(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-303676
(P2005-303676A)
(43)公開日　平成17年10月27日(2005.10.27)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	2C061
B41J 29/38	B41J	29/38	Z	5J104
H04L 9/32	H04L	9/00	675A	

審査請求 未請求　請求項の数 16　OL　（全 16 頁）

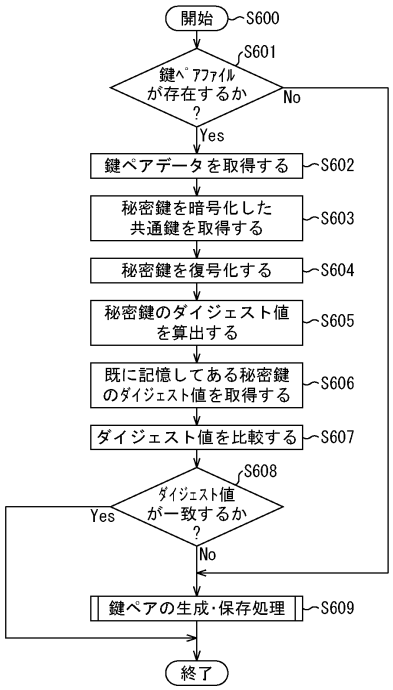
(21)出願番号　特願2004-117117 (P2004-117117)
(22)出願日　平成16年4月12日 (2004.4.12)

(71)出願人　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　山内　久幸
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

Fターム(参考)　2C061 AP01 AP07 CL10 HJ10 HN15
5J104 AA12 EA02 EA23 JA21 PA07

(54)【発明の名称】画像形成装置、鍵ペア生成方法及びコンピュータプログラム

(57)【要約】
【課題】　鍵ペアの再生成を、画像形成装置において簡易に且つ確実に行なえるようにする。
【解決手段】　印刷デバイス１１０の電源が起動すると、印刷デバイス１１０内に鍵ペアデータが存在しているか否かを判断し（ステップＳ６０１）、鍵ペアデータが存在していない場合には、鍵ペアを生成して保存する（ステップＳ６１１）。一方、印刷デバイス１１０内に鍵ペアデータが存在している場合には、その鍵ペアデータに含まれている秘密鍵を復号化してその秘密鍵のダイジェスト値を生成するとともに、前記鍵ペアデータを生成した際に算出した秘密鍵のダイジェスト値を取得し、これらダイジェスト値が一致していない場合には、秘密鍵のデータが破損していると判断して、鍵ペアデータを再生成して更新する（ステップＳ６０２～Ｓ６０９）。
【選択図】　図６



【特許請求の範囲】
【請求項１】
ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断手段と、
前記判断手段によって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成手段と、
前記鍵ペア生成手段によって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶手段とを有することを特徴とする画像形成装置。
【請求項２】
前記判断手段は、前記鍵ペアが前記記憶媒体に記憶されているか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成手段は、前記判断手段によって、前記鍵ペアが前記記憶媒体に記憶されていないと判断された場合に、前記鍵ペアを自動的に生成することを特徴とする請求項１に記載の画像形成装置。
【請求項３】
前記判断手段は、前記記憶媒体に記憶されている鍵ペアが破損されているか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成手段は、前記判断手段によって、前記鍵ペアが破損されていると判断された場合に、前記鍵ペアを自動的に再生成することを特徴とする請求項１又は２に記載の画像形成装置。
【請求項４】
前記鍵ペア生成手段によって生成された鍵ペアの一方向ハッシュ値を生成する第１のハッシュ値生成手段と、
前記第１のハッシュ値生成手段によって生成された一方向ハッシュ値を記憶媒体に記憶するハッシュ値記憶手段と、
前記鍵ペア記憶手段によって前記記憶媒体に記憶された鍵ペアを読み出し、読み出した鍵ペアの一方向ハッシュ値を生成する第２のハッシュ値生成手段とを有し、
前記判断手段は、前記第１のハッシュ値生成手段によって生成された一方向ハッシュ値と、前記第２のハッシュ値生成手段によって生成された一方向ハッシュ値とを比較し、比較した結果に基づいて、前記記憶媒体に記憶されている鍵ペアが破損されているか否かを判断することを特徴とする請求項３に記載の画像形成装置。
【請求項５】
画像形成装置に固有のパラメータ値から擬似乱数を生成し、生成した擬似乱数に基づいて共通鍵暗号方式のパスワード鍵を生成するパスワード鍵生成手段と、
前記パスワード鍵生成手段によって生成されたパスワード鍵を記憶媒体に記憶するパスワード鍵記憶手段と、
前記鍵ペア生成手段によって生成された鍵ペアに含まれる共通鍵と秘密鍵とのうち、少なくとも秘密鍵を、前記パスワード鍵記憶手段によって前記記憶媒体に記憶されたパスワード鍵を用いて暗号化する暗号化手段と、
前記暗号化手段によって暗号化された秘密鍵を、前記パスワード鍵記憶手段によって前記記憶媒体に記憶されたパスワード鍵を用いて復号化する秘密鍵復号化手段とを有し、
前記鍵ペア記憶手段は、前記暗号化手段によって少なくとも秘密鍵が暗号化された鍵ペアを前記記憶媒体に記憶することを特徴とする請求項１に記載の画像形成装置。
【請求項６】
前記判断手段は、前記鍵ペアを再生成するためにユーザによって設定された設定値が有効であるか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成手段は、前記判断手段によって、前記設定値が有効であると判断された場合に、前記鍵ペアを自動的に再生成し、
前記鍵ペア記憶手段は、前記記憶媒体に記憶されている鍵ペアを、前記鍵ペア生成手段によって再生成された鍵ペアに更新することを特徴とする請求項１に記載の画像形成装置

。
【請求項７】
前記鍵ペア生成手段は、公開鍵アルゴリズムと、鍵長とを含むパラメータに基づいて、前記鍵ペアを自動的に生成することを特徴とする請求項１～６の何れか１項に記載の画像形成装置。
【請求項８】
ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断ステップと、
前記判断ステップによって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成ステップと、
前記鍵ペア生成ステップによって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶ステップとを有することを特徴とする鍵ペア生成方法。
【請求項９】
前記判断ステップは、前記鍵ペアが前記記憶媒体に記憶されているか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成ステップは、前記判断ステップによって、前記鍵ペアが前記記憶媒体に記憶されていないと判断された場合に、前記鍵ペアを自動的に生成することを特徴とする請求項８に記載の鍵ペア生成方法。
【請求項１０】
前記判断ステップは、前記記憶媒体に記憶されている鍵ペアが破損されているか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成ステップは、前記判断ステップによって、前記鍵ペアが破損されていると判断された場合に、前記鍵ペアを自動的に再生成することを特徴とする請求項８又は９に記載の鍵ペア生成方法。
【請求項１１】
前記鍵ペア生成ステップによって生成された鍵ペアの一方向ハッシュ値を生成する第１のハッシュ値生成ステップと、
前記第１のハッシュ値生成ステップによって生成された一方向ハッシュ値を記憶媒体に記憶するハッシュ値記憶ステップと、
前記鍵ペア記憶ステップによって前記記憶媒体に記憶された鍵ペアを読み出し、読み出した鍵ペアの一方向ハッシュ値を生成する第２のハッシュ値生成ステップとを有し、
前記判断ステップは、前記第１のハッシュ値生成ステップによって生成された一方向ハッシュ値と、前記第２のハッシュ値生成ステップによって生成された一方向ハッシュ値とを比較し、比較した結果に基づいて、前記記憶媒体に記憶されている鍵ペアが破損されているか否かを判断することを特徴とする請求項１０に記載の鍵ペア生成方法。
【請求項１２】
画像形成装置に固有のパラメータ値から擬似乱数を生成し、生成した擬似乱数に基づいて共通鍵暗号方式のパスワード鍵を生成するパスワード鍵生成ステップと、
前記パスワード鍵生成ステップによって生成されたパスワード鍵を記憶媒体に記憶するパスワード鍵記憶ステップと、
前記鍵ペア生成ステップによって生成された鍵ペアに含まれる共通鍵と秘密鍵とのうち、少なくとも秘密鍵を、前記パスワード鍵記憶ステップによって前記記憶媒体に記憶されたパスワード鍵を用いて暗号化する暗号化ステップと、
前記暗号化ステップによって暗号化された秘密鍵を、前記パスワード鍵記憶ステップによって前記記憶媒体に記憶されたパスワード鍵を用いて復号化する秘密鍵復号化ステップとを有し、
前記鍵ペア記憶ステップは、前記暗号化ステップによって少なくとも秘密鍵が暗号化された鍵ペアを前記記憶媒体に記憶することを特徴とする請求項８に記載の鍵ペア生成方法。
【請求項１３】

前記判断ステップは、前記鍵ペアを再生成するためにユーザによって設定された設定値が有効であるか否かを、画像形成装置が起動したときに判断し、
前記鍵ペア生成ステップは、前記判断ステップによって、前記設定値が有効であると判断された場合に、前記鍵ペアを自動的に再生成し、
前記鍵ペア記憶ステップは、前記記憶媒体に記憶されている鍵ペアを、前記鍵ペア生成ステップによって再生成された鍵ペアに更新することを特徴とする請求項８に記載の鍵ペア生成方法。
【請求項１４】
前記鍵ペア生成ステップは、公開鍵アルゴリズムと、鍵長とを含むパラメータに基づいて、前記鍵ペアを自動的に生成することを特徴とする請求項８～１３の何れか１項に記載の鍵ペア生成方法。
【請求項１５】
ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断ステップと、
前記判断ステップによって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成ステップと、
前記鍵ペア生成ステップによって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶ステップ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１６】
前記請求項１５に記載のコンピュータプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像形成装置、鍵ペア生成方法及びコンピュータプログラムに関し、特に、公開鍵と秘密鍵との鍵ペアを生成するために用いて好適なものである。
【背景技術】
【０００２】
近年、ＰＣ（Personal Computer）等のコンピュータが、個人やオフィス等において急速に普及している。そして、これらのコンピュータを相互に接続するＬＡＮ（Local Area Network）などのネットワークも普及してきている。そのため、最近では、ネットワークに接続されているプリンタやスキャナなどの装置を複数のユーザにて共有して使用することを可能とした環境が、広く構築されるようになってきた。
【０００３】
特に、このような環境下のオフィスにおいては、ネットワークを用いたシステムに対応することが可能なデジタル複合機(ＭＦＰ：Multi Function Peripheral)が広く利用されるようになっている。このＭＦＰは、印刷・プリンタ機能やスキャナ機能等の複数の機能を単体で持つので、ＰＣのユーザは、ネットワークを介してこれらの機能を共有して利用することができる。また、ＭＦＰは、ＬＡＮ（Local Area Network）のようなローカルな環境だけにとどまらず、インターネットやＷＡＮ（Wide Area Network）といった大規模なネットワークにも接続され、利用されている。
【０００４】
そのような大規模なネットワークに接続されているＭＦＰのような印刷デバイスを用いて、オフィスドキュメントのような秘匿性の高い情報データを印刷するような場合には、前記秘匿性の高い情報データを、ネットワークを介して送受信しなければならず、ネットワークの安全性を十分に確保することを考慮しなければならない。
【０００５】
さらに、近年、ＭＦＰの拡張外部コントローラとして、前記ＭＦＰに接続された汎用ＰＣを用いて、前記ＭＦＰの制御を行なうようにするシステムが考案されている。このような汎用ＰＣのプラットフォームの外部コントローラを利用してＭＦＰを制御することによ

って、組込みデバイスであるＭＦＰに設けられている組込みアプリケーションでは実現することが困難であったさまざまな機能を付加することが可能になる。

【０００６】

このような外部コントローラとＭＦＰとの接続形態としては、シリアルケーブルまたはパラレルケーブルによる接続や、Ethernet（登録商標）を利用した接続など、様々な接続形態が考えられる。特に、外部コントローラとＭＦＰとをEthernet（登録商標）を利用して接続した場合には、機器の制御データや、秘匿性の高い内部データなどがネットワーク上に流出してしまうため、それらのデータを何らかの手段によって保護することが重要である。

【０００７】

そこで、ＷＳ（workstation）やＰＣ等により構成されるサーバ・クライアント端末間で、秘匿性の高いデータを、ネットワークを介してやり取りするに際しては、サーバ・クライアント端末間で認証を行なったり、送受信する秘匿性の高いデータの暗号化を行ったりするようにしている。したがって、ネットワークに接続されたＭＦＰを利用する場合にも、通信相手の認証や、通信データの暗号化を行なうことが望ましい。

【０００８】

近年、通信相手の認証や、通信データの暗号化を行なうために、様々な暗号化技術が利用されている。その中でも特にＷＷＷ（World Wide Web）では、ＰＫＩ（Public Key Infrastructure）と呼ばれる暗号化技術が最も広く利用されている。

【０００９】

そして、このＰＫＩの応用技術として、ＰＫＩ技術を利用した暗号化通信を行なうための様々な通信プロトコルであるＴＬＳ（Transport Layer Security：ＲＦＣ２２４６）やＳｅｃＳＨ（SecureSHell：IETF InternetDraft）等が広く普及しつある。これらのプロトコルによって、秘匿性の高いデータを暗号化して通信を行なう場合には、通信を行なうサーバホスト（あるいはクライアントホスト）が公開鍵と秘密鍵との鍵ペアを保持する必要がある。

【００１０】

【特許文献１】特開２００２－２９７５４８号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

前述したようなプロトコルにより、ＷＳやＰＣ等により構成されるサーバ・クライアント端末間で、秘匿性の高いデータを暗号化して通信する場合には、通信のホスト側となる装置（ＷＳ又はＰＣ）で前記鍵ペアを作成する必要がある。

【００１２】

このように鍵ペアを生成する場合、通信のホスト側となる装置（ＷＳ又はＰＣ）では、ネットワーク管理者などの管理ユーザによる手動のオペレーションに従って、鍵ペアを生成し、生成した鍵ペアをＷＳやＰＣの記憶媒体であるハードディスク(ＨＤ)などへ保存するという手法が一般的に行われている。

【００１３】

しかしながら、このようにして鍵ペアの生成及び保存を行なう場合には、鍵ペアを生成するためのアプリケーションを使用するために、専門的な知識や熟練した技術がユーザに要求されるという問題がある。さらに、ユーザは煩雑な操作を行なわなければならないという問題もある。

【００１４】

また、一般に、印刷デバイスのような組込みデバイス（画像形成装置）には、汎用ＰＣのように複雑な処理を実現するユーザインタフェイスが実装されていない。このため、印刷デバイスのような組込みデバイスにおいては、前述したようなユーザの手動のオペレーションによって鍵ペアの生成及び保存を行なえるようにすることが極めて困難である。仮に、印刷デバイスのような組込みデバイスに、汎用ＰＣのように複雑な処理を実現するユ

ーザインタフェイスを実装したとしても、前述した一般的なＷＳやＰＣ等における問題と同様な問題が残る。

【００１５】

こうした問題を解決するために、特許文献１（特開２００２－２９７５４８号公報；端末登録システムとそれを構成する装置および方法）では、印刷デバイスのような組込みデバイス（画像形成装置）において、デバイス自身が自動的に鍵ペアを生成することが検討されている。

【００１６】

しかしながら、印刷デバイスが保持する鍵ペアが何らかの理由によって、消去または破損した場合には、印刷デバイスとＰＣ等の外部機器との間でデータを暗号化して通信することが不可能となる。

このような場合に、印刷デバイスとＰＣ等の外部機器との間でデータを暗号化して通信することを再開させるためには、ユーザが、鍵ペアの異常を検知し、手動のオペレーションにより鍵ペアを再生成させる必要がある。このため、鍵ペアを再生成させるためにユーザが行なう操作が煩雑になるという問題点があった。

【００１７】

また、印刷デバイスとＰＣ等の外部機器との間でデータを暗号化して通信する際に、鍵ペアの公開鍵は不特定の通信相手に対して送信される。ところが、数学的に既知の解読法が公開されているために、第三者によって、送信された公開鍵から秘密鍵が推定されてしまう虞がある。特に、鍵長が比較的短い場合には、鍵ペアの持つ秘匿性が失われ易くなる虞がある。また、何らかの手段によって秘密鍵が第三者に漏洩してしまった場合にも、鍵ペアの持つ秘匿性が失われてしまう。

【００１８】

そこで、このような場合には、鍵ペアを更新する必要があるが、前述した特許文献１に記載されている技術のように、印刷デバイス自身が鍵ペアを常に自動的に生成すると、そのような鍵ペアを更新することができないという問題点があった。

【００１９】

本発明は、前述の問題点に鑑みてなされたものであり、鍵ペアの再生成を、画像形成装置において簡易に且つ確実に行なえるようにすることを目的とする。

【課題を解決するための手段】

【００２０】

本発明の画像形成装置は、ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断手段と、前記判断手段によって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成手段と、前記鍵ペア生成手段によって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶手段とを有することを特徴とする。

【００２１】

本発明の鍵ペア生成方法は、ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断ステップと、前記判断ステップによって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成ステップと、前記鍵ペア生成ステップによって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶ステップとを有することを特徴とする。

【００２２】

本発明のコンピュータプログラムは、ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断する判断ステップと、前記判断ステップによって、前記鍵ペアを生成する必要があると判断された場合に、前記鍵ペアを自動的に生成する鍵ペア生成ステップと、前記鍵ペア生成ステップによって生成された鍵ペアを記憶媒体に記憶する鍵ペア記憶ステップとをコンピュータに実行させることを特徴とする。

本発明のコンピュータ読み取り可能な記録媒体は、前記記載のコンピュータプログラムを記録したことを特徴とする。

【発明の効果】

【００２３】

本発明によれば、ネットワークを介して相互に接続された外部装置と暗号化通信を行なうために、公開鍵と秘密鍵との鍵ペアを生成する必要があるか否かを判断し、前記鍵ペアを生成する必要があると判断された場合には、前記鍵ペアを自動的に生成するようにしたので、鍵ペアの状態を画像形成装置で管理することができる。これにより、ユーザの煩雑な操作によらずに、必要に応じて鍵ペアを自動的に再生成することができる。

【発明を実施するための最良の形態】

【００２４】

次に、図面を参照しながら、本発明の一実施形態について説明する。

図１は、本発明の実施形態を示し、印刷通信システムの構成の一例を示す図である。

本実施形態による印刷デバイス１１０は、印刷デバイス１１０の外部コントローラ端末装置１２０と、ユーザ端末装置１３０と、ネットワーク１００を介して接続されている。そして、印刷デバイス１１０は、これら外部コントローラ端末装置１２０及びユーザ端末装置１３０と相互にデータの通信を行なうことができるようになっている。なお、図１では、印刷デバイス１１０、外部コントローラ端末装置１２０、及びユーザ端末装置１３０をそれぞれ１つのみ示しているが、これらは複数であっても良い。

【００２５】

本実施形態における印刷デバイス１１０は、コピー機としてもネットワークプリンタとしても使用することが可能なＭＦＰ（Multi Function Peripheral）である。

印刷デバイス１１０の外部コントローラ端末装置１２０は、印刷デバイス１１０の制御コマンドあるいは制御データを、ネットワーク１００を介して送受信することによって、印刷デバイス１１０を遠隔制御することを可能にするためのものである。

【００２６】

ユーザ端末装置１３０は、印刷デバイス１１０で保持されている印刷などの各種機能をユーザが利用することを可能にするための装置である。例えば、ユーザ端末装置１３０は、印刷デバイス１１０に対して利用可能な印刷アプリケーションや印刷ドライバを有しており、これら印刷アプリケーションや印刷ドライバを用いて、印刷デバイス１１０あるいは外部コントローラ端末１２０に印刷データを送信する。そして、印刷デバイス１１０は、送信された印刷データに基づいて印刷を実行する。

【００２７】

また、本実施形態における外部コントローラ端末装置１２０は、汎用ＰＣのプラットフォームを利用した端末装置であり、そのハードウェアの構成は、ユーザ端末装置１３０と同様である。

なお、図１に示した全ての装置（印刷デバイス１１０、外部コントローラ端末装置１２０、ユーザ端末装置１３０）は、ネットワーク１００を介した通信を行なうことができるネットワーク対応デバイスである。また、本実施形態では、ネットワーク１００として、ＬＡＮを用いるようにしている。ただし、ネットワーク１００は、ＬＡＮに限定されず、ＷＡＮやインターネット等であってもよいということは言うまでもない。

【００２８】

印刷デバイス１１０と外部コントローラ端末装置１２０との間の通信や、印刷デバイス１１０とユーザ端末装置１３０との間の通信は、既定の暗号化通信プロトコルで実現することが可能である。ここで、暗号化通信プロトコルは、後述する印刷デバイス１１０の鍵ペア生成機能によって生成された鍵ペアを利用して通信相手となる装置を認証したり、通信データの暗号化に使用する共通鍵の生成を行なって通信データを暗号化したりするためのものである。

【００２９】

図２は、ユーザ端末装置１３０の内部構成（ハードウェアの構成）の一例を示すブロッ

ク図である。
図２において、ＣＰＵ２０１は、ＲＯＭ（リードオンリーメモリ）２０２またはハードディスク（ＨＤ）２１１に記憶された制御ソフトウェア、あるいはフレキシブルディスクドライブ（ＦＤ）２１２より供給される制御ソフトウェアを実行し、システムバス２０４に接続される各デバイスを総括的に制御する。
本実施形態では、ＣＰＵ２０１と、ＲＯＭ２０２またはハードディスク（ＨＤ）２１１に記憶されたプログラムとにより、印刷デバイス１１０との暗号化通信が行なわれるようにしている。
【００３０】
ＲＡＭ（ランダムアクセスメモリ）２０３は、ＣＰＵ２０１の主メモリ及びワークエリア等として機能する。キーボードコントローラ（ＫＢＣ）２０５は、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。
ＣＲＴコントローラ（ＣＲＴＣ）２０６は、ＣＲＴディスプレイ（ＣＲＴ）２１０の表示を制御する。ディスクコントローラ（ＤＫＣ）２０７は、ハードディスク（ＨＤ）２１１、及びフレキシブルディスク（ＦＤ）２１２とのアクセスを制御する。
【００３１】
ハードディスク（ＨＤ）２１１は、ブートプログラム（起動プログラム：ハードやソフトの実行（動作）を開始するプログラム）、複数のアプリケーション、編集ファイル、ユーザファイル、及びネットワーク管理プログラム等を記憶する。
ネットワークインタＩ／Ｆ制御装置２０８は、ネットワーク（ＬＡＮ）１００を介して、印刷デバイス１１０、他のネットワーク機器、及び他のＰＣ（パーソナルコンピュータ）と双方向でデータのやり取りを行なう。
なお、外部コントローラ端末装置１２０の内部構成（ハードウェアの構成）は、図２に示したものと同じであるので、詳細な説明を省略する。
【００３２】
図３は、印刷デバイス１１０の内部構成（ハードウェアの構成）の一例を示すブロック図である。図３において、印刷デバイス１１０は、本実施形態における各手段のプログラムが稼動するネットワークデバイスである。
印刷デバイス１１０は、ＣＰＵ（中央処理装置）３０１を備えている。このＣＰＵ３０１は、ＲＯＭ（リードオンリーメモリ）３０２またはハードディスク（ＨＤ）３０９に格納されているプログラムを実行して、システムバス３０４に接続される各デバイスを総括的に制御する。
【００３３】
ＲＡＭ（ランダムアクセスメモリ）３０３は、ＣＰＵ３０１の主メモリ及びワークエリアとして機能する。不揮発性メモリ（NVRAM；Nonvolatile RAM）３０５は、印刷デバイス１１０の各種設定値を保存するためのものである。デバイスコントローラ（ＤＶＣ）３０６は、デバイス（Device）３０７を制御するためのものである。
【００３４】
ディスクコントローラ（ＤＫＣ）３０８は、デバイスを制御するためのプログラムや各種データが記憶されているハードディスク（ＨＤ）３０９とのアクセスを制御する。
ネットワークＩ／Ｆ制御装置３１０は、ネットワーク（ＬＡＮ）１００を介してネットワークプリンタ、他のネットワーク機器、或いは他のＰＣ（パーソナルコンピュータ）と双方向でデータのやり取りを行なう。
【００３５】
本実施形態におけるＵＩ（ユーザインタフェイス）３１１は、タッチパネル方式のディスプレイ画面を有している。ユーザは、このタッチパネル方式のディスプレイ画面を操作することにより、印刷デバイス１１０の各種設定などを実行することができる。
【００３６】
図４は、本実施形態における外部コントローラ端末装置１２０及びユーザ端末装置１３０のソフトウェアの構成の一例を示すブロック図である。

図４において、ネットワークドライバ４０１は、ネットワーク１００に接続され、図２に示したネットワークＩ／Ｆ制御装置２０８を制御して、ネットワーク１００を介して外部とデータの送受信を行なう。

【００３７】

ネットワーク制御部４０２は、ＴＣＰ／ＩＰなどのネットワーク通信プロトコルを制御して、データの送受信を行なう。

暗号化通信部４０３は、前述した既定の暗号化通信プロトコルによって暗号化通信を行なうためのモジュールである。暗号化処理部４０６は、送信する通信データを暗号化したり、受信した通信データを復号化したりするなどの各種暗号化処理を行なう。

【００３８】

アプリケーション４０４は、印刷デバイス１１０における印刷などの機能を利用したり実行したりするためのアプリケーションである。

デバイス制御部４０５は、外部コントローラ端末装置１２０が保持するモジュールであり、印刷デバイス１１０の制御コマンドや制御データを生成し、生成した制御コマンドや制御データを、ネットワーク１００を経由して印刷デバイス１１０に送信することで、印刷デバイス１１０を遠隔制御するための処理を行なう。

【００３９】

図５は、本実施形態における印刷デバイス１１０のソフトウェアの構成の一例を示すブロック図である。

図５において、ネットワークドライバ５０１は、ネットワーク１００に接続され、図３に示したネットワークＩ／Ｆ制御装置３１０を制御して、ネットワーク１００を介して外部とデータの送受信を行なう。

【００４０】

ネットワーク制御部５０２は、ＴＣＰ／ＩＰなどのネットワーク通信プロトコルを制御して、データの送受信を行なう。

暗号化通信部５０３は、前述した既定の暗号化通信プロトコルによって暗号化通信を行なうためのモジュールである。暗号化処理部５０６は、送信する通信データを暗号化したり、受信した通信データを復号化したりするなどの各種暗号化処理を行なう。

【００４１】

アプリケーション５０４は、印刷デバイス１１０における印刷などの機能を実行するためのアプリケーションである。

デバイス制御部５０５は、印刷デバイス１１０の制御コマンドや制御データを生成して、印刷デバイス１１０を統括的に制御するためのモジュールである。

鍵ペア生成処理部５０７は、鍵ペアのデータ（以下、鍵ペアデータと称する）を自動的に生成する処理を実行するためのモジュールである。

鍵ペア保存処理部５０８は、鍵ペア生成処理部５０７の処理によって生成された鍵ペアデータを図３に示したハードディスク（ＨＤ）３０９や不揮発性メモリ（NVRAM）３０５に保存するためのモジュールである。また、他のモジュールからの要求によって、鍵ペアデータをハードディスク３０９や不揮発性メモリ（NVRAM）３０５から読み出し、鍵ペアデータの受け渡しを行なう。

【００４２】

次に、図６のフローチャートを参照しながら、鍵ペアデータを自動生成して保存する際に印刷デバイスで行なわれる動作の一例について述べる。

なお、以下では、印刷デバイス１１０の鍵ペアデータは、図３に示したハードディスク（ＨＤ）３０９に、ファイルとして保存されているものとして説明を行なう。また、鍵ペアデータが保存されているファイルを鍵ペアファイルと称する。

【００４３】

まず、ステップＳ６０１において、暗号化処理部５０６は、印刷デバイス１１０の電源起動時に、ハードディスク（ＨＤ）３０９にアクセスして、鍵ペアデータが保存されている鍵ペアファイルがハードディスク（ＨＤ）３０９に存在するか否かを判断する。

このステップＳ６０１における判断の結果、鍵ペアファイルが存在する場合には、次のステップＳ６０２へ進む。

【００４４】

次に、ステップＳ６０２において、暗号化処理部５０６は、ハードディスク（ＨＤ）３０９に保存されている鍵ペアファイルをオープンし、鍵ペアデータに含まれている公開鍵のデータと秘密鍵のデータとを取得する。

本実施形態において、印刷デバイス１１０が保持する鍵ペアのうち、秘密鍵は、共通鍵暗号方式により暗号化された形式で鍵ペアファイルに保存されている。

また、秘密鍵を暗号化するための共通鍵のデータは、印刷デバイス１１０の内の不揮発性メモリ（NVRAM）３０５に保存されている。

【００４５】

なお、本実施形態においては、共通鍵のデータは、図３に示した不揮発性メモリ（NVRAM）３０５に保存されており、外部からアクセスすることができないようになっている。

また、本実施形態では、秘密鍵のみを共通鍵暗号方式で暗号化しているが、秘密鍵と公開鍵との両方を暗号化してファイルに保持しておいてもよいし、公開鍵暗号方式を用いて秘密鍵や公開鍵を暗号化してもよいことは言うまでも無い。

【００４６】

次に、ステップＳ６０３において、暗号化処理部５０６は、不揮発性メモリ（NVRAM）３０５にアクセスして、秘密鍵を暗号化する際に用いられた共通鍵のデータを取得する。次に、ステップＳ６０４において、暗号化処理部５０６は、この取得した共通鍵を用いてステップＳ６０２において取得した秘密鍵のデータを復号化する。

ステップＳ６０４において秘密鍵の復号化に成功したら、次のステップＳ６０５において、鍵ペア生成処理部５０７は、一方向性ハッシュ関数のアルゴリズムにより、秘密鍵のダイジェスト値を生成する。

【００４７】

この一方向性ハッシュアルゴリズムには、SHA-1（Secure Hash Algorithm - 1）や、MD5（Message Digest Algorithm5 ）などを利用することができる。

本実施形態においては、鍵ペアデータの生成時においても、この秘密鍵のダイジェスト値を生成し、生成した秘密鍵のダイジェスト値を、秘密鍵を暗号化する際に用いられる共通鍵と同様に、不揮発性メモリ（NVRAM）３０５に保存しておく。

【００４８】

次に、ステップＳ６０６において、鍵ペア生成処理部５０７は、不揮発性メモリ（NVRAM）３０５から、鍵生成時に算出した秘密鍵のダイジェスト値を取得する。

次に、ステップＳ６０７において、鍵ペア生成処理部５０７は、ステップＳ６０６において取得したダイジェスト値と、ステップＳ６０５において算出した秘密鍵のダイジェスト値とを比較する。これらのダイジェスト値を比較することによって、保持している秘密鍵のデータが破損しているか否かを検知する。

【００４９】

次に、ステップＳ６０８において、鍵ペア生成処理部６０７は、比較したダイジェスト値のデータが同一であるか否かを判断する。この判断の結果、ダイジェスト値のデータが同一でない場合には、次のステップＳ６０９へ進んで、後述する鍵ペアの生成・保存処理を行ない、この処理が完了したら本フローチャートを終了する。一方、ダイジェスト値のデータが同一である場合には、前記鍵ペアの生成・保存処理を行なわずに、本フローチャートを終了する。

【００５０】

また、前記ステップＳ６０１において、鍵ペアファイルが存在しないと判断された場合には、ステップＳ６０２からステップＳ６０８までの処理を行なわずに、ステップＳＳ６０９まで進み、鍵ペアの生成・保存処理を行なう。

本実施形態において、印刷デバイス１１０が保持する鍵ペアの数は一つであるが、印刷デバイス１１０を利用するユーザ毎や、印刷デバイス１１０上のアプリケーション毎など

、必要な用途に応じて複数の鍵ペアを、前述した図６のフローチャートにおける処理によりそれぞれ自動的に生成及び保存してもよい。

【００５１】

次に、図７のフローチャートを参照しながら、本実施形態における鍵ペアの生成・保存処理を行なう際に印刷デバイス１１０で行なわれる動作の一例を説明する。

なお、図７に示す鍵ペアの生成・保存処理は、図６に示したステップＳ６０９の鍵ペアの生成・保存処理である。

まず、ステップＳ７０１において、鍵ペア生成処理部５０７は、鍵ペアを生成するための設定パラメータ値を取得する。本実施形態における設定パラメータ値は、生成する鍵ペアの公開鍵暗号化アルゴリズムおよび鍵のデータのBit長である。

【００５２】

本実施形態においては、生成する鍵ペアの公開鍵暗号化アルゴリズムとして、ＲＳＡ方式やＤＳＡ方式などの公開鍵暗号化アルゴリズムの鍵ペアを生成することが可能である。印刷デバイス１１０には、あらかじめデフォルトの設定として、公開鍵暗号化アルゴリズムと鍵のデータのBit長とが設定されている。これらの設定値は、印刷デバイス１１０内の不揮発性メモリ（NVRAM）３０５に保存されており、図３に示した、タッチパネル方式のディスプレイ画面であるＵＩ（ユーザインタフェイス）３１１の操作によって、生成する鍵ペアの暗号化アルゴリズムと、生成する鍵のデータのbit長との設定を、ユーザが変更することも可能とする。

【００５３】

次に、ステップＳ７０２において、鍵ペア生成処理部５０７は、ステップＳ７０１で取得した不揮発性メモリ（NVRAM）３０５に保存してある設定値をもとに、鍵ペアの生成を実行する。鍵ペアの生成が正常に終了したら、ステップＳ７０３において、鍵ペア生成処理部５０７は、ステップＳ７０２において生成した鍵ペアの秘密鍵のデータを共通鍵暗号方式で暗号化するための共通鍵として、擬似乱数を生成する。

【００５４】

次に、ステップＳ７０４において、鍵ペア生成処理部５０７は、一方向性ハッシュ関数により、ステップＳ７０２で生成した秘密鍵のダイジェスト値を算出する。前述したように、この秘密鍵のダイジェスト値は、図６のステップＳ６０７において、秘密鍵のデータが破損しているか否かを検証するために用いられるものである。

【００５５】

次に、ステップＳ７０５において、鍵ペア生成処理部５０７は、ステップＳ７０３において生成した秘密鍵を暗号化するための共通鍵によって、秘密鍵のデータの暗号化を行なう。

秘密鍵のデータの暗号化に成功したら、ステップＳ７０６において、鍵ペア保存処理部５０８は、公開鍵のデータと暗号化された秘密鍵のデータとをハードディスク（ＨＤ）３０９へファイルとして出力して、保存する。

さらに、次のステップＳ７０７において、鍵ペア保存処理部５０８は、秘密鍵のデータを暗号化した際に用いた共通鍵のデータを不揮発性メモリ（NVRAM）３０５へ保存する。同様にステップＳ７０８において、鍵ペア保存処理部５０８は、秘密鍵のダイジェスト値のデータを不揮発性メモリ（NVRAM）３０５へ保存して、本フローチャートによる処理を終了する。

【００５６】

前述したように、本実施形態では、印刷デバイス１１０が自動的に鍵ペアを生成して保存するだけではなく、鍵ペアの再生成や更新をユーザが所望した場合に、鍵ペアを再生成して更新することを印刷デバイス１１０で実行することが可能である。

【００５７】

ここで、図８のフローチャートを参照しながら、ユーザの設定によって鍵ペアを再生成して更新する際に印刷デバイス１１０で行なわれる動作の一例を説明する。

本実施形態の印刷デバイス１１０では、前述した、生成する鍵ペアの公開鍵暗号化アル

ゴリズムと、鍵のデータのBit長とをユーザが指定する場合と同様にして、鍵ペアの再生成・更新を指定することができる。

すなわち、この鍵ペアの再生成・更新の設定値も、図３に示した、タッチパネル方式のディスプレイ画面であるＵＩ（ユーザインタフェイス）３１１の操作によって、設定することが可能であり、不揮発性メモリ（NVRAM）３０５にその設定値が保存される。

【００５８】

まず、ステップＳ８０１において、鍵ペア生成処理部５０７は、印刷デバイス１１０の電源投入時に、鍵ペアの再生成・更新の設定値を取得する。次に、ステップＳ８０２において、鍵ペア生成処理部５０７は、ステップＳ８０１において取得した設定値に基づき、設定がオンであるかそれともオフであるか（ＯＮ／ＯＦＦ）を判断する。この判断の結果、ステップＳ８０１において取得した設定値に基づき、設定がオン（ＯＮ）になっている場合には、ステップＳ８１１の処理へ進み、鍵ペアの再生成・更新処理を行なう。

【００５９】

一方、ステップＳ８０２において設定がオフ（ＯＦＦ）である場合には、ステップＳ８０３からステップＳ８１０までの処理を行なう。

なお、ステップＳ８１１の処理は、図６に示したステップＳ６０９（すなわち、図７に示したステップＳ７０１からステップＳ７０８）と同じである。また、ステップＳ８０３からステップＳ８１０までの処理は、図６に示したステップＳ６０１からステップＳ６０８までの処理と同じ処理である。したがって、これらの処理の詳細な説明を省略する。

【００６０】

なお、本実施形態においては、印刷デバイス１１０の起動時に、鍵ペアを再生成して更新する場合を例に挙げて説明したが、印刷デバイス１１０の起動中においても、ユーザによるＵＩ（ユーザインタフェイス）３１１の操作に基づいて、鍵ペアの再生成・更新の設定がオンであるか否かを判断し、設定がオンである場合には、前述したようにして鍵ペアを再生成して更新するようにしてもよい。

【００６１】

以上のように本実施形態では、印刷デバイス１１０の電源が起動すると、印刷デバイス１１０内のハードディスク（ＨＤ）３０９に鍵ペアデータが存在しているか否かを判断し、鍵ペアデータが存在していない場合には、鍵ペアを生成して保存するようにしたので、印刷デバイス１１０で保存されている鍵ペアが何らかの理由によって消去してしまった場合であっても、ユーザの煩雑な操作によらずに、鍵ペアデータを得ることができる。これにより、印刷デバイス１１０とユーザ端末装置１３０との間でデータを暗号化して通信することが不可能になることを容易に且つ確実に防止することができる。

【００６２】

また、印刷デバイス１１０内のハードディスク（ＨＤ）３０９に鍵ペアデータが存在している場合には、その鍵ペアデータに含まれている秘密鍵を復号化してその秘密鍵のダイジェスト値を生成するとともに、前記鍵ペアデータを生成した際に算出した秘密鍵のダイジェスト値を取得し、これらダイジェスト値が一致していない場合には、秘密鍵のデータが破損していると判断して、鍵ペアデータを再生成して更新するようにしたので、印刷デバイス１１０で保存されている鍵ペアが何らかの理由によって破損してしまった場合であっても、ユーザの煩雑な操作によらずに、適切な鍵ペアデータを得ることができる。これにより、印刷デバイス１１０とユーザ端末装置１３０との間でデータを暗号化して通信することが不可能になることを容易に且つ確実に防止することができる。

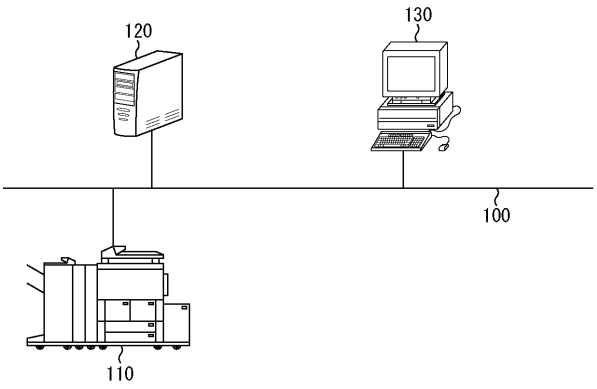
【００６３】

また、印刷デバイス１１０の電源が起動したとき以外にも、印刷デバイス１１０に配設されたＵＩ（ユーザインタフェイス）３１１のユーザによる操作内容に基づいて、鍵ペアデータの再生成して更新するようにしたので、例えば、鍵ペアの持つ秘匿性が失われた虞があるとユーザが判断した場合に、ユーザの意図に従って鍵ペアデータを更新することができる。これにより、印刷デバイス１１０とユーザ端末装置１３０との間で送受信されるデータの秘匿性を可及的に確実に保持させることが可能になる。

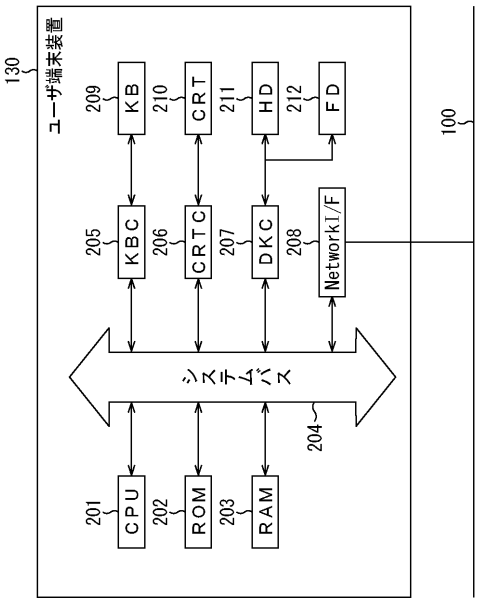
【００６４】
（本発明の他の実施形態）
上述した実施形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。
【００６５】
また、この場合、前記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えば、かかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。
【００６６】
また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。
【００６７】
さらに、供給されたプログラムコードがコンピュータの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格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行ない、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。
【図面の簡単な説明】
【００６８】
【図１】本発明の実施形態を示し、印刷通信システムの構成の一例を示す図である。
【図２】本発明の実施形態を示し、ユーザ端末装置の内部構成（ハードウェアの構成）の一例を示すブロック図である。
【図３】本発明の実施形態を示し、印刷デバイスの内部構成（ハードウェアの構成）の一例を示すブロック図である。
【図４】本発明の実施形態を示し、外部コントローラ端末装置及びユーザ端末装置のソフトウェアの構成の一例を示すブロック図である。
【図５】本発明の実施形態を示し、印刷デバイスのソフトウェアの構成の一例を示すブロック図である。
【図６】本発明の実施形態を示し、鍵ペアデータを自動生成して保存する際に印刷デバイスで行なわれる動作の一例を説明するフローチャートである。
【図７】本発明の実施形態を示し、鍵ペアの生成・保存処理を行なう際に印刷デバイスで行なわれる動作の一例を説明するフローチャートである。
【図８】本発明の実施形態を示し、ユーザの設定によって鍵ペアを再生成して更新する際に印刷デバイスで行なわれる動作の一例を説明するフローチャートである。
【符号の説明】
【００６９】
１００　ネットワーク
１１０　印刷デバイス
１２０　外部コントローラ端末装置
１３０　ユーザ端末装置
５０６　暗号化処理部

５０７　鍵ペア生成処理部
５０８　鍵ペア保存処理部

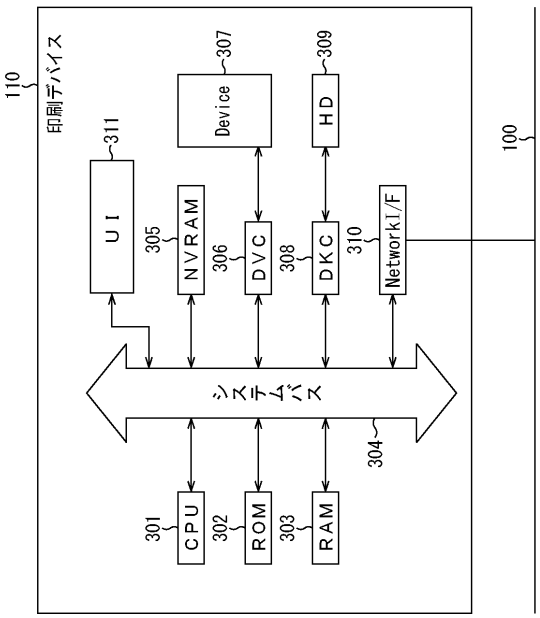
【図１】



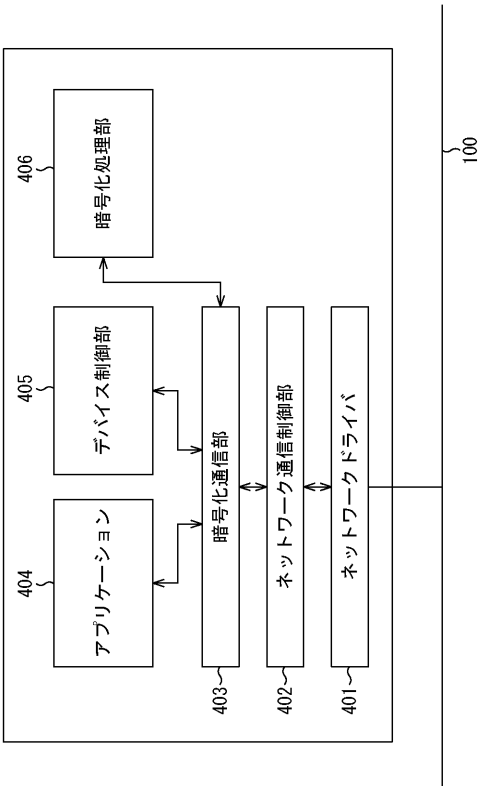
【図２】



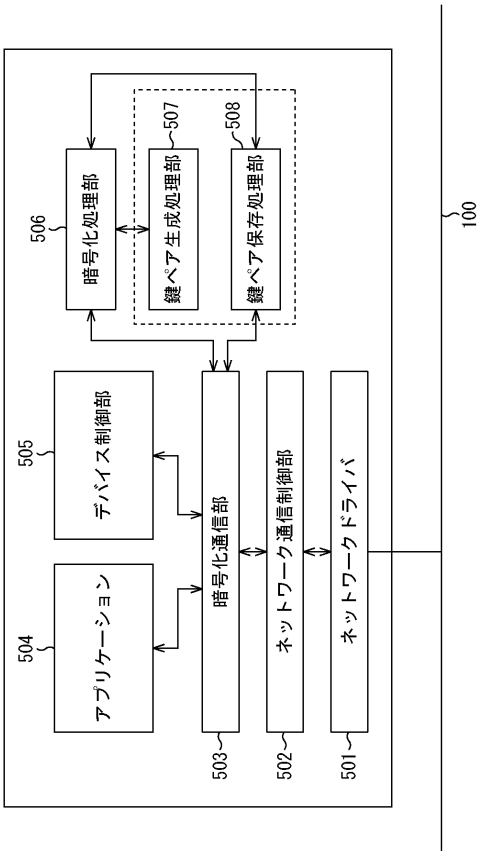
【図３】


110
印刷デバイス
311
UI
305
NVRAM
306
DVC
307
Device
308
DKC
309
HD
310
Network I/F
100
システムバス
304
301
CPU
302
ROM
303
RAM

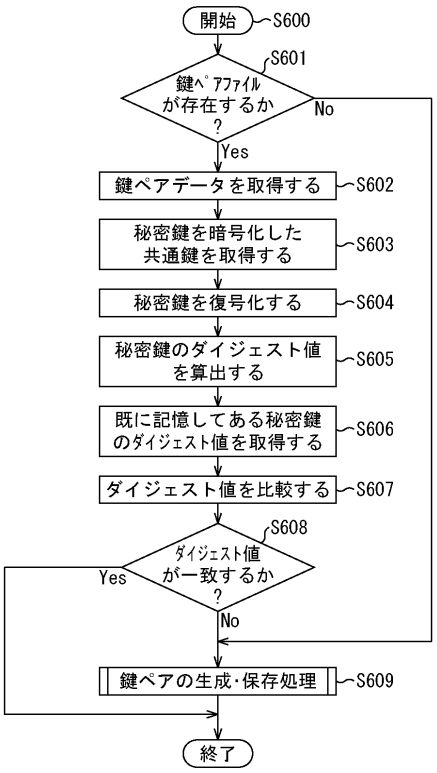
【図４】


406
暗号化処理部
405
デバイス制御部
404
アプリケーション
403
暗号化通信部
402
ネットワーク通信制御部
401
ネットワークドライバ
100

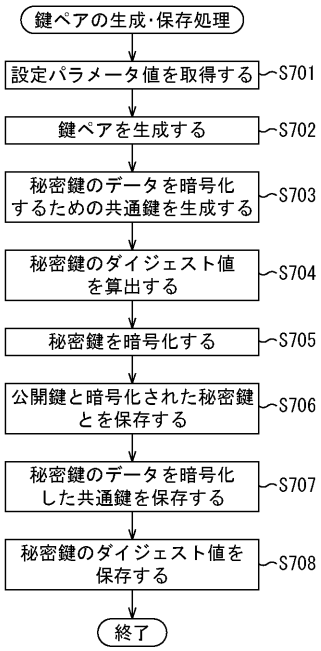
【図５】


506
暗号化処理部
507
鍵ペア生成処理部
508
鍵ペア保存処理部
505
デバイス制御部
504
アプリケーション
503
暗号化通信部
502
ネットワーク通信制御部
501
ネットワークドライバ
100

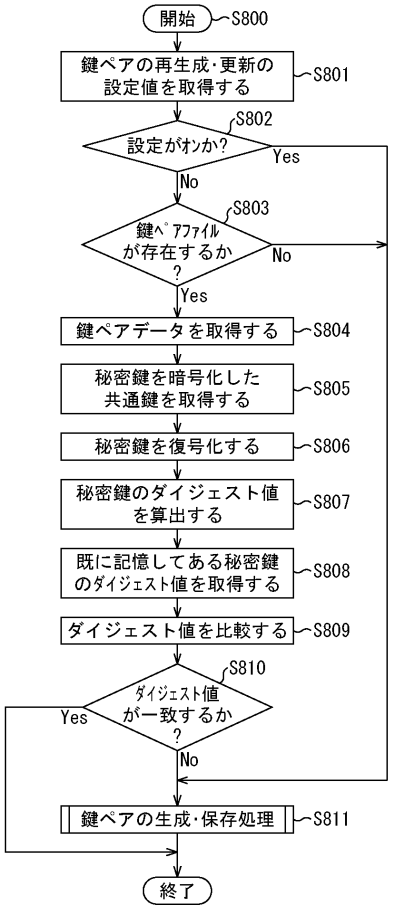
【図６】


開始
S600
S601
鍵ペアファイルが存在するか？
No
Yes
鍵ペアデータを取得する
S602
秘密鍵を暗号化した共通鍵を取得する
S603
秘密鍵を復号化する
S604
秘密鍵のダイジェスト値を算出する
S605
既に記憶してある秘密鍵のダイジェスト値を取得する
S606
ダイジェスト値を比較する
S607
S608
ダイジェスト値が一致するか？
Yes
No
鍵ペアの生成・保存処理
S609
終了

【図７】


鍵ペアの生成･保存処理
設定パラメータ値を取得する
S701
鍵ペアを生成する
S702
秘密鍵のデータを暗号化するための共通鍵を生成する
S703
秘密鍵のダイジェスト値を算出する
S704
秘密鍵を暗号化する
S705
公開鍵と暗号化された秘密鍵とを保存する
S706
秘密鍵のデータを暗号化した共通鍵を保存する
S707
秘密鍵のダイジェスト値を保存する
S708
終了

【図８】


開始
S800
鍵ペアの再生成･更新の設定値を取得する
S801
S802
設定がオンか?
Yes
No
S803
鍵ペアファイルが存在するか?
No
Yes
鍵ペアデータを取得する
S804
秘密鍵を暗号化した共通鍵を取得する
S805
秘密鍵を復号化する
S806
秘密鍵のダイジェスト値を算出する
S807
既に記憶してある秘密鍵のダイジェスト値を取得する
S808
ダイジェスト値を比較する
S809
S810
ダイジェスト値が一致するか?
Yes
No
鍵ペアの生成･保存処理
S811
終了