(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4791818号
(P4791818)
(45)発行日　平成23年10月12日(2011.10.12)　(24)登録日　平成23年7月29日(2011.7.29)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330A
H04L 9/32 (2006.01)　　H04L 9/00 675Z

請求項の数 30　(全 37 頁)

(21)出願番号　特願2005-371139(P2005-371139)
(22)出願日　平成17年12月23日(2005.12.23)
(65)公開番号　特開2006-260530(P2006-260530A)
(43)公開日　平成18年9月28日(2006.9.28)
審査請求日　平成20年12月1日(2008.12.1)
(31)優先権主張番号　特願2005-38883(P2005-38883)
(32)優先日　平成17年2月16日(2005.2.16)
(33)優先権主張国　日本国(JP)

(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
(72)発明者　奈須　政巳
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　和田　財太

(56)参考文献　特開２００３－４０８４４２（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】被管理装置、管理システム、被管理装置の制御方法、プログラム及び記録媒体

(57)【特許請求の範囲】
【請求項１】
通信回線を介して管理装置と通信して該管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信して該管理装置による管理を受ける間接被管理機能とを有する被管理装置であって、
前記直接被管理機能が有効な状態で、前記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、
前記個別証明書取得手段が取得した個別証明書を、前記管理装置と通信する際に使用する証明書として設定する手段とを設けたことを特徴とする被管理装置。
【請求項２】
請求項１記載の被管理装置であって、
前記直接被管理機能は、前記管理装置に認証され、該管理装置と通信して該管理装置による管理を受ける機能であり、
前記間接被管理機能は、前記管理装置に認証された仲介装置に認証され、該仲介装置を介して前記管理装置と通信して該管理装置による管理を受ける機能であることを特徴とする被管理装置。
【請求項３】
請求項１又は２記載の被管理装置であって、

前記個別証明書取得手段が、前記共通証明書を用いて確保した通信経路で前記個別証明書を取得する手段であることを特徴とする被管理装置。

【請求項４】

請求項１乃至３のいずれか一項記載の被管理装置であって、

前記個別証明書取得手段が、前記個別証明書を取得する際に、前記管理装置に当該被管理装置の識別情報を送信する手段を有することを特徴とする被管理装置。

【請求項５】

請求項４記載の被管理装置であって、

前記個別証明書取得手段が前記管理装置に送信した識別情報と、該手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段を設けたことを特徴とする被管理装置。

【請求項６】

請求項４又は５記載の被管理装置であって、

前記個別証明書取得手段が、前記直接被管理機能により管理を受ける際に用いる識別情報を前記管理装置に送信し、該管理装置から当該被管理装置を前記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に前記個別証明書の取得を行う手段であることを特徴とする被管理装置。

【請求項７】

請求項１乃至６のいずれか一項記載の被管理装置であって、

前記間接被管理機能が有効な場合には、前記直接被管理機能を有効にしないようにしたことを特徴とする被管理装置。

【請求項８】

通信回線を介して管理装置と通信して該管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信して該管理装置による管理を受ける間接被管理機能とを有する被管理装置と、前記管理装置とを備える管理システムであって、

前記被管理装置に、

前記直接被管理機能が有効な状態で、前記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、前記管理装置から自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、

前記個別証明書取得手段が取得した個別証明書を、前記管理装置と通信する際に使用する証明書として設定する手段とを設けたことを特徴とする管理システム。

【請求項９】

請求項８記載の管理システムであって、

前記直接被管理機能は、前記被管理装置が、前記管理装置に認証され、該管理装置と通信して該管理装置による管理を受ける機能であり、

前記間接被管理機能は、前記被管理装置が、前記管理装置に認証された仲介装置に認証され、該仲介装置を介して前記管理装置と通信して該管理装置による管理を受ける機能であることを特徴とする被管理システム。

【請求項１０】

請求項８又は９記載の管理システムであって、

前記被管理装置の前記個別証明書取得手段が、前記共通証明書を用いて確保した通信経路で前記個別証明書を取得する手段であることを特徴とする管理システム。

【請求項１１】

請求項８乃至１０のいずれか一項記載の管理システムであって、

前記個別証明書取得手段が、前記個別証明書を取得する際に、前記管理装置に当該被管理装置の識別情報を送信する手段を有することを特徴とする管理システム。

【請求項１２】

請求項１１記載の管理システムであって、

前記管理装置において、

前記被管理装置から受信した識別情報によりその送信元の被管理装置を認証する手段を設け、
該手段による認証が成功した場合のみ前記被管理装置に前記個別証明書を送信するようにしたことを特徴とする管理システム。
【請求項１３】
請求項１１又は１２記載の管理システムであって、
前記被管理装置に、前記個別証明書取得手段が前記管理装置に送信した識別情報と、該手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段を設けたことを特徴とする管理システム。
【請求項１４】
請求項１１乃至１３のいずれか一項記載の管理システムであって、
前記被管理装置の前記個別証明書取得手段が、前記直接被管理機能により管理を受ける際に用いる識別情報を前記管理装置に送信し、該管理装置から当該被管理装置を前記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に前記個別証明書の取得を行う手段であることを特徴とする管理システム。
【請求項１５】
請求項８乃至１４のいずれか一項記載の管理システムであって、
前記被管理装置が、前記間接被管理機能が有効な場合には、前記直接被管理機能を有効にしないようにしたことを特徴とする管理システム。
【請求項１６】
通信回線を介して管理装置と通信して該管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信して該管理装置による管理を受ける間接被管理機能とを有する被管理装置の制御方法であって、
前記被管理装置に、
前記直接被管理機能が有効な状態で、前記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手順と、
前記個別証明書取得手順で取得した個別証明書を、前記管理装置と通信する際に使用する証明書として設定する手順とを実行させるようにしたことを特徴とする被管理装置の制御方法。
【請求項１７】
請求項１６記載の被管理装置の制御方法であって、
前記直接被管理機能は、前記被管理装置が、前記管理装置に認証され、該管理装置と通信して該管理装置による管理を受ける機能であり、
前記間接被管理機能は、前記被管理装置が、前記管理装置に認証された仲介装置に認証され、該仲介装置を介して前記管理装置と通信して該管理装置による管理を受ける機能であることを特徴とする被管理装置の制御方法。
【請求項１８】
請求項１６又は１７記載の被管理装置の制御方法であって、
前記個別証明書取得手順が、前記共通証明書を用いて確保した通信経路で前記個別証明書を取得する手順であることを特徴とする被管理装置の制御方法。
【請求項１９】
請求項１６乃至１８のいずれか一項記載の被管理装置の制御方法であって、
前記個別証明書取得手順が、前記個別証明書を取得する際に、前記管理装置に前記被管理装置の識別情報を送信する手順を有することを特徴とする被管理装置の制御方法。
【請求項２０】
請求項１９記載の被管理装置の制御方法であって、
前記被管理装置に、前記個別証明書取得手順で前記管理装置に送信した識別情報と、該手順で取得した個別証明書に記載されている識別情報とが一致しない場合に、異常である

と判断する手順をさらに実行させるようにしたことを特徴とする被管理装置の制御方法。
【請求項２１】
請求項１９又は２０記載の被管理装置の制御方法であって、
前記個別証明書取得手順が、前記直接被管理機能により管理を受ける際に用いる識別情報を前記管理装置に送信し、該管理装置から前記被管理装置を前記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に前記個別証明書の取得を行う手順であることを特徴とする被管理装置の制御方法。
【請求項２２】
請求項１６乃至２１のいずれか一項記載の被管理装置の制御方法であって、
前記被管理装置に、前記間接被管理機能が有効な場合には、前記直接被管理機能を有効にさせないようにしたことを特徴とする被管理装置の制御方法。
【請求項２３】
通信回線を介して管理装置と通信して該管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信して該管理装置による管理を受ける間接被管理機能とを有する被管理装置を制御するコンピュータを、
前記直接被管理機能が有効な状態で、前記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、前記被管理装置の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、
前記個別証明書取得手段が取得した個別証明書を、前記被管理装置が前記管理装置と通信する際に使用する証明書として設定する手段として機能させるためのプログラムを含むプログラム。
【請求項２４】
請求項２３記載のプログラムであって、
前記直接被管理機能は、前記被管理装置が、前記管理装置に認証され、該管理装置と通信して該管理装置による管理を受ける機能であり、
前記間接被管理機能は、前記被管理装置が、前記管理装置に認証された仲介装置に認証され、該仲介装置を介して前記管理装置と通信して該管理装置による管理を受ける機能であることを特徴とするプログラム。
【請求項２５】
請求項２３又は２４記載のプログラムであって、
前記個別証明書取得手段が、前記共通証明書を用いて確保した通信経路で前記個別証明書を取得する手段であることを特徴とするプログラム。
【請求項２６】
請求項２３乃至２５のいずれか一項記載のプログラムであって、
前記個別証明書取得手段が、前記個別証明書を取得する際に、前記管理装置に前記被管理装置の識別情報を送信する手段を有することを特徴とするプログラム。
【請求項２７】
請求項２６記載のプログラムであって、
前記コンピュータを、
前記個別証明書取得手段が前記管理装置に送信した識別情報と、該手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段として機能させるためのプログラムを更に含むプログラム。
【請求項２８】
請求項２６又は２７記載のプログラムであって、
前記個別証明書取得手段が、前記被管理装置が前記直接被管理機能により管理を受ける際に用いる識別情報を前記管理装置に送信し、該管理装置から前記被管理装置を前記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に前記個別証明書の取得を行う手段であることを特徴とするプログラム。
【請求項２９】

請求項２３乃至２８のいずれか一項記載のプログラムであって、
前記コンピュータに、
前記被管理装置において、前記間接被管理機能が有効な場合には、前記直接被管理機能を有効にしないようにする機能を実現させるためのプログラムをさらに含むプログラム。
【請求項３０】
請求項２３乃至２９のいずれか一項記載のプログラムを記録したコンピュータ読取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、管理装置による遠隔管理を受ける機能を有する被管理装置、このような被管理装置と上記の管理装置とを備えた管理システム、上記のような被管理装置の制御方法、コンピュータに上記のような被管理装置を制御させるためのプログラム、およびこのようなプログラムを記録したコンピュータ読取り可能な記録媒体に関する。
【背景技術】
【０００２】
近年、種々の電子装置を被管理装置とし、クライアント装置あるいはサーバ装置の機能を持たせてネットワークを介して管理装置と通信可能とし、これら相互間の通信を利用して管理装置により電子装置の管理を行う管理システムが提案されている。
このようなシステムを構築する上では、通信を行う際に、通信相手が適切か、あるいは送信されてくる情報が改竄されていないかといった確認が重要である。また、特にインターネットにおいては、情報が通信相手に到達するまでに無関係なコンピュータを経由する場合が多いことから、機密情報を送信する場合、その内容を盗み見られないようにする必要もある。そして、このような要求に応える通信プロトコルとして、例えばＳＳＬ（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、情報の暗号化により改竄及び盗聴の防止を図ることができる。また、通信相手の側でも、通信を要求してきた通信元の装置を認証することができる。
このようなＳＳＬや公開鍵暗号を用いた認証に関連する技術としては、例えば特許文献１及び特許文献２に記載のものが挙げられる。
【特許文献１】特開２００２－３５３９５９号公報
【特許文献２】特開２００２－２５１４９２号公報
【０００３】
ここで、このＳＳＬに従った相互認証を行う場合の通信手順について、認証処理の部分に焦点を当てて説明する。図２８は、通信装置Ａと通信装置ＢとがＳＳＬに従った相互認証を行う際に各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。
図２８に示すように、ＳＳＬに従った相互認証を行う際には、まず双方の通信装置に、ルート鍵証明書及び、私有鍵と公開鍵証明書を記憶させておく必要がある。この私有鍵は、認証局（ＣＡ：certificate authority）が各装置に対して発行した私有鍵であり、公開鍵証明書は、その私有鍵と対応する公開鍵にＣＡがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、ＣＡがデジタル署名に用いたルート私有鍵と対応するルート鍵に、デジタル署名を付してデジタル証明書としたものである。
【０００４】
図２９にこれらの関係を示す。
図２９（ａ）に示すように、公開鍵Ａは、私有鍵Ａを用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（ＣＡ）や有効期間等の情報を含む書誌情報とによって構成される。そして、ＣＡは、鍵本体や書誌情報が改竄されていないことを示すため、公開鍵Ａをハッシュ処理して得たハッシュ値を、ルート私有鍵を用いて暗号化し、

デジタル署名としてクライアント公開鍵に付す。またこの際に、デジタル署名に用いるルート私有鍵の識別情報を署名鍵情報として公開鍵Ａの書誌情報に加える。そして、このデジタル署名を付した公開鍵証明書が、公開鍵証明書Ａである。

【０００５】

この公開鍵証明書Ａを認証処理に用いる場合には、ここに含まれるデジタル署名を、ルート私有鍵と対応する公開鍵であるルート鍵の鍵本体を用いて復号化する。この復号化が正常に行われれば、デジタル署名が確かにＣＡによって付されたことがわかる。また、公開鍵Ａの部分をハッシュ処理して得たハッシュ値と、復号して得たハッシュ値とが一致すれば、鍵自体も損傷や改竄を受けていないことがわかる。さらに、受信したデータをこの公開鍵Ａを用いて正常に復号化できれば、そのデータは、私有鍵Ａの持ち主から送信されたものであることがわかる。

【０００６】

ここで、認証を行うためには、ルート鍵を予め記憶しておく必要があるが、このルート鍵も、図２９（ｂ）に示すように、ＣＡがデジタル署名を付したルート鍵証明書として記憶しておく。このルート鍵証明書は、自身に含まれる公開鍵でデジタル署名を復号化可能な、自己署名形式である。そして、ルート鍵を使用する際に、そのルート鍵証明書に含まれる鍵本体を用いてデジタル署名を復号化し、ルート鍵をハッシュ処理して得たハッシュ値と比較する。これが一致すれば、ルート鍵が破損等していないことを確認できるのである。

【０００７】

図２８のフローチャートの説明に入る。なお、この図において、２本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。

【０００８】

ここでは、通信装置Ａが通信装置Ｂに通信を要求するものとするが、この要求を行う場合、通信装置ＡのＣＰＵは、所要の制御プログラムを実行することにより、図２８の左側に示すフローチャートの処理を開始する。そして、ステップＳ３１１で通信装置Ｂに対して接続要求を送信する。

一方通信装置ＢのＣＰＵは、この接続要求を受信すると、所要の制御プログラムを実行することにより、図２８の右側に示すフローチャートの処理を開始する。そして、ステップＳ３２１で第１の乱数を生成し、これを私有鍵Ｂを用いて暗号化する。そして、ステップＳ３２２でその暗号化した第１の乱数と公開鍵証明書Ｂとを通信装置Ａに送信する。

【０００９】

通信装置Ａ側では、これを受信すると、ステップＳ３１２でルート鍵証明書を用いて公開鍵証明書Ｂの正当性を確認する。

そして確認ができると、ステップＳ３１３で、受信した公開鍵証明書Ｂに含まれる公開鍵Ｂを用いて第１の乱数を復号化する。ここで復号化が成功すれば、第１の乱数は確かに公開鍵証明書Ｂの発行対象から受信したものだと確認できる。そして、これが確認できた場合、通信装置Ｂに対して認証成功の旨を示す情報を送信する。

【００１０】

また、通信装置Ｂ側では、この情報を受信すると、ステップＳ３２３で通信装置Ａに対し、認証のための公開鍵証明書の送信を要求する。

すると、通信装置Ａ側ではこれに応じてステップＳ３１４で第２の乱数及び共通鍵の種を生成する。共通鍵の種は、例えばそれまでの通信でやり取りしたデータに基づいて作成することができる。そして、ステップＳ３１５で第２の乱数を私有鍵Ａを用いて暗号化し、共通鍵の種を公開鍵Ｂを用いて暗号化し、ステップＳ３１６でこれらを公開鍵証明書Ａと共にサーバ装置に送信する。共通鍵の種の暗号化は、通信相手以外の装置に共通鍵の種

を知られないようにするために行うものである。
また、次のステップＳ３１７では、ステップＳ３１４で生成した共通鍵の種から以後の通信の暗号化に用いる共通鍵を生成する。
【００１１】
通信装置Ｂ側では、これを受信すると、ステップＳ３２４でルート鍵証明書を用いて公開鍵証明書Ａの正当性を確認する。そして確認ができると、ステップＳ３２５で、受信した公開鍵証明書Ａに含まれる公開鍵Ａを用いて第２の乱数を復号化する。ここで復号化が成功すれば、第２の乱数は確かに公開鍵証明書Ａの発行対象から受信したものだと確認できる。
その後、ステップＳ３２６で私有鍵Ｂを用いて共通鍵の種を復号化する。ここまでの処理で、通信装置Ａ側と通信装置Ｂ側に共通の共通鍵の種が共有されたことになる。そして、この共通鍵の種は、生成した通信装置Ａと、私有鍵Ｂを持つ通信装置Ｂ以外の装置が知ることはない。ここまでの処理が成功すると、通信装置Ｂ側でもステップＳ３２７で復号化で得た共通鍵の種から以後の通信の暗号化に用いる共通鍵を生成する。
【００１２】
そして、通信装置Ａ側のステップＳ３１７と通信装置Ｂ側のステップＳ３２７の処理が終了すると、相互に認証の成功と以後の通信に使用する暗号化方式とを確認し、生成した共通鍵を用いてその暗号化方式で以後の通信を行うものとして認証に関する処理を終了する。なお、この確認には、通信装置Ｂからの認証が成功した旨の応答も含むものとする。以上の処理によって互いに通信を確立し、以後はステップＳ３１７又はＳ３２７で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行うことができる。
【００１３】
このような処理を行うことにより、通信装置Ａと通信装置Ｂが互いに相手を認証した上で安全に共通鍵を共有することができ、通信を安全に行う経路を確立することができる。
ただし、上述した処理において、第２の乱数を私有鍵Ａで暗号化し、公開鍵証明書Ａを通信装置Ｂに送信することは必須ではない。このようにすると、通信装置Ｂが通信装置Ａを認証することはできないが、通信装置Ａが通信装置Ｂを認証するだけでよい場合にはこの処理で十分である。そしてこの場合には、通信装置Ａに記憶させるのはルート鍵証明書のみでよく、私有鍵Ａ及び公開鍵証明書Ａは不要である。また、通信装置Ｂにはルート鍵証明書を記憶させる必要はない。
【発明の開示】
【発明が解決しようとする課題】
【００１４】
ところで、上述したような認証処理を行う場合、認証の基準には２通りのレベルが考えられる。第１のレベルは、通信相手の機器が、同一のベンダーから供給された機器であるか、一定のテストに合格した機器であるか等、一定の基準を満たす機器か否かを判断するものであり、第２のレベルは、通信相手の機器の個体を特定するものである。
そして、第１のレベルの認証を行う場合は、一定の基準を満たす機器に共通の公開鍵証明書と私有鍵のセットを記憶させておき、ＳＳＬ通信の際にこれを用いて認証を行い、通信相手が確かにその公開鍵証明書の発行対象の装置であると確認できればよい。従って、機器固有の識別情報（ＩＤ）等を交換する必要はない。
【００１５】
しかし、上述したような管理システムにおいては、管理対象の被管理装置を個別に特定する必要があることから、第２のレベルの認証が要求される。
ここで、第２のレベルの認証を行う場合でも、例えば上記の第１のレベルの認証の場合と同様な証明書と鍵を用いて安全な通信経路を確立した後で、通信相手を特定するためにＩＤを送信させ、これを用いて認証を行うことは可能である。
【００１６】
一方で、近年、動作要求を双方向に転送する通信を仲介する仲介装置を設け、管理装置と被管理装置とがこの仲介装置を介して通信するようにシステムを構成することが提案さ

れている。そして、システムをこのように構成すると、仲介装置に被管理装置を認証させるようにすれば、管理装置は、仲介装置を認証するのみで、末端の被管理装置まで間接的に認証できることになり、１つのユーザ環境（事業所等）で多数の被管理装置を使用するような場合には、システムの運用面で効率がよい。

しかし、被管理装置の台数が少ない場合、特に１事業所で１台しか使用しないような場合には、仲介装置を設けても効率化の効果は得られず、仲介装置を設けることにより却ってシステムを複雑化してしまうことになるため、管理装置が直接被管理装置を認証するようにすることが好ましい。

従って、例えば大規模事業所で使用する被管理装置の一部を小規模事業所に移転するような場合には、当初は仲介装置に認証させていた被管理装置を、管理装置が直接認証できるようにすることが望まれる場合もある。そして、このような要望に対しては、被管理装置に前者に対応する間接被管理用の動作モードと後者に対応する直接被管理用の動作モードとを設け、これらを切り替え可能にすることにより対応することが考えられる。

【００１７】

ここで、間接（被）管理の場合と直接（被）管理の場合とでは、被管理装置の認証に要求される安全性のレベルが異なると考えられる。すなわち、間接被管理の場合、仲介装置が、通常は同じユーザ環境に配置される被管理装置を認証するため、直接管理の場合よりは低いセキュリティでもよいと考えられるのに対し、直接被管理の場合は管理装置がどこにでも設置され得る被管理装置を認証するため、高度なセキュリティが要求される。

そして、直接被管理の場合に要求されるセキュリティレベルの認証を行うためには、機器固有のＩＤを記載した証明書を各機器に記憶させ、これを認証に使用することが考えられる。

【００１８】

しかし、機器固有のＩＤを記載した証明書を各機器に記憶させる際には、機器毎に異なる証明書や鍵を記憶させる必要があるため、製造時にこれを記憶させるとすると、それに対応した製造設備が必要となる。例えば、製造した各機器とＣＡとの間の安全な通信経路を確保する設備等である。そして、このような設備を用意すると、コストアップにつながるし、証明書を記憶させる工程が、量産時のリードタイムの増加を招くという問題があった。また、ＯＥＭ（Original Equipment Manufacturer）を行う場合等には、このような設備を用意することが難しい場合もあり、このような場合には、機器固有のＩＤを記載した証明書を各機器に記憶させることができないという問題もあった。

【００１９】

このため、より低いレベルのセキュリティでよい間接被管理が行われることが想定される被管理装置にまで、一律に機器固有のＩＤを記載した証明書を記憶させることは、装置の製造効率の面からは、あまり適当でないと考えられる。一方で、装置を間接被管理から直接被管理に切り替えることも考えられるため、このような事態に対処する仕組みも必要となる。

この発明は、このような問題を解決し、管理装置による管理を受ける被管理装置において、効率よく高いセキュリティを確保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】

【００２０】

上記の目的を達成するため、この発明の被管理装置は、通信回線を介して管理装置と通信してその管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信してその管理装置による管理を受ける間接被管理機能とを有する被管理装置において、上記直接被管理機能が有効な状態で、上記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、上記個別証明書取得手段が取得した個別証明書を、上記管理装置と通信する際に使用する証明書として設定する手段とを設けたものである。

【００２１】

このような被管理装置において、上記直接被管理機能を、上記管理装置に認証され、その管理装置と通信してその管理装置による管理を受ける機能とし、上記間接被管理機能を、上記管理装置に認証された仲介装置に認証され、その仲介装置を介して上記管理装置と通信してその管理装置による管理を受ける機能とするとよい。

さらに、上記個別証明書取得手段を、上記共通証明書を用いて確保した通信経路で上記個別証明書を取得する手段とするとよい。

【００２２】

さらに、上記個別証明書取得手段に、上記個別証明書を取得する際に、上記管理装置にその被管理装置の識別情報を送信する手段を設けるとよい。

さらに、上記個別証明書取得手段が上記管理装置に送信した識別情報と、その手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段を設けるとよい。

【００２３】

さらにまた、上記個別証明書取得手段を、上記直接被管理機能により管理を受ける際に用いる識別情報を上記管理装置に送信し、その管理装置からその被管理装置を上記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に上記個別証明書の取得を行う手段とするとよい。

また、上記の各被管理装置において、上記間接被管理機能が有効な場合には、上記直接被管理機能を有効にしないようにするとよい。

【００２４】

また、この発明の管理システムは、通信回線を介して管理装置と通信してその管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信してその管理装置による管理を受ける間接被管理機能とを有する被管理装置と、上記管理装置とを備える管理システムにおいて、上記被管理装置に、上記直接被管理機能が有効な状態で、上記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、上記管理装置から自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、上記個別証明書取得手段が取得した個別証明書を、上記管理装置と通信する際に使用する証明書として設定する手段とを設けたものである。

【００２５】

このような管理システムにおいて、上記直接被管理機能を、上記被管理装置が、上記管理装置に認証され、その管理装置と通信してその管理装置による管理を受ける機能とし、上記間接被管理機能を、上記被管理装置が、上記管理装置に認証された仲介装置に認証され、その仲介装置を介して上記管理装置と通信してその管理装置による管理を受ける機能とするとよい。

さらに、上記被管理装置の上記個別証明書取得手段を、上記共通証明書を用いて確保した通信経路で上記個別証明書を取得する手段とするとよい。

【００２６】

さらに、上記個別証明書取得手段に、上記個別証明書を取得する際に、上記管理装置にその被管理装置の識別情報を送信する手段を設けるとよい。

さらに、上記管理装置において、上記被管理装置から受信した識別情報によりその送信元の被管理装置を認証する手段を設け、その手段による認証が成功した場合のみ上記被管理装置に上記個別証明書を送信するようにするとよい。

【００２７】

さらに、上記被管理装置に、上記個別証明書取得手段が上記管理装置に送信した識別情報と、その手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段を設けるとよい。

さらにまた、上記被管理装置の上記個別証明書取得手段を、上記直接被管理機能により管理を受ける際に用いる識別情報を上記管理装置に送信し、その管理装置からその被管理装置を上記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に上記

個別証明書の取得を行う手段とするとよい。
また、上記の各管理システムにおいて、上記被管理装置が、上記間接被管理機能が有効な場合には、上記直接被管理機能を有効にしないようにするとよい。
【００２８】
また、この発明の被管理装置の制御方法は、通信回線を介して管理装置と通信してその管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信してその管理装置による管理を受ける間接被管理機能とを有する被管理装置の制御方法において、上記被管理装置に、上記直接被管理機能が有効な状態で、上記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、自身の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手順と、上記個別証明書取得手順で取得した個別証明書を、上記管理装置と通信する際に使用する証明書として設定する手順とを実行させるようにしたものである。
【００２９】
このような被管理装置の制御方法において、上記直接被管理機能を、上記被管理装置が、上記管理装置に認証され、その管理装置と通信してその管理装置による管理を受ける機能とし、上記間接被管理機能を、上記被管理装置が、上記管理装置に認証された仲介装置に認証され、その仲介装置を介して上記管理装置と通信してその管理装置による管理を受ける機能とするとよい。
さらに、上記個別証明書取得手順を、上記共通証明書を用いて確保した通信経路で上記個別証明書を取得する手順とするとよい。
【００３０】
さらに、上記個別証明書取得手順に、上記個別証明書を取得する際に、上記管理装置に上記被管理装置の識別情報を送信する手順を設けるとよい。
さらに、上記被管理装置に、上記個別証明書取得手順で上記管理装置に送信した識別情報と、その手順で取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手順をさらに実行させるようにするとよい。
【００３１】
さらにまた、上記個別証明書取得手順を、上記直接被管理機能により管理を受ける際に用いる識別情報を上記管理装置に送信し、その管理装置から上記被管理装置を上記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に上記個別証明書の取得を行う手順とするとよい。
また、上記の各被管理装置の制御方法において、上記被管理装置に、上記間接被管理機能が有効な場合には、上記直接被管理機能を有効にさせないようにするとよい。
【００３２】
また、この発明のプログラムは、通信回線を介して管理装置と通信してその管理装置による管理を受ける直接被管理機能と、仲介装置を介して管理装置と通信してその管理装置による管理を受ける間接被管理機能とを有する被管理装置を制御するコンピュータを、上記直接被管理機能が有効な状態で、上記管理装置と通信する際に使用する証明書が、機器の識別情報が記載されていないデジタル証明書である共通証明書であると判断した場合に、上記被管理装置の識別情報が記載されたデジタル証明書である個別証明書を取得する個別証明書取得手段と、上記個別証明書取得手段が取得した個別証明書を、上記被管理装置が上記管理装置と通信する際に使用する証明書として設定する手段として機能させるためのプログラムを含むプログラムである。
【００３３】
このようなプログラムにおいて、上記直接被管理機能を、上記被管理装置が、上記管理装置に認証され、その管理装置と通信してその管理装置による管理を受ける機能とし、上記間接被管理機能を、上記被管理装置が、上記管理装置に認証された仲介装置に認証され、その仲介装置を介して上記管理装置と通信してその管理装置による管理を受ける機能とするとよい。

さらに、上記個別証明書取得手段を、上記共通証明書を用いて確保した通信経路で上記個別証明書を取得する手段とするとよい。

【００３４】

さらに、上記個別証明書取得手段に、上記個別証明書を取得する際に、上記管理装置に上記被管理装置の識別情報を送信する手段を設けるとよい。

さらに、上記コンピュータを、上記個別証明書取得手段が上記管理装置に送信した識別情報と、その手段が取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断する手段として機能させるためのプログラムを更に含めるとよい。

【００３５】

さらにまた、上記個別証明書取得手段を、上記被管理装置が上記直接被管理機能により管理を受ける際に用いる識別情報を上記管理装置に送信し、その管理装置から上記被管理装置を上記直接被管理機能による管理対象として登録できる旨の応答を受けた場合に上記個別証明書の取得を行う手段とするとよい。

また、上記の各プログラムにおいて、上記コンピュータに、上記被管理装置において、上記間接被管理機能が有効な場合には、上記直接被管理機能を有効にしないようにする機能を実現させるためのプログラムをさらに含めるとよい。

【００３６】

また、この発明の記録媒体は、上記のいずれかのプログラムを記録したコンピュータ読取可能な記録媒体である。

【発明の効果】

【００３７】

以上のようなこの発明の被管理装置、管理システム又は被管理装置の制御方法によれば、管理装置による管理を受ける被管理装置において、効率よく高いセキュリティを確保できるようにすることができる。

また、この発明のプログラムによれば、コンピュータに被管理装置を制御させてその特徴を実現し、同様な効果を得ることができる。

この発明の記録媒体によれば、上記のプログラムを記憶していないコンピュータにそのプログラムを読み出させて実行させ、上記の効果を得ることができる。

【発明を実施するための最良の形態】

【００３８】

以下、この発明の好ましい実施の形態を図面を参照して説明する。

まず、この発明による被管理装置及び管理システムの構成例について説明する。図１は、その被管理装置を含む管理システムの構成の一例を示す概念図である。

この管理システムは、プリンタ，ＦＡＸ装置，デジタル複写機，スキャナ装置，デジタル複合機等の画像処理装置や、ネットワーク家電，自動販売機，医療機器，電源装置，空調システム，ガス・水道・電気等の計量システム，汎用コンピュータ，自動車，航空機等の種々の電子装置に通信機能を持たせた通信装置を被管理装置１０として構成される。

【００３９】

そして、この管理システムは、被管理装置１０とネットワークを介して通信可能な管理装置２０を備え、その管理装置２０が、各被管理装置１０を集中的に管理できるようにしたものである。また、ここでいう管理とは、管理対象の機器から情報を取得し、その情報に基づいて何らかの動作を行うことである。

【００４０】

この動作としては、例えば被管理装置が画像形成装置であれば、画像形成枚数を集計したり、管理対象の装置からの異常発生通知に対応して適当なサービスセンタに通報を行い、修理担当者の派遣を促したり、管理対象装置のファームウェアのバージョン情報を取得し、そのバージョンが古いものであった場合に新しいファームウェアを送信して更新させたりといった動作が考えられる。また、取得した情報を単に蓄積するのみでもよい。

【００４１】

そして、この管理システムにおいて、被管理装置１０と管理装置２０との間の通信経路

は、有線、無線を問わず任意のものでよく、例えばインターネット４０のような通信回線を用いることができる。また、被管理装置１０と管理装置２０との間の通信を仲介する１又は複数の仲介装置５０を設け、この仲介装置５０に通信を仲介させるようにすることもできる。

【００４２】

例えば、図１に示す設置環境Ａでは、管理装置２０と直接的なコネクションを確立できる仲介装置５０が、被管理装置１０ａ及び１０ｂを従える単純な階層構造としている。また、同図に示す設置環境Ｂでは、４台の被管理装置１０を設置する為、１台の仲介装置５０を設置しただけでは負荷が大きくなるため、管理装置２０と直接的なコネクションを確立できる仲介装置５０ｂが、被管理装置１０ｃ及び１０ｄだけでなく、他の仲介装置５０ｃを従え、この仲介装置５０ｃが被管理装置１０ｅ及び１０ｆを更に従えるという階層構造を形成している。この場合、被管理装置１０ｅ及び１０ｆを管理するために管理装置２０から発せられた情報は、仲介装置５０ｂとその下位のノードである仲介装置５０ｃとを経由して、被管理装置１０ｅ又は１０ｆに到達することになる。

【００４３】

なお、これらの環境における被管理装置１０のように、仲介装置５０を介して管理装置２０と通信して管理を受ける機能が間接被管理機能であり、このような管理を受ける状態の被管理装置１０を間接被管理状態の被管理装置と呼ぶことにする。

そして、このように仲介装置５０を用いれば、遠隔管理のための通信に特殊なプロトコルが必要な場合であっても、仲介装置５０にプロトコル変換機能を設けておくことにより、各被管理装置１０は、一般的なプロトコルを用いて管理装置２０と通信を行うことができる。

また、ここでは仲介装置５０は被管理装置１０と同じローカルエリアネットワーク（ＬＡＮ）内に設けているが、専用線や電話線等、被管理装置１０との間で安全を確保できる通信経路があれば、仲介装置５０を設ける位置は、ＬＡＮ内やユーザ環境内に限られることはない。

【００４４】

また、被管理装置１０に仲介装置５０の機能を併せ持たせることも可能であり、設置環境Ｃの場合のように、このような被管理装置１０を別途仲介装置５０を介さずに管理装置２０に接続するようにしてもよい。

このように、仲介装置５０を介さずに管理装置２０と通信して管理を受ける機能が直接被管理機能であり、このような管理を受ける状態の被管理装置１０を直接被管理状態の被管理装置と呼ぶことにする。

なお。図示はしていないが、直接被管理状態の被管理装置１０の下位にさらに被管理装置１０を接続し、直接被管理状態の被管理装置１０に通信を仲介させることもできる。

また、各設置環境には、セキュリティ面を考慮し、ファイアウォール６０を設置する。

【００４５】

このような管理システムにおいて、仲介装置５０は、その下位のノードである被管理装置１０の制御管理のためのアプリケーションプログラムを実装している。

管理装置２０は、各仲介装置５０の制御管理、更にはこの仲介装置５０を介した被管理装置１０の制御管理を行うためのアプリケーションプログラムを実装している。そして、被管理装置１０も含め、この遠隔管理システムにおけるこれら各ノードは、ＲＰＣ（Remote Procedure Call）により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【００４６】

すなわち、仲介装置５０又はその下位の被管理装置１０では、管理装置２０への要求を生成してこれを管理装置２０へ引き渡し、この要求に対する応答を取得できる一方で、管理装置２０は、上記仲介装置５０側への要求を生成してこれを仲介装置５０側へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、仲介装置５０に

被管理装置１０に対して各種要求を送信させ、被管理装置１０からの応答を仲介装置５０を介して取得することも含まれる。

なお、ＲＰＣを実現するために、ＳＯＡＰ（Simple Object Access Protocol：ソープ），ＨＴＴＰ（HyperText Transfer Protocol），ＦＴＰ（File Transfer Protocol），ＣＯＭ（Component Object Model），ＣＯＲＢＡ（Common Object Request Broker Architecture）等の既知のプロトコル（通信規格），技術，仕様などを利用することができる。

【００４７】

この送受信のデータ送受モデルを図２の概念図に示す。

（Ａ）は、被管理装置１０で管理装置２０に対する要求が発生したケースである。このケースでは、被管理装置１０が被管理装置側要求ａを生成し、これを仲介装置５０を経由して受け取った管理装置２０がこの要求に対する応答ａを返すというモデルになる。同図に示す仲介装置５０は複数であるケースも想定できる（上記図１に示す設置環境Ｂ）。なお、（Ａ）では、応答ａだけでなく応答遅延通知ａ′を返信するケースが表記されている。これは、管理装置２０が、仲介装置５０を経由して被管理装置側要求を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延を通知して一旦接続状態を切断し、次回の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

【００４８】

（Ｂ）は、管理装置２０で被管理装置１０に対する要求が発生したケースである。このケースでは、管理装置２０が管理装置側要求ｂを生成し、これを仲介装置５０を経由して受け取った被管理装置１０が、当該要求に対する応答ｂを返すというモデルになっている。なお、（Ｂ）のケースでも、応答を即座に返せないときに応答遅延通知ｂ′を返すことは（Ａ）のケースと同様である。

【００４９】

次に、図３に、被管理装置１０のハードウェア構成を示す。

図３に示すように、被管理装置１０は、ＣＰＵ１０１，ＲＯＭ１０２，ＲＡＭ１０３，不揮発性メモリ（ＮＶＲＡＭ）１０４，通信Ｉ／Ｆ１０５，操作部１０６，エンジン部１０７を備え、これらがシステムバス１０８により接続されている。

そして、ＣＰＵ１０１は、被管理装置１０全体を統括制御する制御手段であり、ＲＯＭ１０２や不揮発性メモリ１０４に記録された種々のプログラムを実行することにより、個別証明書取得手段等の各手段として機能し、後述するようにこの実施形態の特徴に係る種々の機能を実現する。

【００５０】

ＲＯＭ１０２は、不揮発性の記憶手段であり、ＣＰＵ１０１が実行するプログラムや、固定的なパラメータ等を記憶する。ＲＯＭ１０２を書き換え可能な記憶手段として構成し、これらのデータをアップデートできるようにしてもよい。

ＲＡＭ１０３は、一時的に使用するデータを記憶したり、ＣＰＵ１０１のワークメモリとして使用したりする記憶手段である。

不揮発性メモリ１０４は、フラッシュメモリやＨＤＤ等による書き換え可能な不揮発性記憶手段であり、ＣＰＵ１０１が実行するプログラムや、装置の電源がＯＦＦされた後でも保持しておく必要があるパラメータの値等を記憶する。被管理装置１０が認証処理に使用する証明書等もここに記憶させておく。

【００５１】

通信Ｉ／Ｆ１０５は、被管理装置１０をＬＡＮのようなネットワークを始めとする通信回線に接続するためのインタフェースであり、例えばイーサネット（登録商標）方式の通信を行うためのインタフェースである。そして、通信回線を介して他の装置と通信を行う場合、この通信Ｉ／Ｆ１０５とＣＰＵ１０１とが通信手段として機能する。なお、通信回線としては、有線、無線を問わず種々の方式のものが使用可能であり、通信Ｉ／Ｆ１０５は、通信回線の規格や使用する通信プロトコル等に応じて適切なものを用意する。また、複数の規格に対応させて複数の通信Ｉ／Ｆ１０５を設けることも当然可能である。

操作部１０６は、種々のキーや、ＧＵＩを表示可能な液晶ディスプレイにタッチパネルを積層した操作パネル等を備え、被管理装置１０の動作状態、設定内容、ユーザへのメッセージ等を表示すると共に、ユーザの操作を受け付けるための操作手段である。

【００５２】

エンジン部１０７は、被管理装置１０が装置自体として機能するための、以上説明した各部以外のハードウェアである。例えば被管理装置１０がデジタル複合機である場合には、画像形成部、画像読取部、ファクシミリ通信ユニット等がエンジン部１０７に該当する。そして、ＣＰＵ１０１がこれらの動作を適切に制御することにより、被管理装置１０にコピー，プリント，スキャン，ファクシミリ通信等の種々の動作を実行させることができる。また、被管理装置１０の用途によっては、エンジン部１０７がなくてよい場合もある。そして、この部分は、この実施形態の特徴とはあまり関係ないため、図示は簡単なものに留めている。

【００５３】

また、管理装置２０や仲介装置５０についても、エンジン部１０７は不要であるが、被管理装置１０の場合と同様なハードウェア構成でよい。ただし、特に管理装置２０の場合、管理の目的や運用方法に応じて種々の付加的な構成を設けたり、規模の大きい装置にしたりすることが考えられる。

【００５４】

そして、これらの各装置においては、ＣＰＵに種々の制御プログラムを実行させることにより、上述した各機能及び以下に説明する各機能を実現するようにしている。

また、図１に示した管理システムにおいて、被管理装置１０，仲介装置５０，管理装置２０の各ノードには、認証情報として公開鍵証明書、私有鍵及びルート鍵証明書を記憶させておき、互いに通信を行う際には、これらの認証情報を用い、図２８を用いて説明したような相互認証あるいは片方向認証を行うようにしている。

【００５５】

ここで、図４（ａ）～（ｃ）に、それぞれ被管理装置１０，管理装置２０，および仲介装置５０が記憶している証明書及び鍵の種類を示す。

この図に示すように、被管理装置１０，管理装置２０，および仲介装置５０は、それぞれ自身に関する認証情報である公開鍵証明書及び私有鍵と、通信相手に関する認証情報であるルート鍵証明書とを記憶している。

また、例えば被管理装置用共通公開鍵証明書は、適当なＣＡが発行した公開鍵に、被管理装置認証用ルート鍵を用いて正当性を確認可能なデジタル署名を付したデジタル証明書である。

【００５６】

図５にその構成を示すが、この被管理装置用共通公開鍵証明書は、書誌情報に具体的な装置のＩＤを記載せず、全ての被管理装置に共通に記憶させて使用させることができる共通証明書である（実際に共通に記憶させることは必須ではないが）。従って、この証明書を用いて認証を行う場合、個体を特定するためには、別途ＩＤを送信する必要がある。

この方式では、ＩＤについては、公開鍵証明書のような改竄防止策が施されていないため、ＩＤが改竄される恐れがあり、この場合、他の機器になりすませてしまうという問題があった。また、共通の公開鍵証明書と私有鍵を、広い範囲に配布することになるから、その分だけ盗用される危険性が高まるという問題はある。

しかし、このような証明書であれば、全ての装置に同じものを記憶させることができるので、制御ソフトウェアに含めてしまう等すれば、工場で装置を製造する際に、特別な設備がなくても設定することができる。

【００５７】

そして、このような公開鍵証明書を用いたとしても、仲介装置５０がＬＡＮ外の被管理装置１０とは通信しないようにしておけば、例え認証に用いるＩＤが改竄されたとしても、同一ＬＡＮ内の装置にしかなりすますことができないため、ある程度満足できる水準のセキュリティは確保できる。そこで、被管理装置１０の製造時には、被管理装置用共通公

開鍵証明書を記憶させ、必要に応じてこれを別の証明書に更新してさらにセキュリティを向上させることができるようにしている。

また、被管理装置用共通私有鍵は上記の共通公開鍵と対応する私有鍵、被管理装置認証用ルート鍵証明書は、被管理装置認証用ルート鍵に自身と対応するルート私有鍵を用いて自身で正当性を確認可能なデジタル署名を付したデジタル証明書である。

【００５８】

一方、管理装置用公開鍵証明書と管理装置用私有鍵と管理装置認証用ルート鍵証明書も同様な関係であり、仲介装置用公開鍵証明書と仲介装置用私有鍵と仲介装置認証用ルート鍵証明書も同様な関係である。

しかし、上記のように、機器固有のＩＤを記載していない公開鍵証明書を用いた認証だと、セキュリティレベルは比較的低いものになってしまう。一方で、管理装置２０や仲介装置５０は、管理システムの基幹部分をなす装置であり、証明書設定用の特別な設備を備えた工場で製造することも比較的容易である。そこで、管理装置用公開鍵証明書及び仲介装置用公開鍵証明書については、識別情報として設定する機器に固有のＩＤ（例えばその機器の機番）を記載した個別公開鍵証明書（個別証明書）とし、認証処理の際に、公開鍵証明書に記載したＩＤを用いて個体を特定することができるようにしている。

【００５９】

図６にその例を示すが、このようにした場合、公開鍵証明書に記載したＩＤを改竄すると、もはやルート鍵証明書を用いてその公開鍵証明書の正当性を確認できなくなるため、ＩＤを改竄して他の機器になりすますことが実質的に不可能であり、セキュリティを向上させることができる。

【００６０】

ところで、図１に示した管理システムにおいては、ユーザが管理装置２０による被管理装置１０の遠隔管理を希望する場合、まず管理装置２０の運用者と管理契約を結び、その後管理対象の被管理装置１０を管理装置２０に登録させるようにしている。そして、この登録があった場合に、管理装置２０が登録された被管理装置１０を管理対象である適切な通信相手と認識し、動作要求や動作応答の送受信を利用した遠隔管理を開始するようにしている。

【００６１】

そして、上記の登録は、仲介機能を持たず、または仲介機能を無効にしており、仲介装置５０を介して管理装置２０と通信する被管理装置１０については、その通信を仲介する仲介装置５０が登録を代行すると共に、仲介装置５０自身も、登録する被管理装置１０が自身の仲介機能を利用して管理装置２０と通信すること、すなわちその被管理装置１０が仲介装置５０の管理下にある旨を記憶するようにしている。

【００６２】

一方、仲介機能を有効にし、自身の仲介機能を利用して管理装置２０と通信を行う被管理装置１０の場合は、ユーザの指示により直接管理装置２０と通信して登録を行うようにしている。そして、このような直接被管理状態になる場合には、被管理装置１０の場合にも、仲介装置５０の場合と同程度のセキュリティが要求される。直接通信の場合には、装置のＩＤが改竄された場合、管理対象になり得るどの装置にもなりすますことができてしまうためである。

【００６３】

そこで、ここでは、被管理装置１０において直接被管理機能を有効にする場合、管理装置２０と通信する際に使用する証明書が共通証明書であると判断した場合には、自身の識別情報が記載された被管理装置用個別公開鍵証明書を取得するようにしている。

すなわち、被管理装置１０の管理装置２０への登録は、個体認証のために行うものであり、認証の方式が変わる場合には、登録の方式もそれに合わせて変えるようにしている。そして、管理装置２０が被管理装置１０を認証して直接通信を行う場合には、被管理装置１０に個別公開鍵証明書を記憶させる必要があるため、これを記憶させるようにしているのである。

この点がこの実施形態の主要な特徴であり、以下、この特徴を実現するための処理及びそれに関連する処理について説明する。

【００６４】

ここで、図７に、被管理装置１０と管理装置２０の機能構成を、上記の特徴に関連する部分を中心に示す。なお、この図においては、被管理装置１０が管理装置２０と直接通信を行うように図示しているが、仲介装置５０が仲介する場合の通信も、通信の手順（プロトコル）が異なるのみであり、基本的には同様な機能で実現できる。

【００６５】

まず、被管理装置１０には、ＨＴＴＰＳ（HyperText Transfer Protocol Security）クライアント機能部１１，ＨＴＴＰＳサーバ機能部１２，認証処理部１３，証明書記憶部１４，要求管理部１５，被管理機能部１６を備えている。

ＨＴＴＰＳクライアント機能部１１は、ＳＳＬに従った認証や暗号化の処理を含むＨＴＴＰＳプロトコルを用いて管理装置２０等のＨＴＴＰＳサーバの機能を有する装置に対して通信を要求すると共に、通信相手に対して要求（コマンド）やデータを送信してそれに応じた動作を実行させる機能を有する。

【００６６】

一方、ＨＴＴＰＳサーバ機能部１２は、ＨＴＴＰＳクライアントの機能を有する装置からのＨＴＴＰＳプロトコルを用いた通信要求を受け付け、その装置から要求やデータを受信してそれに応じた動作を装置の各部に実行させ、その結果を応答として要求元に返す機能を有する。

認証処理部１３は、ＨＴＴＰＳクライアント機能部１１やＨＴＴＰＳサーバ機能部１２が通信相手を認証する際に、通信相手から受信したデジタル証明書や、証明書記憶部１４に記憶している各種証明書、私有鍵等を用いて認証処理を行う認証手段の機能を有する。また、通信相手に認証を要求するために証明書記憶部１４に記憶しているデジタル証明書をＨＴＴＰＳクライアント機能部１１やＨＴＴＰＳサーバ機能部１２を介して通信相手に送信する機能も有する。

【００６７】

証明書記憶部１４は、図４に示したような各種の証明書や私有鍵等の認証情報を記憶し、認証処理部１３における認証処理に供する機能を有する。

要求管理部１５は、管理装置２０から受信した要求について、その要求に基づいた動作の実行可否を判断し、実行を許可する場合に、被管理機能部１６中の、その要求に基づいた動作を実行する機能部１６ａ～１６ｅに対して動作要求を伝える機能も有する。

【００６８】

そして、これらの各機能部のうち、状態通知部１６ａは、異常を検知したりユーザによる指示があったりした場合に管理装置２０に対して被管理装置１０の状態を通知するコールを行う機能を有する。この通知は、管理装置２０からの問い合わせに対する応答として送信してもよいし、ＨＴＴＰＳクライアント機能部１１から上位装置に通信を要求して送信してもよい。

【００６９】

ログ通知部１６ｂは、被管理装置１０から管理装置２０へのログの通知を行う機能を有する。その通知の内容としては、被管理装置１０の動作ログの他、例えば画像形成装置であれば画像形成枚数カウンタのカウント値、計量システムであればその計量値等が考えられる。この通知は緊急を要さないので、管理装置２０からの問い合わせに対する応答として送信するとよい。

【００７０】

証明書更新部１６ｃは、管理装置２０から受信した証明書等によって証明書記憶部１４に記憶している証明書等を更新する機能を有する。そして、この機能により、この実施形態の特徴に関連する動作として、管理装置２０から受信した被管理装置用個別公開鍵証明書を、被管理装置用共通公開鍵証明書に代えて管理装置２０との通信に使用する証明書として設定する動作が実現される。

【００７１】
登録要求部１６ｄは、管理装置２０に対して被管理装置１０を管理対象として登録するよう要求する機能を有する。
コマンド受信部１６ｅは、上述した各機能部１６ａ～１６ｄ以外の機能に係る要求に対応する動作を実行する機能を有する。この動作としては、例えば被管理装置１０が記憶しているデータの送信や、必要に応じてエンジン部１０７の動作を制御することが挙げられる。なお、状態通知部１６ａ及びログ通知部１６ｂは、コマンド受信部１６ｅが提供する機能の具体例として示したものであり、これらのような機能を設けることは必須ではない。
そして、以上の各部の機能は、被管理装置１０のＣＰＵ１０１が所要の制御プログラムを実行して被管理装置１０の各部の動作を制御することにより実現される。
【００７２】
また、管理装置２０には、ＨＴＴＰＳクライアント機能部２１，ＨＴＴＰＳサーバ機能部２２，認証処理部２３，証明書更新要求部２４，証明書記憶部２５を，要求管理部２６，管理機能部２７、証明書発行部２８を備えている。
そして、ＨＴＴＰＳクライアント機能部２１は、被管理装置１０のＨＴＴＰＳクライアント機能部１１と同様に、ＨＴＴＰＳプロトコルを用いて被管理装置１０等のＨＴＴＰＳサーバの機能を有する装置に対して通信を要求すると共に、送信する要求やデータ等に応じた動作を実行させる機能を有する。
【００７３】
ＨＴＴＰＳサーバ機能部２２も、被管理装置１０のＨＴＴＰＳサーバ機能部１２と同様であり、ＨＴＴＰＳクライアントの機能を有する装置からの通信要求を受け付け、受信した要求やデータに応じた動作を装置の各部に実行させ、要求元に応答を返す機能を有する。
認証処理部２３の機能も、被管理装置１０の認証処理部１３と同様であるが、認証処理に使用する証明書等は、証明書記憶部２５に記憶しているものである。
【００７４】
証明書更新要求部２４は、所定の場合に、被管理装置１０等の通信相手に対して個別公開鍵証明書を送信し、これを記憶するよう要求する機能を有する。
証明書記憶部２５は、図４に示したような各種の証明書や私有鍵等の認証情報を記憶し、認証処理部２３における認証処理に供する機能を有する。
【００７５】
要求管理部２６は、被管理装置１０から受信した要求について、その要求に基づいた動作の実行可否を判断し、実行を許可する場合に、管理機能部２７中の、その要求に基づいた動作を実行する機能部に対して動作要求を伝える機能も有する。そして、ここではその機能部として登録機能部２７ａのみを示しているが、実際には他にも被管理装置１０の管理に必要な動作を行うための機能部も設ける。
【００７６】
また、登録機能部２７ａは、管理対象とすべき被管理装置１０や仲介装置５０を管理対象として登録する機能を有する。またここでは、被管理装置１０を直接管理の対象として登録する際に被管理装置１０から要求があった場合に、証明書更新要求部２４に指示して被管理装置１０に対して個別公開鍵証明書を送信させる機能も有する。
【００７７】
証明書発行部２８は、被管理装置１０に送信する個別公開鍵証明書を発行するＣＡとしての機能を有する。この機能には、過去に発行した証明書を記憶し、管理する機能を含めるとよい。そして、証明書更新要求部２４は、被管理装置１０に対して個別公開鍵証明書を送信しようとする場合、ここから証明書を取得する。ただし、証明書発行部２８を管理装置２０の内部に設けず、外部のＣＡから証明書を取得するようにしてもよい。
そして、これらの各部の機能は、管理装置２０のＣＰＵが所要の制御プログラムを実行して管理装置２０の各部の動作を制御することにより実現される。

【００７８】
次に、被管理装置１０が管理装置２０に対して直接管理の対象として登録を要求する場合に行う処理について説明する。
この登録の要求は、ユーザの指示に従って行うことが考えられる。そして、この指示を受け付けるためのユーザＩ／Ｆとしては、例えば、被管理装置１０にウェブサービス機能を設け、外部のＰＣ等に備えるブラウザや専用クライアントアプリケーションによって被管理装置１０にアクセスし、被管理装置１０から取得したデータに基づいてディスプレイに表示させた画面中のグラフィカルユーザインタフェース（ＧＵＩ）によって指示を受け付けるようにすることが考えられる。また、被管理装置１０の操作部１０６に備えるディスプレイに同様なＧＵＩを表示させて設定操作を受け付けることができるようにしてもよい。被管理装置１０にブラウザの機能を設けてこのような動作を実現してもよい。
【００７９】
以下、画面例については、ユーザＩ／Ｆとしてブラウザを利用する場合に好適な例について説明する。
図８に、上記のような登録指示を受け付けるための画面の例として、管理用初期画面の表示例を示す。
この図に示す管理用初期画面２００は、被管理装置１０の管理者が種々の設定を行ったり被管理装置１０の稼動状況を参照したりするための画面である。そして、ユーザがユーザＩ／Ｆによって被管理装置１０にアクセスし、管理者用モードの動作を選択した場合、まずこの管理用初期画面２００を表示させるようにしている。
【００８０】
そして、この画面には、被管理装置１０に動作を指示するためのボタンとして、状態ボタン２０１，設定ボタン２０２，設置ボタン２０３を設けている。
このうち状態ボタン２０１は、被管理装置１０においてなされている設定の状態や、被管理装置１０の動作状況を確認するための画面の表示を指示するためのボタンであり、設定ボタン２０２は、被管理装置１０における種々の設定、例えばネットワーク通信設定やユーザの登録、および例えば被管理装置１０がデジタル複合機である場合にはコピーやプリント等の動作の実行に関する設定を行うための画面の表示を指示するボタンである。なお、これらの機能については、この実施形態の特徴とあまり関係ないため、詳細な説明は省略する。
【００８１】
そして、設置ボタン２０３が、被管理装置１０の管理装置２０への登録を行うための画面の表示を指示するボタンである。ただし、このボタンの押下に応じてユーザＩ／Ｆに表示させる画面は、被管理装置１０が記憶している表１に示すような登録完了フラグ及び仲介機能利用フラグの状態によって異なる。
【表１】

登録完了フラグ	被管理装置１０が管理装置２０に管理対象として登録されているか否かを識別するためのフラグ
仲介機能利用フラグ	被管理装置１０が管理装置２０と通信する際に自身の仲介機能を利用するか否かを識別するためのフラグ

【００８２】
そして、登録完了フラグは、被管理装置１０が管理装置２０に管理対象として登録された場合にＯＮにするフラグであり、直接被管理状態か間接被管理状態かに関わらず、管理装置２０に登録された場合にＯＮにするようにしている。また、仲介機能利用フラグは、被管理装置１０が自身の仲介機能を利用して管理装置２０と通信を行う旨が管理装置２０に登録され、直接被管理状態となった場合にＯＮにするフラグである。これらのフラグの内容は、不揮発性メモリ１０４に記憶させ、被管理装置１０の電源がＯＦＦされても記憶

しておくようにする。

【００８３】

また、被管理装置１０は、動作中に適宜これらのフラグを参照し、登録完了フラグがＯＮの場合に管理装置２０による遠隔管理を受ける機能を有効にし、さらに仲介機能利用フラグがＯＮの場合に、自身の仲介機能を有効にし、直接被管理機能を有効にするようにしている。また、仲介機能利用フラグがＯＦＦである場合には、仲介機能は無効にし、間接被管理機能を有効にして、遠隔管理を受けるための通信は、仲介装置５０を介して行うようにしている。

【００８４】

次に、図９及び図１０に、設置ボタン２０３の押下に応じて被管理装置１０のＣＰＵ１０１が実行する処理のフローチャートを示す。

ＣＰＵ１０１は、図８に示した管理用初期画面２００において設置ボタン２０３が押下されたことを検出すると、図９のフローチャートに示す処理を開始する。

そして、まずステップＳ１１で、表１に示した登録完了フラグがＯＮであるか否か判断する。そして、ＯＮでなければ登録に関する処理を行うべくステップＳ１２に進み、ユーザＩ／Ｆに未登録画面のデータを送信してこの画面を表示させる。

ここでは、まず未登録画面の内容及びその画面において受け付けた操作に応じた処理について説明する。

【００８５】

図１１に、この未登録画面の表示例を示す。

この未登録画面２１０は、被管理装置１０を管理装置２０に登録する指示を行うための画面である。なお、管理装置２０との間で仲介装置５０を介した通信を行おうとする場合には、被管理装置１０の登録は、通信を仲介させる仲介装置５０から行うようにしているため、被管理装置１０を操作して管理装置２０への登録を行うということは、被管理装置１０が自身の仲介機能を利用して管理装置２０と通信する直接管理の対象となる旨の登録を行おうとしていることを意味する。

【００８６】

また、ユーザが管理用初期画面２００において設置ボタン２０３が押下した場合にこの画面に移行するということは、被管理装置１０は管理装置２０に登録されていないことを示すものである。

そして、このような未登録画面２１０には、登録ボタン２１１，状態表示部２１２，登録番号入力部２１３，及び戻るボタン２１４を設けている。

このうち状態表示部２１２は、被管理装置１０の現在の状態を表示する部分であるが、未登録画面２１０においては、通常は、未だ登録がなされていないことを示す「未登録」である。

【００８７】

また、登録番号入力部２１３は、照会を行なうため、ユーザが管理装置２０の運用者から予め通知されている登録番号を入力する部分である。この登録番号としては、例えば管理契約の契約書番号等が考えられるが、パスワードのような、番号以外の識別情報でもよい。

そして、登録ボタン２１１は、被管理装置１０に照会動作の実行を指示するためのボタンであり、ユーザが登録番号入力部２１３に必要な情報を入力した後でこのボタンを押下すると、被管理装置１０は、管理装置２０に対して、登録番号入力部２１３に入力された情報を用いて登録を要求する。

【００８８】

フローチャートの説明に戻ると、図９のステップＳ１２の後、処理は図１０のステップＳ１８に進むが、この図１０に示す部分の処理が、未登録画面２１０で受け付ける操作に応じた処理である。

そして、ＣＰＵ１０１は、図１０のステップＳ１８，Ｓ３４において、未登録画面２１０の登録ボタン２１１と戻るボタン２１４のいずれかが押下されるまで待機する。

【００８９】
そして、登録ボタン２１１が押下されると、ステップＳ１９で、登録番号入力部２１３に登録番号が入力されているか否か判断する。そして、入力されていなければ、ステップＳ２０でエラー表示を行って登録番号が入力されていない旨をユーザに報知し、ステップＳ１８に戻って再度入力を受け付ける。
一方、ステップＳ１９で登録番号が入力されていれば、ステップＳ２１に進み、管理装置２０との通信時の認証処理に使用する旨が設定されている認証情報を用いて管理装置２０との間で認証処理を行い、通信経路を確立する。この処理は、より具体的には、公開鍵証明書等を用いてＳＳＬによる認証処理を行うものである。また、ここで使用する公開鍵証明書は、共通公開鍵証明書である場合もあるし、製造時や過去に登録を行った際に個別公開鍵証明書が設定されていれば、個別公開鍵証明書を使用できる場合もある。
そして、通信経路が確立できると、ステップＳ２２で登録番号入力部２１３に入力された情報を管理装置２０に送信して自機の登録を要求して応答を取得する。このとき、必要があれば、ＩＤ等、被管理装置１０自身の識別情報も共に送信するようにしてもよい。
【００９０】
なお、通信先アドレス等の管理装置２０との通信に必要な情報は予め設定しておくものとする。また、この登録要求については、被管理装置１０側でから管理装置２０側に一方的に送信して応答を取得すればよく、被管理装置１０側で管理装置２０側からの要求を受信して処理する必要はないので、仲介機能を有効にしなくても、通常のネットワーク通信機能により対応可能な内容である。通信先アドレス等の情報は予め設定しておく必要はあるが、このような設定は図示しない公知の手法により予め行っておくものとする。
【００９１】
また、上述したように、ここでの登録は、被管理装置１０が直接管理の対象となる旨の登録を意味する。
また、管理装置２０側での登録は、被管理装置１０を、被管理装置として登録すると共に、被管理装置１０と通信するための仲介装置としても登録して行うようにし、後述する間接管理の場合の登録と、データ形式を統一できるようにするとよい。
【００９２】
そしてその後、ステップＳ２３で登録が成功したか否かを管理装置２０からの応答により判断し、登録成功（ＯＫ）であれば、ステップＳ２４に進んで登録完了フラグ及び仲介機能利用フラグをＯＮにして、管理装置２０に直接管理の対象として登録されたことを示し、仲介機能を有効にする。
そして、以降の個別証明書の取得及び設定に関する処理に進む。
【００９３】
この部分の処理では、まずステップＳ２５で、管理装置２０との通信に使用する証明書として設定されている証明書が機器の識別情報が記載されていない共通証明書（被管理装置用共通公開鍵証明書）であるか否か判断する。そして、共通証明書であれば、ステップＳ２６で自機のＩＤを管理装置２０に送信し、以後の通信に使用する個別証明書として、自機のＩＤを記載した個別証明書である被管理装置用個別公開鍵証明書の送信を要求する。
管理装置２０は、そのＩＤにより送信元の被管理装置１０を認証し、ＩＤが確かに登録した被管理装置１０のものである（又は通信相手として適当な被管理装置のものである）と確認できると、そのＩＤを記載した公開鍵証明書を生成し、私有鍵及びルート鍵証明書とセットにして個別証明書セットとして送信してくるので、ステップＳ２７でこれを受信する。
【００９４】
ここで、図１６に、ここで受信する個別証明書セットの構成を示す。
この図に示すように、個別証明書セットには、被管理装置用個別公開鍵証明書の他に、被管理装置用個別私有鍵と管理装置認証用ルート鍵証明書が含まれる。
そして、このうち被管理装置用個別公開鍵証明書は、図６に示したような、発行先装置

の識別情報としてその装置のＩＤの情報を記載した公開鍵証明書であり、被管理装置用個別私有鍵は、その公開鍵証明書に含まれる公開鍵と対応する私有鍵である。また、管理装置認証用ルート鍵証明書は、管理装置２０が被管理装置１０との通信に使用する公開鍵証明書の正当性を確認するためのルート鍵に、自己署名形式の署名を行ったデジタル証明書である。また、被管理装置用個別公開鍵証明書の正当性は、被管理装置用共通公開鍵証明書の場合と同じルート鍵で確認できるようにするとよいが、このようにすることは必須ではない。確認に異なるルート鍵を用いる場合でも、その分のルート鍵証明書を管理装置２０側に記憶させておけばよい。

【００９５】

なお、ここでは管理装置２０がこれらを証明書セットとして送信するようにしているが、最低限は被管理装置用個別公開鍵証明書のみを送信すればよい。ルート鍵証明書については、管理装置２０側の証明書を変更するわけではないので、登録前と同じものを使うことができるし、公開鍵証明書についても、書誌事項を変更して証明書を発行し直せば、公開鍵本体を変更することが必須ではないためである。

【００９６】

図１０のフローチャートの説明に戻ると、ステップＳ２７の後、処理はステップＳ２８に進み、ＣＰＵ１０１は、受信した証明書（被管理装置用個別公開鍵証明書）に記載されているＩＤが自身のものと一致するか否か判断する。ここで誤った証明書を設定してしまうと、管理装置２０との間の通信を行えなくなってしまうためである。

そして、一致していれば、ステップＳ２９で受信した個別証明書セットを管理装置２０との通信に使用する認証情報として設定する。

【００９７】

その後、ステップＳ３０で管理装置との間の通信セッションを一旦終了し、ステップＳ３１で、ステップＳ２９で設定した個別証明書セットを用いて管理装置２０との間で認証処理を行い、通信経路を確立する。この処理は、より具体的には、公開鍵証明書等を用いてＳＳＬによる認証処理を行うものである。

そして、ステップＳ３２で個別証明書セットの設定結果を管理装置２０に通知し、ステップＳ３３でユーザＩ／Ｆに登録完了画面のデータを送信してこの画面を表示させる。

【００９８】

図１２に、この登録完了画面の表示例を示すが、この登録完了画面２２０は、ユーザに被管理装置１０の管理装置２０への登録が完了したことを通知するためのものであり、ユーザがＯＫボタン２２１を押下すると、図８に示した管理用初期画面２００に戻る。

フローチャートにおいては、この処理を図９のステップＳ１６及びＳ１７に示しており、図１０のステップＳ３３の後は、図９のステップＳ１６に進んでＯＫボタン２２１が押下されるまで待機し、その後ステップＳ１７でユーザＩ／Ｆに管理用初期画面２００のデータを送信してこの画面を表示させ、設置ボタン２０３の押下に応じた一連の処理を終了して、管理用初期画面２００における操作受け付けの処理に戻る。

【００９９】

また、図１０のステップＳ２８で受信した証明書に記載されているＩＤが自身のものと一致しなかった場合には、証明書が異常であると判断し、個別証明書セットの登録を行わずに、ステップＳ３６でユーザＩ／Ｆに一部登録完了画面のデータを送信してこの画面を表示させる。

【０１００】

図１３に、この一部登録完了画面の表示例を示すが、この一部登録完了画面２３０は、ユーザに被管理装置１０の管理装置２０への登録が完了したものの、個別証明書の設定は失敗したことを通知するための画面であり、ユーザがＯＫボタン２３１を押下すると、上述した登録完了画面２２０の場合と同様に図８に示した管理用初期画面２００に戻る。

フローチャートにおいては、図９のステップＳ１６に進んで以後の処理を行う。

そして、この場合、当面は管理装置２０との間の通信を共通証明書を用いて行うが、次回以降に被管理装置１０が起動された場合、または管理装置２０と通信を行おうとする場

合に、改めて個別証明書の取得を試みるようにする。この点については、図２５の説明において後述する。

【０１０１】

また、図１０のステップＳ２５で既に個別証明書が設定されていた場合には、新たに個別証明書の取得を行う必要はないので、そのままステップＳ３３に進み、ユーザＩ／Ｆに登録完了画面のデータを送信してこの画面を表示させる。

また、ステップＳ２３で登録失敗（ＮＧ）であった場合には、ステップＳ３５に進み、ユーザＩ／Ｆに登録失敗画面のデータを送信してこの画面を表示させる。

【０１０２】

図１４に、この登録失敗画面の表示例を示すが、この登録失敗画面２４０は、ユーザに登録の過程で不具合が起きたことを通知するためのものであり、ユーザがＯＫボタン２４１を押下すると、上述した登録完了画面２２０の場合と同様に図８に示した管理用初期画面２００に戻る。

フローチャートにおいては、図９のステップＳ１６に進んで以後の処理を行う。

【０１０３】

また、図１０のステップＳ３４で戻るボタン２１４が押下された場合には、図９のステップＳ１７に進み、ユーザＩ／Ｆに管理用初期画面２００のデータを送信してこの画面を表示させ、設置ボタン２０３の押下に応じた一連の処理を終了して、管理用初期画面２００における操作受け付けの処理に戻る。

【０１０４】

次に、設置ボタン２０３が押下された時点で既に被管理装置１０の管理装置２０への登録が完了していた場合の処理について説明する。

この場合、登録完了フラグはＯＮになっているので、図９のステップＳ１１の判断はＹＥＳになり、処理はステップＳ１３に進む。そして、ステップＳ１３では、仲介機能利用フラグがＯＮか否か判断する。

【０１０５】

そして、ＯＮであれば、被管理装置１０は、管理装置２０において直接管理の対象として登録がされていることがわかり、図１０のステップＳ３３の場合と同様な状態であるので、ステップＳ１４で、ユーザＩ／Ｆに図１０のステップＳ３３の場合と同様な登録完了画面２２０のデータを送信してこの画面を表示させる。そして、ＯＫボタン２２１が押下された場合に管理用初期画面２００に戻ることも、上述した通りである。

すなわち、このケースでは、新たに照会や登録の指示を受け付けることはない。なおこのとき、個別証明書の設定の有無を判断し、設定されていない場合に、図１０のステップＳ３６の場合のような一部登録完了画面２３０を表示させるようにしてもよい。

【０１０６】

また、ステップＳ１３で仲介機能利用フラグがＯＦＦであれば、被管理装置１０は、管理装置２０において間接管理の対象として登録されていることがわかる。この場合、新たに直接管理の対象としての登録を可能としてしまうと、二重登録が行われることになったり、管理装置２０側の処理も含めて通信の管理が複雑になってしまうので、ステップＳ１５に進んでユーザＩ／Ｆに未登録画面ではなく間接通信登録済み画面のデータを送信し、この画面を表示させるようにしている。すなわち、間接被管理機能が有効な場合には、直接被管理機能を有効にしないようにしている。

【０１０７】

図１５に、この間接通信登録済み画面の表示例を示すが、この間接通信登録済み画面２５０は、既に被管理装置１０が間接管理の対象として管理装置２０に登録されていることを通知するためのものであり、ユーザがＯＫボタン２５１を押下すると、図８に示した管理用初期画面２００に戻る。このために実行する処理は、上述した登録完了画面２２０の場合と同様なものである。

なお、以上説明してきた図９及び図１０の処理において、ステップＳ２５乃至Ｓ３２の処理が、証明書取得手順の処理であり、これらの処理においてはＣＰＵ１０１が証明書取

得手段として機能する。

【０１０８】

次に、図１７及び図１８に、上述したような処理により被管理装置１０を直接管理の対象として管理装置２０に登録する場合のこれらの装置の動作シーケンス例を示す。なおここでは、被管理装置１０には管理装置２０と通信するために用いる公開鍵証明書として共通証明書が設定されているものとする。

この場合、ユーザがＰＣ等に備えるユーザＩ／Ｆ７０により被管理装置１０にアクセスし、管理者モードでの操作を要求すると（Ｓ１０１）、被管理装置１０は管理用初期画面２００のデータをユーザＩ／Ｆ７０に渡し（Ｓ１０２）、ユーザＩ／Ｆ７０はこのデータに基づき管理用初期画面２００を表示する（Ｓ１０３）。

【０１０９】

そして、ユーザがこの画面で設置ボタン２０３を押下すると、そのイベントを被管理装置１０に伝達し（Ｓ１０４）、ここでは被管理装置１０は未登録状態であるので、被管理装置１０がフラグの状態からその旨判断し（Ｓ１０５）、未登録画面２１０のデータをユーザＩ／Ｆ７０に渡す（Ｓ１０６）。そして、ユーザＩ／Ｆ７０はこのデータに基づき未登録画面２１０の表示を行う（Ｓ１０７）。

そして、ユーザがこの画面において登録番号を入力すると共に登録ボタン２１１を押下すると、ユーザＩ／Ｆ７０はこのイベント及び入力された登録番号を被管理装置１０に伝達する（Ｓ１０８）。

【０１１０】

すると、被管理装置１０は、共通証明書を用いて管理装置２０との間で通信経路を確立し（Ｓ１０９），管理装置２０に対して登録要求と共に入力された登録番号を送信する（Ｓ１１０）。このとき、自機の識別情報であるＩＤも送信するようにしてもよい。そして、管理装置２０は登録要求に応じて、被管理装置１０が送信してきた登録番号が正しいものであることを確認する照会処理（Ｓ１１１）を行い、その照会処理が成功した場合に、被管理装置１０を直接管理の対象として登録する登録処理を行う（Ｓ１１２）。そして、それらの結果を示す登録応答を返す（Ｓ１１３）。

そして、被管理装置１０はこの登録応答に応じて必要なフラグを設定して直接被管理状態に移行する（Ｓ１１４）。

【０１１１】

また、被管理装置１０がここで、設定されている証明書が共通公開鍵証明書であると判断すると（Ｓ１１５）、管理装置２０に対して自機のＩＤと共に認証情報送信要求を送信する（Ｓ１１６）。そして、管理装置２０は、この要求を受けると、被管理装置１０から受信したＩＤにより送信元の被管理装置１０を認証し、個別証明書セットを発行してよいか否か判断する（Ｓ１１７）。例えば、管理対象となっている装置であれば、発行してよいとすることができる。そして、発行してよい場合には、個別証明書セットを発行し（Ｓ１１８）、図１８に示す処理に進んで、発行した個別証明書セットを証明書設定要求と共に被管理装置１０に送信する（Ｓ１１９）。

【０１１２】

そして、被管理装置１０は、これを受信すると、受信した個別証明書セットに含まれる公開鍵証明書に記載されているＩＤが自身のものと一致することを確認し（Ｓ１２０）、確認できると受信した個別証明書セットを管理装置２０との通信に使用する証明書セットとして設定する（Ｓ１２１）。

【０１１３】

そしてその後、管理装置２０との間のセッションを一旦終了し（Ｓ１２２）、ステップＳ１２１で設定した個別証明書セットに含まれる個別証明書を用いて再度管理装置２０との間で通信経路を確立し（Ｓ１２３）、管理装置２０に証明書の更新結果を通知する（Ｓ１２４）。また、登録完了画面２２０のデータを生成してユーザＩ／Ｆ７０に送信し（Ｓ１２５）、ユーザＩ／Ｆ７０はこのデータに基づき登録完了画面２２０の表示を行う（Ｓ１２６）。

以上のような動作を行うことにより、被管理装置１０の管理装置２０への登録及び、被管理装置１０に個別証明書が設定されていない場合には個別証明書の取得及び設定を完了することができる。

【０１１４】

次に、図１９乃至図２３を用いて、被管理装置１０に仲介装置５０を介して管理装置２０と通信させる場合、すなわち被管理装置１０を間接管理の対象として管理装置２０に登録する場合の被管理装置１０の管理装置２０への登録処理について説明する。

図１に示した管理システムにおいては、このような場合、通信を仲介させる仲介装置５０が管理装置２０に未登録であれば、まず仲介装置５０を管理装置２０に登録させるようにしている。

【０１１５】

そこで、図１９に、ユーザが仲介装置５０にユーザＩ／Ｆ８０を用いてアクセスし、仲介装置５０を管理装置２０に登録する際の動作シーケンス例を示す。なお、この図以降の図においては、各装置間の通信経路確立に関する処理の図示は省略している。

図１に示した例においては、仲介装置５０にもユーザＩ／Ｆを介してユーザがアクセスできるようにしている。一例としては、ウェブサービス機能を設け、ＰＣ等に備えるブラウザによって仲介装置５０にアクセスして画面の表示に必要なデータを取得し、ディスプレイに表示させた画面中のＧＵＩにより仲介装置５０の設定操作を行うことができるようにすることが考えられる。ただし、被管理装置１０に対する指示を受け付けるためのユーザＩ／Ｆと、仲介装置５０に対する指示を受け付けるためのユーザＩ／Ｆとが共通である必要はない。

そして、図１９に示すように、この場合の動作シーケンスは、図１７に示した、管理装置２０と直接通信する被管理装置１０を管理装置２０に登録する際の動作シーケンスと、個別証明書の取得に係る処理がない点以外は概ね同様なものである。なお、以下の説明においても、画面例は、ユーザＩ／Ｆとしてブラウザを利用する場合に好適な例を示す。

【０１１６】

すなわち、まずユーザＩ／Ｆ８０に未登録画面を表示させ（Ｓ２０１～Ｓ２０４）、その後登録番号を入力して登録動作を実行させる（Ｓ２０５～Ｓ２１２）という手順になる。

なお、ここでは、仲介装置５０はインターネット４０のような開いたネットワークを介して管理装置２０と通信することが可能であり、このため、初めから個別証明書を記憶させるようにしているので、登録時に個別証明書の取得に係る処理を設けていないが、被管理装置１０と同様に、登録時に個別証明書を取得できるようにすることも考えられる。

【０１１７】

また、これらの動作においてユーザＩ／Ｆ８０に表示させる画面は、仲介装置５０用であることに伴って被管理装置１０の場合とは若干異なるが、図８等に示したものと概ね同様であるので、図示は省略する。

そして、以上の動作により仲介装置５０を管理装置２０に登録した後では、ユーザは、仲介装置５０に、通信を仲介可能な被管理装置１０や他の仲介装置５０を検索させ、その装置の管理装置２０への登録を行わせることができる。

【０１１８】

図２０に、この動作シーケンスを示す。なお、この図に示すのは、被管理装置１０が未登録状態の場合の動作である。

仲介装置５０が既に管理装置２０に登録されている場合、ユーザがユーザＩ／Ｆ８０により仲介装置５０にアクセスして登録に関する操作を要求すると、仲介装置５０はユーザＩ／Ｆ８０に機器登録画面のデータを送信し、この画面を表示させる（Ｓ２２１～Ｓ２２４）。

【０１１９】

図２１にこの機器登録画面の表示例を示すが、機器登録画面３１０には、仲介装置５０に対して、通信を仲介可能な他の通信装置の検索を指示するための、機器検索ボタン３１

１を設けている。また、図２１には示していないが、仲介装置５０を特定するための識別情報等もこの画面に表示させるようにしてもよい。

【０１２０】

図２０の説明に戻ると、以上のような機器登録画面３１０においてユーザが機器検索ボタン３１１を押下すると、ユーザＩ／Ｆ８０はそのイベントを仲介装置５０に伝達する（Ｓ２２５）。

そして、仲介装置５０はこれに応じて、通信装置の検索のための機器検索要求（動作要求の一種である）の送信を行う（Ｓ２２６）。なお、検索を行うまで実際にどのような機器が存在するかはわからないので、この要求は、所定のＩＰアドレス範囲、同一ネットワーク内等の所定の範囲内にブロードキャストし、その範囲内の任意の装置から応答を受け取ることができるようにするとよい。

【０１２１】

ここでは被管理装置１０が機器検索要求の送信範囲内にあるとすると、被管理装置１０は、機器検索要求を受信した際、自機が未登録状態であり、仲介装置５０に通信の仲介を受けることができると判断するので（Ｓ２２７）、機器検索応答と共に自機の識別情報を仲介装置５０に返す（Ｓ２２８）。機器検索要求の送信範囲内に他にも仲介装置５０が通信を仲介可能な装置があれば、仲介装置５０はその装置からも同様に応答を受け取る。

そして、仲介装置５０は、受信した応答を基に検索結果画面のデータを生成してユーザＩ／Ｆ８０に送信し（Ｓ２２９）、この画面を表示させる（Ｓ２３０）。

【０１２２】

図２２に、この検索結果画面の表示例を示す。

この検索結果画面３２０は、ステップＳ２２６で仲介装置５０が行った検索の結果を表示すると共に、発見された機器のうち登録が可能なものについて、仲介装置５０を介して管理装置２０と通信する間接管理の対象として管理装置２０に登録する指示を行うための画面である。

【０１２３】

そして、このような検索結果画面３２０には、登録ボタン３２１及び、発見された各機器についての機器情報表示部３２２を設けている。また、機器情報表示部３２２内には、該当機器の識別情報であるＩＤを表示するＩＤ表示部３２３と、該当機器の現在の状態を表示する状態表示部３２４と、登録を行うため、ユーザが管理装置２０の運用者から予め通知されている登録番号を入力する登録番号入力部３２５とを設けている。登録番号としては、直接管理の場合と同様、契約番号等を使用するようにすることができる。

【０１２４】

そして、登録ボタン３２１は、仲介装置５０に、登録番号を入力した機器の登録実行を指示するためのボタンであり、ユーザが登録を希望する機器について登録番号入力部３２４に必要な情報を入力した後でこのボタンを押下すると、仲介装置５０は、管理装置２０に対して、その機器の登録を要求する。

【０１２５】

シーケンス図の説明に戻ると、ユーザが検索結果画面３２０において登録を行いたい機器に係る登録番号を入力し、登録ボタン３２１を押下すると、ユーザＩ／Ｆ８０はそのイベント及び登録番号を仲介装置５０に伝達する（Ｓ２３１）。

すると、仲介装置５０は、これに応じて管理装置２０に対して登録要求と共にその受け取った登録番号を送信する（Ｓ２３２）。またここでは、管理装置２０は直接被管理装置１０との間で認証処理を行っているわけではないので、被管理装置１０の情報も送信する。そして、管理装置２０はそれらの情報に基づき、図１７のステップＳ１１１及びＳ１１２の場合と同様に照会処理及び登録処理を行い（Ｓ２３３，Ｓ２３４）、その結果を示す登録応答を返す（Ｓ２３５）。

【０１２６】

そして、登録が成功した場合、仲介装置５０は、登録された機器（ここでは被管理装置１０とする）に対して登録通知を送信する（Ｓ２３６）。そして、被管理装置１０はこの

通知を受信すると、登録完了フラグをＯＮにする一方、仲介機能利用フラグはＯＦＦのままにし、また仲介装置５０と通信を行うために必要な設定を行って、仲介装置５０を介して管理装置２０と通信する間接被管理状態に移行し（Ｓ２３７）、仲介装置５０に対して登録応答（Ｓ２３８）を送信する。

【０１２７】

以上で、被管理装置１０は、仲介装置５０を介して管理装置２０と通信を行い、管理装置２０による管理を受けることができる状態になる。

なお、ステップＳ２３１で複数の機器に関する登録番号が入力されていた場合には、仲介装置５０は該当する全ての機器についてステップＳ２３２乃至ステップＳ２３８の処理を行う。

そして、必要な全ての装置から登録応答を受信すると、ユーザＩ／Ｆ８０に登録結果画面のデータを送信し（Ｓ２３９）、この画面を表示させる（Ｓ２４０）。

【０１２８】

図２３に、この登録結果画面の表示例を示すが、この登録結果画面３３０は、ユーザに管理装置２０への登録が完了した機器の情報を通知するためのものであり、ユーザがＯＫボタン３３１を押下すると、登録に関する処理を終了する。

図１に示した管理システムにおいては、以上のような動作シーケンスにより、新たにＬＡＮに接続された装置等、まだ管理装置２０に登録されていない装置の登録を、仲介装置５０を介して行うことができる。

なお、既に直接管理の対象として管理装置２０に登録されている被管理装置１０については、仲介装置５０と通信可能な位置にあったとしても機器検索要求に応答しないようにしておけば、間接管理の対象としても管理装置２０に登録されてしまい、登録が二重になってしまうような事態を防止できる。

【０１２９】

次に、図２４に、被管理装置１０が起動時に実行する処理のフローチャートを示す。上述したように、被管理装置１０を直接管理の対象として管理装置２０に登録する際に個別証明書の取得に失敗した場合には、その後被管理装置１０は再起動時等に再度個別証明書の取得を試みるが、図２４に示す処理は、このための処理を含むものである。

被管理装置１０のＣＰＵ１０１は、被管理装置１０の起動時に図２４のフローチャートに示す処理を開始する。

【０１３０】

そして、まずステップＳ４１で登録完了フラグの値を参照し、これがＯＮ（登録済み）であれば、ステップＳ４２に進む。そしてここでは、仲介機能利用フラグの値を参照し、これがＯＮ（利用する）であれば、ステップＳ４３に進む。このケースでは、被管理装置１０は直接被管理機能を有効にすることになる。

そして、この場合、ステップＳ４３で管理装置２０との通信に使用する証明書として設定されている証明書が機器の識別情報が記載されていない共通証明書であるか否か判断し、共通証明書であれば、ステップＳ４４以下に進み、ステップＳ５１までの処理により、図１０のステップＳ２６乃至Ｓ３２の場合と概ね同様に、個別証明書セットを管理装置２０から取得して設定する。そしてその後、ステップＳ５４で直接被管理状態の動作を行うようにしている。

【０１３１】

なおここでは、ステップＳ４７でＩＤが自身のものと一致しなくても、ステップＳ５５でユーザにエラーを通知した後直接被管理状態に移行するようにしているが、このような場合に、証明書が取得できるまでは管理装置２０による管理を受けない独立機器として動作させるようにしてもよい。

【０１３２】

一方、ステップＳ４３で共通証明書でなければ、すなわち個別証明書であれば、新たに個別証明書を取得する必要はないため、そのままステップＳ５４に進んで直接被管理状態の動作を行う。

また、ステップＳ４２で仲介機器利用フラグがＯＦＦ（利用しない）であれば、ステップＳ５３に進み、間接被管理機能を有効にして間接被管理状態の動作を行う。
また、ステップＳ４１で登録完了フラグがＯＦＦ（未登録）の場合には、ステップＳ５２に進み、被管理機能を無効にして独立機器としての動作を行う。
なお、ステップＳ５２乃至Ｓ５４の動作は、被管理装置１０の電源がＯＦＦされたり再起動されたりするまで行うものであり、その内容としては、種々のイベントの発生を監視し、イベントが発生した場合にそれに対応した処理を行うことが考えられる。

【０１３３】

次に、図２５に、被管理装置１０が図２４に示した処理により管理装置２０から個別証明書を取得する場合の処理シーケンス例を示す。
この図からわかるように、この処理は、図１７及び図１８を用いて説明した登録時の処理と概ね同様なものである。

【０１３４】

すなわち、被管理装置１０が起動時にフラグの状態から直接被管理機能を有効にすべきと判断し（Ｓ１３１）、かつ共通証明書が設定されていると判断すると（Ｓ１３２）、共通証明書を用いて管理装置２０との間で通信経路を確立した上で（Ｓ１３３）、図１７のステップＳ１１６乃至図１８のステップＳ１２４の場合と同様に、管理装置２０から個別証明書セットを取得して設定する処理を行う（Ｓ１３４～Ｓ１４２）。
そして、個別証明書セットの設定が完了した後は、そこに含まれる個別証明書を用いて確立した通信経路により、直接管理状態の動作に係る通信を行うようにしている（Ｓ１４３）。

【０１３５】

ところで、一旦直接管理機能を有効にした後でも、機器の配置換えや、契約期間の満了等により、被管理装置１０の管理を停止する場合もある。そして、このような場合には、管理装置２０における被管理装置１０の登録を抹消するが、被管理装置１０側においても、被管理機能の一部として、これに対応した処理を行う機能を設けている。

【０１３６】

図２６に、このような登録抹消時の処理シーケンス例を示す。
ユーザからの指示により被管理装置１０が管理装置２０に登録解除を求めたり、あるいは管理装置２０側で被管理装置１０の登録を解除すべきと判断したりした場合、管理装置２０は、図２６に示すように、登録解除要求を被管理装置１０に送信する（Ｓ１５１）。そして、管理装置２０側で被管理装置１０の登録を抹消する（Ｓ１５２）。
一方、被管理装置１０側では、登録解除要求を受信すると、登録済みフラグ及び仲介機能利用フラグをクリアする（Ｓ１５３）と共に、独立機器としての動作に移行する（Ｓ１５４）。このとき、自身を再起動して再度図２４に示した処理を行うようにしてもよい。

【０１３７】

以上の処理により、一旦管理装置２０の管理対象となった被管理装置１０を管理対象から外すことができる。ただし、この場合において、被管理装置１０に記憶させた個別公開鍵証明書を抹消する必要はない。そして、被管理装置１０がこの証明書を記憶した状態で再度管理装置２０による直接管理の対象として登録される場合には、新たに個別証明書を取得しなくても、その記憶した証明書を用いて通信を行うようにすることができる。ただし、再登録時に新たに個別証明書を取得することを妨げるものではない。
また、間接被管理の登録を抹消する場合にも、間に仲介装置５０を介す点以外は概ね同様な処理により行うことができるが、仲介装置５０においても、被管理装置１０が通信の仲介対象である旨の登録を抹消するようにする。

【０１３８】

以上で実施形態の構成及び動作の説明を終了するが、以上説明してきた実施形態によれば、被管理装置１０が、直接被管理機能が有効な状態で、管理装置２０と通信する際に使用する証明書が、機器の識別情報が記載されていない共通証明書であると判断した場合に、自身の識別情報が記載された個別証明書を取得するようにしている。従って、始めは被

管理装置１０に容易に設定可能な共通証明書を記憶させておいたとしても、より高度なセキュリティを確保する必要が生じる場合には自動的に個別証明書を取得させることができる。また、間接被管理機能を有効にして間接管理を行う場合には、改めて個別証明書を用意しなくても、共通証明書を利用した認証処理を行わせることができる。そして、このことにより、被管理装置１０及びそれを備える管理システムにおいて効率よく高いセキュリティを確保できるようにすることができる。

【０１３９】

さらに、被管理装置１０に、取得した個別証明書を管理装置２０と通信する際に使用する証明書として設定させるようにしているので、ユーザが証明書の設定操作を行わなくても、自動的に個別証明書を用いた認証処理が可能な状態にすることができる。

また、個別証明書の取得を、それまでに記憶していたデジタル証明書である共通証明書を用いて確保した通信経路で行わせるようにしているので、暗号化した通信経路で証明書を転送することができるので、個別証明書の盗用を防止することができる。

【０１４０】

また、被管理装置１０に、個別証明書を取得する際に、管理装置２０に自身の識別情報を送信させるようにしているので、管理装置２０側で個別証明書を用意する際に、被管理装置１０に記憶させるべき証明書を容易かつ確実に用意することができる。

また、管理装置２０に、被管理装置１０から受信した識別情報によりその送信元の被管理装置を認証させて個別証明書を送信してよいかどうか確認させ、その認証が成功した場合のみ被管理装置１０に個別証明書を送信するようにしているので、誤って無関係な装置に個別証明書を送信してしまうことを防止できる。

【０１４１】

また、被管理装置１０に、管理装置２０に送信した識別情報と、取得した個別証明書に記載されている識別情報とが一致しない場合に、異常であると判断させるようにしているので、誤った証明書を設定してしまい、以後の認証処理が行えなくなってしまうような事態を防止できる。

さらに、直接被管理機能により管理を受ける際に用いる識別情報を管理装置２０に送信し、管理装置２０から管理対象として登録できる旨の応答を受けた場合に個別証明書の取得を行わせるようにしているので、個別証明書を取得できない場合に取得を試み、無駄な通信や判定処理を行ってしまうことを防止できる。

【０１４２】

また、間接被管理機能が有効な場合には、直接被管理機能を有効にしないようにしているので、被管理装置１０が管理装置２０と２つの経路で通信を行ってしまい、管理装置２０側の管理処理が煩雑になる事態を防止することができる。

【０１４３】

以上で実施形態の説明を終了するが、以上説明してきた実施形態及び変形例において、システムの構成、具体的な処理内容、通信に使用する通信プロトコル等が上述の実施形態で説明したものに限られないことはもちろんである。例えば、管理装置２０と被管理装置１０との間に必ずしもファイアウォールを設ける必要はない。

また、図１０のステップＳ２５や図２４のステップＳ４３での判断基準を、自身の識別情報が記載されたデジタル証明書である個別証明書が設定されているか否かとし、個別証明書が設定されていない場合に個別証明書の取得を行うようにしてもよい。また、被管理装置１０と管理装置２０との間の認証処理についても、図２８を用いて説明したような相互認証ではなく、管理装置２０が被管理装置１０を認証するのみの片方向認証でもよい。

【０１４４】

あるいは、個別公開鍵証明書に記載する識別情報が、機番以外の識別情報、例えば認証専用の識別情報であってもよい。また、通信に使用する通信経路も、有線、無線を問わず、任意のものを使用可能である。例えば、ＶＰＮ（Virtual Private Network）やＰＰＰ（Point to Point Protocol）を用いた通信経路を使用することが考えられる。

また、被管理装置とその通信相手となる仲介装置あるいは管理装置との関係や通信の目

的が、必ずしも遠隔管理に限られることはない。例えば、処理の負荷分散のための分散処理システムを構成するノードとしてもよい。また、被管理装置の情報を管理装置や仲介装置に登録することも、必須ではない。

【０１４５】

また、図１に示した遠隔管理システムにおいて、多岐に亘る通信装置を被管理装置とし、図２７に示すような遠隔管理システムを構成することも考えられる。この図においては、間接被管理状態の被管理装置の例としてテレビ受像機１１１ａや冷蔵庫１１１ｂのようなネットワーク家電、医療機器１１１ｃ，自動販売機１１１ｄ，計量システム１１１ｅ，空調システム１１１ｆを挙げている。そして、直接被管理状態の被管理装置の例として、自動車１１１ｇや航空機１１１ｈを挙げている。また、自動車１１１ｇや航空機１１１ｈのように広範囲を移動する装置においては、ファイアウォール６０の機能も併せ持つようにすることが好ましい。

このような遠隔管理システム及びその遠隔管理システムにおいて被管理装置となる各装置にも、この発明はもちろん適用可能である。

【０１４６】

また、この発明によるプログラムは、コンピュータに、上述したような被管理装置を制御させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

このようなプログラムは、はじめからコンピュータに備えるＲＯＭあるいはＨＤＤ等の記憶手段に格納しておいてもよいが、記録媒体であるＣＤ－ＲＯＭあるいはフレキシブルディスク，ＳＲＡＭ，ＥＥＰＲＯＭ，メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてＣＰＵに実行させるか、ＣＰＵにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【産業上の利用可能性】

【０１４７】

以上説明してきたように、この発明の被管理装置、管理システム、被管理装置の制御方法、プログラム又は記録媒体によれば、管理装置による管理を受ける被管理装置において、効率よく高いセキュリティを確保できるようにすることができる。

従って、この発明を利用することにより、安価に一定の水準のセキュリティを確保できる管理システムを構成することができる。

【図面の簡単な説明】

【０１４８】

【図１】この発明の被管理装置の実施形態を含む管理システムの構成の一例を示すブロック図である。

【図２】図１に示した各ノード間のデータ送受モデルを示す概念図である。

【図３】図１に示した被管理装置のハードウェア構成を示すブロック図である。

【図４】図１に示した被管理装置，管理装置，および仲介装置が記憶している証明書及び鍵の種類を示す図である。

【図５】図４に示した証明書のうち共通証明書の構成を示す図である。

【０１４９】

【図６】同じく個別証明書の構成を示す図である。

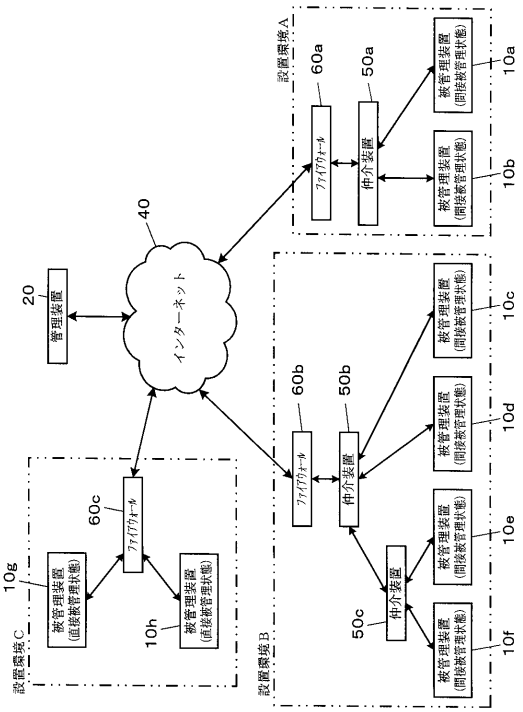
【図７】図１に示した被管理装置と管理装置の機能構成を、この実施形態の特徴に関連する部分を中心に示す図である。

【図８】図１に示した被管理装置がユーザＩ／Ｆに表示させる管理用初期画面の表示例を示す図である。

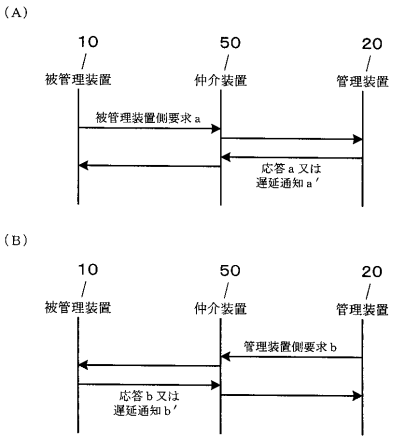
【図９】図８に示した設置ボタンの押下に応じて被管理装置のＣＰＵが実行する処理の一

部を示すフローチャートである。
【図１０】その続きの処理を示すフローチャートである。
【０１５０】
【図１１】図９及び図１０に示した動作においてユーザＩ／Ｆに表示させる未登録画面の表示例を示す図である。
【図１２】同じく登録完了画面の表示例を示す図である。
【図１３】同じく一部登録完了画面の表示例を示す図である。
【図１４】同じく登録失敗画面の表示例を示す図である。
【図１５】同じく間接通信登録済み画面の表示例を示す図である。
【０１５１】
【図１６】図９及び図１０に示した動作において被管理装置が取得する個別証明書セットの構成例を示す図である。
【図１７】図９及び図１０に示した処理により被管理装置を直接管理の対象として管理装置に登録する場合のこれらの装置の動作シーケンス例の一部を示す図である。
【図１８】その続きを示す図である。
【図１９】図１に示した管理システムにおいて、ユーザが仲介装置にユーザＩ／Ｆを用いてアクセスし、その仲介装置を管理装置に登録する際の動作シーケンス例を示す図である。
【図２０】同じく仲介装置に通信を仲介可能な被管理装置を検索させ、その装置の管理装置への登録を行わせる際の動作シーケンス例を示す図である。
【０１５２】
【図２１】図２０に示した動作においてユーザＩ／Ｆに表示させる機器登録画面の表示例を示す図である。
【図２２】同じく検索結果画面の例を示す図である。
【図２３】同じく登録結果画面の例を示す図である。
【図２４】図１に示した被管理装置が起動時に実行する処理のフローチャートである。
【図２５】同じく被管理装置が図２４に示した処理により管理装置から個別証明書を取得する場合の処理シーケンス例を示す図である。
【０１５３】
【図２６】同じく管理装置において被管理装置の登録を抹消する場合の処理シーケンス例を示す図である。
【図２７】この発明の被管理装置の実施形態を含む管理システムの図１とは別の構成例を示すブロック図である。
【図２８】２つの通信装置がＳＳＬに従った相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。
【図２９】図２８に示した認証処理におけるルート鍵、ルート私有鍵、および公開鍵証明書の関係について説明するための図である。
【符号の説明】
【０１５４】
１０：被管理装置、１１，２１：ＨＴＴＰＳクライアント機能部、
１２，２２：ＨＴＴＰＳサーバ機能部、１３，２３：認証処理部、
１４，２５：証明書記憶部、１５，２６：要求管理部、１６：被管理機能部、
１６ｄ：登録要求部、２０：管理装置、２４：証明書更新要求部、２７：管理機能部、
２８：証明書発行部、４０：インターネット、５０：仲介装置、
６０：ファイアウォール、７０，８０：ユーザＩ／Ｆ、１０１：ＣＰＵ、
１０２：ＲＯＭ、１０３：ＲＡＭ、１０４：不揮発性メモリ、１０５：通信Ｉ／Ｆ、
１０６：操作部、１０７：エンジン部、１０８：システムバス、
２００：管理用初期画面、２１０：未登録画面、２２０：登録完了画面、
２３０：一部登録完了画面、２４０：登録失敗画面、２５０：間接通信登録済み画面、
３１０：機器登録画面、３２０：検索結果画面、３３０：登録結果画面

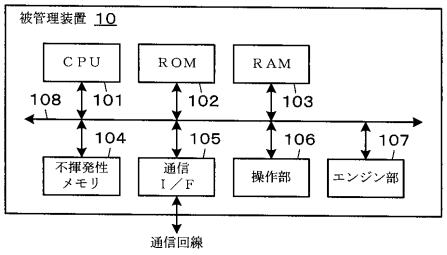
【図１】



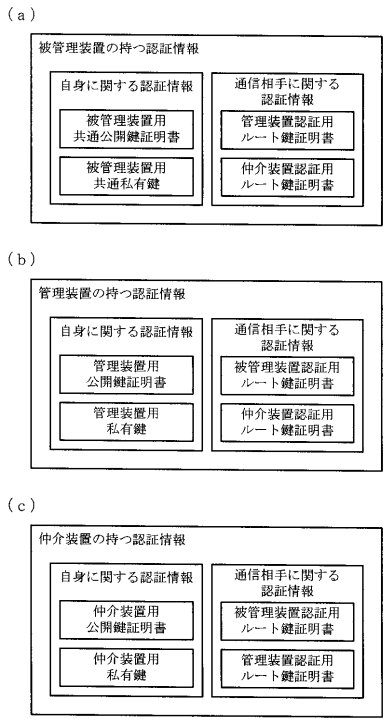
【図２】



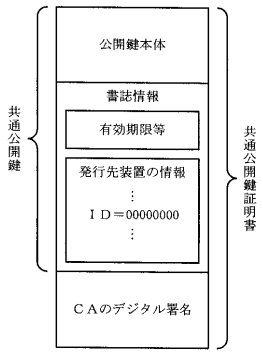
【図３】



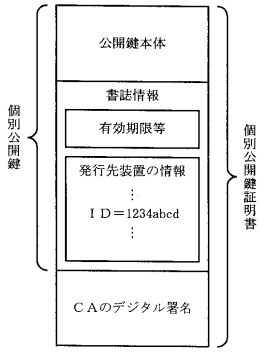
【図４】



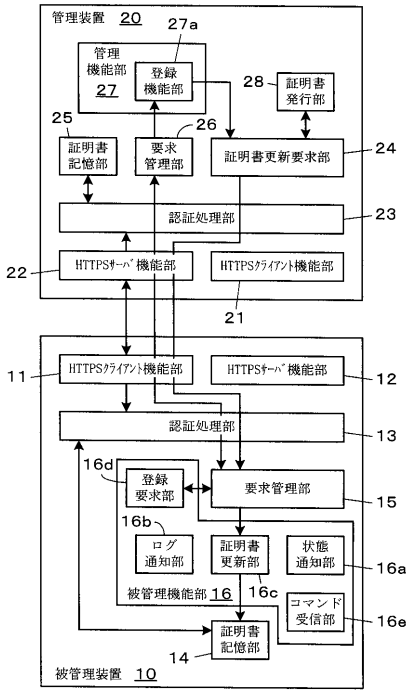
【図５】



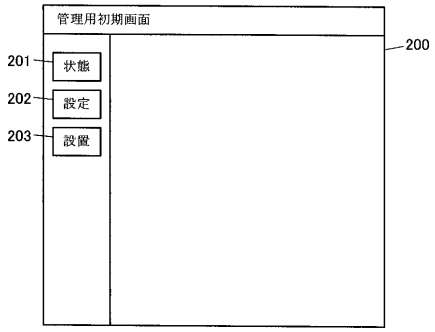
【図６】



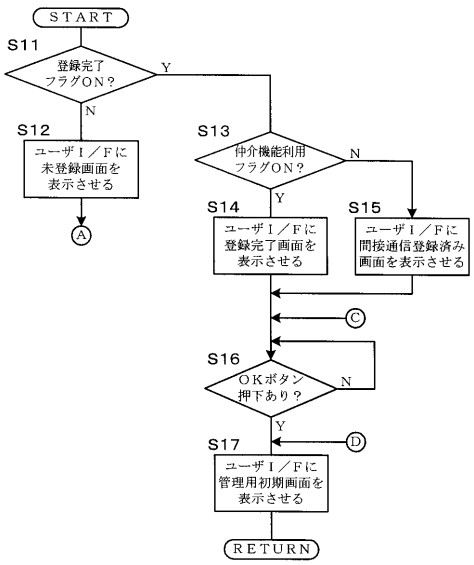
【図７】


管理装置 20
27a
管理機能部 27
登録機能部
28
証明書発行部
25
26
証明書記憶部
要求管理部
証明書更新要求部
24
認証処理部
23
22
HTTPSｻｰﾊﾞ機能部
HTTPSｸﾗｲｱﾝﾄ機能部
21
11
HTTPSｸﾗｲｱﾝﾄ機能部
HTTPSｻｰﾊﾞ機能部
12
認証処理部
13
16d
登録要求部
要求管理部
15
16b
ログ通知部
証明書更新部
状態通知部
16a
被管理機能部 16
16c
コマンド受信部
16e
証明書記憶部
14
被管理装置 10

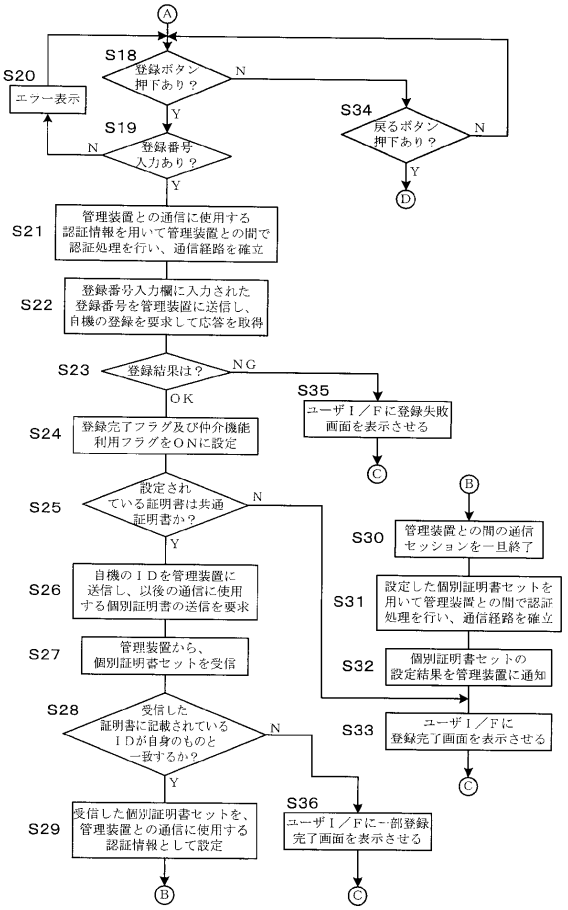
【図８】


管理用初期画面
200
201
状態
202
設定
203
設置

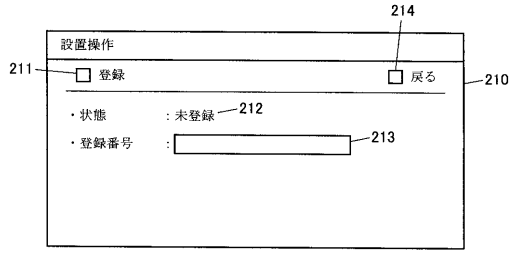
【図９】


START
S11
登録完了フラグON?
Y
N
S12
ユーザＩ／Ｆに未登録画面を表示させる
A
S13
仲介機能利用フラグON?
N
Y
S14
ユーザＩ／Ｆに登録完了画面を表示させる
S15
ユーザＩ／Ｆに間接通信登録済み画面を表示させる
C
S16
ＯＫボタン押下あり?
N
Y
S17
D
ユーザＩ／Ｆに管理用初期画面を表示させる
RETURN

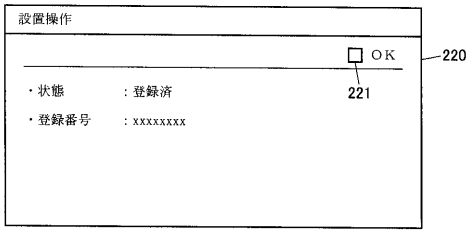
【図１０】


A
S18
登録ボタン押下あり?
N
Y
S20
エラー表示
S19
登録番号入力あり?
N
Y
S34
戻るボタン押下あり?
N
Y
D
S21
管理装置との通信に使用する認証情報を用いて管理装置との間で認証処理を行い、通信経路を確立
S22
登録番号入力欄に入力された登録番号を管理装置に送信し、自機の登録を要求して応答を取得
S23
登録結果は?
NG
OK
S35
ユーザＩ／Ｆに登録失敗画面を表示させる
C
S24
登録完了フラグ及び仲介機能利用フラグをＯＮに設定
S25
設定されている証明書は共通証明書か?
N
Y
B
S30
管理装置との間の通信セッションを一旦終了
S31
設定した個別証明書セットを用いて管理装置との間で認証処理を行い、通信経路を確立
S32
個別証明書セットの設定結果を管理装置に通知
S33
ユーザＩ／Ｆに登録完了画面を表示させる
C
S26
自機のＩＤを管理装置に送信し、以後の通信に使用する個別証明書の送信を要求
S27
管理装置から、個別証明書セットを受信
S28
受信した証明書に記載されているＩＤが自身のものと一致するか?
N
Y
S36
ユーザＩ／Ｆに一部登録完了画面を表示させる
S29
受信した個別証明書セットを、管理装置との通信に使用する認証情報として設定
B
C

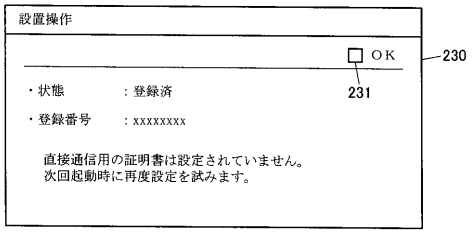
【図１１】



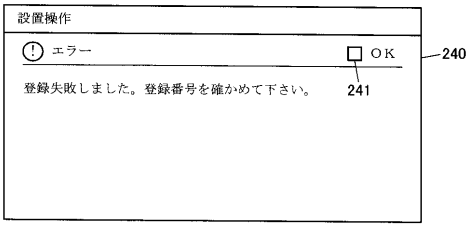
【図１２】



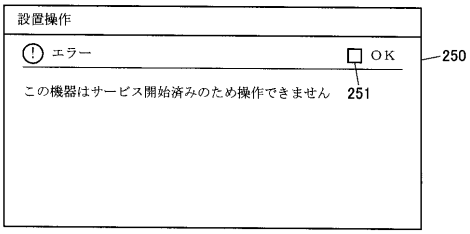
【図１３】



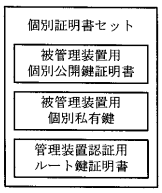
【図１４】



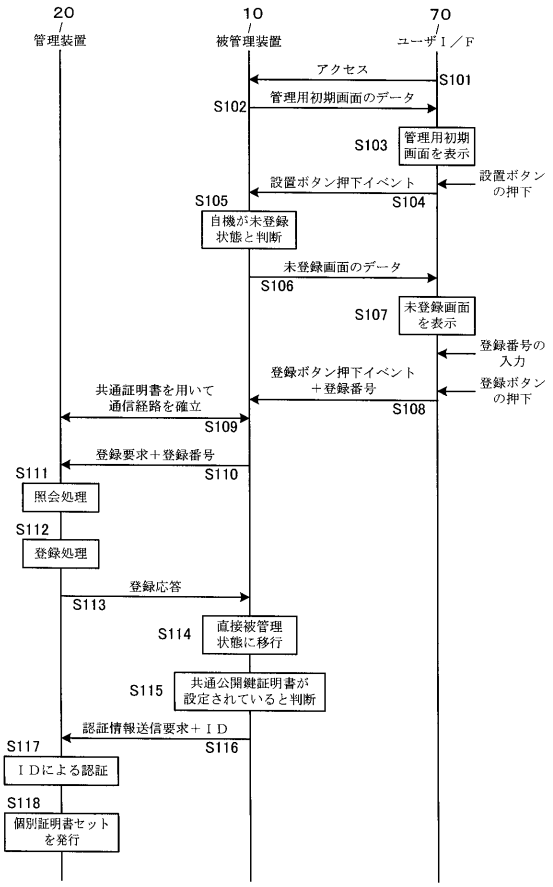
【図１５】



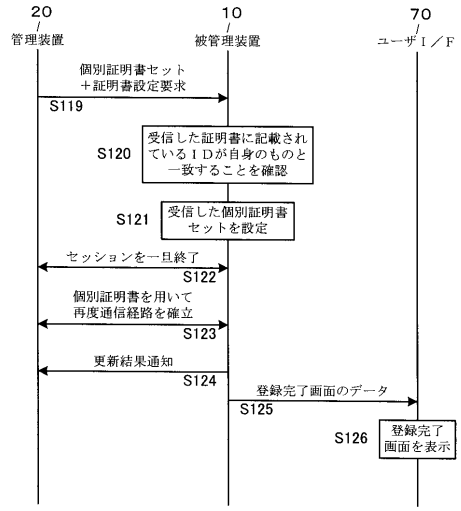
【図１６】



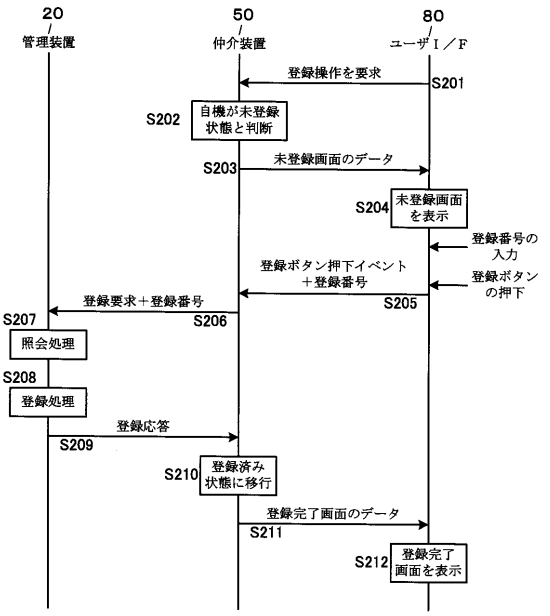
【図１７】



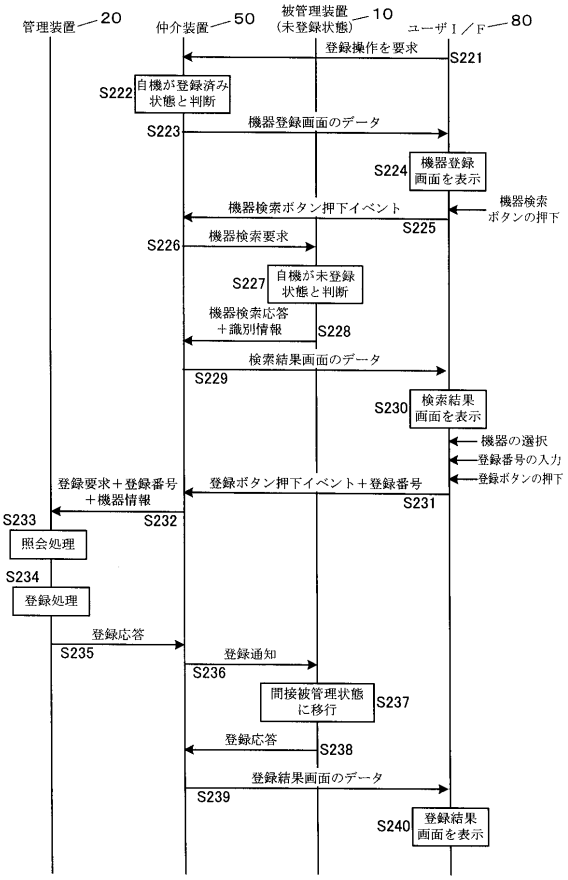
【図１８】



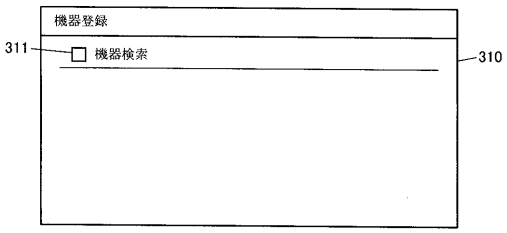
【図１９】



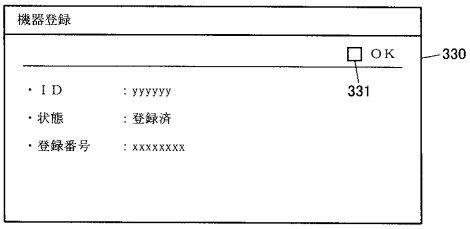
【図２０】



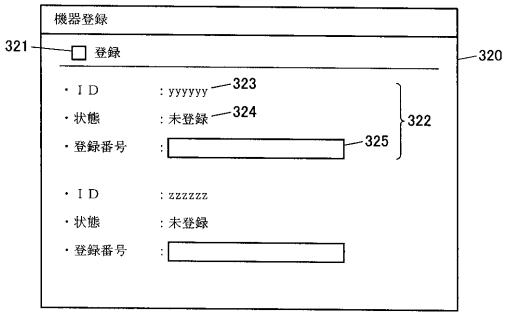
【図２１】



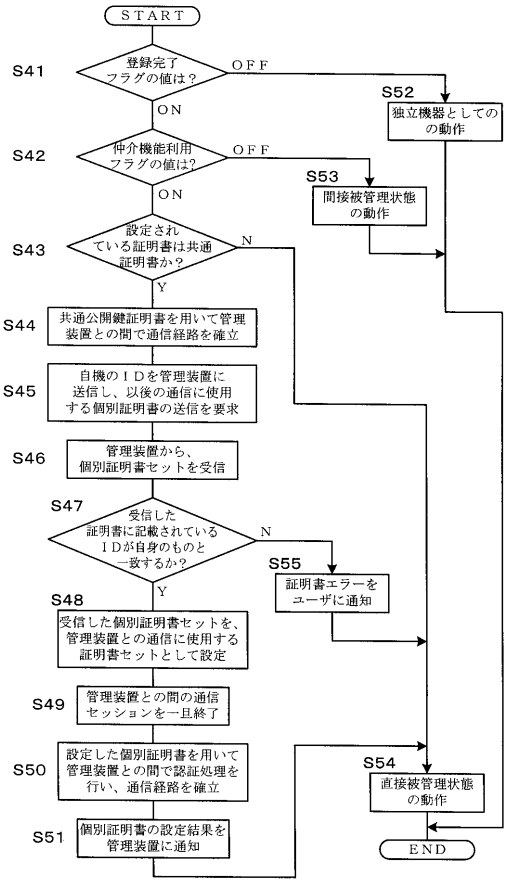
【図２３】



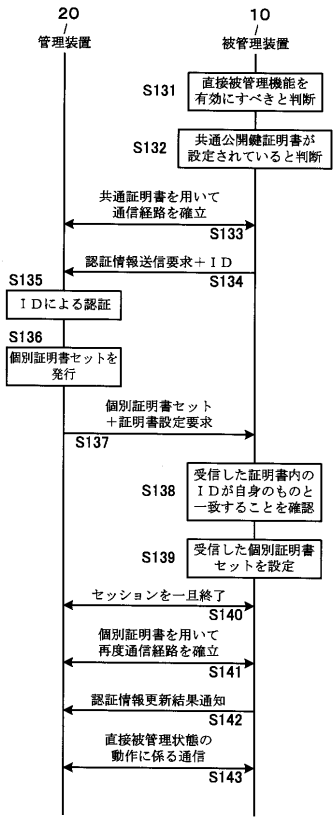
【図２２】



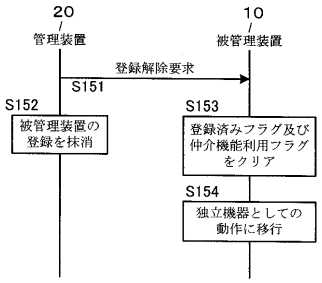
【図２４】



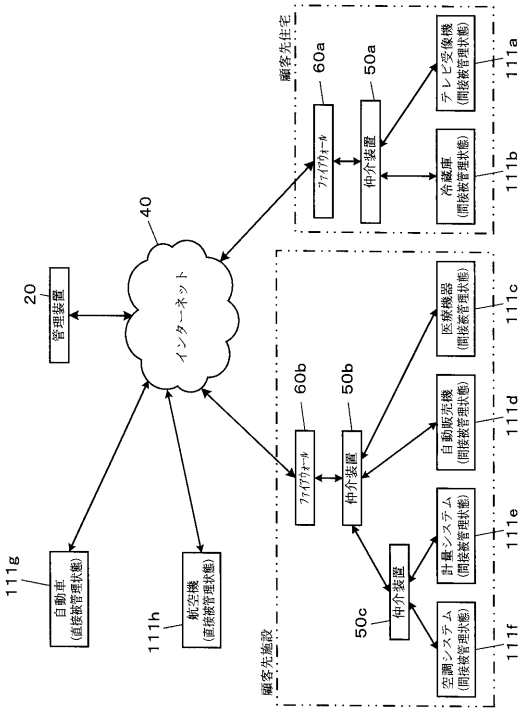
【図２５】



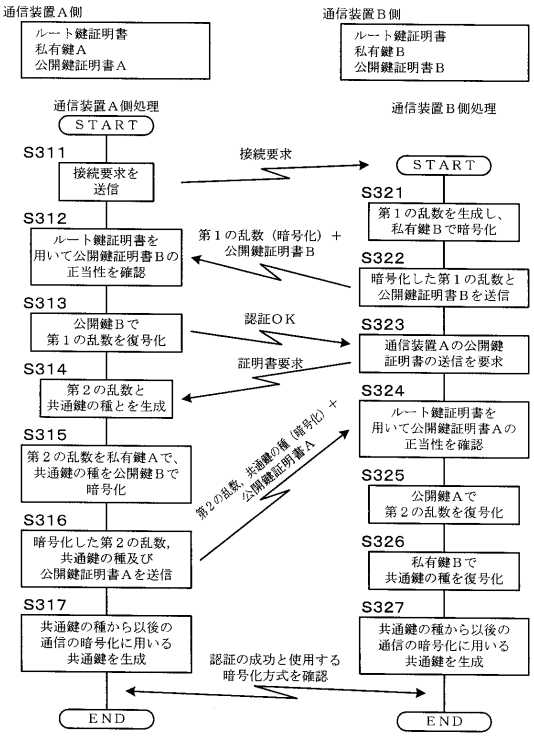
【図２６】



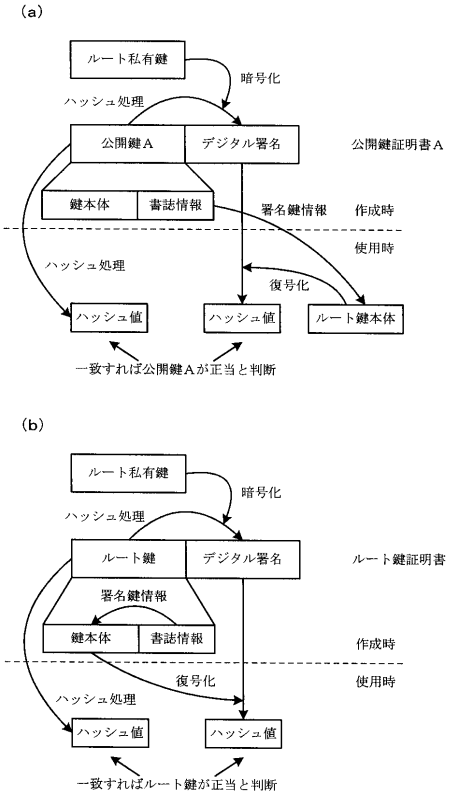
【図２７】



【図２８】


通信装置Ａ側
ルート鍵証明書
私有鍵Ａ
公開鍵証明書Ａ
通信装置Ｂ側
ルート鍵証明書
私有鍵Ｂ
公開鍵証明書Ｂ
通信装置Ａ側処理
通信装置Ｂ側処理
ＳＴＡＲＴ
ＳＴＡＲＴ
S311
接続要求を送信
接続要求
S312
ルート鍵証明書を用いて公開鍵証明書Ｂの正当性を確認
第１の乱数（暗号化）＋公開鍵証明書Ｂ
S313
公開鍵Ｂで第１の乱数を復号化
認証ＯＫ
S314
第２の乱数と共通鍵の種とを生成
証明書要求
S315
第２の乱数を私有鍵Ａで、共通鍵の種を公開鍵Ｂで暗号化
S316
暗号化した第２の乱数，共通鍵の種及び公開鍵証明書Ａを送信
第２の乱数，共通鍵の種（暗号化）＋公開鍵証明書Ａ
S317
共通鍵の種から以後の通信の暗号化に用いる共通鍵を生成
S321
第１の乱数を生成し、私有鍵Ｂで暗号化
S322
暗号化した第１の乱数と公開鍵証明書Ｂを送信
S323
通信装置Ａの公開鍵証明書の送信を要求
S324
ルート鍵証明書を用いて公開鍵証明書Ａの正当性を確認
S325
公開鍵Ａで第２の乱数を復号化
S326
私有鍵Ｂで共通鍵の種を復号化
S327
共通鍵の種から以後の通信の暗号化に用いる共通鍵を生成
認証の成功と使用する暗号化方式を確認
ＥＮＤ
ＥＮＤ

【図２９】


(a)
ルート私有鍵
暗号化
ハッシュ処理
公開鍵Ａ
デジタル署名
公開鍵証明書Ａ
鍵本体
書誌情報
署名鍵情報
作成時
使用時
ハッシュ処理
復号化
ハッシュ値
ハッシュ値
ルート鍵本体
一致すれば公開鍵Ａが正当と判断
(b)
ルート私有鍵
暗号化
ハッシュ処理
ルート鍵
デジタル署名
ルート鍵証明書
署名鍵情報
鍵本体
書誌情報
作成時
使用時
復号化
ハッシュ処理
ハッシュ値
ハッシュ値
一致すればルート鍵が正当と判断

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２