(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4614392号
(P4614392)
(45)発行日　平成23年1月19日(2011.1.19)　(24)登録日　平成22年10月29日(2010.10.29)

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

請求項の数 8　(全 17 頁)

(21)出願番号　特願2005-231167(P2005-231167)
(22)出願日　平成17年8月9日(2005.8.9)
(65)公開番号　特開2007-48002(P2007-48002A)
(43)公開日　平成19年2月22日(2007.2.22)
審査請求日　平成20年8月8日(2008.8.8)

(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　山村　進一
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】情報処理装置及びその制御方法、並びにコンピュータプログラム及びコンピュータ可読記憶媒体

(57)【特許請求の範囲】
【請求項１】
ネットワーク上のサーバに記憶された、印刷対象となる所望のデータファイルを指定し、印刷先の印刷装置を特定するプリンタポートに向けて前記データファイルの前記サーバにおけるパス付きファイル名を記述した印刷制御情報を出力する情報処理装置であって、
前記プリンタポートで示される出力先が、前記サーバが所属するネットワークセグメント内にあるか否かを判断する判断手段と、
該判断手段によって前記出力先が前記ネットワークセグメント内にあると判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、非セキュアプロトコルで行うことを記述した印刷制御情報を生成する第１の印刷制御情報生成手段と、
該判断手段によって前記出力先が前記ネットワークセグメント内にないと判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、セキュアプロトコルで行うことを記述した印刷制御情報を生成する第２の印刷制御情報生成手段と、
前記第１、第２の制御情報生成手段のいずれかで生成された印刷制御情報を、前記プリンタポートに向けて出力する出力手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記判断手段は、

予めサーバが所属するネットワークセグメントのセグメントアドレス範囲を記憶する記憶手段を備え、

プリンタポートで指定されたＩＰアドレスが前記記憶手段に記憶されたセグメントアドレス範囲にある場合に、前記出力先が、サーバが存在するネットワークセグメント内にあると判断し、それ以外には前記情報処理装置が存在するネットワークセグメント外と判断することを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記制御情報はＸＭＬ形式のジョブチケットであって、

前記非セキュアプロトコルはＨＴＴＰ、前記セキュアプロトコルはＨＴＴＰＳとすることを特徴とする請求項１又は２に記載の情報処理装置。

【請求項４】

更に、プリンタポートがＦＩＬＥであるか否かを判断する第２の判断手段を備え、

前記第２の印刷制御情報生成手段は、前記第２の判断手段でプリンタポートとしてＦＩＬＥが指定された場合にもセキュアプロトコルを記述した印刷制御情報を生成することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。

【請求項５】

前記データファイルは画像ファイルであることを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。

【請求項６】

ネットワーク上のサーバに記憶された、印刷対象となる所望のデータファイルを指定し、印刷先の印刷装置を特定するプリンタポートに向けて前記データファイルの前記サーバにおけるパス付きファイル名を記述した印刷制御情報を出力する情報処理装置の制御方法であって、

前記プリンタポートで示される出力先が、前記サーバが所属するネットワークセグメント内にあるか否かを判断する判断工程と、

該判断工程によって前記出力先が前記ネットワークセグメント内にあると判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、非セキュアプロトコルで行うことを記述した印刷制御情報を生成する第１の印刷制御情報生成工程と、

該判断工程によって前記出力先が前記ネットワークセグメント内にないと判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、セキュアプロトコルで行うことを記述した印刷制御情報を生成する第２の印刷制御情報生成工程と、

前記第１、第２の制御情報生成工程のいずれかで生成された印刷制御情報を、前記プリンタポートに向けて出力する出力工程と

を備えることを特徴とする情報処理装置の制御方法。

【請求項７】

コンピュータに読み込ませ実行させることで、ネットワーク上のサーバに記憶された、印刷対象となる所望のデータファイルを指定し、印刷先の印刷装置を特定するプリンタポートに向けて前記データファイルの前記サーバにおけるパス付きファイル名を記述した印刷制御情報を出力する情報処理装置として機能させるコンピュータプログラムであって、

前記プリンタポートで示される出力先が、前記サーバが所属するネットワークセグメント内にあるか否かを判断する判断手段と、

該判断手段によって前記出力先が前記ネットワークセグメント内にあると判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、非セキュアプロトコルで行うことを記述した印刷制御情報を生成する第１の印刷制御情報生成手段と、

該判断手段によって前記出力先が前記ネットワークセグメント内にないと判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、セキュアプロトコルで行うことを記述した印刷制御情報を生成する第２の印刷制

御情報生成手段と、
前記第１、第２の制御情報生成手段のいずれかで生成された印刷制御情報を、前記プリンタポートに向けて出力する出力手段
として機能させることを特徴とするコンピュータプログラム。
【請求項８】
請求項７に記載のコンピュータプログラムを格納したことを特徴とするコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワークを介したセキュア文書の印刷技術に関するものである。
【背景技術】
【０００２】
近年ネットワークを経由して様々なＰＣや入出力装置でセキュアデータが取り扱われ、プリンタでの印刷や配布、個人ＰＣ（パーソナルコンピュータ）への保存やＵＳＢストレージへの保存や持ち出し等、機密情報が外部に流出されうる機会が増えている。そのため情報漏洩を防ぐセキュリティが重要視され、様々な取り組みが行なわれている。
【０００３】
その取り組みとして、例えばセキュアデータ自体を暗号化しアクセス権を有する者のみアクセス出来る仕組みがある。また、ネットワークの伝送データを暗号化して送信者と受信者で解読キーを共有する仕組み、印刷装置自体のアクセスをユーザーＩＤやパスワードで管理し、認証が取れた場合のみ印刷する仕組みなども存在する。
【０００４】
しかしながら、これらのシステムは局所的な処理に対するセキュリティであったり、様々な仕組みを組み合わせてもアクセス権設定者の負荷が増大、あるいは設定漏れによるセキュリティホールが発生したりする。特にアクセス権所有者による情報漏洩を防ぐことは困難であった。
【０００５】
そのため、ネットワークに接続されたＰＣ、入出力装置およびそこで取り扱われるセキュアデータをセキュリティ管理サーバーにて一元管理するセキュアドキュメントシステムという仕組みが注目されている。
【０００６】
セキュアドキュメントシステムの特徴は、暗号化されたセキュアデータとアクセス権管理を行なうセキュリティ管理サーバーを有する。そして、ネットワークに接続されたＰＣや入出力装置が暗号化されたセキュアデータにアクセスするには適時セキュリティ管理サーバーから認証を得るのである。
【０００７】
今後は、ネットワークでセキュリティ管理サーバーと接続されていない会議室ではもちろんのこと、社外への外出時においても、社内のセキュアデータにアクセスして印刷を行う機会は多くなることが予想される。
【０００８】
一方、印刷対象のドキュメントに画像データが含まれている場合、そのドキュメントに画像データを含めるのではなく、画像データの所在位置を示すＵＲＬをジョブチケットと呼ばれる印刷制御コマンドに記載することが行われている（例えば特許文献１）。これを利用して、社外の印刷装置側が、社内のサーバが記憶している画像データをダウンロードすることが可能になり、利便性を増す。
【特許文献１】特開平１０－２７５０６４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００９】

しかしながら、上記のように、上述した従来の技術ではネットワークでセキュリティ管理サーバーと接続されていない会議室や、社外への外出時にセキュアデータにアクセスして印刷を行なうようにすると問題が発生する。なぜなら、これを実現するには、逆に、社内に設置されたＷＷＷサーバにはセキュリティホールを作るかしかないからである。

【００１０】

当然、セキュリティホールは、コンピュータウィルスやハッキングなどに対する防御という観点からは望ましくない。

【００１１】

また、社外向けのＷＷＷサーバを立ち上げて、社外の印刷制御装置からの印刷時のみ、ここから必要な画像データをダウンロードするという方法では、余分な設備を必要とするだけでなく、このＷＷＷサーバの管理、メンテナンスに多大な工数が必要となる。また、社内のサーバから社外の印刷装置へ画像データをダウンロードしようとすると、画像データは外部のインターネットを経由することになるので改ざんが行われる可能性がある。

【００１２】

本発明は上記問題点を解決することを目的としたもので、印刷装置のネットワーク上のロケーションに応じて、ドキュメントのダウンロードプロトコルを記述した印刷指示（ジョブチケット）を発行し、利便性とセキュリティ確保を同時に実現する技術を提供する。

【課題を解決するための手段】

【００１３】

この課題を解決するため、本発明の情報処理装置は以下に示す構成を備える。すなわち、

ネットワーク上のサーバに記憶された、印刷対象となる所望のデータファイルを指定し、印刷先の印刷装置を特定するプリンタポートに向けて前記データファイルの前記サーバにおけるパス付きファイル名を記述した印刷制御情報を出力する情報処理装置であって、

前記プリンタポートで示される出力先が、前記サーバが所属するネットワークセグメント内にあるか否かを判断する判断手段と、

該判断手段によって前記出力先が前記ネットワークセグメント内にあると判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、非セキュアプロトコルで行うことを記述した印刷制御情報を生成する第１の印刷制御情報生成手段と、

該判断手段によって前記出力先が前記ネットワークセグメント内にないと判断した場合、前記パス付きファイル名で特定された前記データファイルの前記サーバからのダウンロードを、セキュアプロトコルで行うことを記述した印刷制御情報を生成する第２の印刷制御情報生成手段と、

前記第１、第２の制御情報生成手段のいずれかで生成された印刷制御情報を、前記プリンタポートに向けて出力する出力手段と

を備えることを特徴とする情報処理装置。

【発明の効果】

【００１４】

本発明によれば、印刷出力先の印刷装置が、サーバが存在するネットワークセグメント内にあるか否かに応じて、非セキュアプロトコル、セキュアプロトコルのいずれかを利用したダウンロードをその印刷装置に行わせる。従って、利便性と高いセキュリティを同時に実現する印刷システムが提供できる。

【発明を実施するための最良の形態】

【００１５】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【００１６】

図１は一般的な印刷処理システムのブロック構成図である。同図は、特にパーソナルコンピュータ等の情報処理装置１００の内部のブロック構成図を示している。

【００１７】

ＣＰＵ１０１はＲＯＭ１０２あるいはＲＡＭ１０３あるいは記憶装置１０５に格納されたプログラムに従って装置全体の制御を行う。ＲＯＭ１０２はＢＩＯＳやブートプログラムを格納するリードオンリメモリである。ＲＡＭ１０３はＣＰＵ１０１のワークエリアとして機能し、且つ、ＣＰＵ１０１が実行するオペレーティングシステム（ＯＳ）、アプリケーションプログラム、実施形態におけるプリンタドライバもここに格納される。

【００１８】

外部記憶装置１０５はハードディスクドライブ等の大容量の記憶装置であって、ここにはオペレーティングシステム（ＯＳ）１０５５やアプリケーションソフト１０５１等を記録する。キーボードやマウスなどの入力機器は、入力Ｉ／Ｆ１０４を通じて、ユーザがコンピュータに対して各種指示を与えるためのデバイスである。出力Ｉ／Ｆ１０６は、データを外部に出力するためのインターフェースであり、モニタやプリンタに対してデータを出力する。１０７は共通データバスで、それぞれのデータのやりとりを行う。また、ネットワークＩ／Ｆ１０８は、情報処理装置１００よりイントラネットやインターネットなどの通信媒介を通して、サーバ１１０や、その他の情報処理装置１２０や、そしてプリンタ１３０などと情報の授受を行うことが出来る。

【００１９】

上記構成において、情報処理装置１００の電源をＯＮにすると、ＣＰＵ１０１はＲＯＭ１０２のブートプログラムを実行し、外部記憶装置１０５からＯＳをＲＡＭ１０３にロードし、情報処理装置として機能するようになる。

【００２０】

図２は、上記のようにしてＯＳ、アプリケーション、プリンタドライバがＲＡＭ１０３にロードされた場合の印刷処理システムのモジュール構成を示している。

【００２１】

ユーザはキーボードやマウスなどといった入力装置１０４を使用して、出力装置１０５のモニタに映し出されたアプリケーションプログラム２０１によるＧＵＩを利用して、作成或いは編集中の文書２０３の印刷処理を実行する。

【００２２】

ユーザによって印刷処理が実行されると、アプリケーション２０１はユーザの印刷操作を理解し、文書の印刷設定２０３１と文書内容の描画データ２０１２を元に、印刷装置に対応したプリンタドライバ２０９を起動する。そして、その後、オペレーティングシステム２０４に印刷処理を通知する。

【００２３】

オペレーティングシステム２０４はグラフィックスエンジン２０５を通じて、スプールファイル２０６への描画や、指定されたプリンタドライバ２０９への描画を行う。これを受けて、プリンタドライバ２０９はプリンタが理解できるデータ言語に変換し、プリントマネージャ２０７が各アプリケーションからの印刷処理のスケジュール管理を行う。プリントマネージャ２０７は、プリンタが印刷できる状態になったときに、Ｉ／Ｏモジュール２０８を介してプリンタ１３０に印刷ジョブデータを送信する。これにより、印刷が実行される。

【００２４】

文書の印刷設定２０３１はプリンタドライバのコンフィギュレーションモジュール２０９１によって初期値が作成される。しかし、この印刷設定をアプリケーションもしくはプリンタドライバのユーザインターフェースを使用してユーザが望む最終印刷結果になるように変更して設定を行うことも可能である。印刷設定には２種類の形態がある。１つはＤＥＶＭＯＤＥと呼ばれるバイナリデータ形式のデータ構造体であり、これは従来の印刷の系で使われていた。もう１つはジョブチケットと呼ばれるタグを用いたマークアップ言語ＸＭＬ形式のテキストデータである。テキストデータであるので可読/編集/追加可能であるという利点があり、従来のＤＥＶＭＯＤＥ形式から徐々にジョブチケット形式に移行していくことが予想される。どちらの印刷設定形式を選択するかは、プリンタドライバやオペレーティングシステムの仕様や、そしてアプリケーションの対応状況によって異なる。

【００２５】
従来良く使われていたＤＥＶＭＯＤＥ構造体は大きく分けて２つの設定領域で構成される。１つはオペレーティングシステムで定義されている共通の基本情報を設定する領域でパブリック領域と呼ばれる。もうひとつは各プリンタに存在するプリンタドライバ２０９が自由に拡張できる領域でプライベート領域と呼ばれる。パブリック領域はその中に含まれる情報が何を示すのかについては、オペレーティングシステムのフォーマットとして一般に広く公開されており、どのアプリケーションからも設定を変更することができる。これはアプリケーションがもつページ設定ダイアログから指定することができる。代表的なものとしては、用紙サイズ、用紙の向きが挙げられる。
【００２６】
一方、プライベート領域（拡張領域）は、更に細かな設定を記述する領域であり、一般的にアプリケーションからは設定、変更は出来ない。その設定を行ったり変更できるのは、プリンタドライバ２０９だけである。そこでプリンタドライバのコンフィギュレーションモジュール２０９１は、このプライベート領域を設定するためのユーザインターフェース（ＧＵＩ）を持ち、その中で拡張領域の印刷設定をすることを可能にしている。
【００２７】
このプライベート領域における設定項目としては、ステイプルを行うか否か、行う場合にはどの位置にするか等が含まれる。
【００２８】
上記のように、文書２０３の一部としてＤＥＶＭＯＤＥ構造体がドライバの存在しない環境に運ばれた場合、その環境ではドキュメントに付加されている印刷設定２０３１のプライベート領域に保存されている情報を知るすべがユーザには存在しなかった。よってDEVMODE構造体で情報を保存した従来の文書は、プリンタドライバ２０９が存在する環境のみ印刷設定の編集や機能追加、またヘルプ情報への参照を行うことが前提となっていた。
【００２９】
図３は印刷装置で選択可能な印刷設定項目の一覧を示す初期設定ジョブチケット、図４は文書に適用する印刷設定を保存した設定ジョブチケットを示している。
【００３０】
ＤＥＶＭＯＤＥ構造体と同様に両ジョブチケットにもパブリックな領域とプライベートな領域がある。しかし、ＸＭＬの形式で記述されたジョブチケットにはＤＥＶＭＯＤＥのように境界線によって各領域が分かれているわけではない。この両者は名前空間と呼ばれる、タグの内部構造における区画に分けられる仕組みによって区別されている。
【００３１】
名前空間は接頭辞としてそれぞれのタグで指定され、接頭辞を持たないタグは名前空間に属さないものとして扱われる。接頭辞はコロン（：）記号の前につけ、ｐｓｆ：Ｆｅａｔｕｒｅのように記述される。
【００３２】
図３のジョブチケットには、５個の名前空間が存在し、それぞれが異なった役割を担っている。ｐｓｆ名前空間はジョブチケットのフレームワークを定義しているプリントスキーマフレームワークである。ジョブチケットとして成り立つ構造を提供するために、ＦｅａｔｕｒｅやＯｐｔｉｏｎ、Ｖａｌｕｅといった基本的なタグを定義している。Ｆｅａｔｕｒｅは印刷機能を表し、Ｏｐｔｉｏｎはその印刷機能の選択肢を、Ｖａｌｕｅは要素の値といった形で定義されている。
【００３３】
ｐｓｋ名前空間はパブリック領域におけるジョブチケットのキーワードを定義している。具体的なキーワードとしては、用紙のサイズを指定するＭｅｄｉａＳｉｚｅなどがある。ｐｓｆ名前空間とｐｓｋ名前空間はオペレーティングシステムによってスキーマという形で一般に公開される形で定義されており、アプリケーションは定義に基づき自由にデータを配置することができる。ｘｓｉ名前空間とｘｓ名前空間はＸＭＬスキーマの規格として一般的に定義されているもので、ｘｓｉ名前空間はＸＭＬスキーマの組み込み属性・イ

ンスタンスを定義している。ｘｓ名前空間はＸＭＬスキーマの既定属性となる。ｎｓ１名前空間はそれぞれ、プリンタドライバが独自に拡張した名前空間となる。この名前空間は、Haftoneなどのプリンタやメーカ依存の機能を記述するために用いられる。

【００３４】

さて、図３の初期設定ジョブチケットには、印刷装置で実施可能な機能の一覧と、その個々の機能で選択可能な選択肢が列挙されている。例えば図３において機能MediaSizeにおいて、Ａ４とＡ５とユーザ定義サイズを示すCustomMediaSizeを選択可能なことを示している。またDefaultというタグは、選択をされていない初期状態の場合に適切と考えられる選択肢を表しており、機能MediaSizeに関してのデフォルトではＡ４である。

【００３５】

図４は図３の初期設定ジョブチケットの各機能の選択肢一覧より、実際に文書に適用する設定を保持する設定ジョブチケットを示す。図３に記述の選択肢一覧より、ユーザが選択した一つの選択肢のみ残して、各機能より削除されている。この例の場合、機能MediaSizeはＡ４が選択されている。

【００３６】

次に、ＨＴＴＰＳ（Hyper Text Transfer Protocol over SSL）について説明する。ＨＴＴＰＳとは、Ｗｅｂサーバとクライアント（Ｗｅｂブラウザなど)がデータを送受信するのに使われるプロトコルであるＨＴＴＰに、ＳＳＬによるデータの暗号化機能を付加したプロトコルである。サーバとブラウザの間の通信を暗号化し、プライバシーに関わる情報やクレジットカード番号などを安全にやり取りすることを目的としている。

【００３７】

ＳＳＬとはSecure Socket Layerの略で、データを暗号化してやり取りする手順の決まり(プロトコル)である。通常、ウェブサーバとブラウザとの間はＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ ＴｒａｎｓｆｅｒＰｒｏｔｏｃｏｌ）というプロトコルで通信が行われている。ＨＴＴＰにはメッセージを暗号化して「盗聴」を防いだり、ウェブサーバを認証して「成りすまし」を防止するという機能がない。そのため、インターネット上で安心して通信を行うためのプロトコルとして、Ｎｅｔｓｃａｐｅ Ｃｏｍｍｎｉｃａｔｉｏｎｓ社が提唱してＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）が開発された。ＳＳＬバージョン ３．０までＮｅｔｓｃａｐｅ Ｃｏｍｍｎｉｃａｔｉｏｎｓ社で仕様が決められ、現在インターネットにアクセスするプロトコルの多くがＳＳＬ ３．０を利用している。その後ＩＥＴＦで標準化作業が行われ、ＲＦＣ２２４６においてＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）１．０として公開されている。

【００３８】

次に、ＳＳＬプロトコルの位置付けを説明する。

図５に示すようにＳＳＬはセッション層に位置するプロトコルとして位置づけられている。そのため下位のレイヤーであるＴＣＰ／ＩＰプロトコルを利用するすべてのアプリケーション層、プレゼンテーション層(ＨＴＴＰ／ＴＥＬＮＥＴ／ＦＴＰ／ＰＯＰなど)からも利用することができる。

図６に示すように、ブラウザ（ホームページ閲覧ソフト）は「通常のＨＴＴＰ」と「ＳＳＬを利用した場合のＨＴＴＰ」をＵＲＬの違い（ｈｔｔｐ：／／～とｈｔｔｐｓ：／／～）によって判別する。

その為、ＵＲＬを「ｈｔｔｐ：／／～」とした場合には、ＳＳＬ機能は利用せずに直接サーバとＴＣＰ／ＩＰ通信を行う。また、ＵＲＬを「ｈｔｔｐｓ：／／～」とした場合、ウェブブラウザは、自身が備えているＳＳＬ機能を介してサーバとＴＣＰ／ＩＰ通信を開始する。デフォルトの設定では、サーバ側ではブラウザから受けたリクエストに対して、「ｈｔｔｐ：／／～」に対してはＴＣＰのポート番号８０番を、「ｈｔｔｐｓ：／／～」に対してはポート番号４４３番を割り当てて区別している。

【００３９】

以上、ジョブチケット、及び、ＨＴＴＰとＨＴＴＰＳとの違いについて説明した。以下、図７以降を参照して、実施形態の説明を行う。

【００４０】
図７は、実施形態における印刷制御システムの構成と、印刷装置の構成ブロック図である。
【００４１】
このシステムは、WWW機能を備えたサーバーコンピュータ７０１と、ジョブチケット（印刷制御情報）を含む印刷ジョブを作成するクライアントコンピュータ７０２と、この各コンピュータとそれぞれ通信する印刷装置７１０で構成される。クライアントコンピュータ７０２は、図１、図２とほぼ同様の構成を有するものである。
【００４２】
印刷装置７１０は、実際に印刷処理を行うプリンタエンジン７１１と、装置全体の制御を行うコントローラ７１２で構成される。プリンタエンジン７１１はＬＢＰエンジンとするが、それ以外の、例えばインクジェットプリンタエンジンでも構わない。
【００４３】
コントローラ７１２は、クライアントコンピュータ７０２からジョブチケットを受信するジョブチケット受信部７１４を有する。ジョブチケットには、サーバーコンピュータ７０１上の画像ファイルのアドレス及び画像ファイルのサイズ、拡大縮小率等の印刷パラメータ等が記述されている。
【００４４】
また、コントローラ７１２は、ジョブチケットで指示された画像ファイルのアドレスに基づきサーバーコンピュータ７０１から印刷すべき画像ファイルを取得する画像ファイル取得部７１５を有する。この画像ファイル取得部７１５は、ジョブチケットと画像ファイルからプリンタエンジン７１１が印刷可能なビットマップデータを生成する処理を行う。そして、生成した印刷データをプリンタエンジンインターフェース（Ｉ／Ｆ）７１７を介してプリンタエンジン７１１に出力する処理を行う。
【００４５】
また、コントローラ７１２は、情報ファイルのキャッシュ機能を有する。すなわち、画像ファイル取得部７１５が取得した画像ファイルを一時記憶する画像ファイルキャッシュ部７１６と、ジョブチケットのアドレスが示す画像ファイルを画像ファイルキャッシュメモリから検索する画像ファイルキャッシュ検索部７１８を備える。これにより、ユーザがクライアントコンピュータ７０２で添付した画像ファイルを高速に印刷処理を行うことが可能な印刷制御システムを実現している。
【００４６】
図８は、印刷装置７１０内のコントローラ７１２のハードウエア構成を示すブロック図である。コントローラ７１２は、ＣＰＵ（中央処理装置）８０１、ＣＰＵ８０１が実行するプログラムを格納しているＲＯＭ８０２、ＣＰＵ８０１のワークエリア、印刷イメージデータを展開するためのＲＡＭ（ランダム・アクセス・メモリ）８０３を備える。また、コントローラ７１２には、ネットワークと通信するための通信インターフェース（Ｉ／Ｆ）８０４、一時的に印刷データを格納するため外部記憶部８０５、メモリカード等の記憶媒体用読取装置８０６、プリンタエンジンＩ／Ｆ８０７を有する。
【００４７】
ＣＰＵ８０１は、ＲＯＭ８０３に格納されたプログラムに従って、通信インターフェース８０４からジョブチケットを受信し、その内容を解析する。そして、そのジョブチケットに記述されたＵＲＬ記述文字列に従って、サーバ７０１より画像ファイル等のデータを受信して外部記憶装置８０５に格納する。また、ＣＰＵ８０１はジョブチケットの記述に従って、外部記憶装置８０５に格納された画像ファイルから印刷用ビットマップイメージデータを生成し、プリンタエンジンインターフェース８０７を介してプリンタエンジン７１１に出力し、印刷させる。
【００４８】
なお、ＣＰＵ８０１は記憶媒体読取装置８０６に記憶媒体がセットされた場合には、その記憶媒体内に格納されたジョブチケットに基づいて、上記処理を行う。つまり、ジョブ

チケットは、ネットワーク、及びメモリカードのいずれからも入力可能としている。

【００４９】

図９は実施形態における印刷プロセスの手順を示している。これを図７の機能ブロック図を用いて説明する。

【００５０】

先ず、ステップＳ９０１において、ユーザはクライアントコンピュータ７０２上でブラウザプログラムを起動し、サーバ７０１に格納に表示されている画像を表示し、その中の所望とする画像ファイルを指定し、印刷処理を実行させる。この結果、クライアントコンピュータ７０２のプリンタドライバが起動する。プリンタドライバは、そのブラウザプログラムから印刷対象の画像ファイルの所在を示すＵＲＬを取得し、ユーザに対して印刷に係る条件の設定を行わせ、その条件に応じたジョブチケットを生成する。このとき生成されるジョブチケットは、印刷する印刷装置に応じたものとなる。ジョブチケットの生成が完了すると、処理はステップＳ９０２に進んで、そのジョブチケットを、ユーザが指定した印刷装置に向けて送信（出力）する。

【００５１】

印刷装置７１０は上記のようにして送信されたジョブチケットを受信する。印刷装置７１０がジョブチケットを受信すると、その内容を解析し、そこに印刷対象である画像ファイルのＵＲＬの記述をサーチし、そのＵＲＬに従ってサーバ７０１にアクセスし、画像ファイルを取得する。

【００５２】

次いでステップＳ９０４に進んで、印刷装置７１０は、受信した画像ファイル（多くの場合、ＰＤＦ、ＪＰＥＧ等の符号化されている）を解釈し、印刷イメージデータに変換する。この後、ステップＳ９０５でプリンタエンジン７１１に印刷イメージデータを出力することで印刷処理を行う。

【００５３】

上記の用に、従来の印刷プロセスと比較すると、ネットワーク上での画像ファイルの伝送を減らすことが出来るので、ネットワークトラフィックの削減ができる。また、この実施の形態ではクライアントコンピュータによる全画像ファイルの取得が不要となり、印刷物作成までの時間を大幅に短縮して高速化を実現できる。

【００５４】

図１０は、クライアントコンピュータ７０２が生成するジョブチケットの構造の例を示している。ジョブチケットは、画像アドレス部と画像の印刷情報（印刷条件情報）で構成される。

【００５５】

画像アドレス部には、サーバーコンピュータ７０１との通信に用いられるプロトコル（１００１）が格納されている。また、ネットワーク上のサーバーコンピュータのサーバーアドレス（１００２）、サーバー上での情報ファイルのディレクトリとファイル名（１００３）（パス付きファイル名）が格納されている。なお、プロトコル、サーバアドレス、パス付きファイル名は通常、ＨＴＴＰ、ＨＴＴＰＳで一体になって記述される。

【００５６】

例えば、「http://abcdefg.co.jp/hijk/image001.jpg」は、サーバ名は「abcdefg.co.jp」であることを示している。また、そのサーバのディレクトリ「hijk」内に格納されているファイル「image001.jpg」が存在することを示している。そして、「http://」はそのファイルをＨＴＴＰプロトコルで要求し、受信することを示している。

【００５７】

また、画像印刷情報には、画像の拡大縮小率（１００４）、画像の回転情報（１００５）、画像の色情報（１００６）等が格納されている。なお、これ以外にも印刷用紙のサイズ、印刷用紙の種類を含めても構わない。

【００５８】

次に、サーバーコンピュータとの通信に用いられるプロトコル１００１について説明す

る。ここに格納されるプロトコルは、本実施形態の場合、ｈｔｔｐ：／／～か、ｈｔｔｐｓ：／／～のいずれかである。前述したように、ｈｔｔｐｓがＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ）を用いたセキュリティの高いプロトコルであるのに対して、ｈｔｔｐは暗号化を伴わない通常の送受信プロトコルである。

【００５９】

そこで、クライアントコンピュータ７０２のプリンタドライバが、如何にしてｈｔｔｐ：／／～にするか、ｈｔｔｐｓ：／／～のいずれに決定するかについて説明する。

【００６０】

先ず、前提として、一般に、プリンタドライバは、印刷データの出力先をポートという概念で管理している。

【００６１】

例えば、クライアントコンピュータ７０２上に実行されるＯＳが、米国マイクロソフト社が提供するＷｉｎｄｏｗ（登録商標）の場合、プリンタポートには、ＬＰＴ１、ＬＰＴ２、…、ＣＯＭ１、…、ＵＳＢ００１、…、ＦＩＬＥ、ＩＰアドレスが存在する。このうち、ＬＰＴ＃、ＣＯＭ＃、ＵＳＢ＃は、クライアントＰＣのローカルな物理インターフェースを示している。ＬＰＴ１は一般には米国セントロニクス社の仕様のパラレルインターフェース、ＣＯＭ＃はＲＳ－２３２Ｃ等のインターフェース、ＵＳＢはUniversal Serial Busを示す。また、ローカルな物理インターフェースは同一種類のインターフェースでも、複数存在する場合があるので、添え字“１”、“２”が便宜的に割振られている。また、プリンタポート「ＦＩＬＥ」は、印刷データ（ジョブチケット）の出力先としてストレージデバイス（例えばＨＤＤやフレキシブルディスク）にする場合に用いられる。

【００６２】

また、プリンタポートとしての「ＩＰアドレス」は、ユーザが望む限り、幾つでも追加登録できるものであり、ネットワーク上の印刷装置のＩＰアドレスを意味する。つまり、プリンタポートとして「ＩＰアドレス」が指定された場合、ジョブチケットはネットワークインターフェースから出力され、そのネットワーク上のＩＰアドレスで特定された印刷装置に向けて送信されることになる。

【００６３】

さて、クライアントコンピュータ７０２上で実行されるプリンタドライバは、図１１の処理に沿って、ジョブチケットに記述するＵＲＬをｈｔｔｐ：／／～、ｈｔｔｐｓ：／／～を決定する。以下、同図に従って説明する。

【００６４】

先ず、アプリケーションより印刷が実行されると、Ｗｉｎｄｏｗｓ（登録商標） ＡＰＩを用いて、現在の選択されているプリンタポート情報を取得する（ステップＳ１１０１）。

【００６５】

次に、ステップＳ１１０２にて、プリンタポートが“ＦＩＬＥ”であるか否かを判断する。“ＦＩＬＥ”である場合には、ステップＳ１１０６に処理を進め、ジョブチケット中のＵＲＬのプロトコルとして「ｈｔｔｐｓ：／／…」を記述する（理由は後述）。

【００６６】

また、プリンタポートがＦＩＬＥではないと判断した場合には、ステップＳ１１０３に進んで、プリンタポートがＴＣＰ／ＩＰアドレスを含むものであるか否かを判断する。つまり、ネットワーク上の印刷装置に向けて送信するか否かを判断する。

【００６７】

このステップＳ１１０３での判断でＮｏと判断された場合（例えば、プリンタポートとしてＬＰＴ１等が指定された場合等）には、ステップＳ１１０７に進んで、通常の処理を行う。ここで通常の処理とは、ステップＳ１１０７に処理が進んだ場合、印刷装置はクライアントコンピュータにローカル接続されていることを示すので、画像ファイルを取得し、それに従って印刷データの作成を意味する。

【００６８】

また、ステップＳ１１０３の判断がＹｅｓの場合、すなわち、ネットワーク上の印刷装置に対して印刷を行うと判断した場合、処理はステップＳ１１０４に進み、送信先となる印刷装置が社内にあるのか、社外にあるのかを判断する。この判断は、社内として予めクライアントコンピュータ１２０２のメモリに登録されたＩＰアドレス範囲（サーバ１２０１のＩＰアドレスの範囲内）に、送信先の印刷装置のＩＰアドレスがあるいか否かをチェックすることで判断する。この判断は、サーバが社内にあることを前提にしているためである。すなわち、サーバと印刷装置とが同じネットワーク（社内）に所属するか判断する。サーバが所属するネットワーク内（社内）に印刷装置が存在すれば、画像ファイルが外部のインターネット等を経由しないので、画像ファイルが改ざんされる恐れが少ない。よって、印刷装置に非セキュアなプロトコルで画像ファイルをサーバからダウンロードさせても問題は少ない。しなしながら、サーバが所属するネットワーク外（社外）に印刷装置が存在すれば、画像ファイルが外部のインターネット等を経由することになるので、画像ファイルが改ざんされる恐れがある。よって、この場合は、非セキュアなプロトコルで通信するより時間がかかるが印刷装置にセキュアなプロトコルで画像ファイルをサーバからダウンロードさせる。

【００６９】

送信先である印刷装置が社外であると判断した場合には、ジョブチケットのプロトコルに「ｈｔｔｐｓ：／／」を設定する（ステップＳ１１０６）。また、送信先が社内の印刷装置であると判断された時には、暗号化を伴わないプロトコル「ｈｔｔｐ：／／」を、ジョブチケットに記載する（ステップＳ１１０５）。

【００７０】

最後に、ステップＳ１１０８に処理を進め、生成された印刷データ、或いはジョブチケットを、アクティブなプリンタポートに向けて出力する。

【００７１】

以上であるが、送信先が社外の印刷装置、或いは、プリンタポートとしてＦＩＬＥの場合に、ジョブチケットに記述するプロトコルを「ｈｔｔｐｓ：／／」にする理由（暗号化を利用したプロトコル）を以下に説明する。

【００７２】

図１２は、本実施形態のジョブチケットの生成とその流れを示す図である。図示の中央の破線は、社内と社外の境界線を意味するものである。

【００７３】

この時、サブセットアドレスが１９０．１８０．ｘｘｘ．ｘｘｘが、社外と社内を分ける境界線である。つまり、サブセットアドレスが、１９０．１８０以外は、社外ということになる。この時、画像ファイルが置かれているサーバーコンピュータは、社内に置かれている。クライアントコンピュータ１２０２から印刷実行を行い、サーバーコンピュータ１２０１に置かれている画像ファイル情報を記載したジョブチケットが社内に置かれている印刷装置１２０３に送られる。この結果、社内の印刷装置１２０３は、暗号化を伴わないｈｔｔｐ：／／プロトコルでサーバーコンピュータから所望の画像ファイルをダウンロードして、印刷実行を行う。これは、社内ではセキュリティ性の高いイントラネットでオフィス環境が作られている為、サーバーコンピュータからの画像ファイルダウンロード時に、暗号化をともなった送受信プロトコルが必要ないからである。

【００７４】

次に、クライアントコンピュータ１２０２から、社外に位置する印刷装置１２０４に印刷実行をした場合を説明する。この時には、社外のプリンタから社内のサーバーコンピュータにアクセスすることになるので、情報の機密性が低い公衆のインターネットを使って画像ファイルがダウンロードされることになる。そのため、このような時には、暗号化を伴うｈｔｔｐｓ：／／送受信プロトコルで、サーバーコンピュータから画像ファイルをダウンロードして、社外に位置するプリンタで印刷実行する。これにより、社外の印刷装置１２０４とサーバ１２０１間の通信をセキュアなものすることが可能になる。

【００７５】

一方、プリンタポートとしてＦＩＬＥを選択され、印刷処理を実行すると、そのジョブチケットをどの記憶媒体に保存するかを問い合わせるダイアログボックス（不図示）を表示し、ユーザにその記憶媒体を選択させる。従って、ユーザはフィレキシブルディスクや、ＵＳＢメモリカード、書き込み可能なＣＤ－ＲＯＭやＤＶＤ等、可搬性の記憶媒体を格納先として指定できる。可搬性であるが故に、そのジョブチケットを格納した記憶媒体を、図８に示すような構成（記憶媒体読取装置８０６）を有する印刷装置であれば、社内、社外を問わず、印刷出力することができる。

【００７６】

図１３は、印刷ポートとしてファイルが選択されたときの印刷の流れを示す図である。プリンタポートにＦＩＬＥが選ばれるのは、前述した通り、一旦ＵＳＢメモリ、あるいはＤＶＤ－ＲＡＭといったリムーバルな記憶媒体に、ジョブチケットつきの印刷データを保存する場合である。つまり、その媒体を社外にある印刷装置、例えば、コンビニエンスストアのカラープリンタから印刷する場合も有り得る。クライアントコンピュータ７０２上で、プリンタポートをＦＩＬＥにして印刷を行うと、暗号化を伴うｈｔｔｐｓ：／／プロトコルが、ジョブチケットのプロトコル欄に記載される。コンビニエンスストア等のカラープリンタに、この記憶媒体を直接差し込むと、社内のサーバコンピュータから、セキュリティー性の高いｈｔｔｐｓ：／／プロトコルで、ジョブチケットに記載されている画像ファイルをダウンロードし、印刷される。従って、機密性の高い印刷が実現できる。

【００７７】

以上の実施形態の説明の通り、画像のような重たいデータを、プリントデータに組み込むのではなく、そのデータへのリンク情報（ＵＲＬ）のみを記述したジョブチケットを入力して印刷装置において、そのジョブチケットを発行する際のコンピュータ上のプリンタポートで示される出力先が社内か社外か、或いは社外と成り得るか否かに応じて、画像データのＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）を、Ｈｔｔｐにするか、よりセキュアーなＨｔｔｐｓにするかを自動的に切り替える。この結果、オリジナルのファイルを加工しなくても、利便性と高いセキュリティを同時に実現する印刷システムを提供することが可能となる。

【００７８】

なお、実施形態では、社内のＩＰアドレスのサブセットアドレスを１９０．１８０．ｘｘｘ．ｘｘｘとしたが、これは一例である。また、比較的大きな企業では、幾つものサブネットアドレスを所有することがあるが、これらは予めプリンタドライバに登録しておくことで、社内か社外か（関係会社か否か）を識別できるようにしても構わない。

【００７９】

また、実施形態では、印刷対象物として画像ファイルを例にして説明したが、印刷装置のコントローラが解釈できる形式のファイルであれば、画像ファイルに限らず、一般の文書ファイルでも構わない。

【００８０】

また、実施形態では、クライアントコンピュータがジョブチケットを受信する装置が印刷装置であるものとして説明したが、受信する装置はローカルに接続された通常のプリンタを有し、プリントサーバとして機能するパーソナルコンピュータであっても構わない。

【００８１】

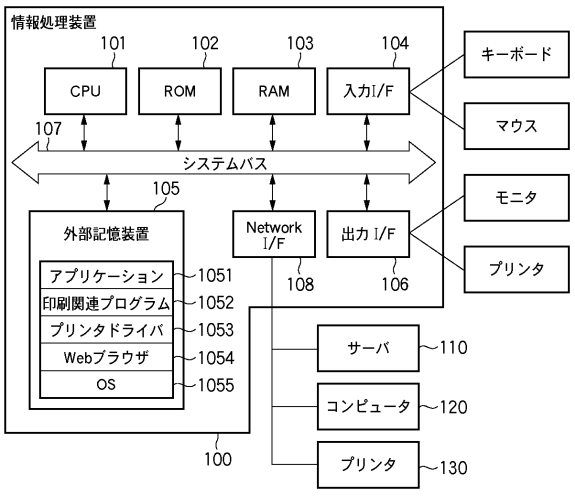
また、実施形態での説明から明らかなように、本実施形態における特徴的な処理は、クライアントコンピュータ上で実行されるプリンタドライバ（コンピュータプログラムの１つ）で実現できるので、本発明はコンピュータプログラムをもその範疇とする。また、通常、コンピュータプログラムは、ＣＤ－ＲＯＭ等のコンピュータ可読記憶媒体に格納されていて、それをコンピュータにセットし、システムにコピーもしくはインストールすることで実行可能になる。従って、このようなコンピュータ可読記憶媒体も、当然に本発明の範疇に入る。

【図面の簡単な説明】

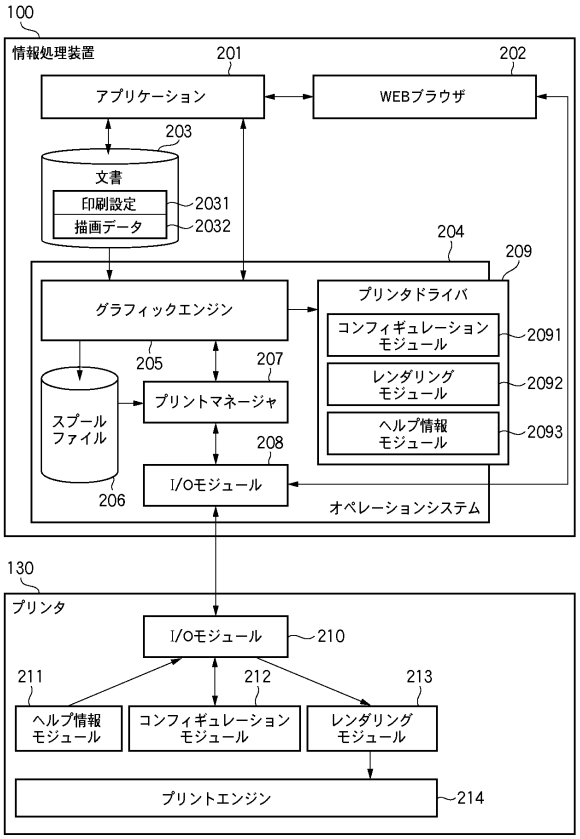
【００８２】

【図１】印刷システムのブロック構成図である。
【図２】一般的な印刷システム・印刷データ生成の構成を説明するブロック図を示す。
【図３】コンピュータにおける印刷設定を保存するＸＭＬ形式の「初期ジョブチケット」の記述例を示す図である。
【図４】コンピュータにおける印刷設定を保存するＸＭＬ形式の「設定ジョブチケット」の記述例を示す図である。
【図５】ＯＳＩ参照モデルにおけるＳＳＬプロトコルを示す図である。
【図６】ＨＴＴＰとＨＴＴＰＳのプロトコルの違いを示す図である。
【図７】実施形態における印刷制御システム全体の構成図である。
【図８】実施形態における印刷装置のハードウエア構成を示すブロック図である。
【図９】実施形態におけるクライアントコンピュータと印刷装置の処理手順を示すフローチャートである。
【図１０】実施形態におけるジョブチケットの例を示す図である。
【図１１】実施形態におけるクライアントコンピュータ上で実行されるプリンタドライバの処理手順を示すフローチャートである。
【図１２】ＩＰアドレスの違いによる印刷フローの違いを示す図である。
【図１３】プリンタポートとしてＦＩＬＥが選択された時の印刷フローを示す図である。

【図１】



【図２】



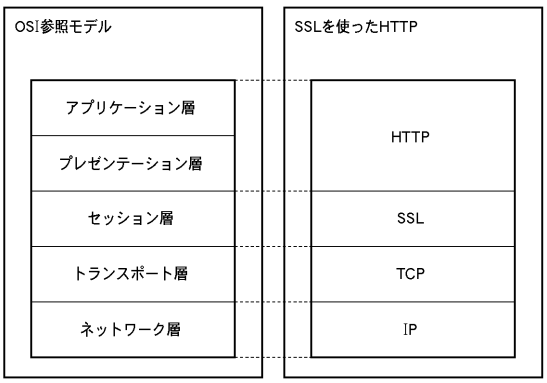
【図３】

```
<psf.InitalJobTichket Version="1"
        xmlns:psf=http://schemas.printer.co.jp/printing/prints chemaframework
        xmlns:psk=http://schemas.printer.co.jp/printing/prints chemakeywords
        xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
        xmlns:xs=http://www.w3.org/2001/XMLSchema
        xmlns:ns1=http://www.privatenamespace1.com>

<psf:Help type="psk:main"URI=http://help.main.PrinterIP/>

<psf:Feature name="psk:MediaSize">
  <psf:Help type="psk:context"URI=http://help.context.MediaSize.IPAddress/>
  <psf:Default name="A4"/>
  <psf:Option name="A4"/>
  <psf:Option name="A5"/>
  <psf:Option name="CustomMediaSize"/>
</psf:Freature>

<psf:Feature name="ns1:HalfTones">
  <psf:Help type="psk:context"URI=http://help.context.HalfTones.IPAddress/>
  <psf:Default name="ns1:Gradation"/>
  <psf:Option name="ns1:Gradation"/>
  <psf:Option name="ns1:ErrorDiffusion"/>
</psf:Freature>
….

</psf:JobTichket>
```

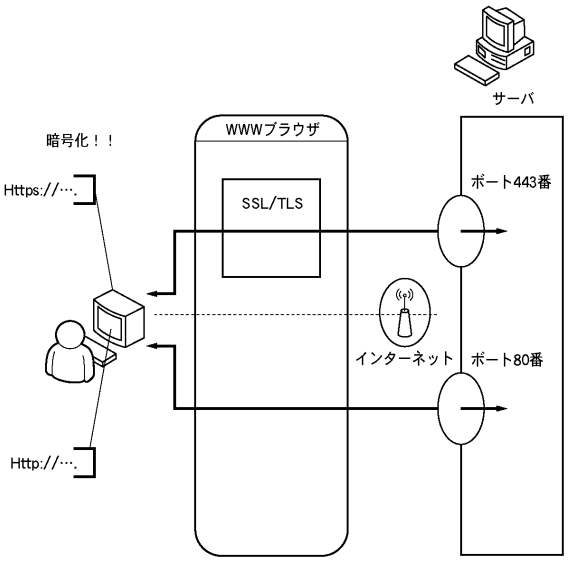
【図４】

```
<psf.InitalJobTichket Version="1"
        xmlns:psf=http://schemas.printer.co.jp/printing/prints chemaframework
        xmlns:psk=http://schemas.printer.co.jp/printing/prints chemakeywords
        xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
        xmlns:xs=http://www.w3.org/2001/XMLSchema
        xmlns:ns1=http://www.privatenamespace1.com>

<psf:Help type="psk:main"URI=http://help.main.PrinterIP/>

<psf:Feature name="psk:MediaSize">
  <psf:Help type="psk:context"URI=http://help.context.MediaSize.IPAddress/>
  <psf:Option name="A4"/>
</psf:Freature>

<psf:Feature name="ns1:HalfTones">
  <psf:Help type="psk:context"URI=http://help.context.HalfTones.IPAddress/>
  <psf:Option name="ns1:Gradation"/>
</psf:Freature>
….

</psf:JobTichket>
```

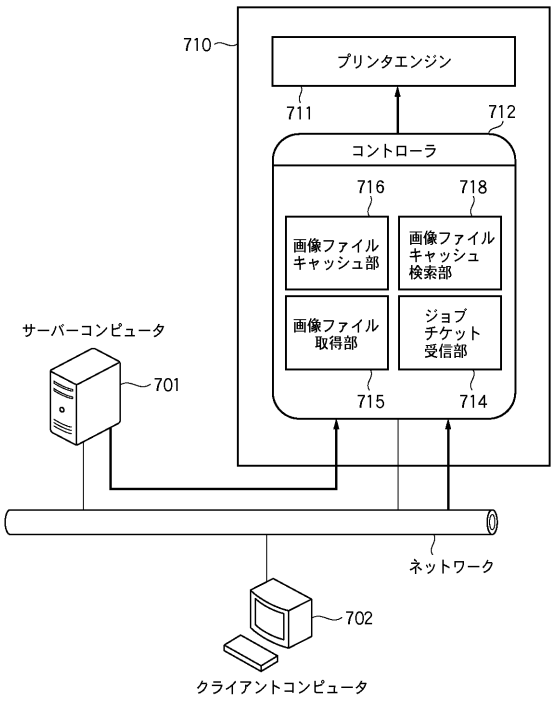
【図５】



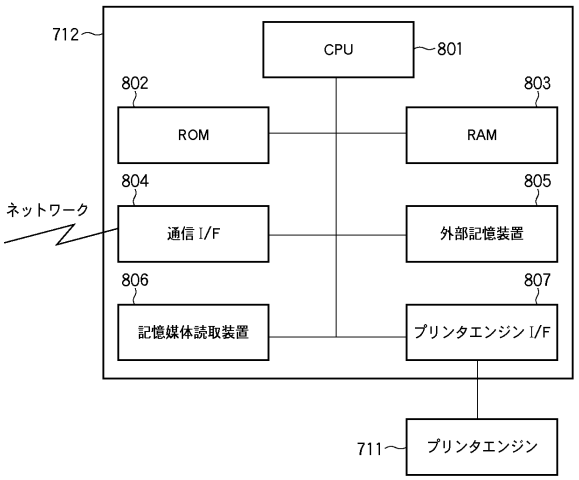
【図６】



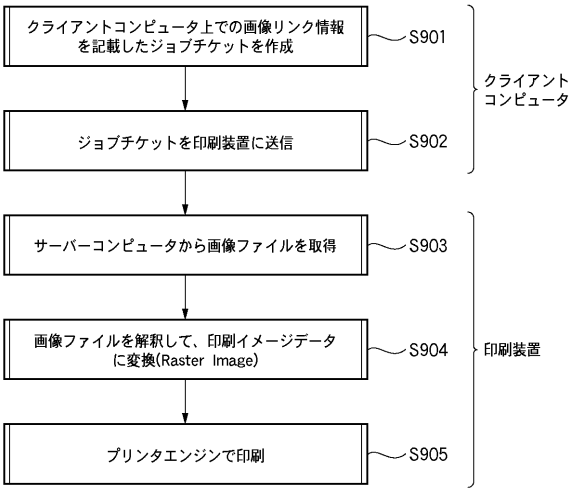
【図７】



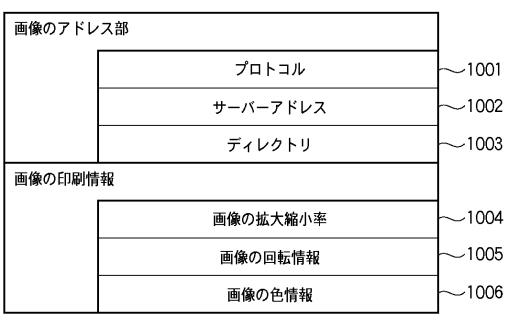
【図８】



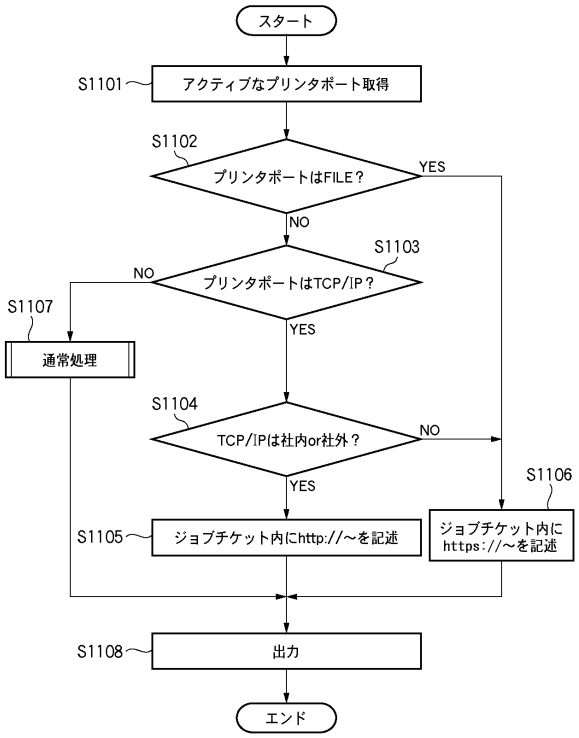
【図９】



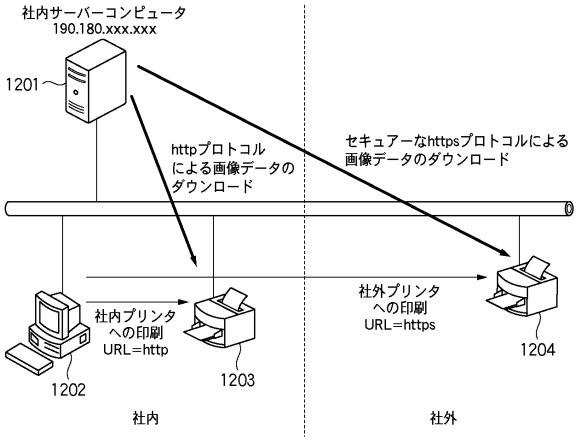
【図１０】



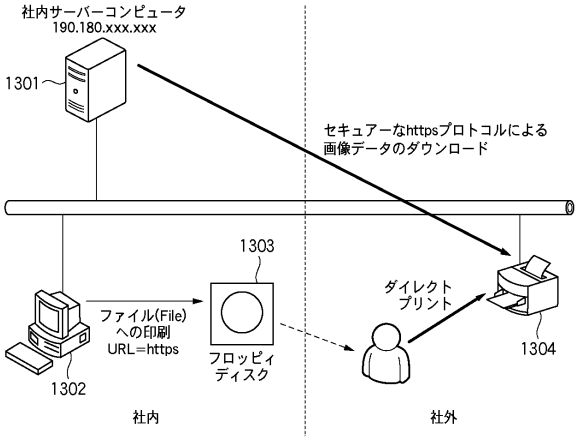
【図１１】



【図１２】


社内サーバーコンピュータ
190.180.xxx.xxx
1201
httpプロトコル
による画像データの
ダウンロード
セキュアーなhttpsプロトコルによる
画像データのダウンロード
社内プリンタ
への印刷
URL=http
社外プリンタ
への印刷
URL=https
1202
1203
1204
社内
社外

【図１３】


社内サーバーコンピュータ
190.180.xxx.xxx
1301
セキュアーなhttpsプロトコルによる
画像データのダウンロード
1303
ファイル(File)
への印刷
URL=https
フロッピィ
ディスク
ダイレクト
プリント
1302
1304
社内
社外

フロントページの続き

審査官　内田　正和

(56)参考文献　特開平１０－２７５０６４（ＪＰ，Ａ）
特開２００４－１６８０５２（ＪＰ，Ａ）
特開２００２－１０８７２９（ＪＰ，Ａ）
特開２００２－３１２１４６（ＪＰ，Ａ）

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