(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2004-32315
(P2004-32315A)
(43)公開日　平成16年1月29日(2004.1.29)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/08	H04L	9/00	601A	5B017
G06F	3/12	G06F	3/12	K	5B021
G06F	12/14	G06F	12/14	320B	5C075
H04L	9/10	H04N	1/44		5J104
H04N	1/44	H04L	9/00	621A	

審査請求 未請求　請求項の数 5　OL　（全 11 頁）

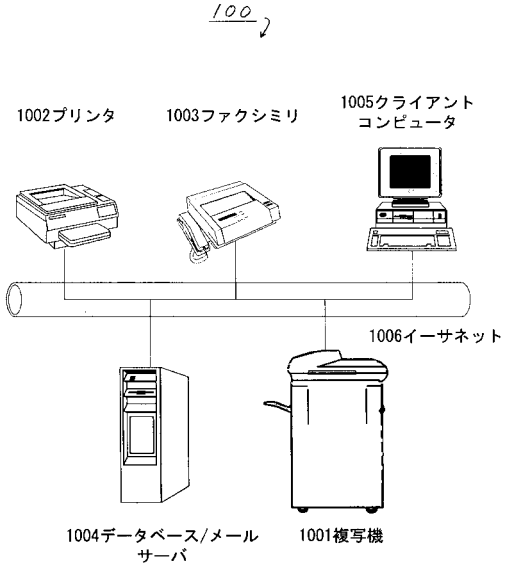
(21)出願番号　特願2002-185075(P2002-185075)
(22)出願日　平成14年6月25日(2002.6.25)

(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　内川　宙志
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)　5B017 AA03　BA07　CA12
5B021 AA19　DD00　NN18
5C075 EE02　EE03　FF03
5J104 AA12　AA16　EA19　NA37　PA14

(54)【発明の名称】デジタル複合機及び暗号化システム

(57)【要約】
【課題】デジタル複合機を利用するユーザについてのユーザ情報の保護を簡易かつ効率的に行うことを目的とする。
【解決手段】ユーザの公開鍵を不揮発性の記憶媒体に記憶し、ユーザの秘密鍵を揮発性の記憶媒体に記憶する記憶手段と、ユーザ情報を暗号復号化する手段とを備え、暗号復号化手段で暗号化しないユーザ情報を揮発性の記憶媒体に記憶する、又は公開鍵に基づき、暗号復号手段で得られた暗号化ユーザ情報を不揮発性の記憶媒体に記憶する手段と、記憶媒体に記憶されたユーザ情報を、揮発性の記憶媒体からそのまま読出すこと、又は不揮発性の記憶媒体から読出した後に秘密鍵に基づき暗号復号化手段で復号化することを実行する読出し手段とを設ける。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ユーザの公開鍵を不揮発性の記憶媒体に記憶する第１の記憶手段と、
前記ユーザの秘密鍵を揮発性の記憶媒体に記憶する第２の記憶手段と、
前記ユーザのユーザ情報を暗号又は復号化する暗号復号化手段とを備え、
前記暗号復号化手段で暗号化しない前記ユーザ情報を揮発性の記憶媒体に記憶する、又は前記第１の記憶手段で記憶された公開鍵に基づき、前記暗号復号手段で得られた暗号化ユーザ情報を不揮発性の記憶媒体に記憶する第３の記憶手段と、
第３の記憶手段で得られた前記ユーザ情報を、前記揮発性の記憶媒体から読出すこと、又は前記不揮発性の記憶媒体から読出した後に前記第２の記憶手段で記憶された秘密鍵に基づき前記暗号復号化手段で復号化することを実行する読出し手段とを設けたことを特徴とするデジタル複合機。
【請求項２】
前記ユーザ情報は、宛先アドレス、ジョブ履歴、及び画像の少なくとも何れかを含むことを特徴とする請求項１記載のデジタル複合機。
【請求項３】
ユーザ情報を揮発性又は不揮発性の記憶媒体に記憶する記憶手段と、
前記ユーザ情報を暗号化する暗号化手段と、
前記記憶手段又は暗号化手段の動作を制御する制御手段とを備え、
前記制御手段は、前記不揮発性の記憶媒体に対してのみ、前記ユーザ情報を前記暗号化手段で暗号化してから記録するように前記記憶手段の動作を制御することを特徴とするデジタル複合機。
【請求項４】
前記ユーザ情報は、宛先アドレス、ジョブ履歴、及び画像の少なくとも何れかを含むことを特徴とする請求項３記載のデジタル複合機。
【請求項５】
ユーザ情報を揮発性の記憶媒体に記憶する第１の記憶手段と、
前記ユーザ情報を不揮発性の記憶媒体に記憶する第２の記憶手段と、
前記ユーザ情報を暗号化する暗号化手段と、
前記第１の記憶手段、前記第２の記憶手段及び前記暗号化手段の動作を制御する制御手段とを備え、
前記制御手段は、前記暗号化手段で暗号化しない前記ユーザ情報を前記第１の記憶手段で記録し、前記暗号化手段で得られた暗号化ユーザ情報を前記第２の記憶手段で記憶するように制御することを特徴とする暗号化システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、例えば、コピーや、プリンタ、ファクス、電子メール、或いはファイル共有機能などを有するデジタル複合機、及びこれに用いられるユーザデータの保護に関するものである。
【０００２】
【従来の技術】
デジタル複合機は、通常、不特定多数のユーザによって使用されるものであり、文書データ等をデジタル複合機で送信する場合、送信相手の宛先アドレスやジョブ履歴などのユーザデータが、第三者に対して公知になってしまう場合がある。このため、従来より、ユーザは、上記情報（宛先アドレスやジョブ履歴等）を秘密状態にしたいという要望があった。
【０００３】
そこで、デジタル複合機は、当該複合機側に記録したユーザＩＤとパスワードの組み合わせによって、デジタル複合機を使用するユーザを認証し、認証確認を得ることができたユ

ーザに対してのみ、当該ユーザに関するデータを取得できる構成にしていた。
【０００４】
また、デジタル複合機は、その電源が切断された場合でも、送信相手の宛先アドレスや、ジョブ履歴、或いは画像などの各種ユーザデータのうち、保持が必要なデータについては不揮発性メモリへ記録し、一方、保持が不要なデータについは揮発性メモリへ記録するなど、データの種類（内容）に応じて記録している。
【０００５】
上述したように、デジタル複合機によって揮発性又は不揮発性メモリにユーザデータが記録される場合、デジタル複合機は、一般的に、そのユーザデータに対して暗号化を行わずにそのまま記録媒体上に記録することが多い。また、デジタル複合機がユーザデータを暗号化する場合でも、所定のアルゴリズムを用いたプログラムで暗号化したり、或いは不揮発性メモリに記録されたパスワードなどの対称鍵によって暗号化することが多い。
【０００６】
【発明が解決しようとする課題】
しかしながら、近年、ネットワークに接続されたコンピュータを介してデジタル複合機を利用できる状況にあり、ユーザデータを暗号化していない場合は勿論のこと、暗号化している場合でも、ユーザデータは不正ユーザによって解読される恐れがあった。
【０００７】
例えば、従来のデジタル複合機で行われているような、デジタル複合機内にユーザ認証のための情報（ユーザＩＤとパスワード）を記録し、このユーザＩＤとパスワードの組み合わせによって行うユーザ認証は、ユーザ認証情報を不正に解読しようとする不正ユーザによって、ネットワーク上に接続された任意のコンピュータからユーザ認証解読プログラムが起動された場合、解読されてしまうという問題点があった。
【０００８】
また、上述したように、従来のデジタル複合機では、電源が切断された場合でも、所定のデータは不揮発性メモリへ記録されるように構成されているが、ハードディスクドライブなどの不揮発性メモリからなる装置自体が抜き取られた場合、暗号化されていないデータに限らず、アルゴリズムやパスワードなどの対称鍵で暗号化されたデータであっても、当該暗号が解読されてしまうという恐れもあった。
【０００９】
そこで、本発明は、上記の点を鑑みてなされたもので、デジタル複合機を利用するユーザについてのユーザ情報の保護を簡易かつ効率的に行うことができる、デジタル複合機及びそれに用いられる暗号化システムを提供することを目的とする。
【００１０】
【課題を解決するための手段】
斯かる目的下において、本発明は、ユーザの公開鍵を不揮発性の記憶媒体に記憶する第１の記憶手段と、前記ユーザの秘密鍵を揮発性の記憶媒体に記憶する第２の記憶手段と、前記ユーザのユーザ情報を暗号又は復号化する暗号復号化手段とを備え、前記暗号復号化手段で暗号化しない前記ユーザ情報を揮発性の記憶媒体に記憶する、又は前記第１の記憶手段で記憶された公開鍵に基づき、前記暗号復号手段で得られた暗号化ユーザ情報を不揮発性の記憶媒体に記憶する第３の記憶手段と、第３の記憶手段で得られた前記ユーザ情報を、前記揮発性の記憶媒体から読出すこと、又は前記不揮発性の記憶媒体から読出した後に前記第２の記憶手段で記憶された秘密鍵に基づき前記暗号復号化手段で復号化することを実行する読出し手段とを設けたことを特徴とする。
【００１１】
また、本発明は、ユーザ情報を揮発性又は不揮発性の記憶媒体に記憶する記憶手段と、前記ユーザ情報を暗号化する暗号化手段と、前記記憶手段又は暗号化手段の動作を制御する制御手段とを備え、前記制御手段は、前記不揮発性の記憶媒体に対してのみ、前記ユーザ情報を前記暗号化手段で暗号化してから記録するように前記記憶手段の動作を制御することを特徴とする。

【００１２】
また、本発明は、ユーザ情報を揮発性の記憶媒体に記憶する第１の記憶手段と、前記ユーザ情報を不揮発性の記憶媒体に記憶する第２の記憶手段と、前記ユーザ情報を暗号化する暗号化手段と、前記第１の記憶手段、前記第２の記憶手段及び前記暗号化手段の動作を制御する制御手段とを備え、前記制御手段は、前記暗号化手段で暗号化しない前記ユーザ情報を前記第１の記憶手段で記録し、前記暗号化手段で得られた暗号化ユーザ情報を前記第２の記憶手段で記憶するように制御することを特徴とする。
【００１３】
【発明の実施の形態】
以下、本発明の実施の形態について図面を用いて説明する。
本発明は、例えば、図１に示すような複写機システム１００に適用される。
【００１４】
図１は、複写機システム１００の基本構成図である。
図１に示すように、複写機システム１００は、複写機１００１、プリンタ１００２、ファクシミリ１００３、データベース／メールサーバ１００４、クライアントコンピュータ１００５を含んだ構成としている。
複写機１００１は、複写対象の原稿を読み取り、当該原稿に記載されたデータを、イーサネット（Ｒ）１００６に接続されたプリンタ１００２、ファクシミリ１００３、データベース／メールサーバ１００４、及びクライアントコンピュータ１００５に送信する送信する装置である。
【００１５】
プリンタ１００２は、複写機１００１が読み取ったデータを印刷する印刷装置である。
ファクシミリ１００３は、複写機１００１が読み取ったデータをファックス送信するファクシミリ装置である。
データベース／メールサーバ１００４は、複写機１００１が読み取ったデータを格納するコンピュータである。
クライアントコンピュータ１００５は、データベースサーバ／メールサーバ１００４に接続し、データベースサーバ／メールサーバ１００４から得られたデータを表示するコンピュータである。
【００１６】
イーサネット（Ｒ）１００６は、複写機１００１、プリンタ１００２、ファクシミリ１００３、データベース／メールサーバ１００４、及びクライアントコンピュータ１００５を相互に接続するためのネットワークである。
【００１７】
図１に示す複写機１００１の構成を図２に示す。
図２に示すように、複写機１００１は、操作部２０１２、コントロールユニット（Ｃｏｎｔｒｏｌｌｅｒ　Ｕｎｉｔ）２０００、スキャナ部２０７０、及びプリンタ部２０９５を含んだ構成としている。
【００１８】
操作部２０１２では、複写機１００１に対してユーザが各種情報を設定する。
スキャナ部２０７０は、画像入力部であり、コントロールユニット２０００に対して画像データを供給する。
プリンタ部２０９５は、画像出力部であり、コントロールユニット２０００からの画像データを印刷する。
【００１９】
コントロールユニット２０００は、画像データ等の入出力制御を司るコントローラであり、スキャナ部２０７０や、プリンタ部２０９５、ＬＡＮ２０１１、或いは公衆回線（ＷＡＮ）２０５１と接続する。
【００２０】
ＣＰＵ２００１は、複写機１００１全体の動作制御をする。

ＲＡＭ２００２は、ＣＰＵ２００１が動作制御するためのシステムワークメモリであり、また、画像データを一時記憶するための画像メモリである。
ＲＯＭ２００３は、複写機１００１で起動するブートプログラムが格納されたブートＲＯＭである。
【００２１】
ＨＤＤ２００４は、複写機１００１が動作制御するためのシステムソフトウェアや画像データが格納されたハードディスクドライブである。
操作部Ｉ／Ｆ２００６は、タッチパネルを有した操作部（ＵＩ）２０１２とのインタフェース部である。操作部Ｉ／Ｆ２００６は、操作部２０１２によってユーザが入力した情報をＣＰＵ２００１に伝達し、また、操作部２０１２に表示するための画像データを出力する。
【００２２】
ネットワークインタフェース（Ｎｅｔｗｏｒｋ　Ｉ／Ｆ）２０１０は、ＬＡＮ２０１１に接続する機器又はシステムと情報の送受信をするためのインタフェースである。
モデム（Ｍｏｄｅｍ）２０５０は、公衆回線（ＷＡＮ）２０５１に接続する機器又はシステムと情報の送受信をするためのものである。
ＰＣカードスロット（ＰＣ　ＣＡＲＤ　Ｓｌｏｔ）２１００は、ＰＣ　カードメディアを複写機１００１に対して脱着可能にするもので、複写機１００１外部との間で情報の入出力を行う。
【００２３】
イメージバス（Ｉｍａｇｅ　Ｂｕｓ）Ｉ／Ｆ２００５は、システムバス２００７と画像バス２００８とを接続するためのインタフェースであり、データ構造を変換するバスブリッジでもある。
画像バス２００８は、画像データを高速で転送するバスであり、例えば、ＰＣＩバスまたはＩＥＥＥ１３９４等で構成される。画像バス２００８には、以下のデバイスが接続される。
【００２４】
ラスターイメージプロセッサ（ＲＩＰ）２０６０は、ＰＤＬコードをビットマップイメージに展開するためのプロセッサである。
デバイスＩ／Ｆ部２０２０は、画像入出力部であるスキャナ部２０７０やプリンタ部２０９５と接続するためのインタフェースであり、画像データの同期系／非同期系の変換を行う。
スキャナ画像処理部２０８０は、入力画像データに対して、補正、加工、及び編集等の画像処理を施す。
プリンタ画像処理部２０９０は、プリント出力画像データに対して、プリンタ部２０９５の補正や解像度変換等の画像処理を施す。
画像回転部２０３０は、画像データ（入力画像データやプリント出力画像データ）に対し、回転変換処理を施した画像を生成する。
画像圧縮部２０４０は、画像データに対して圧縮処理を施し、例えば、多値画像データに対してはＪＰＥＧ、２値画像データに対してはＪＢＩＧや、ＭＭＲ、或いはＭＨ等のデータ圧縮伸張処理を行う。
【００２５】
図３は、本実施の形態の複写機１００１で、ユーザデータ暗号又は解読のために用いられる非対称鍵方式の公開鍵と秘密鍵のデータ配置例を示したものである。
図３に示すように、公開鍵側は、公開鍵テーブル３００１及び公開鍵テーブル３００２に格納された公開鍵で認証したユーザの自動ログアウト時間テーブル３００２を含む構成である。この公開鍵テーブル３００１及び公開鍵テーブル３００２に格納された情報は、図２に示す複写機１００１のＨＤＤ２００４に記録されている。
【００２６】
なお、図３に示した自動ログアウト時間テーブル３００２に格納された時間（例えば、１

０分等）は、複写機１００１の正当なユーザとして認証確認されたユーザの複写機１００１に対するユーザ操作の終了、あるいは認証確認されたユーザが実行したジョブの終了から、複写機１００１側で当該ユーザが自動的にログアウトされるまでの時間を表している。

【００２７】

秘密鍵側は、複写機１００１側で認証確認されたユーザの秘密鍵テーブル３００３を含む構成であり、秘密鍵テーブル３００３に格納された秘密鍵は、図３に示す公開鍵テーブル３００１の各公開鍵とリンクしている。また、秘密鍵テーブル３００３は、図２に示す複写機１００１のＲＡＭ２００２に記録されており、ＣＰＵ２００１は、認証確認されたユーザが、複写機１００１側からログアウトするまでの間、秘密鍵テーブル３００３の内容（秘密鍵）を保持し、ログアウト時には、保持していた内容（秘密鍵）を自動的に消去する。

【００２８】

＜複写機システム１００によるユーザ認証の動作＞

ここでは、複写機システム１００によって、ユーザ認証が行われる動作について説明する。図４は、公開鍵と秘密鍵の非対称鍵方式により、複写機システム１００がユーザ認証を行うときのフローチャートである。

【００２９】

図４に示すように、ユーザが複写機１００１に対してログイン動作を開始する場合（ステップＳ４００１）、ユーザは、複写機１００１に含まれるＨＤＤ２００４に登録された公開鍵テーブル３００１の中から、自己の公開鍵を選択する（ステップＳ４００２）。

【００３０】

次に、ＣＰＵ２００１は、ユーザに対し、ユーザが選択した公開鍵に対する秘密鍵の入力要求をする（ステップＳ４００３）。そこで、ユーザは、複写機１００１のＰＣカードスロット２１００に対して、秘密鍵データを記録したＰＣカードメディアを装着する。

【００３１】

次に、ＣＰＵ２００１は、ユーザが装着したＰＣカードメディアから、秘密鍵の情報を読み込み、当該ユーザが正当なユーザであるか否かを検証するための秘密鍵の正当性チェックを行う（ステップＳ４００４）。

ＣＰＵ２００１による秘密鍵の正当性チェックは次のようにして行う。例えば、ＣＰＵ２００１は、ユーザが選択した公開鍵を用いて、先ず、任意のテストデータを暗号化し、次に、当該暗号化テストデータを、ＰＣカードメディアに記録された秘密鍵によって復号化できるか否かを検証する。

【００３２】

ＣＰＵ２００１は、上記暗号化用テストデータを復号化できないと判断した場合、これまでのユーザ認証動作をステップＳ４００２の処理まで戻し、ステップＳ４００２～ステップＳ４００４の処理を再度実行する。一方、ＣＰＵ２００１が、上記暗号化テストデータを復号化できる判断した場合、ＣＰＵ２００１は、図３に示す複写機１００１のＲＡＭ２００２内に記憶された秘密鍵テーブル３００３へ、当該ユーザの秘密鍵を複写する（ステップＳ４００５）。

【００３３】

次に、ＣＰＵ２００１は、ユーザ認証のためのログイン処理を終了する（ステップＳ４００６）。

尚、この図３に示す秘密鍵テーブル３００３は、ＤＲＡＭなどの揮発性メモリに記録されて構成しているため、例えば、電源遮断後に部品が盗難等されても、これにより秘密鍵テーブル３００３に格納された秘密鍵が漏洩することはない。

【００３４】

＜記録媒体に対するユーザデータの記録動作＞

ここでは、複写機システム１００において、記録媒体にユーザデータを記録する動作について説明する。

図５は、本実施の形態の複写機システム１００で用いられる宛先アドレスや、ジョブ履歴、或いは画像情報などのユーザデータを、記録媒体に記録する処理を示したフローチャートである。

【００３５】

尚、ユーザデータを記録媒体に記録する動作が開始されるときは、その前提として、上述した図４に示すユーザ認証処理が行われていて、ユーザは複写機システム１００よりユーザ認証を得ている必要がある。

【００３６】

ユーザデータ（宛先アドレスや、ジョブ履歴、或いは画像情報など）を記録媒体に記録する場合（ステップＳ５００１）、複写機１００１のＣＰＵ２００１は、先ず、記録媒体が不揮発性メモリであるかを確認する（ステップＳ５００２）。

【００３７】

ＣＰＵ２００１が、記録媒体を揮発性メモリであると判断した場合、次に、ＣＰＵ２００１は、公開鍵へリンクするための情報を設定しないまま、ユーザデータを当該記録媒体（揮発性メモリ）上に記録し（ステップＳ５００６）、記録動作を終了する（ステップＳ５００７）。

【００３８】

一方、ＣＰＵ２００１が、記録媒体を不揮発性メモリであると判断した場合、次に、ＣＰＵ２００１は、複写機１００１を利用しようとしている当該ユーザの公開鍵を、図３に示す公開鍵テーブル３００１から取得する（ステップＳ５００３）。

次に、ＣＰＵ２００１は、公開鍵テーブル３００１から取得した公開鍵を用いて、ユーザデータを暗号化する（ステップＳ５００４）。

次に、ＣＰＵ２００１は、公開鍵テーブル３００１に記録された公開鍵へリンクするための情報、及びステップＳ５００４で暗号化したユーザデータを記録媒体（不揮発性メモリ）に記録し（ステップＳ５００５）、その後、記録動作を終了する（ステップＳ５００７）。

【００３９】

＜記録媒体からのユーザデータの読出し動作＞

ここでは、複写機システム１００において、記録媒体からユーザデータを読出す動作について説明する。

図６は、上記図５のフローチャートで示した記録動作により記録媒体に記録されたユーザデータ（宛先アドレスや、ジョブ履歴、或いは画像等）を、読み出すときの処理を示したフローチャートである。

【００４０】

尚、ユーザデータを記録媒体から読み出す動作が開始されるときは、その前提として、上述した図４に示すユーザ認証処理が行われていて、ユーザは複写機システム１００よりユーザ認証を得ている必要がある。

【００４１】

ＣＰＵ２００１は、記録媒体からユーザデータの読み出し動作を開始する場合（ステップＳ６００１）、先ず、ユーザデータが記録されている記録媒体が不揮発性メモリであるか否かを確認する（ステップＳ６００２）。

【００４２】

ＣＰＵ２００１が、記録媒体を揮発性メモリであると判断した場合、次に、ＣＰＵ２００１は、記録媒体からそのままユーザデータを読み出し（ステップＳ６００８）、その後、読み出し動作を正常終了する（ステップＳ６００９）。

【００４３】

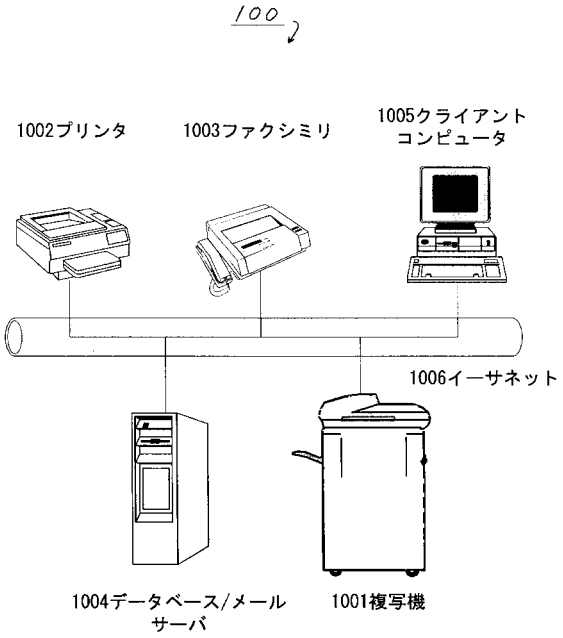
一方、ＣＰＵ２００１が、記録媒体を不揮発性メモリであると判断した場合、次に、ＣＰＵ２００１は、ユーザデータとともに、暗号化の際に不揮発性メモリの記録媒体に記録された公開鍵テーブル３００１へのリンク情報を読み出す（ステップＳ６００３）。

次に、ＣＰＵ２００１は、公開鍵に該当する秘密鍵を、図３に示す秘密鍵テーブル３００

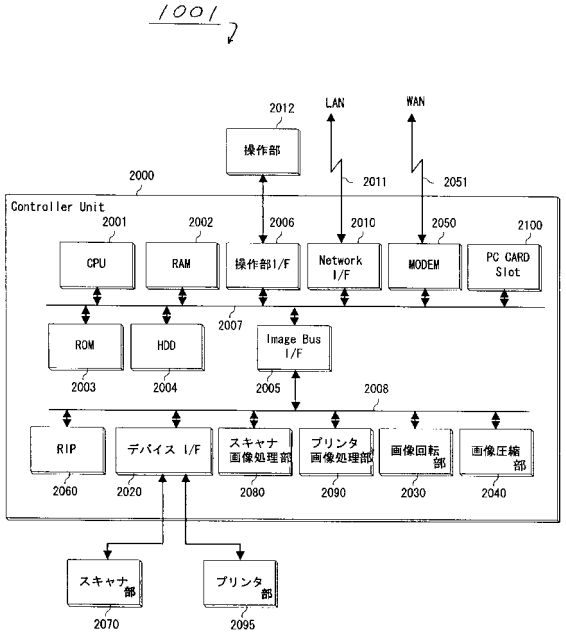
１より取得することを試みる（ステップＳ６００４）。
【００４４】
上述したように、記録媒体からユーザデータを読み出すユーザは、その前提として、複写機システム１００よりユーザ認証を得ているので、図３に示す秘密鍵テーブル３００３には、当該認証を得たユーザの秘密鍵がコピーされている。したがって、ＣＰＵ２００１は、秘密鍵テーブル３００３から秘密鍵を取得することが可能になる。
【００４５】
そこで、ＣＰＵ２００１により、当該秘密鍵を取得できた場合（ステップＳ６００５）、ＣＰＵ２００１は、ユーザデータを読み出す（ステップＳ６００６）とともに、取得した秘密鍵によってユーザデータを復号化し（ステップＳ６００７）、その後、読み出し動作を正常終了する（ステップＳ６００９）。
【００４６】
一方、ＣＰＵ２００１が、何らかの原因により秘密鍵を取得できなかった場合（ステップＳ６００５）、そのまま読み出し動作を異常終了させる（ステップＳ６０１０）。
【００４７】
【発明の効果】
以上説明したように、本発明によれば、ユーザを認証するための情報を、揮発性の記憶媒体と不揮発性の記憶媒体に分けて記憶し、不揮発性の記憶媒体に格納するユーザ情報に対してのみ暗号化又は復号化して情報の入出力を行うように構成しているので、ユーザ側に対して特別な操作負担を強いることなく、ユーザ情報の保護を簡易かつ効率的に行うことが可能となる。
【００４８】
例えば、デジタル複合機又はシステムに記録された登録ユーザＩＤ及びパスワード等の一覧リストに代わり、公開鍵及び暗号鍵の対リストによってデジタル複合機又はシステムを利用するユーザの認証を行えるように構成すれば、不正ユーザによるユーザ認証解読プログラムによって上記パスワード等が漏洩することを防止できるため、ユーザ認証チェックの強化が可能になる。
【００４９】
また、非対称鍵方式の鍵（秘密鍵）が記録される記録媒体を揮発性メモリに限定する構成にすることで、例えば、デジタル複合機又はシステム側からユーザがログアウトする時には秘密鍵が自動消去でき、また、ユーザデータが記録されたハードディスクドライブなどの不揮発性の記録媒体が盗まれた場合でも、ユーザデータが第三者に漏洩することを防止できるので、ユーザデータのセキュリティを高めることが可能となる。
【図面の簡単な説明】
【図１】本実施の形態の複写機システム１００の構成図である。
【図２】複合機１００１のブロック構成図である。
【図３】ユーザデータの暗号又は解読に用いられる非対象鍵方式の公開鍵と秘密鍵のデータ配置例を示した図である。
【図４】複写機システム１００によるユーザ認証処理のフローチャートである。
【図５】複写機システム１００において、宛先アドレスやジョブ履歴や画像などのユーザデータを、記録媒体に記録するときのフローチャートである。
【図６】図５のフローチャートにより記録された宛先アドレスやジョブ履歴や画像などのユーザデータを読み出す処理を示したフローチャートである。
【符号の説明】
１００１　　複写機
１００２　　プリンタ
１００３　　ファクシミリ
１００４　　データベース／メールサーバ
１００５　　クライアントコンピュータ
１００６　　イーサネット（Ｒ）

２０００　コントローラユニット（Ｃｏｎｔｒｏｌｌｅｒ　Ｕｎｉｔ）
２００１　ＣＰＵ
２００２　ＲＡＭ
２００３　ＲＯＭ
２００４　ハードディスク（ＨＤＤ）
２００５　Ｉｍａｇｅ　Ｂｕｓ　Ｉ／Ｆ
２００６　操作部Ｉ／Ｆ
２００７　システムバス
２００８　画像バス
２０１０　Ｎｅｔｗｏｒｋ　Ｉ／Ｆ
２０１１　ＬＡＮ
２０１２　操作部
２０２０　デバイスＩ／Ｆ
２０３０　画像回転部
２０４０　画像圧縮部
２０５０　ＭＯＤＥＭ
２０５１　ＷＡＮ
２０６０　ＲＩＰ
２０７０　スキャナ部
２０８０　スキャナ画像処理部
２０９０　プリンタ画像処理部
２０９５　プリンタ部
２１００　ＰＣ　ＣＡＲＤ　Ｓｌｏｔ
３００１　公開鍵テーブル
３００２　自動ログアウト時間テーブル
３００３　秘密鍵テーブル

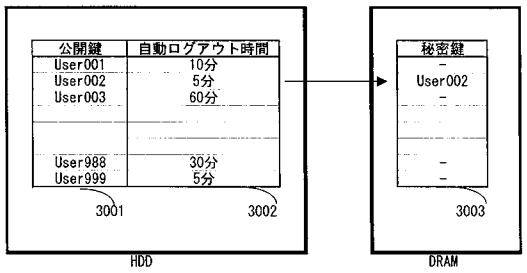
【図１】


100
1002プリンタ
1003ファクシミリ
1005クライアント
コンピュータ
1006イーサネット
1004データベース/メール
サーバ
1001複写機

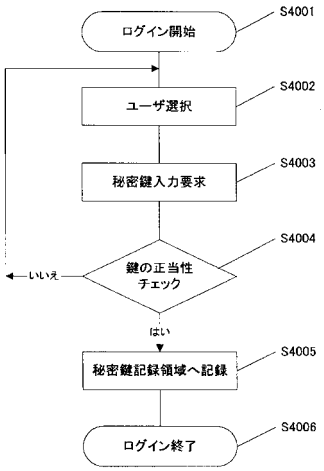
【図２】


1001
2012
操作部
LAN
WAN
2000
2011
2051
Controller Unit
2001
2002
2006
2010
2050
2100
CPU
RAM
操作部I/F
Network I/F
MODEM
PC CARD Slot
2007
ROM
HDD
Image Bus I/F
2003
2004
2005
2008
RIP
デバイス I/F
スキャナ画像処理部
プリンタ画像処理部
画像回転部
画像圧縮部
2060
2020
2080
2090
2030
2040
スキャナ部
プリンタ部
2070
2095

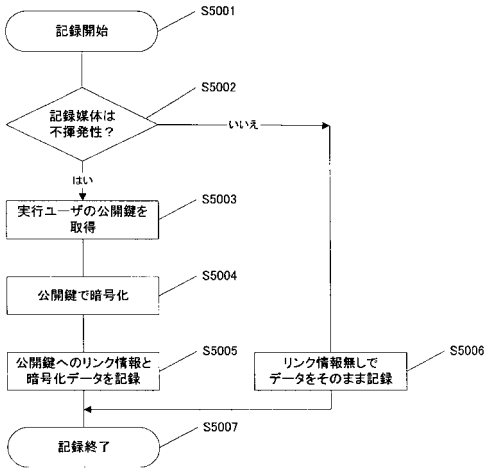
【図３】


公開鍵
自動ログアウト時間
User001
10分
User002
5分
User003
60分
User988
30分
User999
5分
3001
3002
HDD
秘密鍵
User002
3003
DRAM

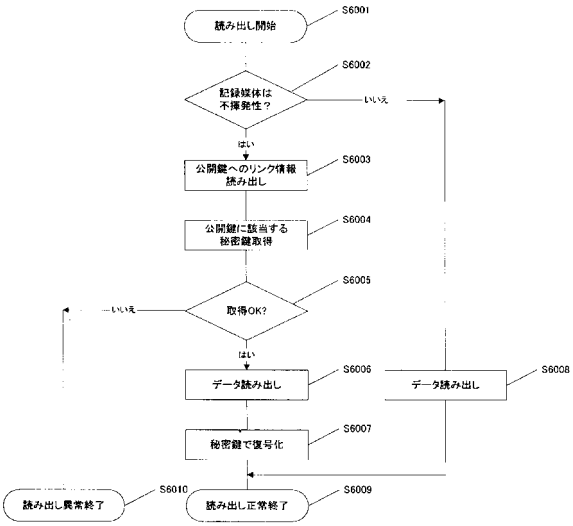
【図４】


ログイン開始
S4001
ユーザ選択
S4002
秘密鍵入力要求
S4003
鍵の正当性チェック
S4004
いいえ
はい
秘密鍵記録領域へ記録
S4005
ログイン終了
S4006

【図５】


記録開始
S5001
記録媒体は不揮発性？
S5002
いいえ
はい
実行ユーザの公開鍵を取得
S5003
公開鍵で暗号化
S5004
公開鍵へのリンク情報と暗号化データを記録
S5005
リンク情報無しでデータをそのまま記録
S5006
記録終了
S5007

【図６】


読み出し開始
S6001
記録媒体は不揮発性？
S6002
いいえ
はい
公開鍵へのリンク情報読み出し
S6003
公開鍵に該当する秘密鍵取得
S6004
取得OK?
S6005
いいえ
はい
データ読み出し
S6006
データ読み出し
S6008
秘密鍵で復号化
S6007
読み出し異常終了
S6010
読み出し正常終了
S6009