(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4954022号
(P4954022)
(45)発行日　平成24年6月13日(2012.6.13)　(24)登録日　平成24年3月23日(2012.3.23)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 21/24 160A
G06F 3/12 (2006.01)　G06F 21/24 163A
G06F 3/12 K

請求項の数 10　(全 15 頁)

(21)出願番号　特願2007-287419 (P2007-287419)
(22)出願日　平成19年11月5日 (2007.11.5)
(65)公開番号　特開2009-116524 (P2009-116524A)
(43)公開日　平成21年5月28日 (2009.5.28)
審査請求日　平成22年11月5日 (2010.11.5)

(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　100125254
弁理士　別役　重尚
(72)発明者　佐光　律人
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

審査官　和田　財太

(56)参考文献　特開２００８－１２９７４９（ＪＰ，Ａ）
特開２００２－０７３６１９（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理装置の制御方法、および情報処理装置の制御プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークを介して外部装置と通信可能な情報処理装置であって、
前記外部装置から電子データを受信する受信手段と、
前記受信手段が受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録手段と、
前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、
前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、前記登録手段によるインデックス情報の登録を行い、前記受信手段が受信した電子データが機密データであると判定した場合は、前記登録手段によるインデックス情報の登録を行わないように制御する制御手段とを備え、
前記判定手段は、前記受信手段が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信手段が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置。
【請求項２】
ネットワークを介して外部装置と通信可能な情報処理装置であって、
前記外部装置から電子データを受信する受信手段と、
前記受信手段が受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録手段と、

前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、
前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、前記登録手段によるインデックス情報の登録を行い、前記受信手段が受信した電子データが機密データであると判定した場合は、前記登録手段によるインデックス情報の登録を行わないように制御する制御手段とを備え、
前記判定手段は、前記受信手段が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信手段が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置。

【請求項３】
ネットワークを介して外部装置と通信可能な情報処理装置であって、
前記外部装置から電子データを受信する受信手段と、
前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、
前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信手段が受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存手段とを備え、
前記判定手段は、前記受信手段が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信手段が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置。

【請求項４】
ネットワークを介して外部装置と通信可能な情報処理装置であって、
前記外部装置から電子データを受信する受信手段と、
前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、
前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信手段が受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存手段とを備え、
前記判定手段は、前記受信手段が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信手段が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置。

【請求項５】
パスワードを入力する入力手段と、
前記入力手段により入力されたパスワードが、前記受信手段が受信した電子データに含まれるパスワードと一致した場合に、当該電子データを印刷する印刷手段とを更に備えることを特徴とする請求項２又は４に記載の情報処理装置。

【請求項６】
ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、
前記外部装置から電子データを受信する受信工程と、
前記受信工程で受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録工程と、
前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、
前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、前記登録工程におけるインデックス情報の登録を行い、前記受信工程で受信した電子データが機密データであると判定した場合は、前記登録工程におけるインデックス情報の登録を行わないよう制御する制御工程とを備え、
前記判定工程では、前記受信工程が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信工程が暗号化通信を用いずに前

記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置の制御方法。
【請求項７】
ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、
前記外部装置から電子データを受信する受信工程と、
前記受信工程で受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録工程と、
前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、
前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、前記登録工程におけるインデックス情報の登録を行い、前記受信工程で受信した電子データが機密データであると判定した場合は、前記登録工程におけるインデックス情報の登録を行わないよう制御する制御工程とを備え、
前記判定工程は、前記受信工程が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信工程が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置の制御方法。
【請求項８】
ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、
前記外部装置から電子データを受信する受信工程と、
前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、
前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信工程で受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存工程とを備え、
前記判定工程は、前記受信工程が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信工程が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置の制御方法。
【請求項９】
ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、
前記外部装置から電子データを受信する受信工程と、
前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、
前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信工程で受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存工程とを備え、
前記判定工程は、前記受信工程が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信工程が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする情報処理装置の制御方法。
【請求項１０】
請求項６乃至９の何れか１項に記載の情報処理装置の制御方法をコンピュータにより実行させるためのコンピュータで読み取り可能な制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子データを複数のユーザで共有する機能を有する情報処理装置、情報処理装置の制御方法、および情報処理装置の制御プログラムに関する。
【背景技術】
【０００２】

従来、外部装置から受信した電子データを印刷するとともに、印刷された電子データを装置内に保存し、複数のユーザが保存した電子データを参照、共有することにより電子データを有効利用する情報処理装置がある。

【０００３】

このような情報処理装置では、電子データを効率的に収集するために、外部装置から受信した電子データを自動的に装置内に蓄積している。また、ユーザが所望の電子データを容易に取得できるようにするため、電子データを蓄積する際に、属性情報を電子データと関連付けて自動的に装置内に保存している。これにより、ユーザは、属性情報をキーとして、所望の電子データを検索することが可能となる。

【０００４】

しかし、このような情報処理装置では、受信した電子データに関する属性情報を自動的に蓄積するため、機密性の高いセキュアな電子データを誤って不特定数のユーザと共有してしまう可能性がある。また、特に登録された電子データをネットワークを介して参照することが可能な場合は、この問題はより深刻なものとなる。また、このような問題に対処するために、電子データの登録時に機密保護コードを入力することが考えられているが、その入力作業が煩雑である。

【０００５】

さらに、電子データに「禁複写」や「社外秘」等の情報が印刷されているか否かを判断し、この判断結果に応じて、コード情報部の機密保護項目にフラグを立て、このフラグに応じて検索や出力を制限する情報処理装置が提案されている（特許文献１）。

【特許文献１】特開平５－１８９５３８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

しかし、上記特許文献１では、受信した電子データに「禁複写」、「社外秘」等の情報が印刷されていない限り、電子データへのアクセスを制限することはできず、機密性の高いセキュアな電子データを誤って不特定数のユーザと共有してしまう可能性がある。

【０００７】

そこで、本発明は、電子データを効率よく収集することができると共に、機密性の高いセキュアな電子データを不特定数のユーザと共有してしまうことを回避することができる情報処理装置、該装置の制御方法及び制御プログラ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】

【０００８】

上記目的を達成するために、本発明の情報処理装置は、ネットワークを介して外部装置と通信可能な情報処理装置であって、前記外部装置から電子データを受信する受信手段と、前記受信手段が受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録手段と、前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、前記登録手段によるインデックス情報の登録を行い、前記受信手段が受信した電子データが機密データであると判定した場合は、前記登録手段によるインデックス情報の登録を行わないように制御する制御手段とを備え、前記判定手段は、前記受信手段が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信手段が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置は、ネットワークを介して外部装置と通信可能な情報処理装置であって、前記外部装置から電子データを受信する受信手段と、前記受信手段が受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録手段と、前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、前記判定手段による判定の結果、前記受

信手段が受信した電子データが機密データでないと判定した場合は、前記登録手段によるインデックス情報の登録を行い、前記受信手段が受信した電子データが機密データであると判定した場合は、前記登録手段によるインデックス情報の登録を行わないように制御する制御手段とを備え、前記判定手段は、前記受信手段が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信手段が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置は、ネットワークを介して外部装置と通信可能な情報処理装置であって、前記外部装置から電子データを受信する受信手段と、前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信手段が受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存手段とを備え、前記判定手段は、前記受信手段が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信手段が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置は、ネットワークを介して外部装置と通信可能な情報処理装置であって、前記外部装置から電子データを受信する受信手段と、前記受信手段が受信した電子データが機密データであるか否かを判定する判定手段と、前記判定手段による判定の結果、前記受信手段が受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信手段が受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存手段とを備え、前記判定手段は、前記受信手段が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信手段が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置の制御方法は、ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、前記外部装置から電子データを受信する受信工程と、前記受信工程で受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録工程と、前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、前記登録工程におけるインデックス情報の登録を行い、前記受信工程で受信した電子データが機密データであると判定した場合は、前記登録工程におけるインデックス情報の登録を行わないよう制御する制御工程とを備え、前記判定工程では、前記受信工程が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信工程が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置の制御方法は、ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、前記外部装置から電子データを受信する受信工程と、前記受信工程で受信した電子データを検索するために用いられるインデックス情報を、当該電子データに関連付けて登録する登録工程と、前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、前記登録工程におけるインデックス情報の登録を行い、前記受信工程で受信した電子データが機密データであると判定した場合は、前記登録工程におけるインデックス情報の登録を行わないよう制御する制御工程とを備え、前記判定工程は、前記受信工程が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信工程が受信した電子データにパスワードが含まれない場合は当該電子データが

機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置の制御方法は、ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、前記外部装置から電子データを受信する受信工程と、前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信工程で受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存工程とを備え、前記判定工程は、前記受信工程が暗号化通信を用いて前記電子データを受信した場合は当該電子データが機密データであると判定し、前記受信工程が暗号化通信を用いずに前記電子データを受信した場合は当該電子データが機密データでないと判定することを特徴とする。

上記目的を達成するために、本発明の情報処理装置の制御方法は、ネットワークを介して外部装置と通信可能な情報処理装置の制御方法であって、前記外部装置から電子データを受信する受信工程と、前記受信工程で受信した電子データが機密データであるか否かを判定する判定工程と、前記判定工程における判定の結果、前記受信工程で受信した電子データが機密データでないと判定した場合は、当該受信した電子データを検索対象のデータとして保存し、前記受信工程で受信した電子データが機密データであると判定した場合は、当該受信した電子データを検索非対象のデータとして保存する保存工程とを備え、前記判定工程は、前記受信工程が受信した電子データにパスワードが含まれる場合は当該電子データが機密データであると判定し、前記受信工程が受信した電子データにパスワードが含まれない場合は当該電子データが機密データでないと判定することを特徴とする。

【発明の効果】

【００１１】

本発明によれば、電子データを効率よく収集することができると共に、機密性の高いセキュアな電子データを誤って不特定数のユーザと共有してしまうことを回避することができる。

【発明を実施するための最良の形態】

【００１２】

以下、本発明の実施の形態の一例を図面を参照して説明する。

【００１３】

図１は、本発明の実施の形態の一例である情報処理装置のハードウェア構成例を説明するためのブロック図である。

【００１４】

図１に示すように、本実施形態の情報処理装置１００は、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、ＨＤＤ１０８、タイマ１１２、プリンタＩ／Ｆ制御部１０４、ＮＶＲＡＭ１０５、パネル制御部１０６、ネットワークＩ／Ｆ制御部１０７を備える。

【００１５】

ＣＰＵ（制御手段）１０１は、ソフトウェアプログラムを実行し、装置全体を制御する。ＲＯＭ（リードオンリーメモリ）１０２には、装置のブートプログラムや固定パラメータ等が格納されている。ＲＡＭ（ランダムアクセスメモリ）１０３は、ＣＰＵ１０１が装置を制御する際に、一時的なデータの格納などに使用する。

【００１６】

ＨＤＤ（ハードディスクドライブ）１０８は、印刷データの格納など、様々なデータの格納に使用する。タイマ１１２は、タイマ処理における経過時刻を管理する。プリンタＩ／Ｆ制御部１０４は、プリンタ１１０を制御する。ＮＶＲＡＭ１０５は、不揮発性のメモリであり、装置の各種設定値を保存する。

【００１７】

パネル制御部１０６は、オペレーションパネル１０９を制御し、各種情報の表示、ユーザからの指示が入力される。ネットワークＩ／Ｆ制御部１０７は、ＬＡＮ（ネットワーク）１１１との間でデータの送受信を制御する。

【００１８】
バス１０８には、ＣＰＵ１０１、ＲＯＭ１０２、ＲＡＭ１０３、ＨＤＤ１０８、タイマ１１２、プリンタＩ／Ｆ制御部１０４、ＮＶＲＡＭ１０５、パネル制御部１０６、ネットワークＩ／Ｆ制御部１０７が接続される。このバス１０８を介してＣＰＵ１０１からの制御信号や各装置間のデータ信号が送受信される。
【００１９】
図２は、本実施形態の情報処理装置１００にＬＡＮ１１１を介してクライアントＰＣ（外部装置）２０１が接続されたシステムを示す図である。
【００２０】
図２に示すように、クライアントＰＣ２０１は、印刷ドキュメント（電子データ）２０６をＬＰＲ等の印刷プロトコルを使用し情報処理装置１００に送信する。印刷ドキュメント２０６には、属性情報２０７が付加されており、この属性情報２０７も印刷ドキュメント２０６と同時に情報処理装置１００に送信される。
【００２１】
属性情報２０７には、文書名、作成者、所属、キーワード等の情報が含まれる。文書名は、ユーザがクライアントＰＣ２０１から印刷を行う際にファイル名から自動的に取得され、作成者、所属、キーワード等の情報は、クライアントＰＣ２０１からユーザが印刷を行う際にユーザが入力することにより取得される。
【００２２】
情報処理装置１００は、受信した印刷ドキュメント２０６から属性情報２０７を取得し、属性情報２０７から抽出したデータを、インデックス情報としてインデックステーブル２０５に登録する（登録手段）。即ち、印刷ドキュメント２０６を検索対象の文書として保存する。なお、インデックステーブル２０５はＨＤＤ１０８内に格納されている。
【００２３】
図２に示す例では、「社員旅行計画書」という文書の属性情報に含まれる「第一開発部」、「田中花子」、「保養所」というインデックスが既に登録されている情報で、「プリンタソフト仕様書」という文書の属性情報が新たに登録される。即ち、「プリンタ仕様書」の属性情報に含まれる「鈴木一郎」、「第一開発部」、「ＬＢＰ」、「管理ツール」というインデックスを登録する。なお、ここでは、「鈴木一郎」、「ＬＢＰ」、「管理ツール」というインデックスはインデックステーブル２０５に新たに登録されるインデックスであるので、新しいレコードが作成される。一方、「第一開発部」というインデックスはすでに登録済みなので、関連文書に印刷ドキュメント２０６を特定するドキュメント名「プリンタソフト仕様書」を追加する。
【００２４】
また、情報処理装置１００は、受信した印刷ドキュメント２０６をジョブ保存エリア２０４に保存するとともに、受信した印刷ドキュメント２０６を印刷出力する。なお、ジョブ保存エリア２０４はＨＤＤ１０８内に設けられた記憶領域である。
【００２５】
図３は、本実施形態の情報処理装置１００がセキュア印刷を実行する場合の処理について説明するための図である。
【００２６】
セキュア印刷とは、一般に、機密文書を印刷する際に使用される機能である。簡単に説明すると、ユーザは、クライアントＰＣ２０１からセキュアなデータの印刷を行う際に、そのジョブに対して暗証番号（パスワード）をセットし、ジョブと暗証番号をセットで情報処理装置１００に送信する。
【００２７】
情報処理装置１００は、暗証番号がセットされたジョブを受信した場合、すぐに印刷は行わず印刷データを装置内に保持する。クライアントＰＣ２０１上で印刷を実行したユーザは、情報処理装置１００のＵＩパネルから暗証番号を入力する。情報処理装置１００は、クライアントＰＣ２０１から送信された暗証番号と、ＵＩパネルから入力された暗証番

号とが一致した場合のみ、暗証番号がセットされたジョブを実行する。

【００２８】

図３の例では、クライアントＰＣ２０１が、印刷ドキュメント２０６をＬＰＲ等の印刷プロトコルを使用して情報処理装置１００に送信する。その際に、セキュア印刷機能を適用して印刷ドキュメントを送信する。

【００２９】

情報処理装置１００は、受信した印刷ドキュメント２０６をジョブ保存エリア２０４に保存する。ユーザ２０８は、情報処理装置１００のオペレーションパネル１０９から暗証番号を入力する。そして、情報処理装置１００は、クライアントＰＣ２０１から送信された暗証番号と、オペレーションパネル１０９から入力された暗証番号とが一致するかどうか判断し、一致した場合、受信したセキュアな印刷ドキュメント２０６を印刷する。

【００３０】

図３の例では、印刷ジョブがセキュアであるため、図２で説明した処理とは異なり、インデックステーブル２０５への属性情報の登録は行わない。即ち、印刷ドキュメント２０６を検索非対象の文書としてジョブ保存エリアに保存する。なお、印刷ドキュメント２０６の印刷後に、該印刷ドキュメント２０６をジョブ保存エリア２０４から消去するようにしてもよい。

【００３１】

図４は、本実施形態の情報処理装置１００がＩＰｓｅｃ等のプロトコルを使用し、通信経路を暗号化して印刷を実行する場合の処理を説明するための図である。

【００３２】

図４の例では、クライアントＰＣ２０１が印刷ドキュメント２０６をＩＰｓｅｃ適用したＬＰＲ等の印刷プロトコルを使用することにより通信経路を暗号化して情報処理装置１００に送信する。ＩＰｓｅｃは、あらかじめ指定されたノード（ＩＰアドレスで特定される）との間でデータを暗号化して通信するものである。どのノードとの間でＩＰｓｅｃを適用するかの情報は、情報処理装置１００のＮＶＲＡＭ１０５保存されている。

【００３３】

情報処理装置１００は、通信コネクションが確立した時点で、通信相手のＩＰアドレスからＩＰｓｅｃ通信であるか否かを判断し、ＩＰｓｅｃ通信である場合、受信した印刷ドキュメント２０６をジョブ保存エリア２０４に保存する。そして、情報処理装置１００は、受信した印刷ドキュメント２０６を印刷する。図４の例では、図２で説明した処理とは異なり、インデックステーブル２０５への属性情報の登録は行わない。即ち、印刷ドキュメント２０６を検索非対象の文書としてジョブ保存エリアに保存する。なお、印刷ドキュメント２０６の印刷後に、該印刷ドキュメント２０６をジョブ保存エリア２０４から消去するようにしてもよい。

【００３４】

図５は、本実施形態の情報処理装置１００におけるインデックス自動登録設定画面例を示す図である。

【００３５】

本実施形態の情報処理装置１００では、オペレーションパネル１０９を介してインデックス自動登録の各種設定を行うことができる。

【００３６】

図５において、「インデックスを自動登録する」の設定５０１がチェックされている場合は、情報処理装置１００は、受信した電子データのインデックス情報を自動的にインデックステーブル２０５に登録する。

【００３７】

また、「機密データはインデックス登録しない」の設定５０２がチェックされている場合は、情報処理装置１００は、機密データ以外のデータのインデックスの登録は行うが、機密データのインデックスの登録は行わない。

【００３８】

さらに、本実施形態では、オペレーションパネル１０９に表示される機密データ定義の設定画面５０３において、機密データを定義することができる。

【００３９】

例えば、「セキュアプリント」の設定５０４がチェックされている場合は、セキュアプリントで印刷されたジョブを機密データとする。また、「ＩＰｓｅｃ」の設定５０５がチェックされている場合は、ＩＰｓｅｃ経由で印刷されたジョブを機密データとする。

【００４０】

図６は、本実施形態の情報処理装置１００が電子データを受信する際の処理を説明するためのフローチャート図である。図６での各処理は、情報処理装置１００のＲＯＭ１０２やＨＤＤ１０８等に記憶された制御プログラムがＲＡＭ１０３にロードされて、ＣＰＵ１０１により実行される。

【００４１】

まず、クライアントＰＣ２０１から電子データを受信すると（ステップＳ６００）、情報処理装置１００は、図５の「インデックスを自動登録する」の設定５０１がチェックされているか否かを判断する（ステップＳ６０１）。

【００４２】

図５の「インデックスを自動登録する」の設定５０１がチェックされていない場合は、情報処理装置１００は、電子データ処理（印刷／格納）を実行（ステップＳ６０６）して処理を終了する。一方、図５の「インデックスを自動登録する」の設定５０１がチェックされている場合、情報処理装置１００は、図５の「機密データはインデックス登録しない」の設定５０２がチェックされているか否かを判断する（ステップＳ６０２）。

【００４３】

図５の「機密データはインデックス登録しない」の設定５０２がチェックされていない場合は、情報処理装置１００は、インデックス情報のインデックステーブル２０５への登録処理を行う（ステップＳ６０５）。続いて、情報処理装置１００は、電子データ処理（印刷／格納）を実行（ステップＳ６０６）して処理を終了する。一方、図５の「機密データはインデックス登録しない」の設定５０２がチェックされている場合は、情報処理装置１００は、電子データが機密データか否かを判断する処理を実行する（ステップＳ６０３）。

【００４４】

そして、電子データが機密データである場合、情報処理装置１００は、インデックス情報のインデックステーブル２０５への登録処理を行なうことなく、電子データ処理（印刷／格納）を実行（ステップＳ６０６）して処理を終了する。また、電子データが機密データでなかった場合、情報処理装置１００は、インデックス情報のインデックステーブル２０５への登録処理を行う（ステップＳ６０５）。続いて、情報処理装置１００は、電子データ処理（印刷／格納）を実行（ステップＳ６０６）して処理を終了する。

【００４５】

図７は、本実施形態の情報処理装置１００が電子データを受信した際に、受信した電子データが機密データか否かを判断する処理（図６のステップＳ６０３の処理）を説明するためのフローチャート図である。図７での各処理は、情報処理装置１００のＲＯＭ１０２やＨＤＤ１０８等に記憶された制御プログラムがＲＡＭ１０３にロードされて、ＣＰＵ１０１により実行される。

【００４６】

まず、情報処理装置１００は、図５の機密データ定義の設定画面５０３において、「セキュアプリント」の設定５０４がチェックされているか否かを判断する（ステップＳ７０１）。

【００４７】

そして、「セキュアプリント」の設定５０４がチェックされていない場合、情報処理装置１００は、図５の機密データ定義の設定画面５０３において、「ＩＰｓｅｃ」の設定５０５がチェックされているか否かを判断する（ステップＳ７０３）。

【００４８】
一方、「セキュアプリント」の設定５０４がチェックされている場合、情報処理装置１００は、受信ジョブがセキュアプリントであるか否かを判断する（ステップＳ７０２）。受信ジョブがセキュアプリントである場合、情報処理装置１００は、受信した電子データが機密データであると判断し（ステップＳ７０６）、処理を終了する。受信ジョブがセキュアプリントでない場合、情報処理装置１００は、図５の機密データ定義の設定画面５０３において、「ＩＰｓｅｃ」の設定５０５がチェックされているか否かを判断する（ステップＳ７０３）。
【００４９】
ステップＳ７０３において、「ＩＰｓｅｃ」の設定５０５がチェックされていない場合、情報処理装置１００は、受信した電子データが機密データでないと判断し（ステップＳ７０５）、処理を終了する。ステップＳ７０３において、「ＩＰｓｅｃ」の設定５０５がチェックされている場合、情報処理装置１００は、受信ジョブがＩＰｓｅｃ経由で送信されたか否かを判断する（ステップＳ７０４）。
【００５０】
そして、受信ジョブがＩＰｓｅｃ経由で送信された場合、情報処理装置１００は、受信した電子データが機密データであると判断し（ステップＳ７０６）、処理を終了する。受信ジョブがＩＰｓｅｃ経由で送信されていない場合、情報処理装置１００は、受信した電子データが機密データでないと判断し（ステップＳ７０５）、処理を終了する。
【００５１】
図８は、本実施形態の情報処理装置１００が作成したインデックステーブル２０５の一例を示す図である。
【００５２】
図８に示すように、このインデックステーブルには、インデックス列８０１に、受信した電子データの属性情報をインデックスキーとして登録し、関連文書列８０２に、そのインデックスを属性としてもつ電子データを登録する。例えば、鈴木一郎というインデックスに、それに関連する文書として、特許提案書やプリンタソフト仕様書等の関連文書が登録されている。
【００５３】
図９は、本実施形態の情報処理装置１００に保存されたドキュメントを検索するＵＩ画面の一例を示す図である。
【００５４】
図９に示すように、このＵＩ画面では、検索キーワード入力欄９０１に検索キーワードを入力する。検索キーワード入力欄９０１での検索キーワードの指定は、「ａｎｄ」，「ｏｒ」を使用することで論理和、論理積を使用することができる。
【００５５】
そして、検索キーワード入力欄９０１に検索キーワードを入力した後、検索ボタン９０２を押下することにより、図８のインデックステーブル２０５を参照することにより印刷ドキュメントが検索され、検索されたドキュメントが検索結果表示欄９０３に表示される。検索結果表示欄９０３に表示されたドキュメントは、参照ボタン９０４を押下することによりプレビューを表示することができる。また、印刷ボタン９０５を押下することにより、検索結果表示欄９０３に表示されたドキュメントを印刷することが可能となる。
【００５６】
以上説明したように、本実施形態では、送信された電子データに関するインデックス情報を自動的に蓄積する機能を持つことにより、効率的に電子データを収集することが可能となる。
【００５７】
また、機密性の高いセキュアな電子データを送信方法から自動的に判断するので、誤って不特定多数のユーザと共有してしまうことをユーザが明示的に指定することなく回避することが可能となる。

【００５８】
なお、本発明は、上記実施の形態に例示したものに限定されるものではなく、本発明の要旨を逸脱しない範囲において適宜変更可能である。
【００５９】
また、本発明の目的は、以下の処理を実行することによって達成される。即ち、上述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）が記憶媒体に格納されたプログラムコードを読み出す処理である。
【００６０】
この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施の形態の機能を実現することになり、そのプログラムコード及び該プログラムコードを記憶した記憶媒体は本発明を構成することになる。
【００６１】
また、プログラムコードを供給するための記憶媒体としては、次のものを用いることができる。例えば、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等である。または、プログラムコードをネットワークを介してダウンロードしてもよい。
【００６２】
また、コンピュータが読み出したプログラムコードを実行することにより、上記実施の形態の機能が実現される場合も本発明に含まれる。加えて、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。
【００６３】
更に、前述した実施形態の機能が以下の処理によって実現される場合も本発明に含まれる。即ち、記憶媒体から読み出されたプログラムコードが、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る。その後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行う場合である。
【図面の簡単な説明】
【００６４】
【図１】本発明の実施の形態の一例である情報処理装置のハードウェア構成例を説明するためのブロック図である。
【図２】本実施形態の情報処理装置にＬＡＮを介してクライアントＰＣが接続されたシステムを示す図である。
【図３】本実施形態の情報処理装置がセキュア印刷を実行する場合の処理について説明するための図である。
【図４】本実施形態の情報処理装置がＩＰｓｅｃ等のプロトコルを使用し、通信経路を暗号化して印刷を実行する場合の処理を説明するための図である。
【図５】本実施形態の情報処理装置におけるインデックス自動登録設定画面例を示す図である。
【図６】本実施形態の情報処理装置が電子データを受信する際の処理を説明するためのフローチャート図である。
【図７】本実施形態の情報処理装置が電子データを受信した際に、受信した電子データが機密データか否かを判断する処理（図６のステップＳ６０３の処理）を説明するためのフローチャート図である。
【図８】本実施形態の情報処理装置が作成したインデックステーブルの一例を示す図である。
【図９】本実施形態の情報処理装置に保存されたドキュメントを検索するＵＩ画面の一例

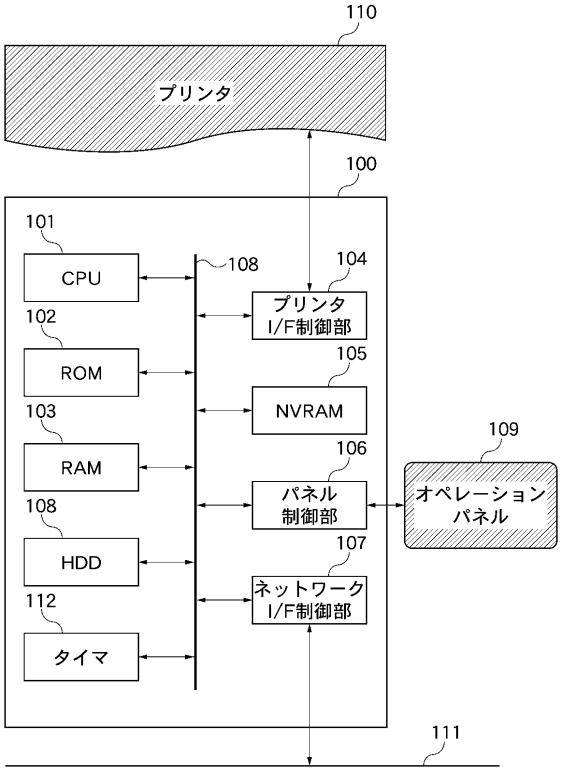
を示す図である。

【符号の説明】

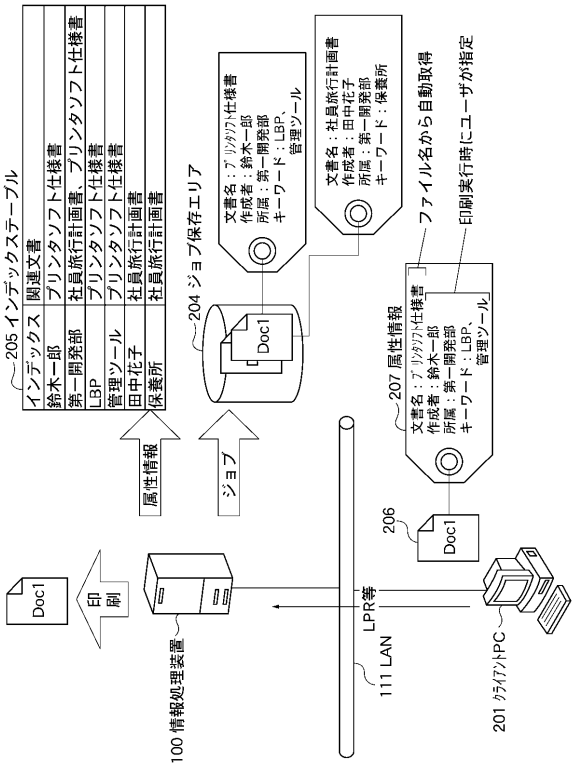
【００６５】

１００　情報処理装置
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ
１０８　ＨＤＤ
１１１　ＬＡＮ
２０１　クライアントＰＣ

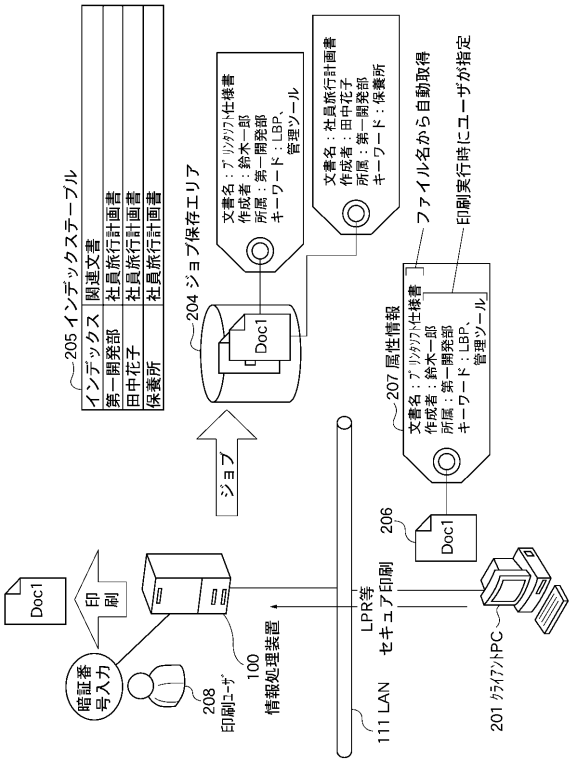
【図１】



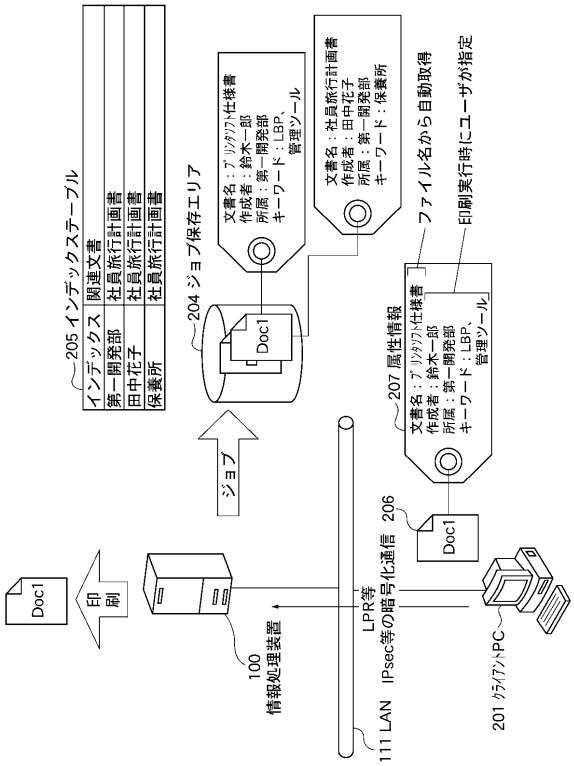
【図２】



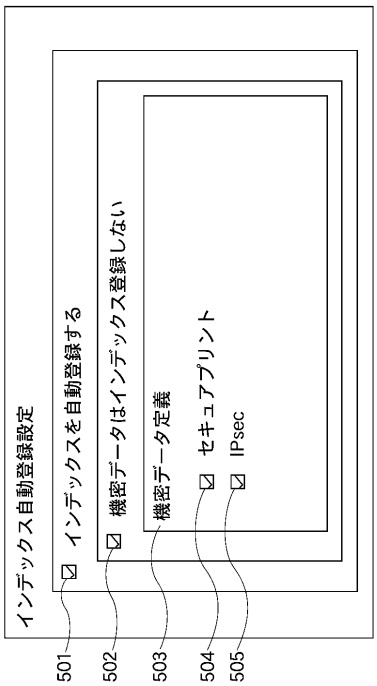
【図３】


205 インデックステーブル
インデックス 関連文書
第一開発部 社員旅行計画書
田中花子 社員旅行計画書
保養所 社員旅行計画書
204 ジョブ保存エリア
Doc1
文書名：ﾌﾟﾘﾝﾀｿﾌﾄ仕様書
作成者：鈴木一郎
所属：第一開発部
キーワード：LBP、管理ツール
文書名：社員旅行計画書
作成者：田中花子
所属：第一開発部
キーワード：保養所
ファイル名から自動取得
印刷実行時にユーザが指定
207 属性情報
文書名：ﾌﾟﾘﾝﾀｿﾌﾄ仕様書
作成者：鈴木一郎
所属：第一開発部
キーワード：LBP、管理ツール
ジョブ
206
Doc1
印刷
Doc1
暗証番号入力
208 印刷ﾕｰｻﾞ
100 情報処理装置
LPR等
セキュア印刷
111 LAN
201 ｸﾗｲｱﾝﾄPC

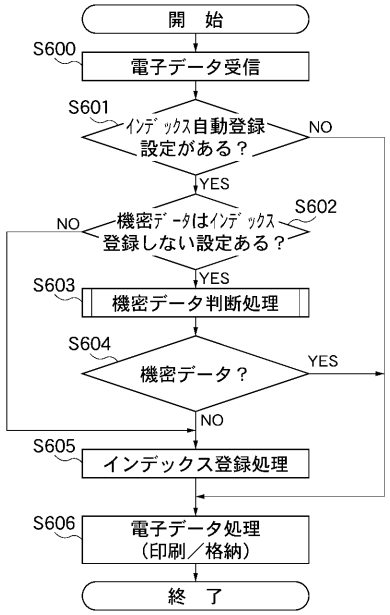
【図４】


205 インデックステーブル
インデックス 関連文書
第一開発部 社員旅行計画書
田中花子 社員旅行計画書
保養所 社員旅行計画書
204 ジョブ保存エリア
Doc1
文書名：ﾌﾟﾘﾝﾀｿﾌﾄ仕様書
作成者：鈴木一郎
所属：第一開発部
キーワード：LBP、管理ツール
文書名：社員旅行計画書
作成者：田中花子
所属：第一開発部
キーワード：保養所
ファイル名から自動取得
印刷実行時にユーザが指定
207 属性情報
文書名：ﾌﾟﾘﾝﾀｿﾌﾄ仕様書
作成者：鈴木一郎
所属：第一開発部
キーワード：LBP、管理ツール
ジョブ
206
Doc1
印刷
Doc1
100 情報処理装置
LPR等
IPsec等の暗号化通信
111 LAN
201 ｸﾗｲｱﾝﾄPC

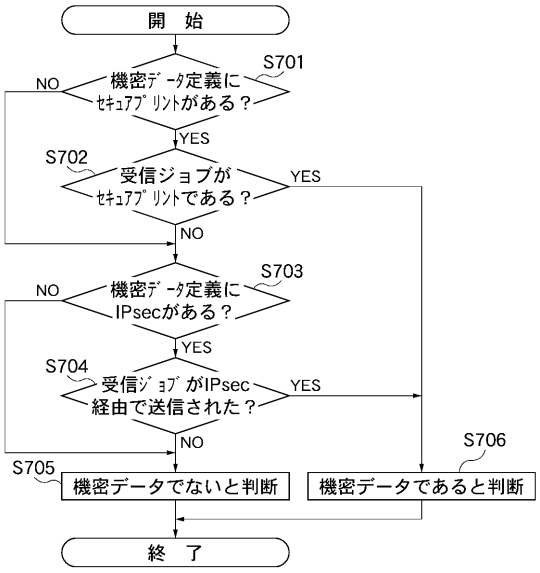
【図５】


インデックス自動登録設定
インデックスを自動登録する
機密データはインデックス登録しない
機密データ定義
セキュアプリント
IPsec
501
502
503
504
505

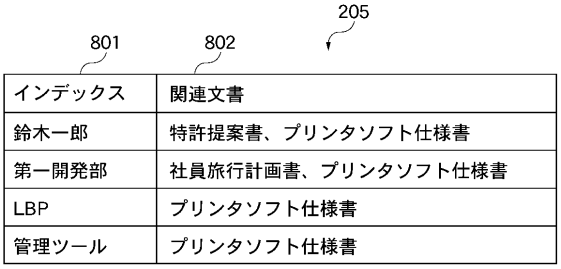
【図６】


開　始
S600
電子データ受信
S601
ｲﾝﾃﾞｯｸｽ自動登録設定がある？
NO
YES
機密ﾃﾞｰﾀはｲﾝﾃﾞｯｸｽ登録しない設定ある？
S602
NO
YES
S603
機密データ判断処理
S604
機密データ？
YES
NO
S605
インデックス登録処理
S606
電子データ処理（印刷／格納）
終　了

【図７】



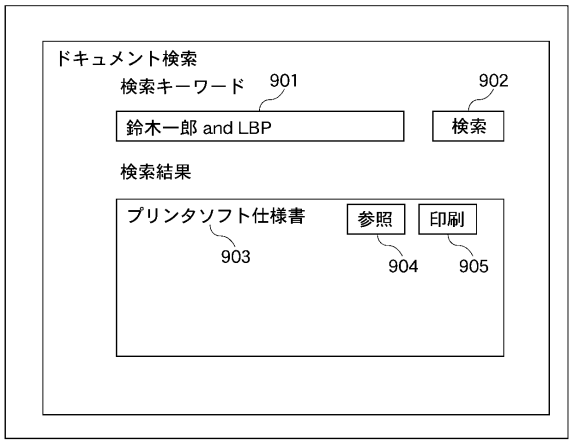
【図８】



801 インデックス	802 関連文書
鈴木一郎	特許提案書、プリンタソフト仕様書
第一開発部	社員旅行計画書、プリンタソフト仕様書
LBP	プリンタソフト仕様書
管理ツール	プリンタソフト仕様書

205

【図９】



フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　１７／３０
Ｇ０６Ｆ　　３／１２