(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2004-355268
(P2004-355268A)
(43)公開日　平成16年12月16日(2004.12.16)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	320B	5B017
H04L 9/08	G06F	12/14	320F	5J104
	H04L	9/00	601A	

審査請求 未請求　請求項の数 10　ＯＬ　（全 14 頁）

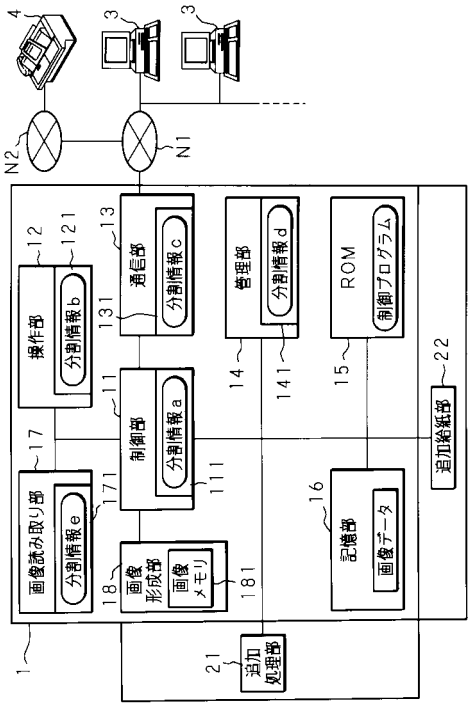
(21)出願番号　特願2003-151341(P2003-151341)
(22)出願日　平成15年5月28日(2003.5.28)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100078868
弁理士　河野　登夫
(74)代理人　100114557
弁理士　河野　英仁
(72)発明者　山中　敏弘
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内

Ｆターム(参考)　5B017 AA07 BA07 CA16
5J104 AA12 AA16 EA04 EA09 EA13
EA15 EA20 JA03 NA02 NA37
PA14

(54)【発明の名称】情報処理装置

(57)【要約】
【課題】情報を暗号化して記憶する情報処理装置にて、暗号化鍵または復号鍵の漏洩を防止する。
【解決手段】本発明の情報処理装置であるプリンタ装置１の機能を実現する構成要素である制御部１１、操作部１２、通信部１３、管理部１４、及び画像読み取り部１７は、ROMで構成された記憶領域１１１，１２１，１３１，１４１，１７１を夫々備えており、記憶領域１１１，１２１，１３１，１４１，１７１は、分割情報ａ，ｂ，ｃ，ｄ，ｅを記憶している。制御部１１は、所定のタイミングで、複数の分割情報を用いて暗号化鍵を生成し、生成した暗号化鍵を用いて画像データを暗号化して記憶部１６に記憶し、暗号化鍵を復号鍵として用いて画像データを復号して出力する。また、制御部１１は、生成した暗号化鍵を所定のタイミングで消去し、外部への暗号化鍵の取り出しを困難にする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
情報を受け付ける手段と、受け付けた情報を、暗号化鍵を用いて暗号化して記憶する情報記憶手段と、記憶している情報を、復号鍵を用いて復号して処理する手段とを備える情報処理装置において、
前記暗号化鍵又は前記復号鍵の素を分割した複数の分割情報の夫々を個別に記憶する記憶手段と、
複数の前記分割情報を用いて前記暗号化鍵又は前記復号鍵を生成する生成手段と
を備えることを特徴とする情報処理装置。
【請求項２】
必要な機能を実現する複数の必須構成要素と、追加の機能を実現する着脱可能な一又は複数の追加構成要素とから構成されており、
前記記憶手段は、複数の前記分割情報のいずれかを記憶する複数の個別記憶手段を備え、
前記個別記憶手段は、複数の前記必須構成要素のいずれかに設けられてあることを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記生成手段は、それの起動時に前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
情報の処理を行うことが可能な状態であるか否かを判定する手段を更に備え、
前記生成手段は、情報の処理を行うことが可能な状態になったと判定した場合に、前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項５】
前記生成手段は、情報を暗号化又は復号するときに前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする請求項１又は２に記載の情報処理装置。
【請求項６】
情報の処理を停止するときに、前記暗号化鍵又は前記復号鍵を無効化する手段を更に備えることを特徴とする請求項１乃至５のいずれか一つに記載の情報処理装置。
【請求項７】
情報の処理が不可能になったことを検出する手段と、
情報の処理が不可能になったことを検出した場合に、前記暗号化鍵又は前記復号鍵を無効化する手段と
を更に備えることを特徴とする請求項１乃至５のいずれか一つに記載の情報処理装置。
【請求項８】
情報の暗号化又は復号を行ったときに、前記暗号化鍵又は前記復号鍵を無効化する手段を更に備えることを特徴とする請求項５に記載の情報処理装置。
【請求項９】
前記情報記憶手段は、画像データを記憶すべくなしてあることを特徴とする請求項１乃至８のいずれか一つに記載の情報処理装置。
【請求項１０】
画像の複写を行う手段、ファクシミリ通信を行う手段、画像のプリントを行う手段、又は画像をスキャンして取り込む手段のうち、いずれかを備えていることを特徴とする請求項１乃至９のいずれか一つに記載の情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、受け付けた情報を暗号化して記憶し、記憶している情報を復号して処理する情報処理装置に関する。
【０００２】

【従来の技術】
近年のプリンタ装置の多くは、通信ネットワークに接続され、該通信ネットワークに接続されたパーソナルコンピュータ（ＰＣ）等の他の装置から画像データを受信して画像を出力するネットワークプリンタの機能を備えている。更に、用紙に記録された画像を走査して画像データとして取り込み、取り込んだ画像データに基づいて画像を形成して出力する複写機能、ファクシミリ通信を用いて外部のファクシミリ装置との間で画像データを送受信するファクシミリ機能、及び取り込んだ画像データを外部の装置へ送信する送信機能など、複数の機能をプリンタ装置に備えた複合機が商品化されている。このような機能の複合化が進んだプリンタ装置では、各機能における画像データの処理を停滞させることなく行うために、画像データ等の情報を記憶するハードディスク等の記憶手段を備え、受け付けた情報を順次記憶する一方、既に記憶手段に記憶されている情報を順次処理していく並行処理機能を備えている。
【０００３】
更に、以上の如きプリンタ装置が備える記憶手段の機能を充実させ、スキャナを用いて取り込んだ画像データ、又は外部のＰＣから受信した画像データ等の画像データを記憶手段に記憶しておき、外部からの出力指示に応じて、用紙に記録された画像として出力する、又は外部のＰＣ等の装置へ画像データを送信する等、記憶された画像データを外部へ出力することを可能にして、画像データのサーバ装置として利用することができるプリンタ装置が実現されている。このようなプリンタ装置を使用することで、一度利用した画像データの再利用が可能となり、使用者は、文章または画像を必要なときに利用することができる。
【０００４】
一方で、プリンタ装置が扱う画像データには、企業秘密を記載した文章などの機密性を有する画像データが含まれる場合があり、プリンタ装置において、画像データの無制限な記憶、及び通信ネットワークに接続された複数のＰＣ等の他の装置からの無制限な画像データの利用を可能にしたときには、情報の漏洩、又は情報の不正使用などのセキュリティ上の問題が発生する。そこで、特許文献１では、画像データを扱う際に、利用者の認証を行って画像データの利用者を制限する技術が開示されており、また、特許文献２では、蓄積される画像データを暗号化しておき、不正な読み出しを困難にする技術が開示されている。
【０００５】
【特許文献１】
特開平４－１９６７５１号公報
【特許文献２】
特開平５－９５４５３号公報
【特許文献３】
特開２０００－１８３８６７号公報
【特許文献４】
特開２００１－２５１２９３号公報
【０００６】
【発明が解決しようとする課題】
プリンタ装置において、利用者の認証を行って画像データの利用者を制限する技術を用いた場合、利用者を認証するためのパスワード等の情報は利用者個人が管理することとなり、前記情報を他者に知られたときには、画像データの利用が許可されていない他者がなりすましによって画像データを利用することが可能となる。また、蓄積される画像データを暗号化する技術を用いた場合、プリンタ装置は、暗号化された画像データを復号するための復号鍵を記憶しており、復号鍵を記憶している記憶手段を取り外して復号鍵を読み出す等の方法により、復号鍵を不正に外部へ取り出されたときには、画像データを不正に読み出すことが可能となる。このように、利用者の制限、又は画像データの暗号化を行うだけでは、情報の漏洩、又は情報の不正使用などのセキュリティ上の問題を防止することは困

難である。
【０００７】
暗号化鍵を外部に漏らさないようにしてセキュリティをより向上させる技術として、特許文献３では、暗号化鍵を、不揮発性のメモリに記憶しておき、装置の不正な持ち出し等により電源が遮断されたときにメモリに記憶してある暗号化鍵が消去される技術が開示されており、また、特許文献４では、暗号化鍵を記憶している記憶装置に、物理的攻撃などの外部からの不正な攻撃があった場合に、暗号化鍵を消去する技術が開示されている。また、他の方法として、暗号化鍵又は復号鍵を、時刻などの情報に基づいて毎回変更する方法も考えられるが、画像データを記憶しておいて再利用する装置では、暗号化鍵を変更することができない。
【０００８】
本発明は、斯かる事情に鑑みてなされたものであって、その目的とするところは、暗号化鍵または復号鍵を直接に記憶せず、暗号化鍵または復号鍵の素を分割した複数の分割情報を分散して記憶することにより、暗号化鍵または復号鍵の漏洩を防止できる情報処理装置を提供することにある。
【０００９】
【課題を解決するための手段】
本発明に係る情報処理装置は、情報を受け付ける手段と、受け付けた情報を、暗号化鍵を用いて暗号化して記憶する情報記憶手段と、記憶している情報を、復号鍵を用いて復号して処理する手段とを備える情報処理装置において、前記暗号化鍵又は前記復号鍵の素を分割した複数の分割情報の夫々を個別に記憶する記憶手段と、複数の前記分割情報から前記暗号化鍵又は前記復号鍵を生成する生成手段とを備えることを特徴とする。
【００１０】
本発明においては、受け付けた情報を暗号化して記憶し、記憶している情報を復号して処理する情報処理装置にて、暗号化鍵又は復号鍵の素を分割した複数の分割情報を記憶しておき、複数の分割情報を用いて暗号化鍵又は復号鍵を生成することにより、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせる。
【００１１】
本発明に係る情報処理装置は、必要な機能を実現する複数の必須構成要素と、追加の機能を実現する着脱可能な一又は複数の追加構成要素とから構成されており、前記記憶手段は、複数の前記分割情報のいずれかを記憶する複数の個別記憶手段を備え、前記個別記憶手段は、複数の前記必須構成要素のいずれかに設けられてあることを特徴とする。
【００１２】
また、本発明においては、複数の分割情報の夫々を、情報処理装置の必須構成要素に分散して記憶することにより、暗号化鍵又は復号鍵の外部への取り出しを困難にすると共に、確実に暗号化鍵又は復号鍵を生成する。
【００１３】
本発明に係る情報処理装置は、前記生成手段は、それの起動時に前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする。
【００１４】
また、本発明においては、電源を投入して情報処理装置が起動するときに暗号化鍵又は復号鍵を生成することにより、情報処理装置が起動する前には内部に暗号化鍵又は復号鍵が存在しなくなり、起動前に暗号化鍵又は復号鍵を外部へ取り出すことができない。
【００１５】
本発明に係る情報処理装置は、情報の処理を行うことが可能な状態であるか否かを判定する手段を更に備え、前記生成手段は、情報の処理を行うことが可能な状態になったと判定した場合に、前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする。
【００１６】
また、本発明においては、情報の処理が可能な状態であるときに暗号化鍵又は復号鍵を生成することにより、情報の処理が不可能な状態では内部に暗号化鍵又は復号鍵が存在しな

くなり、情報の処理を行う前に暗号化鍵又は復号鍵を外部へ取り出すことができない。
【００１７】
本発明に係る情報処理装置は、前記生成手段は、情報を暗号化又は復号するときに前記暗号化鍵又は前記復号鍵を生成すべくなしてあることを特徴とする。
【００１８】
また、本発明においては、情報の処理を行うために暗号化または復号を行うときに暗号化鍵又は復号鍵を生成することにより、暗号化鍵又は復号鍵が存在する期間が限定される。
【００１９】
本発明に係る情報処理装置は、情報の処理を停止するときに、前記暗号化鍵又は前記復号鍵を無効化する手段を更に備えることを特徴とする。
【００２０】
また、本発明においては、電源を遮断して情報処理装置が停止するときに暗号化鍵又は復号鍵を消去するなどして無効化することにより、情報処理装置が停止した後には内部に暗号化鍵又は復号鍵が存在しなくなり、停止後に暗号化鍵又は復号鍵を外部へ取り出すことができない。
【００２１】
本発明に係る情報処理装置は、情報の処理が不可能になったことを検出する手段と、情報の処理が不可能になったことを検出した場合に、前記暗号化鍵又は前記復号鍵を無効化する手段とを更に備えることを特徴とする。
【００２２】
また、本発明においては、トラブル等により情報の処理が不可能な状態となった場合に暗号化鍵又は復号鍵を消去するなどして無効化することにより、情報の処理が不可能になった状態では内部に暗号化鍵又は復号鍵が存在しなくなり、トラブル等による処理の停止中に暗号化鍵又は復号鍵を外部へ取り出すことができない。
【００２３】
本発明に係る情報処理装置は、情報の暗号化又は復号を行ったときに、前記暗号化鍵又は前記復号鍵を無効化する手段を更に備えることを特徴とする。
【００２４】
また、本発明においては、情報の暗号化又は復号を行った後は、用いた暗号化鍵又は復号鍵を消去するなどして速やかに無効化することにより、暗号化鍵又は復号鍵が存在する期間が限定される。
【００２５】
本発明に係る情報処理装置は、前記情報記憶手段は、画像データを記憶すべくなしてあることを特徴とする。
【００２６】
また、本発明においては、情報処理装置は、暗号化で保護された画像データを記憶し、記憶している画像データを利用可能に提供する。
【００２７】
本発明に係る情報処理装置は、画像の複写を行う手段、ファクシミリ通信を行う手段、画像のプリントを行う手段、又は画像をスキャンして取り込む手段のうち、いずれかを備えていることを特徴とする。
【００２８】
更に、本発明においては、情報処理装置は、コピー装置、ファクシミリ装置、プリンタ装置、又はスキャナ装置である。
【００２９】
【発明の実施の形態】
以下本発明をその実施の形態を示す図面に基づき具体的に説明する。
図１は、本発明の情報処理装置であるプリンタ装置の内部の構成を示すブロック図である。プリンタ装置１は、本発明の情報処理装置であり、演算を行うＣＰＵ及び演算に伴う一時的な情報を記憶するＲＡＭ等からなる制御部１１を備え、制御部１１には、プリンタ装

置１の制御を行うための制御プログラムを記憶しているＲＯＭ１５が接続されており、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、プリンタ装置１全体の制御を行う。また、制御部１１には、プリンタ装置１が行う処理を管理するための管理情報を記憶する不揮発性のメモリである管理部１４が接続されており、制御部１１は、管理部１４が記憶している管理情報を参照し、参照した情報に基づいてプリンタ装置１の制御を行う。また、制御部１１には、用紙に記録された画像を走査して読み取り、読みとった画像に基づいた電子的な画像データを生成する画像読み取り部１７と、画像データを一時的に記憶する画像メモリ１８１を内部に備え、画像メモリ１８１が記憶している画像データから画像を形成し、形成した画像を記録用紙に記録して出力する画像形成部１８とが接続されており、プリンタ装置１は、画像読み取り部１７にて読みとった画像を複写する複写装置として機能する。また、制御部１１には、ハードディスク又は不揮発性のメモリからなる記憶部１６が接続されている。記憶部１６は、本発明に係る情報記憶手段であり、記憶部１６は、画像データを暗号化して記憶する。また、制御部１１には、使用者からの操作を受け付ける操作部１２が接続されており、操作部１２は、操作のために必要な情報を表示する液晶パネル等の表示手段と、使用者の操作により制御命令などの情報が入力されるタッチパネル又はテンキー等の入力手段とからなっている。

【００３０】

また、制御部１１には、ＬＡＮ等の外部の通信ネットワークＮ１に接続された通信部１３が接続されており、通信部１３は、通信ネットワークＮ１を介して、外部との間で情報を交換する。通信ネットワークＮ１には、複数のＰＣ３，３，…が接続されており、通信部１３は、ＰＣ３から送信された画像データを通信ネットワークＮ１を介して受信し、画像形成部１８は、通信部１３が受信した画像データから画像を形成して出力することができ、プリンタ装置１は、ネットワークプリンタとして機能する。また、プリンタ装置１は、画像読み取り部１７が画像を読みとって生成した画像データを通信部１３から通信ネットワークＮ１を介してＰＣ３へ送信することができ、ネットワークスキャナとして機能する。また、通信部１３は、ファクシミリ通信を行うことが可能であり、通信ネットワークＮ１に接続された公衆回線網Ｎ２を介して、画像読み取り部１７が画像を読みとって生成した画像データを、公衆回線網Ｎ２に接続された他のファクシミリ装置４へファクシミリ通信にて送信することができる。また、ファクシミリ装置４からファクシミリ通信にて送信された画像データを、公衆回線網Ｎ２を介して受信し、画像形成部１８は通信部１３が受信した画像データから画像を形成して出力することができる。

【００３１】

記憶部１６は、複写、ファクシミリ送受信、画像出力、及び画像読み取り等で使用した画像データを暗号化して記憶している。記憶部１６は、画像データを、処理を行った時刻の順、処理のモードごと、又は使用者が作成したフォルダごと等に整理して記憶しており、出力の失敗または出力部数の不足のために一度出力した画像をもう一度出力する必要がある場合等に、処理を行った画像データを再利用することができる。使用者は、操作部１２での操作により、又はＰＣ３から処理命令を送信することにより、記憶部１６が記憶している画像データを選択し、画像形成部１９での画像の出力、又は通信部１３から外部への画像データの送信などを行って、記憶部１６が記憶している画像データを利用することができる。このように記憶部１６が画像データを蓄積することにより、プリンタ装置１は、画像データのサーバ装置として機能する。

【００３２】

更に、制御部１１には、記録用紙への両面印刷または記録用紙のステープル止め等の処理を行う追加処理部２１、及び大量の記録用紙の供給を可能とする追加給紙部２２が接続されている。追加処理部２１及び追加給紙部２２は、本発明に係る追加構成要素であり、プリンタ装置１に対して着脱可能に構成され、プリンタ装置１に対して追加の機能を実現する。また、制御部１１、操作部１２、通信部１３、管理部１４、ＲＯＭ１５、記憶部１６、画像読み取り部１７、及び画像形成部１８は、本発明に係る必須構成要素であり、プリンタ装置１に必要な機能を実現する。

【００３３】
本発明に係る必須構成要素である制御部１１、操作部１２、通信部１３、管理部１４、及び画像読み取り部１７は、ＲＯＭで構成された記憶領域１１１，１２１，１３１，１４１，１７１を備えており、記憶領域１１１，１２１，１３１，１４１，１７１は、本発明の個別記憶手段であり、また、分割情報ａ，ｂ，ｃ，ｄ，ｅを記憶している。本発明においては、これら複数の分割情報を所定の関数を用いる等して組み合わせることにより、本発明に係る暗号化鍵を生成し、生成した暗号化鍵を用いて画像データを暗号化し、暗号化した画像データを記憶部１６に記憶する。ここで、生成する暗号化鍵は、共通鍵方式の暗号化鍵であり、暗号化した画像データを復号するための復号鍵としても利用される。
【００３４】
次に、本発明の情報処理装置であるプリンタ装置１が行う処理をフローチャートを用いて説明する。図２は、本発明の情報処理装置であるプリンタ装置１が起動時に行う処理の手順を示すフローチャートである。プリンタ装置１の電源が投入された後（Ｓ１１）、制御部１１は、ＲＯＭ１５に記憶している制御プログラムに従って、プリンタ装置１を構成している各種の機器、及びプログラムの状態をチェックし（Ｓ１２）、チェックにより何らかの異常が確認された場合は（Ｓ１３：ＹＥＳ）、制御部１１は、操作部１２にてエラーを出力して（Ｓ１４）、処理を終了し、チェックにより異常が確認されなかった場合は（Ｓ１３：ＮＯ）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、プリンタ装置１のウォームアップを開始する（Ｓ１５）。制御部１１は、次に、ＲＯＭ１５に記憶している制御プログラムに従って、制御部１１、操作部１２、通信部１３、管理部１４、及び画像読み取り部１７が備えている記憶領域１１１，１２１，１３１，１４１，１７１から、分割情報ａ，ｂ，ｃ，ｄ，ｅを収集し（Ｓ１６）、収集した分割情報ａ，ｂ，ｃ，ｄ，ｅを所定の方法で組み合わせて本発明に係る暗号化鍵を生成し（Ｓ１７）、生成した暗号化鍵を管理部１４に記憶する（Ｓ１８）。制御部１１は、次に、ＲＯＭ１５が記憶している制御プログラムに従って、プリンタ装置１のウォームアップを完了し（Ｓ１９）、起動時の処理を終了する。
【００３５】
本発明では、プリンタ装置１は、以上の如き処理にて、起動時に分割情報ａ，ｂ，ｃ，ｄ，ｅから暗号化鍵を生成し、情報の処理で利用すべく暗号化鍵を記憶しておく。また、電源を遮断する等して、情報の処理を停止するときは、プリンタ装置１は、操作部１２にて使用者の操作により処理の停止の指示を受け付け、管理部１４に記憶している暗号化鍵を消去し、処理を停止する。
【００３６】
以上の如く、本発明においては、複数の分割情報がプリンタ装置１の内部に分散して記憶され、プリンタ装置１の起動時に分割情報から暗号化鍵が生成されるため、プリンタ装置１の起動前には、内部に暗号化鍵が存在せず、暗号化鍵を外部へ取り出すことが困難となり、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。また、プリンタ装置１が処理を停止するときに暗号化鍵を消去するため、プリンタ装置１の停止後には、内部に暗号化鍵が存在せず、暗号化鍵を外部へ取り出すことが困難となり、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。更に、分割情報は、着脱可能なオプション機器である追加構成要素ではなく、最小構成要素の中に分散して記憶しているため、暗号化鍵を外部へ取り出すことを困難にすると共に、任意のオプション機器を備えたどのような構成であっても、プリンタ装置１は、確実に暗号化鍵を生成して情報の処理を行うことができる。
【００３７】
プリンタ装置１は、画像形成部１８を用いた画像出力など、画像データを出力する処理を行う際に、処理に係る画像データを記憶部１６に記憶する。図３は、本発明の情報処理装置であるプリンタ装置１が行う画像データ出力の処理の手順を示すフローチャートである。プリンタ装置１は、画像の複写、画像のスキャン、画像の出力、又はファクシミリ送受信などの画像データの出力の指示を、使用者の操作により操作部１２にて受け付けるか、

又は通信ネットワークＮ１を介してＰＣ３若しくはファクシミリ装置４から通信部１３にて受信することにより受け付け、また、処理すべき画像データを、画像読み取り部１７にて画像を読み取って生成することにより受け付けるか、又は通信ネットワークＮ１を介してＰＣ３若しくはファクシミリ装置４から通信部１３にて受信することにより受け付ける（Ｓ２１）。プリンタ装置１の制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、管理部１４に記憶している暗号化鍵を読み出し（Ｓ２２）、読み出した暗号化鍵を用いて、受け付けた画像データを暗号化し（Ｓ２３）、暗号化した画像データを画像メモリ１８１に記憶し（Ｓ２４）、また、暗号化した画像データを記憶部１６に記憶する（Ｓ２５）。制御部１１は、次に、ＲＯＭ１５が記憶している制御プログラムに従って、暗号化鍵を復号鍵として用いて、画像メモリ１８１に記憶した画像データを復号し（Ｓ２６）、復号した画像データから画像形成部１８にて画像を形成して記録用紙に記録して出力する、復号した画像データを通信部１３から通信ネットワークＮ１を介してＰＣ３へ送信する、又は復号した画像データをファクシミリ通信にて通信部１３から通信ネットワークＮ１及び公衆回線網Ｎ２を介してファクシミリ装置４へ送信する等して、復号した画像データを出力し（Ｓ２７）、処理を終了する。以上の処理により、暗号化された画像データが記憶部１６に記憶される。

【００３８】

プリンタ装置１の記憶部１６に記憶された画像データは、プリンタ装置１が操作の指示を受け付けることで再度の処理を行うことが可能である。図４は、記憶部１６に記憶された画像データを処理する手順を示すフローチャートである。プリンタ装置１は、記憶部１６に記憶している画像データについて、削除、記憶部１６内での移動、画像出力、ＰＣ３への送信、及びファクシミリの送信などの画像データの処理の指示を、使用者の操作により操作部１２にて受け付けるか、又は通信ネットワークＮ１を介してＰＣ３から通信部１３にて受信することにより受け付ける（Ｓ３１）。プリンタ装置１の制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、受け付けた処理の指示が、画像データの復号が必要となる画像データの出力の指示であるか否かを判定し（Ｓ３２）、受け付けた処理の指示が、画像データの削除または記憶部１６内での移動など、画像データの復号が必要でない、出力以外の処理であった場合は（Ｓ３２：ＮＯ）、受け付けた処理の指示に従って、画像データの削除または移動などの処理を行い（Ｓ３３）、処理を終了する。受け付けた処理の指示が出力の処理であった場合は（Ｓ３２：ＹＥＳ）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、管理部１４に記憶している暗号化鍵を読み出し（Ｓ３４）、受け付けた処理の指示に指定された画像データを記憶部１６から読み出し（Ｓ３５）、読み出した暗号化鍵を復号鍵として用いて、読み出した画像データを復号し（Ｓ３６）、画像形成部１８にて画像出力、通信部１３からＰＣ３へ送信、又はファクシミリ通信にてファクシミリ装置４へ送信する等して、復号した画像データを出力し（Ｓ３７）、処理を終了する。

【００３９】

以上の如く、本発明においては、暗号化によって保護された画像データを蓄積し、情報の機密性を保持しながら、蓄積された画像データを有効に利用することができる。

【００４０】

本発明では、プリンタ装置１がトラブルなどで情報を処理することが不可能となった場合、管理部１４に記憶している暗号化鍵が漏洩することを防止するために、暗号化鍵を消去する。図５は、本発明の情報処理装置であるプリンタ装置１が行う暗号化鍵の消去および再生成の処理を示すフローチャートである。制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、定期的にプリンタ装置１の状態をチェックし（Ｓ４１）、プリンタ装置１の状態が正常で情報の処理が可能な状態であるか、又は、紙詰まりなどのトラブル、若しくは省電力のために一部の機能が停止している状態など、プリンタ装置１の状態が情報の処理が可能な状態であるかを判定し（Ｓ４２）、情報の処理が可能な状態である場合は（Ｓ４２：ＹＥＳ）、引き続きステップＳ４１の状態チェックの処理を定期的に行う。トラブル又は省電力の状態などでプリンタ装置１の状態が情報の処理が不可能な状態

である場合は（Ｓ４２：ＮＯ）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、管理部１４に記憶している暗号化鍵を消去する（Ｓ４３）。制御部１１は、次に、ＲＯＭ１５が記憶している制御プログラムに従って、定期的にプリンタ装置１の状態をチェックし（Ｓ４４）、紙詰まりなどのトラブルが解消する、又は省電力で一部の機能が停止している状態が解除される等、プリンタ装置１の状態が情報の処理が可能な状態へ戻ったか否かを判定し（Ｓ４５）、プリンタ装置１の状態が依然として情報の処理が不可能な状態である場合は（Ｓ４５：ＮＯ）、引き続きステップＳ４４の状態チェックの処理を定期的に行う。プリンタ装置１の状態が情報の処理が可能な状態へ戻っている場合は（Ｓ４５：ＹＥＳ）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、記憶領域１１１，１２１，１３１，１４１，１７１から、分割情報ａ，ｂ，ｃ，ｄ，ｅを収集し（Ｓ４６）、収集した分割情報ａ，ｂ，ｃ，ｄ，ｅから暗号化鍵を生成し（Ｓ４７）、生成した暗号化鍵を管理部１４に記憶する（Ｓ４８）。制御部１１は、次に、ＲＯＭ１５が記憶している制御プログラムに従って、情報の処理を再開し（Ｓ４９）、暗号鍵の再生成の処理を終了する。

【００４１】

以上の如く、本発明においては、トラブルによる処理の停止状態、又は省電力状態などで情報の処理が不可能な状態である場合に、プリンタ装置１が記憶している暗号化鍵を消去し、情報の処理が可能となった段階で再び暗号化鍵を生成するため、トラブル等でプリンタ装置１が情報の処理を行えない状態では、内部に暗号化鍵が存在せず、暗号化鍵を外部へ取り出すことが困難となり、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。なお、暗号化鍵を消去する以外に、無意味なデータを暗号化鍵に上書きする等、暗号化鍵を無効化する他の方法を用いてもよい。

【００４２】

以上詳述した実施の形態においては、一度生成した暗号化鍵を管理部１４に記憶しておき、必要時に管理部１４から暗号化鍵を読み出して利用する方法を用いているが、暗号化鍵を利用するときに暗号化鍵を生成し、暗号化鍵の利用が終了したときに暗号化鍵を消去する方法を用いてもよい。図６は、本発明の情報処理装置であるプリンタ装置１が行う画像データ出力の処理の他の例の手順を示すフローチャートである。プリンタ装置１は、画像の複写、画像のスキャン、画像の出力、又はファクシミリ送受信などの画像データの出力の指示を、操作部１２、又は通信部１３にて受け付け、また、処理すべき画像データを、画像読み取り部１７又は通信部１３にて受け付け（Ｓ５１）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、記憶領域１１１，１２１，１３１，１４１，１７１から、分割情報ａ，ｂ，ｃ，ｄ，ｅを収集し（Ｓ５２）、収集した分割情報ａ，ｂ，ｃ，ｄ，ｅから暗号化鍵を生成し（Ｓ５３）、生成した暗号化鍵を用いて、受け付けた画像データを暗号化し（Ｓ５４）、暗号化した画像データを画像メモリ１８１に記憶し（Ｓ５５）、また、暗号化した画像データを記憶部１６に記憶する（Ｓ５６）。制御部１１は、次に、ＲＯＭ１５が記憶している制御プログラムに従って、暗号化鍵を復号鍵として用いて、画像メモリ１８１に記憶した画像データを復号し（Ｓ５７）、画像形成部１８にて画像出力、通信部１３からＰＣ３へ送信、又はファクシミリ通信にてファクシミリ装置４へ送信する等して、復号した画像データを出力し（Ｓ５８）、生成した暗号化鍵を消去し（Ｓ５９）、処理を終了する。

【００４３】

図７は、記憶部１６に記憶された画像データを処理する手順の他の例を示すフローチャートである。プリンタ装置１は、記憶部１６に記憶している画像データの処理の指示を、操作部１２又は通信部１３にて受け付け（Ｓ６１）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、受け付けた処理の指示が、画像データの復号が必要となる画像データの出力の指示であるか否かを判定し（Ｓ６２）、受け付けた処理の指示が、画像データの削除または記憶部１６内での移動など、画像データの復号が必要でない、出力以外の処理であった場合は（Ｓ６２：ＮＯ）、受け付けた処理の指示に従って、画像データの削除または移動などの処理を行い（Ｓ６３）、処理を終了する。受け付けた処理の指

示が出力の処理であった場合は（Ｓ６２：ＹＥＳ）、制御部１１は、ＲＯＭ１５が記憶している制御プログラムに従って、記憶領域１１１，１２１，１３１，１４１，１７１から、分割情報ａ，ｂ，ｃ，ｄ，ｅを収集し（Ｓ６４）、収集した分割情報ａ，ｂ，ｃ，ｄ，ｅから暗号化鍵である復号鍵を生成し（Ｓ６５）、受け付けた処理の指示に指定された画像データを記憶部１６から読み出し（Ｓ６６）、生成した復号鍵を用いて、読み出した画像データを復号し（Ｓ６７）、画像形成部１８にて画像出力、通信部１３からＰＣ３へ送信、又はファクシミリ通信にてファクシミリ装置４へ送信する等して、復号した画像データを出力し（Ｓ６８）、生成した復号鍵を消去し（Ｓ６９）、処理を終了する。

【００４４】

以上の如く、この場合においては、情報の処理を行うために暗号化または復号を行うときに暗号化鍵又は復号鍵を生成し、情報の暗号化又は復号を行った後は、暗号化鍵又は復号鍵を速やかに消去するため、暗号化鍵又は復号鍵がプリンタ装置１内部に存在する期間が更に限定され、暗号化鍵を外部へ取り出すことがより困難となり、暗号化鍵の漏洩を防止して情報のセキュリティがより向上する。

【００４５】

なお、本実施の形態においては、暗号化鍵は共通鍵方式の暗号化鍵であり、復号鍵と共通した暗号化鍵を用いる方法を示したが、これに限るものではなく、暗号化鍵と復号鍵とが異なる方式を用い、暗号化鍵と復号鍵とを夫々個別に生成する方法を用いてもよい。また、本実施の形態においては、記憶部１６は、ハードディスクである形態を示したが、これに限るものではなく、不揮発性の半導体メモリ、リムーバルディスク等、他の形態の記憶手段を用いてもよい。

【００４６】

また、本実施の形態においては、画像読み取り部１７を必須構成要素としているが、これに限るものではなく、本発明の情報処理装置であるプリンタ装置１は、画像読み取り部１７を着脱可能な追加構成要素とした形態であってもよい。この場合は、画像読み取り部１７は分割情報を記憶せず、他の必須構成要素が分割情報を記憶することによって、本発明を実現することができる。

【００４７】

また、本実施の形態においては、本発明の情報処理装置は、プリンタ装置、複写装置およびファクシミリ装置などの複数の機能を備えた復号型の装置であるとしたが、これに限るものではなく、本発明の情報処理装置は、プリンタ装置のみ、複写装置のみ及びファクシミリ装置のみ等、単機能の装置であってもよく、また、通信部１３及び記憶部１６を備えて画像データを記憶するストレージ装置であってもよい。

【００４８】

【発明の効果】

本発明においては、受け付けた情報を暗号化して記憶し、記憶している情報を復号して処理する情報処理装置にて、暗号化鍵又は復号鍵の素を分割した複数の分割情報を記憶しておき、複数の分割情報を用いて暗号化鍵又は復号鍵を生成することにより、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。

【００４９】

また、本発明においては、複数の分割情報の夫々を、情報処理装置の必須構成要素に分散して記憶することにより、暗号化鍵又は復号鍵の外部への取り出しを困難にして情報のセキュリティが向上すると共に、確実に暗号化鍵又は復号鍵を生成可能にして、利便性を保つ。

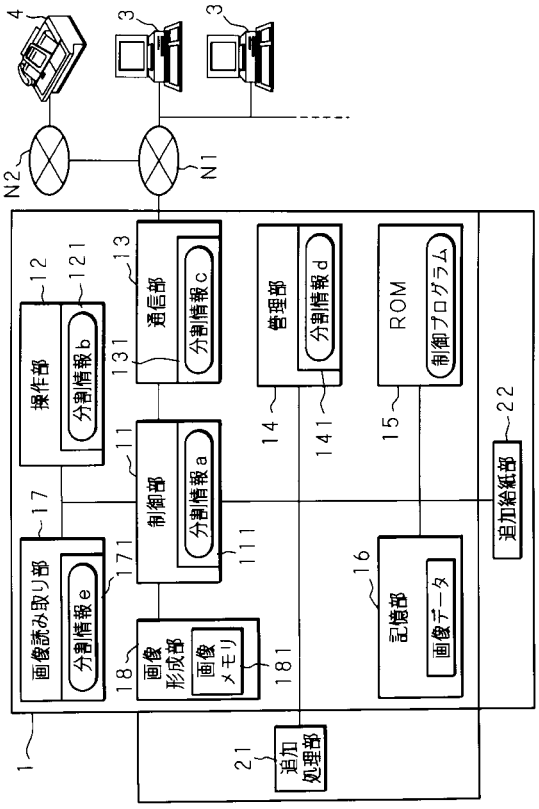
【００５０】

また、本発明においては、電源を投入して情報処理装置が起動するときに暗号化鍵又は復号鍵を生成することにより、情報処理装置が起動する前には内部に暗号化鍵又は復号鍵が存在しなくなり、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。

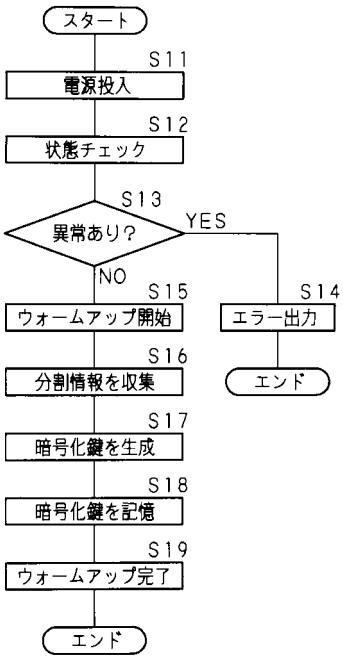
【００５１】
また、本発明においては、情報の処理が可能な状態であるときに暗号化鍵又は復号鍵を生成することにより、情報の処理が不可能な状態では内部に暗号化鍵又は復号鍵が存在しなくなり、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。
【００５２】
また、本発明においては、情報の処理を行うために暗号化または復号を行うときに暗号化鍵又は復号鍵を生成することにより、暗号化鍵又は復号鍵が存在する期間が限定され、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。
【００５３】
また、本発明においては、電源を遮断して情報処理装置が停止するときに暗号化鍵又は復号鍵を消去するなどして無効化することにより、情報処理装置が停止した後には内部に暗号化鍵又は復号鍵が存在しなくなり、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。
【００５４】
また、本発明においては、トラブル等により情報の処理が不可能な状態となった場合に暗号化鍵又は復号鍵を消去するなどして無効化することにより、情報の処理が不可能になった状態では内部に暗号化鍵又は復号鍵が存在しなくなり、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。
【００５５】
また、本発明においては、情報の暗号化又は復号を行った後は、用いた暗号化鍵又は復号鍵を消去するなどして速やかに無効化することにより、暗号化鍵又は復号鍵が存在する期間が限定され、暗号化鍵又は復号鍵を外部へ取り出すことを困難にさせ、暗号化鍵の漏洩を防止して情報のセキュリティが向上する。
【００５６】
また、本発明においては、情報処理装置は、暗号化で保護された画像データを記憶し、情報の機密性を保持しながら、蓄積された画像データを有効に利用することができる。
【００５７】
更に、本発明においては、情報処理装置は、コピー装置、ファクシミリ装置、プリンタ装置、又はスキャナ装置であり、情報の機密性を保持しながら、蓄積された画像データを有効に利用することができる等、本発明は優れた効果を奏する。
【図面の簡単な説明】
【図１】本発明の情報処理装置であるプリンタ装置の内部の構成を示すブロック図である。
【図２】本発明の情報処理装置であるプリンタ装置が起動時に行う処理の手順を示すフローチャートである。
【図３】本発明の情報処理装置であるプリンタ装置が行う画像データ出力の処理の手順を示すフローチャートである。
【図４】記憶部に記憶された画像データを処理する手順を示すフローチャートである。
【図５】本発明の情報処理装置であるプリンタ装置が行う暗号化鍵の消去および再生成の処理を示すフローチャートである。
【図６】本発明の情報処理装置であるプリンタ装置が行う画像データ出力の処理の他の例の手順を示すフローチャートである。
【図７】記憶部に記憶された画像データを処理する手順の他の例を示すフローチャートである。
【符号の説明】
１　プリンタ装置（情報処理装置）
１１　制御部
１４　管理部

１６　記憶部
１１１，１２１，１３１，１４１，１７１　記憶領域（個別記憶手段）
ａ，ｂ，ｃ，ｄ，ｅ　分割情報
Ｎ１　通信ネットワーク

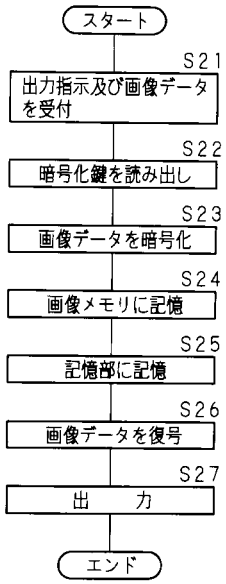
【図１】



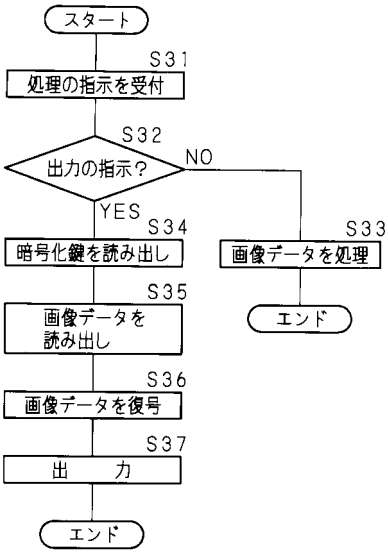
【図２】



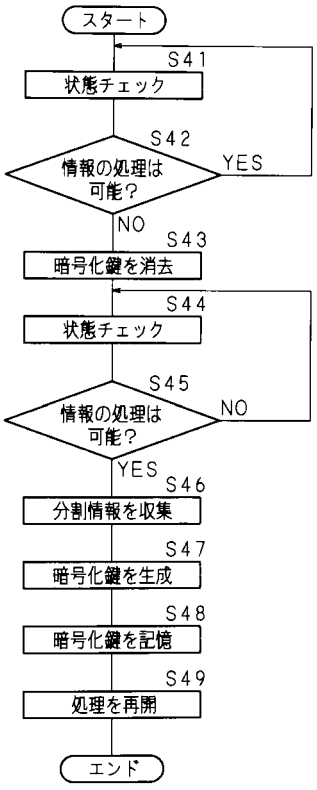
【図３】


スタート
S21
出力指示及び画像データを受付
S22
暗号化鍵を読み出し
S23
画像データを暗号化
S24
画像メモリに記憶
S25
記憶部に記憶
S26
画像データを復号
S27
出　力
エンド

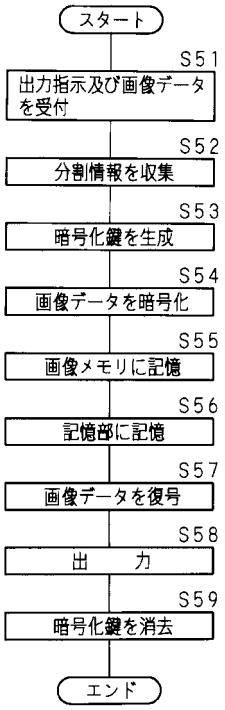
【図４】


スタート
S31
処理の指示を受付
S32
出力の指示？
NO
YES
S34
暗号化鍵を読み出し
S33
画像データを処理
エンド
S35
画像データを読み出し
S36
画像データを復号
S37
出　力
エンド

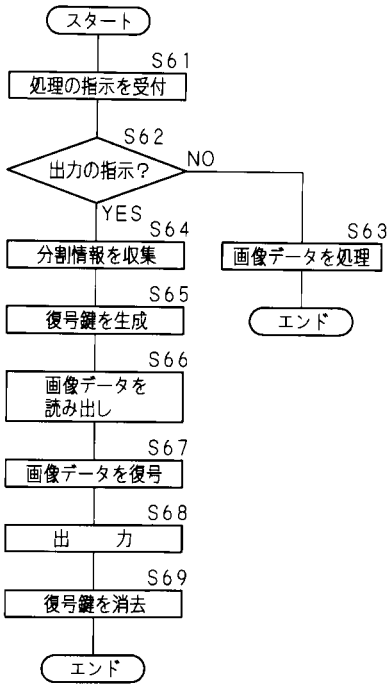
【図５】


スタート
S41
状態チェック
S42
情報の処理は可能？
YES
NO
S43
暗号化鍵を消去
S44
状態チェック
S45
情報の処理は可能？
NO
YES
S46
分割情報を収集
S47
暗号化鍵を生成
S48
暗号化鍵を記憶
S49
処理を再開
エンド

【図６】


スタート
S51
出力指示及び画像データを受付
S52
分割情報を収集
S53
暗号化鍵を生成
S54
画像データを暗号化
S55
画像メモリに記憶
S56
記憶部に記憶
S57
画像データを復号
S58
出　力
S59
暗号化鍵を消去
エンド

【図７】


スタート
S61
処理の指示を受付
S62
出力の指示？
NO
YES
S63
画像データを処理
エンド
S64
分割情報を収集
S65
復号鍵を生成
S66
画像データを
読み出し
S67
画像データを復号
S68
出　力
S69
復号鍵を消去
エンド