(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2006-1089
(P2006-1089A)
(43)公開日　平成18年1月5日(2006.1.5)

(51)Int.Cl.		F I		テーマコード（参考）
B41J 29/38	(2006.01)	B41J 29/38	Z	2C061

審査請求 有　請求項の数 10　ＯＬ　（全 17 頁）

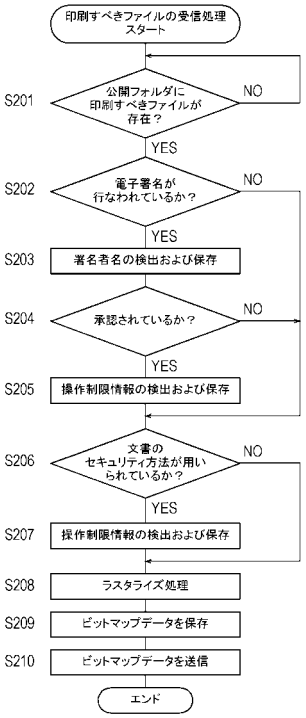
(21)出願番号　特願2004-178425 (P2004-178425)
(22)出願日　平成16年6月16日 (2004.6.16)

(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　100072349
弁理士　八田　幹雄
(74)代理人　100110995
弁理士　奈良　泰男
(74)代理人　100111464
弁理士　齋藤　悦子
(74)代理人　100114649
弁理士　宇谷　勝幸
(74)代理人　100124615
弁理士　藤井　敏史

最終頁に続く

(54)【発明の名称】画像処理装置、画像処理方法、および画像処理プログラム

(57)【要約】
【課題】セキュリティ機能が設定されたデータを展開してビットマップデータを得る場合に、データのセキュリティが損なわれてしまう事態を防止することができる画像処理装置、画像処理方法、および画像処理プログラムを提供する。
【解決手段】画像処理装置としてのプリンタコントローラは、ＰＤＦファイルから当該データに関する操作の制限を示す操作制限情報を検出するとともに（Ｓ２０３，Ｓ２０５，Ｓ２０７）、ＰＤＦファイルを展開してビットマップデータを取得する（Ｓ２０８）。そして、プリンタコントローラは、取得したビットマップデータに対して、検出した操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する（Ｓ２０３，Ｓ２０５，Ｓ２０７，Ｓ２０９）。
【選択図】図６



【特許請求の範囲】
【請求項１】
所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出する検出手段と、
前記所定ファイル形式のデータを展開してビットマップデータを得る展開手段と、
前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する設定手段と、
を有することを特徴とする画像処理装置。
【請求項２】
前記所定ファイル形式のデータは、ページ記述言語で記述されたデータであることを特徴とする請求項１に記載の画像処理装置。
【請求項３】
前記所定ファイル形式のデータは、ＰＤＦデータであることを特徴とする請求項２に記載の画像処理装置。
【請求項４】
前記操作制限情報は、データの印刷の制限を示す情報を含むことを特徴とする請求項１～３のいずれか１つに記載の画像処理装置。
【請求項５】
前記操作制限情報は、データの変更の制限を示す情報を含むことを特徴とする請求項１～４のいずれか１つに記載の画像処理装置。
【請求項６】
前記ビットマップデータを保存する保存手段をさらに有することを特徴とする請求項１～５のいずれか１つに記載の画像処理装置。
【請求項７】
前記ビットマップデータに関する操作の要求を受け付けた場合、当該ビットマップデータに対して設定されている操作の制限に応じて、要求された操作を許可するか否かを判断する判断手段をさらに有することを特徴とする請求項１～６のいずれか１つに記載の画像処理装置。
【請求項８】
所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出するステップと、
前記所定ファイル形式のデータを展開してビットマップデータを得るステップと、
前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定するステップと、
を有することを特徴とする画像処理方法。
【請求項９】
所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出する手順と、
前記所定ファイル形式のデータを展開してビットマップデータを得る手順と、
前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する手順と、
をコンピュータに実行させるための画像処理プログラム。
【請求項１０】
請求項９に記載の画像処理プログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、画像処理装置、画像処理方法、および画像処理プログラムに関する。本発明は、より詳しくは、セキュリティ機能が設定されたデータを展開してビットマップデータ

を得る際の、画像処理装置、画像処理方法、および画像処理プログラムに関する。
【背景技術】
【０００２】
文書の秘匿性を維持するため、文書ファイルに関する操作を制限し得るセキュリティ機能を当該文書ファイルに設定する技術がある。たとえばＰＤＦ（Ｐｏｒｔａｂｌｅ Ｄｏｃｕｍｅｎｔ Ｆｏｒｍａｔ）ファイルには、パスワードを入力しないとファイルを開くことができない機能、文書の著者を明記する機能が付与され得る。
【０００３】
このようなセキュリティ機能を利用した技術として、ネットワークアドレス等の出力先を特定する識別子が付与されたコンテンツの印刷要求を受信した場合、当該識別子をパスワードとして用いてコンテンツをＰＤＦファイルに変換した上で、出力先の印刷装置に送信するファイル変換装置が提案されている（特許文献１参照）。
【０００４】
このファイル変換装置によれば、印刷装置までの転送データの仲介時において、印刷すべき文書ファイルのセキュリティが維持される。
【特許文献１】特開２００２－１０３７２６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ところで、文書ファイルがプリンタコントローラを介して印刷装置に送信されて印刷される場合、当該文書ファイルは、ラスタライズされることにより、ビットマップ化された画像データであるビットマップデータに展開される。こうして得られたビットマップデータは、用紙上に印刷されるとともに、プリンタコントローラ内に保存される。
【０００６】
しかしながら、セキュリティ機能が設定された文書ファイルをラスタライズする際に、当該文書ファイルに関する操作の制限を示す操作制限情報が脱落してしまうため、セキュリティ機能が設定されていないビットマップデータがプリンタコントローラ内に保存されることになる。
【０００７】
したがって、保存されているビットマップデータは、ジョブスプーラユーティリティ等のアプリケーションにより誰でも閲覧、印刷、変更などの操作が可能となる。このように、セキュリティ機能が設定された文書ファイルと同内容のビットマップデータが自由に利用可能となるため、文書ファイルのセキュリティが実質的に失われてしまうという問題があった。
【０００８】
本発明は上記従来技術の有する問題点に鑑みてなされたものであり、本発明の目的は、セキュリティ機能が設定されたデータを展開してビットマップデータを得る場合に、データのセキュリティが損なわれてしまう事態を防止することができる画像処理装置、画像処理方法、および画像処理プログラムを提供することである。
【課題を解決するための手段】
【０００９】
本発明の上記目的は、下記の手段によって達成される。
【００１０】
（１）所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出する検出手段と、前記所定ファイル形式のデータを展開してビットマップデータを得る展開手段と、前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する設定手段と、を有することを特徴とする画像処理装置。
【００１１】
（２）前記所定ファイル形式のデータは、ページ記述言語で記述されたデータであるこ

とを特徴とする上記（１）に記載の画像処理装置。
【００１２】
（３）前記所定ファイル形式のデータは、ＰＤＦデータであることを特徴とする上記（２）に記載の画像処理装置。
【００１３】
（４）前記操作制限情報は、データの印刷の制限を示す情報を含むことを特徴とする上記（１）～（３）のいずれか１つに記載の画像処理装置。
【００１４】
（５）前記操作制限情報は、データの変更の制限を示す情報を含むことを特徴とする上記（１）～（４）のいずれか１つに記載の画像処理装置。
【００１５】
（６）前記ビットマップデータを保存する保存手段をさらに有することを特徴とする上記（１）～（５）のいずれか１つに記載の画像処理装置。
【００１６】
（７）前記ビットマップデータに関する操作の要求を受け付けた場合、当該ビットマップデータに対して設定されている操作の制限に応じて、要求された操作を許可するか否かを判断する判断手段をさらに有することを特徴とする上記（１）～（６）のいずれか１つに記載の画像処理装置。
【００１７】
（８）所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出するステップと、前記所定ファイル形式のデータを展開してビットマップデータを得るステップと、前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定するステップと、を有することを特徴とする画像処理方法。
【００１８】
（９）所定ファイル形式のデータから、当該所定ファイル形式のデータに関する操作の制限を示す操作制限情報を検出する手順と、前記所定ファイル形式のデータを展開してビットマップデータを得る手順と、前記ビットマップデータに対して、前記操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する手順と、をコンピュータに実行させるための画像処理プログラム。
【００１９】
（１０）上記（９）に記載の画像処理プログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の効果】
【００２０】
本発明によれば、セキュリティ機能が設定された所定ファイル形式のデータを展開してビットマップデータを得る場合に、元のデータが保有するセキュリティが、ビットマップデータにおいて損なわれてしまう事態を防止することが可能となる。
【発明を実施するための最良の形態】
【００２１】
以下、本発明の実施の形態を、図面を参照して詳細に説明する。
【００２２】
図１は、印刷システムの全体構成を示すブロック図である。図１に示す印刷システムは、ＰＣ（パーソナルコンピュータ）１００と、画像処理装置としてのプリンタコントローラ２００と、プリンタ３００とを備えている。ＰＣ１００とプリンタコントローラ２００とはネットワーク４００を介して、プリンタコントローラ２００とプリンタ３００とは直接機器間で、それぞれ相互に通信可能に接続されている。
【００２３】
なお、プリンタコントローラ２００とプリンタ３００とは、直接機器間で接続されることなくネットワーク４００を介して接続されていてもよいし、ＰＣ１００とプリンタコン

トローラ２００とは、ネットワーク４００を介することなく直接機器間で接続されていてもよい。また、ネットワーク４００に接続される機器の種類および台数は、図１に示す例に限定されない。

【００２４】

図２は、ＰＣ１００の構成を示すブロック図である。図２に示すように、ＰＣ１００は、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、ハードディスク１０４、ディスプレイ１０５、入力装置１０６、およびネットワークインタフェース１０７を備えており、これらは信号をやり取りするためのバス１０８を介して相互に接続されている。

【００２５】

ＣＰＵ１０１は、プログラムにしたがって、上記各部の制御や各種の演算処理を行う。ＲＯＭ１０２は、各種プログラムや各種データを格納する。ＲＡＭ１０３は、作業領域として一時的にプログラムやデータを記憶する。ハードディスク１０４は、オペレーティングシステムを含む各種プログラムや各種データを格納する。

【００２６】

また、ハードディスク１０４には、文書を作成・編集するためのアプリケーションと、アプリケーションから指示された文書ファイルをプリンタコントローラ２００が解釈可能な言語（たとえばＰｏｓｔＳｃｒｉｐｔ（登録商標）などのＰＤＬ（Ｐａｇｅ Ｄｅｓｃｒｉｐｔｉｏｎ Ｌａｎｇｕａｇｅ：ページ記述言語））に変換するためのプリンタドライバと、プリンタコントローラ２００のステータスの閲覧およびプリンタコントローラ２００に保存されている画像データ（ビットマップデータ）に関する閲覧、印刷、変更などの操作を行うために用いられるＷｅｂブラウザとがインストールされている。

【００２７】

ディスプレイ１０５は、各種の情報を表示する。入力装置１０６は、マウス等のポインティングデバイスやキーボードであり、各種の入力を行うために使用される。

【００２８】

ネットワークインタフェース１０７は、ネットワーク４００を介して他の機器と通信するためのインタフェースであり、イーサネット（登録商標）、トークンリング、ＦＤＤＩ等の規格が用いられる。

【００２９】

図３は、プリンタコントローラ２００の構成を示すブロック図である。図３に示すように、プリンタコントローラ２００は、ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、ハードディスク２０４、ネットワークインタフェース２０５、およびプリンタインタフェース２０６を備えており、これらは信号をやり取りするためのバス２０７を介して相互に接続されている。プリンタコントローラ２００の上記各部のうち、ＰＣ１００の上記各部と同様の機能を有する部分については、説明の重複を避けるためその説明を省略する。

【００３０】

ハードディスク２０４は、プリンタ３００に印刷のために出力したビットマップデータを保存するために使用される。また、ハードディスク２０４には、ビットマップデータに関する操作を実現するためのユーティリティがインストールされている。

【００３１】

プリンタインタフェース２０６は、プリンタ３００と通信するためのインタフェースであり、たとえば専用のビデオインタフェースが使用され得る。ただし、プリンタインタフェース２０６は、ＲＳ－２３２Ｃ、ＩＥＥＥ１３９４、ＵＳＢ等のシリアルインタフェースによるものや、ＩＥＥＥ１２８４等のパラレルインタフェースによるものの他、独自の規格によるものであってもよい。

【００３２】

図４は、プリンタ３００の構成を示すブロック図である。図４に示すように、プリンタ３００は、ＣＰＵ３０１、ＲＯＭ３０２、ＲＡＭ３０３、操作パネル部３０４、印刷部３０５、およびコントローラインタフェース３０６を備えており、これらは信号をやり取りするためのバス３０７を介して相互に接続されている。プリンタ３００の上記各部のうち

、ＰＣ１００の上記各部と同様の機能を有する部分については、説明の重複を避けるためその説明を省略する。

【００３３】

操作パネル部３０４は、タッチパネル、タッチパネル外の固定キー、表示ランプ等で構成されており、各種の入力および表示を行うために使用される。印刷部３０５は、プリンタコントローラ２００から転送されたビットマップデータを電子写真方式等の印刷方式により用紙などの記録材に印刷する。コントローラインタフェース３０６は、プリンタコントローラ２００と通信するためのインタフェースである。

【００３４】

なお、ＰＣ１００、プリンタコントローラ２００、およびプリンタ３００は、それぞれ、上記した構成要素以外の構成要素を含んでいてもよく、あるいは、上記した構成要素のうちの一部が含まれていなくてもよい。

【００３５】

次に、印刷システムの動作について説明する。

【００３６】

本実施形態の印刷システムでは、通常プリントと、ダイレクトプリントの２種類の印刷が実行可能である。通常プリントが実行される場合、印刷すべきファイルは、ＰＣ１００のプリンタドライバによって、ＰＣ１００においてＰＤＬで記述されたプリントデータに変換された後、プリンタコントローラ２００に送信される。一方、ダイレクトプリントが実行される場合、印刷すべきファイルは、ＰＣ１００においてプリンタドライバによってＰＤＬデータに変換されることなく、ＰＣ１００から直接プリンタコントローラ２００に送信される。

【００３７】

ダイレクトプリントの場合、送信可能なファイル形式は、プリンタコントローラ２００においてビットマップデータに展開され得るファイル形式に限定される。ダイレクトプリントは、たとえばＰＤＦ（Ｐｏｒｔａｂｌｅ Ｄｏｃｕｍｅｎｔ Ｆｏｒｍａｔ）、ＴＩＦＦ（Ｔａｇｇｅｄ Ｉｍａｇｅ Ｆｉｌｅ Ｆｏｒｍａｔ）、ＰｏｓｔＳｃｒｉｐｔ（登録商標）、ＥＰＳ（Ｅｎｃａｐｓｕｌａｔｅｄ ＰｏｓｔＳｃｒｉｐｔ（登録商標））などのファイル形式をサポートする。

【００３８】

以下、本実施形態では、セキュリティ機能を設定できるデータとしてＰＤＦファイルを例として取り上げ、このＰＤＦファイルのダイレクトプリントについて説明する。

【００３９】

図５は、ＰＣ１００における印刷すべきファイルの送信処理の手順を示すフローチャートである。なお、図５のフローチャートにより示されるアルゴリズムは、ＰＣ１００のハードディスク１０４などの記憶部にプログラムとして記憶されており、ＣＰＵ１０１によって実行される。

【００４０】

まず、前提として、アプリケーションにより、ＰＤＦファイルを構成するＰＤＦファイルデータ中に、印刷対象データが入力されているものとする。次いで、ユーザの操作に基づいて、ＰＤＦファイルに対してセキュリティ機能が設定される（Ｓ１０１）。ここで、ＰＤＦファイルに関する操作の制限を示す操作制限情報がＰＤＦファイルに追加される。

【００４１】

セキュリティ機能の設定には、ＰＤＦファイルに対して署名をして承認するときに当該ＰＤＦファイルに関する操作の制限を設定する場合と、文書のセキュリティ方法を使用してＰＤＦファイルに関する操作の制限を設定する場合とがある。

【００４２】

ＰＤＦファイルでは、文書の著者である旨を証明するために、電子署名機能が使用される。署名にはデジタルＩＤが使用され得る。ここで、署名者名として、著者名あるいは承認者名が記録される。本実施形態では、署名者名として、ビットマップデータに関する操

作を行うためのユーティリティへのログイン名が用いられる。ただし、署名者名として、ＰＣ１００のホスト名、あるいはＰＣ１００へのログイン名を用いる方法を採用することも可能である。

【００４３】

そして、作成されたＰＤＦファイルがプリンタコントローラ２００に送信される（Ｓ１０２）。具体的には、作成されたファイルが、プリンタコントローラ２００内のＲＡＭ２０３などの記憶部に設定される公開フォルダ（あるいは公開キュー）に転送される。たとえば、ネットワーク４００を経由したＳＭＢ（Ｓｅｒｖｅｒ Ｍｅｓｓａｇｅ Ｂｌｏｃｋ）通信によるデータの転送、ネットワーク４００を経由したＦＴＰ（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）通信によるデータの転送、ＣＤ（Ｃｏｍｐａｃｔ Ｄｉｓｃ）あるいはＭＯ（Ｍａｇｎｅｔｏ Ｏｐｔｉｃａｌ Ｄｉｓｋ）などの記録媒体を用いたデータの転送、および電子メールに添付することによるデータの転送などの各種の転送方法が使用され得る。

【００４４】

図６は、プリンタコントローラ２００における印刷すべきファイルの受信処理の手順を示すフローチャートである。なお、図６のフローチャートにより示されるアルゴリズムは、プリンタコントローラ２００のハードディスク２０４などの記憶部にプログラムとして記憶されており、ＣＰＵ２０１によって実行される。

【００４５】

まず、プリンタコントローラ２００は、公開フォルダに、印刷すべきＰＤＦファイルが存在しているか否かを判断する（Ｓ２０１）。すなわち、定期的に、たとえばＰＣ１００から受信した印刷すべきＰＤＦファイルが公開フォルダに保存されているか否かが確認される。ＰＤＦファイルが公開フォルダに存在していない場合（Ｓ２０１でＮＯ）、ＰＤＦファイルが公開フォルダに新規に保存されるまで待機する。

【００４６】

ＰＤＦファイルが公開フォルダに存在していると判断された場合（Ｓ２０１でＹＥＳ）、当該ＰＤＦファイルに対して電子署名が行われているか否かが判断される（Ｓ２０２）。電子署名が行われていない場合（Ｓ２０２でＮＯ）、ステップＳ２０６に進む。

【００４７】

図７は、電子署名機能を用いることによりセキュリティ機能が設定された場合、ＰＤＦファイルに付加される情報の一例を示す図である。ＰＤＦファイル中に、「／Ｔｙｐｅ／Ｓｉｇ／Ｎａｍｅ」が検出された場合、ＰＤＦファイルに対して電子署名が行われていると判断される。

【００４８】

ＰＤＦファイルに対して電子署名が行われている場合（Ｓ２０２でＹＥＳ）、署名者名の検出および保存が行われる（Ｓ２０３）。図７の場合、「／Ｔｙｐｅ／Ｓｉｇ／Ｎａｍｅ」の後ろのかっこ内の部分（ここでは「ｔｅｓｔｎａｍｅ」）が署名者名を示す。検出された署名者名は、ファイル名とともに、プリンタコントローラ２００内のハードディスク２０４などの記憶部に保存される。ここで、署名者名は、ビットマップデータ情報テーブルにおいて、ファイル名に関連付けられて保存される。

【００４９】

図８は、ビットマップデータ情報テーブルの一例を示す図である。図８において、「Ｊｏｂ Ｎｏ．」の欄は、新規に受信したファイルに対して任意に付与される識別番号を示す。「Ｆｉｌｅ Ｎａｍｅ」の欄は、受信したファイルのファイル名を示す。「Ｓｔａｔｕｓ」の欄は、受信したファイルに関するジョブの状態を示す（「Ｐｒｉｎｔｅｄ」は印刷済みであることを示す）。「Ｊｏｂ Ｃｌａｓｓ」の欄は、プリント、スキャンなどのジョブの種類を示す。「Ｏｗｎｅｒ」の欄は、ジョブの操作者を示す（受信したファイルに対して電子署名が行われている場合、電子署名の部分に記録される署名者名を示す）。「Ｄａｔｅ」の欄の値は、ジョブが終了した日付を示す。なお、データサイズを示す欄などの他の欄が含まれていてもよい。

【００５０】
続いて、印刷すべきＰＤＦファイルにかかる文書が承認されているか否かが判断される（Ｓ２０４）。文書が承認されていない場合（Ｓ２０４でＮＯ）、ステップＳ２０６に進む。
【００５１】
図７に示すように、ＰＤＦファイル中に、「／ＴｒａｎｓｆｏｒｍＰａｒａｍｓ＜＜／Ｔｙｐｅ／ＴｒａｎｓｆｏｒｍＰａｒａｍｓ／Ｐ（数字）」が検出された場合、ＰＤＦファイルにかかる文書が承認されていると判断される。
【００５２】
文書が承認されている場合（Ｓ２０４でＹＥＳ）、操作制限情報の検出および保存が行われる（Ｓ２０５）。図７の場合、「／Ｔｙｐｅ／ＴｒａｎｓｆｏｒｍＰａｒａｍｓ／Ｐ」の後ろに続く数字が操作制限のレベルを示す。ここで、「Ｐ１」は、文書の変更を許可しないことを、「Ｐ２」は、フォームフィールドの入力のみを許可することを、「Ｐ３」は、注釈の作成及びフォームフィールドの入力のみを許可することを示す。なお、注釈は、ファイルに対する追加の書き込み情報であり、フォームフィールドは、値を入力するための領域である。
【００５３】
上記した「Ｐ」の後ろに続く数字に応じて、受信したＰＤＦファイルをラスタライズして得られるビットマップデータに関する操作の制限を設定することができる。すなわち、検出された操作制限情報に応じて、ビットマップデータに関する操作の制限が、ビットマップデータ情報テーブル上で設定される。
【００５４】
たとえば、受信したＰＤＦファイルから操作制限情報として「Ｐ１」が検出された場合、ビットマップデータの変更を一切許可しないという、ビットマップデータに関する操作の制限が設定される。この場合、図８に示すように、ビットマップデータ情報テーブルの「Ｅｄｉｔ」の欄の値が、ファイル名に関連付けられて、「Ｎｏ」に設定されて保存される。つまり、図８において、「Ｅｄｉｔ」の欄は、ビットマップデータの編集が許可されているか否かを示す。また、「Ｐ２」または「Ｐ３」が検出された場合、ヘッダ、フッタ、日付、ナンバリングなどの、画像データに対して付加される情報のみの編集を許可するという、ビットマップデータに関する操作の制限が設定される。この場合、図８に示すように、ビットマップデータ情報テーブルの「Ｈｅａｄｅｒ」の欄の値が、ファイル名に関連付けられて、「Ｙｅｓ」に設定されて保存される。つまり、図８において、「Ｈｅａｄｅｒ」の欄は、画像データ以外の部分の編集が許可されているか否かを示す。なお、操作制限情報として「Ｐ１」のみが使用されてもよい。
【００５５】
ステップＳ２０６では、文書のセキュリティ方法が用いられているか否かが判断される。文書のセキュリティ方法が用いられていない場合（Ｓ２０６でＮＯ）、ステップＳ２０８に進む。
【００５６】
図９は、文書のセキュリティ方法を用いることによりセキュリティ機能が設定された場合、ＰＤＦファイルに付加される情報の一例を示す図である。ＰＤＦファイル中に、「／Ｒ　（数字）」が検出された場合、ＰＤＦファイルに対して文書のセキュリティ方法が使用されていると判断される。「／Ｒ」の後ろに続く数字は、セキュリティのリビジョンを示す。なお、図９は、パスワードによるセキュリティ方法が用いられた場合の例を示すものであるが、デジタルＩＤによるセキュリティ方法が用いられてもよい。
【００５７】
文書のセキュリティ方法が用いられている場合（Ｓ２０６でＹＥＳ）、操作制限情報の検出および保存が行われる（Ｓ２０７）。図９の場合、「／Ｐ－」の後ろに続く数字がセキュリティの内容を示す。この値は、１０進数で表された符号なし整数であり、２進数に変換される。たとえば図９に示す１０進数の「２３６４」は、３２ビットの２進数である

「１１１１１１１１１１１１１１１１１１１１１０１１０１１０００１００」に変換される。変換後の２進数の数値の各ビットの値に基づいて、操作制限情報が検出され得る。

【００５８】

２進数の数値において、３ビット目の値であるＢＩＴ３が「１」の場合、印刷が許可されており、ＢＩＴ３が「０」の場合、印刷が許可されていない。また、１２ビット目の値であるＢＩＴ１２が「１」の場合、高解像度での印刷が許可されており、ＢＩＴ１２が「０」の場合、低解像度（１５０ｄｐｉ）での印刷のみが許可されている。また、４ビット目の値であるＢＩＴ４が「１」の場合、文書の変更が許可されており、ＢＩＴ４が「０」の場合、文書の変更が許可されていない。また、６ビット目の値であるＢＩＴ６が「１」の場合、注釈とフォームフィールドの作成・編集が許可されており、ＢＩＴ６が「０」の場合、注釈とフォームフィールドの作成・編集が許可されていない。また、９ビット目の値であるＢＩＴ９が「１」の場合、フォームフィールドの入力、および署名が許可されており、ＢＩＴ９が「０」の場合、フォームフィールドの入力、および署名が許可されていない。また、１１ビット目の値であるＢＩＴ１１が「１」の場合、文書アセンブリの編集・利用が許可されており、ＢＩＴ１１が「０」の場合、文書アセンブリの編集・利用が許可されていない。文書アセンブリの編集・利用には、ページの挿入、回転、および削除と、ブックマーク、およびサムネールイメージの作成とが含まれる。

【００５９】

上記した「／Ｐ－」の後ろに続く数字に応じて、受信したＰＤＦファイルをラスタライズして得られるビットマップデータに関する操作の制限を設定することができる。すなわち、検出された操作制限情報に応じて、ビットマップデータに関する操作の制限が設定される。

【００６０】

たとえば、ＢＩＴ３が「０」であることが検出された場合、ビットマップデータの印刷を許可しないという、ビットマップデータに関する操作の制限が設定される。このように文書のセキュリティ方法を用いることにより、ビットマップデータの再印刷を拒否することが可能となる。この場合、図８に示すように、ビットマップデータ情報テーブルの「Ｐｒｉｎｔ」の欄の値が、ファイル名に関連付けられて、「Ｎｏ」に設定されて保存される。つまり、図８において、「Ｐｒｉｎｔ」の欄は、印刷が許可されているか否かを示す。

【００６１】

また、ＢＩＴ４が「０」であることが検出された場合、ビットマップデータの変更を一切許可しないという、ビットマップデータに関する操作の制限が設定される。この場合、図８に示すように、ビットマップデータ情報テーブルの「Ｅｄｉｔ」の欄の値が、ファイル名に関連付けられて、「Ｎｏ」に設定されて保存される。また、ＢＩＴ６、ＢＩＴ９、あるいはＢＩＴ１１が「１」であることが検出された場合、ヘッダ、フッタ、日付、ナンバリングなどの、画像データに対して付加される情報のみの編集を許可するという、ビットマップデータに関する操作の制限が設定される。この場合、図８に示すように、ビットマップデータ情報テーブルの「Ｈｅａｄｅｒ」の欄の値が、ファイル名に関連付けられて、「Ｙｅｓ」に設定されて保存される。

【００６２】

ステップＳ２０８では、受信したＰＤＦファイルに対して、ラスタライズ処理が施される。すなわち、ＰＤＦファイルが展開されてビットマップデータが取得される。

【００６３】

取得されたビットマップデータは、ビットマップデータ情報テーブルに登録されているファイル名に関連付けられて、プリンタコントローラ２００内のハードディスク２０４などの記憶部に保存される。つまり、結果として、ビットマップデータに対して、検出した操作制限情報に応じて、当該ビットマップデータに関する操作の制限が設定されることになる。ただし、ビットマップデータと、当該ビットマップデータに関する操作の制限の内容とを関連付ける方法は、ビットマップデータ情報テーブルを使用する方法に限定されるものではない。

【００６４】
続いて、プリンタコントローラ２００は、ステップＳ２０８で得られたビットマップデータを、プリンタ３００に送信する。
【００６５】
図１０は、プリンタ３００における印刷処理の手順を示すフローチャートである。なお、図１０のフローチャートにより示されるアルゴリズムは、プリンタ３００のＲＯＭ３０２などの記憶部にプログラムとして記憶されており、ＣＰＵ３０１によって実行される。
【００６６】
まず、プリンタ３００は、プリンタコントローラ２００から、ビットマップデータを受信する（Ｓ３０１）。受信したビットマップデータは、印刷部３０５により、用紙などの記録材に印刷される（Ｓ３０２）。
【００６７】
次に、プリンタコントローラ２００に処理済みデータとして保存されたビットマップデータを再度利用する場合の処理について説明する。
【００６８】
図１１は、ＰＣ１００におけるビットマップデータに対する操作要求の送信処理の手順を示すフローチャートである。なお、図１１のフローチャートにより示されるアルゴリズムは、ＰＣ１００のハードディスク１０４などの記憶部にプログラムとして記憶されており、ＣＰＵ１０１によって実行される。
【００６９】
まず、ＰＣ１００は、Ｗｅｂブラウザを用いて、プリンタコントローラ２００と通信し、プリンタコントローラ２００内に保存されているビットマップデータを操作するためのユーティリティの起動を要求する（Ｓ４０１）。
【００７０】
続いて、ユーザの入力に基づいて、ユーティリティ起動後のアクセスについての許可を得るためのログインが行われる（Ｓ４０２）。ここで、たとえば入力されたログイン名およびパスワードにしたがって、プリンタコントローラ２００においてログイン認証が行われる。
【００７１】
ログインが終了すると、ビットマップデータに関する操作を受け付けるための操作画面がディスプレイ１０５上に表示される（Ｓ４０３）。図１２は、操作画面の一例を示す図である。図１２の操作画面において、ジョブのリストが示される。
【００７２】
そして、当該リストの中で、操作を希望するファイル（ビットマップデータ）が選択されることにより、操作対象データの設定が行われる（Ｓ４０４）。ここで、ＰＣ１００は、操作対象データの設定に関する情報をプリンタコントローラ２００に送信し、プリンタコントローラ２００は、操作を許可するか否かの通知をＰＣ１００に返信する。
【００７３】
ステップＳ４０５では、操作が許可されたか否かが判断される。すなわち、プリンタコントローラ２００から、操作制限の内容が受信されたか、あるいは警告の通知が受信されたかが判断される。
【００７４】
操作が許可された場合（Ｓ４０５でＹＥＳ）、ビットマップデータに関する操作制限の内容が表示される（Ｓ４０６）。ここで、プリンタコントローラ２００からの受信内容にしたがって、操作画面中のたとえば制限される操作機能の部分がグレイアウトさせられることにより、一部または全部の操作が制限される。
【００７５】
そして、ユーザの選択に基づいて、操作画面を通じて利用可能な操作の中から、所望の操作項目が設定される（Ｓ４０７）。
【００７６】

続いて、設定された操作項目にしたがって、たとえば印刷要求などの操作要求がプリンタコントローラ２００に送信される。

【００７７】

一方、操作が許可されずに、警告の通知が受信された場合（Ｓ４０５でＮＯ）、ディスプレイ１０５に、所定の警告が表示される（Ｓ４０９）。この場合、たとえば権限が無いために操作できないという旨の警告が表示され、ユーザに注意が促される。

【００７８】

図１３は、プリンタコントローラ２００におけるビットマップデータに対する操作要求の受信処理の手順を示すフローチャートである。なお、図１３のフローチャートにより示されるアルゴリズムは、プリンタコントローラ２００のハードディスク２０４などの記憶部にプログラムとして記憶されており、ＣＰＵ２０１によって実行される。

【００７９】

まず、プリンタコントローラ２００は、ＰＣ１００からの要求に基づいて、ビットマップデータを操作するためのユーティリティを起動する（Ｓ５０１）。

【００８０】

続いて、ＰＣ１００から受信したログイン名およびパスワードにしたがってログイン認証が行われ、ログイン名がＲＡＭ２０３などの記憶部に保存される。

【００８１】

続いて、操作画面用のデータがＰＣ１００に送信される（Ｓ５０３）。そして、ＰＣ１００から受信した操作対象データの設定に関する情報にしたがって、操作対象のビットマップデータが特定される（Ｓ５０４）。

【００８２】

ステップＳ５０５では、特定されたビットマップデータの署名者名と、当該ユーティリティへのログイン名とが一致しているか否かが判断される。なお、署名者名は、図８のビットマップデータ情報テーブルにおいて、「Ｏｗｎｅｒ」の欄に記述されている。

【００８３】

署名者名とログイン名とが一致している場合（Ｓ５０５でＹＥＳ）、特定された操作対象のビットマップデータに関する操作が許可される（Ｓ５０６）。続いて、操作制限に関する処理が行われる（Ｓ５０７）。ここで、ビットマップデータ情報テーブルの内容にしたがって、操作画面中の制限される操作機能の部分をグレイアウトさせるための指示がＰＣ１００に送信される。

【００８４】

具体的には、操作が許可された場合、原則として、プリンタコントローラ２００内に保存されているビットマップデータに関して、プレビューでの閲覧、編集、削除、再印刷、電子メール等による転送、データ取得などの操作が可能となる。ただし、利用可能な操作は、元のＰＤＦファイルの操作制限情報に応じて設定された、ビットマップデータに関する操作制限、を受けない範囲内にとどまる。たとえば、元のＰＤＦファイルに対して電子署名が行われて承認されており、操作制限情報が、文書の変更を許可しない「Ｐ１」であった場合、閲覧、および再印刷は可能であるが、ヘッダの追加などの文書の変更にあたる操作は許可されないことになる。これにより、ビットマップデータに関する利用可能な操作内容が限定される。

【００８５】

続いて、ＰＣ１００から、印刷要求などの操作要求が受信される（Ｓ５０８）。そして、操作要求の種類に応じて、特定されたビットマップデータに関する操作が行われる（Ｓ５０９）。たとえば操作要求が印刷要求である場合、当該ビットマップデータは、プリンタ３００に送信されて、印刷される。

【００８６】

一方、ステップＳ５０５で署名者名とログイン名とが一致していないと判断された場合（Ｓ５０５でＮＯ）、ＰＣ１００に対して警告を通知する。この場合、たとえば権限が無いために操作できないという旨の警告ダイアログが、ＰＣ１００に送信される。これによ

り、ビットマップデータに関する操作権限を有するユーザが限定される。

【００８７】

このように本実施形態によれば、プリンタコントローラ２００は、ＰＤＦファイルから当該データに関する操作の制限を示す操作制限情報を検出するとともに、ＰＤＦファイルを展開してビットマップデータを取得する。そして、プリンタコントローラ２００は、取得したビットマップデータに対して、検出した操作制限情報に応じて、当該ビットマップデータに関する操作の制限を設定する。

【００８８】

したがって、セキュリティ機能が設定されたＰＤＦファイルのデータを展開してビットマップデータを得る場合に、元のデータが保有するセキュリティが、ビットマップデータにおいて損なわれてしまう事態を確実に防止することが可能となる。

【００８９】

本発明は、上記した実施形態のみに限定されるものではなく、特許請求の範囲内において、種々改変することができる。

【００９０】

たとえば、上記実施形態において、画像処理装置としてのプリンタコントローラ２００は、プリンタ３００と分離独立して配置されているが、本発明はこれに限定されるものではない。プリンタコントローラ２００は、プリンタ３００に内包されていてもよい。したがって、本発明は、たとえば複写機、ＭＦＰ（Ｍｕｌｔｉ－Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）などの印刷装置にも適用可能である。

【００９１】

また、上記実施形態では、ＰＤＦファイルを展開してビットマップデータを得る場合について説明したが、本発明はこれに限定されるものではない。本発明は、セキュリティ機能を設定し得る他のファイル形式のデータを展開してビットマップデータを得る場合にも適用され得る。

【００９２】

また、ファイルから検出される操作制限情報は、上記実施形態で例示した情報に限定されるものではない。操作制限情報は、データに関する操作の制限につながる情報であれば任意である。さらに、元のファイルの操作制限情報に応じて設定されるビットマップデータに関する操作の制限は、上記実施形態で例示した操作の制限に限定されるものではない。ビットマップデータに関する操作の制限は、元のファイルの操作制限情報と対応関係を有するように任意に設定され得る。

【００９３】

本発明による画像処理装置としてのプリンタコントローラにおける各種処理を行う手段および方法は、専用のハードウェア回路、またはプログラムされたコンピュータのいずれによっても実現することが可能である。上記プログラムは、たとえばフレキシブルディスクやＣＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体によって提供されてもよいし、インターネット等のネットワークを介してオンラインで提供されてもよい。この場合、コンピュータ読み取り可能な記録媒体に記録されたプログラムは、通常、ハードディスク等の記憶部に転送されて記憶される。また、上記プログラムは、単独のアプリケーションソフトとして提供されてもよいし、画像処理装置の一機能としてその装置のソフトウェアに組み込まれてもよい。

【図面の簡単な説明】

【００９４】

【図１】印刷システムの全体構成を示すブロック図である。

【図２】ＰＣの構成を示すブロック図である。

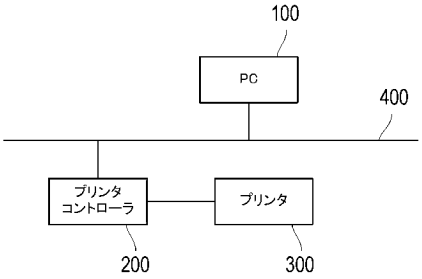
【図３】プリンタコントローラの構成を示すブロック図である。

【図４】プリンタの構成を示すブロック図である。

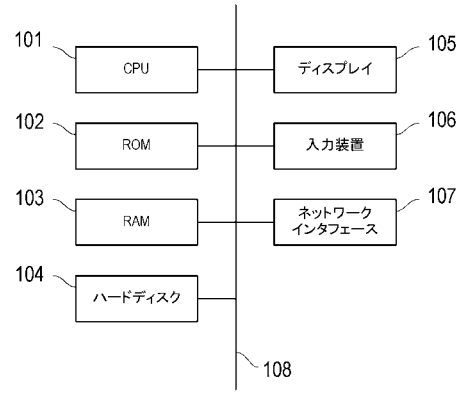
【図５】ＰＣにおける印刷すべきファイルの送信処理の手順を示すフローチャートである。

【図６】プリンタコントローラにおける印刷すべきファイルの受信処理の手順を示すフローチャートである。
【図７】電子署名機能を用いることによりセキュリティ機能が設定された場合、ＰＤＦファイルに付加される情報の一例を示す図である。
【図８】ビットマップデータ情報テーブルの一例を示す図である。
【図９】文書のセキュリティ方法を用いることによりセキュリティ機能が設定された場合、ＰＤＦファイルに付加される情報の一例を示す図である。
【図１０】プリンタにおける印刷処理の手順を示すフローチャートである。
【図１１】ＰＣにおけるビットマップデータに対する操作要求の送信処理の手順を示すフローチャートである。
【図１２】操作画面の一例を示す図である。
【図１３】プリンタコントローラにおけるビットマップデータに対する操作要求の受信処理の手順を示すフローチャートである。
【符号の説明】
【００９５】
１００　ＰＣ、
１０１，２０１，３０１　ＣＰＵ、
１０２，２０２，３０２　ＲＯＭ、
１０３，２０３，３０３　ＲＡＭ、
１０４，２０４　ハードディスク、
１０５　ディスプレイ、
１０６　入力装置、
１０７，２０５　ネットワークインタフェース、
１０８，２０７，３０７　バス、
２００　プリンタコントローラ、
２０６　プリンタインタフェース、
３００　プリンタ、
３０４　操作パネル部、
３０５　印刷部、
３０６　コントローラインタフェース、
４００　ネットワーク。

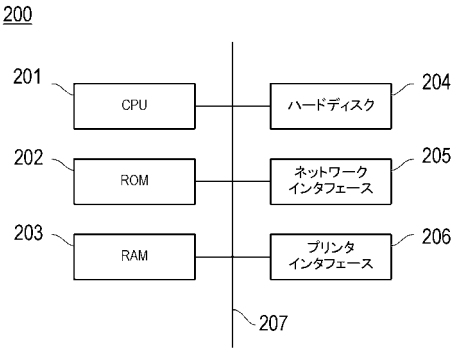
【図１】



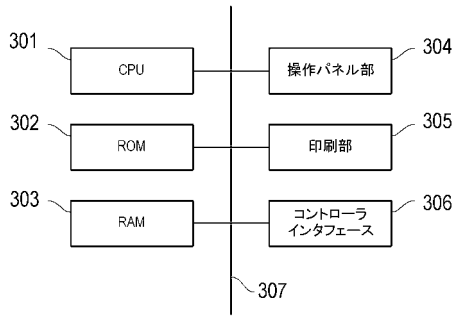
【図２】



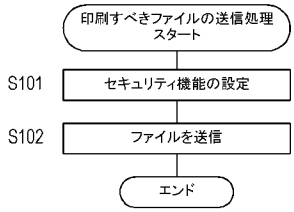
【図３】



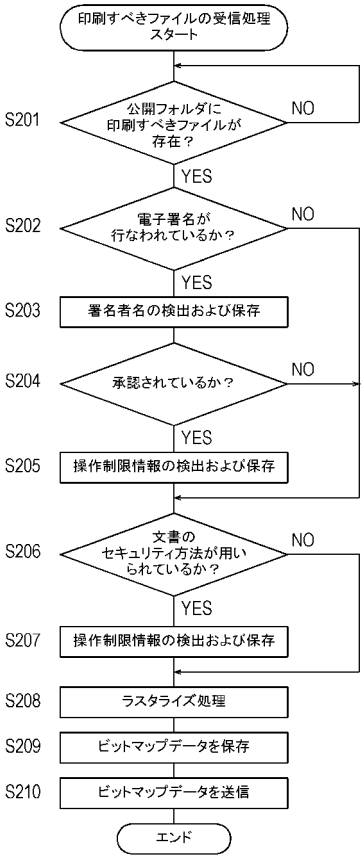
【図４】



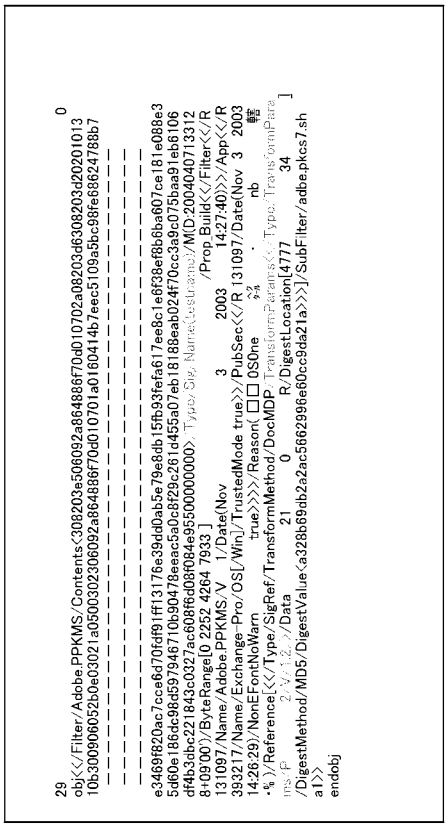
【図５】



【図６】



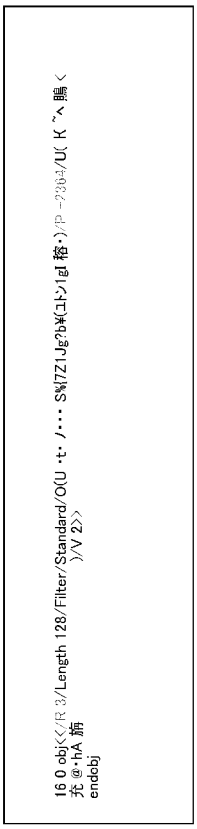
【図７】



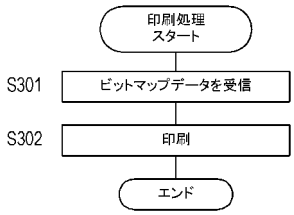
【図８】

Job No.	File Name	Status	Job Class	Owner	Date	…	Print	Edit	Header
…	…	…	…	…	…	…	…	…	…
123	aaa.doc	Printed	Print	AAA	20-Dec-03		Yes	Yes	Yes
124	bbb.xls	Printed	Print	AAA	15-Jan-04		Yes	Yes	Yes
125	ccc.pdf	Printed	Print	BBB	5-Mar-04		No	No	No
…	…	…	…	…	…	…	…	…	…

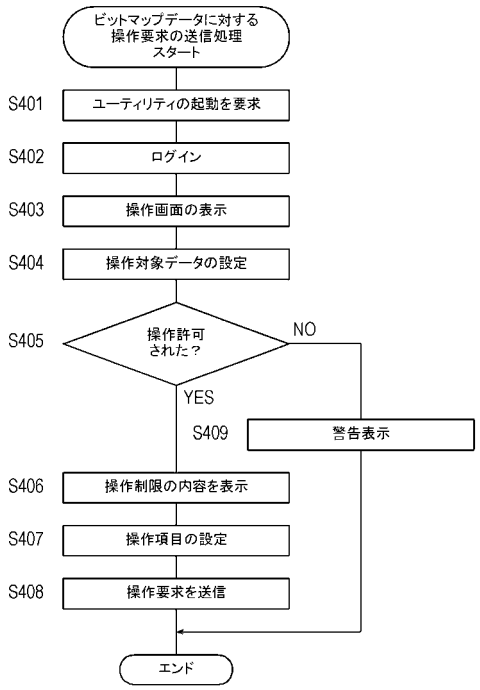
【図９】



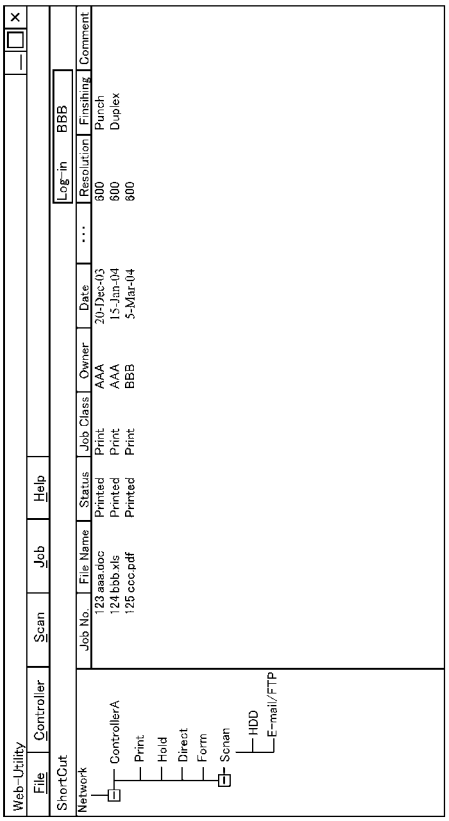
【図１０】



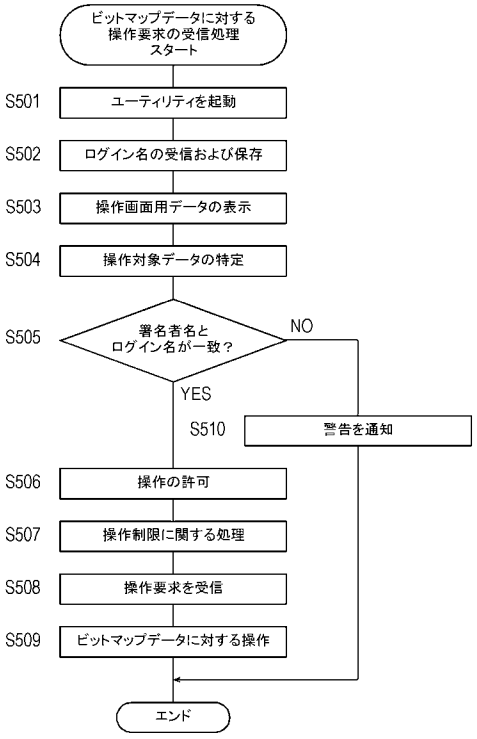
【図１１】


ビットマップデータに対する
操作要求の送信処理
スタート
S401
ユーティリティの起動を要求
S402
ログイン
S403
操作画面の表示
S404
操作対象データの設定
S405
操作許可
された？
NO
YES
S409
警告表示
S406
操作制限の内容を表示
S407
操作項目の設定
S408
操作要求を送信
エンド

【図１２】


Web-Utility
File
Controller
Scan
Job
Help
ShortCut
Network
ControllerA
Print
Hold
Direct
Form
Scan
HDD
E-mail/FTP
Log-in
BBB
Job No.
File Name
Status
Job Class
Owner
Date
...
Resolution
Finishing
Comment
123 aaa.doc
124 bbb.xls
125 ccc.pdf
Printed
Printed
Printed
Print
Print
Print
AAA
AAA
BBB
20-Dec-05
15-Jan-04
5-Mar-04
600
600
600
Punch
Duplex

【図１３】


ビットマップデータに対する
操作要求の受信処理
スタート
S501
ユーティリティを起動
S502
ログイン名の受信および保存
S503
操作画面用データの表示
S504
操作対象データの特定
S505
署名者名と
ログイン名が一致？
NO
YES
S510
警告を通知
S506
操作の許可
S507
操作制限に関する処理
S508
操作要求を受信
S509
ビットマップデータに対する操作
エンド

フロントページの続き

(72)発明者　小野　孝一
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
(72)発明者　新地　俊幹
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
(72)発明者　桜庭　保
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　CL08　HJ06　HK11　HN06　HN15