(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4583833号
(P4583833)
(45)発行日　平成22年11月17日(2010.11.17)　(24)登録日　平成22年9月10日(2010.9.10)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601F

請求項の数 6　(全 32 頁)

(21)出願番号	特願2004-228605 (P2004-228605)
(22)出願日	平成16年8月4日 (2004.8.4)
(65)公開番号	特開2005-130458 (P2005-130458A)
(43)公開日	平成17年5月19日 (2005.5.19)
審査請求日	平成19年3月9日 (2007.3.9)
(31)優先権主張番号	特願2003-321804 (P2003-321804)
(32)優先日	平成15年9月12日 (2003.9.12)
(33)優先権主張国	日本国(JP)
(31)優先権主張番号	特願2003-341329 (P2003-341329)
(32)優先日	平成15年9月30日 (2003.9.30)
(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　100123881
弁理士　大澤　豊
(74)代理人　100080931
弁理士　大澤　敬
(72)発明者　今井　達也
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　速水　雄太

最終頁に続く

(54)【発明の名称】通信装置、通信システム、通信方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して相手先装置と通信を行う通信装置であって、
パブリック認証局によって発行された当該通信装置の証明書である第１の証明書とプライベート認証局によって発行された当該通信装置の証明書である第２の証明書とを記憶可能な記憶手段と、
前記相手先装置と通信を行う際、前記記憶手段に前記第１の証明書が記憶されていない場合は前記第２の証明書を前記相手先装置へ送信する送信手段と、
前記送信手段が送信した前記第２の証明書を用いた前記相手先装置での認証が成功した場合に、前記第１の証明書を前記相手先装置から受信し、該受信した第１の証明書を前記記憶手段に記憶させる証明書設定手段とを設けたことを特徴とする通信装置。
【請求項２】
請求項１に記載の通信装置であって、
前記第１の証明書を前記記憶手段に記憶させた後は、前記相手先装置と通信を行う際、前記第１の証明書を前記相手先装置へ送信することを特徴とする通信装置。
【請求項３】
上位装置と下位装置とを備え、前記上位装置と前記下位装置とがネットワークを介して通信を行う通信システムであって、
前記下位装置に、
パブリック認証局によって発行された前記下位装置の証明書である第１の証明書とプラ

イベート認証局によって発行された前記下位装置の証明書である第２の証明書とを記憶可能な記憶手段と、
前記上位装置と通信を行う際、前記記憶手段に前記第１の証明書が記憶されていない場合は前記第２の証明書を前記上位装置へ送信する送信手段と、
前記送信手段が送信した前記第２の証明書を用いた前記上位装置での認証が成功した場合に、前記第１の証明書を前記上位装置から受信し、該受信した第１の証明書を前記記憶手段に記憶させる証明書設定手段とを設け、
前記上位装置に、
前記下位装置から受信した前記第２の証明書を用いて該下位装置の認証を行う認証手段と、
前記第２の認証手段による認証が成功した場合に、前記第１の証明書を前記下位装置へ送信する送信手段とを設けたことを特徴とする通信システム。
【請求項４】
請求項３に記載の通信システムであって、
前記下位装置は、前記第１の証明書を前記記憶手段に記憶させた後は、前記上位装置と通信を行う際、前記第１の証明書を前記上位装置へ送信し、
前記上位装置は、前記下位装置から受信した前記第１の証明書を用いて該下位装置の認証を行う手段を有することを特徴とする通信システム。
【請求項５】
ネットワークを介して相手先装置と通信を行う通信装置であって、パブリック認証局によって発行された前記通信装置の証明書である第１の証明書とプライベート認証局によって発行された前記通信装置の証明書である第２の証明書とを記憶可能な記憶手段を有する通信装置に、
前記相手先装置と通信を行う際、前記記憶手段に前記第１の証明書が記憶されていない場合は前記第２の証明書を前記相手先装置へ送信する送信手順と、
前記送信手順で送信した前記第２の証明書を用いた前記相手先装置での認証が成功した場合に、前記第１の証明書を前記相手先装置から受信し、該受信した第１の証明書を前記記憶手段に記憶させる証明書設定手順とを実行させることを特徴とする通信方法。
【請求項６】
ネットワークを介して相手先装置と通信を行う通信装置であって、パブリック認証局によって発行された前記通信装置の証明書である第１の証明書とプライベート認証局によって発行された前記通信装置の証明書である第２の証明書とを記憶可能な記憶手段を有する通信装置を制御するコンピュータを、
前記相手先装置と通信を行う際、前記記憶手段に前記第１の証明書が記憶されていない場合は前記第２の証明書を前記相手先装置へ送信する送信手段と、
前記送信手段が送信した前記第２の証明書を用いた前記相手先装置での認証が成功した場合に、前記第１の証明書を前記相手先装置から受信し、該受信した第１の証明書を前記記憶手段に記憶させる証明書設定手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ネットワークを介して相手先装置と通信を行う通信装置、上位装置と下位装置とを備え、その上位装置と下位装置とがネットワークを介して通信を行う通信システム、ネットワークを介して相手先装置と通信を行う通信装置による通信方法、およびネットワークを介して相手先装置と通信を行う通信装置を制御するコンピュータに実行させるプログラムに関する。
【背景技術】
【０００２】
従来から、それぞれ通信機能を備えた複数の通信装置をネットワークを介して通信可能に接続し、様々なシステムを構築することが行われている。その一例としては、クライア

ント装置として機能するＰＣ等のコンピュータから商品の注文を送信し、これとインターネットを介して通信可能なサーバ装置においてその注文を受け付けるといった、いわゆる電子商取引システムが挙げられる。また、種々の電子装置に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接続し、相互間の通信によって電子装置の遠隔管理を行うシステムも提案されている。

【０００３】

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よる通信を行う場合には、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

【０００４】

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１９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１９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。

【０００５】

図２０にこれらの関係を示す。

図２０（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）や有効期限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。

【０００６】

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。

【０００７】

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２０（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。

【０００８】

図１９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。

【０００９】

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１９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Ｓ１１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１９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Ｓ２１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Ｓ２２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。

【００１０】

通信装置Ａ側では、これを受信すると、ステップＳ１２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Ｓ１３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。

その後、ステップＳ１４でこれとは別に第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Ｓ１５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Ｓ１６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Ｓ１７では、ステップＳ１４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、通信装置Ａがステップ１６で送信してくるデータを受信すると、ステップＳ２３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Ｓ２４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Ｓ２５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Ｓ２６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Ｓ１７と通信装置Ｂ側のステップＳ２６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Ｓ１７又はＳ２６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の乱数を公開鍵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。この場合、通信装置Ｂ側のステップＳ２３及びＳ２４の処理は不要になり、処理は図２１に示すようになる。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。

【００１４】

一方、このような公開鍵証明書を発行する第３者機関として、私有鍵の保有者の確認を行い、その私有鍵に対応した公開鍵に対してデジタル署名を行い、公開鍵証明書を発行する商用サービスが、例えばベリサイン社やボルチモア社によって提供されている。そして、公開鍵発行のためのシステムが私有鍵を含めて厳重に管理されている信頼性の高い第３者機関が発行する公開鍵証明書は、広く認証に利用されている。また、デジタル証明書を用いた認証を行う場合、信頼性の高い第３者機関が発行した公開鍵証明書を使用したいという要求もある。

【００１５】

さらに、このような第３者機関の発行する公開鍵証明書を利用する場合、主要な第３者機関によるデジタル署名の内容を確認するためのルート鍵は、インターネットエクスプローラ（登録商標）やネットスケープ（登録商標）のような一般的なウェブブラウザには予め埋め込まれているため、ウェブブラウザの操作者は、新たにルート鍵を入手して設定する必要がないという利点がある。

また、予めルート鍵を設定されていない装置であっても、信頼性の高い第３者機関のものであればユーザがルート鍵の設定に同意しやすいし、ルート鍵を入手して設定すれば、同じ第３者機関が発行した公開鍵証明書を持つ装置は、装置自体のベンダーに関わらず認証することができるという利点もある。従って、自社製の装置を他社製の装置に接続したい場合等には、第３者機関の発行する公開鍵証明書を利用することが効果的である。また、装置のユーザ側からも、このような公開鍵証明書を利用したいという要望がある。

【発明の開示】

【発明が解決しようとする課題】

【００１６】

ところで、装置自体を認証する場合には、ウェブブラウザ等の操作者を特定する認証と異なり、装置にデジタル証明書を予め記憶させておく必要がある。これは、装置の製造時においてもそうであるし、破損や不良等のため証明書を記憶するメモリを有する部品を交換した場合には、交換後にも証明書を記憶させた状態にできなければならない。

しかしながら、上記のような第３者機関が発行した公開鍵証明書を使用する場合、どの機関が発行した公開鍵証明書を使用するかは、システムや装置の運用者が適宜定めるものであるから、装置や部品がどの通信システムあるいは通信装置で使用されるかがわからない状態で、予め適切な機関が発行した公開鍵証明書を記憶させておくことは困難であるという問題があった。また、どのような証明書を記憶させておけばよいかわかる場合であっても、通信システムや通信装置の運用者が従前の契約を打ち切り、新たな第３者機関との契約を締結する等して使用する公開鍵証明書を変更する場合も考えられる。

このような問題を解決するためには、ユーザや用途が特定された後で各装置に個別に証明書を記憶させるようにすることが考えられる。また、証明書を記憶するメモリを有する

部品についても、部品の交換後に証明書を記憶させるような対応を行うことが考えられる。

【００１７】

そこで、図２２に、不揮発性記憶デバイスにこのような個別の書き込みを行うために従来用いられていた方法を示す。

従来用いられていた方法の１つは、図２２（ａ）に示すように、通信装置３００に設けた不揮発性記憶デバイス３０１に接続されている基板パターンに、記憶デバイス書き込み端子３０５を設けておき、ここに書き込み用の専用冶具である専用コネクタ３１２を接続して、書き込み装置３１３から書き込みを行う方法である。

しかしこの方法では、書き込みに専用の冶具が必要となり、冶具の管理上の問題から、ＯＥＭ（Original Equipment Manufacturer）メーカーでの書き込みや、装置が市場に流通した後で証明書を記憶している部品が破損した場合の修復に必要な書き込みを可能とすることが難しいという問題があった。

【００１８】

また、通常動作時には使用しない専用冶具の接続Ｉ／Ｆ（記憶デバイス書き込み端子３０５）は、装置の完成後には通常は装置の内部に位置することになるので、ここに専用コネクタ３１２を接続するには、一旦基板を取り外す等の面倒な作業が必要となり、作業効率が悪いという問題があった。また、この作業によって装置を破損してしまう危険性もある。専用冶具の接続Ｉ／Ｆを装置の外側に設けることも考えられるが、このようにすると、通常動作には不要なＩ／Ｆを追加して設けることになり、コストアップにつながる。

【００１９】

一方、情報の書き込みには、図２２（ｂ）に示すように、ＰＣＭＣＩＡ（Personal Computer Memory Card International Association）カード等のメモリカード３１１を交換可能な記憶デバイスとして用い、通信装置３００にこの記憶デバイスを接続するインタフェース（Ｉ／Ｆ）としてカードスロット３０３を設け、カードスロット３０３に接続したメモリカード３１１の内容をＣＰＵ３０２に読み出させ、不揮発性記憶デバイス３０１に書き込ませる方法も用いられている。

このような方法であれば、適当な証明書を記憶させたメモリカード３１１を用意すれば、ＯＥＭメーカーや市場も含め、どこでも書き込みを行うことができる。しかし、メモリカードは広く普及した一般的な媒体であるため、セキュリティの管理が難しく、メモリカード３１１の正当性の確認や、メモリカード３１１が不正な第３者に渡らないようにするための管理、またメモリカード３１１から第３者が不正にデータを取得することの防止が難しいという問題があった。

【００２０】

さらに、装置の成りすまし等を防止するため、証明書については、悪意のユーザによる交換、読み出し、登録を防止する必要があり、一般のユーザによる証明書の更新を禁止する必要があるので、メモリカード３１１を用いて証明書を設定するようにする場合の権限の確認も困難である。

この発明は、このような事情に鑑みてなされたものであり、セキュリティを維持しながら、認証に必要な証明書を記憶する部品を交換する必要が生じた場合でも、容易かつ速やかに正常な認証が行える状態に容易に回復させることが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】

【００２１】

上記の目的を達成するため、ネットワークを介して相手先装置と通信を行う通信装置において、パブリック認証局によって発行されたその通信装置の証明書である第１の証明書とプライベート認証局によって発行されたその通信装置の証明書である第２の証明書とを記憶可能な記憶手段と、上記相手先装置と通信を行う際、上記記憶手段に上記第１の証明書が記憶されていない場合は上記第２の証明書を上記相手先装置へ送信する送信手段と、上記送信手段が送信した上記第２の証明書を用いた上記相手先装置での認証が成功した場

合に、上記第１の証明書を上記相手先装置から受信し、その受信した第１の証明書を上記記憶手段に記憶させる証明書設定手段とを設けたことを特徴とする通信装置。

このような通信装置において、上記第１の証明書を上記記憶手段に記憶させた後は、上記相手先装置と通信を行う際、上記第１の証明書を上記相手先装置へ送信するようにするとよい。

また、この発明の通信システムは、上位装置と下位装置とを備え、上記上位装置と上記下位装置とがネットワークを介して通信を行う通信システムにおいて、上記下位装置に、パブリック認証局によって発行された上記下位装置の証明書である第１の証明書とプライベート認証局によって発行された上記下位装置の証明書である第２の証明書とを記憶可能な記憶手段と、上記上位装置と通信を行う際、上記記憶手段に上記第１の証明書が記憶されていない場合は上記第２の証明書を上記上位装置へ送信する送信手段と、上記送信手段が送信した上記第２の証明書を用いた上記上位装置での認証が成功した場合に、上記第１の証明書を上記上位装置から受信し、その受信した第１の証明書を上記記憶手段に記憶させる証明書設定手段とを設け、上記上位装置に、上記下位装置から受信した上記第２の証明書を用いてその下位装置の認証を行う認証手段と、上記第２の認証手段による認証が成功した場合に、上記第１の証明書を上記下位装置へ送信する送信手段とを設けたものである。

このような通信システムにおいて、上記下位装置が、上記第１の証明書を上記記憶手段に記憶させた後は、上記上位装置と通信を行う際、上記第１の証明書を上記上位装置へ送信するようにし、上記上位装置に、上記下位装置から受信した上記第１の証明書を用いてその下位装置の認証を行う手段を設けるとよい。

【００２２】

また、この発明の通信方法は、ネットワークを介して相手先装置と通信を行う通信装置であって、パブリック認証局によって発行された上記通信装置の証明書である第１の証明書とプライベート認証局によって発行された上記通信装置の証明書である第２の証明書とを記憶可能な記憶手段を有する通信装置に、上記相手先装置と通信を行う際、上記記憶手段に上記第１の証明書が記憶されていない場合は上記第２の証明書を上記相手先装置へ送信する送信手順と、上記送信手順で送信した上記第２の証明書を用いた上記相手先装置での認証が成功した場合に、上記第１の証明書を上記相手先装置から受信し、その受信した第１の証明書を上記記憶手段に記憶させる証明書設定手順とを実行させるものである。

また、この発明のプログラムは、ネットワークを介して相手先装置と通信を行う通信装置であって、パブリック認証局によって発行された上記通信装置の証明書である第１の証明書とプライベート認証局によって発行された上記通信装置の証明書である第２の証明書とを記憶可能な記憶手段を有する通信装置を制御するコンピュータを、上記相手先装置と通信を行う際、上記記憶手段に上記第１の証明書が記憶されていない場合は上記第２の証明書を上記相手先装置へ送信する送信手段と、上記送信手段が送信した上記第２の証明書を用いた上記相手先装置での認証が成功した場合に、上記第１の証明書を上記相手先装置から受信し、その受信した第１の証明書を上記記憶手段に記憶させる証明書設定手段として機能させるためのプログラムである。

【発明の効果】

【００２３】

以上のようなこの発明の通信装置、通信システム、通信方法及びプログラムによれば、セキュリティを維持しながら、認証に必要な証明書を記憶する部品を交換する必要が生じた場合でも、容易かつ速やかに正常な認証が行える状態に容易に回復させることができる。

【発明を実施するための最良の形態】

【００２４】

以下、この発明を実施するための最良の形態を図面を参照して説明する。

まず、この発明の証明書設定方法を適用する通信装置である下位装置と、同じく通信装置であってその下位装置の通信相手となる上位装置とを用いて構成した通信システムの構

成例について説明する。
図１はその通信システムの構成を示すブロック図である。
この通信システムは、図１に示すように、それぞれ通信手段を備える通信装置である上位装置１０及び下位装置２０をネットワーク３０によって接続して構成している。
ネットワーク３０としては、有線，無線を問わず、ネットワークを構築可能な各種通信回線（通信経路）を採用することができる。また、ここでは下位装置２０を１つしか示していないが、図１８に示すように通信システム内に下位装置２０を複数設けることも可能である。
【００２５】
このような通信システムについて、まず上位装置１０及び下位装置２０のハードウェア構成から説明する。上位装置１０及び下位装置２０のハードウェア構成は、単純化して示すと、図２に示すようなものである。
この図に示す通り、上位装置１０は、ＣＰＵ１１，ＲＯＭ１２，ＲＡＭ１３，ＨＤＤ１４，通信インタフェース（Ｉ／Ｆ）１５を備え、これらがシステムバス１６によって接続されている。そして、ＣＰＵ１１がＲＯＭ１２やＨＤＤ１４に記憶している各種制御プログラムを実行することによってこの上位装置１０の動作を制御し、通信相手の認証や下位装置２０のデジタル証明書更新等の機能を実現している。なお、この明細書において、デジタル証明書とは、偽造されないようにするための署名が付されたデジタルデータを指すものとする。
【００２６】
下位装置２０も、上位装置１０の場合と同様にＣＰＵ２１，ＲＯＭ２２，ＲＡＭ２３，ＨＤＤ２４，通信インタフェース（Ｉ／Ｆ）２５を備え、これらがシステムバス２６によって接続されている。ＣＰＵ２１が、ＲＯＭ２２やＨＤＤ２４に記憶している各種制御プログラムを必要に応じて実行し、装置の制御を行うことにより、通信手段、証明書設定手段等の種々の手段としての機能を実現できるようにしている。また、通信Ｉ／Ｆ２５については、例えば下位装置２０をＬＡＮ（ローカルエリアネットワーク）に接続できるようにするためには、イーサネット（登録商標）規格の通信ケーブルを接続するためのコネクタを含むインタフェースを設ければよい。
なお、この通信システムにおいて、上位装置１０及び下位装置２０が、遠隔管理，電子商取引等の目的に応じて種々の構成をとることができることは、もちろんである。そして、上位装置１０や下位装置２０のハードウェアとしては、適宜公知のコンピュータを採用することもできる。もちろん、必要に応じて他のハードウェアを付加してもよいし、上位装置１０と下位装置２０が同一の構成である必要もない。
【００２７】
次に、この通信システムのうちこの実施形態の特徴に関連する部分として、上位装置１０及び下位装置２０の証明書の設定に関連する部分の機能構成を図３に示す。上位装置１０に係るこれらの機能は、上位装置１０のＣＰＵ１１がＲＯＭ１２やＨＤＤ１４に記憶している所要の制御プログラムを実行することにより実現されるものであり、下位装置２０に係るこれらの機能は、下位装置２０のＣＰＵ２１がＲＯＭ２２やＨＤＤ２４等に記憶している所要の制御プログラムを実行することにより実現されるものである。
【００２８】
図３に示すように、上位装置１０には、ＨＴＴＰＳ（Hypertext Transfer Protocol Security）クライアント機能部３１，ＨＴＴＰＳサーバ機能部３２，認証処理部３３，証明書更新要求部３４，証明書記憶部３５を備えている。
ＨＴＴＰＳクライアント機能部３１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下位装置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。
【００２９】
一方、ＨＴＴＰＳサーバ機能部３２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３３は、ＨＴＴＰＳクライアント機能部３１やＨＴＴＰＳサーバ機能部３２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３５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３５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３１やＨＴＴＰＳサーバ機能部３２を介して通信相手に送信する機能も有する。

【００３０】

証明書更新要求部３４は、後述するように所定の場合に下位装置２０等の通信相手に対して通常公開鍵証明書を送信してこれを記憶するよう要求する機能を有する。なお、ここで送信する証明書は、この通信システムの外部の証明書管理装置（ＣＡ）５０に必要な情報を送信して発行させる。

証明書記憶部３５は、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３３における認証処理に供する機能を有する。これらの各種証明書や私有鍵の種類及びその用途や作成方法については後に詳述する。

【００３１】

一方、下位装置２０には、ＨＴＴＰＳクライアント機能部４１，ＨＴＴＰＳサーバ機能部４２，認証処理部４３，要求管理部４４，証明書記憶部４５，状態通知部４６，ログ通知部４７，証明書設定部４８，コマンド受信部４９を備えている。

ＨＴＴＰＳクライアント機能部４１は、上位装置１０のＨＴＴＰＳクライアント機能部３１と同様に、ＨＴＴＰＳプロトコルを用いて上位装置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。

【００３２】

ＨＴＴＰＳサーバ機能部４２も、上位装置１０のＨＴＴＰＳサーバ機能部３２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４３の機能も、上位装置１０の認証処理部３３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４５に記憶しているものである。

要求管理部４４は、上位装置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する機能を有する。そして、実行を許可する場合に、その要求に基づいた動作を実行する機能部４６～４９に対して動作要求を伝える機能も有する。

【００３３】

図４にこの実行可否の判断基準を示すが、その判断基準は、要求の種類及び認証処理部４３において認証処理に使用したデジタル証明書の種類である。上位装置１０及び下位装置２０が記憶しているデジタル証明書には、詳細は後述するが、第１の認証局であるパブリック認証局により発行された第１の証明書でありパブリック証明書である通常公開鍵証明書と、第２の認証局であるプライベート認証局により発行された第２の証明書でありプライベート証明書であるレスキュー公開鍵証明書があり、要求管理部４４は、図３に示すように、通常公開鍵証明書による認証処理を行った場合には全ての動作を許可するが、レスキュー公開鍵証明書による認証処理を行った場合には証明書の設定動作のみを許可するようにしている。従って、レスキュー公開鍵証明書は、下位装置２０に新たな通常公開鍵証明書を記憶させる場合のみに使用する証明書ということになる。

【００３４】

証明書記憶部４５は、上位装置１０の証明書記憶部３５と同様に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４３における認証処理に供する証明書記憶手段の機能を有する。ただし、記憶している証明書等は、後述するように証明書記憶部３５とは異なる。

状態通知部４６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上位装置１０に対して下位装置２０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、上位装置１０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４１から上位装置１０に通信を要求して送信してもよい。

【００３５】

ログ通知部４７は、下位装置２０から上位装置１０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、下位装置２０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、上位装置１０からの問い合わせに対する応答として送信するとよい。

証明書設定部４８は、上位装置１０から受信する後述する通常公開鍵証明書等によって証明書記憶部４５に記憶している証明書等を設定及び更新する証明書設定手段の機能を有する。

コマンド受信部４９は、上述した各機能部４６～４８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、例えば下位装置２０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の動作を制御することが挙げられる。なお、状態通知部４６やログ通知部４７は、コマンド受信部４９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。

【００３６】

次に、この通信システムにおける上位装置１０と下位装置２０との間の通信方式について説明する。図５はその通信方式の概要を示す説明図である。

この通信システムにおいて、上位装置１０は、下位装置２０と通信を行おうとする場合、まず下位装置２０に対して通信を要求する。そして、従来の技術の項で図１９又は図２１を用いて説明したようなＳＳＬプロトコルに従った認証処理によって下位装置２０を正当な通信相手として認証した場合に、下位装置２０との間で通信を確立させるようにしている。この認証処理は、ＳＳＬハンドシェイクと呼ばれる。ただし、図１９に示したような相互認証は必須ではなく、図２１に示したような片方向認証でもよい。

この処理において、下位装置２０は自身の公開鍵証明書を上位装置１０に送信して、認証を受ける。そして、相互認証を行う場合には上位装置１０も下位装置２０に自身の公開鍵証明書を送信して認証を受けるが、片方向認証の場合にはこちらの認証は行わない。

【００３７】

以上の認証が成功すると、上位装置１０は、下位装置２０が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、構造化言語形式であるＸＭＬ形式で記載したＳＯＡＰメッセージ６０として生成し、ＨＴＴＰ（Hyper Text Transfer Protocol）に従ってＨＴＴＰリクエストとして下位装置２０に送信する。このような要求は、ＲＰＣ（Remote Procedure Call）と呼ばれる。

そして、下位装置２０はこの要求の内容に応じた処理を実行し、その結果を応答のＳＯＡＰメッセージ７０として生成し、ＨＴＴＰレスポンスとして上位装置１０に送信する。ここで、これらの要求と応答は、ＳＳＬハンドシェイクの処理において交換された共通鍵を用いて暗号化して送信し、通信の安全性を確保している。

【００３８】

また、これらの要求と応答とによって、この通信システムは、上位装置１０をクライアント、下位装置２０をサーバとするクライアント・サーバシステムとして機能している。なお、逆に下位装置２０から上位装置１０に通信を要求し、下位装置２０をクライアント、上位装置１０をサーバとするクライアント・サーバシステムとして機能する場合もある。

また、ＲＰＣを実現するためには、上記の技術の他、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。

【００３９】
次に、上述した上位装置１０及び下位装置２０が上述した認証処理に用いる認証情報である各証明書や鍵の特性及び用途について説明する。図６は、（ａ）に下位装置２０が認証情報として記憶している証明書及び鍵の種類を示し、（ｂ）に上位装置１０が認証情報として記憶している証明書及び鍵の種類を示す図である。
図１に示した上位装置１０及び下位装置２０は、図６に示すように、大きく分けて通常認証情報とレスキュー認証情報とを記憶している。そして、これらの認証情報は、それぞれ自分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によって構成される。
【００４０】
また、例えば下位装置用通常公開鍵証明書は、証明書が下位装置２０に対して発行した通常公開鍵に、下位装置認証用通常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り、パブリック証明書に該当する。なお、ここでは証明書管理装置５０がパブリック認証局、あるいはパブリック認証局が証明書の発行及び管理に使用する装置に該当するものとする。また、パブリック認証局とは、背景技術の項で説明した第３者機関のように広く世間で信頼性が認められた認証局、あるいは公的に信頼性が認められた認証局、法的に証明書の効力が認められるような認証局等、一般的に通用するような証明書を発行できる認証局を指すものとする。また、パブリック認証局は、証明書の利用者と異なる運営者が運営する認証局である。
【００４１】
ここで、公開鍵証明書のフォーマットは、例えば図７に示したものを用いることができ、公開鍵そのものの他、証明書の発行者や証明書の有効期限、証明される対象（証明書の発行先の装置あるいは利用者）等の情報が記載されている。具体的には、例えばＸ．５０９と呼ばれるフォーマットに従って作成することができ、このフォーマットに従って作成された公開鍵証明書は、例えば図８に示すようなものになる。
この例においては、ＡがＣＡの識別情報を示し、Ｃが証明書の発行先の装置の識別情報を示す。これらは、それぞれ所在地、名称、機番あるいはコード等の情報を含む。また、Ｂが有効期間を示し、その開始日時と終了日時によって有効期間を指定している。
【００４２】
なお、装置を特定する目的のみであれば、公開鍵証明書に付す識別情報に機番情報を含めることは必須ではないのであるが、ここで識別情報に機番情報と同一の情報を含めるようにしているのは、通信システムを運営する場合の要求に応えるためである。すなわち、この通信システムを装置の管理に使用する場合、装置の特定は機番情報によって行うことが多いが、識別情報が機番情報を含んでいない場合には、上位装置１０側で識別情報と機番情報との対応関係をテーブル等として別途管理しておく必要が生じるのである。そして、このような管理を行う場合、下位装置２０を新たに生産する度にデータを追加する必要があるし、下位装置２０の数は数万台、数十万台あるいはそれ以上になる場合もあり、非常に大きな量のデータを管理する必要が生じるので、管理の負担が大きくなってしまう。
しかし、公開鍵証明書に付す識別情報に機番情報と同一の情報を含めておけば、認証処理において通信相手の機番を直接特定できる。従って、このようにすることにより、公開鍵証明書に付す識別情報と機番情報との対応関係を管理する必要がなくなり、管理負担を低減できるのである。
もちろん、このような機番情報を証明書に記載しなくてもよいし、逆に、この他に下位装置２０の機種番号や登録ユーザ等の情報も記載するようにしてもよい。
【００４３】
また、下位装置用通常私有鍵は、上記の通常公開鍵と対応する私有鍵、下位装置認証用通常ルート鍵証明書は、下位装置認証用通常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。
そして、下位装置２０を複数設けた場合でも、各装置の通常公開鍵に付すデジタル署名は同じルート私有鍵を用いて付し、正当性確認に必要な通常ルート鍵証明書は共通にする

。しかし、通常公開鍵証明書に含まれる通常公開鍵やこれと対応する私有鍵は、装置毎に異なる。

上位装置用通常公開鍵証明書と上位装置用通常私有鍵と上位装置認証用通常ルート鍵証明書も同様な関係である。

また、各装置に、複数のパブリック認証局が発行した公開鍵証明書の正当性を確認できるようにするため、その各パブリック認証局と対応したルート鍵証明書を記憶させるようにすることも考えられる。

【００４４】

そして、例えば上位装置１０と下位装置２０とが通常認証情報を用いて相互認証を行う場合には、上位装置１０からの通信要求に応じて、下位装置２０は下位装置用通常私有鍵を用いて暗号化した第１の乱数を下位装置用通常公開鍵証明書と共に上位装置１０に送信する。上位装置１０側では下位装置認証用通常ルート鍵証明書を用いてまずこの下位装置用通常公開鍵証明書の正当性（損傷や改竄を受けていないこと）を確認し、これが確認できた場合にここに含まれる公開鍵で第１の乱数を復号化する。この復号化が成功した場合に、上位装置１０は通信相手の下位装置２０が確かに下位装置用通常公開鍵証明書の発行先であると認識でき、その証明書に含まれる識別情報から装置を特定することができる。そして、特定した装置が通信相手としてふさわしいか否かに応じて認証の成功と失敗を決定することができる。

また、下位装置２０側でも、上位装置１０側で認証が成功した場合に送信されてくる上位装置用通常公開鍵証明書及び、上位装置用通常私有鍵で暗号化された乱数を受信し、記憶している上位装置認証用ルート鍵証明書を用いて同様な認証を行うことができる。

【００４５】

ところで、これらの公開鍵証明書や私有鍵は、ＲＯＭ２２あるいはＲＡＭ２３を構成するフラッシュメモリのような書き換え可能な不揮発性記憶手段に記憶させておくものである。従って、破損等のため、このような記憶手段を含む部品を交換する場合には、記憶している公開鍵証明書や私有鍵は、取り外した旧部品と共に取り去られてしまう。そしてこのような場合、再度通常公開鍵証明書を用いた認証（通常証明書セットを用いた認証）を可能にするためには、取り去られた証明書や鍵を再度記憶させる必要がある。

【００４６】

ここで、各装置が通常公開鍵証明書を用いた認証しか行えないとすると、この認証が行えなくなっている状態では、新たな通常公開鍵証明書等をネットワーク３０を介して安全に対象の装置に送信する方法はないことになる。しかし、この通信システムを構成する各装置は、このような事態に対処するため、レスキュー認証情報を記憶しており、これを用いることにより、通信相手を異なる２種類のデジタル証明書を用いて認証することができるようにしている。そして、レスキュー認証情報を用いることにより、必要な装置にネットワーク３０を介して新たな通常公開鍵証明書等を安全に送受信できるようにしている。

【００４７】

このレスキュー認証情報は、通常認証情報と概ね同様な構成となっている。例えば下位装置用レスキュー公開鍵証明書は、ＣＡが下位装置に対して発行したレスキュー公開鍵に、上位装置認証用レスキュー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り、プライベート証明書に該当する。また、上位装置用レスキュー私有鍵はそのレスキュー公開鍵と対応する私有鍵、下位装置認証用レスキュールート鍵証明書は、下位装置認証用レスキュールート鍵に自身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。そして、これらのレスキュー公開鍵証明書とレスキュー私有鍵とレスキュールート鍵証明書とを合わせて、レスキュー証明書セットと呼ぶことにする。上位装置１０側に記憶させるレスキュー認証情報についても同様とする。

【００４８】

しかし、正規認証情報と大きく異なる点は、レスキュー公開鍵証明書は、プライベート認証局によって発行された公開鍵証明書である点である。プライベート認証局とは、特に世間に広く信頼性が認められているわけではなく、発行する証明書が一般的に通用するわ

けではない認証局を指す。また、証明書の利用者が運営する認証局であり、例えば、自社内で利用する証明書を管理するためにその企業が運営する認証局である。

このような認証局が発行する証明書は、通常はパブリック認証局が発行する証明書よりも信頼性が低いと考えられるが、プライベート認証局は、安全性と利便性を考慮して設置者が独自のポリシーにより運営することができるため、用途に適合した証明書を発行し易いという利点もある。また、プライベート認証局であっても、安全性に配慮すれば、比較的安全性の高い証明書を提供することも可能である。

【００４９】

ここで、図９に通常公開鍵証明書の例を、図１０にレスキュー公開鍵証明書の例を示す。

これらは、同じ装置に設定して認証処理に使用させる公開鍵証明書である。しかし、証明書の発行者は、通常公開鍵証明書については符号Ｄで示すようにＹＹＹ社の「ＰｕｂｌｉｃＣＡ」としている一方、レスキュー公開鍵証明書については符号Ｇで示すようにＸＸＸ社の「ＰｒｉｖａｔｅＣＡ」というように、異なるＣＡとしている。「ＰｕｂｌｉｃＣＡ」はパブリック認証局、「ＰｒｉｖａｔｅＣＡ」はプライベート認証局に該当するものとする。またここでは、プライベート認証局は、発行先装置のメーカーであるＸＸＸ社が設けている。

そして、このようなレスキュー公開鍵証明書を含むレスキュー認証情報を用意し、レスキュー認証情報の内容を、輸出規制や、各地域で普及している認証処理の内容等を考慮しても下位装置２０が使用されると想定される種々の環境で共通に使用できるような認証処理により認証を行うことができるようなものにするとよい。

【００５０】

このようにすれば、通常公開鍵証明書を用いた認証が行えないような環境下でも、レスキュー公開鍵証明書により通信相手を認証することができる。そして、このような認証が成功すれば、前述のように通信相手との間で共通鍵を共有して共通鍵暗号を用いた安全な通信経路を設けることができる。従って、この通信経路を利用して、通信時点の環境に適合した新しい通常公開鍵証明書を通信相手に送信し、設定させることが可能となる。

また、パブリック認証局の発行する公開鍵証明書では、厳格な管理や安全性が要求されるため、上記のように種々の環境で共通に使用できるような証明書を発行することが難しい場合もあるし、費用もかかる。しかし、プライベート認証局であれば、証明書の仕様を比較的自由に定められるので、暗号強度を低くしたり、最新であまり普及していない認証処理アルゴリズムを避けたりして、種々の環境で共通に使用できるような証明書を発行することも可能である。また、装置のメーカー自身がプライベート認証局を提供すれば、安価に証明書を発行することも可能である。さらに、例えば下位装置２０と上位装置１０でメーカーが異なったり、通信システムの運用者が種々にカスタマイズを行ったりするような場合でも、レスキュー公開鍵証明書を無償で提供する等して、これらのメーカーや運用者に、レスキュー公開鍵証明書を用いた認証に対応できるようにするよう働きかけることも容易となる。

【００５１】

そして、証明書の記憶領域を備える部品の製造時に、予めレスキュー認証情報を記憶させておくようにすれば、レスキュー公開鍵証明書を用いた認証に上位装置１０が対応している場合、通信相手を認証することができる。そして、このような認証が成功すれば、前述のように通信相手との間で共通鍵を共有して共通鍵暗号を用いた安全な通信経路を設けることができる。従って、この通信経路を利用して、通信相手に新しい通常公開鍵証明書（を含む通常認証情報）を送信し、設定することが可能となる。

なお、下位装置２０を用いた通信システムを構成するユーザが、必ずしも上位装置１０をレスキュー公開鍵証明書を用いた認証に対応させるとは限らない。しかし、レスキュー公開鍵証明書を用いた認証に対応させることにより、上記のように、交換後の部品に新しい通常公開鍵証明書を安全にリモートで設定できるという機能を利用できるようになることから、ユーザ側にもレスキュー公開鍵証明書を利用可能にするメリットがある。

【００５２】
また、レスキュー公開鍵証明書については、１つのＣＡが発行した証明書を記憶させておけば足り、またこの証明書はプライベート認証局が提供する証明書であり、装置のメーカー自身が提供することができるので、これを交換部品に記憶させること自体には、さほどコストはかからない。
そこで、当初は上位装置１０がレスキュー公開鍵証明書を用いた認証に対応しておらず、レスキュー認証情報を使用できない状態であっても、証明書記憶領域を有する交換部品全てにレスキュー認証情報を記憶させておき、事後的に上位装置１０をレスキュー公開鍵証明書を用いた認証に対応させるようにすることも考えられる。このような場合でも、上位装置１０の対応後は、部品を交換した下位装置２０に、レスキュー公開鍵証明書を用いた認証を行って確立した安全な通信経路で通常認証情報を設定することができる。
なお、プライベート認証局が発行するレスキュー公開鍵証明書は、パブリック認証局が発行する通常公開鍵証明書と比べた場合に、安全性や信頼性が劣ることも考えられる。しかしながら、レスキュー認証情報を用いて認証処理を行った場合に、通常公開鍵証明書を始めとする正規認証情報の更新のような限られた要求のみ実行を許可するようにすれば、若干安全性が低下したとしても、大きな問題にはならない。
【００５３】
ここで、図９及び図１０の説明に戻ると、これらの２つの公開鍵証明書において、通常公開鍵証明書では、符号Ｅで示すように有効期間が２００３年１月１日午前０時から２００４年１月１日午前０時までの１年間である一方、レスキュー公開鍵証明書では、符号Ｈで示すように２０００年１月１日午前０時から２０５０年１月１日午前０時までの５０年間としている。
すなわち、通常公開鍵証明書はパブリック認証局が発行するものであるから、装置の製造者や使用者が有効期間を自由に定めることができず、また安全性を考慮して有効期間が短く設定されているのが通常である。一方で、レスキュー認証情報は、プライベート認証局が発行するものであるから、装置の製造者が自由に有効期間を定めることができる。そこで、有効期間をこのように通常公開鍵証明書よりも長く設定するようにしている。
このようにすれば、有効期間が長い分、有効期限切れにより使用不能になってしまう事態も生じにくい。従って、証明書の記憶領域を備える部品の製造時に、予めレスキュー認証情報を記憶させておくようにしても、部品を長期間ストックしておき、交換が必要になった場合に速やかにこれに対応することができる。
【００５４】
なお、レスキュー認証情報を用いて認証処理を行った場合に、通常公開鍵証明書を始めとする正規認証情報の更新のような限られた要求のみ実行を許可するようにすれば、有効期間を長くしたために若干安全性が低下したとしても、大きな問題にはならない。
また、この点を考慮すると、レスキュー公開鍵証明書の有効期間経過後には再度レスキュー公開鍵証明書を設定し直す必要が生じてしまうので、レスキュー公開鍵証明書の有効期間は長い方が好ましい。具体的には、例えば記憶させる装置の製品寿命よりも長い有効期間を設定するとよい。この製品寿命は、装置の想定運用期間あるいは想定動作期間であり、開発時に想定している使用期間や想定耐用年数、装置の品質保証期間等から定めることができる。
また、レスキュー公開鍵証明書の有効期間を、装置をメンテナンスしながら正常に動作させられると想定される期間よりも長く設定すれば、レスキュー公開鍵証明書は装置の動作中には有効期限が切れない証明書であるということができる。従って、装置の動作中は、常にレスキュー公開鍵証明書を用いた認証（レスキュー証明書セットを用いた認証）が可能な状態を保つことができる。従って、一旦レスキュー公開鍵証明書を記憶させて製造した装置や部品に対し、ストック中にこの証明書の有効期限が切れて、これを更新する必要が生じることもない。
【００５５】
また、上記の製品寿命や装置の動作期間よりも極めて長い有効期間を定めるようにすれ

ば、なおよい。図１０に示した例では、有効期間を５０年に設定しており、通常の装置であればこの程度で十分と考えられるが、これはＸ．５０９フォーマットに従って設定できる有効期間の最大が５０年であるためこのようにしただけで、さらに長い期間、例えば１００年や数百年を設定してもよいことはもちろんである。このように有効期間を定めた場合、有効期間の終期は、単に公開鍵証明書のフォーマット上の要求により記載したものであり、レスキュー公開鍵証明書の有効期限は事実上ないものと考えることができる。また、対象の装置によっては、２０年や３０年程度あるいはそれ以下の有効期間であっても、同様に考えることができる場合もある。

さらにまた、たとえレスキュー公開鍵証明書の有効期間が製品寿命より短かったとしても、通常公開鍵証明書の有効期間よりも長ければ、通常公開鍵証明書を記憶させておく場合よりも装置や部品のストック可能期間を延ばすことができるという効果を得ることはできる。

通常公開鍵証明書の有効期間については、パブリック認証局の運営者が安全性を考慮して適当な期間を定めるが、上記のように、この期間は、製品寿命よりも短く、また装置の動作中に有効期限が切れるような期間となることが多い。

【００５６】

また、ここでは、レスキュー公開鍵証明書の書誌情報には装置の識別情報を記載せず、同じ階位の装置（図１あるいは図２０に示した例では、上位装置と下位装置の階位が存在するものとする）には、全て同じレスキュー公開鍵証明書を記憶させることができるようにしている。この場合、同じ階位の各装置を個別に区別する必要がないので、証明書に含まれるレスキュー公開鍵及びこれと対応するレスキュー私有鍵も含めて、全く共通のものでよい。そして、通信相手のレスキュー公開鍵証明書が全て同じであることから、ルート鍵証明書については、ある階位の装置の通信相手となる全ての装置について共通となる。すなわち、下位装置２０を複数設けた場合でも、全ての下位装置２０に同じレスキュー認証情報を記憶させることになる。

これは、上位装置１０のレスキュー認証情報についても同様である。

そして、通常公開鍵証明書とデータ形式を統一化するため、図１０に示した例において、発行先装置の機番として０を記載してレスキュー公開鍵証明書であることを示すようにしている。なお、「Subject」の項目を空白としてこのことを示すことも考えられる。

【００５７】

このようにすることは必須ではないが、このように、レスキュー認証情報を同じ階位の装置について全て共通にできるようにすると、証明書の記憶領域を備える部品の製造時に、その部品を装着する装置の機種に応じて定まる階位に対応するものを画一的に記憶させてしまうことができる。そして、このようなレスキュー認証情報を記憶しており、通常認証情報を記憶していない部品であれば、製造時に装置の識別情報が必要ないため、装置の識別情報によらず共通に使用可能な部品として生産することができる。

【００５８】

なお、レスキュー公開鍵証明書には装置の識別情報を付さないようにする場合、レスキュー公開鍵証明書を用いた認証を行った場合でも、通信相手の装置を具体的に特定することはできない。しかし、通信相手についてある程度の情報は得ることができる。

すなわち、例えばあるベンダーが自社製品のうち下位装置２０に該当する装置全てに下位装置用のレスキュー証明書セットを記憶させ、その通信相手となる上位装置１０に該当する装置全てに上位装置用のレスキュー証明書セットを記憶させておけば、認証が成功した場合、下位装置２０は、自己の記憶している上位装置認証用レスキュールート鍵証明書で正当性を確認できる公開鍵証明書を送信してきた相手が同じベンダーの上位装置１０であることを認識できるし、逆に上位装置１０も自己の記憶している下位装置認証用レスキュールート鍵証明書で正当性を確認できる公開鍵証明書を送信してきた相手は同じベンダーの下位装置２０であることを認識できる。

【００５９】

従って、通信を要求した装置あるいは要求してきた装置が通信相手として適当な装置か

否かについて、識別情報を参照できなくてもある程度の判断を行うことができる。
そして、このような認証が成功すれば、前述のように通信相手との間で共通鍵を共有して共通鍵暗号を用いた安全な通信経路を設けることができるので、その後機番情報等を交換して通信相手を特定することも可能である。

【００６０】

ところで、サーバとして機能する下位装置２０は、ＳＳＬハンドシェイクの際に、通信を要求してきた相手を識別できないため、基本的には全ての相手に同一の公開鍵証明書を送信することになる。しかし、この通信システムにおいては、状況に応じて通常公開鍵証明書とレスキュー公開鍵とを使い分ける必要がある。そこで、次にこの使い分けのための構成について図１１を用いて説明する。

ＳＳＬプロトコルにおいては、サーバは、クライアントから通信要求があった時点ではクライアントの状態を知ることができないため、必然的に、特定のＵＲＬ（Uniform Resource Locator）にアクセスされた場合には常に同じ公開鍵証明書を提供することになる。従って基本的には、通常公開鍵証明書を複数持ち、通信相手の持つ通常ルート鍵証明書の種類に合わせて適当なものを選択して送信するといった構成を取ることはできない。しかし、通信要求を受け付けるアドレスが異なる場合には、アドレス毎に異なる公開鍵証明書を返すことも可能である。このアドレスは、例えばＵＲＬによって定めることができる。

【００６１】

従ってここでは、図１１に示すように、上位装置１０及び下位装置２０にそれぞれ、通常公開鍵証明書による認証を行う通常ＵＲＬとレスキュー公開鍵証明書による認証を行うレスキューＵＲＬとを設け、通信を要求する側（クライアントとして機能する側）が、要求する認証の種類に応じていずれかのＵＲＬを選択的に指定して通信要求を送るようにしている。これらのＵＲＬは、ＩＰアドレスやポート番号（いずれか一方でもよい）を変えることにより、物理的には同じ装置のＵＲＬであっても、論理的には異なる装置のＵＲＬとして取り扱うことができるようにしている。すなわち、いわゆるバーチャルサーバの機能を実現するためのものである。

【００６２】

このようにした場合、通信を要求される側（サーバとして機能する側）は、返す証明書を通信要求を受け付けたＵＲＬによって区別し、通常ＵＲＬで受け付けた場合には通常公開鍵証明書を提供し、レスキューＵＲＬで受け付けた場合にはレスキュー公開鍵証明書を提供することができる。
なお、通信を要求するクライアントの側では、どのＵＲＬに対して通信要求を送ったかがわかるので、相互認証を行う場合にはＵＲＬに応じた適切な公開鍵証明書を選択して送信することができる。

【００６３】

従って、この通信システムにおいては、上位装置１０と下位装置２０との間で基本的には通常公開鍵証明書を用いた認証を行いながら、これが部品の交換によって取り去られた場合にも、新たな部品が装着された後でその部品に記憶させてあるレスキュー公開鍵証明書を用いた認証を行い、安全な通信経路を確保することができる。レスキュー公開鍵証明書を用いた認証であっても、共通鍵の共有は通常公開鍵証明書の場合と同様に可能であるためである。そして、この通信経路を用いて上位装置１０から下位装置２０に設定用の通常認証情報を送信して記憶させることにより、再度通常認証情報を用いた認証が可能な状態に復帰させることができる。

【００６４】

また、レスキュー公開鍵証明書を用いた認証であっても、上述のようにある程度相手の装置を特定することができるので、例えば自社の製造した装置のみに通常公開鍵証明書を送信するようにする等の制限をかけることができ、不正な装置に通常公開鍵証明書を送信して記憶させてしまうことを防止できる。
以上のように、この通信システムにおいては、通常認証情報に加えてレスキュー認証情報も使用することにより、認証に必要な証明書を記憶する部品を交換する必要が生じた場

合でも、容易かつ速やかに正常な認証が行える状態に容易に回復させることができる。従って、人手での証明書更新が困難であり自動更新に頼らざるを得ないような装置であっても、信頼性の高いパブリック認証局が発行する証明書を有効に活用することができる。

【００６５】

なお、図６に示した認証情報は、上位装置１０と下位装置２０とが相互認証を行う場合には全て記憶している必要があるが、下位装置２０がサーバとして機能し、かつ上位装置１０が下位装置２０を認証する片方向認証だけを行う場合には、一部の証明書等については記憶しておく必要はない。通常認証情報とレスキュー認証情報の双方について、下位装置２０においては、上位装置認証用ルート鍵証明書は不要となるし、上位装置１０においては、上位装置用公開鍵証明書と上位装置用私有鍵が不要となる。

また、下位装置２０において、上述した通常証明書セット及びレスキュー証明書セットを記憶する記憶領域は、共通の部品上に設けるようにするとよく、ここではこのようにしたものとする。この部品としては、例えばＲＯＭ２２やＲＡＭ２３を構成するフラッシュメモリやＮＶＲＡＭ等を備えたメモリカードやメモリユニット、あるいはＣＰＵ２１と共に書き換え可能な不揮発性メモリを搭載したＣＰＵボード等が考えられる。上位装置１０においても同様とする。

【００６６】

次に、このような証明書セットの記憶領域を設けた部品及びその部品を装着した下位装置２０の製造工程について説明する。この製造工程においては、この発明の証明書設定方法の実施形態により下位装置２０に通常証明書セットを設定する。

まず、これらの製造工程の概略を図１２に示す。この図においては、証明書セットの設定に関する部分を中心に示し、それ以外の部分については大幅に簡略化して示している。

【００６７】

この図に示すように、下位装置２０を製造する場合、まず部品製造工程において証明書セットの記憶領域を設けた部品Ａを製造するが、この工程では、部品Ａを組み立て、検査する。ここでの検査内容は、部品ＡがＣＰＵボードである場合には、ＣＰＵからボードに設けた各チップにアクセスできるか否かを検査することが考えられる。

そしてその後、工場のソフトウェア複写装置１３０によって、下位装置２０の制御に使用するソフトウェアのうち部品Ａに記憶させるものと共に、下位装置２０用のレスキュー証明書セットを書き込む。この時点では、ソフトウェア複写装置１３０と部品Ａとの間でネットワークを介した安全な通信経路を設けることはできないし、レスキュー証明書セットは漏洩した場合の影響が通常証明書セットの場合より大きいため、書き込みは専用の冶具を用いて直接行うようにするとよい。

以上で部品Ａが完成し、これを部品として流通させる場合には、梱包した上出荷することになる。

ここで、レスキュー公開鍵証明書に装置の識別情報を記載しない場合には、書き込むべきレスキュー証明書セットは部品Ａを装着する装置の機種や階位に応じて定まるので、これを予めソフトウェア複写装置１３０に記憶させておけばよい。また、部品Ａが規格化されたメモリカード等の場合には、組み立てる必要がない場合もある。

【００６８】

一方、部品Ａを下位装置２０の製造に使用する場合には、レスキュー証明書セットが書き込まれ、これを記憶している部品Ａを製品組み立て工程に回し、これを組み立て中の下位装置２０の本体部に装着する。この実施形態ではこの手順が第１の手順に該当する。そして、下位装置２０の組み立てが完了した後、その機能検査を行って品質を検査する。ここでの検査内容としては、ＣＰＵボード上のＣＰＵからボードの外のデバイス、例えば通信Ｉ／Ｆ２５等にアクセスできるか否かを検査することが考えられる。この実施形態ではこの手順が検査手順に該当する。

【００６９】

そして、検査に合格した装置に機番を付与する。その後、装置の機番情報や初期設定値を下位装置２０に記憶させる。また、どのような通常証明書セットを記憶させればよいか

がわかる場合には、その通常証明書セットを、証明書書き込み装置１６０によって下位装置２０に記憶させる。この実施形態ではこの手順が第２の手順に該当する。その後、外観を検査し、梱包して出荷する。

以上の工程で下位装置２０を製造することができる。また、記憶させるレスキュー証明書セットは異なるが、上位装置１０についても同様な工程で製造することができる。なお、部品製造工程と製品組み立て工程とは、別々の工場で行われることが多い。

【００７０】

また、図１３に、部品Ａに各証明書セットを記憶させる工程の説明図を示す。

この図に示すように、部品Ａには、部品製造工程においてレスキュー証明書セットのみを記憶させ、通常証明書セットは記憶させない。そしてこの状態で、製品組み立て工程で新しい装置の組み立てに用いる部品と、市場に販売済の装置のための交換部品（サービスパーツ）とのどちらの用途にも使用できる部品として完成する。

そして、工場においてユーザからの注文に応じて装置を生産するような場合には、機番が付与された段階で、その装置を使用するユーザや、その装置が接続される通信システムがわかっている場合もある。そして、このような場合には、利用環境に適した通常証明書セットを、装置製造の段階で設定してしまうことも可能である。

【００７１】

そこで、このような場合、部品Ａが装置の組み立て工場において製品組み立て工程で装置に装着された場合には、その装置が検査に合格し、装置に機番が付与された後で、証明書設定装置である証明書書き込み装置１６０によって通常証明書セットが書き込まれ、設定される。

このとき、機番情報入力装置１６１から証明書書き込み装置１６０に書き込み対象の装置の機番を入力し、証明書書き込み装置１６０がその機番の情報を識別情報として含む通常証明書セットを取得して書き込むことになる。この通常証明書セットは、パブリックＣＡである証明書管理装置５０が発行するものである。そして、証明書管理装置５０は、設定対象の下位装置２０が接続される予定の通信システムにおいて、上位装置１０が行う認証処理で使用可能な証明書を発行するパブリックＣＡである。

【００７２】

なお、このようにパブリックＣＡが発行する公開鍵証明書を利用する場合には、証明書書き込み装置１６０からパブリックＣＡに対して直接証明書の発行を依頼し、証明書の管理もそのＣＡに任せてしまうよりは、発行された証明書を管理する機能を証明書書き込み装置１６０に設けたり、証明書書き込み装置１６０が間に発行された証明書を管理する装置を介してＣＡに証明書の発行を依頼するような構成が好ましい。特に、工場においては複数のパブリックＣＡから証明書を取得することも考えられるから、このような構成が特に好ましいと言える。

【００７３】

また、証明書書き込み装置１６０が下位装置２０に通常証明書セットを設定する際には、証明書書き込み装置１６０と下位装置２０と接続した上で、証明書書き込み装置１６０から下位装置２０のレスキューＵＲＬに通信を要求し、下位装置２０に記憶しているレスキュー証明書セットを用いて、ＳＳＬによる認証処理を行う。そして、証明書書き込み装置１６０が下位装置２０が正当な装置であると認証した場合に証明書設定要求と共に通常証明書セットを送信して部品Ａの通常証明書セット記憶領域に書き込ませるようにしている。すなわち、証明書書き込み装置１６０と下位装置２０とがレスキュー公開鍵証明書を用いた通信を行い、その通信によって、証明書書き込み装置１６０が下位装置２０に通常証明書セットを記憶させる。

【００７４】

ここで、通常証明書セットを書き込む際に下位装置２０側で実行する処理を図１４のフローチャートに示す。

下位装置２０は、通信相手がレスキューＵＲＬに通信を要求してきた場合、図１４のフローチャートに示す処理を開始する。

この処理においては、まずステップＳ２０１で、通信相手（ここでは証明書書き込み装置１６０）に認証を受けるために下位装置用レスキュー公開鍵証明書を、下位装置用レスキュー私有鍵で暗号化した第１の乱数と共に通信相手に送信する。この処理は、図２１のステップＳ２１及びＳ２２の処理に相当する。

【００７５】

通信相手は、下位装置２０が送信した証明書と乱数を受信すると、これを用いて認証処理を行い、その結果を応答として返してくる。また、認証が成功していれば、共通鍵の種を下位装置２０に送信すると共に共通鍵を作成して以後の通信に使用するようにする。ここでの認証には、下位装置認証用レスキュールート鍵証明書を使用し、この処理は図２１のステップＳ１２乃至Ｓ１７の処理に相当する。

下位装置２０は、この認証結果を受け取ると、ステップＳ２０２で認証が成功したか否か判断し、失敗であればそのまま処理を終了するが、成功していればステップＳ２０３に進んで受信した共通鍵の種を用いて共通鍵を作成して以後の通信に使用するようにする。これらの処理は、図２１のステップＳ２５及びＳ２６の処理に相当する。

【００７６】

その後、ステップＳ２０４で要求の受信を待ち、要求を受信するとステップＳ２０５に進む。そして、図４を用いて説明したように、下位装置２０の要求管理部４４は、レスキュー公開鍵証明書を用いた認証を行った場合には、証明書設定動作のみを許可するようにしているので、ステップＳ２０５で受信した要求が証明書設定要求か否かを判断する。そして、証明書設定要求でなければその要求は無視してステップＳ２０４に戻って次の要求を待つ。ここで、要求を受け付けられない旨の応答を返すようにしてもよい。

【００７７】

ステップＳ２０５で証明書設定要求であれば、ステップＳ２０６に進んで証明書設定要求と共に受信（通信相手から取得）した証明書セットを部品Ａの通常証明書セット記憶領域に記憶させて図６（ａ）に示した通常証明書セットをその内容に設定する。この処理において、下位装置２０のＣＰＵ２１が証明書設定手段として機能する。

その後、ステップＳ２０７で設定結果を応答として送信元に通知して処理を終了する。

下位装置２０がこのような処理を実行することにより、証明書書き込み装置１６０が、下位装置２０が通常証明書セットの書き込み対象であることについて少なくとも最低限の確認を行うことができるので、全く異なる装置に誤って通常証明書セットを送信してしまうような事態を防止し、証明書設定の安全性を向上させることができる。

【００７８】

また、証明書書き込み装置１６０側にもレスキュー証明書セットを記憶させ、認証処理において下位装置２０との間で相互認証を行うようにしてもよい。この場合に使用するレスキュー証明書セットは、上位装置１０に記憶させるものと同じものになり、下位装置２０側の認証処理も、図１９に示した処理に対応したものになる。そして、このようにすれば、下位装置２０側でも、不正な証明書書き込み装置から送られてくる通常証明書セットを設定してしまうことがないようにすることができる。

なお、証明書書き込み装置１６０が下位装置２０にレスキュー公開鍵証明書を送信して認証を受けるのみとしても、この効果は得ることができるし、証明書書き込み装置１６０と下位装置２０との間でＳＳＬによる安全な通信経路を確立することもできる。

【００７９】

また、通信要求について、下位装置２０側から証明書書き込み装置１６０に対して通信要求を行うようにすることも考えられる。この場合でも、証明書書き込み装置１６０と下位装置２０とがレスキュー公開鍵証明書を用いた認証処理を行い、これが成功した場合に証明書書き込み装置１６０が下位装置２０に通常公開鍵証明書を送信して設定させることは、上述の処理の場合と同様である。

さらに、通常証明書セットを送信する際に、必要に応じて、その通常証明書セットに含まれる公開鍵証明書や私有鍵を用いた認証処理を行うために必要なソフトウェアも共に送信し、下位装置２０に設定させるようにしてもよい。

【００８０】
一方で、図１３において、部品Ａがサービスパーツとして出荷され、設置先で稼動中の下位装置２０（市場機）に装着された場合には、その下位装置２０と対応する上位装置１０によって通常証明書セットが書き込まれることになる。このとき、機番情報入力装置１７１から上位装置１０に書き込み対象の装置の機番を入力し、上位装置１０がその機番の情報を識別情報として含む通常証明書セットを証明書管理装置５０に発行させ、これを取得して下位装置２０に設定させることになる。下位装置２０の機番等の識別情報については、上位装置１０からの要求に応じて下位装置２０から上位装置１０に送信させるようにしてもよい。
また、証明書管理装置５０は、上位装置１０が行う認証処理で使用可能な証明書を発行するパブリックＣＡである。そして、発行された証明書を管理する機能を上位装置１０に設けたり、上位装置１０が間に発行された証明書を管理する装置を介してＣＡに証明書の発行を依頼するような構成が好ましいことは、上述した証明書書き込み装置１６０の場合と同様である。
【００８１】
また、上位装置１０が下位装置２０に通常証明書セットを設定する際には、上位装置１０から下位装置２０のレスキューＵＲＬに通信を要求し、下位装置２０に記憶しているレスキュー証明書セットを用いて、ＳＳＬによる認証処理を行う。そして、上位装置１０が下位装置２０が正当な装置であると認証した場合に、通常証明書セットを送信して部品Ａの通常証明書セット記憶領域に設定させるようにしている。この場合には、上位装置１０が証明書設定装置として機能し、下位装置２０との間でレスキュー公開鍵証明書を用いた認証処理を行って、その認証処理が成功した場合に下位装置２０に通常証明書セットを記憶させることになる。
【００８２】
この場合に下位装置２０側で行う処理は、図１４のフローチャートに示したものと同じものである。もちろん、相互認証を行うようにしてもよい。このことによる効果は、証明書書き込み装置１６０によって書き込む場合と同様であるが、どのような装置と接続されるかわからない出荷後の方が、接続対象が限定される工場内においてよりも安全性向上の要求は強いと言える。なお、上位装置１０が下位装置２０に認証を受ける片方向認証を採用することもできる。また、下位装置２０が上位装置１０に通信要求を行うようにしてもよいことも、上述の証明書書き込み装置１６０によって書き込む場合と同様である。
以上のように市場機に通常証明書セットを設定する場合には、部品Ａを下位装置２０に装着する工程が第１の手順、下位装置２０に通常証明書セットを記憶させる工程が第２の手順に該当する。また、工場で下位装置２０の通常証明書セットを設定できなかった場合には、部品Ａにレスキュー証明書セットのみを記憶させて出荷し、設置先で上記のように第２の手順を実行して通常証明書セットを記憶させるようにすることができる。
【００８３】
以上の説明から明らかなように、ここで説明した方法によれば、下位装置２０に対して、工場での生産時と市場での部品交換時とにおいて同様な手順で通常証明書セットを記憶させることができる。
また、予め部品に記憶させてあるレスキュー証明書セットを用いて認証を行い、これが成功した場合に通常証明書セットを記憶させるので、通常のネットワークＩ／Ｆである通信Ｉ／Ｆ２５を介した通信を用いても、安全に通常証明書セットを下位装置２０に設定することができる。従って、下位装置２０に証明書設定用の特殊なＩ／Ｆを設けることは不要となり、コストを低減することができる。
そして、レスキュー公開鍵証明書をプライベート認証局によって発行されたものとすることにより、設置先における装置の利用環境や、輸出規制等に関わらず共通に利用可能な証明書を発行することが可能となり、使用される環境や地域に応じて装置や部品を作り分ける必要がないため、製造工程や在庫の管理が容易となり、この点でもコストを低減することができる。

【００８４】
また、レスキュー公開鍵証明書の有効期間を少なくとも通常公開鍵証明書の有効期間よりも長くすれば、上述したように、通常公開鍵証明書を記憶させておく場合よりも部品や装置のストック可能期間を延ばすことができるという効果を得ることができる。また、図１３に示したように製品組み立て工程において通常証明書セットを記憶させた後、出荷される前やユーザ環境に設置される前に通常公開鍵証明書の有効期限が切れてしまったような場合でも、レスキュー公開鍵証明書の有効期間内であれば、市場機の部品交換の場合と同様な手順により、再度新たな通常証明書セットを安全に設定することができる。従って、製造工程において通常証明書セットを設定してしまう場合でも、完成した装置のストック可能期間も延ばすことができる。

【００８５】
また、ネットワークＩ／Ｆは下位装置２０の通常動作時においても使用するＩ／Ｆであることから、装置本体の外部に露出した状態で設けられていることが通常である。従って、このようなＩ／Ｆを使用することにより、装置の製造時の証明書設定に関する作業を容易にすることができる。そして、通常公開鍵証明書の設定に際して特殊な冶具やＩ／Ｆを用いないので、ＯＥＭメーカーや市場への流通後においても、ベンダー自身の工場で製造する場合と同様に容易に設定を行うことができる。
一方で、部品にレスキュー証明書セットを記憶させる場合には、専用の冶具を用いて直接行うことができるので、特に認証等を行わなくても安全性を確保することができる。そして、部品の段階では専用冶具のＩ／Ｆを接続が容易な位置に設けることは容易であるので、専用の冶具を用いるようにしても不都合はない。

【００８６】
なお、下位装置２０に、その機番情報を装置の識別情報として付された通常公開鍵証明書を（通常証明書セットの一部として）記憶させるようにする場合であっても、機番は、欠番が生じることを防止するため、装置の組み立てが完了し、品質検査に合格した装置に付すことが一般的である。従って、機番情報を含む公開鍵証明書を装置の製造工程で記憶させるとすると、組み立てが全て完了した状態で行う必要がある。そして、このような場合においては、下位装置２０において通常使用されるインタフェース（例えばネットワークＩ／ＦであるＰＨＹ）を介して記憶させることの効果は、特に大きい。デザインや機能、そしてコスト上の制約から、特殊なインタフェースの接続口は、装置の組み立てが完了した状態で作業しやすい位置や構成となるように設けることが困難なためである。

【００８７】
そして、ここで説明した下位装置２０においては、ネットワークを介して通常証明書セットを書き込むことが可能であるので、装置の組み立て完了後であっても、装置本体の外部に露出している、イーサネット規格等のネットワークケーブルの接続Ｉ／Ｆを介して証明書書き込み装置１６０と接続し、通常証明書セットの書き込み作業を行うことができる。従って、少ない工数で効率のよい作業を行うことができるし、作業中に装置を破損等してしまう危険も極めて少ない。また、この書き込み工程において通信を暗号化できるので、通常証明書セットを安全に記憶させることができる。
なお、証明書書き込み装置１６０と下位装置２０とをこのネットワークＩ／Ｆを介して接続することは必須ではない。他のＩ／Ｆを使用した場合でも、通常公開鍵証明書を設定する場合に部品に記憶させてあるレスキュー公開鍵証明書を用いた認証を行うことにより、証明書設定の安全性を向上させることができる。
また、装置の識別情報として機番以外の情報、例えば独自のＩＤを用いる場合には、品質検査の後で通常公開鍵証明書を記憶させることも必須ではない。しかし、品質検査の後で記憶させるようにすれば、証明書を記憶させた装置が品質検査で不合格となり、識別情報に欠番を生じる事態を防止できる。従って、証明書の管理が容易になる。

【００８８】
また、通常公開鍵証明書とレスキュー公開鍵証明書とでは用途も機能も異なるため、図１３に示したように、これらの証明書は別々のＣＡが発行するようにすることが好ましい

。
すなわち、レスキュー公開鍵証明書は同じ階位の装置全てに同じものを記憶させるため、レスキュールート私有鍵が漏洩するとセキュリティの維持が著しく困難になるので、秘密保持を特に厳重に行う必要がある。一方で、各装置について通常に異なる証明書を作成して記憶させる必要はない。そこで、安全性を重視し、外部からアクセス不能なＣＡを用いるとよい。プライベートＣＡであれば、このような条件を満たすＣＡを用意することは容易である。

【００８９】

一方、通常公開鍵証明書は必要に応じて更新できるため、通常ルート私有鍵が漏洩したとしても、これを更新すればセキュリティを保つことができる。そして、装置毎に個別に証明書を作成して記憶させる必要があることから、インターネット等のオープンネットワークに接続したＣＡを用いるとよい。

なお、ＣＡをさらに細分化し、下位装置の証明書を発行するＣＡ，上位装置用の証明書を発行するＣＡ等、証明書を発行する対象の装置の階位に応じてＣＡを分けるようにしてもよい。

また、通常証明書セットとレスキュー証明書セットとで全く形式の異なるデジタル証明書を使用することも可能である。

【００９０】

次に、上述した製品組み立て工程において通常証明書セットを下位装置２０に設定するために使用する設備について説明する。図１５はその概略構成を示すブロック図である。

この図に示すように、製品組み立て工程を行う生産工場Ｅには、通常証明書セットを設定するための設備として、生産管理システム１４０，通信端末１５０，証明書書き込み装置１６０が設置されている。

そして、生産管理システム１４０は、上位装置１０や下位装置２０等の装置の日々の生産台数を管理する。

【００９１】

通信端末１５０は、証明書データベース（ＤＢ）１５４ａ，入力装置１５６，表示装置１５７を備えている。そして、生産管理システム１４０からその日の機種別の生産台数及び付与予定の機番の情報（ここでは機種コードとシリアル番号とを含めた情報）を取得する。また、その情報に基づいて、その機番の装置が使用する予定の通常公開鍵証明書を発行するＣＡである証明書管理装置５０に生産予定の装置に記憶させるべき通常証明書セットを発行させ、これを入手して証明書ＤＢ１５４ａに記憶させる。なお、機番毎に通常公開鍵証明書を発行するＣＡが異なることも考えられるし、ＣＡを特定できない、工場からは適切なＣＡと通信できない等の理由により工場では通常証明書セットの設定を行わないという情報を記憶させておくことも考えられる。

証明書書き込み装置１６０は、機番情報入力装置１６１を備えており、装置の生産時にその機番情報入力装置１６１から生産中の装置の機番の入力を受け付ける。そして、これが入力された場合に、その機番に対応する通常証明書セットを通信端末１５０から入手し、それを対応する装置へ送信してその装置の不揮発性メモリに設けた通常証明書セット記憶領域に設定させる。下位装置２０を生産する場合には、部品Ａに設けた記憶領域に設定させることになる。

【００９２】

次に、図１６に生産工場Ｅにおける通信端末１５０および証明書書き込み装置１６０の周辺の状況の概略を示す。

生産工場Ｅにおいては、通信端末１５０は、セキュリティ面を考慮して管理者室Ｆに設置している。そして、その管理者室Ｆは、特定の管理者しか入れないように、ドアＧに鍵をかけるようにしており、通信端末１５０は、特定のＩＤとパスワードが入力された場合にのみ操作できるようにしている。

またこの例では、生産工場Ｅには上位装置１０の生産用ライン１００１と下位装置２０の生産用ライン１００２とを設けている。そして、その各生産用ライン毎に証明書書き込

み装置１６０（１６０ａ，１６０ｂ）を設置している。

【００９３】

そして、各証明書書き込み装置１６０にはそれぞれ、機番情報入力装置１６１（１６１ａ，１６１ｂ）と接続するための機番情報入力用Ｉ／Ｆ１６２（１６２ａ，１６２ｂ）、および生産する装置（上位装置１０及び下位装置２０）と接続するための書き込み用Ｉ／Ｆ１６５（１６５ａ，１６５ｂ）がそれぞれ接続されている。

このような生産ラインにおいては、例えば下位装置２０を生産する場合、品質検査に合格した装置に識別番号を付与する際に、定格銘板を貼付する。この定格銘板の例を図１７に示すが、定格銘板には、定格電圧，消費電力等の情報と共に、装置の機番を記載している。そしてさらに、この機番の情報を示すバーコードＢＣも記載している。

【００９４】

そして、通常証明書セットの設定工程においては、まず書き込み用Ｉ／Ｆ１６５としてイーサネット規格のクロスケーブルを用いて証明書書き込み装置１６０と設定対象の下位装置２０を接続する。ここでクロスケーブルを用いるのは、生産される各装置は初期値として同じＩＰアドレスを有しており、証明書書き込み装置１６０とＬＡＮ接続すると、ＩＰアドレスが重複してしまうためである。

続いて機番情報入力装置１６１としてバーコードリーダを用い、定格銘板上のバーコードＢＣを読み取って作業対象の装置の機番の情報を証明書書き込み装置１６０に入力する。すると、証明書書き込み装置１６０がその機番に対応する通常証明書セットを通信端末１５０から入手し、書き込み用Ｉ／Ｆ１６５を介して接続する下位装置２０へ送信してその装置の部品Ａに設けた通常証明書セット記憶領域に設定させる。なお、証明書ＤＢ１５４ａに証明書を設定しない旨の情報が記憶されていた場合には、通常証明書セットの設定は行わない。

以上の作業及び処理により、生産する各下位装置２０に、その機番情報を装置の識別情報として付され、かつその機番の装置が使用する予定の通常公開鍵証明書を簡単な作業で記憶させることができる。

【００９５】

なお、以上説明した実施形態では、上位装置１０と下位装置２０を始めとする各装置間で、図１９あるいは図２１を用いて説明したようなＳＳＬに従った認証を行う場合の例について説明した。しかし、この認証が必ずしもこのようなものでなくてもこの実施形態は効果を発揮する。

ＳＳＬを改良したＴＬＳ（Transport Layer Security）も知られているが、このプロトコルに基づく認証処理を行う場合にも当然適用可能である。

【００９６】

また、上述した実施形態では、パブリック認証局が発行した通常公開鍵証明書と、プライベート認証局が発行したレスキュー公開鍵証明書とを用いる例について説明したが、前者はセキュリティ強度が高い証明書、後者はセキュリティ強度が比較的低い証明書と捉えることもできる。

一般に、セキュリティ強度が高い証明書には、多くの情報を記載する必要があったり、輸出制限があったり特殊な認証処理プログラムが必要であったりして利用可能な環境が限られていたりするため、全ての装置に同じように記憶させて認証処理に用いることが難しい場合がある。一方で、セキュリティ強度が低い証明書であれば、このような制限が少なく、全ての装置に同じように記憶させて認証処理に用いることが比較的容易であると考えられる。

【００９７】

そこで、セキュリティ強度が低い証明書を記憶させた装置を製造・販売した上で、利用環境に合わせてセキュリティ強度が高い証明書を事後的に記憶させることができるようにしたいという要求がある。例えば、システムの運用者によって種々に認証処理の内容を工夫したり信頼性の高いＣＡを選択したりしてセキュリティの向上を図る場合も考えられるが、このような場合、ある装置を１つのシステムから他のシステムに移動（単に設定を変

更するのみの場合も含む）させる場合、通常の認証処理に使用する証明書を入れ換える必要があることが考えられる。また、セキュリティの高い証明書に後で欠陥が発見され、認証処理の方式を変更する必要が生じることも考えられる。

【００９８】

このような場合に、上述した実施形態の構成を利用し、セキュリティ強度が低い証明書を記憶している部品を通信装置に装着し、その後証明書設定装置との間でその証明書を用いた認証処理を行い、その処理が成功した場合に、証明書設定装置が通信装置に、セキュリティ強度が高い証明書を記憶させるようにすることにより、セキュリティ強度が高い証明書を装置の製造あるいは出荷後に事後的に設定する場合でも、これを容易かつ安全に設定することができる。また、製造する部品や装置に種々の環境で共通に利用できるようなセキュリティの比較的低い証明書を記憶させておくようにすることにより、その部品を種々の環境で共通に利用することができるので、部品や装置の供給が容易になる。

【００９９】

また、上述した実施形態では、通常公開鍵証明書に装置の識別情報を記載する例について説明したが、パブリック認証局がこのようなサービスを提供していれば、通常公開鍵証明書にも装置の識別情報を含めず、同じ階位の装置には、全て同じ通常公開鍵証明書を記憶させるようにしてもよい。このようにしたとしても、通信相手との間で共通鍵を共有して共通鍵暗号を用いた安全な通信経路を設けた後で機番情報等を交換して通信相手を特定することが可能であることは、レスキュー公開鍵証明書の場合と同様である。そして、このようにしたとしても、パブリック認証局が発行するものであるから信頼性は高いと考えられる。また、レスキュー公開鍵証明書よりも有効期間が短ければ、その分だけレスキュー公開鍵証明書よりも安全性を高めることができる。

また、通常公開鍵証明書とレスキュー公開鍵証明書の有効期間についても、特に上述した関係に限定されることはない。さらに、認証局の種類についても、セキュリティ高低の１つの要素と捉え、有効期間、装置の識別情報の有無、証明書を用いた認証処理の暗号強度等により、通常公開鍵証明書とレスキュー公開鍵証明書の差を出すようにすることも考えられる。

【０１００】

また、上述した実施形態では、証明書管理装置５０を上位装置１０と別に設ける例について説明したが、これらが一体である構成を排除するものではない。この場合、証明書管理装置５０の機能を実現するためのＣＰＵ，ＲＯＭ，ＲＡＭ等の部品を独立して設けてもよいが、上位装置１０のＣＰＵ，ＲＯＭ，ＲＡＭ等を使用し、そのＣＰＵに適当なソフトウェアを実行させることにより、証明書管理装置５０として機能させるようにしてもよい。

このような場合において、証明書管理装置５０と、これと一体になっている上位装置１０との間の通信には、ハードウェアを証明書管理装置５０として機能させるためのプロセスと、ハードウェアを上位装置１０として機能させるためのプロセスとの間のプロセス間通信を含むものとする。

【０１０１】

さらに、上述した実施形態では、証明書管理装置５０がルート鍵やデジタル証明書を自ら作成する例について説明したが、証明書管理装置５０は鍵や証明書の管理を専門に行い、他の装置からルート鍵やデジタル証明書の供給を受けてこれらを取得するようにしてもよい。

【０１０２】

また、上述した実施形態では、通信システムを上位装置１０と下位装置２０のみによって構成したが、他の装置を含めて構成する場合にも適用できる。例えば、上位装置１０と下位装置２０との間の通信を仲介する仲介装置を設け、上位装置１０と下位装置２０とがこの仲介装置を介して要求や応答を授受するようにしてもよい。あるいは、上位装置１０のさらに上位の装置を設けてもよい。この場合には、上位装置１０を「下位装置」、その更に上位の装置を「上位装置」と見れば、これらの装置についても上述した実施形態の場

合と同様な取り扱いが可能である。

【０１０３】

また、従来から、通信機能を備えたプリンタ，ファクシミリ（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を被管理装置とし、これらの被管理装置と通信可能な管理装置によってこれらの被管理装置を遠隔管理する遠隔管理システムが提案されている。

例えば、画像形成手段を備えた画像処理装置については、感光体静電プロセスを用いて普通紙に画像形成するものが一般的であるが、このような感光体静電プロセスを行う機構からは、トラブル（異常）が発生する割合も高く、更に性能維持のための定期的なオーバホールの必要性から、保守管理のサービス体制を採っている。

そして、この保守管理を充実させる目的で、画像形成装置を被管理装置とする遠隔管理システムとして、画像形成装置の内部又は外部に通信装置を設け、画像形成装置とサービスセンタ（管理センタ）に設置された管理装置とを公衆回線（電話回線）を介して接続し、画像形成装置の異常発生時にその旨を管理装置に通報するようにしたものが既に開発され運用されている。

【０１０４】

上述した実施形態は、このような遠隔管理システムにおける被管理装置にデジタル証明書を設定する場合にも適用可能であり、この場合、被管理装置を下位装置とし、被管理装置を管理する管理装置やユーザ環境内にあって複数の被管理装置の情報を取りまとめるような装置を上位装置とするとよい。

遠隔管理を行う場合には、被管理装置の近くに管理装置の操作者がいないことが多いため、被管理装置の特定は、通信によって行う必要がある。そして、通信によって特定された被管理装置が確かにその装置であることを保証する仕組みが必要になる。従って、上述の実施形態で説明したように通常公開鍵証明書を製造時及びユーザ環境への設置後に容易に設定できるようにし、通常公開鍵証明書を用いた認証を容易に高い信頼性で運用できるようにすることによる効果は大きい。

【０１０５】

なお、遠隔管理の対象としては、画像処理装置に限られず、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，自動車，航空機あるいは汎用コンピュータ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とすることが考えられる。ただし、下位装置２０が遠隔管理システムにおける被管理装置に限られるものでないことも、もちろんである。

【産業上の利用可能性】

【０１０６】

以上説明してきたように、この発明の通信装置、通信システム、通信方法及びプログラムによれば、セキュリティを維持しながら、認証に必要な証明書を記憶する部品を交換する必要が生じた場合でも、容易かつ速やかに正常な認証が行える状態に容易に回復させることができる。従って、証明書を使用する通信装置の製造や通信システムの運用を容易に高い信頼性で行うことができる。

【図面の簡単な説明】

【０１０７】

【図１】この発明の証明書設定方法を適用する通信装置である下位装置を含む通信システムの構成例を示すブロック図である。

【図２】図１に示した上位装置及び下位装置のハードウェア構成を示すブロック図である。

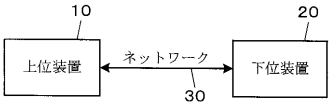
【図３】同じく上位装置及び下位装置の遠隔管理及び証明書の設定に関わる部分の機能構成を示す機能ブロック図である。

【図４】図３に示した要求管理部における動作の実行可否の判断基準を示す図である。

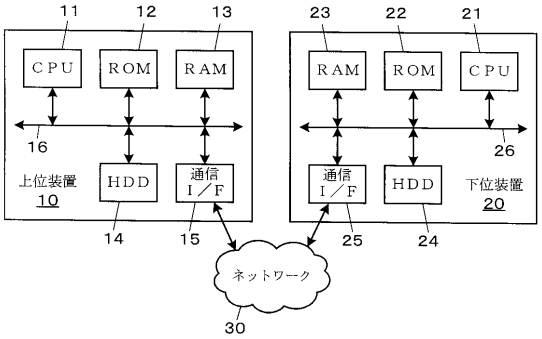
【図５】図１に示した通信システムにおける上位装置と下位装置との間の通信方式の概要を示す説明図である。

【図６】図１に示した上位装置及び下位装置が記憶する認証情報について説明するための図である。
【図７】通常公開鍵証明書のフォーマット例について説明するための図である。
【図８】図７に記載したフォーマットに従って作成した一般的な公開鍵証明書の例を示す図である。
【図９】同じく、レスキュー公開鍵証明書と対比するための、通常公開鍵証明書の例を示す図である。
【図１０】同じく、通常公開鍵証明書と対比するための、レスキュー公開鍵証明書の例を示す図である。
【０１０８】
【図１１】図１に示した上位装置及び下位装置が通常公開鍵証明書とレスキュー公開鍵証明書とを使い分けるための構成について説明するための図である。
【図１２】証明書の記憶領域を設ける部品Ａ及びその部品Ａを装着した下位装置の製造工程の概略を示す図である。
【図１３】その部品Ａに各証明書セットを記憶させる工程について説明するための図である。
【図１４】図１３に示した工程において下位装置に通常証明書セットを書き込む際に下位装置側で実行する処理を示すフローチャートである。
【図１５】図１２及び図１３に示した製品組み立て工程において通常証明書セットを下位装置に設定するために使用する設備の概略を示す図である。
【図１６】生産工場における、図１５に示した通信端末および証明書書き込み装置の周辺の状況の概略を示す図である。
【図１７】機能検査に合格した装置に識別番号を付与する際に貼付する定格銘板の例を示す図である。
【図１８】図１に示した通信システムについて、下位装置を複数設けた場合の構成について説明するための図である。
【図１９】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２０】図１９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。
【図２１】２つの通信装置がＳＳＬに従った片方向認証を行う際の各装置において実行する処理を示す、図１９と対応する図である。
【図２２】通常の情報を不揮発性記憶デバイスに書き込むために従来用いられていた方法について説明するための図である。
【符号の説明】
【０１０９】
１０…上位装置、１１…ＣＰＵ、１２…ＲＯＭ、１３…ＲＡＭ、１４…ＨＤＤ、
１５…通信Ｉ／Ｆ、１６…システムバス、２０…下位装置、
３１，４１…ＨＴＴＰＳクライアント機能部、３２，４２…ＨＴＴＰＳサーバ機能部、
３３，４３…認証処理部、３４…証明書更新要求部、３５，４５…証明書記憶部、
４４…要求管理部、４６…状態通知部、４７…ログ通知部、４８…証明書設定部、
４９…コマンド受信部、５０…証明書管理装置、６０，７０…ＳＯＡＰメッセージ、
１４０…生産管理システム、１５０…通信端末、１５４ａ…証明書ＤＢ、
１５６…入力装置、１５７…表示装置、１６０…証明書書き込み装置、
１６１…機番情報入力装置、１６２…機番情報入力用Ｉ／Ｆ、
１６５…書き込み用Ｉ／Ｆ、ＢＣ…バーコード、Ｅ…生産工場、Ｆ…管理者室、Ｇ…ドア

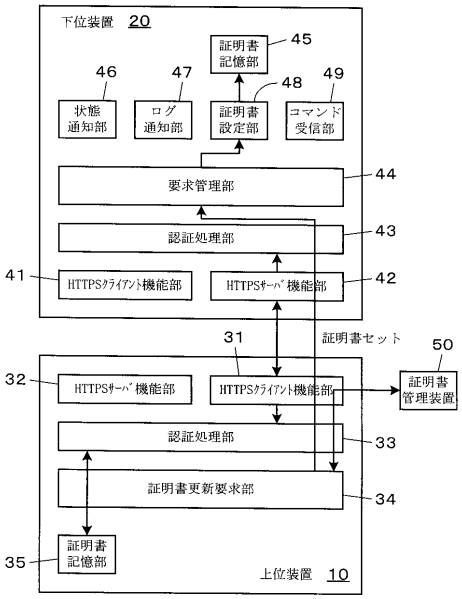
【図１】



【図２】



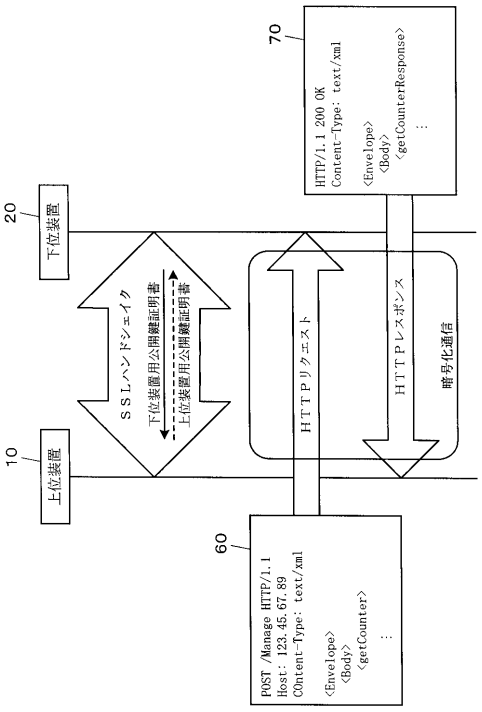
【図３】



【図４】

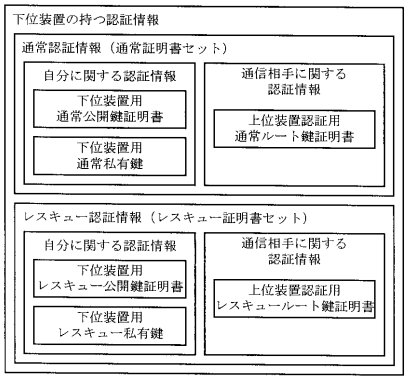
	状態取得	ログ取得	証明書設定	コマンド実行
レスキュー公開鍵証明書	×	×	○	×
通常公開鍵証明書	○	○	○	○

【図５】

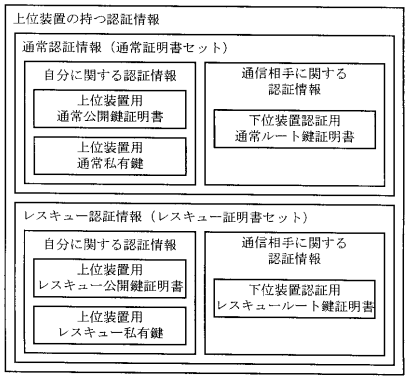


【図６】

（ａ）



（ｂ）



【図７】

```
Data（データ部）
    Version（X509のバージョン）
    Serial Number（シリアル番号）
    Signature Algorithm（ＣＡが利用する暗号化アルゴリズム）
    Issuer（証明書の発行者）
    Validity（有効期限）
    Subject（証明される対象）
    Subject Public Key Info（証明される対象の公開鍵に関する情報）
        Public Key Algorithm（公開鍵のアルゴリズム）
        RSA Public Key（公開鍵）
        X509v3 extensions（X509 Version.3の拡張部）
            ・・・
Signature Algorithm（ＣＡが利用する暗号化アルゴリズム）
Signature（ＣＡによるデジタル署名）
```

【図８】

```
Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
A   Issuer: C=JP, ST=Tokyo, L=Ohtaku, O=XXX Company, Ltd, CN=CA001
B   Validity
        Not Before: May 20 00:00:00 2000 GMT
        Not After : May 20 00:00:00 2001 GMT
C   Subject: C=JP, Tokyo, L=Ohtaku, O=XXX Company, Ltd, CN=Device-0123456
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
            [Device-0123456の公開鍵]
            Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
Signature:
        [CA局　CA001による署名データ]
```

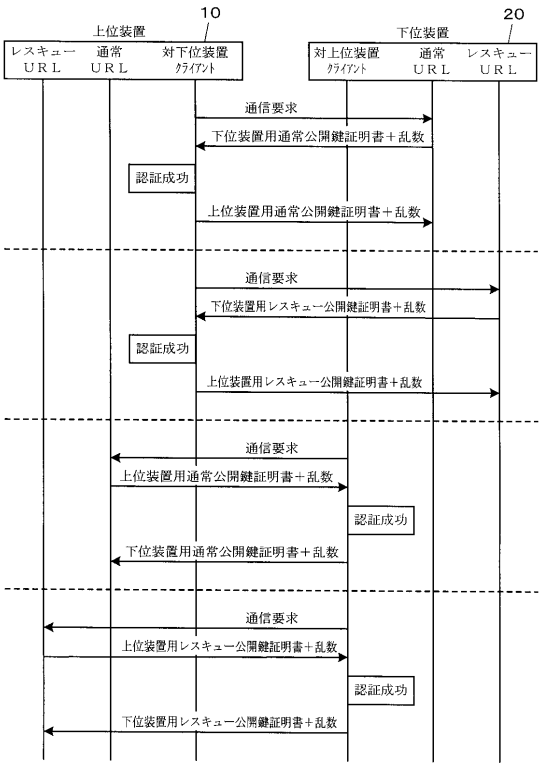
【図９】

```
Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
D   Issuer: C=JP, ST=Tokyo, L=Ohtaku, O=YYY Company, Ltd, CN=PublicCA
E   Validity
        Not Before: Jan 1 00:00:00 2003 GMT
        Not After : Jan 1 00:00:00 2004 GMT
F   Subject: C=JP, Tokyo, L=Ohtaku, O=XXX Company, Ltd, CN=Device-0123456
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
            [Device-0123456の公開鍵]
            Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
Signature:
        [CA局PublicCAによる署名データ]
```

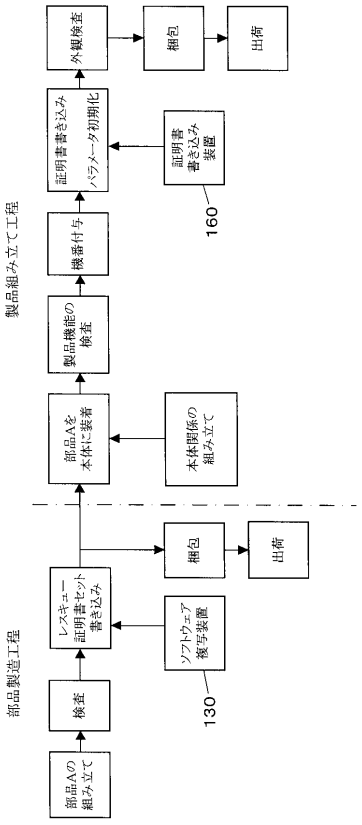
【図１０】

```
Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
G   Issuer: C=JP, ST=Tokyo, L=Ohtaku, O=XXX Company, Ltd, CN=PrivateCA
H   Validity
        Not Before: Jan 1 00:00:00 2000 GMT
        Not After : Jan 1 00:00:00 2050 GMT
I   Subject: C=JP, Tokyo, L=Ohtaku, O=XXX Company, Ltd, CN=0
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
            [Device-0123456の公開鍵]
            Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
Signature:
        [CA局PrivateCAによる署名データ]
```

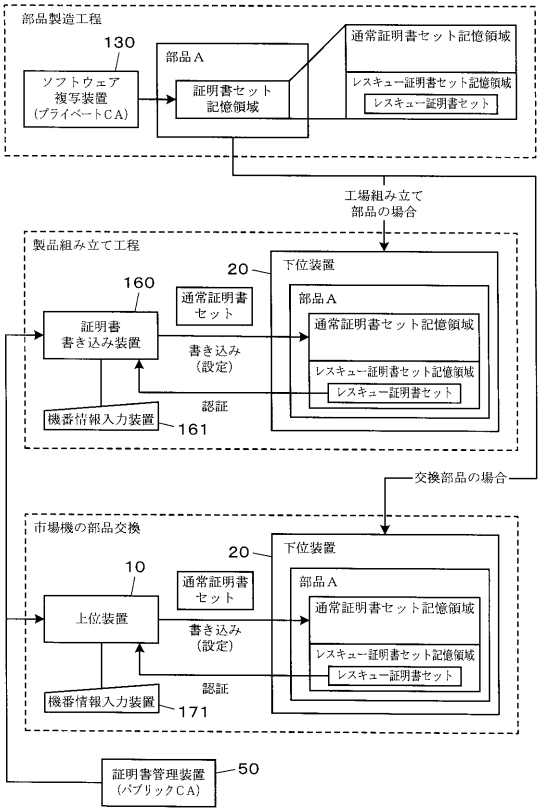
【図１１】



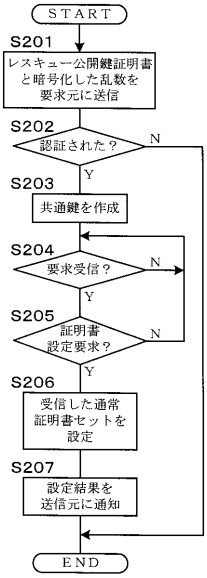
【図１２】



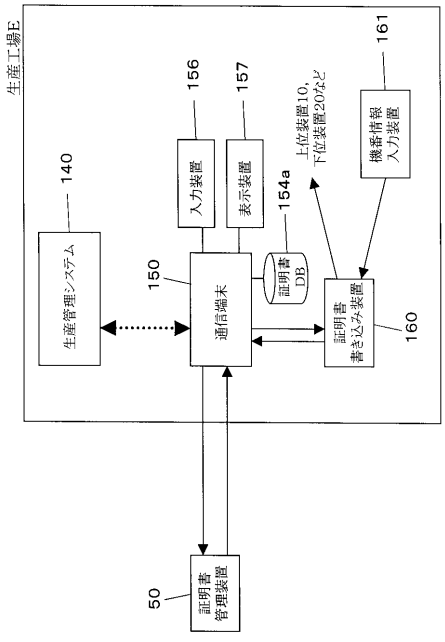
【図１３】



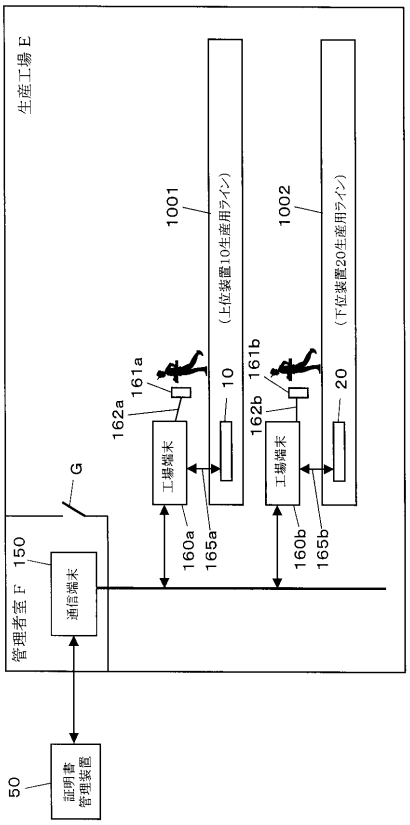
【図１４】



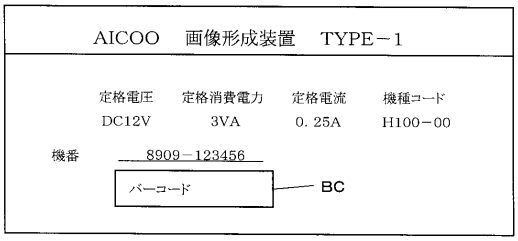
【図１５】



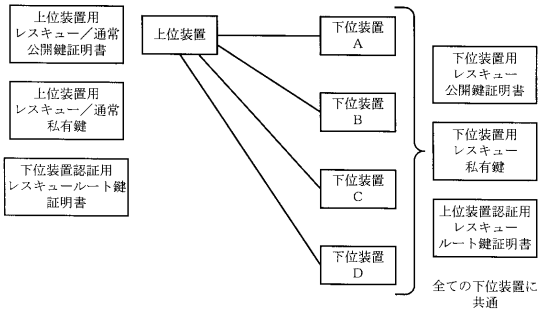
【図１６】



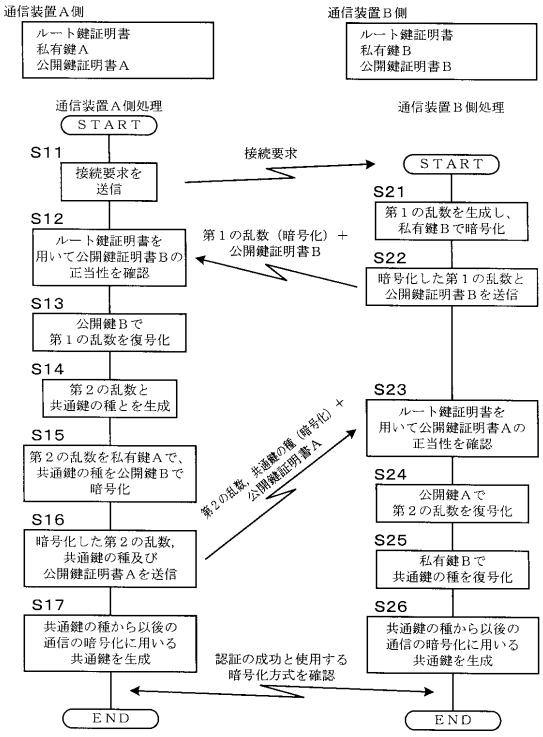
【図１７】



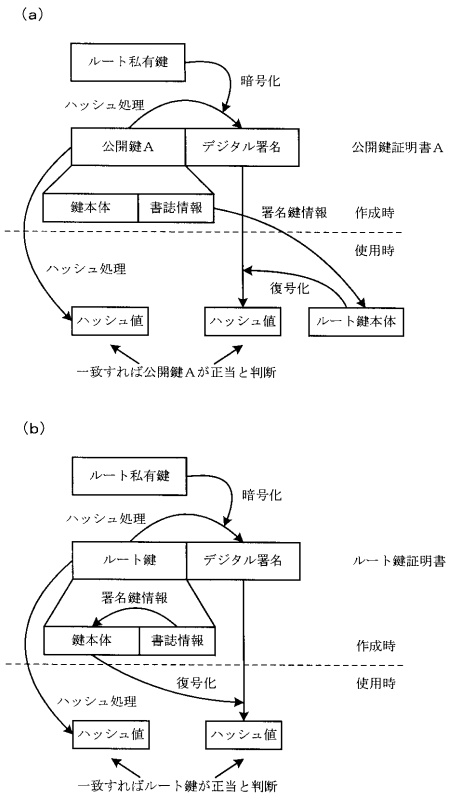
【図１８】



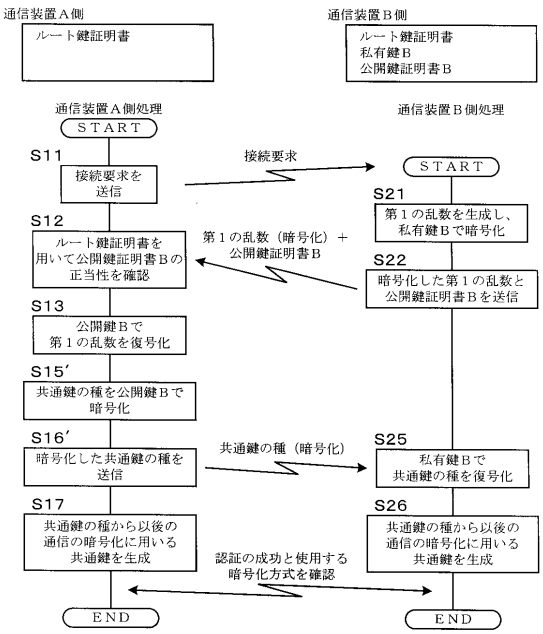
【図１９】



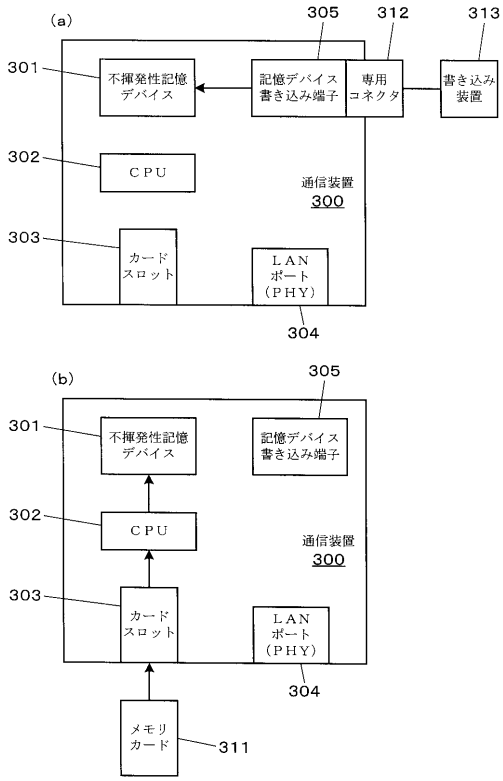
【図２０】



【図２１】



【図２２】


(a)
305
312
313
301
不揮発性記憶デバイス
記憶デバイス書き込み端子
専用コネクタ
書き込み装置
302
ＣＰＵ
通信装置
300
303
カードスロット
ＬＡＮポート（ＰＨＹ）
304
(b)
305
301
不揮発性記憶デバイス
記憶デバイス書き込み端子
302
ＣＰＵ
通信装置
300
303
カードスロット
ＬＡＮポート（ＰＨＹ）
304
メモリカード
311

フロントページの続き

(56)参考文献 米国特許第０５７８１７２３（ＵＳ，Ａ）
国際公開第００／０７９７２４（WO，Ａ１）
米国特許第０６２３３６８５（ＵＳ，Ｂ１）
特表２００２－５２９００８（ＪＰ，Ａ）
特表平０９－５０７７２９（ＪＰ，Ａ）
特開２００３－２２９８５１（ＪＰ，Ａ）
米国特許第０６３１４５２１（ＵＳ，Ｂ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８