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

特許第4494312号
(P4494312)

(45)発行日　平成22年6月30日(2010.6.30)　(24)登録日　平成22年4月16日(2010.4.16)

(51)Int.Cl.			F I		
H04N	1/387	(2006.01)	H04N	1/387	
H04N	1/44	(2006.01)	H04N	1/44	
H04L	9/08	(2006.01)	H04L	9/00	601A
			H04L	9/00	601F

請求項の数 3　(全 12 頁)

(21)出願番号　特願2005-242503(P2005-242503)
(22)出願日　平成17年8月24日(2005.8.24)
(65)公開番号　特開2007-60236(P2007-60236A)
(43)公開日　平成19年3月8日(2007.3.8)
審査請求日　平成20年2月20日(2008.2.20)

(73)特許権者　591044164
株式会社沖データ
東京都港区芝浦四丁目１１番２２号
(74)代理人　100082050
弁理士　佐藤　幸男
(72)発明者　越智　健吾
東京都港区芝浦四丁目１１番２２号　株式会社　沖データ内

審査官　橋爪　正樹

最終頁に続く

(54)【発明の名称】画像処理装置

(57)【特許請求の範囲】
【請求項１】
原稿媒体から画像情報を読取る画像読取部を有する画像処理装置であって、
前記画像情報の送信先を指示する送信先指示部と、
該送信先指示部によって指示された前記画像情報の送信先に対応する暗号化鍵情報を該暗号化鍵情報が前記送信先により予め登録された外部装置から取得する暗号化鍵取得部と、
読取られた前記画像情報を前記外部装置から取得された前記暗号化鍵情報に基いて暗号化する暗号化部とを備えることを特徴とする画像処理装置。
【請求項２】
前記暗号化部によって暗号化された画像情報を電子メール形式に変換する電子メール変換部を更に備えることを特徴とする請求項１に記載の画像処理装置。
【請求項３】
前記暗号化鍵情報は、公開鍵暗号化方式に基く情報であることを特徴とする請求項１又は請求項２に記載の画像処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、読み取った画像情報を画像データに変換して送信する画像処理装置に関し、特に該画像データを暗号化して送信する画像処理装置に関するものである。

【背景技術】
【０００２】
通信ネットワークに接続されている画像処理装置は、該ネットワークに接続されている多数の端末装置から送信要求を受入れて画像データを送信する（例えば特許文献１参照）。このネットワークには、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を含むのは勿論のこと、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を含む場合も多い。従って、送信される画像データの秘密保持は極めて重要な懸案事項の１つとなっている。この懸案事項を解決するために従来の技術では、送信要求されている画像データの送信に秘匿性が要求される場合には、送信する画像データを公開鍵暗号化方式を用いて暗号化していた。送信する画像データを暗号化するためには、先ず利用者が画像処理装置以外の端末装置を用いて公開鍵を予め該画像処理装置に読み込ませておく必要があり、その準備段階での処理が煩雑であった。
【特許文献１】特開平１１－２１５３８４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
解決しようとする問題点は、送信する画像データを暗号化するために、先ず利用者が画像処理装置以外の端末装置を用いて公開鍵を予め該画像処理装置に読み込ませておく必要があり、その準備段階での処理が煩雑であった点である。
【課題を解決するための手段】
【０００４】
本発明は、原稿媒体から画像情報を読取る画像読取部を有する画像処理装置であって、上記画像情報の送信先を指示する送信先指示部と、該送信先指示部によって指示された上記画像情報の送信先に対応する暗号化鍵情報を該暗号化鍵情報が上記送信先により予め登録された外部装置から取得する暗号化鍵取得部と、読取られた上記画像情報を上記外部装置から取得された上記暗号化鍵情報に基いて暗号化する暗号化部とを備えることを主要な特徴とする。
【発明の効果】
【０００５】
第一の発明では、スキャナ装置に暗号化鍵抽出部を備え、暗号化鍵をスキャナ装置で読み取り可能な形式で印刷した暗号化鍵用紙から自動的に暗号化鍵を抽出するので、スキャナ装置で送信原稿を読み込ませるのと一連の動作で準備段階が完了し、処理が極めて簡便になるという効果を得る。第二の発明では、スキャナ装置に暗号化鍵取得部を備え、操作者が送信先を指定すると、暗号化鍵が登録されている暗号化鍵格納サーバからスキャナ装置が自動的に暗号化鍵を取得して送信原稿の暗号化に用いることが可能になるので処理が極めて簡便になるという効果を得る。
【発明を実施するための最良の形態】
【０００６】
公開鍵暗号化方式における公開鍵を暗号化鍵とし、この暗号化鍵は画像データの要求に先立って、要求元から送信元（又は共通機関）へ電子メールで送信され、秘密鍵は画像データの要求元が秘密裏に保持することとした。
【実施例１】
【０００７】
図１は、実施例１の画像処理装置の構成を表すブロック図である。
図に示すように、実施例１のスキャナ装置１００は、読取部１と、指示部２と、切替部３と、暗号化鍵抽出部４と、鍵情報格納部５と、暗号化部６と、送信先指定部７と、メール変換部８と、送信部９とを備える。
【０００８】
読取部１は、原稿から画像情報を読み取って画像データに変換する部分である。例えばラインセンサと、その移動部で構成され、読み取った画像情報を画像データに変換して切

替部３へ送出する部分である。通常は光学的センサが用いられるが特に読み取りの方式を限定する必要はない。

【０００９】

指示部２は、暗号化鍵用紙読込みボタン２－１と、送信原稿読込みボタン２－２を有し、操作者によって指定される原稿の種類を切替部３に通知する部分である。ここで暗号用紙とは、画像データの要求元から受信した暗号化鍵が印刷されている原稿であり、以後暗号化鍵用紙と記す。又送信原稿とは、暗号化して送信される画像データの基に成る画像情報が記載されている原稿媒体である。尚、暗号化鍵用紙に印刷されている暗号化鍵は、例えばバーコードとして印刷されており読取部１によって読み取り可能な形式になっている。但し、暗号化鍵の形式は、バーコードに限定する必要はなく、暗号化鍵を文字列として表現したものや、特定の方式で暗号化鍵を符号化したものであっても良い。

【００１０】

切替部３は、指示部２から通知される原稿の種類によって、読取部１から受入れる画像データの送出先を切替える部分である。指示部２によって読み取る原稿が暗号化鍵用紙であると通知された場合には画像データの送出先を暗号化鍵抽出部４へ切替える。又指示部２によって読み取る原稿が送信原稿であると通知された場合には画像データの送出先を暗号化部６へ切替える。

【００１１】

暗号化鍵抽出部４は、切替部３から暗号化鍵用紙の画像データが送られてくると、その画像データから送信原稿を暗号化するための暗号化鍵を抽出する部分である。抽出された暗号化鍵は、暗号化部６で使用出来るように数値に変換され、鍵情報格納部５へ送出される。

【００１２】

鍵情報格納部５は、暗号化鍵抽出部４から送られてくる暗号化鍵を格納するメモリである。

暗号化部６は、切替部３から送信原稿の画像データが送られてくると、鍵情報格納部５から暗号化鍵を取得し、該暗号化鍵を用いて送信原稿の画像データを暗号化してメール変換部８へ送出する部分である。

【００１３】

送信先指定部７は、入力キー７－１と表示板７－２を有し、暗号化部６によって暗号化された画像データの送信先を指定する部分である。操作者は入力キー７－１を用いて送信先のメールアドレスを入力することになる。そのメールアドレスは表示板７－２に表示される。

【００１４】

メール変換部８は、送信先指定部７から送信先のメールアドレスを取得し、そのメールアドレスを送信先とし、暗号化部６から受入れた暗号化された（送信原稿の）画像データを添付ファイルとし、電子メールを作成して送信部９へ送出する部分である。

【００１５】

送信部９は、メール変換部８によって作成された電子メールをメールサーバ（後記）へ送信する部分である。メールサーバへ送信するための通信プロトコルとしては、通常ＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）が用いられる。勿論このプロトコルに限定する必要はない。

【００１６】

以上説明した実施例１のスキャナ装置１００を含む画像処理システムのシステム構成について以下に説明する。

図２は、実施例１のスキャナ装置を含む画像処理システムのシステム構成図である。

図に示すように画像処理システムは、ネットワーク１５０にスキャナ装置１００と、メールサーバ装置１１０と、送信側端末装置１２０と、（複数台の）受信側端末装置１３０－１～１３０－ｎと、プリンタ装置１４０とを通信接続して構成される。

【００１７】

図に於いて、スキャナ装置１００は、上記実施例１のスキャナ装置である。受信側端末装置１３０は、スキャナ装置１００から送信される暗号化された画像データを受信する端末装置（通常はパーソナルコンピュータ）である。前もって（動作開始の直前でも良い）自己の公開鍵（暗号化鍵）をメールで送信側端末装置１２０へ送信する装置である。メールサーバ装置１１０は、スキャナ装置１００から送信される電子メールを格納するサーバである。送信側端末装置１２０は、受信側端末装置１３０の暗号化鍵を保持し、該暗号化鍵を画像データに変換してプリンタ装置１４０へ送出する送信側の端末装置（通常はパーソナルコンピュータ）である。プリンタ装置１４０は、送信側端末装置１２０から画像データに変換された暗号化鍵を受入れて暗号化鍵用紙を作成する装置である。送信側端末装置１２０とプリンタ装置１４０とは、通常ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）で接続される。ネットワーク１５０は、通常ＬＡＮやＷＡＮを含む通信ネットワークである。

【００１８】

以下に実施例１の動作について説明する。この動作説明は、上記図２のスキャナ装置を含む画像処理システムに於いて、公開鍵暗号化方式に基いてスキャナ装置１００から受信側端末装置１３０－１へ暗号化された（送信画像の）画像データが送信されるものとする。

【００１９】

公開鍵暗号化方式では、２つの鍵が用いられる。一方は秘密鍵であり、他方は公開鍵である。公開鍵は通常誰でも使うことが出来る公共機関等に登録されている。秘密鍵は本人が秘密裏に管理することになる。従って、送信側は、登録された多数の公開鍵の中から受信側に対応する公開鍵を入手し、この公開鍵を用いて（送信画像の）画像データを暗号化してネットワークへ送出する。この暗号化された画像データは、秘密鍵を有する受信側のみが解読可能となる。本実施例では、受信側端末装置１３０－１が自己の公開鍵を電子メールで送信側端末装置１２０へ送り（公開鍵なので秘密保持の必要なし）、スキャナ装置１００がこの公開鍵を用いて（送信画像の）画像データを暗号化し、受信側端末装置１３０－１に向けて送信するものとする。

【００２０】

図３は、実施例１のスキャナ装置の動作フローチャートである。

図４は、暗号化鍵用紙の説明図である。

図５は、実施例１のスキャナ装置の操作盤の説明図である。

【００２１】

図３のステップＳ１－１からステップＳ１－１２までステップ順に実施例１のスキャナ装置の動作について説明する。本動作説明の中で図４及び図５を適宜使用することとする。以下の動作説明では、受信側端末装置１３０－１（図２）から送信側端末装置１２０（図２）へ電子メールで公開鍵（暗号化鍵）が既に送付済みであり、操作者は、プリンタ装置１４０（図２）を用いて公開鍵（暗号化鍵）を印刷した暗号化鍵用紙（図４）を既に取得していることを前提条件とする。

【００２２】

ステップＳ１－１

操作者は、スキャナ装置１００（図１）の入力キー７－１（図１、図５）を用いて送信先指定部７（図１、図５）に送信先のアドレスｙａｍａｄａ@ｂ．ｃｏｍ（図２）を入力する。このアドレスは表示板７－２（図１、図５）に表示される。

【００２３】

ステップＳ１－２

操作者は、暗号化鍵用紙（図４）をスキャナ装置１００（図１）の読取部１（図１）にセットする。

【００２４】

ステップＳ１－３

操作者は、スキャナ装置１００（図１）の暗号化鍵用紙読込みボタン２－１（図１、図

５）を押下する。こうすることによって切替部３（図１）は、画像データを暗号化鍵抽出部４（図１）へ送出すべく出力を切替える。

【００２５】

ステップＳ１－４

読取部１（図１）は、暗号化鍵用紙（図４）から画像情報の読込みを開始する。

【００２６】

ステップＳ１－５

暗号化鍵抽出部４（図１）は、切替部３（図１）から画像データを受入れて暗号化鍵を抽出する。

【００２７】

ステップＳ１－６

抽出された暗号化鍵は鍵情報格納部５（図１）へ格納される。

【００２８】

ステップＳ１－７

操作者は、暗号化して送信したい送信原稿をスキャナ装置１００（図１）の読取部１（図１）にセットする。

【００２９】

ステップＳ１－８

操作者は、スキャナ装置１００（図１）の送信原稿読込みボタン２－２（図１、図５）を押下する。こうすることによって切替部３（図１）は、画像データを暗号化部６（図１）へ送出すべく出力を切替える。

【００３０】

ステップＳ１－９

読取部１（図１）は、送信原稿から画像情報の読込みを開始する。

【００３１】

ステップＳ１－１０

暗号化部６（図１）は、鍵情報格納部５（図１）から暗号化鍵を取得して送信原稿から読み取った画像データを暗号化する。

【００３２】

ステップＳ１－１１

メール変換部８（図１）は、送信先指定部７（図１）からステップＳ１－１で操作者によって入力された送信先のメールアドレスを取得し、そのメールアドレスを送信先とし、暗号化部６（図１）から受入れた暗号化された送信原稿の画像データを添付ファイルとし、電子メールを作成し送信部９（図１）へ送出する。

【００３３】

ステップＳ１－１２

メール変換部８（図１）によって作成された電子メールは送信部９（図１）から所定のプロトコルに基いて、ネットワーク１５０（図２）を介してメールサーバ装置１１０（図１）へ送出されてフローを終了する。所定のプロトコルは、通常ＳＭＴＰが用いられる。勿論このプロトコルに限定する必要はない。

【００３４】

この後、受信者は受信側端末装置１３０－１（図２）を操作して所定のプロトコルに基いてネットワーク１５０（図２）を介してメールサーバ装置１１０（図１）から自分宛の電子メールを取得する。受信したメールの中に暗号化されたメールがあれば受信側端末装置１３０（図１）上で自己の復号化鍵（秘密鍵）を用いて添付ファイルを復号化し、閲覧する。ここで所定のプロトコルとしては通常ＰＯＰ（Ｐｏｓｔ　Ｏｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ）が用いられる。勿論このプロトコルに限定する必要はない。

【００３５】

以上説明したように、スキャナ装置で送信原稿から読取った画像データを公開鍵暗号化方式に基いて暗号して送信する場合に、本実施例によれば、スキャナ装置に暗号化鍵抽出

部を備えることによって、暗号化鍵をスキャナ装置で読み取り可能な形式で印刷した暗号化鍵用紙から暗号化鍵を抽出可能になったので、スキャナ装置で送信原稿を読み込ませるのと一連の動作で準備段階が完了し、処理が極めて簡便になるという効果を得る。

【実施例２】

【００３６】

上記実施例１では、暗号化処理の前（通常は直前）に暗号化鍵用紙から暗号化鍵を抽出して送信原稿の暗号化に用いたが、本実施例では、スキャナ装置に暗号化鍵取得部を備え、暗号化処理の前に予め公開鍵（暗号化鍵）が登録されている暗号化鍵格納サーバから、操作者が送信先を指定すると、暗号化鍵取得部が自動的に暗号化鍵を取得して送信原稿の暗号化に用いることとする。

【００３７】

図６は、実施例２の画像処理装置の構成を表すブロック図である。

図に示すように、実施例２のスキャナ装置２００は、読取部１と、鍵情報格納部５と、暗号化部６と、メール変換部８と、送信部９と、送信先指定部１１と、暗号化鍵取得部１２を備える。以下に実施例１と相違する部分のみについて詳細に説明する。実施例１と同様の部分については実施例１と同一の符号を付して説明を省略する。

【００３８】

送信先指定部１１は、入力キー７－１と表示板７－２と原稿読込みボタン１１－１を有し、暗号化部６によって暗号化された画像データの送信先を指定する部分である。操作者は入力キー７－１を用いて送信先のメールアドレスを入力することになる。そのメールアドレスは表示板７－２に表示される。更に、送信先のメールアドレスを入力した後、操作者が原稿読込みボタン１１－１を押下することによって一連の動作を開始させる部分である。

【００３９】

暗号化鍵取得部１２は、操作者が原稿読込みボタン１１－１を押下すると送信部９とネットワーク１５０を介して送信先のメールアドレスを暗号化鍵格納サーバ装置２４０（後記）へ送信し、暗号化鍵格納サーバ装置２４０（後記）に登録されている送信先の公開鍵を問い合わせて取得し、鍵情報格納部５へ格納する部分である。この問い合わせには、通常ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）が用いられる。勿論このプロトコルに限定する必要はない。

【００４０】

以上説明した実施例２のスキャナ装置２００を含む画像処理システムのシステム構成について以下に説明する。

図７は、実施例２のスキャナ装置を含む画像処理システムのシステム構成図である。

図に示すように画像処理システムは、ネットワーク１５０にスキャナ装置２００と、メールサーバ装置１１０と、暗号化鍵格納サーバ装置２４０と、（複数台の）受信側端末装置２３０－１～２３０－ｎとを通信接続して構成される。

【００４１】

図に於いて、スキャナ装置２００は、上記実施例２のスキャナ装置である。受信側端末装置２３０～２３０－ｎは、スキャナ装置１００から暗号化された送信画像を受信する端末装置（通常はパーソナルコンピュータ）である。前もって自己の公開鍵（暗号化鍵）を暗号化鍵格納サーバ装置２４０へ登録する装置である。メールサーバ装置１１０は、スキャナ装置２００から送信される電子メールを格納するサーバである。暗号化鍵格納サーバ装置２４０は、受信側端末装置２３０～２３０－ｎから公開鍵の登録を受入れて格納するサーバであり、スキャナ装置２００から公開鍵の問い合わせを受けると、該当する公開鍵を検索し、検出した公開鍵をスキャナ装置２００へ送信するサーバである。ネットワーク１５０は、通常ＬＡＮやＷＡＮを含む通信ネットワークである。

【００４２】

以下に実施例２の動作について説明する。

図８は、実施例２のスキャナ装置の動作フローチャートである。

図９は、実施例２のスキャナ装置の操作盤の説明図である。

【００４３】

図８のステップＳ２－１からステップＳ２－１０までステップ順に実施例２のスキャナ装置の動作について説明する。本動作説明の中で図９を適宜使用することとする。但し、受信側端末装置１３０－１（図７）から暗号化鍵格納サーバ装置２４０（図７）へ電子メールで公開鍵が既に登録されていることを前提条件とする。

【００４４】

ステップＳ２－１

操作者は、スキャナ装置２００（図６）の入力キー７－１（図６、図９）を用いて送信先指定部１１（図６、図９）に送信先のアドレスｙａｍａｄａ@ｂ．ｃｏｍ（図７）を入力する。このアドレスは表示板７－２（図６、図９）に表示される。

【００４５】

ステップＳ２－２

操作者は、暗号化して送信したい送信原稿をスキャナ装置２００（図６）の読取部１（図６）にセットする。

【００４６】

ステップＳ２－３

操作者は、スキャナ装置２００（図６）の送信原稿読込みボタン１１－１（図６、図９）を押下する。

【００４７】

ステップＳ２－４

暗号化鍵取得部１２（図６）は、操作者が原稿読込みボタン１１－１（図６、図９）を押下すると送信部９（図６）とネットワーク１５０（図６）を介して送信先のメールアドレスを暗号化鍵格納サーバ装置２４０（図７）へ送信し、暗号化鍵格納サーバ装置２４０（図７）に登録されている送信先の公開鍵を通常ＨＴＴＰで問い合わせる。ここでＨＴＴＰについて説明する。

【００４８】

一例として以下の信号がスキャナ装置２００（図６）から暗号化鍵格納サーバ装置２４０（図７）へ送られる。

ＰＯＳＴ　ｈｔｔｐ：//ｋｅｙ－ｓｅｒｖｅｒ．ｃｏｍ/ｋｅｙ．ｃｇｉ？ｋｅｙ＝ｙａｍａｄａ@ｂ．ｃｏｍ　ＨＴＴＰ・/１．１

ｕｓｅｒ－Ａｇｅｎｔ：Ｓｃａｎ－Ｄｅｖｉｃｅ

Ｈｏｓｔ：ｓｃａｎｎｅｒ．ａ．ｃｏｍ

【００４９】

ここで「ＰＯＳＴ」で始まる行は、このＨＴＴＰヘッダがＵＲＬ「ｈｔｔｐ：//ｋｅｙ－ｓｅｒｖｅｒ．ｃｏｍ/ｋｅｙ．ｃｇｉ？ｋｅｙ＝ｙａｍａｄａ@ｂ．ｃｏｍ」へのＰＯＳＴメソッドであり、使用するＨＴＴＰのバージョンが１．１であることを示している。ＵＲＬ「ｈｔｔｐ：//ｋｅｙ－ｓｅｒｖｅｒ．ｃｏｍ/ｋｅｙ．ｃｇｉ？ｋｅｙ＝ｙａｍａｄａ@ｂ．ｃｏｍ」はドメイン名「ｋｅｙ－ｓｅｒｖｅｒ．ｃｏｍ」の暗号化鍵格納サーバ装置２４０（図７）のＣＧＩ「ｋｅｙ．ｃｇｉ」にｋｅｙパラメータの値として画像データの送信先のアドレス「ｙａｍａｄａ@ｂ．ｃｏｍ」を与えていることを示している。

【００５０】

「ｕｓｅｒ－Ａｇｅｎｔ」で始まる行は、このＨＴＴＰヘッダが送信しているアプリケーションの名称を表している。この例では、スキャナの名称として「Ｓｃａｎ－Ｄｅｖｉｃｅ」を用いている。Ｈｏｓｔで始まる行は、このＨＴＴＰヘッダを作成した装置のドメイン名を示している。この例では、暗号化鍵格納サーバ装置２４０「ｈｔｔｐ：//ｋｅｙ－ｓｅｒｖｅｒ．ｃｏｍ」（図７）のＣＧＩ「ｋｅｙ．ｃｇｉ」に対して画像データの送信先のアドレス「ｙａｍａｄａ@ｂ．ｃｏｍ」をｋｅｙパラメータとして渡し「ｋｅｙ．ｃｇｉ？ｋｅｙ＝ｙａｍａｄａ@ｂ．ｃｏｍ」の公開鍵を要求している。

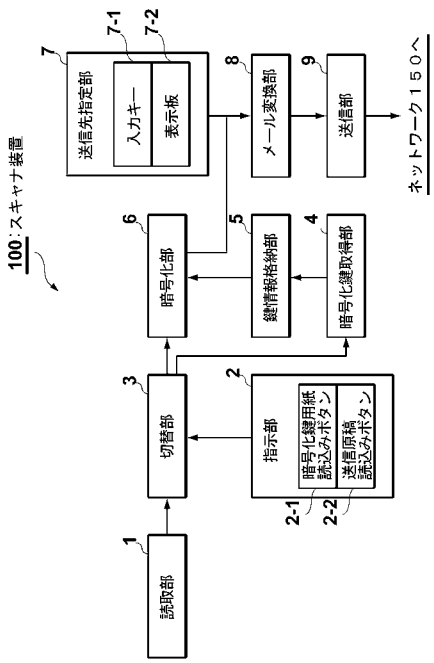
【００５１】
ステップＳ２－５
暗号化鍵格納サーバ装置２４０（図７）は、ｋｅｙパラメータで受け取ったメールアドレスを参照し、サーバに格納されている公開鍵を検索し検出できた公開鍵をスキャナ装置２００（図６）へ送信する。
【００５２】
ステップＳ２－６
暗号化鍵取得部１２（図６）は、受信した暗号化鍵を鍵情報格納部５（図１）へ格納する。
【００５３】
ステップＳ２－７
読取部１（図６）は、送信原稿から画像情報の読込みを開始する。
【００５４】
ステップＳ２－８
暗号化部６（図６）は、鍵情報格納部５（図６）から暗号化鍵を取得して送信原稿から読み取った画像データを暗号化する。
【００５５】
ステップＳ２－９
メール変換部８（図６）は、送信先指定部１１（図６）からステップＳ２－１で操作者によって入力された送信先のメールアドレスを取得し、そのメールアドレスを送信先とし、暗号化部６（図６）から受入れた暗号化された送信原稿の画像データを添付ファイルとし、電子メールを作成し送信部９（図６）へ送出する。
【００５６】
ステップＳ２－１０
メール変換部８（図６）によって作成された電子メールは送信部９（図６）から所定のプロトコルに基いて、ネットワーク１５０（図７）を介してメールサーバ装置１１０（図７）へ送出されてフローを終了する。所定のプロトコルは、通常ＳＭＴＰが用いられる。勿論このプロトコルに限定する必要はない。
【００５７】
以上説明したように、スキャナ装置で送信原稿から読取った画像データを公開鍵暗号化方式に基いて暗号して送信する場合に、本実施例によれば、スキャナ装置に暗号化鍵取得部を備えることによって、操作者が送信先を指定すると、暗号化処理の前に予め公開鍵が登録されている暗号化鍵格納サーバからスキャナ装置が自動的に公開鍵を取得して送信原稿の暗号化に用いることが可能になるので処理が極めて簡便になるという効果を得る。
【産業上の利用可能性】
【００５８】
以上の説明では、本発明をスキャナ装置に適用した場合について説明したが、本発明は、この例に限定されるものではない。即ち、ファクシミリ装置や、複写機などにも適用可能である。
【図面の簡単な説明】
【００５９】
【図１】実施例１の画像処理装置の構成を表すブロック図である。
【図２】実施例１のスキャナ装置を含む画像処理システムのシステム構成図である。
【図３】実施例１のスキャナ装置の動作フローチャートである。
【図４】暗号化鍵用紙の説明図である。
【図５】実施例１のスキャナ装置の操作盤の説明図である。
【図６】実施例２の画像処理装置の構成を表すブロック図である。
【図７】実施例２のスキャナ装置を含む画像処理システムのシステム構成図である。
【図８】実施例２のスキャナ装置の動作フローチャートである。
【図９】実施例２のスキャナ装置の操作盤の説明図である。

【符号の説明】

【００６０】

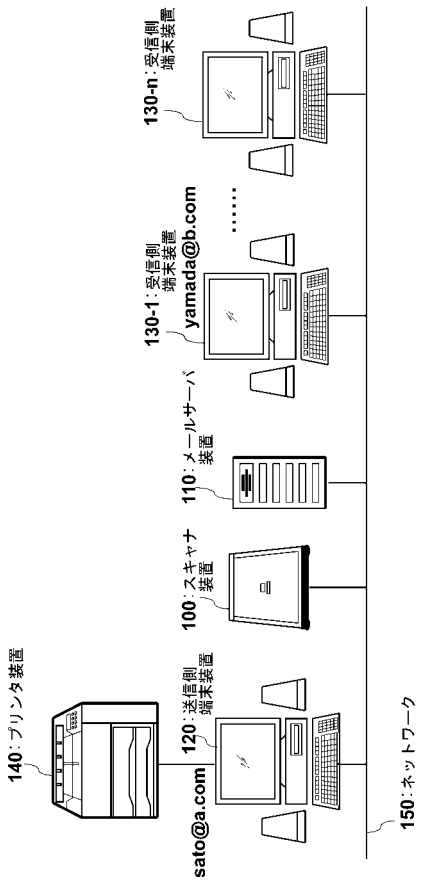
１　　読取部
２　　指示部
２－１　　暗号化鍵用紙読込みボタン
２－２　　送信原稿読込みボタン
３　　切替部
４　　暗号化鍵抽出部
５　　鍵情報格納部
６　　暗号化部
７　　送信先指定部
７－１　　入力キー
７－２　　表示板
８　　メール変換部
９　　送信部
１００　　スキャナ装置

【図１】



実施例１の画像処理装置の構成を表すブロック図

【図２】

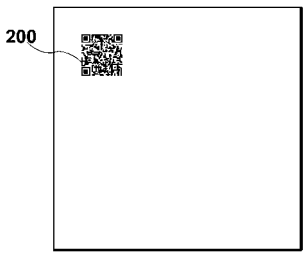


実施例１のスキャナ装置を含む画像処理システムのシステム構成図

【図３】

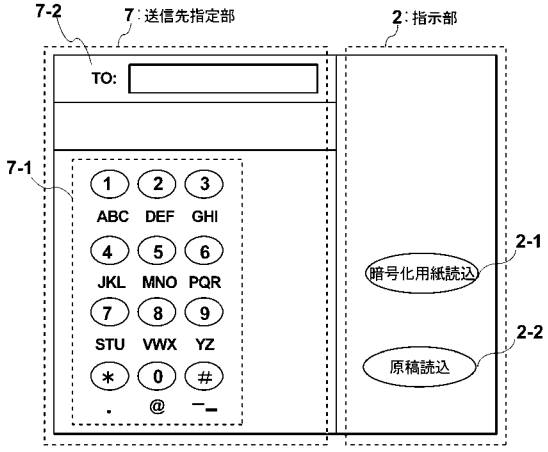
実施例１のスキャナ装置の動作フローチャート

【図４】



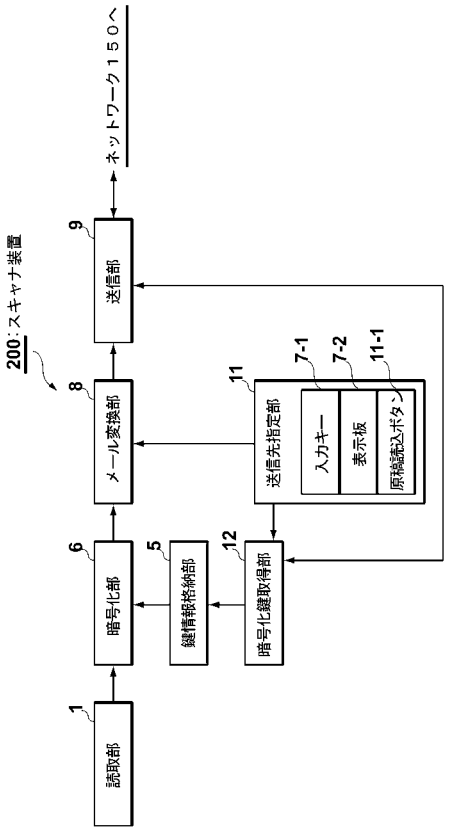
暗号化鍵用紙の説明図

【図５】



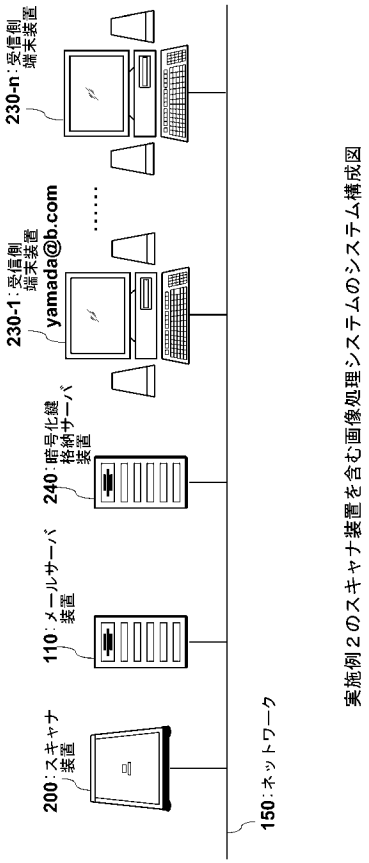
実施例１のスキャナ装置の操作盤の説明図

【図６】



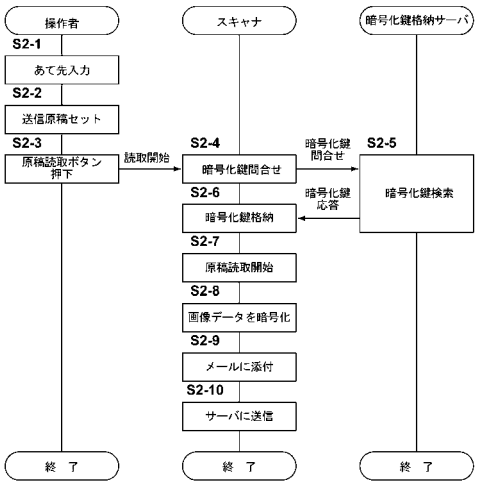
実施例２の画像処理装置の構成を表すブロック図

【図７】



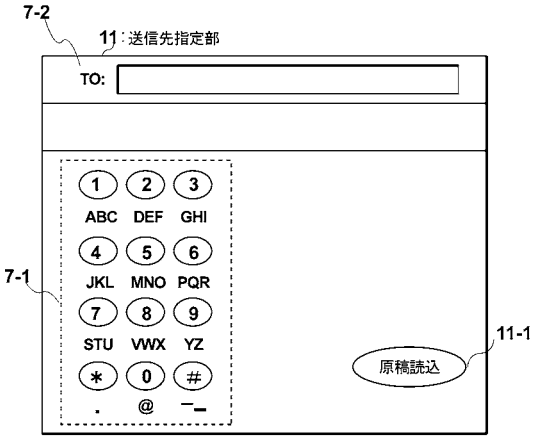
実施例２のスキャナ装置を含む画像処理システムのシステム構成図

【図８】



実施例２のスキャナ装置の動作フローチャート

【図９】



実施例２のスキャナ装置の操作盤の説明図

フロントページの続き

(56)参考文献 特開平０８－０６９２５０（ＪＰ，Ａ）
特開平０５－１３０４３６（ＪＰ，Ａ）
特開平０９－０８３５０８（ＪＰ，Ａ）
特開２００１－２３７８７２（ＪＰ，Ａ）
特開２００１－２１１３０６（ＪＰ，Ａ）
特開２００５－０５００４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｎ １／３８－ １／３９３
Ｈ０４Ｎ １／４４
Ｇ０９Ｃ １／００－ ５／００