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

特許第4712325号
(P4712325)

(45)発行日　平成23年6月29日(2011.6.29)　(24)登録日　平成23年4月1日(2011.4.1)

| (51)Int.Cl. | | | F I | | |
|---|---|---|---|---|---|
| H04L | 9/10 | (2006.01) | H04L | 9/00 | 621A |
| H04L | 9/32 | (2006.01) | H04L | 9/00 | 675B |
| H04L | 9/08 | (2006.01) | H04L | 9/00 | 601F |

請求項の数 8　(全 29 頁)

(21)出願番号　特願2004-211396 (P2004-211396)
(22)出願日　平成16年7月20日 (2004.7.20)
(65)公開番号　特開2005-110212 (P2005-110212A)
(43)公開日　平成17年4月21日 (2005.4.21)
審査請求日　平成18年12月18日 (2006.12.18)
(31)優先権主張番号　特願2003-321762 (P2003-321762)
(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)

前置審査

(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　青木　重徳

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、

当該通信装置を一意に特定するための識別情報を含む第１の証明書と当該通信装置を一意に特定するための識別情報を含まない第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る場合は前記第１の証明書を前記相手先装置へ送信し、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】

請求項１又は２に記載の通信装置であって、

当該通信装置を一意に特定するための識別情報は、当該通信装置の機番であることを特徴とする通信装置。

【請求項４】

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、
前記下位装置を一意に特定するための識別情報を含む第１の証明書と前記下位装置を一意に特定するための識別情報を含まない第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る場合は前記第１の証明書を前記上位装置へ送信し、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５】
請求項４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６】
請求項４又は５に記載の通信システムであって、
前記下位装置を一意に特定するための識別情報は、前記下位装置の機番であることを特徴とする通信システム。
【請求項７】
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、前記通信装置を一意に特定するための識別情報を含む第１の証明書と前記通信装置を一意に特定するための識別情報を含まない第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る場合は前記第１の証明書を前記相手先装置へ送信し、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８】
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、前記通信装置を一意に特定するための識別情報を含む第１の証明書と前記通信装置を一意に特定するための識別情報を含まない第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る場合は前記第１の証明書を前記相手先装置へ送信し、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１８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１８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１９にこれらの関係を示す。

図１９（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１９（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１８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１８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１８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２０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。

【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、通信相手の機器の固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。
また、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ができる。

【００１５】

ここで、通信装置間で通信を行わせる通信システムを運用する場合、装置の近くに操作者がいないことが想定される場合には、装置の特定を、通信によって行えるようにしたいという要求がある。そして、このような要求を満たすためには、通信によって特定された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。すなわち、上記の第２のレベルの認証が必要になる。
しかし、上記のように安全な通信経路を確立した後でＩＤを送信させて通信相手を特定する方式では、ＩＤをアプリケーションによってＳＳＬに従った認証処理とは別に管理する必要が生じる。
また、共通の公開鍵証明書と私有鍵が漏洩すると、これを取得した第３者はＩＤのわかる機器ならどの機器にでも成りすませてしまうため、著しく通信の安全が損われる。そしてこの場合、全ての機器の鍵を更新しなければ通信の安全は回復できず、この作業は多大な労力を要するものである。

【００１６】
そして、この問題を解決するためには、公開鍵証明書と私有鍵を装置毎に発行し、公開鍵証明書の書誌情報に装置の識別情報を記載し、公開鍵証明書の正当性を確認する際に書誌情報に含まれる識別情報も参照して、その証明書を送信してきた相手（証明書の発行対象の装置）が適当な通信相手であることを確認するようにすることが考えられる。このようにした場合には、装置毎に異なった公開鍵証明書と私有鍵のペアを記憶させるため、１つの機器の鍵が漏洩したとしても、その機器にしかなりすますことはできず、また、その機器の鍵を更新してしまえば、通信を再び安全な状態に保つことができる。
【００１７】
ところで、装置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、当然ながら装置を特定する認証が必要になる。そこで、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が、デジタル証明書を記憶する部品を交換してしまうと、デジタル証明書も部品と共に取り去られてしまう。このため、装置の認証が不可能になってしまうことになる。従って、装置の識別情報を記載した公開鍵証明書を使用する場合には、破損や故障等によりデジタル証明書を記憶する部品を交換する必要が生じた場合に問題が生じることになる。
【００１８】
交換後の部品にデジタル証明書が記憶されていれば問題ないが、機器やユーザの特定を行うためには部品の交換時に使用する識別情報が変わってしまうことは好ましくない。しかし、交換後の部品にも交換前と同じ識別情報を記載した公開鍵証明書を記憶させるようにするためには、交換後の部品を製造する際に装着予定の装置の識別情報が必要となり、新たな公開鍵証明書を記録した交換用部品を予め用意しておくことができない。このため、部品を交換する装置が判明してから必要に応じて製造することになり、極めて効率の悪い生産体制を強いられることになるという問題がある。
また、迅速に部品を供給できないため、ある程度の期間は装置をＳＳＬに従った認証処理を正常に行うことができない状態に置かねばならず、その間は部品を交換した装置に対する安全な通信経路を確保できないという問題もある。
【００１９】
部品を交換してから別途公開鍵証明書や私有鍵を記憶させることも考えられるが、これらを持たない状態ではＳＳＬに従った認証処理を正常に行うことができず、部品を交換した装置に対する安全な通信経路を確保することができない。そこで、新たな公開鍵証明書等を安全に配布するためには、これを記録媒体に記録して、装置の設置先に郵送したり、部品交換のサービスマンが持参したりする必要がある。しかし、この記録媒体の作成においても、上述の部品製造の場合と同様な問題がある。
さらに、装置の成りすまし等を防止するため、デジタル証明書については、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デジタル証明書の更新を禁止する必要があるので、手動でデジタル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。
【００２０】
この発明は、このような問題を解決し、通信手段によって通信相手と通信可能な通信装置あるいはこのような通信装置を備える通信システムにおいて、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、この発明の通信装置は、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において、その通信装置を一意に特定するための識別情報を含む第１の証明書とその通信装置を一意に特定するための識別情報を含まない第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る場合は上記第１の証明書を上記相手先装置へ送信し、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ものである。

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。

さらに、その通信装置を一意に特定するための識別情報を、その通信装置の機番とするとよい。

【００２２】

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、上記下位装置を一意に特定するための識別情報を含む第１の証明書と上記下位装置を一意に特定するための識別情報を含まない第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る場合は上記第１の証明書を上記上位装置へ送信し、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。

さらに、上記下位装置を一意に特定するための識別情報を、上記下位装置の機番とするとよい。

【００２３】

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、上記通信装置を一意に特定するための識別情報を含む第１の証明書と上記通信装置を一意に特定するための識別情報を含まない第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る場合は上記第１の証明書を上記相手先装置へ送信し、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。

【００２４】

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、上記通信装置を一意に特定するための識別情報を含む第１の証明書と上記通信装置を一意に特定するための識別情報を含まない第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る場合は上記第１の証明書を上記相手先装置へ送信し、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】

【００２９】
以上のようなこの発明の通信装置、通信システムあるいは通信方法によれば、通信手段によって通信相手と通信可能な通信装置あるいはこのような通信装置を備える通信システムにおいて、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。また、この発明のプログラムによれば、コンピュータに通信装置を制御させることにより上記の通信装置として機能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。

【発明を実施するための最良の形態】

【００３０】
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、この発明による通信装置と、その通信装置を用いて構成したこの発明の通信システムの実施形態の構成について説明する。
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。そして、下位装置２０がこの発明の通信装置の実施形態である。また、上位装置１０も通信機能を備えた通信装置であり、下位装置２０の通信相手となる。
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１７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。

【００３１】
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。

【００３２】
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、個別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。
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。

【００３３】
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。

【００３４】

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。

【００３５】

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。

【００３６】

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個別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。

【００３７】

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。

【００３８】

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。

【００３９】

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、個別証明書であり装置（自機）の識別情報が付された公開鍵証明書である個別公開鍵証明書と、共通証明書であり

装置の識別情報が付されていない公開鍵証明書である共通公開鍵証明書があり、要求管理部４４は、図３に示すように、個別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、共通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、共通証明書は、下位装置２０に新たな個別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。

【００４０】

証明書記憶部４５は、上位装置の証明書記憶部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。

【００４１】

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４０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個別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個別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。

【００４２】

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１８又は図２０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１８に示したような相互認証は必須ではなく、図２０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。

【００４３】

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共有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。

【００４４】

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。

【００４５】

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、大きく分けて個別認証情報と共通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。

【００４６】

また、例えば下位装置用個別公開鍵証明書は、個別証明書であり、図示しない認証局（ＣＡ）が下位装置２０に対して発行した個別公開鍵に、下位装置認証用個別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。

ここで、図７に下位装置用個別公開鍵証明書に含まれる情報の例を示すが、この証明書は、書誌情報に発行対象である下位装置２０の識別情報として下位装置２０の機番情報を含むものである。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含めるようにしてもよい。

【００４７】

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。

【００４８】

また、図６の説明に戻ると、下位装置用個別私有鍵はその個別公開鍵と対応する私有鍵、上位装置認証用個別ルート鍵証明書は、上位装置認証用個別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。下位装置２０を複数設けた場合でも、各装置の個別公開鍵は同じルート私有鍵を用いてデジタル署名を付し、正当性確認に必要な個別ルート鍵証明書は共通にする。しかし、個別公開鍵証明書に含まれる個別公開鍵やこれと対応する私有鍵は、装置毎に異なる。ここで、これらの個別公開鍵証明書と個別私有鍵と個別ルート鍵証明書とを合わせて、個別証明書セットと呼ぶことにする。

上位装置用個別公開鍵証明書と上位装置用個別私有鍵と上位装置認証用個別ルート鍵証

明書も、これらと同様な関係を有する。

【００４９】

そして、例えば上位装置１０と下位装置２０とが個別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は下位装置用個別私有鍵を用いて暗号化した第１の乱数を下位装置用個別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個別ルート鍵証明書を用いてまずこの下位装置用個別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個別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個別公開鍵証明書及び、上位装置用個別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。

【００５０】

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、発明の開示の項で述べたように、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、再度個別公開鍵証明書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。

【００５１】

ここで、各装置が個別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、新たな個別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、この実施形態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に共通認証情報を記憶しており、これを用いることにより、必要な装置にネットワーク３０を介して新たな個別公開鍵証明書等を安全に送信できるようにしている。

【００５２】

この共通認証情報は、個別認証情報と概ね同様な構成となっている。例えば下位装置用共通公開鍵証明書は、共通証明書であり、ＣＡが下位装置に対して発行した共通公開鍵に、上位装置認証用共通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、上位装置用共通私有鍵はその共通公開鍵と対応する私有鍵、下位装置認証用共通ルート鍵証明書は、下位装置認証用共通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、これらの共通公開鍵証明書と共通私有鍵と共通ルート鍵証明書とを合わせて、共通証明書セットと呼ぶことにする。上位装置１０側に記憶させる共通認証情報についても同様とする。

【００５３】

しかし、個別認証情報と大きく異なる点は、共通公開鍵証明書の書誌情報には装置の識別情報が含まれておらず、同じ階位の装置（図１あるいは図１７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、全て同じ共通公開鍵証明書を記憶させることができる点である。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、証明書に含まれる共通公開鍵及びこれと対応する共通私有鍵も含めて、全く共通のものでよい。そして、通信相手の共通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に同じ共通認証情報を記憶させることになる。

これは、上位装置１０の共通認証情報についても同様である。

なお、個別公開鍵証明書とデータ形式を統一化する場合には、例えば図７に示した形式

において機番として０を記載して共通公開鍵証明書であることを示すこと等も考えられる。

【００５４】

このような共通認証情報は、同じ階位の装置について全て共通にできるという特性から、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、このように部品に予め共通認証情報を記憶させておくようにすれば、記憶部品を交換して装置内に個別認証情報がなくなってしまったとしても、新たな部品に記憶させてある共通認証情報に含まれる共通公開鍵証明書を用いた認証が可能な状態を保つことができる。また、このような共通認証情報を記憶しており、個別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。従って、部品をストックしておき、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。

【００５５】

ここで、共通公開鍵証明書には装置の識別情報を付していないため、共通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共通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共通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共通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共通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。

【００５６】

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。

【００５７】

なお、図６に示した認証情報において、個別ルート鍵証明書は認証対象によらず同じものを用いるようにしてもよい（例えば上位装置認証用個別ルート鍵証明書と下位装置認証用個別ルート鍵証明書が同じものでもよい）。これは、個別公開鍵証明書には装置の識別情報が付されているため、ルート鍵証明書を用いてその正当性を確認できれば、あとはその識別情報を参照して装置の機種や階位を特定できるためである。一方、共通証明書には装置の識別情報が付されていないため、その種類の区別は特定のルート鍵証明書で正当性を確認できるか否かによって行うことになる。従って、共通ルート鍵証明書は区別すべき認証対象のグループ毎に異なるようにするとよい。

【００５８】

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、状況に応じて個別公開鍵証明書と共通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８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、個別公開鍵証明書を複数持ち、通信相手の持つ個別ルート鍵証明書の

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。

【００５９】

従ってここでは、図８に示すように、上位装置１０及び下位装置２０にそれぞれ、個別公開鍵証明書による認証を行う通常ＵＲＬと共通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。

【００６０】

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個別公開鍵証明書を返し、レスキューＵＲＬで受け付けた場合には共通公開鍵証明書を返すことができる。

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。

【００６１】

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個別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共通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。共通公開鍵証明書を用いた認証であっても、共通鍵の共有は個別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に設定用の個別認証情報を送信して記憶させることにより、再度個別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。

【００６２】

また、共通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個別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、不正な装置に個別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、個別認証情報に加えて共通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。

【００６３】

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。個別認証情報と共通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。

【００６４】

次に、下位装置２０や上位装置１０において、上述した認証情報を記憶する記憶領域を設けるハードウェアについて説明する。

下位装置２０や上位装置１０において、このような記憶領域は、不揮発性の記録媒体であれば設計上はどこにでも設けることができる（ただし、個別証明書セットを記憶する領域は書き換え可能な記録媒体に設けることが好ましい）。例えば、下位装置２０において、個別証明書セットを記憶する記憶領域をＲＡＭ２３に、共通証明書セットを記憶する記

憶領域をＲＯＭ２２に設けることもできる。
しかしながら、個別証明書セットと共通証明書セットの記憶領域を別々に交換可能な部品に設けると、以下のような問題が生じる。図９を用いてこの問題について説明する。図９は、この実施形態の比較例における、証明書の記憶領域を設ける交換部品の構成及びその問題点について説明するための図である。

【００６５】
比較例として、図９（ａ）に示すように、別々に交換可能な部品Ｘと部品Ｙにそれぞれ個別証明書セット記憶領域と共通証明書セット記憶領域を設けた構成を考える。すると、この場合には、部品Ｘについては、製造時には通常は装着対象の装置の機番を知ることができないため、個別証明書を用意することができないので、個別証明書セットは記憶させない状態で製造することになる。一方、部品Ｙについては、装着対象装置の機種や階位であれば製造時に特定することができるので、その機種や階位に適した共通証明書セットをあらかじめ記憶させた状態で製造することができる。

【００６６】
そして、下位装置２０′において部品Ｘと部品Ｙが破損等してこれらを交換した場合（部品Ｘのみを交換した場合でも同じ）、（ｂ）に示すように、下位装置２０′には、共通証明書セットのみが記憶され、個別証明書セットは記憶されていない状態となる。この状態において、上位装置１０がこの下位装置２０′を共通証明書セットに含まれる下位装置用共通公開鍵証明書を用いた認証処理によって認証すると、個別証明書セットを下位装置２０′に送信し、これを個別証明書セット記憶領域に設定させる。そしてこの後は、この個別証明書セットに含まれる下位装置用個別公開鍵証明書を用いて認証可能な状態となる。

【００６７】
しかし、その後（ｃ）に示すように下位装置２０′から部品Ｘを取り外して部品Ｘと同様な記憶領域を有する偽部品Ｘ′を装着した場合、（ｂ）の場合と同様に下位装置２０′に共通証明書セットのみが記憶された状態となるため、上位装置１０は再度下位装置２０′に個別証明書セットを送信して記憶させてしまう。そして、証明書の記憶領域を設ける部品自体はメモリカード等の汎用性の高い部品とすることも多いため、正規の部品Ｘと同様な記憶領域を設けることのできる偽部品Ｘ′を入手することは容易である場合が多い。従って、偽部品への交換を繰り返すことにより、ユーザは正規の個別証明書セットを記憶させた偽部品Ｘ′を大量に取得し、場合によっては成りすまし等に悪用することも可能になってしまうという問題があるのである。なお、部品Ｙさえ正規のものを使用すれば、正規の部品Ｘを一切使用しなくても上記と同様なことが可能になってしまう。

【００６８】
次に、この実施形態の構成及びその効果について、図１０を用いて説明する。図１０は、下位装置２０における、証明書の記憶領域を設ける交換部品の構成及びその効果について説明するための図である。
この実施形態の下位装置２０においては、上記の問題を解決するため、図９（ａ）に示した比較例の構成とは異なり、図１０（ａ）に示すように、個別証明書セットを記憶する記憶領域と、共通証明書セットを記憶する記憶領域とを両方とも、交換可能な最小単位の交換部品上に設けている。しかし、このような構成を採る場合でも、証明書の特性は変わらないので、この部品Ａを、共通証明書セットのみ予め記憶させ、個別証明書セットは記憶させない状態で製造することになる点は、図９（ａ）の場合と同様である。

【００６９】
ここで、下位装置２０において部品Ａが破損等してこれらを交換した場合、図１０（ｂ）に示すように、下位装置２０には、共通証明書セットのみが記憶され、個別証明書セットは記憶されていない状態となる。そして、図９（ｂ）の場合と同様に、上位装置１０がこの下位装置２０を下位装置用共通公開鍵証明書を用いた認証処理によって認証すると、個別証明書セットを下位装置２０に送信して設定させ、下位装置用個別公開鍵証明書を用いて認証可能な状態とする。

【００７０】
しかし、その後図１０（ｃ）に示すように下位装置から部品Ａを取り外して部品Ａと同様な記憶領域を有する偽部品Ａ′を装着した場合でも、偽部品Ａ′は正しい共通証明書セットを記憶していない。正当なベンダー以外は正しい共通証明書セットを知らないので、正しい共通証明書セットを記憶した偽部品Ａ′を製造することができないためである。従って、図９（ｃ）の場合とは異なり、下位装置２０は上位装置１０に認証を受けることができないので、上位装置１０が下位装置に個別証明書セットを送信して記憶させてしまうこともない。従って、部品Ａをハードウェアとしては汎用性の高い部品で構成したとしても、個別証明書セットを偽部品Ａ′に不正に設定されてしまうことを防止できる。
部品Ａを取り外して別の正規の部品Ａに交換した場合には、新たな個別証明書セットがそこに記憶されることになるが、正規の部品Ａであれば、ベンダー側が流通をコントロールすることが可能であるので、ユーザに必要以上の数の部品Ａを供給しないようにすればよい。
【００７１】
この通信システムにおいては、以上のような構成を採ることにより、個別証明書を不正に取得されることを防止し、成りすまし等の危険を低減して通信の高い安全性を維持することができる。
なお、ここでいう交換可能な最小単位の交換部品とは、ユーザの作業やサービスマンによる出張メンテナンス等の作業によって交換可能な部品のうち、交換する場合にはその全部を交換する必要がある部品を指すものとする。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。しかし、例えば、ＣＰＵボード上に複数のメモリチップが搭載されており、工場等で特殊な設備を使用すればこれらを個別に交換可能であったとしても、ユーザの作業やサービスマンによる出張メンテナンス等の作業では通常交換できない場合には、それは交換可能とは言わないものとする。
【００７２】
次に、このような証明書セットの記憶領域を設けた部品Ａ及びその部品Ａを装着した下位装置２０の製造工程について説明する。
まず、これらの製造工程の概略を図１１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。
【００７３】
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用の共通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、共通証明書セットは漏洩した場合の影響が個別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している。またこの時、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に記憶させるものも同時に書き込むようにするとよい。
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、共通証明書セットは、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。
【００７４】
一方、部品Ａを下位装置２０の製造に使用する場合には、共通証明書セットを書き込んだ部品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。そして、下位装置２０の組み立てが完了した後、その機能検査を行い、合格した装置に機番を付与する。その後、その機番を装置の識別情報として個別公開鍵証明書に含む個

別証明書セットを、証明書書き込み装置１６０によって下位装置２０に記憶させ、また装置の機番情報や初期設定値もこの工程で記憶させる。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、記憶させる共通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。

【００７５】

また、図１２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共通証明書セットのみを記憶させ、個別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、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、証明書書き込み装置１６０によって個別証明書セットが書き込まれる。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個別証明書セットを取得して書き込むことになる。この個別証明書セットは、個別証明書を管理するＣＡである証明書管理装置５０が発行するものである。

【００７６】

なおこのとき、証明書書き込み装置１６０と下位装置２０とを接続した上で、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に記憶している共通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個別証明書セットを送信して部品Ａの個別証明書セット記憶領域に書き込ませるようにしている。

【００７７】

ここで、個別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１３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１３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共通公開鍵証明書を、下位装置用共通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２０のステップＳ２１及びＳ２２の処理に相当する。

【００７８】

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、下位装置認証用共通ルート鍵証明書を使用し、この処理は図２０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２０のステップＳ２５及びＳ２６の処理に相当する。

【００７９】

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、共通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。

【００８０】

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の個別証明書セット記憶領域に記憶させて図６（ａ）に示した個別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が個別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が個別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個別証明書セットを送信してしまうような事態を防止できる。

【００８１】

また、証明書書き込み装置１６０側にも共通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共通証明書セットは、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１８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個別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。

さらに、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とが共通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に個別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。

【００８２】

一方で、図１２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によって個別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個別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。

【００８３】

なおこのとき、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に記憶している共通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は正当な装置であると認証した場合に個別証明書セットを送信して部品Ａの個別証明書セット記憶領域に設定させるようにしている。この場合に下位装置２０側で行う処理は、図１３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。

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。

【００８４】

以上の説明から明らかなように、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全く同じ手順で個別公開鍵証明書を記憶させることができる。

図６及び図７を用いて説明した通り、この通信システムを構成する下位装置２０には、その機番情報を装置の識別情報として付された個別公開鍵証明書を記憶させるようにして

いる。一方で、機番は、装置の組み立てが完了し、機能の検査に合格した装置に付すようにしたいという要求がある。なぜなら、検査前に機番を付してしまうと、検査に不合格となった装置の機番が欠番になってしまい、このような欠番があるとその後の製品管理に不都合があるためにである。

【００８５】

従って、この要求を満たしつつ、機番情報を装置の識別情報として付された公開鍵証明書を装置の製造工程で記憶させるとすると、必然的に組み立てが全て完了した状態で行うことになる。そして、このような状態においては、共通証明書セットの場合のように特殊なインタフェース（専用の冶具）を用いて証明書を記憶させるよりも、下位装置２０が備え、かつ通常使用するインタフェースを介して記憶させる方が好ましい。デザインや機能上の制約から、特殊なインタフェースの接続口は、作業しやすい位置や構成では設けにくいためである。

【００８６】

ここで説明した下位装置２０は、ネットワークを介して個別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、装置に備えている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、個別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、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、個別証明書セットを安全に記憶させることができる。

【００８７】

なお、個別証明書と共通証明書とでは用途も機能も異なるため、図１２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、共通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、共通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、各装置について個別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。

【００８８】

一方、個別証明書は必要に応じて更新できるため、個別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、下位装置用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、個別証明書と共通証明書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。

【００８９】

次に、上述した製品組み立て工程において個別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１４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、個別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。

【００９０】

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、個別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個別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。
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証明書を通信端末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個別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。
【００９１】
次に、図１５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。
【００９２】
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、機能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１６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。
【００９３】
そして、個別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証明書を通信端末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に設けた個別証明書セット記憶領域に設定させる。
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た個別公開鍵証明書を簡単な作業で記憶させることができる。
【００９４】
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１８あるいは図２０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。
【００９５】
また、上述した実施形態では、装置の識別情報が付された個別証明書と、装置の識別情報が付されていない共通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。

【００９６】

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。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高い証明書を記憶する記憶領域とセキュリティ強度が低い証明書を記憶する記憶領域とを、交換可能な最小単位の交換部品に設けることにより、セキュリティ強度が高い証明書を不正に取得されることを防止し、成りすまし等の危険を低減して通信の高い安全性を維持することができる。

【００９７】

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、これと一体として設けることを妨げるものではない。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。

【００９８】

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。

【００９９】

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ようにしてもよい。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の更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。

【０１００】

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。

【０１０１】

上述した実施形態は、このような遠隔管理システム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個別公開鍵証明書を用いた認証を容易に運用できるようにすることによる効果は大きい。

【０１０２】

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】

【０１０３】

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、通信方法あるいはプログラムを用いれば、通信手段によって通信相手と通信可能な通信装置あるいはこのような通信装置を備える通信システムにおいて、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、この発明を、このような通信装置あるいは通信システムに適用することにより、より安全性の高い装置あるいはシステムを提供することができる。

【図面の簡単な説明】

【０１０４】

【図１】この発明の通信システムの実施形態の構成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】図６に示した下位装置用個別公開鍵証明書に含まれる情報の例を示す図である。

【図８】図１に示した上位装置及び下位装置が個別公開鍵証明書と共通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９】図１等に示した実施形態の比較例における、証明書の記憶領域を設ける交換部品の構成及びその問題点について説明するための図である。

【図１０】図１に示した下位装置における、証明書の記憶領域を設ける交換部品の構成及びその効果について説明するための図である。

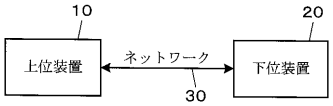
【０１０５】

【図１１】図１０に示した部品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。

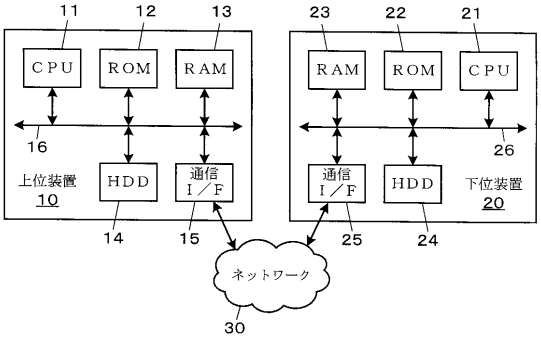
【図１２】その部品Ａに各証明書セットを記憶させる工程について説明するための図である。

【図１３】図１２に示した工程において下位装置に個別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１４】図１１及び図１２に示した製品組み立て工程において個別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１５】生産工場における、図１４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１６】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１７】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１８】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１９】図１８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２０】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１８と対応する図である。
【符号の説明】
【０１０６】
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、２０，２０′…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

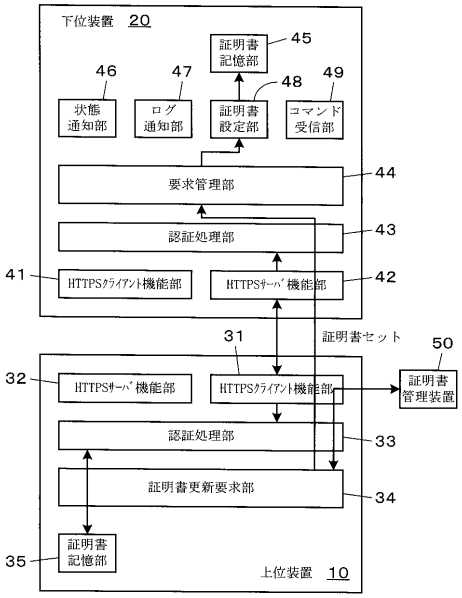
【図１】




【図２】



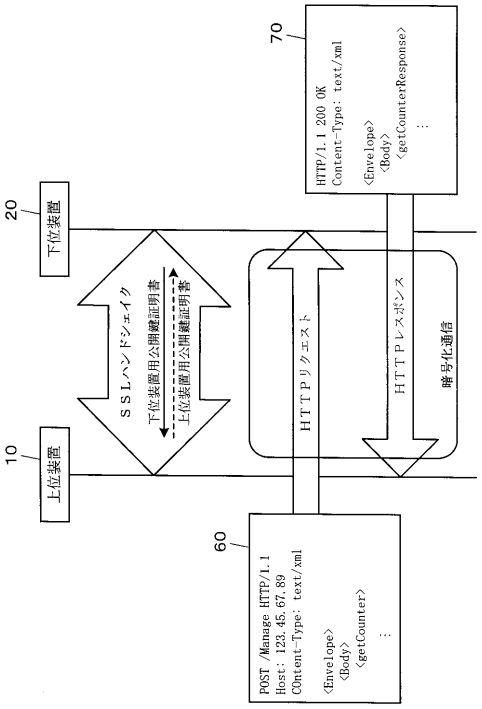

【図３】




【図４】

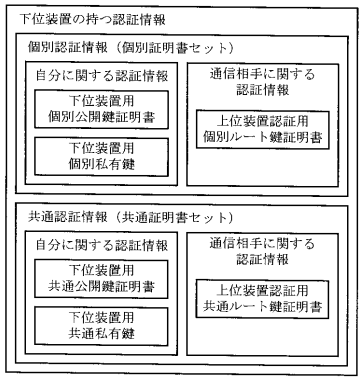
| | 状態取得 | ログ取得 | 証明書設定 | コマンド実行 |
|---|---|---|---|---|
| 共通証明書 | × | × | ○ | × |
| 個別証明書 | ○ | ○ | ○ | ○ |

【図５】

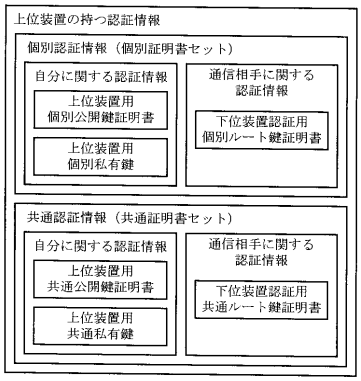



【図６】

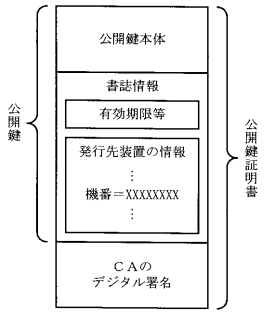
（ａ）



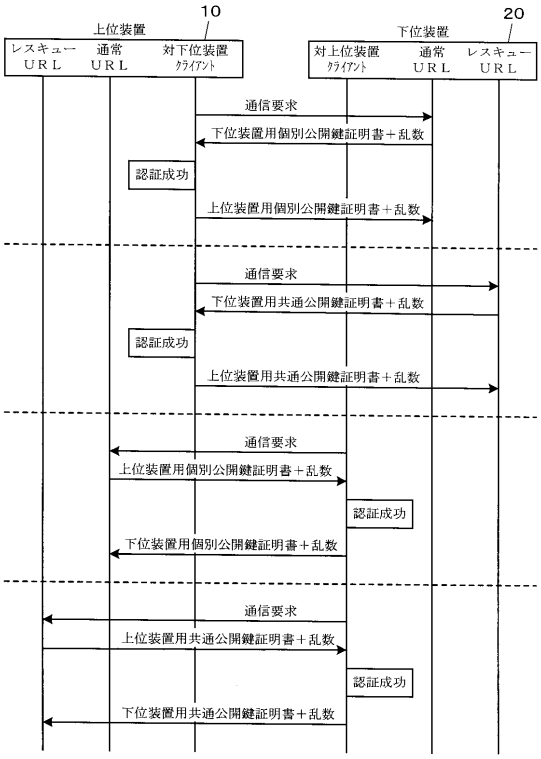

（ｂ）



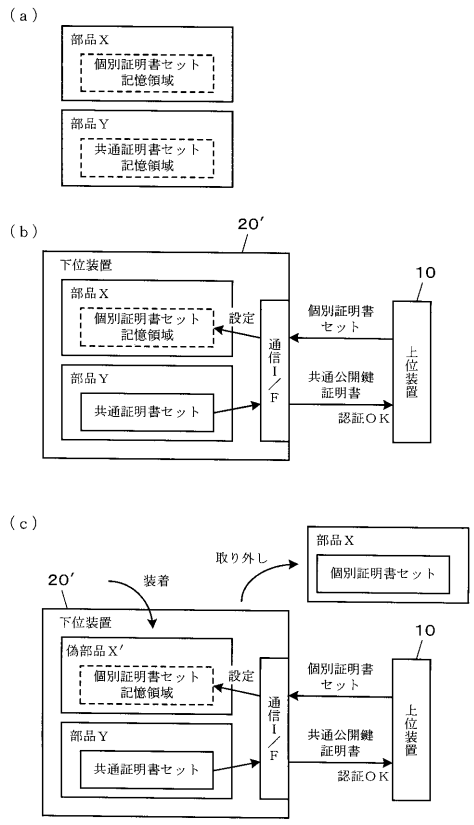
【図７】


公開鍵本体
書誌情報
有効期限等
発行先装置の情報
機番＝XXXXXXXX
ＣＡの
デジタル署名
公開鍵
公開鍵証明書

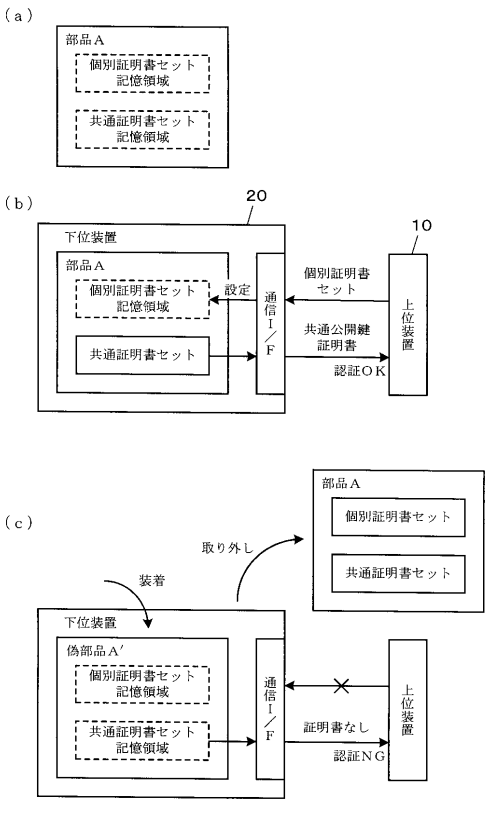
【図８】


上位装置
10
レスキュー URL
通常 URL
対下位装置 ｸﾗｲｱﾝﾄ
下位装置
20
対上位装置 ｸﾗｲｱﾝﾄ
通常 URL
レスキュー URL
通信要求
下位装置用個別公開鍵証明書＋乱数
認証成功
上位装置用個別公開鍵証明書＋乱数
通信要求
下位装置用共通公開鍵証明書＋乱数
認証成功
上位装置用共通公開鍵証明書＋乱数
通信要求
上位装置用個別公開鍵証明書＋乱数
認証成功
下位装置用個別公開鍵証明書＋乱数
通信要求
上位装置用共通公開鍵証明書＋乱数
認証成功
下位装置用共通公開鍵証明書＋乱数

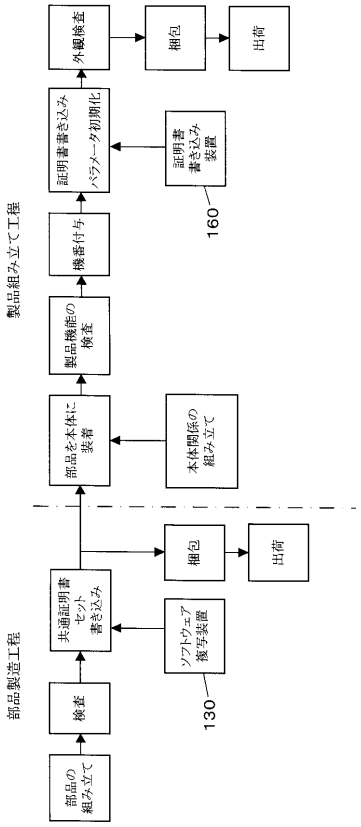
【図９】


(a)
部品X
個別証明書セット
記憶領域
部品Y
共通証明書セット
記憶領域
(b)
20′
下位装置
部品X
個別証明書セット
記憶領域
設定
部品Y
共通証明書セット
通信Ｉ／Ｆ
個別証明書セット
共通公開鍵証明書
認証ＯＫ
10
上位装置
(c)
部品X
個別証明書セット
取り外し
装着
20′
下位装置
偽部品X′
個別証明書セット
記憶領域
設定
部品Y
共通証明書セット
通信Ｉ／Ｆ
個別証明書セット
共通公開鍵証明書
認証ＯＫ
10
上位装置

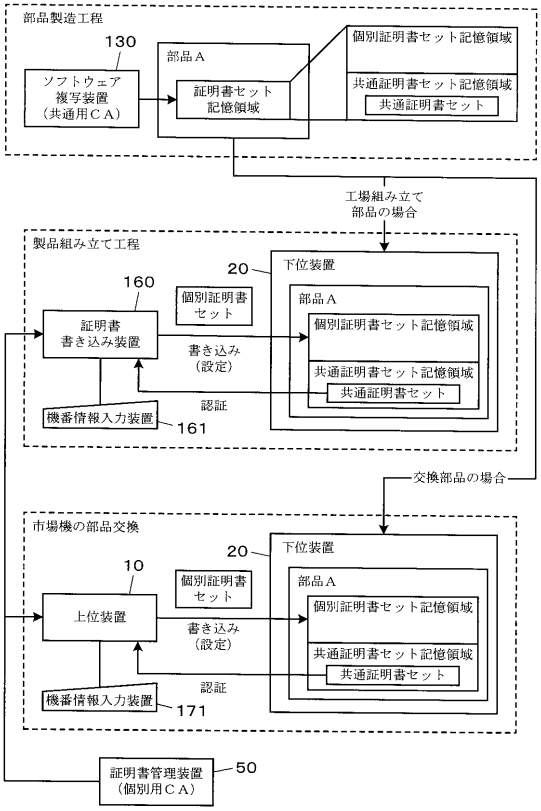
【図１０】


(a)
部品A
個別証明書セット
記憶領域
共通証明書セット
記憶領域
(b)
20
下位装置
部品A
個別証明書セット
記憶領域
設定
共通証明書セット
通信Ｉ／Ｆ
個別証明書セット
共通公開鍵証明書
認証ＯＫ
10
上位装置
(c)
部品A
個別証明書セット
共通証明書セット
取り外し
装着
下位装置
偽部品A′
個別証明書セット
記憶領域
共通証明書セット
記憶領域
通信Ｉ／Ｆ
証明書なし
認証ＮＧ
上位装置

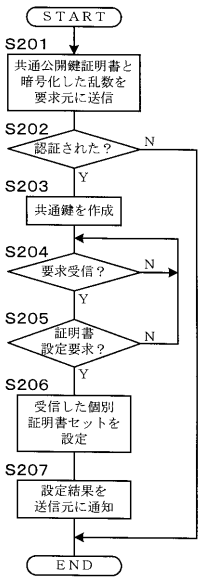
【図１１】



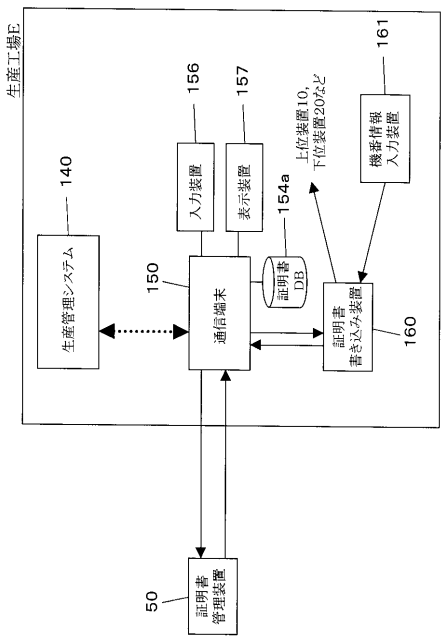

【図１２】



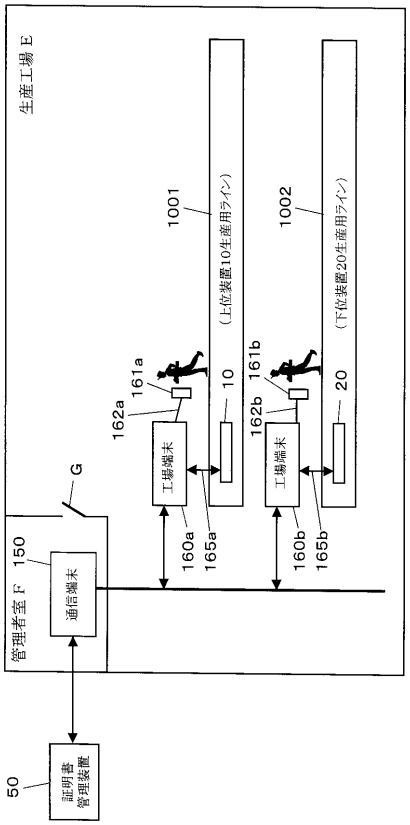

【図１３】



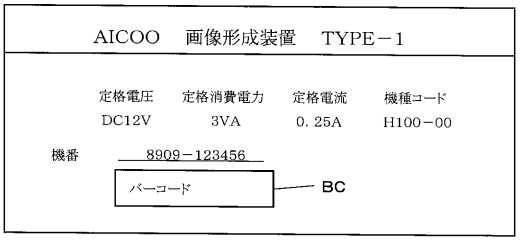

【図１４】



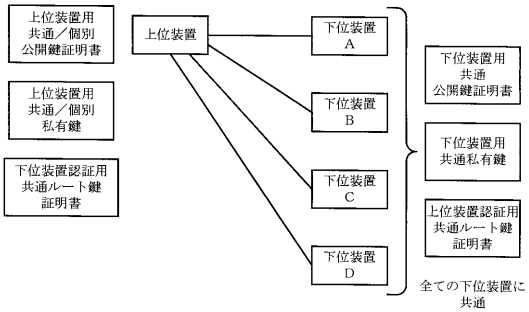
【図１５】



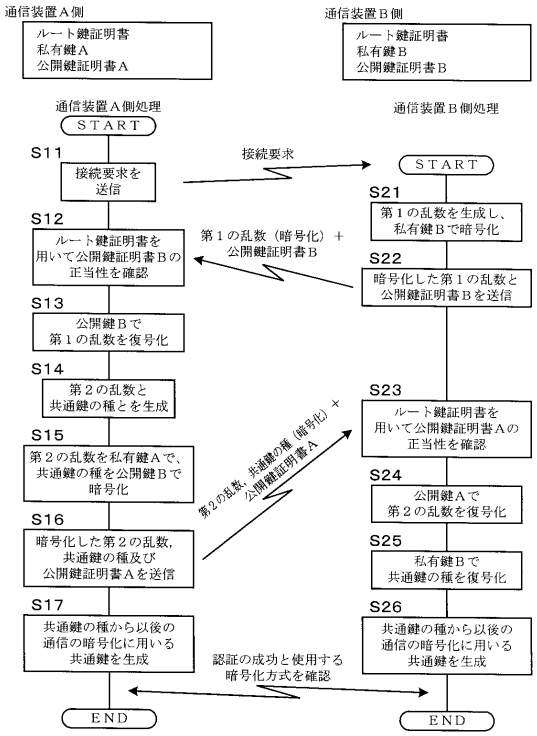

【図１６】



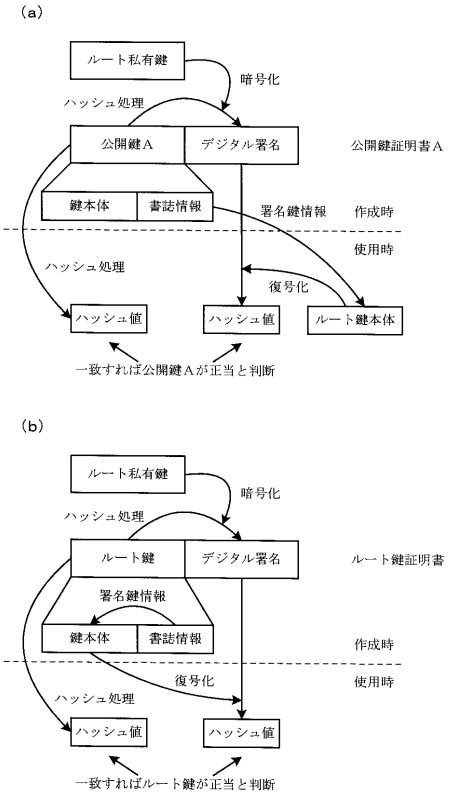

【図１７】



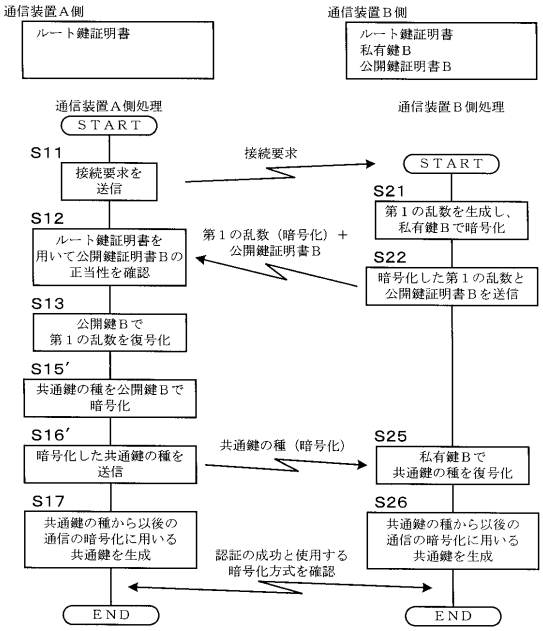

【図１８】




【図１９】



【図２０】


通信装置Ａ側
ルート鍵証明書
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
ＳＴＡＲＴ
Ｓ11
接続要求を送信
接続要求
ＳＴＡＲＴ
Ｓ21
第１の乱数を生成し、私有鍵Ｂで暗号化
Ｓ12
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
Ｓ22
暗号化した第１の乱数と公開鍵証明書Ｂを送信
Ｓ13
公開鍵Ｂで第１の乱数を復号化
Ｓ15′
共通鍵の種を公開鍵Ｂで暗号化
Ｓ16′
暗号化した共通鍵の種を送信
共通鍵の種（暗号化）
Ｓ25
私有鍵Ｂで共通鍵の種を復号化
Ｓ17
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
Ｓ26
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

フロントページの続き

(56)参考文献 特開平０９－２００１９４（ＪＰ，Ａ）
特開２００１－０９４５５３（ＪＰ，Ａ）
特表２００３－５０３９６３（ＪＰ，Ａ）
特開２００３－００６１６１（ＪＰ，Ａ）
特開２００２－３６８７３３（ＪＰ，Ａ）
特開２００１－２６６０７８（ＪＰ，Ａ）
特開平１１－１７４９５６（ＪＰ，Ａ）
米国特許第０５７８１７２３（ＵＳ，Ａ）
Larry J. Hughes, Jr. 著／長原宏治 監訳, “インターネットセキュリティ”, 株式会社インプレス, １９９７年 2月２１日, 初版, ｐ．８６－１０８, システム管理者のためのリスクマネージメント
Paul Ashley, Heather Hinton, Mark Vandenwauver, “Wired versus Wireless Security: The Internet, WAP and iMode for E-Commerce”, Proceedings of 17th Annual Computer Security Applications Conference (ACSAC 2001), ２００１年, pp. 296-306

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／１０
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２