(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4906068号
(P4906068)
(45)発行日　平成24年3月28日(2012.3.28)　(24)登録日　平成24年1月20日(2012.1.20)

(51)Int.Cl.		F I		
B41J 29/38	(2006.01)	B41J	29/38	Z
B41J 29/00	(2006.01)	B41J	29/00	Z
G06F 3/12	(2006.01)	G06F	3/12	K

請求項の数 13　(全 34 頁)

(21)出願番号　特願2006-111366 (P2006-111366)
(22)出願日　平成18年4月13日 (2006.4.13)
(65)公開番号　特開2007-283562 (P2007-283562A)
(43)公開日　平成19年11月1日 (2007.11.1)
審査請求日　平成21年4月13日 (2009.4.13)

(73)特許権者　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　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(72)発明者　土樋　直基
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

最終頁に続く

(54)【発明の名称】印刷システム、その制御方法、及びコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
複数の認証サーバとネットワークを介して通信可能なクライアントと、印刷装置と、を含む印刷システムであって、
前記クライアントは、
前記複数の認証サーバの中から割り当てられた何れかの認証サーバに、ユーザ認証情報を伴ってアクセスを行うアクセス制御手段と、
前記アクセスに応じて前記何れかの認証サーバから応答され且つ印刷ジョブの実行を制限するためのアクセス制限情報を含む印刷ジョブを印刷装置に出力する印刷ジョブ出力手段とを有し、
前記認証サーバは、
前記クライアントから通知されたユーザ認証情報に基づき、前記認証サーバの識別子、および、自身が保持する暗号化情報により暗号化処理を施したアクセス制限情報を前記クライアントへ発行する発行手段を有し、
前記印刷装置は、
受信した前記アクセス制限情報に施された暗号化処理を復号するための復号化情報を保持するための保持手段と、
受信した前記印刷ジョブに含まれる前記認証サーバの識別子に対応した復号化情報を前記保持手段に保持しているか否かを判定する判定手段と、
前記判定手段により前記保持手段が保持していないと判定された場合に、前記識別子に

より特定される前記認証サーバから前記復号化情報を取得する取得手段と、
前記取得手段により取得した復号化情報、又は、前記保持している復号化情報により、前記アクセス制限情報に含まれるデジタル署名の検証を行う検証手段と、
前記検証手段による検証に基づき印刷ジョブの実行を制御するジョブ実行制御手段と
を有することを特徴とする印刷システム。
【請求項２】
前記印刷装置は、
受信した前記印刷ジョブに前記アクセス制限情報が付与されているかどうかを判断する判断手段と、
前記判断手段によって受信した前記印刷ジョブに前記アクセス制限情報が付与されていないと判断された場合、或は、前記検証手段によって前記復号化情報によるデジタル署名の検証が失敗した場合に、受信した前記印刷ジョブを取り消すジョブ取消手段と
を有することを特徴とする請求項１に記載の印刷システム。
【請求項３】
前記取得手段は、前記検証手段における前記検証の成否に基づき、再度、前記認証サーバから復号化情報を取得し、前記保持手段に格納し、
前記検証手段は、再取得された前記復号化情報に応じて、再度、前記アクセス制限情報に含まれるデジタル署名の検証を実施することを特徴とする請求項１又は２に記載の印刷システム。
【請求項４】
前記取得手段は、
前記保持手段の空き容量を判定し、前記復号化情報が格納できない場合に、アクセス履歴を元に使用頻度の低い認証サーバを検索し、検索された認証サーバの識別子および復号化情報を破棄し、新たな認証サーバの復号化情報を前記保持手段に格納することを特徴とする請求項１乃至３の何れか１項に記載の印刷システム。
【請求項５】
印刷システムであって、
複数の認証サーバの中から割り当てられた何れかの認証サーバに、ユーザ認証情報を伴ってアクセスを行うアクセス制御手段と、
前記割り当てられた何れかの認証サーバの識別子を参照し、該何れかの認証サーバに対応した復号化情報を保持しているか否かを判定し、保持していないと判定した場合、前記識別子により特定される前記認証サーバから前記復号化情報を取得する取得手段と、
前記取得手段により取得した復号化情報、又は、前記保持している復号化情報により、前記アクセスに応じて前記何れかの認証サーバから応答され且つ印刷ジョブの実行を制限するためのアクセス制限情報に含まれるデジタル署名の検証を行う検証手段と、
前記検証手段による検証に基づき印刷ジョブの実行を制御するジョブ実行制御手段と
を有することを特徴とする印刷システム。
【請求項６】
前記何れかの認証サーバ自身が保持する暗号化情報により暗号化処理が施されたアクセス制限情報と前記何れかの認証サーバの識別子とを含む印刷ジョブを、印刷装置へ出力する出力手段を有し、
前記取得手段は、受信した前記印刷ジョブに含まれる認証サーバの前記識別子を参照し、前記判定を行うことを特徴とする請求項５に記載の印刷システム。
【請求項７】
複数の認証サーバとネットワークを介して通信可能なクライアントと、印刷装置と、を含む印刷システムの制御方法であって、
前記クライアントのアクセス制御手段が、前記複数の認証サーバの中から割り当てられた何れかの認証サーバに、ユーザ認証情報を伴ってアクセスを行うアクセス制御工程と、
前記認証サーバの発行手段が、通知された前記ユーザ認証情報に基づき、前記認証サーバの識別子、および、自身が保持する暗号化情報により暗号化処理を施し且つ印刷ジョブ

の実行を制限するためのアクセス制限情報を発行する発行工程と、
前記クライアントの印刷ジョブ出力手段が、発行された前記アクセス制限情報を含む印刷ジョブを印刷装置に出力する印刷ジョブ出力工程と、
前記印刷装置の判定手段が、受信した前記印刷ジョブに含まれる前記認証サーバの識別子に対応し、受信した前記アクセス制限情報に施された暗号化処理を復号するための復号化情報を、該復号化情報を保持するための保持手段に保持しているか否かを判定する判定工程と、
前記印刷装置の取得手段が、前記判定工程において前記保持手段が保持していないと判定された場合に、前記識別子により特定される前記認証サーバから前記復号化情報を取得する取得工程と、
前記印刷装置の検証手段が、前記取得工程において取得した復号化情報、または、前記保持している復号化情報により、前記アクセス制限情報のデジタル署名の検証を行う検証工程と、
前記印刷装置のジョブ実行制御手段が、前記検証工程における検証に基づき印刷ジョブの実行を制御するジョブ実行制御工程と
を有することを特徴とする印刷システムの制御方法。
【請求項８】
前記印刷装置の判断手段が、受信した前記印刷ジョブに前記アクセス制限情報が付与されているかどうかを判断する判断工程と、
前記印刷装置のジョブ取消手段が、前記判断工程において、受信した前記印刷ジョブに前記アクセス制限情報が付与されていないと判断された場合、或は、前記検証工程によって前記復号化情報によるデジタル署名の検証が失敗した場合に、受信した前記印刷ジョブを取り消すジョブ取消工程と
を有することを特徴とする請求項７に記載の印刷システムの制御方法。
【請求項９】
前記取得工程では、前記検証工程における前記検証の成否に基づき、再度、前記認証サーバから復号化情報を取得し、前記保持手段に格納し、
前記検証工程では、再取得された前記復号化情報に応じて、再度、前記アクセス制限情報のデジタル署名の検証を実施することを特徴とする請求項７又は８に記載の印刷システムの制御方法。
【請求項１０】
前記取得工程では、
前記保持手段の空き容量を判定し、前記復号化情報が格納できない場合に、アクセス履歴を元に使用頻度の低い認証サーバを検索し、検索された認証サーバの識別子および復号化情報を破棄し、新たな認証サーバの復号化情報を前記保持手段に格納することを特徴とする請求項７乃至９の何れか１項に記載の印刷システムの制御方法。
【請求項１１】
印刷システムの制御方法であって、
アクセス制御手段が、複数の認証サーバの中から割り当てられた何れかの認証サーバに、ユーザ認証情報を伴ってアクセスを行うアクセス制御工程と、
取得手段が、前記割り当てられた何れかの認証サーバの識別子を参照し、該何れかの認証サーバに対応した復号化情報を保持しているか否かを判定し、保持していないと判定した場合、前記識別子により特定される前記認証サーバから前記復号化情報を取得する取得工程と、
検証手段が、前記取得工程において取得した復号化情報、又は、前記保持している復号化情報により、前記アクセスに応じて前記何れかの認証サーバから応答され且つ印刷ジョブの実行を制限するためのアクセス制限情報に含まれるデジタル署名の検証を行う検証工程と、
ジョブ実行制御手段が、前記検証工程における検証に基づき印刷ジョブの実行を制御するジョブ実行制御工程と

を有することを特徴とする印刷システムの制御方法。
【請求項１２】
出力手段が、前記何れかの認証サーバ自身が保持する暗号化情報により暗号化処理が施されたアクセス制限情報と前記何れかの認証サーバの識別子とを含む印刷ジョブを、印刷装置へ出力する出力工程を有し、
前記取得工程では、受信した前記印刷ジョブに含まれる認証サーバの前記識別子を参照し、前記判定を行うことを特徴とする請求項１１に記載の印刷システムの制御方法。
【請求項１３】
請求項７乃至１２の何れか１項に記載の印刷システムの制御方法をコンピュータに実行させるコンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証機能を備えた印刷システム、その制御方法及びコンピュータプログラムに関する。
【背景技術】
【０００２】
近年、オフィス環境における印刷システムにおいて、ＴＣＯ（Ｔｏｔａｌ　Ｃｏｓｔ　ｏｆ　Ｏｗｎｅｒｓｈｉｐ）削減が、益々重要視されている。ＴＣＯの削減については、印刷装置やシステムの初期導入費用だけではなく、印刷用紙やトナーに代表される着色剤などの消耗品のコスト削減についても注目されている。このような消耗品のコスト削減は、オフィスの経費削減、あるいは地球環境の保全の点から非常に重要な課題とされている。
【０００３】
従来からの問題点は、印刷装置がオフィスに設置されており、ネットワークにアクセスできれば、誰でも当該印刷装置を使用して印刷できてしまうということがあげられる。さらに、これらの印刷装置は、誰にも印刷制限がかからず、形跡も残らないため、使用者の精神的な歯止めも効かず本来必要な出力を超えた印刷が行なわれている。これにより、ＴＣＯは、必要以上に増大を招いていた。
【０００４】
特許文献１は、ユーザ毎に出力を制限するユーザ制限機能を有する情報処理装置を開示している。特許文献１に記載の情報処理装置は、ユーザ毎に出力を制限しているためＴＣＯの削減に有効である。
【特許文献１】特開平１１－１３４１３６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
特許文献１のような出力に関する制限は、印刷システムが大規模になると、機能制限を司る認証サーバシステムを印刷装置の外部に配置し、このコンピュータに認証等を行わせることが想定される。一方、大規模オフィス等では、ホストコンピュータは何百台、何千台と置かれる状況も想定される。しかし、多数のホストコンピュータからの認証を１つの認証サーバシステムで受け持つ形態では、認証サーバシステムに過剰な負荷がかかり、不都合を生じることがある。例えば、認証サーバは、多数の外部からのアクセスにより処理能力の限界を超えてしまい、認証サーバシステムがダウンする虞がある。また、認証サーバは、極度の負荷により、極度に遅くなってしまい、印刷処理が遅延し、使い勝手の悪くなるという問題がある。
【０００６】
本発明は、上述した問題に鑑みてなされたものであり、印刷処理に係る認証サーバ機能を安定して動作させつつ、印刷によるコストを低減する印刷システム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】
【０００７】
上記課題を解決するための一の形態に対応する本発明は、複数の認証サーバとネットワークを介して通信可能なクライアントと、印刷装置と、を含む印刷システムであって、前記クライアントは、前記複数の認証サーバの中から割り当てられた何れかの認証サーバに、ユーザ認証情報を伴ってアクセスを行うアクセス制御手段と、前記アクセスに応じて前記何れかの認証サーバから応答され且つ印刷ジョブの実行を制限するためのアクセス制限情報を含む印刷ジョブを印刷装置に出力する印刷ジョブ出力手段とを有し、前記認証サーバは、前記クライアントから通知されたユーザ認証情報に基づき、前記認証サーバの識別子、および、自身が保持する暗号化情報により暗号化処理を施したアクセス制限情報を前記クライアントへ発行する発行手段を有し、前記印刷装置は、受信した前記アクセス制限情報に施された暗号化処理を復号するための復号化情報を保持するための保持手段と、受信した前記印刷ジョブに含まれる前記認証サーバの識別子に対応した復号化情報を前記保持手段に保持しているか否かを判定する判定手段と、前記判定手段により前記保持手段が保持していないと判定された場合に、前記識別子により特定される前記認証サーバから前記復号化情報を取得する取得手段と、前記取得手段により取得した復号化情報、又は、前記保持している復号化情報により、前記アクセス制限情報の検証を行う検証手段と、前記検証手段による検証に基づき印刷ジョブの実行を制御するジョブ実行制御手段とを有することを特徴とする。

【発明の効果】
【０００８】
本発明は、印刷処理に係る認証サーバ機能を安定して動作させつつ、印刷によるコストを低減する印刷システムを提供できる。
【発明を実施するための最良の形態】
【０００９】
以下、本発明に係る実施形態について図面を用いて説明する。なお、以下の実施の形態は特許請求の範囲に記載された発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。
【００１０】
［第１の実施形態］
以下では、本発明における第１の実施形態について説明する。図１は、第１の実施形態における印刷システムの構成を示すブロック図である。ここでは、説明を容易にするため、それぞれのコンポーネントを１台または２台として説明される。しかしながら、本発明は、コンポーネントの数を限定するわけではなく、大規模な印刷システムにおいても適用しうる。また、図１では各装置を機能毎に分類して区別し示しているが、ある装置の一部の機能を別の装置に組み込んでもよく、柔軟な装置構成でシステムを構築できる。以後、印刷システムという場合に、単体の装置を指しても良いし、複数の装置を指しても良い、以下で説明するある装置に別の装置の一部又は全部の機能を組み込んだものを指しても良い。例えば、以下、第１乃至４の実施形態で夫々説明する印刷装置単体のことを印刷システムと呼ぶ場合もある。
【００１１】
印刷システム１００は、ホストコンピュータ１０１、認証サーバ１０２、認証サーバ１０５、印刷装置１０３、アドレス解決サーバ１０６およびネットワーク１０７を含んで構成される。各々のコンポーネント（装置）はネットワーク１０７を介して通信可能に接続されている。ホストコンピュータ１０１は、ユーザに使用されて画像データを生成し、印刷を行なう。認証サーバ１０２および認証サーバ１０５は、ユーザの認証情報やアクセス制限情報を備える。アドレス解決サーバ１０６は、ホストコンピュータ１０１の要求によって認証サーバ１０２および１０５へのアドレスを解決する。印刷装置１０３は、ネット

ワークを介して受信した印刷データを受け取り、電子写真技術やインクジェット技術などの既知の印刷技術を利用して実際の用紙に印刷を行なう。

【００１２】

ホストコンピュータ１０１、認証サーバ１０２、認証サーバ１０５、アドレス解決サーバ１０６および印刷装置１０３は、イーサネット（登録商標）などの既知の技術によるネットワーク１０７により相互に接続されている。なお、各コンポーネントは、それぞれ固有のアドレスが割り振られており、例えば、図１に示す括弧内の４桁の数字のように、ＩＰｖ４におけるアドレスを持つ。図２を参照して、本実施形態のホストコンピュータ１０１、認証サーバ１０２或いはアドレス解決サーバ１０６として機能しえる情報処理装置のハードウェア構成の一例を説明する。図２において、情報処理装置２００は、ＲＯＭ２０３内のプログラム用ＲＯＭあるいは外部メモリ２１１に記憶された文書処理プログラム等に基づいて図形、イメージ、文字、表（表計算等を含む）等が混在した処理を実行するＣＰＵ２０１を備える。さらに、情報処理装置２００は、システムバス２０４に接続される各デバイスをＣＰＵ２０１が総括的に制御する。

【００１３】

また、このＲＯＭ２０３内のプログラム用ＲＯＭあるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるオペレーティングシステムプログラム等を記憶する。また、ＲＯＭ２０３内のフォント用ＲＯＭあるいは外部メモリ２１１には、上記文書処理の際に使用するフォントデータ等を記憶する。また、ＲＯＭ２０３内のデータ用ＲＯＭあるいは外部メモリ２１１には、上記文書処理等を行う際に使用する各種データを記憶する。ＲＡＭ２０２は、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。

【００１４】

キーボードコントローラ（ＫＢＣ）２０５は、キーボード（ＫＢ）２０９や不図示のポインティングデバイスからのキー入力を制御する。ＣＲＴコントローラ（ＣＲＴＣ）２０６は、ＣＲＴディスプレイ（ＣＲＴ）２１０の表示を制御する。２０７はディスクコントローラ（ＤＫＣ）で、ハードディスク（ＨＤ）、フロッピー（登録商標）ディスク（ＦＤ）等の外部メモリ２１１とのアクセスを制御する。外部メモリ２１１は、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、プリンタ制御コマンド生成プログラム（以下プリンタドライバ）等を記憶する。プリンタコントローラ（ＰＲＴＣ）２０８は、双方向性インタフェース（インタフェース）２１を介してプリンタ１０７に接続されて、プリンタ１０７との通信制御処理を実行する。ＮＣ２１２はネットワークに接続されて、ネットワークに接続された他の機器との通信制御処理を実行する。このＮＣ２１２は外部の装置との各種データの入出力を行う入出力手段として機能する。

【００１５】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０２上に設定された表示情報ＲＡＭへのアウトラインフォントの展開（ラスタライズ）処理を実行し、ＣＲＴ２１０上でのＷＹＳＩＷＹＧを可能としている。また、ＣＰＵ２０１は、ＣＲＴ２１０上の不図示のマウスカーソル等で指示されたコマンドに基づいて登録された種々のウインドウを開き、種々のデータ処理を実行する。ユーザは印刷を実行する際、印刷の設定に関するウインドウを開き、プリンタの設定や、印刷モードの選択を含むプリンタドライバに対する印刷処理方法の設定を行える。

【００１６】

次に、図３を参照して、本実施形態に対応する印刷装置１０３のハードウェア構成の一例を説明する。印刷装置１０３は、ＣＰＵ３１２により制御される。プリンタのＣＰＵ３１２は、ＲＯＭ３１３内に記憶された制御プログラム等あるいは外部メモリ３１４に記憶された制御プログラム等に基づいてシステムバス３１５に接続される印刷部（プリンタエンジン）３１７に画像信号を出力する。この画像信号は、後述の図１７のステップＳ１６０６で印刷データ格納部に格納された印刷データに基づき生成されたものに対応する。また、このＲＯＭ３１３内のプログラムＲＯＭには、ＣＰＵ３１２の制御プログラム等を記

憶する。ＲＯＭ３１３内のフォント用ＲＯＭには、上記出力情報を生成する際に使用するフォントデータ等が記憶されている。また、ＲＯＭ３１３内のデータ用ＲＯＭには、ハードディスク等の外部メモリ３１４がないプリンタの場合には、ホストコンピュータ上で利用される情報等が記憶されている。

【００１７】

ＣＰＵ３１２は入力部３１８を介してホストコンピュータとの通信処理が可能となっており、プリンタ内の情報等をホストコンピュータ１００に通知できる。ＲＡＭ３１９は、ＣＰＵ３１２の主メモリや、ワークエリア等として機能するＲＡＭで、図示しない増設ポートに接続されるオプションＲＡＭによりメモリ容量を拡張することができるように構成されている。なお、ＲＡＭ３１９は、出力情報展開領域、環境データ格納領域、ＮＶＲＡＭ等に用いられる。前述したハードディスク（ＨＤ）、ＩＣカード等の外部メモリ３１４は、メモリコントローラ（ＭＣ）２０によりアクセスを制御される。外部メモリ３１４は、オプションとして接続され、フォントデータ、エミュレーションプログラム、フォームデータ等を記憶する。また、３２１は操作パネルで、操作のためのスイッチ及びＬＥＤ表示器等が配されている。また、タッチパネル式のディスプレイを含み、各種動作設定を受け付けることができる。

【００１８】

また、前述した外部メモリ３１４は１個に限らず、複数個備えられ、内蔵フォントに加えてオプションカード、言語系の異なるプリンタ制御言語を解釈するプログラムを格納した外部メモリを複数接続できるように構成されていてもよい。更に、図示しないＮＶＲＡＭを有し、操作パネル３２１からのプリンタモード設定情報を記憶するようにしてもよい。

【００１９】

＜システム全体を表すシーケンス図＞

次に、図４を参照して、印刷システムにおける印刷時の処理概要を説明する。図４は、第１の実施形態におけるシステム全体を説明するシーケンス図である。４００は、ユーザに対応する利用者を示す。なお、ここでは、複数の認証サーバ（認証サーバ１０２、認証サーバ２０５）の中で、認証サーバ１０２が選択された場合ついて説明される。もちろん、認証サーバ１０５が選択された場合であっても同様の説明となる。

【００２０】

ステップＳ４０１において、利用者４００は、ホストコンピュータ１０１に印刷ジョブの発行依頼を入力する。ステップＳ４０２において、ホストコンピュータ１０１は、印刷を行うために、アドレス解決サーバ１０６に対して認証サーバ１０２のアドレス解決依頼を依頼する。これは、認証サーバ１０２からアクセス制限チケットの取得するために行われる。ホストコンピュータ１０１は、アクセス制限チケットを発行する複数の認証サーバ群を、例えば「ＰｒｉｎｔＳｅｒｖｉｃｅ」という名前で認識している。「ＰｒｉｎｔＳｅｒｖｉｃｅ」という名称を固有のアドレスに解決するため、ホストコンピュータ１０１は、アドレス解決サーバ４０３に要求を出す。

【００２１】

次に、ステップＳ４０３において、アドレス解決サーバ１０６は、通知された「ＰｒｉｎｔＳｅｒｖｉｃｅ」に基づき、周期的に、またはランダムに複数の認証サーバから任意の認証サーバを割り当て選択する。ここでは、上述したように認証サーバ１０２が割り当てられる。ステップＳ４０４において、アドレス解決サーバ１０６は、認証サーバ１０２のアドレス、すなわち、図１に示すように１７２．１６．１．３をホストコンピュータ１０１に返却する（通知する）。このアドレス解決の仕組みは、一般に「ダイナミックＤＮＳ」と言われる。

【００２２】

続いて、ステップＳ４０５において、ホストコンピュータ１０１は、通知されたアドレスに従って認証サーバ１０２に対してアクセス制限チケットの発行を要求する。ここで、ホストコンピュータ１０１は、保持している利用者４００のユーザ名およびパスワード等

のユーザ認証情報を認証サーバ１０２に出力し、アクセス制限情報の問い合わせを行うこととなる。ユーザ認証情報は、秘密を守る必要があるため、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）等のセキュア・チャネルを用いて送信される。

【００２３】

アクセス制限チケットの発行要求が通知されると、ステップＳ４０６において、認証サーバ１０２は、送信されたユーザ認証情報が正しいか否かを判定する。この認証は、通知されたユーザ名およびパスワードと、認証サーバ１０２自身が保持しているユーザ名およびパスワードを比較して、通知された認証情報が正確な情報であるか否かを判定する。認証が成功した場合、ステップＳ４０７において、認証サーバ１０２は、アクセス制限チケットを生成する。なお、このアクセス制限チケットは、認証サーバ１０２自身が保持する暗号化情報で暗号しか処理が施されている。アクセス制限チケットの詳細な説明については、図５を用いて後述する。ここでは具体的に、アクセス制限チケットには、認証サーバ１０２の自分のアドレス情報（１７２．１６．１．３）と、認証サーバ自身が保持する公開鍵ペアの秘密（私有）鍵でデジタル署名を行った結果とが含まれる。このアドレス情報は、アクセス制限チケットを用いてジョブ依頼が行われる印刷装置１０３において、認証サーバ１０２を識別するための識別子として用いられる。従って、認証サーバ１０２を一意に識別可能な情報であれば、ＩＰアドレスに限定されるものではなく、物理（ＭＡＣ）アドレスを用いても良い。また、認証サーバ１０２ごとにユニークな認証サーバ名が与えられている場合には、係る認証サーバ名を用いても良い。いずれにしても、認証サーバ１０２が一意に識別するための識別子として機能する限りは、どのような情報であっても良い。アクセス制限チケットを生成すると、ステップＳ４０８において、認証サーバ１０２は、ホストコンピュータ１０１にアクセス制限チケットを返却（応答）する。

【００２４】

次に、ステップ４０９において、ホストコンピュータ１０１は、利用者４００が依頼した印刷ジョブに関するデータに認証サーバから応答されたアクセス制限チケットを添付してアクセス制限チケットを含む印刷ジョブを、印刷装置１０３に出力する。

【００２５】

印刷ジョブが通知されると、ステップＳ４１０において、印刷装置１０３は、送信されたアクセス制限チケットを確認する。ここではまず、アクセス制限チケットに含まれる或は付加される認証サーバ１０２のアドレス情報に紐づいた公開鍵を保有しているか否かを判定する。保持していないと判定した場合には、先の検証した認証サーバのアドレス情報に従いステップＳ４１１において、印刷装置１０３は、認証サーバ１０２に公開鍵を取得する要求を発行する。ここでの公開鍵の取得は、新たな認証サーバに対応する公開鍵の取得である場合と、以前から認識していた認証サーバに対応する公開鍵が変更された場合の複数通りの場合が考えられる。

【００２６】

また、ステップＳ４１１では、復号化情報としての公開鍵をアクセス制限チケットに含まれる或は付加される認証サーバのアドレス情報に従いネットワークを介して取得している。しかしこの形態には限定されない。例えば、まず割り当てられた認証サーバの識別子にＭＡＣアドレスや認証サーバ名が適用されている場合には、該ＭＡＣアドレスや認証サーバ名を用いＤＮＳサーバ等より認証サーバのアドレスを取得する。そして、該取得したアドレスに従い復号化情報としての公開鍵を取得しても良い。即ち、アクセス制限情報に含まれる認証サーバの識別子に応じた復号化情報（公開鍵等）を取得する点が特徴的動作となる。

【００２７】

ステップＳ４１２において、印刷装置１０３は、認証サーバ１０２から公開鍵を受信して公開鍵格納部に格納する。ステップＳ４１３において、印刷装置１０３は、アクセス制限チケットに含まれる署名の検証を実施する。署名の検証が成功した場合、ステップＳ４１４において、印刷装置１０３は、印刷を実施する。

【００２８】

なお、本実施形態においては、認証サーバ１０２が、自身が保持する秘密鍵（暗号化情報）でアクセス制限情報を暗号化処理し、印刷装置１０３で公開鍵（復号化情報）を用いて復号化される例を挙げている。しかしながら、この暗号化方法は、一適用例であり、例えば、認証サーバ１０２が複数の印刷装置ごとに対応する秘密鍵でアクセス制限情報を暗号化し、印刷装置において、自身が保持する公開鍵を利用して復号化するようにしてもよい。また、公開鍵や秘密鍵等を用いず、その他の暗号化や復号化を行う為の暗号化情報及び復号化情報を適用しても良い。以下では、説明をわかりやすくするために、暗号化情報として秘密鍵を、復号化情報として公開鍵を例に説明していく。

【００２９】

次に、図５を参照して、アクセス制限チケットに含まれる情報について説明する。図５は、第１の実施形態に対応する認証サーバが保持するアクセス制限情報に関連した情報を示す図である。アクセス制限チケットは、ユーザ名、パスワードからなる認証情報に対して発行される。例えば、アクセス制限チケットは、アクセス制限情報として印刷可能枚数、ページレイアウトおよびカラー設定等の情報が含まれる。

【００３０】

認証サーバ１０２は、ユーザ名５０１、パスワード５０２、枚数最大値５０３、枚数実績値５０４および印刷制限５０５の情報を有する。ユーザ名５０１は、印刷システムにアクセス可能なユーザに対してユニークなＩＤが割り当てられる。さらに、１つのユーザ毎に、それぞれパスワード５０２が設定される。枚数最大値５０３は、当該ユーザが一ヶ月内に実施できる印刷枚数の最大値を示す。また、枚数実績値５０４は、当該ユーザが今月に入って実際に印刷した枚数を示す。さらに、印刷制限５０５は、ユーザによって制限される印刷条件を示す。印刷条件とは、モノクロ印刷もしくはカラー印刷、または片面印刷もしくは両面印刷等の印刷時の設定における制限を示す。例えば、本実施形態に対応する印刷システムの管理者は、コスト削減を目的として、印刷条件を両面印刷と、モノクロ印刷のみに制限することができる。

【００３１】

なお、ここでは、図５に示すように、パスワード５０２を平文のパスワードとしているが、実際にはセキュリティの都合上、パスワードが漏洩しないように、平文の一方向ハッシュ値だけを格納することが望ましい。そのため、認証の際には、入力されたパスワードのハッシュ値と比較することによって認証を行なうなどの方法が実施される。しかしながら、本発明の趣旨から外れるため、詳細については省略する。また、本発明におけるデータベースは、同じくセキュリティの都合上、管理者権限でのみ読み書き可能であることはいうまでもない。

【００３２】

以下では、具体例について、行５１１を参照して説明する。ユーザ名５０１は、”Ｕｓｅｒ１”というユーザのエントリを示し、パスワード５０２は、”Ａｋｄ５ｓｊ４ｆ”という文字列を示す。また、枚数最大値５０３は、５００枚となっており、Ｕｓｅｒ１は、月の印刷枚数が５００枚までに制限されていることがわかる。さらに、枚数実績値５０４は、１２３枚となっており、Ｕｓｅｒ１が今月１２３枚の印刷をすでに行なっていることを示す。

【００３３】

同様に、行５１２にはＵｓｅｒ２についての各情報が定義され、行５１３にはＵｓｅｒ３の各情報が定義されている。行５１４は、ゲストユーザの情報を定義している。ゲストユーザについては、パスワード５０２が設定されていないが、枚数最大値が０であることから、ゲストユーザが印刷できないことを示している。ゲストユーザを設けるか否かは、システムポリシーによって決まるものであり、このようなユーザが設定されてもよいし、設定されなくてもよい。

【００３４】

ユーザは、ホストコンピュータ１０１にログオンするため、ユーザ名５０１およびパスワード５０２を入力する。この入力された認証情報は、認証サーバ１０２に伝達され、認

証サーバ１０２で保持されているユーザ名５０１およびパスワード５０２と照合される。認証が成功すると、枚数最大値５０３と枚数実績値５０４を含むアクセス制限チケットをホストコンピュータ１０１に通知する。例えば、ユーザがＵｓｅｒ１である場合、アクセス制限チケットは、枚数最大値＝５００、枚数実績値＝１２３および印刷条件としてモノクロ印刷および両面印刷が返される。なお、アクセス制限チケットは、上述したような情報（アクセス制御リスト）を有する。

【００３５】

アクセス制限チケットが通知されると、ホストコンピュータ１０１は、アクセス制御リストに応じて、枚数最大値＝５００、枚数実績値＝１２３を考慮して、５００－１２３＝３７７枚までを印刷可能と認識する。したがって、ホストコンピュータ１０１は、印刷ジョブの枚数が３７７枚以内である場合、印刷を実行し、印刷ジョブの枚数が３７８枚以上である場合、印刷可能枚数を超えているとして、警告を発してユーザに操作を促す。

【００３６】

＜ホストコンピュータからの印刷指示ユーザインタフェース＞

次に、図６を参照して、ホストコンピュータ１０１からユーザに報知される印刷指示について説明する。図６は、第１の実施形態に対応するホストコンピュータが出力する印刷指示に関するダイアログのＧＵＩを示す図である。ダイアログ６０１は、印刷を実行する印刷ボタン６０２および印刷の取り消しを行う取り消しボタン６０３を含んで構成される。また、表示６０４は、印刷ジョブが印刷可能枚数を超えている場合、正常に印刷されないことを報知するための警告が表示される。

【００３７】

印刷ボタン６０２が押下されると、ホストコンピュータ１０１は、印刷ジョブの出力枚数を３７７枚に縮退して印刷を行なう。したがって、残りの２３枚は印刷されない。そのため、ユーザにとっては、所望の印刷結果が得られないこととなる。取り消しボタン６０３が押下されると、ホストコンピュータ１０１は、印刷要求そのものを破棄し、印刷が取り消される。

【００３８】

＜印刷装置の機能ブロック図＞

次に、図７を参照して、印刷装置１０３の制御を機能ブロックごとに説明する。図７は、第１の実施形態に対応する印刷装置において、詳細な機能構成の一例を示すブロック図である。図７に示す各ブロックは、ハードウェア、或は、ソフトウェア、或は、それらの協働により構築される。

【００３９】

印刷装置１０３は、インタフェース部７０１、制限チケット判定部７０２、パケット変換部７０４、印刷データ格納部７０７、公開鍵取得部７１３、公開鍵格納部７１４、ＧＵＩ部７０６および印刷ジョブ取消部７０５を含んで構成される。さらに、印刷装置１０３は、ジョブ管理部７０８、印刷データ解釈部７０９、イメージデータ格納部７１０およびプリンタエンジン７１１を含んで構成される。

【００４０】

インタフェース部７０１は、ネットワーク１０７と接続され、ホストコンピュータ１０１から印刷ジョブを受信する。制限チケット判定部７０２は、受信した印刷ジョブの形式を判別してアクセス制限チケットが付与されているか否かを判定する。公開鍵格納部７１４は、１台以上の認証サーバから取得した公開鍵を格納する保持手段として機能する。公開鍵取得部７１３は、インタフェース部７０１を介して認証サーバから固有の公開鍵を取得する。

【００４１】

パケット変換部７０４は、アクセス制限チケットが付与されている場合に、その制限情報に基づき、署名検証の実施と、印刷ジョブに対する指示を縮退して後段に通知する。印刷ジョブ取消部７０５は、アクセス制限チケットが付与されていない印刷ジョブに対して印刷の取消を指示する。印刷データ格納部７０７は、印刷ジョブに含まれる印刷データ、

すなわちＰＤＬ（ページ記述言語）データを一時的に格納する。ジョブ管理部７０８は、印刷ジョブの印刷するページ数やカラーなどの出力属性情報を一時的に格納する。印刷データ解釈部７０９は、ジョブ管理部７０８に格納された属性情報に従うとともに、印刷データ格納部７０７から印刷データを取得して画像生成処理を行ない、印刷するイメージデータを生成する。イメージデータ格納部７１０は、印刷データ解釈部７０９によって生成されたイメージデータを印刷が完了するまで一時的に格納する。プリンタエンジン７１１は、イメージデータ格納部７１０に格納されているイメージデータを、電子写真技術やインクジェット技術などの既知の印刷技術を用いて印刷用紙などのメディアに実際に印刷する。なお、印刷データ格納部７０７およびイメージデータ格納部７１０が大容量のハードディスクなどの二次記憶装置で構成される場合もあるが、本発明は、このような物理構成を限定するものではない。

【００４２】

＜印刷ジョブの形式について＞

次に、図８を参照して、印刷ジョブに含まれるジョブパケットの形式について説明する。印刷ジョブは、印刷ジョブの開始と終了の認識および印刷ジョブの属性の設定が容易に行われるように規格化された１つ以上のジョブパケットによって構成されている。図８は、第１の実施形態に対応するジョブパケットの構造を示す図である。縦軸８０１は、バイトを示し、横軸８０２は、各バイトのビットを示している。なお、０～１１バイトまでは固定領域８２０であってこれによりヘッダ部が構成され、１２バイト目以降のデータ部８０９は変動領域であってボディ部が構成される。

【００４３】

０～１バイト目のオペレーションコード８０３は、パケットの機能を示す長さ２バイトのＩＤである。

０ｘ０２０１　ジョブ開始オペレーション
０ｘ０２０２　ジョブ属性設定オペレーション
０ｘ０２０４　ＰＤＬデータ送信オペレーション
０ｘ０２０５　ジョブ終了オペレーション
０ｘ０３０１　制限情報オペレーション

ジョブパケットは、例えば、上記に示すようなパケットの機能が設定されうる。

【００４４】

２～３バイト目のブロック番号８０４は、ジョブパケットを送信された受信側が返答要求をする場合に、受信側からの返答が送信側のどの返答要求に対するものであるか、その対応を取るために使用する番号である。例えば、送信側がそれぞれブロック番号８０４が１、２、３というジョブパケットを立て続けに送信したと想定する。ここで、ブロック番号８０４が２というエラーパケットが返答された場合、送信側は、２番目に送ったジョブパケットにエラーが発生したことを特定して、再送することが可能である。

【００４５】

４～５バイト目のパラメータ長８０５は、データ部８０９のバイト長を示す領域で、０～６４Ｋバイトまでを示すことが可能である。６～７バイト目はジョブパケットの各種フラグ８０６が格納される領域で、それぞれ以下の内容を示す。

【００４６】

エラーフラグ８１１は、値が１である場合、印刷装置１０３で何らかのエラーが発生したことを示す。エラーフラグ８１１は、印刷装置１０３からホストコンピュータ１０１に送られる返信パケットに付加される。通知フラグ８１２は、値が１である場合、ホストコンピュータ１０１からの要求パケットに対する返答ではなく、印刷装置１０３が何らかの通知事項があることをホストコンピュータ１０１に通知することを示している。

【００４７】

返答要求８１３は、ホストコンピュータ１０１が印刷装置１０３に対して返答パケットを要求する場合に１をセットする。０の場合は、送ったパケットが正常に処理された場合に、返答を必要としないことを示す。印刷装置１０３でエラーが発生した場合には返答要

求が０または１であるに関わらず、常にエラーフラグを１にした返答パケットが送られる。継続フラグ８１４は、この値が１の場合、データ部８０９に全てのデータが入らなかったため、分割されて次のジョブパケットに残りのデータが送られることを示す。この場合、ジョブパケットは、前のパケットと同じオペレーションコードが設定される。返答送信８１５は、何らかの送信に対しての返答であるか或いは新たな送信であるかを示す。例えば、返答送信８１５は、１が設定された場合に、何らかの送信に対する返答であることを示すようにしてもよい。

【００４８】

８～９バイト目のユーザＩＤ８０７および１０～１１バイト目のパスワード８０８は、送ったパケットでできる操作にセキュリティ的制限を設ける際にその認証に使われる領域である。本実施形態においては使用しなくてもよい。

【００４９】

１２バイト目以降のデータ部８０９は、オペレーションコードに対応したデータが格納される。ジョブ開始オペレーションおよびジョブ終了オペレーションの場合、データ部８０９には、データが格納されない。

【００５０】

ジョブ属性設定オペレーションの場合、設定したいジョブ属性ＩＤとジョブ属性値をデータ部８０９に格納する。ジョブ属性ＩＤとは、ジョブに関する属性或いは環境に対応して付けられた識別子で、ＩＳＯ－１０１７５（ＤＰＡ）（ＩＳＯ：国際標準化機構）で規定されるジョブの属性に相当するＩＤが予め割り振られている。以下にジョブ属性ＩＤの代表的なものを挙げる。

０ｘ０１０１　　ジョブ名称
０ｘ０１０３　　ジョブオーナ名
０ｘ０１６ａ　　ジョブサイズ
０ｘ０１７４　　印刷ページ数

このほか、印刷装置１０３の機能に応じて、印刷部数またはモノクロもしくはカラーなどのジョブ属性とそれに対応するＩＤを割り振ることができる。

【００５１】

＜機能制限情報なし印刷ジョブ＞

次に、図９を参照して、従来の印刷ジョブに含まれる内容について説明する。図９は、従来における印刷ジョブの構成を示した図である。ここでは、上方のジョブパケットから下方のジョブパケットに向かって順番に、ホストコンピュータ１０１から印刷装置１０３に送られてくるものとする。また、一つのパケットに関してヘッダ部と記入されているのは、図８における０～１１バイト目の固定領域８２０に対応し、ボディ部は１２バイト目以降のデータ部８０９に対応する。

【００５２】

印刷ジョブ９００は、ジョブ開始９０１、属性設定９０２、９０３、印刷データ９０４、９０５およびジョブ終了９０６のジョブパケットを含んで構成される。なお、この印刷ジョブ９００は、一適用例であり、印刷ジョブの構成を限定するものではない。

【００５３】

ジョブ開始９０１は、印刷ジョブの開始を宣言するジョブパケットから構成される。ジョブ開始９０１は、オペレーションコード８０３がジョブ開始オペレーションを示す０ｘ０２０１であることから判断される。属性設定９０２、９０３は、印刷ジョブのジョブ名称やオーナ名称、印刷条件などを設定する属性設定である。属性設定９０２、９０３は、オペレーションコード８０３が属性設定オペレーションを示す０ｘ０２０２であることから判断される。複数の属性設定を行なう場合、ホストコンピュータ１０１は、複数の属性設定９０２、９０３を生成して、印刷装置１０３へ送信する。

【００５４】

印刷データ９０４、９０５は、紙などのメディア等に形成される画像のデータが含まれる。印刷データ９０４、９０５は、オペレーションコード８０３がＰＤＬデータ送信オペ

レーションを示す０ｘ０２０４であることから判断される。属性設定９０２、９０３と同様に、ホストコンピュータ１０１は、複数の印刷データ９０４、９０５を生成して、印刷装置１０３に送信してもよい。最後に、印刷ジョブ９００は、ジョブ終了９０６を示すジョブパケットで構成される。ジョブ終了９０６は、オペレーションコード８０３がジョブ終了オペレーションを示す０ｘ０２０５であることから判断される。印刷装置１０３は、ジョブ終了９０６を受信した段階で印刷ジョブ９００が終了したことを認識する。

【００５５】

＜機能制限情報付き印刷ジョブ＞

次に、図１０および図１１を参照して、本実施形態における印刷ジョブに含まれる内容およびアクセス制限チケットに含まれる制限情報について説明する。図１０は、第１の実施形態に対応する印刷ジョブの構成を示した図である。ここでは、説明の重複を避けるため図９に示す従来の印刷ジョブとの違いについてのみ説明される。

【００５６】

印刷ジョブ１０００は、先頭に制限情報１００１を示すジョブパケットをさらに含んで構成される。制限情報１００１は、オペレーションコード８０３が制限情報オペレーションを示す０ｘ３０１であることによって判断される。制限情報オペレーションを指定されたジョブパケットは、データ部分にアクセス制限チケットが記載されている。

【００５７】

図１１は、第１の実施形態に対応するアクセス制限チケットに含まれる制限情報の書式例を示す図である。”ＭＡＸ＿ＰＲＩＮＴ”という文字列は、当該印刷ジョブで出力できる枚数の上限数を示しており、”＝１００”は、その値の設定を示している。したがって、当該印刷ジョブにおける印刷可能枚数は、上限値が１００枚ということになる。

【００５８】

”ＳＴＲＩＣＴ＿ＤＵＰＬＥＸ”という文字列は両面印刷を強制するか否かを示しており、”＝ＴＲＵＥ”は強制的に両面印刷を行うことを示している。”ＳＴＲＩＣＴ＿Ｎｉｎ１”は１つの紙面にいくつの論理ページをレイアウトするか（すなわち、Ｎｉｎ１やＮｕｐ機能）を決定するものであり、”＝２”は強制的に２ｉｎ１を実施することを示している。”ＳＴＲＩＣＴ＿ＭＯＮＯＣＯＬＯＲ”はカラー印刷機能のある印刷装置において印刷出力をモノクロに制限するか否かを示しており、”＝ＴＲＵＥ”は強制的に白黒で印刷することを示している。

【００５９】

上記の設定は印刷用紙、トナーおよびインクなどの着色剤の消費節約に繋がるものであり、ＴＣＯの削減に有効である。さらに、印刷装置１０３は、アクセス制限チケットが正規な認証サーバから発行されたことを検証するために、デジタル署名による検証を実施している。

【００６０】

＜アクセス制御チケットのフォーマット構造＞

次に、制限情報１００１を構成するジョブパケットの構成について説明する。図１２は、第１の実施形態に対応するアクセス制限チケットのジョブパケットを示す図である。なお、ここでは、説明の重複を避けるため、図８と同様の説明のについては、省略される。

【００６１】

制限情報１００１のジョブパケットは、０－１１バイト目までのヘッダ部８２０および１２バイト目以降のデータ領域であるボディ部８０９を含んで構成される。また、ボディ部８０９は、制限情報１２０１、認証サーバアドレス情報１２０２および署名１２０３を含んで構成される。

【００６２】

制限情報１２０１は、先頭からＮＵＬＬ文字１２０４までの領域を有する。制限情報１２０１は、図５を用いて説明した情報が設定される。認証サーバアドレス情報１２０２は、当該認証サーバに対応した公開鍵を保持しているか検索するためのキーと、公開鍵を保持していない場合に、公開鍵を取得する認証サーバのアドレスが設定されている。認証サ

ーバアドレス情報１２０２の後の領域には、１２８ｂｙｔｅのデジタル署名である署名１２０３が設定されている。この署名１２０３は、制限情報１００１が正規な認証サーバ１０２もしくは１０５から発行されており、途中経路で不正な手段で書き換えられていないことを保証するものである。なお、どちらの認証サーバであるかは、認証サーバアドレス情報１２０２に記載されてる。

【００６３】

署名１２０３は、例えば、ＲＳＡ（Ｒｉｖｅｓｔ　Ｓｈａｍｉｒ　Ａｄｌｅｍａｎ）公開鍵暗号方式を使った方式が一般的である。公開鍵方式によるデジタル署名は、署名対象（この場合、制限情報１２０１）から一方向関数によるダイジェストを生成する。さらに、このデジタル署名は、当該ダイジェストを発行元（この場合は認証サーバ１０２もしくは１０５）において保有する秘密鍵で暗号化される。署名検証については、印刷装置１０３が公開鍵を使用して実施する。秘密鍵は、正規な認証サーバだけが内部に保持しており、正しい公開鍵を使った署名検証が成功すれば署名対象が正規なものであることを証明できる。ここで、デジタル署名に使用する公開鍵は、認証サーバ１０２もしくは１０５が保持する公開鍵ペアが利用される。したがって、公開鍵は、印刷に先立って予め認証サーバ１０２もしくは１０５から印刷装置１０３に渡されることとなる。一度認証サーバから公開鍵を取得すると、印刷装置１０３は、取得した公開鍵を公開鍵格納部７１４に保持する。なお、前述したように、認証サーバ１０２、１０５が複数の印刷装置ごとに対応する秘密鍵でアクセス制限情報を暗号化し、印刷装置１０３において、自身が保持する公開鍵を利用して復号化するようにしてもよい。

【００６４】

次に、図１３を参照して、制限情報１１０１が付与されていない印刷ジョブを受け付けた場合の、印刷装置１０３の動作設定について説明する。図１３は、第１の実施形態に対応する印刷装置１０３の操作部３２１のタッチパネルに表示される表示される画面の一例を示す図である。印刷装置１０３の管理者は、図１３のような画面を利用して、印刷ジョブにおける先頭のジョブパケットが制限情報１１０１でない場合に、印刷装置１０３が印刷ジョブを実行するか否かを、予め設定しておくことができる。

【００６５】

ダイアログ１３０１は、印刷を許可する印刷許可ボタン１３０２および印刷を無効にする印刷無効ボタン１３０３を含んで構成される。また、表示１３０４は、現状の設定値を示している。

【００６６】

印刷許可ボタン１３０２が操作された場合には、印刷装置１０３は、制限情報１１０１が含まれていない印刷ジョブであっても、印刷を実行する設定となる。この場合、対応する設定値が印刷装置１０３のＲＡＭ３１９に格納される。この設定がなされた場合、印刷装置１０３は、印刷ジョブに制限情報１１０１が付与されない場合であっても、印刷を実行することとなる。しかしながら、消耗品等のコストを考慮すると、この設定は、常に無効であることが望ましい。なお、図１３では一律に許可するか無効とするかを設定可能な場合を示しているが、ユーザ毎にこの設定を許可するか否かを設定するようにしてもよい。一方、印刷無効ボタン１３０３が操作された場合には、印刷装置１０３は制限情報１１０１が含まれていない印刷ジョブを無効として印刷を実行しない設定となる。この場合、対応する設定値が印刷装置１０３のＲＡＭ３１９に格納される。

【００６７】

＜印刷ジョブの受信処理＞

次に図１４を参照して、印刷装置１０３における制限チケット判定部７０２の制御について説明する。図１４は、第１の実施形態に対応する制限チケット判定部の動作を説明するフローチャートである。なお、アクセス制限チケット判定部７０２は印刷装置１０３の起動とともに動作を開始し、以降印刷装置１０３の電源遮断まで動作を継続する。

【００６８】

ステップＳ１４０１において、制限チケット判定部７０２は、インターフェイス部７０

１を検査する。これは、印刷ジョブのジョブパケットがインタフェース部７０１に送信されているか否かを検査する処理である。ステップＳ１４０２において、Ｓ１４０１で印刷ジョブが受信できていない場合、制限チケット判定部７０２は、再度、Ｓ１４０１へ処理を遷移させる。一方、印刷ジョブが受信できている場合、制限チケット判定部７０２は、処理をＳ１４０３に遷移させる。

【００６９】

ステップＳ１４０３において、制限チケット判定部７０２は、インタフェース部７０１から印刷ジョブ中の最初（先頭）のジョブパケットを１個取得する。さらに、ステップＳ１４０４において、制限チケット判定部７０２は、取得したジョブパケットからヘッダ部のオペレーションコードを取り出す。ステップＳ１４０５において、アクセス制限チケットの有無を検知する。より具体的には、制限チケット判定部７０２は、オペレーションコードが制限情報オペレーションを示す０ｘ０３０１であるか否かを判定する。

【００７０】

Ｓ１４０５で制限情報オペレーションであると判定した場合、ステップＳ１４０６において、制限チケット判定部７０２は、取得したジョブパケットをパケット変換部７０４に送信する。その後、ステップＳ１４０７において、制限チケット判定部７０２は、さらにインタフェース部７０１から次のジョブパケットを取得する。次のジョブパケットを取得すると、ステップＳ１４０８において、制限チケット判定部７０２は、オペレーションコードが０ｘ０２０５、即ち、ジョブ終了を示すオペレーションであるか否かを判定する。ジョブ終了オペレーションであると判定すると処理をＳ１４０１に遷移させて、次の印刷ジョブが送信されてきた場合に備える。一方、ジョブ終了オペレーションでないと判定した場合、制限チケット判定部７０２は、処理をＳ１４０６に遷移させて取得したジョブパケットをパケット変換部７０４に送信する。

【００７１】

一方、Ｓ１４０５で制限情報オペレーションコードでないと判定した場合、ステップＳ１４０９において、制限チケット判定部７０２は、制限情報が付与されていない印刷ジョブであっても、印刷を許可するか否かを判定する。ここでの判定は、図１３を用いて予め設定された設定内容に基づいて行うことができる。即ち、図１３の設定画面において「印刷を許可する（１３０２）」との設定がなされていた場合には、印刷を許可するとの判定（ステップＳ１４０９において「ＹＥＳ」）が行われる。一方、「印刷を無効にする（１３０３）」との設定が成されていた場合には、印刷を無効とする判定（ステップＳ１４０９において「ＮＯ」）が行われる。ステップＳ１４０９において印刷を許可する場合は、処理をステップＳ１４０６に遷移し、許可しない場合は、印刷ジョブのジョブパケットを破棄するため、処理をＳ１４１０に遷移する。ステップ１４１０において、制限チケット判定部７０２は、不正な印刷ジョブと認識して、パケットを印刷ジョブ取消部７０５に送信する。

【００７２】

次に、ステップＳ１４１１において、さらに、制限チケット判定部７０２は、次のジョブパケットを取得する。その後、ステップＳ１４１２において、制限チケット判定部７０２は、オペレーションコードが０ｘ０２０５、即ち、ジョブ終了を示すオペレーションであるか否かを判定する。ジョブ終了オペレーションであると判定すると処理をＳ１４０１に遷移させて、次の印刷ジョブが送信されてきた場合に備える。一方、ジョブ終了オペレーションでないと判定した場合、制限チケット判定部７０２は、処理をＳ１４０９に遷移させて、不正な印刷ジョブに含まれる全てのジョブパケットを破棄するまで繰り返すこととなる。

【００７３】

＜パケット変換部７０４の動作説明＞

次に、図１５、図１６を参照して、パケット変換部７０４の動作を説明する。図１５、図１６は、第１の実施形態に対応するパケット変換部におけるパケット交換処理の動作を示すフローチャートである。なお、パケット変換部７０４は、印刷装置１０３の起動とと

もに動作を開始し、以降印刷装置１０３の電源遮断まで動作を継続する。

【００７４】

ステップＳ１５０１において、パケット変換部７０４は、制限チケット判定部７０２からジョブパケットを１つ取得する。ジョブパケットを取得すると、まず、ステップＳ１５０２において、アクセス制限チケットの有無を検知する。具体的には、パケット変換部７０４は、オペレーションコードの領域を検査して制限情報を示す０ｘ０３０１であるか否かを比較する。ジョブパケットが制限情報パケット１００１である場合は、Ｓ１５０３に処理を遷移し、制限情報パケット１００１以外である場合は、図１６に示すＳ１６０１に処理を遷移する。図１６は検証手段により入力されたデータが正当であると検証された場合に入力された印刷ジョブの実行を制御するジョブ実行制御手段の処理を示す。

【００７５】

ジョブパケットが制限情報パケット１００１である場合、ステップＳ１５０３において、パケット変換部７０４は、アクセス制限チケットに含まれる認証サーバアドレス情報１２０２を取り出す。認証サーバアドレス情報には、図１２で説明したように、アクセス制限チケットを発行した認証サーバのアドレス（識別子）が格納されている。次に、ステップＳ１５０４において、パケット変換部７０４は、当該認証サーバ１０２に対応する公開鍵が取得済であるか否かを公開鍵格納部７１４に保持される情報を元に確認する。取得済みでない場合、ステップＳ１５０５において、パケット変換部７０４は、公開鍵の取得を公開鍵取得部７１３に依頼して、当該認証サーバ１０２から公開鍵を取得する。その後、処理をＳ１５０６に遷移する。なお、Ｓ１５０５における復号化情報としての公開鍵の取得方法については、上に説明したステップＳ４１１と基本的に同様である。つまり、復号化情報としての公開鍵をアクセス制限チケットに含まれる、或は付加される認証サーバのアドレス情報に従いネットワークを介して取得しているが、これには限定されない。例えば、割り当てられた認証サーバの識別子にＭＡＣアドレスや認証サーバ名が適用されている場合には、該ＭＡＣアドレスや認証サーバ名を用いＤＮＳサーバ等より認証サーバのアドレスを取得する。そして、該取得したアドレスに従い復号化情報としての公開鍵を取得しても良い。即ち、アクセス制限情報に含まれる認証サーバの識別子に応じた復号化情報（公開鍵等）を取得する点が特徴的動作となる。

【００７６】

公開鍵が所得済みであるか、または取得されると、ステップＳ１５０６において、パケット変換部７０４は、取得した公開鍵を利用して署名１２０３の検証を実施する。署名の検証結果が一致した場合、ステップＳ１５０７において、パケット変換部７０４は、検証結果が一致した（成功した）か否かを判定する。一致した場合は、ステップＳ１５０８において、パケット変換部は、制限情報１２０１を取得し、所定の記憶部に記憶してＳ１５０１に戻る。検証結果が一致しなかった場合には、ステップＳ１５０９において、パケット変換部７０４は、当該ジョブパケットを破棄し、ステップＳ１５１０において、次のジョブパケットを取得する。その後、ステップＳ１５１１において、パケット変換部７０４は、取得したジョブパケットについて、ジョブ終了を示すオペレーションコードであるか否かを判定する。ジョブ終了である場合は、処理をＳ１５０１に遷移し、ジョブ終了でない場合は、処理をＳ１５０９に戻してジョブパケットを破棄する。したがって、検証が失敗した場合には、当該印刷ジョブのジョブ終了までジョブは破棄されることとなる。

【００７７】

一方、Ｓ１５０２において、ジョブパケットが制限情報でないと判断された場合、パケット変換部７０４は、通常のジョブパケットの解釈処理を行う。図１６のステップＳ１６０１において、パケット変換部７０４は、オペレーションコードがジョブ開始を示しているか否かを判定する。ジョブ開始の場合、ステップＳ１６０２において、パケット変換部７０４は、新規のジョブ生成として、ジョブ管理部７０８上に当該印刷ジョブの領域を確保し、ジョブ識別子を割り当てる。また、Ｓ１６０１でオペレーションコードがジョブ開始以外であると判定した場合、ステップＳ１６０３において、パケット判定部７０４は、オペレーションコードが属性設定であるか否かを判定する。属性設定である場合は、ステ

ップＳ１６０４において、パケット変換部７０４は、ジョブ管理部７０８上の当該印刷ジョブの属性領域に当該属性値を設定する。次に、ステップＳ１６０５において、オペレーションコードがＰＤＬデータ送信を示す場合は、印刷データ格納部７０７に印刷データを格納する。その後、ジョブ開始、属性設定またはデータ送信の何れの場合であっても、パケット変換部７０４は、処理をＳ１５０１に遷移させる。

【００７８】

＜印刷データ解釈部７０９の動作説明＞

次に、図１７を参照して、制限情報に基づく印刷データ解釈部７０９における印刷データ解釈処理の動作を説明する。この図１７は、印刷ジョブの処理をするジョブ実行手段として機能する。図１７は、第１の実施形態に対応する印刷データ解釈部７０９の処理動作を説明するフローチャートである。印刷データ解釈部７０９は、ＰＤＬデータ送信オペレーションのジョブパケットにおけるデータ部８０９に設定されたＰＤＬ（ページ記述言語）を解釈し、実際の印刷に使用するイメージデータを生成する。ＰＤＬは、ポストスクリプトやＬＩＰＳなど多種の規格が実現化されている。なお、印刷データ解釈部７０９は、印刷ジョブを受信し、当該印刷ジョブの最後のページの解釈が完了するまで処理を継続する。

【００７９】

ステップＳ１７０１において、印刷データ解釈部７０９は、ページ数を示す変数ｎを１に初期化する。変数ｎは、全てのジョブパケットを受信した段階で、印刷するページ数をカウントするために使用される。次に、ステップＳ１７０２において、印刷データ解釈部７０９は、ＰＤＬコマンドを印刷データ格納部７０７から取得する。ＰＤＬコマンドを取得すると、ステップＳ１７０３において、ＰＤＬコマンドの解釈処理を行なう。ここで、ＰＤＬコマンドとは、例えば、ＬＩＰＳ言語における「矩形描画」や「イメージ描画」のような実際に描画を行なうコマンドを想定している。

【００８０】

ステップＳ１７０４において、印刷データ解釈部７０９は、Ｓ１７０３で処理したコマンドがページ終了コマンドであるか否かを判定する。ページ終了コマンドでない場合、Ｓ１７０２に処理を遷移する。一方、ページ終了コマンドである場合、ステップＳ１７０５において、印刷データ解釈部７０９は、ページ数を示す変数ｎをインクリメントする。次に、ステップＳ１７０６において、印刷データ解釈部７０９は、変数ｎがＳ１７０５で設定された制限情報に従って制限ページ数を超えているか否かを判定する。超えていなければ、処理をＳ１７０２に遷移し、超えていれば、処理をＳ１７０７に遷移する。制限ページ数を超えている場合は、ステップＳ１７０７において、印刷データ解釈部１７０６において、残りのジョブパケットを破棄する。図１１の例でいえば、最大印刷枚数が１００枚であるため、印刷データのページ終了コマンドを１００回検知した時点で残りのデータは読み飛ばされ、印刷されずに破棄されることとなる。

【００８１】

次に、図１８を参照して、送信された印刷ジョブを取り消す場合の印刷ジョブ取消部７０５の印刷ジョブ取消処理を説明する。図１８は、第１の実施形態に対応する印刷ジョブ取消部の処理動作を説明するフローチャートである。印刷ジョブ取消部７０５は、印刷装置１０３の起動とともに動作を開始し、以降印刷装置１０３の電源遮断まで動作を継続する。

【００８２】

印刷ジョブ取消部７０５には、アクセス制限チケット判定部７０２で制限情報を含まないと判断され、図１４に示すＳ１４０９において許可されない場合に、当該印刷ジョブが転送される。１８０２においてジョブパケットを取得し、１８０３においてジョブパケットの破棄を行なう。１８０４においてジョブ終了かどうかを判定し、終了でない場合は１８０２に戻り、処理を継続する。終了ならそのまま処理を終える。

【００８３】

［第２の実施形態］

次に、第２の実施形態について説明する。第１の実施形態においては、異なる認証サーバを認識したときに、すなわち、公開鍵を取得済みでない場合に、新規で公開鍵を取得する技術について記載した。しかし、認証サーバに格納される公開鍵ペアは、通常、一意に決定されると想定されるが、下記の条件によっては公開鍵ペアそのものが置き換わる可能性もある。

【００８４】

例えば、認証サーバそのものの置き換え（リプレイス）によって以前の公開鍵が使えなくなった場合、何らかの攻撃により公開鍵ペアの漏えいが行われたために従来の公開鍵ペアを無効とした場合または公開鍵の有効期限を過ぎた場合等の可能性が想定される。

【００８５】

第２の実施形態では、これらの状態を想定して、第１の実施形態に加えた改良について記載する。システム構成は図１と同様であり、印刷装置の内部構成は図７と同様であるが、パケット変換部７０４の動作に変更を加える。以下では、本実施形態と第１の実施形態の異なる技術について主に記載する。

【００８６】

図１９を参照して、本実施形態に対応するパケット変換部７０４の動作を説明する。図１９は、第２の実施形態に対応するパケット変換部の動作を示すフローチャートであり、第１の実施形態における図１５を更に詳細に説明するものである。なお、図１９に示すＡおよびＢは、第１の実施形態と同様に図１６に接続するものとする。また、説明の重複を避けるため、本実施形態において特徴的なステップのみ説明を記載する。

【００８７】

Ｓ１９０３で認証サーバのアドレス情報を取得した後に、ステップＳ１９０４において、パケット変換部７０４は、認証サーバに対応する公開鍵が取得済みであるか否かを公開鍵格納部７１４に確認する。取得済みである場合、ステップＳ１９０５において、パケット変換部７０４は、公開鍵を用いて署名の検証を行う。次に、ステップＳ１９０６において、Ｓ１９０５での検証が成功した場合、Ｓ１９１０において、パケット変換部７０４は、制限情報を取得する。一方、検証が成功しなかった場合、パケット変換部７０４は、処理をＳ１９０７に遷移させる。

【００８８】

Ｓ１９０４で取得済みでないと判断した場合およびＳ１９０５の検証が失敗した場合、ステップＳ１９０７において、パケット変換部７０４は、公開鍵の取得を公開鍵取得部７１３に依頼して、新たに認証サーバから公開鍵を再度取得する。このように、本実施形態によれば、取得済みである公開鍵での署名の検証が失敗した場合、パケット変換部７０４は、上述した何れかの理由で公開鍵が無効であると判断し、再度、公開鍵を取得する。例えば、認証サーバ識別子には変更が無いが、その認証サーバに保持される秘密鍵及び公開鍵が変更され、該変更された公開鍵を印刷装置１０３が未だ図２０のように保持していない場合に、Ｓ１９０６でＮｏと判断する。Ｓ１９０７の処理により、再度公開鍵を取得する仕組みがあるので、印刷装置に大きな復号化情報保持のリソースを設ける必要がなくなる。また、大きなリソースを確保しなくとも、ユーザの運用により自由に秘密鍵や公開鍵を更新でき、セキュリティの高い印刷システムを構築することができる。

【００８９】

新たに公開鍵を取得すると、ステップＳ１９０８において、パケット変換部７０４は、取得した公開鍵を利用し、署名１２０２の検証を実施する。その後、ステップＳ１９０９において、Ｓ１９０６と同様に検証が成功したか否かを判定する。

【００９０】

以上のように、本実施形態によれば、取得済みである公開鍵で署名の検証が失敗した場合、再度、公開鍵を認証サーバから取得して署名の検証を実施する。これにより、本実施形態における印刷システムは、既知の認証サーバにおいて公開鍵が変更された場合であっても、再度、公開鍵を取得することによって対応しうる。

【００９１】

［第３の実施形態］
次に、第３の実施形態について説明する。第１および第２の実施形態において、公開鍵格納部７１４は、印刷装置１０３内部に配置される。しかしながら、印刷装置１０３は、コストの都合上、ハードディスクドライブなどの高価な記憶装置が搭載できない場合がある。本実施形態は、このような場合であっても本発明の印刷システムを導入しうることを特徴とする。
【００９２】
本実施形態における公開鍵格納部７１４は、フラッシュ・メモリやＳＲＡＭ（スタティック・ランダム・アクセス・メモリ）のような容量の比較的少ない不揮発メモリによって構成されうる。また、本実施形態における不揮発メモリ上には、例えば、最大８宛先の認証サーバの公開鍵を記憶しておく容量が必要とされる。さらに、本実施形態において、８宛先以上の認証サーバが使用される場合、９宛先目以降は、過去に記憶されている宛先のうち、最も使用履歴（アクセス履歴）の古いものから開放し、新しい認証サーバの宛先を記憶することが望ましい。これにより、本実施形態における公開鍵格納部７１４は、８宛先以上の認証サーバを扱うことが可能となる。
【００９３】
まず、図２０を参照して、公開鍵格納部７１４における公開鍵の格納処理について説明する。図２０は、第３の実施形態に対応する公開鍵格納部に記憶（保持）されるデータ構造の一例を示す図である。なお、ここでは、容易に説明を記載するため、公開鍵格納部７１４の最大宛先数を３とした場合について説明する。
【００９４】
公開鍵格納部７１４は、認証サーバのアドレス情報２００１、参照カウンタ２００２および公開鍵２００３の情報を有する。参照カウンタ２００２は、格納されている公開鍵がどのような順で使用されたかの公開鍵の使用履歴（公開鍵へのアクセス履歴）を示す値である。例えば、最大格納数が８宛先である場合、例えば、最も新しく参照されたまたは格納された公開鍵を８とし、最も古く参照されたまたは格納された公開鍵を１とする。図２０に示すように、公開鍵格納部７１４には、３つ公開鍵２００４、２００５、２００６が格納されている。このような場合に、印刷装置１０３が新たに公開鍵を取得し、格納する場合について、図２１を参照して以下に説明する。
【００９５】
図２１は、第３の実施形態に対応する公開鍵格納部の動作を示すフローチャートである。第１および第２の実施形態においては、単純に認証サーバに対応する公開鍵を保持するだけであったが、本実施形態では、より複雑なスケジュールを使用するためにフローチャートを用いて説明する。公開鍵格納部７１４は印刷装置の起動とともに動作を開始し、以降印刷装置の電源遮断まで処理を継続する。
【００９６】
ステップＳ２１０１において、公開鍵格納部７１４は、変数Ｎを初期化する。初期化値は、図２０の表の各エントリの履歴を管理するための変数である。なお、初期化値は、公開格納部７１４に１つも公開鍵が保持されていない場合に１となる。さらに、最大格納数が３で、現状、既に２つ格納されている場合、初期値は３となる。また、既に３つ格納されている場合、初期値は最大の参照カウンタ２００２の値に１を加算した値となる。
【００９７】
ステップＳ２１０２において、公開鍵格納部７１４は、パケット変換部７０４から公開鍵の取得依頼が来ているか否かを確認する。取得依頼が来ていない場合は、再度、Ｓ２１０２に戻り、公開鍵取得の依頼を待つ。
【００９８】
公開鍵の取得依頼が来ると、ステップＳ２１０３において、公開鍵格納部７１４は、認証サーバの公開鍵を保持しているかの確認を実施する。保持している場合は、ステップＳ２１０８において、公開鍵格納部７１４は、当該エントリの参照カウンタにＮの値を格納する。さらに、ステップＳ２１０９において、公開鍵格納部７１４は、公開鍵をパケット

変換部に渡す。そして、ステップＳ２１１０において、公開鍵格納部７１４は、変数Ｎに１を加算する。

【００９９】

Ｓ２１０３で公開鍵を保持していない場合、ステップＳ２１０４において、公開鍵格納部７１４は、復号化情報としての公開鍵を格納する空領域があるか否かを判定する。図２０に示すようなケースでは、エントリできる空領域がないため、ステップＳ２１０５において、公開鍵格納部７１４は、参照カウンタが一番小さいエントリの公開鍵を削除する。即ち、アクセス履歴としての参照カウンタ値を元に使用頻度の低い認証サーバを検索し、該検索された認証サーバのに係る情報を削除する。この場合には、公開鍵２００６に係る情報を削除する。ここで削除する情報には認証サーバアドレス（認証サーバ識別子）、参照カウンタ、公開鍵（復号化情報）が含まれる。公開鍵２００６の参照カウンタは、もっとも最近参照されていないことを示す。エントリの空領域ができると、ステップＳ２１０６において、公開鍵格納部７１４は、認証サーバに公開鍵の取得を依頼して取得する。公開鍵を取得すると、ステップＳ２１０７において、公開鍵格納部７１４は、空領域のエントリに認証サーバのアドレスと公開鍵を格納する。さらに、Ｓ２１０８に遷移されて、当該エントリの参照カウンタにＮの値を格納する。その後は、上述したＳ２１０９、Ｓ２１１０の処理が実行される。

【０１００】

本実施形態による公開鍵格納部は、メモリのキャッシュ方式に類似したスケジューリングを行う。これにより、公開鍵格納部７１４では、頻繁にアクセスする認証サーバの公開鍵は保持するが、あまり頻度の高くない認証サーバの公開鍵は破棄されることとなる。なお、本印刷システムは、破棄された公開鍵に関して、再度、必要な時に取得するため、容量が少なくてもサービスは継続でき、かつ公開鍵取得による速度低下も抑えることが可能となる。

【０１０１】

［第４の実施形態］

次に、第４の実施形態について説明する。第１、第２および第３の実施形態においては、ホストコンピュータ１０１からの印刷に関してアクセス制限情報の要求を行う系について説明を行った。本実施形態においては、アクセス制限情報を利用して、印刷装置１０３そのものから実行するローカルジョブ、例えば、コピージョブについて出力を制限することを特徴とする。以下では、第４の実施形態における印刷装置を印刷装置２２００と呼ぶ。

【０１０２】

まず、図２２を参照して、本実施形態における印刷装置２２００（印刷システム）の制御を機能ブロックごとに説明する。図２２は、第４の実施形態における印刷装置の構成の一例を示すブロック図である。

【０１０３】

印刷装置２２００は、インタフェース部２２０１、制限チケット取得部２２０２、公開鍵取得部２０３、公開鍵格納部２２０５およびＧＵＩ部を含んで構成される。さらに、印刷装置２２００は、ジョブ制御部２２０６、スキャナ部２２０７、イメージ格納部２２０８部およびプリンタエンジン２２０９を含んで構成される。

【０１０４】

インタフェース部２２０１は、ネットワーク１０７と接続し、認証サーバから公開鍵を取得する。公開鍵格納部２２０５は、１台以上の認証サーバから取得した公開鍵を格納する。公開鍵取得部２２０３は、インターフェイス部２２０１を介して認証サーバから固有の公開鍵を取得する。

【０１０５】

制限チケット取得部２２０２は、認証サーバからアクセス制限チケットを取得し、その制限情報に基づき、署名の検証の実施する。ＧＵＩ（グラフィック・ユーザ・インターフェイス）部２２０４は、ユーザの指示を機器の内部に伝える。ジョブ制御部２２０６は、

ＧＵＩ部２２０４からの指示に従い、コピー処理などのジョブ制御を実施する。スキャナ部２２０７は、光学読み取り方式を利用して、物理メディアから原稿の内容を読み出してイメージデータを生成する。イメージ格納部２２０８は、スキャナ部２２０７が生成したイメージデータを印刷が完了するまで一時的に格納する。プリンタエンジン２２０９は、イメージ格納部２２０８に格納されたイメージデータを、電子写真技術やインクジェット技術などの既知の印刷技術を用いて印刷用紙などのメディアに実際に印刷する。

【０１０６】

次に、図２３を参照して、印刷システムにおける印刷時の処理概要を説明する。図２３は、第４の実施形態におけるシステム全体を説明するシーケンス図である。２３０１は利用者、２３０３はアドレス解決サーバ、２３０４は認証サーバ、２２００は印刷装置を示す。なお、図４と重複する説明については、省略される。

【０１０７】

ステップＳ２３２１において、利用者２３０１は、印刷装置２２００に、自分の権限でのコピージョブの発行依頼を行う。ステップＳ２３２２において、印刷装置２２００は、印刷を行うためにアドレス解決サーバ２３０３に対して、認証サーバのアドレス解決依頼を依頼する。次に、ステップＳ２３２３において、アドレス解決サーバ２３０３は、周期的、あるいはランダムに複数の認証サーバから任意の認証サーバを選択する。その後、ステップＳ２３２４において、そのアドレスを印刷装置２２００に返却する。

【０１０８】

続いて、ステップＳ２３２５において、印刷装置２２００は、認証サーバ２３０４に対してアクセス制限チケットの発行を要求する。ここでも、利用者４００のユーザ名およびパスワード等のユーザ認証情報を認証サーバ１０２に送信して、アクセス制限情報の問い合わせを行っている。このユーザ認証情報の問合せタイミングはジョブ要求時でも良いし、ユーザが印刷装置１０３の操作部からログイン操作を行ったタイミングでも良い。ステップＳ２３２６において、認証サーバ２３０４は、認証情報を用いて認証を実施する。認証が成功した場合、ステップＳ２３２７において、認証サーバ２３０４は、アクセス制限チケットの生成を実施する。このとき、認証サーバ２３０４は、自分のアドレスを図１２の認証サーバアドレス情報１２０２に記載し、さらに認証サーバ自身が保持する公開鍵ペアの秘密（私有）鍵でデジタル署名を行った結果を署名１２０３に添付する。ステップＳ２３２８において、認証サーバ２３０４は、印刷装置２２００にアクセス制限チケットを返却する。その後、印刷装置２２００は、上述の図４と同様にステップＳ４１０からＳ４１４の処理をステップＳ２３３０からＳ２３３４において実行する。

【０１０９】

次に、図２４を参照して、チケット取得部の動作を説明する。図２４は、第４の実施形態におけるチケット取得部の動作を示すフローチャートである。チケット取得部２２０２は、印刷装置２２００の動作開始とともに動作を開始し、以降、印刷装置２２００の電源遮断まで動作を継続する。

【０１１０】

ステップＳ２４０１において、チケット取得部２２０２は、認証サーバに対して、印刷装置２２００を操作しているユーザの権限でアクセス制限チケットを取得する。次に、ステップＳ２４０２において、チケット取得部２２０２は、アクセス制限チケットに含まれた認証サーバアドレス情報１２０２を取得する。認証サーバアドレス情報１２０２には、アクセス制限チケットを発行した認証サーバのアドレスが格納されている。

【０１１１】

続いて、ステップＳ２４０３において、チケット取得部２２０２は、当該認証サーバに対応する公開鍵が取得済みか否かを公開鍵格納部２２０５に確認する。取得済みでない場合、ステップＳ２４０４において、アクセス制限チケットに含まれる認証サーバアドレス情報に基づき公開鍵の取得を公開鍵取得部２２０３に依頼して取得する。のお、公開鍵の取得方法については、上述のステップＳ４１１、Ｓ１５０４と同様なので、詳しい説明は省略する。また、復号化情報としての公開鍵の再取得方法として、上述の実施形態で説明

した、図１９のＳ１９０４乃至Ｓ１９０９と同様の処理を印刷装置１０３に組み込んでも良い。さらに、図２１で説明した保持公開鍵の更新処理についても、同様に印刷装置１０３に適用しても良い。

【０１１２】

その後、ステップＳ２４０５において、チケット取得部２２０２は、取得した復号鍵としての公開鍵を利用し、デジタル署名１２０２の検証を実施する。Ｓ２４０５において検証結果が一致した場合、ステップＳ２４０７において、チケット取得部２２０２は、制限情報１２０１を取得し、かつ、記憶してＳ２４０１に処理を遷移させる。検証が失敗した場合には、Ｓ２４０８において、チケット取得部２２０２は、アクセス制限チケットを破棄して処理をＳ２４０１に遷移させる。結果的に、検証が失敗した場合には、制限情報の取得は不可能となる。また、検証が成功した場合、記憶された制限情報は、ＧＵＩ部２２０４において利用される。

【０１１３】

次に図２５を参照して、ＧＵＩ部２２０４の概要について説明する。図２５は、第４の実施形態に対応するＧＵＩ部の概観を示す図である。ＧＵＩ画面２５００は、不図示の操作パネルに表示される。また、ＧＵＩ画面２５００は、コピー動作を実施する際のカラー選択を示すプルダウン・メニュー２５０１および両面印刷を選択するボタン２５０２を含む。

【０１１４】

これらの操作ボタンは、画面表示以前に取得した制限情報があれば、該制限情報を利用して操作に制約を設けるようにしてもよい。例えば、図１１に示すような制限情報が設定されている場合、当該ユーザは、「ＳＴＲＩＣＴ＿ＭＯＮＯＣＯＬＯＲ＝ＴＲＵＥ」の記載により、モノクロ印刷のみ許可されているため、プルダウン・メニュー２５０１ではカラー印刷を選択することができない。この場合、プルダウン・メニュー２５０１からカラー印刷の選択項目が消去またはグレイ・アウトされ、明示的に選択できないようにしてもよい。また、カラー印刷を選択できるようにした場合であっても、印刷を実行すると「カラー印刷は許可されない」というダイアログが表示され、印刷処理が中止されるようにしてもよい。

【０１１５】

また、「ＳＴＲＩＣＴ＿ＤＵＰＬＥＸ＝ＴＲＵＥ」の記載により、片面の印刷が不可能となり、ボタン２５０２において片面印刷を指定することができなくなる。この場合、ボタンの選択項目から片面印刷の選択項目が消去あるいはグレイ・アウトされ、明示的に選択できないようにしてもよい。また、片面印刷を選択できるようにした場合であっても、印刷を実行すると「片面印刷は許可されない」というダイアログが表示され、印刷処理が中止されるようにしてもよい。

【０１１６】

そして、これら図２５に示されるＧＵＩは、ユーザ毎に異なり得る。つまり、Ｓ２３２５で、ユーザ認証情報の問合せについて説明を行ったが、ログインユーザ等が異なれば、それに応じて、Ｓ２３２８で認証サーバ２３０４から応答されるアクセス制限チケットの内容が異なり、図２５のＧＵＩも異なる表示に表示制御される。

【０１１７】

上述したように、本発明によれば、大量のホストコンピュータまたはデバイスを保持するオフィスにおいて、複数の認証サーバを用いて個々のサーバがアクセス制限チケットを発行することによって、同時に複数の印刷要求に対応しうる。

【０１１８】

また、複数の認証サーバによって発行されたアクセス制限チケットの署名を検証する際に、複数ある認証サーバのどの公開鍵を使って署名検証を行ってよいか印刷装置が識別できる。例えば、複数の認証サーバで一つの公開鍵を利用する方法もあるが、この場合、複数の認証サーバ間で公開鍵ペア（公開鍵および秘密鍵）の共有を行わなくてはならないという問題がある。例えば、公開鍵ペアをＰＫＣＳ＃１２（Ｐｕｂｌｉｃ Ｋｅｙ Ｃｒｙｐ

ｔｏｇｒａｐｈｙ Ｓｔａｎｄａｒｄ Ｎｏ．１２）形式でエキスポートし、管理者がフロッピー（登録商標）ディスクなどで受け渡し先に送る方法もある。しかし、上記方法は、手作業が発生するために、管理者の手間がかかる。また、一般的に、公開鍵ペアの秘密鍵がなんらかの形で認証サーバの外部にでることは望ましくなく、秘密鍵が完全に守られない可能性がある。さらに、機器が故障したり、入れ替えの際に第３者に解体され、公開鍵ペアが漏えいすると、システム全体に影響するといった問題もある。上記の問題から言って、複数の認証サーバが保持する公開鍵ペアは個々に異なることが望ましい。本実施形態では、この問題を解決できる。

【０１１９】

本印刷システムは、認証サーバシステムを分散でき、また、その分散に対応して、認証処理をスムース且つ安定化させて行える、結果、使い勝手の良い、印刷システムを構築することができる。また、制限情報により、認証サーバが発行する制限情報により印刷ジョブの出力枚数を制限することができるため、使用者の印刷枚数を制限可能となり、無秩序な印刷を抑え、ＴＣＯ削減に寄与する。

【０１２０】

また、本印刷システムは、制限情報を保持しない印刷ジョブの出力を抑制することができ、制限ポリシーに反した印刷の実施を抑制することが可能となる。

【０１２１】

また、本印刷システムは、認証サーバが発行する制限情報により印刷ジョブの両面指定、ページレイアウト指定、モノクロ指定を強制することが可能となり、無秩序な印刷を抑え、ＴＣＯ削減に寄与しうる。

【０１２２】

また、本印刷システムは、複数の異なる認証サーバが個々に異なる公開鍵ペアを保持している場合でも、印刷装置が個々の認証サーバのアドレス情報に紐づけられた公開鍵を保持し、必要に応じて認証サーバへ公開鍵の取得を実施する。そのため、本印刷システムは、複数の認証サーバを利用者に意識させることなく拡張することが可能となり、多量の印刷サービス要求に対して負荷分散を実施することが可能となる。

【０１２３】

さらに、本印刷システムは、印刷装置が必要に応じて自動的に認証サーバの公開鍵を取得するために、管理者は認証サーバの設置だけ行えばよく、公開鍵ペアの転送の手間を省くことが可能である。また、秘密鍵（私有鍵）が認証サーバから漏れ出さないために、管理者も含めた悪意による攻撃を防ぎ、高度なセキュリティを保持しうる。

【０１２４】

［他の実施形態］

以下では、他の実施形態について説明する。上記の実施形態では、アクセス制限チケットに、機能毎の使用許可／不許可を設定した機能制限情報が含まれていた。印刷装置１０３では、この機能制限情報に基づいて、依頼されたジョブを実行するか否かを判定していた。これに対し、ジョブを実行するか否かの判定を認証サーバ１０２側で行うこともできる。その場合、アクセス制限チケットの内容は、ユーザに指定された印刷要求の内容に対して、印刷装置１０３における印刷を許可するか否かを示す情報のみとなる。ここでの印刷要求の内容とは、カラー印刷であるか否かや、ステイプル処理を行うか否かや、ある枚数の印刷を行うか否か等を指す。

【０１２５】

また、この場合、認証サーバ１０２は、アクセス制限チケット要求を受け付ける際にホストコンピュータ１０１や、印刷装置１０３から、利用者４００が実行しようとするジョブの情報を取得する。ここでのジョブの情報には、印刷部数、カラー／モノクロ、Ｎｉｎ１等、印刷装置１０３で実行可能な機能に関する情報が含まれる。認証サーバ１０２は、該ジョブの情報に基づいて、図５に示すようなアクセス制限情報に基づき、ジョブを実行しようとするユーザーが該ジョブを実行可能か否かを判定する。もし、実行しようとしているジョブに制限事項が含まれている場合には、ジョブの実行を禁止するアクセス制限チ

ケットを発行する。一方、制限事項が含まれない場合には、ジョブの実行を許可するアクセス制限チケットを発行する。このときのアクセス制限チケットの例は、図２６に示すようになる。ここでは、ジョブの実行許可を示す「Ｓｔａｔｕｓ＝ＯＫ」との内容が含まれる。

【０１２６】

このようなアクセス制限チケットを用いることで、印刷装置１０３側では、署名検証に成功すれば、ジョブの実行拒否の内容を見るだけで、依頼されたジョブを実行するか否かを判定することができる。

【０１２７】

次に、図２７、図２８を参照して、認証サーバが発行するアクセス制限情報に自身の識別子を含まない例について説明する。図２７は、他の実施形態に対応するアクセス制限チケットのジョブパケットを示す図である。

【０１２８】

図１２の制限情報１００１を示すジョブパケットと比較すると、図２７に示すように、制限情報２７００を示すジョブパケットは、認証サーバアドレス情報１２０２を含まない。この認証サーバアドレス情報１２０２には、上述したように、各認証サーバにおける自身の識別子を有する情報が含まれる。このような情報を含まない場合は、クライアント側（ホストコンピュータ１０１）で印刷ジョブに対して、制限情報２７００とは別のジョブパケットに認証サーバを示す識別子を付与する必要がある。したがって、クライアント側では、予め複数の認証サーバにおける識別子を保持していることが前提となる。

【０１２９】

図２８は、他の実施形態に対応する印刷ジョブの構成を示した図である。図２８に示すように、クライアント側から依頼される印刷ジョブ２８００は、制限情報２７００、認証サーバ情報２８０１、ジョブ開始９０１、属性設定９０２、９０３、印刷データ９０４、９０５およびジョブ終了９０６を示すジョブパケットを有する。認証サーバ情報２８０１を示すジョブパケットは、クライアント側が予め保持している情報から対象となる認証サーバの識別子を付与してある。

【０１３０】

このように、本発明によれば、認証サーバはアクセス制限チケットの発行要求に対して、必ずしも自身を識別する識別子を付与する形式に限定されない。しかしながら、その場合は、クライアント側などで認証サーバを示す識別子を保持しておく必要がある。

【０１３１】

以上、様々な実施形態を詳述したが、本発明は、複数の機器から構成されるシステムに適用してもよいし、また、一つの機器からなる装置に適用してもよい。例えば、プリンタ、ファクシミリ、ＰＣ、サーバとクライアントとを含むコンピュータシステムなどの如くである。

【０１３２】

本発明は、前述した実施形態の各機能を実現するソフトウェアプログラムを、システム若しくは装置に対して直接または遠隔から供給し、そのシステム等に含まれるコンピュータが該供給されたプログラムコードを読み出して実行することによっても達成される。

【０１３３】

従って、本発明の機能・処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、上記機能・処理を実現するためのコンピュータプログラム自体も本発明の一つである。

【０１３４】

その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。

【０１３５】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハー

ドディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷなどがある。また、記録媒体としては、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などもある。

【０１３６】

また、プログラムは、クライアントコンピュータのブラウザを用いてインターネットのホームページからダウンロードしてもよい。すなわち、該ホームページから本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルをハードディスク等の記録媒体にダウンロードしてもよいのである。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明の構成要件となる場合がある。

【０１３７】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布してもよい。この場合、所定条件をクリアしたユーザにのみ、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報で暗号化されたプログラムを復号して実行し、プログラムをコンピュータにインストールしてもよい。

【０１３８】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現されてもよい。なお、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行ってもよい。もちろん、この場合も、前述した実施形態の機能が実現され得る。

【０１３９】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれてもよい。そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ってもよい。このようにして、前述した実施形態の機能が実現されることもある。

【図面の簡単な説明】

【０１４０】

【図１】第１の実施形態における印刷システムの構成を示すブロック図である。

【図２】本発明における制御部の一例を示すブロック図である。

【図３】本発明における印刷装置のハードウェア構成の一例を示す図である。

【図４】第１の実施形態におけるシステム全体の処理の流れを説明するシーケンス図である。

【図５】第１の実施形態に対応する認証サーバが保持するアクセス制限情報に関連した情報を示す図である。

【図６】第１の実施形態に対応するホストコンピュータが出力する印刷指示に関するダイアログのＧＵＩを示す図である。

【図７】第１の実施形態に対応する印刷装置において、詳細な機能構成の一例を示すブロック図である。

【図８】第１の実施形態に対応するジョブパケットの構造を示す図である。

【図９】従来における印刷ジョブの構成を示した図である。

【図１０】第１の実施形態に対応する印刷ジョブの構成を示した図である。

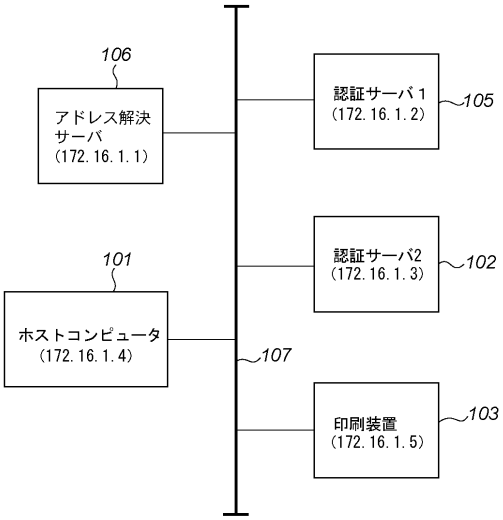
【図１１】第１の実施形態に対応するアクセス制限チケットに含まれる制限情報の書式例を示す図である。

【図１２】第１の実施形態に対応するアクセス制限チケットのジョブパケットを示す図である。

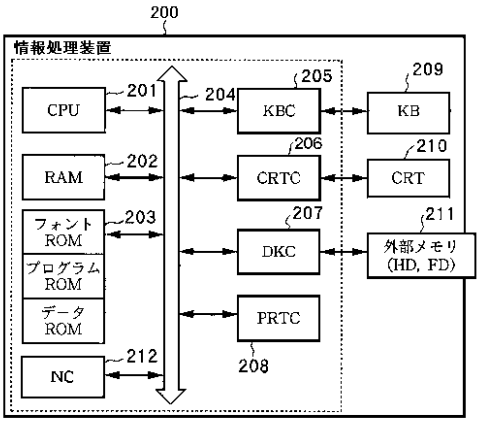
【図１３】第１の実施形態に対応するホストコンピュータが出力する印刷指示に関するダイアログのＧＵＩを示す図である。

【図１４】第１の実施形態に対応する制限チケット判定部の動作を説明するフローチャートである。
【図１５】第１の実施形態に対応するパケット変換部の動作を示すフローチャートである。
【図１６】第１の実施形態に対応するパケット変換部の動作を示すフローチャートである。
【図１７】第１の実施形態に対応する印刷データ解釈部の動作を説明するフローチャートである。
【図１８】第１の実施形態に対応する印刷ジョブ取消部の動作を説明するフローチャートである。
【図１９】第２の実施形態に対応するパケット変換部の動作を示すフローチャートである。
【図２０】第３の実施形態に対応する公開鍵格納部に記憶されるデータ構造の一例を示す図である。
【図２１】第３の実施形態に対応する公開鍵格納部の動作を示すフローチャートである。
【図２２】第４の実施形態における印刷装置の構成の一例を示すブロック図である。
【図２３】第４の実施形態におけるシステム全体の処理の流れを説明するシーケンス図である。
【図２４】第４の実施形態におけるチケット取得部の動作を示すフローチャートである。
【図２５】第４の実施形態に対応するＧＵＩ部の概観を示す図である。
【図２６】他の実施形態に対応する認証サーバが保持するアクセス制限情報に関連した情報を示す図である。
【図２７】他の実施形態に対応するアクセス制限チケットのジョブパケットを示す図である。
【図２８】他の実施形態に対応する印刷ジョブの構成を示した図である。
【符号の説明】
【０１４１】
１０１：ホストコンピュータ
１０２：認証サーバ
１０３：印刷装置
１０６：アドレス解決サーバ
４００：利用者

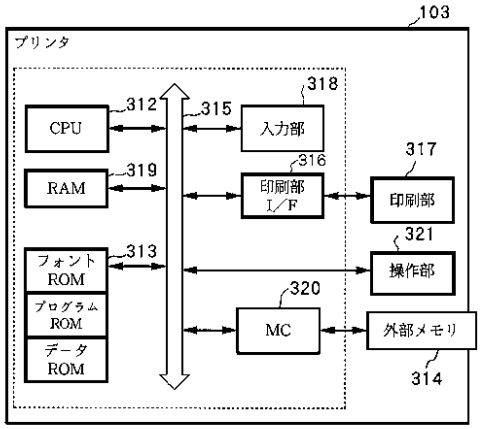
【図１】


106
アドレス解決サーバ
(172.16.1.1)
認証サーバ1
(172.16.1.2)
105
認証サーバ2
(172.16.1.3)
102
101
ホストコンピュータ
(172.16.1.4)
107
印刷装置
(172.16.1.5)
103

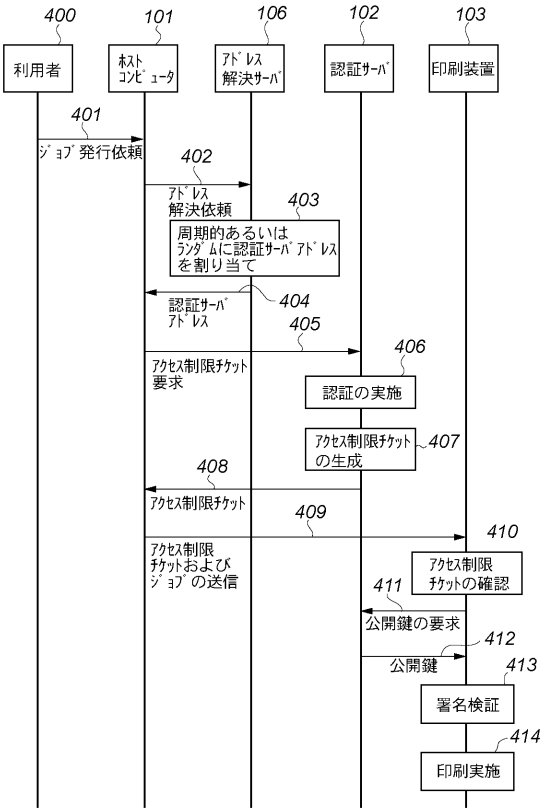
【図２】


200
情報処理装置
CPU
201
RAM
202
フォントROM
203
プログラムROM
データROM
NC
212
204
KBC
205
CRTC
206
DKC
207
PRTC
208
KB
209
CRT
210
外部メモリ
(HD, FD)
211

【図３】


103
プリンタ
CPU
312
RAM
319
フォントROM
313
プログラムROM
データROM
315
入力部
318
印刷部I/F
316
印刷部
317
操作部
321
MC
320
外部メモリ
314

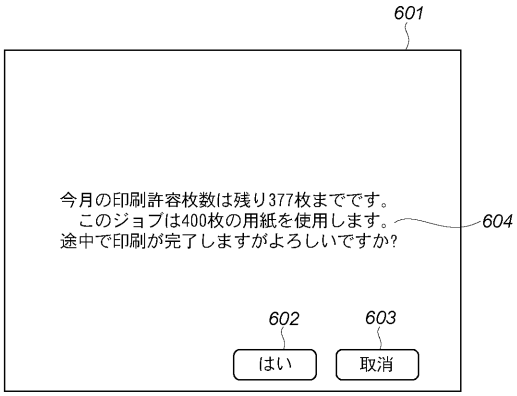
【図４】


400
利用者
101
ホストコンピュータ
106
アドレス解決サーバ
102
認証サーバ
103
印刷装置
401
ジョブ発行依頼
402
アドレス解決依頼
403
周期的あるいはランダムに認証サーバアドレスを割り当て
404
認証サーバアドレス
405
アクセス制限チケット要求
406
認証の実施
407
アクセス制限チケットの生成
408
アクセス制限チケット
409
アクセス制限チケットおよびジョブの送信
410
アクセス制限チケットの確認
411
公開鍵の要求
412
公開鍵
413
署名検証
414
印刷実施

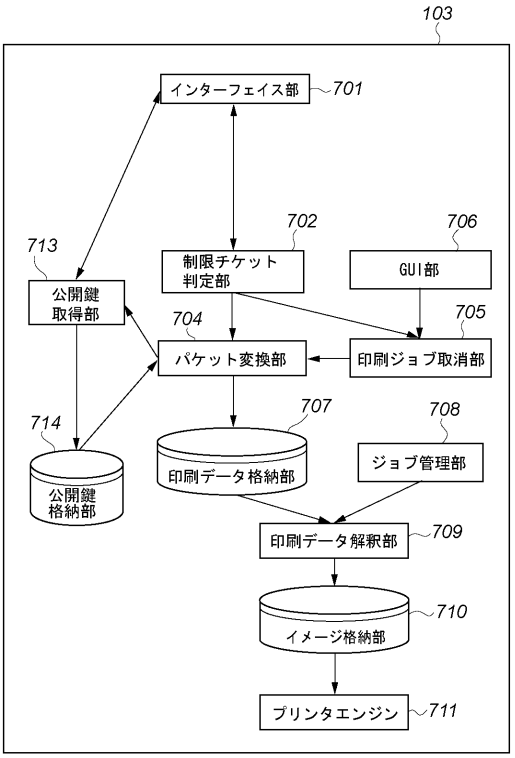
【図５】

501 ユーザ名	502 パスワード	503 枚数最大値	504 枚数実積値	505 印刷制限	
User1	Akd5sj4f	500	123	ﾓﾉｸﾛ、両面	511
User2	saFjf98w	1000	515	ﾓﾉｸﾛのみ	512
User3	vGks9jg1a	2000	1021	なし	513
Guest	なし	0	0	なし	514

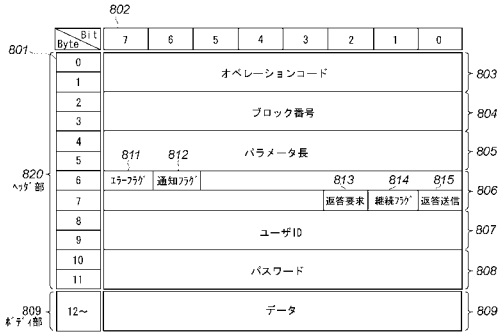
【図６】



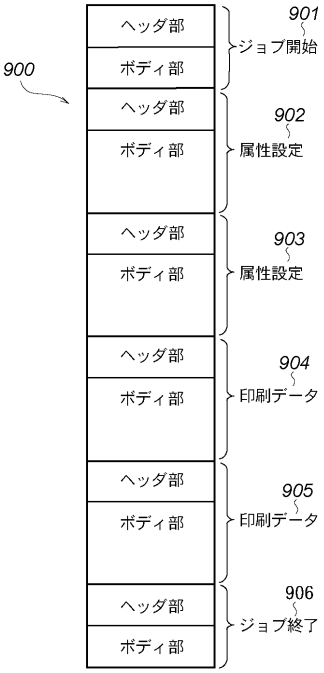
【図７】



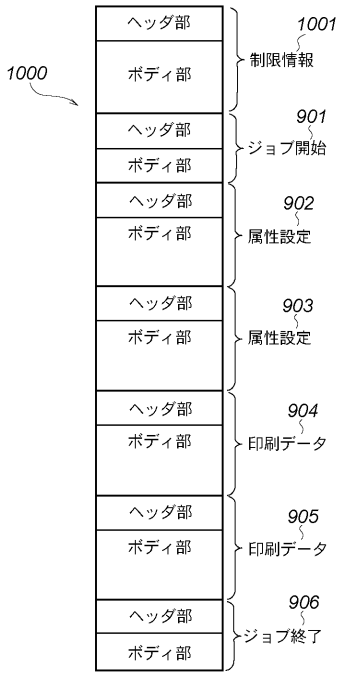
【図８】



【図９】



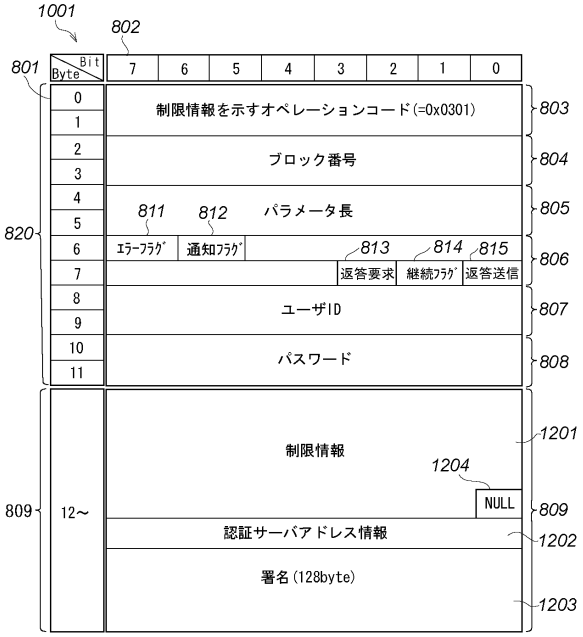
【図１０】



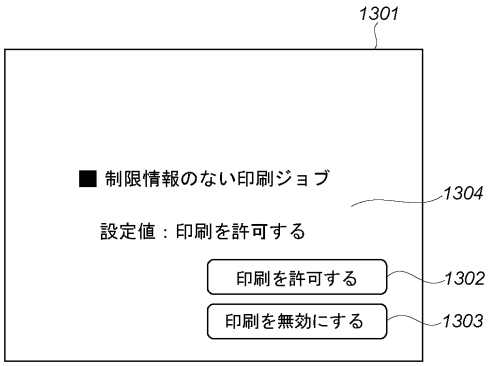
【図１１】

```
MAX_PRINT=100
STRICT_DUPLEX=TRUE
STRICT_Nin1=2
STRICT_MONOCOLOR=TRUE
```

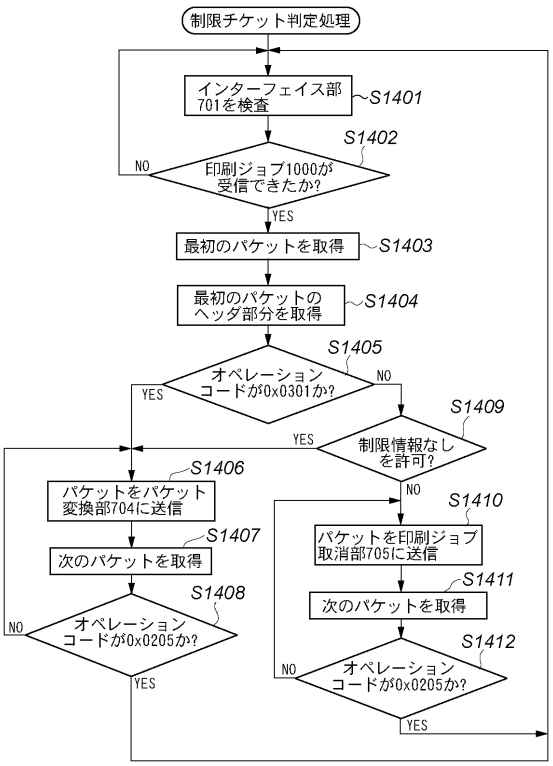
【図１２】



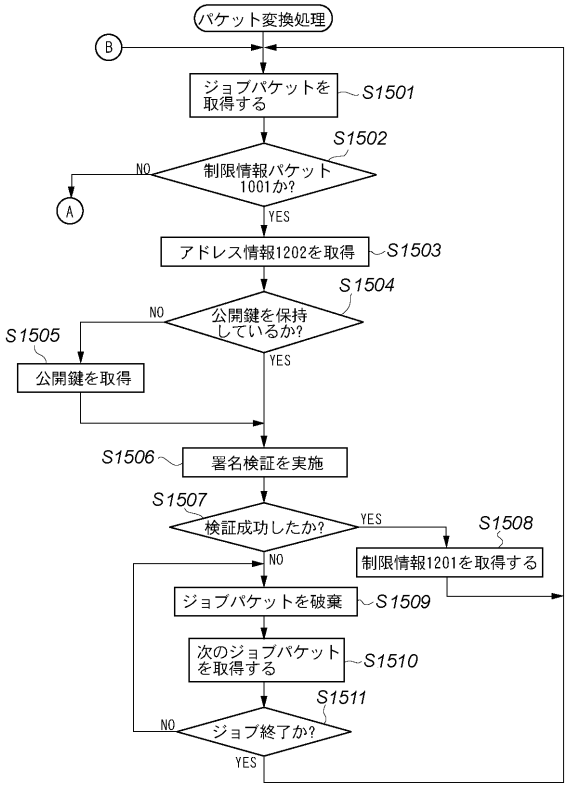
【図１３】



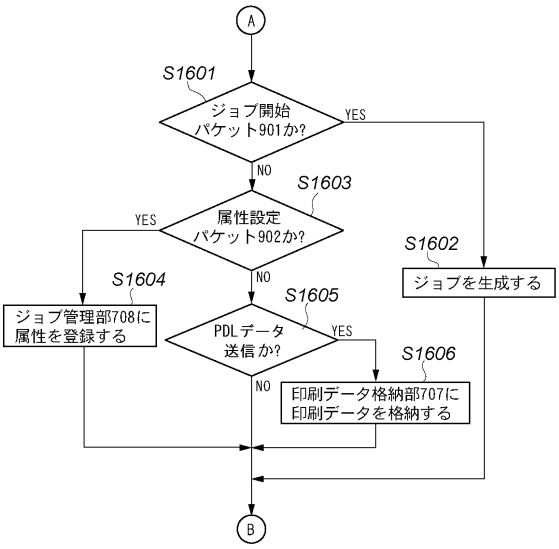
【図１４】



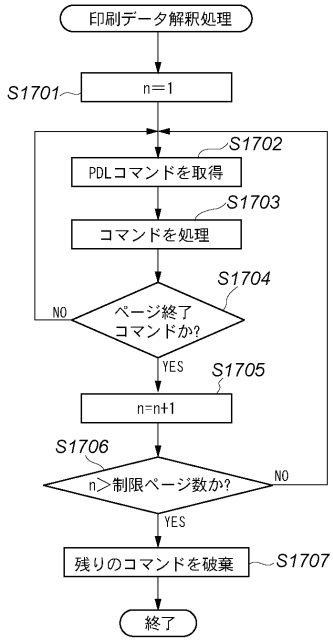
【図１５】



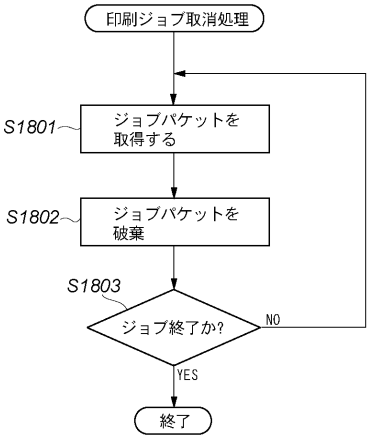
【図１６】



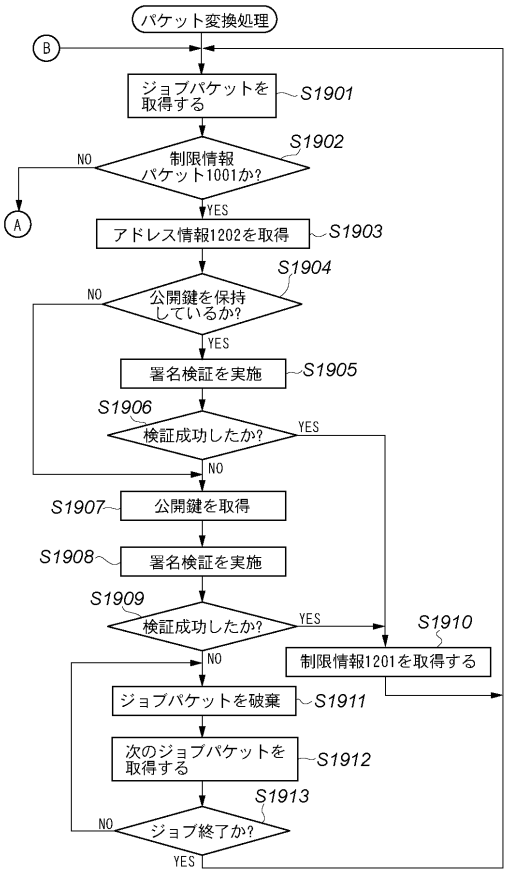
【図１７】



【図１８】



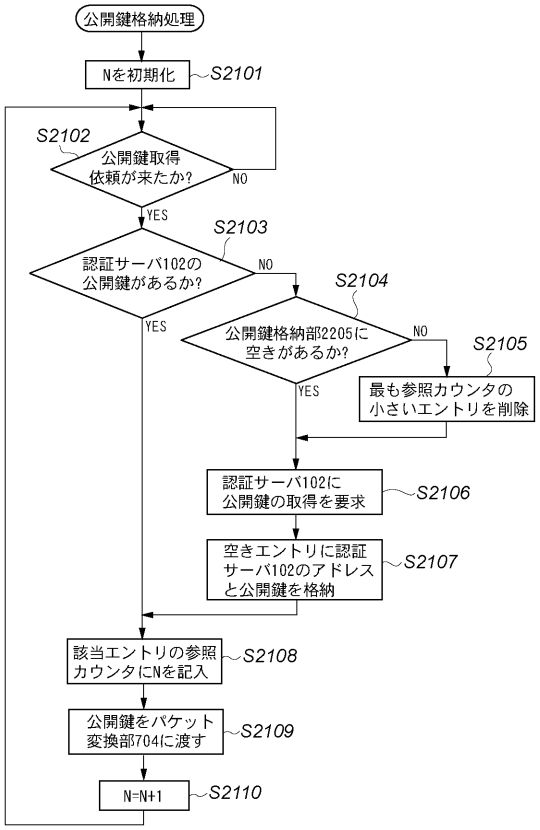
【図１９】



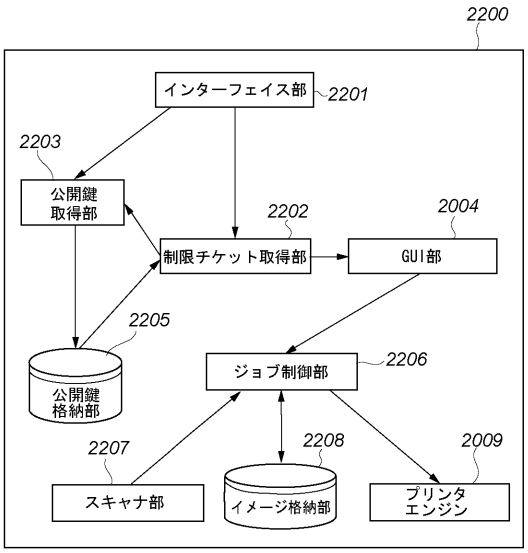
【図２０】

2001 認証サーバアドレス	2002 参照カウンタ	2003 公開鍵	
172.16.1.2	3	認証サーバ1の公開鍵	2004
172.16.1.3	2	認証サーバ2の公開鍵	2005
172.16.1.1	1	認証サーバ3の公開鍵	2006

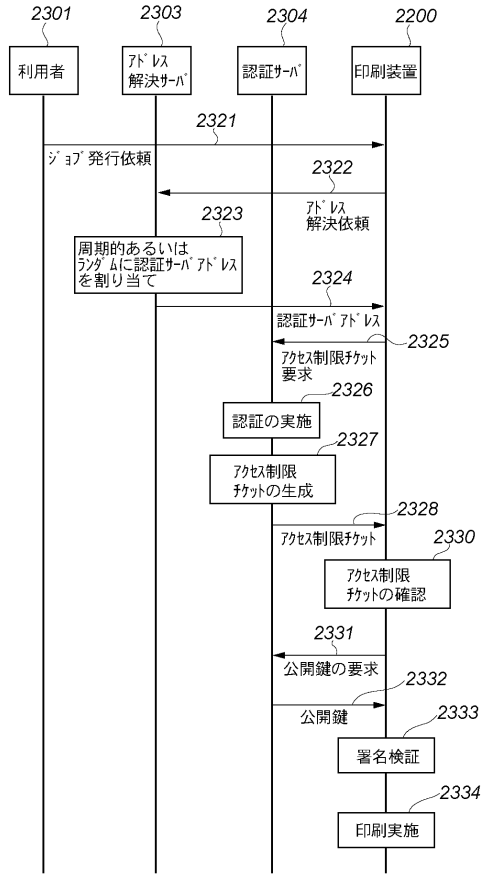
【図２１】



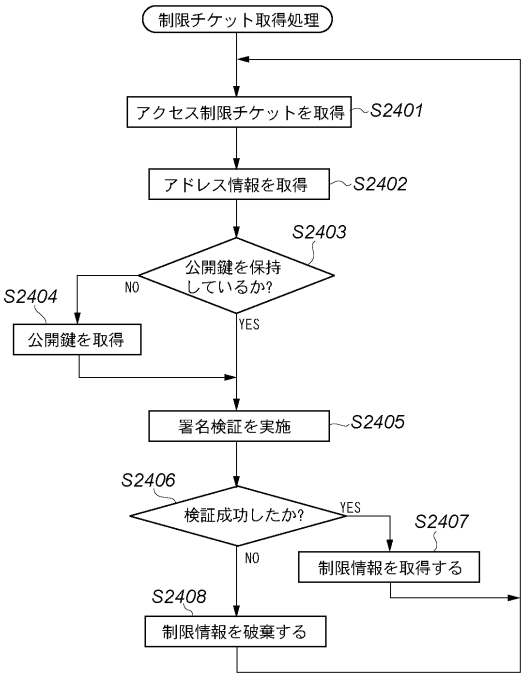
【図２２】



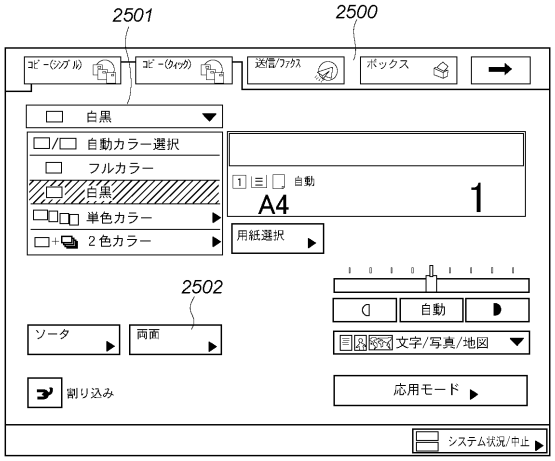
【図２３】



【図２４】

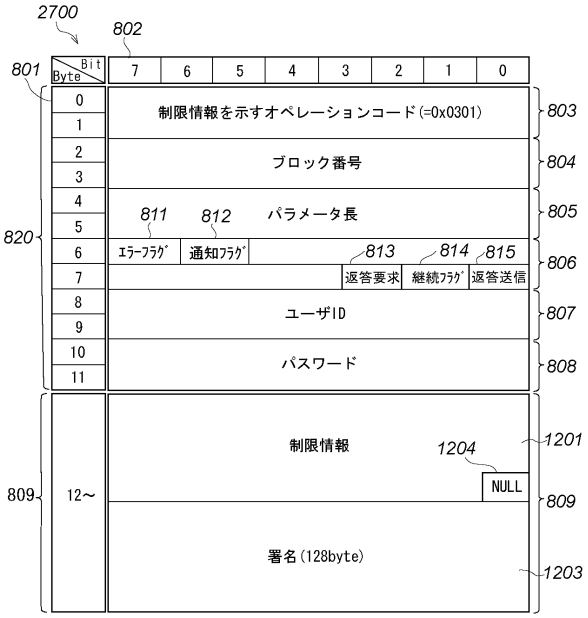


【図２５】

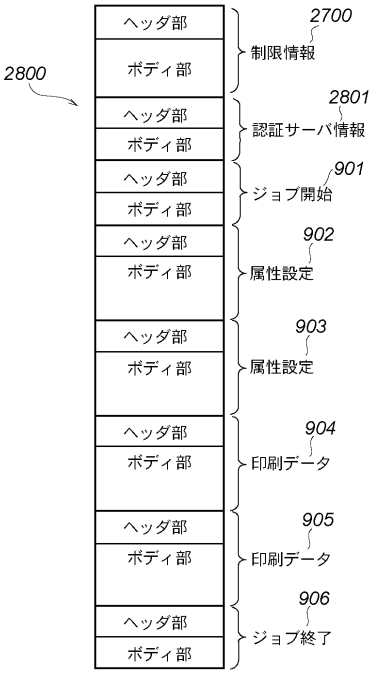


【図２６】

【図２７】



【図２８】


2800
ヘッダ部
ボディ部
2700
制限情報
ヘッダ部
ボディ部
2801
認証サーバ情報
ヘッダ部
ボディ部
901
ジョブ開始
ヘッダ部
ボディ部
902
属性設定
ヘッダ部
ボディ部
903
属性設定
ヘッダ部
ボディ部
904
印刷データ
ヘッダ部
ボディ部
905
印刷データ
ヘッダ部
ボディ部
906
ジョブ終了

フロントページの続き

審査官　大浜　登世子

(56)参考文献　特開２００５－３０１４２４（ＪＰ，Ａ）
特開２００２－２１５３４６（ＪＰ，Ａ）
特開２００５－１３５３７３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｂ４１Ｊ　２９／３８
Ｂ４１Ｊ　２９／００
Ｇ０６Ｆ　３／１２