

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4831461号  
(P4831461)

(45) 発行日 平成23年12月7日(2011.12.7)

(24) 登録日 平成23年9月30日(2011.9.30)

(51) Int. Cl.		F I			
<b>HO4L</b>	<b>9/08</b>	<b>(2006.01)</b>	HO4L	9/00	6O1C
<b>GO6F</b>	<b>21/24</b>	<b>(2006.01)</b>	GO6F	12/14	54OA
			GO6F	12/14	54OP

請求項の数 10 (全 14 頁)

(21) 出願番号	特願2005-72316 (P2005-72316)	(73) 特許権者	000005496
(22) 出願日	平成17年3月15日 (2005.3.15)		富士ゼロックス株式会社
(65) 公開番号	特開2006-261716 (P2006-261716A)		東京都港区赤坂九丁目7番3号
(43) 公開日	平成18年9月28日 (2006.9.28)	(74) 代理人	110000039
審査請求日	平成20年2月21日 (2008.2.21)		特許業務法人アイ・ピー・エス
		(72) 発明者	大西 健司
			神奈川県足柄上郡中井町境430 グリー
			ンテクなかい 富士ゼロックス株式会社内
		審査官	金沢 史明

最終頁に続く

(54) 【発明の名称】 文書処理装置及び方法

(57) 【特許請求の範囲】

【請求項1】

電子文書内の秘匿化対象部分のデータを暗号化した暗号データ及び該暗号データを識別する識別情報を関連付けて記憶する記憶部と、

記録媒体を画像データとして読み取る読取部と、

前記読取部により読み取られた画像データから機械可読コードを抽出し、該コードから該画像データ内の機密部分のデータに対応する識別情報及び暗号化された該機密部分の復号に用いる復号鍵を取り出す取出部と、

前記記憶部が記憶する暗号データのうち、前記読取部により読み取られた画像データには含まれていないデータについて暗号化された暗号データを、前記取出部により取り出された識別情報に基づいて、取得する暗号データ取得部と、

前記暗号データ取得部により取得された暗号データを、前記取出部により取り出された復号鍵を用いて復号する復号部と、

前記読取部により読み取られた画像データに、前記復号部により復号されたデータを合成する復号データ合成部と

を備えることを特徴とする文書処理装置。

【請求項2】

電子文書から秘匿化対象部分のデータを抽出する秘匿化対象部分抽出部と、

前記電子文書の前記秘匿化対象部分のデータを、該データの内容とは異なる内容である代用情報に置き換えた秘匿化文書を生成する秘匿化処理部と、

10

20

前記秘匿化対象部分のデータを暗号化する暗号化処理部と、  
前記暗号化処理部によって暗号化された秘匿化対象部分のデータを識別する識別情報を生成する識別情報生成部と、  
前記暗号化された秘匿化対象部分のデータと前記識別情報とを関連付けて前記記憶部に格納する処理を行う格納処理部と、  
前記暗号化された秘匿化対象部分のデータを復号するための復号鍵と前記識別情報を含む機械可読コードを生成するコード生成部と、  
前記秘匿化文書と前記機械可読コードとを合成するコード合成部と  
を備えることを特徴とする請求項 1 に記載の文書処理装置。

## 【請求項 3】

暗号化鍵と復号鍵のペアを生成する鍵生成部を更に備えることを特徴とする請求項 2 に記載の文書処理装置。

## 【請求項 4】

前記鍵生成部は、前記電子文書の少なくとも一部分に基づいて、暗号化鍵と復号鍵のペアを生成することを特徴とする請求項 3 に記載の文書処理装置。

## 【請求項 5】

前記格納処理部は、可搬記録媒体に、前記秘匿化対象部分と前記識別情報とを関連付けて格納することを特徴とする請求項 2 ～ 4 のいずれか一項に記載の文書処理装置。

## 【請求項 6】

前記秘匿化対象部分抽出部は、前記電子文書の出力結果における前記秘匿化対象部分の配置に関する情報を算出することを特徴とする請求項 2 ～ 5 のいずれか一項に記載の文書処理装置。

## 【請求項 7】

電子文書から秘匿化対象部分のデータを抽出する秘匿化対象部分抽出部と、  
 前記電子文書の前記秘匿化対象部分のデータを、該データの内容とは異なる内容である代用情報に置き換えた秘匿化文書を生成する秘匿化処理部と、

前記秘匿化対象部分のデータを外部に送信する送信部と、

前記送信部が送信した秘匿化対象部分のデータについて暗号化された暗号データを識別する識別情報を外部から受信する識別情報受信部と、

前記暗号化された秘匿化対象部分のデータを復号するための復号鍵と前記識別情報を含む機械可読コードを生成するコード生成部と、

前記秘匿化文書と前記機械可読コードとを合成するコード合成部と、

記録媒体を画像データとして読み取る読取部と、

前記読取部により読み取られた画像データから機械可読コードを抽出し、該コードから該画像データ内の機密部分のデータに対応する識別情報及び暗号化された該機密部分の復号に用いる復号鍵を取り出す取出部と、

前記読取部により読み取られた画像データには含まれていないデータについて暗号化されたデータであり、かつ、電子文書内の秘匿化対象部分のデータである暗号データを、前記取出部により取り出された識別情報に基づいて、受信する暗号データ受信部と、

前記受信部により受信された暗号データを、前記取出部により取り出された復号鍵を用いて復号する復号部と、

前記読取部により読み取られた画像データに、前記復号部により復号されたデータを合成する復号データ合成部と

を備えることを特徴とする文書処理装置。

## 【請求項 8】

請求項 7 に記載の文書処理装置と連係して動作する文書処理装置であって、

請求項 7 に記載の文書処理装置から送られてくる秘匿化対象部分のデータを暗号化する暗号化処理部と、

10

20

30

40

50

前記秘匿化対象部分のデータを識別する識別情報を生成する識別情報生成部と、  
前記暗号化された秘匿化対象部分のデータと前記識別情報とを関連付けて格納する処理を行う格納処理部と、

請求項 7 に記載の文書処理装置に、前記識別情報を送信する識別情報送信部と、  
請求項 7 に記載の文書処理装置から送られてくる識別情報に基づいて、前記格納処理部により格納された、暗号化された秘匿化対象部分のデータを請求項 7 に記載の文書処理装置に送信する暗号データ送信部と

を備えたことを特徴とする文書処理装置。

【請求項 9】

文書処理装置を用いて文書処理する文書処理方法であって、  
前記文書処理装置は、  
電子文書内の秘匿化対象部分のデータを暗号化した暗号データ及び該暗号データを識別する識別情報を関連付けて記憶し、

記録媒体を画像データとして読み取り、

読み取られた画像データから機械可読コードを抽出し、該コードから該画像データ内の機密部分のデータに対応する識別情報及び暗号化された該機密部分の復号に用いる復号鍵を取り出し、

記憶する暗号データのうち、読み取られた画像データには含まれていないデータについて暗号化された暗号データを、取り出された識別情報に基づいて、取得し、

取得された暗号データを、取り出された復号鍵を用いて復号し、

読み取られた画像データに、復号されたデータを合成することを特徴とする文書処理方法。

【請求項 10】

文書の処理を行う文書処理プログラムであって、コンピュータを、  
電子文書内の秘匿化対象部分のデータを暗号化した暗号データ及び該暗号データを識別する識別情報を関連付けて記憶する記憶部、

記録媒体を画像データとして読み取る読取部、

前記読取部により読み取られた画像データから機械可読コードを抽出し、該コードから該画像データ内の機密部分のデータに対応する識別情報及び暗号化された該機密部分の復号に用いる復号鍵を取り出す取出部、

前記記憶部が記憶する暗号データのうち、前記読取部により読み取られた画像データには含まれていないデータについて暗号化された暗号データを、前記取出部により取り出された識別情報に基づいて、取得する暗号データ取得部、

前記暗号データ取得部により取得された暗号データを、前記取出部により取り出された復号鍵を用いて復号する復号部、及び、

前記読取部により読み取られた画像データに、前記復号部により復号されたデータを合成する復号データ合成部

として機能させることを特徴とする文書処理プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、プリンタ等によって出力される文書の処理に関する。

【背景技術】

【0002】

企業や研究機関等が有する各種の機密情報は、機密情報が印刷された紙文書が企業等から持ち出されることで漏洩することが少なくない。そのため、現在では、機密情報は原則として電子データで管理して、紙媒体への出力はできるだけ制限するような運用を行う場合がある。

【0003】

10

20

30

40

50

しかしながら、このような運用を行っている場合であっても、紙媒体の有用性から、可能な限り、紙媒体への出力が行えた方が望ましい。また、文書に含まれる情報のうち、機密にすべき情報は、その一部である場合も少なくない。

【0004】

なお、特開平6-214862号公報には、サーバノードが管理する文書ファイルをアクセスできる各ユーザ毎に、読み込みや印刷のアクセス権レベルを設定するとともに、各文書内の所定領域（ページ、文、図等）単位に、読み込みや印刷等のアクセス権レベルを設定しておき、ユーザがクライアントノードで所望の文書の表示や印刷を行う際に、前記アクセス権レベルを比較することによって当該ユーザが各部分の表示や印刷が可能か否かを判別し、表示や印刷ができない部分については、マスクが行ってから、表示や印刷を行うクライアント・サーバシステムが開示されている。

10

【特許文献1】特開平6-214862号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

本発明の目的は、機密情報の漏洩を防止しつつ、機密情報を含む文書の利便性を向上させることにある。

【課題を解決するための手段】

【0006】

本発明に係る文書処理装置は、電子文書から秘匿化対象部分を抽出する秘匿化対象部分抽出部と、前記電子文書の前記秘匿化対象部分を代用情報に置き換えた秘匿化文書を生成する秘匿化処理部と、前記秘匿化対象部分に対応する識別情報を生成する識別情報生成部と、前記秘匿化対象部分と前記識別情報とを関連付けて格納する処理を行う格納処理部と、前記識別情報を含む機械可読コード（例えば、二次元コード）を生成するコード生成部と、前記秘匿化文書と前記機械可読コードとを合成する合成部とを備えることを特徴とする。

20

【0007】

この場合において、前記秘匿化対象部分を暗号化する暗号化処理部を更に備え、前記識別情報生成部は、前記暗号化処理部によって暗号化された秘匿化対象部分に対応する識別情報を生成し、前記格納処理部は、前記暗号化された秘匿化対象部分と前記識別情報とを関連付けて格納するようにしてもよい。また、前記コード生成手段は、前記暗号化された秘匿化対象部分を復号するための復号鍵を更に含む機械可読コードを生成するようにしてもよい。また、暗号化鍵と復号鍵のペアを生成する鍵生成部を更に備えるようにしてもよい。前記鍵生成部は、例えば、前記電子文書の少なくとも一部分に基づいて、暗号化鍵と復号鍵のペアを生成する。

30

【0008】

また、前記格納処理部は、可搬記録媒体に、前記秘匿化対象部分と前記識別情報とを関連付けて格納するようにしてもよい。

【0009】

また、前記秘匿化対象部分抽出部は、前記電子文書の出力結果における前記秘匿化対象部分の配置に関する情報を算出するようにしてもよい。

40

【0010】

本発明に係る第二の文書処理装置は、電子文書から秘匿化対象部分を抽出する秘匿化対象部分抽出部と、前記電子文書の前記秘匿化対象部分を代用情報に置き換えた秘匿化文書を生成する秘匿化処理部と、前記秘匿化対象部分を外部に送信する送信部と、前記秘匿化対象部分に対応する識別情報を外部から受信する受信部と、前記識別情報を含む機械可読コードを生成するコード生成部と、前記秘匿化文書と前記機械可読コードとを合成する合成部とを備えることを特徴とする。

【0011】

本発明に係る第三の文書処理装置は、前記第二の文書処理装置と連係して動作する文書

50

処理装置であって、前記第二の文書処理装置から送られてくる秘匿化対象部分を暗号化する暗号化処理部と、前記秘匿化対象部分に対応する識別情報を生成する識別情報生成部と、前記暗号化された秘匿化対象部分と前記識別情報とを関連付けて格納する処理を行う格納処理部と、前記識別情報を前記第二の文書処理装置に送信する送信部とを備えたことを特徴とする。

【0012】

本発明に係る文書処理方法は、電子文書から秘匿化対象部分を抽出し、前記電子文書の前記秘匿化対象部分を代用情報に置き換えた秘匿化文書を生成し、前記秘匿化対象部分に対応する識別情報を生成し、前記秘匿化対象部分と前記識別情報とを関連付けて格納し、前記識別情報を含む機械可読コードを生成し、前記秘匿化文書と前記機械可読コードとを合成することを特徴とする。

10

【0013】

この場合において、前記秘匿化対象部分を暗号化するようにしてもよい。

【0014】

本発明に係るプログラムは、文書の処理を行う文書処理プログラムであって、コンピュータを、電子文書から秘匿化対象部分を抽出する秘匿化対象部分抽出部、前記電子文書の前記秘匿化対象部分を代用情報に置き換えた秘匿化文書を生成する秘匿化処理部、前記秘匿化対象部分に対応する識別情報を生成する識別情報生成部、前記秘匿化対象部分と前記識別情報とを関連付けて格納する処理を行う格納処理部、前記識別情報を含む機械可読コードを生成するコード生成部、及び、前記秘匿化文書と前記機械可読コードとを合成する合成部として機能させることを特徴とする。

20

【0015】

この場合において、前記コンピュータを、更に、前記秘匿化対象部分を暗号化する暗号化処理部として機能させるようにしてもよい。

【0016】

なお、前記プログラムは、CD-ROM等の可搬記録媒体やネットワーク等の手段を介して頒布されうる。

【発明の効果】

【0017】

本発明によれば、電子文書の秘匿化対象部分（例えば、機密情報部分）が代用情報に置き換えられるので、出力文書を介した機密情報の漏洩を防ぐことが可能となる。

30

【発明を実施するための最良の形態】

【0018】

以下、本発明の実施の形態について、図面を参照しつつ詳細に説明する。

【0019】

図1は、本発明による文書処理システムの構成を示す図である。

【0020】

同図に示すように、本発明による文書処理システム100は、文書サーバ110と、文書閲覧用端末装置120と、スキャナ121と、プリンタ130と、機密文書処理サーバ140とを備えている。そして、文書サーバ110、文書閲覧用端末装置120、プリンタ130及び機密文書処理サーバ140は、それぞれ、LAN等のネットワーク180に接続されている。また、スキャナ121は、USB等のインタフェースを介して、文書閲覧用端末装置120にローカル接続されている。

40

【0021】

文書サーバ110は、電子化された機密文書を保持・管理するサーバであり、例えば、通常のパーソナルコンピュータ（以下、PCという）その他のコンピュータで構成される。より具体的には、文書サーバ110は、CPU、メインメモリ、表示装置、ハードディスク装置、入力装置等を備える。表示装置は、例えば、CRT表示装置やLCD表示装置等によって構成され、入力装置は、例えば、キーボードやマウスその他のポインティングデバイス等によって構成される。

50

## 【 0 0 2 2 】

文書閲覧用端末装置 1 2 0 は、文書サーバ 1 1 0 に格納されている機密文書をネットワーク 1 8 0 を介して読み出して、画面上に表示することで、機密文書を閲覧し、必要に応じて、当該機密文書をプリンタ 1 3 0 に出力するための端末装置であり、例えば、通常の P C その他のコンピュータで構成される。

## 【 0 0 2 3 】

スキャナ 1 2 1 は、プリンタ 1 3 0 で出力された紙文書等の読取りを行い、画像データとして文書閲覧用端末装置 1 2 0 内に取り込むための文書読取り装置である。

## 【 0 0 2 4 】

プリンタ 1 3 0 は、文書閲覧用端末装置 1 2 0 等からの指示に従って、文書等の出力を行う出力装置であり、例えば、通常のネットワーク対応のレーザープリンタやインクジェットプリンタで構成される。

## 【 0 0 2 5 】

機密文書処理サーバ 1 4 0 は、文書閲覧用端末装置 1 2 0 等から送られてくる機密文書に対して、プリンタ 1 3 0 で出力できるように、秘匿化処理（後述）を行うものである。また、秘匿化処理がされて出力された紙文書等から、秘匿化された機密部分の復元（秘匿化解除）を行うものでもある。機密文書処理サーバ 1 4 0 は、例えば、通常の P C その他のコンピュータで構成される。

## 【 0 0 2 6 】

図 2 及び図 3 は、機密文書処理サーバ 1 4 0 の機能構成を示す図である。図 2 は、機密文書をプリンタ 1 3 0 で印刷できるように、機密部分の秘匿化処理を行う場合の機能構成を示し、図 3 は、秘匿化処理がされて出力された紙文書等から、秘匿化された機密部分を復元する場合の機能構成を示している。

## 【 0 0 2 7 】

まず、機密文書を印刷できるように、機密部分の秘匿化処理を行う場合の機能構成について説明する。

## 【 0 0 2 8 】

図 2 に示すように、機密文書処理サーバ 1 4 0 は、機密部分抽出部 2 1 0 と、暗号化処理部 2 2 0 と、鍵生成部 2 2 1 と、識別情報生成部 2 3 0 と、格納処理部 2 4 0 と、二次元コード生成部 2 5 0 と、秘匿化処理部 2 6 0 と、文書合成部 2 7 0 とを備える。各部 2 1 0 ~ 2 7 0 は、基本的に、C P U が、メインメモリにロードされたプログラムを実行することで実現される。

## 【 0 0 2 9 】

機密部分抽出部 2 1 0 は、文書閲覧用端末装置 1 2 0 等から送られてくる機密文書データから、機密部分を抽出するものである。機密部分には、例えば、顧客情報等の個人情報や、研究データ、会社の業績データなどのテキストデータのほか、グラフなどの画像データが含まれる。文書処理システム 1 0 0 においては、機密文書データは、機密部分を識別できるような形式で作成されている。例えば、通常のワードプロセッサ文書データ等の場合は、機密部分については、機密部分識別用として予め定められた特定のフォントや特定の色などを使って作成される。また、文書作成用のソフトウェア等で、利用者が指定する部分に、機密部分であることを示す特定の属性を設定できるような場合は、機密部分に当該属性が設定される。また、X M L 等で記述された文書データの場合は、機密部分であることを示すタグを定義し、当該タグで機密部分が指定される。機密部分抽出部 2 1 0 は、機密文書データを解析して、上記属性等が設定された部分を機密部分として抽出する。更に、機密部分抽出部 2 1 0 は、機密文書をプリンタ 1 3 0 等に出力した場合に、出力結果において、抽出した機密部分が配置される位置（配置情報）の算出も行う。算出された配置情報は、機密部分データに含めて出力される。

## 【 0 0 3 0 】

暗号化処理部 2 2 0 は、機密部分抽出部 2 1 0 によって抽出された機密部分データの暗号化を行うものである。暗号化処理部 2 2 0 で行われる暗号化とは、機密部分データを、

10

20

30

40

50

元の内容がわからないデータに変換することをいい、暗号化の方法は、実装条件に応じて、DES等の共通鍵暗号方式や、RSA暗号等の公開鍵暗号方式や、機密部分データを所定の規則に従って並び替える方法等、適当な方法を選択することができる。ここでは、暗号化処理部220は、鍵生成部221によって生成される暗号化鍵を使って、機密部分データの暗号化を行うものとする。

**【0031】**

鍵生成部221は、暗号化処理部220によって使用される暗号化鍵、及び、暗号化処理部220によって暗号化された機密部分データを復号するための復号鍵を生成するものである。例えば、一方向性ハッシュ関数を使用して、機密文書データのハッシュ値を求め、当該ハッシュ値に基づいて、暗号化鍵及び復号鍵を生成する。なお、暗号化処理部220における暗号化手法が、各機密文書毎に異なる暗号化鍵等を必要としない場合は、鍵生成部221はなくてもよい。

10

**【0032】**

識別情報生成部230は、暗号化処理部220によって暗号化された機密部分データを識別するための識別情報を生成するものである。当該識別情報は、後に、暗号化された機密部分データをアクセスするために用いられる。識別情報としては、例えば、一方向性ハッシュ関数を使用して、暗号化された機密部分データから生成されるハッシュ値を用いることができる。

**【0033】**

格納処理部240は、暗号化された機密部分データと当該データの識別情報とを関連付けて、機密文書処理サーバ140が備える記憶装置（例えば、ハードディスク装置）等に格納するものである。

20

**【0034】**

二次元コード生成部250は、識別情報生成部230によって生成された識別情報と、鍵生成部221によって生成された復号鍵を、QRコード等の二次元コードデータに変換（符号化）するものである。二次元コード生成部250によって生成された二次元コードデータは、文書合成部270に渡される。

**【0035】**

秘匿化処理部260は、機密文書の機密部分を人間が読むことができないようにする秘匿化処理、すなわち、機密文書データの機密部分データを所定の代用データで置き換える処理を行うものである。例えば、機密部分データが文字等のテキストデータであった場合は、各文字が「 」や「×」等の代用文字で置き換えられる。また、機密部分データがグラフ等の画像データであった場合は、元の画像が、代用画像（例えば、単一色で塗りつぶされた同一サイズの画像）で置き換えられる。

30

**【0036】**

文書合成部270は、秘匿化処理部260によって秘匿化処理が行われた機密文書データ（秘匿化文書データ）と、二次元コードデータとを合成するものである。文書合成部270から出力された機密文書データは、機密処理済文書データとして、文書閲覧用端末装置120等に送り返される。

**【0037】**

次に、秘匿化処理がされてプリンタ130で出力された紙文書から、秘匿化された機密部分を復元する場合の機密文書処理サーバ140の機能構成について説明する。

40

**【0038】**

図3に示すように、機密文書処理サーバ140は、二次元コード抽出・復号部310と、機密部分データ取得部320と、復号処理部330と、画像合成部340とを備える。各部310～340は、基本的に、CPUが、メインメモリにロードされたプログラムを実行することで実現される。

**【0039】**

二次元コード抽出・復号部310は、スキャナ121で読み取られ、文書閲覧用端末装置120から送られてくる文書画像データから、二次元コードを抽出し、抽出した二次元

50

コードの復号を行って、当該二次元コードに含まれている機密部分データの識別情報及び復号鍵を取り出すものである。

【 0 0 4 0 】

機密部分データ取得部 3 2 0 は、二次元コード抽出・復号部 3 1 0 から渡される機密部分データ識別情報を使って、当該識別情報に対応する機密部分データを、機密文書処理サーバ 1 4 0 が備える記憶装置（例えば、ハードディスク装置）等から取得するものである。

【 0 0 4 1 】

復号処理部 3 3 0 は、機密部分データ取得部 3 2 0 によって取得された機密部分データを、二次元コード抽出・復号部 3 1 0 から渡される復号鍵を使って復号するものである。

10

【 0 0 4 2 】

画像合成部 3 4 0 は、復号処理部 3 3 0 によって復号された機密部分データを、文書閲覧用端末装置 1 2 0 から受け取った文書画像データに合成して、文書閲覧用端末装置 1 2 0 に送り返すものである。画像合成部 3 4 0 は、機密部分データに含まれる配置情報を利用して、文書画像における本来の位置に、機密部分画像（機密部分データに基づいて生成される画像）を貼り付ける。

【 0 0 4 3 】

次に、以上のような構成を有する文書処理システム 1 0 0 の動作について具体的に説明する。まず、機密文書をプリンタ 1 3 0 で印刷する際の動作について説明する。

【 0 0 4 4 】

20

文書サーバ 1 1 0 から読み出した機密文書を、文書閲覧用端末装置 1 2 0 の画面上で閲覧等していた利用者が、当該機密文書の印刷を文書閲覧用端末装置 1 2 0 に指示すると、文書閲覧用端末装置 1 2 0 は、当該機密文書を印刷可能な状態にするため、当該機密文書データを、ネットワーク 1 8 0 を介して、機密文書処理サーバ 1 4 0 に送信する。

【 0 0 4 5 】

機密文書処理サーバ 1 4 0 は、文書閲覧用端末装置 1 2 0 から機密文書データを受け取ると、まず、機密部分抽出部 2 1 0 によって、当該機密文書データから、機密部分を抽出する。次に、暗号化処理部 2 2 0 によって、抽出された機密部分データの暗号化を行う。そして、識別情報生成部 2 3 0 によって、暗号化された機密部分データを識別するための識別情報を生成する。そして、機密部分格納処理部 2 4 0 によって、暗号化された機密部分データとその識別情報を関連付けて、機密文書処理サーバ 1 4 0 が備えるハードディスク装置に格納する。また、二次元コード生成部 2 5 0 によって、識別情報生成部 2 3 0 によって生成された識別情報と、鍵生成部 2 2 1 によって生成された復号鍵を、QRコード等の二次元コードデータに変換する。また、秘匿化処理部 2 6 0 によって、機密文書データの機密部分データを所定の代用データで置き換える。最後に、秘匿化処理部 2 6 0 によって秘匿化処理が行われた機密文書データ（秘匿化文書データ）と、二次元コードデータとを、文書合成部 2 7 0 によって合成し、合成結果を文書閲覧用端末装置 1 2 0 に送り返す。

30

【 0 0 4 6 】

文書閲覧用端末装置 1 2 0 は、機密文書処理サーバ 1 4 0 から秘匿化処理がされた機密文書データを受け取ると、当該機密文書データをプリンタ 1 3 0 で出力する。

40

【 0 0 4 7 】

図 4 は、機密文書処理サーバ 1 4 0 による秘匿化処理前後の機密文書の例を示す図である。同図（a）は、秘匿化処理前の機密文書の例を示し、同図（b）は、秘匿化処理後の機密文書の例を示している。同図に示すように、機密部分として設定されている文字部分 4 1 0（「10万」）が、代用文字 4 2 0（「」）で置き換えられている。また、同図（b）に示すように、秘匿化処理後の機密文書は、所定位置（右下隅の余白部分）に、二次元コード 4 3 0 が付加されている。なお、二次元コード 4 3 0 は、暗号化された機密部分データの識別情報及び暗号化された機密部分データの復号に必要な復号鍵を符号化したものである。

50

## 【 0 0 4 8 】

以上のような処理を行うことにより、機密文書を印刷する際、機密文書に含まれる機密部分は、秘匿化されて印刷されるので、印刷された機密文書が持ち出されること等による機密漏洩を防止することができる。

## 【 0 0 4 9 】

次に、以上のようにして印刷された機密文書から、秘匿化された機密部分を復元する場合の動作について説明する。

## 【 0 0 5 0 】

二次元コード付きで印刷された機密文書を所持している利用者が、秘匿化されている機密部分（代用データで置き換えられている部分）の内容を確認したくなった場合は、まず、文書閲覧用端末装置 1 2 0 に接続されたスキャナ 1 2 1 に、二次元コード付きの機密文書をセットし、スキャナ 1 2 1 によって当該機密文書の読取りを行う。スキャナ 1 2 1 によって読み取られた機密文書の画像データは、文書閲覧用端末装置 1 2 0 によって、機密文書処理サーバ 1 4 0 に送られる。

10

## 【 0 0 5 1 】

機密文書処理サーバ 1 4 0 は、文書閲覧用端末装置 1 2 0 から機密文書の画像データを受け取ると、まず、二次元コード抽出・復号部 3 1 0 によって、機密文書の画像データから、二次元コードを抽出し、抽出した二次元コードの復号を行って、当該二次元コードに含まれている機密部分データの識別情報及び復号鍵を取り出す。次に、機密部分データ取得部 3 2 0 によって、取り出した機密部分データ識別情報を使って、当該識別情報に対応する機密部分データを、機密文書処理サーバ 1 4 0 が備えるハードディスク装置から取得する。次に、復号処理部 3 3 0 によって、ハードディスク装置から読み出された機密部分データを、二次元コードから取り出された復号鍵を使って復号する。次に、画像合成部 3 4 0 によって、復号された機密部分データを、文書閲覧用端末装置 1 2 0 から受け取った機密文書画像データに合成して、文書閲覧用端末装置 1 2 0 に送り返す。

20

## 【 0 0 5 2 】

機密文書処理サーバ 1 4 0 から、秘匿解除処理がされた機密文書の画像データを受け取ると、文書閲覧用端末装置 1 2 0 は、当該データを、表示装置に表示する。

## 【 0 0 5 3 】

以上のような処理を行うことにより、機密部分を秘匿化して印刷した場合であっても、秘匿化した機密部分の内容を容易に確認することができる。

30

## 【 0 0 5 4 】

なお、ここでは、機密文書処理サーバ 1 4 0 において、復号処理部 3 3 0 によって復号された機密部分データを、文書閲覧用端末装置 1 2 0 から受け取った機密文書画像データに合成して、文書閲覧用端末装置 1 2 0 に送り返しているが、文書サーバ 1 1 0 に格納されている元の機密文書の識別情報を、二次元コードに含ませておき、機密文書処理サーバ 1 4 0 において、当該識別情報を使って、文書サーバ 1 1 0 から該当する元の機密文書を取得して、文書閲覧用端末装置 1 2 0 に送り返すようにしてもよい。この場合、元の機密文書の識別情報としては、例えば、一方向性ハッシュ関数を使用して、機密文書データから生成されるハッシュ値が用いられることが考えられる。

40

## 【 0 0 5 5 】

また、ここでは、暗号化された機密部分データとその識別情報を、機密文書処理サーバ 1 4 0 が備えるハードディスク装置に格納しているが、暗号化された機密部分データとその識別情報を、文書閲覧用端末装置 1 2 0 等に送信して、文書閲覧用端末装置 1 2 0 等が備える記憶装置（例えば、ハードディスク装置）に格納することも考えられる。更に、暗号化された機密部分データとその識別情報を、文書閲覧用端末装置 1 2 0 等に装着された CD-R、MO、USBメモリ等の可搬記録媒体に格納することも考えられる。このように機密部分データを可搬記録媒体に格納した場合は、当該可搬記録媒体を、秘匿化処理がされて出力がされた紙文書と一緒に持ち運ぶことで、一定の機密性を確保しつつ、機密文書の持ち運びをすることが可能になる。

50

## 【 0 0 5 6 】

上述した実施形態では、機密部分抽出部 2 1 0 で算出された配置情報（機密部分が配置される位置の情報）を、機密部分データに含めて、機密文書処理サーバ 1 4 0 が備えるハードディスク装置に格納しているが、当該配置情報を、二次元コードに含めるようにすることも考えられる。この場合、図 2 に示した機密部分の秘匿化処理を行う場合の機密情報処理サーバ 1 4 0 の機能構成では、機密部分抽出部 2 1 0 で算出された配置情報が、二次元コード生成部 2 5 0 に直接渡されて、機密部分データ識別情報及び復号鍵とともに二次元コードに変換される。また、図 3 に示した秘匿化処理がされて出力された紙文書等から元の機密文書を復元する場合の機密情報処理サーバ 1 4 0 の機能構成では、二次元コード抽出・復号部 3 1 0 で抽出・復号されて出力される配置情報が直接、画像合成部 3 4 0 に渡されて、画像合成時に利用される。

10

## 【 0 0 5 7 】

また、上述した実施形態では、秘匿化処理や秘匿化解除処理を、機密文書処理サーバ 1 4 0 で行っていたが、これらをすべて、文書閲覧用端末装置 1 2 0 で行うようにしてもよい。また、機密文書処理サーバ 1 4 0 で行わせていた処理の一部を、文書閲覧用端末装置 1 2 0 で行うことも考えられる。

## 【 0 0 5 8 】

図 5 は、機密文書の秘匿化処理を、文書閲覧用端末装置 1 2 0 と機密文書処理サーバ 1 4 0 とで連係して行う場合の機能構成例を示す図である。なお、同図では、図 2 に示した構成要素と同様の構成要素については、同じ参照符号を付している。

20

## 【 0 0 5 9 】

図 5 に示すように、文書閲覧用端末装置 1 2 0 は、機密部分抽出部 2 1 0 と、二次元コード生成部 2 5 0 と、秘匿化処理部 2 6 0 と、文書合成部 2 7 0 とを備える。また、機密文書処理サーバ 1 4 0 は、暗号化処理部 2 2 0 と、鍵生成部 2 2 1 と、識別情報生成部 2 3 0 と、格納処理部 2 4 0 とを備える。

## 【 0 0 6 0 】

同図に示した構成の場合、文書閲覧用端末装置 1 2 0 の画面上で機密部署の閲覧等していた利用者が、当該機密文書の印刷を文書閲覧用端末装置 1 2 0 に指示すると、文書閲覧用端末装置 1 2 0 は、機密部分抽出部 2 1 0 によって、機密文書データから、機密部分を抽出し、抽出された機密部分データを、ネットワーク 1 8 0 を介して、機密文書処理サーバ 1 4 0 に送信する。機密文書処理サーバ 1 4 0 では、ネットワーク 1 8 0 を介して、機密部分データを受信すると、暗号化処理部 2 2 0 によって、受信した機密部分データの暗号化を行う。そして、識別情報生成部 2 3 0 によって、暗号化された機密部分データを識別するための識別情報を生成し、機密部分格納処理部 2 4 0 によって、暗号化された機密部分データとその識別情報とを関連付けて、機密文書処理サーバ 1 4 0 が備えるハードディスク装置に格納する。そして、機密文書処理サーバ 1 4 0 は、識別情報生成部 2 3 0 によって生成された識別情報と、鍵生成部 2 2 1 によって生成された復号鍵を、ネットワーク 1 8 0 を介して、文書閲覧用端末装置 1 2 0 に送信する。文書閲覧用端末装置 1 2 0 は、ネットワーク 1 8 0 を介して、機密文書処理サーバ 1 4 0 から機密部分データ識別情報と復号鍵を受信すると、受信した識別情報と復号鍵を、二次元コード生成部 2 5 0 によって QR コード等の二次元コードデータに変換する。そして、当該二次元コードと、秘匿化処理部 2 6 0 によって秘匿化処理がされた機密文書データとを、文書合成部 2 7 0 によって合成し、合成結果を、プリンタ 1 3 0 で出力する。

30

40

## 【 図面の簡単な説明 】

## 【 0 0 6 1 】

【 図 1 】 本発明による文書処理システム 1 0 0 の構成を示す図である。

【 図 2 】 機密文書の秘匿化を行う際の機密文書処理サーバ 1 4 0 の機能構成を示す図である。

【 図 3 】 機密文書の秘匿化解除を行う際の機密文書処理サーバ 1 4 0 の機能構成を示す図である。

50

【図4】機密文書処理サーバ140による秘匿化処理前後の機密文書の例を示す図である。

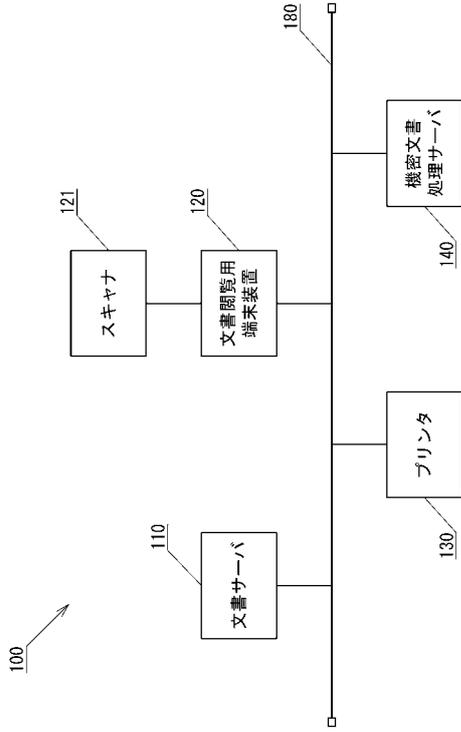
【図5】機密文書の秘匿化を連係して行う場合の文書閲覧用端末装置120と機密文書処理サーバ140の機能構成を示す図である。

【符号の説明】

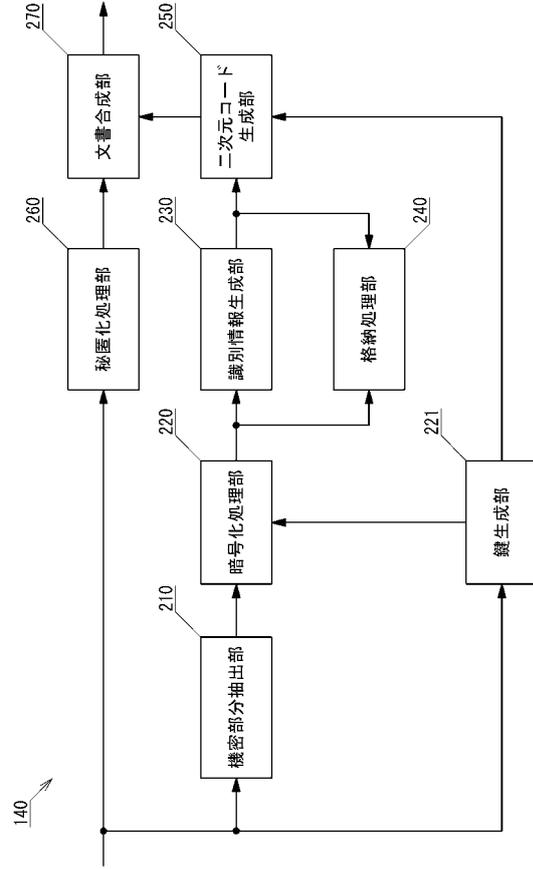
【0062】

100	文書処理システム	
110	文書サーバ	
120	文書閲覧用端末装置	
121	スキャナ	10
130	プリンタ	
140	機密文書処理サーバ	
180	ネットワーク	
210	機密部分抽出部	
220	暗号化処理部	
221	鍵生成部	
230	識別情報生成部	
240	機密部分格納処理部	
250	二次元コード生成部	
260	秘匿化処理部	20
270	文書合成部	
310	復号部	
320	機密部分データ取得部	
330	復号処理部	
340	画像合成部	
410	機密文字部分	
420	代用文字	
430	二次元コード	

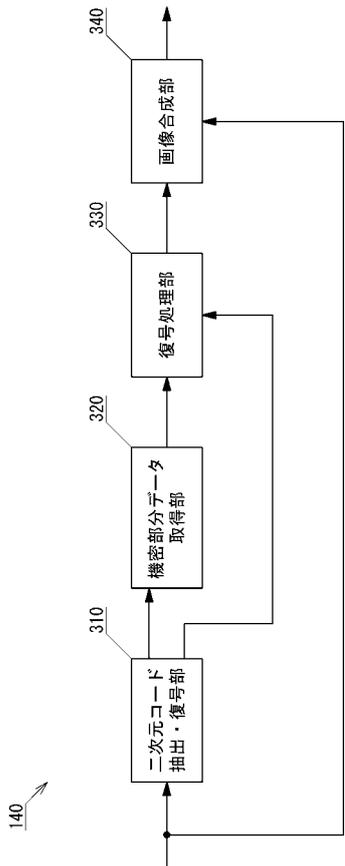
【図 1】



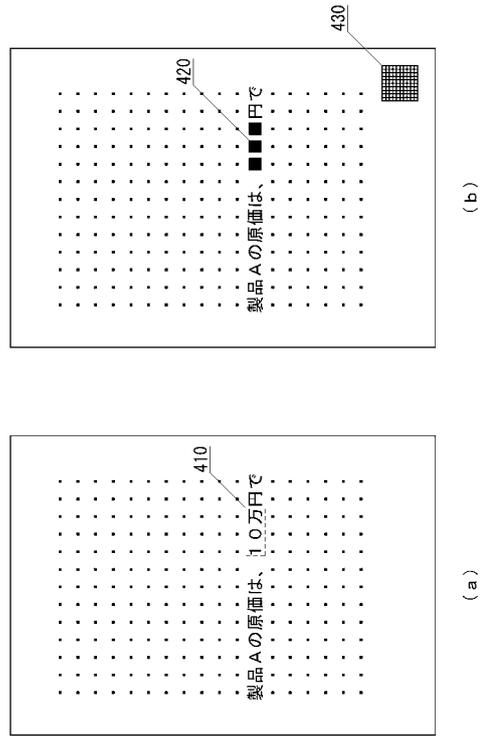
【図 2】



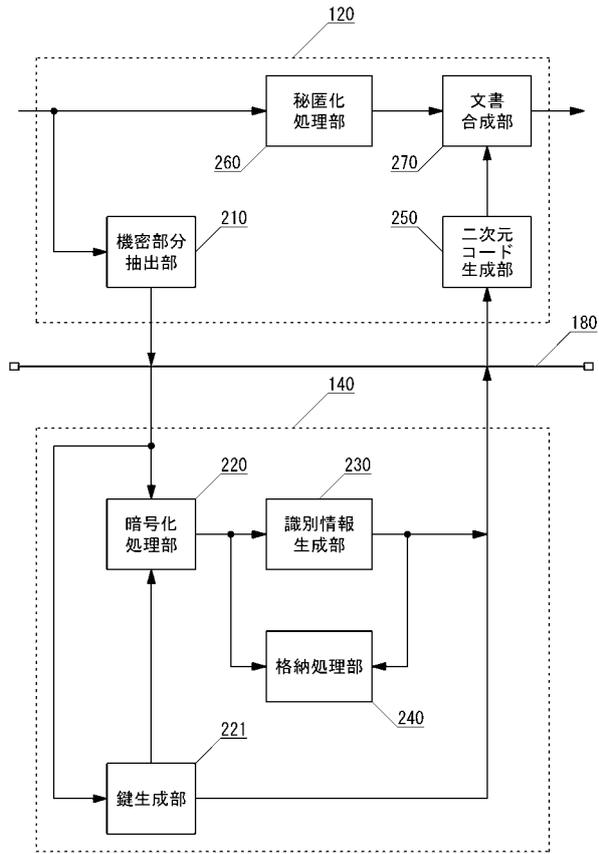
【図 3】



【図 4】



【 図 5 】



---

フロントページの続き

- (56)参考文献 特開2004-260750(JP,A)  
特開2004-058410(JP,A)  
特開2002-175169(JP,A)  
特開2003-101762(JP,A)  
特開2006-139699(JP,A)  
特開2004-151163(JP,A)  
特開平11-112950(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 9/00 - 9/32  
G06F 21/24  
G09C 1/00