(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2007-181945
(P2007-181945A)
(43)公開日　平成19年7月19日(2007.7.19)

| (51)Int.Cl. | | F I | | | テーマコード（参考） |
|---|---|---|---|---|---|
| B41J 29/38 | (2006.01) | B41J | 29/38 | Z | 2C061 |
| H04N 1/44 | (2006.01) | H04N | 1/44 | | 5B021 |
| G06F 3/12 | (2006.01) | G06F | 3/12 | K | 5B285 |
| H04N 1/00 | (2006.01) | H04N | 1/00 | 107Z | 5C062 |
| B41J 29/00 | (2006.01) | B41J | 29/00 | Z | 5C075 |

審査請求 未請求　請求項の数 13　ＯＬ　（全 21 頁）　最終頁に続く

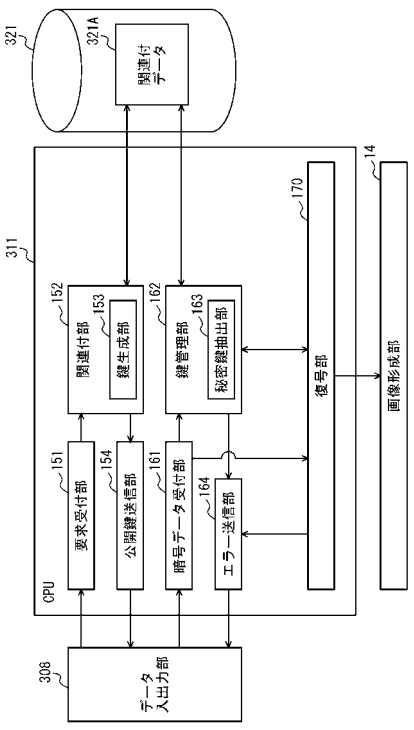
(21)出願番号　特願2006-455 (P2006-455)
(22)出願日　平成18年1月5日 (2006.1.5)

(71)出願人　303000372
コニカミノルタビジネステクノロジーズ株式会社
東京都千代田区丸の内一丁目６番１号
(74)代理人　100108523
弁理士　中川　雅博
(72)発明者　川畑　博征
東京都千代田区丸の内一丁目６番１号　コニカミノルタビジネステクノロジーズ株式会社内

Ｆターム(参考)　2C061 AP01 AP03 AP04 AP07 CL10 HJ06 HJ08 HK03 HK11 HN05 HN15 HP00
5B021 AA05 AA19 NN18
5B285 AA04 BA07 CB43 CB53 CB95
最終頁に続く

(54)【発明の名称】画像形成装置、出力判断プログラムおよび出力判断方法

(57)【要約】
【課題】　ネットワーク経由で受信されるプリントデータのセキュリティを確保する。
【解決手段】　ＭＦＰ１００は、公開鍵と秘密鍵を生成する鍵生成部１５３と、ＰＣのＩＰアドレスを含む要求信号の受信に応じて、公開鍵および秘密鍵とＩＰアドレスとを関連付けた関連付データ３２１Ａを記憶するＨＤＤ３２１と、ＩＰアドレスに関連付けられた公開鍵を返信する公開鍵送信部１５４と、ＩＰアドレスが付加された暗号データを、ネットワークを介して受信する暗号データ受付部１６１と、暗号データに付加されたＩＰアドレスと関連付けられた秘密鍵で暗号データを復号する復号部１７０と、画像形成部１４による復号されたプリントデータの画像形成に応じて、ＩＰアドレスに関連付けられた秘密鍵での復号を禁止する秘密鍵抽出部１６３と、を備える。
【選択図】　図５



【特許請求の範囲】
【請求項１】
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成する鍵生成手段と、
装置を識別するための識別情報を含む要求信号を受信する要求信号受信手段と、
前記要求信号の受信に応じて、生成された前記暗号鍵および前記復号鍵の組と前記識別情報とを関連付けた関連付データを記憶する鍵テーブル記憶手段と、
前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信する暗号鍵返信手段と、
前記識別情報が付加されたデータを、ネットワークを介して受信するデータ受信手段と、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号する復号手段と、
前記復号されたデータを画像形成する画像形成手段と、
前記画像形成手段による画像形成に応じて、前記受信されたデータに付加された前記識別情報に関連付けられた復号鍵を用いた前記復号手段による復号を禁止する禁止手段と、
を備えた画像形成装置。
【請求項２】
前記禁止手段は、前記受信されたデータに付加された前記識別情報を含む前記関連付データを削除する削除手段を含む、請求項１に記載の画像形成装置。
【請求項３】
前記禁止手段は、前記復号手段に前記受信されたデータに付加された前記識別情報を含む前記関連付データの使用を禁止させる使用禁止手段を含む、請求項１に記載の画像形成装置。
【請求項４】
前記禁止手段は、前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵および暗号鍵の組を前記鍵生成手段に生成させない生成禁止手段を含む、請求項３に記載の画像形成装置。
【請求項５】
前記鍵生成手段は、前記要求信号の受信に応じて、前記暗号鍵および前記復号鍵の組を生成する、請求項１に記載の画像形成装置。
【請求項６】
前記鍵生成手段は、前記暗号鍵および前記復号鍵の組を予め複数生成して記憶する鍵記憶手段を含み、
前記鍵記憶手段に記憶された複数の前記暗号鍵および前記復号鍵の組のうち前記識別情報に関連付けられていない組の数が所定数以下になると新たな組を生成する、請求項１に記載の画像形成装置。
【請求項７】
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶する鍵記憶手段と、
装置を識別するための識別情報を含む要求信号を受信する要求信号受信手段と、
前記要求信号の受信に応じて、前記鍵記憶手段に記憶された前記暗号鍵および前記復号鍵の前記複数の組のいずれか１つと前記識別情報とを関連付けた関連付データを記憶する鍵テーブル記憶手段と、
前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信する暗号鍵返信手段と、
前記識別情報が付加されたデータを、ネットワークを介して受信するデータ受信手段と、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号する復号手段と、

前記復号されたデータを画像形成する画像形成手段と、
前記画像形成手段による画像形成に応じて、前記受信されたデータに付加された前記識別情報を含む前記関連付データを削除する削除手段と、を備えた画像形成装置。
【請求項８】
前記復号手段により前記受信されたデータを復号できない場合には、前記データに付加された識別情報を予め定められた送信先に送信するメッセージ送信手段をさらに含む、請求項１または７に記載の画像形成装置。
【請求項９】
前記暗号化鍵と前記復号鍵とは、同じである、請求項１または７に記載の画像形成装置。
【請求項１０】
データが入力されると画像形成する画像形成手段を備えた画像形成装置で実行される出力判断プログラムであって、
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成するステップと、
装置を識別するための識別情報を含む要求信号を受信するステップと、
前記要求信号の受信に応じて、生成された前記暗号鍵および前記復号鍵の組と前記識別情報とを関連付けた関連付データを記憶するステップと、
前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信するステップと、
前記識別情報が付加されたデータを、ネットワークを介して受信するステップと、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号するステップと、
前記復号されたデータを前記画像形成手段に画像形成させるステップと、
前記画像形成手段による画像形成に応じて、前記受信されたデータに付加された前記識別情報に関連付けられた復号鍵を用いた復号を禁止するステップと、を画像形成装置に実行させる出力判断プログラム。
【請求項１１】
データが入力されると画像形成する画像形成手段を備えた画像形成装置で実行される出力判断プログラムであって、
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶するステップと、
装置を識別するための識別情報を含む要求信号を受信するステップと、
前記要求信号の受信に応じて、前記暗号鍵および前記復号鍵の前記複数の組のいずれか１つと前記識別情報とを関連付けた関連付データを記憶するステップと、
前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信するステップと、
前記識別情報が付加されたデータを、ネットワークを介して受信するステップと、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号するステップと、
前記復号されたデータを前記画像形成装置に画像形成させるステップと、
前記画像形成手段による画像形成に応じて、前記受信されたデータに付加された前記識別情報を含む前記関連付データを削除するステップと、を画像形成装置に実行させる出力判断プログラム。
【請求項１２】
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成するステップと、
装置を識別するための識別情報を含む要求信号を受信するステップと、
前記要求信号の受信に応じて、生成された前記暗号鍵および前記復号鍵の組と前記識別情報とを関連付けた関連付データを記憶するステップと、

前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信するステップと、
前記識別情報が付加されたデータを、ネットワークを介して受信するステップと、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号するステップと、
前記復号されたデータを画像形成するステップと、
前記画像形成ステップによる画像形成に応じて、前記受信されたデータに付加された前記識別情報に関連付けられた復号鍵を用いた復号を禁止するステップとを、画像形成装置に実行させる出力判断方法。
【請求項１３】
データを暗号化するための暗号鍵と前記暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶するステップと、
装置を識別するための識別情報を含む要求信号を受信するステップと、
前記要求信号の受信に応じて、前記暗号鍵および前記復号鍵の前記複数の組のいずれか１つと前記識別情報とを関連付けた関連付データを記憶するステップと、
前記識別情報に前記関連付データにより関連付けられた前記暗号鍵を返信するステップと、
前記識別情報が付加されたデータを、ネットワークを介して受信するステップと、
前記受信されたデータに付加された前記識別情報に前記関連付データにより関連付けられた復号鍵を用いて前記受信されたデータを復号するステップと、
前記復号されたデータを画像形成するステップと、
前記画像形成ステップによる画像形成に応じて、前記受信されたデータに付加された前記識別情報を含む前記関連付データを削除するステップと、を画像形成装置に実行させる出力判断方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、画像形成装置、出力判断プログラムおよび出力判断方法に関し、特に、ネットワークを介してプリントデータを受信する画像形成装置およびその画像形成装置で実行される出力判断プログラムおよび出力判断方法に関する。
【背景技術】
【０００２】
近年、ネットワークが普及しており、パーソナルコンピュータとＭＦＰ（Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）で代表される画像形成装置とをネットワークで接続して使用することが多い。パーソナルコンピュータでプリントデータをＭＦＰに送信して、ＭＦＰでプリントデータが用紙などの記録媒体に画像形成される。しかしながら、プリントデータは、ネットワーク上を流れるため、ネットワークに接続された他のコンピュータがネットワーク上を流れるプリントデータを容易に受信できてしまう。また、ネットワーク上のプリントデータが他のコンピュータで受信されることに備えて、暗号化することが可能であるが、暗号化されたデータを再度ＭＦＰに送信することにより、ＭＦＰが暗号化されたデータを復号して、プリントデータを画像形成してしまうといった問題がある。
【０００３】
一方、ネットワーク上を流れる認証情報のセキュリティを確保した印刷システムが特開２００４－１１８７０９号公報（特許文献１）に記載されている。特開２００４－１１８７０９号公報に記載の印刷システムは、印刷ジョブを印刷する少なくとも１台以上の印刷装置と、ジョブサーバとがネットワークを介して接続されており、ジョブサーバが、ユーザ認証情報を暗号化・復号化するための公開鍵・秘密鍵を生成する処理と、ユーザ識別情報と公開鍵によって暗号化されているユーザ認証情報を印刷装置から受信する処理と、公開鍵によって暗号化されているユーザ認証情報を秘密鍵により復号化する処理と、ユーザ

識別情報と復号化されたユーザ認証情報を、その対応を記したユーザ認証ファイルを用いて認証を行う処理と、生成された公開鍵・秘密鍵を削除する処理とを実行する。

【０００４】

しかしながら、特開２００４－１１８７０９号公報では、ネットワーク上を流れるユーザ認証情報のセキュリティを確保することはできるが、プリントデータ（印刷ジョブ）がネットワーク上を流れるために、プリントデータのセキュリティを確保することはできないといった問題がある。

【特許文献１】特開２００４－１１８７０９号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

この発明は上述した問題点を解決するためになされたもので、この発明の目的の一つは、ネットワーク経由で受信されるプリントデータのセキュリティを確保した画像形成装置およびその画像形成装置で実行される出力判断プログラムおよび出力判断方法を提供することである。

【課題を解決するための手段】

【０００６】

上述した目的を達成するためにこの発明のある局面によれば、画像形成装置は、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成する鍵生成手段と、装置を識別するための識別情報を含む要求信号を受信する要求信号受信手段と、要求信号の受信に応じて、生成された暗号鍵および復号鍵の組と識別情報とを関連付けた関連付データを記憶する鍵テーブル記憶手段と、識別情報に関連付データにより関連付けられた暗号鍵を返信する暗号鍵返信手段と、識別情報が付加されたデータを、ネットワークを介して受信するデータ受信手段と、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号する復号手段と、復号されたデータを画像形成する画像形成手段と、画像形成手段による画像形成に応じて、受信されたデータに付加された識別情報に関連付けられた復号鍵を用いた復号手段による復号を禁止する禁止手段と、を備える。

【０００７】

この局面に従えば、暗号鍵と復号鍵との組が生成され、要求信号の受信に応じて、生成された暗号鍵および復号鍵の組と要求信号に含まれる識別情報とを関連付けた関連付データが記憶され、暗号鍵が返信される。そして、識別情報が付加されたデータがネットワークを介して受信されると、データに付加された識別情報と関連付データにより関連付けられた復号鍵を用いて受信されたデータが復号されて画像形成される。さらに、画像形成に応じて、受信されたデータに付加された識別情報に関連付けられた復号鍵を用いた復号が禁止される。このため、復号鍵を用いたデータの復号が１回の画像形成に制限されるので、例えば、画像形成装置にネットワークを介して送信途中のデータを第三者が取得した場合、その第三者がデータを復号することなく画像形成装置に送信しても、そのデータを復号するための復号鍵による復号が禁止されるので、第三者が送信したデータが復号されて画像形成されることがない。その結果、ネットワーク経由で受信されるデータのセキュリティを確保した画像形成装置を提供することができる。

【０００８】

好ましくは、禁止手段は、受信されたデータに付加された識別情報を含む関連付データを削除する削除手段を含む。

【０００９】

好ましくは、禁止手段は、復号手段に受信されたデータに付加された識別情報を含む関連付データの使用を禁止させる使用禁止手段を含む。

【００１０】

好ましくは、禁止手段は、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵および暗号鍵の組を鍵生成手段に生成させない生成禁止手段を含

む。

【００１１】

好ましくは、鍵生成手段は、要求信号の受信に応じて、暗号鍵および復号鍵の組を生成する。

【００１２】

好ましくは、鍵生成手段は、暗号鍵および復号鍵の組を予め複数生成して記憶する鍵記憶手段を含み、鍵記憶手段に記憶された複数の暗号鍵および復号鍵の組のうち識別情報に関連付けられていない組の数が所定数以下になると新たな組を生成する。

【００１３】

この発明の他の局面によれば、画像形成装置は、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶する鍵記憶手段と、装置を識別するための識別情報を含む要求信号を受信する要求信号受信手段と、要求信号の受信に応じて、鍵記憶手段に記憶された暗号鍵および復号鍵の複数の組のいずれか１つと識別情報とを関連付けた関連付データを記憶する鍵テーブル記憶手段と、識別情報に関連付データにより関連付けられた暗号鍵を返信する暗号鍵返信手段と、識別情報が付加されたデータを、ネットワークを介して受信するデータ受信手段と、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号する復号手段と、復号されたデータを画像形成する画像形成手段と、画像形成手段による画像形成に応じて、受信されたデータに付加された識別情報を含む関連付データを削除する削除手段と、を備える。

【００１４】

この局面に従えば、暗号鍵と復号鍵との組が複数記憶されており、要求信号の受信に応じて、暗号鍵および復号鍵の複数の組のいずれか１つと要求信号に含まれる識別情報とを関連付けた関連付データが記憶され、暗号鍵が返信される。そして、識別情報が付加されたデータがネットワークを介して受信されると、データに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータが復号されて画像形成される。さらに、画像形成に応じて、受信されたデータに付加された識別情報を含む関連付データが削除される。このため、復号鍵を用いたデータの復号が１回の画像形成に制限されるので、例えば、画像形成装置にネットワークを介して送信途中のデータを第三者が取得した場合、その第三者がデータを復号することなく画像形成装置に送信しても、データを復号するための復号鍵が記憶されていないので、第三者が送信したデータが復号されて画像形成されることがない。その結果、ネットワーク経由で受信されるデータのセキュリティを確保した画像形成装置を提供することができる。

【００１５】

好ましくは、復号手段により受信されたデータを復号できない場合には、データに付加された装置識別情報を予め定められた送信先に送信するメッセージ送信手段をさらに含む。

【００１６】

好ましくは、暗号化鍵と復号鍵とは、同じである。

【００１７】

この発明のさらに他の局面によれば、出力判断プログラムは、データが入力されると画像形成する画像形成手段を備えた画像形成装置で実行される出力判断プログラムであって、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成するステップと、装置を識別するための識別情報を含む要求信号を受信するステップと、要求信号の受信に応じて、生成された暗号鍵および復号鍵の組と識別情報とを関連付けた関連付データを記憶するステップと、識別情報に関連付データにより関連付けられた暗号鍵を返信するステップと、識別情報が付加されたデータを、ネットワークを介して受信するステップと、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号するステップと、復号されたデータを画像形成手段に画像形成させるステップと、画像形成手段による画像形成に応じ

て、受信されたデータに付加された識別情報に関連付けられた復号鍵を用いた復号を禁止するステップと、を画像形成装置に実行させる。

【００１８】

この発明に従えば、ネットワーク経由で受信されるデータのセキュリティを確保した出力判断プログラムを提供することができる。

【００１９】

この発明のさらに他の局面によれば、出力判断プログラムは、データが入力されると画像形成する画像形成手段を備えた画像形成装置で実行される出力判断プログラムであって、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶するステップと、装置を識別するための識別情報を含む要求信号を受信するステップと、要求信号の受信に応じて、暗号鍵および復号鍵の複数の組のいずれか１つと識別情報とを関連付けた関連付データを記憶するステップと、識別情報に関連付データにより関連付けられた暗号鍵を返信するステップと、識別情報が付加されたデータを、ネットワークを介して受信するステップと、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号するステップと、復号されたデータを画像形成装置に画像形成させるステップと、画像形成手段による画像形成に応じて、受信されたデータに付加された識別情報を含む関連付データを削除するステップと、を画像形成装置に実行させる。

【００２０】

この局面に従えば、ネットワーク経由で受信されるデータのセキュリティを確保した出力判断プログラムを提供することができる。

【００２１】

この発明のさらに他の局面によれば、出力判断方法は、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を生成するステップと、装置を識別するための識別情報を含む要求信号を受信するステップと、要求信号の受信に応じて、生成された暗号鍵および復号鍵の組と識別情報とを関連付けた関連付データを記憶するステップと、識別情報に関連付データにより関連付けられた暗号鍵を返信するステップと、識別情報が付加されたデータを、ネットワークを介して受信するステップと、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号するステップと、復号されたデータを画像形成するステップと、画像形成ステップによる画像形成に応じて、受信されたデータに付加された識別情報に関連付けられた復号鍵を用いた復号を禁止するステップとを、画像形成装置に実行させる。

【００２２】

この局面に従えば、ネットワーク経由で受信されるデータのセキュリティを確保した出力判断方法を提供することができる。

【００２３】

この発明のさらに他の局面によれば、出力判断方法は、データを暗号化するための暗号鍵と暗号鍵で暗号化されたデータを復号するための復号鍵との組を複数記憶するステップと、装置を識別するための識別情報を含む要求信号を受信するステップと、要求信号の受信に応じて、暗号鍵および復号鍵の複数の組のいずれか１つと識別情報とを関連付けた関連付データを記憶するステップと、識別情報に関連付データにより関連付けられた暗号鍵を返信するステップと、識別情報が付加されたデータを、ネットワークを介して受信するステップと、受信されたデータに付加された識別情報に関連付データにより関連付けられた復号鍵を用いて受信されたデータを復号するステップと、復号されたデータを画像形成するステップと、画像形成ステップによる画像形成に応じて、受信されたデータに付加された識別情報を含む関連付データを削除するステップと、を画像形成装置に実行させる。

【００２４】

この局面に従えば、ネットワーク経由で受信されるデータのセキュリティを確保した出力判断方法を提供することができる。

【発明を実施するための最良の形態】
【００２５】
以下、本発明の実施の形態について図面を参照して説明する。以下の説明では同一の部品には同一の符号を付してある。それらの名称および機能も同じである。したがってそれらについての詳細な説明は繰返さない。
【００２６】
＜第１の実施の形態＞
図１は、本発明の第１の実施の形態におけるネットワークシステムの全体概要を示す図である。図１を参照して、ネットワークシステムは、ＭＦＰ１００と、パーソナルコンピュータ（以下「ＰＣ」という）１０１，１０２とが、ネットワーク１０３にそれぞれ接続されている。ＭＦＰ１００は、複写機能、スキャナ機能、ファクシミリ送受信機能、プリント機能を備えた画像形成装置である。ネットワーク１０３は、有線および無線のいずれであってもよく、ＰＳＴＮ（Ｐｕｂｌｉｃ Ｓｗｉｔｃｈｅｄ Ｔｅｌｅｐｈｏｎｅ Ｎｅｔｗｏｒｋｓ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅｓ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、パケット交換網等の公衆網、ＬＡＮ（Ｌｏａｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）またはインターネット等のコンピュータネットワークを含む。ＰＣ１０１，１０２は、そのハード構成および機能は周知なのでここでは説明を繰り返さない。なお、図１は、ネットワーク１０３に、１台のＭＦＰ１００と、２台のＰＣ１０１，１０２が接続される例を示すが、台数を限定するものではなく、それぞれが少なくとも１台接続されていればよい。また、ＭＦＰ１００と、ＰＣ１０１，１０２とをネットワーク１０３で接続する例を示すが、シリアルインターフェースまたはパラレルインターフェースを用いて、直接接続するようにしてもよい。
【００２７】
本実施の形態におけるＭＦＰ１００は、ＰＣ１０１，１０２のいずれからもアクセスが可能であり、いずれか一方からプリントデータを、ネットワーク１０３を経由して受信すると、受信したプリントデータを画像形成する。プリントデータがネットワーク１０３を流れるため、ＭＦＰ１００は、ＰＣ１０１，１０２毎に暗号鍵を割り当てている。例えば、ユーザＡがＰＣ１０１でプリントデータを送信する操作をすると、ＰＣ１０１は、ＰＣ１０１に割り当てられた暗号鍵でプリントデータを暗号化してＭＦＰ１００に送信する。一方、ＭＦＰ１００はＰＣ１０１から受信したデータをＰＣ１０１に割り当てた暗号鍵で復号し、復号したプリントデータを画像形成する。ＰＣ１０１からＭＦＰ１００に送信したデータがネットワーク１０３を流れるので、ＰＣ１０２のユーザＢがそのデータを取得することが可能であるが、データはＰＣ１０１に割り当てられた暗号鍵で暗号化されているので、暗号鍵を知らないユーザＢは暗号化されたプリントデータを復号できず、プリントデータの内容がわからない。
【００２８】
さらに、本実施の形態におけるＭＦＰ１００は、ユーザＢが、ネットワークから取得したデータをＰＣ１０１に入力し、ＰＣ１０１からデータをそのままＭＦＰ１００に送信するような場合に備えて、そのようなデータを画像形成しないようにしている。なお、暗号鍵は、共通鍵であってもよく、公開鍵および秘密鍵の組であってもよい。以下、ＰＣ１０１からＭＦＰ１００にプリントデータを送信する場合を例に説明する。
【００２９】
図２は、ＭＦＰの外観を示す斜視図である。図２を参照して、ＭＦＰ１００は、自動原稿搬送装置（ＡＤＦ）１７と、画像読取部１３と、画像形成部１４と、給紙部１８とを含む。ＡＤＦは、原稿台に搭載された複数枚の原稿を１枚ずつ順にさばいて、画像読取部１３に搬送する。画像読取部１３は、写真、文字、絵等の画像情報を原稿から光学的に読み取って画像データを取得する。画像形成部１４は、画像データが入力されると、画像データに基づいて用紙等の記録シート上に画像を印刷する。給紙部１８は、記録シートを格納しており、格納した記録シートを１枚ずつ画像形成部１４に供給する。また、ＭＦＰ１００は、その上面に操作パネル１１を備える。

【００３０】
図３は、ＭＦＰのハード構成の一例を示すブロック図である。図３を参照して、ＭＦＰ１００は、情報処理部３０１と、ファクシミリ部３０２と、通信制御部３０３と、画像読取部１３と、画像形成部１４と、給紙部１８と、ＡＤＦ１７とを含む。情報処理部３０１は、中央演算装置（ＣＰＵ）３１１と、ＣＰＵ３１１の作業領域として使用されるＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）３１１ａと、画像メモリ３１２と、データを不揮発的に記憶するためのハードディスクドライブ（ＨＤＤ）３２１と、タイマ３２０と、表示部３１３と、操作部３１０と、データ通信制御部３０９と、データ入出力部３０８とを含む。ＣＰＵ３１１は、データ入出力部３０８、データ通信制御部３０９、操作部３１０、画像メモリ３１２および表示部３１３とそれぞれ接続され、情報処理部３０１の全体を制御する。また、ＣＰＵ３１１は、ファクシミリ部３０２、通信制御部３０３、画像読取部１３、画像形成部１４、給紙部１８およびＡＤＦ１７と接続され、ＭＦＰ１００の全体を制御する。画像メモリ３１２は、画像形成部１４で印刷するための画像データを記憶する。タイマ３２０は、時間を計時し、計時した時刻をＣＰＵ３１１に出力する。
【００３１】
表示部３１３は、液晶表示装置（ＬＣＤ）、有機ＥＬＤ（Ｅｌｅｃｔｒｏ Ｌｕｍｉｎｅｓｃｅｎｃｅ Ｄｉｓｐｌａｙ）等の表示装置であり、ユーザに対する指示メニューや取得した画像データに関する情報等を表示する。操作部３１０は、複数のキーを備え、キーに対応するユーザの操作による各種の指示、文字、数字などのデータの入力を受付ける。操作部３１０は、表示部３１３上に設けられたタッチパネルを含む。表示部３１３と操作部３１０とで、操作パネル１１が構成される。
【００３２】
データ通信制御部３０９は、データ入出力部３０８と接続される。データ通信制御部３０９は、ＣＰＵ３１１からの指示に従って、データ入出力部３０８を制御して、データ入出力部３０８に接続された外部の機器との間でデータを送受信する。データ入出力部３０８は、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）で通信するためのインターフェースであるＬＡＮ端子３１４、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）端子３１５、セントロニクス端子３１６、ＲＳ－２３２Ｃ（Ｒｅｃｏｍｍｅｎｄｅｄ Ｓｔａｎｄａｒｄ ２３２ Ｖｅｒｓｉｏｎ Ｃ）等のシリアルインターフェース端子３１７、およびＪＴＡＧ（Ｊｏｉｎｔ Ｔｅｓｔ Ａｃｔｉｏｎ Ｇｒｏｕｐ）端子３１８を有する。
【００３３】
ＭＦＰ１００は、ＬＡＮ端子３１４に、ネットワーク１０３に接続するためのＬＡＮケーブルが接続される場合、データ通信制御部３０９は、データ入出力部３０８を制御してＬＡＮ端子３１４を介して接続されたＰＣ１０１，１０２と通信する。ＵＳＢ端子３１５、セントロニクス端子３１６、シリアルインターフェース端子３１７、ＪＴＡＧ端子３１８のいずれかに機器が接続された場合、データ通信制御部３０９は、データ入出力部３０８を制御して、接続された機器との間で通信してデータを入出力する。ＵＳＢ端子３１５には、フラッシュメモリを内蔵したＵＳＢメモリ３１９が接続される。ＵＳＢメモリ３１９には、後述する出力判断プログラムが記憶されており、ＣＰＵ３１１は、データ通信制御部３０９を制御して、ＵＳＢメモリ３１９から出力判断プログラムを読出し、読み出した出力判断プログラムをＲＡＭ３１１ａに記憶し、実行する。
【００３４】
なお、出力判断プログラムを記憶する記録媒体としては、ＵＳＢメモリ３１９に限られず、フレキシブルディスク、カセットテープ、光ディスク（ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ－Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）／ＭＯ（Ｍａｇｎｅｔｉｃ Ｏｐｔｉｃａｌ Ｄｉｓｃ／ＭＤ（Ｍｉｎｉ Ｄｉｓｃ）／ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ））、ＩＣカード（メモリカードを含む）、光カード、マスクＲＯＭ、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｏｎｉｃａｌｌｙ ＥＰＲＯＭ）などの半導体メモリ等の固定的にプロ

グラムを担持する媒体でもよい。ここでいうプログラムは、ＣＰＵ３１１により直接実行可能なプログラムだけでなく、ソースプログラム形式のプログラム、圧縮処理されたプログラム、暗号化されたプログラム等を含む。

【００３５】

ファクシミリ部３０２は、ＰＳＴＮに接続され、ＰＳＴＮにファクシミリデータを送信するまたはＰＳＴＮからファクシミリデータを受信する。ファクシミリ部３０２は、受信したファクシミリデータを、画像形成部１４で印刷可能なプリントデータに変換して、画像形成部１４に出力する。これにより、画像形成部１４は、ファクシミリ部３０２により受信されたファクシミリデータを記録シートに印刷する。

【００３６】

通信制御部３０３は、ＣＰＵ３１１をＰＳＴＮに接続するためのモデムである。通信制御部３０３は、ＰＳＴＮに接続された他のコンピュータとの間で通信する。これにより、ＣＰＵ３１１は、ＰＳＴＮを介して他のコンピュータとデータの送受信が可能となる。ＭＦＰ１００を、ＰＣ１０１，１０２とＰＳＴＮを介して接続する場合に、通信制御部３０３が用いられる。

【００３７】

図４は、第１の実施の形態におけるＰＣで実行される暗号データ作成処理の流れの一例を示すフローチャートである。この暗号データ作成処理は、例えば、アプリケーションプログラムを実行するＰＣ１０１に、プリント指示が入力されたときにＰＣ１０１で実行される処理である。プリント指示には、データを暗号化するか否かの指示が含まれる。図４を参照して、ＰＣ１０１は、プリント指示が入力されると、プリント対象となるデータからプリントデータを作成する（ステップＳ１０１）。そして、暗号化が指示されていれば（ステップＳ１０２でＹＥＳ）処理をステップＳ１０３に進め、指示されていなければ（ステップＳ１０２でＮＯ）処理をステップＳ１０７に進める。ＰＣ１０１は、暗号化が指示されていなければ、ステップＳ１０１で作成したプリントデータをそのままＭＦＰ１００に送信して（ステップＳ１０７）、処理を終了する。一方、ＰＣ１０１は、暗号化が指示されていればＭＦＰ１００に公開鍵の送信を要求し（ステップＳ１０３）、公開鍵を受信するまで待機状態となる（ステップＳ１０４でＮＯ）。公開鍵を受信すると（ステップＳ１０４でＹＥＳ）、ステップＳ１０１で作成したプリントデータを暗号化し（ステップＳ１０５）、暗号化した暗号データをＭＦＰ１００に送信する（ステップＳ１０６）。

【００３８】

図５は、ＭＦＰのＣＰＵの機能の概要をＨＤＤで記憶する情報とともに示す機能ブロック図である。図５を参照して、ＣＰＵ３１１は、ＰＣ１０１から送信されてくる公開鍵の送信要求を受付けるための要求受付部１５１と、送信要求してきたＰＣ１０１と公開鍵および秘密鍵とを関連付けるための関連付部１５２と、公開鍵をＰＣ１０１に送信する公開鍵送信部１５４とを含む。

【００３９】

暗号データ受付部１５１は、データ入出力部３０８が出力する公開鍵の送信要求を受付ける。ネットワーク１０３に接続されたＰＣ１０１が公開鍵の送信要求をＭＦＰ１００に送信すると、データ入出力部３０８により公開鍵の送信要求が受信される。データ入出力部３０８は、受信した公開鍵の送信要求と、ＰＣ１０１に割り当てられたＩＰアドレスとを要求受付部１５１に出力する。要求受付部１５１は、送信要求が入力されると、ＰＣ１０１のＩＰアドレスを関連付部１５２に出力する。ＰＣ１０１に割り当てられたＩＰアドレスは、ＰＣ１０１を識別するための識別情報である。なお、ここでは、識別情報にＰＣ１０１に割り当てられたＩＰアドレスを用いたが、ＰＣ１０１またはその周辺装置に割り当てられたＭＡＣアドレスを用いるようにしてもよい。また、ＭＦＰ１００にプリントさせる場合にＭＦＰ１００においてユーザ認証が求められる場合には、ＰＣ１０１でプリント指示をする際に、ユーザの識別情報および認証情報の入力を要求するようにして、ＰＣ１０１の識別情報に代えて、ユーザの識別情報を用いるようにしてもよい。これにより、ユーザごとに、プリント対象となるデータのネットワーク１０３上のセキュリティを確保

することができる。

【００４０】

関連付部１５２は、要求受付部１５１からＰＣ１０１のＩＰアドレスが入力されると、そのＩＰアドレスと秘密鍵と公開鍵の組とを関連付けた関連付データを生成して、ＨＤＤ３２１に記憶するとともに、ＩＰアドレスおよび公開鍵を公開鍵送信部１５４に出力する。これにより、関連付データ３２１ＡがＨＤＤ３２１に記憶される。関連付部１５２は、鍵生成部１５３を含み、鍵生成部１５３は、秘密鍵と公開鍵の組を生成する。公開鍵送信部１５４は、入力されるＩＰアドレス宛に公開鍵を送信する。これにより、データ入出力部３０８からＰＣ１０１に公開鍵が送信される。

【００４１】

さらに、ＣＰＵ３１１は、ネットワーク１０３を介して送信されてきた暗号化された暗号データを受付けるための暗号データ受付部１６１と、暗号データを送信してきたＰＣ１０１に関連付けた秘密鍵を抽出するための鍵管理部１６２と、受付けられた暗号データを秘密鍵で復号するための復号部１７０と、エラー送信部１６４とを含む。

【００４２】

暗号データ受付部１６１は、データ入出力部３０８が出力する暗号データを受付ける。ネットワーク１０３に接続されたＰＣ１０１が暗号データをＭＦＰ１００に送信すると、データ入出力部３０８により暗号データが受信される。データ入出力部３０８は、受信した暗号データと、ＰＣ１０１に割り当てられたＩＰアドレスとを暗号データ受付部１６１に出力する。暗号データ受付部１６１は、暗号データを復号部１７０に出力するとともに、ＰＣ１０１に割り当てられたＩＰアドレスを鍵管理部１６２に出力する。

【００４３】

鍵管理部１６２は、暗号データ受付部１６１からＰＣ１０１のＩＰアドレスが入力されると、そのＩＰアドレスに関連付データ３２１Ａにより関連付けられた秘密鍵を復号部１７０に出力する。鍵管理部１６２は、秘密鍵抽出部１６３を含み、秘密鍵抽出部１６３は、暗号データ受付部１６１からＰＣ１０１のＩＰアドレスが入力されると、そのＩＰアドレスでＨＤＤ３２１に記憶されている関連付データ３２１Ａを検索し、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１Ａを抽出する。秘密鍵抽出部１６３は、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１Ａを抽出できた場合には、その関連付データ３２１Ａに含まれる秘密鍵を復号部１７０に出力し、ＰＣ１０１のＩＰアドレスをエラー送信部１６４に出力する。ＰＣ１０１のＩＰアドレスをエラー送信部１６４に出力するのは、後述する復号部１７０で復号できなかった場合に、エラー送信部１６４がエラーメッセージを送信するためである。一方、鍵抽出部は、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１ＡがＨＤＤ３２１に記憶されていない場合には、ＰＣ１０１のＩＰアドレスとエラー信号とをエラー送信部１６４に出力する。鍵管理部１６２は、また、復号部１７０から暗号データを復号できたか否かを示す信号が入力され、復号できたことを示す信号が入力されると、秘密鍵抽出部１６３が抽出した関連付データ３２１Ａを使用できないようにする。具体的には、秘密鍵抽出部１６３は、秘密鍵抽出部１６３が抽出した関連付データ３２１ＡをＨＤＤ３２１から削除する。

【００４４】

復号部１７０は、暗号データ受付部１６１から暗号データが入力され、鍵管理部１６２から秘密鍵が入力され、暗号データを秘密鍵で復号する。復号部１７０は、暗号データを復号できた場合は、暗号データを復号したプリントデータを画像形成部１４に出力するとともに、復号できたことを示す信号を鍵管理部１６２に出力する。これにより、画像形成部１４で、プリントデータが用紙などの記録媒体に画像として形成される。一方、復号部１７０は、暗号データを復号できない場合は、エラー信号をエラー送信部１６４に出力する。

【００４５】

エラー送信部１６４は、秘密鍵抽出部１６３からエラー信号が入力される場合、または、復号部１７０からエラー信号が入力される場合、予めＨＤＤ３２１に記憶された送信先

に、秘密鍵抽出部１６３から入力されるＩＰアドレスとエラーメッセージとを送信する。送信方法は、特に限定するわけではないが、電子メールで送信する。エラーメッセージは、不正なプリントがされたことを示し、例えば、「＊＊＊＊のＰＣから不正なプリント指示がありました。」などである。

【００４６】

図６は、ＨＤＤに記憶される関連付データの一例を示す図である。図６を参照して、関連付データ３２１Ａは、公開鍵Ａおよび秘密鍵Ｂの組と、ＩＰアドレスＡとを関連付ける。ここでは、１つの関連付データ３２１Ａが記憶される場合を示しているが、複数が記憶される場合もあり得る。

【００４７】

図７は、第１の実施の形態におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。図７を参照して、ＣＰＵ３１１は、鍵要求信号を受信したか否かを判断し（ステップＳ０１）、受信したならば処理をステップＳ０２に進め、受信しなければ受信するまで待機状態となる（ステップＳ０１でＮＯ）。ここでは、ＰＣ１０１から要求信号を受信する場合を例に説明する。そして、ＣＰＵ３１１は、ＰＣ１０１に割り当てられたＩＰアドレスを取得し（ステップＳ０２）、鍵を生成する（ステップＳ０３）。生成する鍵は、共通鍵であってもよいし、公開鍵と秘密鍵との組であってもよい。ここでは、公開鍵と秘密鍵とを生成する場合を説明する。そして、ＣＰＵ３１１は、ステップＳ０２で取得したＩＰアドレスと、ステップＳ０３で生成した公開鍵および秘密鍵の組とを関連付けた関連付データを生成し（ステップＳ０４）、ＨＤＤ３２１に記憶し（ステップＳ０５）、さらに、ステップＳ０２で取得したＩＰアドレス宛に公開鍵のみを送信する（ステップＳ０６）。これにより、ＰＣ１０１で公開鍵が受信される。

【００４８】

図８は、第１の実施の形態におけるＭＦＰのＣＰＵで実行される印刷処理の流れの一例を示すフローチャートである。図８を参照して、ＣＰＵ３１１は、プリントデータを受信したか否かを判断し（ステップＳ１１）、受信したならば処理をステップＳ１２に進め、受信しなければプリントデータを受信するまで待機状態となる（ステップＳ１１でＮＯ）。ステップＳ１２では、受信したプリントデータが暗号データか否かを判断し、暗号データならば処理をステップＳ１３に進め、暗号データでなければ処理をステップＳ２１に進める。ステップＳ２１では、受信したプリントデータをそのまま画像形成部１４に出力する。これにより、画像形成部１４でプリントデータが用紙等の記録媒体に画像形成される。

【００４９】

以下、ステップＳ１１において、ＰＣ１０１からプリントデータを暗号化した暗号データを受信する場合を例に説明する。ＣＰＵ３１１は、ＰＣ１０１に割り当てられたＩＰアドレスを取得し（ステップＳ１３）、ＰＣ１０１に割り当てられたＩＰアドレスを含む関連付データ３２１ＡがＨＤＤ３２１に記憶されているか否かを判断する（ステップＳ１４）。そのような関連付データ３２１Ａが記憶されていれば処理をステップＳ１５に進めるが、記憶されていなければ処理をステップＳ２０に進める。ＣＰＵ１０１は、ＨＤＤ３２１に記憶されている関連付データ３２１Ａを検索し、ＩＰアドレスを含む関連付データ３２１Ａを抽出する。ＩＰアドレスを抽出できたならば、記憶されていると判断し、抽出できなければ記憶されていないと判断する。

【００５０】

そして、ＣＰＵ３１１は、ステップＳ１４で抽出した関連付データ３２１Ａから秘密鍵を取得し（ステップＳ１５）、ステップＳ１１で受信したプリントデータを秘密鍵で復号する（ステップＳ１６）。そして、ＣＰＵ３１１は、暗号データを復号できたか否かを判断し（ステップＳ１７）、正しく復号できた場合には処理をステップＳ１８に進め、正しく復号できなければ処理をステップＳ２０に進める。ＣＰＵ３１１は、暗号データを復号したプリントデータを画像形成部１４に出力する（ステップＳ１８）。これにより、画像形成部１４でプリントデータが用紙等の記録媒体に画像形成される。次に、ＣＰＵ３１１

は、ステップＳ１４で抽出した関連付データ３２１ＡをＨＤＤ３２１から消去し（ステップＳ１９）、処理を終了する。

【００５１】

一方、ステップＳ２０に進む場合は、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１ＡがＨＤＤ３２１に記憶されていない場合、または、記憶されているがその関連付データ３２１Ａに含まれる秘密鍵で暗号データを正しく復号できない場合である。そのような場合、ＣＰＵ３１１は、ＨＤＤ３２１に予め記憶された送信先に、ステップＳ１３で取得したＰＣ１０１のＩＰアドレスとエラーメッセージとを含む電子メールを送信する。予め記憶された送信先は、ＰＣ１０１を主に使用するユーザの電子メールアドレス、またはＭＦＰ１００の管理者の電子メールアドレスが好ましい。これにより、不正なプリントがされたことを管理者またはＰＣ１０１を主に使用するユーザに知らせることができる。

【００５２】

以上説明したように第１の実施の形態におけるＭＦＰ１００は、ＰＣ１０１から要求信号を受信すると、公開鍵と秘密鍵との組を生成し、生成した公開鍵および秘密鍵の組とＰＣ１０１のＩＰアドレスとを関連付けた関連付データ３２１ＡをＨＤＤ３２１に記憶し、公開鍵をＰＣ１０１に返信する。そして、ＰＣ１０１から暗号データをネットワーク１０３を介して受信すると、ＰＣ１０１のＩＰアドレスと関連付データにより関連付けられた秘密鍵を用いて受信した暗号データを復号して画像形成する。さらに、画像形成に応じて、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１Ａを消去する。このため、秘密鍵を用いた暗号データの復号が１回に制限されるので、例えば、ＰＣ１０１からＭＦＰ１００にネットワーク１０３を介して送信途中の暗号データがＰＣ１０２で取得され、復号することなく再度ＭＦＰ１００に送信されたとしても、その暗号データを復号するための秘密鍵が記憶されていないので、復号されて画像形成されることがない。その結果、ネットワーク経由で受信されるデータのセキュリティを確保することができる。

【００５３】

＜第１の変形例＞

上述した第１の実施の形態におけるＭＦＰ１００は、プリントデータの画像形成後に、関連付データ３２１Ａを削除するものであった。第１の変形例におけるＭＦＰ１００は、使用済みの関連付データ３２１ＡをＨＤＤ３２１から消去することなく、使用履歴を記憶しておくようにしたものである。その他の構成は、上述したＭＦＰ１００と同じなのでここでは説明を繰り返さない。

【００５４】

図９は、第１の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す図である。図９を参照して、関連付データ３２１Ａは、公開鍵Ｅおよび秘密鍵Ｅの組と、ＩＰアドレスＥとを関連付ける。また、その他の公開鍵Ａ～Ｄおよび秘密鍵Ａ～Ｄのそれぞれの組は、既に使用されたことを示す印「使用済み」が付されている。

【００５５】

第１の変形例におけるＭＦＰ１００は、図５に示した機能ブロック図と同様の構成を有するが、鍵生成部１５３は、新たに鍵を生成する場合、関連付データ３２１Ａに含まれる公開鍵および秘密鍵の組と同じ公開鍵および秘密鍵の組の生成が禁止される。このため、鍵生成部１５３は、新たに鍵を生成する場合、関連付データ３２１Ａを参照して、関連付データ３２１Ａに含まれる公開鍵および秘密鍵の組とは異なる公開鍵および秘密鍵の組を生成する。また、鍵管理部１６２は、復号部１７０で暗号データを正しく復号できた場合には、関連付データ３２１Ａに含まれるＩＰアドレスを、「使用済み」の印に書き換える。これにより、同一の公開鍵および秘密鍵の組が複数生成されることがないので、プリントデータのセキュリティをより確実なものとすることができる。

【００５６】

図１０は、第１の変形例におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。図１０を参照して、図７に示した処理と同じ処理には同じ符号を付してある。図７に示した処理と異なる点は、ステップＳ０３の処理をステップＳ

０３Ａの処理に変更した点である。ＣＰＵ３１１は、ステップＳ０３Ａでは、関連付データ３２１Ａを参照して、関連付データ３２１Ａに含まれる公開鍵および秘密鍵の組とは異なる公開鍵および秘密鍵の組を生成する。

【００５７】

図１１は、第１の変形例におけるＭＦＰのＣＰＵで実行される印刷処理の流れの一例を示すフローチャートである。図１１を参照して、図８に示した処理と同じ処理には同じ符号を付してある。図８に示した処理と異なる点は、ステップＳ１９に代えてステップＳ１９Ａが実行される点である。ＣＰＵ３１１は、ステップＳ１９Ａでは、ステップＳ１４で抽出した関連付データ３２１Ａを使用禁止に設定する。具体的には、関連付データ３２１Ａに含まれるＩＰアドレスを、「使用済み」の印に書き換える。

【００５８】

以上説明したように、第１の変形例におけるＭＦＰ１００は、使用済みの関連付データ３２１ＡをＨＤＤ３２１から消去することなく、使用履歴を記憶しておくようにし、使用済みの関連付データの使用を禁止させ、使用済みの関連付データに含まれる公開鍵と秘密鍵の組と同一の組を生成しないようにしたので、ネットワーク１０３上を流れるプリントデータのセキュリティをより確実なものとすることができる。

【００５９】

＜第２の変形例＞

上述した第１の実施の形態におけるＭＦＰ１００は、ＰＣ１０１から公開鍵の送信を要求する要求信号が受信されると、鍵を生成するようにしたが、第２の変形例におけるＭＦＰ１００は、予め未使用の鍵を生成しておき、要求信号の受信に応じて未使用の鍵を割り当てるようにしたものである。要求信号の受信から公開鍵の送信までの間に鍵を生成する必要がないので、処理時間を短縮することができる。

【００６０】

第２の変形例におけるＭＦＰ１００は、図５に示した機能ブロック図と同様の構成を有するが、鍵生成部１５３は、関連付データ３２１Ａを参照して、未使用の関連付データ３２１Ａが予め定められた数を下回った時点で、新たに公開鍵および秘密鍵の組を生成してＨＤＤ３２１に関連付データ３２１Ａを記憶する。また、関連付部１５２は、要求受付部１５１からＰＣ１０１のＩＰアドレスが入力されると、そのＩＰアドレスにＨＤＤ３２１に記憶されている関連付データ３２１Ａのうち未使用の関連付データを割り当てる。

【００６１】

図１２は、第２の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す第１の図である。図１２を参照して、図６に示した関連付データ３２１Ａと異なる点は、ＩＰアドレスに割り当てられていないことを示す印「未割り当て」が付された公開鍵Ｂおよび秘密鍵Ｂの組と、公開鍵Ｃおよび秘密鍵Ｃの組と、公開鍵Ｄおよび秘密鍵Ｄの組とを含む点である。

【００６２】

図１３は、第２の変形例におけるＭＦＰのＣＰＵで実行される鍵生成処理の流れの一例を示すフローチャートである。図１３を参照して、ＣＰＵ３１１は、関連付データ３２１ＡのうちＩＰアドレスが割り当てられていないことを示す印「未割り当て」が付された未使用の関連付データの数がしきい値Ｔより小さいか否かを判断し（ステップＳ３１）、しきい値Ｔより小さければ処理をステップＳ３２に進め、しきい値Ｔより小さくなければ処理を終了する。ＣＰＵ３１１は、ステップＳ３２では、新たな公開鍵と秘密鍵の組を生成してＨＤＤ３２１に記憶する（ステップＳ３３）。この際、公開鍵と秘密鍵の組にＩＰアドレスが割り当てられていないことを示す印「未割り当て」を付して記憶する。これにより、しきい値Ｔの数の未使用の関連付データ３２１ＡがＨＤＤ３２１に記憶される。

【００６３】

図１４は、第２の変形例におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。図１４を参照して、図７に示した処理と同じ処理には同じ符号を付してある。図７に示した処理と異なる点は、ステップＳ０３～ステップＳ０５が

削除され、ステップＳ０３Ｂが追加された点である。ＣＰＵ３１１は、ステップＳ０３Ｂでは、関連付データ３２１Ａを参照して、ＩＰアドレスが割り当てられていないことを示す印「未割り当て」が付された公開鍵Ｂおよび秘密鍵Ｂの組を含む関連付データ３２１Ａを選択し、ステップＳ０２で取得したＰＣ１０１のＩＰアドレスを割り当てる。そして、ステップＳ０２で取得したＩＰアドレス宛に、ステップＳ０４Ｂで選択した関連付データ３２１Ａに含まれる公開鍵Ｂのみを送信する（ステップＳ０６）。

【００６４】

第２の変形例におけるＭＦＰ１００のＣＰＵでは、図８に示した印刷処理が実行される。なお、第２の変形例におけるＭＦＰ１００のＣＰＵで、図１１に示した印刷処理を実行するようにしてもよい、この場合には、関連付データ３２１Ａは、図１５に示すように、使用済みの関連付けデータ３２１Ａを履歴情報として含むことになる。図１５は、第２の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す第２の図である。

【００６５】

第２の変形例におけるＭＦＰ１００は、予め未使用の公開鍵および秘密鍵の組を複数生成し、要求信号の受信に応じて未使用の鍵を割り当てるようにしたので、要求信号の受信から公開鍵の送信までの処理時間を短縮することができる。また、未使用の鍵の組の数が所定数以下になると新たな組を生成するようにしたので、複数の要求信号が同時に受信されたとしても未使用の鍵の組を直ちに割り当てることができる。

【００６６】

＜第２の実施の形態＞

第１の実施の形態におけるＭＦＰ１００は、鍵を生成するようにしたが、第２の実施の形態におけるＭＦＰ１００は、複数の鍵を予め記憶しておくようにしたものである。以下、第１の実施の形態におけるＭＦＰ１００と異なる点を主に説明する。

【００６７】

図１６は、第２の実施の形態におけるＭＦＰのＣＰＵの機能の概要をＨＤＤで記憶する情報とともに示す機能ブロック図である。図１６を参照して、ＨＤＤ３２１には、鍵データ３２１Ｂが予め記憶される。鍵データ３２１Ｂは、公開鍵と秘密鍵との組を複数含む。ＣＰＵ３１１は、要求受付部１５１と、関連付部１５２Ａと、公開鍵送信部１５４とを含む。関連付部１５２Ａは、要求受付部１５１からＰＣ１０１のＩＰアドレスが入力されると、鍵データ３２１Ｂで定義された複数の公開鍵および秘密鍵の組のうちからランダムに１つを抽出して、抽出した公開鍵および秘密鍵の組とＰＣ１０１のＩＰアドレスとを関連付けた関連付データを生成して、ＨＤＤ３２１に記憶するとともに、ＩＰアドレスおよび公開鍵を公開鍵送信部１５４に出力する。これにより、関連付データ３２１ＡがＨＤＤ３２１に記憶される。

【００６８】

さらに、ＣＰＵ３１１は、暗号データ受付部１６１と、暗号データを送信してきたＰＣ１０１に関連付けた秘密鍵を抽出するための秘密鍵抽出部１６３と、復号部１７０と、エラー送信部１６４と、データ削除部１６５とを含む。暗号データ受付部１６１は、データ入出力部３０８が出力する暗号データを受付け、暗号データを復号部１７０に出力するとともに、ＰＣ１０１に割り当てられたＩＰアドレスを秘密鍵抽出部１６３に出力する。

【００６９】

秘密鍵抽出部１６３は、暗号データ受付部１６１からＰＣ１０１のＩＰアドレスが入力されると、そのＩＰアドレスでＨＤＤ３２１に記憶されている関連付データ３２１Ａを検索し、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１Ａを抽出する。秘密鍵抽出部１６３は、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１Ａを抽出できた場合には、その関連付データ３２１Ａに含まれる秘密鍵を復号部１７０に出力し、ＰＣ１０１のＩＰアドレスをエラー送信部１６４に出力する。一方、秘密鍵抽出部１６３は、ＰＣ１０１のＩＰアドレスを含む関連付データ３２１ＡがＨＤＤ３２１に記憶されていない場合には、ＰＣ１０１のＩＰアドレスとエラー信号とをエラー送信部１６４に出力する。

【００７０】

復号部１７０は、暗号データを復号できた場合は、暗号データを復号したプリントデータを画像形成部１４に出力するとともに、暗号データを復号できたことを示す信号をデータ削除部１６５に出力する。復号部１７０は、暗号データを復号できない場合は、エラー信号をエラー送信部１６４に出力する。

【００７１】

データ削除部１６５は、復号部１７０から暗号データを復号できたか否かを示す信号が入力され、復号できたことを示す信号が入力されると、秘密鍵抽出部１６３が抽出した関連付データ３２１ＡをＨＤＤ３２１から削除する。関連付データが削除されるので、その後、ＰＣ１０１，１０２から暗号データが送信されてきたとしてもその暗号データは復号されることなく、プリントデータが画像形成されない。

【００７２】

図１７（Ａ）は、第２の実施の形態におけるＭＦＰ１００のＨＤＤ３２１に記憶される鍵データの一例を示す図である。図１７（Ａ）を参照して、鍵データ３２１Ｂは、公開鍵と秘密鍵との組を複数含む。ここでは、鍵データ３２１Ｂが、１０組の公開鍵と秘密鍵を含む例を示している。図１７（Ｂ）は、第２の実施の形態におけるＭＦＰ１００のＨＤＤ３２１に記憶される関連付データの一例を示す図である。図１７（Ｂ）を参照して、関連付データ３２１Ａは、図６に示した関連付データ３２１Ａと同じである。

【００７３】

図１８は、第２の実施の形態におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。図１８を参照して、図７に示した鍵送信処理と異なる点は、ステップＳ０３の処理をステップＳ０３Ｃの処理に変更した点である。ＣＰＵ３１１は、ＰＣ１０１に割り当てられたＩＰアドレスを取得すると（ステップＳ０２）、鍵データ３２１Ｂで定義された複数の公開鍵および秘密鍵の組のうちからランダムに１つを抽出する（ステップＳ０３Ｃ）。そして、抽出した公開鍵および秘密鍵の組とＰＣ１０１のＩＰアドレスとを関連付けた関連付データを生成する（ステップＳ０４）。

【００７４】

第２の実施の形態におけるＭＦＰ１００のＣＰＵでは、図８に示した印刷処理が実行される。

【００７５】

以上説明したように第２の実施の形態におけるＭＦＰ１００は、公開鍵と秘密鍵の組の複数を予め記憶しておき、要求信号の受信に応じて、暗号鍵および復号鍵の複数の組のいずれか１つとＰＣ１０１のＩＰアドレスとを関連付けた関連付データ３２１Ａを生成するようにしたので、公開鍵と秘密鍵の組を生成する必要がなく、ＭＦＰ１００の負荷を低減して処理速度を速くすることができる。また、画像形成に応じて、ＰＣ１０１のＩＰデータを含む関連付データを削除するので、ネットワーク上を流れるプリントデータのセキュリティを確保することができる。

【００７６】

なお、上述した実施の形態においては、ＭＦＰ１００について説明したが、図７、図８、図１０、図１１、図１３、図１４および図１８に示した処理をＣＰＵ３１１に実行させるための出力判断方法、または出力判断プログラムとして、本発明を把握できることは言うまでもない。

【００７７】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

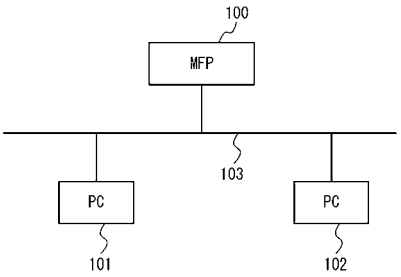
【図面の簡単な説明】

【００７８】

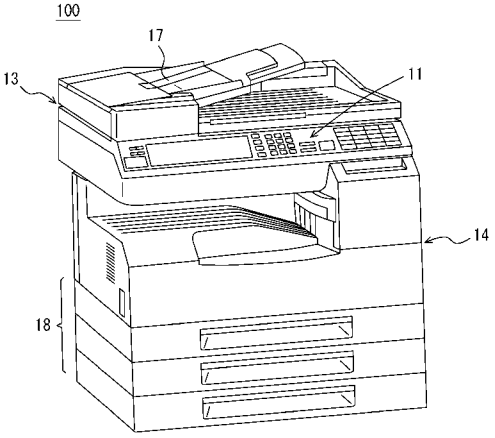
【図１】本発明の第１の実施の形態におけるネットワークシステムの全体概要を示す図である。

【図２】ＭＦＰの外観を示す斜視図である。
【図３】ＭＦＰのハード構成の一例を示すブロック図である。
【図４】第１の実施の形態におけるＰＣで実行される暗号データ作成処理の流れの一例を示すフローチャートである。
【図５】ＭＦＰのＣＰＵの機能の概要をＨＤＤで記憶する情報とともに示す機能ブロック図である。
【図６】ＨＤＤに記憶される関連付データの一例を示す図である。
【図７】第１の実施の形態におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。
【図８】第１の実施の形態におけるＭＦＰのＣＰＵで実行される印刷処理の流れの一例を示すフローチャートである。
【図９】第１の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す図である。
【図１０】第１の変形例におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。
【図１１】第１の変形例におけるＭＦＰのＣＰＵで実行される印刷処理の流れの一例を示すフローチャートである。
【図１２】第２の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す第１の図である。
【図１３】第２の変形例におけるＭＦＰのＣＰＵで実行される鍵生成処理の流れの一例を示すフローチャートである。
【図１４】第２の変形例におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。
【図１５】第２の変形例におけるＭＦＰのＨＤＤに記憶される関連付データの一例を示す第２の図である。
【図１６】第２の実施の形態におけるＭＦＰのＣＰＵの機能の概要をＨＤＤで記憶する情報とともに示す機能ブロック図である。
【図１７】第２の実施の形態におけるＭＦＰのＨＤＤに記憶される鍵データおよび関連付データの一例を示す図である。
【図１８】第２の実施の形態におけるＭＦＰのＣＰＵで実行される鍵送信処理の流れの一例を示すフローチャートである。
【符号の説明】
【００７９】
１３　画像読取部、１４　画像形成部、１７　ＡＤＦ、１８　給紙部、１００　ＭＦＰ、１０１，１０２　ＰＣ、１０３　ネットワーク、１５１　要求受付部、１５２，１５２Ａ　関連付部、１５３　鍵生成部、１５４　公開鍵送信部、１６１　暗号データ受付部、１６２　鍵管理部、１６３　秘密鍵抽出部、１６４　エラー送信部、１６５　データ削除部、１７０　復号部、３０１　情報処理部、３０２　ファクシミリ部、３０３　通信制御部、３０８　データ入出力部、３０９　データ通信制御部、３１０　操作部、３１２　画像メモリ、３１３　表示部、３１９　ＵＳＢメモリ、３２１　ＨＤＤ、３２１Ａ　関連付データ、３２１Ｂ　鍵データ。

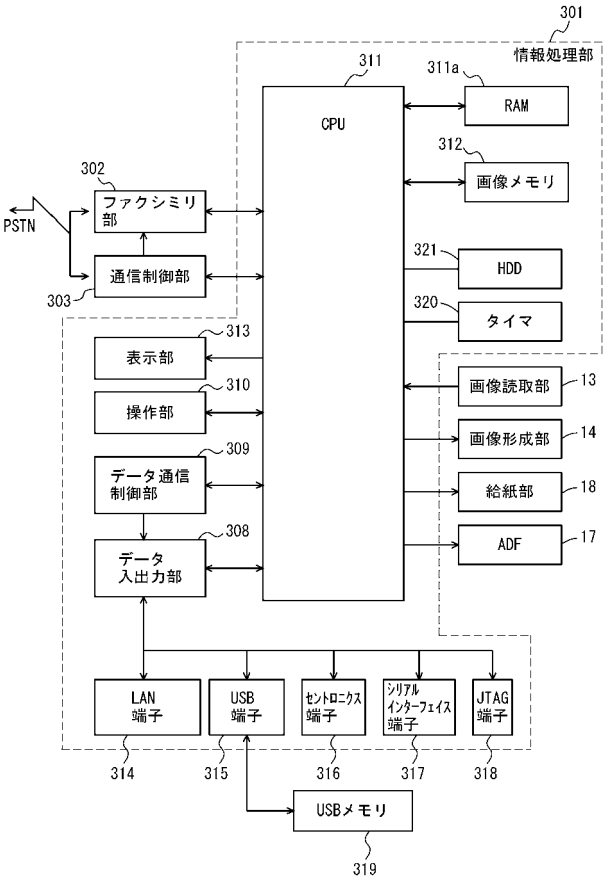
【図１】



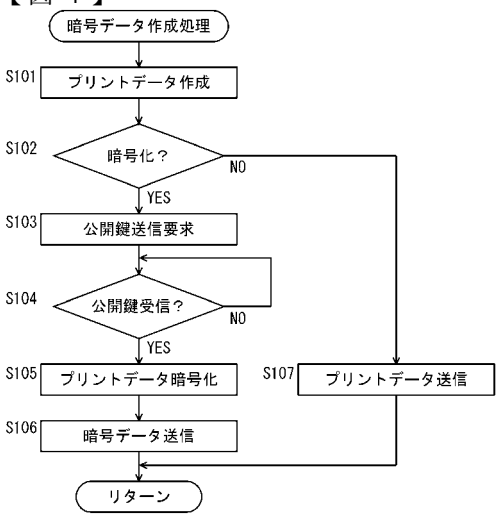

【図２】



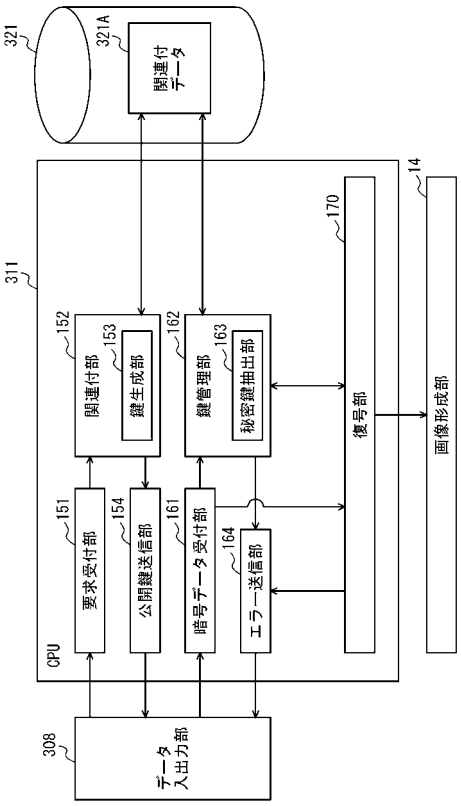

【図３】




【図４】



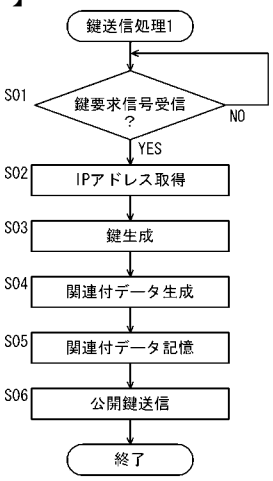

【図５】



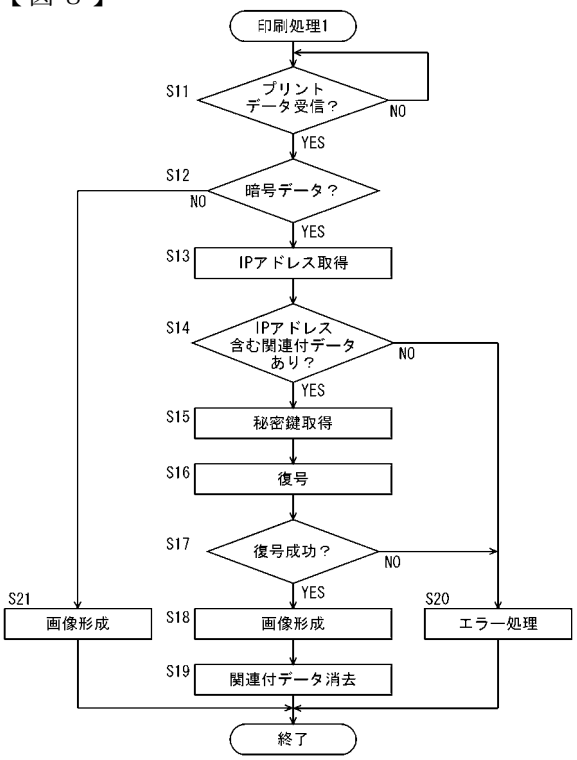

【図６】

| 公開鍵A | 秘密鍵A | IPアドレスA |
|---|---|---|

【図７】



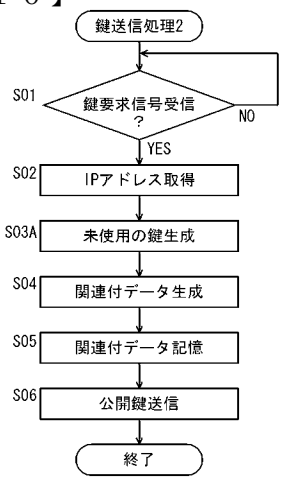

【図８】



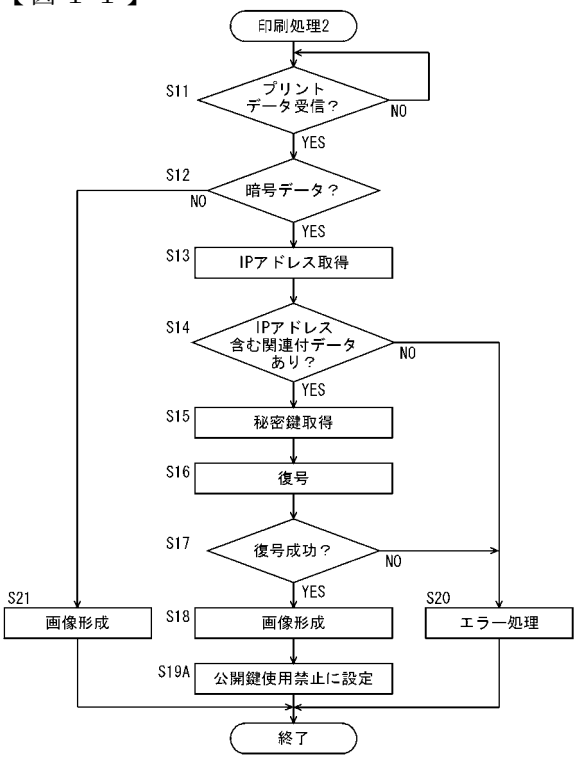

【図９】

| | | |
|---|---|---|
| 公開鍵A | 秘密鍵A | 使用済み |
| 公開鍵B | 秘密鍵B | 使用済み |
| 公開鍵C | 秘密鍵C | 使用済み |
| 公開鍵D | 秘密鍵D | 使用済み |
| 公開鍵E | 秘密鍵E | IPアドレスA |

【図１０】



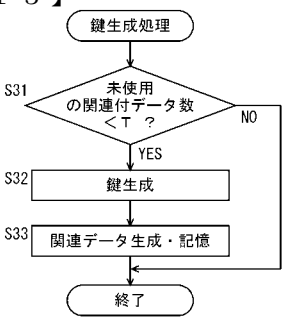

【図１１】



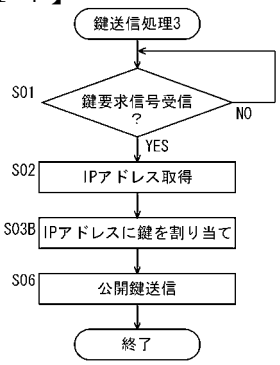

【図１２】

| | | |
|---|---|---|
| 公開鍵A | 秘密鍵A | IPアドレスA |
| 公開鍵B | 秘密鍵B | 未割り当て |
| 公開鍵C | 秘密鍵C | 未割り当て |
| 公開鍵D | 秘密鍵D | 未割り当て |

【図１３】



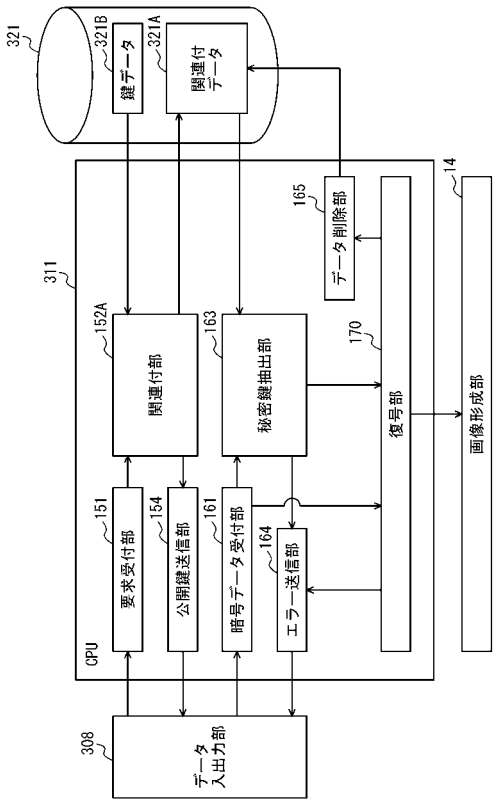

【図１４】




【図１５】

| | | |
|---|---|---|
| 公開鍵A | 秘密鍵A | 使用済み |
| 公開鍵B | 秘密鍵B | 使用済み |
| 公開鍵C | 秘密鍵C | 使用済み |
| 公開鍵D | 秘密鍵D | 使用済み |
| 公開鍵E | 秘密鍵E | IPアドレスA |
| 公開鍵F | 秘密鍵F | 未割り当て |
| 公開鍵G | 秘密鍵G | 未割り当て |
| 公開鍵H | 秘密鍵H | 未割り当て |

【図１６】




【図１７】

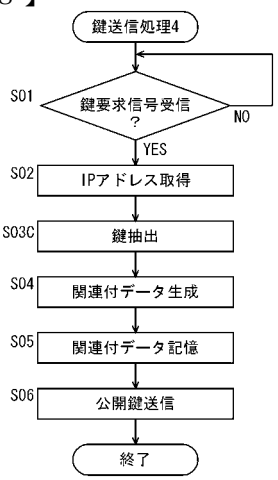
(A)

| | | |
|---|---|---|
| 1 | 公開鍵A | 秘密鍵A |
| 2 | 公開鍵B | 秘密鍵B |
| 3 | 公開鍵C | 秘密鍵C |
| 4 | 公開鍵D | 秘密鍵D |
| 5 | 公開鍵E | 秘密鍵E |
| 6 | 公開鍵F | 秘密鍵F |
| 7 | 公開鍵G | 秘密鍵G |
| 8 | 公開鍵H | 秘密鍵H |
| 9 | 公開鍵I | 秘密鍵I |
| 10 | 公開鍵J | 秘密鍵J |

(B)

| | | |
|---|---|---|
| 公開鍵A | 秘密鍵A | IPアドレスA |

【図１８】



フロントページの続き

| (51)Int.Cl. | | | FI | | | テーマコード（参考） |
|---|---|---|---|---|---|---|
| ***G06F 21/20*** | | ***(2006.01)*** | Ｇ０６Ｆ | 15/00 | ３３０Ａ | ５Ｊ１０４ |
| ***H04L 9/08*** | | ***(2006.01)*** | Ｈ０４Ｌ | 9/00 | ６０１Ｄ | |
| | | | Ｈ０４Ｌ | 9/00 | ６０１Ｆ | |

Ｆターム(参考) 5C062 AA02 AA05 AA13 AA35 AB38 AC35 AE01 AF12 BC03
5C075 AB90 EE02 EE03
5J104 EA01 EA16 PA07