(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2010-3166
(P2010-3166A)
(43)公開日　平成22年1月7日(2010.1.7)

(51)Int.Cl.			F I			テーマコード（参考）
G06F	3/12	(2006.01)	G06F	3/12	K	2C061
H04N	1/387	(2006.01)	H04N	1/387		5B021
G06T	1/00	(2006.01)	G06T	1/00	500B	5B057
H04N	1/00	(2006.01)	H04N	1/00	107Z	5C062
B41J	29/00	(2006.01)	B41J	29/00	Z	5C076

審査請求 未請求　請求項の数 18　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願2008-162303 (P2008-162303)
(22)出願日　平成20年6月20日 (2008.6.20)

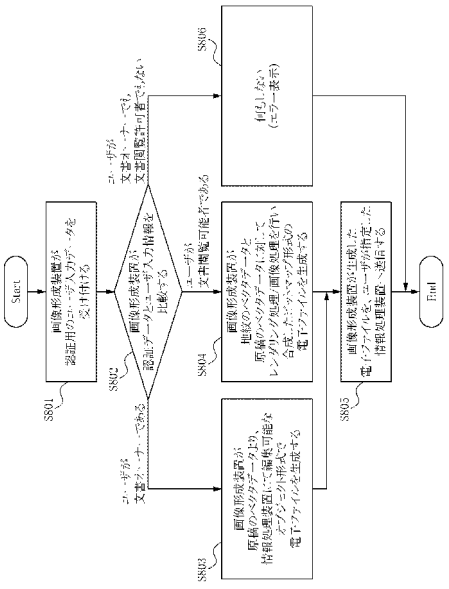
(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100090538
弁理士　西山　恵三
(74)代理人　100096965
弁理士　内尾　裕一
(72)発明者　小笠原　拓
東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

Ｆターム(参考)　2C061 AP01 AP07 BB10 CL10 HJ06
HJ08 HK11
5B021 AA01 NN00
5B057 AA20 CA12 CA16 CB12 CB16
CE08 CG07

最終頁に続く

(54)【発明の名称】画像形成装置及び画像形成方法

(57)【要約】
【課題】　画像形成装置が保存している地紋文書を情報処理装置へ電子ファイルとして送信する処理に関して、安全かつ実用的なセキュリティを施す。
【解決手段】　画像形成装置が記憶領域に保存された地紋文書をネットワークで接続された情報処理装置へ電子ファイルとして送信する処理において、認証を行い閲覧許可者には原稿と地紋を合成し情報処理装置にて編集不可能な電子ファイルを、文書オーナーに対しては情報処理装置にて編集可能な形式で電子ファイルを送信する。
【選択図】　図８



【特許請求の範囲】
【請求項１】
認証データを有する原稿データと地紋データとから構成される文書データを記憶領域に保存する保存手段と、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認手段と、
を備え、
該権限確認手段の結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、又は、前記地紋データと前記原稿データを前記情報処理装置において前記地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信手段、
を有することを特徴とする画像形成装置。
【請求項２】
前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルとは、ビットマップ形式のデータであることを特徴とする請求項１に記載の画像形成装置。
【請求項３】
認証データを有する原稿データと地紋データとから構成される印刷データを作成するデータ作成手段と、
前記印刷データを送信するデータ送信手段と、
を有することを特徴とする情報処理装置。
【請求項４】
認証データを有する原稿データと地紋データとから構成される印刷データを受信する受信手段を有し、
前記保存手段は更に
前記受信手段にて受信した印刷データを解析して、内部データを生成し、
該内部データを文書データとして保存することを特徴とする請求項１に記載の画像形成装置。
【請求項５】
前記保存手段は、更に
前記記憶領域に記憶されていて認証データを有していない文書データに対して地紋設定を行う地紋設定手段を有し、
該地紋設定が行われた文書を、認証データを有する原稿データと地紋データとで構成される文書データとして保存することを特徴とする請求項１に記載の画像形成装置。
【請求項６】
認証データを有する原稿データと地紋データとから構成された文書データを記憶領域に保存する保存手段と、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認手段と、
を備え、
該権限確認手段の結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、
又は、前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信手段、
を有することを特徴とする情報処理装置。
【請求項７】

前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルとは、ビットマップ形式のデータであることを特徴とする請求項６に記載の情報処理装置。
【請求項８】
画像形成装置と情報処理装置からなる画像形成システムにおいて、
前記画像形成装置は、
認証データを有する原稿データと地紋データから構成される文書データを、
前記認証データとユーザの権限に基づいて、
前記情報処理装置が編集可能なデータ形式のファイル、または、前記地紋データと前記原稿データを前記情報処理装置が編集不可能なイメージデータ形式のファイルで
前記情報処理装置へ送信することを特徴とする画像形成システム。
【請求項９】
認証データを有する原稿データと地紋データとから構成される文書データを記憶領域に保存する保存ステップと、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認ステップと、
を備え、
該権限確認ステップの結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、
又は、前記地紋データと前記原稿データを前記情報処理装置において前記地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信ステップ、
を有することを特徴とする画像形成方法。
【請求項１０】
前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルとは、ビットマップ形式のデータであることを特徴とする請求項９に記載の画像形成方法。
【請求項１１】
認証データを有する原稿データと地紋データとから構成される印刷データを作成するデータ作成ステップと、
前記印刷データを送信するデータ送信ステップと、
を有することを特徴とする情報処理方法。
【請求項１２】
認証データを有する原稿データと地紋データとから構成される印刷データを受信する受信ステップを有し、
前記保存ステップは更に
前記受信ステップにて受信した印刷データを解析して、内部データを生成し、
該内部データを文書データとして保存することを特徴とする請求項９に記載の画像形成方法。
【請求項１３】
前記保存ステップは、更に
前記記憶領域に記憶されていて認証データを有していない文書データに対して地紋設定を行う地紋設定ステップを有し、
該地紋設定が行われた文書を、認証データを有する原稿データと地紋データとで構成される文書データとして保存することを特徴とする請求項９に記載の画像形成方法。
【請求項１４】
認証データを有する原稿データと地紋データとから構成された文書データを記憶領域に保存する保存ステップと、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認

証データを比較する権限確認ステップと
を備え、
該権限確認ステップの結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、
又は、前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信ステップ、
を有することを特徴とする情報処理方法。
【請求項１５】
前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルとは、ビットマップ形式のデータであることを特徴とする請求項１４に記載の情報処理方法。
【請求項１６】
コンピュータに
認証データを有する原稿データと地紋データとから構成される文書データを記憶領域に保存する保存ステップと、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認ステップと、
を備え、
該権限確認ステップの結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、
又は、前記地紋データと前記原稿データを前記情報処理装置において前記地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信ステップ、
を実行させるためのプログラム。
【請求項１７】
コンピュータに
認証データを有する原稿データと地紋データとから構成された文書データを記憶領域に保存する保存ステップと、
前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認ステップと
を備え、
該権限確認ステップの結果に応じて、
前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、
又は、前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信する
送信ステップ、
を実行させるためのプログラム。
【請求項１８】
請求項１６又は１７に記載のプログラムを記憶したコンピュータで読み取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
地紋文書を取り扱うことが出来る画像形成装置とその制御方法に関するものである。
【背景技術】
【０００２】

従来の画像形成装置に関連したアクセス権による地紋制御については、情報処理装置がプリンタドライバ（不図示）によって地紋制御を施したものがある（例えば、特許文献１参照）。

【０００３】

この従来の地紋制御を行うシステムの構成図を図１０に示す。

１００１は管理サーバ、１００２は情報処理装置、１００３は画像形成装置である。

これらは、ＬＡＮ１００４によってネットワーク接続されている。

【０００４】

このシステムの情報処理装置において、地紋制御を行う際の処理手順を図１１のフローチャートに示す。

このフローチャートのＳ１１０１～１１０６における処理は、情報処理装置１００３におけるＣＰＵ（不図示）によって制御される。また、Ｓ１１０７は、情報処理装置１００２のＣＰＵ（不図示）によって制御される。

【０００５】

情報処理装置１００２より画像形成装置１００３へ印刷指示を行う場合（Ｓ１１０１）に、まず、情報処理装置１００２は管理サーバ１００１へ認証を要求する（Ｓ１１０２）。

認証処理（Ｓ１１０３）により、管理サーバ１００１に登録されているユーザであると判断された場合には、原稿に地紋パターンを付加した印刷データを作成する（Ｓ１１０４）。

認証処理（Ｓ１１０３）により、管理サーバ１００１に登録されていないユーザであると判断された場合には、地紋パターンを付加しない原稿の印刷データを作成する（Ｓ１１０５）。情報処理装置１００２は作成した印刷データを画像形成装置１００３へ送信する（Ｓ１１０６）。画像形成装置１００３は受診した印刷データを印刷する（Ｓ１１０７）。

これによって、ユーザ権限によって地紋パターンの付加／非付加が制御可能になる。

【０００６】

さらには認証したユーザＩＤを地紋へ埋め込むことが可能となり、地紋文書が流出した場合にそのユーザを特定することができる。

【０００７】

また、従来の画像形成装置が扱う地紋文書に対して出力形式の変更を施したものがある（例えば、特許文献２参照）。

【０００８】

この従来の地紋制御を行うシステムの構成図を図１２に示す。

１２０１は情報処理装置、１２０２は１２００ｄｐｉ解析度を有する画像形成装置、１２０３は６００ｄｐｉ解析度を有する画像形成装置である。

これらは、ＬＡＮ１２０４によってネットワーク接続されている。

【０００９】

このシステムの情報処理装置において、地紋制御を行う際の処理手順を図１３のフローチャートに示す。

このフローチャートの各ステップにおける処理は、情報処理装置１２０１のＣＰＵ（不図示）又は画像形成装置１２０２、１２０３のＣＰＵ（不図示）によって制御される。

【００１０】

画像形成装置１２０２、１２０３が情報処理装置１２０１より受信する地紋文書の印刷データは、原稿データと地紋ビットマップデータと地紋ベクタデータから構成される。画像形成装置１２０２、１２０３が、この印刷データを受信する（Ｓ１３０１）と地紋ビットマップデータの解像度を解析する（Ｓ１３０２）。

【００１１】

そして、印刷データ中の地紋ビットマップデータが解像度変換を行うことなく出力可能かを判断する（Ｓ１３０３）。

【００１２】

画像形成装置が出力可能と判断した場合は、原稿ビットマップデータと地紋ビットマップデータを合成し印刷を行う（Ｓ１３０４）。

【００１３】

例えば、情報処理装置から１２００ｄｐｉの解析度を有するデータを、画像形成装置１２０２が受信した場合、出力可能なので、原稿ビットマップデータと地紋ビットマップデータを合成し印刷を行う。

【００１４】

また、画像形成装置が、出力不可能と判断した場合には、地紋ベクタデータより出力可能な解像度の地紋ビットマップデータを作成する（Ｓ１３０５）。

【００１５】

例えば、情報処理装置から１２００ｄｐｉの解析度を有するデータを、画像形成装置１２０３が受信した場合、出力不可能なので、地紋ベクタデータより出力可能な解像度の地紋ビットマップデータを作成する。

【００１６】

そして、原稿ビットマップデータと作成した地紋ビットマップデータを合成し印刷を行う（Ｓ１３０６）。

【００１７】

これにより、解像度の差異により地紋が正しく印刷されないことを防止することができる。

つまり、出力先の条件によって地紋のパターンを変更できる。

【００１８】

しかしこの方法では、画像形成装置に一旦保存された地紋文書を、他の画像形成装置や情報処理装置へ送信する際に、地紋文書の印刷データから地紋ビットマップデータや地紋ベクタデータを削除するといった編集を行う。すると、本来地紋によって複製に対する牽制を行う必要のある機密文書を、権限のない者を含む誰に対しても原稿データのみが送信されてしまう可能性がある。

【００１９】

これを回避するために、例えば特許文献３などに示されるように画像形成装置が情報処理装置へ地紋文書等の複写禁止画像データを送信する際には、常に原稿と地紋の合成処理を強制する方法がある。

【特許文献１】特開２００４－０７８７５２

【特許文献２】特開２００７－３３１３１３

【特許文献３】特開２００７－１６６３０３

【発明の開示】

【発明が解決しようとする課題】

【００２０】

従来の地紋文書の制御方法に印刷に関しては情報処理装置において認証を行い、その結果により情報処理装置が原稿のみの印刷データを作成するか、原稿と地紋パターンを合成した印刷データを作成するかを選択し、画像形成装置へ送信を行っていた。

【００２１】

しかし情報処理装置で原稿と地紋パターンとを合成した印刷データを画像形成装置へ保存する方法では、画像形成装置で原稿データと地紋データに再び分離するのは困難であった。

【００２２】

また上述したように、画像形成装置が情報処理装置へ地紋文書を送信する際に常に原稿と地紋の合成処理を強制する方法では、本来原稿のみを取得したい文書オーナーに対しても原稿と地紋を合成したイメージデータを送信する。

このため、文書オーナーの利便性を制限してしまう問題があった。

【００２３】

本提案では、画像形成装置の記憶領域に保存された地紋文書を、画像形成装置がネット

ワークで接続された情報処理装置へ電子ファイルとして出力する際の上記問題を解決することを目的とする。

【００２４】

つまり、画像形成装置の記憶領域に地紋文書として保存された地紋文書を、情報処理装置へ送信する際、送信を指示するユーザの権限によってファイル形式を変更する。

【００２５】

具体的には、ユーザの権限によって地紋文書をビットマップ化する前であり文書が情報処理装置において編集可能なデータ形式のファイルで送信する。

【００２６】

又は、地紋文書の地紋データと原稿データを情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信することを目的とする。

【課題を解決するための手段】

【００２７】

前記課題を解決するため、本発明における画像形成装置は、

認証データを有する原稿データと地紋データとから構成される文書データを記憶領域に保存する保存手段と、前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認手段と、

を備え、該権限確認手段の結果に応じて、前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、又は、前記地紋データと前記原稿データを前記情報処理装置において前記地紋データに対して編集不可能なイメージデータ形式のファイルで送信する送信手段を有することを特徴とする。

【００２８】

また、前記課題を解決するため本発明における情報処理装置は、

認証データを有する原稿データと地紋データとから構成された文書データを記憶領域に保存する保存手段と、前記文書データを情報処理装置へ送信する際、該送信を指示するユーザの権限と前記認証データを比較する権限確認手段と、を備え、該権限確認手段の結果に応じて、前記文書データを、ビットマップ化する前であり前記文書データが前記情報処理装置において編集可能なデータ形式のファイルで送信する、又は、前記地紋データと前記原稿データを前記情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信する送信手段、を有することを特徴とする。

【発明の効果】

【００２９】

本発明によれば、画像形成装置が情報処理装置へ地紋文書を電子ファイルとして出力する場合に、送信を指示するユーザの権限によってファイル形式を変更することが可能になる。

【００３０】

即ち、ユーザの権限によって地紋文書をビットマップ化する前であり文書が情報処理装置において編集可能なデータ形式のファイルで送信する。

【００３１】

又は、地紋文書の地紋データと原稿データを情報処理装置において地紋データに対して編集不可能なイメージデータ形式のファイルで送信することが可能になる。

【００３２】

また、本発明によれば画像形成装置の記憶領域に保存される文書データが原稿データに加えて地紋データと認証データを保持するため、認証を行うための管理サーバや、地紋パターンを蓄積するデータベースを必要としない。

【００３３】

このため地紋文書に対する効果的なセキュリティを単純な構成により実現することが可能になる。

【発明を実施するための最良の形態】

【００３４】
（実施例１）
以下、本発明の前提となる画像形成システム構成及び処理の流れについて説明する。
【００３５】
図１は画像形成装置１０１と情報処理装置１０２がＬＡＮ１０３などのネットワークを介して互いに接続されている。
【００３６】
画像形成装置（ＭＦＰ：Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｅｒａｌ）１０１について説明する。
【００３７】
パネル１１１は、ユーザが画像形成装置１０１の各種設定を行うための操作部である。
【００３８】
ＣＰＵ１１２は画像形成装置１０１で行われる処理を統括的に制御する。
【００３９】
ＲＡＭ１１３はＣＰＵ１１２のワークエリアとして使用される。またデータの保存場所としても使用される。
【００４０】
ハードディスク（ＨＤＤ）１１４はソフトウェアや文書データ等を保存する。プリンタエンジン１１５は受信した画像データを出力用紙上に形成する。
【００４１】
スキャナ１１６は印刷物を光学的に読み取って電子的なイメージを作成する。通信インターフェース（Ｉ／Ｆ）１１７は、ＬＡＮ１０３を介して他装置とデータ送受信を行う。
【００４２】
情報処理装置１０２について説明する。
ＣＰＵ１２１は情報処理装置１０２で行われる処理を統括的に制御する。
ＲＡＭ１２２はＣＰＵ１２１のワークエリアとして使用される。
【００４３】
またデータの保存場所としても使用される。
ハードディスク（ＨＤＤ）１２３は、ソフトウェアやデータ等を保存する。
通信インターフェース１２４はネットワーク１０３を介して他装置とのデータ送受信を行う。
【００４４】
図２に本画像形成システム内に存在するソフトウェアモジュール及びハードウェアモジュールの概念図を示す。
【００４５】
まず、画像形成装置１０１におけるのソフトウェアモジュール及びハードウェアモジュールの概念図について説明する。
これらは、ＣＰＵ１１２によって制御される。
【００４６】
データ受信部２０２は通信インターフェース１１７を介して外部装置からデータを受信する。
【００４７】
データ送信部２０７はネットワークに接続された外部装置に対して通信インターフェース１１７を介してデータを送信する。
【００４８】
ＰＤＬ解析部（インタプリタ）２０３は受信した印刷データの解釈を行い、内部データ生成部２０４が当該解釈より内部（中間言語）データを生成する。
【００４９】
レンダラ２０５は内部データをビットマップ展開しイメージデータを作成する。制御部２０１では後述する本発明のアクセス権による地紋文書制御を含む処理を行う。

【００５０】
次に、情報処理装置１０２におけるのソフトウェアモジュール及びハードウェアモジュールの概念図について説明する。
これらは、ＣＰＵ１２１によって制御される。
【００５１】
ハードディスク（ＨＤＤ）１２３又は図１に示すＲＡＭ１２２にはデータが保存され、これらのデータはプリンタドライバ２１１により印刷可能である。
【００５２】
図３に、地紋を設定する対象の原稿を情報処理装置１０２から画像形成装置１０１に送信するフローチャートを示す。
フローチャートにおけるすべての動作は、情報処理装置内のＣＰＵ１２１によって制御される。
【００５３】
情報処理装置は印刷設定画面にてユーザより原稿に対する地紋の設定を受け付ける（Ｓ３０１）。
【００５４】
情報処理装置は印刷設定画面にてユーザより、文書オーナーのパスワードと文書管理閲覧者のパスワード設定を受け付ける（Ｓ３０２）。
【００５５】
この地紋設定に使用する情報処理装置のＵＩ画面構成を図６に示す。
【００５６】
これは後述する画像形成装置の操作部パネル１１１における地紋設定画面構成も同じである。
【００５７】
画面６０１は一般的な地紋設定である、印字する文字列、印字する文字列サイズ、文字列の向き、文字列を白抜きにするか否か、背景模様、文字／背景のコントラスト調整等の設定欄から構成される。
【００５８】
これに加えて、文書オーナーのパスワード設定欄６０２と文書閲覧許可者のパスワード設定欄６０３とから構成される。
【００５９】
情報処理装置１０２は、原稿ＰＤＬデータと地紋ＰＤＬデータと認証データとから印刷データ作成をする（Ｓ３０３）。
【００６０】
情報処理装置１０２は作成した印刷データを画像形成装置１０１へ送信する（Ｓ３０４）。
【００６１】
図４に画像形成装置１０１が受信した印刷データを記憶領域であるＲＡＭ１１３に保存するフローチャートを示す。
【００６２】
画像形成装置１０１は、情報処理装置１０２より送信された印刷データを受信する（Ｓ４０１）。
【００６３】
画像形成装置１０１は、受信した印刷データに対してＰＤＬ解析を行い、原稿のベクタデータと地紋のベクタデータを生成する（Ｓ４０２）。
【００６４】
画像形成装置１０１は原稿のベクタデータと地紋のベクタデータと認証データから構成される文書データを作成する（Ｓ４０３）。
【００６５】
画像形成装置１０１は作成した文書データを記憶領域に保存する（Ｓ４０４）。

【００６６】
図７に画像形成装置１０１の記憶領域に保存される文書データ構成図を示す。
【００６７】
画像形成装置１０１の記憶領域に保存される文書データ７０１は、認証データ７０２を有する原稿のベクタデータ７０３と地紋のベクタデータ７０４とより構成される。
【００６８】
ベクタデータとは画像形成装置１０１における内部処理のためのデータフォーマットであり、原稿のベクタデータ７０３は原稿の描画に使用され、地紋のベクタデータ７０４は地紋パターンの描画に使用される。
【００６９】
認証データ７０２は、画像形成装置１０１がユーザ操作によりＰＣなどの情報処理装置１０２へ文書データ７０１を電子ファイルとして出力する場合に、アクセス権の確認に使用される。
【００７０】
認証データ７０２は、文書オーナー用のパスワードと文書閲覧可能者用のパスワードで構成される。
【００７１】
画像形成装置１０１における認証及び文書データの出力方法は図８のフローチャートへ示す。
【００７２】
なお、認証データ７０２は、文書オーナーと文書閲覧可能者以外のパスワードが含まれてもよい。
【００７３】
また、地紋を付加する原稿は、上述したように情報処理装置１０２にて作成される必要はない。
【００７４】
画像形成装置１０１の記憶領域に保存された原稿に対して地紋設定を付加することもできる。
【００７５】
この場合について、図５に示す。
【００７６】
図５は、画像形成装置１０１が記憶領域に保存した原稿から構成される文書データに地紋設定を行うフローチャートを示す。
【００７７】
画像形成装置１０１が地紋付与の設定を受け付ける（Ｓ５０１）。
【００７８】
設定する情報としてはまず一般的な地紋設定である。
【００７９】
例えば、印字する文字列、印字する文字列サイズ、文字列の向き、文字列を白抜きにするか否か、背景模様、文字／背景のコントラスト調整等である。
【００８０】
これらの地紋設定に加えて、画像形成装置は文書オーナーのパスワードと文書閲覧可能者のパスワードを受け付ける（Ｓ５０２）。
【００８１】
上述した図６にこれらの地紋設定に使用する画像形成装置１０２の操作部を示す。画像形成措置１０２は、受け付けた地紋設定より地紋のベクタデータ７０４を作成する。
【００８２】
さらに画像形成装置１０１は原稿のベクタデータ７０３と地紋のベクタデータ７０４と認証データ７０２より文書データを構成する（Ｓ５０３）。
【００８３】

画像形成装置１０１は作成した文書データ７０１を記憶領域に保存する（Ｓ５０４）。
【００８４】
図８に画像形成装置１０１が地紋文書を情報処理装置１０２へ送信するフローチャートを示す。
【００８５】
画像形成装置１０１の記憶領域には文書データ７０１が保存されている。
画像形成装置１０１は、送信された文書データ７０１が認証データ７０２を保持する場合には、認証のためユーザより入力データを受け付ける（Ｓ８０１）。
画像形成装置１０１は文書データ７０１の認証データ７０２とユーザ入力データを比較する（Ｓ８０２）。これにより、文書データに対するユーザの権限確認が行われる。
【００８６】
権限確認の結果、画像形成装置１０１がユーザ入力データと文書オーナーのパスワードが一致すると判断した場合、Ｓ８０３へ進む。
【００８７】
Ｓ８０３では、画像形成装置１０１は情報処理装置１０１においてユーザが原稿のベクタデータ７０３を編集可能なオブジェクト形式で電子ファイルを生成する。
即ち、情報処理装置１０２では、原稿のベクタデータ７０３と地紋のベクタデータ７０４を分離するといった編集が可能となる。
【００８８】
この電子ファイルを図９の９０１へ示す。
【００８９】
Ｓ８０２の認証で、画像形成装置１０１がユーザ入力データと文書閲覧可能者のパスワードが一致すると判断した場合、Ｓ８０４へ進む。
【００９０】
Ｓ８０４では、画像形成装置１０１は地紋のベクタデータと原稿のベクタデータに対してレンダリング処理及び画像処理を行い合成しビットマップ化した電子ファイルを生成する。
【００９１】
この場合、情報処理装置１０２では、原稿データと地紋データはビットマップ上で合成されているので、原稿から地紋を取り除くといった地紋データに対する編集は不可能となる。
【００９２】
この電子ファイルを図９の９０４へ示す。
【００９３】
Ｓ８０５では、以上のようにデータ形式を変換して生成された電子ファイルを、画像形成装置１０１は、ユーザが指定した情報処理装置へ送信する。
【００９４】
Ｓ８０３の認証において、ユーザ入力データが文書データの保持する認証データ７０２のいずれにも一致しない場合は、８０６へ進む。
【００９５】
Ｓ８０６では、文書ファイルを情報処理装置１０２へ送信しない。
【００９６】
なお、この場合画像形成装置１０１は、操作部にパスワード不一致により送信できない旨を表示してもよい。
【００９７】
また、画像形成装置１０１は記憶領域に保存されている文書データ７０１を印刷することも可能である。
【００９８】
図９は、画像形成装置１０１によって生成される文書ファイルである。
【００９９】

９０１は画像形成装置１０１によって図８におけるＳ８０３で生成される電子ファイルである。
電子ファイル９０１はＰＣなどの情報処理装置１０２で編集可能であり、例えばユーザは原稿９０２の編集や、貼り付けたイメージ図である９０３を別のイメージ図に変更することができる。
９０４は画像形成装置１０１によって図８におけるＳ８０４で生成される電子ファイルである。
電子ファイル９０４は、原稿と地紋が合成されたビットマップ形式の電子ファイルである。

【０１００】
このため、この電子ファイルが画像形成装置１０１よりＰＣなどの情報処理装置１０２へ出力され、この電子ファイルを受信した情報処理装置にて、ユーザがこの電子ファイルの編集を行うことは不可能である。

【０１０１】
例えばユーザは原稿の改竄や、地紋の削除を行えないため、機密文書として一定のセキュリティが保つことができる。

【０１０２】
この電子ファイルは所謂一般的な地紋文書であり、複写が行われた場合には背景に埋め込まれた「Ｃｏｎｆｉｄｅｎｔｉａｌ」などのコピー牽制文字列が浮き上がり、不正なコピーを抑制する。

【０１０３】
なお、ここで地紋に対して編集不可能と表現されているのは、地紋データに対して削除を行うことが不可能ということを意味している。

【０１０４】
これにより、画像形成装置１０１が情報処理装置１０２へ地紋文書を電子ファイルとして出力する場合に、文書オーナーであれば認証後に情報処理装置１０１にて編集可能なデータ形式で原稿を出力することができる。

【０１０５】
また文書閲覧許可者であれば、原稿と地紋パターンが合成されたイメージデータ形式で情報処理装置１０２にて編集不可能な電子ファイルを得ることができる。

【０１０６】
つまり、画像形成装置１０１は機密文書を情報処理装置１０２へ出力指示を行った人が、文書閲覧可能者の場合は地紋付与した編集不可能な電子ファイルとして出力する。

【０１０７】
一方で、画像形成装置１０１は機密文書を情報処理装置１０２へ出力指示を行った人が文書オーナーの場合は編集可能な電子ファイルとして出力するといった安全かつ実用的なセキュリティを施すことができる。

【０１０８】
また、画像形成装置１０１の記憶領域に保存される文書データが原稿データに加えて地紋データと認証データを保持するため、認証を行うための管理サーバや、地紋パターンを蓄積するデータベースを必要としない。

【０１０９】
このため地紋文書に対する効果的なセキュリティを単純な構成により実現することが可能である。

【０１１０】
（実施例２）
本実施例２では機密文書を情報処理装置が保存・出力する場合について説明する。

【０１１１】
実施例１の画像処理装置における処理を情報処理装置で行うものである。

【０１１２】

図１４に本実施列の構成を示す。本実施例では機密文書を保持・出力する情報処理装置であるサーバ装置１４０１と文書を受け取る情報処理装置であるクライアント装置２０１がＬＡＮ１０３などのネットワークを介して互いに接続されている。

【０１１３】

サーバ装置１４０１について説明する。ＣＰＵ１４０２はサーバ装置で行われる処理を統括的に制御する。ＲＡＭ１４０３はＣＰＵ１４０２のワークエリアとして使用される。またデータの保存場所としても使用される。ハードディスク（ＨＤＤ）１４０４は、ソフトウェアやデータ等を保存する。通信インターフェース１４０５はネットワーク１０３を介して他装置とのデータ送受信を行う。

【０１１４】

クライアント装置２０１に関しては実施例１で示した情報処理装置１０２と同様である。

【０１１５】

図１５にサーバ装置１４０１が地紋文書をクライアント装置２０１へ送信するフローチャートを示す。

【０１１６】

サーバ装置１４０１の記憶領域には文書データ７０１が保存されている。文書データ７０１は実施例１で述べたように、認証データ７０２を有する原稿のベクタデータ７０２と地紋のベクタデータ７０３とより構成される。サーバ装置１４０１は送信を指示された文書データ７０１が認証データ７０２を保持する場合に認証のためユーザより入力データを受け付ける（Ｓ１５０１）。サーバ装置１４０１は文書データ７０１の認証データ７０２とユーザ入力データを比較する（Ｓ１５０２）。

【０１１７】

サーバ装置１４０１がユーザ入力データと文書オーナーのパスワードが一致すると判断した場合、サーバ装置１４０１は原稿のベクタデータ７０３よりクライアント装置２０１においてユーザが編集可能なオブジェクト形式で電子ファイルを生成する（Ｓ１５０３）。この電子ファイルを図９の９０１に示す。

【０１１８】

Ｓ１５０２で、サーバ装置１４０１がユーザ入力データと文書閲覧可能者のパスワードが一致すると判断した場合、サーバ装置１４０１は地紋のベクタデータと原稿のベクタデータに対してレンダリング処理及び画像処理を行う。

【０１１９】

即ち、この２つのデータを合成して、ビットマップ形式の電子ファイルを生成する（Ｓ１５０４）。この電子ファイルを図９の９０４に示す。サーバ装置１４０１は、生成した電子ファイルをユーザが指定したクライアント装置２０１へ送信する（Ｓ１５０５）。

【０１２０】

上記に示したようにクライアント装置２０１にて、この電子ファイル中の地紋データを削除することは不可能である。

【０１２１】

Ｓ１５０３の認証において、ユーザ入力データが文書データの保持する認証データ７０２のいずれにも一致しない場合は、文書ファイルをクライアント装置２０１へ送信しない。

【０１２２】

なお、この場合は、クライアント装置２０１は画面上にパスワード不一致により送信できない旨を表示してもよい。

【０１２３】

これにより、サーバ装置１４０１がクライアント装置２０１へ地紋文書を電子ファイルとして出力する場合に、文書オーナーであれば認証後にクライアント装置２０１にて編集可能なデータ形式で原稿を出力することができる。

【０１２４】

また文書閲覧許可者であれば、原稿と地紋パターンが合成されたイメージデータ形式でクライアント装置２０１にて編集不可能な電子ファイルを得ることができる。

【０１２５】

つまり、サーバ装置１４０１は、機密文書をクライアント装置２０１へ出力指示を行った人が文書閲覧可能者の場合は、クライアント装置２０１へ地紋付与した編集不可能な電子ファイルを出力する。

【０１２６】

一方で、サーバ装置１４０１において、機密文書をクライアント装置２０１へ出力指示を行った人が文書オーナーの場合は、クライアント装置２０１へ編集可能な電子ファイルを出力すること。

【０１２７】

以上によって、安全かつ実用的なセキュリティを提供することができる。

【０１２８】

また、サーバ装置１４０１の記憶領域に保存される文書データが原稿データに加えて地紋データと認証データを保持するため、認証を行うための管理サーバや、地紋パターンを蓄積するデータベースを必要としない。

【０１２９】

このため地紋文書に対する効果的なセキュリティを単純な構成により実現することが可能である。

【０１３０】

「本発明の他の実施形態」

前述した実施形態の機能を実現するように前述した実施形態の構成を動作させるプログラムを記憶媒体に記憶させ、該記憶媒体に記憶されたプログラムをコードとして読み出し、コンピュータにおいて実行する処理方法も上述の実施形態の範疇に含まれる。また、前述のプログラムが記憶された記憶媒体はもちろんそのプログラム自体も上述の実施形態に含まれる。

【０１３１】

かかる記憶媒体としてはたとえばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性メモリカード、ＲＯＭを用いることができる。

【０１３２】

また前述の記憶媒体に記憶されたプログラム単体で処理を実行しているものに限らず、他のソフトウェア、拡張ボードの機能と共同して、ＯＳ上で動作し前述の実施形態の動作を実行するものも前述した実施形態の範疇に含まれる。

【図面の簡単な説明】

【０１３３】

【図１】本画像形成システムのシステム構成図

【図２】本画像形成システムのソフトウェア及びハードウェアを概念的に表した図

【図３】情報処理装置における地紋文書の作成処理を示すフローチャート

【図４】画像形成装置が地紋文書を記憶領域に保存するフローチャート

【図５】画像形成装置が記憶領域に保存された文書データに地紋設定を行うフローチャート

【図６】画像形成装置にて文書データへ地紋設定を行う操作部を表す図

【図７】画像形成装置に保存される文書データを示す図

【図８】画像形成装置における地紋文書に対する処理を示すフローチャート

【図９】画像形成装置が出力する電子ファイルを示す図

【図１０】従来のアクセス権による地紋制御の構成図

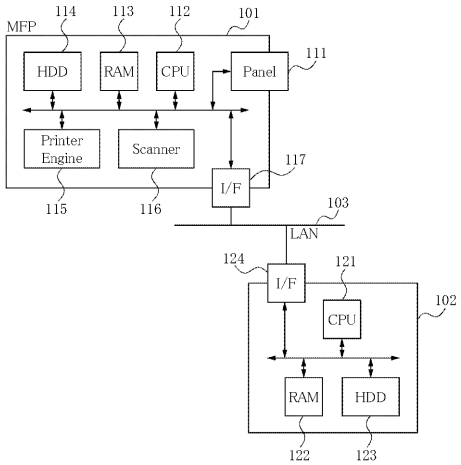
【図１１】従来のアクセス権による地紋制御のフローチャート

【図１２】従来の地紋文書の出力形式を変換する構成図

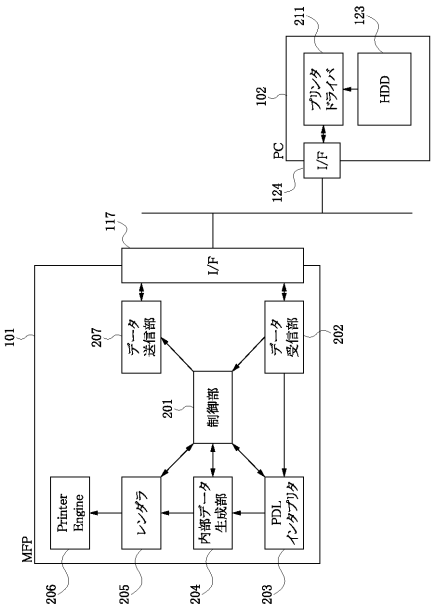
【図１３】従来の地紋文書の出力形式を変換するフローチャート

【図１４】本画像形成システムの実施例２におけるシステム構成図
【図１５】サーバ装置における地紋文書に対する処理を示すフローチャート

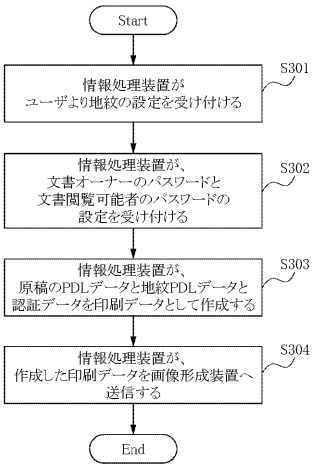
【図１】



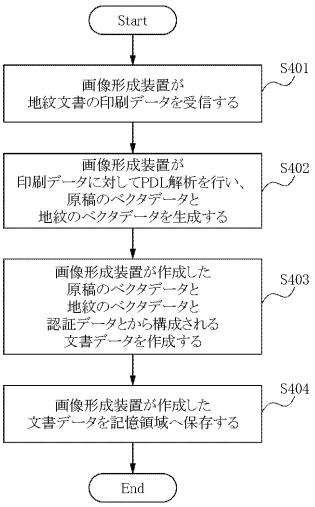
【図２】



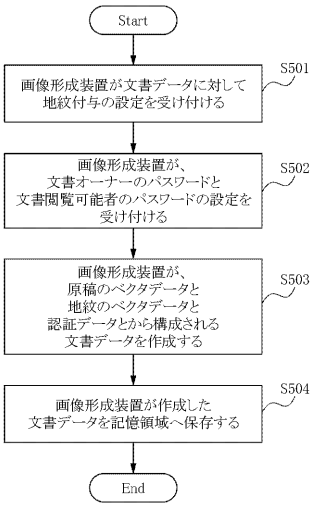
【図３】


Start
情報処理装置が
ユーザより地紋の設定を受け付ける
S301
情報処理装置が、
文書オーナーのパスワードと
文書閲覧可能者のパスワードの
設定を受け付ける
S302
情報処理装置が、
原稿のPDLデータと地紋PDLデータと
認証データを印刷データとして作成する
S303
情報処理装置が、
作成した印刷データを画像形成装置へ
送信する
S304
End

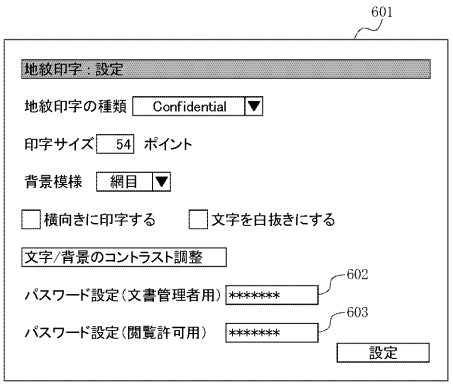
【図４】


Start
画像形成装置が
地紋文書の印刷データを受信する
S401
画像形成装置が
印刷データに対してPDL解析を行い、
原稿のベクタデータと
地紋のベクタデータを生成する
S402
画像形成装置が作成した
原稿のベクタデータと
地紋のベクタデータと
認証データとから構成される
文書データを作成する
S403
画像形成装置が作成した
文書データを記憶領域へ保存する
S404
End

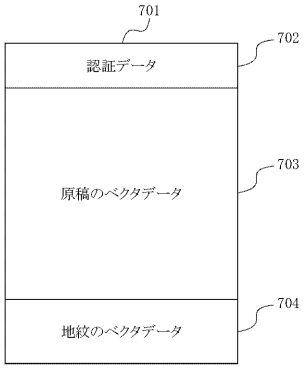
【図５】


Start
画像形成装置が文書データに対して
地紋付与の設定を受け付ける
S501
画像形成装置が、
文書オーナーのパスワードと
文書閲覧可能者のパスワードの設定を
受け付ける
S502
画像形成装置が、
原稿のベクタデータと
地紋のベクタデータと
認証データとから構成される
文書データを作成する
S503
画像形成装置が作成した
文書データを記憶領域へ保存する
S504
End

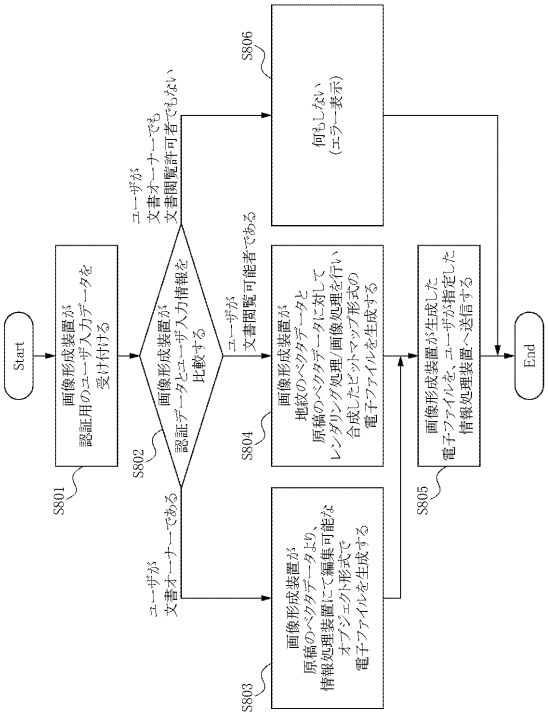
【図６】


601
地紋印字：設定
地紋印字の種類
Confidential
印字サイズ
54
ポイント
背景模様
網目
横向きに印字する
文字を白抜きにする
文字/背景のコントラスト調整
パスワード設定（文書管理者用）
602
****
パスワード設定（閲覧許可用）
603
****
設定

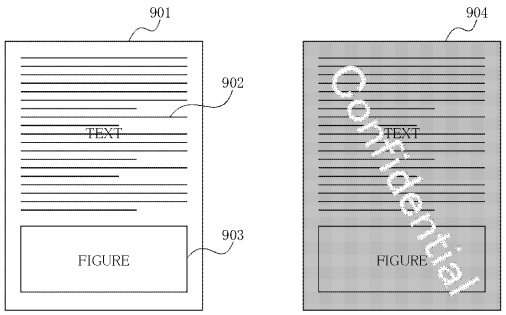
【図７】


701
認証データ
702
原稿のベクタデータ
703
地紋のベクタデータ
704

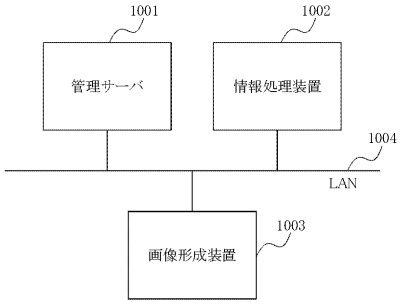
【図８】


Start
画像形成装置が
認証用のユーザ入力データを
受け付ける
S801
画像形成装置が
認証データとユーザ入力情報を
比較する
S802
ユーザが
文書閲覧可能者である
ユーザが
文書オーナーである
ユーザが
文書オーナーでも
文書閲覧許可者でもない
何もしない
(エラー表示)
S806
画像形成装置が
地紋のベクタデータと
原稿のベクタデータに対して
レンダリング処理/画像処理を行い
合成したビットマップ形式の
電子ファイルを生成する
S804
画像形成装置が
原稿のベクタデータより、
情報処理装置にて編集可能な
オブジェクト形式で
電子ファイルを生成する
S803
画像形成装置が生成した
電子ファイルを、ユーザが指定した
情報処理装置へ送信する
S805
End

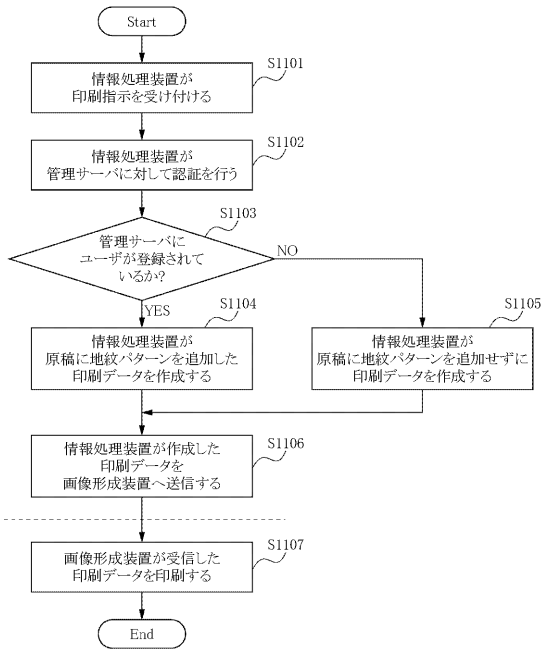
【図９】


901
902
TEXT
903
FIGURE
904
Confidential
TEXT
FIGURE

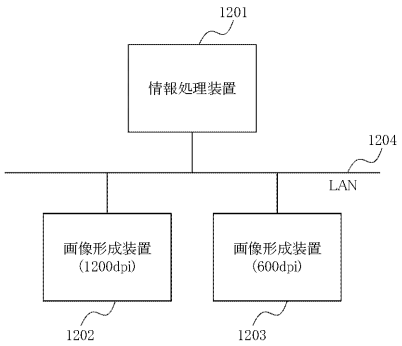
【図１０】


1001
管理サーバ
1002
情報処理装置
1004
LAN
1003
画像形成装置

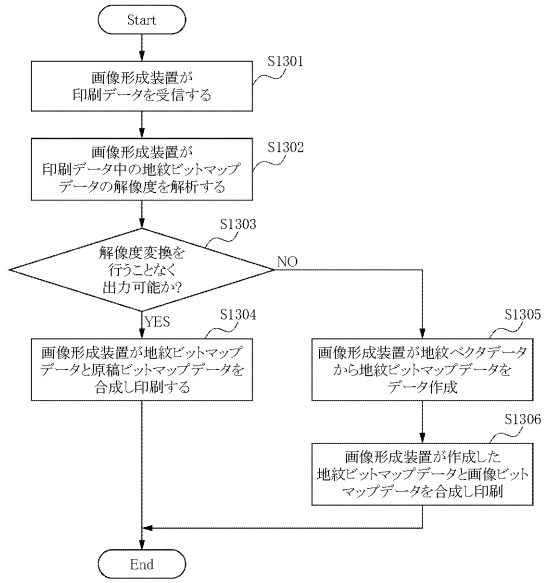
【図１１】



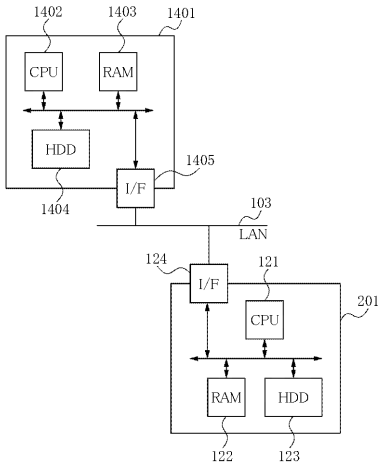
【図１２】



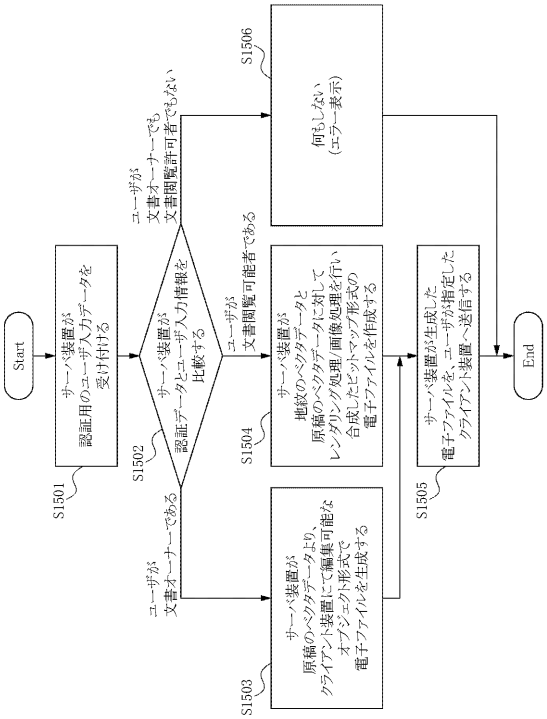
【図１３】



【図１４】



【図１５】


Start
サーバ装置が
認証用のユーザ入力データを
受け付ける
S1501
サーバ装置が
認証データとユーザ入力情報を
比較する
S1502
ユーザが
文書オーナーである
ユーザが
文書オーナーでも
文書閲覧許可者でもない
ユーザが
文書閲覧可能者である
S1503
サーバ装置が
原稿のベクタデータより、
クライアント装置にて編集可能な
オブジェクト形式で
電子ファイルを生成する
S1504
サーバ装置が
指紋のベクタデータと
原稿のベクタデータに対して
レンダリング処理/画像処理を行い
合成したビットマップ形式の
電子ファイルを作成する
S1506
何もしない
(エラー表示)
S1505
サーバ装置が生成した
電子ファイルを、ユーザが指定した
クライアント装置へ送信する
End

フロントページの続き

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

Ｆターム(参考) 5C062 AA05 AA14 AA35 AB11 AB42 AC22 AC24 AC38 AF14
5C076 AA14 BA06 CA10