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

特許第6372432号
(P6372432)

(45)発行日　平成30年8月15日(2018.8.15)　(24)登録日　平成30年7月27日(2018.7.27)

(51)Int.Cl.		F I		
G06F 3/12	(2006.01)	G06F	3/12	338
H04L 9/08	(2006.01)	G06F	3/12	322
B41J 29/00	(2006.01)	G06F	3/12	392
		G06F	3/12	389
		H04L	9/00	601E

請求項の数 4　(全 10 頁)　最終頁に続く

(21)出願番号　特願2015-135704(P2015-135704)
(22)出願日　平成27年7月6日(2015.7.6)
(65)公開番号　特開2017-16596(P2017-16596A)
(43)公開日　平成29年1月19日(2017.1.19)
審査請求日　平成29年4月25日(2017.4.25)

(73)特許権者　000006150
京セラドキュメントソリューションズ株式会社
大阪府大阪市中央区玉造１丁目２番２８号
(74)代理人　100115831
弁理士　藤岡　隆浩
(72)発明者　中尾　幸広
大阪府大阪市中央区玉造１丁目２番２８号　京セラドキュメントソリューションズ株式会社内

審査官　三橋　竜太郎

最終頁に続く

(54)【発明の名称】画像形成システム、画像形成方法及び制御プログラム

(57)【特許請求の範囲】

【請求項１】

所定のネットワークに接続されている複数のサーバを使用する画像形成システムであって、

一の暗号鍵を生成し、前記生成された一の暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成装置と、

前記画像データに基づいて画像を形成する画像形成装置と、

前記所定のネットワークに接続可能な携帯端末と、を備え、

前記暗号化画像データ生成装置は、前記一の暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記複数のサーバのうちの一のサーバにアップロードし、

前記携帯端末は、前記一の暗号鍵を受信し、前記暗号化画像データを前記一のサーバからダウンロードし、前記ダウンロードされた暗号化画像データと、前記受信した一の暗号鍵とを前記複数のサーバのうちの他のサーバに送信し、前記他のサーバに前記一の暗号鍵で前記暗号化画像データを復号化させて前記画像データを生成させ、前記生成された画像データを前記他のサーバから受信して前記画像形成装置に送信し、

前記携帯端末は、前記一の暗号鍵よりも処理負担の小さな他の暗号鍵を使用して前記他のサーバとの間の前記送受信を行う画像形成システム。

【請求項２】

請求項１に記載の画像形成システムであって、

前記携帯端末は、前記他の暗号鍵を共通鍵として使用して前記他のサーバとＳＳＬ（Ｓ

ｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）通信を実行する画像形成システム。
【請求項３】
所定のネットワークに接続されている複数のサーバと、一の暗号鍵を生成し、前記生成された一の暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成装置と、前記画像データに基づいて画像を形成する画像形成装置と、前記所定のネットワークに接続可能な携帯端末とを使用する画像形成方法であって、
前記暗号化画像データ生成装置が、前記一の暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記複数のサーバのうちの一のサーバにアップロードする工程と、
前記携帯端末が、前記一の暗号鍵を受信し、前記暗号化画像データを前記一のサーバからダウンロードし、前記ダウンロードされた暗号化画像データと、前記受信した一の暗号鍵とを前記複数のサーバのうちの他のサーバに送信し、前記他のサーバに前記一の暗号鍵で前記暗号化画像データを復号化させて前記画像データを生成させ、前記生成された画像データを前記他のサーバから受信して前記画像形成装置に送信する工程と、
を備え、
前記携帯端末は、前記一の暗号鍵よりも処理負担の小さな他の暗号鍵を使用して前記他のサーバとの間の前記送受信を行う画像形成方法。
【請求項４】
所定のネットワークに接続されている複数のサーバを使用する画像形成システムを制御するための制御プログラムであって、
一の暗号鍵を生成し、前記生成された一の暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成装置、
前記画像データに基づいて画像を形成する画像形成装置、及び
前記所定のネットワークに接続可能な携帯端末として前記画像形成システムを機能させ、
前記暗号化画像データ生成装置が、前記一の暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記複数のサーバのうちの一のサーバにアップロードし、
前記携帯端末が、前記一の暗号鍵を受信し、前記暗号化画像データを前記一のサーバからダウンロードし、前記ダウンロードされた暗号化画像データと、前記受信した一の暗号鍵とを前記複数のサーバのうちの他のサーバに送信し、前記他のサーバに前記一の暗号鍵で前記暗号化画像データを復号化させて前記画像データを生成させ、前記生成された画像データを前記他のサーバから受信して前記画像形成装置に送信し、
前記携帯端末は、前記一の暗号鍵よりも処理負担の小さな他の暗号鍵を使用して前記他のサーバとの間の前記送受信を行う制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像形成システム、画像形成方法及び制御プログラムに関し、特に携帯端末と連携して作動する画像形成装置を含む画像形成システムに関する。
【背景技術】
【０００２】
近年、コンビニエンスストア等の店舗に設置された画像形成装置を利用し、目的地やその近くで、文書その他の画像データを印刷することが多くなっている。このような一般に対して利用が開放されている画像形成装置で印刷する際の秘匿性を確保するための技術として特許文献１の技術が提案されている。特許文献１は、印刷対象データから一部のデータを抜粋し、残りのデータを通信回線で画像形成装置に送信する一方、一部の抜粋されたデータを携帯端末に送信する。この画像形成装置は、残りのデータに加えて、一部の抜粋されたデータを携帯端末を介して受信することによって印刷を実行することができる。これにより、仮に通信回線で画像形成装置側に送信されている文書データが傍受された場合でも情報漏洩を防止することができる。
【先行技術文献】

【特許文献】
【０００３】
【特許文献１】特開２０１３－１６４８０１号公報
【特許文献２】特開２００５－１７３７９３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、本技術は、一般に対して利用が開放されている画像形成装置側に、その実現のためだけの固有の機能を実装する必要がある。このため、本技術の利用は、その固有の技術を実装した画像形成装置での利用に限定される。
【０００５】
本発明は、このような状況に鑑みてなされたものであり、特定の機種に依存せず、一般に対して利用が開放されている画像形成装置で秘匿性を確保しつつ印刷を実行する技術を提供することを目的とする。
【課題を解決するための手段】
【０００６】
本発明は、所定のネットワークに接続されているサーバを使用する画像形成システムを提供する。前記画像形成システムは、暗号鍵を生成し、前記生成された暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成装置と、前記画像データに基づいて画像を形成する画像形成装置と、前記所定のネットワークに接続可能な携帯端末とを備える。前記暗号化画像データ生成装置は、前記暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記サーバにアップロードする。前記携帯端末は、前記暗号化画像データを前記サーバからダウンロードし、前記ダウンロードされた暗号化画像データを前記受信した暗号鍵で復号化して、前記画像データを生成し、前記生成された画像データを前記画像形成装置に送信する。
【０００７】
本発明は、所定のネットワークに接続されているサーバを使用する画像形成方法を提供する。前記画像形成方法は、暗号鍵を生成し、前記生成された暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成工程と、前記画像データに基づいて画像を形成する画像形成工程と、前記所定のネットワークに接続する接続工程とを備える。前記暗号化画像データ生成工程は、前記暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記サーバにアップロードする工程を含む。前記接続工程は、前記暗号化画像データを前記サーバからダウンロードし、前記ダウンロードされた暗号化画像データを前記受信した暗号鍵で復号化して、前記画像データを生成し、前記生成された画像データを前記画像形成装置に送信する工程を含む。
【０００８】
本発明は、所定のネットワークに接続されているサーバを使用する画像形成システムを制御するための制御プログラムを提供する。前記制御プログラムは、暗号鍵を生成し、前記生成された暗号鍵で画像データを暗号化して暗号化画像データを生成する暗号化画像データ生成装置、前記画像データに基づいて画像を形成する画像形成装置及び前記所定のネットワークに接続可能な携帯端末として前記画像形成システムを機能させる。前記暗号化画像データ生成装置は、前記暗号鍵を前記携帯端末に送信し、前記暗号化画像データを前記サーバにアップロードする。前記携帯端末は、前記暗号化画像データを前記サーバからダウンロードし、前記ダウンロードされた暗号化画像データを前記受信した暗号鍵で復号化して、前記画像データを生成し、前記生成された画像データを前記画像形成装置に送信する。
【発明の効果】
【０００９】
本発明によれば、特定の機種に依存せず、一般に対して利用が開放されている画像形成装置で秘匿性を確保しつつ印刷を実行する技術を提供する。

【図面の簡単な説明】
【００１０】
【図１】本発明の一実施形態に係る画像形成システムの機能構成を示すブロックダイアグラム。
【図２】画像形成システムにおける第１処理形態に係る印刷処理の内容を示すブロックダイアグラム。
【図３】画像形成システムにおける第２処理形態に係るアップロード処理の内容を示すブロックダイアグラム。
【図４】画像形成システムにおける第３処理形態に係る印刷処理の内容を示すブロックダイアグラム。
【図５】画像形成システムにおける第４処理形態に係るアップロード処理の内容を示すブロックダイアグラム。
【発明を実施するための形態】
【００１１】
以下、本発明を実施するための形態（以下、「実施形態」という）を、図面を参照して説明する。
【００１２】
図１は、本発明の一実施形態に係る画像形成システム１の機能構成を示すブロックダイアグラムである。画像形成システム１は、パーソナルコンピュータ１０と、携帯端末２０と、クラウドサーバ３０と、Ｗｅｂサーバ４０と、画像形成装置５０とを備えている。携帯端末２０は、記憶部２１を有している。携帯端末２０は、パーソナルコンピュータ１０にインストールされている一実施形態を実行するためのソフトウェアに予め登録されている。画像形成装置５０は、コンビニエンスストア等に配置されている一般に対して利用が開放されている装置である。なお、画像形成システム１は、パーソナルコンピュータ１０の代わりにタブレットその他の情報機器を使用してもよい。
【００１３】
パーソナルコンピュータ１０は、画像データ生成部１１と、暗号化処理部１２と、制御部１５と、記憶部１６と、通信部１７とを備える。画像データ生成部１１は、文章編集ソフトウェアや画像処理ソフト、画像読み取り機能によって画像データＤｉを生成する。画像データＤｉは、たとえばＰｏｒｔａｂｌｅ　Ｄｏｃｕｍｅｎｔ　Ｆｏｒｍａｔ（ｐｄｆ）形式ファイルといった汎用のファイル形式で生成される。なお、パーソナルコンピュータ１０は、暗号化画像データ生成装置とも呼ばれる。
【００１４】
暗号化処理部１２は、共通鍵暗号方式で画像データＤｉを暗号化して暗号化画像データＤｓを生成する。すなわち、暗号化処理部１２は、共通鍵Ｃｋｓを生成し、この共通鍵Ｃｋｓを使用して画像データＤｉを暗号化して暗号化画像データＤｓを生成する。暗号化画像データＤｓは、共通鍵暗号方式なので、共通鍵Ｃｋｓを使用して復号化することができる。暗号化処理部１２は、暗号化画像データＤｓをクラウドサーバ３０に通信部１７から通信回線を介してアップロードする。
【００１５】
暗号化処理部１２は、公開鍵暗号方式で通信部１７を介して携帯端末２０に共通鍵Ｃｋｓを送信する。具体的には、暗号化処理部１２は、携帯端末２０から予め受け取った公開鍵Ｐｋｓ２を使用して、共通鍵Ｃｋｓを暗号化して通信部１７から携帯端末２０に送信する。携帯端末２０は、秘密鍵Ｓｋｓ２を使用して暗号化された共通鍵Ｃｋｓを復号化して記憶部に記憶する。
【００１６】
暗号化処理部１２は、クラウドサーバ３０のアドレス並びにクラウドサーバ３０にアクセスするための情報やパスワードなどのログイン情報を共通鍵暗号方式で携帯端末に送信する。このように、暗号化処理部１２は、携帯端末２０との間にＳｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒｐｒｏｔｏｃｏｌ（ＳＳＬ）通信を確立して通信を行う。

【００１７】
ＳＳＬ通信は、共通鍵暗号方式と公開鍵暗号方式とを組み合わせて使用する通信方式である。共通鍵暗号方式は、暗号化と復号化の処理負担が軽い一方、秘匿性を確保して共通鍵を相手側に渡す必要があるという問題がある。公開鍵暗号方式は、暗号化に必要な公開鍵のみを渡して復号化に必要な秘密鍵は他に渡さずに暗号化通信を開始できるが、暗号化と復号化の処理負担が大きいという問題がある。ＳＳＬ通信は、公開鍵暗号方式の通信で共通鍵を相手側に渡し、データの授受は、共通鍵を使用する通信方式である。これにより、ＳＳＬ通信は、安全に共通鍵を渡して軽い処理負担で高速通信を可能とすることができる。
【００１８】
本実施形態は、暗号化処理部１２と携帯端末２０との間にＳＳＬ通信を確立する一方、ＳＳＬ通信の確立で携帯端末２０が取得した共通鍵Ｃｋｓを使用してクラウドサーバ３０からダウンロードした暗号化画像データＤｓを復号化することができるという特徴を有している。このように、本実施形態は、画像データＤｉの通信においては、ＳＳＬ通信に類似するが、通信対象の画像データＤｉと共通鍵Ｃｋｓの通信ルートが相違するという新規かつ固有の特徴を有している。
【００１９】
制御部１５は、ＲＡＭやＲＯＭ等の主記憶手段、及びＭＰＵ（Ｍｉｃｒｏ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）やＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）等の制御手段を備えている。また、制御部１５は、各種Ｉ／Ｏ、ＵＳＢ（ユニバーサル・シリアル・バス）、バス、その他ハードウェア等のインターフェイスに関連するコントローラ機能を備え、パーソナルコンピュータ１０全体を制御する。
【００２０】
記憶部１６は、非一時的な記録媒体であるハードディスクドライブやフラッシュメモリー等からなる記憶装置で、制御部１５が実行する処理の制御プログラムやデータを記憶する。
【００２１】
本実施形態を実行するアプリケーションプログラムは、オフィスや自宅などのいつも使用される場所に設置される画像形成装置５０のドライバ、あるいはネットショップなどで配布されるアプリケーションとして提供することができる。本アプリケーションプログラムは、パーソナルコンピュータやタブレット、スマートフォンといったデバイスにインストールされても良いし、インターネット上のＷｅｂサーバでその処理を行なえる形態で提供されてもよい。
【００２２】
このように、一実施形態に係る画像形成システム１は、共通鍵Ｃｋｓなしでは復号化できない暗号化画像データＤｓをクラウドサーバ３０上に保存することができる。これにより、仮に暗号化画像データＤｓが流出してもクラウドサーバ３０上には、暗号化画像データＤｓの復号化や解読に必要な情報が存在しないので、高い秘匿性を確保することができる。一方、携帯端末２０は、共通鍵Ｃｋｓを有するので、いつでもクラウドサーバ３０から暗号化画像データＤｓをダウンロードし、復号化することによって画像データＤｉを利用可能である。この結果、携帯端末２０は、その記憶部２１の記憶領域を消費することなく、安全かつ事実上無制限にデータ用の格納領域を利用可能である。
【００２３】
携帯端末２０は、第三者による傍受が事実上困難な近距離通信を介して画像形成装置５０に画像データＤｉを送信して画像形成装置５０に印刷を実行させる。本実施形態では、近距離通信は、ＢＬＵＥＴＯＯＴＨ（登録商標）のＣＬＡＳＳ１を使用している。ＢＬＵＥＴＯＯＴＨのＣＬＡＳＳ１は、出力１ｍＷの通信であり、携帯端末２０と画像形成装置５０との距離が１ｍ以内程度での通信が可能な近距離無線通信である。通信距離が極めて短いので、第三者による傍受が事実上困難である。なお、近距離通信は、第三者による傍受が事実上困難なものであれば、ＵＳＢケーブル（図示せず）を介した有線通信やＢＬＵ

ＥＴＯＯＴＨ以外の他の無線通信方式（たとえば電磁誘導方式）であってもよい。

【００２４】

図２は、画像形成システム１における第１処理形態に係る印刷処理の内容を示すブロックダイアグラムである。本処理は、画像形成装置５０で復号化を行わずに、携帯端末２０で復号化を行う処理である。画像形成装置５０には、暗号化や復号化の機能が必要とされないので、画像形成装置５０が復号化機能を有しない場合等に実行される処理である。

【００２５】

本処理では、携帯端末２０は、暗号化画像データＤｓを復号化し、画像形成装置５０に画像データＤｉを送信して印刷させる。具体的には、携帯端末２０は、暗号化処理部１２から予め受け取ったログイン情報を使用して、クラウドサーバ３０にログインする。携帯端末２０は、ログイン後に暗号化画像データＤｓをクラウドサーバ３０からダウンロードし、予め取得している前述の共通鍵Ｃｋｓで復号化して画像データＤｉを生成する。携帯端末２０は、第三者による傍受が事実上困難な前述の近距離通信を介して画像形成装置５０に画像データＤｉを送信して画像形成装置５０に印刷を実行させる。

【００２６】

なお、画像形成システム１は、復号化処理をＷｅｂサーバ４０で行うことも可能である。たとえば共通鍵Ｃｋｓが極めて高い暗号化強度を有し、復号化の処理負担が大きい場合や大きなメモリ領域を必要とする場合等には、携帯端末２０の代わりにＷｅｂサーバ４０で復号化処理を実行する。携帯端末２０とＷｅｂサーバ４０との間の通信は、比較的に暗号強度が低く処理負担が軽い共通鍵Ｃｋｓｗを使用したＳＳＬ通信あるいは暗号化なしで行うこともできる。共通鍵Ｃｋｓｗは、Ｗｅｂサーバ４０から予め受け取った公開鍵Ｐｋｓ３を使用してＷｅｂサーバ４０が予め取得し、秘密鍵Ｓｋｓ３で復号化されて記憶される。

【００２７】

図３は、画像形成システム１における第２処理形態に係るアップロード処理の内容を示すブロックダイアグラムである。本処理は、第１処理形態と同様に画像形成装置５０が暗号化や復号化機能を有しない場合等に実行される処理である。

【００２８】

本処理では、画像形成装置５０がスキャン対象Ｄから画像データＤｉを生成し、画像形成装置５０の外部で画像データＤｉを暗号化する。具体的には、携帯端末２０は、近距離通信を介して画像形成装置５０から画像データＤｉを取得し、この画像データＤｉを共通鍵Ｃｋｓを使用して暗号化する。これにより、携帯端末２０は、暗号化画像データＤｓを生成してクラウドサーバ３０にアップロードする。なお、画像形成システム１は、暗号化処理をＷｅｂサーバ４０で行うことが可能である点は、第１処理形態と同様である。

【００２９】

図４は、画像形成システム１における第３処理形態に係る印刷処理の内容を示すブロックダイアグラムである。本処理では、画像形成装置５０で復号化が行われる。画像形成装置５０には、暗号化や復号化の機能が必要とされるが、暗号化や復号化は、他の目的で実装され、一般的な機能となっていくものと考えられる。本処理では、携帯端末２０は、暗号化画像データＤｓと共通鍵Ｃｋｓとを画像形成装置５０に近距離通信を介して送信し、画像形成装置５０で復号化して印刷する。

【００３０】

図５は、画像形成システム１における第４処理形態に係るアップロード処理の内容を示すブロックダイアグラムである。本処理では、画像形成装置５０で暗号化が行われる。本処理では、画像形成装置５０は、スキャン対象Ｄから画像データＤｉを生成し、画像形成装置５０の内部で暗号化する。画像形成装置５０は、共通鍵Ｃｋｓを使用して画像データＤｉを暗号化して暗号化画像データＤｓを生成する。画像形成装置５０は、暗号化画像データＤｓを携帯端末２０に近距離通信を介して送信する。携帯端末２０は、暗号化画像データＤｓをクラウドサーバ３０にアップロードする。

【００３１】

このように、本実施形態によれば、一般に対して利用が開放されている画像形成装置５０で秘匿性を確保しつつ印刷や画像データ（スキャンデータ等）のアップロードを実行することができる。画像形成装置５０は、本実施形態に固有の機能を実装しなくても、暗号化や復号化といった一般的に使用される機能を使用して、本実施形態を実行することができる。よって、本実施形態は、特定の機種に依存せず、一般的な画像形成装置５０を使用して、秘匿性を確保しつつ目的地またはその近くで印刷することができる。

【００３２】

本発明は、上記各実施形態だけでなく、以下のような変形例でも実施することができる。

【００３３】

変形例１：上記実施形態では、画像データの暗号化と復号化に使用される共通鍵は、１つであるが、複数の共通鍵を使用するようにしてもよい。この場合、復号化に使用すべき共通鍵は、暗号化画像データを格納するクラウドサーバに格納してもよい。ただし、暗号化画像データが格納されているクラウドサーバではなく、その外部の携帯端末に暗号化画像データと共通鍵の対応関係を示すテーブルを保存するようにすることが高い秘匿性確保の観点から好ましい。

【００３４】

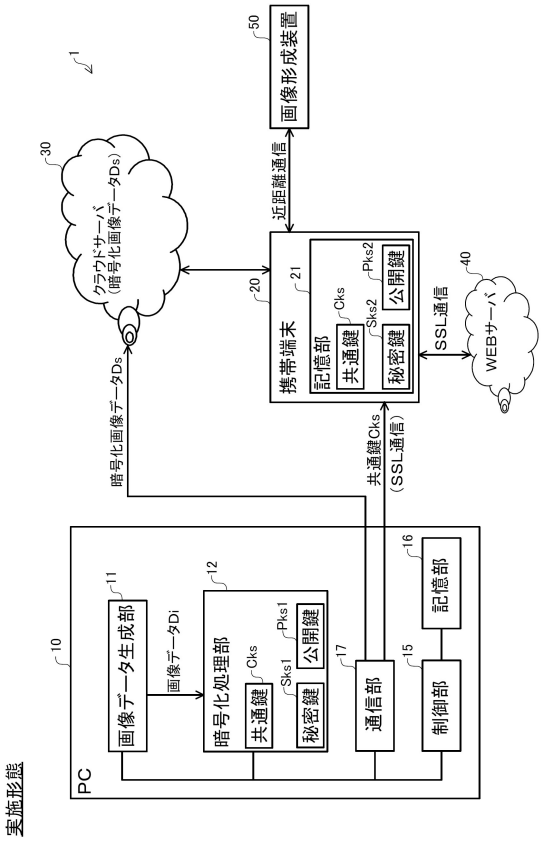
変形例２：上記実施形態では、共通鍵暗号方式と公開鍵暗号方式とを使用しているが、このような暗号方式に限られず、単にパスワードを使用して秘密性を確保するようにしてもよい。本明細書では、パスワードを使用して秘密性が確保された場合も暗号化と呼ばれる。

【符号の説明】

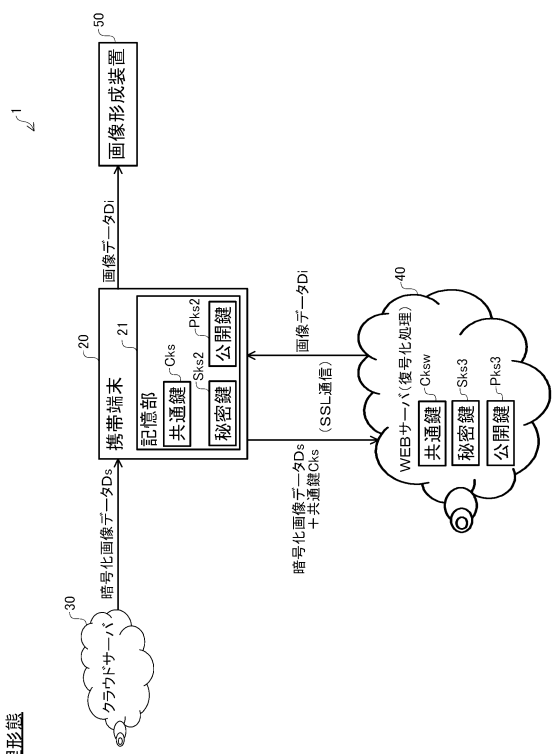
【００３５】

１　画像形成システム
１０　パーソナルコンピュータ
１１　画像データ生成部
１２　暗号化処理部
１５　制御部
１６　記憶部
１７　通信部
２０　携帯端末
３０　クラウドサーバ
４０　サーバ
５０　画像形成装置

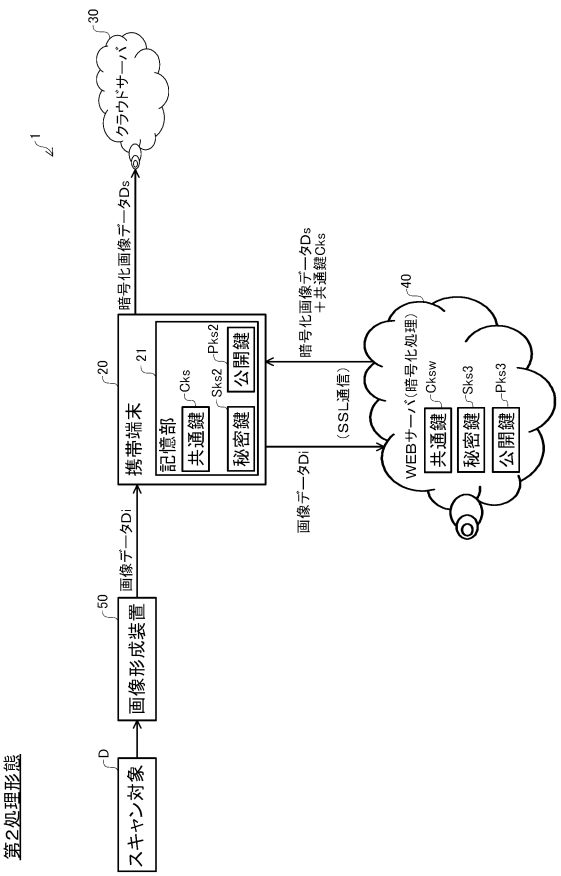
【図１】


実施形態
PC
10
画像データ生成部
11
画像データDi
暗号化処理部
12
共通鍵
Cks
秘密鍵
Sks1
公開鍵
Pks1
通信部
17
制御部
15
記憶部
16
暗号化画像データDs
共通鍵Cks
（SSL通信）
1
クラウドサーバ
（暗号化画像データDs）
30
携帯端末
20
記憶部
21
共通鍵
Cks
秘密鍵
Sks2
公開鍵
Pks2
近距離通信
画像形成装置
50
SSL通信
WEBサーバ
40

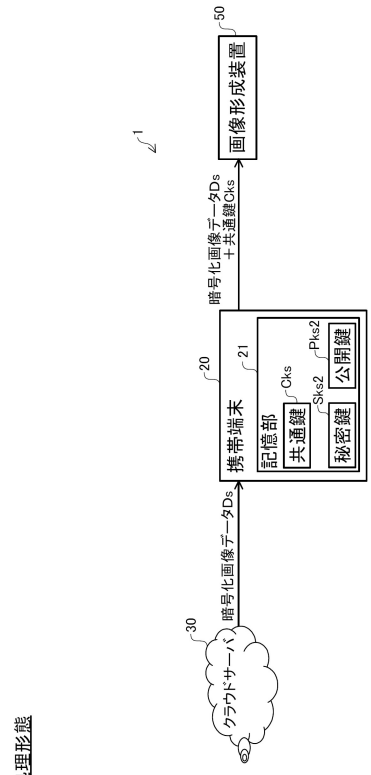
【図２】


第1処理形態
1
クラウドサーバ
30
暗号化画像データDs
携帯端末
20
記憶部
21
共通鍵
Cks
秘密鍵
Sks2
公開鍵
Pks2
画像データDi
画像形成装置
50
暗号化画像データDs
＋共通鍵Cks
（SSL通信）
画像データDi
WEBサーバ（復号化処理）
40
共通鍵
Cksw
秘密鍵
Sks3
公開鍵
Pks3

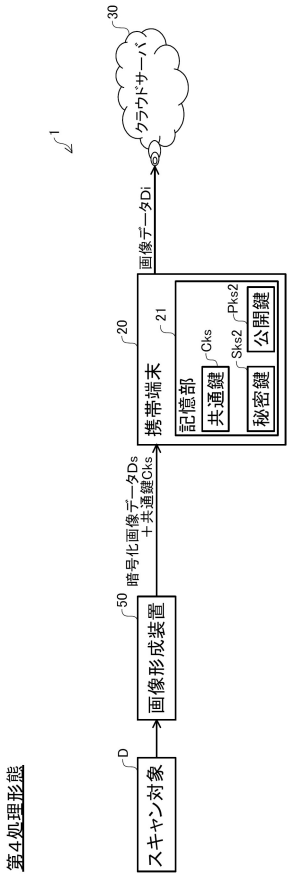
【図３】


第2処理形態
スキャン対象
D
画像形成装置
50
画像データDi
携帯端末
20
記憶部
21
共通鍵
Cks
秘密鍵
Sks2
公開鍵
Pks2
暗号化画像データDs
クラウドサーバ
30
暗号化画像データDs
＋共通鍵Cks
（SSL通信）
画像データDi
WEBサーバ（暗号化処理）
40
共通鍵
Cksw
秘密鍵
Sks3
公開鍵
Pks3

【図４】


第3処理形態
1
クラウドサーバ
30
暗号化画像データDs
携帯端末
20
記憶部
21
共通鍵
Cks
秘密鍵
Sks2
公開鍵
Pks2
暗号化画像データDs
＋共通鍵Cks
画像形成装置
50

【図５】


第４処理形態
1
D
スキャン対象
50
画像形成装置
暗号化画像データDs
＋共通鍵Cks
20
携帯端末
21
記憶部
共通鍵
Cks
Sks2
秘密鍵
Pks2
公開鍵
画像データDi
30
クラウドサーバ

フロントページの続き

(51)Int.Cl.	FI		
	H04L	9/00	601C
	B41J	29/00	E

(56)参考文献 特開２００５－１５７４１４（ＪＰ，Ａ）
米国特許出願公開第２０１４／０３６８８６７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｂ４１Ｊ	５／００－２９／７０
Ｇ０３Ｇ	１５／００－２１／２０
Ｇ０６Ｆ	３／０９－２１／４６
Ｇ０９Ｃ	１／００－５／００
Ｈ０４Ｂ	７／２４－７／２６
Ｈ０４Ｋ	１／００－３／００
Ｈ０４Ｌ	９／００－９／３８
Ｈ０４Ｍ	１／００－９９／００
Ｈ０４Ｎ	１／００
Ｈ０４Ｗ	４／００－９９／００