器情報を取得するメンテナンス用機器情報取得手段と、該メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットであるか否かを判定するフォーマット判定手段と、該フォーマット判定手段による判定の結果、前記メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットでない場合に、該メンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、該メンテナンス用機器情報が保持されている電子機器の機器情報を前記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、前記管理装置からメンテナンス用機器情報を受

信した場合に、該メンテナンス用機器情報を含む変更要求を前記不正なメンテナンス用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、
前記管理装置に、
前記通信アダプタより送信されてくる前記不正なメンテナンス用機器情報が保持されている電子機器の機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しいメンテナンス用機器情報を入力するためのメンテナンス用機器情報入力手段と、該メンテナンス用機器情報入力手段によって入力されたメンテナンス用機器情報を前記通信アダプタへ送信するメンテナンス用機器情報送信手段とを設けたことを特徴とする遠隔機器管理システム。
【請求項２】
請求項１記載の遠隔機器管理システムにおいて、
前記通信アダプタに、
前記機器検索手段によって検索した電子機器より該電子機器の稼動情報，状態情報，設定情報等の機器使用情報を含む機器情報を取得する機器情報取得手段を設け、
前記通信アダプタの前記不正機器情報送信手段は、前記不正なメンテナンス用機器情報が保持されている電子機器の機器情報として、前記機器情報取得手段によって取得した機器情報を前記管理装置へ送信することを特徴とする遠隔機器管理システム。
【請求項３】
請求項２記載の遠隔機器管理システムにおいて、
前記通信アダプタに、前記機器検索手段によって検索した電子機器より前記機器情報取得手段によって取得した機器情報に基づいて該電子機器の状態変更を検出する状態変更検出手段と、該状態変更検出手段による検出の結果、前記機器検索手段によって検索した電子機器の状態がメンテナンスが必要な状態に変動した場合に、その旨を示す情報を前記管理装置へ送信する状態変動情報送信手段とを設けたことを特徴とする遠隔機器管理システム。
【請求項４】
管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、
前記電子機器に、
遠隔管理用機種機番等のメンテナンス用機器情報を保持するメンテナンス用機器情報保持手段と、前記通信アダプタからの要求に対し、前記メンテナンス用機器情報を変更するメンテナンス用機器情報変更手段とを設け、
前記通信アダプタに、
管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、
ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を前記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による前記管理装置への前記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、前記ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されているメンテナンス用機器情報を取得するメンテナンス用機器情報取得手段と、該メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットであるか否かを判定するフォーマット判定手段と、該フォーマット判定手段による判定の結果、前記メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットでない場合に、該メンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、前記不正なメンテナンス用機器情報が保持されている電子機器の機器情報を報

知する不正機器情報報知手段と、正しいメンテナンス用機器情報を入力するためのメンテナンス用機器情報入力手段と、前記不正機器情報報知手段による報知に対して、前記メンテナンス用機器情報入力手段によってメンテナンス用機器情報が入力された場合に、該メンテナンス用機器情報を含む変更要求を前記不正なメンテナンス用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、

前記管理装置に、

特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、前記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を前記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を前記通信アダプタへ送信するユーザ認証結果送信手段とを設けたことを特徴とする遠隔機器管理システム。

【請求項５】

請求項４記載の遠隔機器管理システムにおいて、

前記通信アダプタに、

前記機器検索手段によって検索した電子機器より該電子機器の稼動情報，状態情報，設定情報等の機器使用情報を含む機器情報を取得する機器情報取得手段を設け、

前記通信アダプタの前記不正機器情報報知手段は、前記不正なメンテナンス用機器情報が保持されている電子機器の機器情報として、前記機器情報取得手段によって取得した機器情報を報知することを特徴とする遠隔機器管理システム。

【請求項６】

管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、

前記電子機器に、

相互認証を行う暗号化通信手段と、相互認証用証明書として当該電子機器の識別情報を持つ機器個別証明書を保持する機器個別証明書保持手段と、相互認証用証明書として機器管理対象となる電子機器全体での識別情報を持つ機器共通証明書を保持する機器共通証明書保持手段と、前記通信アダプタからの前記機器共通証明書での暗号化通信による要求により、前記機器個別証明書を変更する機器個別証明書変更手段とを設け、

前記通信アダプタに、

相互認証を行う暗号化通信手段と、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器の機器情報を暗号化通信によって取得する機器情報取得手段と、該機器情報取得手段による機器情報取得時の暗号化通信に用いる相互認証用証明書の不正を検出する証明書不正検出手段と、該証明書不正検出手段によって相互認証用証明書の不正が検出された時に前記機器情報取得手段によって取得した前記電子機器の機器情報を不正な機器情報として前記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、前記管理装置から機器個別証明書を受信した場合に、該機器個別証明書を含む変更要求を前記機器検索手段によって検索した電子機器へ暗号化通信によって送信する変更要求送信手段とを設け、

前記管理装置に、

前記通信アダプタより送信されてくる前記不正な機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しい機器個別証明書を入力するための機器個別証明書入力手段と、該機器個別証明書入力手段によって入力された機器個別証明書を前記通信アダプタへ送信する機器個別証明書送信手段とを設けたことを特徴とする遠隔機器管理システム。

【請求項７】

管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、

前記電子機器に、
相互認証を行う暗号化通信手段と、相互認証用証明書として当該電子機器の識別情報を持つ機器個別証明書を保持する機器個別証明書保持手段と、相互認証用証明書として機器管理対象となる電子機器全体での識別情報を持つ機器共通証明書を保持する機器共通証明書保持手段と、前記通信アダプタからの前記機器共通証明書での暗号化通信による要求により、前記機器個別証明書を変更する機器個別証明書変更手段とを設け、
前記通信アダプタに、
相互認証を行う暗号化通信手段と、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を前記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による前記管理装置への前記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、前記ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器の機器情報を暗号化通信によって取得する機器情報取得手段と、該機器情報取得手段による機器情報取得時の暗号化通信に用いる相互認証用証明書の不正を検出する証明書不正検出手段と、該証明書不正検出手段によって相互認証用証明書の不正が検出された時に前記機器情報取得手段によって取得した前記電子機器の機器情報を不正な機器情報として報知する不正機器情報報知手段と、正しい機器個別証明書を入力するための機器個別証明書入力手段と、前記不正機器情報報知手段による報知に対して、前記機器個別証明書入力手段によって機器個別証明書が入力された場合に、該機器個別証明書を含む変更要求を前記機器検索手段によって検索した電子機器へ暗号化通信によって送信する変更要求送信手段とを設け、
前記管理装置に、
特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、前記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を前記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を前記通信アダプタへ送信するユーザ認証結果送信手段とを設けたことを特徴とする遠隔機器管理システム。
【請求項８】
管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、
前記電子機器に、
前記通信アダプタのＩＰアドレス等の遠隔機器管理用機器情報を保持する遠隔機器管理用機器情報保持手段と、前記通信アダプタからの要求に対し、前記遠隔機器管理用機器情報を変更する遠隔機器管理用機器情報変更手段とを設け、
前記通信アダプタに、
管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されている遠隔機器管理用機器情報を取得する遠隔機器管理用機器情報取得手段と、該遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定する照合判定手段と、該照合判定手段による判定の結果、前記遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、該遠隔機器管理用機器情

報を不正な遠隔機器管理用機器情報と判断して、該遠隔機器管理用機器情報が保持されている電子機器の機器情報を前記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、前記管理装置から遠隔機器管理用機器情報を受信した場合に、該遠隔機器管理用機器情報を含む変更要求を前記不正な遠隔機器管理用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、

前記管理装置に、

前記通信アダプタより送信されてくる前記不正な遠隔機器管理用機器情報が保持されている電子機器の機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しい遠隔機器管理用機器情報を入力するための遠隔機器管理用機器情報入力手段と、該遠隔機器管理用機器情報入力手段によって入力された遠隔機器管理用機器情報を前記通信アダプタへ送信する遠隔機器管理用機器情報送信手段とを設けたことを特徴とする遠隔機器管理システム。

【請求項９】

管理装置と電子機器とが通信アダプタを介して通信可能であり、前記管理装置により前記通信アダプタを介して前記電子機器を遠隔管理する遠隔機器管理システムにおいて、

前記電子機器に、

前記通信アダプタのＩＰアドレス等の遠隔機器管理用機器情報を保持する遠隔機器管理用機器情報保持手段と、前記通信アダプタからの要求に対し、前記遠隔機器管理用機器情報を変更する遠隔機器管理用機器情報変更手段とを設け、

前記通信アダプタに、

管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、

ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を前記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による前記管理装置への前記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、前記ネットワークセグメント指定手段によって指定された前記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されている遠隔機器管理用機器情報を取得する遠隔機器管理用機器情報取得手段と、該遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定する照合判定手段と、該照合判定手段による判定の結果、前記遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、該遠隔機器管理用機器情報を不正な遠隔機器管理用機器情報と判断して、該不正な遠隔機器管理用機器情報が保持されている電子機器の機器情報を報知する不正機器情報報知手段と、正しい遠隔機器管理用機器情報を入力するための遠隔機器管理用機器情報入力手段と、前記不正機器情報報知手段による報知に対して、前記遠隔機器管理用機器情報入力手段によって遠隔機器管理用機器情報が入力された場合に、該遠隔機器管理用機器情報を含む変更要求を前記不正な遠隔機器管理用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、

前記管理装置に、

特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、前記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を前記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を前記通信アダプタへ送信するユーザ認証結果送信手段とを設けたことを特徴とする遠隔機器管理システム。

【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、管理装置により通信アダプタを介してＯＡ機器（例えば複写機，ファクシミリ装置，プリンタ，又は印刷機）等の電子機器を遠隔管理する遠隔機器管理システムに関する。
【背景技術】
【０００２】
遠隔機器管理システムとしては、例えば特許文献１に見られるように、ユーザ（顧客）のオフィス等に設置された複写機等の画像形成装置（ＯＡ機器）を通信アダプタ（データ通信装置）および公衆回線等の通信回線を利用し、サービスセンタ等に設置された中央管理装置（管理装置）と接続可能にした画像形成装置管理システムが一般に知られている。
【特許文献１】特開２０００－２９３５４号公報
【０００３】
このような遠隔機器管理システムにおいて、顧客先（顧客サイト）のＯＡ機器は、自己診断機能を備えており、故障等の異常が発生したり、メンテナンス時期又は消耗品の補充時期に到達すると、その旨を示すＳＣ（サービスマンコール）情報を通信アダプタおよび通信回線を介して管理装置へ送信する。管理装置は、顧客先のＯＡ機器置からＳＣ情報を受信すると、その情報をその送信元のＯＡ機器の異常修復，メンテナンス，又はサプライ補充等の作業を担当するサービスマンが使用しているモバイル端末（例えばノート型のパーソナルコンピュータ）等の端末装置へ送信してその表示画面に表示させる。
【０００４】
サービスマンは、端末装置の表示画面の表示内容を見て、ＳＣ情報の送信元のＯＡ機器が設置されている顧客先に出向き、そのＯＡ機器の異常修復，メンテナンス，又はサプライ補充等の作業を行う。
一方、このような遠隔機器管理システムでは、近年、顧客先に複数台のＯＡ機器を設置する際に、それらをＬＡＮ（ローカル・エリア・ネットワーク）等のネットワークによって接続するケースが増えてきており、その各ＯＡ機器を顧客側のネットワーク管理者（機器管理担当者）が管理を行っている。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、このような従来の遠隔機器管理システムでは、以下の（１）～（３）に示すようにメンテナンス業務の負荷が大きいという問題がある。
（１）ネットワーク上に接続されたＯＡ機器の管理のために、ネットワーク管理者は多大な労力を消費していた。
（２）顧客先へのＯＡ機器の新規導入に対して、ＯＡ機器の遠隔機器管理のための情報の設定（保持）が確認されておらず、機器管理も導入するにあたり、サービスマンがメンテナンス作業を行わなければならないことがある。
【０００６】
（３）顧客先にＯＡ機器の遠隔機器管理サービスが導入されている環境において、ＯＡ機器のメンテナンス作業（ボード交換等）のための遠隔管理に必要な情報（機器識別番号，証明書）の設定が変更又は削除され、遠隔機器管理業務への影響が発生し、顧客への遠隔機器管理サービスが提供できず、サービスマンがメンテナンス作業を行わなければならないことがある。
この発明は、上記の点に鑑みてなされたものであり、遠隔機器管理システムにおいて、ＯＡ機器等の電子機器の配置位置（レイアウト）の変更等による電子機器の遠隔機器管理の異常を早期に発見し、ネットワーク管理者による管理業務やメンテナンス担当者（サービスマン等）によるメンテナンス業務の負荷軽減を実現できるようにすることを目的とする。

【課題を解決するための手段】
【０００７】
この発明は、管理装置と電子機器とが通信アダプタを介して通信可能であり、上記管理装置により上記通信アダプタを介して上記電子機器を遠隔管理する遠隔機器管理システムにおいて、上記の目的を達成するため、次のようにしたことを特徴とする。
【０００８】
請求項１の発明による遠隔機器管理システムは、上記電子機器に、遠隔管理用機種機番等のメンテナンス用機器情報を保持するメンテナンス用機器情報保持手段と、上記通信アダプタからの要求に対し、上記メンテナンス用機器情報を変更するメンテナンス用機器情報変更手段とを設け、上記通信アダプタに、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されているメンテナンス用機器情報を取得するメンテナンス用機器情報取得手段と、該メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットであるか否かを判定するフォーマット判定手段と、該フォーマット判定手段による判定の結果、上記メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットでない場合に、該メンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、該メンテナンス用機器情報が保持されている電子機器の機器情報を上記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、上記管理装置からメンテナンス用機器情報を受信した場合に、該メンテナンス用機器情報を含む変更要求を上記不正なメンテナンス用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、上記管理装置に、上記通信アダプタより送信されてくる上記不正なメンテナンス用機器情報が保持されている電子機器の機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しいメンテナンス用機器情報を入力するためのメンテナンス用機器情報入力手段と、該メンテナンス用機器情報入力手段によって入力されたメンテナンス用機器情報を上記通信アダプタへ送信するメンテナンス用機器情報送信手段とを設けたものである。
【０００９】
請求項２の発明による遠隔機器管理システムは、請求項１の遠隔機器管理システムにおいて、上記通信アダプタに、上記機器検索手段によって検索した電子機器より該電子機器の稼動情報，状態情報，設定情報等の機器使用情報を含む機器情報を取得する機器情報取得手段を設け、上記通信アダプタの上記不正機器情報送信手段は、上記不正なメンテナンス用機器情報が保持されている電子機器の機器情報として、上記機器情報取得手段によって取得した機器情報を上記管理装置へ送信するものである。
【００１０】
請求項３の発明による遠隔機器管理システムは、請求項２の遠隔機器管理システムにおいて、上記通信アダプタに、上記機器検索手段によって検索した電子機器より上記機器情報取得手段によって取得した機器情報に基づいて該電子機器の状態変更を検出する状態変更検出手段と、該状態変更検出手段による検出の結果、上記機器検索手段によって検索した電子機器の状態がメンテナンスが必要な状態に変動した場合に、その旨を示す情報を上記管理装置へ送信する状態変動情報送信手段とを設けたものである。
【００１１】
請求項４の発明による遠隔機器管理システムは、上記電子機器に、遠隔管理用機種機番等のメンテナンス用機器情報を保持するメンテナンス用機器情報保持手段と、上記通信アダプタからの要求に対し、上記メンテナンス用機器情報を変更するメンテナンス用機器情報変更手段とを設け、上記通信アダプタに、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別

手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を上記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による上記管理装置への上記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、上記ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されているメンテナンス用機器情報を取得するメンテナンス用機器情報取得手段と、該メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットであるか否かを判定するフォーマット判定手段と、該フォーマット判定手段による判定の結果、上記メンテナンス用機器情報取得手段によって取得したメンテナンス用機器情報が正しいフォーマットでない場合に、該メンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、上記不正なメンテナンス用機器情報が保持されている電子機器の機器情報を報知する不正機器情報報知手段と、正しいメンテナンス用機器情報を入力するためのメンテナンス用機器情報入力手段と、上記不正機器情報報知手段による報知に対して、上記メンテナンス用機器情報入力手段によってメンテナンス用機器情報が入力された場合に、該メンテナンス用機器情報を含む変更要求を上記不正なメンテナンス用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、上記管理装置に、特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、上記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を上記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を上記通信アダプタへ送信するユーザ認証結果送信手段とを設けたものである。

【００１２】

請求項５の発明による遠隔機器管理システムは、請求項４の遠隔機器管理システムにおいて、上記通信アダプタに、上記機器検索手段によって検索した電子機器より該電子機器の稼動情報，状態情報，設定情報等の機器使用情報を含む機器情報を取得する機器情報取得手段を設け、上記通信アダプタの上記不正機器情報報知手段は、上記不正なメンテナンス用機器情報が保持されている電子機器の機器情報として、上記機器情報取得手段によって取得した機器情報を報知するものである。

【００１３】

請求項６の発明による遠隔機器管理システムは、上記電子機器に、相互認証を行う暗号化通信手段と、相互認証用証明書として当該電子機器の識別情報を持つ機器個別証明書を保持する機器個別証明書保持手段と、相互認証用証明書として機器管理対象となる電子機器全体での識別情報を持つ機器共通証明書を保持する機器共通証明書保持手段と、上記通信アダプタからの上記機器共通証明書での暗号化通信による要求により、上記機器個別証明書を変更する機器個別証明書変更手段とを設け、上記通信アダプタに、相互認証を行う暗号化通信手段と、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器の機器情報を暗号化通信によって取得する機器情報取得手段と、該機器情報取得手段による機器情報取得時の暗号化通信に用いる相互認証用証明書の不正を検出する証明書不正検出手段と、該証明書不正検出手段によって相互認証用証明書の不正が検出された時に上記機器情報取得手段によって取得した上記電子機器の機器情報を不正な機器情報として上記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、上記管理装置から機器個別証明書を受信した場合に、該機器個別証明書を含む変更要求を上記機器検索手段によって検索した電子機器へ暗号化通信によって送信する変更要求送信手段とを設け、上記管理装置に、上記通信アダプタより送信されてくる上記不正な機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しい機器個別証明書を入力するための機器個別証明書入力手

段と、該機器個別証明書入力手段によって入力された機器個別証明書を上記通信アダプタへ送信する機器個別証明書送信手段とを設けたものである。

【００１４】

請求項７の発明による遠隔機器管理システムは、上記電子機器に、相互認証を行う暗号化通信手段と、相互認証用証明書として当該電子機器の識別情報を持つ機器個別証明書を保持する機器個別証明書保持手段と、相互認証用証明書として機器管理対象となる電子機器全体での識別情報を持つ機器共通証明書を保持する機器共通証明書保持手段と、上記通信アダプタからの上記機器共通証明書での暗号化通信による要求により、上記機器個別証明書を変更する機器個別証明書変更手段とを設け、上記通信アダプタに、相互認証を行う暗号化通信手段と、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を上記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による上記管理装置への上記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、上記ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器の機器情報を暗号化通信によって取得する機器情報取得手段と、該機器情報取得手段による機器情報取得時の暗号化通信に用いる相互認証用証明書の不正を検出する証明書不正検出手段と、該証明書不正検出手段によって相互認証用証明書の不正が検出された時に上記機器情報取得手段によって取得した上記電子機器の機器情報を不正な機器情報として報知する不正機器情報報知手段と、正しい機器個別証明書を入力するための機器個別証明書入力手段と、上記不正機器情報報知手段による報知に対して、上記機器個別証明書入力手段によって機器個別証明書が入力された場合に、該機器個別証明書を含む変更要求を上記機器検索手段によって検索した電子機器へ暗号化通信によって送信する変更要求送信手段とを設け、上記管理装置に、特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、上記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を上記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を上記通信アダプタへ送信するユーザ認証結果送信手段とを設けたものである。

【００１５】

請求項８の発明による遠隔機器管理システムは、上記電子機器に、上記通信アダプタのＩＰアドレス等の遠隔機器管理用機器情報を保持する遠隔機器管理用機器情報保持手段と、上記通信アダプタからの要求に対し、上記遠隔機器管理用機器情報を変更する遠隔機器管理用機器情報変更手段とを設け、上記通信アダプタに、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、該ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されている遠隔機器管理用機器情報を取得する遠隔機器管理用機器情報取得手段と、該遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定する照合判定手段と、該照合判定手段による判定の結果、上記遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、該遠隔機器管理用機器情報を不正な遠隔機器管理用機器情報と判断して、該遠隔機器管理用機器情報が保持されている電子機器の機器情報を上記管理装置へ送信する不正機器情報送信手段と、該不正機器情報送信手段による送信に対して、上記管理装置から遠隔機器管理用機器情報を受信した場合に、該遠隔機器管理用機器情

報を含む変更要求を上記不正な遠隔機器管理用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、上記管理装置に、上記通信アダプタより送信されてくる上記不正な遠隔機器管理用機器情報が保持されている電子機器の機器情報を受信した場合に、該機器情報を記憶する不正機器情報記憶手段と、正しい遠隔機器管理用機器情報を入力するための遠隔機器管理用機器情報入力手段と、該遠隔機器管理用機器情報入力手段によって入力された遠隔機器管理用機器情報を上記通信アダプタへ送信する遠隔機器管理用機器情報送信手段とを設けたものである。

【００１６】

請求項９の発明による遠隔機器管理システムは、上記電子機器に、上記通信アダプタのＩＰアドレス等の遠隔機器管理用機器情報を保持する遠隔機器管理用機器情報保持手段と、上記通信アダプタからの要求に対し、上記遠隔機器管理用機器情報を変更する遠隔機器管理用機器情報変更手段とを設け、上記通信アダプタに、管理対象とするネットワークセグメントを指定するネットワークセグメント指定手段と、ユーザ認証情報を入力するユーザ認証情報入力手段と、該ユーザ認証情報入力手段によって入力されたユーザ認証情報から該ユーザ認証情報を入力するための操作を行ったユーザを判別するユーザ判別手段と、該ユーザ判別手段によって判別されたユーザが特殊権限ユーザであった場合に、該特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求を上記管理装置へ送信するユーザ認証要求送信手段と、該ユーザ認証要求送信手段による上記管理装置への上記ユーザ認証要求に対して、該管理装置から認証成功を示すユーザ認証結果を受信した場合に、上記ネットワークセグメント指定手段によって指定された上記ネットワークセグメントに接続されている電子機器を検索する機器検索手段と、該機器検索手段によって検索した電子機器より該電子機器に保持されている遠隔機器管理用機器情報を取得する遠隔機器管理用機器情報取得手段と、該遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定する照合判定手段と、該照合判定手段による判定の結果、上記遠隔機器管理用機器情報取得手段によって取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、該遠隔機器管理用機器情報を不正な遠隔機器管理用機器情報と判断して、該不正な遠隔機器管理用機器情報が保持されている電子機器の機器情報を報知する不正機器情報報知手段と、正しい遠隔機器管理用機器情報を入力するための遠隔機器管理用機器情報入力手段と、上記不正機器情報報知手段による報知に対して、上記遠隔機器管理用機器情報入力手段によって遠隔機器管理用機器情報が入力された場合に、該遠隔機器管理用機器情報を含む変更要求を上記不正な遠隔機器管理用機器情報が保持されている電子機器へ送信する変更要求送信手段とを設け、上記管理装置に、特殊権限ユーザのユーザ認証情報を記憶するユーザ認証情報記憶手段と、上記通信アダプタからユーザ認証要求を受信した場合に、該ユーザ認証要求中のユーザ認証情報を上記記憶手段内のユーザ認証情報と照合し、該記憶手段に一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行うユーザ認証手段と、該ユーザ認証手段によるユーザ認証の結果を上記通信アダプタへ送信するユーザ認証結果送信手段とを設けたものである。

【発明の効果】

【００１７】

この発明の遠隔機器管理システムによれば、電子機器の配置位置（レイアウト）の変更等による電子機器の遠隔機器管理の異常を早期に発見し、ネットワーク管理者による管理業務やメンテナンス担当者（サービスマン等）によるメンテナンス業務の負荷軽減を実現することができる。

【発明を実施するための最良の形態】

【００１８】

以下、この発明を実施するための最良の形態を図面に基づいて具体的に説明する。

図１は、この発明による遠隔機器管理システム（画像形成装置管理システム）の構成例を示すブロック図である。

この画像形成装置管理システムは、サービスセンタに設置されている中央管理装置としてのセンタシステム１と、各顧客サイト（ユーザ側）Ａ，Ｂにそれぞれ設置されている電子機器群とによって構成している。

【００１９】

センタシステム１は、ルータ２と、複数のサーバ３ａ，３ｂと、それらを相互に通信可能に接続するためのＬＡＮ等のネットワーク４とによって構成されている。

顧客サイトＡの電子機器群は、ルータ１１と、そのルータ１１およびインタネット５を介してセンタシステム１に通信可能に接続する通信アダプタ１２と、複写機１３，プリンタ１４等のＯＡ機器（画像形成装置）と、それらのＯＡ機器，ルータ１１，および通信アダプタ１２を相互に通信可能に接続するためのＬＡＮ等のネットワーク１５とによってネットワークセグメントを構成している。

【００２０】

顧客サイトＢの電子機器群は、公衆通信回線網６およびアクセスポイント７を介してセンタシステム１に通信可能に接続する通信アダプタ２１と、ファクシミリ（ＦＡＸ）装置２２，複写機２３，プリンタ２４等のＯＡ機器と、通信アダプタ２１，複写機２３，およびプリンタ２４を相互に通信可能に接続するためのＬＡＮ等のネットワーク２５と、通信アダプタ２１とファクシミリ装置２２とを通信可能に接続するための有線による専用Ｉ／Ｆ２６とによってネットワークセグメントを構成している。

【００２１】

図２は、サーバ３ａの構成例を示すブロック図である。

サーバ３ａは、ＣＰＵ３１，リアルタイムクロック回路３２，ＲＯＭ３３，ＲＡＭ３４，外部メモリ制御ユニット３５，ネットワークＩ／Ｆユニット３６，ハードディスク装置（以下「ＨＤＤ」と略称する）３７等によって構成されている。なお、サーバ３ｂもサーバ３ａと同様の構成なので、ネットワークＩ／Ｆユニット３６以外の各部の図示および説明は省略する。

【００２２】

ＣＰＵ３１は、ＲＯＭ３３内の制御プログラムによってサーバ３ａ全体を統括的に制御する中央処理装置である。

リアルタイムクロック回路３２は、時刻情報を発生するものであり、ＣＰＵ３１がそれを読み込むことによって現在の時刻を知ることができる。

ＲＯＭ３３は、ＣＰＵ３１が使用する制御プログラムを含む各種固定データを格納している読み出し専用メモリである。

ＲＡＭ３４は、ＣＰＵ３１がデータ処理を行う際に使用するワークメモリ等として使用する読み書き可能なメモリである。

【００２３】

外部メモリ制御ユニット３５は、ＨＤＤ３７とのインタフェース制御を行う。

ネットワークＩ／Ｆユニット３６は、ネットワーク４に接続されている他のサーバ３ｂやルータ２等とのインタフェース制御を行う。

ＨＤＤ３７は、最新の特殊権限ユーザ（メンテナンス担当者）のユーザ認証情報（ユーザ情報等）およびメンテナンス権限（アクセス権限）を含む各種情報をＤＢ（データベース）として記憶する記憶手段である。よって、このＨＤＤ３７が、不正機器情報記憶手段およびユーザ認証情報記憶手段としての機能を果たす。なお、サーバ３ａに不揮発性メモリを備え、それに各種情報を記憶することもできる。

【００２４】

ここで、サーバ３ａ，３ｂのＣＰＵ３１が、ＲＯＭ３３内の制御プログラムに従って動作し、その際にＲＡＭ３４，外部メモリ制御ユニット３５，ネットワークＩ／Ｆユニット３６等を使用することにより、この発明による各種機能であるメンテナンス用機器情報送信手段，機器個別証明書送信手段，遠隔機器管理用機器情報送信手段，ユーザ認証手段，およびユーザ認証結果送信手段としての機能を実現することができる。

【００２５】

あるいは、内蔵のあるいは外付けのフレキシビルディスク装置あるいは光ディスク装置等のディスク装置によって、挿着された記録媒体（フレキシビルディスクや光ディスク等のディスク）に記録されている制御プログラムを読み込んで、内蔵のＨＤＤあるいはＲＡＭにインストールし、その制御プログラムに従って動作することにより上記各種機能を実現することもできる。

また、サーバ３ａ，３ｂに接続されている図示しないパーソナルコンピュータ等の端末装置が、メンテナンス用機器情報入力手段，機器個別証明書入力手段，および遠隔機器管理用機器情報入力手段としての機能を果たす。

【００２６】

図３は、図１の通信アダプタ２１の構成例を示すブロック図である。なお、通信アダプタ１２も同様の構成なので、その図示および説明は省略する。但し、通信アダプタ１２はルータ１１と通信する点が通信アダプタ２１と異なる。

通信アダプタ２１において、公衆通信回線網６からのデータは、まず回線切替回路４１に入力される。ここでは、公衆通信回線網６側からの通信が通信アダプタ２１に接続されているファクシミリ装置２２宛のものであれば、公衆通信回線網６側をファクシミリ装置２２に接続し、センタシステム１からの通信であれば、公衆通信回線網６側をモデム４２に接続する。

【００２７】

また、ネットワークＩ／Ｆユニット４３によって複写機２３等のＯＡ機器側との通信を行う。

これらの制御・処理は、ＲＯＭ４５内の制御プログラム（ファームウェアを含むソフトウェア）に従ってＣＰＵ４４を中心に行われる。

ＲＯＭ４５は、ＣＰＵ４４が使用する制御プログラムを含む各種固定データを格納している。

【００２８】

ＲＡＭ４６は、各ＯＡ機器へのアクセス権限を持つユーザのユーザ認証情報（ユーザ情報，アクセス権限等）を含む各種情報を記憶する記憶手段である。このＲＡＭ４６には、バックアップ用の電池（バッテリ）４７が接続されている。

スイッチ４８は、各種モードを選択的に設定するためのものである。

表示部４９は、各種情報を表示するものである。

通信アダプタ２１は、自己に接続されている各ＯＡ機器に対して、絶えず周期的に、且つこれらに付与されたデバイスアドレス順にポーリング動作を行う。

【００２９】

ここで、通信アダプタ２１，１２のＣＰＵ４４が、ＲＯＭ４５内の制御プログラムに従って動作し、その際にネットワークＩ／Ｆユニット４３，ＲＡＭ４６，および表示部４９等を使用することにより、この発明による各種機能であるネットワークセグメント指定手段，機器検索手段，メンテナンス用機器情報取得手段，フォーマット判定手段，不正機器情報送信手段，変更要求送信手段，機器情報取得手段，状態変更検出手段，状態変動情報送信手段，ユーザ認証情報入力手段，ユーザ判別手段，ユーザ認証要求送信手段，機器検索手段，メンテナンス用機器情報取得手段，フォーマット判定手段，不正機器情報報知手段，メンテナンス用機器情報入力手段，暗号化通信手段，証明書不正検出手段，遠隔機器管理用機器情報取得手段，照合判定手段，および遠隔機器管理用機器情報入力手段としての機能を実現することができる。

【００３０】

図４は、図１の複写機１３，２３の制御系の構成例を示すブロック図である。

複写機１３，２３の制御は、ＣＰＵ１０１を中心としてＲＯＭ１０２に記憶されている制御プログラムやデータに基づいて行われる。また、処理の中間結果や各種設定値，装置の状態などを蓄えるためにＲＡＭ１０３（記憶手段）を使用する。このＲＡＭ１０３は、電池によってバックアップされた不揮発性ＲＡＭとする。それによって、ＲＡＭ１０３はメンテナンス用機器情報保持手段，機器個別証明書保持手段，機器共通証明書保持手段，

および遠隔機器管理用機器情報保持手段としての機能を果たす。なお、ＲＡＭ１０３とは別に、不揮発性メモリ又はＨＤＤ等の不揮発性記憶媒体を設け、それにメンテナンス用機器情報保持手段等の各手段としての機能を果たせるようにしても構わない。

【００３１】

Ａ／Ｄコンバータ１０４は、露光ランプへの供給電圧，Ｐセンサの発光電圧と受光電圧，電位センサの出力，ＡＤＳセンサの出力，露光ランプの光量を検出するランプ光量センサの出力，感光体ドラムに流れる電流を検出するドラム電流センサの出力，定着ユニット内のサーミスタ電圧等を入力するために使用する。

光学系制御ユニット１０５は、露光ランプを制御する。

高圧電源ユニット１０６は、帯電チャージャ，分離チャージャ，転写チャージャ，転写前チャージャ（ＰＴＣ）にそれぞれ印加する高電圧、および現像ユニット内の現像ローラに印加する現像バイアス電圧を供給する。

【００３２】

モータ制御ユニット１０７は、感光体ドラムおよび各給紙ユニットや搬送部のローラ等を駆動するメインモータのコントロールを行う。

ヒータ制御ユニット１０８は、定着ユニットの定着ローラを加熱する定着ヒータへの通電を制御して、定着ローラの表面温度を所定範囲に保持する。

センサ制御ユニット１０９は、ランプ光量センサの受光ゲイン，ＡＤＳセンサの受光ゲイン，Ｐセンサの受光ゲイン，ＰセンサのＬＥＤの発光電圧等を可変するために使用する。

ネットワークＩ／Ｆユニット１１０は、通信アダプタ１２，２１との通信を行うユニットである。

【００３３】

操作部１１１は、各種情報を表示する表示部と、各種情報を入力するスイッチ部（操作キー）とを有する操作・表示パネルである。

ここで、複写機１３，２３のＣＰＵ１０１が、ＲＯＭ１０２内の制御プログラムに従って動作し、その際にＲＡＭ１０３，ネットワークＩ／Ｆユニット１１０，および操作部１１１等を使用することにより、この発明による各種機能であるメンテナンス用機器情報変更手段，暗号化通信手段，機器個別証明書変更手段，および遠隔機器管理用機器情報変更手段としての機能を実現することができる。

以上、複写機１３，２３の制御系について説明したが、プリンタ１４，２４等の他のＯＡ機器も、同様な制御系を備えているので、それらの図示および説明は省略する。

【００３４】

以下、上述したように構成された遠隔機器管理システムにおけるこの発明に係わる各制御（実施例）について、図５～図１７の各図面も参照して具体的に説明する。なお、説明の都合上、顧客サイトＢに設置されている通信アダプタ２１と複写機２３等の画像形成装置（以下「ＯＡ機器」という）との間の通信制御、およびその通信アダプタ２１とセンタシステム１のサーバ３ａとの間の通信制御について説明する。また、例えば図５に示すように、通信アダプタ２１には、図１の複写機２３およびプリンタ２４以外に、複写機２３１～２３３およびプリンタ２４１～２４３が接続されているものとする。

【００３５】

〔第１実施例〕

まず、第１実施例について説明する。

図５は、通信アダプタ２１が不正なメンテナンス情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の第１例を説明するための図である。

図６は、通信アダプタ２１が不正なメンテナンス情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の第２例を説明するための図である。

図７は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第１例を示すフローチャートである。

【００３６】

通信アダプタ２１は、例えば図５に示すように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、管理対象とするネットワークセグメントは「192.168.30.0　サブネットマスク255.255.255.0」、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングは「１日１回　ＡＭ０：００」、ネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングは「１週１回　日曜ＡＭ０：００」と指定されている。

【００３７】

この通信アダプタ２１のＣＰＵ４４は、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングになり、その検索の要求（セグメント検索要求）が発生すると、指定（設定）されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、任意のタイミング「１日１回　ＡＭ０：００」でのセグメント検索要求の発生によって機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。

【００３８】

この機器検索では、指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」中の各ＩＰアドレス「192.168.30.1～192.168.30.255」に対して、１ＩＰアドレスづつ、ＳＮＭＰ（Simple Network Management Protocol）によりＭＩＢ（Management Information Base）情報を取得することにより、指定されたネットワークセグメントに接続されている電子機器がＯＡ機器であるか否かを判定する。

【００３９】

例えば、ＭＩＢ情報を取得する際のＨＴＴＰＳ（Hypertext Transfer Protocol Security）によるＷｅｂサービスに対する要求に応答があるか、もしくは、取得したＭＩＢ情報（例えば「RFC1514 1.3.6.1.2.1.25. HostResourceMIB」）がＯＡ機器を示す情報（例えば「OID　hrDevicePrinter　(1.3.6.1.2.1.25.3.1.5)」）であった場合に、指定されたネットワークセグメントに接続されている電子機器がＯＡ機器であると判定する。つまり、指定されたネットワークセグメントに接続されているＯＡ機器を検索できる。

【００４０】

そして、その場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ（インタフェース）経由で検索したＯＡ機器（ＯＡ機器と判定したＯＡ機器）からそのＯＡ機器に保持されている（例えば図４のＲＡＭ１０３に記憶保持されている）メンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてセンタシステム１へ送信する。

【００４１】

具体的には、図７のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で検索したＯＡ機器より、そのＯＡ機器に保持されているメンテナンス用機器情報（遠隔管理用機種番号）を含むメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。そして、管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報に関して、メンテナンス用機器情報（遠隔管理用機種番号）のフォーマットをチェックし、そのメンテナンス用機器情報が正しいフォーマットであるか否かを判定する。

【００４２】

例えば、桁数や文字に制御コードが混じっていない場合に、メンテナンス用機器情報は正しいフォーマットであると判定するが、桁数や文字に制御コードが混じっている場合には、メンテナンス用機器情報は正しいフォーマットではないと判定する。

なお、メンテナンス用機器情報は、遠隔機器遠隔管理用機種機番（遠隔機器遠隔管理用ＩＤ）であった場合、例えば１０桁の英数字の文字列であれば正しいフォーマットとなる。ＯＡ機器に保持されているメンテナンス用機器情報は、ＯＡ機器のＵＩ（ユーザインタ

フェース）によって変更することはできない。メンテナンス用機器情報が正しいフォーマットでない場合には、顧客サイトＢにおけるＯＡ機器の配置が変更になっている可能性がある。

【００４３】

そして、メンテナンス用機器情報のフォーマットのチェック（判定）の結果、メンテナンス用機器情報が正しいフォーマットでない場合に、そのメンテナンス用機器情報、つまりそれを含むメンテナンス情報を不正なメンテナンス情報と判断して、そのメンテナンス情報が保持されているＯＡ機器の機器情報（そのＯＡ機器から取得したメンテナンス情報およびＭＩＢ情報を含むＯＡ機器情報）をセンタシステム１へ送信する。センタシステム１へ送信するＯＡ機器情報としては、ＯＡ機器を識別するＩＤが含まれていないもの（図５）と、ＯＡ機器を識別するＩＤが含まれているもの（図６）がある。

【００４４】

センタシステム１のサーバ３ａのＣＰＵ３１は、通信アダプタ２１より送られてくるＯＡ機器情報（顧客サイトＢにおけるネットワークセグメントに接続されている不正なメンテナンス情報が保持されているＯＡ機器の機器情報）を受信し、それをＨＤＤ（ＤＢ）３７に蓄積（記憶）する。そして、そのＯＡ機器情報を図示しない端末装置の表示部の画面上に一覧表示させる。

それによって、オペレータは、端末装置の表示部の画面上に一覧表示されたＯＡ機器情報を確認でき、正しいメンテナンス情報（メンテナンス用機器情報を含む）が判明した場合、それを画面上の操作又は図示しない入力部の操作によって入力する。

【００４５】

センタシステム１のサーバ３ａのＣＰＵ３１は、その入力されたメンテナンス情報を通信アダプタ２１へ送信する。

なお、通信アダプタ２１より送られてくるＯＡ機器情報（不正なメンテナンス情報を含む）を受信した場合に、次のような処理を行うこともできる。つまり、受信したＯＡ機器情報に対応するＨＤＤ（ＤＢ）３７内の機器情報をそのＯＡ機器情報中のメンテナンス情報以外の情報（ＭＩＢ情報等）に基づいて検索する処理を行い、その機器情報が既に登録（記憶）されていれば、通信アダプタ２１へ送信すべき正しいメンテナンス情報（メンテナンス用機器情報（遠隔管理用機種番号）を含む）を自動的に決定する。

【００４６】

通信アダプタ２１のＣＰＵ４４は、センタシステム１へのＯＡ機器情報の送信に対して、そのセンタシステム１からメンテナンス情報を受信した場合に、そのメンテナンス情報を含む変更要求を不正なメンテナンス情報が保持されているＯＡ機器へ送信する。

【００４７】

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれているメンテナンス情報（正しいメンテナンス情報）を不揮発性メモリに書き込む（不正なメンテナンス情報に上書きする）。例えば、不正なメンテナンス情報が保持されているＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１が正しいメンテナンス情報をＲＡＭ１０３（不揮発性ＲＡＭ）に書き込む。

【００４８】

なお、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングが「１日１回 ＡＭ０：００」、ネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングが「１週１回 日曜ＡＭ０：００」であるため、検索したＯＡ機器からメンテナンス情報等を取得するタイミングをネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングに合わせて「１週１回 日曜ＡＭ０：００」とすればよい。もし、検索したＯＡ機器からメンテナンス情報等を取得するタイミングをネットワークセグメントに接続されているＯＡ機器を検索するタイミングに合わせて「１日１回 ＡＭ０：００」とする場合には、このタイミングで取得するメンテナンス情報を含むＯＡ機器情報をＲＡＭ４６に記憶保持し、センタシステム１へ通知するタイミングで読み出すことになる。

【００４９】
このように、通信アダプタが、指定したネットワークセグメントに接続されているＯＡ機器を検索し、そのＯＡ機器よりそのＯＡ機器に保持されているメンテナンス用機器情報を取得し、そのメンテナンス用機器情報が正しいフォーマットであるか否かを判定し、その判定の結果、取得したメンテナンス用機器情報が正しいフォーマットでない場合（これはＯＡ機器の配置変更等によって発生する）に、そのメンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、そのメンテナンス用機器情報が保持されているＯＡ機器の機器情報をセンタシステム（管理装置）へ送信し、そのセンタシステムが、そのＯＡ機器の機器情報を受信した場合に、正しいメンテナンス用機器情報を通信アダプタへ送信し、そのメンテナンス用機器情報を受信した通信アダプタが、そのメンテナンス用機器情報を含む変更要求を不正なメンテナンス用機器情報が保持されているＯＡ機器へ送信してメンテナンス用機器情報の書き換え（変更）を行わせるので、顧客先のネットワークにおけるＯＡ機器の配置位置変更等によるＯＡ機器の遠隔機器管理の異常を早期に発見して、そのＯＡ機器のメンテナンス用機器情報の変更を行えることになる。したがって、顧客先のネットワーク管理者によるＯＡ機器の管理業務やメンテナンス担当者（サービスマン等）によるＯＡ機器のメンテナンス業務の負荷軽減につながる。

【００５０】
〔第２実施例〕
次に、第２実施例について説明する。
図８は、通信アダプタ２１が不正なメンテナンス情報が保持されているＯＡ機器の機器情報を表示（報知）する際の通信制御の一例を説明するための図である。
図９は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第２例を示すフローチャートである。

【００５１】
第２実施例の場合、通信アダプタ２１は、例えば図８に示したように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、更にユーザ認証を行うためにカードリーダ５１を備えている。
この通信アダプタ２１のＣＰＵ４４は、表示部４９（タッチパネルが重ねられているものとする）上の操作によってセグメント検索要求が発生すると、図９のフローチャートに記述しているように、ネットワーク２５に接続された複写機２３等のＯＡ機器のメンテナンスを行うために、外部から派遣されるメンテナンス担当者（サービスマン）は、通信アダプタ２１のカードリーダ５１を用いて（通信アダプタ２１に操作部があればそれを用いてもよい）ユーザ認証を実施する。

【００５２】
このとき、カードリーダ５１は、カード（カード挿入口に挿入されたＩＣカード又は読取部に近づいたＩＣカード等）に記録されているユーザ情報を読み取って入力し、そのユーザ情報を通信アダプタ２１に入力する。
通信アダプタ２１のＣＰＵ４４は、カードリーダ５１からユーザ情報が入力されると、そのユーザ情報を入力するための操作を行ったユーザを判別し、そのユーザが特殊権限ユーザであるメンテナンス担当者であった場合に、カードリーダ５１から入力されたユーザ情報（メンテナンス担当者のユーザ認証情報）を含むユーザ認証要求をＨＴＴＰＳによる暗号化通信にてセンタシステム１へ送信する。

【００５３】
センタシステム１のサーバ３ａのＣＰＵ３１は、通信アダプタ２１から送られてくるＨＴＴＰＳ通信によるユーザ認証要求を受信し、ユーザ認証を実施する。つまり、受信したユーザ認証要求中のユーザ情報をＨＤＤ３７（ＤＢ）内のユーザ認証情報（最新のメンテナンス担当者のユーザ認証情報）と照合し、その照合の結果、受信したユーザ認証要求中のユーザ情報と一致するユーザ認証情報がＨＤＤ３７内にあれば認証成功（認証ＯＫ）、一致するユーザ認証情報がなければ認証失敗（認証ＮＧ）と判定する。そして、認証成功と判定した場合には、その認証結果およびメンテナンス権限を含む認証結果情報を生成し

、ＨＴＴＰＳ通信にて通信アダプタ２１へ送信する。認証失敗と判定した場合には、その認証結果を含む認証結果情報を生成し、ＨＴＴＰＳ通信にて通信アダプタ２１へ送信する。また、認証結果を認証履歴としてＨＤＤ（ＤＢ）３７に蓄積する。

【００５４】

通信アダプタ２１のＣＰＵ４４は、センタシステム１へのユーザ認証要求の送信に対して、そのセンタシステム１から認証結果情報を受信した場合に、その認証結果情報中の認証結果を表示部４９上に表示する。また、その認証結果情報中の認証結果が認証成功を示すものである場合、メンテナンス担当者による画面操作を許可する。

メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上の操作により、メンテナンス対象とするネットワークセグメントを指定する。ここでは、ネットワークセグメントを「192.168.30.0　サブネットマスク255.255.255.0」とする。

【００５５】

通信アダプタ２１のＣＰＵ４４は、その指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。この機器検索の詳細は、第１実施例と同様である。

そして、指定されたネットワークセグメントに接続されているＯＡ機器を検索した場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由でその検索したＯＡ機器からそのＯＡ機器に保持されているメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてＲＡＭ４６に蓄積する。

【００５６】

具体的には、図９のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で検索したＯＡ機器より、そのＯＡ機器に保持されているメンテナンス用機器情報（遠隔管理用機種番号）を含むメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。そして、管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報に関して、メンテナンス用機器情報（遠隔管理用機種番号）のフォーマットをチェックし、そのメンテナンス用機器情報が正しいフォーマットであるか否かを判定する。この判定の詳細は、第１実施例と同様である。

【００５７】

メンテナンス用機器情報のフォーマットのチェック（判定）の結果、メンテナンス用機器情報が正しいフォーマットでない場合に、そのメンテナンス用機器情報、つまりそれを含むメンテナンス情報を不正なメンテナンス情報と判断して、そのメンテナンス情報が保持されているＯＡ機器の機器情報（そのＯＡ機器から取得したメンテナンス情報およびＭＩＢ情報）をＲＡＭ４６に蓄積する。そして、そのＯＡ機器の機器情報（ＯＡ機器情報）を表示部４９の画面上に一覧表示させる。

【００５８】

それによって、メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上に一覧表示されたＯＡ機器情報を確認でき、正しいメンテナンス情報（メンテナンス用機器情報を含む）が判明した場合、それを表示部４９の画面上の操作によって入力する。

通信アダプタ２１のＣＰＵ４４は、その入力されたメンテナンス情報を含む変更要求を不正なメンテナンス情報が保持されているＯＡ機器へ送信する。

【００５９】

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれているメンテナンス情報（正しいメンテナンス情報）を不揮発性メモリに書き込む（不正なメンテナンス情報に上書きする）。例えば、不正なメンテナンス情報が保持されているＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１がメンテナンス情報をＲＡＭ１０３に書き込む。

【００６０】
このように、通信アダプタが、ユーザ認証情報を入力された場合に、そのユーザ認証情報からそのユーザ認証情報を入力するための操作を行ったユーザを判別し、そのユーザが特殊権限ユーザであった場合に、その特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求をセンタシステムへ送信し、そのユーザ認証要求を受信したセンタシステムが、そのユーザ認証要求中のユーザ認証情報をＤＢ内のユーザ認証情報（特殊権限ユーザのユーザ認証情報）と照合し、ＤＢに一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行い、その結果を通信アダプタへ送信し、その通信アダプタが、認証成功を示すユーザ認証結果を受信した場合に、指定したネットワークセグメントに接続されているＯＡ機器を検索し、そのＯＡ機器よりそのＯＡ機器に保持されているメンテナンス用機器情報を取得し、そのメンテナンス用機器情報が正しいフォーマットであるか否かを判定し、その判定の結果、取得したメンテナンス用機器情報が正しいフォーマットでない場合に、そのメンテナンス用機器情報を不正なメンテナンス用機器情報と判断して、不正なメンテナンス用機器情報が保持されているＯＡ機器の機器情報を報知した後、正しいメンテナンス用機器情報が入力された場合に、そのメンテナンス用機器情報を含む変更要求を不正なメンテナンス用機器情報が保持されているＯＡ機器へ送信してメンテナンス用機器情報の書き換えを行わせるので、第１実施例と同様の効果を得ることができる。また、センタシステムにおいて、メンテナンス担当者のユーザ認証を行うことにより、偽メンテナンス担当者の不正アクセスの検出、離職した過去の担当者の不正アクセスの阻止が可能となり、ＯＡ機器の安定稼動につながる。

【００６１】
〔第３実施例〕
次に、第３実施例について説明する。
通信アダプタ２１は、例えば図５に示したように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、管理対象とするネットワークセグメントは「192.168.30.0　サブネットマスク255.255.255.0」、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングは「１日１回　ＡＭ０：００」、ネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングは「１週１回 日曜ＡＭ０：００」と指定されている。また、ネットワークセグメントのＯＡ機器情報の変動を検出した場合、その変動したＯＡ機器情報をセンタシステム１へ通知するタイミングは「即時」と指定されている。

【００６２】
この通信アダプタ２１のＣＰＵ４４は、セグメント検索要求が発生すると、第１実施例と略同様の処理に加え、以下の処理も行う。つまり、検索したＯＡ機器からメンテナンス情報を取得する（そのタイミングは「１日１回　ＡＭ０：００」）際に、そのＯＡ機器の稼動情報，状態情報，設定情報等の機器使用情報も取得する。
そして、その取得した機器使用情報の状態変更を検出する処理を行い、その結果、該当するＯＡ機器（検索したＯＡ機器）の状態がメンテナンスが必要な状態に変動している場合（例えば故障等の異常が発生している場合）には、その旨を示す状態変動情報をセンタシステム１へ送信する。

【００６３】
センタシステム１のサーバ３ａのＣＰＵ３１は、通信アダプタ２１より送られてくる状態変動情報を受信し、それをＨＤＤ（ＤＢ）３７に蓄積する。そして、その状態変動情報を端末装置の表示部の画面上に表示させる。
それによって、オペレータは、端末装置の表示部の画面上に表示された状態変動情報を確認でき、メンテナンス担当者を手配する。
なお、通信アダプタ２１のＣＰＵ４４が、ネットワークセグメントのＯＡ機器情報の変動を検出し、その変動したＯＡ機器情報をセンタシステム１へ通知する処理は、第２実施例および第４実施例以降の各実施例に追加することもできる。

【００６４】
このように、通信アダプタが、検索したＯＡ機器よりそのＯＡ機器の稼動情報，状態情報，設定情報等の機器使用情報を含む機器情報を取得し、不正なメンテナンス用機器情報が保持されているＯＡ機器の機器情報として、その取得した機器情報をセンタシステムへ送信することにより、そのセンタシステムでは、ＯＡ機器の使用状況を把握できる。よって、ＯＡ機器の最適配置を行えるため、ＯＡ機器の運用効率の向上が図れる。
また、通信アダプタが、検索したＯＡ機器より取得した機器情報に基づいてそのＯＡ機器の状態変更を検出する処理を行い、そのＯＡ機器の状態がメンテナンスが必要な状態（故障状態等の異常状態）に変動した場合に、その旨を示す情報をセンタシステムへ送信することにより、メンテナンス担当者を手配するため、顧客先のネットワーク管理者によるＯＡ機器の管理業務の一層の負荷軽減につながる。
【００６５】
〔第４実施例〕
次に、第４実施例について説明する。
図１０は、通信アダプタ２１が不正な証明書情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の一例を説明するための図である。
図１１は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第３例を示すフローチャートである。
【００６６】
通信アダプタ２１は、例えば図１０に示すように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、管理対象とするネットワークセグメントは「192.168.30.0　サブネットマスク255.255.255.0」、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングは「１日１回　ＡＭ０：００」、ネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングは「１週１回　日曜ＡＭ０：００」と指定されている。
【００６７】
この通信アダプタ２１のＣＰＵ４４は、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングになり、その検索の要求（セグメント検索要求）が発生すると、指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、任意のタイミング「１日１回　ＡＭ０：００」でのセグメント検索要求の発生によって機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。この機器検索の詳細は、第１実施例と同様である。
【００６８】
そして、指定されたネットワークセグメントに接続されているＯＡ機器を検索した場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由でその検索したＯＡ機器からそのＯＡ機器に保持されているメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてセンタシステム１へ送信する。
【００６９】
具体的には、図１１のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で検索したＯＡ機器より、そのＯＡ機器に保持されているメンテナンス用機器情報（遠隔管理用機種番号）を含むメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。これらの情報の取得は、暗号化通信を利用して行う。このとき、この暗号化通信に用いる相互認証用証明書（以下単に「証明書」ともいう）の不正を検出する処理を行う。
【００７０】
そして、証明書の不正を検出する処理の結果、該当するＯＡ機器（検索したＯＡ機器）

の証明書がない（相互認証ができない）場合、もしくはその証明書が個別証明書ではなく共通証明書であった場合に、証明書の不正として検出して、該当するＯＡ機器の機器情報（ＯＡ機器の証明書がない旨を示す証明書異常情報や共通証明書を含む）を不正なＯＡ機器情報としてセンタシステム１へ送信する。

【００７１】

センタシステム１のサーバ３ａのＣＰＵ３１は、通信アダプタ２１より送られてくるＯＡ機器情報（顧客サイトＢにおけるネットワークセグメントに接続されている証明書が不正なＯＡ機器の機器情報）を受信し、それをＨＤＤ（ＤＢ）３７に蓄積する。そして、そのＯＡ機器情報を図示しない端末装置の表示部の画面上に一覧表示させる。

それによって、オペレータは、端末装置の表示部の画面上に一覧表示されたＯＡ機器情報を確認でき、正しい個別証明書が判明した場合、それを画面上の操作又は図示しない入力部の操作によって入力する。

【００７２】

センタシステム１のサーバ３ａのＣＰＵ３１は、その入力された個別証明書を通信アダプタ２１へ送信する。

なお、通信アダプタ２１より送られてくるＯＡ機器情報（ＯＡ機器の証明書がない旨を示す証明書異常情報や共通証明書を含む）を受信した場合に、次のような処理を行うこともできる。つまり、受信したＯＡ機器情報に対応するＨＤＤ（ＤＢ）３７内の機器情報をそのＯＡ機器情報中のＭＩＢ情報等に基づいて検索する処理を行い、その機器情報が既に登録されていれば、通信アダプタ２１へ送信すべき正しい個別証明書を自動的に決定する。

【００７３】

通信アダプタ２１のＣＰＵ４４は、センタシステム１へのＯＡ機器情報の送信に対して、そのセンタシステム１から個別証明書を受信した場合に、その個別証明書を含む変更要求を証明書が不正なＯＡ機器へ送信する。

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれている個別証明書（正しい個別証明書）を不揮発性メモリに書き込む。例えば、証明書が不正なＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１が正しい個別証明書をＲＡＭ１０３に書き込む。

【００７４】

このように、指定したネットワークセグメントに接続されているＯＡ機器を検索し、そのＯＡ機器よりそのＯＡ機器の機器情報を暗号化通信によって取得すると共に、その機器情報取得時の暗号化通信に用いる証明書（相互認証用証明書）の不正を検出する処理を行い、証明書の不正を検出した場合に、その時に取得したＯＡ機器の機器情報を不正な機器情報としてセンタシステムへ送信し、その管理装置が、その機器情報を受信した場合に、正しい機器個別証明書を通信アダプタへ送信し、その機器個別証明書を受信した通信アダプタが、その機器個別証明書を含む変更要求を証明書が不正なＯＡ機器へ暗号化通信によって送信して機器個別証明書の書き換えを行わせるので、第１実施例と同様の効果を得ることができる。

【００７５】

〔第５実施例〕

次に、第５実施例について説明する。

図１２は、通信アダプタ２１が不正な証明書情報を含むＯＡ機器情報を表示（報知）する際の通信制御の一例を説明するための図である。

図１３は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第４例を示すフローチャートである。

【００７６】

第５実施例の場合、通信アダプタ２１は、例えば図１２に示したように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、更にユーザ認証を行うためにカードリーダ５１を備えている。

この通信アダプタ２１のＣＰＵ４４は、表示部４９（タッチパネルが重ねられているものとする）上の操作によってセグメント検索要求が発生すると、図１３のフローチャートに記述しているように、ネットワーク２５に接続された複写機２３等のＯＡ機器のメンテナンスを行うために、外部から派遣されるメンテナンス担当者は、通信アダプタ２１のカードリーダ５１を用いて（通信アダプタ２１に操作部があればそれを用いてもよい）ユーザ認証を実施する。

【００７７】

以後、センタシステム１から認証結果情報を受信して、その認証結果情報中の認証結果を表示部４９上に表示すると共に、その認証結果情報中の認証結果が認証成功を示すものである場合、メンテナンス担当者による画面操作を許可するまでの処理は、第２実施例と同様である。

メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上の操作により、メンテナンス対象とするネットワークセグメントを指定する。ここでは、ネットワークセグメントを「192.168.30.0　サブネットマスク255.255.255.0」とする。

【００７８】

通信アダプタ２１のＣＰＵ４４は、その指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。この機器検索の詳細は、第１実施例と同様である。

そして、指定されたネットワークセグメントに接続されているＯＡ機器を検索した場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由でその検索したＯＡ機器からそのＯＡ機器に保持されているメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてＲＡＭ４６に蓄積する。

【００７９】

具体的には、図１３のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で検索したＯＡ機器より、そのＯＡ機器に保持されているメンテナンス用機器情報（遠隔管理用機種番号）を含むメンテナンス情報（遠隔管理用機種番号，モデル名，機種番号，機番）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。これらの情報の取得は、暗号化通信を利用して行う。このとき、この暗号化通信に用いる証明書（相互認証用証明書）の不正を検出する処理を行う。

【００８０】

そして、証明書の不正を検出する処理の結果、該当するＯＡ機器（検索したＯＡ機器）の証明書がない（相互認証ができない）場合、もしくはその証明書が個別証明書ではなく共通証明書であった場合に、証明書の不正として検出して、該当するＯＡ機器の機器情報（ＯＡ機器の証明書がない旨を示す証明書異常情報や共通証明書を含む）を不正なＯＡ機器情報としてＲＡＭ４６に蓄積する。そして、そのＯＡ機器の機器情報（ＯＡ機器情報）を表示部４９の画面上に一覧表示させる。

【００８１】

それによって、メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上に一覧表示されたＯＡ機器情報を確認でき、正しい個別証明書が判明した場合、それを表示部４９の画面上の操作によって入力する。

通信アダプタ２１のＣＰＵ４４は、その入力された個別証明書を含む変更要求を証明書が不正なＯＡ機器へ送信する。

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれている個別証明書（正しい個別証明書）を不揮発性メモリに書き込む。例えば、証明書が不正なＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１が正しい個別証明書をＲＡＭ１０３に書き込む。

【００８２】
このように、通信アダプタが、ユーザ認証情報を入力された場合に、そのユーザ認証情報からそのユーザ認証情報を入力するための操作を行ったユーザを判別し、そのユーザが特殊権限ユーザであった場合に、その特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求をセンタシステムへ送信し、そのユーザ認証要求を受信したセンタシステムが、そのユーザ認証要求中のユーザ認証情報をＤＢ内のユーザ認証情報（特殊権限ユーザのユーザ認証情報）と照合し、ＤＢに一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行い、その結果を通信アダプタへ送信し、その通信アダプタが、認証成功を示すユーザ認証結果を受信した場合に、指定したネットワークセグメントに接続されているＯＡ機器を検索し、そのＯＡ機器よりそのＯＡ機器の機器情報を暗号化通信によって取得すると共に、その機器情報取得時の暗号化通信に用いる証明書の不正を検出する処理を行い、証明書の不正を検出した場合に、その時に取得したＯＡ機器の機器情報を不正な機器情報として報知した後、正しい機器個別証明書が入力された場合に、その機器個別証明書を含む変更要求を証明書が不正なＯＡ機器へ暗号化通信によって送信して機器個別証明書の書き換えを行わせるので、第２実施例と同様の効果を得ることができる。

【００８３】
〔第６実施例〕
次に、第６実施例について説明する。
図１４は、通信アダプタ２１が不正な遠隔機器管理用機器情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の一例を説明するための図である。
図１５は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第５例を示すフローチャートである。

【００８４】
通信アダプタ２１は、例えば図１４に示すように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、管理対象とするネットワークセグメントは「192.168.30.0　サブネットマスク255.255.255.0」、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングは「１日１回　ＡＭ０：００」、ネットワークセグメントのＯＡ機器情報をセンタシステム１へ通知するタイミングは「１週１回　日曜ＡＭ０：００」と指定されている。

【００８５】
この通信アダプタ２１のＣＰＵ４４は、ネットワークセグメントに接続されているＯＡ機器を検索するタイミングになり、その検索の要求（セグメント検索要求）が発生すると、指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、任意のタイミング「１日１回　ＡＭ０：００」でのセグメント検索要求の発生によって機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。この機器検索の詳細は、第１実施例と同様である。

【００８６】
そして、指定されたネットワークセグメントに接続されているＯＡ機器を検索した場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由でその検索したＯＡ機器からそのＯＡ機器に保持されている当該通信アダプタ２１の遠隔機器管理用機器情報（ＩＰアドレス等）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてセンタシステム１へ送信する。

【００８７】
具体的には、図１５のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で該当するＯＡ機器（検索したＯＡ機器）より、そのＯＡ機器に保持されている当該通信アダプタ２１の遠隔機器管理用機器情報（ＩＰアドレス等）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。そして、管理対象としたネットワークセグメントに接続されているＯＡ機

器の機器情報に関して、取得した遠隔機器管理用機器情報よりその機器登録状態をチェックし、その機器登録状態をＲＡＭ４６に予め記憶保持されている機器登録状態（当該通信アダプタ２１の遠隔機器管理用機器情報の機器登録状態）と照合して、両機器登録状態が一致するか否かを判定する。

【００８８】

その判定の結果、両機器登録状態が一致しない場合（機器登録状態が正しくない場合）に、取得した遠隔機器管理用機器情報が不正な遠隔機器管理用機器情報と判断して、その遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報（そのＯＡ機器から取得した当該通信アダプタ２１の遠隔機器管理用機器情報およびＭＩＢ情報を含むＯＡ機器情報）をセンタシステム１へ送信する。

【００８９】

センタシステム１のサーバ３ａのＣＰＵ３１は、通信アダプタ２１より送られてくるＯＡ機器情報（顧客サイトＢにおけるネットワークセグメントに接続されている不正な遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報）を受信し、それをＨＤＤ（ＤＢ）３７に蓄積する。そして、そのＯＡ機器情報を端末装置の表示部の画面上に一覧表示させる。

それによって、オペレータは、端末装置の表示部の画面上に一覧表示されたＯＡ機器情報を確認でき、通信アダプタ２１の正しい機器登録状態の遠隔機器管理用機器情報（ＩＰアドレス等）が判明した場合、それを画面上の操作又は図示しない入力部の操作によって入力する。

【００９０】

センタシステム１のサーバ３ａのＣＰＵ３１は、その入力された遠隔機器管理用機器情報を通信アダプタ２１へ送信する。

なお、通信アダプタ２１より送られてくるＯＡ機器情報（不正な遠隔機器管理用機器情報を含む）を受信した場合に、次のような処理を行うこともできる。つまり、受信したＯＡ機器情報に対応するＨＤＤ（ＤＢ）３７内の機器情報をそのＯＡ機器情報中のＭＩＢ情報等に基づいて検索する処理を行い、その機器情報が既に登録されていれば、通信アダプタ２１へ送信すべき正しい登録状態の遠隔機器管理用機器情報を自動的に決定する。

【００９１】

通信アダプタ２１のＣＰＵ４４は、センタシステム１へのＯＡ機器情報の送信に対して、そのセンタシステム１から当該通信アダプタ２１の遠隔機器管理用機器情報を受信した場合に、その遠隔機器管理用機器情報を含む変更要求を該当するＯＡ機器へ送信する。

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれている遠隔機器管理用機器情報（通信アダプタ２１の正しい遠隔機器管理用機器情報）を不揮発性メモリに書き込む（不正な遠隔機器管理用機器情報に上書きする）。例えば、不正な遠隔機器管理用機器情報が保持されているＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１が正しい遠隔機器管理用機器情報をＲＡＭ１０３に書き込む。

【００９２】

このように、通信アダプタが、指定したネットワークセグメントに接続されているＯＡ機器を検索し、その検索したＯＡ機器よりそのＯＡ機器に保持されている遠隔機器管理用機器情報を取得し、その遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定し、その判定の結果、取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、その遠隔機器管理用機器情報を不正な遠隔機器管理用機器情報と判断して、その遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報をセンタシステムへ送信し、そのセンタシステムが、そのＯＡ機器の機器情報を受信した場合に、正しい遠隔機器管理用機器情報を通信アダプタへ送信し、その遠隔機器管理用機器情報を受信した通信アダプタが、その遠隔機器管理用機器情報を含む変更要求を不正な遠隔機器管理用機器情報が保持されているＯＡ機器へ送信して遠隔機器管理用機器情報の書き換えを行わせるので、第１実施例と同様の効果を得ることができる。

【００９３】
〔第７実施例〕
次に、第７実施例について説明する。
図１６は、通信アダプタ２１が不正な遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報を表示（報知）する際の通信制御の一例を説明するための図である。
図１７は、通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第６例を示すフローチャートである。
【００９４】
第７実施例の場合、通信アダプタ２１は、例えば図１６に示したように、複数のネットワークセグメントを構築している顧客サイトＢに設置されており、更にユーザ認証を行うためにカードリーダ５１を備えている。
この通信アダプタ２１のＣＰＵ４４は、表示部４９（タッチパネルが重ねられているものとする）上の操作によってセグメント検索要求が発生すると、図１７のフローチャートに記述しているように、ネットワーク２５に接続された複写機２３等のＯＡ機器のメンテナンスを行うために、外部から派遣されるメンテナンス担当者は、通信アダプタ２１のカードリーダ５１を用いて（通信アダプタ２１に操作部があればそれを用いてもよい）ユーザ認証を実施する。
【００９５】
以後、センタシステム１から認証結果情報を受信して、その認証結果情報中の認証結果を表示部４９上に表示すると共に、その認証結果情報中の認証結果が認証成功を示すものである場合、メンテナンス担当者による画面操作を許可するまでの処理は、第２実施例と同様である。
メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上の操作により、メンテナンス対象とするネットワークセグメントを指定する。ここでは、ネットワークセグメントを「192.168.30.0　サブネットマスク255.255.255.0」とする。
【００９６】
通信アダプタ２１のＣＰＵ４４は、その指定されたネットワークセグメント「192.168.30.0　サブネットマスク255.255.255.0」に対して、機器検索（ネットワークセグメントに接続されているＯＡ機器の検索）を実施する。この機器検索の詳細は、第１実施例と同様である。
そして、指定されたネットワークセグメントに接続されているＯＡ機器を検索した場合、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由でその検索したＯＡ機器からそのＯＡ機器に保持されている当該通信アダプタ２１の遠隔機器管理用機器情報（ＩＰアドレス等）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（例えば「printerMIB情報」）も取得して、それらの情報を管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報（ＯＡ機器情報）としてＲＡＭ４６に蓄積する。
【００９７】
具体的には、図１７のフローチャートに記述しているように、ＨＴＴＰＳによるＷｅｂサービスが提供されているなら、このＩ／Ｆ経由で該当するＯＡ機器（検索したＯＡ機器）より、そのＯＡ機器に保持されている当該通信アダプタ２１の遠隔機器管理用機器情報（ＩＰアドレス等）を取得し、更にＳＮＭＰにより他のＭＩＢ情報（「printerMIB情報」）を取得する。そして、管理対象としたネットワークセグメントに接続されているＯＡ機器の機器情報に関して、取得した遠隔機器管理用機器情報よりその機器登録状態をチェックし、その機器登録状態をＲＡＭ４６に予め記憶保持されている機器登録状態（当該通信アダプタ２１の遠隔機器管理用機器情報の機器登録状態）と照合して、両機器登録状態が一致するか否かを判定する。
【００９８】
その判定の結果、両機器登録状態が一致しない場合（機器登録状態が正しくない場合）に、取得した遠隔機器管理用機器情報が不正な遠隔機器管理用機器情報と判断して、その遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報（そのＯＡ機器から取得し

た当該通信アダプタ２１の遠隔機器管理用機器情報およびＭＩＢ情報を含むＯＡ機器情報）をＲＡＭ４６に蓄積する。そして、そのＯＡ機器情報を表示部４９の画面上に一覧表示させる。

【００９９】

それによって、メンテナンス担当者は、通信アダプタ２１の表示部４９の画面上に一覧表示されたＯＡ機器情報を確認でき、通信アダプタ２１の正しい機器登録状態の遠隔機器管理用機器情報（ＩＰアドレス等）が判明した場合、それを表示部４９の画面上の操作によって入力する。

通信アダプタ２１のＣＰＵ４４は、その入力された遠隔機器管理用機器情報を含む変更要求を該当するＯＡ機器へ送信する。

【０１００】

そのＯＡ機器のＣＰＵは、その変更要求を受信し、それに含まれている遠隔機器管理用機器情報（通信アダプタ２１の正しい遠隔機器管理用機器情報）を不揮発性メモリに書き込む。例えば、不正な遠隔機器管理用機器情報が保持されているＯＡ機器が複写機２３の場合には、その複写機２３のＣＰＵ１０１が正しい遠隔機器管理用機器情報をＲＡＭ１０３に書き込む。

【０１０１】

このように、通信アダプタが、ユーザ認証情報を入力された場合に、そのユーザ認証情報からそのユーザ認証情報を入力するための操作を行ったユーザを判別し、そのユーザが特殊権限ユーザであった場合に、その特殊権限ユーザの操作によって入力されたユーザ認証情報を含むユーザ認証要求をセンタシステムへ送信し、そのユーザ認証要求を受信したセンタシステムが、そのユーザ認証要求中のユーザ認証情報をＤＢ内のユーザ認証情報（特殊権限ユーザのユーザ認証情報）と照合し、ＤＢに一致するユーザ認証情報があれば認証成功、一致するユーザ認証情報がなければ認証失敗と判定するユーザ認証を行い、その結果を通信アダプタへ送信し、その通信アダプタが、認証成功を示すユーザ認証結果を受信した場合に、指定したネットワークセグメントに接続されているＯＡ機器を検索し、そのＯＡ機器よりそのＯＡ機器に保持されている遠隔機器管理用機器情報を取得し、その遠隔機器管理用機器情報を当該通信アダプタの遠隔機器管理用機器情報と照合して、両遠隔機器管理用機器情報が一致するか否かを判定し、その判定の結果、取得した遠隔機器管理用機器情報が当該通信アダプタの遠隔機器管理用機器情報と一致しない場合に、その遠隔機器管理用機器情報を不正な遠隔機器管理用機器情報と判断して、その遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報を報知した後、正しい遠隔機器管理用機器情報が入力された場合に、その遠隔機器管理用機器情報を含む変更要求を不正な遠隔機器管理用機器情報が保持されているＯＡ機器へ送信して遠隔機器管理用機器情報の書き換えを行わせるので、第２実施例と同様の効果を得ることができる。

【産業上の利用可能性】

【０１０２】

以上の説明から明らかなように、この発明によれば、電子機器の配置位置の変更等による電子機器の遠隔機器管理の異常を早期に発見し、ネットワーク管理者による管理業務やメンテナンス担当者によるメンテナンス業務の負荷軽減を実現することができる。したがって、業務効率のよい遠隔機器管理システムを提供することができる。

【図面の簡単な説明】

【０１０３】

【図１】この発明による遠隔機器管理システムの構成例を示すブロック図である。

【図２】図１のサーバ３ａの構成例を示すブロック図である。

【図３】図１の通信アダプタ２１の構成例を示すブロック図である。

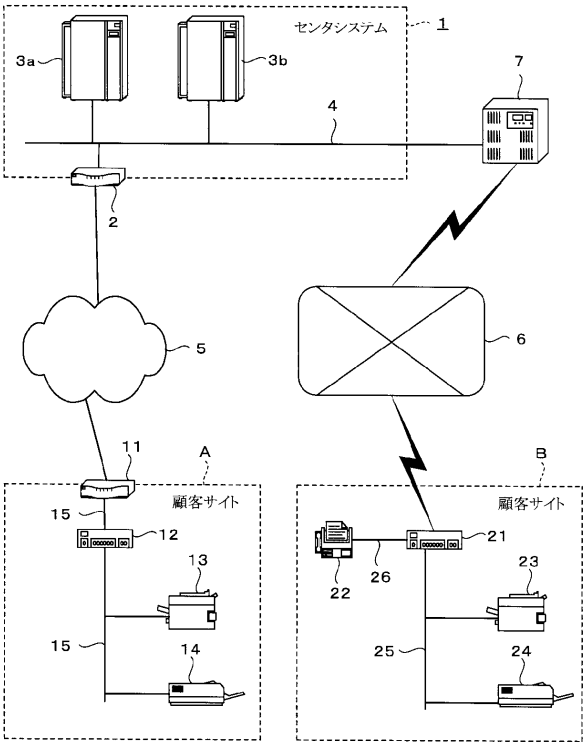
【図４】図１の複写機１３，２３の制御系の構成例を示すブロック図である。

【図５】図１の通信アダプタ２１が不正なメンテナンス情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の第１例を説明するための図である。

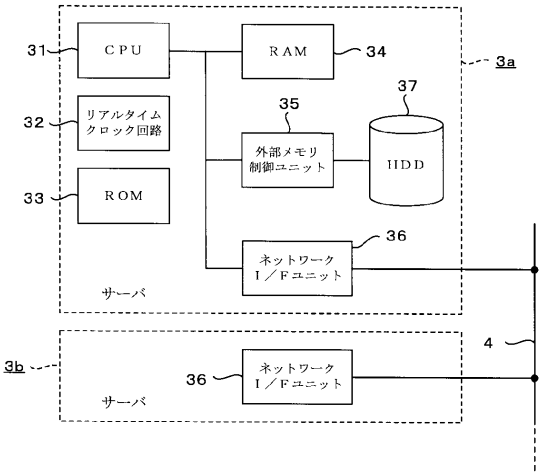
【０１０４】

【図６】図１の通信アダプタ２１が不正なメンテナンス情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の第２例を説明するための図である。
【図７】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第１例を示すフロー図である。
【図８】図１の通信アダプタ２１が不正なメンテナンス情報が保持されているＯＡ機器の機器情報を表示する際の通信制御の一例を説明するための図である。
【図９】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第２例を示すフロー図である。
【図１０】図１の通信アダプタ２１が不正な証明書情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の一例を説明するための図である。
【０１０５】
【図１１】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第３例を示すフロー図である。
【図１２】図１の通信アダプタ２１が不正な証明書情報を含むＯＡ機器情報を表示する際の通信制御の一例を説明するための図である。
【図１３】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第４例を示すフロー図である。
【図１４】図１の通信アダプタ２１が不正な遠隔機器管理用機器情報を含むＯＡ機器情報をセンタシステム１へ通知する際の通信制御の一例を説明するための図である。
【図１５】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第５例を示すフロー図である。
【０１０６】
【図１６】図１の通信アダプタ２１が不正な遠隔機器管理用機器情報が保持されているＯＡ機器の機器情報を表示する際の通信制御の一例を説明するための図である。
【図１７】図１の通信アダプタ２１でセグメント検索要求が発生した時の通信アダプタ２１とセンタシステム１との通信制御の第６例を示すフロー図である。
【符号の説明】
【０１０７】
１：センタシステム（中央管理装置）　２，１１：ルータ　３ａ，３ｂ：サーバ
４，１５，２５：ネットワーク　５：インタネット　６：公衆通信回線網
７：アクセスポイント　１２，２１：通信アダプタ
１３，２３，２３１，２３２，２３３：複写機
１４，２４，２４１，２４２，２４３：プリンタ　２２：ファクシミリ装置
２６：専用Ｉ／Ｆ　３１，４４，１０１：ＣＰＵ　３２：リアルタイムクロック回路
３５：外部メモリ制御ユニット　３６，４３，１１０：ネットワークＩ／Ｆユニット
３７：ハードディスク装置　４１：回線切替回路　４２：モデム　４７：電池
４９：表示部　５１：カードリーダ　１１１：操作部

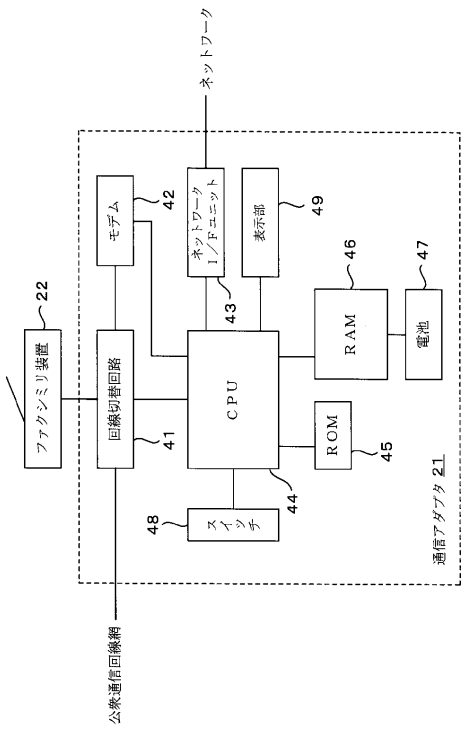
【図１】


センタシステム
1
3a
3b
4
7
2
5
6
11
A
B
顧客サイト
顧客サイト
15
12
13
15
14
22
26
21
23
25
24

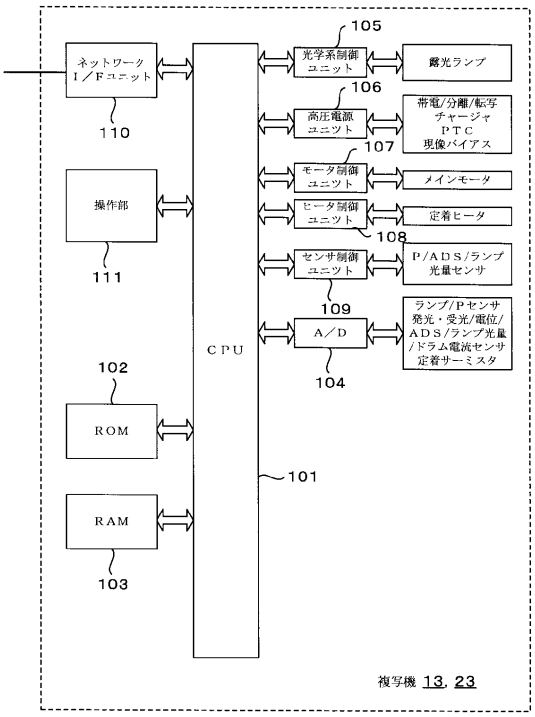
【図２】


31
CPU
RAM
34
3a
32
リアルタイム
クロック回路
35
37
外部メモリ
制御ユニット
HDD
33
ROM
36
ネットワーク
I／Fユニット
サーバ
4
3b
36
ネットワーク
I／Fユニット
サーバ

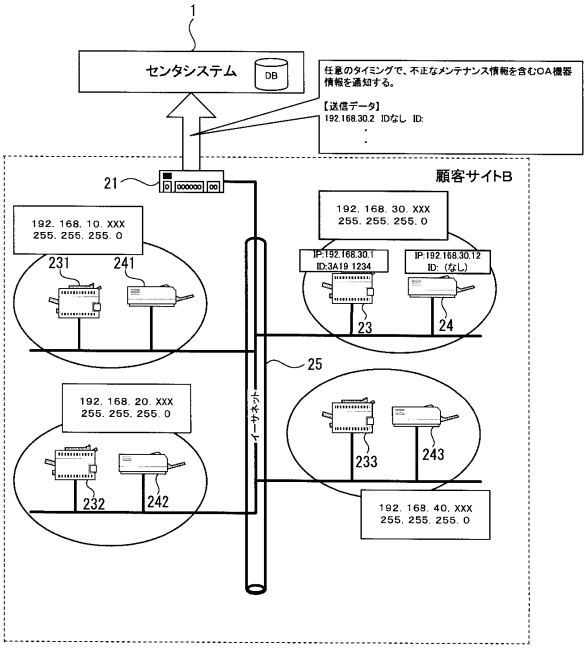
【図３】


ネットワーク
22
ファクシミリ装置
モデム
42
ネットワーク
I／Fユニット
43
表示部
49
46
47
RAM
電池
回線切替回路
41
CPU
ROM
45
44
48
スピーカ
通信アダプタ 21
公衆通信回線網

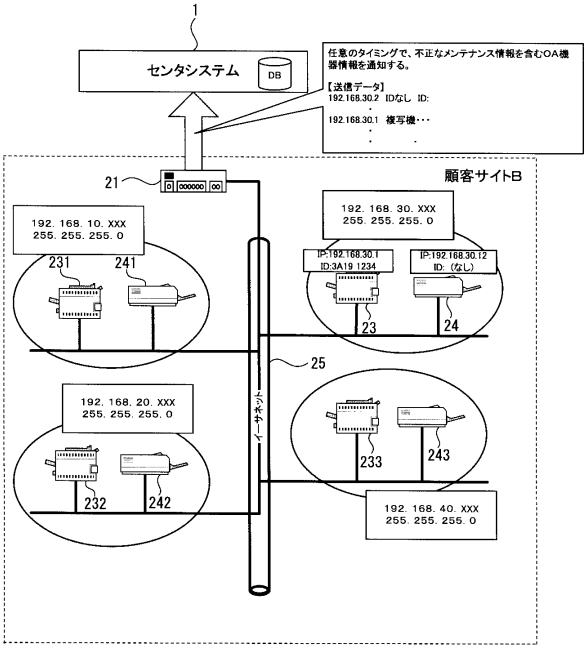
【図４】


105
ネットワーク
I／Fユニット
光学系制御
ユニット
露光ランプ
106
高圧電源
ユニット
帯電/分離/転写
チャージャ
PTC
現像バイアス
110
107
モータ制御
ユニット
メインモータ
操作部
ヒータ制御
ユニット
定着ヒータ
108
センサ制御
ユニット
P/ADS/ランプ
光量センサ
111
109
A／D
ランプ/Pセンサ
発光・受光/電位/
ADS/ランプ光量
/ドラム電流センサ
定着サーミスタ
104
CPU
102
ROM
101
RAM
103
複写機 13, 23

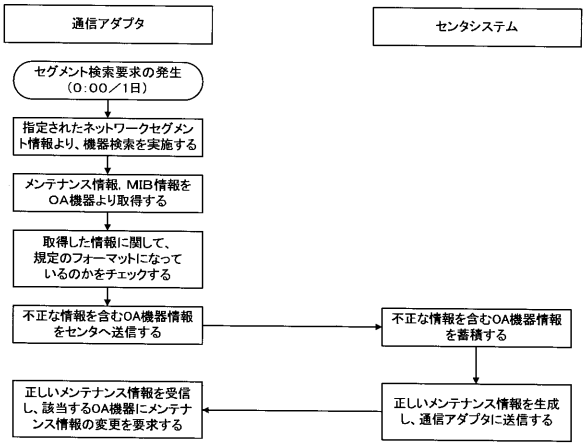
【図５】


1
センタシステム
DB
任意のタイミングで、不正なメンテナンス情報を含むOA機器情報を通知する。
【送信データ】
192.168.30.2 IDなし ID:
21
顧客サイトB
192. 168. 10. XXX
255. 255. 255. 0
231
241
192. 168. 30. XXX
255. 255. 255. 0
IP:192.168.30.1
ID:3A19 1234
IP:192.168.30.12
ID:（なし）
23
24
25
192. 168. 20. XXX
255. 255. 255. 0
232
242
233
243
192. 168. 40. XXX
255. 255. 255. 0
イーサネット

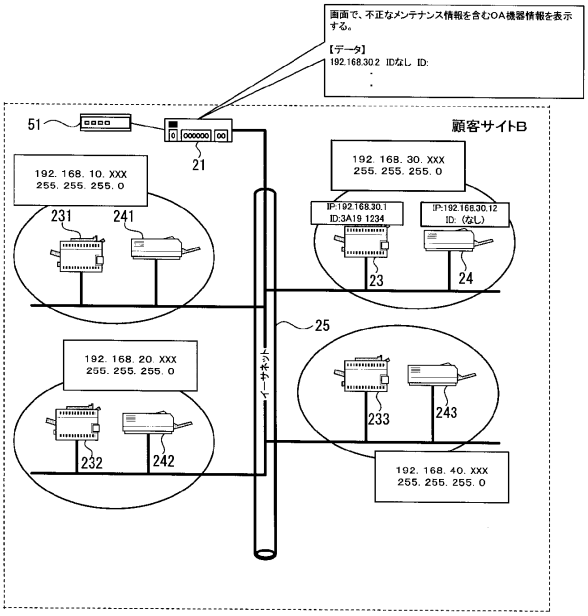
【図６】


1
センタシステム
DB
任意のタイミングで、不正なメンテナンス情報を含むOA機器情報を通知する。
【送信データ】
192.168.30.2 IDなし ID:
192.168.30.1 複写機・・・
21
顧客サイトB
192. 168. 10. XXX
255. 255. 255. 0
231
241
192. 168. 30. XXX
255. 255. 255. 0
IP:192.168.30.1
ID:3A19 1234
IP:192.168.30.12
ID:（なし）
23
24
25
192. 168. 20. XXX
255. 255. 255. 0
232
242
233
243
192. 168. 40. XXX
255. 255. 255. 0
イーサネット

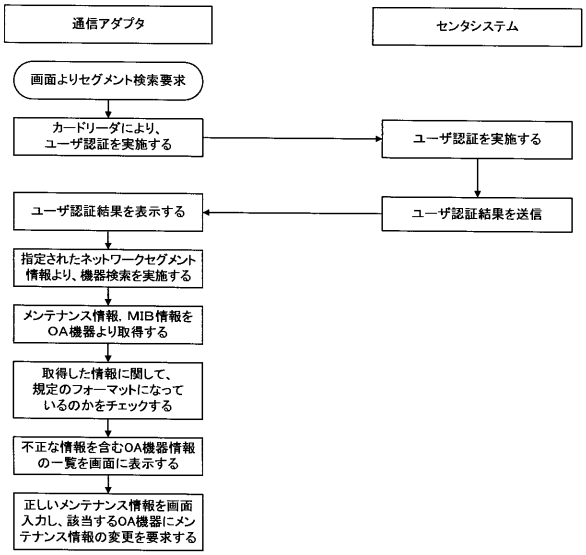
【図７】


通信アダプタ
センタシステム
セグメント検索要求の発生
（0:00／1日）
指定されたネットワークセグメント情報より、機器検索を実施する
メンテナンス情報，MIB情報をOA機器より取得する
取得した情報に関して、規定のフォーマットになっているのかをチェックする
不正な情報を含むOA機器情報をセンタへ送信する
不正な情報を含むOA機器情報を蓄積する
正しいメンテナンス情報を生成し、通信アダプタに送信する
正しいメンテナンス情報を受信し、該当するOA機器にメンテナンス情報の変更を要求する

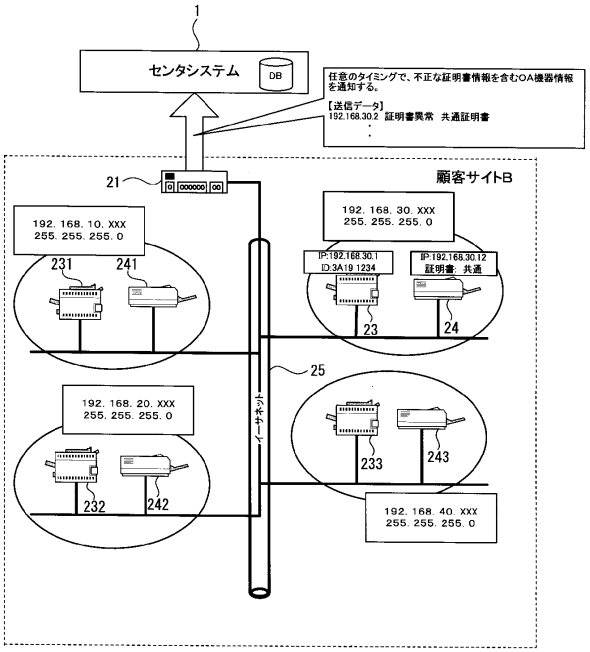
【図８】


画面で、不正なメンテナンス情報を含むOA機器情報を表示する。
【データ】
192.168.30.2 IDなし ID:
51
21
顧客サイトB
192. 168. 10. XXX
255. 255. 255. 0
231
241
192. 168. 30. XXX
255. 255. 255. 0
IP:192.168.30.1
ID:3A19 1234
IP:192.168.30.12
ID:（なし）
23
24
25
192. 168. 20. XXX
255. 255. 255. 0
232
242
233
243
192. 168. 40. XXX
255. 255. 255. 0
イーサネット

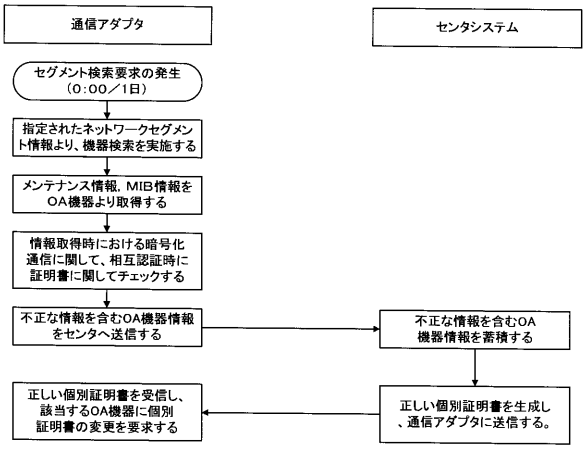
【図９】



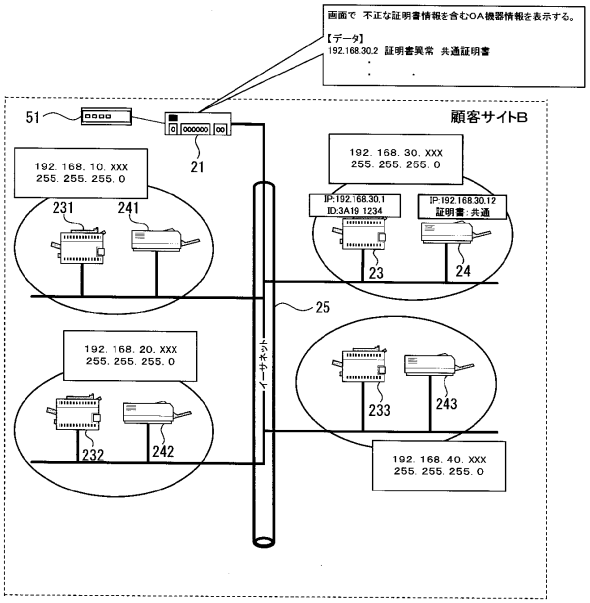
【図１０】



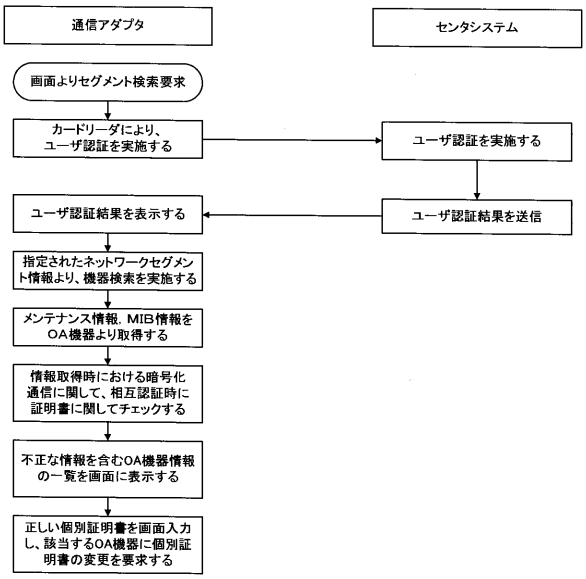
【図１１】



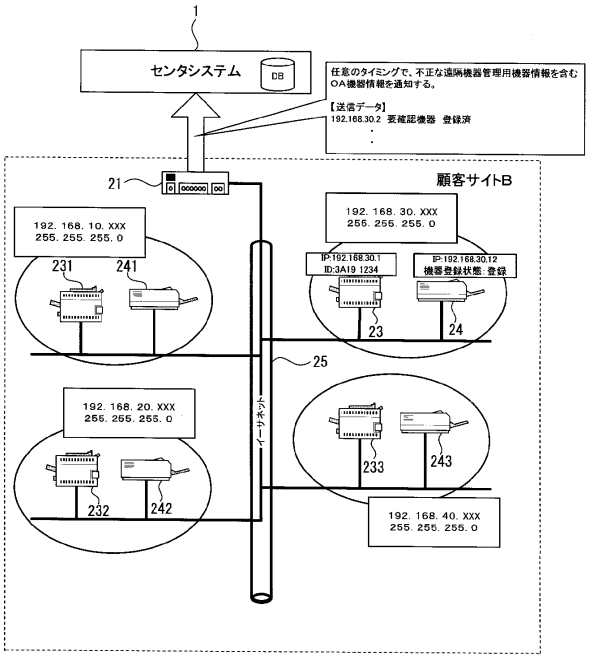
【図１２】



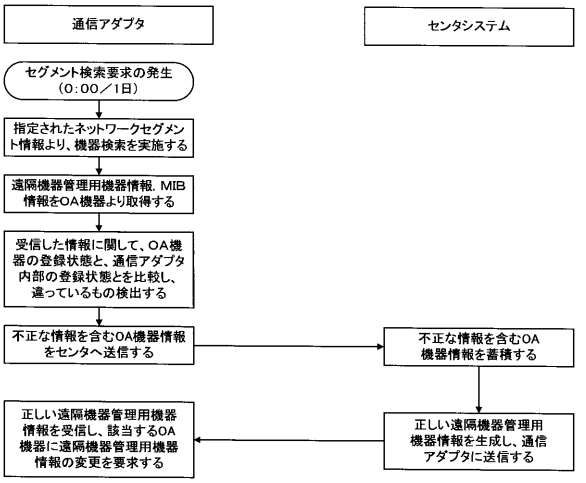
【図１３】



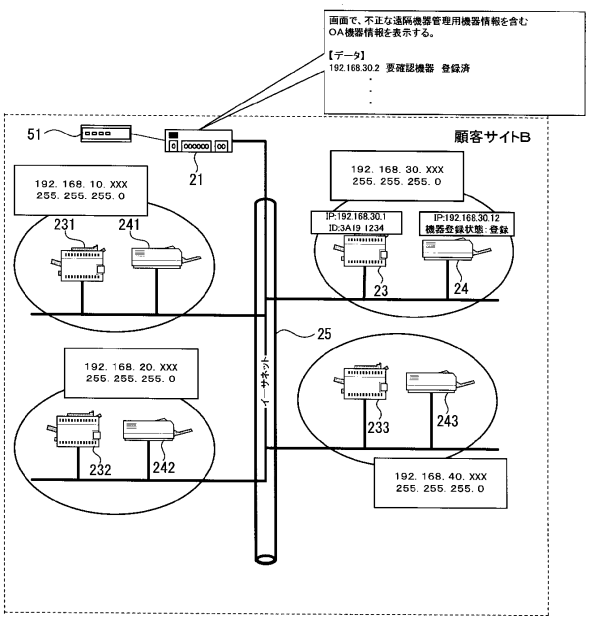
【図１４】



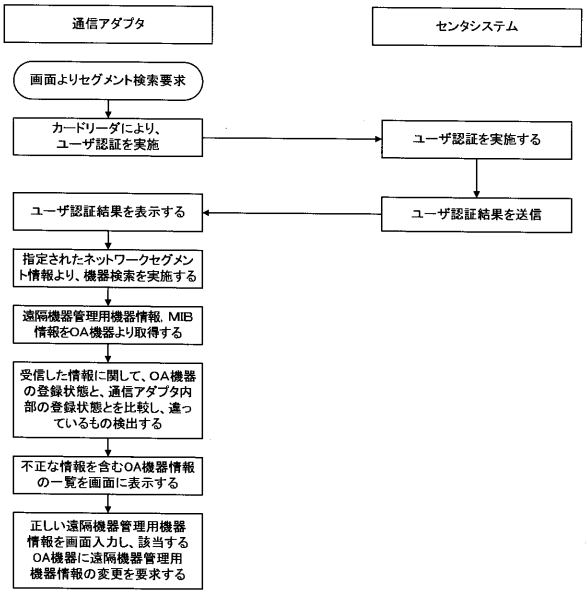
【図１５】



【図１６】



【図１７】


通信アダプタ
センタシステム
画面よりセグメント検索要求
カードリーダにより、ユーザ認証を実施
ユーザ認証を実施する
ユーザ認証結果を送信
ユーザ認証結果を表示する
指定されたネットワークセグメント情報より、機器検索を実施する
遠隔機器管理用機器情報, MIB情報をOA機器より取得する
受信した情報に関して、OA機器の登録状態と、通信アダプタ内部の登録状態とを比較し、違っているもの検出する
不正な情報を含むOA機器情報の一覧を画面に表示する
正しい遠隔機器管理用機器情報を画面入力し、該当するOA機器に遠隔機器管理用機器情報の変更を要求する

フロントページの続き

(56)参考文献 特開２００６－３４０２３９（ＪＰ，Ａ）
特開２００２－０３２２３８（ＪＰ，Ａ）
特開２００６－２８５９５１（ＪＰ，Ａ）
特開２００５－２８４９８５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　３／１２
Ｇ０３Ｇ　２１／００
Ｇ０３Ｇ　２１／０４
Ｈ０４Ｍ　１１／００
Ｈ０４Ｎ　１／００
Ｂ４１Ｊ　２９／３８