(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4789432号
(P4789432)
(45)発行日　平成23年10月12日(2011.10.12)　(24)登録日　平成23年7月29日(2011.7.29)

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

請求項の数 11　(全 14 頁)

(21)出願番号　特願2004-191542(P2004-191542)
(22)出願日　平成16年6月29日(2004.6.29)
(65)公開番号　特開2006-14182(P2006-14182A)
(43)公開日　平成18年1月12日(2006.1.12)
審査請求日　平成18年12月6日(2006.12.6)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090273
弁理士　國分　孝悦
(72)発明者　深澤　伸朗
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　金沢　史明

最終頁に続く

(54)【発明の名称】データ処理装置、データ処理装置の制御方法、コンピュータプログラム及び記憶媒体

(57)【特許請求の範囲】
【請求項１】
外部装置と通信可能なデータ処理装置であって、
公開鍵の初期値及び秘密鍵の初期値を格納する格納手段と、
前記格納手段に格納された公開鍵を前記外部装置に送信する送信手段と、
前記送信手段によって送信された公開鍵によって暗号化された鍵を受信する受信手段と、
前記受信手段によって受信された鍵を前記格納手段に格納された秘密鍵によって復号する復号手段と、
前記復号手段によって復号された鍵を使って、前記外部装置と、前記外部装置から新たな公開鍵及び新たな秘密鍵を取得するための暗号化通信を行う通信手段と、
前記通信手段によって行われる暗号化通信の中で取得された前記新たな公開鍵及び前記新たな秘密鍵を前記公開鍵の初期値及び前記秘密鍵の初期値に代えて使用すべく前記データ処理装置にインストールするインストール手段とを有することを特徴とするデータ処理装置。
【請求項２】
前記外部装置からログイン要求を受付ける受付手段と、
前記受付手段によって受け付けたログイン要求に基づくログインが許可されている場合に、前記インストール手段による前記新たな公開鍵及び前記新たな秘密鍵のインストールを許可する許可手段とをさらに有することを特徴とする請求項１に記載のデータ処理装置

。
【請求項３】
ユーザからの指示により前記データ処理装置内で前記公開鍵の初期値及び秘密鍵の初期値を作成する作成手段を有し、
前記格納手段は、前記作成手段により作成された公開鍵の初期値及び秘密鍵の初期値を格納することを特徴とする請求項１または２に記載のデータ処理装置。
【請求項４】
前記インストール手段によってインストールされた前記新たな公開鍵の情報を表示装置に表示する表示手段をさらに有することを特徴とする請求項１～３の何れか１項に記載のデータ処理装置。
【請求項５】
前記新たな公開鍵の情報は、前記新たな公開鍵がインストールされた日時を含むことを特徴とする請求項４に記載のデータ処理装置。
【請求項６】
前記新たな公開鍵の情報は、前記新たな公開鍵の値及び公開鍵証明書の内容を含むことを特徴とする請求項４または５に記載のデータ処理装置。
【請求項７】
前記表示手段によって表示された前記新たな公開鍵の情報を印刷するよう指示する印刷指示手段をさらに有することを特徴とする請求項４～６の何れか１項に記載のデータ処理装置。
【請求項８】
前記表示手段によって表示された前記新たな公開鍵の情報をメールで送信するよう指示する送信指示手段をさらに有することを特徴とする請求項４～７の何れか１項に記載のデータ処理装置。
【請求項９】
外部装置と通信可能なデータ処理装置の制御方法であって、
公開鍵の初期値及び秘密鍵の初期値を格納手段に格納する格納工程と、
前記格納手段に格納された公開鍵によって暗号化された鍵を受信する受信工程と、
前記受信工程で受信された鍵を前記格納手段に格納された秘密鍵によって復号する復号工程と、
前記復号工程で復号された鍵を使って、前記外部装置と、前記外部装置から新たな公開鍵及び新たな秘密鍵を取得するための暗号化通信を行う通信工程と、
前記通信工程で行われる暗号化通信の中で取得された前記新たな公開鍵及び前記新たな秘密鍵を前記公開鍵の初期値及び前記秘密鍵の初期値に代えて使用すべく前記データ処理装置にインストールするインストール工程とを有することを特徴とするデータ処理装置の制御方法。
【請求項１０】
外部装置と通信可能なデータ処理装置の制御方法をコンピュータに実行させるコンピュータプログラムであって、
公開鍵の初期値及び秘密鍵の初期値を格納手段に格納する格納工程と、
前記格納手段に格納された公開鍵によって暗号化された鍵を受信する受信工程と、
前記受信工程で受信された鍵を前記格納手段に格納された秘密鍵によって復号する復号工程と、
前記復号工程で復号された鍵を使って、前記外部装置と、前記外部装置から新たな公開鍵及び新たな秘密鍵を取得するための暗号化通信を行う通信工程と、
前記通信工程で行われる暗号化通信の中で取得された前記新たな公開鍵及び前記新たな秘密鍵を前記公開鍵の初期値及び前記秘密鍵の初期値に代えて使用すべく前記データ処理装置にインストールするインストール工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。
【請求項１１】

請求項１０に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ読取可能な記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はデータ処理装置、データ処理装置の制御方法、コンピュータプログラム及び記憶媒体に関する。

【背景技術】

【０００２】

最近は、ネットワークを介して端末と接続されたデータ処理装置においては、ネットワークセキュリティ機能を求められるようになってきている。このような要求に応えるために、例えば、特許文献１においては、プリンタは公開鍵証明書とこれに対応する秘密鍵とを保有し、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行うようにしている。

【０００３】

【特許文献１】特開２００２－２５９１０８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

前記公開鍵証明書や公開鍵を使用してデバイス認証を行う場合、外部で暗号用公開鍵・復号用秘密鍵ペアを作成し、信頼できる機関からその証明書を発行してもらい、それらを前記データ処理装置へインストールしなければならない場合があるので、面倒であり、かつ多くの時間がかかるセキュリティの設定をユーザに強要する問題点があった。

【０００５】

前述のインストールを行う際に、ＦＤやＣＤなどの入力装置を持たないデータ処理装置は、前記秘密鍵・公開鍵のペアや前記証明書はネットワーク上の端末からネットワークを介してインストールを行うようにする必要がある。

【０００６】

その際、現在では端末からデータ処理装置へ暗号通信により安全にインストールすることを行うため、秘密鍵・公開鍵のインストールを行うときの暗号通信で使用するための一時的に作成される共通鍵（セッション鍵）を端末とデータ処理装置との間で交換する必要がある。

【０００７】

しかし、工場出荷状態のデータ処理装置などにおいては、自身の公開鍵・秘密鍵ペアを持っていない状態も考えられ、前記セッション鍵の交換を暗号通信で行えない場合がある。そのような場合には、PKCS＃12などで秘密鍵のみをパスワードで暗号化し、安全に秘密鍵を運搬、転送する手段を使っていた。しかし、この場合はデバイスのローカルＵＩに直接パスワードを入力しなければならず、遠隔地のデバイスに対して安全にインストールする手段としては適切とは言えなかった。

【０００８】

また、前記公開鍵・秘密鍵ペアを保持していないデータ処理装置と端末間で暗号通信を行うために、データ処理装置で公開鍵・秘密鍵ペアを生成させた後に暗号通信によりインストールを行う手段を使用する場合もあったが、セキュリティに関心の薄い環境、またはかならずしも完璧なセキュリティでなくても良い環境もあり、デバイスを操作する全てのユーザが必ずしも、前記公開鍵・秘密鍵の生成を指示するとは限らない。

【０００９】

一方、セキュリティに関心の高いユーザも多く存在するので、高セキュリティを望むユーザに対しては、その要求も満足させる必要があった。

【００１０】

本発明は上述の問題点にかんがみ、外部装置からデータ処理装置に暗号化通信を行って

、新たな公開鍵と新たな秘密鍵をインストールすることを目的とする。
【課題を解決するための手段】
【００１１】
本発明のデータ処理装置は、外部装置と通信可能なデータ処理装置であって、公開鍵の初期値及び秘密鍵の初期値を格納する格納手段と、前記格納手段に格納された公開鍵を前記外部装置に送信する送信手段と、前記送信手段によって送信された公開鍵によって暗号化された鍵を受信する受信手段と、前記受信手段によって受信された鍵を前記格納手段に格納された秘密鍵によって復号する復号手段と、前記復号手段によって復号された鍵を使って、前記外部装置と、前記外部装置から新たな公開鍵及び新たな秘密鍵を取得するための暗号化通信を行う通信手段と、前記通信手段によって行われる暗号化通信の中で取得された前記新たな公開鍵及び前記新たな秘密鍵を前記公開鍵の初期値及び前記秘密鍵の初期値に代えて使用すべく前記データ処理装置にインストールするインストール手段とを有することを特徴としている。
【発明の効果】
【００１５】
本発明によれば、外部装置からデータ処理装置に暗号化通信を行って、新たな公開鍵と新たな秘密鍵とをインストールすることができる。
【発明を実施するための最良の形態】
【００１６】
（第１の実施の形態）
本発明は、以下の実施の形態に詳述するように、ネットワーク上に端末と画像形成装置が接続されたネットワーク印刷システムにおいて、端末から画像形成装置に対して公開鍵・秘密鍵のペアや公開鍵証明書を、高度なセキュリティを求めないユーザのために簡易にインストールできる方法と、漏洩無く及び改ざん無く安全にネットワークを介してインストールする方法の両方を実現できるようにしたものである。
【００１７】
図１は、本実施の形態の印刷システムが動作可能な構成を示す図である。
図１において、１１０、１１１は端末（ＰＣ）であり、１２０、１２１は複合機能画像装置（以下MFP（Multi ＦＵＮＣtion Printer）と呼ぶ）、１３０、１３１は単機能画像形成装置（以下SFP（Single ＦＵＮＣtion Printer）であり、それぞれＬＡＮ１００に接続されている。以下の説明において、１２０、１２１、１３０、１３１を総称して画像形成装置と呼ぶ。
【００１８】
１４０はファイアウォールであり、ＬＡＮ１００を外部のインタネット１５０に接続する。またＬＡＮ１００はファイアウォール１４０、インタネット１５０を介して更に別のネットワーク１６０に接続される。
【００１９】
ユーザは、端末１１０にて印刷ジョブを作成し、例えばMFP１２０へ印刷ジョブを転送する。MFP１２０は現在の処理状況を保存しながら復帰するのが不可能なエラー（例えば復帰するには電源OFF／ONが必要なエラー、サービスマンの操作が必要なエラー）が発生していなければ印刷ジョブを受付け、データを受信し、印刷処理を実行する。
【００２０】
紙ジャムや紙切れなどの定常状態へ復帰する際に現状の処理状況の保存が可能な状態では、通常どおりデータの受信動作を行い、定常状態へ復帰後に印刷処理を実行する。また前記復帰不可能なエラーが発生していたとしても、要求が印刷ジョブ以外の処理であれば通常と同様に受信し、処理を行う。
【００２１】
図２は、一般的なパーソナルコンピュータの内部構成を示した図であり、図１における端末１１０、端末１１１の内部構成はこのようになっている。ＰＣ２００は、ROM２０２もしくはハードディスク（ＨＤ）２１１に記憶された、あるいはフロッピー（登録商標）

ディスクドライブ（ＦＤ）２１２より供給される各種ソフトウェアを実行するＣＰＵ２０１を備え、システムバス２０４に接続される各機器を総括的に制御する。

【００２２】

２０３はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。２０５はキーボードコントローラ（ＫＢＣ）で、キーボード（KB）２０９や不図示のポインティングデバイス等からの指示入力を制御する。２０６はＣＲＴコントローラ（ＣＲＴＣ）で、ＣＲＴディスプレイ（ＣＲＴ）２１０の表示を制御する。

【００２３】

２０７はディスクコントローラ（ＤＫＣ）で、ブートプログラム、種々のアプリケーション、編集ファイル、ユーザファイル等を記憶するハードディスク（ＨＤ）２１１及びフロッピー（登録商標）ディスクコントローラ（ＦＤ）２１２とのアクセスを制御する。２０８はネットワークインタフェースカード（ＮＩＣ）で、ＬＡＮ２２０を介して、ネットワークプリンタ、他のネットワーク機器あるいは他のＰＣと双方向にデータをやりとりする。なお、本実施の形態においては、ＬＡＮ２２０は図１におけるＬＡＮ１００と同じものである。

【００２４】

図３において、３００は、本実施の形態のプログラムが稼動するMFPまたはSFPの内部構成の一例であり、図１における１２０、１２１、１３０、１３１と同等である。デバイス３００は、ＲＯＭ３０２もしくはハードディスク（ＨＤ）３１０に記憶された、あるいはフロッピー（登録商標）ディスクドライブ（ＦＤ）３１１より供給される各種プログラムを実行するＣＰＵ３０１を備え、システムバス３０４に接続される各機器を総括的に制御する。

【００２５】

３０３はＲＡＭで、ＣＰＵ３０１の主メモリ、ワークエリア等として機能する。３０５はユーザインタフェースコントローラ（ＵＩＣ）で、ユーザインタフェース（ＵＩ）３０９への表示、３０９からの指示入力を制御する。

【００２６】

ファンクションコントローラ（ＦＵＮＣＣ）３０６は、各デバイス特有の機能であるファンクション（ＦＵＮＣ）３１０を実現／制御する。モノクロプリンタであればモノクロプリントエンジンコントローラとモノクロプリントエンジン、カラープリンタであればカラープリントエンジンコントローラとカラープリントエンジン、MFPであればデバイス３００は各機能のファンクションコントローラ（ＦＵＮＣＣ）３０６とファンクション（ＦＵＮＣ）３１０をそれぞれ持つ。

【００２７】

３０７はディスクコントローラ（ＤＫＣ）で、ブートプログラム、本実施の形態の動作を行うプログラム、種々のアプリケーション、データファイルを記憶するハードディスク（ＨＤ）３１１及びフロッピー（登録商標）ディスクコントローラ（ＦＤ）３１２とのアクセスを制御する。３０８はネットワークインタフェースカード（ＮＩＣ）で、ＬＡＮ３２０を介して、ネットワークプリンタ、他のネットワーク機器あるいは他のＰＣと双方向にデータをやりとりする。なお、本実施の形態においては、ＬＡＮ３２０は図１におけるＬＡＮ１００と同じものである。

【００２８】

図４は、本実施の形態の印刷システムのモデルを示す図である。図４において、４１０は画像形成装置であり、図１における１２０、１２１、１３０、１３１と同等である。４２０はクライアント端末（ＰＣ）であり、図１における１１０、１１１と同等である。画像形成装置４１０とクライアント端末４２０はＬＡＮ４３０を介して接続されている。

【００２９】

４１１はネットワークインタフェース機能であり、画像形成装置４１０をＬＡＮ４３０に接続する。４１２はセキュア通信機能であり、ＬＡＮ４３０を介してクライアント端末４２０とセキュリティを確保したデータ通信を行う機能である。４１３は画像形成装置に

搭載されるアプリケーションである。４１４は鍵管理機能であり、画像形成装置が保持する鍵の管理を行う。鍵管理機能４１４はアプリケーション４１３の一種である。４１５は鍵ペアであり、非対称鍵方式の公開鍵、秘密鍵のペアである。

【００３０】

４２１はネットワークインタフェース機能であり、クライアント端末４２０をＬＡＮ４３０に接続する。４２２はセキュア通信機能であり、ＬＡＮ４３０を介して画像形成装置４１０とセキュリティを確保したデータ通信を行う機能である。４２３はクライアント端末４２０に搭載されるアプリケーションである。

【００３１】

４２４は鍵インストール機能であり、非対称鍵方式の鍵ペアを画像形成装置へインストールするものである。鍵インストール機能４２４は、アプリケーション４２３の一種である。４２５は鍵ペアであり、非対称鍵方式の公開鍵、秘密鍵のペアであり、鍵インストール機能４２４によって画像形成装置４１０へインストールされるものである。なお、本実施の形態においては、ＬＡＮ４３０は図１におけるＬＡＮ１００と同じものである。

【００３２】

図５は、公開鍵及び秘密鍵が既に用意されているという前提において、本実施の形態の画像形成装置と端末との間の、鍵を画像形成装置へインストールする際のシーケンスを示す図である。公開鍵及び秘密鍵がどのようにして用意されるかについては、後に、図６～図８を用いて説明する。図５において、５０１は端末（ＰＣ）であり、図４の４２０と同等である。画像形成装置５０２は図４の４１０と同等である。

【００３３】

端末５０１は鍵をインストールする際、まずメッセージ５１０にて画像形成装置５０２へ暗号通信開始を要求する。画像形成装置５０２は５１０の要求に対して了承するのであれば、メッセージ５２２にて公開鍵５２０、または公開鍵５２０を内包した公開鍵証明書を端末５０１へ送付する。

【００３４】

メッセージ５２２を受信した端末５０１は、鍵インストールの暗号通信で使用する共通鍵方式であるのセッション鍵を処理５１１において生成し、処理５１２にてセッション鍵を公開鍵で暗号化する。その後、メッセージ５１３にて処理５１２にて暗号化したセッション鍵を端末５０１から画像形成装置５０２へ送付する。

【００３５】

画像形成装置５０２では、処理５２３にて受信した暗号化されたセッション鍵を復号化し、端末５０１が処理５１１において生成したセッション鍵を秘密裏に獲得することができる。５１４、５１５は鍵ペアであり、画像形成装置へインストールされる公開鍵、秘密鍵で、図４の４２５と同等のものである。

【００３６】

端末５０１は、セッション鍵を使用して暗号通信を開始し、必要であれば新しい鍵ペア５１４、５１５を暗号メッセージ５１６において画像形成装置５０２へ送付し、画像形成装置５０２は端末５０１から新しい鍵ペア５１４、５１５を秘密裏に及び安全に獲得することができる。

【００３７】

図６は、図５と同じく本実施の形態の画像形成装置と端末との間のシーケンスの一例である。

図６において、６０１は端末（ＰＣ）であり、図４の４２０と同等である。画像形成装置６０２は図４の４１０と同等である。このシーケンスで特徴的であるのは、画像形成装置６０２が工場出荷状態であることであり、既に公開鍵６２０、秘密鍵６２１を工場出荷値として持っていて、画像形成装置が公開鍵６２０、秘密鍵６２１を新たに作成せずともセキュア通信を開始することが可能である点である。

【００３８】

端末６０１は、まず、管理者権限でログインするために、メッセージ６１０を送付する

。画像形成装置６０２は了承するのであれば、メッセージ６２２で「ＯＫ」を返答する。端末６０１はログイン成功後、メッセージ６１１にて暗号通信開始要求を画像形成装置６０２へ送信する。

【００３９】

画像形成装置６０２は、メッセージ６１１の応答として公開鍵６２０か、または公開鍵６２０を内包した公開鍵証明書をメッセージ６２３において送付する。端末６０１はメッセージ６２３を受信後、処理６１２にてセッション鍵を生成し、さらにメッセージ６２３で獲得した前記公開鍵を使用して、処理６１３にて前記セッション鍵を暗号化する。

【００４０】

その後、端末６０１はメッセージ６１４にて暗号化した前記セッション鍵を画像形成装置６０２へ送付する。画像形成装置６０２は処理６２４で前記セッション鍵を復号化し、秘密裏に前記セッション鍵を獲得することができる。

【００４１】

端末６０１は、セッション鍵を送付後、セッション鍵によって暗号通信を開始し、必要であればメッセージ６１７で新しい鍵ペアである６１５、６１６を画像形成装置６０２へ送付する。画像形成装置６０２は、暗号通信上のメッセージとして６１７を受信し、新しい秘密鍵６１５及び新しい公開鍵６１６を秘密裏にかつ安全に獲得することが可能である。

【００４２】

このシーケンスでは処理６１３、処理６２４で使用する公開鍵６２０、秘密鍵６２１のペアが工場出荷値のため、メッセージ６１４にて送付するセッション鍵が他者に漏洩する可能性があるが、ユーザは面倒で時間のかかるセキュリティ設定をせずとも、セキュリティのレベルは低いが暗号通信を行うことができる。

【００４３】

図７は、図５と同じく本実施の形態の画像形成装置とＰＣとの間のシーケンスの一例である。７０１は端末（ＰＣ）であり、図４の４２０と同等である。画像形成装置７０２は図４の４１０と同等である。このシーケンスで特徴的であるのは、画像形成装置が自己生成した公開鍵７２０、秘密鍵７２１のペアを持っている点で、セッション鍵交換において他者に漏洩する可能性が無い点である。画像形成装置は、付随の操作パネルにおいて入力された指示に従って、或いは端末からの指示に従って、公開鍵７２０及び秘密鍵７２１のペアを自己生成することが考えられる。

【００４４】

端末７０１は、まず、管理者権限でログインするために、メッセージ７１０を送付する。画像形成装置７０２は了承するのであれば、メッセージ７２２で「ＯＫ」を返答する。端末７０１は、ログイン成功後、メッセージ７１１にて暗号通信開始要求を画像形成装置７０２へ送信する。

【００４５】

画像形成装置７０２は、メッセージ７１１の応答として公開鍵７２０かまたは公開鍵７２０を内包した公開鍵証明書をメッセージ７２３において送付する。

端末７０１はメッセージ７２３を受信後、処理７１２にてセッション鍵を生成し、さらにメッセージ７２３で獲得した前記公開鍵を使用して、処理７１３にて前記セッション鍵を暗号化する。

【００４６】

その後、端末７０１はメッセージ７１４にて暗号化した前記セッション鍵を画像形成装置７０２へ送付し、処理７２４で画像形成装置７０２は前記セッション鍵を復号化し、秘密裏に前記セッション鍵を獲得することができる。端末７０１はセッション鍵を送付後、セッション鍵によって暗号通信を開始し、必要であればメッセージ７１７で新しい鍵ペアである７１５、７１６を画像形成装置７０２へ送付する。画像形成装置７０２は暗号通信上のメッセージとして７１７を受信し、新しい秘密鍵７１５及び新しい公開鍵７１６を秘密裏にかつ安全に獲得することが可能である。

【００４７】
このシーケンスでは処理７１３、処理７２４で使用する公開鍵７２０、秘密鍵７２１のペアが自己生成のため、メッセージ７１４にて送付するセッション鍵が他者に漏洩する可能性がない。
【００４８】
したがって、暗号通信における漏洩、改ざんについては全く安全であると言える。しかしながら、メッセージ７２３にて送付される公開鍵または公開鍵証明書は自己生成物であり、信頼できるＣＡ局（ HYPERLINK "http://e-words.jp/w/E8AA8DE8A8BCE5B180.html" 認証局）などから証明されていない。したがって、端末７０１に対する画像形成装置７０２のなりすましに関しては、防御されていないと言える。
【００４９】
図８は、図５と同じく本実施の形態の画像形成装置と端末との間のシーケンスの一例である。８０１は端末（ＰＣ）であり、図４の４２０と同等である。画像形成装置８０２は図４の４１０と同等である。このシーケンスで特徴的であるのは、画像形成装置が自己生成した公開鍵８２０、秘密鍵８２１のペアを持っている点で、セッション鍵交換において他者に漏洩する可能性が無い点である。
【００５０】
端末８０１は、まず、管理者権限でログインするために、メッセージ８１０を送付する。画像形成装置８０２は了承するのであれば、メッセージ８２３で「ＯＫ」を返答する。端末８０１はログイン成功後、メッセージ８１１にて暗号通信開始要求を画像形成装置８０２へ送信する。
【００５１】
画像形成装置８０２は、メッセージ８１１の応答として公開鍵８２０かまたは公開鍵８２０を内包した公開鍵証明書をメッセージ８２４において送付する。端末８０１の使用者は処理８１２にてメッセージ８２４の受信で獲得した画像形成装置８０２の前記公開鍵を確認する。
【００５２】
確認する方法は、前記画像形成装置８０２のＵＩ画面に表示された公開鍵値を目視で確認する方法、もしくは離れた場所に前記装置が存在する場合は、装置管理者にＵＩで公開鍵を確認してもらい、郵便、メール、電話、新聞や雑誌に公表、などにより端末８０１の使用者に通知する。
【００５３】
その後、処理８１３にてセッション鍵を生成し、さらにメッセージ８２３で獲得した前記公開鍵を使用して、処理８１４にて前記セッション鍵を暗号化する。その後、端末８０１はメッセージ８１５にて暗号化した前記セッション鍵を画像形成装置８０２へ送付する。
【００５４】
画像形成装置８０２は、前記セッション鍵を処理８２５で復号化し、秘密裏に前記セッション鍵を獲得することができる。端末８０１はセッション鍵を送付後、セッション鍵によって暗号通信を開始し、必要であればメッセージ８１８で新しい鍵ペアである８１６、８１７を画像形成装置８０２へ送付する。
【００５５】
画像形成装置８０２は、暗号通信上のメッセージとして８１８を受信し、新しい秘密鍵８１６及び新しい公開鍵８１７を秘密裏にかつ安全に獲得することが可能である。
【００５６】
このシーケンスでは処理８１４、処理８２５で使用する公開鍵８２０、秘密鍵８２１のペアが自己生成のため、メッセージ８１５にて送付するセッション鍵が他者に漏洩する可能性がない。
【００５７】
したがって、暗号通信における漏洩、改ざんについては全く安全であると言える。また

、メッセージ８２４にて送付される公開鍵または公開鍵証明書は自己生成物ではあるが、処理８１２にて公開鍵が装置８０２のものであることを確認するため、画像形成装置８０２のなりすましに関しても全く安全であると言える。

【００５８】

図９は、図８において装置管理者が公開鍵情報を確認するためのＵＩ画面の一例を示す図である。ペイン９１０では装置８０２が保持している鍵をリスト表示するものである。列９１１は鍵名、列９１２は鍵が使用するアルゴリズムを表す。

【００５９】

行９１３は鍵名が「銀次の鍵」であり、使用するアルゴリズムがRSAであることを示している。行９１４は鍵名が「文太郎の鍵」であり、使用するアルゴリズムがRSAであることを示している。ボタン９１５は９１０にて選択した鍵の詳細情報を表示を指示するものである。ボタン９１６は鍵情報の画面を閉じる動作を指示するものである。

【００６０】

図９の例では、行９１３を選択して鍵情報の詳細をペイン９２０にて表示している。９２１は選択された鍵の詳細情報を表示する場所である。図９の例では、鍵名が銀次の鍵、インストールされた日が2003/12/18、アルゴリズムがRSA、鍵長が1024bitであることを示し、加えて公開鍵値を表示している。

【００６１】

ボタン９３２では、鍵情報の詳細を印刷することを支持するものであり、ボタン９２３は表示場所９２１にて表示している鍵情報の詳細をメールすることを指示するものである。ボタン９２４はペイン９２０を閉じることを指示するものである。図９の表示例は、あくまで例であり、例えば公開鍵証明書の情報をペイン９２０に加えても良い。

【００６２】

図１０は、記憶媒体の一例であるＣＤ－ＲＯＭのメモリマップを示す図である。９９９９はディレクトリ情報を記憶してある領域で、以降のインストールプログラムを記憶してある領域９９９８及び本実施の形態を実現するプログラムを記憶してある領域９９９７の位置を示している。９９９８は、本実施の形態を実現するプログラムをインストールするためのプログラムを記憶してある領域である。

【００６３】

９９９７は、本実施の形態を実現するプログラムを記憶してある領域である。本実施の形態を実現するプログラムが、例えば画像形成装置３００にインストールされる際には、まずインストールプログラムを記憶してある領域９９９８に記憶されているインストールプログラムがシステムにロードされ、ＣＰＵ３０１によって実行される。

【００６４】

次に、ＣＰＵ３０１によって実行されるインストールプログラムが、本実施の形態を実現するプログラムを記憶してある領域９９９７から本実施の形態を実現するプログラムを読み出して、ハードディスク３１１に格納する。

【００６５】

なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダなど）から構成されるシステムあるいは統合装置に適用しても、ひとつの機器からなる装置に適用してもよい。

【００６６】

また、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、本発明の目的が達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００６７】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピー（登録商標

）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ，ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００６８】

また、コンピュータが読み出したプログラムコードを実行することによって、前述した実施形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【００６９】

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

【００７０】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体から、そのプログラムをパソコン通信など通信ラインを介して要求者にそのプログラムを配信する場合にも適用できることは言うまでもない。

【図面の簡単な説明】

【００７１】

【図１】本実施の形態の印刷システムの構成を示す図である。

【図２】一般的なパーソナルコンピュータの内部構成を示した図である。

【図３】一般的な画像形成装置の内部構成を示した図である。

【図４】端末と画像形成装置のモデルを示す図である。

【図５】端末と画像形成装置との間のシーケンスの一例を示す図である。

【図６】端末と画像形成装置との間のシーケンスの一例を示す図である。

【図７】端末と画像形成装置との間のシーケンスの一例を示す図である。

【図８】端末と画像形成装置との間のシーケンスの一例を示す図である。

【図９】画像形成装置のＵＩ画面の一例を示す図である。

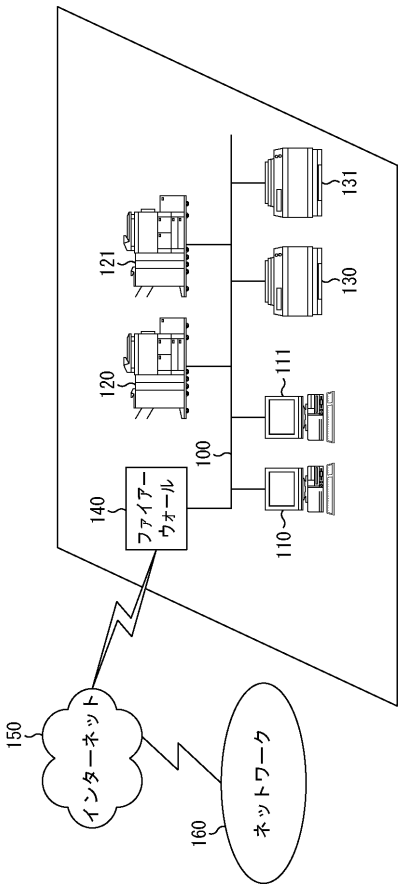
【図１０】本実施の形態のプログラムの記憶媒体におけるメモリマップを示す図である。

【符号の説明】

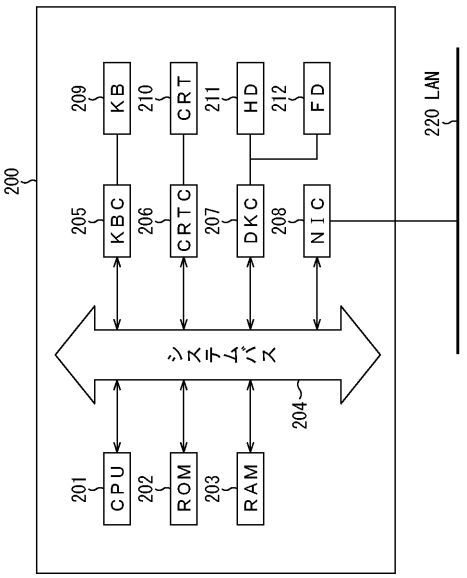
【００７２】

４１０　画像形成装置
４１１　ネットワークインタフェース機能
４１２　セキュア通信機能
４１３　アプリケーション
４１４　鍵管理機能
４１５　鍵ペア
４２０　クライアント端末
４２１　ネットワークインタフェース機能
４２２　セキュア通信機能
４２３　アプリケーション
４２４　鍵インストール機能
４２５　４２５は鍵ペア
４３０　ＬＡＮ

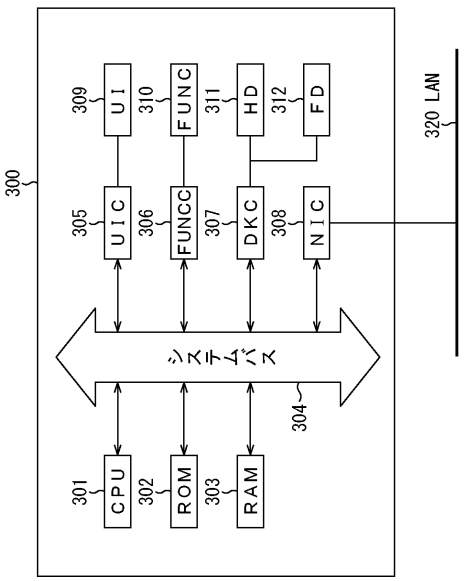
【図１】


インターネット
ファイアーウォール
ネットワーク
100
110
111
120
121
130
131
140
150
160

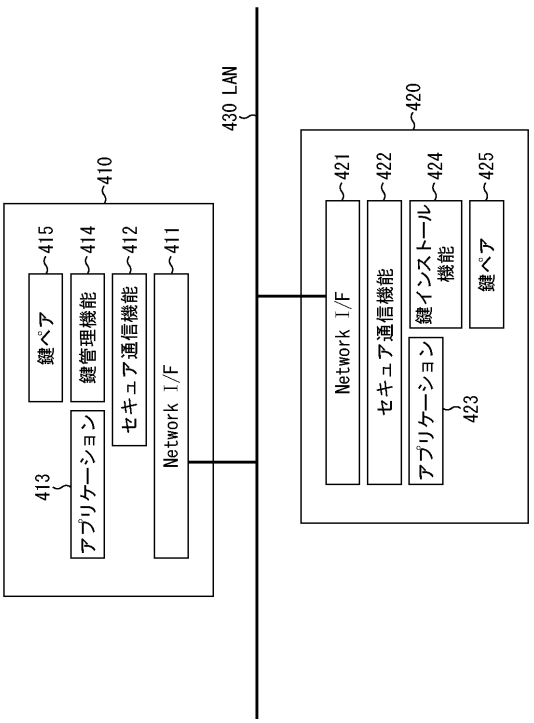
【図２】


200
CPU
ROM
RAM
KBC
CRTC
DKC
NIC
KB
CRT
HD
FD
システムバス
204
220 LAN

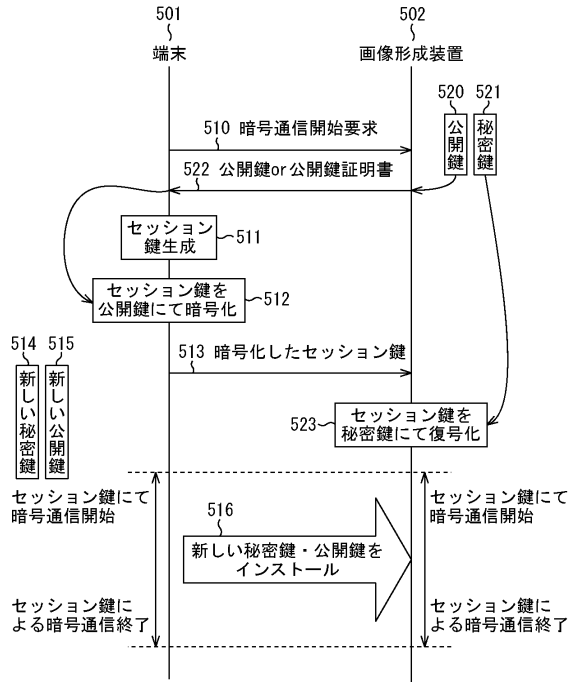
【図３】


300
CPU
ROM
RAM
UIC
FUNCC
DKC
NIC
UI
FUNC
HD
FD
システムバス
304
320 LAN

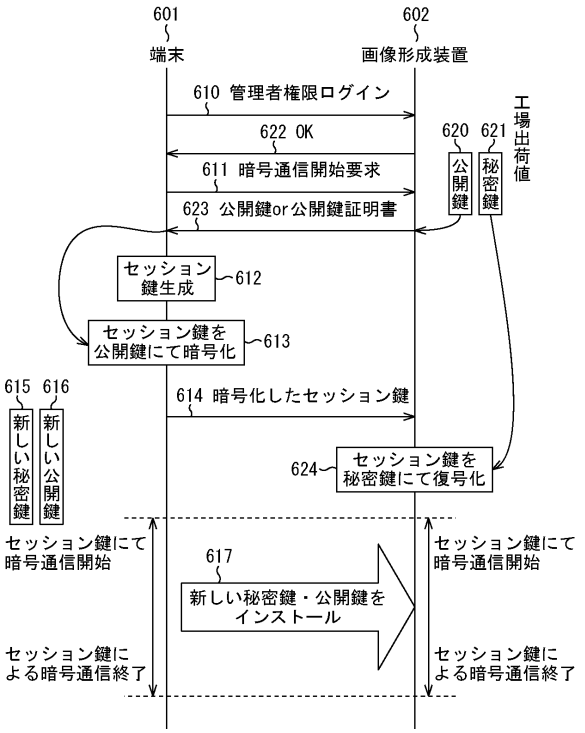
【図４】


410
413
アプリケーション
鍵ペア
鍵管理機能
セキュア通信機能
Network I/F
411
412
414
415
430 LAN
420
421
422
423
424
425
Network I/F
セキュア通信機能
アプリケーション
鍵インストール機能
鍵ペア

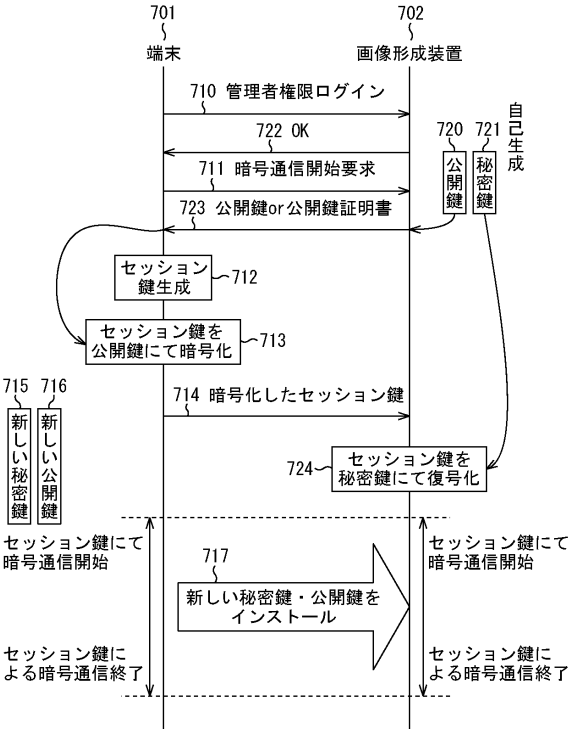
【図５】


501
端末
502
画像形成装置
520 521
公開鍵
秘密鍵
510 暗号通信開始要求
522 公開鍵or公開鍵証明書
セッション鍵生成
511
セッション鍵を公開鍵にて暗号化
512
514 515
新しい秘密鍵
新しい公開鍵
513 暗号化したセッション鍵
523
セッション鍵を秘密鍵にて復号化
セッション鍵にて暗号通信開始
516
新しい秘密鍵・公開鍵をインストール
セッション鍵にて暗号通信開始
セッション鍵による暗号通信終了
セッション鍵による暗号通信終了

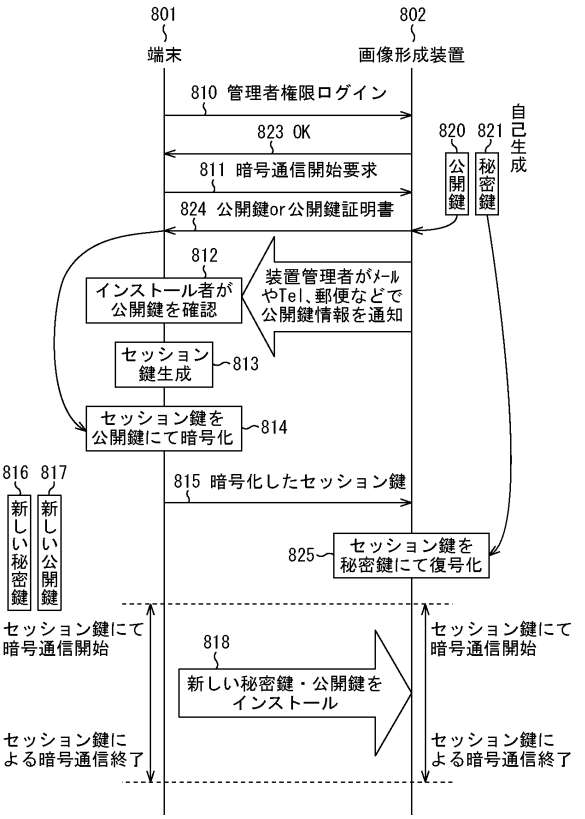
【図６】


601
端末
602
画像形成装置
610 管理者権限ログイン
622 OK
611 暗号通信開始要求
623 公開鍵or公開鍵証明書
工場出荷値
620 621
公開鍵
秘密鍵
セッション鍵生成
612
セッション鍵を公開鍵にて暗号化
613
615 616
新しい秘密鍵
新しい公開鍵
614 暗号化したセッション鍵
624
セッション鍵を秘密鍵にて復号化
セッション鍵にて暗号通信開始
617
新しい秘密鍵・公開鍵をインストール
セッション鍵にて暗号通信開始
セッション鍵による暗号通信終了
セッション鍵による暗号通信終了

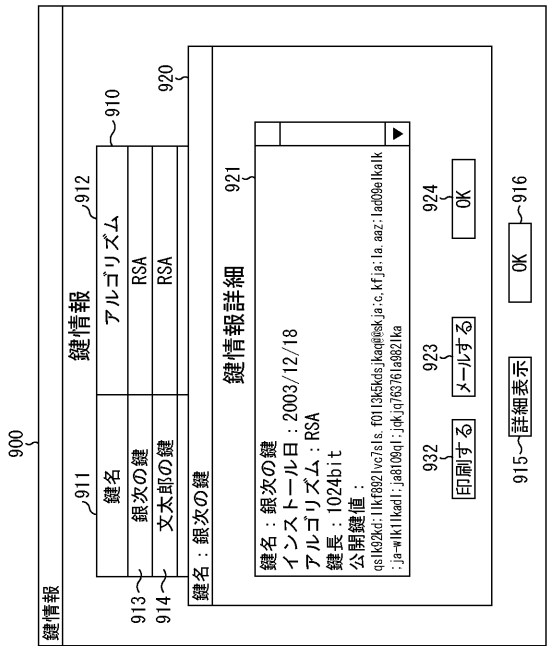
【図７】


701
端末
702
画像形成装置
710 管理者権限ログイン
722 OK
711 暗号通信開始要求
723 公開鍵or公開鍵証明書
自己生成
720 721
公開鍵
秘密鍵
セッション鍵生成
712
セッション鍵を公開鍵にて暗号化
713
715 716
新しい秘密鍵
新しい公開鍵
714 暗号化したセッション鍵
724
セッション鍵を秘密鍵にて復号化
セッション鍵にて暗号通信開始
717
新しい秘密鍵・公開鍵をインストール
セッション鍵にて暗号通信開始
セッション鍵による暗号通信終了
セッション鍵による暗号通信終了

【図８】


801
端末
802
画像形成装置
810 管理者権限ログイン
823 OK
811 暗号通信開始要求
824 公開鍵or公開鍵証明書
自己生成
820 821
公開鍵
秘密鍵
812
インストール者が公開鍵を確認
装置管理者がメールやTel、郵便などで公開鍵情報を通知
セッション鍵生成
813
セッション鍵を公開鍵にて暗号化
814
816 817
新しい秘密鍵
新しい公開鍵
815 暗号化したセッション鍵
825
セッション鍵を秘密鍵にて復号化
セッション鍵にて暗号通信開始
818
新しい秘密鍵・公開鍵をインストール
セッション鍵にて暗号通信開始
セッション鍵による暗号通信終了
セッション鍵による暗号通信終了

【図９】


900
鍵情報
鍵情報
911
鍵名
912
アルゴリズム
910
銀次の鍵
RSA
913
文太郎の鍵
RSA
914
920
鍵名：銀次の鍵
鍵情報詳細
921
鍵名：銀次の鍵
インストール日：2003/12/18
アルゴリズム：RSA
鍵長：1024bit
公開鍵値：
924
OK
932
印刷する
923
メールする
915
詳細表示
OK
916

【図１０】


ディレクトリ情報
9999
・・・
インストールプログラム
9998
・・・
本発明を実現する
プログラム
9997
・・・

フロントページの続き

(56)参考文献 特開２００１－１１１５３９（ＪＰ，Ａ）
特開２００３－１６９０４９（ＪＰ，Ａ）
特開２００３－１１０５５３（ＪＰ，Ａ）
特開２００３－９２５６５（ＪＰ，Ａ）
特開２００２－３７４２４０（ＪＰ，Ａ）
特開平１１－９８１３３（ＪＰ，Ａ）
特開平１１－１６８４６０（ＪＰ，Ａ）
特開２００２－６４４７９（ＪＰ，Ａ）
特開２００２－１５８６４９（ＪＰ，Ａ）
特開平１０－１３３９５６（ＪＰ，Ａ）
国際公開第２００４／０２２３５０（WO，Ａ１）
特開２００２－１８２５６２（ＪＰ，Ａ）
欧州特許出願公開第１０９６７２１（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／００－　９／３２
Ｇ０９Ｃ　　１／００